# SANストレージの管理

ONTAP 9

NetApp
December 20, 2024

# 目次

# SANストレージの管理

## SANの概念

### iSCSIを使用したSANプロビジョニング

SAN環境では、ストレージシステムはストレージターゲットデバイスを含むターゲットです。iSCSIおよびFCの場合、ストレージターゲットデバイスはLUN（論理ユニット）と呼ばれます。Non-Volatile Memory Express（NVMe）over Fibre Channelでは、ストレージターゲットデバイスをネームスペースと呼びます。

iSCSIおよびFCの場合はLUNを作成するか、NVMeの場合はネームスペースを作成してストレージを構成します。LUNまたはネームスペースには、ホストからInternet Small Computer Systems Interface（iSCSI）またはFibre Channel（FC；ファイバチャネル）プロトコルネットワークを使用してアクセスします。

iSCSIネットワークに接続するために、ホストは標準のイーサネットネットワークアダプタ（NIC）、ソフトウェアイニシエータを搭載したTCPオフロードエンジン（TOE）カード、Converged Network Adapter（CNA；統合ネットワークアダプタ）、または専用のiSCSI Host Bus Adapter（HBA；ホストバスアダプタ）を使用できます。

FCネットワークに接続するには、ホストにFC HBAまたはCNAが必要です。

サポートされるFCプロトコルは次のとおりです。

- FC
- FCoE
- NVMe

#### iSCSIターゲットノードのネットワーク接続と名前

iSCSIターゲットノードは、いくつかの方法でネットワークに接続できます。

- ONTAPに統合されたソフトウェアを使用して、イーサネットインターフェイスを介して接続します。
- 複数のシステムインターフェイス上。iSCSIに使用されるインターフェイスで、SMBやNFSなどの他のプロトコルのトラフィックも転送できます。
- ユニファイドターゲットアダプタ（UTA）またはConverged Network Adapter（CNA；統合ネットワークアダプタ）を使用する。

すべてのiSCSIノードにはノード名が必要です。

iSCSI ノード名の 2 つの形式、つまり、タイプ指定子は、 _iqn と _eui _ です。SVM iSCSIターゲットでは、常にiqnタイプ指定子が使用されます。イニシエータには、iqnタイプまたはeuiタイプの指定子を使用できます。

ストレージシステムのノード名

iSCSIを実行している各SVMには、逆ドメイン名と一意のエンコード番号に基づいたデフォルトのノード名があります。

ノード名は次の形式で表示されます。

iqn.1992-08.com.netapp:sn.*unique-encoding-number*

次の例は、一意のエンコード番号を持つストレージシステムのデフォルトのノード名を示しています。

```
iqn.1992-08.com.netapp:sn.812921059e6c11e097b3123478563412:vs.6
```

#### **iSCSI**の**TCP**ポート

iSCSIプロトコルは、TCPポート番号3260を使用するようにONTAPで設定されています。

ONTAPでは、iSCSIのポート番号の変更はサポートされていません。ポート番号3260はiSCSI仕様の一部として登録されており、他のアプリケーションやサービスでは使用できません。

関連情報

"NetAppのマニュアル：「ONTAP SANホスト構成」"

## **iSCSI**サービスの管理

#### **iSCSI**サービスの管理

Storage Virtual Machine（SVM）のiSCSI論理インターフェイスでiSCSIサービスの可用性を管理するには、コマンドまたは `vserver iscsi interface disable`コマンドを使用し `vserver iscsi interface enable`ます。

デフォルトでは、iSCSIサービスはすべてのiSCSI論理インターフェイスで有効になっています。

#### ホストでの**iSCSI**の実装方法

iSCSIは、ハードウェアまたはソフトウェアを使用してホストに実装できます。

iSCSIは次のいずれかの方法で実装できます。

- ホストの標準イーサネットインターフェイスを使用するイニシエータソフトウェアを使用する。
- iSCSI Host Bus Adapter （ HBA ；ホストバスアダプタ）を使用する。ホストオペレーティングシステムでは、 iSCSI HBA をローカルディスクを搭載した SCSI ディスクアダプタとみなします。
- TCP / IP処理をオフロードするTCP Offload Engine（TOE）アダプタを使用する。

  iSCSIプロトコルの処理は、引き続きホストソフトウェアによって実行されます。

#### **iSCSI**認証の仕組み

iSCSIセッションの第1段階では、イニシエータがストレージシステムにログイン要求を送信してiSCSIセッションを開始します。ストレージシステムは、ログイン要求を許可または拒否するか、ログインが不要であると判断します。

iSCSI認証方式は次のとおりです。

- Challenge Handshake Authentication Protocol（CHAP）--イニシエータはCHAPユーザ名とパスワードを使用してログインします。

  CHAPパスワードを指定するか、16進数のシークレットパスワードを生成できます。CHAPユーザ名およびパスワードには、次の2種類があります。

  - インバウンド - ストレージシステムがイニシエータを認証します。

    CHAP認証を使用する場合は、インバウンド設定が必要です。

  - アウトバウンド - イニシエータがストレージシステムを認証できるようにするオプションの設定です。

    インバウンドユーザ名およびパスワードをストレージシステムで定義した場合にのみ、アウトバウンド設定を使用できます。

- deny --イニシエータはストレージシステムへのアクセスを拒否されます
- none --ストレージシステムはイニシエータの認証を必要としません

イニシエータとその認証方法の一覧を定義できます。このリストにないイニシエータに適用されるデフォルトの認証方法を定義することもできます。

関連情報

"Data ONTAP での Windows マルチパス・オプション：ファイバ・チャネルおよび iSCSI"

**iSCSI**イニシエータのセキュリティ管理

ONTAP は、 iSCSI イニシエータのセキュリティを管理するためのさまざまな機能を備えています。iSCSI イニシエータのリストと各イニシエータに対する認証方法の定義、認証リスト内のイニシエータと関連する認証方法の表示、認証リストに対するイニシエータの追加と削除、リストにないイニシエータに対するデフォルトの iSCSI イニシエータ認証方法の定義を行うことができます。

**iSCSI**エンドポイントの分離

ONTAP 9 .1以降では、既存のiSCSIセキュリティコマンドが拡張され、IPアドレスの範囲または複数のIPアドレスを指定できるようになりました。

すべてのiSCSIイニシエータは、ターゲットとのセッションまたは接続を確立する際に、発信元IPアドレスを提供する必要があります。この新機能は、発信元IPアドレスがサポート対象外または不明な場合にイニシエータがクラスタにログインできないようにすることで、一意の識別方式を提供します。サポート対象外または不明なIPアドレスから発信されたイニシエータではログインがiSCSIセッションレイヤで拒否されるため、イニシエータはクラスタ内のLUNまたはボリュームにアクセスできません。

既存のエントリの管理に役立つ2つの新しいコマンドを使用して、この新機能を実装します。

#### イニシエータのアドレス範囲を追加する

iSCSIイニシエータのセキュリティ管理を改善するには、IPアドレスの範囲を追加するか、コマンドを使用して複数のIPアドレスを追加し `vserver iscsi security add-initiator-address-range`ます。

```
cluster1::> vserver iscsi security add-initiator-address-range
```

#### イニシエータのアドレス範囲を削除する

IPアドレスの範囲または複数のIPアドレスを削除するには、コマンドを使用し `vserver iscsi security remove-initiator-address-range`ます。

```
cluster1::> vserver iscsi security remove-initiator-address-range
```

### CHAP認証とは

Challenge Handshake Authentication Protocol（CHAP）を使用すると、iSCSIイニシエータとターゲット間の認証された通信が可能CHAP認証を使用する場合は、イニシエータとストレージシステムの両方でCHAPユーザ名とパスワードを定義します。

iSCSIセッションの第1段階では、イニシエータがストレージシステムにログイン要求を送信してセッションを開始します。ログイン要求には、イニシエータのCHAPユーザ名とCHAPアルゴリズムが含まれます。ストレージシステムはCHAPチャレンジで応答します。イニシエータはCHAP応答を提供します。ストレージシステムは応答を検証し、イニシエータを認証します。CHAPパスワードは、応答の計算に使用されます。

#### CHAP認証の使用に関するガイドライン

CHAP認証を使用する場合は、一定のガイドラインに従う必要があります。

- インバウンドユーザ名とパスワードをストレージシステムで定義する場合は、イニシエータのアウトバウンドCHAP設定にも同じユーザ名とパスワードを使用する必要があります。ストレージシステムでアウトバウンドユーザ名とパスワードも定義して双方向認証を有効にする場合は、イニシエータのインバウンドCHAP設定にも同じユーザ名とパスワードを使用する必要があります。
- ストレージシステムのインバウンド設定とアウトバウンド設定には、同じユーザ名とパスワードを使用できません。
- CHAPユーザ名には1~128バイトを指定できます。

  ユーザ名をnullにすることはできません。

- CHAPパスワード（secrets）には1~512バイトを指定できます。

  パスワードには、16進数の値または文字列を使用できます。16 進数値を使用する場合は、プレフィックス「 0x 」または「 0X 」を付けた値を入力する必要があります。パスワードをnullにすることはできません。

ONTAPでは'CHAPパスワード（シークレット）に特殊文字'英語以外の文字'数字'およびスペースを使用できますただし、これはホストの制限の対象となります。これらのいずれかが特定のホストで許可されていない場合、それらを使用することはできません。

たとえば、Microsoft iSCSIソフトウェアイニシエータでは、IPsec暗号化を使用しない場合、イニシエータとターゲットの両方のCHAPパスワードを12バイト以上にする必要があります。パスワードの最大長は、IPsecが使用されているかどうかに関係なく16バイトです。

その他の制限事項については、イニシエータのマニュアルを参照してください。

**iSCSI**インターフェイスアクセスリストを使用したイニシエータインターフェイスの制限によるパフォーマンスとセキュリティの向上

iSCSI インターフェイスアクセスリストを使用して、イニシエータがアクセスできる SVM 内の LIF の数を制限できます。これにより、パフォーマンスとセキュリティが向上します。

イニシエータがiSCSIコマンドを使用して検出セッションを開始すると、アクセスリストにあるLIF（ネットワークインターフェイス）に関連付けられたIPアドレスがイニシエータ `SendTargets`に渡されます。デフォルトでは、すべてのイニシエータが SVM 内のすべての iSCSI LIF にアクセスできます。アクセスリストを使用すると、イニシエータがアクセスできる SVM 内の LIF の数を制限できます。

**Internet Storage Name Service（iSNS）**

Internet Storage Name Service（iSNS）は、TCP / IPストレージネットワーク上のiSCSIデバイスの自動検出と管理を可能にするプロトコルです。iSNSサーバでは、ネットワーク上でアクティブなiSCSIデバイスに関する情報（IPアドレス、iSCSIノード名IQN、ポータルグループなど）が維持されます。

iSNSサーバはサードパーティベンダーから入手できます。ネットワーク内に iSNS サーバがあり、イニシエータとターゲットで使用するように設定および有効化されている場合、 Storage Virtual Machine （ SVM ）の管理 LIF を使用して、その SVM のすべての iSCSI LIF を iSNS サーバに登録できます。登録が完了すると、iSCSI イニシエータは iSNS サーバを照会して、その SVM のすべての LIF を検出できるようになります。

iSNSサービスを使用する場合は、Storage Virtual Machine（SVM）をInternet Storage Name Service（iSNS）サーバに適切に登録する必要があります。

ネットワークにiSNSサーバがない場合は、各ターゲットがホストから認識できるように手動で設定する必要があります。

**iSNS**サーバの機能

iSNSサーバは、Internet Storage Name Service（iSNS）プロトコルを使用して、ネットワーク上のアクティブなiSCSIデバイスに関する情報（IPアドレス、iSCSIノード名（IQN）、ポータルグループなど）を維持します。

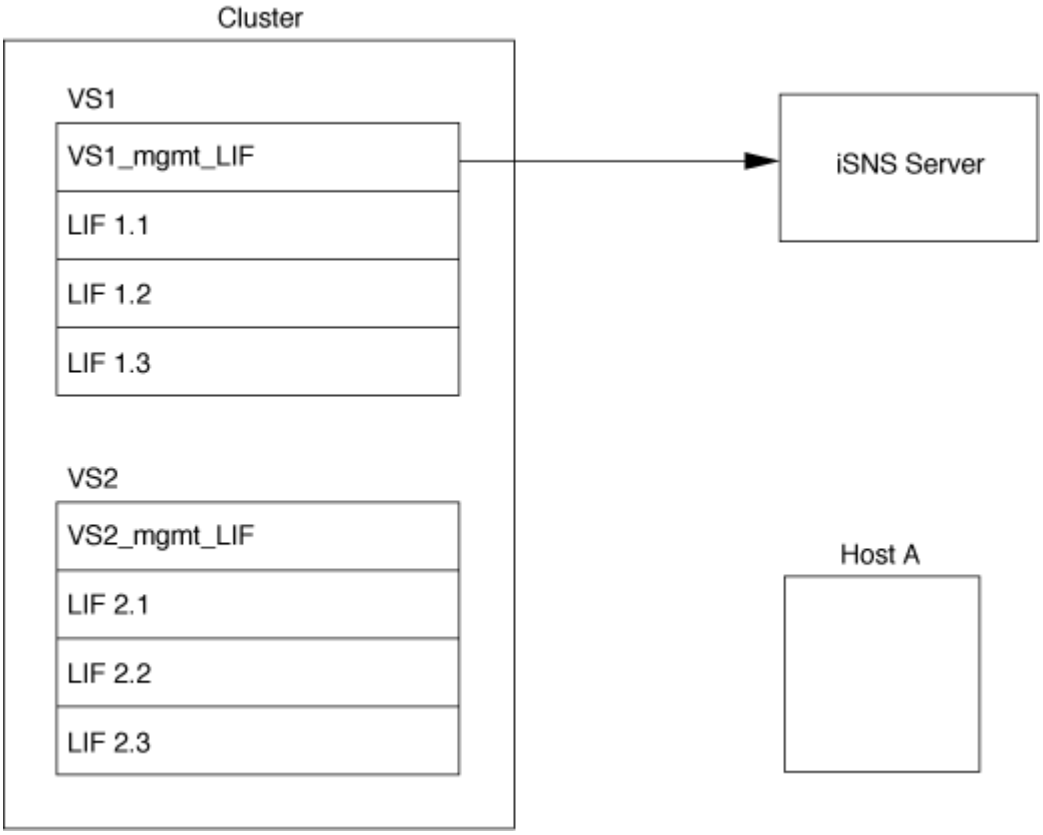
iSNSプロトコルを使用すると、IPストレージネットワーク上のiSCSIデバイスの自動検出と管理が可能になります。iSCSIイニシエータは、iSNSサーバに照会してiSCSIターゲットデバイスを検出できます。

NetAppでは、iSNSサーバの提供や再販は行われません。これらのサーバは、NetAppでサポートされているベンダーから入手できます。

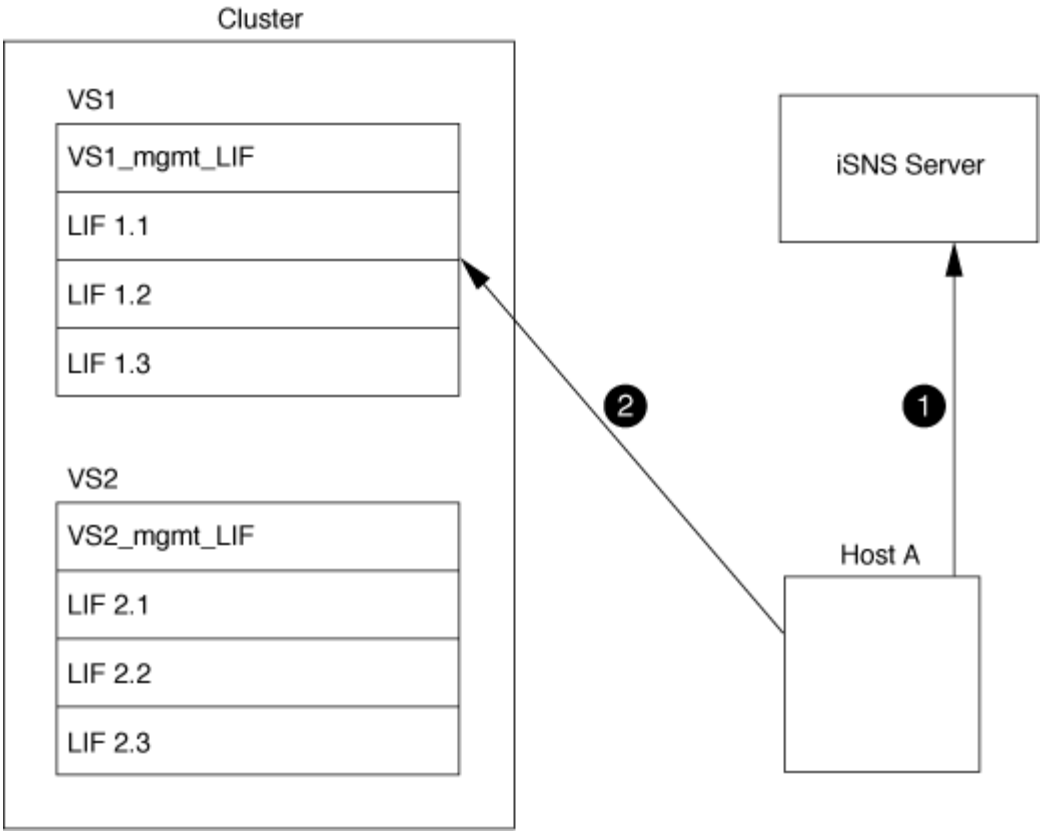
**SVM**と**iSNS**サーバの連動

iSNS サーバは、 Storage Virtual Machine （ SVM ）の管理 LIF を介して各 SVM と通信します。管理 LIF は、特定の SVM のすべての iSCSI ターゲットのノード名、エイリアス、およびポータル情報を iSNS サーバに登録します。

次の例では、SVM「VS1」はSVM管理LIF「VS1_mgmt_LIF'」を使用してiSNSサーバに登録しています。iSNS に登録中、 SVM はすべての iSCSI LIF を SVM 管理 LIF を介して iSNS サーバに送信します。iSNSの登録が完了すると、iSNSサーバには「VS1」でiSCSIを提供するすべてのLIFのリストが格納されます。クラスタに複数のSVMが含まれている場合は、iSNSサービスを使用するために、各SVMを個別にiSNSサーバに登録する必要があります。




次の例では、iSNSサーバによるターゲットへの登録が完了すると、ホストAがiSNSサーバを介して「VS1」のすべてのLIFを検出できるようになります（手順1を参照）。ホストAが「VS1」のLIFの検出を完了すると、ホストAは「VS1」の任意のLIFとの接続を確立できます（手順2を参照）。「VS2」の管理LIF「VS2_mgmt_LIF」がiSNSサーバに登録されるまで、ホストAは「VS2」内のLIFを認識しません。




ただし、インターフェイスアクセスリストを定義した場合、ホストはインターフェイスアクセスリストに定義されているLIFのみを使用してターゲットにアクセスできます。

一度 iSNS が設定されると、 SVM の設定を変更するたびに ONTAP によって iSNS サーバが自動的に更新されます。

設定を変更してからONTAPからiSNSサーバに更新情報が送信されるまでには、数分程度の遅れが生じる可能性があります。iSNSサーバのiSNS情報を強制的に更新します。 `vserver iscsi isns update`

#### **iSNS**の管理用コマンド

ONTAPには、iSNSサービスを管理するためのコマンドが用意されています。

| 状況 | 使用するコマンド |
| --- | --- |
| iSNSサービスを設定する | `vserver iscsi isns create` |
| iSNSサービスを開始する | `vserver iscsi isns start` |
| iSNSサービスを変更する | `vserver iscsi isns modify` |
| iSNSサービス設定を表示します。 | `vserver iscsi isns show` |
| 登録済みのiSNS情報を強制的に更新します。 | `vserver iscsi isns update` |

| | |
|---|---|
| iSNSサービスを停止する | `vserver iscsi isns stop` |
| iSNSサービスを削除する | `vserver iscsi isns delete` |
| コマンドのマニュアルページを表示する | `man command name` |

詳細については、各コマンドのマニュアルページを参照してください。

# FCを使用したSANプロビジョニング

ONTAP で FC SAN を実装する方法について理解する際に必要となる重要な概念について説明します。

## FCターゲットノードをネットワークに接続する方法

ストレージシステムとホストにはアダプタが搭載されているため、ケーブルを使用してFCスイッチに接続できます。

ノードを FC SAN に接続すると、各 SVM の LIF の World Wide Port Name （ WWPN ；ワールドワイドポート名）がスイッチのファブリックネームサービスに登録されます。SVM の WWNN と各 LIF の WWPN は、ONTAP によって自動的に割り当てられます。

FCを使用してホストからノードに直接接続することはできません。NPIVが必要なため、スイッチを使用する必要があります。iSCSIセッションでは、通信はネットワークルーティングされた接続または直接接続された接続で機能します。ただし、これらの方法はどちらもONTAPでサポートされています。

## FCノードの識別方法

FCが設定された各SVMは、World Wide Node Name（WWNN；ワールドワイドノード名）で識別されます。

## WWPNの使用方法

WWPN により、 FC をサポートするように設定されている SVM 内の各 LIF が識別されます。これらのLIFは、クラスタ内の各ノードの物理FCポート（ノードでFCまたはFCoEとして設定されたFCターゲットカード、UTA、UTA2）を使用します。

- igroupの作成

  ホストのHBAのWWPNは、イニシエータグループ（igroup）の作成に使用されます。igroupは、特定のLUNへのホストアクセスの制御に使用されます。igroupを作成するには、FCネットワーク内のイニシエータの一連のWWPNを指定します。ストレージシステム上のLUNをigroupにマッピングすると、そのグループ内のすべてのイニシエータに、そのLUNへのアクセスを許可できます。ホストのWWPNがLUNにマッピングされたigroupに含まれていない場合、そのホストはLUNにアクセスできません。つまり、LUNはそのホストではディスクとして表示されません。

  また、ポートセットを作成して、特定のターゲットポートでのみLUNが認識されるようにすることもできます。ポートセットは、FCターゲットポートをグループ化したものです。igroupはポートセットにバインドできます。igroup内のすべてのホストは、ポートセット内のターゲットポートからのみLUNにアクセス

できます。

- FC LIFを一意に識別

  WWPNはFC論理インターフェイスを一意に識別します。ホストオペレーティングシステムでは、WWNNとWWPNを組み合わせて使用してSVMとFC LIFを識別します。一部のオペレーティングシステムでは、ホスト上でLUNが同じターゲットIDで表示されるようにするためにパーシスタントバインディングが必要です。

**World Wide Name**の割り当ての仕組み

WWNは、ONTAPでシーケンシャルに作成されます。ただし、ONTAPによる割り当て方法が原因で、シーケンシャルではない順序で割り当てられているように見える場合があります。

各アダプタにはWWPNとWWNNが事前に設定されていますが、ONTAPでは事前設定された値は使用されません。代わりに、ONTAPはオンボードイーサネットポートのMACアドレスに基づいて、独自のWWPNまたはWWNNを割り当てます。

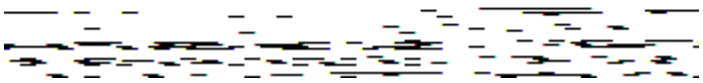
WWNが割り当て時にシーケンシャルでないように見える理由は次のとおりです。

- WWN は、クラスタ内のすべてのノードと Storage Virtual Machine （ SVM ）で一意に割り当てられます。
- 解放されたWWNはリサイクルされ、使用可能な名前のプールに再び追加されます。

**FC**スイッチの識別方法

Fibre Channelスイッチには、デバイス自体に1つのWorld Wide Node Name（WWNN；ワールドワイドノード名）、デバイスの各ポートに1つのWorld Wide Port Name（WWPN；ワールドワイドポート名）があります。

たとえば、次の図は、16ポートBrocadeスイッチの各ポートにWWPNがどのように割り当てられているかを示しています。特定のスイッチのポート番号の詳細については、そのスイッチに対応するベンダー提供のマニュアルを参照してください。



ポート* 0 *、WWPN 20： **00** ：00：60：69：51：06：b4

ポート * 1 * 、 WWPN 20 ： **01** 00 ： 60 ： 69 ： 51 ： 06 ： b4

ポート * 14 * 、 WWPN 20 ： **0e** ： 00 ： 60 ： 69 ： 51 ： 06 ： B4

ポート * 15 * 、 WWPN 20 ： **0f** ： 00 ： 60 ： 69 ： 51 ： 06 ： B4

## **NVMe**を使用した**SAN**プロビジョニング

SAN.4以降では、ONTAP 9環境でNVMe/FCがサポートされます。NVMe/FCでは、FCお

よびiSCSIでLUNをプロビジョニングしてigroupにマッピングするのと同じように、ネームスペースとサブシステムをプロビジョニングし、ネームスペースをサブシステムにマッピングできます。

NVMeネームスペースは、論理ブロックにフォーマット可能な不揮発性メモリの容量です。ネームスペースはFCプロトコルやiSCSIプロトコルのLUNに相当し、NVMeサブシステムはigroupに相当します。NVMeサブシステムはイニシエータに関連付けることができます。これにより、サブシステム内のネームスペースに関連付けられたイニシエータがアクセスできるようになります。

NVMeネームスペースは機能に似ていますが、LUNでサポートされるすべての機能がサポートされるわけではありません。

ONTAP 9 .5以降では、NVMeによるホスト側のデータアクセスをサポートするにはライセンスが必要です。ONTAP 9でNVMeが有効になっている場合は、ONTAP 9にアップグレードしたあと90日間の猶予期間が与えられます。5.を使用している場合は"ONTAP One"、NVMeライセンスが含まれます。ライセンスを有効にするには、次のコマンドを使用します。

```
system license add -license-code NVMe_license_key
```

関連情報

"NetAppテクニカルレポート4684：『Implementing and Configuring Modern SANs with NVMe/FC』"

## SANホリユウム

### SANボリュームについて

ONTAPには、基本的なボリュームプロビジョニングオプションとして、シックプロビジョニング、シンプロビジョニング、セミシックプロビジョニングの3つが用意されています。各オプションでは、ボリュームスペースおよびONTAPブロック共有テクノロジのスペース要件がさまざまな方法で管理されます。これらのオプションの仕組みを理解することで、環境に最も適したオプションを選択できるようになります。

SAN LUNとNAS共有を同じFlexVol volumeに配置することは推奨されません。SAN LUN用とFlexVol NAS共有用にそれぞれ別 々 のFlexVolボリュームをプロビジョニングする必要があります。これにより、管理とレプリケーションの導入が簡易化され、Active IQ Unified Manager（旧OnCommand Unified Manager）でのFlexVolボリュームのサポート方法と同様に機能します。

#### ボリュームのシンプロビジョニング

シンプロビジョニング ボリュームは、作成時に追加のスペースが確保されません。ボリュームにデータが書き込まれるときに、書き込み処理に対応するために必要なアグリゲート内のストレージをボリュームが要求します。シンプロビジョニング ボリュームを使用する場合はアグリゲートをオーバーコミットできますが、アグリゲートの空きスペースが不足すると、必要なスペースをボリュームが確保できなくなる可能性があります。

シンプロビジョニングFlexVol volumeを作成するには、そのオプションをに `none`設定し `-space-guarantee`ます。

ボリュームのシックプロビジョニング

シックプロビジョニングは、ボリューム内のブロックにいつでも書き込むことができるように、作成時にアグリゲートから十分なストレージが確保されます。シックプロビジョニングを利用するようにボリュームを設定した場合は、ONTAPの任意のStorage Efficiency機能（圧縮や重複排除など）を使用して、さらに大容量のストレージ要件にも事前に対応できます。

シックプロビジョニングFlexVol volumeを作成するには、その（サービスレベル目標）オプションをに `thick` 設定し `-space-slo` ます。

ボリュームのセミシックプロビジョニング

セミシックプロビジョニングを利用するボリュームを作成すると、ボリューム サイズに相当するストレージスペースがアグリゲートから確保されます。ブロック共有テクノロジでブロックが使用されているためにボリュームの空きスペースが不足しそうになると、保護データ オブジェクト（Snapshotコピー、FlexCloneファイル、FlexClone LUN）が削除され、該当するオブジェクトが保持しているスペースが解放されます。上書きに必要なスペースを確保できる速度でONTAPが保護データ オブジェクトを削除できるかぎり、書き込み処理は続行されます。これは「ベストエフォート」書き込み保証と呼ばれます。

- 注： * セミシックプロビジョニングを使用するボリュームでは、次の機能はサポートされていません。
- 重複排除、圧縮、コンパクションなどのStorage Efficiencyテクノロジ
- Microsoftオフロードデータ転送（ODX）

セミシックプロビジョニングFlexVol volumeを作成するには、その（サービスレベル目標）オプションをに `semi-thick` 設定し `-space-slo` ます。

スペースリザーブファイルおよびスペースリザーブ**LUN**での使用

スペースリザーブファイルまたはスペースリザーブLUNは、ストレージの作成時にストレージが割り当てられるファイルまたはLUNです。ネットアップではこれまで、スペース・リザベーションが無効になっている LUN （スペース・リザーブなしの LUN ）を「シン・プロビジョニング LUN 」と呼んできました。

- 注意： * スペースリザーブなしのファイルは、一般的に「シンプロビジョニングされたファイル」とは呼ばれません。

次の表に、スペースリザーブファイルおよびスペースリザーブLUNで使用できる3つのボリュームプロビジョニングオプションの主な違いを示します。

| ボリュームのプロビジョニング | **LUN/file** のスペースリザベーション | 上書き | 保護データ [2] | ストレージ効率 [3] |
|---|---|---|---|---|
| シック | サポート対象 | 保証された ^1 | 保証 | サポート対象 |
| シン | 効果なし | なし | 保証 | サポート対象 |
| セミシック | サポート対象 | ベストエフォート ^1 ^ | ベストエフォート | サポート対象外 |

- メモ *

1. 上書きを保証したり、ベストエフォートで上書きを保証できるようにするには、LUNまたはファイルでスペースリザベーションが有効になっている必要があります。
2. 保護データには、Snapshotコピー、自動削除の対象としてマークされたFlexCloneファイルとLUN（バックアップクローン）が含まれます。
3. Storage Efficiencyには、重複排除、圧縮、自動削除の対象としてマークされていないFlexCloneファイルとLUN（アクティブクローン）、およびFlexCloneサブファイル（コピーオフロードに使用）が含まれます。

**SCSI**シンプロビジョニング**LUN**のサポート

ONTAPは、T10 SCSIシンプロビジョニングLUNとNetAppシンプロビジョニングLUNをサポートしています。T10 SCSIシンプロビジョニングを使用すると、ホストアプリケーションは、ブロック環境向けのLUNのスペース再生機能やスペース監視機能などのSCSI機能をサポートできます。T10 SCSIシンプロビジョニングがSCSIホストソフトウェアでサポートされている必要があります。

LUNのT10シンプロビジョニングのサポートを有効または無効にするには、ONTAP設定を使用し `space-allocation`ます。ONTAPの設定を使用し `space-allocation enable`て、LUNでT10 SCSIシンプロビジョニングを有効にします。

`[-space-allocation {enabled|disabled}]`の T10シンプロビジョニングのサポートを有効または無効にする方法、およびLUNでT10 SCSIシンプロビジョニングを有効にする方法の詳細については、『ONTAPコマンドリファレンスマニュアル』のコマンドを参照してください。

"ONTAPコマンド リファレンス"

ボリュームプロビジョニングオプションの設定

## ボリュームにシンプロビジョニング、シックプロビジョニング、またはセミシックプロビジョニングを設定できます。

タスクの内容

このオプションをに `thick`設定する `-space-slo`と、次の処理が実行されます。

- ボリューム全体がアグリゲートに事前に割り当てられます。コマンドまたは `volume modify`コマンドを使用してボリュームのオプションを設定する `-space-guarantee`ことはできません `volume create`。
- 上書きに必要なスペースの100%がリザーブされます。コマンドを使用してボリュームのオプションを設定する `-fractional-reserve`ことはできません。 `volume modify`

このオプションをに `semi-thick`設定する `-space-slo`と、次の処理が実行されます。

- ボリューム全体がアグリゲートに事前に割り当てられます。コマンドまたは `volume modify`コマンドを使用してボリュームのオプションを設定する `-space-guarantee`ことはできません `volume create`。
- スペースは上書き用にリザーブされません。コマンドを使用して、ボリュームのオプションを設定 `-fractional-reserve`できます `volume modify`。

- Snapshot コピーの自動削除が有効になります。

ステップ

1. ボリュームのプロビジョニングオプションを設定します。

   ```
   volume create -vserver vserver_name -volume volume_name -aggregate
   aggregate_name -space-slo none|thick|semi-thick -space-guarantee none|volume
   ```

   AFFシステムおよびAFF以外のDPボリュームでは、この `-space-guarantee`オプションのデフォルトはです `none`。それ以外の場合は、デフォルトでになり `volume`ます。既存のFlexVolボリュームの場合は、コマンドを使用し `volume modify`てプロビジョニングオプションを設定します。

   次のコマンドを使うと、 SVM vs1 上の vol1 にシンプロビジョニングが設定されます。

   ```
   cluster1::> volume create –vserver vs1 -volume vol1 -space-guarantee
   none
   ```

   次のコマンドを使うと、 SVM vs1 上の vol1 にシックプロビジョニングが設定されます。

   ```
   cluster1::> volume create –vserver vs1 -volume vol1 -space-slo thick
   ```

   次のコマンドを使うと、 SVM vs1 上の vol1 にセミシックプロビジョニングが設定されます。

   ```
   cluster1::> volume create –vserver vs1 -volume vol1 -space-slo semi-
   thick
   ```

**SAN**ボリュームの構成オプション

## LUNを含むボリュームにさまざまなオプションを設定する必要があります。ボリュームオプションの設定方法によって、ボリューム内のLUNで使用できるスペースの量が決まります。

自動拡張

自動拡張は有効または無効にすることができます。有効にすると、ONTAPでボリュームのサイズを事前に設定した最大サイズまで自動的に拡張できます。ボリュームの自動拡張をサポートするには、使用可能なスペースを包含アグリゲートに確保する必要があります。そのため、自動拡張を有効にする場合は、包含アグリゲートの空きスペースを監視し、必要に応じて追加してください。

自動拡張をトリガーしてSnapshotの作成をサポートすることはできません。自動拡張が有効になっていても、ボリュームに十分なスペースがないとSnapshotの作成は失敗します。

自動拡張が無効な場合、ボリュームのサイズに変更はありません。

自動縮小

自動縮小は有効または無効にすることができます。有効にすると、ボリュームで消費されるスペースの量が事前に設定したしきい値を下回った場合に、ONTAPでボリューム全体のサイズを自動的に縮小できます。これにより、ボリュームで未使用の空きスペースの自動的な解放が開始されて、ストレージ効率が向上します。

**Snapshot**の自動削除

Snapshotの自動削除では、次のいずれかの状況が発生すると、Snapshotコピーが自動的に削除されます。

- ボリュームがフルに近い状態の場合
- Snapshotリザーブスペースがほぼフルです。
- オーバーライトリザーブスペースがフルです。

古いものから新しいもの、または新しいものから順にSnapshotコピーを削除するようにSnapshotの自動削除を設定できます。Snapshotの自動削除では、クローンボリュームまたはLUN内のSnapshotコピーにリンクされているSnapshotコピーは削除されません。

自動拡張とSnapshotの自動削除の両方が有効になっている場合にボリュームで追加のスペースが必要になると、デフォルトでは、ONTAPは最初に自動拡張をトリガーして、必要なスペースを確保しようとします。自動拡張で十分なスペースが確保されない場合は、Snapshotの自動削除がトリガーされます。

**Snapshot**リザーブ

Snapshotリザーブは、Snapshotコピー用にリザーブされるボリューム内のスペースの量を定義します。Snapshotリザーブに割り当てられたスペースを他の目的に使用することはできません。Snapshotリザーブ用に割り当てられたすべてのスペースが使用されると、Snapshotコピーはボリューム上の追加スペースを消費し始めます。

**SAN**環境でのボリューム移動に関する要件

LUN またはネームスペースを含むボリュームを移動する場合は、一定の要件を満たす必要があります。

- ボリュームに 1 つ以上の LUN が含まれている場合は、クラスタ内の各ノードに接続する LUN （ LIF ）ごとに少なくとも 2 つのパスが必要です。

  これにより、単一点障害（Single Point of Failure）が排除され、コンポーネント障害からシステムを保護できます。

- ボリュームにネームスペースが含まれている場合は、クラスタで ONTAP 9.6 以降が実行されている必要があります。

  ボリューム移動は、ONTAP 9を実行するNVMe構成ではサポートされません。5.

フラクショナルリザーブの設定に関する考慮事項

フラクショナルリザーブは、 _lun overwrite reserve _ とも呼ばれ、 FlexVol ボリューム内のスペースリザーブ LUN およびファイルのオーバーライトリザーブを無効にすることができます。これはストレージ利用率を最大限に高めるのに役立ちますが、スペース不

足による書き込み処理の失敗が悪影響を及ぼす環境では、この構成に伴う要件を理解しておく必要があります。

フラクショナルリザーブ設定はパーセンテージで表され、有効な値は `0`と `100`パーセントのみです。フラクショナルリザーブ設定はボリュームの属性です。

フラクショナルリザーブを設定して `0`ストレージ利用率を高めます。ただし、ボリュームの空きスペースがなくなると、ボリュームギャランティがに設定されていても、ボリュームに格納されたデータにアクセスするアプリケーションでデータを利用できなくなる可能性があります `volume`。ただし、ボリュームを適切に構成して使用すれば、書き込みが失敗する可能性を最小限に抑えることができます。 `0`次の要件の_all_が満たされている場合、ONTAPはフラクショナルリザーブがに設定されたボリュームに対して「ベストエフォート」書き込み保証を提供します。

- 重複排除を使用していない
- 圧縮を使用していない
- FlexCloneサブファイルは使用されていません
- すべてのFlexCloneファイルとFlexClone LUNで自動削除が有効になっている

  これはデフォルト設定ではありません。FlexCloneファイルやFlexClone LUNの自動削除は、作成時に設定するか作成後に変更して明示的に有効にする必要があります。

- ODXコピー オフロードとFlexCloneコピー オフロードを使用していない
- ボリュームギャランティがに設定されている `volume`
- ファイルまたはLUNのスペースリザベーション： `enabled`
- ボリュームのSnapshotリザーブの設定： `0`
- ボリュームのSnapshotコピーの自動削除は `enabled`、コミットメントレベルが、 `destroy`削除リストが、 `lun_clone,vol_clone,cifs_share,file_clone,sfsr`トリガーが `volume`

  この設定では、必要に応じてFlexCloneファイルとFlexClone LUNも削除されます。

変更率が高いと、上記の必要な設定をすべて行っていても、まれに Snapshot コピーの自動削除が追いつかなくなり、ボリュームのスペースが不足することがあります。

また、必要に応じてボリュームの自動拡張機能を使用することで、ボリュームのSnapshotコピーが自動的に削除される可能性を減らすことができます。自動拡張機能を有効にする場合は、関連付けられたアグリゲートの空きスペースを監視する必要があります。アグリゲートの空きスペースがなくなり、ボリュームを拡張できなくなると、ボリュームの空きスペースがなくなったときに削除されるSnapshotコピーが増える可能性があります。

上記の設定要件をすべて満たすことができず、ボリュームのスペース不足を防ぐ必要がある場合は、ボリュームのフラクショナルリザーブ設定をに設定する必要があります `100`。これにより、事前に確保する必要がある空きスペースは増えますが、上記のテクノロジを使用する場合でもデータ変更処理が確実に実行されるようになります。

フラクショナル リザーブ設定のデフォルト値と有効値は、ボリュームのギャランティによって異なります。

| ボリュームギャランティ | デフォルトのフラクショナルリザーブ | 有効な値 |
| --- | --- | --- |
| ボリューム | 100 | 0、100 |
| なし | 0 | 0、100 |

## SANホスト側のスペース管理

シンプロビジョニング環境では、ホストファイルシステムで解放されたスペースをストレージシステムから管理するプロセスを、ホスト側のスペース管理によって実行します。

ホストファイルシステムには、新しいデータの格納に使用できるブロックと、上書きしてはならない有効なデータが含まれているブロックを追跡するためのメタデータが含まれています。このメタデータはLUNまたはネームスペース内に格納されます。ホストファイルシステムでファイルが削除されると、ファイルシステムのメタデータが更新され、そのファイルのブロックが空きスペースとしてマークされます。ファイルシステム内の合計空きスペースが再計算され、新しく解放されたブロック分のスペースが組み入れられます。一方、ストレージ システム側では、こうしたメタデータの更新が、ホストによって実行される他の書き込みとまったく相違ないものとして認識されます。このため、ストレージ システム側では、削除が行われた事実が検知されません。

その結果、ホスト側と基盤のストレージ システム側で報告される空きスペース容量に不一致が生じます。たとえば、新しくプロビジョニングされた200GBのLUNがストレージ システムによってホストに割り当てられているとします。この場合、ホストとストレージ システムの双方で、200GBの空きスペースが報告されます。ここでホストに100GBのデータが書き込まれた場合、この時点では、ホストもストレージ システムも、使用済みスペースが100GB、未使用スペースが100GBと報告します。

次に、ホストから50GBのデータが削除されました。このとき、ホスト側では使用済みスペースが50GB、未使用スペースが150GBであると報告されます。一方、ストレージ システム側で報告される数値は、依然として使用済みスペース100GB、未使用スペース100GBとなります。

ホスト側のスペース管理では、さまざまな方法を使用して、ホストとストレージ システム間のスペースの差分を調整します。

### SnapCenterによるホスト管理の簡易化

SnapCenterソフトウェアを使用すると、iSCSIストレージやFCストレージに関連する管理作業とデータ保護作業を簡単に行うことができます。SnapCenterは、WindowsとUNIXホストに対応するオプションの管理パッケージです。

SnapCenterソフトウェアを使用すると、複数のストレージ システムに分散されたストレージ プールから簡単に仮想ディスクを作成することができます。また、ストレージのプロビジョニング タスクを自動化し、ホスト データと整合性のあるSnapshotコピーおよびそのクローンの作成プロセスを簡易化できます。

の詳細については、NetAppの製品ドキュメントを参照してください "SnapCenter"。

関連リンク

"SANプロトコルのONTAPスペース割り当てを有効にする"

## igroupについて

イニシエータグループ（igroup）は、FCプロトコルホストWWPNまたはiSCSIホストノード名のテーブルです。igroupを定義してLUNにマッピングすることで、どのイニシエータがLUNにアクセスできるかを制御できます。

通常は、ホストのすべてのイニシエータポートまたはソフトウェアイニシエータがLUNにアクセスできることが必要です。マルチパスソフトウェアを使用している場合、またはクラスタホストがある場合は、各イニシエータポートまたは各クラスタホストのソフトウェアイニシエータが同じLUNへの冗長パスを必要とします。

LUNにアクセスできるイニシエータを指定するigroupは、LUNの作成前または作成後に作成できますが、LUNをigroupにマッピングする前にigroupを作成する必要があります。

イニシエータグループには複数のイニシエータを含めることができ、複数のigroupに同じイニシエータを含めることができます。ただし、イニシエータが同じ複数のigroupに1つのLUNをマッピングすることはできません。1つのイニシエータを、ostypeが異なる複数のigroupのメンバーにすることはできません。

### igroupによるLUNアクセスの提供例

複数のigroupを作成して、ホストで使用できるLUNを定義できます。たとえば、ホストクラスタを使用している場合、複数のigroupを使用して、クラスタ内の1つのホストだけ、またはすべてのホストから特定のLUNが認識されるように設定できます。

次の表は、ストレージシステムにアクセスしている4つの異なるホストについて、4つのigroupによってLUNにアクセスできるようにする方法を示しています。クラスタ化されたホスト（Host3とHost4）は、両方とも同じigroup（group3）のメンバーであり、このigroupにマッピングされたLUNにアクセスできます。group4というigroupにはHost4のWWPNが含まれ、パートナーには表示されないローカルの情報が格納されます。

| **HBA WWPN** 、 **IQN** 、または **EUI** のホスト | **igroup** | **igroup** に追加されている **WWPN** 、 **IQN** 、 **EUI** | **igroup** にマッピングされている **LUN** |
|---|---|---|---|
| Host1、シングルパス（iSCSIソフトウェアイニシエータ）<br><br>iqn.1991-05.com.microsoft:host1 | group1 | iqn.1991-05.com.microsoft:host1 | `/vol/vol2/lun1` |
| Host2、マルチパス（HBA×2）<br><br>10:00:00:00:c9:2b:6b:3c<br><br>10:00:00:00:c9:2b:02:3c | group2 | 10:00:00:00:c9:2b:6b:3c<br><br>10:00:00:00:c9:2b:02:3c | `/vol/vol2/lun2` |

| **HBA WWPN** 、 **IQN** 、または **EUI** のホスト | **igroup** | **igroup** に追加されている **WWPN** 、 **IQN** 、 **EUI** | **igroup** にマッピングされている **LUN** |
|---|---|---|---|
| Host3、マルチパス、Host4でクラスタ構成<br><br>10:00:00:00:c9:2b:32:1b<br><br>10:00:00:00:c9:2b:41:02 | group3 | 10:00:00:00:c9:2b:32:1b<br><br>10:00:00:00:c9:2b:41:02<br><br>10:00:00:00:c9:2b:51:2c<br><br>10:00:00:00:c9:2b:47:a2 | `/vol/vol2/qtree1/lun3` |
| Host4、マルチパス、クラスタ構成（Host3には認識されない）<br><br>10:00:00:00:c9:2b:51:2c<br><br>10:00:00:00:c9:2b:47:a2 | group4 | 10:00:00:00:c9:2b:51:2c<br><br>10:00:00:00:c9:2b:47:a2 | `/vol/vol2/qtree2/lun4`<br>`/vol/vol2/qtree1/lun5` |

## igroupのイニシエータのWWPNとiSCSIノード名を指定する

イニシエータのiSCSIノード名およびWWPNは、igroupの作成時に指定することも、あとから追加することもできます。LUNの作成時にイニシエータのiSCSIノード名とWWPNを指定するように選択した場合は、必要に応じてあとで削除できます。

Host Utilitiesのマニュアルの手順に従って、WWPNを取得し、特定のホストに関連付けられているiSCSIノード名を確認します。ESXソフトウェアを実行するホストでは、Virtual Storage Consoleを使用します。

## VMwareとMicrosoftのコピーオフロードによるストレージ仮想化

### VMwareとMicrosoftのコピーオフロードによるストレージ仮想化の概要

VMwareとMicrosoftは、パフォーマンスとネットワークスループットを向上させるために、コピーオフロード処理をサポートしています。コピーオフロード機能を使用するには、VMwareとWindowsのオペレーティングシステム環境の要件を満たすようにシステムを設定する必要があります。

仮想環境でVMwareとMicrosoftのコピーオフロードを使用する場合は、LUNをアライメントする必要があります。LUNをアライメントしないと、パフォーマンスが低下する可能性があります。

#### 仮想SAN環境を使用する利点

Storage Virtual Machine（SVM）とLIFを使用して仮想環境を作成すると、SAN環境をクラスタ内のすべてのノードに拡張できます。

- 分散管理

  SVM内の任意のノードにログインして、クラスタ内のすべてのノードを管理できます。

- データアクセスの向上

  MPIOとALUAを使用すると、SVMのすべてのアクティブなiSCSI LIFまたはFC LIFを介してデータにアクセスできます。

- LUNアクセスの制御

  SLMとポートセットを使用すると、イニシエータがLUNへのアクセスに使用できるLIFを制限できます。

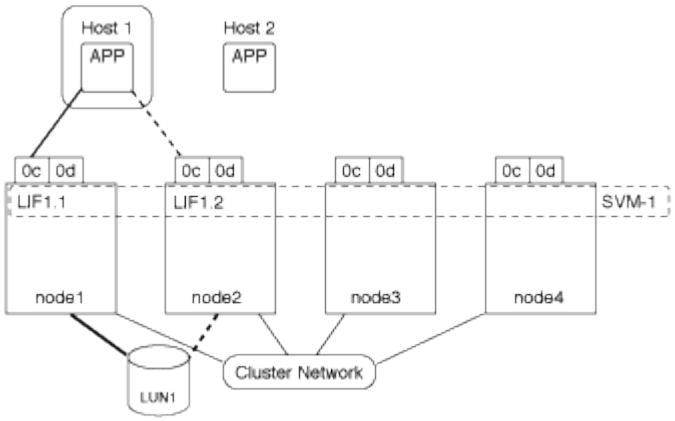
仮想環境での**LUN**へのアクセスの仕組み

## 仮想環境では、ホスト（クライアント）は LIF を使用して、最適パスおよび非最適パス経由で LUN にアクセスします。

LIF は、 SVM を物理ポートに接続する論理インターフェイスです。複数のSVMが同じポート上に複数のLIFを設定できますが、1つのLIFは1つのSVMに属します。LUNには、SVMのLIFを介してアクセスできます。

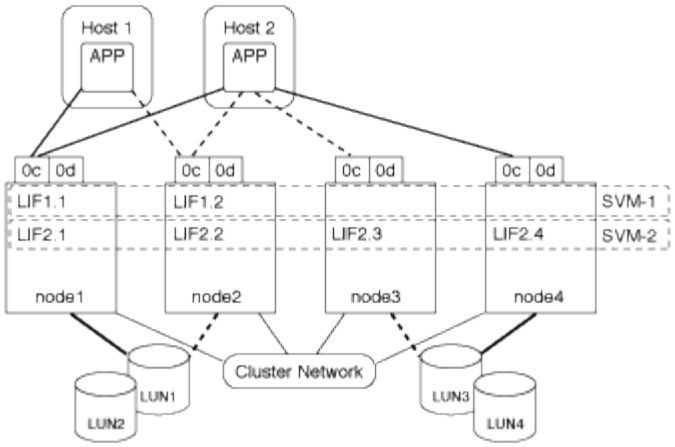
クラスタ内の**1**つの**SVM**を使用した**LUN**へのアクセス例

次の例では、ホスト1がSVM-1のLIF1.1とLIF1.2に接続してLUN1にアクセスします。LIF1.1 は物理ポート node1 ： 0c を、 LIF1.2 は node2 ： 0c を使用します。LIF1.1 と LIF1.2 は SVM-1 のみに属しています。SVM-1 のノード 1 またはノード 2 で新しい LUN を作成した場合は、その LUN でもこれらの同じ LIF を使用できます。新しい SVM を作成した場合は、両方のノードの物理ポート 0c または 0d を使用して新しい LIF を作成できます。



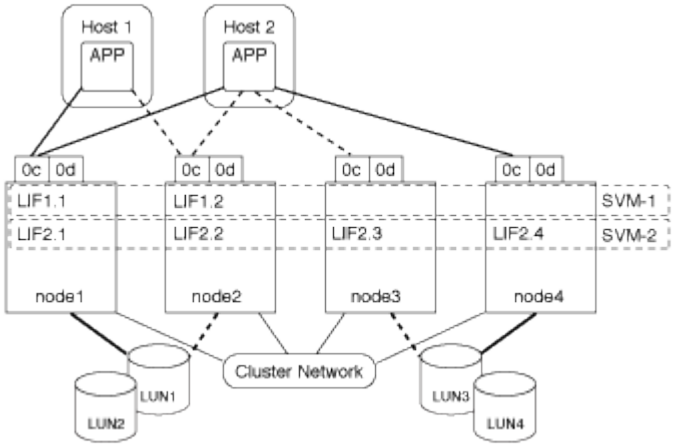

クラスタ内の複数の**SVM**を使用した**LUN**へのアクセス例

1つの物理ポートで複数のLIFをサポートし、異なるSVMを接続できます。LIF は特定の SVM に関連付けられているため、クラスタノードは受信データトラフィックを正しい SVM に送信できます。次の例では、 1~4 の各ノードに、各ノードの物理ポート 0c を使用して SVM-2 用の LIF を 1 つずつ設定しています。ホスト1はSVM-1のLIF1.1とLIF1.2に接続してLUN1にアクセスします。ホスト 2 は、 SVM-2 の LIF2.1 と LIF2.2 に接続して LUN2 にアクセスします。両方のSVMがノード1とノード2の物理ポート0cを共有しています。SVM-2 には追加の LIF があり、ホスト 2 はこの LIF を使用して LUN3 と LUN4 にアクセスします。これらの LIF はノード 3 とノード 4 の物理ポート 0c を使用します。複数のSVMでノードの物理ポートを共有できます。



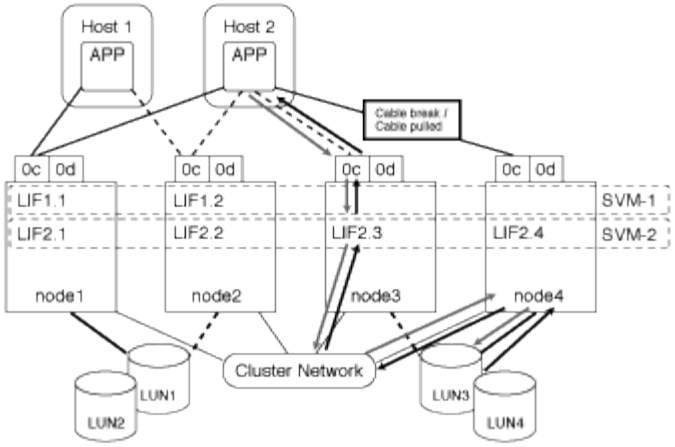

ホストシステムから**LUN**へのアクティブパスまたは最適パスの例

アクティブパスまたは最適パスでは、データトラフィックはクラスタネットワークを経由せずに、 LUN への最短ルートをとります。LUN1へのアクティブパスまたは最適パスは、物理ポート0cを使用して、ノード1のLIF1.1を経由します。ホスト 2 には、アクティブパスまたは最適パスが 2 つあります。 1 つは node1 へのパスで、 LIF2.1 は物理ポート 0c を共有し、もう 1 つは node4 、 LIF2.4 は物理ポート 0c を使用します。




ホストシステムから**LUN**へのアクティブパスまたは非最適（間接）パスの例

アクティブパスまたは非最適（間接）パスでは、データトラフィックはクラスタネットワークを経由します。この問題は、ホストからのアクティブパスまたは最適パスがすべて使用できず、トラフィックを処理できない場合にのみ発生します。ホスト 2 から SVM-2 LIF2.4 へのパスが失われた場合は、クラスタネットワークを経由して LUN3 と LUN4 にアクセスします。ホスト 2 からのアクセスには、ノード 3 の LIF2.3 が使用されます。トラフィックは、クラスタネットワークスイッチに入ったあと、 LUN3 と LUN4 にアクセスできるようノード 4 にバックアップされます。次に、クラスタネットワークスイッチ経由で逆方向に戻り、 LIF2.3 経由でホスト 2 にバックアウトされます。このアクティブパスまたは非最適パスは、 LIF2.4 へのパスがリストアされるか、ノード 4 のもう 1 つの物理ポートで SVM-2 の新しい LIF が確立されるまで使用されます。




=
:allow-uri-read:

**ESX**ホストの**VMware VAAI**パフォーマンスの向上

ONTAP では、 ESX ホストで ESX 4.1 以降が実行されている場合、 VMware vStorage APIs for Array Integration （ VAAI ）の一部の機能がサポートされます。これらの機能は、ESXホストからストレージシステムに処理をオフロードし、ネットワークスループットを向上させるのに役立ちます。これらの機能は、適切な環境でESXホストによって自動的に有効になります。

VAAI 機能は、次の SCSI コマンドをサポートします。

- `EXTENDED_COPY`

  この機能により、ホストは、データ転送の際にホストに影響を与えることなく、 LUN 間または LUN 内のデータ転送を開始できます。その結果、 ESX CPU サイクルが節約され、ネットワークスループットが増加します。拡張コピー機能は「コピーオフロード」とも呼ばれ、仮想マシンのクローニングなどで使用されます。ESX ホストからコピーオフロード機能が呼び出されると、ホストネットワークを経由せずにストレージシステム内でデータがコピーされます。コピーオフロードでは、次の方法でデータが転送されます。

  - LUN 内で組み合わせることができます
  - ボリューム内の LUN 間
  - Storage Virtual Machine （ SVM ）内の異なるボリューム上の LUN 間
  - クラスタ内の異なる SVM 上の LUN 間：この機能を呼び出すことができない場合、 ESX ホストはコピー処理の標準の読み取りコマンドと書き込みコマンドを自動的に使用します。

- `WRITE_SAME`

  この機能により、すべてゼロなどの繰り返しパターンをストレージアレイに書き込む処理がオフロードされます。この機能は、ファイルをゼロで埋める場合などに使用されます。

- `COMPARE_AND_WRITE`

  特定のファイルへの同時アクセス制限がバイパスされ、仮想マシンのブートなどの処理が高速になります。

#### VAAI 環境を使用するための要件

VAAI 機能は ESX オペレーティングシステムの一部であり、環境を正しく設定すると、 ESX ホストによって自動的に起動されます。

環境の要件は次のとおりです。

- ESX ホストで ESX 4.1 以降が実行されている必要があります。
- VMwareデータストアをホストするNetAppストレージシステムでONTAPが実行されている必要があります。
- （コピーオフロードのみ） VMware コピー操作のソースとデスティネーションの両方が同じクラスタ内の同じストレージシステムでホストされている。

> コピーオフロード機能は、現時点では、異なるストレージシステムでホストされている VMware データストア間のコピーに対応していません。

#### VAAI機能がESXでサポートされているかどうかの確認

ESX オペレーティングシステムで VAAI 機能がサポートされているかどうかを確認するには、 vSphere Client を確認するか、他の方法でホストにアクセスします。ONTAP はデフォルトで SCSI コマンドをサポートします。

ESX ホストの詳細設定を確認して、 VAAI 機能が有効になっているかどうかを確認できます。次の表に、 SCSI コマンドと対応する ESX コントロールの名前を示します。

| SCSIコマンド | ESX コントロール名（ VAAI 機能） |
|---|---|
| extended_copy の実行が可能です | `HardwareAcceleratedMove` |
| WRITE_Same | `HardwareAcceleratedInit` |
| _ と _ を比較します | `HardwareAcceleratedLocking` |

#### Microsoftオフロードデータ転送（ODX）

Microsoft Offloaded Data Transfer （ ODX ；オフロードデータ転送）は _ コピーオフロード _ とも呼ばれ、この機能を使用すると、ストレージデバイス内または互換性があるストレージデバイス間で、ホストコンピュータを介さずにデータを直接転送できます。

ONTAPでは、SMBプロトコルとSANプロトコルの両方でODXがサポートされます。

ODX以外のファイル転送では、ソースからデータが読み取られ、ネットワーク経由でホストに転送されます。ホストは、データをネットワーク経由でデスティネーションに転送します。ODXファイル転送では、ホストを経由せずに、データがソースからデスティネーションに直接コピーされます。

ODXオフロードコピーはソースとデスティネーションの間で直接実行されるため、同じボリューム内でコピーを実行するとパフォーマンスが大幅に向上します。たとえば、同じボリュームコピーのコピー時間の短縮、クライアントでのCPUとメモリの使用量の削減、ネットワークI/O帯域幅の使用量の削減などが挙げられます。複数のボリュームにコピーが存在する場合は、ホストベースのコピーに比べてパフォーマンスが大幅に向

上することはありません。

SAN環境でODXを使用できるのは、ホストとストレージシステムの両方でODXがサポートされている場合のみです。ODXをサポートしていてODXが有効になっているクライアントコンピュータでは、ファイルの移動またはコピー時にオフロードされたファイル転送が自動的かつ透過的に使用されます。ODXは、ファイルをエクスプローラでドラッグアンドドロップしたか、コマンドラインのファイルコピーコマンドを使用したか、クライアントアプリケーションによってファイルコピー要求が開始されたかに関係なく使用されます。

#### ODXの使用要件

コピーオフロードにODXを使用する場合は、ボリュームのサポートに関する考慮事項、システム要件、およびソフトウェア機能の要件を理解しておく必要があります。

ODXを使用するには、システムが次の要件を満たしている必要があります。

- ONTAP

  サポート対象のバージョンのONTAPでは、ODXが自動的に有効になります。

- 最小ソースボリューム：2GB

  最適なパフォーマンスを得るには、ソースボリュームが260GBを超えている必要があります。

- WindowsクライアントでのODXのサポート

  ODXは、Windows Server 2012以降およびWindows 8以降でサポートされます。サポートされているWindowsクライアントの最新情報については、Interoperability Matrixを参照してください。

  "NetApp Interoperability Matrix Tool"

- コピーアプリケーションによるODXのサポート

  データ転送を実行するアプリケーションでODXがサポートされている必要があります。ODXをサポートするアプリケーションの処理は次のとおりです。

  - Virtual Hard Disk （ VHD ；仮想ハードディスク）の作成および変換、 Snapshot コピーの管理、仮想マシン間でのファイルのコピーなど、 Hyper-V の管理処理
  - エクスプローラでの操作
  - Windows PowerShell の copy コマンド
  - Windows コマンドプロンプトのコピーコマンド Microsoft TechNet ライブラリに、 Windows サーバおよびクライアントでサポートされている ODX アプリケーションの詳細が記載されている。

- 圧縮されたボリュームを使用する場合は、圧縮グループサイズを8Kにする必要があります。

  32Kの圧縮グループサイズはサポートされていません。

ODXは、次のボリュームタイプでは機能しません。

- 容量が2GB未満のソースボリューム
- 読み取り専用ボリューム
- "FlexCacheホリユウム"

ODXはFlexCache元のボリュームでサポートされます。

- "セミシックプロビジョニングされたボリューム"

特殊なシステムファイル要件

qtreeで見つかったODXファイルを削除できます。テクニカルサポートから指示がないかぎり、他のODXシステムファイルは削除または変更しないでください。

ODX機能を使用すると、システムのすべてのボリュームにODXシステムファイルが存在します。これらのファイルを使用すると、ODX転送中に使用されるデータのポイントインタイム表示が可能になります。次のシステムファイルは、データのオフロード先のLUNまたはファイルを含む各ボリュームのルートレベルにあります。

- `.copy-offload`（非表示のディレクトリ）
- `.tokens`（非表示ディレクトリの下にあるファイル `.copy-offload`）

コマンドを使用すると、ODXファイルを含むqtreeを削除できます `copy-offload delete-tokens -path dir_path -node node_name`。

**ODX**のユースケース

SVMでODXを使用する前に、どのような場合にパフォーマンスを向上できるかを判断できるようにユースケースについて確認しておく必要があります。

ODXをサポートするWindowsサーバおよびクライアントでは、リモートサーバ間でデータをコピーするデフォルトの方法として、コピーオフロードが使用されます。Windowsサーバまたはクライアントで ODXがサポートされていない場合や、ODXコピーオフロードがいずれかの時点で失敗した場合、コピー処理または移動処理は、その処理の従来の読み取りと書き込みにフォールバックされます。

ODXコピーと移動の使用は次のユースケースでサポートされます。

- ボリューム内

  ソースとデスティネーションのファイルまたはLUNは、同じボリューム内にあります。

- ボリュームが異なり、ノードとSVMは同じ

  ソースとデスティネーションのファイルまたはLUNは、同じノード上の異なるボリュームにあります。データは同じSVMに所有されます。

- ボリュームとノードが異なり、SVMは同じ

  ソースとデスティネーションのファイルまたはLUNは、異なるノード上の異なるボリュームにあります。データは同じSVMに所有されます。

- SVMが異なり、ノードは同じ

  ソースとデスティネーションのファイルまたはLUNは、同じノード上の異なるボリュームにあります。データは複数のSVMに所有されます。

- SVMとノードが異なる

ソースとデスティネーションのファイルまたはLUNは、異なるノード上の異なるボリュームにあります。データは複数のSVMに所有されます。

- クラスタ間

  ソースLUNとデスティネーションLUNは、クラスタの異なるノードにある異なるボリュームにあります。これはSANでのみサポートされ、SMBでは機能しません。

その他にも、次のような特殊なユースケースがあります。

- ONTAP ODXの実装では、ODXを使用して、SMB共有とFCまたはiSCSIで接続された仮想ドライブの間でファイルをコピーできます。

  Windowsエクスプローラ、Windows CLI（PowerShell）、Hyper-V、またはODXをサポートするその他のアプリケーションでODXコピーオフロードを使用すると、SMB共有と接続されたLUNが同じクラスタにある場合に、それらの間でシームレスにファイルをコピーまたは移動できます。

- Hyper-Vでは、その他にもODXコピーオフロードのユースケースがいくつか用意されています。

  - Hyper-VでODXコピーオフロードのパススルーを使用すると、仮想ハードディスク（VHD）ファイル内またはVHDファイル間でデータをコピーしたり、同じクラスタ内のマッピングされたSMB共有と接続されたiSCSI LUNの間でデータをコピーしたりできます。

    これにより、ゲストオペレーティングシステムからのコピーを基盤となるストレージに渡すことができます。

  - 容量固定VHDを作成する場合、ODXを使用してディスクを初期化します。初期化された既知のトークンを使用してディスクを初期化します。
  - ソースとデスティネーションのストレージが同じクラスタにある場合、ODXコピーオフロードを使用して仮想マシンのストレージを移行します。

> Hyper-VでのODXコピーオフロードのパススルーのユースケースを利用するには、ゲストオペレーティングシステムでODXがサポートされている必要があります。また、ゲストオペレーティングシステムのディスクが、ODXをサポートするストレージ（SMBまたはSAN）から作成されたSCSIディスクである必要があります。ゲストオペレーティングシステムのIDEディスクは、ODXパススルーをサポートしていません。

# SAN管理

## SANプロビジョニング

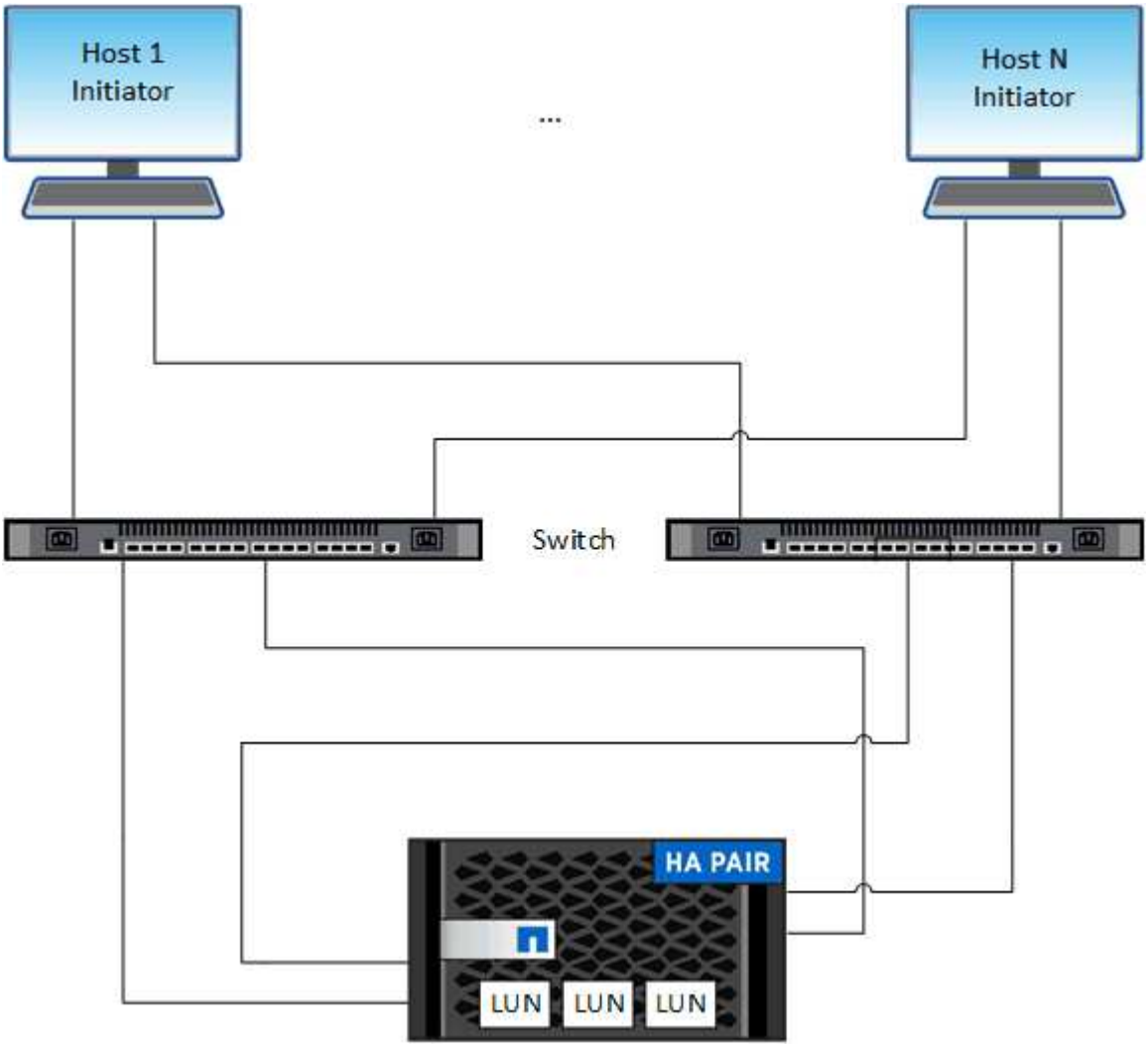
### SAN管理の概要

このセクションでは、ONTAP 9 .7以降のリリースで、ONTAPコマンドラインインターフェイス（CLI）およびSystem Managerを使用してSAN環境を構成および管理する方法について説明します。

従来のSystem Manager（ONTAP 9 .7以前でのみ使用可能）を使用している場合は、次のトピックを参照してください。

- "iSCSIプロトコル"
- "FC/FCoE プロトコル"

SAN環境では、iSCSIプロトコルとFCプロトコルを使用してストレージを提供できます。




iSCSIおよびFCでは、ストレージターゲットはLUN（論理ユニット）と呼ばれ、ホストには標準のブロックデバイスとして認識されます。LUNを作成し、イニシエータグループ（igroup）にマッピングします。イニシエータグループはFCホストのWWPSおよびiSCSIホストノード名のテーブルであり、どのイニシエータがどのLUNにアクセスできるかを制御します。

FCターゲットは、FCスイッチおよびホスト側アダプタを介してネットワークに接続し、World-Wide Port Name（WWPN）で識別されます。iSCSIターゲットは、標準のイーサネットネットワークアダプタ（NIC）、ソフトウェアイニシエータを搭載したTCPオフロードエンジン（TOE）カード、統合ネットワークアダプタ（CNA）または専用のホストバスアダプタ（HBA）を介してネットワークに接続し、iSCSI Qualified Name（IQN）で識別されます。

詳細情報

ASA R2ストレージシステム（ASA A1K、ASA A70、ASA A90）を使用している場合は、を参照してください"ASA R2ストレージシステムのドキュメント"。

**FCoE用のスイッチの設定**

# 既存のイーサネットインフラでFCサービスを実行するには、FCoE用にスイッチを設定する必要があります。

必要なもの

- SAN構成がサポートされている必要があります。

  サポートされる構成の詳細については、を参照してください "NetApp Interoperability Matrix Tool"。

- ユニファイドターゲットアダプタ（UTA）がストレージシステムにインストールされている必要があります。

  UTA2を使用する場合は、modeに設定する必要があります `cna`。

- Converged Network Adapter（CNA；統合ネットワークアダプタ）がホストにインストールされている必要があります。

手順

1. スイッチのドキュメントを参照して、FCoE用にスイッチを設定します。
2. クラスタ内の各ノードのDCB設定が正しく設定されていることを確認します。

   ```
   run -node node1 -command dcb show
   ```

   DCB設定はスイッチ上で行います。設定が正しくない場合は、スイッチのマニュアルを参照してください。

3. FCターゲットポートのオンラインステータスがのときに、FCoEログインが機能していることを確認します `true`。

   ```
   fcp adapter show -fields node,adapter,status,state,speed,fabric-
   established,physical-protocol
   ```

   FCターゲットポートのオンラインステータスがの場合は `false`、スイッチのマニュアルを参照してください。

関連情報

- "NetApp Interoperability Matrix Tool"
- "NetAppテクニカルレポート3800：『Fibre Channel over Ethernet（FCoE）End-to-End Deployment Guide』"
- "Cisco MDS 9000 NX-OSおよびSAN-OSソフトウェア構成ガイド"
- "Brocade製品"

システム要件

# LUNのセットアップでは、LUNを作成し、igroupを作成して、LUNをigroupにマッピングします。LUNをセットアップするには、システムが一定の前提条件を満たしている必要があります。

- 使用するSAN構成がサポート対象としてInteroperability Matrixで確認されている必要があります。
- SAN環境が、使用しているONTAPソフトウェアのバージョンに対応するに記載されたSANホスト数とコントローラ数の制限を満たしている必要があります "NetApp Hardware Universe"。
- サポートされているバージョンのHost Utilitiesがインストールされている必要があります。

  詳細については、Host Utilitiesのマニュアルを参照してください。

- LUNの所有者ノードと所有者ノードのHAパートナーにSAN LIFが必要です。

関連情報

- "NetApp Interoperability Matrix Tool"
- "ONTAP SANホスト構成"
- "NetAppテクニカルレポート4017：『ファイバチャネルSANのベストプラクティス』"

## LUNを作成する際の注意事項

### LUNの実際のサイズが少し異なる理由

LUNのサイズについては、次の点に注意してください。

- LUNを作成する場合、LUNの実際のサイズはLUNのOSタイプによって多少異なります。LUNの作成後にLUNのOSタイプを変更することはできません。
- 最大LUNサイズでLUNを作成する場合は、LUNの実際のサイズが若干小さくなる可能性があることに注意してください。ONTAPは、制限を切り捨ててわずかに小さくします。
- 各LUNのメタデータ用に、包含アグリゲートに約64KBのスペースが必要です。LUNの作成時には、包含アグリゲートにLUNのメタデータ用の十分なスペースがあることを確認する必要があります。アグリゲートにLUNのメタデータ用のスペースが十分にないと、一部のホストがLUNにアクセスできなくなる可能性があります。

### LUN IDの割り当てに関するガイドライン

通常、デフォルトのLUN IDは0で始まり、LUNをマッピングするたびに1ずつ割り当てられます。ホストはLUN IDをLUNの場所とパス名に関連付けます。有効なLUN ID番号の範囲はホストによって異なります。詳細については、Host Utilitiesに付属のマニュアルを参照してください。

### LUNをigroupにマッピングする場合のガイドライン

- LUNは、igroupに一度だけマッピングできます。
- ベストプラクティスとして、1つのLUNをigroupを介して1つの特定のイニシエータにのみマッピングすることを推奨します。
- 1つのイニシエータを複数のigroupに追加できますが、イニシエータをマッピングできるLUNは1つだけです。

- 同じigroupにマッピングされた2つのLUNに同じLUN IDを使用することはできません。
- igroupとポートセットには、同じプロトコルタイプを使用する必要があります。

プロトコル**FC**または**iSCSI**ライセンスを確認して追加する

FCまたはiSCSIでStorage Virtual Machine（SVM）のブロックアクセスを有効にするには、ライセンスが必要です。FCとiSCSIのライセンスはに含まれて"ONTAP One"います。

例 **1.** 手順

**System Manager**

ONTAP Oneをお持ちでない場合は、ONTAP System Manager（9.7以降）でFCまたはiSCSIのライセンスを確認して追加します。

1. System Managerで、*[クラスタ]>[設定]>[ライセンス]*を選択します
2. ライセンスが表示されない場合は、を選択し + Add てライセンスキーを入力します。
3. 「 * 追加」を選択します。

**CLI**

ONTAP Oneをお持ちでない場合は、ONTAP CLIを使用してFCまたはiSCSIのライセンスを確認して追加します。

1. FCまたはiSCSIのアクティブなライセンスがあることを確認します。

```
system license show
```

```
Package           Type    Description           Expiration
 ----------------- ------- ---------------------
--------------------
 Base              site    Cluster Base License  -
 NFS               site    NFS License           -
 CIFS              site    CIFS License          -
 iSCSI             site    iSCSI License         -
 FCP               site    FCP License           -
```

2. FCまたはiSCSIのアクティブなライセンスがない場合は、ライセンス コードを追加します。

```
license add -license-code <your_license_code>
```

# この手順では、FCまたはiSCSIプロトコルがすでに設定されている既存のStorage VMに新しいLUNを作成します。

タスクの内容

この手順は、FAS、AFF、および現在のASAシステムに適用されます。ASA R2システム（ASA A1K、ASA A70、またはASA A90）を使用し"以下の手順を実行します"ている場合は、に従ってストレージをプロビジョニングします。ASA R2システムは、SANのみのお客様に特化したシンプルなONTAPエクスペリエンスを提供します。

新しいStorage VMを作成してFCプロトコルまたはiSCSIプロトコルを設定する必要がある場合は、またはを参照してください"FC用のSVMの設定""SVMをiSCSI用に設定する"。

FCライセンスが有効になっていない場合、LIFとSVMはオンラインとして表示されますが、動作ステータスはdownになります。

LUNは、ホストにはディスク デバイスとして表示されます。

> LUNの作成時、Asymmetric Logical Unit Access（ALUA）は常に有効になります。ALUAの設定は変更できません。

イニシエータをホストするには、SVM内のすべてのFC LIFで単一イニシエータ ゾーニングを使用する必要があります。

ONTAP 9 8以降では、ストレージのプロビジョニング時にデフォルトでQoSが有効になります。プロビジョニングプロセス中またはあとで、QoSを無効にしたり、カスタムのQoSポリシーを選択したりできます。

例 **2.** 手順

**System Manager**

ONTAP System Manager（9.7以降）でFCまたはiSCSIプロトコルを使用して、SANホスト用のストレージを提供するLUNを作成します。

System Manager Classic（9.7以前で利用可能）を使用してこのタスクを実行するには、 "Red Hat Enterprise Linux向けのiSCSIの設定"

手順

1. ホストに適切なをインストールし"SANホストユーティリティ"ます。
2. System Manager で、 * Storage > LUNs * をクリックし、 * Add * をクリックします。
3. LUNの作成に必要な情報を入力します。
4. ONTAP のバージョンに応じて、「その他のオプション」をクリックすると、次のいずれかの操作を実行できます。

| オプション | 以降で使用可能 |
| --- | --- |
| • 親ボリュームではなくLUNにQoSポリシーを割り当てる<br>◦ * その他のオプション > ストレージと最適化 *<br>◦ パフォーマンスサービスレベル * を選択します。<br>◦ ボリューム全体ではなく個々の LUN に QoS ポリシーを適用するには、 * これらのパフォーマンス制限を各 LUN に適用 * を選択します。<br>デフォルトでは、パフォーマンス制限はボリュームレベルで適用されます。 | ONTAP 9 10.1 |
| • 既存のigroupを使用して新しいイニシエータグループを作成する<br>◦ * 「その他のオプション」 > 「ホスト情報」 *<br>◦ 既存のイニシエータグループを使用して新しいイニシエータグループを選択します * 。<br>他のigroupを含むigroupは、作成後にOSタイプを変更することはできません。 | ONTAP 9 .9.1 |
| • igroupまたはホストイニシエータに説明を追加する<br>この説明は、igroupまたはホストイニシエータのエイリアスとして機能します。<br>◦ * 「その他のオプション」 > 「ホスト情報」 * | ONTAP 9 .9.1 |

| | |
|---|---|
| • 既存のボリュームにLUNを作成する<br><br>デフォルトでは、新しいボリュームに新しいLUNが作成されます。<br><br>◦ * その他のオプション > LUN の追加 *<br>◦ ［ * グループ関連の LUN * ］ を選択します。 | ONTAP 9 .9.1 |
| • QoSを無効にするかカスタムQoSポリシーを選択<br><br>◦ * その他のオプション > ストレージと最適化 *<br>◦ パフォーマンスサービスレベル * を選択します。<br><br>ONTAP 9.9.1以降では、カスタムのQoSポリシーを選択した場合、指定したローカル階層への手動配置を選択することもできます。 | ONTAP 9.8 |

5. FCの場合は、FCスイッチをWWPNでゾーニングします。イニシエータごとに1つのゾーンを使用し、各ゾーンにすべてのターゲットポートを含めます。
6. ホストでLUNを検出します。

   VMware vSphereでは、Virtual Storage Console（VSC）を使用してLUNを検出、初期化してください。
7. LUNを初期化し、必要に応じてファイルシステムを作成します。
8. ホストからLUNのデータの読み取りと書き込みができることを確認します。

**CLI**

ONTAP CLIでFCまたはiSCSIプロトコルを使用して、SANホスト用のストレージを提供するLUNを作成します。

1. FCまたはiSCSIのライセンスがあることを確認します。

```
system license show
```

```
Package           Type    Description           Expiration
 ----------------- ------- ---------------------
--------------------
 Base              site    Cluster Base License  -
 NFS               site    NFS License           -
 CIFS              site    CIFS License          -
 iSCSI             site    iSCSI License         -
 FCP               site    FCP License           -
```

2. FCまたはiSCSIのライセンスがない場合は、コマンドを使用し `license add`ます。

```
license add -license-code <your_license_code>
```

3. SVMでプロトコルサービスを有効にします。

   ◦ iSCSIの場合：*

   ```
   vserver iscsi create -vserver <svm_name> -target-alias <svm_name>
   ```

   ◦ FCの場合：*

   ```
   vserver fcp create -vserver <svm_name> -status-admin up
   ```

4. 各ノードにSVM用のLIFを2つ作成します。

   ```
   network interface create -vserver <svm_name> -lif <lif_name> -role
   data -data-protocol <iscsi|fc> -home-node <node_name> -home-port
   <port_name> -address <ip_address> -netmask <netmask>
   ```

   NetAppでは、データを提供する各SVMについて、ノードごとに少なくとも1つのiSCSI LIFまたはFC LIFがサポートされます。ただし、冗長性を確保するためにはノードごとに2つのLIFが必要です。iSCSIの場合は、別々のイーサネットネットワークにあるノードごとに少なくとも2つのLIFを設定することを推奨します。

5. LIFが作成され、動作ステータスがになっていることを確認し `online`ます。

   ```
   network interface show -vserver <svm_name> <lif_name>
   ```

6. LUNを作成します。

   ```
   lun create -vserver <svm_name> -volume <volume_name> -lun <lun_name>
   -size <lun_size> -ostype linux -space-reserve <enabled|disabled>
   ```

   LUN名は255文字以内で、スペースは使用できません。

   NVFAILオプションは、ボリュームにLUNが作成されると自動的に有効になります。

7. igroupを作成します。

   ```
   igroup create -vserver <svm_name> -igroup <igroup_name> -protocol
   <fcp|iscsi|mixed> -ostype linux -initiator <initiator_name>
   ```

8. LUNをigroupにマッピングします。

```
lun mapping create -vserver <svm_name> -volume <volume_name> -lun
<lun_name> -igroup <igroup_name>
```

9. LUNが正しく設定されていることを確認します。

```
lun show -vserver <svm_name>
```

10. 必要に応じて、"ポートセットを作成してigroupにバインドします"。
11. 特定のホストでブロックアクセスを有効にするには、ホストのマニュアルの手順に従います。
12. Host Utilitiesを使用してFCまたはiSCSIマッピングを完了し、ホスト上のLUNを検出します。

関連情報

- "SANの管理の概要"
- "ONTAP SANホスト構成"
- "System ManagerでのSANイニシエータグループの表示と管理"
- "NetAppテクニカルレポート4017：『ファイバチャネルSANのベストプラクティス』"

## NVMeプロビジョニング

### NVMeの概要

SAN環境では、Non-Volatile Memory Express（NVMe）プロトコルを使用してストレージを提供できます。NVMeプロトコルは、ソリッドステートストレージのパフォーマンスを最大限に引き出すように最適化されています。

NVMeでは、ストレージターゲットをネームスペースと呼びます。NVMeネームスペースは、論理ブロックにフォーマット可能な不揮発性ストレージの容量で、ホストには標準のブロックデバイスとして提供されます。FCおよびiSCSIでLUNをプロビジョニングしてigroupにマッピングするのと同じように、ネームスペースとサブシステムを作成し、ネームスペースをサブシステムにマッピングします。

NVMeターゲットは、FCスイッチを使用する標準のFCインフラ、またはイーサネットスイッチとホスト側アダプタを使用する標準のTCPインフラを通じてネットワークに接続されます。

NVMeのサポートは、ONTAPのバージョンによって異なります。詳細は、を参照してください "NVMeのサポートと制限" 。

#### NVMeとは

Nonvolatile Memory express（NVMe）プロトコルは、不揮発性ストレージメディアへのアクセスに使用される転送プロトコルです。

NVMe over Fabrics（NVMeoF）は仕様で定義されたNVMeの拡張機能であり、PCIe以外の接続を介し

たNVMeベースの通信を可能にします。このインターフェイスを使用すると、外部ストレージエンクロージャをサーバに接続できます。

NVMeは、フラッシュテクノロジから高パフォーマンスの永続的メモリテクノロジまで、不揮発性メモリを搭載したストレージデバイスに効率的にアクセスできるように設計されています。そのため、ハードディスクドライブ用に設計されたストレージプロトコルと同じ制限はありません。フラッシュデバイスとソリッドステートデバイス（SSD）は、不揮発性メモリ（NVM）の一種です。NVMは、停電時にコンテンツを保持するメモリの一種です。NVMeは、そのメモリにアクセスできる方法です。

NVMeには、データ転送の速度、生産性、スループット、容量の向上などのメリットがあります。具体的な特徴は次のとおりです。

- 最大64、000個のキューを保持できるように設計されています。

  各キューには、最大64、000個のコマンドを同時に実行できます。

- NVMeは複数のハードウェアベンダーやソフトウェアベンダーでサポートされている
- フラッシュテクノロジによりNMVeの生産性が向上し、応答時間が短縮
- NVMe では、 SSD に送信される「検索」ごとに複数のデータ要求を行うことができます。

  NVMe は「要求」のデコードにかかる時間が短く、マルチスレッドプログラムでスレッドロックを必要としません。

- CPUレベルでのボトルネックを防止する機能をサポートし、システムの拡張に応じて並外れた拡張性を実現します。

#### **NVMe**ネームスペースについて

NVMeネームスペースは、論理ブロックにフォーマット可能な不揮発性メモリ（NVM）の容量です。ネームスペースは、Storage Virtual MachineでNVMeプロトコルが設定されている場合に使用され、FCプロトコルおよびiSCSIプロトコルのLUNに相当します。

NVMeホストには、1つ以上のネームスペースがプロビジョニングされて接続されています。各ネームスペースは、さまざまなブロックサイズをサポートできます。

NVMeプロトコルは、複数のコントローラ経由でネームスペースへのアクセスを提供します。ほとんどのオペレーティングシステムでサポートされているNVMeドライバを使用すると、ソリッドステートドライブ（SSD）ネームスペースは標準ブロックデバイスとして表示され、このデバイス上にファイルシステムやアプリケーションを変更することなく導入できます。

ネームスペースID（NSID）は、コントローラがネームスペースへのアクセスを提供するために使用する識別子です。ホストまたはホストグループのNSIDを設定する場合は、ホストからボリュームへのアクセスも設定します。論理ブロックは一度に1つのホストグループにのみマッピングでき、1つのホストグループに重複するNSIDはありません。

#### **NVMe**サブシステムについて

NVMeサブシステムには、1つ以上のNVMeコントローラ、ネームスペース、NVMサブシステムポート、NVMストレージメディア、およびコントローラとNVMストレージメディア間のインターフェイスが含まれます。作成したNVMeネームスペースは、デフォルトではサブシステムにマッピングされません。新規または既存のサブシステムにマッピングすることもできます。

関連情報

- "NVMe ストレージをプロビジョニングする"ASA、AFF、FASシステムの学習
- "NVMeネームスペースをサブシステムにマッピングする"ASA AFFおよびFASシステムについて学習します。
- "SANホストとクラウドクライアントを設定"
- "SANストレージのプロビジョニング"ASA R2（ASA A1K、ASA A70、またはASA A90）ストレージシステムの操作方法を学習します。

**NVMe**のライセンス要件

ONTAP 9 .5以降では、NVMeをサポートするにはライセンスが必要です。ONTAP 9でNVMeが有効になっている場合は、ONTAP 9にアップグレードしたあと90日間の猶予期間が与えられます。5.

ライセンスを有効にするには、次のコマンドを使用します。

```
system license add -license-code NVMe_license_key
```

**NVMe**の設定、サポート、制限事項

SAN.4以降では、ONTAP 9環境でこの"Non-Volatile Memory Express（NVMe）"プロトコルを使用できます。FC-NVMeでは、物理的なセットアップとゾーニングの手法を従来のFCネットワークと同じにしますが、FC-SCSIよりも帯域幅が広く、IOPSが高く、レイテンシが低減されます。

NVMeのサポートと制限事項は、ONTAPのバージョン、プラットフォーム、構成によって異なります。特定の設定の詳細については、を参照して"NetApp Interoperability Matrix Tool"ください。サポートされる制限については、を参照してください"Hardware Universe"。

クラスタあたりの最大ノード数は、Hardware Universeの*サポートされるプラットフォームの混在*で確認できます。

構成

- NVMe構成は、単一ファブリックまたはマルチファブリックを使用してセットアップできます。
- SANをサポートするSVMごとに管理LIFを1つ設定する必要があります。
- 組み込みブレードスイッチの場合を除き、異機種混在のFCスイッチファブリックの使用はサポートされていません。

  特定の例外については、を"NetApp Interoperability Matrix Tool"参照してください。

- カスケードファブリック、パーシャルメッシュファブリック、フルメッシュファブリック、コアエッジファブリック、およびディレクタファブリックは、FCスイッチをファブリックに接続する業界標準の方法であり、すべてサポートされます。

  ファブリックは1つまたは複数のスイッチで構成でき、ストレージコントローラは複数のスイッチに接続できます。

特徴

ONTAPのバージョンに応じて、次のNVMe機能がサポートされます。

| ONTAPバージョン | NVMeのサポート |
| --- | --- |
| 9.15.1 | • NVMe/TCPテノ4ノオトMetroCluster IPコウセイ |
| 9.14.1 | • サブシステムでのホストプライオリティの設定（ホストレベルのQoS） |
| 9.12.1 | • NVMe/FCテノ4ノオトMetroCluster IPコウセイ<br>• ONTAP 9より前のフロントエンドNVMeネットワークでは、MetroCluster構成はサポートされません。12.1.<br>• MetroCluster構成はNVMe/TCPではサポートされません。 |
| 9.10.1 | ネームスペースのサイズ変更 |
| 9.9.1 | • 同じボリューム上でのネームスペースとLUNの共存 |
| 9.8 | • プロトコルの共存<br><br>SCSI、NAS、NVMeの各プロトコルを同じStorage Virtual Machine（SVM）に共存させることができます。<br><br>ONTAP 9.8より前のバージョンでは、SVMで使用できるプロトコルはNVMeのみです。 |
| 9.6 | • ネームスペース用に512バイトブロック、4096バイトブロック<br><br>デフォルト値は4096です。512は、ホストオペレーティングシステムが4096バイトブロックをサポートしていない場合にのみ使用してください。<br><br>• ネームスペースがマッピングされたボリュームの移動 |
| 9.5 | • マルチパスHAペアのフェイルオーバー/ギブバック |

プロトコル

サポートされるNVMeプロトコルは次のとおりです。

| プロトコル | ONTAPバージョン | 許可するユーザ |
| --- | --- | --- |
| TCP | 9.10.1 | デフォルト |
| FC | 9.4 | デフォルト |

ONTAP 9 .8以降では、同じStorage Virtual Machine（SVM）にSCSI、NAS、NVMeの各プロトコルを設定できます。ONTAP 9.7以前では、SVMで使用できるプロトコルはNVMeのみです。

ネームスペース

NVMeネームスペースを使用するときは、次の点に注意してください。

- ONTAPでは、スペース再生用にNVMeを使用したNVMeデータセット管理（deallocate）コマンドはサポートされていません。
- SnapRestoreを使用してLUNからネームスペースをリストアしたり、LUNからネームスペースをリストアしたりすることはできません。
- ネームスペースのスペースギャランティは、それを含むボリュームのスペースギャランティと同じです。
- Data ONTAP 7-Modeから移行するボリュームでネームスペースを作成することはできません。
- ネームスペースでは、次のものはサポートされません。
  - 名前変更
  - ボリューム間での移動
  - ボリューム間でのコピー
  - オンデマンド コピー

その他の制限事項

**ONTAP**の次の機能は、**NVMe**構成ではサポートされません。

- SnapMirrorアクティブ同期
- Virtual Storage Console
- 永続的予約

次の考慮事項は**ONTAP 9.4**を実行しているノードだけに該当します。

- NVMe LIFとネームスペースは同じノードでホストされている必要があります。
- NVMe LIFを作成する前に、NVMeサービスを作成しておく必要があります。

関連情報

"最新SANのベストプラクティス"

**NVMe**用の**Storage VM**の設定

## ノードでNVMeプロトコルを使用する場合は、SVMをNVMe専用に設定する必要があります。

開始する前に

FCアダプタまたはイーサネットアダプタでNVMeがサポートされている必要があります。サポートされているアダプタについては、を "NetApp Hardware Universe"参照してください。

例 **3.** 手順

**System Manager**

ONTAP System Manager（9.7以降）でNVMe用のStorage VMを設定します。

| 新しい**Storage VM**に**NVMe**を設定するには | 既存の**Storage VM**に**NVMe**を設定するには |
| --- | --- |
| 1. System Managerで、* Storage > Storage VM*をクリックし、* Add *をクリックします。<br>2. Storage VMの名前を入力してください。<br>3. アクセスプロトコル*として「* nvme」を選択します。<br>4. 「* NVMe/FCを有効にする」または「* NVMe/FCを有効にする」および「*保存」を選択します。 | 1. System Manager で、 * Storage > Storage VM*をクリックします。<br>2. 設定するStorage VMをクリックします。<br>3. [設定]*タブをクリックし、NVMeプロトコルの横にあるをクリックし ます。<br>4. 「* NVMe/FCを有効にする」または「* NVMe/FCを有効にする」および「*保存」を選択します。 |

**CLI**

ONTAP CLIを使用してNVMe用のStorage VMを設定します。

1. 既存のSVMを使用しない場合は作成します。

```
vserver create -vserver <SVM_name>
```

   a. SVMが作成されたことを確認します。

```
vserver show
```

2. クラスタにNVMeまたはTCP対応アダプタがインストールされていることを確認します。

   NVMeの場合：

```
network fcp adapter show -data-protocols-supported fc-nvme
```

   TCPの場合：

```
network port show
```

3. ONTAP 9.7以前を実行している場合は、SVMからすべてのプロトコルを削除します。

```
vserver remove-protocols -vserver <SVM_name> -protocols
iscsi,fcp,nfs,cifs,ndmp
```

ONTAP 9.8以降では、NVMeを追加するときに他のプロトコルを削除する必要はありません。

4. SVMにNVMeプロトコルを追加します。

```
vserver add-protocols -vserver <SVM_name> -protocols nvme
```

5. ONTAP 9.7以前を実行している場合は、SVMで許可されているプロトコルがNVMeだけであることを確認します。

```
vserver show -vserver <SVM_name> -fields allowed-protocols
```

列にはNVMeプロトコルのみが表示されます `allowed protocols`。

6. NVMeサービスを作成します。

```
vserver nvme create -vserver <SVM_name>
```

7. NVMeサービスが作成されたことを確認します。

```
vserver nvme show -vserver <SVM_name>
```

SVMのが `Administrative Status`と表示されます `up`。

8. NVMe/FC LIFを作成します。
   - ONTAP 9 .9.1以前の場合、FC：

```
network interface create -vserver <SVM_name> -lif <lif_name>
-address <ip address> -netmask <netmask_value> -role data -data
-protocol fc-nvme -home-node <home_node> -home-port <home_port>
```

   - ONTAP 9 .10.1以降、FCまたはTCPの場合：

```
network interface create -vserver <SVM_name> -lif <lif_name>
-address <ip address> -netmask <netmask_value> -service-policy
<default-data-nvme-tcp | default-data-nvme-fc> -data-protocol
<fcp | fc-nvme | nvme-tcp> -home-node <home_node> -home-port
<home_port> -status-admin up -failover-policy disabled -firewall
-policy data -auto-revert false -failover-group <failover_group>
-is-dns-update-enabled false
```

9. HAパートナーノードにNVMe/FC LIFを作成します。

- ONTAP 9 .9.1以前の場合、FC：

```
network interface create -vserver <SVM_name> -lif <lif_name>
-role data -data-protocol fc-nvme -home-node <home_node> -home
-port <home_port>
```

- ONTAP 9 .10.1以降、FCまたはTCPの場合：

```
network interface create -vserver <SVM_name> -lif <lif_name>
-service-policy <default-data-nvme-tcp | default-data-nvme-fc>
-data-protocol <fcp | fc-nvme | nvme-tcp> -home-node <home_node>
-home-port <home_port> -status-admin up -failover-policy disabled
-firewall-policy data -auto-revert false -failover-group
<failover_group> -is-dns-update-enabled false
```

10. NVMe/FC LIFが作成されたことを確認します。

```
network interface show -vserver <SVM_name>
```

11. LIFと同じノードにボリュームを作成します。

```
vol create -vserver <SVM_name> -volume <vol_name> -aggregate
<aggregate_name> -size <volume_size>
```

auto効率化ポリシーに関する警告メッセージが表示された場合は、無視してかまいません。

**NVMe**ストレージのプロビジョニング

## 次の手順に従って、既存のStorage VMでNVMe対応ホスト用のネームスペースを作成し、ストレージをプロビジョニングします。

タスクの内容

この手順は、FAS、AFF、および現在のASAシステムに適用されます。ASA R2システム（ASA A1K、ASA A70、またはASA A90）を使用し"以下の手順を実行します"ている場合は、に従ってストレージをプロビジョニングします。ASA R2システムは、SANのみのお客様に特化したシンプルなONTAPエクスペリエンスを提供します。

ONTAP 9 8以降では、ストレージのプロビジョニング時にデフォルトでQoSが有効になります。プロビジョニングプロセス中またはあとで、QoSを無効にしたり、カスタムのQoSポリシーを選択したりできます。

開始する前に

Storage VMがNVMe用に設定されていて、FCまたはTCP転送のセットアップが完了している必要がありま

す。

**System Manager**

ONTAP System Manager（9.7以降）を使用して、NVMeプロトコルを使用してストレージを提供するネームスペースを作成します。

手順

1. System Manager で、 * Storage > NVMe 名前空間 * をクリックし、 * Add * をクリックします。

   新しいサブシステムを作成する必要がある場合は、 * その他のオプション * をクリックします。

2. ONTAP 9.8 以降を実行していて、 QoS を無効にする場合やカスタムの QoS ポリシーを選択する場合は、「その他のオプション」をクリックし、「 * ストレージおよび最適化 * 」で「 * パフォーマンスサービスレベル * 」を選択します。
3. FCスイッチをWWPNでゾーニングします。イニシエータごとに1つのゾーンを使用し、各ゾーンにすべてのターゲットポートを含めます。
4. ホストで、新しいネームスペースを検出します。
5. ネームスペースを初期化し、ファイルシステムでフォーマットします。
6. ホストがネームスペースのデータを読み書きできることを確認します。

**CLI**

ONTAP CLIを使用して、NVMeプロトコルを使用してストレージを提供するネームスペースを作成します。

この手順では、NVMeプロトコル用に設定済みの既存のStorage VMにNVMeネームスペースとサブシステムを作成し、ネームスペースをサブシステムにマッピングしてホストシステムからのデータアクセスを許可します。

Storage VMをNVMe用に設定する必要がある場合は、を参照してください"NVMe用のSVMの設定"。

手順

1. SVMがNVMe用に設定されていることを確認します。

   ```
   vserver show -vserver <svm_name> -fields allowed-protocols
   ```

   `NVMe`が列の下に表示されます `allowed-protocols`。

2. NVMeネームスペースを作成します。

   パラメータで参照するボリュームは、すでに存在している必要があります。存在していない場合は、このコマンドを実行する前にボリュームを `-path`作成する必要があります。

   ```
   vserver nvme namespace create -vserver <svm_name> -path <path> -size
   <size_of_namespace> -ostype <OS_type>
   ```

3. NVMeサブシステムを作成します。

```
vserver nvme subsystem create -vserver <svm_name> -subsystem
<name_of_subsystem> -ostype <OS_type>
```

NVMeサブシステム名では大文字と小文字が区別されます。1~96文字で指定する必要があります。特殊文字を使用できます。

4. サブシステムが作成されたことを確認します。

```
vserver nvme subsystem show -vserver <svm_name>
```

`nvme`列の下にサブシステムが表示され `Subsystem`ます。

5. ホストからNQNを取得します。
6. ホストNQNをサブシステムに追加します。

```
vserver nvme subsystem host add -vserver <svm_name> -subsystem
<subsystem_name> -host-nqn <Host_NQN>
```

7. ネームスペースをサブシステムにマッピングします。

```
vserver nvme subsystem map add -vserver <svm_name> -subsystem
<subsystem_name> -path <path>
```

ネームスペースは1つのサブシステムにのみマッピングできます。

8. ネームスペースがサブシステムにマッピングされていることを確認します。

```
vserver nvme namespace show -vserver <svm_name> -instance
```

サブシステムがと表示され `Attached subsystem`ます。

**NVMe**ネームスペースをサブシステムにマッピングする

## NVMeネームスペースをサブシステムにマッピングすると、ホストからのデータアクセスが可能になります。NVMeネームスペースは、ストレージのプロビジョニング時にサブシステムにマッピングすることも、ストレージのプロビジョニング後にマッピングすることもできます。

ONTAP 9 14.1以降では、特定のホストのリソース割り当てに優先順位を付けることができます。デフォルト

では、NVMeサブシステムに追加されたホストには標準優先度が与えられます。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。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 9 .13.1以前でサブシステムに追加されたホストに高い優先度を設定する場合は、を使用できますホスト優先度の変更。

開始する前に

ネームスペースとサブシステムはすでに作成されている必要があります。ネームスペースとサブシステムを作成する必要がある場合は、を参照してください"NVMeストレージのプロビジョニング"。

手順

1. ホストからNQNを取得します。
2. ホストNQNをサブシステムに追加します。

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

ホストのデフォルト優先度をregularからhighに変更する場合は、オプションを使用し `-priority high`ます。このオプションは、ONTAP 9.14.1以降で使用できます。

3. ネームスペースをサブシステムにマッピングします。

```
vserver nvme subsystem map add -vserver <SVM_name> -subsystem
<subsystem_name> -path <path>
```

ネームスペースは1つのサブシステムにのみマッピングできます。

4. ネームスペースがサブシステムにマッピングされていることを確認します。

```
vserver nvme namespace show -vserver <SVM_name> -instance
```

サブシステムがと表示され `Attached subsystem`ます。

## LUNの管理

### LUNのQoSポリシー グループの編集

**10.1**以降では、**ONTAP 9 Manager**を使用して、複数の**LUN**に対するサービス品質（**QoS**）ポリシーを同時に割り当てたり削除したりできます。

QoSポリシーがボリュームレベルで割り当てられている場合は、ボリュームレベルで変更する必要があります。QoSポリシーをLUNレベルで編集できるのは、元 々 LUNレベルで割り当てられていた場合のみです。

手順

1. System Manager で、 * Storage > LUNs * をクリックします。
2. 編集するLUNを選択します。

   一度に複数のLUNを編集する場合は、それらのLUNが同じStorage Virtual Machine（SVM）に属している必要があります。同じSVMに属していないLUNを選択した場合、QoSポリシーグループを編集するオプションは表示されません。

3. [ * その他 * ] をクリックし、 [ * QoS ポリシーグループの編集 * ] を選択します。

**LUN**をネームスペースに変換する

ONTAP 9 .11.1以降では、ONTAP CLIを使用して、既存のLUNをNVMeネームスペースにインプレース変換できます。

開始する前に

- 指定したLUNにigroup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。
- MetroClusterが設定されたSVMまたはSnapMirrorのアクティブな同期関係にあるLUNは使用できません。
- LUNはプロトコルエンドポイントではなく、プロトコルエンドポイントにバインドしないでください。
- LUNにゼロ以外のプレフィックスやサフィックスストリームを使用することはできません。
- Snapshotの一部であったり、読み取り専用LUNとしてSnapMirror関係のデスティネーション側であったりすることはできません。

ステップ

1. LUNをNVMeネームスペースに変換します。

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

**LUN**のオフライン化

ONTAP 9 .10.1以降では、System Managerを使用してLUNをオフラインにすることができます。LUN.10.1より前のバージョンでは、ONTAP CLIを使用してONTAP 9をオフラインにする必要があります。

**System Manager**

手順

1. System Manager で、 * Storage > LUNs * をクリックします。
2. 単一のLUNまたは複数のLUNをオフラインにする

| 実行する操作 | 操作 |
| --- | --- |
| 単一の LUN をオフラインにします | LUN名の横にあるをクリック ⋮ し、*[Take Offline]* を選択します。 |
| 複数の LUN をオフラインにします | 1. オフラインにするLUNを選択します。<br>2. 「 * 詳細」をクリックし、「 * オフラインにする * 」を選択します。 |

**CLI**

CLIを使用してオフラインにできるLUNは一度に1つだけです。

ステップ

1. LUNをオフラインにします。

```
lun offline <lun_name> -vserver <SVM_name>
```

**ONTAP**で**LUN**のサイズを変更する

## LUNのサイズは増やすことも減らすこともできます。

タスクの内容

この手順は、FAS、AFF、および現在のASAシステムに適用されます。ASA R2システム（ASA A1K、ASA A70、またはASA A90）を使用している場合は、次の手順に従って"以下の手順を実行します"ストレージユニットのサイズを拡張します。ASA R2システムは、SANのみのお客様に特化したシンプルなONTAPエクスペリエンスを提供します。

ⓘ Solaris LUNのサイズは変更できません。

**LUN**のサイズを拡張する

LUNを拡張できるサイズは、ONTAPのバージョンによって異なります。

| ONTAPのバージョン | LUNの最大サイズ |
| --- | --- |
| ONTAP 9.12.1P2以降 | AFF、FAS、ASAプラットフォームの場合は128TB |

| | |
|---|---|
| ONTAP 9.8以降 | • オールフラッシュSANアレイ（ASA）プラットフォームの場合は128TB<br>• ASA以外のプラットフォームの場合は16TB |
| ONTAP 9.5 、 9.6 、 9.7 | 16TB |
| ONTAP 9 .4以前 | 元のLUNサイズの10倍。ただし、LUNの最大サイズである16TBを超えないようにする必要があります。たとえば、100GBで作成したLUNは1、000GBまでしか拡張できません。LUNの実際の最大サイズが正確に16TBであるとは限りません。ONTAPは、制限を切り捨ててわずかに小さくします。 |

サイズを拡張するためにLUNをオフラインにする必要はありません。ただし、サイズを拡張したあとにホストでLUNを再スキャンして、サイズの変更を認識できるようにする必要があります。

https://docsというリンクの詳細についてはNetApp、『ONTAPコマンドリファレンス』を参照してください。ONTAP lun .com/us-en/lun-resize.html#description^][`lun resize`コマンドを参照してください。

例 **4.** 手順

**System Manager**

ONTAP System Manager（9.7以降）でLUNのサイズを拡張します。

1. System Manager で、 * Storage > LUNs * をクリックします。
2. をクリック ⋮ し、*[編集]*を選択します。
3. Storage and Optimization では、**LUN**のサイズが拡張され、 Save *が表示されます。

**CLI**

ONTAP CLIを使用してLUNのサイズを拡張します。

1. LUNのサイズを拡張します。

```
lun resize -vserver <SVM_name> -volume <volume_name> -lun <lun_name>
-size <lun_size>
```

2. 拡張したLUNのサイズを確認します。

```
lun show -vserver <SVM_name>
```

ONTAP処理では、LUNの実際の最大サイズが想定値よりわずかに小さく切り捨てられます。また、LUNの実際のサイズは、LUNのOSタイプによって多少異なる場合があります。サイズ変更後の正確な値を確認するには、アドバンス・モードで次のコマンドを実行します。

```
set -unit B
```

```
lun show -fields max-resize-size -volume volume_name -lun lun_name
```

1. ホストのLUNを再スキャンします。
2. ホストのマニュアルに従って、新しく作成したLUNサイズをホストファイルシステムが認識できるようにします。

#### LUNのサイズを縮小する

LUNのサイズを縮小する前に、ホストはLUNデータを含むブロックを小さいLUNサイズの境界に移行する必要があります。LUNデータを含むブロックを切り捨てずにLUNを適切に縮小するには、SnapCenterなどのツールを使用する必要があります。LUNのサイズを手動で縮小することは推奨されません。

LUNのサイズを縮小すると、サイズが縮小されたことがONTAPからイニシエータに自動的に通知されます。ただし、ホストが新しいLUNサイズを認識するために、ホストで追加の手順が必要になる場合があります。ホストのファイル構造のサイズの縮小に固有の情報については、ホストのマニュアルを参照してください。

### LUNの移動

Storage Virtual Machine（SVM）内のボリューム間でLUNを移動できますが、SVM間でLUNを移動することはできません。SVM内のボリューム間で移動されたLUNはただちに移動され、接続が失われることはありません。

#### 必要なもの

LUNでSelective LUN Map（SLM；選択的LUNマップ）を使用している場合は、LUNを移動する前に、デスティネーションノードとそのHAパートナーを含める必要があり"SLMレポートノードリストの変更"ます。

#### タスクの内容

重複排除、圧縮、コンパクションなどのStorage Efficiency機能は、LUNの移動時には維持されません。LUNの移動の完了後に再適用する必要があります。

Snapshotコピーによるデータ保護はボリュームレベルで行われます。そのため、移動したLUNにはデスティネーションボリュームのデータ保護形式が適用されます。デスティネーションボリューム用のSnapshotコピーが確立されていない場合、LUNのSnapshotコピーは作成されません。また、LUNのすべてのSnapshotコピーは、Snapshotコピーが削除されるまで元のボリュームに残ります。

次のボリュームにはLUNを移動できません。

- SnapMirrorデスティネーションボリューム
- SVMルートボリューム

次のタイプのLUNは移動できません。

- ファイルから作成されたLUN
- NVFail状態のLUN
- 負荷共有関係にあるLUN
- プロトコルエンドポイントクラスのLUN

1TB以上のos_type Solaris LUNの場合、LUNの移動中にホストでタイムアウトが発生することがあります。このタイプのLUNでは、移動を開始する前にLUNをアンマウントする必要があります。

例 **5.** 手順

**System Manager**

ONTAP System Manager（9.7以降）でLUNを移動します。

ONTAP 9 .10.1以降では、単一のLUNを移動する際にSystem Managerを使用して新しいボリュームを作成できます。ONTAP 9 .8および9.9.1では、LUNの移動を開始する前に、LUNの移動先となるボリュームを用意しておく必要があります。

手順

1. System Manager で、 * Storage > LUNs * をクリックします。
2. 移動するLUNを右クリックし、 *[LUNの移動]*を選択します。

   ONTAP 9.10.1 では、 LUN を既存のボリューム * または新しいボリューム * に移動するように選択します。

   新しいボリュームの作成を選択した場合は、ボリュームの仕様を指定します。
3. [ 移動（ Move ） ] をクリックします。

**CLI**

ONTAP CLIを使用してLUNを移動します。

1. LUNを移動します。

   ```
   lun move start
   ```

   ごく短時間、元のボリュームとデスティネーションボリュームの両方でLUNが表示されます。これは移動が完了するまでの一時的な状態で、想定内の動作です。
2. 移動のステータスを追跡し、正常に完了したことを確認します。

   ```
   lun move show
   ```

関連情報

- "選択的LUNマップ"

**LUN**の削除

不要になった LUN は Storage Virtual Machine （ SVM ）から削除できます。

必要なもの

LUNを削除する前に、そのigroupからLUNのマッピングを解除する必要があります。

手順

1. アプリケーションまたはホストがLUNを使用していないことを確認します。
2. igroupからLUNのマッピングを解除します。

```
lun mapping delete -vserver <SVM_name> -volume <volume_name> -lun
<LUN_name> -igroup <igroup_name>
```

3. LUNを削除します。

```
lun delete -vserver <SVM_name> -volume <volume_name> -lun <LUN_name>
```

4. LUNが削除されたことを確認します。

```
lun show -vserver <SVM_name>
```

```
Vserver   Path              State    Mapped  Type     Size
--------- ----------------- -------- ------- -------- ------
vs5       /vol/vol16/lun8   online   mapped  windows  10.00GB
```

**LUN**ヲコピースルサイノコウリョジコウ

## LUNをコピーする前に、特定の事項について理解しておく必要があります。

クラスタ管理者は、コマンドを使用して、クラスタ内のStorage Virtual Machine（SVM）間でLUNをコピーできます `lun copy`。クラスタ管理者は、Storage Virtual Machine（SVM）間のLUNコピー処理を実行する前に、コマンドを使用してSVMピア関係を確立する必要があります `vserver peer create`。ソースボリュームにSISクローン用の十分なスペースが必要です。

Snapshotコピー内のLUNをコマンドのソースLUNとして使用できます `lun copy`。コマンドを使用してLUNをコピーする `lun copy`と、LUNコピーに対する読み取りと書き込みがすぐに可能になります。ソースLUNは、LUNコピーを作成しても変更されません。ソースLUNとLUNコピーは、LUNシリアル番号が異なる一意のLUNとして存在します。ソースLUNに加えられた変更はLUNコピーには反映されず、LUNコピーに加えられた変更はソースLUNにも反映されません。ソースLUNのLUNマッピングは新しいLUNにコピーされないため、LUNコピーをマッピングする必要があります。

Snapshotコピーによるデータ保護はボリュームレベルで行われます。そのため、ソースLUNのボリュームとは異なるボリュームにLUNをコピーする場合、デスティネーションLUNにはデスティネーションボリュームのデータ保護形式が適用されます。デスティネーションボリューム用のSnapshotコピーが確立されていない場合、LUNコピーのSnapshotコピーは作成されません。

LUNのコピーはノンストップオペレーションです。

次のタイプのLUNはコピーできません。

- ファイルから作成されたLUN
- NVFAIL状態のLUN
- 負荷共有関係にあるLUN
- プロトコルエンドポイントクラスのLUN

**LUN**の構成済みスペースと使用済みスペースを確認する

## LUN の設定済みスペースと実際に使用されているスペースを把握しておくと、スペース再生時に再生可能なスペースの量、データを含むリザーブスペースの量、および LUN の設定済みの合計サイズと実際に使用されているサイズを特定するのに役立ちます。

ステップ

1. LUNの設定済みスペースと実際に使用されているスペースを表示します。

   ```
   lun show
   ```

   次の例は、vs3というStorage Virtual Machine（SVM）内のLUNの設定済みスペースと実際に使用されているスペースを示しています。

   ```
   lun show -vserver vs3 -fields path, size, size-used, space-reserve
   ```

   ```
   vserver path                    size    space-reserve size-used
   ------- ------------------      ------- ------------- ---------
   vs3     /vol/vol0/lun1          50.01GB disabled      25.00GB
   vs3     /vol/vol0/lun1_backup   50.01GB disabled      32.15GB
   vs3     /vol/vol0/lun2          75.00GB disabled      0B
   vs3     /vol/volspace/lun0      5.00GB  enabled       4.50GB
   4 entries were displayed.
   ```

ストレージ**QoS**を使用して**LUN**への**I/O**パフォーマンスを制御および監視

## LUN への入出力（ I/O ）パフォーマンスは、 LUN をストレージ QoS ポリシーグループに割り当てることによって制御できます。I/O パフォーマンスを制御することで、ワークロードが特定のパフォーマンス目標を達成できるようにしたり、他のワークロードに悪影響を与えるワークロードを抑制したりできます。

タスクの内容

ポリシーグループは最大スループット制限（ 100MB/s など）を適用します。ポリシーグループは最大スループットを指定せずに作成することもでき、ワークロードの制御に先立ってパフォーマンスを監視できます。

FlexVolボリュームとLUNを含むStorage Virtual Machine（SVM）をポリシーグループに割り当てることもできます。

ポリシーグループへの LUN の割り当てについては、次の要件に注意してください。

- LUN は、ポリシーグループが属する SVM に含まれている必要があります。

  SVM は、ポリシーグループを作成するときに指定します。

- LUN をポリシーグループに割り当てた場合、その LUN を含むボリュームまたは SVM をポリシーグループに割り当てることはできなくなります。

ストレージQoSの使用方法の詳細については、を参照して"システムアドミニストレーションリファレンス"ください。

手順

1. コマンドを使用し `qos policy-group create`て、ポリシーグループを作成します。
2. `lun create`コマンドまたは `lun modify`コマンドでパラメータを指定し `-qos-policy-group`て、LUNをポリシーグループに割り当てます。
3. パフォーマンスデータを表示するには、コマンドを使用し `qos statistics`ます。
4. 必要に応じて、コマンドを使用し `qos policy-group modify`てポリシーグループの最大スループット制限を調整します。

**LUN**を効果的に監視するためのツール

## LUN を効果的に監視し、スペース不足になるのを防ぐためのツールが用意されています。

- Active IQ Unified Manager は、環境内のすべてのクラスタのすべてのストレージを管理するための無償ツールです。
- System Manager は、 ONTAP に組み込まれているグラフィカルユーザインターフェイスです。クラスタレベルで必要なストレージを手動で管理できます。
- OnCommand Insight を使用すると、ストレージインフラの状況を一元的に確認できます。また、自動監視やアラートの機能、および LUN 、ボリューム、アグリゲートでストレージスペース不足が発生したときにレポートする機能を設定できます。

移行した**LUN**の機能と制限事項

## SAN環境では、7-ModeボリュームをONTAPに移行する際にサービスの中断が必要です。移行を完了するには、ホストをシャットダウンする必要があります。移行後は、ONTAPでデータの提供を開始する前にホスト構成を更新する必要があります。

ホストをシャットダウンできる時間帯にメンテナンスのスケジュールを設定して、移行を完了する必要があります。

Data ONTAP 7-ModeからONTAPに移行されたLUNには、LUNの管理方法に影響する特定の機能と制限があります。

移行したLUNでは、次の操作を実行できます。

- コマンドを使用してLUNを表示する `lun show`
- コマンドを使用して、7-Modeボリュームから移行したLUNのインベントリを表示する `transition 7-mode show`

- 7-Mode Snapshotコピーからボリュームをリストアする

  ボリュームをリストアすると、Snapshotコピーにキャプチャされたすべてのlunが移行されます。

- コマンドを使用して、7-Mode Snapshotコピーから単一のLUNをリストアする `snapshot restore-file`
- 7-Mode Snapshotコピー内のLUNのクローンを作成する
- 7-Mode Snapshotコピーにキャプチャされたlunから一連のブロックをリストアする
- 7-Mode Snapshotコピーを使用してボリュームのFlexCloneを作成する

移行したLUNでは、次の操作は実行できません。

- Snapshotコピーでバックアップされたボリューム内にキャプチャされたLUNクローンにアクセスする

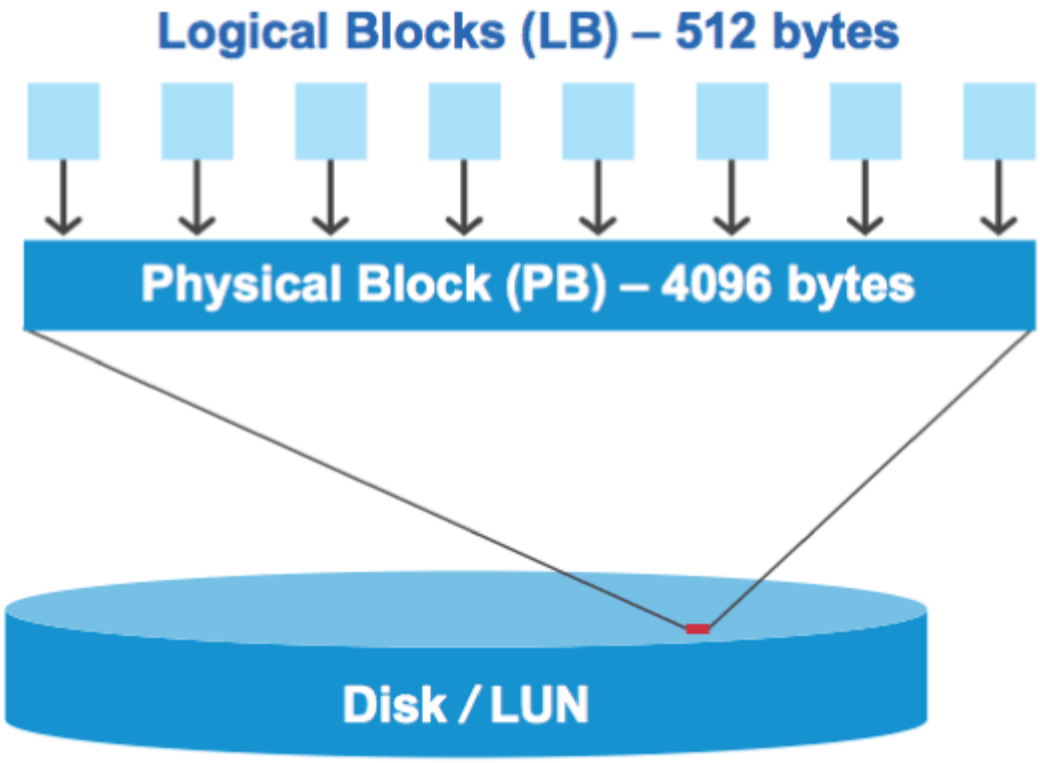
関連情報

"コピーベースの移行"

適切にアライメントされた**LUN**での**I/O**ミスアライメントの概要

ONTAPでは、適切にアライメントされたLUNでI/Oのミスアライメントが報告されることがあります。一般に、これらのミスアライメントの警告は、LUNが適切にプロビジョニングされていて、パーティションテーブルが正しいことに確信があれば無視してかまいません。

LUNとハードディスクはどちらもストレージをブロックとして提供します。ホスト上のディスクのブロックサイズは512バイトであるため、LUNはそのサイズのブロックをホストに提供しますが、実際にはより大きな4KBのブロックを使用してデータを格納します。ホストで使用される512バイトのデータブロックを論理ブロックと呼びます。LUNがデータの格納に使用する4KBのデータブロックを物理ブロックと呼びます。つまり、4KBの各物理ブロックに512バイトの論理ブロックが8個あります。




ホストオペレーティングシステムは、任意の論理ブロックで読み取りまたは書き込みのI/O処理を開始できます。I/O処理は、物理ブロック内の最初の論理ブロックで開始されたときにのみアライメントされたとみなされます。I/O処理が物理ブロックの始点でもない論理ブロックから開始された場合、I/Oはミスアライメントされているとみなされます。ONTAPは、LUNのミスアライメントを自動的に検出して報告します。ただし、ミスアライメントI/Oがあるからといって、LUNもミスアライメントされているとは限りません。適切にアライメントされたLUNで、ミスアライメントI/Oが報告される可能性があります。

詳細な調査が必要な場合は、ナレッジベースの記事を参照してください。"LUNのミスアライメントされたIOを特定する方法"

アライメントの問題を修正するためのツールの詳細については、 + を参照してください

- "Windows Unified Host Utilities 7.1"
- "SANストレージのドキュメントのプロビジョニング"

#### LUNのOSタイプを使用したI/Oアライメントの実現

ONTAP 9 .7以前の場合は、OSのパーティショニングスキームでI/Oがアライメントされるように、オペレーティングシステムに最も近い推奨ONTAP LUN値を使用する必要があります `ostype`。

ホストオペレーティングシステムで採用されているパーティション方式は、I/Oのミスアライメントの主な要因です。一部のONTAP LUN `ostype`値では、「プレフィックス」と呼ばれる特別なオフセットを使用して、アライメント対象のホストオペレーティングシステムが使用するデフォルトのパーティショニングスキームを有効にします。

> 場合によっては、I/Oアライメントを実行するためにカスタムのパーティショニングテーブルが必要になることがあります。ただし、「prefix」の値がより大きい値の `0`場合 `ostype`、カスタムパーティションを使用するとミスアライメントI/Oが発生する可能性があります。

ONTAP 9 .7以前でプロビジョニングされたLUNの詳細については、技術情報アーティクルを参照して"LUNでアライメントされていないIOを特定する方法"ください。

デフォルトでは、ONTAP 9 .8以降でプロビジョニングされる新しいLUNには、すべてのLUN OSタイプでプレフィックスおよびサフィックスサイズが0に設定されます。I/Oは、デフォルトでサポートされるホストOSとアライメントされている必要があります。

#### Linux固有のI/Oアライメントに関する考慮事項

Linuxディストリビューションでは、データベース、各種ボリュームマネージャ、ファイルシステムのrawデバイスなど、さまざまな方法でLUNを使用できます。rawデバイスまたは論理ボリューム内の物理ボリュームとして使用される場合、LUNにパーティションを作成する必要はありません。

RHEL 5以前およびSLES 10以前で、ボリュームマネージャを使用せずにLUNを使用する場合は、アライメントされたオフセットから始まる1つのパーティション（8個の論理ブロックの偶数倍のセクター）を持つようにLUNをパーティショニングする必要があります。

#### Solaris LUN固有のI/Oアライメントに関する考慮事項

ostypeと `solaris_efi`ostypeのどちらを使用するかを決定する際には、さまざまな要因を考慮する必要があり `solaris`ます。

詳細については、を参照してください "Solaris Host Utilities Installation and Administration Guide"。

#### ESXブートLUNがミスアライメントとして報告される

ESXブートLUNとして使用されるLUNは、通常、ミスアライメントとしてONTAPから報告されます。ESXではブートLUNに複数のパーティションが作成されるため、アライメントが非常に困難になります。ミスアライメントされたI/Oの総量は小さいため、ミスアライメントされたESXブートLUNは通常、パフォーマンス上の問題にはなりません。VMwareを使用してLUNが正しくプロビジョニングされていれば、 `ostype`対処は不要です。

関連情報

"VMware vSphereをはじめとする仮想環境、NetAppストレージシステム向けのゲストVMファイルシステムのパーティション/ディスクアライメント"

### LUNがオフラインになった場合の問題の対処方法

書き込みに使用できるスペースがない場合、LUNはデータの整合性を維持するためにオフラインになります。LUNのスペースが不足してオフラインになる原因はさまざまですが、いくつかの方法で問題に対処できます。

| 状況 | 可能です |
| --- | --- |
| アグリゲートがフルです | • ディスクを追加します。<br>• コマンドを使用して `volume modify`、使用可能なスペースがあるボリュームを縮小します。<br>• 使用可能なスペースがあるスペースギャランティボリュームがある場合は、コマンドを使用して `volume modify`ボリュームのスペースギャランティをに変更します `none`。 |
| ボリュームがフルですが、包含アグリゲートに利用可能なスペースがあります | • スペースギャランティボリュームの場合は、コマンドを使用し `volume modify`てボリュームのサイズを拡張します。<br>• シンプロビジョニングボリュームの場合は、コマンドを使用し `volume modify`てボリュームの最大サイズを拡張します。<br><br>ボリュームの自動拡張が有効になっていない場合は、を使用 `volume modify -autogrow-mode`して有効にします。<br><br>• コマンドを使用してSnapshotコピーを手動で削除する `volume snapshot delete`か、コマンドを使用し `volume snapshot autodelete modify`てSnapshotコピーを自動的に削除します。 |

関連情報

"ディスクとローカル階層（アグリゲート）の管理"

"論理ストレージ管理"

ホストで**iSCSI LUN**が表示されない場合のトラブルシューティング

iSCSI LUNは、ホストではローカルディスクとして表示されます。ストレージシステムのLUNをホストでディスクとして使用できない場合は、構成設定を確認する必要があります。

| 構成設定 | 対処方法： |
| --- | --- |
| ケーブル接続 | ホストとストレージシステムの間のケーブルが正しく接続されていることを確認します。 |

| 構成設定 | 対処方法： |
| --- | --- |
| ネットワーク接続 | ホストとストレージシステムの間にTCP / IP接続が確立されていることを確認します。<br><br>• ストレージシステムのコマンドラインから、iSCSIに使用されているホストインターフェイスをpingします。<br><br>`ping -node node_name -destination host_ip_address_for_iSCSI`<br><br>• ホストのコマンドラインから、iSCSIに使用されているストレージシステムインターフェイスをpingします。<br><br>`ping -node node_name -destination host_ip_address_for_iSCSI` |
| システム要件 | 構成のコンポーネントが認定されていることを確認します。また、ホストオペレーティングシステム（OS）のサービスパックレベル、イニシエータバージョン、ONTAPバージョンなどのシステム要件を満たしていることも確認してください。Interoperability Matrixに最新のシステム要件が記載されています。 |
| ジャンボフレーム | ご使用の構成でジャンボフレームを使用している場合は、ネットワークパス（ホストのイーサネットNIC、ストレージシステム、スイッチ）上のすべてのデバイスでジャンボフレームが有効になっていることを確認します。 |
| iSCSIサービスステータス | iSCSIサービスのライセンスが設定され、ストレージシステムで開始されていることを確認します。 |
| イニシエータログイン | イニシエータがストレージシステムにログインしていることを確認します。ログインしているイニシエータがコマンド出力に表示されない場合は `iscsi initiator show`、ホストのイニシエータ設定を確認します。また、ストレージシステムがイニシエータのターゲットとして設定されていることを確認します。 |
| iSCSIノード名（IQN） | 正しいイニシエータのノード名をigroup設定で使用していることを確認します。ホストでは、イニシエータのツールとコマンドを使用してイニシエータのノード名を表示できます。igroupおよびホストに設定されているイニシエータのノード名が一致している必要があります。 |
| LUNマツヒンク | LUNがigroupにマッピングされていることを確認します。ストレージシステムコンソールでは、次のいずれかのコマンドを使用できます。<br><br>• `lun mapping show`すべてのLUN、およびLUNがマッピングされているigroupを表示します。<br>• `lun mapping show -igroup`特定のigroupにマッピングされているLUNを表示します。 |

| 構成設定 | 対処方法： |
| --- | --- |
| iSCSI LIFの有効化 | iSCSI論理インターフェイスが有効になっていることを確認します。 |

関連情報

"NetApp Interoperability Matrix Tool"

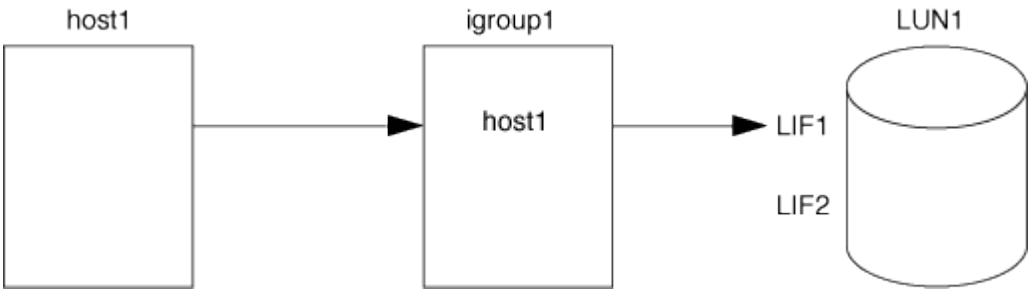
## igroupとポートセットを管理します。

ポートセットと**igroup**によって**LUN**アクセスを制限する方法

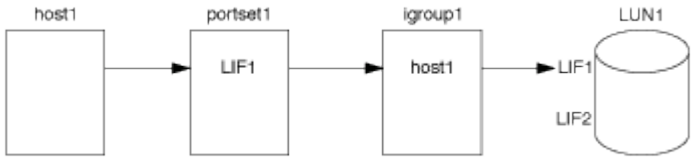
### Selective LUN Map（SLM；選択的LUNマップ）に加えて、igroupおよびポートセットを使用してLUNへのアクセスを制限することができます。

ポートセットとSLMを併用すると、特定のターゲットのアクセスを特定のイニシエータだけに制限できます。SLMとポートセットを併用する場合、LUNには、そのLUNを所有するノードおよびノードのHAパートナーのポートセットに含まれる一連のLIF経由でアクセスできます。

次の例では、initiator1にポートセットがありません。ポートセットがない場合、initiator1はLIF1とLIF2の両方を介してLUN1にアクセスできます。




ポートセットを使用すると、LUN1へのアクセスを制限できます。次の例では、initiator1はLIF1経由でのみLUN1にアクセスできます。ただし、LIF2がportset1に含まれていないため、LIF2を介してLUN1にアクセスすることはできません。




関連情報

- 選択的LUNマップ
- ポートセットを作成してigroupにバインドする

**SAN**イニシエータと**igroup**の表示と管理

### System Managerを使用して、イニシエータグループ（igroup）とイニシエータを表示および管理できます。

タスクの内容

- イニシエータグループは、どのホストがストレージシステム上の特定のLUNにアクセスできるかを識別します。
- イニシエータとイニシエータグループを作成したあと、それらを編集したり削除したりすることもできます。
- SANイニシエータグループおよびイニシエータを管理するには、次のタスクを実行できます。
  - [view-manage-san-igroups]
  - [view-manage-san-inits]

#### SANイニシエータグループの表示と管理

System Managerを使用して、イニシエータグループ（igroup）のリストを表示できます。リストから追加の処理を実行できます。

手順

1. System Managerで、* Hosts > SAN Initiator Groups *をクリックします。

   イニシエータグループ（igroup）のリストがページに表示されます。リストが大きい場合は、ページの右下隅にあるページ番号をクリックして、リストの追加ページを表示できます。

   igroupに関するさまざまな情報が列に表示されます。9.11.1以降では、igroupの接続ステータスも表示されます。ステータスアラートにカーソルを合わせると、詳細が表示されます。

2. （オプション）：リストの右上にあるアイコンをクリックすると、次のタスクを実行できます。
   - * 検索 *
   - *ダウンロード*リスト。
   - *リストの*または*隠す*列を表示します。
   - *リスト内のデータをフィルタリングします。
3. リストから操作を実行できます。
   - をクリックし + Add てigroupを追加します。
   - igroup名をクリックすると、そのigroupの詳細が表示されます。* Overview *ページが表示されます。

     概要*ページでは、igroupに関連付けられているLUNを確認できます。また、処理を開始してLUNの作成やLUNのマッピングを行うこともできます。「*すべてのSANイニシエータ」をクリックしてメインリストに戻ります。

   - igroupにカーソルを合わせ、igroup名の横にあるをクリックして、 ⋮ igroupを編集または削除します。
   - igroup名の左側の領域にカーソルを合わせ、チェックボックスをオンにします。イニシエータグループに追加をクリックすると、そのigroupを別のigroupに追加できます。
   - Storage VM *列で、Storage VMの名前をクリックして詳細を確認します。

#### SANイニシエータの表示と管理

System Managerを使用して、イニシエータのリストを表示できます。リストから追加の処理を実行できます。

手順

1. System Managerで、* Hosts > SAN Initiator Groups *をクリックします。

   イニシエータグループ（igroup）のリストがページに表示されます。

2. イニシエータを表示するには、次の手順に従います。

   ◦ FCイニシエータの一覧を表示するには、* FCイニシエータ*タブをクリックします。

   ◦ iSCSIイニシエータのリストを表示するには、* iSCSIイニシエータ*タブをクリックします。

   各列には、イニシエータに関するさまざまな情報が表示されます。

   9.11.1以降では、イニシエータの接続ステータスも表示されます。ステータスアラートにカーソルを合わせると、詳細が表示されます。

3. （オプション）：リストの右上にあるアイコンをクリックすると、次のタスクを実行できます。

   ◦ * Search *：特定のイニシエータを一覧表示します。

   ◦ *ダウンロード*リスト。

   ◦ *リストの*または*隠す*列を表示します。

   ◦ *リスト内のデータをフィルタリングします。

ネストされた**igroup**を作成する

## ONTAP 9.9.1以降では、他の既存のigroupで構成されるigroupを作成できます。

1. System Manager で、 * Host > SAN Initiator Groups * をクリックし、 * Add * をクリックします。
2. igroup 名 * と * 概要 * を入力します。

   この説明はigroupエイリアスとして機能します。

3. Storage VM * および * Host Operating System * を選択します。

   ネストされたigroupのOSタイプは、作成後は変更できません。

4. イニシエータグループメンバー * で、 * 既存のイニシエータグループ * を選択します。

   ◦ Search * を使用して、追加する igroup を検索して選択できます。

**igroup**を複数の**LUN**にマッピング

## ONTAP 9.9.1以降では、igroupを複数のLUNに同時にマッピングできます。

1. System Manager で、 * Storage > LUNs * をクリックします。
2. マッピングするLUNを選択します。
3. [ * 詳細 * ] をクリックし、 [ * イニシエータ・グループへのマップ * ] をクリックします。

   選択したigroupが選択したLUNに追加されます。既存のマッピングは上書きされません。

## ポートセットを作成して**igroup**にバインドする

を使用するだけでなく"選択的LUNマップ（SLM）"、ポートセットを作成してigroupにバインドし、イニシエータがLUNへのアクセスに使用するLIFをさらに制限することもできます。

ポートセットをigroupにバインドしない場合、igroup内のすべてのイニシエータが、LUNを所有するノードおよび所有者ノードのHAパートナーのすべてのLIFを介してマッピングされたLUNにアクセスできます。

### 必要なもの

少なくとも1つのLIFと1つのigroupが必要です。

インターフェイスグループを使用しないかぎり、iSCSIとFCの冗長性を確保するために推奨されるLIFの数は2つです。インターフェイスグループに推奨されるLIFは1つだけです。

### タスクの内容

ノード上にLIFが3つ以上あり、特定のイニシエータを一部のLIFに制限する場合は、ポートセットとSLMを併用する方が効果的です。ポートセットを使用しない場合は、LUNへのアクセス権を持つすべてのイニシエータが、LUNを所有するノードおよび所有者ノードのHAパートナー経由でノード上のすべてのターゲットにアクセスできます。

例 **6.** 手順

**System Manager**

ONTAP 9 .10.1以降では、System Managerを使用してポートセットを作成し、igroupにバインドできます。

ONTAP 9.10.1より前のリリースでポートセットを作成してigroupにバインドする必要がある場合は、ONTAP CLI手順 を使用する必要があります。

1. System Manager で、 * Network > Overview > portsets * をクリックし、 * Add * をクリックします。
2. 新しいポートセットの情報を入力し、 * Add * をクリックします。
3. [*Hosts] ＞ [SAN Initiator Groups] をクリックします
4. ポートセットを新しい igroup にバインドするには、 * Add * をクリックします。

   ポートセットを既存のigroupにバインドするには、igroupを選択してをクリックし、 *[イニシエータグループの編集]*をクリックします。

関連情報

"イニシエータとigroupの表示と管理"

**CLI**

1. 適切なLIFを含むポートセットを作成します。

   `portset create -vserver` *`vserver_name`* `-portset` *`portset_name`* `-protocol` *`protocol`* `-port-name` *`port_name`*

   FCを使用する場合は、パラメータをに `fcp`指定します `protocol`。iSCSIを使用する場合は、パラメータをに `iscsi`指定します `protocol`。

2. igroupをポートセットにバインドします。

   `lun igroup bind -vserver` *`vserver_name`* `-igroup` *`igroup_name`* `-portset` *`portset_name`*

3. ポートセットとLIFが正しいことを確認します。

   `portset show -vserver` *`vserver_name`*

```
Vserver   Portset   Protocol Port Names    Igroups
--------- --------- -------- ------------- --------
vs3       portset0  iscsi    lif0,lif1     igroup1
```

ポートセットを管理します。

"選択的LUNマップ（SLM）"また、ポートセットを使用して、イニシエータがLUNへのアクセスに使用するLIFをさらに制限することもできます。

ONTAP 9 .10.1以降では、System Managerを使用して、ポートセットに関連付けられているネットワークインターフェイスを変更したり、ポートセットを削除したりできます。

ポートセットに関連付けられているネットワークインターフェイスの変更

1. System Managerで、*[ネットワーク]>[概要]>[ポートセット]*を選択します。
2. 編集するポートセットを選択し、*[ポートセットの編集]*を選択します。

ポートセットを削除します。

1. System Manager で、 * Network > Overview > portsets * をクリックします。
2. 単一のポートセットを削除するには、ポートセットを選択し、*[ポートセットの削除]*を選択します。

   複数のポートセットを削除するには、ポートセットを選択し、 * 削除 * をクリックします。

選択的**LUN**マップの概要

Selective LUN Map（SLM；選択的LUNマップ）を使用すると、ホストからLUNへのパスの数が削減されます。SLMで新しいLUNマップを作成すると、LUNを所有するノードとそのHAパートナーのパス経由でのみLUNにアクセスできます。

SLMを使用すると、ホストごとに1つのigroupを管理できます。また、ポートセットの操作やLUNの再マッピングを必要としない、無停止のLUN移動処理もサポートされます。

"ポートセット"SLMと併用すると、特定のターゲットのアクセスを特定のイニシエータだけに制限できます。SLMとポートセットを併用する場合、LUNには、そのLUNを所有するノードおよびノードのHAパートナーのポートセットに含まれる一連のLIF経由でアクセスできます。

すべての新しいLUNマップでは、SLMがデフォルトで有効になります。

**SLM**が**LUN**マップで有効になっているかどうかを確認する

ONTAP 9リリースで作成されたLUNと以前のバージョンから移行されたLUNが環境内に混在している場合は、特定のLUNで選択的LUNマップ（SLM）が有効になっているかどうかを確認しなければならないことがあります。

コマンドの出力に表示される情報を使用して、LUNマップでSLMが有効になっているかどうかを確認できます `lun mapping show -fields reporting-nodes, node`。SLMが有効になっていない場合は、コマンド出力の「reporting-nodes」列の下のセルにと表示されます。SLMが有効な場合、「nodes」列の下に表示されるノードのリストが「reporting-nodes」列に複製されます。

**SLM**レポートノードリストの変更

LUNまたはLUNを含むボリュームを同じクラスタ内の別のハイアベイラビリティ（HA）ペアに移動する場合は、最適化されたアクティブなLUNパスが維持されるように、移動を開始する前に選択的LUNマップ（SLM）のレポートノードリストを変更する必要があります。

手順

1. デスティネーションノードとそのパートナーノードをアグリゲートまたはボリュームのレポートノードリストに追加します。

```
lun mapping add-reporting-nodes -vserver <vserver_name> -path <lun_path>
-igroup <igroup_name> [-destination-aggregate <aggregate_name>|-
destination-volume <volume_name>]
```

一貫した命名規則がある場合は、の代わりにを使用して、複数のLUNマッピングを同時に変更できます `igroup_prefix*` `igroup_name`。

2. ホストを再スキャンして、新しく追加したパスを検出します。
3. OSで必要な場合は、マルチパス ネットワークI/O（MPIO）構成に新しいパスを追加します。
4. 必要な移動処理のためのコマンドを実行して、処理が完了するまで待ちます。
5. I/Oがアクティブな最適パス経由で処理されていることを確認します。

```
lun mapping show -fields reporting-nodes
```

6. レポート ノード リストから、前のLUN所有者とそのパートナー ノードを削除します。

```
lun mapping remove-reporting-nodes -vserver <vserver_name> -path
<lun_path> -igroup <igroup_name> -remote-nodes
```

7. 既存のLUNマップからLUNが削除されていることを確認します。

```
lun mapping show -fields reporting-nodes
```

8. ホストOSの古いデバイスのエントリを削除します。
9. 必要に応じて、マルチパス構成ファイルを変更します。
10. ホストを再スキャンして古いパスが削除されたことを確認します。+ ホストを再スキャンする手順については、ホストのマニュアルを参照してください。

## iSCSIプロトコルを管理します。

最適なパフォーマンスを実現するためのネットワークの設定

イーサネットネットワークによってパフォーマンスは大きく異なります。特定の設定値を選択することで、iSCSIに使用するネットワークのパフォーマンスを最大限に高めることができます。

手順

1. ホストポートとストレージポートを同じネットワークに接続します。

   同じスイッチに接続することを推奨します。ルーティングを使用することはできません。

2. 最も速度の速いポートを選択し、それらをiSCSI専用にします。

   10GbEポートが最適です。最小要件は1GbEポートです。

3. すべてのポートでイーサネット フロー制御を無効にします。

   CLIを使用してイーサネットポートのフロー制御を設定するには、を参照してください"ネットワーク管理"。

4. ジャンボフレームを有効にする（通常MTUは9000）。

   イニシエータ、ターゲット、スイッチを含むデータパス内のすべてのデバイスでジャンボフレームがサポートされている必要があります。そうしないと、ジャンボフレームを有効にすると、ネットワークのパフォーマンスが大幅に低下します。

**SVM**を**iSCSI**用に設定する

## iSCSI用にStorage Virtual Machine（SVM）を設定するには、SVM用のLIFを作成し、それらのLIFにiSCSIプロトコルを割り当てる必要があります。

タスクの内容

iSCSIプロトコルを使用してデータを提供する各SVMについて、各ノードに少なくとも1つのiSCSI LIFが必要です。冗長性を確保するために、ノードごとに少なくとも2つのLIFを作成する必要があります。

例 **7.** 手順

**System Manager**

ONTAP System Manager（9.7以降）でiSCSI用のStorage VMを設定します。

| 新しい**Storage VM**で**iSCSI**を設定する方法 | 既存の**Storage VM**で**iSCSI**を設定する方法 |
| --- | --- |
| 1. System Managerで、* Storage > Storage VM* をクリックし、* Add *をクリックします。<br>2. Storage VMの名前を入力してください。<br>3. アクセスプロトコル*として「* iSCSI *」を選択します。<br>4. Enable iSCSI（iSCSIを有効にする）をクリックし、ネットワークインタフェースのIPアドレスとサブネットマスクを入力します。+各ノードに少なくとも2つのネットワークインターフェイスが必要です。<br>5. [ 保存（ Save ） ] をクリックします。 | 1. System Manager で、 * Storage > Storage VM* をクリックします。<br>2. 設定するStorage VMをクリックします。<br>3. [設定]*タブをクリックし、iSCSIプロトコルの横にあるをクリックし ます。<br>4. Enable iSCSI（iSCSIを有効にする）をクリックし、ネットワークインタフェースのIPアドレスとサブネットマスクを入力します。+各ノードに少なくとも2つのネットワークインターフェイスが必要です。<br>5. [ 保存（ Save ） ] をクリックします。 |

**CLI**

ONTAP CLIを使用してiSCSI用にStorage VMを設定します。

1. SVMがiSCSIトラフィックをリスンするようにします。

   ```
   vserver iscsi create -vserver vserver_name -target-alias vserver_name
   ```

2. iSCSIに使用する各ノードにSVM用のLIFを作成します。
   - ONTAP 9.6以降：

     ```
     network interface create -vserver vserver_name -lif lif_name -data
     -protocol iscsi -service-policy default-data-iscsi -home-node node_name
     -home-port port_name -address ip_address -netmask netmask
     ```

   - ONTAP 9.5以前：

     ```
     network interface create -vserver vserver_name -lif lif_name -role data
     -data-protocol iscsi -home-node node_name -home-port port_name -address
     ip_address -netmask netmask
     ```

3. LIFが正しく設定されたことを確認します。

   ```
   network interface show -vserver vserver_name
   ```

4. iSCSIが稼働していること、およびそのSVMのターゲットIQNを確認します。

   ```
   vserver iscsi show –vserver vserver_name
   ```

5. ホストから、LIFへのiSCSIセッションを作成します。

関連情報

"NetAppテクニカルレポート4080：『Best Practices for Modern SAN』"

イニシエータのセキュリティポリシー方式を定義する

## イニシエータとその認証方法のリストを定義できます。また、ユーザ定義の認証方法がないイニシエータに適用されるデフォルトの認証方法を変更することもできます。

タスクの内容

製品のセキュリティポリシーアルゴリズムを使用して一意のパスワードを生成することも、使用するパスワードを手動で指定することもできます。

一部のイニシエータが16進数のCHAPシークレットパスワードをサポートしていません。

手順

1. コマンドを使用し `vserver iscsi security create`て、イニシエータのセキュリティポリシー方式を作成します。

   ```
   vserver iscsi security create -vserver vs2 -initiator iqn.1991-
   05.com.microsoft:host1 -auth-type CHAP -user-name bob1 -outbound-user-name
   bob2
   ```

2. 画面に表示されるコマンドに従ってパスワードを追加します。

   インバウンドとアウトバウンドのCHAPユーザ名とパスワードを使用して、イニシエータiqn.1991-05.com.microsoft:host1のセキュリティポリシー方式を作成します。

関連情報

- iSCSI認証の仕組み
- CHAP認証

**SVM**の**iSCSI**サービスを削除する

## Storage Virtual Machine（SVM）の不要になったiSCSIサービスは削除できます。

必要なもの

iSCSI サービスを削除するには、 iSCSI サービスの管理ステータスが「所有」状態である必要があります。コマンドを使用すると、管理ステータスをdownに切り替えることができます `vserver iscsi modify`。

手順

1. コマンドを使用し `vserver iscsi modify`て、LUNへのI/Oを停止します。

   ```
   vserver iscsi modify -vserver vs1 -status-admin down
   ```

2. コマンドを使用し `vserver iscsi delete`て、SVMからiSCSIサービスを削除します。

   ```
   vserver iscsi delete -vserver vs_1
   ```

3. を使用 `vserver iscsi show command`して、iSCSIサービスがSVMから削除されたことを確認します。

```
vserver iscsi show -vserver vs1
```

**iSCSI**セッションのエラーリカバリに関する詳細情報の取得

## iSCSIセッションのエラーリカバリレベルを上げると、iSCSIエラーリカバリに関する詳細情報を取得できます。高いレベルのエラーリカバリを使用すると、iSCSIセッションのパフォーマンスが若干低下する可能性があります。

タスクの内容

ONTAPは、iSCSIセッションに対してエラーリカバリレベル0を使用するようにデフォルトで設定されています。エラーリカバリレベル1または2に対応したイニシエータを使用している場合は、エラーリカバリレベルを上げるように選択できます。変更したセッションのエラーリカバリレベルは、新しく作成されたセッションにのみ影響し、既存のセッションには影響しません。

ONTAP 9 .4以降では、 `max-error-recovery-level`コマンドおよび `iscsi modify`コマンドでオプションはサポートされません `iscsi show`。

手順

1. advancedモードに切り替えます。

```
set -privilege advanced
```

2. コマンドを使用して、現在の設定を確認します `iscsi show`。

```
iscsi show -vserver vs3 -fields max-error-recovery-level
```

```
vserver max-error-recovery-level
------- ------------------------
vs3     0
```

3. コマンドを使用して、エラーリカバリレベルを変更します `iscsi modify`。

```
iscsi modify -vserver vs3 -max-error-recovery-level 2
```

**SVM**を**iSNS**サーバに登録

## iSNSサーバに登録するようにStorage Virtual Machine（SVM）を設定するには、コマンドを使用し `vserver iscsi isns`ます。

タスクの内容

コマンドは、 `vserver iscsi isns create`SVMをiSNSサーバに登録します。SVM には、 iSNS サーバの設定や管理を行うコマンドはありません。iSNS サーバを管理するには、 iSNS サーバのベンダーが提供するサーバ管理ツールまたはインターフェイスを使用します。

手順

1. iSNS サーバで、 iSNS サービスが開始しており、サービスを提供可能な状態であることを確認します。
2. データポートにSVM管理LIFを作成します。

   ```
   network interface create -vserver SVM_name -lif lif_name -role data -data
   -protocol none -home-node home_node_name -home-port home_port -address
   IP_address -netmask network_mask
   ```

3. SVMにiSCSIサービスを作成します（存在しない場合）。

   ```
   vserver iscsi create -vserver SVM_name
   ```

4. iSCSIサービスが正常に作成されたことを確認します。

   ```
   iscsi show -vserver SVM_name
   ```

5. SVMのデフォルトルートが存在することを確認します。

   ```
   network route show -vserver SVM_name
   ```

6. SVMのデフォルトルートが存在しない場合は、デフォルトルートを作成します。

   ```
   network route create -vserver SVM_name -destination destination -gateway
   gateway
   ```

7. iSNSサービスに登録するようにSVMを設定します。

   ```
   vserver iscsi isns create -vserver SVM_name -address IP_address
   ```

   IPv4アドレスファミリーとIPv6アドレスファミリーの両方がサポートされます。iSNS サーバのアドレスファミリーは、 SVM 管理 LIF のアドレスファミリーと同じである必要があります。

   たとえば、IPv4アドレスを使用するSVM管理LIFを、IPv6アドレスを使用するiSNSサーバに接続することはできません。

8. iSNSサービスが実行されていることを確認します。

   ```
   vserver iscsi isns show -vserver SVM_name
   ```

9. iSNSサービスが実行されていない場合は開始します。

   ```
   vserver iscsi isns start -vserver SVM_name
   ```

ストレージシステムの**iSCSI**エラーメッセージを解決する

iSCSI関連の一般的なエラーメッセージは、コマンドで確認できます `event log show`。これらのメッセージの意味と、特定された問題の解決方法を把握する必要があります。

次の表に、最も一般的なエラーメッセージと、それらを解決する手順を示します。

| メッセージ | 説明 | 対処方法： |
| --- | --- | --- |
| `ISCSI: network interface identifier disabled for use; incoming connection discarded` | このインターフェイスの iSCSI サービスが有効になっていません。 | インターフェイスでiSCSIサービスを有効にするには、コマンドを使用し `iscsi interface enable`ます。例：<br><br>`iscsi interface enable -vserver vs1 -lif lif1` |
| `ISCSI: Authentication failed for initiator nodename` | 指定されたイニシエータに対して CHAP が正しく設定されていません。 | CHAP 設定をチェックします。ストレージシステムのインバウンド設定とアウトバウンド設定には、同じユーザ名およびパスワードを使用できません。<br><br>• ストレージシステムのインバウンドクレデンシャルは、イニシエータのアウトバウンドクレデンシャルと一致する必要があります<br>• ストレージシステムのアウトバウンドクレデンシャルは、イニシエータのインバウンドクレデンシャルと一致する必要があります |

**iSCSI LIF**の自動フェイルオーバーの有効化または無効化

## ONTAP 9.11.1以降にアップグレードした場合は、ONTAP 9.10.1以前で作成したすべてのiSCSI LIFでLIFの自動フェイルオーバーを手動で有効にする必要があります。

ONTAP 9 .11.1以降では、オールフラッシュSANアレイプラットフォームでiSCSI LIFに対してLIFの自動フェイルオーバーを有効にすることができます。ストレージフェイルオーバーが発生すると、iSCSI LIFはホームノードまたはポートからHAパートナーノードまたはポートに自動的に移行され、フェイルオーバーの完了後に再び移行されます。または、iSCSI LIFのポートが正常な状態でなくなった場合、そのLIFは現在のホームノードの正常なポートに自動的に移行され、ポートが正常な状態に戻った時点で元のポートに戻ります。を使用すると、iSCSIで実行されているSANワークロードは、フェイルオーバー後にI/Oサービスを迅速に再開できます。

ONTAP 9 .11.1以降では、次のいずれかの条件に該当する場合、新しく作成したiSCSI LIFでLIFの自動フェイルオーバーがデフォルトで有効になります。

- SVMにiSCSI LIFがありません
- LIFの自動フェイルオーバーがSVMのすべてのiSCSI LIFで有効になっている

**iSCSI LIF**の自動フェイルオーバーの有効化

ONTAP 9.10.1以前で作成したiSCSI LIFでは、デフォルトでLIFの自動フェイルオーバーが有効になっていません。SVM上にLIFの自動フェイルオーバーが有効になっていないiSCSI LIFがある場合、新しく作成したLIFでもLIFの自動フェイルオーバーは有効になりません。LIFの自動フェイルオーバーが有効になっていない状態

でフェイルオーバーが発生すると、iSCSI LIFは移行されません。

詳細については、をご覧ください "LIFのフェイルオーバーとギブバック"。

ステップ

1. iSCSI LIFの自動フェイルオーバーを有効にします。

```
network interface modify -vserver <SVM_name> -lif <iscsi_lif> -failover
-policy sfo-partner-only -auto-revert true
```

SVM上のすべてのiSCSI LIFを更新するには、の代わりに `lif`を使用し `-lif*`ます。

#### iSCSI LIFの自動フェイルオーバーを無効にする

ONTAP 9 10.1以前で作成したiSCSI LIFに対するiSCSI LIFの自動フェイルオーバーを有効にしていた場合は、無効にすることもできます。

ステップ

1. iSCSI LIFの自動フェイルオーバーを無効にします。

```
network interface modify -vserver <SVM_name> -lif <iscsi_lif> -failover
-policy disabled -auto-revert false
```

SVM上のすべてのiSCSI LIFを更新するには、の代わりに `lif`を使用し `-lif*`ます。

関連情報

- "LIFの作成"
- シユトウ"LIFを移行する"
- シユトウ"LIFをホームポートにリバートします。"
- "LIFのフェイルオーバーを設定する"

## FCプロトコルを管理します。

#### FC用のSVMの設定

### FC用にStorage Virtual Machine（SVM）を設定するには、SVM用のLIFを作成し、それらのLIFにFCプロトコルを割り当てる必要があります。

開始する前に

FCライセンス（"ONTAP Oneに付属"）があり、有効になっている必要があります。FCライセンスが有効になっていない場合、LIFとSVMはオンラインとして表示されますが、動作ステータスはになります。 `down`LIFとSVMを動作させるには、FCサービスを有効にする必要があります。イニシエータをホストするには、SVM内のすべてのFC LIFで単一イニシエータゾーニングを使用する必要があります。

タスクの内容

NetAppでは、FCプロトコルを使用してデータを提供する各SVMについて、ノードごとに少なくとも1つのFC LIFがサポートされます。ノードごとに1つのLIFを接続した状態で、ノードごとに2つのLIFと2つのファブリックを使用する必要があります。これにより、ノードレイヤとファブリックで冗長性が確保されます。

例 **8.** 手順

**System Manager**

ONTAP System Manager（9.7以降）でiSCSI用のStorage VMを設定します。

| 新しい**Storage VM**で**FC**を設定する方法 | 既存の**Storage VM**に**FC**を設定するには |
| --- | --- |
| 1. System Managerで、* Storage > Storage VM*をクリックし、* Add *をクリックします。<br>2. Storage VMの名前を入力してください。<br>3. アクセスプロトコル*として「* FC」を選択します。<br>4. [FCを有効にする]をクリックします。+ FCポートが自動的に割り当てられます。<br>5. [ 保存（ Save ） ] をクリックします。 | 1. System Manager で、 * Storage > Storage VM*をクリックします。<br>2. 設定するStorage VMをクリックします。<br>3. [Settings]*タブをクリックし、FCプロトコルの横にあるをクリックし ⚙ ます。<br>4. Enable FC（FCを有効にする）をクリックし、ネットワークインタフェースのIPアドレスとサブネットマスクを入力します。+ FCポートが自動的に割り当てられます。<br>5. [ 保存（ Save ） ] をクリックします。 |

**CLI**

1. SVMでFCサービスを有効にします。

   ```
   vserver fcp create -vserver vserver_name -status-admin up
   ```

2. FCを提供する各ノードのSVM用のLIFを2つ作成します。

   - ONTAP 9.6以降：

     ```
     network interface create -vserver vserver_name -lif lif_name -data
     -protocol fcp -service-policy default-data-fcp -home-node node_name
     -home-port port_name -address ip_address -netmask netmask -status-admin
     up
     ```

   - ONTAP 9.5以前：

     ```
     network interface create -vserver vserver_name -lif lif_name -role data
     -data-protocol fcp -home-node node_name -home-port port
     ```

3. LIFが作成され、動作ステータスがになっていることを確認し `online`ます。

   ```
   network interface show -vserver vserver_name lif_name
   ```

関連情報

"NetAppのサポート"

"NetApp Interoperability Matrix Tool"

クラスタSAN環境でのLIFに関する考慮事項

### SVMのFCサービスを削除する

Storage Virtual Machine（SVM）の不要になったFCサービスは削除できます。

必要なもの

SVM の FC サービスを削除するには、事前に管理ステータスを「所有」にする必要があります。管理ステータスをdownに設定するには、コマンドまたは `vserver fcp stop`コマンドを使用し `vserver fcp modify`ます。

手順

1. コマンドを使用し `vserver fcp stop`て、LUNへのI/Oを停止します。

   ```
   vserver fcp stop -vserver vs_1
   ```

2. コマンドを使用し `vserver fcp delete`て、SVMからサービスを削除します。

   ```
   vserver fcp delete -vserver vs_1
   ```

3. を使用し `vserver fcp show`て、FCサービスがSVMから削除されたことを確認します。

   ```
   vserver fcp show -vserver vs_1
   ```

### FCoEジャンボフレーム用のMTUの推奨設定

Fibre Channel over Ethernet（FCoE）の場合は、CNAのイーサネットアダプタ部分のジャンボフレームを9000 MTUで設定する必要があります。CNAのFCoEアダプタ部分については、ジャンボフレームを1500 MTU以上に設定する必要があります。イニシエータ、ターゲット、および介在するすべてのスイッチがジャンボフレームをサポートし、ジャンボフレーム用に設定されている場合にのみ、ジャンボフレームを設定します。

## 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
```

# FCアダプタを搭載したシステムを管理する

## FCアダプタを搭載したシステムを管理する

オンボードFCアダプタとFCアダプタカードを管理するためのコマンドを使用できます。これらのコマンドを使用して、アダプタモードの設定、アダプタ情報の表示、および速度の変更を行うことができます。

ほとんどのストレージシステムには、イニシエータまたはターゲットとして設定できるオンボードFCアダプタが搭載されています。イニシエータまたはターゲットとして設定されたFCアダプタカードを使用することもできます。イニシエータはバックエンドディスクシェルフに接続します。場合によっては、外部ストレージアレイ（FlexArray）にも接続します。ターゲットはFCスイッチにのみ接続します。FCターゲットのHBAポートとスイッチポートの速度は、両方とも同じ値に設定し、autoには設定しないでください。

関連情報

"SAN構成"

## FCアダプタの管理用コマンド

FC コマンドを使用して、ストレージコントローラの FC ターゲットアダプタ、 FC イニシエータアダプタ、およびオンボード FC アダプタを管理できます。FC アダプタの管理に使用するコマンドは、 FC プロトコルと FC-NVMe プロトコルで同じです。

FC イニシエータアダプタのコマンドは、ノードレベルでのみ機能します。FCイニシエータアダプタのコマンドを使用する前に、コマンドを使用する必要があります `run -node node_name`。

### FC ターゲットアダプタの管理用コマンド

| 状況 | 使用するコマンド |
| --- | --- |
| ノードの FC アダプタ情報を表示する | `network fcp adapter show` |
| FC ターゲットアダプタのパラメータを変更する | `network fcp adapter modify` |
| FC プロトコルトラフィック情報を表示します | `run -node node_name sysstat -f` |
| FC プロトコルの実行時間を表示します | `run -node node_name uptime` |

| 状況 | 使用するコマンド |
| --- | --- |
| アダプタの設定とステータスを表示します | `run -node node_name sysconfig -v adapter` |
| 拡張カードが取り付けられていること、および構成にエラーがないかどうかを確認します | `run -node node_name sysconfig -ac` |
| コマンドのマニュアルページを表示します | `man command_name` |

**FC** イニシエータアダプタの管理用コマンド

| 状況 | 使用するコマンド |
| --- | --- |
| ノードのすべてのイニシエータおよびそのアダプタの情報を表示する | `run -node node_name storage show adapter` |
| アダプタの設定とステータスを表示します | `run -node node_name sysconfig -v adapter` |
| 拡張カードが取り付けられていること、および構成にエラーがないかどうかを確認します | `run -node node_name sysconfig -ac` |

オンボード **FC** アダプタの管理用コマンド

| 状況 | 使用するコマンド |
| --- | --- |
| オンボード FC ポートのステータスを表示します | `run -node node_name system hardware unified-connect show` |

### FCアダプタの設定

オンボードのFCポートは、それぞれイニシエータまたはターゲットとして個別に構成できます。特定のFCアダプタのポートは、オンボードのFCポートと同様に、ターゲットポートまたはイニシエータポートとして個別に構成することもできます。ターゲットモードに設定できるアダプタのリストについては、を参照"NetApp Hardware Universe"してください。

ターゲットモードは、ポートをFCイニシエータに接続するために使用されます。イニシエータモードは、テープドライブ、テープライブラリ、またはFlexArray仮想化またはForeign LUN Import（FLI）を使用するサードパーティストレージへのポートの接続に使用されます。

FCアダプタを設定する手順は、FCプロトコルとFC-NVMeプロトコルで同じです。ただし、FC-NVMeをサポートするFCアダプタは一部のみです。FC-NVMeプロトコルをサポートするアダプタのリストについては、を参照してください"NetApp Hardware Universe"。

### FCアダプタのターゲットモード設定

手順

1. アダプタをオフラインにします。

   ```
   node run -node node_name storage disable adapter adapter_name
   ```

   アダプタがオフラインにならない場合は、システムの適切なアダプタポートからケーブルを取り外すこともできます。

2. アダプタをイニシエータからターゲットに変更します。

   ```
   system hardware unified-connect modify -t target -node node_name adapter
   adapter_name
   ```

3. 変更したアダプタをホストしているノードをリブートします。
4. ターゲットポートの設定が正しいことを確認します。

   ```
   network fcp adapter show -node node_name
   ```

5. アダプタをオンラインにします。

   ```
   network fcp adapter modify -node node_name -adapter adapter_port -state up
   ```

### FCアダプタのイニシエータモード設定

必要なもの

- アダプタのLIFを、メンバーになっているすべてのポートセットから削除する必要があります。
- 物理ポートのパーソナリティをターゲットからイニシエータに変更する前に、変更対象の物理ポートを使用するすべてのStorage Virtual Machine（SVM）のすべてのLIFを移行または破棄する必要があります。

NVMe/FCではイニシエータモードがサポートされます。

手順

1. アダプタからすべてのLIFを削除します。

   ```
   network interface delete -vserver SVM_name -lif LIF_name,LIF_name
   ```

2. アダプタをオフラインにします。

   ```
   network fcp adapter modify -node node_name -adapter adapter_port -status-admin
   down
   ```

   アダプタがオフラインにならない場合は、システムの適切なアダプタポートからケーブルを取り外すこともできます。

3. アダプタをターゲットからイニシエータに変更します。

   ```
   system hardware unified-connect modify -t initiator adapter_port
   ```

4. 変更したアダプタをホストしているノードをリブートします。
5. 構成に対してFCポートが正しい状態で設定されていることを確認します。

   `system hardware unified-connect show`

6. アダプタをオンラインに戻します。

   `node run -node node_name storage enable adapter adapter_port`

アダプタ設定の表示

## 特定のコマンドを使用して、FC / UTAアダプタに関する情報を表示できます。

#### FCターゲットアダプタ

ステップ

1. アダプタ情報を表示するには、コマンドを使用し `network fcp adapter show`ます。 `network fcp adapter show -instance -node node1 -adapter 0a`

   出力には、使用されている各スロットのシステム設定情報およびアダプタ情報が表示されます。

#### ユニファイドターゲットアダプタ（UTA）X1143A-R6

手順

1. ケーブルを接続していない状態でコントローラをブートします。
2. コマンドを実行し `system hardware unified-connect show`て、ポートの設定とモジュールを確認します。
3. CNAとポートを設定する前に、ポート情報を確認してください。

#### UTA2ポートのCNAモードからFCモードへの変更

## FCイニシエータモードとFCターゲットモードをサポートするには、UTA2ポートをConverged Network Adapter（CNA；統合ネットワークアダプタ）モードからFibre Channel（FC；ファイバチャネル）モードに変更する必要があります。ポートをネットワークに接続する物理メディアを変更する必要がある場合は、パーソナリティを CNA モードから FC モードに変更します。

手順

1. アダプタをオフラインにします。

   `network fcp adapter modify -node node_name -adapter adapter_name -status-admin down`

2. ポートのモードを変更します。

   `ucadmin modify -node node_name -adapter adapter_name -mode fcp`

3. ノードをリブートし、アダプタをオンラインにします。

```
network fcp adapter modify -node node_name -adapter adapter_name -status-admin
up
```

4. 状況に応じて、管理者にポートの削除を依頼するか、 VIF マネージャでポートを削除します。

   - ポートが LIF のホームポートとして使用されている場合、インターフェイスグループ（ ifgrp ）のメンバーである場合、または VLAN をホストしている場合は、管理者は次の作業を行う必要があります。

     i. LIF を移動するか、 ifgrp からポートを削除する、または VLAN をそれぞれ削除します。

     ii. コマンドを実行して、ポートを手動で削除し `network port delete`ます。

     コマンドが失敗した場合は `network port delete`、エラーに対処してからもう一度コマンドを実行する必要があります。

   - ポートが LIF のホームポートとして使用されていない場合、 ifgrp のメンバーでない場合、および VLAN をホストしていない場合は、リブート時に VIF マネージャのレコードからポートが削除されます。

     VIFマネージャでポートが削除されない場合は、管理者がリブート後にコマンドを使用して手動で削除する必要があります `network port delete`。

```
net-f8040-34::> network port show

    Node: net-f8040-34-01
                                                          Speed(Mbps) Health
    Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
    --------- ------------ ---------------- ---- ---- -----------
--------
    ...
    e0i       Default      Default          down 1500  auto/10     -
    e0f       Default      Default          down 1500  auto/10     -
    ...

    net-f8040-34::> ucadmin show
                               Current  Current    Pending  Pending
Admin
    Node            Adapter   Mode     Type       Mode     Type
Status
    ------------    -------   -------  ---------  -------  ---------
-----------
    net-f8040-34-01   0e       cna      target     -        -
offline
    net-f8040-34-01   0f       cna      target     -        -
offline
    ...

    net-f8040-34::> network interface create -vs net-f8040-34 -lif m
-role
```

```
node-mgmt-home-node net-f8040-34-01 -home-port e0e -address 10.1.1.1
-netmask 255.255.255.0


    net-f8040-34::> network interface show -fields home-port, curr-port

    vserver lif                   home-port curr-port
    ------- --------------------- --------- ---------
    Cluster net-f8040-34-01_clus1 e0a       e0a
    Cluster net-f8040-34-01_clus2 e0b       e0b
    Cluster net-f8040-34-01_clus3 e0c       e0c
    Cluster net-f8040-34-01_clus4 e0d       e0d
    net-f8040-34
            cluster_mgmt          e0M       e0M
    net-f8040-34
            m                     e0e       e0i
    net-f8040-34
            net-f8040-34-01_mgmt1 e0M       e0M
    7 entries were displayed.

    net-f8040-34::> ucadmin modify local 0e fc

    Warning: Mode on adapter 0e and also adapter 0f will be changed to
fc.
    Do you want to continue? {y|n}: y
    Any changes will take effect after rebooting the system. Use the
"system node reboot" command to reboot.

    net-f8040-34::> reboot local
      (system node reboot)

    Warning: Are you sure you want to reboot node "net-f8040-34-01"?
    {y|n}: y
```

5. 適切な SFP+ が取り付けられていることを確認します。

   `network fcp adapter show -instance -node -adapter`

   CNAの場合は、10GbイーサネットSFPを使用する必要があります。FC の場合は、ノードで構成を変更する前に、 8Gb SFP または 16Gb SFP を使用します。

**CNA / UTA2**ターゲットアダプタの光モジュールの変更

ユニファイドターゲットアダプタ（CNA / UTA2）用に選択したパーソナリティモードをサポートするように、ユニファイドターゲットアダプタ（CNA / UTA2）の光モジュールを変更する必要があります。

手順

1. カードで使用されている現在の SFP+ を確認します。次に、現在の SFP+ を、優先して使用するパーソナリティ（ FC または CNA ）に適した SFP+ に差し替えます。
2. X1143A-R6アダプタから現在の光モジュールを取り外します。
3. 使用するパーソナリティモード（FCまたはCNA）光ファイバに適したモジュールを挿入します。
4. 適切な SFP+ が取り付けられていることを確認します。

   ```
   network fcp adapter show -instance -node -adapter
   ```

   サポートされている SFP+ モジュールと Cisco ブランドの銅線（ Twinax ）ケーブルについては、 Hardware Universe を参照してください。

関連情報

"NetApp Hardware Universe"

**X1143A-R6**アダプタでサポートされるポート構成

## FCターゲットモードは、X1143A-R6アダプタポートのデフォルト設定です。ただし、このアダプタのポートは、10GbイーサネットポートおよびFCoEポート、または16Gb FCポートとして設定できます。

イーサネットおよびFCoE用に設定した場合、X1143A-R6アダプタは、同じ10-GBEポート上でNICおよびFCoEターゲットトラフィックを同時にサポートします。FC用に設定した場合、同じASICを共有する2ポートの各ペアをFCターゲットモードまたはFCイニシエータモード用に個別に設定できます。つまり、1つのX1143A-R6アダプタで、1つの2ポートペアでFCターゲットモードをサポートし、もう1つの2ポートペアでFCイニシエータモードをサポートできます。

関連情報

"NetApp Hardware Universe"

"SAN構成"

ポートの設定

## ユニファイドターゲットアダプタ（ X1143A-R6 ）を設定するには、同じチップ上の隣接する 2 個のポートを同じパーソナリティモードで設定する必要があります。

手順

1. コマンドを使用して、必要に応じてFibre Channel（FC；ファイバチャネル）またはConverged Network Adapter（CNA；統合ネットワークアダプタ）にポートを設定し `system node hardware unified-connect modify`ます。
2. FC または 10Gb イーサネットに適したケーブルを接続します。
3. 適切な SFP+ が取り付けられていることを確認します。

   ```
   network fcp adapter show -instance -node -adapter
   ```

   CNAの場合は、10GbイーサネットSFPを使用する必要があります。FC の場合は、接続先の FC ファブリ

ックに応じて 8Gb SFP または 16Gb SFP を使用します。

**X1133A-R6**アダプタ使用時の接続の切断を防止

## 別のX1133A-R6 HBAへの冗長パスをシステムに設定することで、ポート障害時に接続が失われないようにすることができます。

X1133A-R6 HBA は、 4 ポート 16Gb の FC アダプタで、 2 組の 2 ポートペアで構成されます。X1133A-R6 アダプタは、ターゲットモードまたはイニシエータモードとして設定できます。2 ポートペアはそれぞれ 1 つの ASIC でサポートされます（たとえば、ポート 1 とポート 2 は ASIC 1 、ポート 3 とポート 4 は ASIC 2 ）。単一のASIC上の両方のポートは、ターゲットモードまたはイニシエータモードのいずれかで同じモードで動作するように設定する必要があります。ペアをサポートする ASIC でエラーが発生すると、そのペアの両方のポートがオフラインになります。

接続が切断されないようにするには、別の X1133A-R6 HBA への冗長パスか、 HBA の別の ASIC でサポートされるポートへの冗長パスを構成します。

## すべての**SAN**プロトコルの**LIF**を管理します。

すべての**SAN**プロトコルの**LIF**を管理します。

## SAN環境でクラスタのフェイルオーバー機能を利用するには、イニシエータでMultipath I/O（MPIO；マルチパスI/O）とAsymmetric Logical Unit Access（ALUA；非対称論理ユニットアクセス）を使用する必要があります。ノードで障害が発生しても、LIFは障害が発生したパートナーノードのIPアドレスを引き継ぎません。代わりに、MPIOソフトウェアが、ホストのALUAを使用して、LIF経由でLUNにアクセスするための適切なパスを選択します。

HAペアの各ノードから1つ以上のiSCSIパスを作成し、HAペアで処理されるLUNに論理インターフェイス（LIF）を使用してアクセスできるようにする必要があります。SANをサポートするStorage Virtual Machine（SVM）ごとに管理LIFを1つ設定する必要があります。

直接接続またはイーサネットスイッチを使用した接続がサポートされています。両方のタイプの接続用にLIFを作成する必要があります。

- SANをサポートするStorage Virtual Machine（SVM）ごとに管理LIFを1つ設定する必要があります。ノードごとに2つのLIFを設定できます。LIFはFCで使用するファブリックごとに1つ、iSCSI用のイーサネットネットワークを分離します。

作成したLIFは、ポートセットから削除したり、Storage Virtual Machine（SVM）内の別のノードに移動したり、LIFを削除したりできます。

関連情報

- "LIFの設定の概要"
- "LIFの作成"

**NVMe LIF**の設定

## NVMe LIFを設定するときは、一定の要件を満たす必要があります。

開始する前に

LIFを作成するFCアダプタでNVMeがサポートされている必要があります。サポートされているアダプタをに示し "Hardware Universe"ます。

タスクの内容

12.1以降では、ノードあたり2つのONTAP 9 LIFを設定できます。最大ノード数は12です。NVMe.11.1以前では、ノードごとに2つのONTAP 9 LIFを設定できます（最大ノード数は2）。

NVMe LIFを作成するときは、次のルールが適用されます。

- データLIFで使用できるデータプロトコルはNVMeだけです。
- SANをサポートするSVMごとに管理LIFを1つ設定する必要があります。
- ONTAP 9 .5以降の場合は、ネームスペースを含むノードとそのHAパートナーにNVMe LIFを設定する必要があります。
- ONTAP 9 .4の場合のみ：
  - NVMe LIFとネームスペースは同じノードでホストされている必要があります。
  - 設定できる NVMe データ LIF は SVM ごとに 1 つだけです。

手順

1. LIFを作成します。

```
network interface create -vserver <SVM_name> -lif <LIF_name> -role
<LIF_role> -data-protocol {fc-nvme|nvme-tcp} -home-node <home_node>
-home-port <home_port>
```

NVMe/TCPはONTAP 9 10.1以降で使用できます。

2. LIFが作成されたことを確認します。

```
network interface show -vserver <SVM_name>
```

作成後、NVMe/TCP LIFはポート8009で検出をリスンします。

**SAN LIF**を移動する際の注意事項

クラスタへのノードの追加やクラスタからのノードの削除など、クラスタの内容を変更する場合にのみ、LIFを移動する必要があります。LIFを移動する場合は、FCファブリックを再ゾーニングしたり、クラスタに接続されたホストと新しいターゲットインターフェイスの間に新しいiSCSIセッションを作成したりする必要はありません。

コマンドを使用してSAN LIFを移動することはできません `network interface move`。SAN LIFを移動するには、対象のLIFをオフラインにし、別のホームノードまたはポートに移動してから、移動先の新しい場所でLIFをオンラインに戻します。ONTAP SANソリューションでは、Asymmetric Logical Unit Access（ALUA；

非対称論理ユニットアクセス）によってパスの冗長化と自動選択が実現します。そのため、移動時にLIFがオフラインになっても、I/Oの中断はありません。ホストは再試行してから別のLIFにI/Oを移動するだけです。

LIFの移動を使用すると、システムを停止することなく次の処理を実行できます。

- クラスタの1つのHAペアを、LUNデータにアクセスするホストに対して透過的な方法で、アップグレードされたHAペアに置き換える
- ターゲットインターフェイスカードのアップグレード
- Storage Virtual Machine（SVM）のリソースをクラスタ内のノードセットから別のノードセットに移行する

ポートセットから**SAN LIF**を削除する

削除または移動するLIFがポートセットに含まれている場合、LIFを削除または移動する前に、そのLIFをポートセットから削除する必要があります。

タスクの内容

次の手順1は、1つのLIFがポートセットにある場合にのみ実行する必要があります。ポートセットがイニシエータグループにバインドされている場合、ポートセット内の最後のLIFを削除することはできません。複数のLIFがポートセットにある場合は、手順2から始めることができます。

手順

1. ポートセットにLIFが1つしかない場合は、コマンドを使用し `lun igroup unbind`てイニシエータグループからポートセットのバインドを解除します。

   イニシエータグループとポートセットのバインドを解除すると、イニシエータグループ内のすべてのイニシエータが、すべてのネットワークインターフェイス上のそのイニシエータグループにマッピングされているすべてのターゲットLUNにアクセスできるようになります。

   ```
   cluster1::>lun igroup unbind -vserver vs1 -igroup ig1
   ```

2. コマンドを使用し `lun portset remove`て、ポートセットからLIFを削除します。

   ```
   cluster1::> port set remove -vserver vs1 -portset ps1 -port-name lif1
   ```

**SAN LIF**を移動する

ノードをオフラインにする必要がある場合、 SAN LIF を移動して WWPN などの設定情報を保持しておけば、スイッチファブリックの再ゾーニングを行わずに済みます。SAN LIF は移動前にオフラインにする必要があるため、ホストトラフィックについては、ホストマルチパスソフトウェアを使用して、 LUN への無停止アクセスを確保する必要があります。SAN LIF はクラスタ内の任意のノードに移動できますが、 SAN LIF を別の Storage Virtual Machine （ SVM ）に移動することはできません。

必要なもの

LIF がポートセットのメンバーである場合、 LIF を別のノードに移動する前に、その LIF をポートセットから削除しておく必要があります。

タスクの内容

移動する LIF のデスティネーションノードおよび物理ポートは、同じ FC ファブリック上またはイーサネットネットワーク上に存在する必要があります。適切にゾーニングされていない別のファブリック上に LIF を移動したり、 iSCSI イニシエータとターゲットを接続していないイーサネットネットワーク上に LIF を移動したりすると、その LIF をオンラインに戻しても接続できなくなります。

手順

1. LIFの管理ステータスと動作ステータスを表示します。

   ```
   network interface show -vserver vserver_name
   ```

2. LIFのステータスを（オフライン）に変更し `down`ます。

   ```
   network interface modify -vserver vserver_name -lif LIF_name -status-admin
   down
   ```

3. LIFを新しいノードとポートに割り当てます。

   ```
   network interface modify -vserver vserver_name -lif LIF_name -home-node
   node_name -home-port port_name
   ```

4. LIFのステータスを（オンライン）に変更し `up`ます。

   ```
   network interface modify -vserver vserver_name -lif LIF_name -status-admin up
   ```

5. 変更内容を確認します。

   ```
   network interface show -vserver vserver_name
   ```

**SAN**環境で**LIF**を削除する

## LIFを削除する前に、LIFに接続されているホストが別のパスを介してLUNにアクセスできることを確認する必要があります。

必要なもの

削除するLIFがポートセットのメンバーである場合、LIFを削除する前にポートセットからLIFを削除する必要があります。

**System Manager**

ONTAP System Manager（9.7以降）でLIFを削除する。

手順

1. System Managerで、* Network > Overview をクリックし、 Network Interfaces *を選択します。
2. LIFを削除するStorage VMを選択します。
3. をクリック ⋮ し、*[削除]*を選択します。

**CLI**

ONTAP CLIを使用してLIFを削除する。

手順

1. 削除するLIFの名前と現在のポートを確認します。

   ```
   network interface show –vserver vserver_name
   ```

2. LIFを削除します。

   ```
   network interface delete

   network interface delete -vserver vs1 -lif lif1
   ```

3. LIFが削除されたことを確認します。

   ```
   network interface show

   network interface show -vserver vs1
   ```

   ```
   Logical Status     Network                       Current   Current Is
   Vserver Interface  Admin/Oper Address/Mask     Node      Port
   Home
   ------- ---------- ---------- ---------------- --------- -------
   ----
   vs1
           lif2       up/up      192.168.2.72/24  node-01   e0b
   true
           lif3       up/up      192.168.2.73/24  node-01   e0b
   true
   ```

クラスタにノードを追加する際の**SAN LIF**の要件

## クラスタにノードを追加する場合は、一定の考慮事項について理解しておく必要があります。

- 新しいノードにLUNを作成する前に、必要に応じて新しいノードにLIFを作成する必要があります。
- これらのLIFは、ホストスタックとプロトコルの指示に従って、ホストから検出する必要があります。
- クラスタインターコネクトネットワークを使用せずにLUNやボリュームを移動できるように、新しいノードにLIFを作成する必要があります。

### ホストによる**iSCSI SendTargets**検出処理に対して**FQDN**を返すように**iSCSI LIF**を設定

ONTAP 9以降では、ホストOSから送信されたiSCSI SendTargets検出処理で完全修飾ドメイン名（FQDN）を返すようにiSCSI LIFを設定できます。FQDNを返すと、ホストOSとストレージサービスの間にネットワークアドレス変換（NAT）デバイスがある場合に便利です。

#### タスクの内容

IPアドレスはNATデバイスの片側では意味がありませんが、FQDNであれば両側で意味があります。

FQDN値の互換性の上限は、すべてのホストOSで128文字です。

#### 手順

1. 権限の設定をadvancedに変更します。

   ```
   set -privilege advanced
   ```

2. FQDNを返すようにiSCSI LIFを設定します。

   ```
   vserver iscsi interface modify -vserver SVM_name -lif iscsi_LIF_name
   -sendtargets_fqdn FQDN
   ```

   次の例では、FQDNとしてstoragehost-005.example.comを返すようにiSCSI LIFを設定しています。

   ```
   vserver iscsi interface modify -vserver vs1 -lif vs1_iscsi1 -sendtargets-fqdn
   storagehost-005.example.com
   ```

3. SendTargetsがFQDNになっていることを確認します。

   ```
   vserver iscsi interface show -vserver SVM_name -fields sendtargets-fqdn
   ```

   この例では、sendtargets-fqdn出力フィールドにstoragehost-005.example.comが表示されています。

   ```
   cluster::vserver*> vserver iscsi interface show -vserver vs1 -fields
   sendtargets-fqdn
   vserver lif        sendtargets-fqdn
   ------- ---------- --------------------------
   vs1     vs1_iscsi1 storagehost-005.example.com
   vs1     vs1_iscsi2 storagehost-006.example.com
   ```

#### 関連情報

"ONTAPコマンド リファレンス"

## SANプロトコルのONTAPスペース割り当てを有効にする

ONTAPのスペース割り当ては、LUNまたはNVMeネームスペースがスペース不足になった場合にオフラインになるのを防ぎ、SANホストでスペースを再生できるようにします。

ONTAPでスペースが割り当てられるかどうかは、使用しているSANプロトコルとONTAPのバージョンによって異なります。lun.16.1以降では、新規に作成するすべてのONTAP 9およびネームスペースに対して、iSCSI、FC、およびNVMeの各プロトコルに対してスペース割り当てがデフォルトで有効になります。

| ONTAPのバージョン | プロトコル | スペース割り当て |
|---|---|---|
| 9.16.1以降 | • iSCSI<br>• FC<br>• NVMe | 新規作成されたLUNおよびネームスペースに対してデフォルトで有効 |
| 9.15.1 | • iSCSI<br>• FC | 新規作成されたLUNに対してデフォルトで有効 |
| | NVMe | サポート対象外 |
| 9.14.1以前 | • iSCSI<br>• FC | 新規作成されたLUNではデフォルトで無効 |
| | NVMe | サポート対象外 |

スペース割り当てが有効な場合：

- LUNまたはネームスペースのスペースが不足すると、ONTAPはホストに書き込み処理に使用できる空きスペースがないことを通知します。そのため、LUNまたはネームスペースはオンラインのままで、読み取り処理は継続されます。ホストの設定に応じて、成功するか、ホストのファイルシステムがオフラインになるまで、ホストは書き込み処理を再試行します。LUNまたはネームスペースで使用可能な空きスペースが増えると、書き込み処理が再開されます。

  スペース割り当てが有効になっていない場合、LUNまたはネームスペースのスペースが不足すると、すべてのI/O処理が失敗し、LUNまたはネームスペースがオフラインになります。通常の処理を再開するには、スペースの問題を解決する必要があります。パスとデバイスを動作状態にリストアするには、ホストでLUNデバイスの再スキャンが必要になる場合もあります。

- ホストはSCSIまたはNVMe（とも呼ばれる `TRIM`）処理を実行できます `UNMAP`。マッピング解除処理を使用すると、有効なデータがなくなったために不要になったデータブロックをホストが特定できます。識別は通常、ファイルの削除後に行われます。その後、ストレージシステムはこれらのデータブロックの割り当てを解除して、スペースを他の場所で消費できるようにします。このように割り当てを解除することで、特にデータの書き替え率が高いファイルシステムでは、全体的なストレージ効率が大幅に向上します。

開始する前に

スペース割り当てを有効にするには、書き込みを完了できない場合にスペース割り当てエラーを正しく処理で

きるホスト構成が必要です。SCSIまたはNVMeを活用 `UNMAP`するには、SCSI SBC-3標準で定義されている論理ブロックプロビジョニングを使用できる構成が必要です。

現在、スペース割り当てを有効にした場合にシンプロビジョニングをサポートしているホストは次のとおりです。

- Citrix XenServer 6.5以降
- VMware ESXi 5.0以降
- Oracle Linux 6.2 UEKカーネル以降
- Red Hat Enterprise Linux 6.2以降
- SUSE Linux Enterprise Server 11以降
- Solaris 11.1以降
- ウィンドウ

タスクの内容

クラスタをONTAP 9 .15.1以降にアップグレードした場合、ソフトウェアのアップグレード前に作成されたすべてのLUNのスペース割り当て設定は、ホストタイプに関係なく、アップグレード後も変更されません。たとえば、スペース割り当てが無効になっているVMwareホスト用にONTAP 9 .13.1でLUNが作成された場合、ONTAP 9 .15.1にアップグレードしても、そのLUNでのスペース割り当ては無効なままになります。

手順

1. スペース割り当てを有効にします。

```
lun modify -vserver <vserver_name> -volume <volume_name> -lun <lun_name>
-space-allocation enabled
```

2. スペース割り当てが有効になっていることを確認します。

```
lun show -vserver <vserver_name> -volume <volume_name> -lun <lun_name>
-fields space-allocation
```

3. ホストOSでスペース割り当てが有効になっていることを確認します。

VMware ESXiの一部のバージョンなど、一部のホスト構成では、設定の変更が自動的に認識されるため、ユーザの操作は必要ありません。その他の設定では、デバイスの再スキャンが必要になる場合があります。一部のファイルシステムやボリュームマネージャでは、を使用したスペース再生を有効にするために、追加の設定が必要になる場合があります `SCSI UNMAP`。ファイルシステムの再マウントまたはOSの完全なリブートが必要になる場合があります。詳細については、ご使用のホストのドキュメントを参照してください。

**VMware ESXi 8.x**以降の**NVMe**ホスト用のホストの設定

NVMeプロトコルを使用してESXi 8.x以降を実行しているVMwareホストでは、ONTAPでスペース割り当てを有効にしたあとに、ホストで次の手順を実行する必要があります。

手順

1. ESXiホストで、DSMが無効になっていることを確認します。

   ```
   esxcfg-advcfg -g /SCSi/NVmeUseDsmTp4040
   ```

   想定される値は0です。

2. NVMe DSMを有効にします。

   ```
   esxcfg-advcfg -s 1 /Scsi/NvmeUseDsmTp4040
   ```

3. DSMが有効になっていることを確認します。

   ```
   esxcfg-advcfg -g /SCSi/NVmeUseDsmTp4040
   ```

   想定される値は1です。

関連リンク

詳細については、をご覧ください "ESXi 8.x（ONTAP）向けのNVMe-oFホストの設定"。

## 推奨されるボリュームとファイルまたは**LUN**の設定の組み合わせ

### 推奨されるボリュームとファイルまたは**LUN**の設定の組み合わせの概要

使用可能な FlexVol の設定とファイルまたは LUN の設定の組み合わせは、使用するアプリケーションと管理要件によって異なります。これらの組み合わせのメリットとデメリットを理解しておくと、環境に適したボリュームと LUN の設定の組み合わせを決定する際に役立ちます。

推奨されるボリュームと LUN の設定の組み合わせは次のとおりです。

- スペースリザーブファイルまたはスペースリザーブ LUN とシックボリュームプロビジョニング
- スペースリザーブなしのファイルまたはスペースリザーブなしの LUN とシンボリュームプロビジョニング
- スペースリザーブファイルまたはスペースリザーブ LUN とセミシックボリュームプロビジョニング

これらのいずれかの設定の組み合わせとともに、 LUN で SCSI シンプロビジョニングを使用できます。

#### スペースリザーブファイルまたはスペースリザーブ **LUN** とシックボリュームプロビジョニング

- 利点 :*
- スペースリザーブファイルでのすべての書き込み処理が保証されます。スペース不足のために失敗することはありません。
- ボリュームでの Storage Efficiency テクノロジとデータ保護テクノロジに関する制限はありません。
- コストと制限： *
- シックプロビジョニングボリュームをサポートするための十分なスペースをアグリゲートから事前に確保しておく必要があります。

- LUN 作成時に、 LUN の 2 倍のサイズのスペースがボリュームから割り当てられます。

スペースリザーブなしのファイルまたはスペースリザーブなしの **LUN** とシンボリュームプロビジョニング

- 利点 :*
- ボリュームでの Storage Efficiency テクノロジとデータ保護テクノロジに関する制限はありません。
- スペースは使用時に初めて割り当てられます。
- 費用および制限 :*
- 書き込み処理は保証されず、ボリュームの空きスペースが不足すると失敗する場合があります。
- アグリゲートの空きスペースを効果的に管理して、空きスペースが不足しないようにする必要があります。

スペースリザーブファイルまたはスペースリザーブ **LUN** とセミシックボリュームプロビジョニング

- 利点 :*

事前に確保されるスペースがシックボリュームプロビジョニングの場合よりも少なく、ベストエフォートの書き込み保証も提供されます。

- 費用および制限 :*
- このオプションを指定すると、書き込み処理が失敗することがあります。

  このリスクは、ボリュームの空きスペースとデータの揮発性の適切なバランスを維持することで軽減できます。

- Snapshot コピー、 FlexClone ファイル、 FlexClone LUN などのデータ保護オブジェクトは保持できません。
- 重複排除、圧縮、 ODX / コピーオフロードなど、自動で削除できない ONTAP のブロック共有ストレージ効率化機能は使用できません。

環境に適したボリュームと**LUN**の設定の組み合わせの決定

## 環境に関するいくつかの基本的な質問に答えることで、環境に最適なFlexVol volumeとLUNの設定を決定できます。

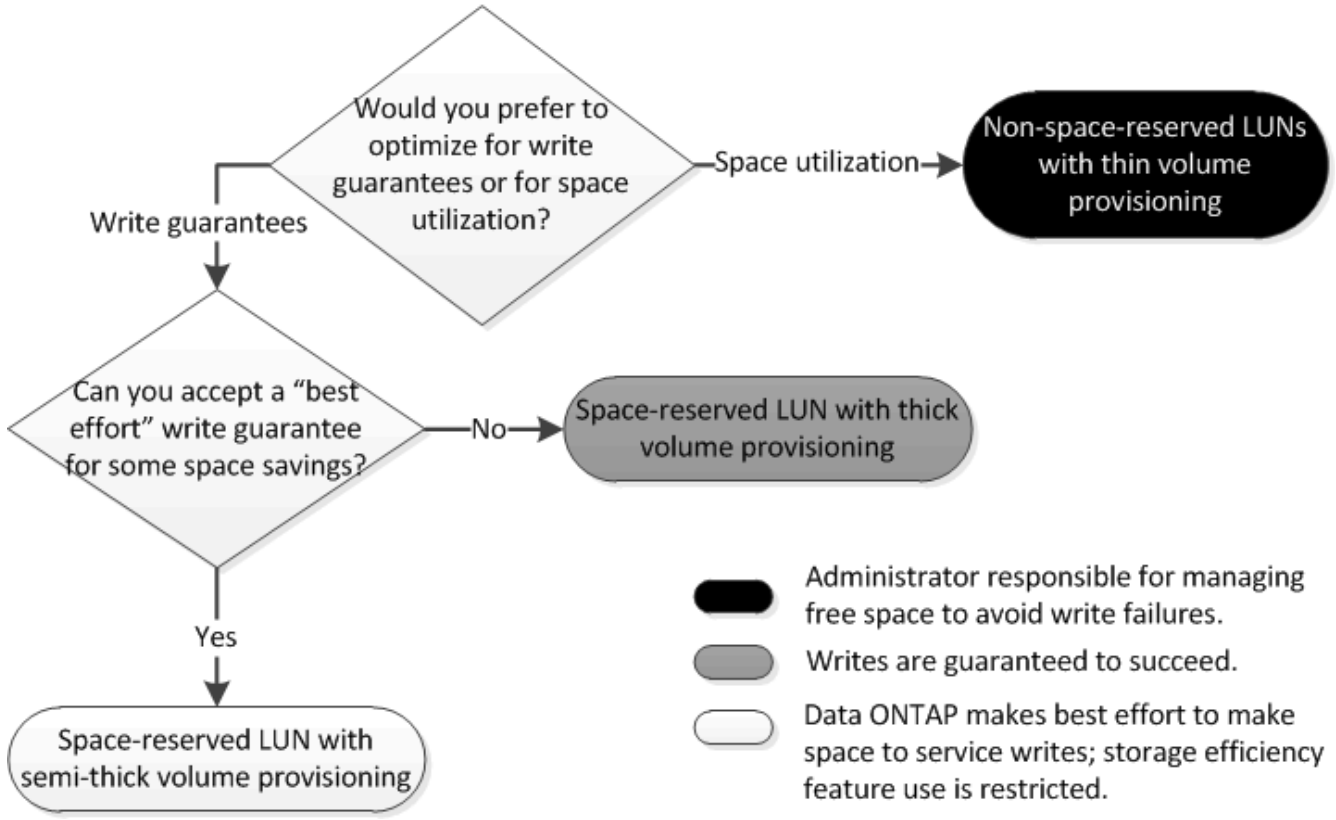
タスクの内容

LUNおよびボリュームの設定を最適化して、ストレージ利用率を最大限に高めたり、書き込みを保証したりすることができます。ストレージ利用要件、および空きスペースを監視して迅速に補充できるかどうかに基づいて、ご使用の環境に適したFlexVol volumeボリュームとLUNボリュームを決定する必要があります。

LUNごとに個別のボリュームを作成する必要はありません。

ステップ

1. 次のデシジョンツリーを使用して、環境に最適なボリュームとLUNの設定の組み合わせを決定してください。




**LUN**のデータ増加率の計算

## スペースリザーブ LUN とスペースリザーブなしの LUN のどちらが適切かを判断するには、時間の経過に伴う LUN データの増加率を把握する必要があります。

タスクの内容

データの増加率が一貫して高い場合は、スペースリザーブLUNの方が適しています。データの増加率が低い場合は、スペースリザーブなしのLUNを検討してください。

OnCommand Insightなどのツールを使用してデータの増加率を計算することも、手動で計算することもできます。手動で計算する手順は次のとおりです。

手順

1. スペースリザーブLUNをセットアップします。
2. 一定期間（1週間など）、LUN上のデータを監視します。

   定期的に発生するデータ増加の代表的なサンプルを形成するのに十分な監視期間があることを確認してください。たとえば、各月末に一貫して大量のデータが増加しているとします。

3. 毎日、増大するデータの量をGB単位で記録します。
4. 監視期間の終了時に、各日の合計を合計し、監視期間の日数で除算します。

   この計算により、平均成長率が算出されます。

例

この例では、200GBのLUNが必要です。LUNを1週間監視し、次の日次データの変更を記録します。

- 日曜日： 20GB
- 月曜日： 18GB
- 火曜日： 17GB
- 水曜日： 20GB
- 木曜日： 20GB
- 金曜日： 23GB
- 土曜日： 22GB

この例では、増加率は（ 20+18+17+20+20+23+22 ） / 7 で求めることができ、 1 日あたり 20GB となります。

スペースリザーブファイルまたはスペースリザーブ**LUN**とシックプロビジョニングボリュームを組み合わせた場合の構成設定

この FlexVol とファイルまたは LUN の設定の組み合わせでは、 Storage Efficiency テクノロジを使用できます。また、事前に十分なスペースが割り当てられるため、空きスペースを能動的に監視する必要がありません。

シックプロビジョニングを使用するボリュームでスペースリザーブファイルまたはスペースリザーブ LUN を設定するには、次の設定が必要です。

| 音量設定 | 値 |
| --- | --- |
| 保証 | ボリューム |
| フラクショナルリザーブ | 100 |
| Snapshotリザーブ | 任意 |
| Snapshotの自動削除 | オプション |
| 自動拡張 | オプション。有効にした場合は、アグリゲートの空きスペースを能動的に監視する必要があります。 |

| ファイルまたは **LUN** の設定 | 値 |
| --- | --- |
| スペースリザベーション | 有効 |

スペースリザーブなしのファイルまたはスペースリザーブなしの**LUN**とシンプロビジョニングボリュームを組み合わせた場合の構成設定

この FlexVol とファイルまたは LUN の設定の組み合わせでは、事前に割り当てられるストレージの量が最小になりますが、スペース不足によるエラーを回避するために空きス

ペースを能動的に管理する必要があります。

シンプロビジョニングボリュームでスペースリザーブなしのファイルまたはスペースリザーブなしの LUN を設定するには、次の設定が必要です。

| 音量設定 | 値 |
| --- | --- |
| 保証 | なし |
| フラクショナルリザーブ | 0 |
| Snapshotリザーブ | 任意 |
| Snapshotの自動削除 | オプション |
| 自動拡張 | オプション |

| ファイルまたは **LUN** の設定 | 値 |
| --- | --- |
| スペースリザベーション | 無効にする |

その他の考慮事項

ボリュームまたはアグリゲートのスペースが不足すると、ファイルまたは LUN への書き込み処理が失敗する場合があります。

ボリュームとアグリゲートの両方の空きスペースを能動的に監視しない場合は、ボリュームの自動拡張を有効にして、ボリュームの最大サイズをアグリゲートのサイズに設定してください。この設定では、アグリゲートの空きスペースを能動的に監視する必要がありますが、ボリュームの空きスペースを監視する必要はありません。

スペースリザーブファイルまたはスペースリザーブ**LUN**とセミシックボリュームプロビジョニングを組み合わせた場合の構成設定

この FlexVol とファイルまたは LUN の設定の組み合わせでは、フルプロビジョニングとの組み合わせに比べて事前に割り当てるストレージが少なくて済みますが、ボリュームに使用できる効率化テクノロジが制限されます。この設定の組み合わせでは、上書きがベストエフォートベースで行われます。

セミシックプロビジョニングを使用するボリュームでスペースリザーブ LUN を設定するには、次の設定が必要です。

| 音量設定 | 値 |
| --- | --- |
| 保証 | ボリューム |
| フラクショナルリザーブ | 0 |

| 音量設定 | 値 |
| --- | --- |
| Snapshotリザーブ | 0 |
| Snapshotの自動削除 | オン。この場合、コミットメントレベルを destroy に設定し、削除リストにすべてのオブジェクトを追加し、トリガーを volume に設定し、すべての FlexClone LUN と FlexClone ファイルの自動削除を有効にします。 |
| 自動拡張 | オプション。有効にした場合は、アグリゲートの空きスペースを能動的に監視する必要があります。 |

| ファイルまたは **LUN** の設定 | 値 |
| --- | --- |
| スペースリザベーション | 有効 |

テクノロジの制限事項

この設定の組み合わせでは、次のボリュームの Storage Efficiency テクノロジを使用できません。

- 圧縮
- 重複排除
- ODX コピーオフロードと FlexClone コピーオフロード
- 自動削除の対象としてマークされていない FlexClone LUN と FlexClone ファイル（アクティブクローン）
- FlexClone サブファイル
- ODX / コピーオフロード

その他の考慮事項

この設定の組み合わせを使用する場合は、次の点を考慮する必要があります。

- 対象の LUN をサポートするボリュームのスペースが不足した場合は、保護データ（ FlexClone LUN 、 FlexClone ファイル、および Snapshot コピー）が削除されます。
- ボリュームの空きスペースが不足すると、書き込み処理がタイムアウトして失敗することがあります。

AFF プラットフォームではデフォルトで圧縮が有効になります。AFF プラットフォームのセミシックプロビジョニングを使用するボリュームに対しては、明示的に圧縮を無効にする必要があります。

# SANのデータ保護

## SANカンキヨウノテエタホコホウホウノカイヨウ

データを保護するには、データのコピーを作成して、偶発的な削除、アプリケーションのクラッシュ、データの破損、災害が発生した場合にデータをリストアできるようにし

ます。ONTAPは、データ保護とバックアップのニーズに応じて、データを保護するためのさまざまな方法を提供します。

**SnapMirror**アクティブ同期

ONTAP 9 .9.1の一般提供開始以降では、目標復旧時間ゼロ（ゼロRTO）または透過的アプリケーションフェイルオーバー（TAF）が提供され、SAN環境でビジネスクリティカルなアプリケーションを自動的にフェイルオーバーできます。SnapMirrorアクティブな同期を実行するには、2つのAFFクラスタまたは2つのオールフラッシュSANアレイ（ASA）クラスタを使用する構成にONTAPメディエーター1.2がインストールされている必要があります。

"SnapMirrorアクティブ同期"

**Snapshot**コピー

LUNの複数のバックアップを手動または自動で作成、スケジュール、および保守できます。Snapshotコピーは、最小限のボリュームスペースしか使用せず、パフォーマンスコストもかかりません。LUNデータを誤って変更または削除してしまった場合でも、最新のSnapshotコピーから簡単かつ迅速にリストアできます。

**FlexClone LUN**（**FlexClone**のライセンスが必要）

アクティブボリューム内やSnapshotコピー内にある別のLUNの書き込み可能なポイントインタイムコピーを提供します。クローンとその親は、相互に影響を及ぼさずに個別に変更できます。

**SnapRestore**（ライセンスが必要）

ボリューム全体のSnapshotコピーから高速かつスペース効率に優れたデータ リカバリを必要に応じて実行できます。SnapRestoreを使用すると、ストレージ システムをリブートしなくても、LUNを以前保存した状態にリストアできます。

データ保護ミラー コピー（**SnapMirror**のライセンスが必要）

非同期のディザスタ リカバリを提供します。そのために、ボリューム上にあるデータのSnapshotコピーを定期的に作成し、それらのSnapshotコピーを通常は別のクラスタ上にあるパートナー ボリュームにローカル エリア ネットワークまたはワイド エリア ネットワーク経由でコピーして保持します。ソース ボリューム上のデータが破損した場合や失われた場合には、パートナー ボリューム上のミラー コピーにより、最新のSnapshotコピーの時点におけるデータをすぐに使用およびリストアすることができます。

**SnapVault**バックアップ（**SnapMirror**のライセンスが必要）

ストレージ効率に優れた、長期間保持できるバックアップを提供します。SnapVault関係により、ボリュームの選択したSnapshotコピーをデスティネーション ボリュームにバックアップし、保持することができます。

テープ バックアップおよびアーカイブ処理を行っている場合は、SnapVaultセカンダリ ボリュームにすでにバックアップされているデータに対してそれらの処理を実行できます。

**SnapDrive for Windows**または**SnapDrive for UNIX**（**SnapDrive**のライセンスが必要）

LUNへのアクセスを設定し、LUNを管理し、ストレージ システムのSnapshotコピーをWindowsまたはUNIXホストから直接管理します。

ネイティブ テープ バックアップ / リカバリ

ONTAPはほとんどの既存のテープ ドライブに対応しており、テープ ベンダーが新しいデバイスのサポートを動的に追加するための方策も用意されています。ONTAPはRemote Magnetic Tape（RMT）プロトコルもサポートしているため、RMT対応システムへのバックアップやリカバリも可能です。

関連情報

"NetAppのマニュアル：「SnapDrive for UNIX」"

"NetAppのマニュアル：「SnapDrive for Windows（現在のリリース）」"

"テープバックアップを使用したデータ保護"

## LUNの移動またはコピーがSnapshotコピーに与える影響

### LUNの移動またはコピーがSnapshotコピーに与える影響の概要

Snapshotコピーはボリュームレベルで作成されます。LUNを別のボリュームにコピーまたは移動すると、コピーまたは移動したボリュームにデスティネーションvolune のSnapshotコピーポリシーが適用されます。デスティネーションボリュームのSnapshotコピーが確立されていない場合、移動またはコピーされたLUNのSnapshotコピーは作成されません。

### Snapshotコピーから単一LUNをリストアする

ボリューム全体をリストアすることなく、ボリューム内の単一 LUN のみを Snapshot コピーからリストアできます。LUN は、元の場所またはボリューム内の新しいパスにリストアできます。この処理では、ボリューム内の他のファイルまたは LUN に影響を与えることなく、単一の LUN だけがリストアされます。ファイルは、ストリームを使用してリストアすることもできます。

必要なもの

- リストア処理を完了するには、ボリュームに十分なスペースが必要です。
  - フラクショナルリザーブが0%のスペースリザーブLUNをリストアする場合は、リストアするLUNの1倍のサイズが必要です。
  - フラクショナルリザーブが100%のスペースリザーブLUNをリストアする場合は、リストアするLUNの2倍のサイズが必要です。
  - スペースリザーブなしのLUNをリストアする場合は、リストアするLUNで実際に使用されているスペースのみが必要です。
- デスティネーション LUN の Snapshot コピーを作成しておく必要があります。

  リストア処理が失敗すると、デスティネーション LUN が切り捨てられる可能性があります。このような場合は、 Snapshot コピーを使用してデータ損失を防ぐことができます。

- ソース LUN の Snapshot コピーを作成しておく必要があります。

  まれに、 LUN のリストアに失敗したときに、ソース LUN が使用不能になることがあります。この場合、

Snapshot コピーを使用して、リストアを試みる直前の状態に LUN を復帰させることができます。

- デスティネーション LUN とソース LUN の OS タイプが同じである必要があります。

  デスティネーション LUN の OS タイプがソース LUN の OS タイプと異なる場合は、リストア処理後、ホストからデスティネーション LUN へのデータアクセスが失われる可能性があります。

手順

1. ホストから、 LUN へのホストアクセスをすべて停止します。
2. ホスト上の LUN をアンマウントして、ホストが LUN にアクセスできないようにします。
3. LUNのマッピングを解除します。

   ```
   lun mapping delete -vserver vserver_name -volume volume_name -lun lun_name
   -igroup igroup_name
   ```

4. LUN のリストア先にする Snapshot コピーを決定します。

   ```
   volume snapshot show -vserver vserver_name -volume volume_name
   ```

5. LUNをリストアする前に、LUNのSnapshotコピーを作成します。

   ```
   volume snapshot create -vserver vserver_name -volume volume_name -snapshot
   snapshot_name
   ```

6. ボリューム内の指定した LUN をリストアします。

   ```
   volume snapshot restore-file -vserver vserver_name -volume volume_name
   -snapshot snapshot_name -path lun_path
   ```

7. 画面の手順に従います。
8. 必要に応じて、LUNをオンラインにします。

   ```
   lun modify -vserver vserver_name -path lun_path -state online
   ```

9. 必要に応じて、LUNを再マッピングします。

   ```
   lun mapping create -vserver vserver_name -volume volume_name -lun lun_name
   -igroup igroup_name
   ```

10. ホストから、 LUN を再マウントします。
11. ホストから、 LUN へのアクセスを再開します。

**Snapshot**コピーからボリューム内のすべての**LUN**をリストア

## コマンドを使用すると、指定したボリューム内のすべてのLUNをSnapshotコピーからリストアできます `volume snapshot restore`。

手順

1. ホストから、LUNへのホストアクセスをすべて停止します。

ボリューム内のLUNへのホストアクセスをすべて停止せずにSnapRestoreを使用すると、データの破損やシステムエラーが発生する可能性があります。

2. ホスト上の LUN をアンマウントして、ホストが LUN にアクセスできないようにします。
3. LUNのマッピングを解除します。

   ```
   lun mapping delete -vserver vserver_name -volume volume_name -lun lun_name
   -igroup igroup_name
   ```

4. ボリュームのリストア先となるSnapshotコピーを決定します。

   ```
   volume snapshot show -vserver vserver_name -volume volume_name
   ```

5. 権限の設定をadvancedに変更します。

   ```
   set -privilege advanced
   ```

6. データをリストアします。

   ```
   volume snapshot restore -vserver vserver_name -volume volume_name -snapshot
   snapshot_name
   ```

7. 画面の指示に従います。
8. LUNを再マッピングします。

   ```
   lun mapping create -vserver vserver_name -volume volume_name -lun lun_name
   -igroup igroup_name
   ```

9. LUNがオンラインであることを確認します。

   ```
   lun show -vserver vserver_name -path lun_path -fields state
   ```

10. LUNがオンラインになっていない場合は、オンラインにします。

    ```
    lun modify -vserver vserver_name -path lun_path -state online
    ```

11. 権限の設定をadminに変更します。

    ```
    set -privilege admin
    ```

12. ホストから、 LUN を再マウントします。
13. ホストから、 LUN へのアクセスを再開します。

ボリュームから**1**つ以上の既存の**Snapshot**コピーを削除する

ボリュームから既存のSnapshotコピーを手動で削除できます。この処理は、ボリュームのスペースを増やす必要がある場合に実行します。

手順

1. コマンドを使用し `volume snapshot show`て、削除するSnapshotコピーを確認します。

```
cluster::> volume snapshot show -vserver vs3 -volume vol3

                                                  ---Blocks---
Vserver  Volume  Snapshot                  Size   Total% Used%
-------- ------- ------------------------ -----  ------ -----
vs3      vol3
                 snap1.2013-05-01_0015   100KB   0%    38%
                 snap1.2013-05-08_0015   76KB    0%    32%
                 snap2.2013-05-09_0010   76KB    0%    32%
                 snap2.2013-05-10_0010   76KB    0%    32%
                 snap3.2013-05-10_1005   72KB    0%    31%
                 snap3.2013-05-10_1105   72KB    0%    31%
                 snap3.2013-05-10_1205   72KB    0%    31%
                 snap3.2013-05-10_1305   72KB    0%    31%
                 snap3.2013-05-10_1405   72KB    0%    31%
                 snap3.2013-05-10_1505   72KB    0%    31%
10 entries were displayed.
```

2. コマンドを使用し `volume snapshot delete`て、Snapshotコピーを削除します。

| 状況 | 入力するコマンド |
| --- | --- |
| 1 つの Snapshot コピーを削除します | `volume snapshot delete -vserver` *`svm_name`* `-volume` *`vol_name`* `-snapshot` *`snapshot_name`* |
| 複数の Snapshot コピーを削除する | `volume snapshot delete -vserver` *`svm_name`* `-volume` *`vol_name`* `-snapshot` *`snapshot_name1`*`[,`*`snapshot_name2`*`,…]` |
| すべての Snapshot コピーを削除します | `volume snapshot delete -vserver` *`svm_name`* `-volume` *`vol_name`* `-snapshot *` |

次の例は、ボリュームvol3上のすべてのSnapshotコピーを削除します。

```
cluster::> volume snapshot delete -vserver vs3 -volume vol3 *

10 entries were acted on.
```

## FlexClone LUNを使用してデータを保護する

### FlexClone LUNを使用したデータ保護の概要

FlexClone LUNは、アクティブボリューム内やSnapshotコピー内にある別のLUNの書き

込み可能なポイントインタイムコピーです。クローンとその親は、相互に影響を及ぼさずに個別に変更できます。

FlexClone LUNは、最初は親LUNとスペースを共有します。デフォルトでは、FlexClone LUNは親LUNのスペースリザーブ属性を継承します。たとえば、親LUNがスペースリザーブなしの場合、FlexClone LUNもデフォルトでスペースリザーブなしになります。ただし、スペースリザーブLUNである親からスペースリザーブなしのFlexClone LUNを作成することはできます。

LUNクローンを作成すると、バックグラウンドでブロック共有が発生し、ブロック共有が完了するまでボリュームのSnapshotコピーを作成できません。

コマンドを使用して、ボリュームでFlexClone LUNの自動削除機能を有効にする必要があります `volume snapshot autodelete modify`。そうしないと、FlexClone LUNを自動的に削除するように設定されていても、ボリュームでFlexCloneの自動削除が設定されていない場合、FlexClone LUNは削除されません。

FlexClone LUNを作成すると、FlexClone LUNの自動削除機能はデフォルトで無効になります。FlexClone LUNを自動的に削除するには、FlexClone LUNごとに手動で有効にする必要があります。ボリュームのセミシックプロビジョニングを使用している場合に、このオプションが提供する「ベストエフォート」の書き込み保証が必要な場合は、 _ALL_FlexClone LUN を自動削除できるようにする必要があります。

> SnapshotコピーからFlexClone LUNを作成すると、スペース効率に優れたバックグラウンドプロセスを使用して、LUNがSnapshotコピーから自動的にスプリットされます。そのため、LUNがSnapshotコピーに依存したり、追加のスペースを消費したりすることはありません。このバックグラウンドスプリットが完了しておらず、Snapshotコピーが自動的に削除された場合、そのFlexClone LUNに対してFlexCloneの自動削除機能が無効になっていても、そのFlexClone LUNは削除されます。バックグラウンドスプリットの完了後は、Snapshotコピーが削除されても、FlexClone LUNは削除されません。

関連情報

"論理ストレージ管理"

**FlexClone LUN**を使用する理由

## FlexClone LUNを使用すると、LUNの読み取り/書き込みコピーを複数作成できます。

これは、次のような場合に行います。

- テスト用にLUNの一時的なコピーを作成する必要があります。
- 本番環境のデータへのアクセスを許可せずに、追加のユーザが利用できるデータのコピーを作成する必要があります。
- 操作や投影のためにデータベースのクローンを作成し、元のデータを変更せずに保持したいと考えています。
- LUNのデータの特定のサブセット（ボリュームグループ内の特定の論理ボリュームまたはファイルシステム、またはファイルシステム内の特定のファイルまたはファイルセット）にアクセスし、元のLUNの残りのデータをリストアすることなく、そのサブセットを元のLUNにコピーする。これは、LUNとLUNのクローンを同時にマウントできるオペレーティングシステムで機能します。SnapDrive for UNIXでは、コマンドを使用してこれをサポートしてい `snap connect`ます。
- オペレーティングシステムが同じ複数のSANブートホストが必要な場合。

自動削除設定で**FlexVol volume**が空きスペースを再生する仕組み

## FlexVol の自動削除設定を有効にすると、 FlexClone ファイルおよび FlexClone LUN を自動的に削除できます。自動削除を有効にすると、ボリュームがフルに近くなったときに、指定した量の空きスペースをボリューム内に再生できます。

ボリュームの空きスペースが一定のしきい値を下回ったときに FlexClone ファイルおよび FlexClone LUN の削除を自動的に開始し、ボリュームの空きスペースを指定の量だけ再生したらクローンの削除を自動的に中止するように設定できます。クローンの自動削除を開始するしきい値を指定することはできませんが、それぞれのクローンを削除対象に含めるかどうかと、ボリュームの空きスペースの目標量を指定することができます。

ボリュームの空きスペースが一定のしきい値を下回ったとき、および次の要件の両方に達したときに、FlexClone ファイルおよび FlexClone LUN が自動的に削除されます。

- FlexClone ファイルおよび FlexClone LUN が格納されているボリュームに対して自動削除機能が有効になっている。

  FlexVol volumeに対して自動削除機能を有効にするには、コマンドを使用し `volume snapshot autodelete modify`ます。ボリュームで`FlexClone`ファイルおよび`FlexClone LUN`を自動的に削除するには、パラメータをまたは `snap_reserve`に `volume`設定する必要があります `-trigger`。

- FlexClone ファイルおよび FlexClone LUN に対して自動削除機能が有効になっている。

  FlexCloneファイルまたはFlexClone LUNに対して自動削除を有効にするには、 `file clone create`コマンドでパラメータを指定し `-autodelete`ます。このクローン設定はボリュームの他の設定よりも優先されるため、この設定で個別に自動削除を無効にすることで、特定の FlexClone ファイルや FlexClone LUN を保持することができます。

**FlexClone**ファイルおよび**FlexClone LUN**を自動的に削除するように**FlexVol volume**を設定する

## ボリュームの空きスペースが一定のしきい値を下回った場合に、自動削除を有効にしたFlexCloneファイルおよびFlexClone LUNをFlexVol volumeで自動的に削除するように設定できます。

必要なもの

- FlexVol volumeにFlexCloneファイルとFlexClone LUNが含まれていて、オンラインになっている必要があります。
- FlexVol volumeを読み取り専用ボリュームにすることはできません。

手順

1. コマンドを使用して、FlexVol volumeでFlexCloneファイルおよびFlexClone LUNの自動削除を有効にします `volume snapshot autodelete modify`。
   - パラメータには `-trigger`、またはを `snap_reserve`指定できます `volume`。
   - パラメータには `-destroy-list`、1種類のクローンのみを削除するかどうかに関係なく、常に指定する必要があり `lun_clone,file_clone`ます。+ 次の例は、ボリューム vol1 で FlexClone ファイルおよび FlexClone LUN の自動削除を有効にし、ボリュームの 25% が空きスペースになるまでスペースが再生されるようにします。

```
cluster1::> volume snapshot autodelete modify -vserver vs1 -volume
vol1 -enabled true -commitment disrupt -trigger volume -target-free
-space 25 -destroy-list lun_clone,file_clone

Volume modify successful on volume:vol1
```

FlexVolボリュームで自動削除を有効にする際にパラメータの値をに `destroy`設定する `-commitment`と、ボリュームの空きスペースが指定したしきい値を下回った場合に、パラメータがに設定された `true`すべてのFlexCloneファイルおよびFlexClone LUNが `-autodelete`削除される可能性があります。ただし、パラメータがに設定されて `false`いるFlexCloneファイルとFlexClone LUN `-autodelete`は削除されません。

2. コマンドを使用して、FlexVol volumeでFlexCloneファイルおよびFlexClone LUNの自動削除が有効になっていることを確認します `volume snapshot autodelete show`。

   次の例は、ボリュームvol1でFlexCloneファイルとFlexClone LUNの自動削除が有効になっていることを示しています。

```
cluster1::> volume snapshot autodelete show -vserver vs1 -volume vol1

         Vserver Name: vs1
          Volume Name: vol1
          Enabled: true
           Commitment: disrupt
         Defer Delete: user_created
         Delete Order: oldest_first
  Defer Delete Prefix: (not specified)*
    Target Free Space: 25%
              Trigger: volume
     Destroy List: lun_clone,file_clone
Is Constituent Volume: false
```

3. 次の手順を実行して、削除するボリューム内のFlexCloneファイルおよびFlexClone LUNで自動削除が有効になっていることを確認します。

   a. コマンドを使用して、特定のFlexCloneファイルまたはFlexClone LUNの自動削除を有効にします `volume file clone autodelete`。

      コマンドでパラメータを指定する `-force`と、特定の`FlexClone`ファイルまたは`FlexClone LUN`を強制的に自動削除できます `volume file clone autodelete`。

      次の例は、ボリュームvol1に含まれるFlexClone LUN lun1_cloneの自動削除が有効になっていることを示しています。

```
cluster1::> volume file clone autodelete -vserver vs1 -clone-path
/vol/vol1/lun1_clone -enabled true
```

自動削除は、FlexCloneファイルおよびFlexClone LUNの作成時に有効にすることができます。

b. コマンドを使用して、FlexCloneファイルまたはFlexClone LUNで自動削除が有効になっていることを確認します `volume file clone show-autodelete`。

次の例は、FlexClone LUN lun1_cloneで自動削除が有効になっていることを示しています。

```
cluster1::> volume file clone show-autodelete -vserver vs1 -clone
-path vol/vol1/lun1_clone
                                                                Vserver
Name: vs1
                                                                Clone
Path: vol/vol1/lun1_clone

**Autodelete Enabled: true**
```

コマンドの使用方法の詳細については、該当するマニュアルページを参照してください。

アクティブボリュームからの**LUN**のクローニング

アクティブボリューム内のLUNをクローニングして、LUNのコピーを作成できます。これらのFlexClone LUNは、アクティブボリューム内の元のLUNの読み書き可能なコピーです。

> この手順は、FAS、AFF、および現在のASAシステムに適用されます。ASA R2システム（ASA A1K、ASA A70、またはASA A90）を使用している場合は、次の手順に従って"以下の手順を実行します"データをクローニングします。ASA R2システムは、SANのみのお客様に特化したシンプルなONTAPエクスペリエンスを提供します。

必要なもの

FlexCloneライセンスがインストールされている必要があります。このライセンスはに含まれてい"ONTAP One"ます。

タスクの内容

スペースリザーブFlexClone LUNには、親のスペースリザーブLUNと同じ量のスペースが必要です。FlexClone LUNのスペースをリザーブしない場合は、FlexClone LUNに対する変更に対応できるだけの十分なスペースがボリュームにあることを確認する必要があります。

手順

1. クローンを作成する前に、LUNがigroupにマッピングされていないこと、または書き込まれていないことを確認しておく必要があります。
2. コマンドを使用し `lun show`て、LUNが存在することを確認します。

```
lun show -vserver vs1
```

```
Vserver   Path                State      Mapped     Type      Size
--------- ------------------- ---------- ---------- --------- -------
vs1       /vol/vol1/lun1      online     unmapped   windows   47.07MB
```

3. コマンドを使用し `volume file clone create`て、FlexClone LUNを作成します。

   ```
   volume file clone create -vserver vs1 -volume vol1 -source-path lun1
   -destination-path/lun1_clone
   ```

   FlexClone LUNを自動削除できるようにする必要がある場合は、を含めます `-autodelete true`。セミシックプロビジョニングを使用してボリュームにこのFlexClone LUNを作成する場合は、すべてのFlexClone LUNに対して自動削除を有効にする必要があります。

4. コマンドを使用し `lun show`て、LUNが作成されたことを確認します。

   ```
   lun show -vserver vs1
   ```

   ```
   Vserver   Path                      State    Mapped   Type      Size
   --------- ------------------------- -------- -------- --------- ------
   vs1       /vol/volX/lun1            online   unmapped windows   47.07MB
   vs1       /vol/volX/lun1_clone      online   unmapped windows   47.07MB
   ```

ボリューム内の**Snapshot**コピーから**FlexClone LUN**を作成する

## ボリューム内のSnapshotコピーを使用して、LUNのFlexCloneコピーを作成できます。LUNのFlexCloneコピーは読み書き可能です。

必要なもの

FlexCloneライセンスがインストールされている必要があります。このライセンスはに含まれてい"ONTAP One"ます。

タスクの内容

FlexClone LUNは親LUNのスペースリザベーション属性を継承します。スペースリザーブFlexClone LUNには、親のスペースリザーブLUNと同じ量のスペースが必要です。FlexClone LUNのスペースをリザーブしない場合は、クローンに対する変更を保存するための十分なスペースがボリュームに必要です。

手順

1. LUNがマッピングされていないこと、または書き込まれていないことを確認します。
2. LUNが含まれているボリュームのSnapshotコピーを作成します。

   ```
   volume snapshot create -vserver vserver_name -volume volume_name -snapshot
   snapshot_name
   ```

   クローニングするLUNのSnapshotコピー（元のSnapshotコピー）を作成する必要があります。

3. SnapshotコピーからFlexClone LUNを作成します。

   `file clone create -vserver vserver_name -volume volume_name -source-path source_path -snapshot-name snapshot_name -destination-path destination_path`

   FlexClone LUNを自動削除できるようにする必要がある場合は、を含めます `-autodelete true`。セミシックプロビジョニングを使用してボリュームにこのFlexClone LUNを作成する場合は、すべてのFlexClone LUNに対して自動削除を有効にする必要があります。

4. FlexClone LUNが正しいことを確認します。

   `lun show -vserver vserver_name`

```
Vserver Path                      State    Mapped    Type     Size
------- ----------------------    -------- --------- -------- -------
vs1     /vol/vol1/lun1_clone      online   unmapped windows   47.07MB
vs1     /vol/vol1/lun1_snap_clone online   unmapped windows   47.07MB
```

**FlexClone**ファイルまたは**FlexClone LUN**の自動削除を禁止する

FlexCloneファイルおよびFlexClone LUNを自動的に削除するようにFlexVol volumeを設定すると、指定した条件を満たすクローンがすべて削除される可能性があります。特定のFlexCloneファイルまたはFlexClone LUNを保持したい場合は、それらのファイルまたはLUNをFlexCloneの自動削除プロセスから除外できます。

開始する前に

FlexCloneライセンスがインストールされている必要があります。このライセンスはに含まれてい"ONTAP One"ます。

タスクの内容

FlexCloneファイルまたはFlexClone LUNを作成すると、クローンの自動削除設定はデフォルトで無効になります。自動削除が無効になっているFlexCloneファイルおよびFlexClone LUNは、ボリュームのスペースを再生するためにクローンを自動的に削除するようにFlexVol volumeを設定しても保持されます。

> ボリュームのレベルをまたは `disrupt`に `try`設定した場合は `commitment`、特定のFlexCloneファイルまたはFlexClone LUNの自動削除を無効にすることで、それらのクローンを個別に保持できます。ただし、ボリュームのレベルをに `destroy`設定し、削除リストに`include`を指定 `lun_clone,file_clone`した場合は `commitment`、ボリューム設定がクローン設定よりも優先され、クローンの自動削除設定に関係なく、すべてのFlexCloneファイルとFlexClone LUNが削除されます。

手順

1. コマンドを使用して、特定のFlexCloneファイルまたはFlexClone LUNが自動的に削除されないようにし`volume file clone autodelete`ます。

   次の例は、vol1に含まれるFlexClone LUN lun1_cloneの自動削除を無効にする方法を示しています。

```
cluster1::> volume file clone autodelete -vserver vs1 -volume vol1
-clone-path lun1_clone -enable false
```

自動削除を無効にしたFlexCloneファイルまたはFlexClone LUNは、ボリュームのスペース再生のために自動的に削除することはできません。

2. コマンドを使用して、FlexCloneファイルまたはFlexClone LUNで自動削除が無効になっていることを確認します `volume file clone show-autodelete`。

次の例は、FlexClone LUN lun1_cloneの自動削除がfalseになっていることを示しています。

```
cluster1::> volume file clone show-autodelete -vserver vs1 -clone-path
vol/vol1/lun1_clone
                                                                Vserver
Name: vs1
                                                                Clone Path:
vol/vol1/lun1_clone
                                                                Autodelete
Enabled: false
```

## SAN環境でのSnapVaultバックアップの設定と使用

### SAN環境でのSnapVaultバックアップの設定と使用の概要

SAN環境でのSnapVaultの設定および使用方法は、NAS環境での設定および使用方法と非常によく似ていますが、SAN環境でLUNをリストアするには、いくつか特別な手順が必要になります。

SnapVaultバックアップには、ソースボリュームの読み取り専用コピーのセットが含まれています。SAN環境では、必ず個 々 のLUNではなく、ボリューム全体をSnapVaultセカンダリボリュームにバックアップします。

LUNを含むプライマリボリュームとSnapVaultバックアップとして機能するセカンダリボリューム間のSnapVault関係を作成および初期化する手順は、ファイルプロトコルに使用するFlexVolボリュームで使用する手順と同じです。この手順の詳細については、を"データ保護"参照してください。

Snapshotコピーを作成してSnapVaultセカンダリボリュームにコピーする前に、バックアップ対象のLUNが整合性のある状態であることを確認することが重要です。SnapCenterを使用してSnapshotコピーの作成を自動化すると、バックアップされたLUNが完全に作成され、元のアプリケーションで使用できるようになります。

SnapVaultセカンダリボリュームからLUNをリストアする場合、次の3つの基本的な選択肢があります。

- SnapVaultセカンダリボリュームからLUNを直接マッピングし、ホストをLUNに接続してLUNの内容にアクセスできます。

  LUNは読み取り専用で、SnapVaultバックアップ内の最新のSnapshotコピーからのみマッピングできます。永続的予約およびその他のLUNメタデータは失われます。必要に応じて、元のLUNに引き続きアクセスできる場合は、ホスト上でコピープログラムを使用してLUNの内容をコピーし、元のLUNに戻すことが

できます。

LUNのシリアル番号はソースLUNとは異なります。

- SnapVaultセカンダリボリューム内のSnapshotコピーを、新しい読み書き可能ボリュームにクローニングできます。

  その後、ボリューム内の任意のLUNをマッピングし、ホストをLUNに接続してLUNの内容にアクセスできます。必要に応じて、元のLUNに引き続きアクセスできる場合は、ホスト上でコピープログラムを使用してLUNの内容をコピーし、元のLUNに戻すことができます。

- SnapVaultセカンダリボリューム内の任意のSnapshotコピーから、LUNを含むボリューム全体をリストアできます。

  ボリューム全体をリストアすると、ボリューム内のすべてのLUNとすべてのファイルが置き換えられます。Snapshotコピーの作成後に作成された新しいLUNはすべて失われます。

  LUNでは、マッピング、シリアル番号、UUID、および永続的予約が保持されます。

**SnapVault**バックアップからの読み取り専用**LUN**コピーへのアクセス

LUN の読み取り専用コピーには、 SnapVault バックアップ内の最新の Snapshot コピーからアクセスできます。LUN の ID 、パス、およびシリアル番号はソース LUN のものとは異なり、あらかじめマッピングしておく必要があります。永続的予約、 LUN マッピング、および igroup は、 SnapVault セカンダリボリュームにレプリケートされません。

必要なもの

- SnapVault 関係が初期化されていて、 SnapVault セカンダリボリューム内の最新の Snapshot コピーに目的の LUN が含まれている必要があります。
- SnapVaultバックアップがあるStorage Virtual Machine（SVM）に、適切なSANプロトコル対応のLIFが1つ以上あり、LUNコピーへのアクセスに使用するホストからアクセスできる必要があります。
- SnapVaultセカンダリボリュームからLUNコピーに直接アクセスする場合は、事前にSnapVault SVMにigroupを作成しておく必要があります。

  LUN には SnapVault セカンダリボリュームから直接アクセスできます。 LUN を含むボリュームのリストアやクローニングを行う必要はありません。

タスクの内容

SnapVault セカンダリボリュームに新しい Snapshot コピーが追加されたときに、以前の Snapshot コピーに LUN がマッピングされている場合、マッピングされた LUN の内容が変更されます。LUN は引き続き同じ ID でマッピングされますが、データは新しい Snapshot コピーから取得されます。LUN のサイズが変更された場合、一部のホストはサイズの変更を自動的に検出します。 Windows ホストでは、サイズ変更を検知するためにディスクの再スキャンが必要です。

手順

1. コマンドを実行し `lun show`て、SnapVaultセカンダリボリューム内の使用可能なLUNのリストを表示します。

   この例では、プライマリボリューム srcvolA 内の元の LUN と、 SnapVault セカンダリボリューム dstvolB

内のコピーされた LUN の両方が表示されています。

```
cluster::> lun show

Vserver   Path                State   Mapped   Type          Size
--------  ------------------  ------  -------  --------      -------
vserverA  /vol/srcvolA/lun_A  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_B  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_C  online  mapped   windows  300.0GB
vserverB  /vol/dstvolB/lun_A  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_B  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_C  online  unmapped windows  300.0GB

6 entries were displayed.
```

2. 目的のホストのigroupが、SnapVaultセカンダリボリュームがあるSVM内にまだ存在していない場合は、コマンドを実行し `igroup create`てigroupを作成します。

   このコマンドでは、 iSCSI プロトコルを使用する Windows ホスト用の igroup を作成します。

```
cluster::> igroup create -vserver vserverB -igroup temp_igroup
  -protocol iscsi -ostype windows
  -initiator iqn.1991-05.com.microsoft:hostA
```

3. コマンドを実行し `lun mapping create`て、目的のLUNコピーをこのigroupにマッピングします。

```
cluster::> lun mapping create -vserver vserverB -path /vol/dstvolB/lun_A
  -igroup temp_igroup
```

4. ホストを LUN に接続し、適宜 LUN の内容にアクセスします。

**SnapVault**バックアップから単一の**LUN**をリストア

単一の LUN を新しい場所または元の場所にリストアできます。SnapVault セカンダリボリューム内の任意の Snapshot コピーを使用してリストアできます。LUN を元の場所にリストアするには、まず新しい場所にリストアしてから、元の場所にコピーします。

必要なもの

- SnapVault 関係が初期化されていて、 SnapVault セカンダリボリュームに、リストアに使用する適切な Snapshot コピーが含まれている必要があります。
- SnapVault セカンダリボリュームがある Storage Virtual Machine （ SVM ）に、適切な SAN プロトコル対応の LIF が 1 個以上あり、 LUN コピーへのアクセスに使用するホストからこの LIF にアクセスできることが必要です。
- igroup が SnapVault SVM 上にすでに存在している必要があります。

タスクの内容

このプロセスでは、 SnapVault セカンダリボリューム内の Snapshot コピーから、読み書き可能なボリュームクローンを作成します。このクローン内の LUN を直接使用することも、必要に応じて LUN の内容を元の LUN の場所にコピーすることもできます。

クローン内の LUN のパスとシリアル番号は、元の LUN のものとは異なります。永続的予約は維持されません。

手順

1. コマンドを実行し `snapmirror show`て、SnapVaultバックアップが含まれているセカンダリボリュームを確認します。

```
cluster::> snapmirror show

Source          Dest     Mirror  Relation  Total             Last
Path     Type   Path     State   Status    Progress  Healthy Updated
-------- ---- --------- ------- --------- --------- ------- -------
vserverA:srcvolA
         XDP  vserverB:dstvolB
                        Snapmirrored
                                Idle       -         true    -
```

2. コマンドを実行し `volume snapshot show`て、LUNのリストア元となるSnapshotコピーを特定します。

```
cluster::> volume snapshot show

Vserver  Volume  Snapshot                State Size   Total% Used%
-------- ------- ---------------------- ----- ------ ------ -----
vserverB
         dstvolB
                 snap2.2013-02-10_0010  valid  124KB     0%    0%
                 snap1.2013-02-10_0015 valid  112KB     0%    0%
                 snap2.2013-02-11_0010  valid  164KB     0%    0%
```

3. コマンドを実行し `volume clone create`て、目的のSnapshotコピーから読み書き可能クローンを作成します。

   ボリュームクローンは、 SnapVault バックアップと同じアグリゲート内に作成されます。アグリゲート内に、クローンを格納できるだけの十分なスペースが必要です。

```
cluster::> volume clone create -vserver vserverB
  -flexclone dstvolB_clone -type RW -parent-volume dstvolB
  -parent-snapshot daily.2013-02-10_0010
[Job 108] Job succeeded: Successful
```

4. コマンドを実行し `lun show`て、ボリュームクローン内のLUNのリストを表示します。

```
cluster::> lun show -vserver vserverB -volume dstvolB_clone

Vserver   Path                        State   Mapped   Type
--------- ------------------------  ------- -------- --------
vserverB  /vol/dstvolB_clone/lun_A  online  unmapped windows
vserverB  /vol/dstvolB_clone/lun_B  online  unmapped windows
vserverB  /vol/dstvolB_clone/lun_C  online  unmapped windows

3 entries were displayed.
```

5. 目的のホストのigroupが、SnapVaultバックアップがあるSVM内にまだ存在していない場合は、コマンドを実行し `igroup create`てigroupを作成します。

   この例では、 iSCSI プロトコルを使用する Windows ホスト用の igroup を作成しています。

```
cluster::> igroup create -vserver vserverB -igroup temp_igroup
  -protocol iscsi -ostype windows
  -initiator iqn.1991-05.com.microsoft:hostA
```

6. コマンドを実行し `lun mapping create`て、目的のLUNコピーをこのigroupにマッピングします。

```
cluster::> lun mapping create -vserver vserverB
  -path /vol/dstvolB_clone/lun_C -igroup temp_igroup
```

7. ホストを LUN に接続し、適宜 LUN の内容にアクセスします。

   この LUN は読み書き可能であり、元の LUN の代わりに使用できます。LUN のシリアル番号が異なるため、ホストはこの LUN が元の LUN とは別の LUN であると解釈します。

8. ホスト上でコピープログラムを使用して、 LUN の内容を元の LUN にコピーします。

ボリューム内のすべての**LUN**を**SnapVault**バックアップからリストア

## ボリューム内の1つ以上のLUNをSnapVaultバックアップからリストアする必要がある場合は、ボリューム全体をリストアできます。ボリュームをリストアする場合は、ボリューム内のすべての LUN が対象になります。

必要なもの

SnapVault 関係が初期化されていて、 SnapVault セカンダリボリュームに、リストアに使用する適切な Snapshot コピーが含まれている必要があります。

タスクの内容

ボリューム全体をリストアすると、ボリュームの状態は、リストアに使用した Snapshot コピーが作成された

時点の状態に戻ります。Snapshot コピーの作成後にボリュームに追加された LUN がある場合、その LUN はリストアの過程で削除されます。

ボリュームのリストア後も、 LUN と igroup とのマッピングはリストアの直前と同じ状態が維持されます。LUN のマッピングは、 Snapshot コピー作成時点のマッピングとは異なる場合があります。ホストクラスタによる LUN の永続的予約は維持されます。

手順

1. ボリューム内のすべての LUN に対する I/O を停止します。
2. コマンドを実行し `snapmirror show`て、SnapVaultセカンダリボリュームが含まれているセカンダリボリュームを確認します。

```
cluster::> snapmirror show

Source          Dest     Mirror  Relation  Total             Last
Path     Type   Path     State   Status    Progress  Healthy Updated
-------- ---- --------- ------- --------- --------- ------- -------
vserverA:srcvolA
         XDP  vserverB:dstvolB
                        Snapmirrored
                                Idle       -         true    -
```

3. コマンドを実行し `volume snapshot show`て、リストア元のSnapshotコピーを特定します。

```
cluster::> volume snapshot show

Vserver  Volume  Snapshot                State Size   Total% Used%
-------- ------- ----------------------- ----- ------ ------ -----
vserverB
         dstvolB
                 snap2.2013-02-10_0010  valid  124KB     0%    0%
                 snap1.2013-02-10_0015 valid  112KB     0%    0%
                 snap2.2013-02-11_0010  valid  164KB     0%    0%
```

4. コマンドを実行し `snapmirror restore`、使用するSnapshotコピーを指定するオプションを指定し `-source-snapshot`ます。

   リストア先として指定するのは、リストア先の元のボリュームです。

```
cluster::> snapmirror restore -destination-path vserverA:srcvolA
  -source-path vserverB:dstvolB -source-snapshot daily.2013-02-10_0010

Warning: All data newer than Snapshot copy hourly.2013-02-11_1205 on
volume vserverA:src_volA will be deleted.
Do you want to continue? {y|n}: y
[Job 98] Job is queued: snapmirror restore from source
"vserverB:dstvolB" for the snapshot daily.2013-02-10_0010.
```

5. ホストクラスタ間で LUN を共有している場合は、影響を受けるホストから LUN に対する永続的予約をリストアします。

#### SnapVault バックアップからのボリュームのリストア

次の例では、 Snapshot コピーの作成後に lun_D という名前の LUN がボリュームに追加されています。Snapshot コピーからボリューム全体をリストアしたあと、 lun_D は表示されなくなります。

コマンド出力では `lun show`、プライマリボリュームsrcvolA内のLUNと、SnapVaultセカンダリボリュームdstvolB内のこれらのLUNの読み取り専用コピーを確認できます。SnapVault バックアップに lun_D のコピーはありません。

```
cluster::> lun show
Vserver   Path                 State   Mapped   Type          Size
--------- ------------------   ------- -------- --------      -------
vserverA  /vol/srcvolA/lun_A  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_B  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_C  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_D  online  mapped   windows  250.0GB
vserverB  /vol/dstvolB/lun_A  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_B  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_C  online  unmapped windows  300.0GB

7 entries were displayed.

cluster::>snapmirror restore -destination-path vserverA:srcvolA
  -source-path vserverB:dstvolB
  -source-snapshot daily.2013-02-10_0010

Warning: All data newer than Snapshot copy hourly.2013-02-11_1205
on volume vserverA:src_volA will be deleted.
Do you want to continue? {y|n}: y
[Job 98] Job is queued: snapmirror restore from source
"vserverB:dstvolB" for the snapshot daily.2013-02-10_0010.

cluster::> lun show
Vserver   Path                 State   Mapped   Type          Size
--------- ------------------   ------- -------- --------      -------
vserverA  /vol/srcvolA/lun_A  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_B  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_C  online  mapped   windows  300.0GB
vserverB  /vol/dstvolB/lun_A  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_B  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_C  online  unmapped windows  300.0GB

6 entries were displayed.
```

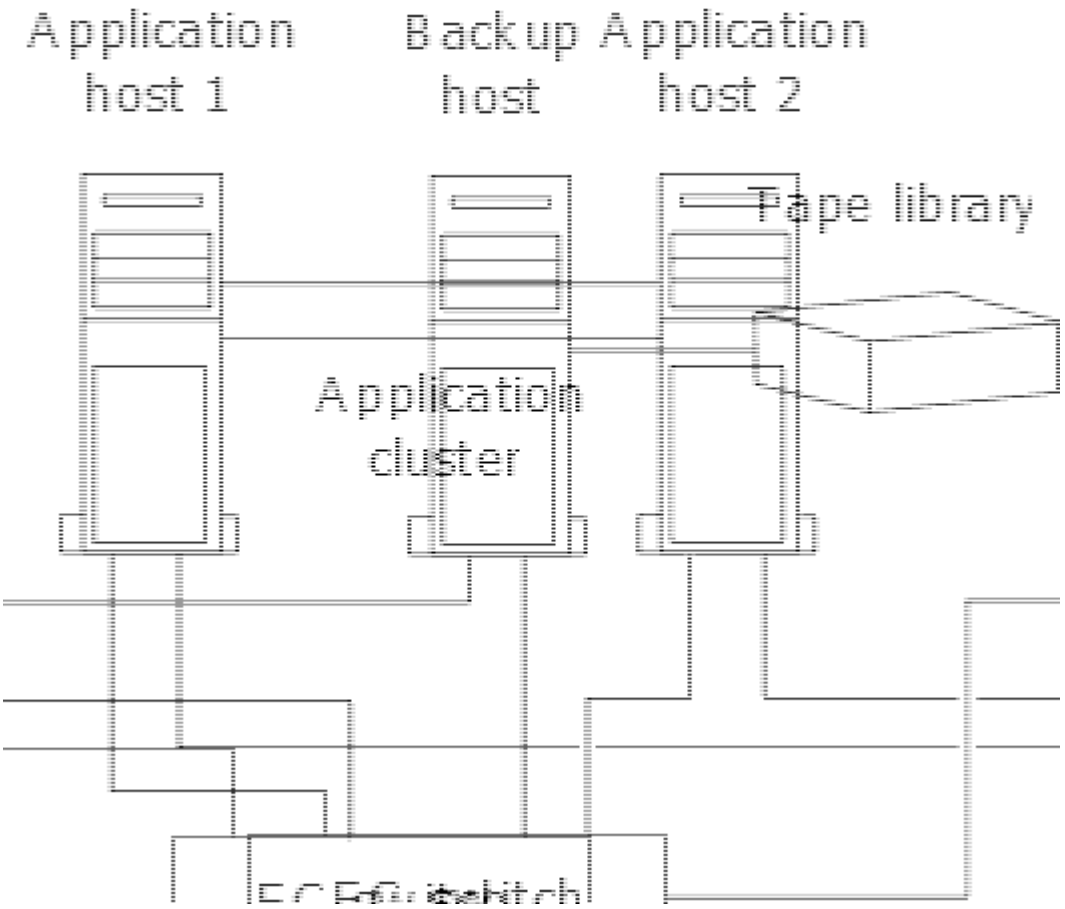
ボリュームが SnapVault セカンダリボリュームからリストアされると、ソースボリュームには lun_D が存在しなくなりますリストア後もソースボリューム内の LUN のマッピングは維持されるため、再マッピングする必要はありません。

## ホストバックアップシステムをプライマリストレージシステムに接続する方法

## 別のバックアップホストを使用してSANシステムをテープにバックアップすると、アプリケーションホストのパフォーマンス低下を回避できます。

バックアップのためには、SANデータとNASデータを分離しておくことが不可欠です。次の図は、プライマリストレージシステムに対するホストバックアップシステムの推奨される物理構成を示しています。ボリュー

ムはSAN専用として設定する必要があります。LUNは単一のボリュームに限定することも、複数のボリュームまたはストレージシステムに分散させることもできます。




ホスト上のボリュームは、ストレージシステムからマッピングされた単一のLUN、またはボリュームマネージャを使用する複数のLUN（HP-UXシステムのVxVMなど）で構成できます。

## ホストバックアップシステムを使用した**LUN**のバックアップ

## ホストバックアップシステムのソースデータとして、Snapshotコピーからクローニングしたを使用できます。

必要なもの

本番用LUNが存在し、アプリケーションサーバのWWPNまたはイニシエータノード名を含むigroupにマッピングされている必要があります。また、LUNがフォーマットされていて、ホストからアクセスできる必要があります。

手順

1. ホストファイルシステムバッファの内容をディスクに保存します。

   ホストオペレーティングシステムのコマンドを使用するか、SnapDrive（Windows）またはSnapDrive（UNIX）を使用できます。この手順をSANバックアップの前処理スクリプトに含めることもできます。

2. コマンドを使用し `volume snapshot create`て、本番用LUNのSnapshotコピーを作成します。

   ```
   volume snapshot create -vserver vs0 -volume vol3 -snapshot vol3_snapshot
   ```

```
-comment "Single snapshot" -foreground false
```

3. コマンドを使用し `volume file clone create`て、本番用LUNのクローンを作成します。

```
volume file clone create -vserver vs3 -volume vol3 -source-path lun1 -snapshot
-name snap_vol3 -destination-path lun1_backup
```

4. コマンドを使用し `lun igroup create`て、バックアップサーバのWWPNを含むigroupを作成します。

```
lun igroup create -vserver vs3 -igroup igroup3 -protocol fc -ostype windows
-initiator 10:00:00:00:c9:73:5b:91
```

5. コマンドを使用し `lun mapping create`て、手順3で作成したLUNクローンをバックアップホストにマッピングします。

```
lun mapping create -vserver vs3 -volume vol3 -lun lun1_backup -igroup igroup3
```

この手順をSANバックアップアプリケーションのポストプロセススクリプトに含めることもできます。

6. ホストから、新しいLUNを検出し、ファイルシステムをホストで使用できるようにします。

この手順をSANバックアップアプリケーションのポストプロセススクリプトに含めることもできます。

7. SANバックアップアプリケーションを使用して、バックアップホストのLUNクローン内のデータをテープにバックアップします。
8. コマンドを使用し `lun modify`て、LUNクローンをオフラインにします。

```
lun modify -vserver vs3 -path /vol/vol3/lun1_backup -state offline
```

9. を使用し `lun delete`てLUNクローンを削除します。

```
lun delete -vserver vs3 -volume vol3 -lun lun1_backup
```

10. コマンドを使用し `volume snapshot delete`て、Snapshotコピーを削除します。

```
volume snapshot delete -vserver vs3 -volume vol3 -snapshot vol3_snapshot
```

# SAN構成のリファレンス

## SANコウセイノカイヨウ

Storage Area Network（SAN；ストレージエリアネットワーク）は、iSCSIやFCなどのSAN転送プロトコルを使用してホストに接続されるストレージソリューションで構成されます。ストレージソリューションが1つ以上のスイッチを介してホストに接続されるようにSANを設定できます。iSCSIを使用している場合は、スイッチを使用せずにストレージソリューションをホストに直接接続するようにSANを設定することもできます。

SANでは、Windows、Linux、UNIXなど、異なるオペレーティングシステムを使用する複数のホストが、ストレージソリューションに同時にアクセスできます。および"ポートセット"を使用すると、ホストとストレージの間のデータアクセスを制限できます"選択的LUNマッピング"。

iSCSIの場合、ストレージソリューションとホスト間のネットワークトポロジをネットワークと呼びます。FC、FC / NVMe、FCoEの場合、ストレージソリューションとホストの間のネットワークトポロジをファブリックと呼びます。冗長性を確保してデータアクセスの中断からデータを保護するには、マルチネットワークまたはマルチファブリック構成のHAペアを使用してSANをセットアップする必要があります。シングルノードまたはシングルネットワーク/ファブリックを使用する構成は完全な冗長性がないため、推奨されません。

SANの設定が完了したら"iSCSIまたはFC用のストレージのプロビジョニング"、またはを実行できます"FC / NVMe用のストレージのプロビジョニング"。その後、ホストに接続してデータの提供を開始できます。

SANプロトコルのサポートは、ONTAPのバージョン、プラットフォーム、構成によって異なります。特定の設定の詳細については、を参照して"NetApp Interoperability Matrix Tool"ください。

関連情報

- "SANの管理の概要"
- "NVMeの構成、サポート、制限事項"

## iSCSIコウセイ

### iSCSI SANホストの構成方法

iSCSI構成は、iSCSI SANホストに直接接続されたハイアベイラビリティ（HA）ペアか、1つ以上のIPスイッチを介してホストと接続されたHAペアでセットアップします。

"HAペア"ホストがLUNへのアクセスに使用するアクティブ/最適化パスとアクティブ/非最適パスのレポートノードとして定義されます。Windows、Linux、UNIXなど、異なるオペレーティングシステムを使用する複数のホストから同時にストレージにアクセスできます。ホストには、ALUAをサポートするサポート対象のマルチパスソリューションがインストールおよび設定されている必要があります。サポートされるオペレーティングシステムとマルチパスソリューションは、で確認できます"NetApp Interoperability Matrix Tool"。

マルチネットワーク構成では、ホストをストレージシステムに接続するスイッチが複数あります。完全な冗長性を備えたマルチネットワーク構成を推奨します。シングルネットワーク構成では、1台のスイッチでホストをストレージシステムに接続します。シングルネットワーク構成では完全な冗長性は確保されません。

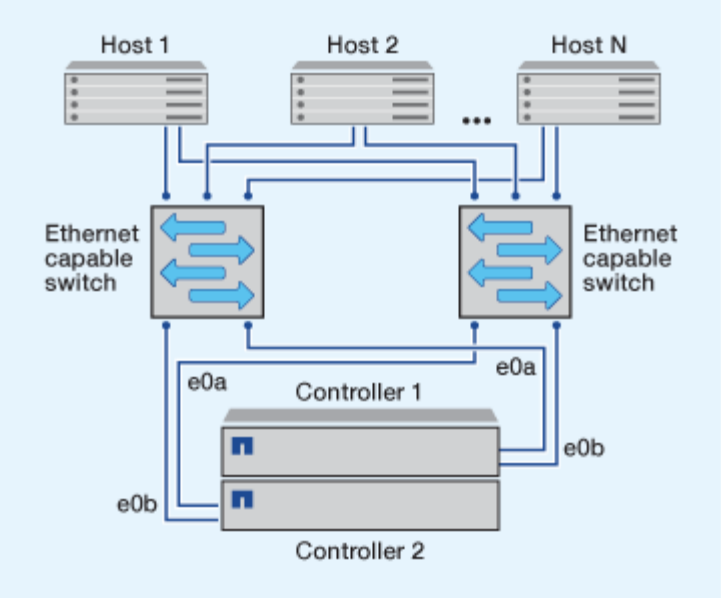
"シングルノードコウセイ"は、フォールトトレランスやノンストップオペレーションのサポートに必要な冗長性が確保されないため、推奨されません。

関連情報

- HAペアが所有するLUNへのアクセスに使用するパスを制限する方法について説明します。"選択的LUNマッピング（SLM）"
- 詳細はこちらをご覧ください "SAN LIF"。
- については、を参照して"iSCSIにおけるVLANの利点"ください。

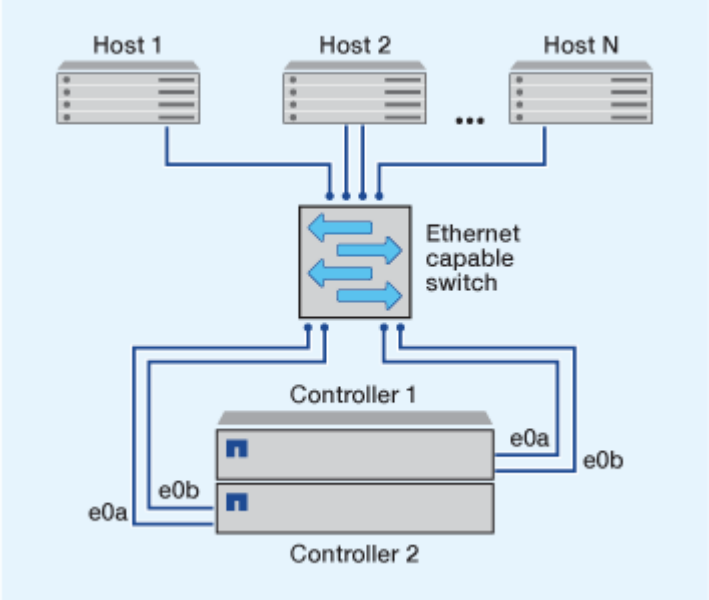
#### マルチネツトワアクiSCSIコウセイ

マルチネットワークのHAペア構成では、HAペアを複数のスイッチで1つ以上のホストに接続します。スイッチが複数あるため、この構成では完全な冗長性が確保されます。



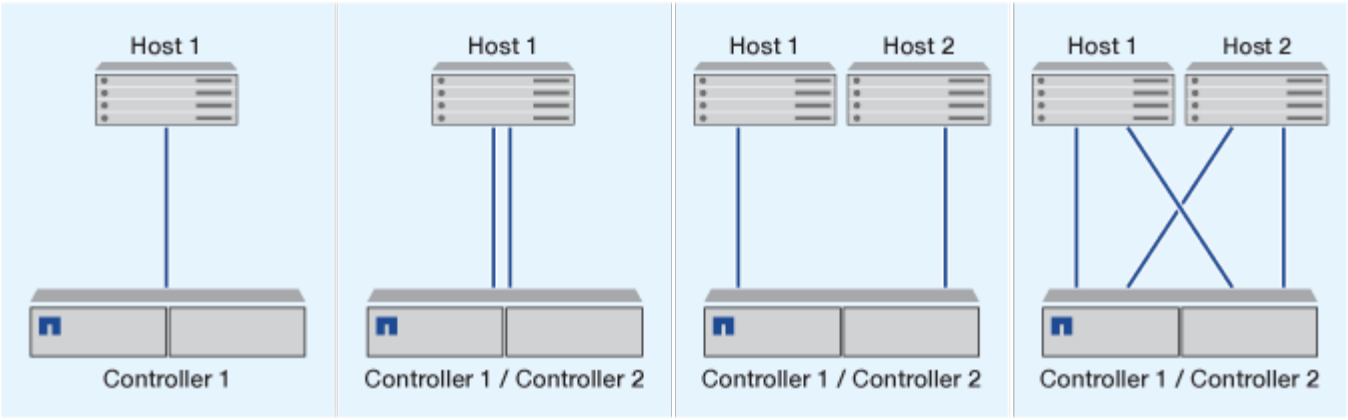

タンイチネツトワアクノ**iSCSI**コウセイ

単一ネットワークのHAペア構成では、HAペアを1つのスイッチで1つ以上のホストに接続します。スイッチが1台しかないため、この構成では完全な冗長性は確保されません。




直接接続型**iSCSI**構成

直接接続型の構成では、1つ以上のホストをコントローラに直接接続します。




**iSCSI**構成で**VLAN**を使用する利点

VLANは、ブロードキャストドメインにグループ化されたスイッチポートのグループで構成されます。VLANは、単一のスイッチ上に配置することも、複数のスイッチシャーシにまたがって配置することもできます。静的VLANと動的VLANを使用すると、IPネットワークインフラ内のセキュリティを強化し、問題を切り分け、使用可能なパスを制限できます。

大規模なIPネットワークインフラにVLANを実装すると、次のような利点が得られます。

- セキュリティの強化：

  VLANを使用すると、イーサネットネットワークまたはIP SANの異なるノード間のアクセスが制限されるため、既存のインフラを活用しながらセキュリティを強化できます。

- 問題を切り分けることで、イーサネットネットワークとIP SANの信頼性が向上します。
- 問題領域を制限することで、問題解決時間を短縮
- 特定のiSCSIターゲットポートへの使用可能なパスの数が削減されます。
- ホストで使用されるパスの最大数が削減されます。

  パスが多すぎると、再接続時間が遅くなります。ホストにマルチパスソリューションがない場合は、VLANを使用してパスを1つだけ許可できます。

動的な**VLAN**

ダイナミックVLANはMACアドレスベースです。VLANを定義するには、含めるメンバーのMACアドレスを指定します。

動的VLANは柔軟性を提供し、デバイスがスイッチに物理的に接続されている物理ポートへのマッピングを必要としません。VLANを再設定することなく、1つのポートから別のポートにケーブルを移動できます。

セイテキナ**VLAN**

静的なVLANはポートベースです。スイッチとスイッチポートは、VLANとそのメンバーを定義するために使用されます。

スタティックVLANは、メディアアクセス制御（MAC）スプーフィングを使用してVLANを侵害できないた

め、セキュリティが向上します。ただし、誰かがスイッチに物理的にアクセスできる場合は、ケーブルを交換してネットワークアドレスを再設定するとアクセスが許可されます。

環境によっては、動的なVLANよりも静的なVLANを作成および管理する方が簡単です。これは、スタティックVLANでは、48ビットのMACアドレスではなく、スイッチとポートの識別子だけを指定する必要があるためです。さらに、VLAN IDを使用してスイッチポート範囲にラベルを付けることもできます。

## FCコウセイ

### FCおよびFC-NVMe SANホストの構成方法

FCおよびFC-NVMe SANホストは、HAペアと、少なくとも2つのスイッチを使用して構成することを推奨します。これにより、ファブリック レイヤとストレージ システム レイヤで冗長性が確保され、フォールト トレランスとノンストップ オペレーションがサポートされます。FCまたはFC-NVMe SANホストをスイッチを使用せずにHAペアに直接接続することはできません。

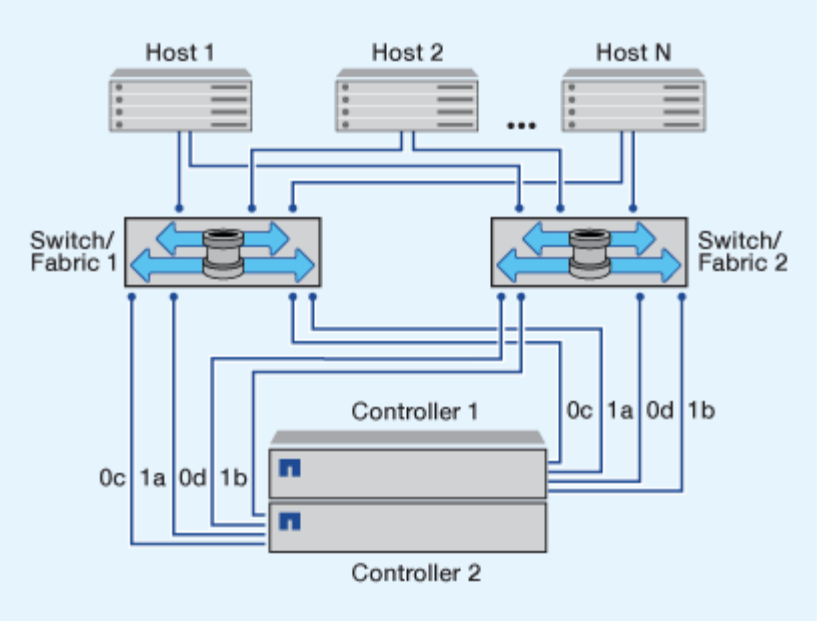
カスケード ファブリック、部分メッシュ ファブリック、フルメッシュ ファブリック、コアエッジ ファブリック、およびディレクタ ファブリックは、FCスイッチをファブリックに接続する業界標準の方法であり、いずれもサポートされます。異機種混在のFCスイッチ ファブリックの使用は、組み込みのブレード スイッチ以外はサポートされません。特定の例外については、を"Interoperability Matrix Tool"参照してください。ファブリックは1つまたは複数のスイッチで構成でき、ストレージコントローラは複数のスイッチに接続できます。

Windows、Linux、UNIXなど、異なるオペレーティングシステムを使用する複数のホストから、ストレージコントローラに同時にアクセスできます。ホストには、サポートされているマルチパスソリューションがインストールおよび設定されている必要があります。サポートされるオペレーティングシステムとマルチパスソリューションは、Interoperability Matrix Toolで確認できます。

#### マルチファブリックノFCコウセイオヨビFC-NVMeコウセイ

マルチファブリックのHAペア構成では、HAペアを複数のスイッチで1つ以上のホストに接続します。次の図は、マルチファブリックのHAペアを示しています。わかりやすいように、この図ではファブリックが2つだけになっていますが、マルチファブリック構成は2つ以上の任意の数のファブリックで構成できます。

次の図のFCターゲット ポート番号（0c、0d、1a、1b）は一例です。実際のポート番号は、使用しているストレージ ノードのモデル、および拡張アダプタを使用しているかどうかによって異なります。

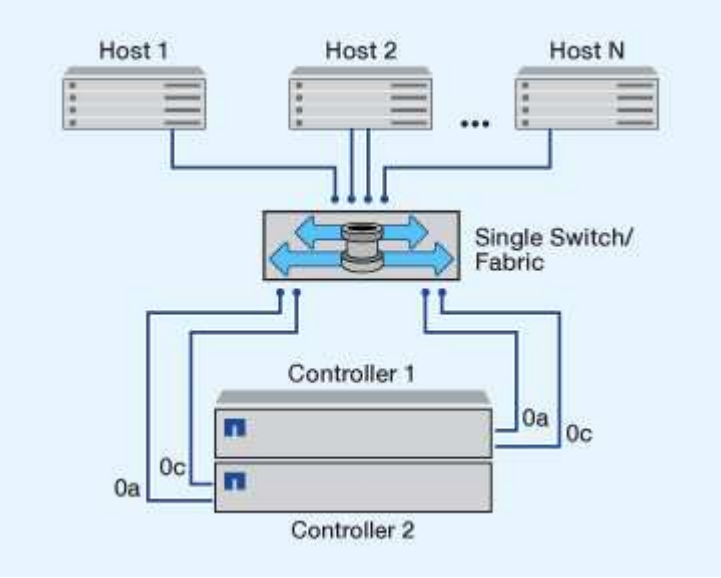



タンイツファブリックノ**FC**コウセイオヨビ**FC-NVMe**コウセイ

単一ファブリックのHAペア構成では、HAペアの両方のコントローラを1つのファブリックで1つ以上のホストに接続します。ホストとコントローラは単一のスイッチを介して接続されるため、単一ファブリックのHAペア構成では完全な冗長性は確保されません。

次の図のFCターゲットポート番号（0a、0c）は一例です。実際のポート番号は、ストレージノードのモデル、および拡張アダプタを使用しているかどうかによって異なります。

単一ファブリックのHAペア構成は、FC構成をサポートするすべてのプラットフォームでサポートされます。




"シングルノードコウセイ"は、フォールトトレランスやノンストップオペレーションのサポートに必要な冗長性が確保されないため、推奨されません。

関連情報

- HAペアが所有するLUNへのアクセスに使用するパスを制限する方法について説明します。"選択的LUNマ

ッピング（SLM）"

- 詳細はこちらをご覧ください "SAN LIF"。

**FC**スイッチ構成のベストプラクティス

## FCスイッチを設定する際には、パフォーマンスを最大限に高めるために一定のベストプラクティスを考慮する必要があります。

FCスイッチの構成では、リンク速度を固定に設定することを推奨します。これは、ファブリックのリビルド時に最適なパフォーマンスが得られるため、時間を大幅に節約できるため、大規模なファブリックに特に適しています。自動ネゴシエーションは柔軟性に優れていますが、FCスイッチの構成が必ずしも期待どおりのパフォーマンスを発揮するとは限らず、ファブリック全体の構築時間が長くなります。

ファブリックに接続されているすべてのスイッチでN_Port ID Virtualization（NPIV）がサポートされ、NPIVが有効になっている必要があります。ONTAPは、NPIVを使用してFCターゲットをファブリックに提示します。

サポートされる環境の詳細については、を参照してください "NetApp Interoperability Matrix Tool"。

FCとiSCSIのベストプラクティスについては、を参照してください "NetAppテクニカルレポート4080：『Best Practices for Modern SAN』"。

サポートされる**FC**ホップ数

## ホストとストレージシステムの間でサポートされるFCの最大ホップ数は、スイッチベンダーとストレージシステムによるFC構成のサポートによって異なります。

ホップ数は、イニシエータ（ホスト）とターゲット（ストレージシステム）の間のパスにあるスイッチの数として定義されます。Cisco では、この値を「 SAN ファブリックの直径」とも呼びます。

| スイッチベンダー | サポートされるホップ数 |
| --- | --- |
| Brocade | FCでは7、FCoEでは5 |
| Cisco | 7 FCの場合、最大3つのスイッチをFCoEスイッチにすることができます。 |

関連情報

"NetAppのダウンロード：Brocadeスケーラビリティマトリックスドキュメント"

"NetAppのダウンロード：Ciscoスケーラビリティマトリックスドキュメント"

**FC**ターゲットポート構成に関する推奨事項

## FC-NVMeプロトコル用のFCターゲットポートは、FCプロトコル用の設定および使用とまったく同じ方法で設定および使用できます。FC-NVMeプロトコルがサポートされるかどうかは、プラットフォームとONTAPのバージョンによって異なります。NetApp Hardware Universeを使用してサポートを確認します。

最適なパフォーマンスと可用性を実現するには、使用するプラットフォームに対応したに記載されている推奨

されるターゲットポート構成を使用する必要があります "NetApp Hardware Universe"。

#### 共有ASICを使用するFCターゲットポートの設定

次のプラットフォームには、ASIC（特定用途向け共有集積回路）を使用したポートペアがあります。これらのプラットフォームで拡張アダプタを使用する場合は、接続に同じASICが使用されないようにFCポートを設定する必要があります。

| コントローラ | ASIC を共有するポートペア | ターゲットポートの数：推奨ポート |
|---|---|---|
| • FAS8200<br>• AFF A300用 | 0g+0h | 1：0g 2：0g、0h |
| • FAS2720<br>• FAS2750<br>• AFF A220用 | 0c+0d 0e+0f | 1：0c 2：0c、0e 3：0c、0e、0d 4：0c、0e、0d、0f |

#### サポートされるFCターゲットポートの速度

FCターゲットポートは、さまざまな速度で実行するように設定できます。特定のホストで使用されるすべてのターゲットポートを同じ速度に設定する必要があります。ターゲットポートの速度は、接続先デバイスの速度と同じに設定する必要があります。ポート速度に自動ネゴシエーションを使用しないでください。自動ネゴシエーションを設定したポートの方が、ギブバックやテイクオーバーなどの中断後の再接続に時間がかかる可能性があります。

オンボードポートと拡張アダプタは、次の速度で実行するように設定できます。コントローラと拡張アダプタのポートは、必要に応じて、さまざまな速度で実行するように個別に構成することができます。

| 4Gb ポート | 8Gb ポート | 16Gb ポート | 32Gb ポート |
|---|---|---|---|
| • 4 Gb<br>• 2Gb<br>• 1Gb | • 8Gb<br>• 4 Gb<br>• 2Gb | • 16Gb<br>• 8Gb<br>• 4 Gb | • 32Gb<br>• 16Gb<br>• 8Gb |

UTA2 ポートでは、必要に応じて、 8Gb の SFP+ アダプタを使用して 8Gb 、 4Gb 、 2Gb の速度をサポートできます。

### FCアダプタを搭載したシステムを管理する

#### FCアダプタを搭載したシステムの管理の概要

オンボードFCアダプタとFCアダプタカードを管理するためのコマンドを使用できます。これらのコマンドを使用して、アダプタモードの設定、アダプタ情報の表示、および速度の変更を行うことができます。

ほとんどのストレージシステムには、イニシエータまたはターゲットとして設定できるオンボードFCアダプタが搭載されています。イニシエータまたはターゲットとして設定されたFCアダプタカードを使用すること

もできます。イニシエータはバックエンドディスクシェルフに接続します。場合によっては、外部ストレージアレイ（FlexArray）にも接続します。ターゲットはFCスイッチにのみ接続します。FCターゲットのHBAポートとスイッチポートの速度は、両方とも同じ値に設定し、autoには設定しないでください。

**FC**アダプタの管理用コマンド

## FC コマンドを使用して、ストレージコントローラの FC ターゲットアダプタ、 FC イニシエータアダプタ、およびオンボード FC アダプタを管理できます。FC アダプタの管理に使用するコマンドは、 FC プロトコルと FC-NVMe プロトコルで同じです。

FC イニシエータアダプタのコマンドは、ノードレベルでのみ機能します。FCイニシエータアダプタのコマンドを使用する前に、コマンドを使用する必要があります `run -node node_name`。

**FC** ターゲットアダプタの管理用コマンド

| 状況 | 使用するコマンド |
| --- | --- |
| ノードの FC アダプタ情報を表示する | `network fcp adapter show` |
| FC ターゲットアダプタのパラメータを変更する | `network fcp adapter modify` |
| FC プロトコルトラフィック情報を表示します | `run -node node_name sysstat -f` |
| FC プロトコルの実行時間を表示します | `run -node node_name uptime` |
| アダプタの設定とステータスを表示します | `run -node node_name sysconfig -v adapter` |
| 拡張カードが取り付けられていること、および構成にエラーがないかどうかを確認します | `run -node node_name sysconfig -ac` |
| コマンドのマニュアルページを表示します | `man command_name` |

**FC** イニシエータアダプタの管理用コマンド

| 状況 | 使用するコマンド |
| --- | --- |
| ノードのすべてのイニシエータおよびそのアダプタの情報を表示する | `run -node node_name storage show adapter` |
| アダプタの設定とステータスを表示します | `run -node node_name sysconfig -v adapter` |
| 拡張カードが取り付けられていること、および構成にエラーがないかどうかを確認します | `run -node node_name sysconfig -ac` |

オンボード **FC** アダプタの管理用コマンド

| 状況 | 使用するコマンド |
| --- | --- |
| オンボード FC ポートのステータスを表示します | `system node hardware unified-connect show` |

**FC**アダプタのイニシエータモード設定

## オンボードアダプタの個 々 のFCポートおよび特定のFCアダプタカードをイニシエータモードに設定できます。イニシエータモードは、テープドライブ、テープライブラリ、またはFlexArray仮想化またはForeign LUN Import（FLI）を使用するサードパーティストレージへのポートの接続に使用されます。

必要なもの

- アダプタのLIFを、メンバーになっているすべてのポートセットから削除する必要があります。
- 物理ポートのパーソナリティをターゲットからイニシエータに変更する前に、変更対象の物理ポートを使用するすべてのStorage Virtual Machine（SVM）のすべてのLIFを移行または破棄する必要があります。

タスクの内容

オンボードのFCポートは、それぞれイニシエータまたはターゲットとして個別に構成できます。特定のFCアダプタのポートは、オンボードのFCポートと同様に、ターゲットポートまたはイニシエータポートとして個別に構成することもできます。ターゲットモードに設定できるアダプタのリストについては、を参照し"NetApp Hardware Universe"てください。

NVMe/FCではイニシエータモードがサポートされます。

手順

1. アダプタからすべてのLIFを削除します。

   `network interface delete -vserver` *`SVM_name`* `-lif` *`lif_name`*`,`*`lif_name`*

2. アダプタをオフラインにします。

   `network fcp adapter modify -node` *`node_name`* `-adapter` *`adapter_port`* `-status-admin down`

   アダプタがオフラインにならない場合は、システムの適切なアダプタポートからケーブルを取り外すこともできます。

3. アダプタをターゲットからイニシエータに変更します。

   `system hardware unified-connect modify -t initiator` *`adapter_port`*

4. 変更したアダプタをホストしているノードをリブートします。
5. 構成に対してFCポートが正しい状態で設定されていることを確認します。

   `system hardware unified-connect show`

6. アダプタをオンラインに戻します。

   ```
   node run -node node_name storage enable adapter adapter_port
   ```

### FCアダプタのターゲットモード設定

## オンボードアダプタの個 々 のFCポートおよび特定のFCアダプタカードをターゲットモードに設定できます。ターゲットモードは、ポートをFCイニシエータに接続するために使用されます。

タスクの内容

オンボードのFCポートは、それぞれイニシエータまたはターゲットとして個別に構成できます。特定のFCアダプタのポートは、オンボードのFCポートと同様に、ターゲットポートまたはイニシエータポートとして個別に構成することもできます。ターゲットモードに設定できるアダプタのリストについては、を参照"NetApp Hardware Universe"してください。

FCアダプタを設定する手順は、FCプロトコルとFC-NVMeプロトコルで同じです。ただし、FC-NVMeをサポートするFCアダプタは一部のみです。FC-NVMeプロトコルをサポートするアダプタのリストについては、を参照してください"NetApp Hardware Universe"。

手順

1. アダプタをオフラインにします。

   ```
   node run -node node_name storage disable adapter adapter_name
   ```

   アダプタがオフラインにならない場合は、システムの適切なアダプタポートからケーブルを取り外すこともできます。

2. アダプタをイニシエータからターゲットに変更します。

   ```
   system node hardware unified-connect modify -t target -node node_name adapter
   adapter_name
   ```

3. 変更したアダプタをホストしているノードをリブートします。
4. ターゲットポートの設定が正しいことを確認します。

   ```
   network fcp adapter show -node node_name
   ```

5. アダプタをオンラインにします。

   ```
   network fcp adapter modify -node node_name -adapter adapter_port -state up
   ```

### FCターゲットアダプタに関する情報を表示する

## コマンドを使用すると、システム内のFCアダプタのシステム設定やアダプタ情報を表示できます `network fcp adapter show`。

ステップ

1. コマンドを使用して、FCアダプタに関する情報を表示します `network fcp adapter show`。

出力には、使用されている各スロットのシステム設定情報およびアダプタ情報が表示されます。

```
network fcp adapter show -instance -node node1 -adapter 0a
```

#### FCアダプタの速度を変更する

自動ネゴシエーションを使わずに、アダプタのターゲットポートの速度を接続先デバイスの速度と同じにすることを推奨します。自動ネゴシエーションを設定したポートの方が、ギブバックやテイクオーバーなどの中断後の再接続に時間がかかる可能性があります。

必要なもの

このアダプタをホームポートとして使用しているすべての LIF をオフラインにする必要があります。

タスクの内容

この処理ではクラスタ内のすべてのStorage Virtual Machine（SVM）とLIFが対象となるため、パラメータと`-home-lif`パラメータを使用して処理範囲を制限する必要があります `-home-port`。これらのパラメータを使用しないと、処理環境によってクラスタ内のすべての LIF が処理によって使用されなくなる可能性があります。

手順

1. アダプタのすべての LIF をオフラインにします。

   ```
   network interface modify -vserver * -lif * { -home-node node1 -home-port 0c }
   -status-admin down
   ```

2. アダプタをオフラインにします。

   ```
   network fcp adapter modify -node node1 -adapter 0c -state down
   ```

   アダプタがオフラインにならない場合は、システムの適切なアダプタポートからケーブルを取り外すこともできます。

3. ポートアダプタの最大速度を確認します。

   ```
   fcp adapter show -instance
   ```

   アダプタ速度を最大速度よりも速くすることはできません。

4. アダプタ速度を変更します。

   ```
   network fcp adapter modify -node node1 -adapter 0c -speed 16
   ```

5. アダプタをオンラインにします。

   ```
   network fcp adapter modify -node node1 -adapter 0c -state up
   ```

6. アダプタのすべての LIF をオンラインにします。

   ```
   network interface modify -vserver * -lif * { -home-node node1 -home-port 0c }
   ```

```
-status-admin up
```

サポートされる**FC**ポート

## オンボードのFCポートおよびFC用に構成されるCNA / UTA2ポートの数は、コントローラのモデルによって異なります。また、 FC ポートは、サポートされている FC ターゲット拡張アダプタのほか、 FC SFP+ アダプタ用の追加の UTA2 カードからも提供されます。

オンボードの**FC**、**UTA**、および**UTA2**ポート

- オンボードポートは、ターゲットまたはイニシエータのどちらかのFCポートとして個別に構成できます。
- オンボードFCポートの数は、コントローラのモデルによって異なります。

  に "NetApp Hardware Universe"は、各コントローラモデルのオンボードFCポートの一覧が記載されています。

- FAS2520システムはFCをサポートしていません。

ターゲット拡張アダプタの**FC**ポート

- 使用可能なターゲット拡張アダプタは、コントローラのモデルによって異なります。

  に "NetApp Hardware Universe"は、各コントローラモデルのターゲット拡張アダプタの一覧が記載されています。

- 一部のFC拡張アダプタのポートは、工場出荷時にイニシエータまたはターゲットとして構成されており、変更することはできません。

  その他のポートについては、オンボードのFCポートと同様に、ターゲットまたはイニシエータのどちらかのFCポートとして個別に構成できます。完全なリストについては、を参照して "NetApp Hardware Universe"ください。

**X1133A-R6**アダプタ使用時の接続の切断を防止

## 別のX1133A-R6 HBAへの冗長パスをシステムに設定することで、ポート障害時に接続が失われないようにすることができます。

X1133A-R6 HBA は、 4 ポート 16Gb の FC アダプタで、 2 組の 2 ポートペアで構成されます。X1133A-R6 アダプタは、ターゲットモードまたはイニシエータモードとして設定できます。2 ポートペアはそれぞれ 1 つの ASIC でサポートされます（たとえば、ポート 1 とポート 2 は ASIC 1 、ポート 3 とポート 4 は ASIC 2 ）。単一のASIC上の両方のポートは、ターゲットモードまたはイニシエータモードのいずれかで同じモードで動作するように設定する必要があります。ペアをサポートする ASIC でエラーが発生すると、そのペアの両方のポートがオフラインになります。

接続が切断されないようにするには、別の X1133A-R6 HBA への冗長パスか、 HBA の別の ASIC でサポートされるポートへの冗長パスを構成します。

# FCoEコウセイ

## FCoEの設定方法の概要

FCoEは、FCoEスイッチを使用してさまざまな方法で設定できます。直接接続型の構成はFCoEではサポートされません。

FCoE構成はすべてデュアルファブリックで、完全に冗長化されており、ホスト側のマルチパスソフトウェアが必要です。いずれのFCoE構成でも、イニシエータとターゲット間のパスには、最大ホップ数の範囲内でFCoEスイッチとFCスイッチを複数配置できます。スイッチを相互に接続するには、イーサネットISLに対応したバージョンのファームウェアがスイッチで実行されている必要があります。FCoE構成の各ホストでオペレーティングシステムが異なることがあります。

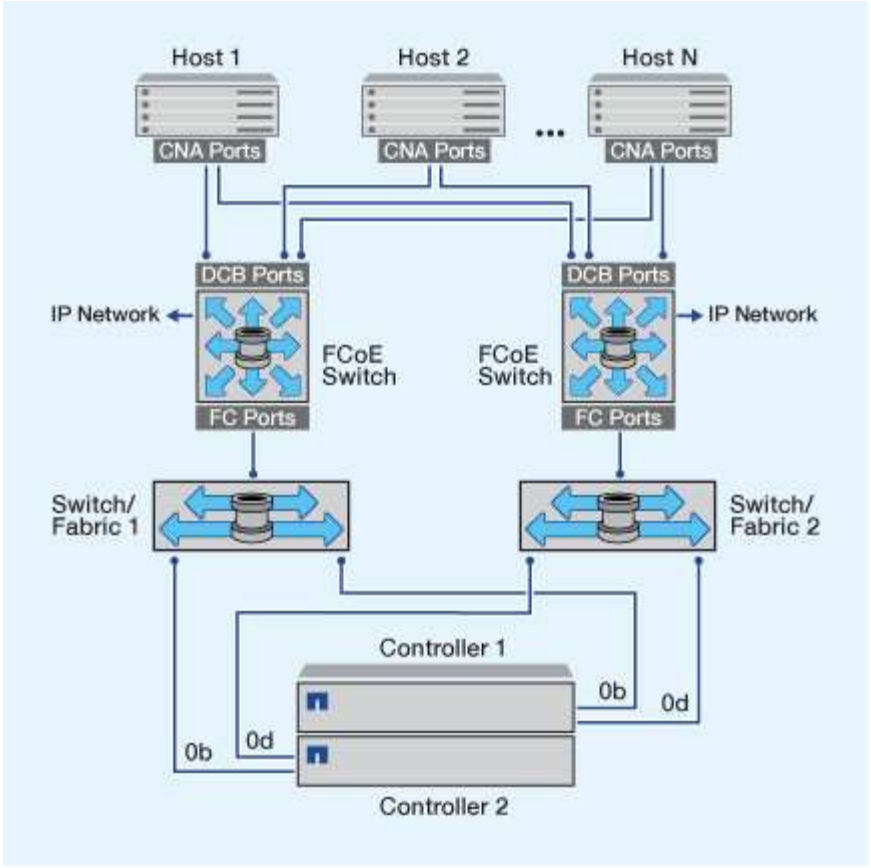
FCoE構成には、FCoEの機能を明示的にサポートするイーサネットスイッチが必要です。FCoE構成は、FCスイッチと同じ相互運用性と品質管理のプロセスで検証されます。サポートされる構成の一覧については、Interoperability Matrixを参照してください。サポートされる構成に含まれるパラメータには、スイッチモデル、単一ファブリックに導入できるスイッチの数、サポートされるスイッチファームウェアのバージョンなどがあります。

次の図のFCターゲット拡張アダプタのポート番号は一例です。実際のポート番号は、FCoEターゲット拡張アダプタがインストールされている拡張スロットによって変わる場合があります。

### FCoEイニシエータからFCターゲット

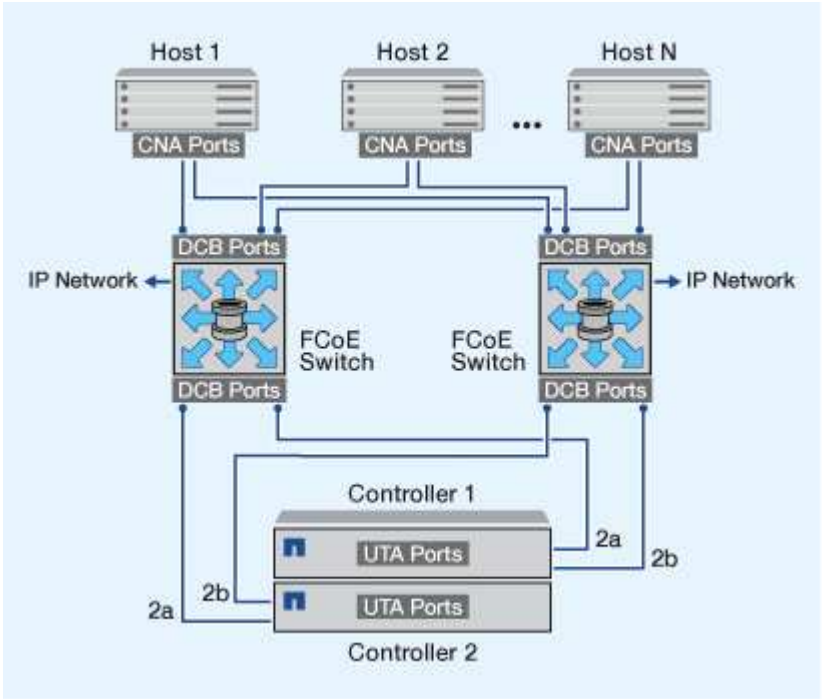
FCoEイニシエータ（CNA）を使用すると、FCoEスイッチからFCターゲットポートに接続して、ホストをHAペアの両方のコントローラに接続できます。FCoEスイッチにはFCポートも必要です。ホストのFCoEイニシエータは常にFCoEスイッチに接続されます。FCoEスイッチは、FCターゲットに直接接続することも、FCスイッチを介してFCターゲットに接続することもできます。

次の図では、ホストのCNAをFCoEスイッチに接続し、FCスイッチをHAペアに接続しています。



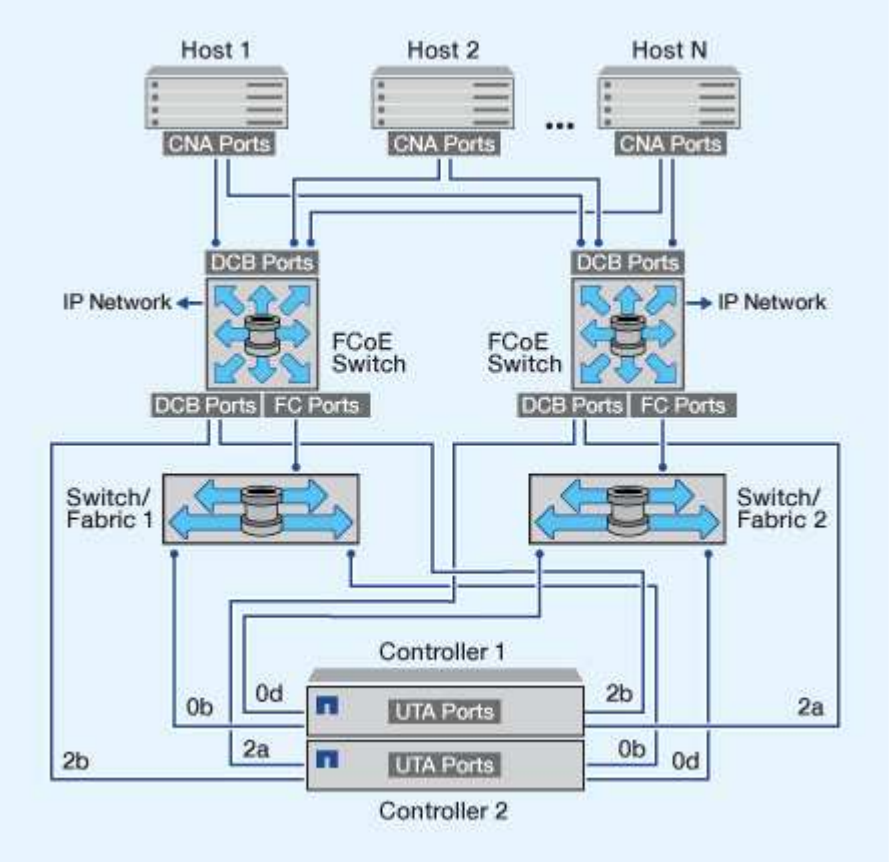

**FCoE**イニシエータから**FCoE**ターゲット

ホストのFCoEイニシエータ（CNA）を使用すると、FCoEスイッチを介して、ホストをHAペアの両方のコントローラのFCoEターゲットポート（UTAまたはUTA2とも呼ばれる）に接続できます。



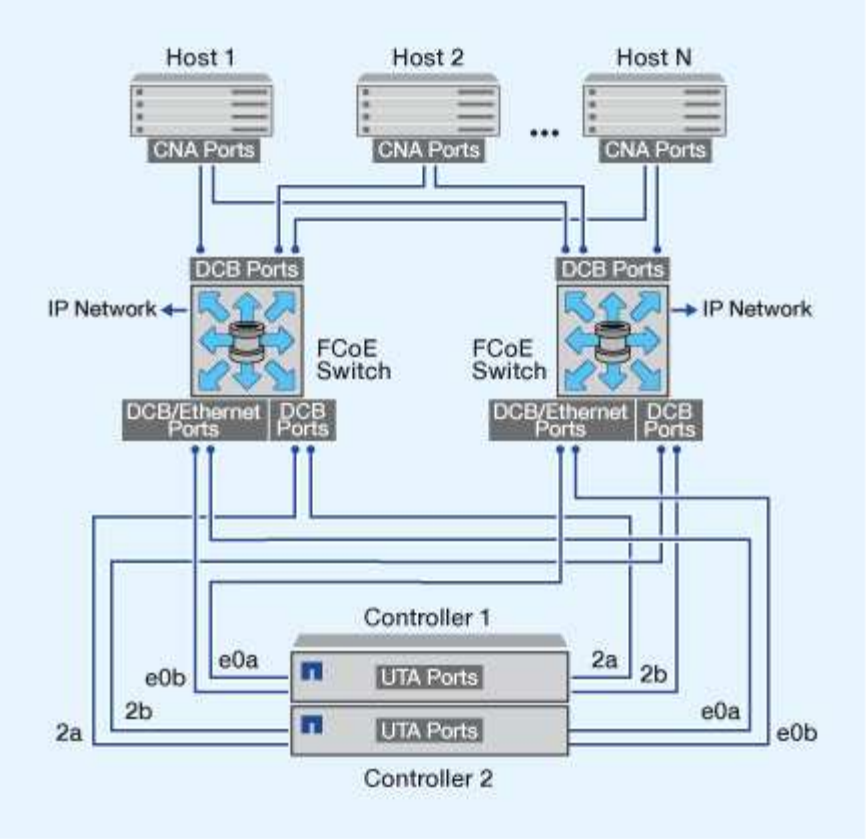
**FCoE**イニシエータから**FCoE**および**FC**ターゲット

ホストのFCoEイニシエータ（CNA）を使用すると、FCoEスイッチを介して、ホストをHAペアの両方のコントローラのFCoEおよびFCターゲットポート（UTAまたはUTA2とも呼ばれる）に接続できます。




**FCoE**と**IP**ストレージプロトコルの混在

ホストのFCoEイニシエータ（CNA）を使用すると、FCoEスイッチを介して、ホストをHAペアの両方のコントローラのFCoEターゲットポート（UTAまたはUTA2とも呼ばれる）に接続できます。FCoEポートは、単一のスイッチへの従来のリンクアグリゲーションを使用できません。Ciscoスイッチでは、FCoEをサポートする特殊なタイプのリンクアグリゲーション（仮想ポートチャネル）がサポートされます。仮想ポートチャネルは、2つのスイッチへの個 々 のリンクを集約します。仮想ポートチャネルは、他のイーサネットトラフィックにも使用できます。NFS、SMB、iSCSI、およびその他のイーサネットトラフィックなど、FCoE以外のトラフィックに使用されるポートでは、FCoEスイッチの通常のイーサネットポートを使用できます。




**FCoE**イニシエータとターゲットの組み合わせ

## FCoEと従来のFCのイニシエータとターゲットの特定の組み合わせがサポートされます。

**FCoE**イニシエータ

ホストコンピュータのFCoEイニシエータは、ストレージコントローラのFCoEターゲットと従来のFCターゲットの両方で使用できます。ホストのFCoEイニシエータはFCoE DCB（Data Center Bridging）スイッチに接続する必要があります。ターゲットに直接接続することはできません。

次の表に、サポートされる組み合わせを示します。

| イニシエータ | ターゲット | サポートの有無 |
|---|---|---|
| FC | FC | ○ |
| FC | FCoE | ○ |
| FCoE | FC | ○ |
| FCoE | FCoE | ○ |

### FCoEターゲット

ストレージコントローラでFCoEターゲットポートと4Gb、8Gb、または16GbのFCポートを混在させることができます。FCポートがアドインのターゲットアダプタであるかオンボードのポートであるかは関係ありません。FCoEとFCの両方のターゲットアダプタを同じストレージコントローラに搭載できます。

FCのオンボードポートと拡張ポートの組み合わせルールも適用されます。

### サポートされるFCoEホップ数

ホストとストレージシステムの間でサポートされるFibre Channel over Ethernet（FCoE）の最大ホップ数は、スイッチベンダーとストレージシステムでのFCoE構成のサポートによって異なります。

ホップ数は、イニシエータ（ホスト）とターゲット（ストレージシステム）の間のパスにあるスイッチの数として定義されます。Cisco Systems のマニュアルでは、この値のことを「 SAN fabric_ の直径」とも呼んでいます。

FCoEでは、FCoEスイッチをFCスイッチに接続できます。

エンドツーエンドのFCoE接続では、イーサネットInter-Switch Link（ISL；スイッチ間リンク）に対応するバージョンのファームウェアがFCoEスイッチで実行されている必要があります。

次の表に、サポートされる最大ホップ数を示します。

| スイッチベンダー | サポートされるホップ数 |
| --- | --- |
| Brocade | FCの場合は7<br><br>FCoEの場合は5 |
| Cisco | 7<br><br>最大3つのスイッチをFCoEスイッチにすることができます。 |

## ファイバチャネルとFCoEのゾーニング

### ファイバチャネルとFCoEのゾーニングの概要

FC ゾーン、 FC-NVMe ゾーン、または FCoE ゾーンは、ファブリック内の 1 つ以上のポートを論理的にグループ化したものです。デバイスがお互いを認識し、接続し、相互にセッションを作成し、通信できるようにするには、両方のポートが共通のゾーンメンバーシップを持っている必要があります。シングルイニシエータゾーニングを推奨します。

#### ゾーニングを行う理由

- イニシエータ HBA 間のクロストークを削減または解消できます。

これは小規模な環境でも発生し、ゾーニングを実装する最大の理由の 1 つです。ゾーニングによってファブリックの論理サブセットを作成することで、クロストークの問題が解消されます。

- 特定の FC 、 FC-NVMe 、または FCoE ポートへの使用可能なパスの数と、ホストと特定の LUN の間に認識されるパスの数を減らすことができます。

  たとえば、一部のホスト OS のマルチパスソリューションには、管理できるパスの数に制限があります。ゾーニングを使用すると、 OS のマルチパスドライバで認識されるパスの数を減らすことができます。ホストにマルチパス解決策がインストールされていない場合は、ファブリックのゾーニングまたは SVM の選択的 LUN マッピング（ SLM ）とポートセットの組み合わせを使用して、認識される LUN へのパスが 1 つだけであることを確認する必要があります。

- ゾーンを共有するエンドポイントへのアクセスと接続を制限することで、セキュリティを強化します。

  共通のゾーンがないポート同士が通信することはできません。

- 発生する問題を切り離すことで SAN の信頼性が高まり、問題の範囲を限定することで解決時間を短縮する効果があります。

ゾーニングに関する推奨事項

- 1 つの SAN にホストを 4 つ以上接続する場合や SAN に接続されたノードで SLM が実装されていない場合は、常にゾーニングを実装してください。
- 一部のスイッチベンダーでは World Wide Node Name のゾーニングも使用できますが、特定のポートを正しく定義し、 NPIV を効果的に利用するには、 World Wide Port Name のゾーニングを使用する必要があります。
- 管理性を損なわない範囲でゾーンサイズを制限することを推奨します。

  複数のゾーンを重複させてサイズを制限することができます。ホストまたはホストクラスタごとにゾーンを定義することを推奨します。

- イニシエータ HBA 間のクロストークを解消するために、単一イニシエータのゾーニングを使用してください。

**World Wide Name**に基づくゾーニング

World Wide Name（WWN）に基づくゾーニングでは、ゾーンに含めるメンバーのWWNを指定します。ONTAPのゾーニングでは、World Wide Port Name（WWPN）ゾーニングを使用する必要があります。

WWPNゾーニングは柔軟性に優れており、デバイスがファブリックに物理的に接続されている場所によってアクセスが決まりません。ゾーンを再設定することなく、1つのポートから別のポートにケーブルを移動できます。

ONTAPを実行するストレージコントローラへのファイバチャネルパスでは、ノードの物理ポートのWWPNではなく、ターゲットの論理インターフェイス（LIF）のWWPNを使用してFCスイッチをゾーニングしてください。LIF の詳細については、『 ONTAP ネットワーク管理ガイド』を参照してください。

"ネットワーク管理"

個 々 のゾーン

推奨されるゾーニング設定では、ゾーンごとに 1 つのホストイニシエータを配置します。ゾーンは、ホストイニシエータポートとストレージノード上の 1 つ以上のターゲット LIF で構成され、ターゲットあたりの希望する数のパスまで LUN へのアクセスを提供します。つまり、同じノードにアクセスする複数のホストはお互いのポートを認識できませんが、各イニシエータはすべてのノードにアクセスできます。

Storage Virtual Machine（SVM）のすべてのLIFを、ホストイニシエータを含むゾーンに追加する必要があります。これにより、既存のゾーンを編集したり、新しいゾーンを作成したりせずに、ボリュームや LUN を移動できます。

ONTAP を実行するノードへのファイバチャネルパスでは、ノードの物理ポートの WWPN ではなく、ターゲットの論理インターフェイス（ LIF ）の WWPN を使用して FC スイッチをゾーニングしてください。物理ポートの WWPN は「 50 」で始まり、 LIF の WWPN は「 20 」で始まります。

単一ファブリックゾーニング

単一ファブリック構成でも、各ホストイニシエータを各ストレージノードに接続できます。複数のパスを管理するには、ホストにマルチパスソフトウェアが必要です。ソリューションの耐障害性を確保するために、マルチパス用に各ホストに2つのイニシエータが必要です。

各イニシエータには、そのイニシエータがアクセスできる各ノードのLIFを少なくとも1つ設定する必要があります。ホストイニシエータからクラスタ内のHAペアのノードへのパスが少なくとも1つあるようにゾーニングを設定して、LUN接続用のパスを提供する必要があります。つまり、ホスト上の各イニシエータには、そのゾーン構成内のノードごとにターゲットLIFが1つだけ割り当てられます。クラスタ内の同じノードまたは複数のノードへのパスが複数必要な場合は、ゾーン構成内の各ノードに複数のLIFが割り当てられます。これにより、ノードに障害が発生した場合や、LUNを含むボリュームが別のノードに移動された場合でも、ホストはLUNに引き続きアクセスできます。また、レポートノードを適切に設定する必要があります。

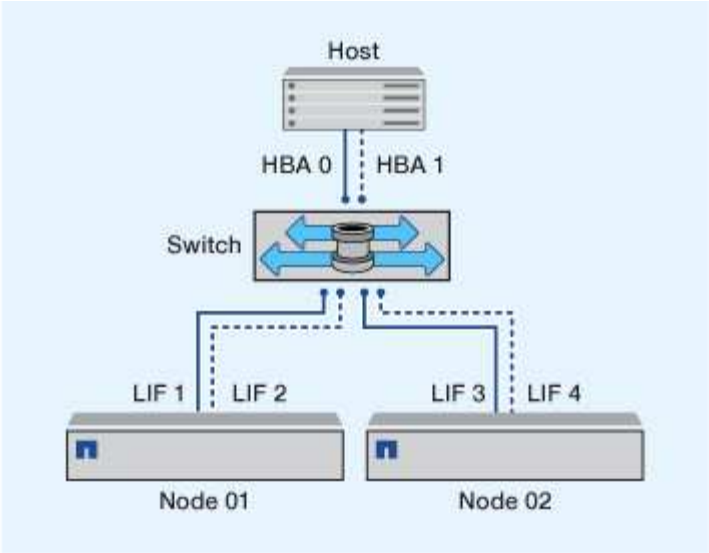
単一ファブリック構成はサポートされていますが、可用性に優れているとはみなされません。1つのコンポーネントの障害が、データ アクセスの中断を招く可能性があります。

次の図では、ホストに2つのイニシエータがあり、マルチパス ソフトウェアを実行しています。次の2つのゾーンがあります。

この図で使用されている命名規則は、ONTAPソリューションで使用できる一例です。

- ゾーン1：HBA 0、LIF_1、およびLIF_3
- ゾーン2：HBA 1、LIF_2、およびLIF_4

構成に追加のノードが含まれている場合は、追加のノードのLIFがこれらのゾーンに含まれます。




この例では、各ゾーンに4つのLIFをすべて配置することもできます。その場合のゾーンは次のようになります。

- ゾーン1：HBA 0、LIF_1、LIF_2、LIF_3、およびLIF_4
- ゾーン2：HBA 1、LIF_1、LIF_2、LIF_3、およびLIF_4

ホストオペレーティングシステムとマルチパスソフトウェアが、ノード上のLUNへのアクセスに使用される数のパスをサポートしている必要があります。ノードのLUNへのアクセスに使用するパスの数については、SAN構成の制限に関するセクションを参照してください。

関連情報

"NetApp Hardware Universe"

デュアルファブリックの**HA**ペアのゾーニング

## デュアルファブリック構成では、各ホストイニシエータを各クラスタノードに接続できます。各ホストイニシエータは、異なるスイッチを使用してクラスタノードにアクセスします。複数のパスを管理するには、ホストにマルチパスソフトウェアが必要です。

1つのコンポーネントで障害が発生してもデータへのアクセスが維持されるため、デュアルファブリック構成はハイアベイラビリティとみなされます。

次の図では、ホストに2つのイニシエータがあり、マルチパスソフトウェアを実行しています。2つのゾーンがあります。SLMは、すべてのノードがレポートノードとみなされるように設定されています。

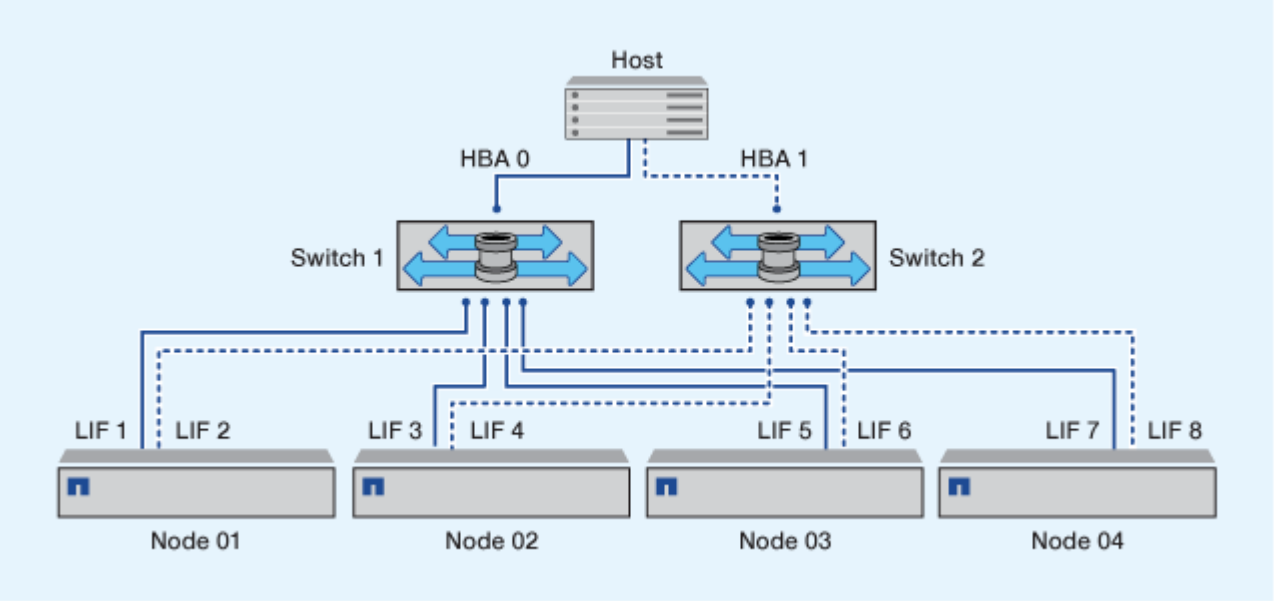
この図で使用されている命名規則は、ONTAPソリューションで使用できる一例です。

- ゾーン1：HBA 0、LIF_1、LIF_3、LIF_5、およびLIF_7
- ゾーン2：HBA 1、LIF_2、LIF_4、LIF_6、およびLIF_8

各ホストイニシエータは、異なるスイッチを使用してゾーニングされます。ゾーン1にはスイッチ1からアクセスします。ゾーン2にはスイッチ2からアクセスします。

各イニシエータは、すべてのノードのLIFにアクセスできます。これにより、ノードで障害が発生しても、ホストはLUNに引き続きアクセスできます。SVMは、選択的LUNマップ（SLM）とレポートノードの設定に基づいて、クラスタソリューション内のすべてのノードのすべてのiSCSI LIFとFC LIFにアクセスできます。SLM、ポートセット、またはFCスイッチゾーニングを使用して、SVMからホストへのパスの数とSVMからLUNへのパスの数を減らすことができます。

構成に追加のノードが含まれている場合は、追加のノードのLIFがこれらのゾーンに含まれます。




ホストオペレーティングシステムとマルチパスソフトウェアが、ノード上のLUNへのアクセスに使用される数のパスをサポートしている必要があります。

関連情報

"NetApp Hardware Universe"

**Cisco FC**および**FCoE**スイッチのゾーニング制限

Cisco FC スイッチおよび FCoE スイッチを使用する場合、 1 つのファブリックゾーンに同じ物理ポートのターゲット LIF を複数含めることはできません。同じポートの LIF を同じゾーンに複数配置すると、接続が失われた場合に LIF ポートがリカバリできなくなる可能性があります。

FC-NVMe プロトコルには、通常の FC スイッチが FC プロトコルとまったく同じ方法で使用されます。

- FC および FCoE プロトコルの複数の LIF は、ゾーンが同じでなければノード上の物理ポートを共有することができます。
- FC-NVMe と FCoE は、同じ物理ポートを共有できません。
- FC と FC-NVMe は、同じ 32Gb 物理ポートを共有できます。
- Cisco FC スイッチおよび FCoE スイッチでは、特定のポートの各 LIF をそのポートの他の LIF とは別のゾーンに配置する必要があります。
- 1 つのゾーンに FC と FCoE 両方の LIF を配置することができます。ゾーンにはクラスタ内のすべてのターゲットポートのLIFを含めることができますが、ホストのパス制限を超えないように注意し、SLMの設

定を確認してください。

- 物理ポートが異なる LIF は、同じゾーンに配置することもできます。
- Cisco スイッチを使用する場合は、 LIF を分離する必要があります。

  必須ではありませんが、 LIF の分離はすべてのスイッチで推奨されます

## 共有SAN構成の要件

### 共有SAN構成とは、ONTAPストレージシステムと他社のストレージシステムの両方に接続されるホストのことです。ONTAPストレージシステムと他のベンダーのストレージシステムに単一のホストからアクセスする場合は、いくつかの要件を満たす必要があります。

すべてのホストオペレーティングシステムで、各ベンダーのストレージシステムへの接続には別 々 のアダプタを使用することを推奨します。別 々 のアダプタを使用すると、ドライバと設定が競合する可能性が低くなります。ONTAPストレージシステムに接続する場合は、NetApp Interoperability Matrix Toolにサポート対象として記載されているアダプタモデル、BIOS、ファームウェア、ドライバを使用する必要があります。

必須または推奨のタイムアウト値や、ホストのその他のストレージパラメータを設定する必要があります。NetAppソフトウェアをインストールするか、NetApp設定を最後に適用する必要があります。

- AIXの場合、構成に対応するAIX Host Utilitiesバージョンの値をInteroperability Matrix Toolで確認して適用します。
- ESXの場合、Virtual Storage Console for VMware vSphereを使用してホスト設定を適用します。
- HP-UXの場合は、HP-UXのデフォルトのストレージ設定を使用する必要があります。
- Linuxの場合、構成に対応するLinux Host Utilitiesバージョンの値をInteroperability Matrix Toolで確認して適用します。
- Solarisの場合、構成に対応するSolaris Host Utilitiesバージョンの値をInteroperability Matrix Toolで確認して適用します。
- Windowsの場合、構成に対応するWindows Host UtilitiesバージョンをInteroperability Matrix Toolで確認してインストールする必要があります。

関連情報

"NetApp Interoperability Matrix Tool"

## MetroCluster環境でのSAN構成

#### MetroCluster環境でのSAN構成

### MetroCluster環境でSAN構成を使用する場合は、一定の考慮事項に注意する必要があります。

- MetroCluster 構成では ' フロントエンド FC ファブリックのルーテッド VSAN 構成はサポートされません
- ONTAP 9 .15.1以降では、NVMe/TCPで4ノードのMetroCluster IP構成がサポートされます。
- ONTAP 9.12.1以降では、NVMe / FCで4ノードのMetroCluster IP構成がサポートされます。MetroCluster構成は、ONTAP 9.12.1よりも前のフロントエンドNVMeネットワークではサポートされません。

- MetroCluster構成では、iSCSI、FC、FCoEなどのその他のSANプロトコルがサポートされます。
- SANクライアント構成を使用している場合は、（IMT）に記載されているメモにMetroCluster構成に関する特別な考慮事項がないかどうかを確認する必要があります"NetApp Interoperability Matrix Tool"。
- MetroClusterの自動計画外スイッチオーバーとTiebreakerまたはMediatorで開始されるスイッチオーバーをサポートするには、オペレーティングシステムとアプリケーションで120秒のI/O耐障害性を提供する必要があります。
- MetroCluster構成では、フロントエンドFCファブリックの両側で同じWWNNとWWPNが使用されます。

関連情報

- "MetroClusterのデータ保護とディザスタリカバリの概要"
- "技術情報アーティクル：「What are AIX Host support considerations in a MetroCluster configuration？」"
- "技術情報アーティクル：「Solaris host support considerations in a MetroCluster configuration」"

スイッチオーバーとスイッチバックの間でポートの重複を防止

## SAN環境では、古いポートがオフラインになって新しいポートがオンラインになったときに重複しないようにフロントエンドスイッチを設定できます。

スイッチオーバーの実行中、ディザスタサイトのFCポートがオフラインであることがファブリックで検出され、ネームサービスとディレクトリサービスからこのポートが削除される前に、サバイバーサイトのFCポートがファブリックにログインすることがあります。

災害時にFCポートをまだ削除していない場合、WWPNの重複が原因でサバイバーサイトのFCポートのファブリックログイン試行が拒否されることがあります。FCスイッチのこの動作は、既存のデバイスではなく以前のデバイスのログインを維持するように変更できます。この動作が他のファブリックデバイスに与える影響を確認する必要があります。詳細については、スイッチベンダーにお問い合わせください。

スイッチのタイプに応じて、正しい手順を選択します。

例 **9.** 手順

**Cisco**スイッチ

1. スイッチに接続してログインします。
2. コンフィギュレーションモードを開始します。

```
switch# config t
switch(config)#
```

3. ネームサーバデータベースの最初のデバイスエントリを新しいデバイスで上書きします。

```
switch(config)# no fcns reject-duplicate-pwwn vsan 1
```

4. NX-OS 8.xを実行しているスイッチで、flogi quiesce timeoutがゼロに設定されていることを確認します。

   a. 休止時間を表示します。

   ```
   switch(config)# show flogi interval info \| i quiesce
   ```

   ```
   Stats:  fs flogi quiesce timerval:  0
   ```

   b. 前の手順の出力でtimervalがゼロであることが示されていない場合は、ゼロに設定します。

   ```
   switch(config)# flogi scale enable
   ```

```
switch(config)$ flogi quiesce timeout 0
```

**Brocade**スイッチ

1. スイッチに接続してログインします。
2. コマンドを入力します `switchDisable`。
3. コマンドを入力し `configure`、プロンプトでを押し `y`ます。

```
 F-Port login parameters (yes, y, no, n): [no] y
```

4. 設定1を選択：

```
- 0: First login take precedence over the second login (default)
- 1: Second login overrides first login.
- 2: the port type determines the behavior
Enforce FLOGI/FDISC login: (0..2) [0] 1
```

5. 残りのプロンプトに応答するか、 * Ctrl+D* を押します。
6. コマンドを入力します `switchEnable`。

関連情報

"テストまたはメンテナンスのためのスイッチオーバーの実行"

## ホストでのマルチパスのサポート

### ホストでのマルチパスサポートの概要

**ONTAPでは、FCとiSCSIの両方のパスに常にAsymmetric Logical Unit Access（ALUA；非対称論理ユニットアクセス）が使用されます。FCプロトコルとiSCSIプロトコルのALUAをサポートするホスト構成を使用してください。**

ONTAP 9 .5以降では、Asynchronous Namespace Access（ANA）を使用するNVMe構成でマルチパスHAペアのフェイルオーバー/ギブバックがサポートされます。ONTAP 9 .4では、NVMeでサポートされるホストからターゲットへのパスは1つだけです。アプリケーションホストは、ハイアベイラビリティ（HA）パートナーへのパスフェイルオーバーを管理する必要があります。

ALUAまたはANAをサポートする具体的なホスト構成については、ご使用のホストオペレーティングシステムに対応したおよび "ONTAP SANホスト構成"を参照して "NetApp Interoperability Matrix Tool"ください。

### ホストのマルチパスソフトウェアが必要な場合

**Storage Virtual Machine（SVM）の論理インターフェイス（LIF）からファブリックへのパスが複数ある場合は、マルチパスソフトウェアが必要です。ホストが複数のパスを介してLUNにアクセスできる場合は、常にホストにマルチパスソフトウェアが必要です。**

マルチパスソフトウェアは、LUNへのすべてのパスで単一のディスクをオペレーティングシステムに提供します。マルチパスソフトウェアがないと、各パスがオペレーティングシステムで別 々 のディスクとして扱われ、データが破損する可能性があります。

次のいずれかに該当する場合、ソリューションには複数のパスがあるとみなされます。

- ホストの単一のイニシエータポートをSVMの複数のSAN LIFに接続している場合
- 複数のイニシエータポートをSVMの単一のSAN LIFに接続している場合
- 複数のイニシエータポートをSVMの複数のSAN LIFに接続している場合

HA構成では、マルチパスソフトウェアを推奨します。選択的LUNマップに加えて、FCスイッチのゾーニングまたはポートセットを使用してLUNへのアクセスに使用するパスを制限することを推奨します。

マルチパスソフトウェアは、マルチパスI/O（MPIO）ソフトウェアとも呼ばれます。

### ホストからクラスタ内のノードへの推奨されるパス数

**ホストからクラスタ内の各ノードへのパスは8個までにする必要があります。ホストOSやホストで使用されるマルチパスでサポートされるパスの総数に注意してください。**

選択的LUNマップ（SLM）を使用して、クラスタ内のStorage Virtual Machine（SVM）が使用する各レポートノードへのパスをLUNごとに少なくとも2つ確保します。これにより、単一点障害（Single Point of Failure）が排除され、コンポーネント障害からシステムを保護できます。

クラスタにノードが4つ以上ある場合、またはいずれかのノードのSVMで5つ以上のターゲットポートを使用している場合は、次の方法でノード上のLUNへのアクセスに使用できるパスの数を制限して、推奨される最大数の8個を超えないようにすることができます。

- SLM

  SLMを使用すると、ホストからLUNへのパスの数が、LUNを所有するノードとそのHAパートナーのパスだけになります。SLMはデフォルトで有効になっています。

- iSCSIのポートセット
- ホストのFC igroupマッピング
- FCスイッチゾーニング

関連情報

"SAN管理"

## 構成の制限

**SAN**構成でサポートされるノード数の確認

### ONTAPでサポートされるクラスタあたりのノード数は、ONTAPのバージョン、クラスタ内のストレージコントローラのモデル、およびクラスタノードのプロトコルによって異なります。

タスクの内容

FC、FC-NVMe、FCoE、またはiSCSIが設定されたノードがクラスタにある場合、そのクラスタにはSANノードの制限が適用されます。クラスタ内のコントローラに基づくノードの制限については、 _ Hardware Universe _ を参照してください。

手順

1. に進みます "NetApp Hardware Universe"。
2. 左上の [* ホーム ] ボタンの横にある [* プラットフォーム ] をクリックし、プラットフォームの種類を選択します。
3. 使用しているONTAPのバージョンの横にあるチェックボックスをオンにします。

   プラットフォームを選択するための新しい列が表示されます。

4. ソリューションで使用するプラットフォームの横にあるチェックボックスをオンにします。
5. [ 仕様を選択 ] 列の [ すべて選択 *] チェックボックスをオフにします。
6. [ クラスタあたりの最大ノード数（ NAS / SAN ） * ] チェックボックスをオンにします。
7. [ 結果を表示（ Show Results ） ] をクリックする。

関連情報

"NetApp Hardware Universe"

**FC**構成および**FC-NVMe**構成におけるクラスタあたりのサポートされるホスト数を確認する

## クラスタに接続できる SAN ホストの最大数は、クラスタの各ノードに接続されるホストの数、ホストあたりのイニシエータ数、ホストあたりのセッション数、クラスタ内のノード数など、クラスタのさまざまな属性の組み合わせによって大きく異なります。

タスクの内容

FC 構成および FC-NVMe 構成では、システムの Initiator-Target Nexus （ ITN ；イニシエータ - ターゲット接続）の数に基づいて、クラスタにホストを追加できるかどうかを判断します。

1 つの ITN は、ホストのイニシエータからストレージシステムのターゲットへの 1 つのパスに該当します。FC 構成および FC-NVMe 構成のノードあたりの最大 ITN 数は 2 、 048 です。ITN がこの最大数を超えない限り、クラスタにホストを追加することができます。

クラスタで使用されている ITN の数を確認するには、クラスタの各ノードで次の手順を実行します。

手順

1. ノードの LIF をすべて特定します。
2. ノードのすべてのLIFに対して次のコマンドを実行します。

   ```
   fcp initiator show -fields wwpn, lif
   ```

   コマンド出力の一番下に表示されたエントリ数が、その LIF の ITN 数です。

3. それぞれの LIF について、表示された ITN 数を記録します。
4. クラスタのすべてのノードの各 LIF の ITN 数を合計します。

   この値がクラスタの ITN の総数になります。

**iSCSI**構成でサポートされるホスト数の確認

## iSCSI 構成で接続できる SAN ホストの最大数は、クラスタの各ノードに接続されるホストの数、ホストあたりのイニシエータ数、ホストあたりのログイン数、クラスタ内のノード数など、クラスタのさまざまな属性の組み合わせによって大きく異なります。

タスクの内容

ノードに直接または 1 つ以上のスイッチを介して接続できるホストの数は、使用可能なイーサネットポートの数で決まります。使用可能なイーサネットポートの数は、コントローラのモデル、およびコントローラにインストールされているアダプタの数とタイプによって決まります。コントローラおよびアダプタでサポートされるイーサネットポートの数は、 _ Hardware Universe _ で確認できます。

マルチノードクラスタ構成の場合は、ノードあたりの iSCSI セッションの数に基づいて、クラスタにホストを追加できるかどうかを判断する必要があります。ノードあたりの iSCSI セッションの最大数をクラスタが下回っている場合は、引き続きクラスタにホストを追加できます。ノードあたりの iSCSI セッションの最大数は、クラスタ内のコントローラのタイプによって異なります。

手順

1. ノードのターゲットポータルグループをすべて特定します。
2. ノードのすべてのターゲットポータルグループについて、それぞれ iSCSI セッションの数を確認します。

   `iscsi session show -tpgroup tpgroup`

   コマンド出力の一番下に表示されたエントリ数が、そのターゲットポータルグループの iSCSI セッション数です。
3. 各ターゲットポータルグループについて、表示された iSCSI セッション数を記録します。
4. ノードの各ターゲットポータルグループの iSCSI セッション数を追加します。

   この値がノードの iSCSI セッションの総数になります。

### FCスイッチノコウセイノセイゲン

ファイバチャネルスイッチには、ポート、ポートグループ、ブレード、およびスイッチごとにサポートされるログイン数など、最大構成制限があります。サポートされる制限については、スイッチベンダーのドキュメントを参照してください。

各FC論理インターフェイス（LIF）がFCスイッチポートにログインします。ノード上の1つのターゲットからのログインの総数は、LIFの数に、基盤となる物理ポートへのログイン数1を足した数です。スイッチベンダーが設定しているログインやその他の設定値の制限を超えないようにしてください。これは、NPIVが有効な仮想環境でホスト側で使用されているイニシエータにも当てはまります。ソリューションで使用しているターゲットまたはイニシエータのログインに関して、スイッチベンダーが設定している制限を超えないようにしてください。

#### Brocadeスイッチの最大数

Brocade スイッチの最大構成数は、 _Brocade 拡張性ガイドライン _ で確認できます。

#### Ciscoシステムのスイッチ制限

Ciscoスイッチの構成の制限については、使用しているバージョンのCiscoスイッチソフトウェアのガイドを参照して "Cisco設定の制限"ください。

### キュー深度の計算の概要

ノードおよびFCポートのファンインあたりのITN数を最大にするために、ホストのFCキュー深度の調整が必要になる場合があります。LUNの最大数と1つのFCポートに接続できるHBAの数は、FCターゲット ポートで使用可能なキューの深度によって制限されます。

#### タスクの内容

キュー深度は、ストレージコントローラで一度にキューに格納できるI/O要求（SCSIコマンド）の数です。ホストのイニシエータHBAからストレージコントローラのターゲットアダプタへのI/O要求ごとに、キューエントリが1つ作成されます。通常、キュー深度が大きいほどパフォーマンスは向上します。ただし、ストレージコントローラの最大キュー深度に達すると、ストレージコントローラはQFULL応答を返して受信コマンドを拒否します。QFULL状態が発生するとシステムパフォーマンスが大幅に低下し、一部のシステムでエラーが発生する可能性があるため、1台のストレージコントローラに多数のホストがアクセスしている場合は、QFULLが発生しないように慎重に計画する必要があります。

複数のイニシエータ（ホスト）を含む構成では、すべてのホストでキュー深度を同程度に設定する必要があります。同じターゲットポートを介してストレージコントローラに接続されているホスト間でキュー深度が異なるため、キュー深度が小さいホストは、キュー深度が大きいホストからリソースにアクセスできなくなります。

キュー深度を「チューニング」する場合は、次の一般的な推奨事項を考慮してください。

- 小規模から中規模のシステムでは、HBAキュー深度を32にします。
- 大規模なシステムでは、HBAキュー深度を128にします。
- 例外的なケースやパフォーマンステストでは、キュー深度を256にして、キューの問題の可能性を回避します。
- すべてのホストに均等にアクセスできるようにするには、すべてのホストのキュー深度を同じ値に設定する必要があります。
- パフォーマンスの低下やエラーを回避するために、ストレージコントローラのターゲットFCポートのキュー深度を超えないようにする必要があります。

手順

1. 1つのFCターゲットポートに接続しているすべてのホストのFCイニシエータの総数を数えます。
2. 128を掛けます。
   - 2 、 048 より小さい場合は、すべてのイニシエータのキュー深度を 128 に設定します。15台のホストがあり、1つのイニシエータがストレージコントローラ上の2つのターゲットポートのそれぞれに接続されています。15 × 128 = 1 、 920 。これは合計最大キュー深度の 2 、 048 より少ないため、すべてのイニシエータのキュー深度を 128 に設定できます。
   - この値が 2 、 048 よりも大きい場合は、手順 3 に進みます。30台のホストがあり、1つのイニシエータがストレージコントローラ上の2つのターゲットポートのそれぞれに接続されています。30 × 128 = 3 、 840 。これは合計最大キュー深度の 2 、 048 より大きいため、手順 3 に記載されているいずれかのオプションを実行して調整します。
3. 次のいずれかのオプションを選択して、ストレージコントローラにホストを追加します。
   - オプション1：
     i. FCターゲットポートを追加します。
     ii. FCイニシエータを再配置します。
     iii. 手順1と2を繰り返します。+ 必要なキュー深度 3 、 840 は、ポートあたりの使用可能なキュー深度を超えています。これを解決するには、各コントローラに2ポートのFCターゲットアダプタを追加し、30台のホストのうち15台を1つのポートセットに接続し、残りの15台を2つ目のポートセットに接続するようにFCスイッチをゾーニングし直します。これで、ポートあたりのキュー深度は 15 × 128 = 1 、 920 となります。
   - オプション2：
     i. 各ホストを「ラージ」または「モール」として指定します。これは、予想される I/O ニーズに基づいています。
     ii. 大規模イニシエータの数に128を掛けます。
     iii. 小規模イニシエータの数に32を掛けます。
     iv. 2つの結果を足し合わせます。
     v. 2 、 048 より小さい場合は、大規模ホストのキュー深度を 128 に、小規模ホストのキュー深度を

32 に設定します。

vi. 2 、 048 よりも大きい場合は、合計キュー深度が 2 、 048 以下になるまで各イニシエータのキュー深度を下げます。

> 特定の1秒あたりのI/Oスループットを達成するために必要なキュー深度を見積もるには、次の式を使用します。
>
> 必要なキュー深度=（1秒あたりのI/O数）×（応答時間）
>
> たとえば、応答時間 3 ミリ秒で 40 、 000 IOPS のスループットに必要なキュー深度は、 40 、 000 × （ .003 ） = 120 です。

基本的な推奨構成に従ってキュー深度を32に制限した場合、ターゲットポートに接続できるホストの最大数は64です。ただし、キュー深度を128にすると、1つのターゲットポートに接続できるホストの最大数は16になります。キュー深度が大きいほど、1つのターゲットポートでサポートできるホストの数が少なくなります。キュー深度を妥協できないような要件の場合は、追加のターゲットポートを用意する必要があります。

必要とされるキュー深度 3 、 840 は、ポートあたりの使用可能なキュー深度を超えています。ストレージ I/O のニーズが高い「大規模」ホストが 10 台あり、 I/O のニーズが低い「モール」ホストが 20 台あります。大規模ホストのイニシエータのキュー深度を128に、小規模ホストのイニシエータのキュー深度を32に設定します。

その結果、合計キュー深度は（ 10 × 128 ） + （ 20 × 32 ） = 1 、 920 になります。

使用可能なキュー深度を、各イニシエータに均等に分配できます。

そのため、イニシエータあたりのキュー深度は 2 、 048 ÷ 30 = 68 となります。

**SAN** ホストでキュー深度を設定します

## ノードあたりおよびFCポートのファンインあたりのITN数を最大にするために、ホストのキュー深度の変更が必要になる場合があります。

**AIX** ホスト

AIXホストのキュー深度は、コマンドを使用して変更できます `chdev`。コマンドを使用して行った変更 `chdev`はリブート後も維持されます。

例：

- hdisk7デバイスのキュー深度を変更するには、次のコマンドを使用します。

  ```
  chdev -l hdisk7 -a queue_depth=32
  ```

- fcs0 HBAのキュー深度を変更するには、次のコマンドを使用します。

  ```
  chdev -l fcs0 -a num_cmd_elems=128
  ```

  のデフォルト値 `num_cmd_elems`は200です。最大値は2、048です。

場合によっては、コマンドと `makdev -l fcs0 -P`コマンドを使用してHBAをオフラインにして変更後にオンラインに戻し `rmdev -l fcs0 -R`なければならないことがあり `num_cmd_elems`ます。

**HP-UX** ホスト

HP-UXホストのLUNまたはデバイスのキュー深度は、kernelパラメータを使用して変更できます `scsi_max_qdepth`。HBAのキュー深度は、カーネルパラメータを使用して変更できます `max_fcp_reqs`。

- のデフォルト値 `scsi_max_qdepth`は8です。最大値は255です。

  `scsi_max_qdepth`コマンドのオプションを `kmtune`使用すると、実行中のシステムで動的に変更できます `-u`。この変更は、システム上のすべてのデバイスに有効になります。たとえば、LUNのキュー深度を64に増やすには、次のコマンドを使用します。

  ```
  kmtune -u -s scsi_max_qdepth=64
  ```

  コマンドを使用すると、個 々 のデバイスファイルのキュー深度を変更でき `scsictl`ます。コマンドを使用した変更 `scsictl`は、システムのリブート後は維持されません。特定のデバイスファイルのキュー深度を表示および変更するには、次のコマンドを実行します。

  ```
  scsictl -a /dev/rdsk/c2t2d0

  scsictl -m queue_depth=16 /dev/rdsk/c2t2d0
  ```

- のデフォルト値 `max_fcp_reqs`は512です。最大値は1024です。

  変更を有効にするには、カーネルを再構築し、システムを再起動する必要があり `max_fcp_reqs`ます。たとえば、HBAのキュー深度を256に変更するには、次のコマンドを使用します。

  ```
  kmtune -u -s max_fcp_reqs=256
  ```

**Solaris** ホストの場合

SolarisホストのLUNおよびHBAのキュー深度を設定できます。

- LUN のキュー深度の場合：ホストで使用中の LUN の数に LUN あたりのスロットル（ lun-queue-depth ）をかけた値が、ホストの tgt-queue-depth の値以下になる必要があります。
- Sunスタックのキュー深度の場合：標準ドライバでは、LUN単位またはターゲット単位でHBAレベルを設定することはできません `max_throttle`。ネイティブドライバの値は、ファイルおよび `/kernel/drv/ssd.conf`ファイルのデバイスタイプ（`VID_PID`）単位で設定することを `/kernel/drv/sd.conf`推奨します `max_throttle`。ホストユーティリティでは、この値がMPxIO構成では64、Veritas DMP構成では8に設定されます。

手順

1. `# cd/kernel/drv`
2. `# vi lpfc.conf`
3. 検索対象 `/tft-queue (/tgt-queue)`

```
tgt-queue-depth=32
```

デフォルト値はインストール時に32に設定されます。

4. 環境の構成に基づいて、必要な値を設定します。
5. ファイルを保存します。
6. コマンドを使用してホストをリブートし `sync; sync; sync; reboot -- -r`ます。

#### QLogicHBAヨウノVMwareホスト

HBAタイムアウト設定を変更するには、コマンドを使用し `esxcfg-module`ます。ファイルを手動で更新すること `esx.conf`は推奨されません。

手順

1. rootユーザとしてサービスコンソールにログオンします。
2. コマンドを使用し `#vmkload_mod -l`て、現在ロードされているQlogic HBAモジュールを確認します。
3. Qlogic HBAの単一インスタンスの場合は、次のコマンドを実行します。

```
#esxcfg-module -s ql2xmaxqdepth=64 qla2300_707
```

この例では、qla2300_707モジュールを使用しています。の出力に基づいて、適切なモジュールを使用し `vmkload_mod -l`ます。

4. 次のコマンドを使用して変更を保存します。

```
#/usr/sbin/esxcfg-boot -b
```

5. 次のコマンドを使用してサーバをリブートします。

```
#reboot
```

6. 次のコマンドを使用して変更を確認します。
   a. `#esxcfg-module -g qla2300_707`
   b. `qla2300_707 enabled = 1 options = 'ql2xmaxqdepth=64'`

#### Emulex HBAヨウノVMwareホスト

HBAタイムアウト設定を変更するには、コマンドを使用し `esxcfg-module`ます。ファイルを手動で更新すること `esx.conf`は推奨されません。

手順

1. rootユーザとしてサービスコンソールにログオンします。
2. コマンドを使用し `#vmkload_mod -l grep lpfc`て、どのEmulex HBAが現在ロードされているかを確認します。
3. Emulex HBAの単一インスタンスの場合は、次のコマンドを入力します。

```
#esxcfg-module -s lpfc0_lun_queue_depth=16 lpfcdd_7xx
```

HBAのモデルに応じて、モジュールはlpfcdd_7xxまたはlpfcdd_732のいずれかになります。上記のコマンドはlpfcdd_7xxモジュールを使用します。の結果に基づいて、適切なモジュールを使用する必要があります `vmkload_mod -l`。

このコマンドを実行すると、lpfc0で表されるHBAのLUNキュー深度が16に設定されます。

4. Emulex HBAの複数のインスタンスの場合は、次のコマンドを実行します。

```
a esxcfg-module -s "lpfc0_lun_queue_depth=16 lpfc1_lun_queue_depth=16"
lpfcdd_7xx
```

lpfc0のLUNキュー深度とlpfc1のLUNキュー深度が16に設定されます。

5. 次のコマンドを入力します。

```
#esxcfg-boot -b
```

6. を使用してリブートします `#reboot`

#### Emulex HBAヨウノWindowsホスト

Windowsホストでは、ユーティリティを使用してEmulex HBAのキュー深度を更新できます `LPUTILNT`。

手順

1. ディレクトリにあるユーティリティを `C:\WINNT\system32`実行し `LPUTILNT`ます。
2. 右側のメニューから * Drive Parameters * （ドライブパラメータ）を選択します。
3. スクロールダウンして、 [**QueueDepth**] をダブルクリックします。

150 より大きい * QueueDepth * を設定する場合は、次の Windows レジストリ値も適切に増やす必要があります。

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\lpxnds\Parameters\Device\NumberOfRequests
```

#### Qlogic HBA用のWindowsホスト

Windowsホストでは、およびHBAマネージャユーティリティを使用してQlogic HBAのキュー深度を更新できます `SANsurfer`。

手順

1. HBAマネージャユーティリティを実行し `SANsurfer`ます。
2. [* HBA ポート > 設定 ] をクリックします。
3. リスト・ボックスの * HBA ポートの詳細設定 * をクリックします。
4. パラメータを更新し `Execution Throttle`ます。

#### Emulex HBAヨウノLinuxホスト

Linux ホストでは Emulex HBA のキュー深度を更新できます。更新をリブート後も維持するには、新しい RAM ディスクイメージを作成してホストをリブートする必要があります。

手順

1. 変更するキュー深度パラメータを特定します。

   ```
   modinfo lpfc|grep queue_depth
   ```

   キュー深度パラメータとその概要のリストが表示されます。使用しているオペレーティングシステムのバージョンに応じて、次のキュー深度パラメータを 1 つ以上変更できます。

   - `lpfc_lun_queue_depth`：特定のLUNのキューに格納できるFCコマンドの最大数（uint）
   - `lpfc_hba_queue_depth`：lpfc HBAのキューに格納できるFCコマンドの最大数（uint）
   - `lpfc_tgt_queue_depth`：特定のターゲットポートのキューに格納できるFCコマンドの最大数（uint）

     > `lpfc_tgt_queue_depth`パラメータは、`Red Hat Enterprise Linux 7.x`システム、`SUSE Linux Enterprise Server 11 SP4`システム、および`12.x`システムにのみ適用されます。

2. キュー深度を更新するには、Red Hat Enterprise Linux 5.xシステムの場合はファイル、Red Hat Enterprise Linux 6.x / 7.xシステム、またはSUSE Linux Enterprise Server 11.x / 12.xシステムの場合はファイルに、`/etc/modprobe.d/scsi.conf`キュー深度パラメータを追加します `/etc/modprobe.conf`。

   使用しているオペレーティングシステムのバージョンに応じて、次のコマンドを 1 つ以上追加できます。

   - `options lpfc lpfc_hba_queue_depth=new_queue_depth`
   - `options lpfc lpfc_lun_queue_depth=new_queue_depth`
   - `options lpfc_tgt_queue_depth=new_queue_depth`

3. 新しい RAM ディスクイメージを作成し、ホストをリブートして、リブート後も更新内容を維持します。

   詳細については、使用しているLinuxオペレーティングシステムのバージョンに対応したを参照してください"システム管理"。

4. 変更したキュー深度パラメータの値が更新されていることを確認します。

   ```
   root@localhost ~]#cat /sys/class/scsi_host/host5/lpfc_lun_queue_depth
         30
   ```

   キュー深度の現在の値が表示されます。

Linux ホストでは QLogic ドライバのデバイスキュー深度を更新できます。更新をリブート後も維持するには、新しい RAM ディスクイメージを作成してホストをリブートする必要があります。QLogic HBA のキュー深度を変更するには、 QLogic HBA の管理 GUI またはコマンドラインインターフェイス（ CLI ）を使用します。

このタスクでは、 QLogic HBA の CLI を使用して QLogic HBA のキュー深度を変更する方法を示します

手順

1. 変更するデバイスキュー深度パラメータを特定します。

   ```
   modinfo qla2xxx | grep ql2xmaxqdepth
   ```

   変更できるのはキュー深度パラメータのみ `ql2xmaxqdepth`です。このパラメータは、LUNごとに設定できる最大キュー深度を示します。RHEL 7.5以降のデフォルト値は64です。RHEL 7.4以前のデフォルト値は32です。

   ```
   root@localhost ~]# modinfo qla2xxx|grep ql2xmaxqdepth
   parm:       ql2xmaxqdepth:Maximum queue depth to set for each LUN.
   Default is 64. (int)
   ```

2. デバイスのキュー深度の値を更新します。

   - 永続的に変更する場合は、次の手順を実行します。

     i. キュー深度を更新するには、Red Hat Enterprise Linux 5.xシステムの場合はファイルに、`/etc/modprobe.d/scsi.conf`Red Hat Enterprise Linux 6.x / 7.xシステムまたはSUSE Linux Enterprise Server 11.x / 12.xシステムの場合はファイルに、キュー深度パラメータを追加し `/etc/modprobe.conf`ます。 `options qla2xxx ql2xmaxqdepth=new_queue_depth`

     ii. 新しい RAM ディスクイメージを作成し、ホストをリブートして、リブート後も更新内容を維持します。

     詳細については、使用しているLinuxオペレーティングシステムのバージョンに対応したを参照してください"システム管理"。

   - 現在のセッションだけでパラメータを変更する場合は、次のコマンドを実行します。

     ```
     echo new_queue_depth > /sys/module/qla2xxx/parameters/ql2xmaxqdepth
     ```

     次の例では、キュー深度を 128 に設定します。

   ```
   echo 128 > /sys/module/qla2xxx/parameters/ql2xmaxqdepth
   ```

3. キュー深度の値が更新されたことを確認します。

   ```
   cat /sys/module/qla2xxx/parameters/ql2xmaxqdepth
   ```

キュー深度の現在の値が表示されます。

4. QLogic HBA BIOSからファームウェアパラメータを更新して、QLogic HBAのキュー深度を変更します `Execution Throttle`。

   a. QLogic HBA管理CLIにログインします。

      ```
      /opt/QLogic_Corporation/QConvergeConsoleCLI/qaucli
      ```

   b. メインメニューからオプションを選択します `Adapter Configuration`。

      ```
      [root@localhost ~]#
      /opt/QLogic_Corporation/QConvergeConsoleCLI/qaucli
      Using config file:
      /opt/QLogic_Corporation/QConvergeConsoleCLI/qaucli.cfg
      Installation directory: /opt/QLogic_Corporation/QConvergeConsoleCLI
      Working dir: /root

      QConvergeConsole

              CLI - Version 2.2.0 (Build 15)

          Main Menu

          1:  Adapter Information
          **2:  Adapter Configuration**
          3:  Adapter Updates
          4:  Adapter Diagnostics
          5:  Monitoring
          6:  FabricCache CLI
          7:  Refresh
          8:  Help
          9:  Exit


              Please Enter Selection: 2
      ```

   c. アダプタ設定パラメータのリストから、オプションを選択し `HBA Parameters`ます。

```
1:  Adapter Alias
    2:  Adapter Port Alias
    **3:  HBA Parameters**
    4:  Persistent Names (udev)
    5:  Boot Devices Configuration
    6:  Virtual Ports (NPIV)
    7:  Target Link Speed (iiDMA)
    8:  Export (Save) Configuration
    9:  Generate Reports
   10:  Personality
   11:  FEC
(p or 0: Previous Menu; m or 98: Main Menu; ex or 99: Quit)
        Please Enter Selection: 3
```

d. HBA ポートのリストから、必要な HBA ポートを選択します。

```
Fibre Channel Adapter Configuration

    HBA Model QLE2562 SN: BFD1524C78510
      1: Port   1: WWPN: 21-00-00-24-FF-8D-98-E0 Online
      2: Port   2: WWPN: 21-00-00-24-FF-8D-98-E1 Online
    HBA Model QLE2672 SN: RFE1241G81915
      3: Port   1: WWPN: 21-00-00-0E-1E-09-B7-62 Online
      4: Port   2: WWPN: 21-00-00-0E-1E-09-B7-63 Online


        (p or 0: Previous Menu; m or 98: Main Menu; ex or 99: Quit)
        Please Enter Selection: 1
```

HBA ポートの詳細が表示されます。

e. [HBA Parameters]メニューで、オプションの現在の値を表示するオプションを `Execution Throttle`選択します `Display HBA Parameters。

このオプションのデフォルト値 `Execution Throttle`は65535です。

```
HBA Parameters Menu

======================================================
HBA           : 2 Port: 1
SN            : BFD1524C78510
HBA Model     : QLE2562
HBA Desc.     : QLE2562 PCI Express to 8Gb FC Dual Channel
FW Version    : 8.01.02
```

```
WWPN          : 21-00-00-24-FF-8D-98-E0
WWNN          : 20-00-00-24-FF-8D-98-E0
Link          : Online
=====================================================

    1:  Display HBA Parameters
    2:  Configure HBA Parameters
    3:  Restore Defaults


        (p or 0: Previous Menu; m or 98: Main Menu; x or 99: Quit)
        Please Enter Selection: 1
-------------------------------------------------------------------------
--------
HBA Instance 2: QLE2562 Port 1 WWPN 21-00-00-24-FF-8D-98-E0 PortID 03-
07-00
Link: Online
-------------------------------------------------------------------------
--------
Connection Options             : 2 - Loop Preferred, Otherwise Point-to-
Point
Data Rate                      : Auto
Frame Size                     : 2048
Hard Loop ID                   : 0
Loop Reset Delay (seconds)     : 5
Enable Host HBA BIOS           : Enabled
Enable Hard Loop ID            : Disabled
Enable FC Tape Support         : Enabled
Operation Mode                 : 0 - Interrupt for every I/O completion
Interrupt Delay Timer (100us)  : 0
**Execution Throttle             : 65535**
Login Retry Count              : 8
Port Down Retry Count          : 30
Enable LIP Full Login          : Enabled
Link Down Timeout (seconds)    : 30
Enable Target Reset            : Enabled
LUNs Per Target                : 128
Out Of Order Frame Assembly    : Disabled
Enable LR Ext. Credits         : Disabled
Enable Fabric Assigned WWN     : N/A

Press <Enter> to continue:
```

a. Enter * を押して続行します。

b. [HBA Parameters]メニューから、HBAパラメータを変更するオプションを選択します `Configure HBA Parameters`。

c. [Configure Parameters]メニューからオプションを選択し `Execute Throttle`、このパラメータの値を更新します。

```
Configure Parameters Menu

=======================================================
HBA           : 2 Port: 1
SN            : BFD1524C78510
HBA Model     : QLE2562
HBA Desc.     : QLE2562 PCI Express to 8Gb FC Dual Channel
FW Version    : 8.01.02
WWPN          : 21-00-00-24-FF-8D-98-E0
WWNN          : 20-00-00-24-FF-8D-98-E0
Link          : Online
=======================================================

    1:  Connection Options
    2:  Data Rate
    3:  Frame Size
    4:  Enable HBA Hard Loop ID
    5:  Hard Loop ID
    6:  Loop Reset Delay (seconds)
    7:  Enable BIOS
    8:  Enable Fibre Channel Tape Support
    9:  Operation Mode
   10:  Interrupt Delay Timer (100 microseconds)
   11:  Execution Throttle
   12:  Login Retry Count
   13:  Port Down Retry Count
   14:  Enable LIP Full Login
   15:  Link Down Timeout (seconds)
   16:  Enable Target Reset
   17:  LUNs per Target
   18:  Enable Receive Out Of Order Frame
   19:  Enable LR Ext. Credits
   20:  Commit Changes
   21:  Abort Changes


        (p or 0: Previous Menu; m or 98: Main Menu; x or 99: Quit)
        Please Enter Selection: 11
Enter Execution Throttle [1-65535] [65535]: 65500
```

d. Enter * を押して続行します。

e. [Configure Parameters]メニューから、変更を保存するオプションを選択し `Commit Changes`ます。

f. メニューを終了します。

## 著作権に関する情報



## 商標に関する情報