SANストレージの管理

ONTAP 9

NetApp
February 12, 2026

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環境においては、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では、ストレージ ターゲット デバイスをLUN（論理ユニット）と呼びます。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、NVMeの場合はネームスペースを作成することでストレージを構成します。それらのLUNまたはネームスペースに、ホストからInternet Small Computer System Interface（iSCSI）またはFibre Channel（FC）プロトコル ネットワーク経由でアクセスします。

iSCSIネットワークに接続するために、ホストで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TOEカード、CNA、または専用のiSCSI HBAを使用します。

FCネットワークに接続する場合、ホストでは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に統合されている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する。
- 複数のシステム インターフェイスを介して接続する。iSCSIに使用されるインターフェイスで、SMBやNFSなど、別のプロトコルのトラフィックも送信できます。
- ユニファイド ターゲット アダプタ（UTA）またはコンバージド ネットワーク アダプタ（CNA）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ノード名には、_iqn_と_eui_という2つの形式（タイプ指定子）があります。SVM iSCSI targetは常にiqnタイプ指定子を使用します。イニシエータはiqnタイプまたはeuiタイプ指定子のいずれかを使用できます。

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から成るデフォルトのノード名が付いています。

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です。

```
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が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、その他のアプリケーションやサーバ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サービス管理

iSCSIサービス管理

`vserver iscsi interface enable`または `vserver iscsi interface disable`コマンドを使用して、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できます。

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

ホストでiSCSIを実装する方法

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 ホスト バス アダプタ（HBA）経由：iSCSI HBA は、ホスト オペレーティング システムに対して、ローカル ディスクを持つ SCSI ディスク アダプタとして表示されます。
- TCP / IP処理をオフロードするTCPオフロード エンジン（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セッションの第一段階では、イニシエータはストレージ 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 システムでは、このログイン要求を許可または拒否するか、またはログインが不要であると判断します。

iSCSI認証方法は次のとおりです。

- Challenge Handshake Authentication Protocol（CHAP） - イニシエータはCHAPユーザ名および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、または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ーを認証します。

    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：これは、イニシエーターがストレージ システムを認証できるようにするための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限って、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に対する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。この一覧にないイニシエータに適用するデフォルトの認証方法も定義できます。

関連情報

"Data ONTAPを使用したWindowsマルチパス オプション：Fibre Channelと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提供します。iSCSIイニシエータのリストとそれぞれの認証方式を定義したり、認証リストにイニシエータとそれに関連付けられた認証方式を表示したり、認証リストにイニシエータを追加または削除したり、リストにないイニシエータのデフォルトのiSCSIイニシエータ認証方式を定義したりできます。

iSCSIエンドポイントの分離

既存の iSCSI セキュリティ コマンドは、IP アドレス範囲または複数の IP アドレスを受け入れることができます。

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ときに、発信元IPアドレスを提供する必要があります。これは、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をログインできないようにするための、新しい独自の識別機能です。サポート対象外または不明なIPアドレスを発信したイニシエータは、iSCSIセッション レイヤでログインが拒否されるため、クラスタ内のLUNやボリュームにアクセスできません。

この新しい機能では、2つの新しいコマンドを使用して既存のエントリを管理します。

イニシエータのアドレス範囲を追加する

`vserver iscsi security add-initiator-address-range`コマンドを使用して IPアドレス範囲または複数のIPアドレスを追加することで、iSCSIイニシエータのセキュリティ管理を改善します。

```
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

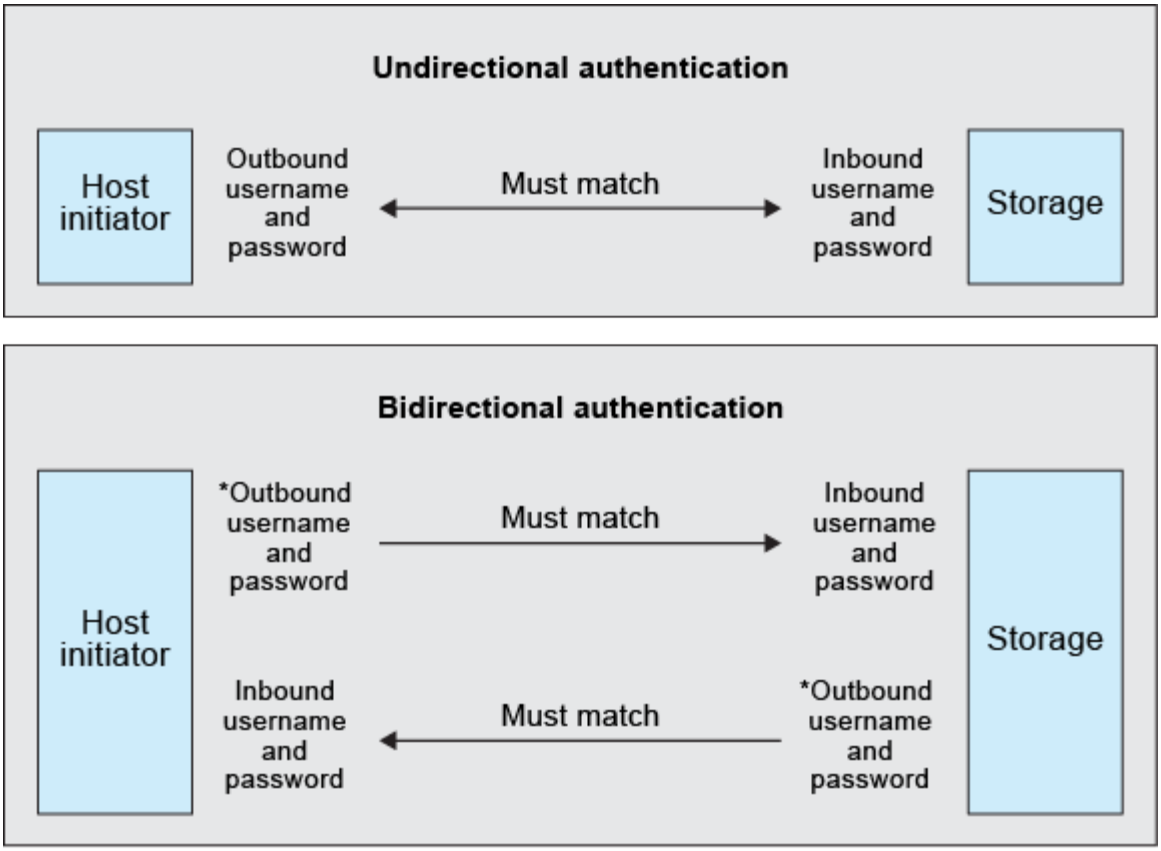
`vserver iscsi security remove-initiator-address-range`コマンドを使用して、IPアドレス範囲または複数のIPアドレスを削除します。

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

ONTAPの**iSCSI**イニシエータの**CHAP**認証について説明します

Challenge Handshake Authentication Protocol（CHAP）は、iSCSIイニシエータとターゲットの間で認証に基づいた通信を可能にします。CHAP認証を使用する場合、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セッションの第一段階では、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ています。これに対し、ストレージ システムはCHAPチャレンジで応答します。CHAP応答はイニシエータが提供します。ストレージ システムはCHAP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。



認証	アウトバウンド	インバウンド	一致？
一方向	ホストイニシエーターのユーザー名とパスワード	ストレージのユーザー名とパスワード	一致する必要があります
双方向	ホストイニシエーターのユーザー名とパスワード	ストレージのユーザー名とパスワード	一致する必要があります
双方向	ストレージのユーザー名とパスワード	ホストイニシエーターのユーザー名とパスワード	一致する必要があります

ホスト イニシエーターのアウトバウンド ユーザー名とパスワードは、ストレージ システムのアウトバウンド ユーザー名とパスワードとは異なる必要があります。

CHAP認証を使用する場合のガイドライン

CHAP 認証を使用する場合は、次のガイドラインに従ってください。

- インバウンド ユーザ名とパスワードをストレージ システムで定義している場合は、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可能にしている場合は、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ユーザ名は1～128バイトで指定できます。

  システムでは null ユーザー名は許可されません。

- CHAPパスワード（シークレット）は1～512バイトで指定できます。

  パスワードは16進数値または文字列で入力できます。16進数値の場合は、先頭に「0x」または「0X」を付けて入力してください。

  システムでは null パスワードは許可されません。

> 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、スペースを使用できます。ただし、ホストでの制限の対象にはなります。これらの文字が許可されていないホストでは、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に、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を使用するかどうかにかかわらず16バイトです。
>
> 追加の制限については、イニシエータのドキュメントを参照してください。

イニシエータのインターフェイスを制限する**iSCSI**インターフェイス アクセス リストの使用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の数を制限できるため、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 `SendTargets`コマンドを使用して検出セッションを開始すると、アクセスリストに登録されているLIF（ネットワークインターフェイス）に関連付けられたIPアドレスを受け取ります。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ことで、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。

ONTAPの**Internet Storage Name Service**（**iSNS**）

iSNSは、TCP / IPストレージ ネットワークでiSCSIデバイスを自動的に検出して管理できるプロトコルです。iSNSサーバでは、ネットワークでアクティブな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、使用するStorage Virtual Machine（SVM）がInternet Storage Name Service（iSNS）サーバに正しく登録されていることを確認してください。

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

iSNSサーバの機能

iSNSサーバではInternet Storage Name Service（iSNS）プロトコルが使用され、ネットワークでアクティブな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。

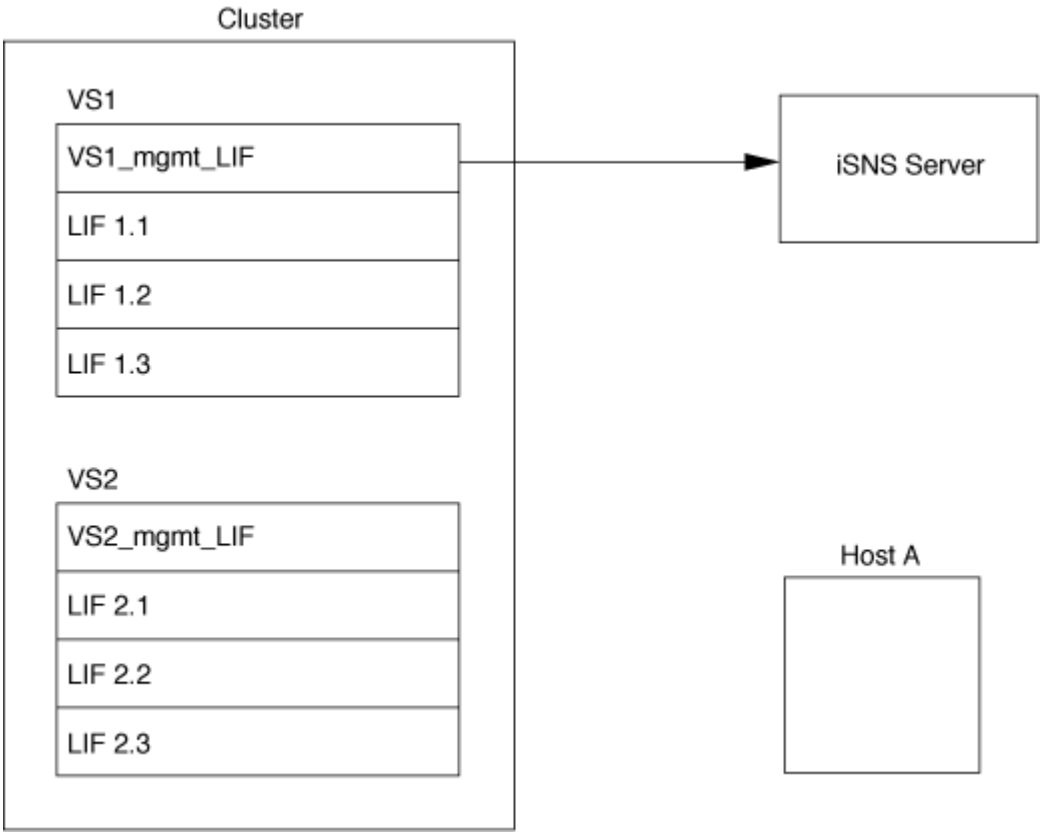
iSNSプロトコルを使用すると、IPストレージ ネットワークでiSCSIデバイスを自動的に検出し、管理できるようになります。iSCSIイニシエータが、iSNSサーバに照会することにより、iSCSIターゲット デバイスを検出します。

NetAppでは、iSNSサーバの提供や再販は行っていません。これらのサーバは、NetAppがサポートするベンダーから取得できます。

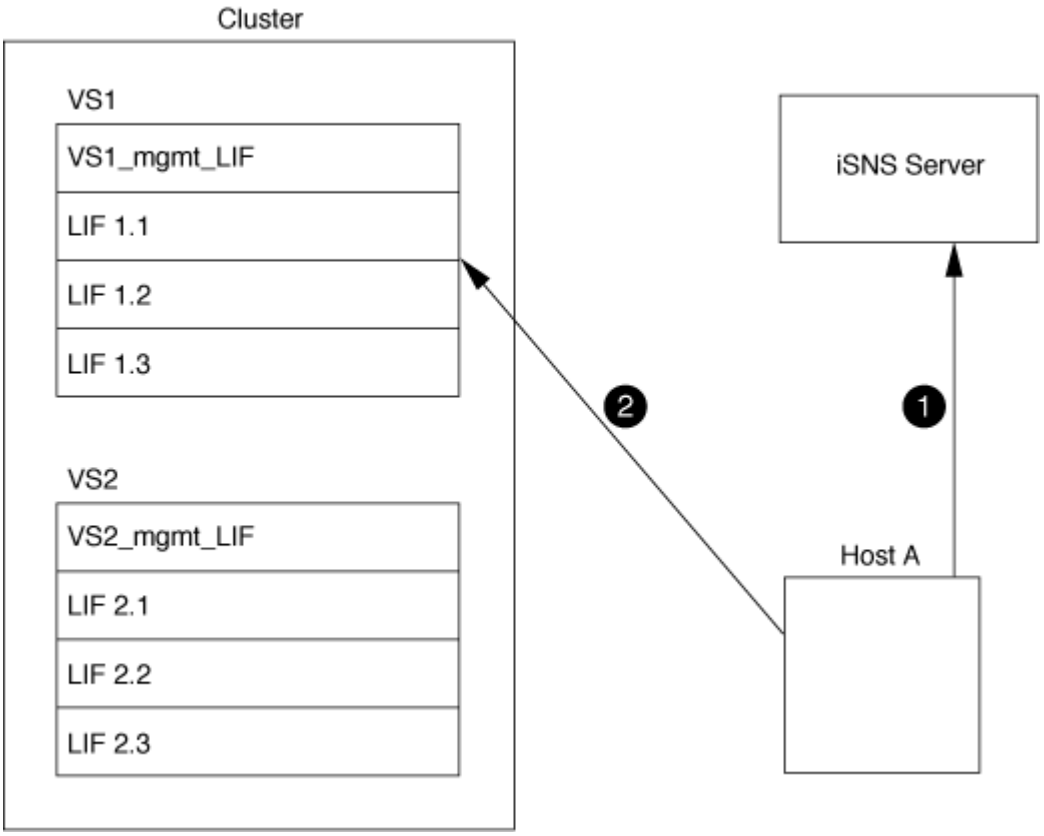
SVMとiSNSサーバの連動

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サーバに登録します。iSNS登録中、SVMはすべてのiSCSI LIFをSVM管理LIF経由でiSNSサーバに送信します。iSNS登録が完了すると、iSNSサーバは「vs1」でiSCSIサービスを提供しているすべてのLIFのリストを取得します。クラスタに複数のSVMが含まれている場合、iSNSサービスを利用するには、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サーバがターゲットへの登録を完了すると、ステップ1に示すように、ホストAはiSNSサーバを介して「vs1」のすべてのLIFを検出できます。ホストAが「vs1」のLIFの検出を完了すると、ステップ2に示すように、ホストAは「vs1」内の任意のLIFとの接続を確立できます。「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」内のどのLIFも認識しません。



ただし、インターフェイス アクセス リストを定義すると、ホストがターゲットへのアクセスに使用できるのは、インターフェイス アクセス リストに定義されたLIFのみとなります。

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。

設定変更を行ってからONTAPがiSNSサーバに更新を送信するまでの間に、数分間の遅延が発生する場合があります。iSNSサーバ上のiSNS情報を強制的に即時更新するには、次の手順を実行します： `vserver iscsi isns update`。詳細については、"ONTAPコマンド リファレンス"の `vserver iscsi isns update`を参照してください。

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サービスの設定を表示する	`vserver iscsi isns show`

登録済みのiSNS情報を強制的に更新する	`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`

`vserver iscsi isns`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+iscsi+isns["ONTAPコマンド リファレンス"^]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 システムとホストはいずれもアダプタを備えているので、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、スイッチのファブリック ネーム サービスに各SVMのLIFのWorld Wide Port Name（WWPN）が登録されます。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を使用したホストからノードへの直接接続はサポートされていません。接続にはNPIVが必要なため、スイッチを使用する必要があります。iSCSIセッションの場合、ネットワーク経由の接続または直接接続がサポートされます。ONTAPはこれら両方の方法をサポートしています。

FCノードの識別方法

FCを使用して設定された個々のSVMは、World Wide Node Name（WWNN）で識別されます。

WWPNの使用方法

WWPNは、FCをサポートするように設定されたSVM内の各LIFを識別します。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、またはUTA2）を使用します。

- イニシエータ グループの作成

  ホストのHBAのWWPNは、イニシエータ グループ（igroup）の作成に使用します。igroupは、特定LUNへのホスト アクセスの制御に使用します。igroupを作成するには、FCネットワーク内の一連のイニシエータのWWPNを指定します。ストレージ システムのLUNをigroupにマッピングすると、このグループ内のすべてのイニシエータに対し、このLUNへのアクセスを許可することができます。LUNにマッピングされて

いるigroupにWWPNが含まれていないホストは、そのLUNにアクセスできません。つまり、そのホストでは、そのLUNが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することで、特定のターゲット ポートに関してだけLUNを表示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。ポートセットにはigroupをバインドできます。このigroup内のすべてのホストは、ポートセット内のターゲット ポートからのみ各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。ホストのOSは、WWNNとWWPNを組み合わせて使用し、SVMおよびFC LIFを識別します。一部のOSでは、パーシスタント バインディングがないと、ホストにおいて同じターゲットIDでLUNが表示されません。

World Wide Name（WWN）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、WWNがシーケンシャルに割り当てられていないように見える場合があります。

各アダプタにはWWPNおよびWWNNがあらかじめ設定されていますが、ONTAPではあらかじめ設定された値が使用されません。その代わりに、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、固有のWWPNまたはWWNNを割り当てます。

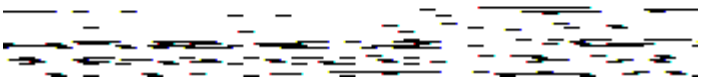
WWNが割り当て時にシーケンシャルでないように見える理由は次のとおりです。

- 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、利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、デバイスの各ポートに1つ、Worldwide Port Name（WWPN）が割り当てられています。

たとえば次の図では、16ポートのBrocadeスイッチの各ポートにWWPNが割り当てられています。特定のスイッチのポート番号のレイアウトについては、ベンダーが提供しているそのスイッチのドキュメント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

ONTAP 9.4以降では、SAN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することができます。

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および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と関連付けることができ、これにより関連付けられたイニシエータからサブシステム内のネームスペースにアクセスできるようになります。

> NVMeネームスペースは、機能的にはLUN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、NVMeを使用したホスト側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 9.4でNVMeが有効になっている場合、ONTAP 9.5へのアップグレード後、ライセンスを取得するための90日間の猶予期間が与えられます。"ONTAP One"をお持ちの場合は、NVMeライセンスも含まれています。ライセンスは次のコマンドで有効化できます：

```
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ボリューム

SANボリュームの概要

ONTAPでは、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つを提供しています。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、オプションごとに異なる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に配置することは推奨されません。SAN LUNとNAS共有それぞれに専用のFlexVolをプロビジョニングしてください。これにより、管理とレプリケーションの導入が簡素化され、Active IQ Unified Manager（旧OnCommand Unified Manager）でのFlexVolのサポート方法が統一されます。

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。

FlexVolボリュームの `-space-guarantee`オプションを `none`に設定して、シンプロビジョニング ボリューム

を作成します。

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ボリュームを作成するには、 `-space-slo`（サービス レベル目標）オプションを `thick`に設定します。

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使用するボリュームが作成されると、ONTAPはボリュームサイズに合わせてアグリゲートからストレージスペースを確保します。ブロック共有テクノロジによって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ている場合、ONTAPは保護データオブジェクト（スナップショット、FlexCloneファイル、LUN）を削除して、それらが保持しているスペースを解放しようとします。ONTAPが保護データオブジェクトを上書きに必要なスペースに追いつくだけの速度で削除できる限り、書き込み処理は継続して成功します。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ません：

- 重複排除、圧縮、コンパクションなどのストレージ効率化テクノロジ
- Microsoftオフロード データ転送（ODX）

FlexVolボリュームの `-space-slo`（サービス レベル目標）オプションを `semi-thick`に設定して、セミシック プロビジョニング ボリュームを作成します。

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

スペース予約ファイル（LUN）とは、作成時にストレージが割り当てられるファイルです。従来、NetAppでは、スペース リザベーションが無効になっているLUN（スペース予約されていないLUN）を指すために「シンプロビジョニングLUN」という用語が使用されてきました。

*注：*スペース予約されていないファイルは、通常、「`thin-provisioned`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**/ファイルのスペース 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	保証済み[1]	保証	サポート
シン	効果なし	なし	保証	サポート
セミシック	サポート	ベストエフォート[1]	ベスト エフォート	サポート対象外

注記

1. 上書きの保証またはベスト エフォートの上書き保証が行われるには、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、スナップショット、および自動削除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、自動削除の対象とマークされていないFlexCloneファイルとFlexClone 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に加え、NetAppシンプロビジョニングLUNもサポートしています。T10 SCSIシンプロビジョニングにより、ホスト アプリケーションはSCSI機能（ブロック環境でのLUNのスペース再生機能やスペース監視機能など）をサポートできるようになります。使用するSCSIホスト ソフトウェアも、T10 SCSIシンプロビジョニングをサポートしている必要があります。

ONTAP `space-allocation`設定を使用して、LUN上でT10シンプロビジョニングのサポートを有効化または無効化します。ONTAP `space-allocation enable`設定を使用して、LUN上でT10 SCSIシンプロビジョニングを有効にします。

"ONTAPコマンド リファレンス"の `[-space-allocation {enabled|disabled}]`コマンドには、T10 シン プロビジョニングのサポートを有効/無効にする方法と、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情報が含まれています。

ボリューム プロビジョニング オプションの設定

ボリュームを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用に設定できます。

タスク概要

`-space-slo`オプションを `thick`に設定すると、次のことが保証されます：

- ボリューム全体がアグリゲートに事前割り当てされています。 `volume create`コマンドまたは `volume modify`コマンドを使用して、ボリュームの `-space-guarantee`オプションを設定することはできません。
- 上書きに必要なスペースの100%が予約されています。 `volume modify`コマンドを使用してボリュームの `-fractional-reserve`オプションを設定することはできません。

`-space-slo`オプションを `semi-thick`に設定すると、次のことが保証されます：

- ボリューム全体がアグリゲートに事前割り当てされています。 `volume create`コマンドまたは `volume modify`コマンドを使用して、ボリュームの `-space-guarantee`オプションを設定することはできません。
- 上書き用のスペースは予約されていません。 `volume modify`コマンドを使用して、ボリュームの `-fractional-reserve`オプションを設定できます。
- Snapshotの自動削除が有効になっています。

手順

1. ボリューム 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
```

この `-space-guarantee`オプションは、AFFシステムおよび非AFF DPボリュームの場合はデフォルトで `none`になります。それ以外の場合は、デフォルトで `volume`になります。既存のFlexVolボリュームの場合は、 `volume modify`コマンドを使用してプロビジョニングオプションを設定してください。

次のコマンドは、SVM vs1のvol1をシンプロビジョニング用に設定します。

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

次のコマンドは、SVM vs1のvol1をシックプロビジョニング用に設定します。

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

次のコマンドは、SVM vs1のvol1をセミシックプロビジョニング用に設定します。

```
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が含まれているボリュームに対して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で使用可能な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、ボリュームのサイズを事前設定した最大サイズまでONTAP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。

ボリュームの自動拡張は、Snapshot作成をサポートするためにトリガーできません。Snapshotを作成しようとした際にボリュームに十分なスペースがない場合は、ボリュームの自動拡張が有効であっても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たスペースの量が事前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の自動削除は、次のいずれかの状況が発生すると、Snapshotを自動的に削除します。

- ボリュームがフルに近い状態の場合
- Snapshotリザーブ スペースがほぼいっぱいです。
- オーバーライト リザーブ スペースがフルの場合

スナップショットの自動削除を設定すると、古いものから新しいものへ、または新しいものから古いものの順にスナップショットを削除できます。スナップショットの自動削除では、クローンボリュームまたはLUN内のスナップショットにリンクされているスナップショットは削除されません。

ボリュームに追加のスペースが必要で、自動拡張とスナップショットの自動削除の両方を有効にしている場合、デフォルトでONTAPはまず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できない場合は、スナップショット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、ボリューム内でスナップショット用に予約される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は、他の目的には使用できません。Snapshotリザーブに割り当てられたスペースがすべて使用されると、スナップショットはボリューム上の追加の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前に、特定の要件を満たす必要があります。

- ボリュームにLUNが含まれている場合は、クラスタの各ノードに接続するパス（LIF）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。

- 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。

  ONTAP 9.5を実行するNVMe構成では、ボリューム移動はサポートされません。

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（_LUN オーバーライト リザーブ_とも呼ばれます）を使用すると、FlexVolボリューム内のスペース リザベーションされたLUNとファイルに対するオーバーライト リザーブを無効にすることができます。これによりストレージ使用率を最大化できますが、スペース不足による書き込み操作の失敗によって環境に悪影響が出る場合は、この構成に課される要件を理解する必要があります。

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ます。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 `0`に設定すると、ストレージ使用率が向上します。ただし、ボリュームギャランティを `volume`に設定していても、ボリューム内のデータにアクセスするアプリケーションで、ボリュームの空き容量が不足している場合、データ障害が発生する可能性があります。ただし、ボリュームを適切に設定し、使用することで、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。ONTAPは、フラクショナルリザーブを `0`に設定したボリュームに対して、以下の_すべて_の要件が満たされている場合に「ベストエフォート」の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サブファイルを使用していない
- 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
- ボリューム保証が `volume`に設定されています
- ファイルまたはLUNのスペース リザベーションは `enabled`
- ボリュームSnapshotリザーブは `0`に設定されています
- ボリュームスナップショットの自動削除は、 `enabled`コミットメントレベルが `destroy`、破棄リストが `lun_clone,vol_clone,cifs_share,file_clone,sfsr`、トリガーが `volume`で実行されます。

  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。

変更率が高い場合、上記の必要な構成設定をすべて使用していても、まれにSnapshotの自動削除が遅れてボリュームの容量が不足する可能性があることに注意してください。

さらに、ボリュームの自動拡張機能をオプションで使用して、ボリュームのスナップショットを自動的に削除する必要が生じ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容量を監視する必要があります。アグリゲートがいっぱいになり、ボリュームの拡張ができなくなると、ボリュームの空き容量が枯渇するにつれて、より多くのスナップショットが削除される可能性があります。

上記の構成要件をすべて満たすことができず、ボリュームの容量不足を回避する必要がある場合は、ボリュームのフラクショナルリザーブ設定を `100`に設定する必要があります。これにより、事前により多くの空き容量が必要になりますが、上記のテクノロジが使用されている場合でもデータ変更操作が成功することが保証されます。

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	デフォルトの部分リザーブ	有効な値
Volume	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において、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 システム側で管理するプロセスを担っているのがホスト側のスペース管理です。

ホスト ファイルシステムでは、新しいデータの格納に利用できるブロックはどれか、また、有効なデータを含んでいるため上書きしてはならないブロックはどれかを追跡するための情報がメタデータに記録されます。このメタデータはLUNかネームスペースに格納されています。ホスト ファイルシステム内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、削除された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 システム間に分散できるストレージ プールから仮想ディスクを簡単に作成し、ストレージ プロビジョニング タスクを自動化して、ホスト データと一致するスナップショットからスナップショットとクローンを作成するプロセスを簡素化できます。

NetApp製品ドキュメントで "SnapCenter"の詳細を参照してください。

関連リンク

"SANプロトコルのONTAPスペース割り当ての有効化"

igroupについて

initiator group（igroup;イニシエータ グループ）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にマッピングし、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 イニシエータがすべてLUNにアクセスできることが必要とされます。マルチパス ソフトウェアを使用しているか、またはクラスタ ホストがある場合、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 イニシエータは同じ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の作成前後どちらでも作成できますが、LUNをigroupにマッピングするためにはigroupを作成しておく必要があります。

igroup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、同じイニシエータを持つ複数の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、ホストで利用できるLUNを定義することができます。たとえば、ホスト クラスタを使用している場合は、いくつかの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に特定の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する4つのホストを、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およびHost4）は、どちらも同じigroup（group3）のメンバーであり、このigroupにマッピングされている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な情報が格納されます。

HBA WWPN、**IQN**、または**EUI**を持つホスト	**igroup**	**igroup**に追加された**WWPN**、**IQN**、**EUI**	**igroup**にマッピングされた**LUN**
Host1、シングルパス（iSCSIソフトウェア イニシエータ） iqn.1991-05.com.microsoft:host1	グループ1	iqn.1991-05.com.microsoft:host1	`/vol/vol2/lun1`
Host2、マルチパス（HBA 2個） 10:00:00:00:c9:2b:6b:3c 10:00:00:00:c9:2b:02:3c	group2	10:00:00:00:c9:2b:6b:3c 10:00:00:00:c9:2b:02:3c	`/vol/vol2/lun2`
Host3、マルチパス、Host4でクラスタ構成 10:00:00:00:c9:2b:32:1b 10:00:00:00:c9:2b:41:02	group3	10:00:00:00:c9:2b:32:1b 10:00:00:00:c9:2b:41:02 10:00:00:00:c9:2b:51:2c 10:00:00:00:c9:2b:47:a2	`/vol/vol2/qtree1/lun3`

HBA WWPN、IQN、またはEUIを持つホスト	igroup	igroupに追加されたWWPN、IQN、EUI	igroupにマッピングされたLUN
Host4、マルチパス、クラスタ構成（Host3には認識されない） 10:00:00:00:c9:2b:51:2c 10:00:00:00:c9:2b:47:a2	group4	10:00:00:00:c9:2b:51:2c 10:00:00:00:c9:2b:47:a2	`/vol/vol2/qtree2/lun4` `/vol/vol2/qtree1/lun5`

igroupのイニシエータのWWPNとiSCSIノード名の指定

igroupの作成時に、イニシエータのiSCSIノード名とWWPNを指定できます。それらをあとから指定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、必要に応じてそれらをあとから削除できます。

Host Utilitiesのマニュアルに記載されている手順に従って、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しているホストでは、Virtual Storage Consoleを使用します。

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を使用することで、SVMのアクティブなiSCSI LIFまたはFC LIFから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するLIFを制限できます。

ESXホストのVMware VAAIパフォーマンスの向上

ONTAPは、ESXホストがESX 4.1以降を実行している場合、特定のVMware vStorage APIs for Array Integration（VAAI）機能をサポートします。これらの機能は、ESXホストからストレージ システムへの処理のオフロードとネットワーク スループットの向上に役立ちます。ESXホストは、適切な環境でこれらの機能を自動的に有効化します。

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に関与することなく、LUN間またはLUN内でのデータ転送を開始できます。これにより、ESXのCPUサイクルが節約され、ネットワークスループットが向上します。拡張コピー機能（「コピー オフロード」とも呼ばれます）は、仮想マシンのクローン作成などのシナリオで使用されます。ESXホストによって呼び出されると、コピー オフロード機能は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をコピーします。コピー オフロードは、以下の方法でデータを転送します：

  - LUN内
  - ボリューム内のLUN間
  - ストレージ仮想マシン（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は、ESXホストはコピー操作に標準のREADコマンドとWRITEコマンドを自動的に使用します。

- `WRITE_SAME`

  この機能は、すべてゼロなどの繰り返しパターンをストレージ アレイに書き込む作業をオフロードします。ESXホストは、ファイルのゼロフィルなどの操作でこの機能を使用します。

- `COMPARE_AND_WRITE`

  この機能は、特定のファイル アクセスの同時実行制限をバイパスし、仮想マシンの起動などの操作を高速化します。

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、適切な環境を設定するとESXホストによって自動的に呼び出されます。

環境要件は次のとおりです：

- ESXホストはESX 4.1以降を実行し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を実行する。
- （コピー オフロードのみ）VMware コピー操作のソースと宛先は、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必要があります。

> コピー オフロード機能は現在、異なるストレージ システムでホストされているVMwareデータストア間でのデータのコピーをサポートしていません。

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 システムが VAAI 機能をサポートしているかどうかを確認するには、vSphere Client を確認するか、ホストにアクセスする他の手段を使用します。ONTAP はデフォルトで SCSI コマンドをサポートしています。

ESXホスト詳細設定を確認することで、VAAI機能が有効になっているかどうかを確認できます。表は、ESX制御名に対応するSCSIコマンドを示しています。

SCSIコマンド	ESXコントロール名（VAAI機能）
EXTENDED_COPY	`HardwareAcceleratedMove`
WRITE_SAME	`HardwareAcceleratedInit`
COMPARE_AND_WRITE	`HardwareAcceleratedLocking`

SANコピー オフロード

Microsoftオフロード データ転送（ODX）

Microsoft Offloaded Data Transfer（ODX）は、*copy offload* とも呼ばれ、ホスト コンピューター経由でデータを転送せずに、ストレージ デバイス内または互換性のあるストレージ デバイス間で直接データを転送することを可能にします。

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ためには、VMwareとWindowsそれぞれ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構成する必要があります。

VMwareとMicrosoftのコピー オフロードを仮想環境で使用する場合は、LUNをアライメントする必要があります。LUNがアライメントされていないと、パフォーマンスが低下する可能性があります。"非整列LUNの詳細"。

ONTAPでは、SMBプロトコルとSANプロトコルの両方でODXをサポートしています。

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、コピーが同じボリューム内で行われるとパフォーマンスが大幅に向上します。実現するパフォーマンスの向上には、同じボリュームで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またがってコピーを実行する場合は、ホストベースのコピーの場合ほど大幅にはパフォーマンスが向上しない可能性があります。

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がサポートされていて有効になっているクライアント コンピュータでは、ファイルの移動やコピーを行う際に、オフロード 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について理解しておく必要があります。

ODXを使用するためのシステム要件は次のとおりです。

- 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。

- ソース ボリュームの最小サイズ：2GB

  最適なパフォーマンスを確保するには、260GB以上のソース ボリュームが必要です。

- 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。サポート対象の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がODXをサポートする必要があります。ODXがサポートされるアプリケーション処理は次のとおりです。

  - 仮想ハードディスク（VHD）の作成と変換、スナップショットの管理、仮想マシン間のファイルのコピーなどのHyper-V管理操作
  - エクスプローラ操作
  - Windows PowerShellコピーコマンド
  - Windows コマンド プロンプトのコピー コマンド Microsoft TechNet ライブラリには、Windows サーバーおよびクライアントでサポートされている ODX アプリケーションに関する詳細情報が含まれています。

- 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を次のタイプのボリュームで使用することはできません。

- 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ボリューム"

  ODXはFlexCacheの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 ファイルの要件

qtree内のODXファイルは削除できます。テクニカルサポートから指示がない限り、その他の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機能を使用する場合、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。これらのファイルにより、ODX転送中に使用されるデータのポイントインタイム表現が可能になります。以下のシステムファイルは、データがオフロードされた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`（隠しディレクトリ）
- `.tokens`（非表示の `.copy-offload`ディレクトリ下のファイル）

> `copy-offload delete-tokens -path dir_path -node _node_name_`コマンドを使用して、ODXファイルを含むqtreeを削除できます。

ODXの使用事例

SVMでODXを使用する前にユースケースについて確認し、どのような場合にパフォーマンスが向上するかを判断できるように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際に、デフォルトでコピー オフロードが使用されます。WindowsサーバおよびクライアントでODXがサポートされていない場合や、ODXコピー オフロードが任意の時点で失敗した場合は、コピーまたは移動処理が従来の読み取りと書き込みの処理を使用して実行されます。

ODXコピーおよび移動の使用は、以下の事例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。データは異なる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。データは異なるSVMに所有されます。

- クラスタ間

  ソースとデスティネーションのLUNは、異なるクラスタの異なるノード上の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。

さらに、いくつかの特殊なユースケースがあります。

- ONTAPのODXの実装では、ODXを使用してSMB共有とFC / iSCSI接続の仮想ドライブと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、さらに次のようなユースケースでもODXコピー オフロードが使用されます。

  - Hyper-VでODXコピー オフロードのパススルーを使用して、仮想ハード ディスク（VHD）ファイル内およびVHDファイル間でのデータのコピー、または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の間でのデータのコピーを実行できます。

    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を作成する際に、ODXを使用して、既知の初期化済みトークンによっ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に、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用途を活用するには、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 システムのディスクがIDEディスクの場合、ODXのパススルーはサポートされません。

NVMeコピー オフロードについて

NVMeコピー オフロードにより、NVMeホストはコピー処理をホストCPUからONTAPストレージ コントローラのCPUにオフロードできます。ホストは、CPUリソースをアプリケーション ワークロード用に確保しながら、あるNVMeネームスペースから別のNVMeネームスペースにデータをコピーできます。

例えば、パフォーマンス分散を改善するためにストレージワークロードの再バランス調整が必要だとします。これには、平均サイズがそれぞれ500 GBのNVMeネームスペースを45個含む10台の仮想マシン（VM）を移行する必要があります。つまり、約22.5 TBのデータをコピーする必要があるということです。ホストは、データ移行に自身のCPUを使用する代わりに、NVMeコピー オフロードで、データのコピー中にアプリケーションワークロード用のCPUリソースが減少することを防ぐことができます。

NVMeコピー オフロードのサポートと制限事項

NVMeコピー オフロードはONTAP 9.18.1以降でサポートされます。ONTAPはNVMeコピー オフロードを開始できません。ホストによってサポートされ、開始される必要があります。

ONTAPを使用したNVMeコピー オフロード処理には、次の制限事項があります：

- サポートされるコピー操作の最大サイズは16MBです。
- データは同じサブシステム内のNVMe名前空間間でのみ移行できます。
- データは同じ HA ペア内のノード間でのみ移行できます。

SAN管理

SANプロビジョニング

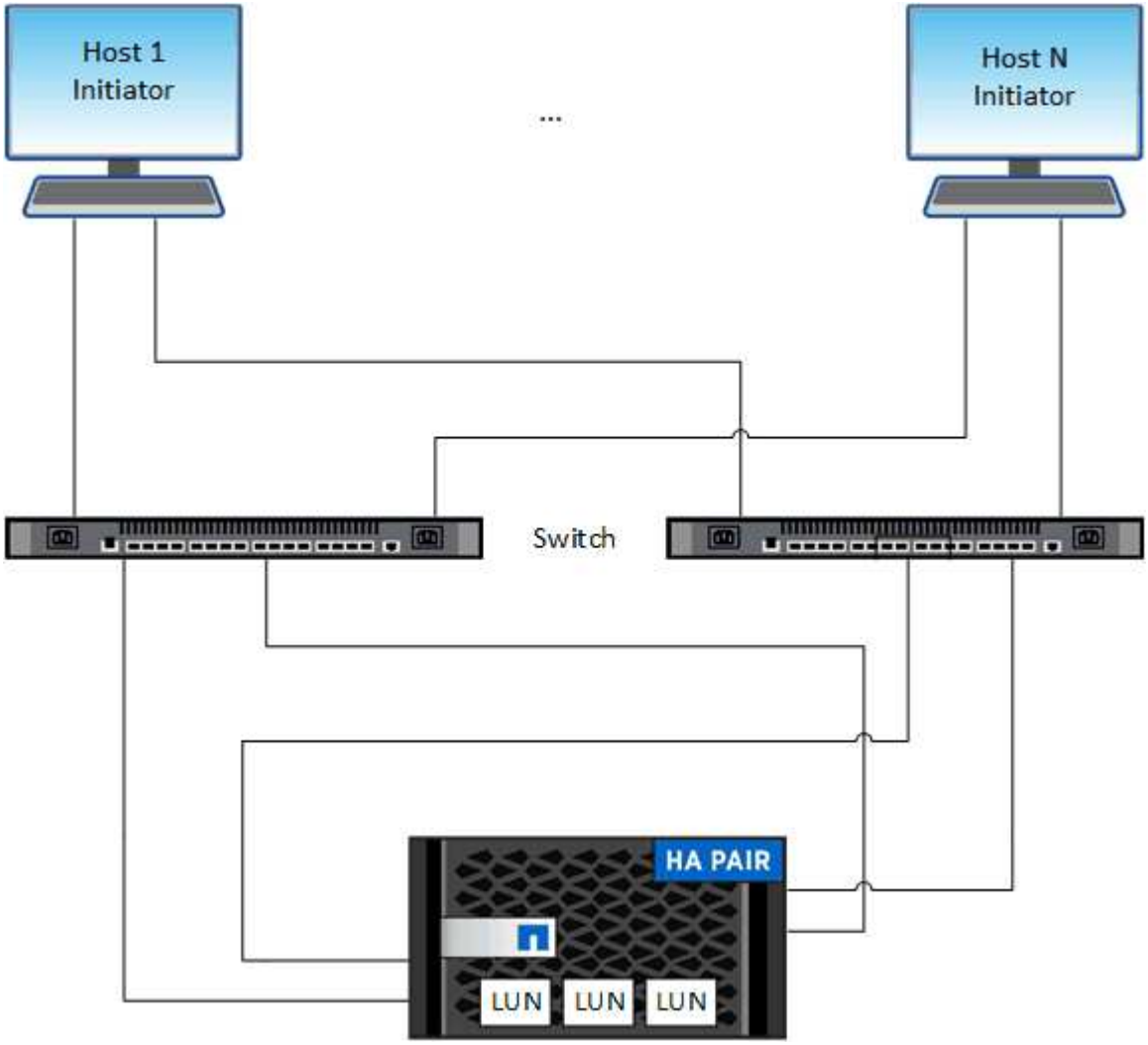
SANの管理 - 概要

このセクションでは、ONTAP 9.7以降のリリースで、ONTAPのコマンドライン インターフェイス（CLI）およびSystem Managerを使用してSAN環境を設定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のストレージ ターゲットはLUN（論理ユニット）と呼び、ホストからは標準のブロック デバイスとして認識されます。作成したLUNはイニシエータ 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WWPとiSCSIホスト ノード名のテーブルで、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、ワールドワイド ポート名（WWPN）によって識別されます。iSCSIターゲットは、標準イーサネット ネットワーク アダプタ（NIC）、ソフトウェア イニシエーターを備えた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修飾名（IQN）によって識別されます。

詳細情報

ASA r2ストレージ システム（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、またはASA A20）をお持ちの場合は、"ASA r2ストレージ システムのドキュメント"を参照してください。

オールフラッシュ**SAN**アレイ構成について学ぶ

NetAppオールフラッシュSANアレイ（ASA）は、ONTAP 9.7以降で使用できます。ASAは、実績のあるNetApp AFFプラットフォーム上に構築されたオールフラッシュのSANオンリー ソリューションです。

ASAプラットフォームには次のものがあります：

- ASA A150
- ASA A250
- ASA A400
- ASA A800
- ASA A900
- ASA C250
- ASA C400
- ASA C800

ONTAP 9.16.0以降、SANのみをご利用のお客様向けに、簡素化されたONTAPエクスペリエンスがASA r2システム（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、またはASA A20）で利用可能になりました。ASA r2システムをご利用の場合は、"ASA r2 システムドキュメント"をご覧ください。

ASAプラットフォームでは、マルチパスにシンメトリック アクティブ / アクティブを使用します。すべてのパスがアクティブで最適化されているため、ストレージ フェイルオーバーの際、ホストはALUAによるフェイルオーバー パスの移行を待つことなくI/Oを再開できます。そのためフェイルオーバーにかかる時間が短縮されます。

ASAのセットアップ

オールフラッシュSANアレイ（ASA）のセットアップ手順はASA以外のシステムと同じです。

System Managerでは、画面の指示に従って、ASAを対象としたクラスタの初期化、ローカル階層の作成、プロトコルの設定、およびストレージのプロビジョニングに必要な手順を実行できます。

ONTAPクラスタのセットアップの開始。

ASAのホスト設定とユーティリティ

オールフラッシュSANアレイ（ASA）をセットアップするためのホスト設定は、他のすべてのSANホストと同じです。

サポート サイトから特定のホスト用の"NetAppホストユーティリティソフトウェア"をダウンロードできます。

ASAシステムの特定方法

ASAシステムは、System ManagerまたはONTAPコマンドライン インターフェイス（CLI）を使用して特定できます。

- **System Manager**ダッシュボードから：*クラスター > 概要*をクリックし、システム ノードを選択します。

  PERSONALITY は **All-Flash SAN Array** として表示されます。

- **CLI**から： `san config show`コマンドを入力します。

  ASAシステムに対しては「All-Flash SAN Array」の値がtrueと表示されます。

  `san config show`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/san-config-show.html["ONTAPコマンド リファレンス"^]を参照してください。

関連情報

- "テクニカルレポート4968：NetApp All-SANアレイのデータ可用性と整合性"
- "NetAppテクニカルレポート4080：最新SANのベストプラクティス"

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。

開始する前に

- 使用するSAN構成がサポートされている必要があります。

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

- ユニファイド ターゲット アダプタ（UTA）をストレージ システムに取り付ける必要があります。

  UTA2 を使用している場合は、 `cna` モードに設定する必要があります。

- コンバージド ネットワーク アダプタ（CNA）をホストに取り付ける必要があります。

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設定が正しく行われていることを確認します。

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

DCB設定はスイッチに対して行われます。設定が正しくない場合は、スイッチのドキュメント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 `true`の場合、FCoE ログインが機能していることを確認します。

```
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 `false`の場合は、スイッチのドキュメント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）エンドツーエンド導入ガイド"
- "Cisco MDS 9000 NX-OSおよびSAN-OSソフトウェアの構成ガイド"
- "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、システムが特定の前提条件を満たしている必要があります。

- Interoperability Matrixにサポート対象として掲載されているSAN構成を使用する。
- SAN 環境は、ONTAPソフトウェアのバージョンに対して "NetApp Hardware Universe"で指定されているSANホストおよびコントローラの構成制限を満たしている必要があります。
- 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。

  詳細については、Host Utilitiesのドキュメント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がある。

関連情報

- "NetApp Interoperability Matrix Tool"
- "ONTAP SAN Host Configuration"
- "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

クラスタで LUN のセットアップを開始する前に、これらの LUN ガイドラインを確認する必要があります。

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。
- 最大サイズでLUNを作成する場合、LUNの実際のサイズは少し小さくなる可能性があります。ONTAPは端数を切り捨てるため、少し小さくなります。
- 各LUNのメタデータ用として、LUNを含むアグリゲートに約64KBのスペースが必要です。LUNの作成時には、LUNを含むアグリゲートにLUNのメタデータ用のスペースが十分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

一般的にデフォルトのLUN IDは0で始まり、LUNをマッピングするたびに1ずつ増加します。LUN IDは、ホストによってLUNの場所とパス名に対応付けられます。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、LUNは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。
- 同じイニシエータを複数のigroupに追加できますが、その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にマッピングされている2つのLUNに、同じLUN IDを使用することはできません。
- igroupおよびポートセットで同じ種類のプロトコルを使用する必要があります。

FCまたはiSCSIプロトコルのライセンスの確認と追加

FCまたはiSCSIを使用した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およびiSCSIのライセンスは"ONTAP One"に含まれています。

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. ライセンスがリストされていない場合は、+ Add を選択してライセンス 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で、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>
```

SANストレージのプロビジョニング

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

タスク概要

この手順は、FAS、AFF、およびASAシステムに適用されます。ASA r2システム（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、ASA A20、またはASA C30）をご利用の場合は、"これらの手順"に従ってストレージをプロビジョニングしてください。ASA r2システムは、SANのみをご利用のお客様向けに、簡素化されたONTAPエクスペリエンスを提供します。

新しいストレージ VM を作成し、FC または iSCSI プロトコルを構成する必要がある場合は、"FC用のSVMの設定"または"iSCSI用のSVMの設定"を参照してください。

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、QoSはストレージのプロビジョニング時にデフォルトで有効になります。プロビジョニング時またはあとでQoSを無効にしたり、カスタムのQoSポリシーを選択したりすることができます。

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完了するには、 "Red Hat Enterprise Linux向けのiSCSIの設定"を参照してください。

手順

1. ホストに適切な"SAN ホスト ユーティリティ"をインストールします。
2. System Managerで、*ストレージ > LUN*をクリックし、*追加*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*をクリックして次のいずれかを実行できます。

オプション	追加されたリリース
• 親ボリュームではなくLUNにQoSポリシーを割り当てる ◦ その他のオプション > ストレージと最適化 ◦ *Performance Service Level*を選択します。 ◦ 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の適用を各LUNに適用する*を選択します。 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 グループを作成する ◦ その他のオプション＞ホスト情報 ◦ *既存のイニシエータグループを使用した新しいイニシエータグループ*を選択します。 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 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なります。 ◦ 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 デフォルトでは、新しいLUNは新しいボリュームに作成されます。 ◦ その他のオプション **>** **LUN**の追加 ◦ 関連する **LUN** をグループ化 を選択します。	ONTAP 9.9.1
• QoSを無効にするか、カスタムのQoSポリシーを選択する ◦ その他のオプション **>** ストレージと最適化 ◦ *Performance Service Level*を選択します。 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 ポートを配置します。
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サーバ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、 `license add` コマンドを使用します。

```
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>
   ```

   データを提供する各SVMで、ノードごとにiSCSIまたはFC LIFが少なくとも1つ必要です。ただし、冗長性を確保するためにはノードごとにLIFが2つ必要です。iSCSIでは、ノードごとに少なくとも2つのLIFを別々のイーサネット ネットワークに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 `online`であることを確認します：

   ```
   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文字以内で指定し、スペースは使用できません。

   NVFAILオプションは、ボリュームで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. オプションで、"ポートセットを作成し、igroupにバインドする"。
11. ホストのマニュアルに記載されている手順に従って、特定のホストでブロック アクセスを有効にします。
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 - 概要"
- "ONTAP SAN Host Configuration"
- "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化する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 デバイスとして表示されます。FCや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て、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、標準のFCインフラ（FCスイッチを使用）またはTCPインフラ（イーサネット スイッチとホスト側アダプタを使用）を介し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。詳細については、"NVMeのサポートと制限"を参照してください。

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以外の接続経由によるNVMeベースの通信を実現します。このインターフェイスを使用すると、外部のストレージ エンクロージャをサーバに接続できます。

NVMeは、不揮発性メモリ（フラッシュ テクノロジ、高パフォーマンスの永続的メモリ テクノロジなど）を搭載したストレージ デバイスへの効率的なアクセスを提供するように設計されています。そのため、ハード ディスク ドライブ向けに設計されたストレージ プロトコルのような制限はありません。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では停電時にもデータが失われません。NVMeはこのメモリにアクセスするための手段です。

NVMeのメリットとしては、データ転送速度、生産性、スループット、容量の向上が挙げられます。NVMeの特徴は次のとおりです。

- 最大64,000個のキューを使用できるように設計されています。

  各キューには最大64,000個のコマンドを保持できます。

- NVMeは、複数のハードウェアおよびソフトウェア ベンダーでサポートされています。
- フラッシュ テクノロジを使用するとNVMeの生産性がさらに向上し、応答時間が短縮されます。
- NVMe では、SSD に送信される各「`request`」に対して複数のデータ リクエストが可能です。

  NVMeでは、「`request`」のデコードにかかる時間が短縮され、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ます。各ネームスペースが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、Solid State Drive（SSD;ソリッド ステート ドライブ）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、そのままでファイルシステムとアプリケーションを導入できます。

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 グループに対して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ます。同じホスト グループに複数のNSIDが割り当てられることはありません。

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。オプションで、新規または既存のサブシステムにマッピングできます。

関連情報

- ASA、AFF、FASシステムで"NVMeストレージをプロビジョニングする"する方法を学ぶ
- ASA AFFおよびFASシステムで"NVMe名前空間をサブシステムにマッピングする"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する"
- ASA r2（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、またはASA A20）ストレージ システムで"SANストレージのプロビジョニング"する方法を学習します。

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。NVMeが有効なONTAP 9.4をONTAP 9.5にアップグレードした場合、90日間の猶予期間中にライセンスを取得する必要があります。

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
```

NVMeの構成、サポート、制限事項

ONTAP 9.4以降、"不揮発性メモリエクスプレス（NVMe）"プロトコルはSAN環境で利用可能になりました。FC-NVMeは、従来のFCネットワークと同じ物理構成とゾーニング手法を採用していますが、FC-SCSIよりも広い帯域幅、高いIOPS、低いレイテンシを実現します。

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、および構成によって異なります。特定の構成の詳細については、"NetApp Interoperability Matrix Tool"を参照してください。サポートされる制限については、"Hardware Universe"を参照してください。

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構成できます。
- 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。
- 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。

  具体的な例外については"NetApp Interoperability Matrix Tool"に記載されています。

- 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。

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

各ONTAPバージョンでサポートされるNVMe機能は以下のとおりです。

ONTAPバージョン	NVMeのサポート
9.17.1	• SnapMirror アクティブ同期 NVMe/FC および NVMe/TCP ホスト アクセス（VMware ワークロード用）。
9.15.1	• NVMe / TCPでの4ノードMetroCluster IP構成
9.14.1	• サブシステムでのホストの優先度の設定（ホストレベルのQoS）
9.12.1	• NVMe / FCでの4ノードMetroCluster IP構成 • 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。 • NVMe / TCPでは、MetroCluster構成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 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。 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	• ネームスペースでの512バイト ブロックと4096バイト ブロックのサポート デフォルト値は4096です。ホスト オペレーティング システムで4096バイト ブロックがサポートされていない場合のみ、512を使用してください。 • 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	許可の状況
TCP	9.10.1	デフォルト
FC	9.4	デフォルト

ONTAP 9.8以降では、SCSI、NAS、NVMeの各プロトコルを同じStorage Virtual Machine（SVM）に設定できます。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 9.15.1 以前では、ONTAP はスペース再利用のための NVMe での NVMe DataSet Management（割り当て解除）コマンドをサポートしていません。
- SnapRestoreを使用してLUNからネームスペースをリストアすることはできません。また、その逆もできません。
- 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になります。
- Data ONTAP 7-Modeから移行されたボリュームでは、ネームスペースを作成できません。
- 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。

- 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のLIFとネームスペースは、同じノードでホストする必要があります。
- NVMe LIFを作成する前に、NVMeサービスを作成する必要があります。

関連情報

"『Best practices for modern SAN』"

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 または Ethernet アダプターは NVMe をサポートしている必要があります。サポートされているアダプターは "NetApp Hardware Universe"に記載されています。

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**で**NVMe**を設定する場合	既存の**Storage VM**で**NVMe**を設定する場合
1. System Managerで、*ストレージ > ストレージVM*をクリックし、*追加*をクリックします。 2. Storage VMの名前を入力します。 3. アクセス プロトコル に **NVMe** を選択します。 4. **NVMe/FC** を有効にする または **NVMe/TCP** を有効にする を選択し、保存 します。	1. System Manager で、**Storage > Storage VM** をクリックします。 2. 設定するStorage VMをクリックします。 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。 4. **NVMe/FC** を有効にする または **NVMe/TCP** を有効にする を選択し、保存 します。

CLI

ONTAP CLIで、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、SVMを作成します。

```
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に対応した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
```

   `network port show`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-port-show.html["ONTAPコマンド リファレンス"^]を参照してください。

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
```

`allowed protocols`列の下に表示されるプロトコルは NVMe のみになります。

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>
```

`Administrative Status`SVM の `up`
としてリストされます。link:https://docs.netapp.com/us-en/ontap-cli/up.html["ONTAPコマンド リファレンス"^]の
`up`の詳細については、を参照してください。

8. NVMe/FC LIFを作成します。
   - ONTAP 9.9.1以前のFCの場合

```
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 以降の場合、FC：

```
network interface create -vserver <SVM_name> -lif <lif_name>
-service-policy <default-data-nvme-tcp | default-data-nvme-fc>
-data-protocol <fc-nvme> -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
```

- ONTAP 9.10.1 以降の場合、TCP：

```
network interface create -vserver <SVM_name> -lif <lif_name>
-address <ip address> -netmask <netmask_value> -service-policy
<default-data-nvme-tcp> -data-protocol <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FCの場合

```
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 以降の場合、FC：

```
network interface create -vserver <SVM_name> -lif <lif_name>
-service-policy <default-data-nvme-fc> -data-protocol <fc-nvme>
-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
```

   - ONTAP 9.10.1 以降の場合、TCP：

```
network interface create -vserver <SVM_name> -lif <lif_name>
-address <ip address> -netmask <netmask_value> -service-policy
<default-data-nvme-tcp> -data-protocol <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>
```

自動効率化ポリシーに関する警告メッセージが表示されることがありますが、このメッセージ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。

タスク概要

この手順は、FAS、AFF、およびASAシステムに適用されます。ASA r2システム（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、ASA A20、またはASA C30）をご利用の場合は、"これらの手順"に従ってストレージをプロビジョニングしてください。ASA r2システムは、SANのみをご利用のお客様向けに、簡素化されたONTAPエクスペリエンスを提供します。

ONTAP 9.8以降では、QoSはストレージのプロビジョニング時にデフォルトで有効になります。プロビジョニング時またはあとでQoSを無効にしたり、カスタムのQoSポリシーを選択したりすることができます。

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ことを前提としています。

System Manager

ONTAP System Manager（9.7以降）で、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、*ストレージ > NVMe Namespaces*をクリックし、*追加*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、**More Options** をクリックします。

2. ONTAP 9.8 以降を実行していて、QoS を無効にするか、カスタム 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、[ストレージと最適化] の下で [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 ポートを配置します。
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. ホストからネームスペース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、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、すでにNVMeプロトコル用に設定されている既存の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。

NVMe 用にストレージ VM を構成する必要がある場合は、"NVMe用のSVMの設定"を参照してください。

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`は `allowed-protocols`列の下に表示されます。

2. NVMeネームスペースを作成します。

   > ⓘ `-path`パラメータで参照するボリュームがすでに存在している必要があります。存在しない場合は、このコマンドを実行する前にボリュームを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サブシステムの名前では大文字と小文字が区別されます。1～96文字にする必要があります。特殊文字も使用できます。

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`サブシステムは `Subsystem`列の下に表示される必要があります。

5. ホストからNQNを取得します。
6. ホストの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しかマッピングできません。

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
```

サブシステムは `Attached subsystem`としてリストされる必要があります。

サブシステムへの**NVMe**ネームスペースのマッピング

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。サブシステムへのNVMeネームスペースのマッピングは、ストレージのプロビジョニング時に行うことも、プロビジョニング後に行うこともできます。

ONTAP 9.17.1以降では、SnapMirror Active Sync構成を使用している場合、ホストをNVMeサブシステムに追加する際に、SVMを近接vserverとしてホストに追加できます。NVMeサブシステム内のネームスペースのア

クティブ最適化パスは、近接vserverとして設定されているSVMからのみホストに公開されます。

ONTAP 9.14.1以降では、特定のホストへのリソース割り当てを優先できます。デフォルトでは、ホストがNVMeサブシステムに追加されると、「通常」の優先度が付与されます。ONTAPコマンドラインインターフェイス（CLI）を使用して、デフォルトの優先度を「通常」から「高」に手動で変更できます。「高」の優先度が割り当てられたホストには、より大きな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与える場合は、ホストの優先順位を変更するできます。

開始する前に

名前空間とサブシステムはすでに作成されているはずです。名前空間とサブシステムを作成する必要がある場合は、"NVMeストレージのプロビジョニング"を参照してください。

NVMe名前空間をマップする

手順

1. ホストからNQNを取得します。
2. ホストの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の優先度を通常から高に変更するには、 `-priority high`オプションを使用します。このオプションはONTAP 9.14.1以降で利用できます。"ONTAPコマンド リファレンス"の `vserver nvme subsystem host add`の詳細を確認してください。

SnapMirror Active Sync構成でNVMeサブシステムにホストを追加する際に、SVMを `proximal-vserver`としてホストに追加する場合は、 `-proximal-vservers`オプションを使用できます。このオプションはONTAP 9.17.1以降で使用できます。ソースSVM、デスティネーションSVM、またはその両方を追加できます。このコマンドを実行しているSVMがデフォルトです。

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>
```

名前空間は単一のサブシステムにのみマッピングできます。 `vserver nvme subsystem map add`の詳細については、"ONTAPコマンド リファレンス"を参照してください。

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
```

サブシステムは `Attached subsystem`としてリストされるはずです。 `vserver nvme namespace show`の詳細については、"ONTAPコマンド リファレンス"を参照してください。

LUNを管理する

LUNのQoSポリシー グループの編集

ONTAP 9.10.1以降では、System Managerを使用して、複数のLUNに対して同時にQoS（Quality of Service）ポリシーを割り当てたり削除したりすることができます。

> ボリューム レベルで割り当てられているQoSポリシーは、ボリューム レベルで変更する必要があります。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るQoSポリシーだけです。

手順

1. System Managerで、*ストレージ > LUN*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. ［詳細］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からネームスペースへの変換

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で変換できます。

開始する前に

- igroupへの既存のマッピングがあるLUNは指定できません。
- LUN はMetroCluster構成された SVM 内またはSnapMirrorアクティブな同期関係内に存在してはなりません。
- プロトコル エンドポイントであるLUN、またはプロトコル エンドポイントにバインドされているLUNは指定できません。
- ゼロ以外のプレフィックスやサフィックス ストリームがあるLUNは指定できません。
- Snapshotの一部であるLUN、またはSnapMirror関係のデスティネーション側で読み取り専用になっているLUNは指定できません。

手順

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。ONTAP 9.10.1より前のバージョンでLUNをオフラインにするには、ONTAP CLI

を使用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. 1つまたは複数のLUNをオフラインにします。

次の操作を行う場合：	操作
単一のLUNをオフラインにする	LUN名の横にあるをクリックし、*オフラインにする*を選択します。
複数のLUNをオフラインにする	1. オフラインにするLUNを選択します。 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を使用する場合、一度にオフラインにできるLUNは1つだけです。

手順

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。

タスク概要

この手順は、FAS、AFF、およびASAシステムに適用されます。ASA r2システム（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、ASA A20、またはASA C30）をご利用の場合は、"これらの手順"に従ってストレージユニットのサイズを増やしてください。ASA r2システムは、SANのみをご利用のお客様向けに、簡素化された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のサイズの拡張

LUNのサイズをどこまで拡張できるかは、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 • ASA以外のプラットフォームの場合は16TB
ONTAP 9.5、9.6、9.7	16 TB
ONTAP 9.4以前	元のLUNサイズの10倍ですが、LUNの最大サイズである16TBを超えることはできません。例えば、100GBのLUNを作成した場合、拡張できるのは1,000GBまでです。LUNの実際の最大サイズは16TBと異なる場合があります。ONTAPは、この制限値をわずかに下回る値に切り捨てます。

サイズを拡張するときに、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でホストがサイズの変更を認識するには、ホスト上のLUNを再スキャンする必要があります。

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、*ストレージ > LUN*をクリックします。
2. をクリックして*編集*を選択します。
3. *ストレージと最適化*で、LUNのサイズを増やして*保存*します。

CLI

ONTAP CLIで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>
```

`lun resize`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli//lun-resize.html#description["ONTAPコマンド リファレンス"^]を参照してください。

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の端数が切り捨てられるため、想定値よりも少し小さくなります。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ります。サイズ変更後の正確な値を確認する

には、advanced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
```

+
`lun show`の詳細については、"ONTAPコマンド リファレンス"を参照してください。

1. ホスト上の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のサイズをホスト ファイルシステムに認識させます。

LUNのサイズの縮小

LUNのサイズを縮小する前に、ホストが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のサイズを適切に縮小するには、SnapCenterなどのツールを使用してください。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サイズを認識するには、ホストで追加の手順が必要になることがあります。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る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。

開始する前に

LUN が選択的 LUN マップ（SLM）を使用している場合は、LUN を移動する前に、"SLMレポートノードリストを変更する"宛先ノードとその HA パートナーを含める必要があります。

タスク概要

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

スナップショット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、LUNを移動すると、そのLUNは移動先ボリュームのデータ保護スキームの対象となります。移動先ボリュームにスナップショットが設定されていない場合、LUNのスナップショットは作成されません。また、LUNのすべてのスナップショットは、スナップショット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LUNを移動することはできません。

- 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

クラスタ内のノードが異なるONTAPバージョンを使用している場合、ソースがデスティネーションよりも新しいバージョンである場合にのみ、異なるノード上のボリューム間でLUNを移動できます。たとえば、ソースボリュームのノードがONTAP 9.15.1で、デスティネーション ボリュームのノードがONTAP 9.16.1の場合、LUNを移動することはできません。同じONTAPバージョンのノード上のボリューム間では、LUNを移動できます。

サイズが1TB以上でos_typeがSolarisのLUNでは、LUNの移動時にホストでタイムアウトが発生する場合があります。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、System Managerを使用して、単一のLUNを移動する際に新しいボリュームを作成できます。ONTAP 9.8 / 9.9.1では、LUNの移動を開始する時点でLUNの移動先ボリュームが存在している必要があります。

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、⋮をクリックして **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 に移動するか、新しいボリューム に移動するかを選択します。

   新しいボリュームを作成する場合は、ボリュームの詳細を指定します。

3. *移動*をクリックします。

CLI

ONTAP CLIでLUNを移動します。

1. LUNを移動します。

   ```
   lun move start
   ```

   ごく短時間、移動したLUNが元のボリュームと移動後のボリュームの両方に表示されます。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を削除する

LUN が不要になった場合は、ストレージ仮想マシン（SVM）から LUN を削除できます。

開始する前に

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. アプリケーションやホストが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をコピーする際の注意事項

LUNをコピーする際は、次の点に注意してください。

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

スナップショット内のLUNは、 `lun copy`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をコピーすると、LUNコピーはすぐに読み取りおよび書き込みアクセスが可能になります。LUNコピーの作成によってソースLUNは変更されません。ソースLUNとLUNコピーは、それぞれ異なるLUNシリアル番号を持つ固有のLUNとして存在します。ソースLUNへの変更はLUNコピーには反映されず、LUNコピーへの変更はソースLUNには反映されません。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。

スナップショット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、LUNをソースLUNのボリュームとは異なるボリュームにコピーした場合、コピー先LUNはコピー先ボリュームのデータ保護スキームの対象となります。コピー先ボリュームにスナップショットが設定されていない場合、LUNコピーのスナップショットは作成されません。

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 copy`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=lun+copy["ONTAPコマンド リファレンス"^]を参照してください。

LUNの設定済みスペースと使用済みスペースの検証

LUN に設定されている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、スペース再利用時に再利用できるスペースの量、データを格納するリザーブ スペースの量、および LUN に設定されている合計サイズと実際に使用されているサイズを判断するのに役立ちます。

手順

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.
   ```

> `lun show`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/lun-show.html["ONTAPコマンド リファレンス"^]を参照してください。

ストレージ**QoS**を使用した**LUN**への**I/O**パフォーマンスの制御と監視

LUNをストレージQoSポリシーグループに割り当てることで、LUNへの入出力（I/O）パフォーマンスを制御できます。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。

タスク概要

ポリシー グループを使用して、最大スループット制限（100MB / 秒など）を適用します。最大スループットを指定せずにポリシー グループを作成することもできます。これにより、ワークロードを制御する前にパフォーマンスを監視できます。

FlexVolとLUNが含まれている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。

LUNをポリシーグループに割り当てる場合は、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 グループの作成時に指定します。

- LUNをポリシーグループに割り当てる場合、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ません。

Storage QoS の使用方法の詳細については、"システム管理リファレンス"を参照してください。

手順

1. `qos policy-group create`コマンドを使用してポリシーグループを作成します。

   `qos policy-group create`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/qos-policy-group-create.html["ONTAPコマンド リファレンス"^]を参照してください。

2. `lun create`コマンドまたは `lun modify`パラメータ付きの `-qos-policy-group`コマンドを使用して、ポリシーグループにLUNを割り当てます。

   `lun`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=lun["ONTAPコマンド リファレンス"^]を参照してください。

3. `qos statistics`コマンドを使用してパフォーマンスデータを表示します。
4. 必要に応じて、 `qos policy-group modify`コマンドを使用し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。

   `qos policy-group modify`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/qos-policy-group-modify.html["ONTAPコマンド リファレンス"^]を参照してください。

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、スペース不足を回避するのに役立つツールが利用可能です。

- Active IQ Unified Managerは、環境内のすべてのクラスターにわたるすべてのストレージを管理できる無料ツールです。
- System Manager は ONTAP に組み込まれたグラフィカル ユーザー インターフェイスであり、クラスタレベルでストレージのニーズを手動で管理できます。
- OnCommand Insightは、ストレージインフラストラクチャを一元的に表示し、LUN、ボリューム、アグリゲートのストレージ容量が不足しそうな場合に自動監視、アラート、レポートの設定を可能にします。

移行した**LUN**の機能と制限

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、ホスト構成を更新してから、ONTAPでデータの提供を開始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の管理方法に影響を及ぼす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。

- `lun show`コマンドを使用してLUNを表示します
- `transition 7-mode show`コマンドを使用して、7-Modeボリュームから移行されたLUNのインベントリを表示します
- 7-Mode Snapshot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にキャプチャされたすべての LUN が移行されます。

- `snapshot restore-file`コマンドを使用した7-Modeスナップショットからの単一LUNのリストア
- 7-Mode SnapshotでLUNのクローンを作成する
- 7-Modeスナップショットでキャプチャされ たLUNからブロックの範囲を復元する
- 7-Modeスナップショットを使用してボリュームのFlexCloneを作成します

移行したLUNでは、次の操作を実行することはできません。

- ボリュームにキャプチャされたSnapshotベースのLUNクローンにアクセスします

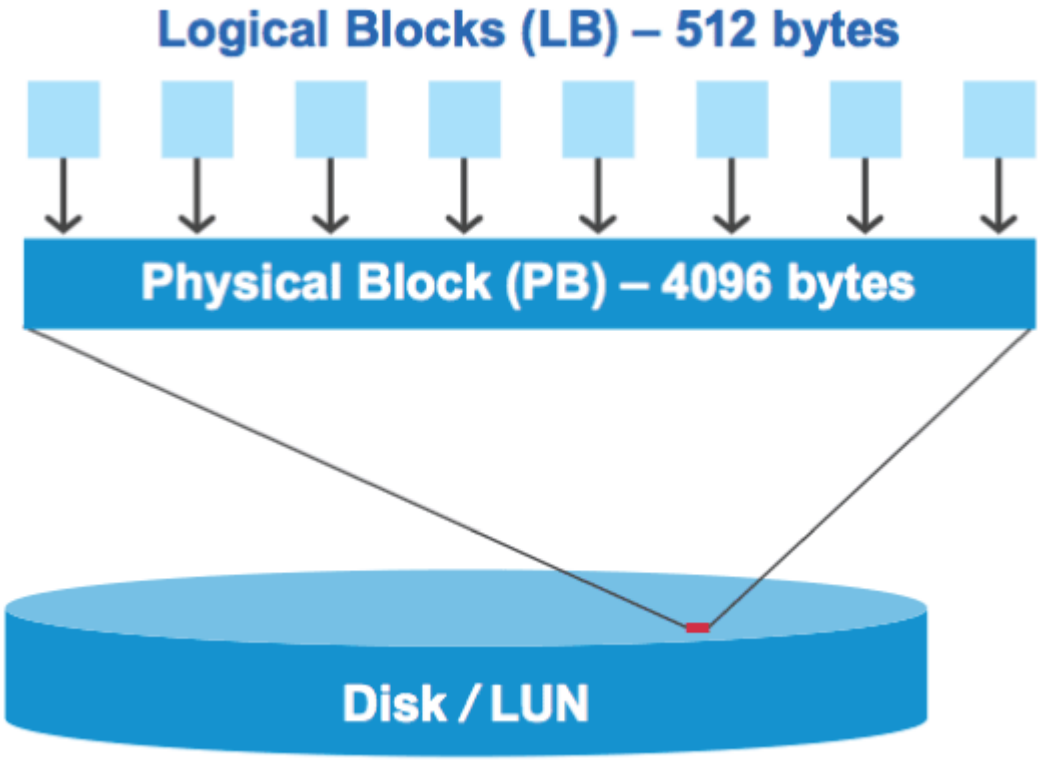
関連情報

- "コピーベースの移行"
- "lun show"

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

ONTAPでは、適切にアライメントされたLUNにおける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、このような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 テーブルが適正である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バイトなので、LUNはそのサイズのブロックをホストに提供します。しかし実際は、よりサイズの大きい4KBのブロックを使用してデータを保存します。ホストで使用される512バイトのデータ ブロックは論理ブロックと呼ばれ、LUNがデータの保存に使用する4KBのデータ ブロックは物理ブロックと呼ばれます。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OS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がアライメントされているとみなされるのは、I/O処理が物理ブロック内の最初の論理ブロックで開始される場合だけです。I/O処理が物理ブロックの最初の論理ブロック以外のブロックで開始される場合は、I/Oがミスアライメントされているとみなされます。ONTAPは、LUNにおけるミスアライメントを自動検出して報告します。ただし、ミスアライメントI/Oが検出されたからといって、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でも、ミスアライメントI/Oが報告される場合があります。

さらに調査が必要な場合は、"NetAppナレッジベース：LUN上の未調整IOを識別するにはどうすればよいでしょうか?"を参照してください。

位置合わせの問題を修正するためのツールの詳細については、次のドキュメントを参照してください：+

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

LUNのOSタイプを使用したI/Oアライメントの実行

ONTAP 9.7以前の場合は、OSのパーティショニング スキームとのI/Oアライメントを実現するために、オペレーティング システムに最も近い推奨ONTAP LUN `ostype`値を使用する必要があります。

ホスト オペレーティング システムが採用しているパーティション スキームは、I/O ミスアライメントの大きな要因です。一部のONTAP LUN `ostype`値は、「`prefix`」と呼ばれる特殊なオフセットを使用してお

り、これによりホスト 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ン スキームをアライメントすることが可能になります。

状況によっては、I/Oアライメントを実現するためにカスタムパーティションテーブルが必要になる場合があります。ただし、 `ostype`値の「`prefix」値が`0`より大きい場合、カスタムパーティションによってI/Oのアライメントがずれ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、"NetApp ナレッジベース：LUN 上の非整列 IO を識別する方法"を参照してください。

ONTAP 9.8以降でプロビジョニングされた新しいLUNには、すべてのLUN OSタイプでサイズが0のプレフィックスとサフィックスがデフォルトで設定されます。I/Oは、デフォルトでサポートされているホスト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注意事項

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、およびファイルシステム用の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する場合、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以前でのLinuxでボリューム マネージャなしでLUNを使用する場合は、LUNをパーティショニングして、1つのパーティション（8個の論理ブロックの偶数倍となるセクター）がアライメントされたオフセットから始まるように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注意事項

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

詳細については、 "Solaris Host Utilitiesのインストールおよび管理ガイド"を参照してください。

ESXブートLUNがミスアライメントとしてレポートされる

ESXブートLUNとして使用されるLUNは、通常ONTAPによってミスアライメントとして報告されます。ESXはブートLUN上に複数のパーティションを作成するため、アライメントが非常に困難です。ミスアライメントされたESXブートLUNは、ミスアライメントされたI/Oの総量が少ないため、通常はパフォーマンスの問題にはなりません。LUNがVMware `ostype`で正しくプロビジョニングされていると仮定すると、何もする必要はありません。

関連情報

"Guest VM file system partition/disk alignment for VMware vSphere, other virtual environments, and NetApp storage systems"

LUNがオフラインになった場合の問題の対処方法

書き込みに利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がスペース不足でオフラインになる理由はさまざまですが、いくつかの方法でこの問題に対処できます。

もし...	次の操作を実行できます。
アグリゲートがフルである	• ディスクを追加します。 • `volume modify`コマンドを使用して、使用可能な領域があるボリュームを縮小します。 • 使用可能なスペースがあるスペース保証ボリュームがある場合は、 `volume modify`コマンドを使用してボリュームのスペース保証を `none`に変更します。
ボリュームはフルだが、アグリゲートには使用可能なスペースがある	• スペース ギャランティ ボリュームの場合は、 `volume modify`コマンドを使用してボリュームのサイズを増やします。 • シンプロビジョニングされたボリュームの場合は、 `volume modify` コマンドを使用してボリュームの最大サイズを増やします。 ボリュームの自動拡張が有効になっていない場合は、 `volume modify -autogrow-mode`を使用して有効にします。 • `volume snapshot delete`コマンドを使用してスナップショットを手動で削除するか、 `volume snapshot autodelete modify`コマンドを使用してスナップショット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

ホストでは、iSCSI LUNがローカル ディスクとして表示されます。ストレージ システムのLUNをホストがディスクとして使用できない場合は、設定を確認してください。

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適切に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。 • 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。 `ping -node node_name -destination host_ip_address_for_iSCSI` • 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。 `ping -node node_name -destination host_ip_address_for_iSCSI`
システム要件	各構成コンポーネントが要件を満たしていることを確認します。ホスト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、任意のスイッチ）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てください。
iSCSIサービス ステータス	iSCSIサービスがライセンス供与されており、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	イニシエーター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てください。 `iscsi initiator show`コマンド出力にイニシエーターがログインしていないと表示される場合は、ホスト上のイニシエーターの設定を確認してください。また、ストレージシステムがイニシエーターのターゲットとして設定されていることも確認してください。
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。イニシエータのツールおよびコマンドをホストで使用し、イニシエータのノード名を表示します。igroupおよびホストで設定したイニシエータのノード名は、互いに一致する必要があります。
LUNマッピング	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、次のいずれかのコマンドを使用できます。 • `lun mapping show`すべてのLUNとそれらがマッピングされているigroupが表示されます。 • `lun mapping show -igroup`特定のigroupにマップされたLUNを表示します。
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"
- "lun mapping show"

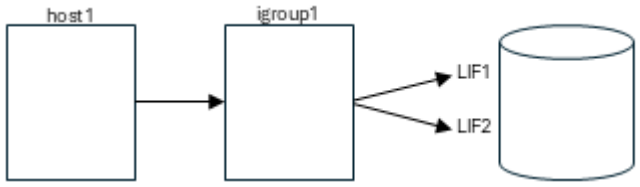
igroupとポートセットの管理

ポートセットと**igroup**で**LUN**アクセスを制限する方法

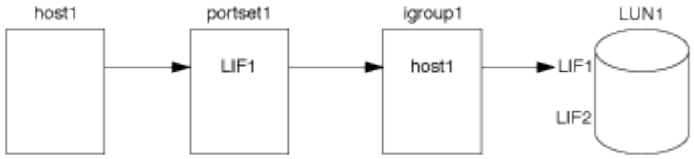
選択的LUNマップ（SLM）に加えて、igroupおよびポートセットを使用してLUNへのアクセスを制限することができます。

ポートセットをSLMと併用することで、特定のターゲットから特定のイニシエータへのアクセスをさらに制限できます。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経由でアクセス可能になります。

次の例では、host1にはポートセットがありません。ポートセットがない場合、host1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して、LUN1へのアクセスを制限できます。次の例では、host1はLIF1経由でのみLUN1にアクセスできます。ただし、LIF2はportset1に含まれていないため、host1はLIF2経由でLUN1にアクセスできません。



関連情報

- 選択的LUNマップ
- ポートセットの作成とigroupへのバインド

SANのイニシエータと**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。

タスク概要

- 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 グループは、作成後に編集または削除することもできます。
- SANのイニシエータ グループとイニシエータについて、次の管理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、ホスト **> SAN** イニシエーター グループ をクリックします。

   イニシエータ グループ（igroup）のリストが表示されます。リストが1ページに収まらない場合は、ページ右下にあるページ番号をクリックして次のページを表示できます。

   igroupに関するさまざまな情報が各列に表示されます。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）：リストの右上隅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
   - リストを*ダウンロード*します。
   - リスト内の列を*表示*または*非表示*にします。
   - リスト内のデータを*フィルタリング*します。
3. リストから処理を実行できます。
   - + Add をクリックしてigroupを追加します。
   - igroup 名をクリックすると、igroup の詳細を示す **Overview** ページが表示されます。

     *概要*ページでは、igroupに関連付けられたLUNを確認でき、LUNの作成とLUNのマッピングの操作を開始できます。*すべてのSANイニシエータ*をクリックすると、メインリストに戻ります。

   - igroupの上にマウスを移動し、igroupの名前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名の左側の領域にマウスを移動し、チェックボックスをオンにします。*+Add to Initiator Group*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表示します。

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、ホスト **> SAN** イニシエーター グループ をクリックします。

   イニシエータ グループ（igroup）のリストが表示されます。

2. イニシエータを表示するには、次の手順を実行します。

- **FC** イニシエーター タブをクリックして、FC イニシエーターのリストを表示します。
- *iSCSI イニシエーター*タブをクリックして、iSCSI イニシエーターのリストを表示します。

  イニシエータに関するさまざまな情報が各列に表示されます。

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）：リストの右上隅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：
   - リスト内で特定のイニシエーターを*検索*します。
   - リストを*ダウンロード*します。
   - リスト内の列を*表示*または*非表示*にします。
   - 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**の作成

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 の **Name** と **Description** を入力します。

   この説明はigroupのエイリアスとなります。

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

   ネストされたigroupのOSタイプは作成後に変更することはできません。

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

   *検索*を使用して、追加するイニシエータ グループを検索して選択できます。

複数の**LUN**への**igroup**のマッピング

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、*ストレージ > LUN*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、**[イニシエーター グループにマップ]** 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。

ポートセットの作成と**igroup**へのバインド

"選択的LUNマップ（SLM）"を使用するだけでなく、ポートセットを作成し、そのポートセットをigroupにバインドして、イニシエータがLUNにアクセスするために使用でき

るLIFをさらに制限することもできます。

igroupにポートセットをバインドしないと、igroup内のすべてのイニシエータが、LUNを所有するノードとそのノードの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。

開始する前に

少なくとも1個の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個です。インターフェイス グループを使用する場合に推奨されるLIFの数は1個です。

タスク概要

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にバインドすることができます。

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の手順を使用する必要があります。

ONTAP 9.12.1以降、既存のポートセットがない場合は、ONTAP CLI手順を使用して最初のポートセットを作成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、*追加*をクリックします。
3. *ホスト > SAN イニシエータグループ*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、[追加] 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、⋮をクリックして、*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. 該当する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を使用している場合は、 `protocol`パラメータを `fcp`として指定します。iSCSIを使用している場合は、 `protocol`パラメータを `iscsi`として指定します。

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
   ```

   > `lun igroup bind`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/lun-igroup-bind.html["ONTAPコマンド リファレンス"^]を参照してください。

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する

"選択的LUNマップ（SLM）"に加えて、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できるLIFをさらに制限できます。

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、*Network > Overview > Portsets*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。

ポートセットの削除

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、を選択してから*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 **-** 概要

選択的LUNマップ（SLM）では、ホストからLUNへのパスの数を減らすことができます。SLMを使用して新しい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、システム停止を伴わないLUNの移動処理がサポートされます。ポートセットの操作やLUNの再マッピングは不要です。

"ポートセット"をSLMと併用することで、特定のターゲットから特定のイニシエータへのアクセスをさらに制限できます。SLMをポートセットと併用すると、LUNは、LUNを所有するノードとそのノードのHAパートナー上のポートセット内のLIFセットからアクセス可能になります。

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**マップで有効かどうかの確認

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Selective LUN Map（SLM;選択的LUNマップ）が有効になっているかどうかを判断しなければならないことがあります。

`lun mapping show -fields reporting-nodes, node`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。SLMが有効になっていない場合、コマンド出力の「`reporting-nodes`」列の下のセルに「-」が表示されます。SLMが有効になっている場合、「`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。

`lun mapping show`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/lun-mapping-show.html["ONTAPコマンド リファレンス"^]を参照してください。

SLMレポート ノード リストの変更

LUNまたはLUNが含まれている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、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 リストを変更して、LUNのアクティブな最適パスが維持されるように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、 `igroup_name`の代わりに `igroup_prefix*`を使用して、複数のLUNマッピングを同時に変更できます。

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具体的な手順については、ホストのドキュメントを参照してください。

iSCSIプロトコルの管理

パフォーマンスを最大化するためのネットワーク設定

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変わります。特定の設定値を選択することで、iSCSIに使用され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方法については、"ネットワーク管理"を参照してください。

4. ジャンボ フレームを有効にします（通常はMTUが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。サポートされていない場合にジャンボ 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。

iSCSI用のSVMの設定

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。

タスク概要

iSCSIプロトコルを使用してデータを提供するそれぞれのSVMについて、各ノードに少なくとも1個のiSCSI LIFが必要です。冗長性を確保するには、各ノードに少なくとも2個の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**を設定する場合	既存の**Storage VM**で**iSCSI**を設定する場合
1. System Managerで、*ストレージ > ストレージVM*をクリックし、*追加*をクリックします。 2. Storage VMの名前を入力します。 3. * Access Protocol * に * iSCSI * を選択します。 4. **Enable iSCSI** をクリックし、ネットワーク インターフェイスの IP アドレスとサブネット マスクを入力します。+ 各ノードには少なくとも 2 つのネットワーク インターフェイスが必要です。 5. *保存*をクリックします。	1. System Manager で、**Storage > Storage VM** をクリックします。 2. 設定するStorage VMをクリックします。 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。 4. **Enable iSCSI** をクリックし、ネットワーク インターフェイスの IP アドレスとサブネット マスクを入力します。+ 各ノードには少なくとも 2 つのネットワーク インターフェイスが必要です。 5. *保存*をクリックします。

CLI

ONTAP CLIで、iSCSI用の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
   ```

   `network interface show`
   の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-interface-show.html["ONTAPコマンド リファレンス"^]を参照してください。

4. iSCSIが正常に稼働していることと、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：最新SANのベストプラクティス"

イニシエータのセキュリティ ポリシー方式の定義

一連のイニシエータとその認証方式を定義できます。ユーザ定義の認証方式がないイニシエータに適用されるデフォルトの認証方式を変更することもできます。

タスク概要

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。

すべてのイニシエータが16進数のCHAPシークレット パスワードをサポートしているわけではありません。

手順

1. `vserver iscsi security create`コマンドを使用して、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で、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**サービスの削除

Storage Virtual Machine（SVM）のiSCSIサービスは、不要になったら削除できます。

開始する前に

iSCSIサービスを削除する前に、iSCSIサービスの管理ステータスが「down」状態である必要があります。`vserver iscsi modify`コマンドを使用して管理ステータスをダウン状態にすることができます。

手順

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

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

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

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

3. `vserver iscsi show command`を使用して、SVMからiSCSIサービスが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 リカバリにおける詳細情報の確認

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 リカバリの詳細情報を確認できます。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少し低下する可能性があります。

タスク概要

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、新しく作成する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、 `max-error-recovery-level`オプションは `iscsi show`コマンドおよび `iscsi modify`コマンドではサポートされていません。

手順

1. advancedモードに切り替えます。

   ```
   set -privilege advanced
   ```

2. `iscsi show`コマンドを使用して現在の設定を確認します。

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

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

3. `iscsi modify`コマンドを使用してエラー回復レベルを変更します。

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

iSNSサーバへの**SVM**の登録

`vserver iscsi isns`コマンドを使用して、ストレージ仮想マシン（SVM）をiSNSサーバに登録するように設定できます。

タスク概要

この `vserver iscsi isns create`コマンドは、SVMをiSNSサーバに登録するように設定します。SVMには、iSNSサーバを設定または管理するためのコマンドは用意されていません。iSNSサーバを管理するには、サーバ管理ツール、またはiSNSサーバのベンダーが提供するインタフェースを使用してください。

手順

1. iSNS サーバーで、iSNS サービスが稼働しており、利用可能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
   ```

   `network interface create`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-interface-create.html["ONTAPコマンド リファレンス"^]を参照してください。

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 ルートが存在してい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
   ```

   `network route create`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-route-create.html["ONTAPコマンド リファレンス"^]を参照してください。

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とIPv6の両方のアドレスファミリがサポートされています。iSNSサーバのアドレスファミリは、SVM管理LIFのアドレスファミリ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、iSNSサービスを開始します。

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

ストレージ システムの**iSCSI**エラー メッセージの解決

`event log show`コマンドで表示できる、iSCSI関連の一般的なエラーメッセージがいくつかあります。これらのメッセージの意味と、メッセージで特定される問題を解決するために何ができるかを理解しておく必要があります。

次の表には、最も一般的なエラー メッセージとその解決手順が記載されています：

メッセージ	説明	対処方法
`ISCSI: network interface identifier disabled for use; incoming connection discarded`	iSCSIサービスがインターフェイスで有効になっていません。	`iscsi interface enable`コマンドを使用して、インターフェース上でiSCSIサービスを有効にすることができます。例： `iscsi interface enable -vserver vs1 -lif lif1`

メッセージ	説明	対処方法
`ISCSI: Authentication failed for initiator nodename`	指定されたイニシエーターに対してCHAPが正しく設定されていません。	CHAP設定を確認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同じユーザー名とパスワードを使用することはできません： • ストレージ システムのインバウンド クレデンシャルは、イニシエーターのアウトバウンド クレデンシャルと一致する必要があります。 • 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、イニシエーターのインバウンド クレデンシャルと一致する必要があります。

`event log show`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/event-log-show.html["ONTAPコマンド リファレンス"^]を参照してください。

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のLIFの自動フェイルオーバーを有効にできます。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元のノードまたはポートに移行されます。また、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移行されます。これにより、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では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がない
- 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。

"LIFのフェイルオーバーとギブバック"についての詳細をご覧ください。

手順

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、 `lif`の代わりに `-lif*`を使用します。

iSCSI LIFの自動フェイルオーバーの無効化

ONTAP 9.10.1以前で作成したiSCSI LIFでiSCSI LIFの自動フェイルオーバーを有効にしていた場合、それを無効にすることができます。

手順

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、 `lif`の代わりに `-lif*`を使用します。

関連情報

- "LIFの作成"
- 手動で"LIFを移行する"
- 手動で"LIFをホーム ポートに戻す"
- "LIFのフェイルオーバーの設定"

FCプロトコルの管理

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に含まれる"）が必要であり、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 `down`になります。LIFとSVMを動作させるには、FCサービスが有効になっている必要があります。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。

タスク概要

NetAppでは、FCプロトコルを使用してデータを提供する各SVMで、ノードごとに少なくとも1つのFC LIFをサポートします。2つのファブリックとノードごとに2つのLIFを使用し、各ファブリックにそれぞれのノードから1つのLIFを接続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**を設定する場合	既存の**Storage VM**で**FC**を設定する場合
1. System Managerで、*ストレージ > ストレージVM*をクリックし、*追加*をクリックします。 2. Storage VMの名前を入力します。 3. **Access Protocol** に **FC** を選択します。 4. *Enable FC*をクリックします。+ FCポートは自動的に割り当てられます。 5. *保存*をクリックします。	1. System Manager で、**Storage > Storage VM** をクリックします。 2. 設定するStorage VMをクリックします。 3. *設定*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。 4. **FC** を有効にする をクリックし、ネットワークインターフェイスの IP アドレスとサブネットマスクを入力します。+ FC ポートは自動的に割り当てられます。 5. *保存*をクリックします。

CLI

1. SVMのFCサービスを有効にします。

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

2. FCを使用する各ノード上に、SVM用に2つのLIFを作成します。
   - 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 `online`であることを確認します：

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

`network interface show`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-interface-show.html["ONTAPコマンド リファレンス"^]を参照してください。

関連情報

- "NetAppサポート"
- "NetApp Interoperability Matrix Tool"
- クラスタSAN環境でのLIFに関する注意事項

SVMのFCサービスの削除

Storage Virtual Machine（SVM）のFCサービスは、不要になったら削除できます。

開始する前に

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

手順

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

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

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

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

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

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

FCoEジャンボ フレーム用の推奨されるMTU設定

Fibre Channel over Ethernet（FCoE）では、CNAのイーサネット アダプタ部分については、ジャンボ フレームを9000MTUに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 フレームのMTUを1500より大きく設定する必要があります。ジャンボ フレームは、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、かつジャンボ フレーム用に設定されている場合にのみ設定します。

NVMeプロトコルの管理

SVMのNVMeサービスの開始

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

開始する前に

NVMeプロトコルがシステムで許可されている必要があります。

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 9.9.1以降では…	許可の状況
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からの**NVMe**サービスの削除

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変更

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では、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 サイズの拡張

System Manager

1. *ストレージ > NVMe Namespaces*をクリックします。
2. 増やしたい名前空間にマウスを移動し、⋮をクリックして、*編集*をクリックします。
3. **CAPACITY** の下で、名前空間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 サイズの縮小

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
   ```

ネームスペースから**LUN**への変換

ONTAP 9.11.1以降では、ONTAP CLIを使用して、既存のNVMeネームスペースをLUNにインプレースで変換できます。

開始する前に

- サブシステムへの既存のマッピングがあるNVMeネームスペースは指定できません。
- Snapshotの一部であるネームスペースやSnapMirror関係のデスティネーション側で読み取り専用になっているネームスペースは指定できません。
- 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 カードでしかサポートされないため、この処理も特定のハードウェアでのみ機能します。

手順

1. NVMeネームスペースをLUNに変換するには、次のコマンドを入力します。

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

   `lun convert-from-namespace`
   の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/lun-convert-from-namespace.html["ONTAPコマンド リファレンス"^]をご覧ください。

NVMe経由のインバンド認証の設定

ONTAP 9.12.1以降では、ONTAPコマンドライン インターフェイス（CLI）を使用して、NVMeホストとNVMeコントローラの間にNVMe / TCPおよびNVMe / FCプロトコルを介したDH-HMAC-CHAP認証によるインバンドの（セキュアな）双方向認証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、そのピアに関連付けられているキーを認識している必要があります。

単方向認証では、ホストにはシークレット キーを設定しますが、コントローラには設定しません。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 キーを設定します。

デフォルトのハッシュ関数はSHA-256で、デフォルトのDHグループは2048ビットです。

System Manager

ONTAP 9.14.1以降では、NVMe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NVMeネームスペースを使用した整合グループの追加を行うときに、System Managerでインバンド認証を設定できます。

手順

1. System Manager で、**Hosts > NVMe Subsystem** をクリックし、**Add** 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NQNを入力します。
4. ホスト 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. 各ホストで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かった場合には、それぞれのデフォルト設定（ハッシュ関数はSHA-256、DHグループは2048ビット）が割り当てられます。

7. オプションで、*追加*をクリックし、必要に応じて手順を繰り返してさらにホストを追加します。
8. *保存*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、**System Manager > Hosts > NVMe Subsystem > Grid > Peek view** をクリックします。

   ホスト名の横にあるキー アイコンが透明な場合、単方向モードが有効であることを示しています。ホスト名の横にあるキー アイコンが不透明な場合、双方向モードが有効であることを示しています。

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>
```

`vserver nvme subsystem host add`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/vserver-nvme-subsystem-host-add.html["ONTAPコマンド リファレンス
"^]をご覧ください。

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
```

`vserver nvme subsystem host show`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/vserver-nvme-subsystem-host-show.html["ONTAPコマンド リファレンス
"^]をご覧ください。

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
```

関連情報

- "vserver nvme subsystem controller show"

NVMe経由のインバンド認証の無効化

DH-HMAC-CHAPを使用したNVMe経由のインバンド認証を設定している場合、いつでもその認証を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を使用したインバンド認証が無効になっていないと、リバートは失敗します。

手順

1. サブシステムからホストを削除して、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. ホストを認証なしで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サブシステムでTLSを有効にできます。ONTAPはTLSハードウェアオフロードをサポートしていません。

System Manager

ONTAP 9.16.1以降では、NVMe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NVMeネームスペースを使用した整合グループの追加を行うときに、System ManagerでNVMe / TCP接続にTLSを設定できます。

手順

1. System Manager で、**Hosts > NVMe Subsystem** をクリックし、**Add** 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NQNを入力します。
4. ホスト NQN の横にある **Transport Layer Security**（**TLS**）が必要 を選択します。
5. 事前共有キー（PSK）を指定します。
6. *保存*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、* System Manager > Hosts > NVMe Subsystem > Grid > Peek view* 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。 `tls-configured-psk` 引数を使用して事前共有キー（PSK）を指定できます：

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

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 `tls-key-type`引数を使用して、そのキータイプを使用しているホストのみを表示することもできます：

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

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てください。オプションで `tls-key-type`、 `tls-identity`、または `tls-cipher`引数のいずれかを使用して、これらのTLS属性を持つコントローラのみを表示することもできます。

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

関連情報

- "vserver nvme サブシステム"

NVMe / TCPのTLSセキュア チャネルの無効化

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接続にTLSセキュア チャネルを設定している場合、いつでもそれを無効にできます。

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. ホストをTLSセキュア チャネルなしで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>
```

関連情報

- "vserver nvme サブシステム ホスト"

NVMeホストの優先度の変更

ONTAP 9.14.1以降では、特定のホストに対するリソース割り当てを優先するようにNVMeサブシステムを設定できます。デフォルトでは、サブシステムにホストを追加した時点で、ホストに優先度regularが割り当てられます。優先度highを割り当てられたホストには、それよりも多くのI/Oキュー数とキュー深度が割り当てられます。

デフォルトの優先度を手動でregularからhighに変更するには、ONTAPのコマンドライン インターフェイス（CLI）を使用します。ホストに割り当てられている優先度を変更する場合には、サブシステムからホストをいったん削除したうえで、追加し直す必要があります。

手順

1. ホストの優先度がregularに設定されていることを確認します。

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

`vserver nvme show-host-priority`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/vserver-nvme-show-host-priority.html["ONTAPコマンド リファレンス"^]をご覧ください。

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>
```

`vserver nvme subsystem host remove`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/vserver-nvme-subsystem-host-remove.html["ONTAPコマンド リファレンス"^]をご覧ください。

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
```

`vserver nvme subsystem host show`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/vserver-nvme-subsystem-host-show.html["ONTAPコマンド リファレンス"^]をご覧ください。

4. 優先度をhighに設定して、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
```

`vserver nvme subsystem host add`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/vserver-nvme-subsystem-host-add.html["ONTAPコマンド リファレンス"^]をご覧ください。

ONTAPでの**NVMe/TCP**コントローラの自動ホスト検出の管理

ONTAP 9.14.1 以降では、IP ベースのファブリックで NVMe/TCP プロトコルを使用した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コントローラの自動ホスト検出の有効化

以前に自動ホスト検出を無効にしていても、ニーズが変わった場合には、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 -fields mdns-service-discovery-enabled
```

NVMe / TCPコントローラの自動ホスト検出の無効化

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 -fields mdns-service-discovery-enabled
```

ONTAPでNVMeホスト仮想マシン識別子を無効にする

ONTAP 9.14.1以降、ONTAPはデフォルトで、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使用率を監視する機能をサポートしています。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。

この機能を無効にするには、bootarg を使用します。"NetAppナレッジベース：ONTAPでNVMeホスト仮想マシン識別子を無効にする方法"を参照してください。

FCアダプタを搭載したシステムの管理

FCアダプタを搭載したシステムの管理

オンボードFCアダプタとFCアダプタ カードの管理に使用できるコマンドが用意されています。これらのコマンドを使用すると、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。また、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、および場合によっては外部ストレージ アレイに接続します。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HBAポートとスイッチ ポート速度は、同じ値に設定し、自動に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プロトコルとFC-NVMeプロトコルのFCアダプタの管理には、同じコマンドを使用します。

FCイニシエータアダプタ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コマンドを使用する前に、 `run -node *node_name*`コマンドを使用する必要があります。

FC ターゲット アダプタを管理するためのコマンド

状況	使用するコマンド
ノード上のFCアダプタ情報を表示する	`network fcp adapter show`
FCターゲット アダプタパラメータを変更する	`network fcp adapter modify`
FCプロトコルのトラフィック情報を表示する	`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`
ディスプレイ アダプタの設定とステータス	`run -node *node_name* sysconfig -v *adapter*`

状況	使用するコマンド
インストールされている拡張カードと構成エラーの有無を確認します	`run -node node_name sysconfig -ac`
コマンドのマニュアル ページを表示する	`man <command_name>`

FCイニシエータ アダプタを管理するためのコマンド

状況	使用するコマンド
ノード内のすべてのイニシエーターとそのアダプターの情報を表示します	`run -node node_name storage show adapter`
ディスプレイ アダプタの設定とステータス	`run -node node_name sysconfig -v adapter`
インストールされている拡張カードと構成エラーの有無を確認します	`run -node node_name sysconfig -ac`

オンボード **FC** アダプタを管理するためのコマンド

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する	`run -node node_name system hardware unified-connect show`

関連情報

- "ネットワーク FCP アダプタ"

FCアダプタの設定

各オンボード FC ポートは、イニシエータまたはターゲットとして個別に設定できます。一部の FC アダプタ上のポートも、オンボード 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設定できます。ターゲット モードに設定できるアダプタのリストは、"NetApp Hardware Universe"で確認できます。

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。イニシエータ モードは、ポートをテープ ドライブ、テープ ライブラリ、または Foreign LUN Import（FLI）を備えたサードパーティ製ストレージに接続するために使用されます。

FCアダプタをFCプロトコルとFC-NVMeプロトコル用に設定する手順は同じです。ただし、FC-NVMeをサポートしているのは一部のFCアダプタのみです。FC-NVMeプロトコルをサポートするアダプタの一覧については、"NetApp Hardware Universe"をご覧ください。

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、システムの該当するアダプタ 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
   ```

   `network fcp adapter show`
   の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-fcp-adapter-show.html["ONTAPコマンド リファレンス"^]をご覧ください。

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

開始する前に

- アダプタのLIFを、メンバーとして属するすべてのポート 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、変更する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、移行するか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
   ```

   `network interface delete`
   の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-interface-delete.html["ONTAPコマンド リファレンス"^]をご覧ください。

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、システムの該当するアダプタ 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`

アダプタ設定の確認

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

手順

1. `network fcp adapter show`コマンドを使用してアダプタ情報を表示します： `network fcp adapter show -instance -node node1 -adapter 0a`

   使用中の各スロットのシステム構成情報とアダプタ情報が出力に表示されます。

   > `network fcp adapter show`
   > の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-fcp-adapter-show.html["ONTAPコマンド リファレンス"^]をご覧ください。

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. `system hardware unified-connect show`コマンドを実行して、ポート構成とモジュールを確認します。
3. ポート情報を確認してから、CNAとポートを設定します。

CNAモードからFCモードへのUTA2ポートの変更

FCイニシエータおよび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）モードからFibre Channel（FC）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モードに変更する必要があります。

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. 必要に応じて、管理者または VIF マネージャーにポートの削除または除去を通知します。
   - 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、管理者は次の操作を行う必要があります：
     i. それぞれ、LIF を移動するか、ifgrp からポートを削除するか、VLAN を削除します。
     ii. `network port delete`コマンドを実行してポートを手動で削除します。

     `network port delete`コマンドが失敗した場合、管理者はエラーに対処してからコマンドを再度実行する必要があります。

     `network port delete`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-port-delete.html["ONTAPコマンド リファレンス"^]をご覧ください。

   - ポートが LIF のホーム ポートとして使用されておらず、ifgrp のメンバーではなく、VLAN をホストしていない場合、VIF マネージャは再起動時にそのポートをレコードから削除する必要があります。

     VIFマネージャーがポートを削除しない場合は、管理者は再起動後に `network port delete` コマンドを使用して手動でポートを削除する必要があります。

     ```
     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
```

`network port show`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-port-show.html["ONTAPコマンド リファレンス"^]を参照してください。

5. 正しい SFP+ がインストールさ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 Ethernet SFPを使用する必要があります。FCの場合は、ノードの設定を変更する前に、8 Gb SFPまたは16 Gb SFPを使用する必要があります。

   `network fcp adapter show`
   の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-fcp-adapter-show.html["ONTAPコマンド リファレンス"^]をご覧ください。

関連情報

- "ネットワーク インターフェイス"

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には、そのアダプタで光モジュールを変更する必要があります。

手順

1. カードで現在使用されているSFP+を確認してください。その後、現在のSFP+を、優先パーソナリティ（FCまたはCNA）に適したSFP+に交換してください。
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. 優先して使用するパーソナリティ モード（FCまたはCNA）の光ファイバに適したモジュールを取り付けます。
4. 正しい SFP+ がインストールさ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）ケーブルは、*Hardware Universe* にリストされています。

関連情報

- "NetApp Hardware Universe"
- "network fcp adapter show"

X1143A-R6アダプタでサポートされるポート設定

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10GbEポートのNICおよびFCoEのターゲット 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、単一のX1143A-R6アダプタが、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

統合ターゲット 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つ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. `system node hardware unified-connect modify`コマンドを使用して、必要に応じてFibre Channel（FC）または Converged Network Adapter（CNA）のポートを構成します。
2. FC または 10 Gb Ethernet に適切なケーブルを接続します。
3. 正しい SFP+ がインストールさ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 Ethernet 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を使用する必要があります。

`network fcp adapter show`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-fcp-adapter-show.html["ONTAPコマンド リファレンス"^]をご覧ください。

X1133A-R6アダプタ使用時の接続の切断回避

別のX1133A-R6 HBAへの冗長パスを構成することによって、ポート障害時に接続が切断されるのを回避できます。

X1133A-R6 HBAは、2つの2ポートペアで構成される4ポート、16Gb FCアダプタです。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。各2ポートペアは、1つのASICによってサポートされます（例：ポート1とポート2はASIC 1、ポート3とポート4はASIC 2）。1つの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。ペアをサポートしているASICでエラーが発生した場合、ペアの両方のポートはオフラインになります。

この接続の損失を防ぐには、個別のX1133A-R6 HBAへの冗長パス、またはHBA上の異なるASICでサポートされているポートへの冗長パスを使用してシステムを構成します。

すべての**SAN**プロトコルの**LIF**の管理

すべての**SAN**プロトコルの**LIF**の管理

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、イニシエータでマルチパスI/O（MPIO）と非対称論理ユニット アクセス（ALUA）を使用する必要があります。ノードで障害が発生した場合、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ペアのノードごとにiSCSIパスを1つ以上作成し、HAペアで処理する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構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。

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。どちらのタイプの接続でも、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。ノードあたり2つのLIFを設定できます。LIFは、iSCSI用のイーサネット ネットワークと分離するために、FCで使用するファブリックごとに1つ必要になります。

LIFが作成されたら、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そのものを削除したりすることができます。

関連情報

- "LIFの設定 - 概要"
- "LIFの作成"

ONTAPで**NVMe LIF**を設定

NVMe LIFを設定するときは、特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アダプタはNVMeをサポートしている必要があります。サポートされているアダプタは"Hardware Universe"に記載されています。

タスク概要

ONTAP 9.12.1以降では、最大12ノードでノードあたり2つのNVMe LIFを設定できます。ONTAP 9.11.1以前では、最大2ノードでノードあたり2つのNVMe LIFを設定できます。

NVMe LIFを作成するときのルールは次のとおりです。

- 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以降では、NVMe LIFはネームスペースを含むノードとそのHAパートナーに設定する必要があります。
- ONTAP 9.4のみ：
  - NVMeのLIFとネームスペースは、同じノードでホストする必要があります。
  - SVM ごとに 1 つの NVMe データ LIF のみ設定できます。

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>
```

作成後は、NVMe / TCP LIFがポート8009で検出をリスンします。

関連情報

- "ネットワーク インターフェイス"

SAN LIFを移動する際の注意事項

クラスタにノードを追加したりクラスタからノードを削除するなど、クラスタの構成を

変更する場合は、LIFを移動するだけで済みます。LIFを移動すれば、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その新しいターゲット インターフェイスとの間に新しいiSCSIセッションを作成したりする必要がありません。

`network interface move`コマンドを使用してSAN LIFを移動することはできません。SAN LIFの移動は、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、新しい場所でオンラインに戻すという手順で実行する必要があります。Asymmetric Logical Unit Access（ALUA）は、すべてのONTAP SANソリューションの一部として冗長パスと自動パス選択を提供します。そのため、LIFを移動のためにオフラインにしてもI/O中断は発生しません。ホストは単に再試行し、その後I/Oを別のLIFに移動します。

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タスクを実行できます。

- クラスタの1個のHAペアを、LUNデータにアクセスするホストにはまったく支障のない形で、アップグレードしたHAペアに置き換える
- ターゲット インターフェイス カードをアップグレードする
- 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

ポートセットからの**SAN LIF**の削除

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は、LIFを削除または移動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。

タスク概要

次の手順1は、ポートセットにLIFが1つしかない場合にのみ実行します。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、そのポートセット内の最後のLIFは削除できません。ポートセットに複数のLIFがある場合は、手順2から開始してください。

手順

1. ポート セット内に LIF が 1 つだけ存在する場合は、 `lun igroup unbind`コマンドを使用してポート セットをイニシエータ グループからバインド解除します。

   ポートセットとイニシエータ グループ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 インターフェイスで当該イニシエータ 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
   ```

   `lun igroup unbind`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/lun-igroup-unbind.html["ONTAPコマンド リファレンス"^]をご覧ください。

2. `lun portset remove`コマンドを使用して、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
```

> `lun portset remove`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/lun-portset-remove.html["ONTAPコマンド リファレンス"^]をご覧ください。

SAN LIFの移動

ノードをオフラインにする必要がある場合、SAN LIFを移動することで、WWPNなどの設定情報を保持し、スイッチファブリックの再ゾーニングを回避できます。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提供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、Storage Virtual Machine（SVM）間で移動することはできません。

開始する前に

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、LIFをポート セットから削除する必要があります。

タスク概要

移動するLIFの宛先ノードと物理ポートは、同じFCファブリックまたはイーサネット ネットワーク上になければなりません。適切にゾーニングされていない別のファブリックにLIFを移動した場合、またはiSCSIイニシエータとターゲット間の接続がないイーサネット ネットワークにLIFを移動した場合、LUNをオンラインに戻してもアクセスできなくなります。

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
```

> `network interface show`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-interface-show.html["ONTAPコマンド リファレンス"^]を参照してください。

2. LIF のステータスを down（オフライン）に変更します：

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

> `network interface modify`
> の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-interface-modify.html["ONTAPコマンド リファレンス"^]を参照してください。

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 up（オンライン）に変更します：

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

   `up`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/up.html["ONTAPコマンド リファレンス"^]を参照してください。

5. 変更が適用されたことを確認します。

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

SAN環境の**LIF**の削除

LIFを削除する前に、LIFに接続しているホストが、別のパスを介してLUNにアクセスできることを確認してください。

開始する前に

削除するLIFがポートセットのメンバーである場合は、LIFを削除する前に、あらかじめポートセットからそのLIFを削除しておく必要があります。

System Manager

ONTAP System Manager（9.7以降）でLIFを削除します。

手順

1. System Managerで、*ネットワーク > 概要*をクリックし、*ネットワークインターフェイス*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でLIFを削除します。

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
   ```

   `network interface delete`
   の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-interface-delete.html["ONTAPコマンド リファレンス"^]をご覧ください。

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
   ```

`network interface show`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-interface-show.html["ONTAPコマンド リファレンス"^]を参照してください。

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、一定の注意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、必要に応じてそれらのノードにLIFを作成する必要があります。
- ホスト スタックとプロトコルの指示に従って、作成したLIFを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しないでもLUNやボリュームを移動できるようにするには、新しいノード上に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**を返すための**iSCSI LIF**の設定

ONTAP 9以降では、ホストOSから送信されたiSCSI SendTargets検出処理に対してFully Qualified Domain Name（FQDN;完全修飾ドメイン名）を返すようにiSCSI LIFを設定できます。FQDNを返すように設定すると、ホストOSとストレージ サービスの間にNetwork Address Translation（NAT;ネットワークアドレス変換）デバイスがある場合に便利です。

タスク概要

IPアドレスはNATデバイスを挟んだ反対側では認識されませんが、FQDNであれば両方で認識されます。

FQDN値の互換性のある最大文字数は、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スペース割り当ての有効化

ONTAPのスペース割り当て機能は、LUNや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利用できるようにします。

ONTAPのスペース割り当てサポートは、SANプロトコルとONTAPのバージョンに基づいています。ONTAP 9.16.1以降では、新規作成されたLUNとすべてのネームスペースに対して、iSCSI、FC、NVMeプロトコルのスペース割り当てがデフォルトで有効になっています。

ONTAPのバージョン	プロトコル	スペース割り当てのサポート
9.16.1以降	• iSCSI • FC • NVMe	新しく作成されたLUNとすべてのネームスペースに対してデフォルトで有効
9.15.1	• iSCSI • FC	新規作成されたLUNについてデフォルトで有効
	NVMe	サポート対象外
9.14.1以前	• iSCSI • FC	新規作成されたLUNについてデフォルトで無効
	NVMe	サポート対象外

スペース割り当てが有効になっている場合の処理は、以下のとおりです。

- LUNまたはネームスペースでスペースが不足すると、ONTAPからホストに対して、書き込み処理に使用できる空きスペースがないことが通知されます。このとき、LUNまたはネームスペースはオンライン状態を維持し、読み取り処理は継続されます。ホストの設定に応じて、成功するまでホストが書き込み処理を再試行するか、ホスト ファイルシステムがオフラインに切り替わります。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には、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は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ために、ホストでLUNデバイスを再スキャンする必要が生じる場合もあります。

- ホストはSCSIまたはNVME `UNMAP`（`TRIM`とも呼ばれる）操作を実行できます。UNMAP操作により、ホストは有効なデータが含まれていないため不要になったデータブロックを識別できます。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、そのスペースを他の場所で使用できるようにします。この割り当て解除により、特にデータの回転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、書き込みが完了できない場合にスペース割り当てエラーを適切に処理できるホスト構成が必要です。SCSIまたはNVME `UNMAP`を活用するには、SCSI SBC-3規格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のシンプロビジョニングに対応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
- Windows

タスク概要

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、ONTAP 9.13.1でスペース割り当てが無効なVMwareホストにLUNが作成されていた場合、ONTAP 9.15.1にアップグレードしたあとも、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。

一部のホスト構成（VMware ESXiの一部のバージョンを含む）では、設定変更が自動的に認識されるため、ユーザーの介入は必要ありません。その他の構成では、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およびボリュームマネージャでは、 `SCSI UNMAP`を使用したスペース再利用を有効にするために、追加の特定の設定が必要になる場合があります。ファイルシステムの再マウントまたはOSの完全な再起動が必要になる場合があります。手順については、お使い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、ホストで以下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
   ```

   正しい値は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
   ```

   正しい値は1です。

関連リンク

"ONTAPを使用したESXi 8.xのNVMe-oFホスト設定"についての詳細をご覧ください。

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 **-** 概要

アプリケーションや管理要件に応じて、使用できるFlexVolボリュームとファイルまたはLUN構成の特定の組み合わせがあります。これらの組み合わせの利点とコストを理解することで、環境に最適なボリュームとLUN構成の組み合わせを決定できます。

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

上記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することができます。

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がありません。

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がありません。
- スペースは使用時に初めて割り当てられます。

費用と制限事項：

- 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した場合は失敗することがあります。
- 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。

費用と制限事項：

- 書き込み処理が失敗する可能性があります。

  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。

- スナップショット、FlexCloneファイル、LUNなどのデータ保護オブジェクトの保持に依存することはできません。
- 自動的に削除できないONTAPのブロック共有Storage Efficiency機能（重複排除、圧縮、ODX / コピー オフロードなど）は使用できません。

環境に適したボリュームと**LUN**の構成の組み合わせの決定

使用する環境に関するいくつかの基本的な質問に答えることで、環境に最も適したFlexVolとLUNの設定を決定できます。

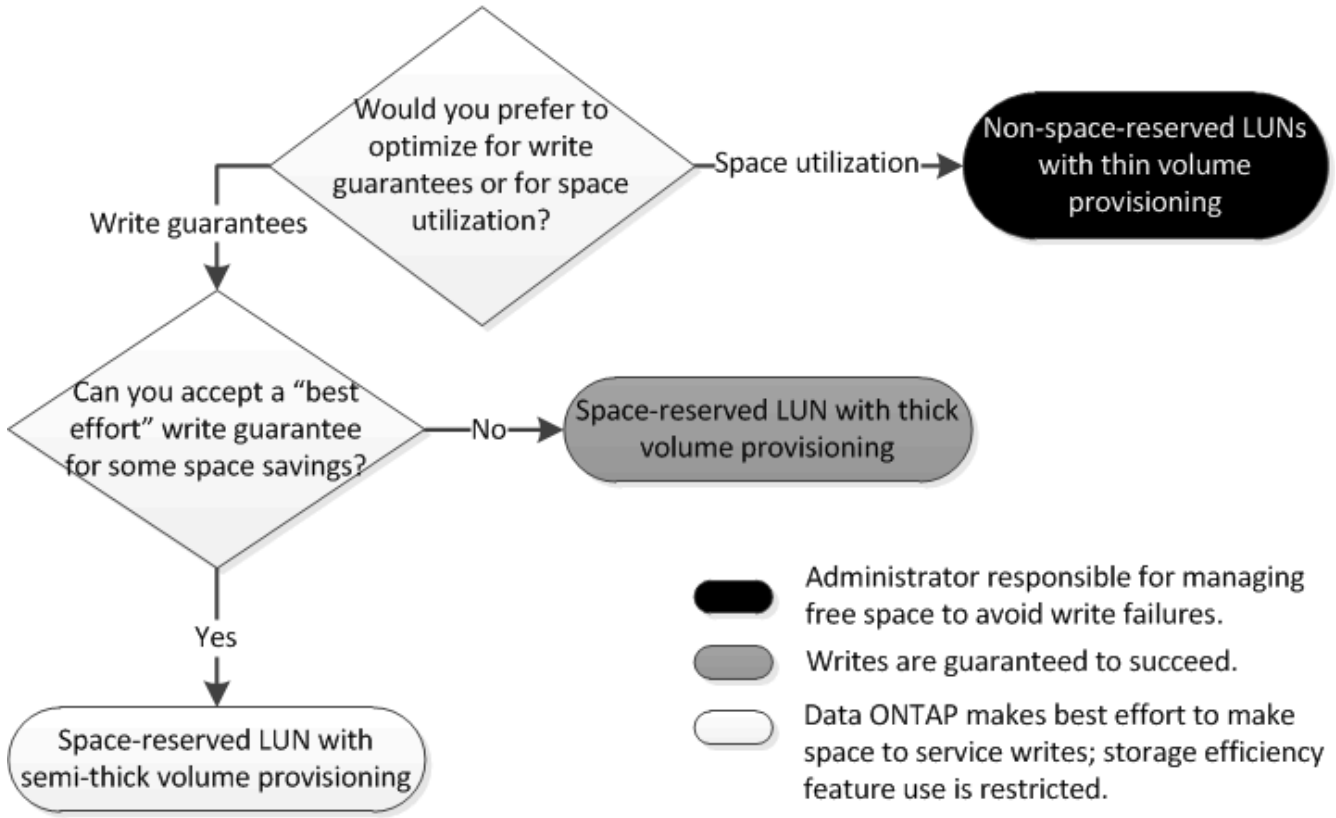
タスク概要

LUNとボリュームの設定は、ストレージ利用率を最大限に高めるため、または書き込みを確実に保証するために最適化することができます。ストレージの利用要件と、空きスペースを監視し迅速に補充するための要件に基づいて、ご使用の環境に適したFlexVolボリュームとLUNボリュームを決める必要があります。

LUNごとに個別のボリュームを設定する必要はありません。

手順

1. 次のデシジョン ツリーを使用して、環境に最も適したボリュームと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

スペース予約済みLUNを使用するか、スペース予約なしLUNを使用するかを判断するには、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。

タスク概要

データの増加率が一定して高い場合は、スペース リザーブLUNの使用が適しています。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。

データの増加率は、OnCommand Insightなどのツールで計算できるほか、手動でも計算できます。手動で計

算する手順を次に示します。

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、たとえば1週間、LUN上のデータを監視します。

   データ量の定期的な増加を示す代表的なサンプルを得られるように、十分な監視期間を確保してください。たとえば、毎月末に一貫してデータ量が増加する場合があります。

3. 期間中は毎日、増加したデータ量をGB単位で記録します。
4. 監視期間の最終日に、各日の合計を合算し、監視期間の日数で割ります。

   これで平均増加率が算出されます。

例

たとえば、200GBのLUNが必要であるとします。LUNを1週間監視し、毎日のデータの変化を記録しました。記録内容は次のとおりです。

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

この例では、増加率は（20+18+17+20+20+23+22）/ 7 = 1 日あたり 20 GB となります。

シックプロビジョニングされたボリュームを持つスペース予約ファイルまたは**LUN**の構成設定

このFlexVol volumeとファイルまたはLUN構成の組み合わせにより、ストレージ効率化テクノロジを使用でき、十分なスペースが事前に割り当てられるため、空きスペースを積極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LUNを設定するには、次の設定が必要です。

ボリューム設定	**Value**
保証	Volume
フラクショナル リザーブ	100
Snapshotリザーブ	any

ボリューム設定	**Value**
Snapshotの自動削除	オプション
自動拡張	オプション。有効にすると、アグリゲートの空きスペースをアクティブに監視する必要があります。

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

スペース予約されていないファイルまたはシンプロビジョニング ボリュームを持つ **LUN** 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、事前に割り当てる必要があるストレージの量は最小限ですが、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アクティブ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。

ボリューム設定	**Value**
保証	なし
フラクショナル リザーブ	0
Snapshotリザーブ	any
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	**Value**
スペース リザベーション	無効

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ことがあります。

ボリュームとアグリゲートの両方の空きスペースをアクティブに監視しない場合は、ボリュームの自動拡張を有効にし、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ます。この設定では、アグリゲートの空きスペースをアクティブ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設定

このFlexVolボリュームとファイルまたはLUNの構成の組み合わせでは、完全プロビジョニングの組み合わせよりも事前に割り当てるストレージ容量が少なくなりますが、ボリュームに使用できる効率化テクノロジーに制限があります。この構成の組み合わせでは、上書きはベストエフォート方式で実行されます。

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。

ボリューム設定	**Value**
保証	Volume
フラクショナル リザーブ	0
Snapshotリザーブ	0
Snapshotの自動削除	オン。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含め、トリガーをvolumeに設定し、すべてのFlexClone LUNおよび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。有効にすると、アグリゲートの空きスペースをアクティブに監視する必要があります。

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

テクノロジに関する制限事項

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および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。

- その LUN をサポートするボリュームの空き容量が少なくなると、保護データ（FlexClone LUN とファイル、スナップショット）が破棄されます。
- 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プラットフォームでセミシック 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データ保護

SAN環境向けのONTAPデータ保護方法について学習します

データを保護するには、データのコピーを作成して、誤ってデータを削除してしまった場合、アプリケーションがクラッシュした場合、データが破損した場合、災害が発生した場合にそのコピーをリストアできるようにします。データ保護およびバックアップのニーズに応じて、ONTAPは、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の正式版以降では、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）によって、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することができます。SnapMirrorアクティブ同期を利用するには、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 Mediator 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

LUNの複数のバックアップを手動または自動で作成、スケジュール設定、維持できます。スナップショットは最小限の追加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発生しません。LUNデータが誤って変更または削除された場合でも、最新のスナップショットから簡単かつ迅速にデータを復元できます。

FlexClone LUN（**FlexClone**のライセンスが必要）

アクティブボリュームまたはスナップショット内の別のLUNの、ポイントインタイムで書き込み可能なコピーを提供します。クローンとその親は、互いに影響を与えることなく個別に変更できます。

SnapRestore（ライセンスが必要）

ボリューム全体のスナップショットから、高速でスペース効率に優れた、オンデマンドのデータリカバリを実行できます。SnapRestoreを使用すると、ストレージシステムを再起動することなく、LUNを以前の保存状態に復元できます。

データ保護ミラー コピー（**SnapMirror**のライセンスが必要）

非同期の災害復旧機能を提供します。ボリューム上のデータのスナップショットを定期的に作成し、それらのスナップショットをローカルエリアネットワークまたは広域ネットワーク経由でパートナーボリューム（通常は別のクラスター上）にコピーし、保持することができます。パートナーボリューム上のミラーコピーにより、ソースボリューム上のデータが破損または失われた場合でも、最後のスナップショット時点からデータを迅速に利用および復元できます。

SnapVaultバックアップ（**SnapMirror**のライセンスが必要）

ストレージ効率が高く、バックアップを長期保存できます。SnapVault関係により、ボリュームの選択したSnapshotを宛先ボリュームにバックアップし、バックアップを保持できます。

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へのアクセスを構成し、LUNを管理し、WindowsまたはUNIXホストから直接ストレージシステムのスナップショットを管理します。

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"

ONTAPスナップショットから単一のLUNを復元する

スナップショットから単一のLUNを復元できます。そのLUNを含むボリューム全体を復元する必要はありません。LUNは、ボリューム内の既存の場所または新しいパスに復元できます。この操作では、ボリューム内の他のファイルやLUNに影響を与えることなく、単一のLUNのみが復元されます。ストリームを含むファイルを復元することもできます。

開始する前に

- 復元操作を完了するには、ボリュームに十分な空き容量が必要です：
  - 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、リストアするLUNと同じサイズのスペースが必要です。
  - 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、リストアするLUNの2倍のサイズのスペースが必要です。
  - スペース リザーブなしのLUNをリストアする場合、リストアするLUNが実際に使用しているサイズのスペースのみが必要です。
- デスティネーション LUN のスナップショットが作成されている必要があります。

  復元操作が失敗した場合、復元先の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 のスナップショットが作成されている必要があります。

  稀に、LUNの復元に失敗し、ソースLUNが使用できなくなる場合があります。このような場合は、スナップショットを使用して、LUNを復元試行直前の状態に戻すことができます。

- デスティネーション LUN とソース LUN の OS タイプは同じである必要があります。

  復元先 LUN の OS タイプが復元元 LUN と異なる場合、復元操作後にホストは復元先 LUN へのデータ アクセスを失う可能性があります。

手順

1. ホストから、LUNへのすべてのホスト アクセスを停止します。
2. ホストが LUN にアクセスできないように、ホスト上の LUN をアンマウントします。
3. 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>
```

4. LUN を復元するスナップショットを決定します：

```
volume snapshot show -vserver <SVM_name> -volume <volume_name>
```

5. LUN を復元する前に、LUN のスナップショットを作成します：

```
volume snapshot create -vserver <SVM_name> -volume <volume_name>
-snapshot <snapshot_name>
```

6. ボリューム内の指定されたLUNを復元します：

```
volume snapshot restore-file -vserver <SVM_name> -volume <volume_name>
-snapshot <snapshot_name> -path <lun_path>
```

7. 画面上の手順に従います。
8. 必要に応じて、LUNをオンラインにします。

```
lun modify -vserver <SVM_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 <SVM_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。

ONTAPスナップショットからボリューム内のすべてのLUNを復元する

`volume snapshot restore`コマンドを使用して、スナップショットから指定されたボリューム内のすべてのLUNを復元できます。

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。

   ボリューム内のLUNへのすべてのホスト アクセスを停止せずに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. ホストがLUNにアクセスできないように、そのホスト上のLUNをアンマウントします。
3. 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>
   ```

4. ボリュームを復元するスナップショットを決定します。

   ```
   volume snapshot show -vserver <SVM_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 <SVM_name> -volume <volume_name>
   -snapshot <snapshot_name>
   ```

7. 画面の指示に従ってください。
8. LUNを再マッピングします。

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

9. LUNがオンラインになっていることを確認します。

```
lun show -vserver <SVM_name> -path <lun_path> -fields state
```

10. LUNがオフラインの場合は、オンラインにします。

```
lun modify -vserver <SVM_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。

ONTAP FlexClone LUNでデータを保護する

FlexClone LUNは、アクティブボリュームまたはスナップショット内の別のLUNのポイントインタイムの書き込み可能なコピーです。クローンとその親は、互いに影響を与えることなく独立して変更できます。

FlexClone LUNを使用すると、LUNの読み書き可能なコピーを複数作成できます。

FlexClone LUNを作成する理由

- テストを目的としてLUNの一時的なコピーを作成する必要がある場合。
- 追加のユーザに本番データへのアクセスを許可することなくデータのコピーを提供する場合。
- 変更や開発用にデータベースのクローンを作成し、元のデータを未変更のまま残す場合。
- 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、あるいはファイル 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、それを元のLUNにコピーします。ただし、元のLUNの残りのデータは復元しません。これは、LUNとLUNのクローンの同時マウントをサポートするオペレーティング システムで機能します。SnapDrive for UNIXでは、`snap connect`コマンドでこれをサポートしています。
- 同じオペレーティング システムを使用する複数のSANブート ホストが必要な場合。

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は、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を作成することもできます。

LUNのクローンを作成すると、ブロック共有がバックグラウンドで発生し、ブロック共有が完了するまでボリューム Snapshotを作成することはできません。

FlexClone LUNの自動削除機能を有効にするには、`volume snapshot autodelete modify`コマンドを使用してボリュームを設定する必要があります。FlexClone LUNを自動削除したいのにボリュームがFlexClone自動削除に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を自動削除するには、各FlexClone LUNでこの機能を手動で有効にする必要があります。セミシックボリュームプロビジョニングを使用しており、このオプションが提供する「ベストエフォート」書き込み保証を利用するには、すべてのFlexClone LUNを自動削除対象にする必要があります。

> スナップショットからFlexClone LUNを作成すると、LUNは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スナップショットから自動的に分割されます。これにより、LUNがスナップショットに依存し続けたり、追加のスペースを消費したりすることがなくなります。このバックグラウンド分割が完了せずにこのスナップショットが自動的に削除された場合、そのFlexClone LUNのFlexClone自動削除機能を無効にしていても、そのFlexClone LUNは削除されます。バックグラウンド分割が完了した後は、そのスナップショットが削除されてもFlexClone LUNは削除されません。

関連情報

- "FlexClone LUNを作成する"
- "FlexVol volumeを構成してFlexClone LUNを自動的に削除する"
- "FlexClone LUN が自動的に削除されないようにする"

SAN環境でのSnapVaultバックアップの設定と使用

SAN環境でのONTAP SnapVaultバックアップについて学ぶ

SAN環境でSnapVaultを設定し、使用する方法は、NAS環境の場合とほぼ同じですが、SAN環境でLUNをリストアする場合は、いくつか特別な手順を踏む必要があります。

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 ボリュームの間でSnapVault関係を作成して初期化する手順は、ファイル プロトコルに使用されるFlexVolボリュームで使用される手順と同じです。この手順の詳細については、"データ保護"を参照してください。

スナップショットを作成して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を使用してスナップショットの作成を自動化することで、バックアップされたLUNが完全な状態になり、元のアプリケーションで使用可能になります。

SnapVaultセカンダリ ボリュームからLUNをリストアする場合には、3つの基本の選択肢があります。

- 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は読み取り専用であり、SnapVaultバックアップ内の最新のスナップショットからのみマッピングできます。永続的な予約やその他のLUNメタデータは失われます。必要に応じて、ホスト上のコピープログラムを使用して、LUNの内容を元のLUNにコピーし直すことができます（元のLUNにまだアクセス可能な場合）。

  コピーしたLUNのシリアル番号は、元のLUNのものとは異なります。

- SnapVault セカンダリ ボリューム内の任意のSnapshotを新しい読み取り/書き込みボリュームに複製できます。

  続いて、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可能であれば、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にコピーできます。

- SnapVaultセカンダリ ボリュームの任意のSnapshotからLUNを含むボリューム全体をリストアできます。

  ボリューム全体を復元すると、ボリューム内のすべてのLUNとファイルが置き換えられます。スナップショットの作成以降に作成された新しいLUNは失われます。

  LUNでは、マッピング、シリアル番号、UUID、永続的予約が維持されます。

ONTAP SnapVaultバックアップから読み取り専用**LUN**コピーにアクセスする

SnapVaultバックアップ内の最新のスナップショットから、LUNの読み取り専用コピーにアクセスできます。LUN ID、パス、シリアル番号はソースLUNとは異なるため、事前にマッピングする必要があります。永続的予約、LUNマッピング、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。

開始する前に

- SnapVault関係を初期化する必要があり、SnapVaultセカンダリ ボリュームの最新のSnapshot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。
- 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、あらかじめSnapVault SVMにigroupを作成しておきます。

  SnapVault セカンダリ ボリュームから、LUN を含むボリュームを最初にリストアまたはクローニングすることなく、LUN に直接アクセスできます。

タスク概要

SnapVault セカンダリ ボリュームに新しいスナップショットが追加されたときに、以前のスナップショットから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は同じ識別子でマッピングされたままですが、データは新しいスナップショットから取得されます。LUNのサイズが変更されると、一部のホストでは自動的にサイズ変更が検出されますが、Windowsホストではサイズ変更を検出するためにディスクの再スキャンが必要です。

手順

1. SnapVault セカンダリ ボリュームで使用可能なLUNをリストします。

   ```
   lun show
   ```

   この例では、プライマリ ボリューム srcvolA の元の LUN とSnapVault セカンダリ ボリューム dstvolB のコピーの両方を確認できます。

```
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.
```

`lun show`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/lun-show.html["ONTAPコマンド リファレンス"^]を参照してください。

2. 目的のホストの igroup が SnapVault セカンダリ ボリュームを含む SVM にまだ存在しない場合は、igroup を作成します。

```
igroup create -vserver <SVM_name> -igroup <igroup_name> -protocol
<protocol> -ostype <ostype> -initiator <initiator_name>
```

このコマンドは、iSCSI プロトコルを使用する Windows ホストの 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. 必要な LUN コピーを igroup にマップします。

```
lun mapping create -vserver <SVM_name> -path <LUN_path> -igroup
<igroup_name>
```

```
cluster::> lun mapping create -vserver vserverB -path /vol/dstvolB/lun_A
  -igroup temp_igroup
```

`lun mapping create`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/lun-mapping-create.html["ONTAPコマンド リファレンス"^]を参照してください。

4. ホストをLUNに接続し、必要に応じてLUNの内容にアクセスします。

ONTAP SnapVaultバックアップから単一の**LUN**を復元する

単一のLUNを新しい場所または元の場所に復元できます。SnapVault セカンダリ ボリューム内の任意のSnapshotから復元できます。LUNを元の場所に復元するには、まず新しい場所に復元してからコピーします。

開始する前に

- SnapVault関係を初期化する必要があり、SnapVaultセカンダリ ボリュームには復元する適切なスナップショットが含まれている必要があります。
- SnapVault セカンダリ ボリュームを含むStorage Virtual Machine（SVM）には、LUNコピーへのアクセスに使用されるホストからアクセス可能な、必要なSANプロトコルを備えた1つ以上のLIFが必要です。
- igroup は SnapVault SVM 上にすでに存在している必要があります。

タスク概要

このプロセスには、SnapVaultセカンダリ ボリュームのSnapshotから読み書き可能なボリューム クローンを作成することが含まれます。クローンから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とは異なります。永続的な予約は保持されません。

手順

1. 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。

```
snapmirror show
```

```
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. LUN を復元するスナップショットを特定します。

```
volume snapshot show
```

```
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. 目的のスナップショットから読み書き可能なクローンを作成する

```
volume clone create -vserver <SVM_name> -flexclone <flexclone_name>
-type <type> -parent-volume <parent_volume_name> -parent-snapshot
<snapshot_name>
```

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。クローンを格納するには、アグリゲート内に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. ボリューム クローン内の LUN を一覧表示します。

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

```
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.
```

`lun show`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/lun-show.html["ONTAPコマンド リファレンス"^]を参照してください。

5. SnapVaultバックアップを含むSVM上に目的のホストのigroupがまだ存在しない場合は、igroupを作成します。

```
igroup create -vserver <SVM_name> -igroup <igroup_name> -protocol
<protocol> -ostype <os_type> -initiator <initiator_name>
```

この例では、iSCSIプロトコルを使用するWindowsホストの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
```

6. 必要な LUN コピーを igroup にマップします。

```
lun mapping create -vserver <SVM_name> -path <lun_path> -igroup
<igroup_name>
```

```
cluster::> lun mapping create -vserver vserverB
  -path /vol/dstvolB_clone/lun_C -igroup temp_igroup
```

`lun mapping create`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/lun-mapping-create.html["ONTAPコマンド リファレンス"^]を参照してください。

7. ホストを LUN に接続し、必要に応じて LUN の内容にアクセスします。

このLUNは読み取り/書き込み可能で、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、ホストは元のLUNとは異なるLUNとして認識します。

8. ホスト上のコピー 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。

関連情報

- "snapmirror show"

ONTAP SnapVaultバックアップからボリューム内のすべての**LUN**を復元する

ボリューム内の1つ以上のLUNをSnapVaultバックアップから復元する必要がある場合は、ボリューム全体を復元できます。ボリュームの復元は、ボリューム内のすべて

のLUNに影響します。

開始する前に

SnapVault関係を初期化する必要があり、SnapVaultセカンダリ ボリュームには復元する適切なスナップショットが含まれている必要があります。

タスク概要

ボリューム全体を復元すると、ボリュームはスナップショット作成時の状態に戻ります。スナップショット後にボリュームにLUNが追加された場合、そのLUNは復元プロセス中に削除されます。

ボリュームをリストアした後も、LUNはリストア直前にマッピングされていたigroupにマッピングされたままです。LUNのマッピングは、スナップショット時のマッピングと異なる場合があります。ホストクラスタからのLUNの永続的な予約は保持されます。

手順

1. ボリューム内のすべての LUN への I/O を停止します。
2. SnapVault セカンダリ ボリュームを含むセカンダリ ボリュームを確認します。

```
snapmirror show
```

```
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. 復元するスナップショットを特定します。

```
volume snapshot show
```

```
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. 使用するSnapshotを指定します。

```
snapmirror restore -destination-path <destination_path> -source-path
<source_path> -source-snapshot <snapshot_name>
```

復元に指定する宛先は、復元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 クラスター全体で LUN を共有している場合は、影響を受けるホストから LUN の永続的な予約を復元します。

SnapVaultバックアップからボリュームを復元する

次の例では、スナップショットの作成後に lun_D という LUN がボリュームに追加されました。スナップショットからボリューム全体を復元すると、lun_D は表示されなくなります。

`lun show`コマンド出力には、プライマリ ボリューム `srcvolA` 内の `LUN` と、それらの `LUN` の読み取り専用コピーが`SnapVault` セカンダリ ボリューム `dstvolB` にあることが表示されます。`SnapVault` バックアップには `lun_D` のコピーは存在しません。

```
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 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.
```

SnapVault セカンダリ ボリュームからボリュームがリストアされた後、ソース ボリュームには lun_D が含まれなくなります。リストア後もソース ボリュームの LUN はマッピングされたままなので、再マッピングする必要はありません。

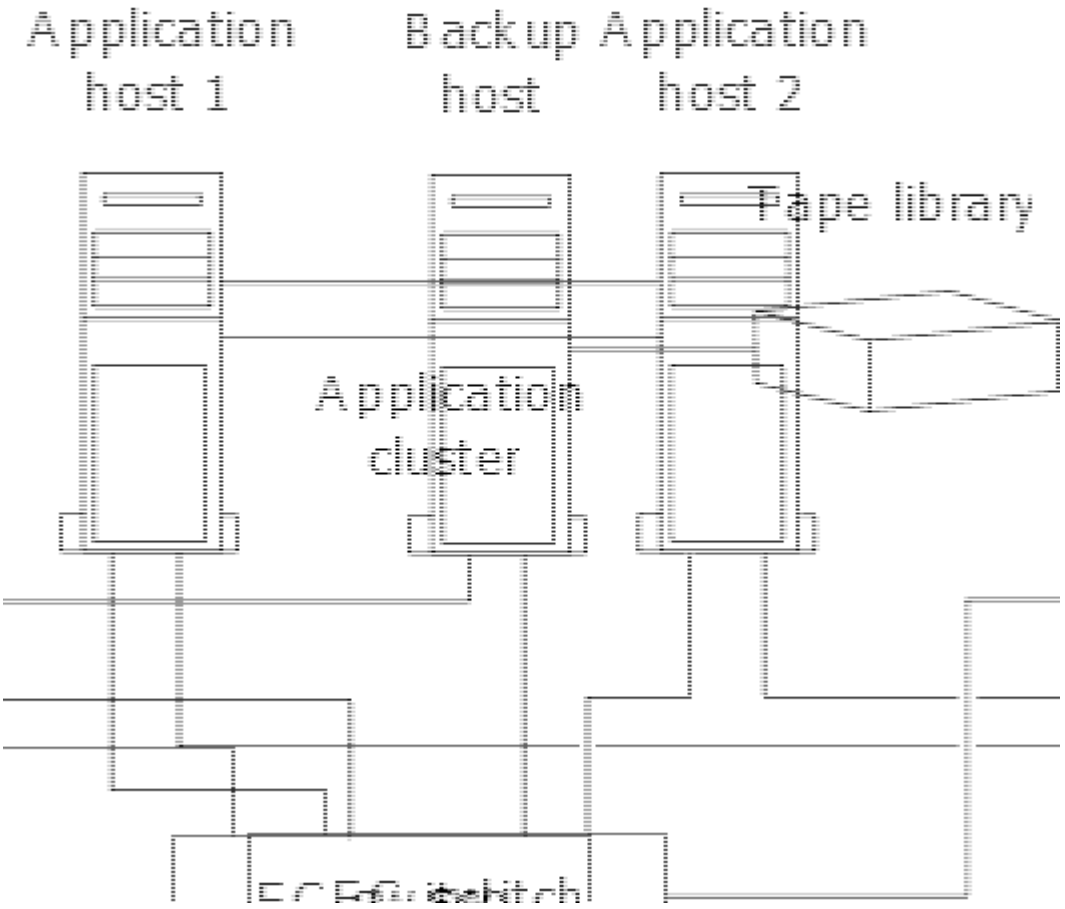
関連情報

- "snapmirror restore"
- "snapmirror show"

ホストバックアップシステムを**ONTAP**に接続するための推奨構成

テープへのSANシステムのバックアップは、アプリケーション ホストのパフォーマンス低下を避けるため、別のバックアップ ホストで実行できます。

バックアップのためには、SANとNetwork Attached Storage（NAS;ネットワーク接続型ストレージ）のデータは別々に保存することが不可欠です。次の図は、プライマリ ストレージ システムに接続するホスト バックアップ システムに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 システムに分散して設定することもできます。



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（HP-UXシステムのVxVMなど）を使用する複数のLUNで構成されます。

ホスト バックアップ システムを使用して、**ONTAP**ストレージ システム上の**LUN**を保護します。

スナップショットからクローンされたLUNをホスト バックアップ システムのソース データとして使用できます。

開始する前に

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 ノード名が含まれているigroupにマッピングされている必要があります。LUNはフォーマット済みで、ホストからアクセスできることが必要です。

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 for WindowsまたはSnapDrive for UNIXを使用できます。この手順をSANバックアップのプリプロセス スクリプトに組み込むこともできます。

2. 実稼働LUNのスナップショットを作成します。

```
volume snapshot create -vserver <SVM_name> -volume <volume_name>
-snapshot <snapshot> -comment <comment> -foreground false
```

3. 本番LUNクローンを作成します。

```
volume file clone create -vserver <SMV_name> -volume <volume> -source
-path <path> -snapshot-name <snapshot> -destination-path
<destination_path>
```

4. バックアップ サーバーの WWPN を含む igroup を作成します。

```
lun igroup create -vserver <SVM_name> -igroup <igroup> -protocol
<protocol> -ostype <os_type> -initiator <initiator>
```

5. 手順 3 で作成した LUN クローンをバックアップ ホストにマップします。

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

   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 スクリプトに組み込むことができます。

6. ホストから新しいLUNを検出して、ファイルシステムを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 スクリプトに組み込むことができます。

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クローン内にあるデータをテープにバックアップします。
8. LUNクローンをオフラインにします。

```
lun modify -vserver <SVM_name> -path <path> -state offline
```

9. LUNクローンを削除します。

```
lun delete -vserver <SVM_name> -volume <volume> -lun <lun_name>
```

10. スナップショットを削除します。

```
volume snapshot delete -vserver <SVM_name> -volume <volume> -snapshot
<snapshot>
```

SAN構成に関するリファレンス

ONTAP SAN構成について学ぶ

ストレージ エリア ネットワーク（SAN）は、iSCSIやFCなどのSAN転送プロトコルを介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。1つ以上のスイッチを介してホストにストレージ ソリューションを接続するように、SANを構成できます。iSCSIを使用している場合は、スイッチを使用せずにホストにストレージ ソリューションを直接接続するように、SANを構成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同時にストレージソリューションにアクセスできます。"選択的なLUNマッピング"と"ポートセット"を使用して、ホストとストレージ間のデータアクセスを制限できます。

iSCSIでは、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 トポロジをネットワークと呼びます。FC、FC / NVMe、FCoEでは、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 アクセスが失われるのを防ぐには、マルチネットワーク構成かマルチファブリック構成のHAペアで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単一のネットワーク / 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用のストレージをプロビジョニングする"、または"FC/NVMe用のストレージをプロビジョニングする"を実行できます。その後、ホストに接続してデータの処理を開始できます。

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、および構成によって異なります。具体的な構成の詳細については、"NetApp Interoperability Matrix Tool"を参照してください。

関連情報

- "SANの管理 - 概要"
- "NVMeの構成、サポート、制限事項"

iSCSI構成

ONTAPシステムでiSCSIネットワークを構成する

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"は、ホストがLUNにアクセスするために使用するアクティブ/最適化パスとアクティブ/非最適化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が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。サポートされてい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、"NetApp Interoperability Matrix Tool"で確認できます。

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ているので、マルチネットワーク構成が推奨されます。単一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は1つです。単一ネットワーク構成では、完全な冗長性は確保されません。

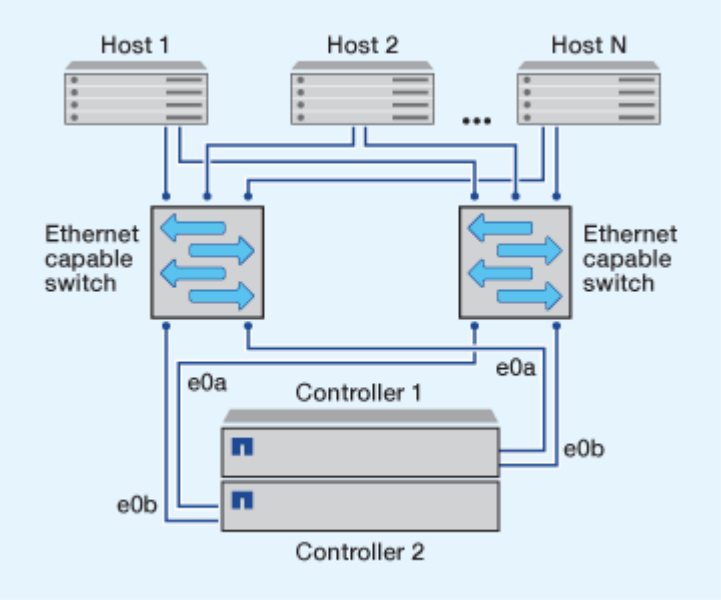
"単一ノード構成"は、フォールト トレランスと中断のない運用をサポートするために必要な冗長性が提供されないため、推奨されません。

関連情報

- "選択的 LUN マッピング（SLM）"が HA ペアが所有する LUN へのアクセスに使用されるパスを制限する方法について説明します。
- "SAN LIF"について学びましょう。
- "iSCSI における VLAN の利点"について学びましょう。

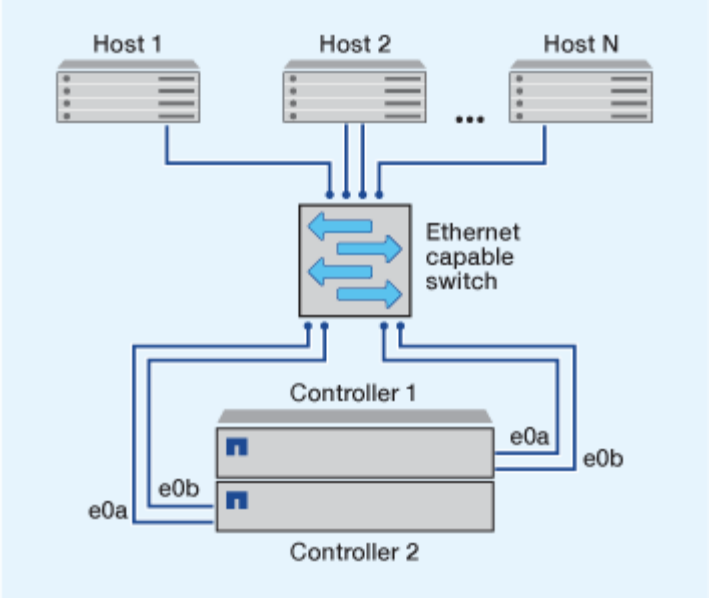
マルチネットワークの**iSCSI**構成

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つまたは複数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。



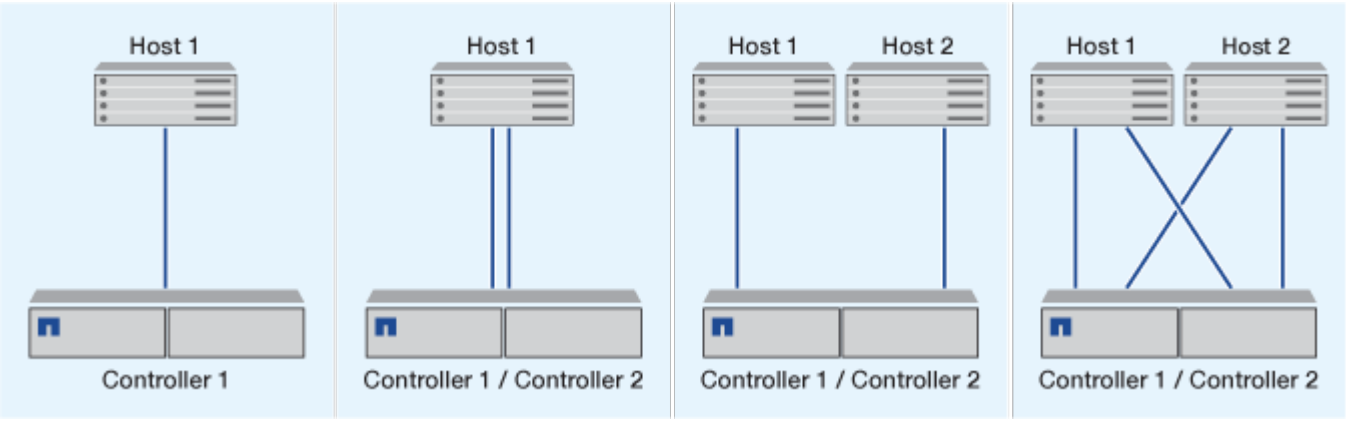
単一ネットワークの**iSCSI**構成

単一ネットワークのHAペア構成では、HAペアを1台のスイッチで1つまたは複数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。



直接接続型の**iSCSI**構成

直接接続型の構成では、1つまたは複数のホストをコントローラに直接接続します。



iSCSI構成の**ONTAP**システムで**VLAN**を使用する利点

VLANは、ブロードキャスト ドメインにまとめられたスイッチ ポートのグループで、単一のスイッチに配置することも、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。静的なVLANと動的なVLANを使用することで、IPネットワーク インフラにおけるセキュリティの強化、問題の切り分け、使用可能なパスの制限が可能になります。

大規模なIPネットワーク インフラにVLANを実装すると、次のようなメリットがあります。

- セキュリティの強化。

  VLANではイーサネット ネットワークやIP SANのノード間アクセスが制限されるため、既存のインフラを活用しつつセキュリティを向上させることができます。

- 問題を切り分けることで、イーサネット ネットワークやIP SANの信頼性が向上します。
- 問題の範囲が限定されるため、解決時間を短縮できます。

- 特定のiSCSIターゲット ポートへの利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に時間がかかります。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1つのパスのみを許可できます。

動的な**VLAN**

動的なVLANはMACアドレスに基づいています。VLANは、VLANに含めるメンバーのMACアドレスを指定して定義します。

動的なVLANは柔軟性に優れ、デバイスをスイッチに接続する物理ポートへのマッピングが必要ありません。ケーブルを別のポートに接続するたびにVLANを再設定する必要はありません。

静的な**VLAN**

静的なVLANはポートベースです。スイッチとスイッチ ポートを使用してVLANとそのメンバーが定義されます。

静的なVLANを使用すると、MAC（メディア アクセス制御）のスプーフィングを使用したVLANへの不正アクセスを防止できるため、セキュリティが向上します。ただし、第三者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 アドレスの構成を変更することでアクセスが可能になります。

環境によっては、動的なVLANよりも静的なVLANの方が簡単に作成および管理できます。静的なVLANでは、48ビットのMACアドレスを指定する必要がなく、スイッチとポートの識別子を指定するだけで済むためです。また、VLANの識別子をスイッチのポート範囲のラベルとして設定することもできます。

FCの構成

ONTAPシステムで**FC**または**FC-NVME**ファブリックを設定する

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。

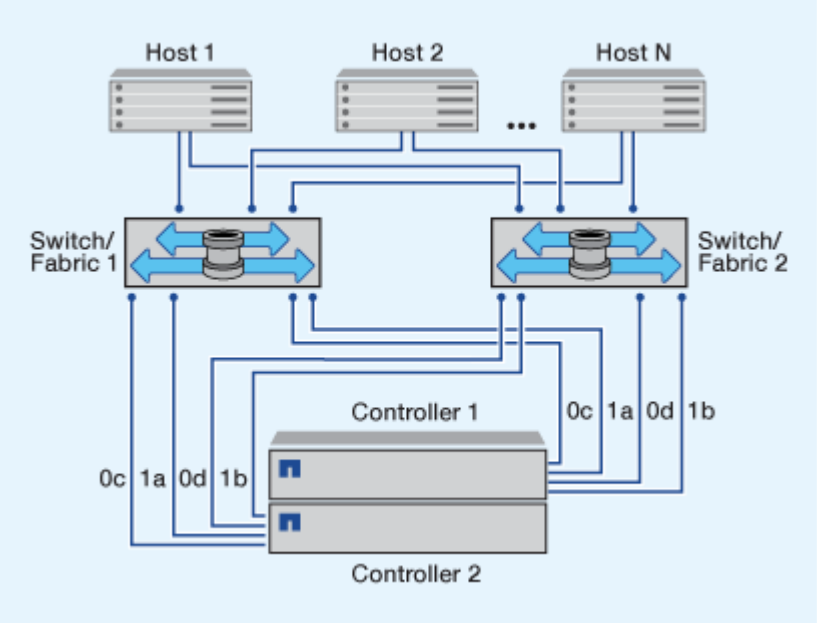
カスケード、部分メッシュ、フルメッシュ、コアエッジ、およびディレクタファブリックはすべて、FCスイッチをファブリックに接続するための業界標準の方法であり、すべてサポートされています。組み込みブレードスイッチを除き、異機種混在のFCスイッチファブリックの使用はサポートされていません。具体的な例外については、"Interoperability Matrix Tool"を参照してください。ファブリックは1つまたは複数のスイッチで構成でき、ストレージ コントローラは複数のスイッチに接続できます。

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、サポートされるマルチパス ソリューションをインストールおよび設定しておく必要があります。サポートされるオペレーティング システムおよびマルチパス ソリューションについては、Interoperability Matrix Toolを参照してください。

マルチファブリックのFCとFC-NVMeの構成

マルチファブリックのHAペア構成では、各HAペアを複数のスイッチで1つまたは複数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。

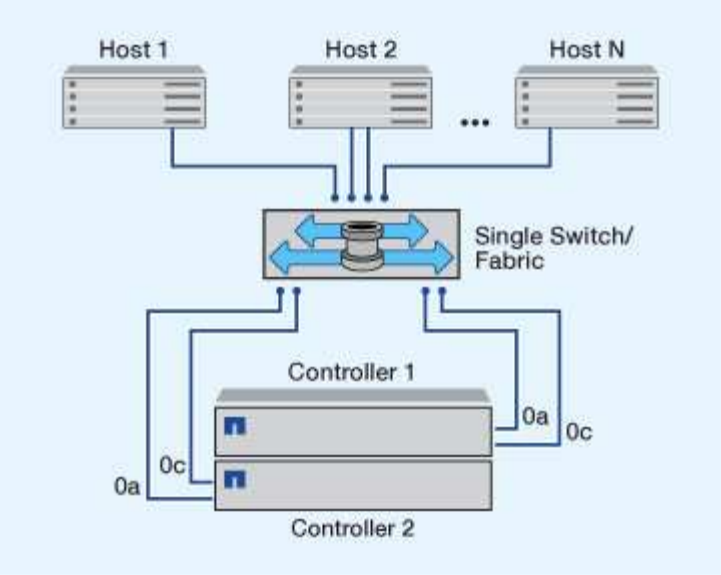


単一ファブリックのFCとFC-NVMeの構成

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つまたは複数のホストに接続します。ホストとコントローラが1台のスイッチで接続されるため、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、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。

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。



"単一ノード構成"は、フォールト トレランスと中断のない運用をサポートするために必要な冗長性が提供されないため、推奨されません。

関連情報

- "選択的 LUN マッピング（SLM）"が HA ペアが所有する LUN へのアクセスに使用されるパスを制限する方法について説明します。
- "SAN LIF"について学びましょう。

ONTAP システムで **FC** スイッチを構成するためのベストプラクティス

FCスイッチを構成するときは、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に従うことを推奨します。

FCスイッチの構成では、リンク速度を固定の値に設定すると効果的です。これは大規模なファブリックに特に適した方法で、ファブリックを再構築する際のパフォーマンスが最大限に高まり、時間を大幅に短縮することができます。自動ネゴシエーションは柔軟性に優れていますが、FCスイッチの構成では期待したパフォーマンスを常に得られるとは限らないため、全体の構築時間は長くなります。

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）がサポートされていて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。

サポートされている環境の詳細については、 "NetApp Interoperability Matrix Tool"を参照してください。

FCおよびiSCSIのベストプラクティスについては、 "NetAppテクニカルレポート4080：最新SANのベストプラクティス"を参照してください。

ONTAPシステムに推奨される**FC**ターゲット ポート構成と速度

FCターゲットポートは、FCプロトコルとまったく同じ方法でFC-NVMeプロトコル用に設定および使用できます。FC-NVMeプロトコルのサポートは、プラットフォームおよびONTAP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てください。

最高のパフォーマンスと最高の可用性を得るには、 "NetApp Hardware Universe"に記載されている特定のプラットフォームの推奨ターゲット ポート構成を使用する必要があります。

共有ASICを使用したFCターゲット ポートの構成

以下のプラットフォームには、共有ASIC（Application-Specific Integrated Circuit）を備え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を使用しないようにFCポートを設定する必要があります。

コントローラ	共有ASICを備えたポートペア	ターゲット ポート数：推奨ポート
• FAS8200 • AFF A300用	0g+0h	1: 0g 2: 0g、0h
• FAS2720 • FAS2750 • 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、異なる速度で動作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 ポートは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、接続先のデバイスの速度に合わせて設定してください。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に設定されたポートは、テイクオーバー/ギブバックなどの中断後の再接続に時間がかかる場合があります。

オンボード ポートと拡張アダプタは、以下の速度で実行するように構成できます。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。

4 Gbポート	8 Gbポート	16 Gbポート	32 Gbポート
• 4Gb • 2Gb • 1Gb	• 8Gb • 4Gb • 2Gb	• 16Gb • 8Gb • 4Gb	• 32Gb • 16Gb • 8Gb

サポートされているアダプタとその速度の完全なリストについては、 "NetApp Hardware Universe"を参照してください。

ONTAP FCアダプタ ポートを設定する

オンボードFCアダプタと一部のFC拡張アダプタカードは、イニシエーターポートまたはターゲットポートとして個別に設定できます。その他のFC拡張アダプタは、工場出荷時にイニシエーターまたはターゲットとして設定されており、変更できません。FC SFP+アダプタを搭載したサポート対象のUTA2カードを使用することで、追加のFCポートも利用できます。

イニシエータ ポートはバックエンド ディスク シェルフや、場合によっては外部ストレージ アレイに直接接続するために使用できます。ターゲット ポートは、FC スイッチへの接続にのみ使用できます。

FC用に設定されているオンボード ポートと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。サポートされるターゲット拡張アダプタもコントローラ モデルによって異なります。ご使用のコントローラ モデルでサポートされているオンボードFCポートとターゲット拡張アダプタの完全なリストについては、"NetApp Hardware Universe"を参照してください。

FCアダプタのイニシエータ モード設定

イニシエーター モードは、ポートをテープ ドライブ、テープ ライブラリ、または Foreign LUN Import（FLI）を使用したサードパーティのストレージに接続するために使用されます。

開始する前に

- アダプタのLIFを、メンバーとして属するすべてのポート 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、変更する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、移行するか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、システムの該当するアダプタ 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

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します。

FCアダプタをFCプロトコルとFC-NVMeプロトコル用に設定する手順は同じです。ただし、FC-NVMeをサポートしているのは一部のFCアダプタのみです。FC-NVMeプロトコルをサポートするアダプタの一覧については、"NetApp Hardware Universe"をご覧ください。

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、システムの該当するアダプタ 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アダプタの速度を設定する

自動ネゴシエーションを使用するのではなく、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に合わせて設定する必要があります。自動ネゴシエーションに設定されたポートは、テイクオーバー/ギブバックなどの中断後に再接続するまでに時間がかかる場合があります。

タスク概要

このタスクはクラスタ内のすべてのStorage Virtual Machine（SVM）とすべてのLIFを対象としているため、`-home-port`パラメータと `-home-lif`パラメータを使用して、この操作の範囲を制限する必要があります。これらのパラメータを使用しない場合、操作はクラスタ内のすべてのLIFに適用されるため、望ましくない可能性があります。

開始する前に

このアダプタをホームポートとして使用するすべてのLIFはオフラインである必要があります。

手順

1. このアダプタ上のすべての 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、システムの該当するアダプタ 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
```

アダプタの速度を最大速度を超えて変更することはできません。

4. アダプタの速度を変更します：

```
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. アダプタ上のすべての 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
```

FCアダプタを管理するための**ONTAP**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プロトコルとFC-NVMeプロトコルのFCアダプタの管理には、同じコマンドを使用します。

FCイニシエータアダプタ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コマンドを使

用する前に、 `run -node *node_name*`コマンドを使用する必要があります。

FC ターゲット アダプタを管理するためのコマンド

状況	使用するコマンド
ノード上のFCアダプタ情報を表示する	`network fcp adapter show`
FCターゲット アダプタパラメータを変更する	`network fcp adapter modify`
FCプロトコルのトラフィック情報を表示する	`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`
ディスプレイ アダプタの設定とステータス	`run -node *node_name* sysconfig -v *adapter*`
インストールされている拡張カードと構成エラーの有無を確認します	`run -node *node_name* sysconfig -ac`
コマンドのマニュアル ページを表示する	`man command_name`

FCイニシエータ アダプタを管理するためのコマンド

状況	使用するコマンド
ノード内のすべてのイニシエーターとそのアダプターの情報を表示します	`run -node *node_name* storage show adapter`
ディスプレイ アダプタの設定とステータス	`run -node *node_name* sysconfig -v *adapter*`
インストールされている拡張カードと構成エラーの有無を確認します	`run -node *node_name* sysconfig -ac`

オンボード **FC** アダプタを管理するためのコマンド

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する	`system node hardware unified-connect show`

関連情報

- "ネットワーク FCP アダプタ"

X1133A-R6アダプタを使用した**ONTAP**システムへの接続損失の回避

別のX1133A-R6 HBAへの冗長パスを構成することによって、ポート障害時に接続が切断されるのを回避できます。

X1133A-R6 HBAは、2つの2ポートペアで構成される4ポート、16Gb FCアダプタです。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。各2ポートペアは、1つのASICによってサポートされます（例：ポート1とポート2はASIC 1、ポート3とポート4はASIC 2）。1つの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。ペアをサポートしているASICでエラーが発生した場合、ペアの両方のポートはオフラインになります。

この接続の損失を防ぐには、個別のX1133A-R6 HBAへの冗長パス、またはHBA上の異なるASICでサポートされているポートへの冗長パスを使用してシステムを構成します。

FCoE構成

ONTAPシステムで**FCoE**ファブリックを構成する

FCoEは、FCoEスイッチを使用してさまざまな方法で構成できます。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す。完全な冗長性を提供し、ホスト側でマルチパス 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いくつでもFCoEスイッチとFCスイッチを配置できます。スイッチ同士を接続するためには、イーサネットISLをサポートするファームウェア バージョン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 システムが同じである必要はありません。

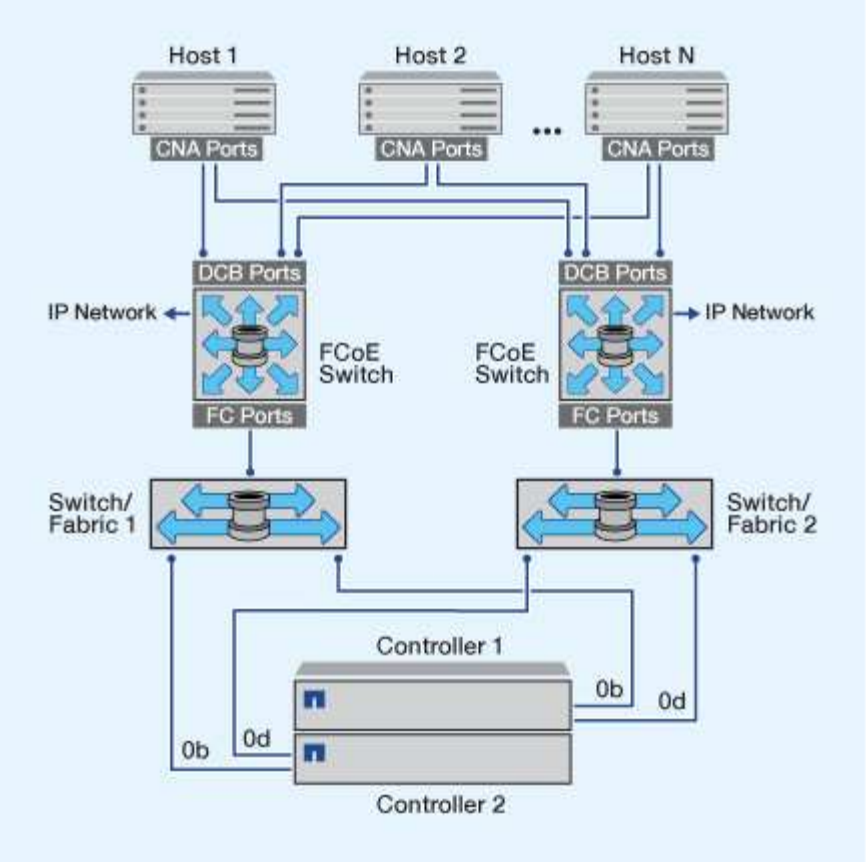
FCoE構成では、FCoEの機能を明示的にサポートするイーサネット スイッチが必要です。FCoE構成は、FCスイッチと同じ相互運用性と品質管理プロセスに照らして検証されます。サポートされる構成の一覧は、Interoperability Matrixを参照してください。これらのサポートされる構成には、スイッチ モデル、単一ファブリックに導入可能なスイッチの数、サポートされるスイッチ ファームウェアのバージョンなどのパラメータが含まれています。

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

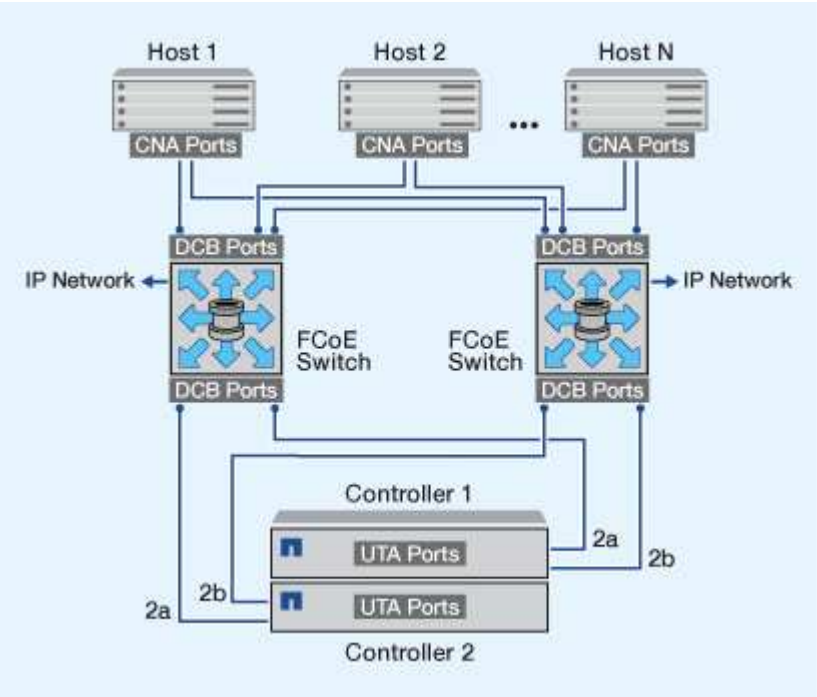
FCoEイニシエータ（CNA）を使用すると、FCoEスイッチを介して、ホストをHAペアの両方のコントローラのFCターゲット ポートに接続できます。FCoEスイッチにはFCポートも必要です。ホストのFCoEイニシエータは、常にFCoEスイッチに接続されます。FCoEスイッチは、FCターゲットに直接接続することも、FCスイッチを介してFCターゲットに接続することもできます。

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。



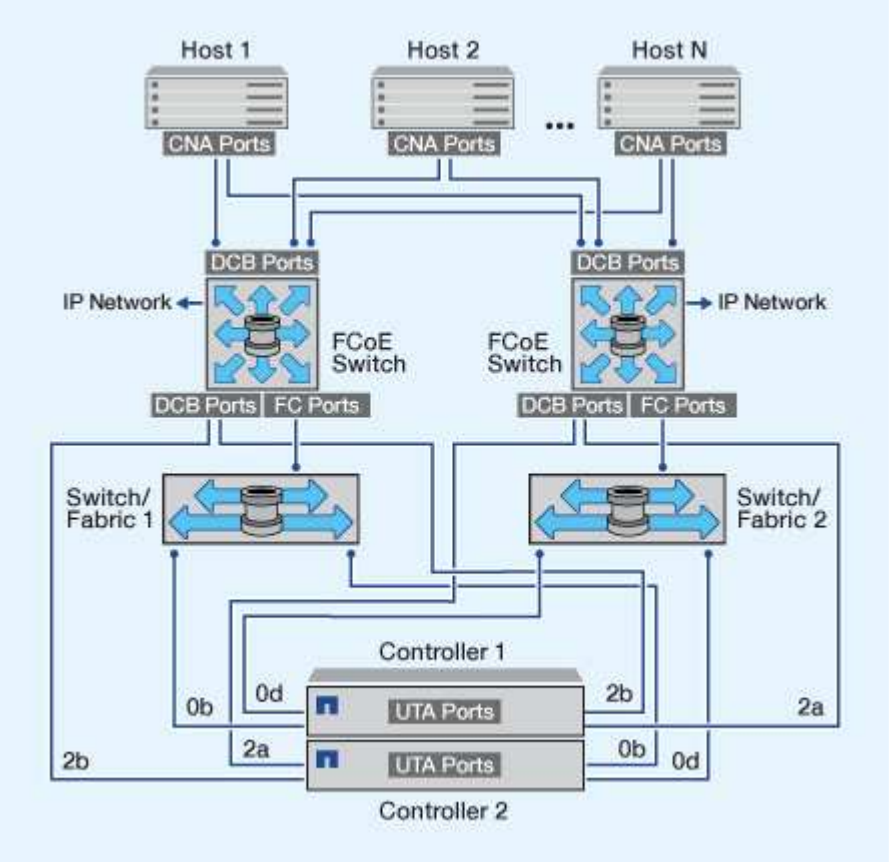
FCoEイニシエータから**FCoE**ターゲット

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。



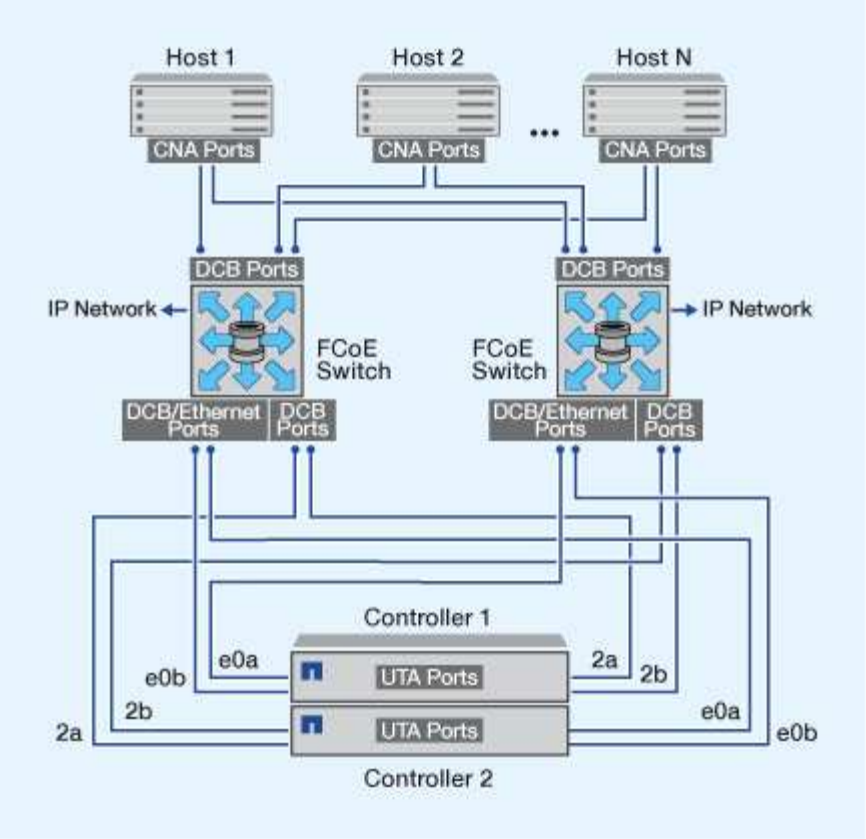
FCoEイニシエータから**FCoE**および**FC**ターゲット

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ポートでは、単一スイッチへの従来のリンク アグリゲーションは使用できません。Cisco製スイッチは、FCoEに対応した特別なタイプのリンク アグリゲーション（仮想ポート チャネル）をサポートします。仮想ポート チャネルが、2つのスイッチへの個別のリンクを統合（アグリゲート）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、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するポートでは、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。



ONTAPでサポートされる**FCoE**イニシエータとターゲット ポートの組み合わせ

FCoEおよび従来の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ターゲットのどちらとも組み合わせて使用できます。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	はい
FC	FCoE	はい
FCoE	FC	はい
FCoE	FCoE	はい

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、16Gbの各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 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。

この場合も、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が適用されます。

FCおよびFCoEゾーニング

ONTAPシステムによるFCおよびFCoEゾーニングについて学習します

FC、FC-NVMe、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。デバイスが互いを認識し、接続し、セッションを作成して通信できるようにするには、両方のポートが同じゾーンのメンバーである必要があります。

ゾーニングは、共通の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。同じゾーンに属さないポートは相互に通信できません。これにより、イニシエータHBA間の_クロストーク_が低減または排除されます。接続の問題が発生した場合、ゾーニングによって問題が特定のポートセットに切り分けられ、解決までの時間が短縮されます。

ゾーニングは、特定のポートへの利用可能なパス数を減らし、ホストとストレージ システム間のパス数を削減します。例えば、一部のホスト OS マルチパス ソリューションでは、管理可能なパス数に制限があります。ゾーニングは、ホストへのパス数がホスト OS で許可されている最大数を超えないように、ホストから見えるパス数を減らすことができます。

World Wide Nameに基づくゾーニング

ワールドワイドネーム（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。一部のスイッチベンダーではワールドワイドノードネーム（WWNN）ゾーニングが可能ですが、ONTAPでゾーニングを行う場合は、ワールドワイドポートネーム（WWPN）ゾーニングを使用する必要があります。

特定のポートを適切に定義し、NPIVを効果的に使用するには、WWPNゾーニングが必要です。FCスイッチは、ノード上の物理ポートのWWPNではなく、ターゲットの論理インターフェース（LIF）のWWPNを使用してゾーニングする必要があります。物理ポートのWWPNは「50」で始まり、LIFのWWPNは「20」で始まります。

WWPNゾーニングは柔軟性に優れており、デバイスをファブリックに接続する物理的な場所によってアクセスが制限されることがありません。ケーブルを別のポートに接続するたびにゾーンを再設定する必要はありません。

ONTAPシステムに推奨されるFCおよびFCoEゾーニング設定

ホストにマルチパス ソリューションがインストールされていない場合、4 台以上のホストが SAN に接続されている場合、またはクラスター内のノードに選択的 LUN マッピングが実装されていない場合は、ゾーニング設定を作成する必要があります。

推奨されるFCおよびFCoEゾーニング設定では、各ゾーンに1つのイニシエータ ポートと1つ以上のターゲットLIFが含まれます。この構成により、各ホスト イニシエータは任意のノードにアクセスできますが、同じノードにアクセスするホストが互いのポートを参照することはできません。

ストレージ仮想マシン（SVM）のすべてのLIFを、ホスト イニシエータのゾーンに追加します。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することなく、ボリュームまたはLUNを移動できます。

デュアル ファブリック ゾーニング設定

デュアルファブリックゾーニング設定は、単一コンポーネントの障害によるデータ損失を防ぐため、推奨されます。デュアルファブリック構成では、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内の各ノードに接続されます。1つのスイッチが使用できなくなった場合でも、残りのスイッチを介してデータアクセスが維持されます。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。

次の図では、ホストには2つのイニシエーターがあり、マルチパスソフトウェアが実行されています。2つのゾーンがあります。"選択的 LUN マッピング（SLM）"は、すべてのノードがレポートノードとして扱われるように設定されています。

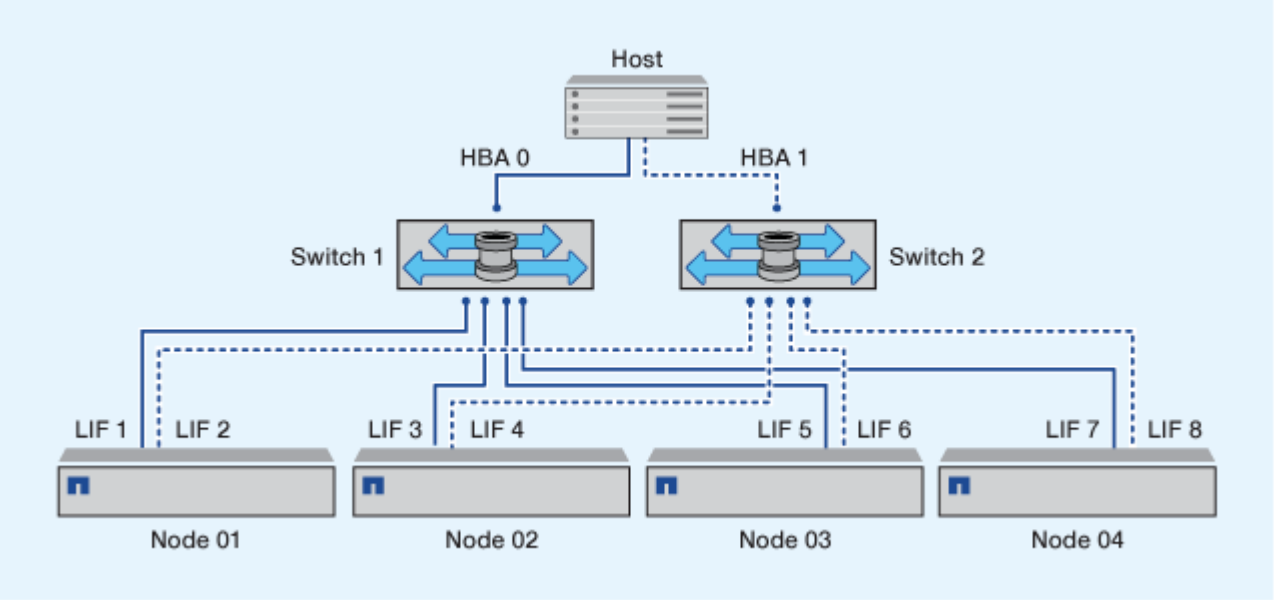
この図で使用されている命名規則は、ONTAPソリューションで使用できる一例です。

- 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ています。ゾーン1は、スイッチ1からアクセスされます。ゾーン2は、スイッチ2からアクセスされます。

各ホストは、すべてのノードのLIFにアクセスできます。これにより、ノードに障害が発生した場合でも、ホストはLUNに引き続きアクセスできます。SVMは、SLMレポートノードの設定に基づいて、クラスタ内のすべてのノードにあるすべての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設定を使用することで、SVMからホストへのパス数と、SVMからLUNへのパス数を削減できます。

構成にさらにノードが含まれる場合、追加ノードの LIF がこれらのゾーンに含まれます。



ホストOS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。

単一ファブリック構成では、各ホストイニシエータを単一のスイッチを介して各ストレージ ノードに接続します。単一ファブリックゾーニング設定は、単一コンポーネントの障害によるデータ損失に対する保護が提供されないため、推奨されません。単一ファブリックゾーニングを構成する場合、ソリューションの耐障害性を確保するために、各ホストにマルチパス用の2つのイニシエータを配置する必要があります。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。

各ホスト イニシエータは、イニシエータがアクセスできる各ノードから少なくとも 1 つの LIF を持つ必要があります。ゾーニングでは、LUN 接続のためのパスを提供するために、ホスト イニシエータからクラスタ内の HA ペア ノードへのパスを少なくとも 1 つ許可する必要があります。つまり、ホスト上の各イニシエータは、ゾーニング設定においてノードごとに 1 つのターゲット LIF のみを持つことができます。クラスタ内の同一ノードまたは複数のノードへのマルチパスが必要な場合は、各ノードのゾーニング設定においてノードごとに複数の LIF を持つことになります。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、ホストは引き続き LUN にアクセスできます。また、レポート ノードを適切に設定する必要があります。

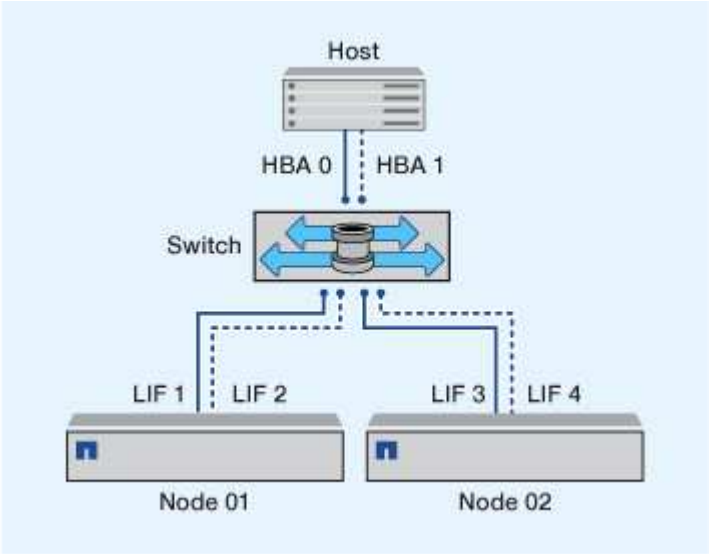
Cisco FC および FCoE スイッチを使用する場合、単一のファブリック ゾーンに同じ物理ポートに対して複数のターゲット LIF を含めることはできません。同じポートの複数の LIF が同じゾーンにある場合、LIF ポートは接続の切断から回復できない可能性があります。

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

構成にさらに多くのノードが含まれている場合、追加ノードの 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個の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OS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。

Cisco製FC / FCoEスイッチでのゾーニング制限

Cisco FC および FCoE スイッチを使用する場合、ゾーン内の物理ポートと論理インターフェイス（LIF）の使用には特定の制限が適用されます。

物理ポート

- FC-NVMeとFCは同じ32 Gb物理ポートを共有できる
- FC-NVMeとFCoEは同じ物理ポートを共有できません
- FC と FCoE は同じ物理ポートを共有できますが、プロトコル LIF は別々のゾーンに存在する必要があります。

論理インターフェース（**LIF**）

- ゾーンには、クラスタ内のすべてのターゲット ポートからの LIF を含めることができます。

  ホストに許可されているパスの最大数を超えないように、SLM設定を確認します。

- 特定のポート上の各LIFは、そのポート上の他のLIFとは別のゾーンに存在する必要があります。
- 異なる物理ポート上の LIF は同じゾーンに配置できます。

ONTAPおよび非NetAppシステムに接続されたSANホストの要件

共有SAN構成とは、ホストを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する構成です。単一のホストからONTAPストレージ システムと他社のストレージ システムに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。

いずれのホスト オペレーティング システムでも、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ことで、ドライバや設定が競合する可能性が低くなります。ONTAPストレージ システムへの接続には、NetApp Interoperability Matrix Toolにサポート対象として記載されたアダプタ 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。

要件や推奨事項に従って、タイムアウト値などのホストのストレージ パラメータを設定します。NetApp ソフトウェアのインストールやNetApp設定の適用は必ず最後に行ってください。

- 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、HP-UXのデフォルトのストレージ設定を使用します。
- 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します。

関連情報

"NetApp Interoperability Matrix Tool"

MetroCluster環境におけるSAN構成

ONTAP MetroCluster環境でサポートされるSAN構成

MetroCluster環境でSAN構成を使用する際の注意事項は次のとおりです。

- MetroCluster構成では、フロントエンドFCファブリックの「routed」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する場合は、"NetApp Interoperability Matrix Tool"（IMT）に記載されている注記に MetroCluster 構成に関する特別な考慮事項が含まれているかどうかを確認する必要があります。
- MetroClusterの自動計画外スイッチオーバーとTiebreakerまたはMediatorによって開始されるスイッチオーバーに対応するために、オペレーティング システムとアプリケーションに120秒のI/O耐障害性が必要です。
- 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を使用します。

関連情報

- "MetroClusterのデータ保護およびディザスタ リカバリの概要"
- "NetAppナレッジベース：MetroCluster構成におけるAIXホスト サポートの考慮事項は何ですか？"
- "NetAppナレッジベース：MetroCluster構成におけるSolarisホストのサポートに関する考慮事項"

ONTAP MetroClusterスイッチオーバーおよびスイッチバック中のポートの重複を回避する

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る際にポートの重複が起こらないように、フロントエンド スイッチを設定できます。

スイッチオーバー中に、ファブリック側でディザスタ サイトのFCポートがオフラインであることが検出されてネーム サービスとディレクトリ サービスから削除される前に、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場合があります。

ディザスタ サイトのFC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しようとすると、WWPNの重複によりログインが拒否される可能性があります。FCスイッチのこの動作は、既存のデバイスではなく前のデバイスのログインを優先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 タイプに合った正しい手順を実行してください。

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. 設定モードに入ります：

```
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. スイッチでNX-OS 8.xが実行されている場合は、flogi quiesce timeoutがゼロに設定されていることを確認します。

   a. quiesce timerval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がゼロになっていない場合は、timervalをゼロに設定します。

   ```
   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. `switchDisable`コマンドを入力します。
3. `configure`コマンドを入力し、プロンプトで `y`を押します。

```
 F-Port login parameters (yes, y, no, n): [no] y
```

4. 設定1を選択します。

```
- 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** キーを押します。
6. `switchEnable`コマンドを入力します。

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"

ONTAPによるSANホスト マルチパスのサポート

ONTAPは、FCホストとiSCSIホストの両方でのマルチパスに非対称論理ユニット アクセス（ALUA）ソフトウェアを使用します。

ONTAP 9.5以降では、非同期名前空間アクセス（ANA）を使用するNVMeホストで、マルチパス高可用性（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はホストからターゲットへのパスを1つしかサポートしないため、アプリケーションホストは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。

SANホストが複数のパスを介してLUNまたはNVMeネームスペースにアクセスできる場合、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またはNVMeネームスペースへのすべてのパスを単一のディスクとしてオペレーティングシステムに提示します。マルチパスソフトウェアがない場合、オペレーティングシステムは各パスを別々のディスクとして扱い、データ破損につながる可能性があります。

パスが複数あるとみなされるのは、次のいずれかに該当する場合です。

- ホストの1つのイニシエータ 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

マルチパス ソフトウェア（MPIO（マルチパスI/O）ソフトウェアとも呼ばれる）は、HA構成で推奨されます。選択的LUNマップに加えて、FCスイッチのゾーニングや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も推奨されます。

ALUA または ANA をサポートする特定のホスト構成については、ホスト オペレーティング システムの"NetApp Interoperability Matrix Tool"および "ONTAP SAN Host Configuration"を参照してください。

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本以下にしてください。また、ホストOSとホストで使用されるマルチパスでサポートできるパスの総数も超えないようにしてください。

クラスタ内のストレージ仮想マシン（SVM）によって使用される"選択的LUNマップ（SLM）"を介して各レポートノードに接続するLUNごとに、少なくとも2つのパスが必要です。これにより、単一障害点が排除され、コンポーネント障害が発生してもシステムが動作を継続できるようになります。

クラスタにノードが4つ以上ある場合や、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、推奨される最大数である8個以内になるようにすることができます。

- SLM

SLM は、ホストから LUN へのパスの数を、LUN を所有するノードとその HA パートナー上のパスのみに削減します。SLM はデフォルトで有効になっています。

- "ポートセット（iSCSIの場合）"
- ホストのFC igroupマッピング
- FCスイッチ ゾーニング

構成の制限

ONTAPクラスタごとにサポートされるノードと**SAN**ホストの最大数を決定する

クラスタあたりでサポートされるノード数は ONTAP のバージョン、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。クラスタに接続できる SAN ホストの最大数も、特定の構成によって異なります。

クラスタごとにサポートされる最大ノード数を決定する

クラスター内のいずれかのノードがFC、FC-NVMe、FCoE、またはiSCSI用に設定されている場合、そのクラスターはSANノードの制限に従います。クラスター内のコントローラに基づくノード制限は、_Hardware Universe_に記載されています。

手順

1. "NetApp Hardware Universe"に進みます。
2. 左上の*ホーム*の横にある*プラットフォーム*を選択し、プラットフォームの種類を選択します。
3. ONTAP のバージョンを選択します。

   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を選択します。
5. *仕様を選択*で、*すべて選択*の選択を解除します。
6. クラスターあたりの最大ノード数（**NAS/SAN**） を選択します。
7. *Show Results*をクリックします。

結果

選択したプラットフォームのクラスタあたりの最大ノード数が表示されます。

クラスタがより多くの**FC**ホストをサポートできるかどうかを判断する

FC および FC-NVMe 構成の場合、システム内のイニシエーター-ターゲット ネクサス（ITN）の数を使用して、クラスターにさら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。

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までの1つのパスを表します。FCおよびFC-NVMe構成では、ノードあたりのITNの最大数は2,048です。ITNの最大数を下回っている場合は、クラスターにホストを追加し続けることができます。

クラスターで使用されている ITN の数を確認するには、クラスター内の各ノードに対して次の手順を実行します。

手順

1. 特定のノード上のすべての LIF を識別します。
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
```

   コマンド出力の下部に表示されるエントリの数は、その LIF の ITN の数を表します。

3. 各 LIF に表示される ITN の数を記録します。
4. クラスタ内のすべてのノード上の各 LIF の ITN の数を追加します。

   この合計は、クラスター内の ITN の数を表します。

クラスタがより多くの**iSCSI**ホストをサポートできるかどうかを判断する

ノードに直接接続できるホストの台数、または1台以上のスイッチを介して接続できるホストの台数は、利用可能なイーサネットポートの数によって異なります。利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と、コントローラに搭載されているアダプタの数と種類によって決まります。コントローラと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。

すべてのマルチノード クラスタ構成において、クラスタにホストを追加できるかどうかを判断するには、ノードあたりの iSCSI セッション数を確認する必要があります。クラスタの iSCSI セッション数がノードあたりの最大セッション数を下回っている限り、クラスタにホストを追加し続けることができます。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種類によって異なります。

手順

1. ノード上のすべてのターゲット ポータル グループを特定します。
2. ノード上のすべてのターゲット ポータル グループの iSCSI セッションの数を確認します：

```
iscsi session show -tpgroup _tpgroup_
```

   コマンド出力の下部に表示されるエントリの数は、そのターゲット ポータル グループのiSCSIセッションの数を表します。

3. 各ターゲット ポータル グループに表示される iSCSI セッションの数を記録します。
4. ノード上の各ターゲット ポータル グループの iSCSI セッション数を追加します。

   合計はノード上のiSCSIセッションの数を表します。

オールフラッシュ**SAN**アレイ構成の制限とサポート

オールフラッシュSANアレイ（ASA）構成の制限とサポートは、ONTAPのバージョンによって異なります。

サポートされている構成制限に関する最新の詳細情報は、"NetApp Hardware Universe"で参照できます。

これらの制限はASAシステムに適用されます。ASA r2システム（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、ASA A20、またはASA C30）をご利用の場合は、"ASA r2 システムのストレージ制限"を参照してください。

SANプロトコルとサポートされるクラスタあたりのノード数

サポートされるSANプロトコルとクラスタあたりの最大ノード数は、MetroCluster以外の構成とMetroCluster構成のどちらを使用しているかによって異なります。

MetroCluster以外の構成

次の表は、MetroCluster以外の構成での、ASAでサポートされるSANプロトコルとクラスタあたりのノード数をまとめたものです。

ONTAPバージョン	プロトコルのサポート	クラスタあたりの最大ノード数
9.11.1	• NVMe/TCP • NVMe/FC	12
9.10.1	• NVMe/TCP	2
9.9.1	• NVMe/FC	2
	• FC • iSCSI	12
9.7	• FC • iSCSI	2

MetroCluster IP構成

次の表は、MetroCluster IP構成での、ASAでサポートされるSANプロトコルとクラスタあたりのノード数をまとめたものです。

ONTAPバージョン	プロトコルのサポート	クラスタあたりの最大ノード数
9.15.1	• NVMe/TCP	4ノードMetroCluster IP構成ではクラスタあたり2ノード
9.12.1	• NVMe/FC	4ノードMetroCluster IP構成ではクラスタあたり2ノード
9.9.1	• FC • iSCSI	8ノードMetroCluster IP構成ではクラスタあたり4ノード
9.7	• FC • iSCSI	4ノードMetroCluster IP構成ではクラスタあたり2ノード

永続ポートのサポート

ONTAP 9.8以降、FCプロトコルを使用するように設定されたオールフラッシュSANアレイ（ASA）では永続ポートがデフォルトで有効になります。永続ポートはFCでのみ使用でき、World Wide Port Name（WWPN）で識別されるゾーン メンバーシップが必要です。

永続ポートは、ハイアベイラビリティ（HA）パートナーの対応する物理ポートにシャドウLIFを作成することで、テイクオーバーの影響を軽減します。ノードがテイクオーバーされると、パートナー ノードのシャドウLIFにWWPNなどの元のLIFの識別情報が引き継がれます。テイクオーバーされたノードへのパスのステータスが「障害」に変更される前に、シャドウLIFがホストのMPIOスタックへのアクティブな最適パスとして表示され、I/Oが移行されます。これにより、ストレージ フェイルオーバー処理の実行中も含めてホストが認識するターゲットへのパス数は変わらないため、I/Oの中断が軽減されます。

永続ポートについては、FCPポートの次の特性がHAペア間で同じでなければなりません。

- FCPポートの数
- FCPポートの名前
- FCPポートの速度
- FCP LIFのWWPNベースのゾーニング

これらの特性のいずれかがHAペア間で同じでない場合、次のEMSメッセージが生成されます。

```
EMS : scsiblade.lif.persistent.ports.fcp.init.error
```

永続ポートの詳細については、"NetAppテクニカルレポート4080：最新SANのベストプラクティス"を参照してください。

ONTAPシステムで使用される**FC**スイッチの構成制限

Fibre Channel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の構成制限（上限）があります。各スイッチ ベンダーのドキュメントに、サポートされる制限が記載されています。

FCのスイッチ ポートには、各FCの論理インターフェイス（LIF）がログインします。ノードの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のログイン分の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数やその他の構成値の制限を超えないようにする必要があります。これは、NPIVが有効になっている仮想環境のホスト側で使用し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とイニシエータのどちらについても、スイッチ ベンダーが設定しているログイン数の制限を超えないようにしてください。

Brocadeスイッチの制限

Brocadeスイッチの構成制限については、_Brocade Scalability Guidelines_を参照してください。

Cisco Systemsスイッチの制限

Ciscoスイッチの設定制限については、 "Ciscoの構成制限に関するドキュメント"Ciscoスイッチ ソフトウェアのバージョンのガイドを参照してください。

ONTAPでサポートされる最大FCおよびFCoEホップ数

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）間のパスにおけるスイッチの数として定義されます。ホストとストレージシステム間でサポートされる最大FCホップ数は、スイッチの供給元によって異なります。

Cisco Systems のドキュメントでは、この値は *SAN* ファブリックの直径 とも呼ばれています。

FCoEでは、FCoEスイッチをFCスイッチに接続することができます。エンドツーエンドのFCoE接続では、イーサネットのスイッチ間リンク（ISL）に対応したファームウェア バージョンがFCoEスイッチで実行されている必要があります。

サプライヤーを切り替える	サポートされているホップ数
Brocade	• FCの場合は7 • FCoEの場合は5
Cisco	• FCの場合は7 • 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。

ONTAP FCホストのキュー深度を計算する

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。

タスク概要

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することができる、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。一般に、キュー深度が深い（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応答を返して受け取ったコマンドを拒否します。QFULL状態はシステム パフォーマンスの大幅な低下を招き、一部のシステムではエラーを引き起こすこともあります。そのため、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環境では、QFULLが発生しないように慎重に計画してください。

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たホスト間では、キュー深度に応じてリソースへのアクセスに差があり、キュー深度が小さいホストよりもキュー深度の大きいホストのアクセスが優先されます。

キューの深さの「`tuning`」については、次のような一般的な推奨事項があります。

- 小規模から中規模のシステムでは、HBAキュー深度を32にする。
- 大規模のシステムでは、HBAキュー深度を128にする。
- 例外的なケースまたはパフォーマンス テストでは、キュー深度を256にしてキュー関連の問題の発生を避ける。

- すべてのホストにアクセスが均等に保証されるよう、どのホストにも同程度のキュー深度を設定する。
- パフォーマンスの低下やエラーを避けるために、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。

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イニシエータの数を数えます。
2. 128をかけます。
   - 結果が2,048未満の場合は、すべてのイニシエーターのキュー深度を128に設定してください。ストレージコントローラーの2つのターゲットポートにそれぞれ1つのイニシエーターが接続されたホストが15台あります。15 × 128 = 1,920です。1,920はキュー深度の合計制限である2,048より小さいため、すべてのイニシエーターのキュー深度を128に設定できます。
   - 結果が2,048より大きい場合は、手順3に進みます。ストレージコントローラの2つのターゲットポートそれぞれに1つのイニシエーターが接続されたホストが30台あります。30 × 128 = 3,840です。3,840はキュー深度の合計制限である2,048より大きいため、手順3のいずれかのオプションを選択して修復する必要があります。
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分します。
     iii. 手順1と2を繰り返します。+ 必要なキュー深度3,840は、ポートあたりの利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、FCスイッチを再ゾーン化して、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台を別のポートセットに接続するようにします。これにより、ポートあたりのキュー深度は15 × 128 = 1,920に減少します。
   - オプション2：
     i. 予想される I/O ニーズに基づいて、各ホストを「`large`」または「`small`」として指定します。
     ii. 大規模イニシエータの台数に128をかけます。
     iii. 小規模イニシエータの台数に32をかけます。
     iv. 2つの計算結果を合算します。
     v. 結果が2,048未満の場合は、大規模ホストのキュー深度を128に設定し、小規模ホストのキュー深度を32に設定します。
     vi. 結果が依然としてポートあたり2,048を超える場合は、キューの深さの合計が2,048以下になるまで、イニシエーターあたりのキューの深さを減らします。

> 1秒間のI/O数（IOPS）による特定の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 = （IOPS）×（応答時間）
>
> たとえば、応答時間が3ミリ秒で1秒あたり40,000回のI/Oが必要な場合、必要なキューの深さは40,000 × (.003) = 120になります。

基本となる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。一方、キュー深度を128にした場合は、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。このように、1つのターゲット ポートでサポートできるホストの数はキュー深度が大きいほど少なくなります。キュー深度を小さくできないような要件がある場合は、その分ターゲット ポートを増やしてください。

必要なキュー深度3,840は、ポートあたりの利用可能なキュー深度を超えています。ストレージI/Oニーズが高い「large」ホストが10台と、I/Oニーズが低い「small」ホストが20台あります。大規模ホストのイニシエーター キュー深度を128に、小規模ホストのイニシエーター キュー深度を32に設定してください。

結果として得られるキューの合計深度は（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。

結果として、イニシエーターあたりのキューの深さは2,048÷30=68になります。

ONTAP SANホストのキュー深度を変更する

ノードあたりのITN数とFCポートのファンインの最大値を達成するには、ホスト上のキューの深さを変更する必要がある場合があります。環境に応じて"最適なキュー深度を計算する"できます。

AIXホスト

AIXホストのキュー デプスは、 `chdev`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は、再起動後も保持されます。

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
```

`num_cmd_elems`のデフォルト値は200です。最大値は2,048です。

`num_cmd_elems`を変更するには HBA をオフラインにして、 `rmdev -l fcs0 -R`コマンドと `makdev -l fcs0 -P`コマンドを使用してオンラインに戻す必要がある場合があります。

HP-UXホスト

HP-UXホスト上のLUNまたはデバイスのキュー深度は、カーネル パラメータ `scsi_max_qdepth`を使用して変更できます。HBAのキュー深度は、カーネル パラメータ `max_fcp_reqs`を使用して変更できます。

- `scsi_max_qdepth`のデフォルト値は8です。最大値は255です。

  `scsi_max_qdepth`は、 `kmtune`コマンドの `-u`オプションを使用して、実行中のシステムで動的に変更できます。変更はシステム上のすべてのデバイスに反映されます。例えば、LUNキューの深さを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
  ```

  > `scsictl`コマンドを使用して、個々のデバイスファイルのキュー深度を変更できます。 `scsictl`コマンドによる変更は、システムの再起動後には保持されません。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
  ```

- `max_fcp_reqs`のデフォルト値は512です。最大値は1024です。

  変更 `max_fcp_reqs`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ます。例えば、HBAキューの深さを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

SolarisホストのLUNおよびHBAのキュー深度を設定できます。

- LUNキューの深さの場合：ホストで使用中のLUNの数にLUNごとのスロットル（lun-queue-depth）を掛けた値は、ホストのtgt-queue-depth値以下である必要があります。
- Sunスタックのキュー深度について：ネイティブドライバでは、HBAレベルでLUNごとまたはターゲットごと `max_throttle`の設定はできません。ネイティブドライバの `max_throttle`値を設定する場合は、 `/kernel/drv/sd.conf`ファイルおよび `/kernel/drv/ssd.conf`ファイルでデバイスタイプ（VID_PID）ごとに設定することをお勧めします。ホストユーティリティは、MPxIO構成ではこの値を64、Veritas DMP構成では8に設定します。

手順

1. `# cd/kernel/drv`
2. `# vi lpfc.conf`
3. 検索する `/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. `sync; sync; sync; reboot -- -r`コマンドを使用してホストを再起動します。

VMwareホスト（**QLogic HBA**の場合）

`esxcfg-module`コマンドを使用してHBAタイムアウト設定を変更します。
`esx.conf`ファイルを手動で更新することは推奨されません。

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. `#vmkload_mod -l`コマンドを使用して、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の単一のインスタンスが1つの場合は、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。 `vmkload_mod -l`の出力に基づいて適切なモジュールを使用してください。

4. 次のコマンドを使用して変更内容を保存します。

   ```
   #/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内容を確認します。
   a. `#esxcfg-module -g qla2300_707`
   b. `qla2300_707 enabled = 1 options = 'ql2xmaxqdepth=64'`

VMwareホスト（**Emulex HBA**の場合）

`esxcfg-module`コマンドを使用してHBAタイムアウト設定を変更します。
`esx.conf`ファイルを手動で更新することは推奨されません。

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. `#vmkload_mod -l grep lpfc`コマンドを使用して、現在ロードされているEmulex HBAを確認します。
3. Emulex HBAのインスタンスが1つの場合は、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。上記のコマンドではlpfcdd_7xxモジュールを使用しています。 `vmkload_mod -l`の結果に応じて適切なモジュールを使用してください。

   このコマンドを実行すると、lpfc0で表されるHBAに対してLUNのキュー深度が16に設定されます。

4. Emulex HBAのインスタンスが複数の場合は、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に対するLUNのキュー深度とlpfc1に対するLUNのキュー深度が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. `#reboot`を使用して再起動します。

Windowsホスト（**Emulex HBA**の場合）

Windowsホストでは、 `LPUTILNT`ユーティリティを使用してEmulex HBAのキューの深さを更新できます。

手順

1. `C:\WINNT\system32`ディレクトリにある `LPUTILNT`ユーティリティを実行します。
2. 右側のメニューから*ドライブ パラメータ*を選択します。
3. 下にスクロールして*QueueDepth*をダブルクリックします。

> *QueueDepth*を150より大きく設定する場合は、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`

Windowsホスト（**Qlogic HBA**の場合）

Windows ホストでは、 `SANsurfer` 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。

手順

1. `SANsurfer` HBA マネージャー ユーティリティを実行します。
2. **HBA** ポート > 設定 をクリックします。
3. リスト ボックスで **Advanced HBA port settings** をクリックします。
4. `Execution Throttle`パラメータを更新します。

Linuxホスト（**Emulex HBA**の場合）

Linuxホスト上のEmulex HBAのキュー深度を更新できます。更新内容を再起動後も維持するには、新しいRAMディスクイメージを作成し、ホストを再起動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のリストとその説明が表示されます。オペレーティングシステムのバージョンに応じて、以下のキュー深度パラメータの1つ以上を変更できます：

- `lpfc_lun_queue_depth`：特定のLUNにキューイングできるFCコマンドの最大数（uint）
- `lpfc_hba_queue_depth`：lpfc HBA にキューイングできる 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にキューイングできる 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. Red Hat Enterprise Linux 5.x システムの `/etc/modprobe.conf`ファイルと、Red Hat Enterprise Linux 6.x または 7.x システム、あるいは SUSE Linux Enterprise Server 11.x または 12.x システムの `/etc/modprobe.d/scsi.conf`ファイルにキュー深度パラメータを追加して、キュー深度を更新します。

   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、ホストを再起動して、再起動後も更新が保持されるようにします。

   詳細については、ご使用の Linux オペレーティング システムのバージョンの"システム管理"を参照してください。

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（QLogic HBAの場合）

Linuxホスト上のQLogicドライバのデバイスキュー深度を更新できます。更新内容を再起動後も維持するには、新しいRAMディスクイメージを作成し、ホストを再起動する必要があります。QLogic HBA管理GUIまたはコマンドラインインターフェース（CLI）を使用して、QLogic HBAのキュー深度を変更できます。

このタスクでは、QLogic HBA CLI を使用して QLogic HBA キューの深さ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 `ql2xmaxqdepth`キュー深度パラメータのみです。これは、各LUNに設定できる最大キュー深度を示します。デフォルト値はRHEL 7.5以降では64です。デフォルト値はRHEL 7.4以前では32です。

```
root@localhost ~]# modinfo qla2xxx|grep ql2xmaxqdepth
parm:       ql2xmaxqdepth:Maximum queue depth to set for each LUN.
Default is 64. (int)
```

2. デバイスのキューの深さの値を更新します：

   - 変更を永続的にする場合は、次の手順を実行します：

     i. `/etc/modprobe.conf`ファイルに `Red Hat Enterprise Linux 5.x` システム用のキュー デプス パラメータを追加し、 `/etc/modprobe.d/scsi.conf`ファイルに `Red Hat Enterprise Linux 6.x` または `7.x` システム、または `SUSE Linux Enterprise Server 11.x` または `12.x` システム用のキュー デプス パラメータを追加して、キュー デプスを更新します： `options qla2xxx ql2xmaxqdepth=new_queue_depth`

     ii. 新しい RAM ディスク イメージを作成し、ホストを再起動して、再起動後も更新が保持されるようにします。

     詳細については、ご使用の Linux オペレーティング システムのバージョンの"システム管理"を参照してください。

   - 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、キューの深さは128に設定されています。

```
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 `Execution Throttle`を更新して、QLogic HBA キューの深さを変更します。

   a. QLogic HBAの管理CLIにログインします。

      ```
      /opt/QLogic_Corporation/QConvergeConsoleCLI/qaucli
      ```

   b. メインメニューから `Adapter Configuration`オプションを選択します。

```
[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. アダプタ構成パラメータのリストから `HBA Parameters`オプションを選択します。

```
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 パラメータ メニューから `Display HBA Parameters`オプションを選択して、 `Execution Throttle`オプションの現在の値を表示します。

`Execution Throttle`オプションのデフォルト値は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. 続行するには **Enter** を押してください。

b. HBA パラメータ メニューから、 `Configure HBA Parameters`オプションを選択して HBA パラメータを変更します。

c. 「パラメータの構成」メニューから `Execute Throttle`オプションを選択し、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. 続行するには **Enter** を押してください。

e. 「パラメータの構成」メニューから、 `Commit Changes`オプションを選択して変更を保存します。

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