SAN構成に関するリファレンス

ONTAP 9

NetApp
February 12, 2026

目次

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。

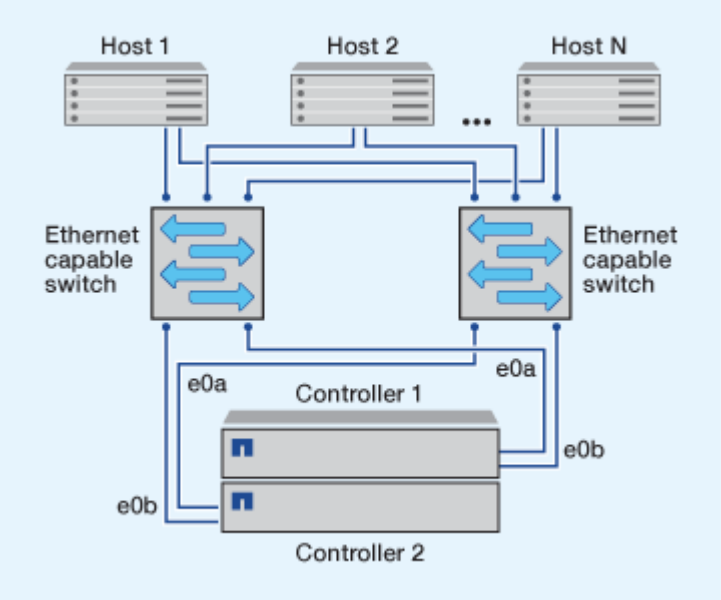
"単一ノード構成"は、フォールト トレランスと中断のない運用をサポートするために必要な冗長性が提供されないため、推奨されません。

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。

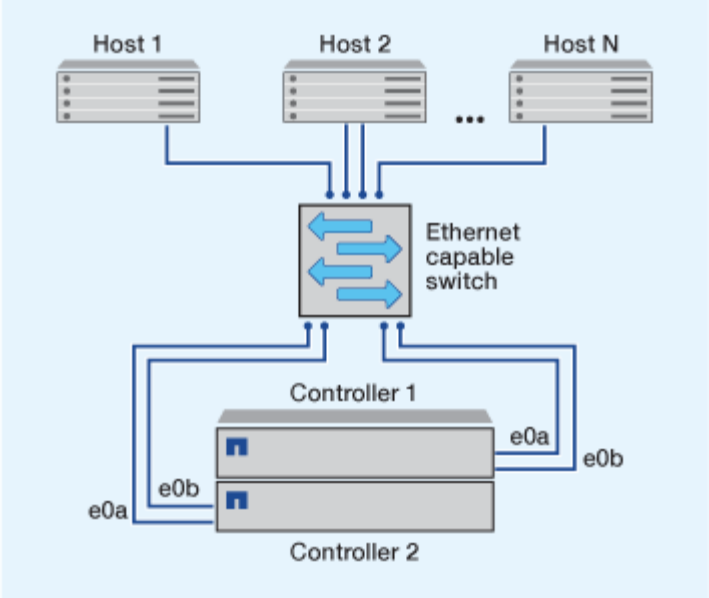
マルチネットワークの**iSCSI**構成

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。



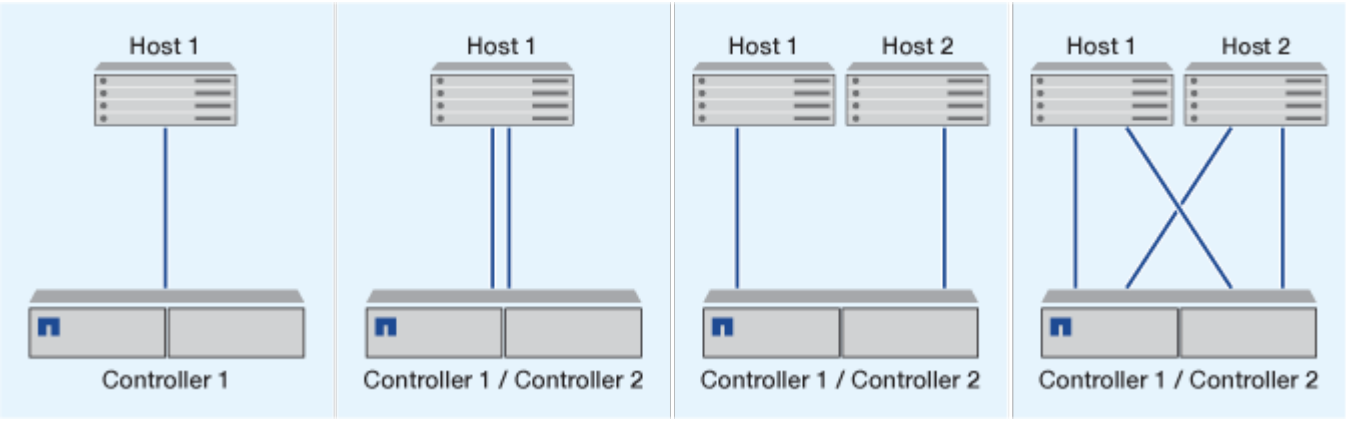
単一ネットワークの**iSCSI**構成

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。

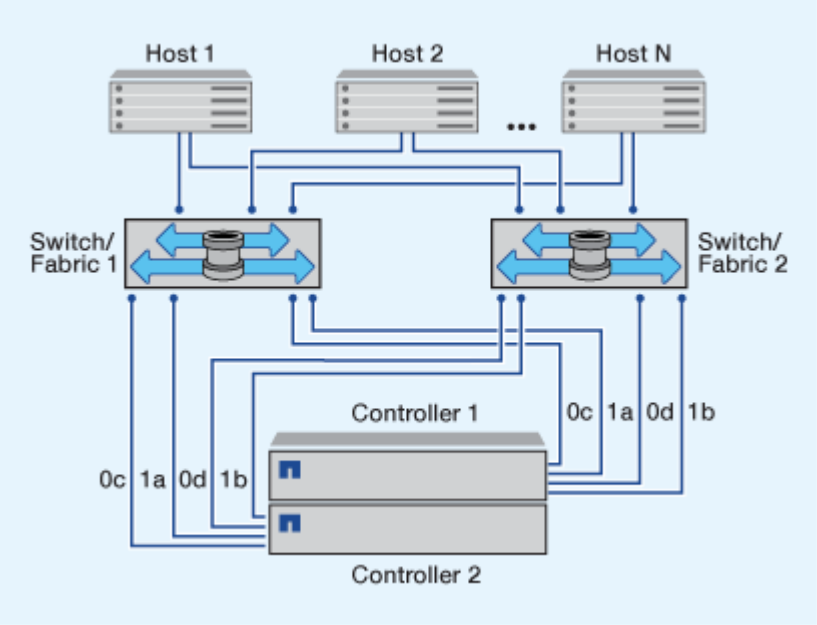
カスケード、部分メッシュ、フルメッシュ、コアエッジ、およびディレクタファブリックはすべて、FCスイッチをファブリックに接続するための業界標準の方法であり、すべてサポートされています。組み込みブレードスイッチを除き、異機種混在のFCスイッチファブリックの使用はサポートされていません。具体的な例外については、"Interoperability Matrix Tool"を参照してください。ファブリックは1つまたは複数のスイッチで構成でき、ストレージ コントローラは複数のスイッチに接続できます。

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。

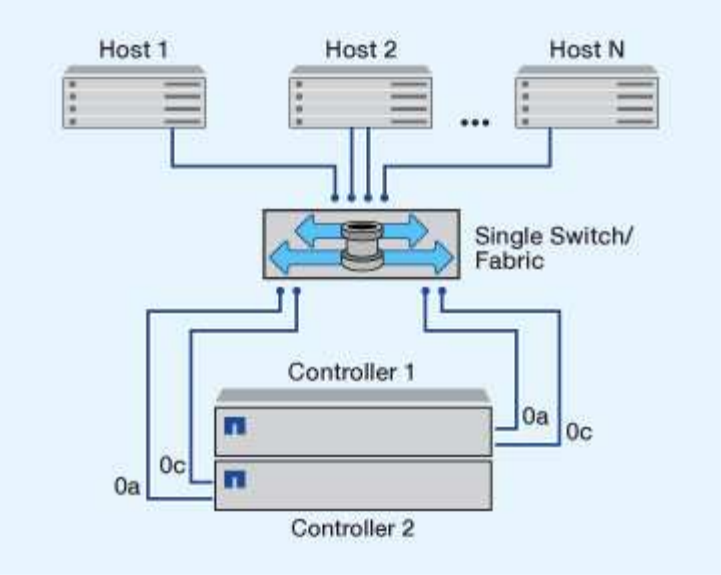


単一ファブリックの**FC**と**FC-NVMe**の構成

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。

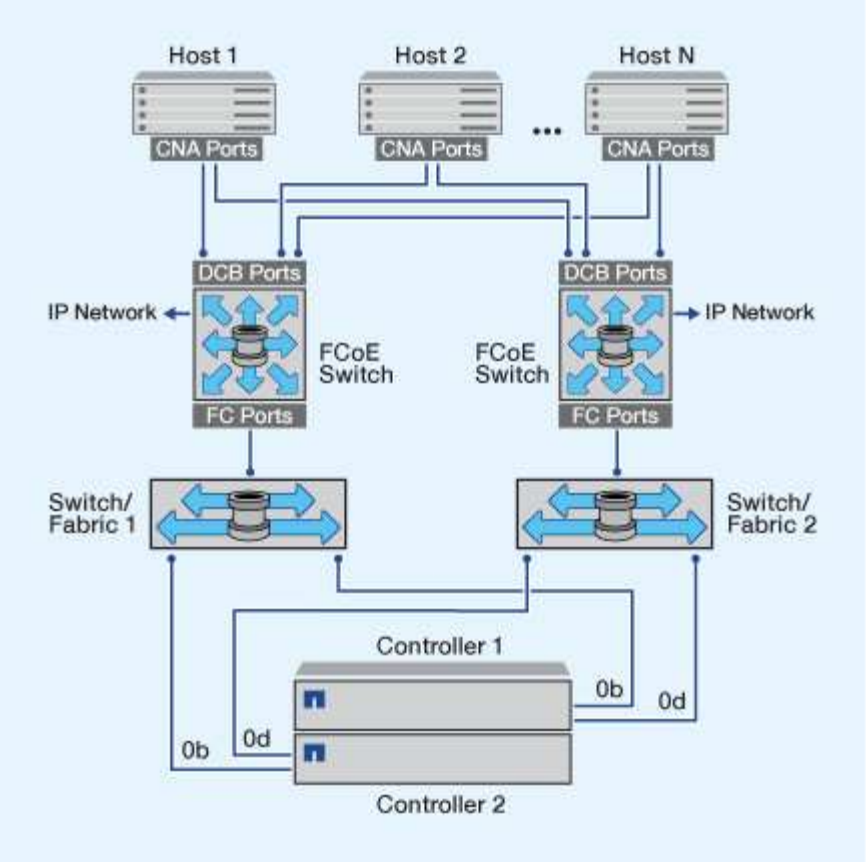
FCoE構成では、FCoEの機能を明示的にサポートするイーサネット スイッチが必要です。FCoE構成は、FCスイッチと同じ相互運用性と品質管理プロセスに照らして検証されます。サポートされる構成の一覧は、Interoperability Matrixを参照してください。これらのサポートされる構成には、スイッチ モデル、単一ファブリックに導入可能なスイッチの数、サポートされるスイッチ ファームウェアのバージョンなどのパラメータが含まれています。

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

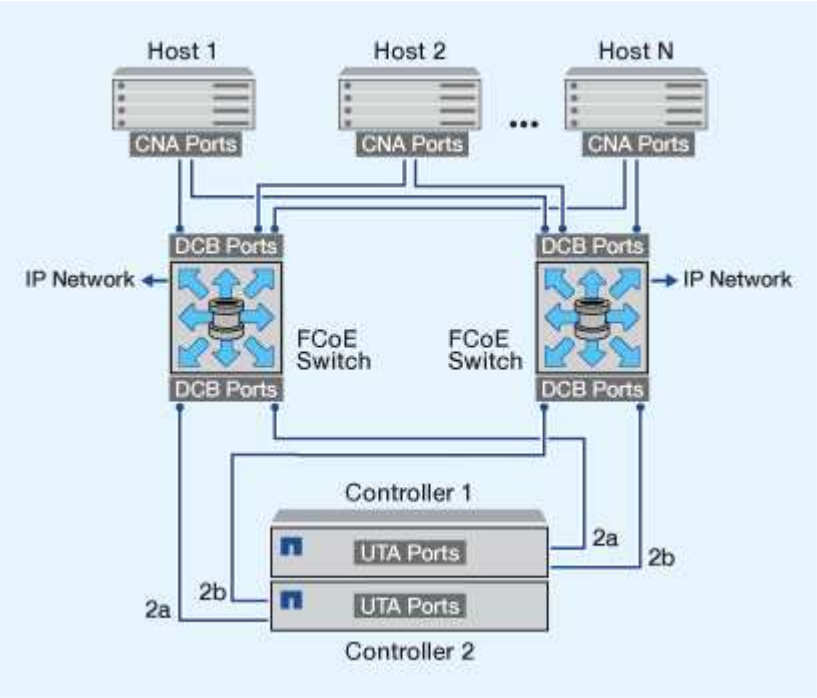
FCoEイニシエータ（CNA）を使用すると、FCoEスイッチを介して、ホストをHAペアの両方のコントローラのFCターゲット ポートに接続できます。FCoEスイッチにはFCポートも必要です。ホストのFCoEイニシエータは、常にFCoEスイッチに接続されます。FCoEスイッチは、FCターゲットに直接接続することも、FCスイッチを介してFCターゲットに接続することもできます。

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。



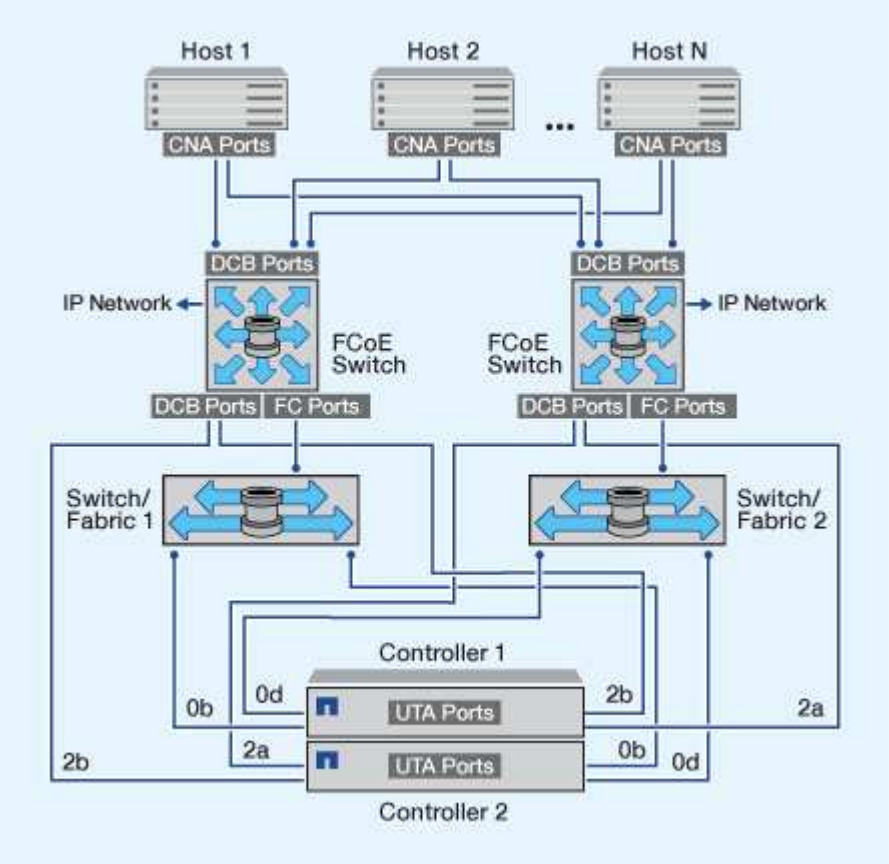
FCoEイニシエータから**FCoE**ターゲット

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。



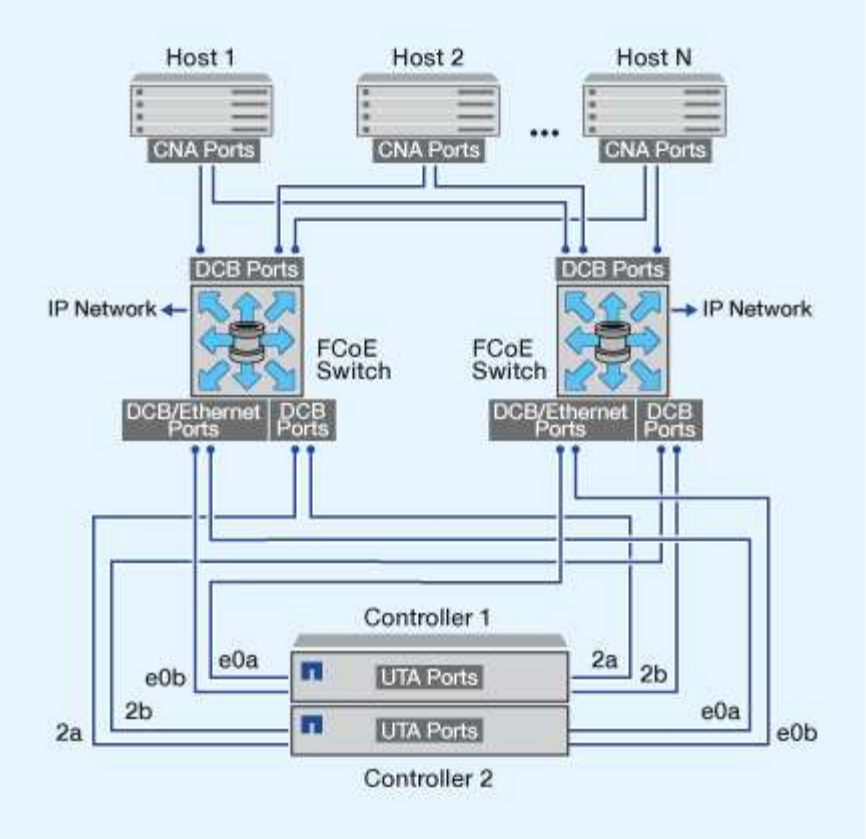
FCoEイニシエータから**FCoE**および**FC**ターゲット

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。

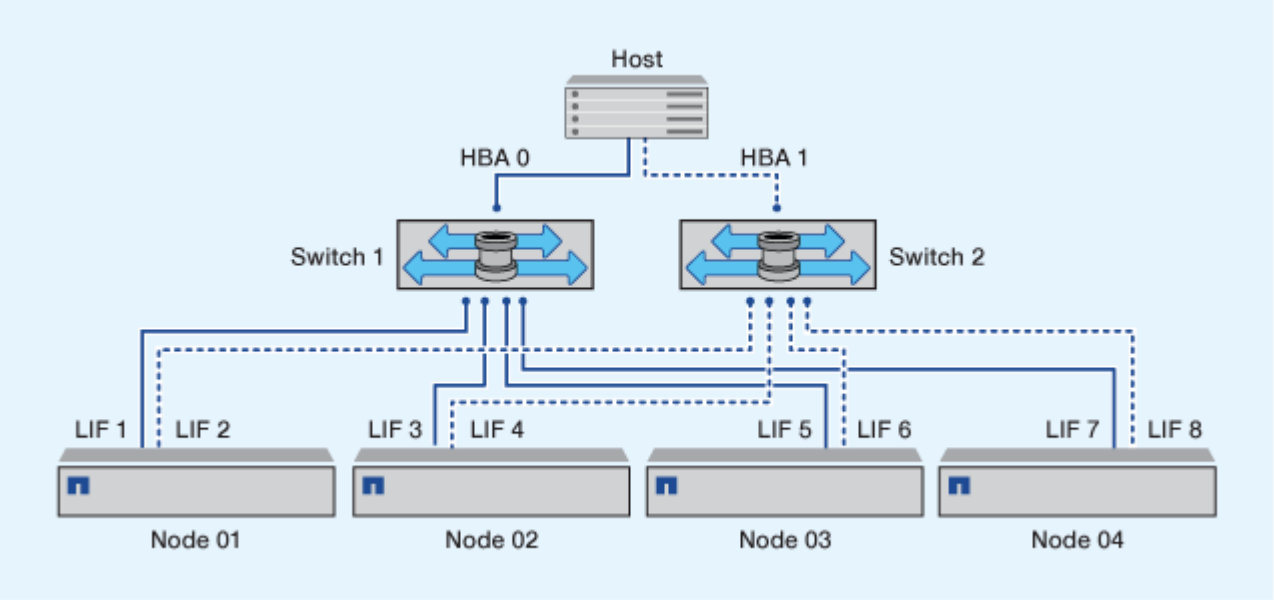
この図で使用されている命名規則は、ONTAPソリューションで使用できる一例です。

- 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 ゾーニング

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。

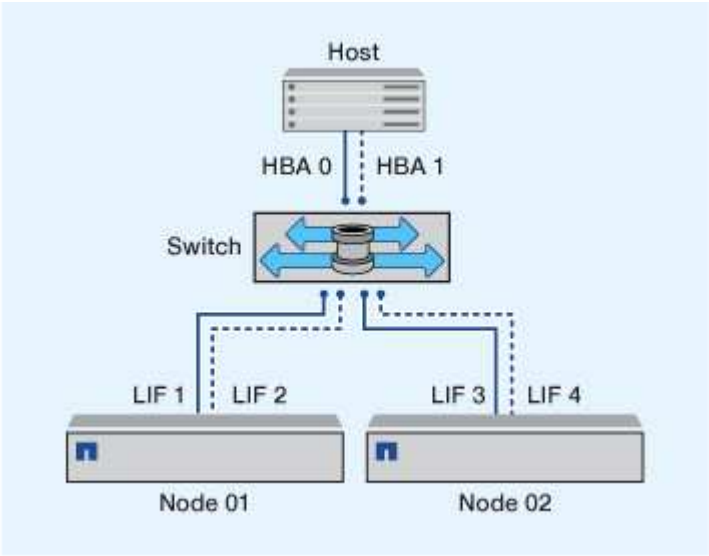
Cisco FC および FCoE スイッチを使用する場合、単一のファブリック ゾーンに同じ物理ポートに対して複数のターゲット LIF を含めることはできません。同じポートの複数の LIF が同じゾーンにある場合、LIF ポートは接続の切断から回復できない可能性があります。

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 **1.** 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