SAN構成のリファレンス

ONTAP 9

NetApp
December 20, 2024

目次

SAN構成のリファレンス

SANコウセイノカイヨウ

Storage Area Network（SAN；ストレージエリアネットワーク）は、iSCSIやFCなどのSAN転送プロトコルを使用してホストに接続されるストレージソリューションで構成されます。ストレージソリューションが1つ以上のスイッチを介してホストに接続されるようにSANを設定できます。iSCSIを使用している場合は、スイッチを使用せずにストレージソリューションをホストに直接接続するようにSANを設定することもできます。

SANでは、Windows、Linux、UNIXなど、異なるオペレーティングシステムを使用する複数のホストが、ストレージソリューションに同時にアクセスできます。および"ポートセット"を使用すると、ホストとストレージの間のデータアクセスを制限できます"選択的LUNマッピング"。

iSCSIの場合、ストレージソリューションとホスト間のネットワークトポロジをネットワークと呼びます。FC、FC / NVMe、FCoEの場合、ストレージソリューションとホストの間のネットワークトポロジをファブリックと呼びます。冗長性を確保してデータアクセスの中断からデータを保護するには、マルチネットワークまたはマルチファブリック構成のHAペアを使用してSANをセットアップする必要があります。シングルノードまたはシングルネットワーク/ファブリックを使用する構成は完全な冗長性がないため、推奨されません。

SANの設定が完了したら"iSCSIまたはFC用のストレージのプロビジョニング"、またはを実行できます"FC / NVMe用のストレージのプロビジョニング"。その後、ホストに接続してデータの提供を開始できます。

SANプロトコルのサポートは、ONTAPのバージョン、プラットフォーム、構成によって異なります。特定の設定の詳細については、を参照して"NetApp Interoperability Matrix Tool"ください。

関連情報

- "SANの管理の概要"
- "NVMeの構成、サポート、制限事項"

iSCSIコウセイ

iSCSI SANホストの構成方法

iSCSI構成は、iSCSI SANホストに直接接続されたハイアベイラビリティ（HA）ペアか、1つ以上のIPスイッチを介してホストと接続されたHAペアでセットアップします。

"HAペア"ホストがLUNへのアクセスに使用するアクティブ/最適化パスとアクティブ/非最適パスのレポートノードとして定義されます。Windows、Linux、UNIXなど、異なるオペレーティングシステムを使用する複数のホストから同時にストレージにアクセスできます。ホストには、ALUAをサポートするサポート対象のマルチパスソリューションがインストールおよび設定されている必要があります。サポートされるオペレーティングシステムとマルチパスソリューションは、で確認できます"NetApp Interoperability Matrix Tool"。

マルチネットワーク構成では、ホストをストレージシステムに接続するスイッチが複数あります。完全な冗長性を備えたマルチネットワーク構成を推奨します。シングルネットワーク構成では、1台のスイッチでホストをストレージシステムに接続します。シングルネットワーク構成では完全な冗長性は確保されません。

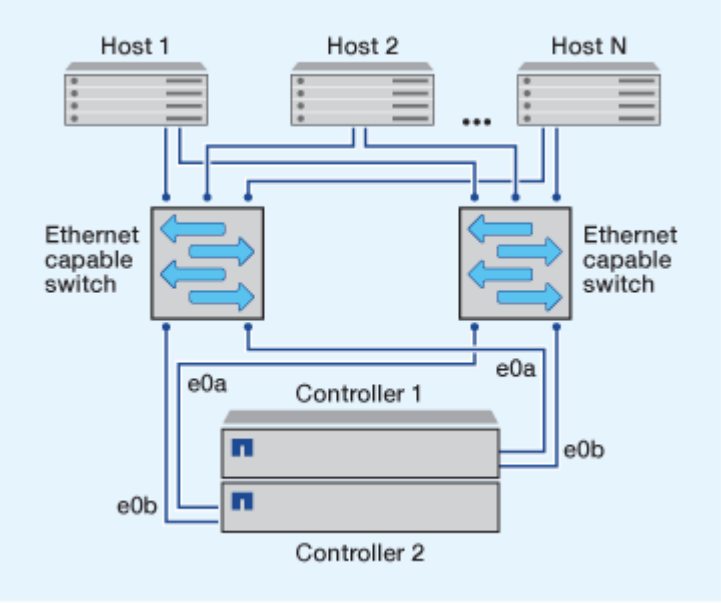
"シングルノードコウセイ"は、フォールトトレランスやノンストップオペレーションのサポートに必要な冗長性が確保されないため、推奨されません。

関連情報

- HAペアが所有するLUNへのアクセスに使用するパスを制限する方法について説明します。"選択的LUNマッピング（SLM）"
- 詳細はこちらをご覧ください "SAN LIF"。
- については、を参照して"iSCSIにおけるVLANの利点"ください。

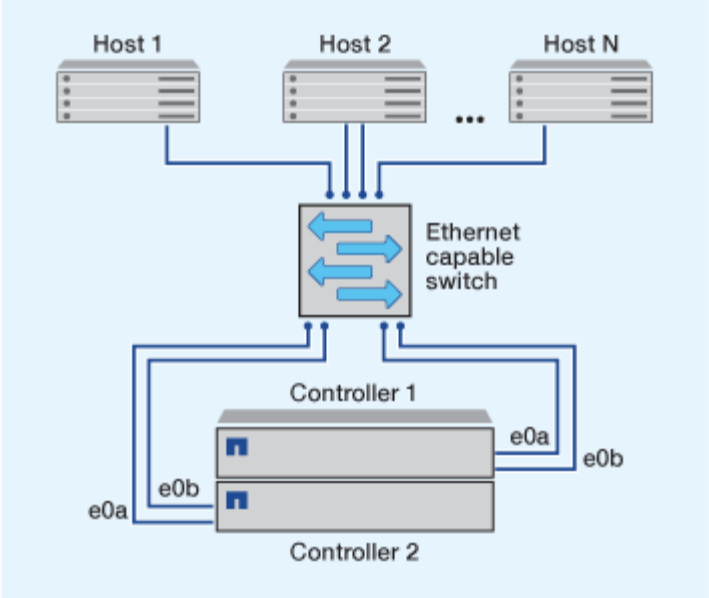
マルチネツトワアク**iSCSI**コウセイ

マルチネットワークのHAペア構成では、HAペアを複数のスイッチで1つ以上のホストに接続します。スイッチが複数あるため、この構成では完全な冗長性が確保されます。



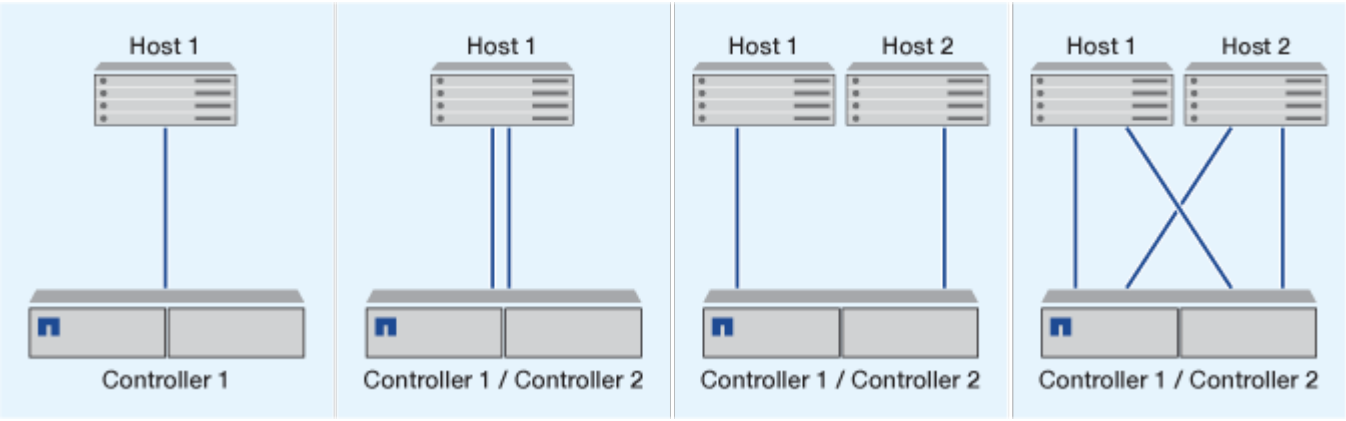
タンイチネツトワアクノ**iSCSI**コウセイ

単一ネットワークのHAペア構成では、HAペアを1つのスイッチで1つ以上のホストに接続します。スイッチが1台しかないため、この構成では完全な冗長性は確保されません。



直接接続型**iSCSI**構成

直接接続型の構成では、1つ以上のホストをコントローラに直接接続します。



iSCSI構成で**VLAN**を使用する利点

VLANは、ブロードキャストドメインにグループ化されたスイッチポートのグループで構成されます。VLANは、単一のスイッチ上に配置することも、複数のスイッチシャーシにまたがって配置することもできます。静的VLANと動的VLANを使用すると、IPネットワークインフラ内のセキュリティを強化し、問題を切り分け、使用可能なパスを制限できます。

大規模なIPネットワークインフラにVLANを実装すると、次のような利点が得られます。

- セキュリティの強化：

  VLANを使用すると、イーサネットネットワークまたはIP SANの異なるノード間のアクセスが制限されるため、既存のインフラを活用しながらセキュリティを強化できます。

- 問題を切り分けることで、イーサネットネットワークとIP SANの信頼性が向上します。

- 問題領域を制限することで、問題解決時間を短縮
- 特定のiSCSIターゲットポートへの使用可能なパスの数が削減されます。
- ホストで使用されるパスの最大数が削減されます。

  パスが多すぎると、再接続時間が遅くなります。ホストにマルチパスソリューションがない場合は、VLANを使用してパスを1つだけ許可できます。

動的な**VLAN**

ダイナミックVLANはMACアドレスベースです。VLANを定義するには、含めるメンバーのMACアドレスを指定します。

動的VLANは柔軟性を提供し、デバイスがスイッチに物理的に接続されている物理ポートへのマッピングを必要としません。VLANを再設定することなく、1つのポートから別のポートにケーブルを移動できます。

セイテキナ**VLAN**

静的なVLANはポートベースです。スイッチとスイッチポートは、VLANとそのメンバーを定義するために使用されます。

スタティックVLANは、メディアアクセス制御（MAC）スプーフィングを使用してVLANを侵害できないため、セキュリティが向上します。ただし、誰かがスイッチに物理的にアクセスできる場合は、ケーブルを交換してネットワークアドレスを再設定するとアクセスが許可されます。

環境によっては、動的なVLANよりも静的なVLANを作成および管理する方が簡単です。これは、スタティックVLANでは、48ビットのMACアドレスではなく、スイッチとポートの識別子だけを指定する必要があるためです。さらに、VLAN IDを使用してスイッチポート範囲にラベルを付けることもできます。

FCコウセイ

FCおよび**FC-NVMe SAN**ホストの構成方法

FCおよびFC-NVMe SANホストは、HAペアと、少なくとも2つのスイッチを使用して構成することを推奨します。これにより、ファブリック レイヤとストレージ システム レイヤで冗長性が確保され、フォールト トレランスとノンストップ オペレーションがサポートされます。FCまたはFC-NVMe SANホストをスイッチを使用せずにHAペアに直接接続することはできません。

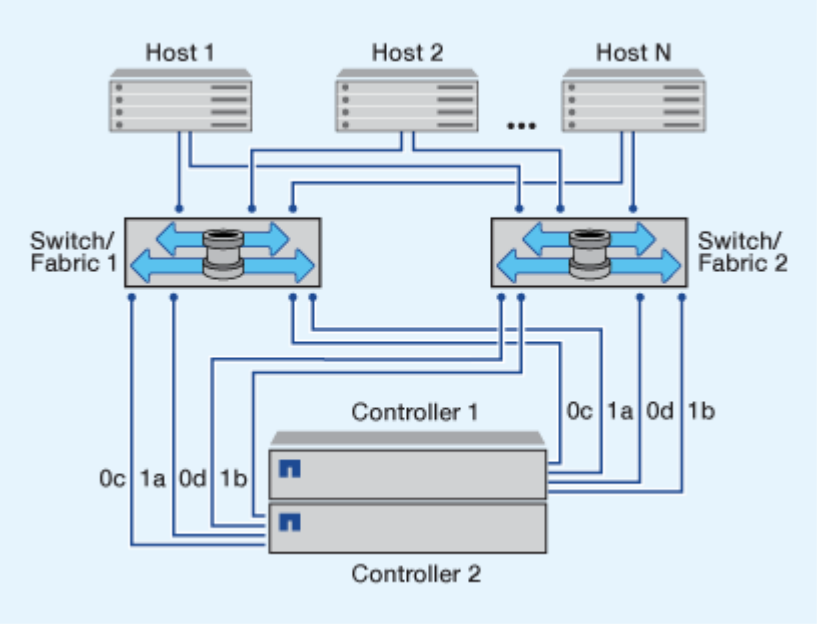
カスケード ファブリック、部分メッシュ ファブリック、フルメッシュ ファブリック、コアエッジ ファブリック、およびディレクタ ファブリックは、FCスイッチをファブリックに接続する業界標準の方法であり、いずれもサポートされます。異機種混在のFCスイッチ ファブリックの使用は、組み込みのブレード スイッチ以外はサポートされません。特定の例外については、を"Interoperability Matrix Tool"参照してください。ファブリックは1つまたは複数のスイッチで構成でき、ストレージコントローラは複数のスイッチに接続できます。

Windows、Linux、UNIXなど、異なるオペレーティングシステムを使用する複数のホストから、ストレージコントローラに同時にアクセスできます。ホストには、サポートされているマルチパスソリューションがインストールおよび設定されている必要があります。サポートされるオペレーティングシステムとマルチパスソリューションは、Interoperability Matrix Toolで確認できます。

マルチファブリックノ**FC**コウセイオヨビ**FC-NVMe**コウセイ

マルチファブリックのHAペア構成では、HAペアを複数のスイッチで1つ以上のホストに接続します。次の図は、マルチファブリックのHAペアを示しています。わかりやすいように、この図ではファブリックが2つだけになっていますが、マルチファブリック構成は2つ以上の任意の数のファブリックで構成できます。

次の図のFCターゲット ポート番号（0c、0d、1a、1b）は一例です。実際のポート番号は、使用しているストレージ ノードのモデル、および拡張アダプタを使用しているかどうかによって異なります。

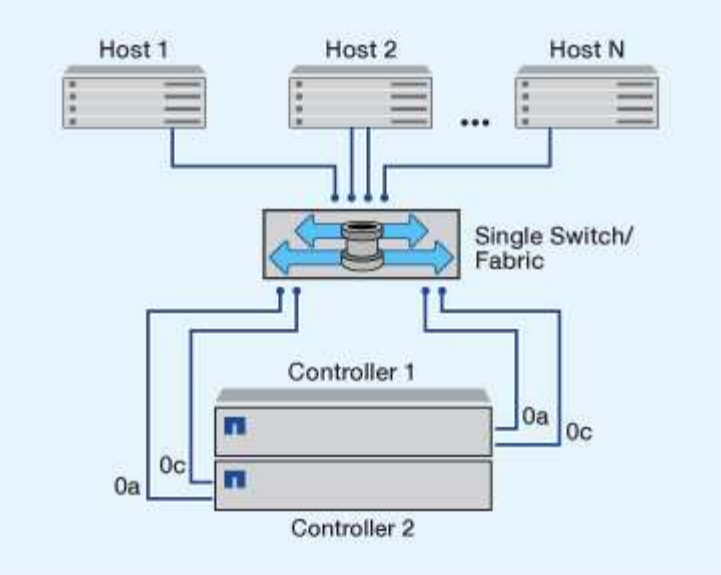


タンイツファブリックノ**FC**コウセイオヨビ**FC-NVMe**コウセイ

単一ファブリックのHAペア構成では、HAペアの両方のコントローラを1つのファブリックで1つ以上のホストに接続します。ホストとコントローラは単一のスイッチを介して接続されるため、単一ファブリックのHAペア構成では完全な冗長性は確保されません。

次の図のFCターゲットポート番号（0a、0c）は一例です。実際のポート番号は、ストレージノードのモデル、および拡張アダプタを使用しているかどうかによって異なります。

単一ファブリックのHAペア構成は、FC構成をサポートするすべてのプラットフォームでサポートされます。



"シングルノードコウセイ"は、フォールトトレランスやノンストップオペレーションのサポートに必要な冗長性が確保されないため、推奨されません。

関連情報

- HAペアが所有するLUNへのアクセスに使用するパスを制限する方法について説明します。"選択的LUNマッピング（SLM）"
- 詳細はこちらをご覧ください "SAN LIF"。

FCスイッチ構成のベストプラクティス

FCスイッチを設定する際には、パフォーマンスを最大限に高めるために一定のベストプラクティスを考慮する必要があります。

FCスイッチの構成では、リンク速度を固定に設定することを推奨します。これは、ファブリックのリビルド時に最適なパフォーマンスが得られるため、時間を大幅に節約できるため、大規模なファブリックに特に適しています。自動ネゴシエーションは柔軟性に優れていますが、FCスイッチの構成が必ずしも期待どおりのパフォーマンスを発揮するとは限らず、ファブリック全体の構築時間が長くなります。

ファブリックに接続されているすべてのスイッチでN_Port ID Virtualization（NPIV）がサポートされ、NPIVが有効になっている必要があります。ONTAPは、NPIVを使用してFCターゲットをファブリックに提示します。

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

FCとiSCSIのベストプラクティスについては、を参照してください "NetAppテクニカルレポート4080：『Best Practices for Modern SAN』"。

サポートされるFCホップ数

ホストとストレージシステムの間でサポートされるFCの最大ホップ数は、スイッチベンダーとストレージシステムによるFC構成のサポートによって異なります。

ホップ数は、イニシエータ（ホスト）とターゲット（ストレージシステム）の間のパスにあるスイッチの数として定義されます。Cisco では、この値を「 SAN ファブリックの直径」とも呼びます。

スイッチベンダー	サポートされるホップ数
Brocade	FCでは7、FCoEでは5
Cisco	7 FCの場合、最大3つのスイッチをFCoEスイッチにすることができます。

関連情報

"NetAppのダウンロード：Brocadeスケーラビリティマトリックスドキュメント"

"NetAppのダウンロード：Ciscoスケーラビリティマトリックスドキュメント"

FCターゲットポート構成に関する推奨事項

FC-NVMeプロトコル用のFCターゲットポートは、FCプロトコル用の設定および使用とまったく同じ方法で設定および使用できます。FC-NVMeプロトコルがサポートされるかどうかは、プラットフォームとONTAPのバージョンによって異なります。NetApp Hardware Universeを使用してサポートを確認します。

最適なパフォーマンスと可用性を実現するには、使用するプラットフォームに対応したに記載されている推奨されるターゲットポート構成を使用する必要があります "NetApp Hardware Universe"。

共有ASICを使用するFCターゲットポートの設定

次のプラットフォームには、ASIC（特定用途向け共有集積回路）を使用したポートペアがあります。これらのプラットフォームで拡張アダプタを使用する場合は、接続に同じASICが使用されないようにFCポートを設定する必要があります。

コントローラ	ASIC を共有するポートペア	ターゲットポートの数：推奨ポート
• FAS8200 • 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、さまざまな速度で実行するように設定できます。特定のホストで使用されるすべてのターゲットポートを同じ速度に設定する必要があります。ターゲットポートの速度は、接続先デバイスの速度と同じに設定する必要があります。ポート速度に自動ネゴシエーションを使用しないでください。自動ネゴシエーションを設定したポートの方が、ギブバックやテイクオーバーなどの中断後の再接続に時間がかかる可能性があります。

オンボードポートと拡張アダプタは、次の速度で実行するように設定できます。コントローラと拡張アダプタ

のポートは、必要に応じて、さまざまな速度で実行するように個別に構成することができます。

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

UTA2 ポートでは、必要に応じて、 8Gb の SFP+ アダプタを使用して 8Gb 、 4Gb 、 2Gb の速度をサポートできます。

FCアダプタを搭載したシステムを管理する

FCアダプタを搭載したシステムの管理の概要

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

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

FCアダプタの管理用コマンド

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

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

FC ターゲットアダプタの管理用コマンド

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

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

FC イニシエータアダプタの管理用コマンド

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

オンボード **FC** アダプタの管理用コマンド

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

FCアダプタのイニシエータモード設定

オンボードアダプタの個 々 のFCポートおよび特定のFCアダプタカードをイニシエータモードに設定できます。イニシエータモードは、テープドライブ、テープライブラリ、またはFlexArray仮想化またはForeign LUN Import（FLI）を使用するサードパーティストレージへのポートの接続に使用されます。

必要なもの

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

タスクの内容

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

"NetApp Hardware Universe"てください。

NVMe/FCではイニシエータモードがサポートされます。

手順

1. アダプタからすべてのLIFを削除します。

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

2. アダプタをオフラインにします。

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

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

3. アダプタをターゲットからイニシエータに変更します。

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

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

   ```
   system hardware unified-connect show
   ```

6. アダプタをオンラインに戻します。

   ```
   node run -node node_name storage enable adapter adapter_port
   ```

FCアダプタのターゲットモード設定

オンボードアダプタの個 々 のFCポートおよび特定のFCアダプタカードをターゲットモードに設定できます。ターゲットモードは、ポートをFCイニシエータに接続するために使用されます。

タスクの内容

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

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

手順

1. アダプタをオフラインにします。

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

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

2. アダプタをイニシエータからターゲットに変更します。

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

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

   `network fcp adapter show -node node_name`

5. アダプタをオンラインにします。

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

FCターゲットアダプタに関する情報を表示する

コマンドを使用すると、システム内のFCアダプタのシステム設定やアダプタ情報を表示できます `network fcp adapter show`。

ステップ

1. コマンドを使用して、FCアダプタに関する情報を表示します `network fcp adapter show`。

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

   ```
   network fcp adapter show -instance -node node1 -adapter 0a
   ```

FCアダプタの速度を変更する

自動ネゴシエーションを使わずに、アダプタのターゲットポートの速度を接続先デバイスの速度と同じにすることを推奨します。自動ネゴシエーションを設定したポートの方が、ギブバックやテイクオーバーなどの中断後の再接続に時間がかかる可能性があります。

必要なもの

このアダプタをホームポートとして使用しているすべての LIF をオフラインにする必要があります。

タスクの内容

この処理ではクラスタ内のすべてのStorage Virtual Machine（SVM）とLIFが対象となるため、パラメータと`-home-lif`パラメータを使用して処理範囲を制限する必要があります `-home-port`。これらのパラメータを使用しないと、処理環境によってクラスタ内のすべての LIF が処理によって使用されなくなる可能性があります。

手順

1. アダプタのすべての LIF をオフラインにします。

```
network interface modify -vserver * -lif * { -home-node node1 -home-port 0c }
-status-admin down
```

2. アダプタをオフラインにします。

   ```
   network fcp adapter modify -node node1 -adapter 0c -state down
   ```

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

3. ポートアダプタの最大速度を確認します。

   ```
   fcp adapter show -instance
   ```

   アダプタ速度を最大速度よりも速くすることはできません。

4. アダプタ速度を変更します。

   ```
   network fcp adapter modify -node node1 -adapter 0c -speed 16
   ```

5. アダプタをオンラインにします。

   ```
   network fcp adapter modify -node node1 -adapter 0c -state up
   ```

6. アダプタのすべての LIF をオンラインにします。

   ```
   network interface modify -vserver * -lif * { -home-node node1 -home-port 0c }
   -status-admin up
   ```

サポートされる**FC**ポート

オンボードのFCポートおよびFC用に構成されるCNA / UTA2ポートの数は、コントローラのモデルによって異なります。また、 FC ポートは、サポートされている FC ターゲット拡張アダプタのほか、 FC SFP+ アダプタ用の追加の UTA2 カードからも提供されます。

オンボードの**FC**、**UTA**、および**UTA2**ポート

- オンボードポートは、ターゲットまたはイニシエータのどちらかのFCポートとして個別に構成できます。
- オンボードFCポートの数は、コントローラのモデルによって異なります。

  に "NetApp Hardware Universe"は、各コントローラモデルのオンボードFCポートの一覧が記載されています。

- FAS2520システムはFCをサポートしていません。

ターゲット拡張アダプタの**FC**ポート

- 使用可能なターゲット拡張アダプタは、コントローラのモデルによって異なります。

  に "NetApp Hardware Universe"は、各コントローラモデルのターゲット拡張アダプタの一覧が記載されて

います。

- 一部のFC拡張アダプタのポートは、工場出荷時にイニシエータまたはターゲットとして構成されており、変更することはできません。

  その他のポートについては、オンボードのFCポートと同様に、ターゲットまたはイニシエータのどちらかのFCポートとして個別に構成できます。完全なリストについては、を参照して "NetApp Hardware Universe"ください。

X1133A-R6アダプタ使用時の接続の切断を防止

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

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

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

FCoEコウセイ

FCoEの設定方法の概要

FCoEは、FCoEスイッチを使用してさまざまな方法で設定できます。直接接続型の構成はFCoEではサポートされません。

FCoE構成はすべてデュアルファブリックで、完全に冗長化されており、ホスト側のマルチパスソフトウェアが必要です。いずれのFCoE構成でも、イニシエータとターゲット間のパスには、最大ホップ数の範囲内でFCoEスイッチとFCスイッチを複数配置できます。スイッチを相互に接続するには、イーサネットISLに対応したバージョンのファームウェアがスイッチで実行されている必要があります。FCoE構成の各ホストでオペレーティングシステムが異なることがあります。

FCoE構成には、FCoEの機能を明示的にサポートするイーサネットスイッチが必要です。FCoE構成は、FCスイッチと同じ相互運用性と品質管理のプロセスで検証されます。サポートされる構成の一覧については、Interoperability Matrixを参照してください。サポートされる構成に含まれるパラメータには、スイッチモデル、単一ファブリックに導入できるスイッチの数、サポートされるスイッチファームウェアのバージョンなどがあります。

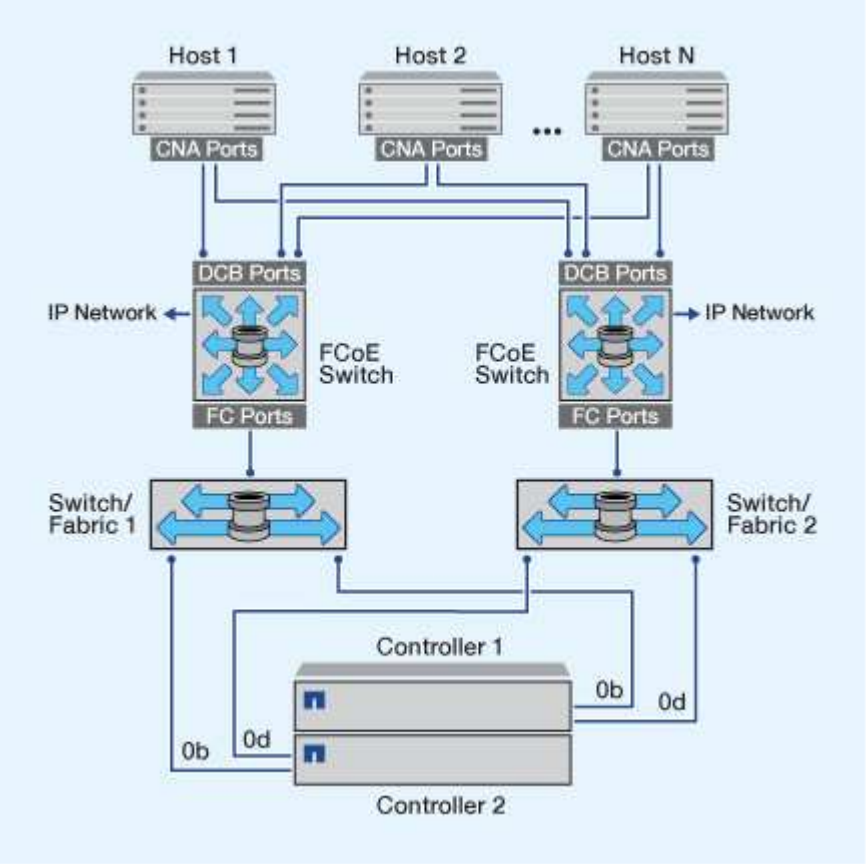
次の図のFCターゲット拡張アダプタのポート番号は一例です。実際のポート番号は、FCoEターゲット拡張アダプタがインストールされている拡張スロットによって変わる場合があります。

FCoEイニシエータから**FC**ターゲット

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

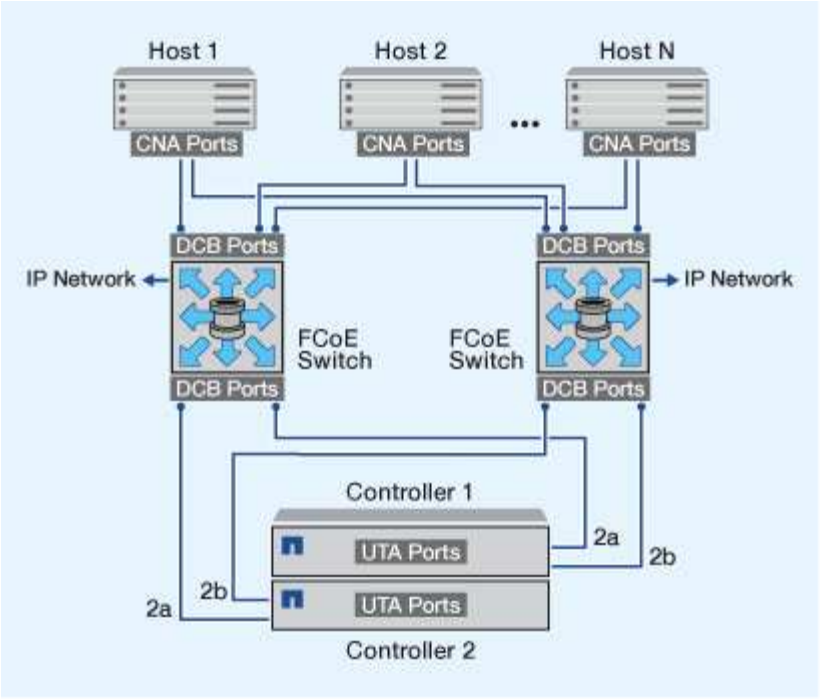
イッチを介してFCターゲットに接続することもできます。

次の図では、ホストのCNAをFCoEスイッチに接続し、FCスイッチをHAペアに接続しています。



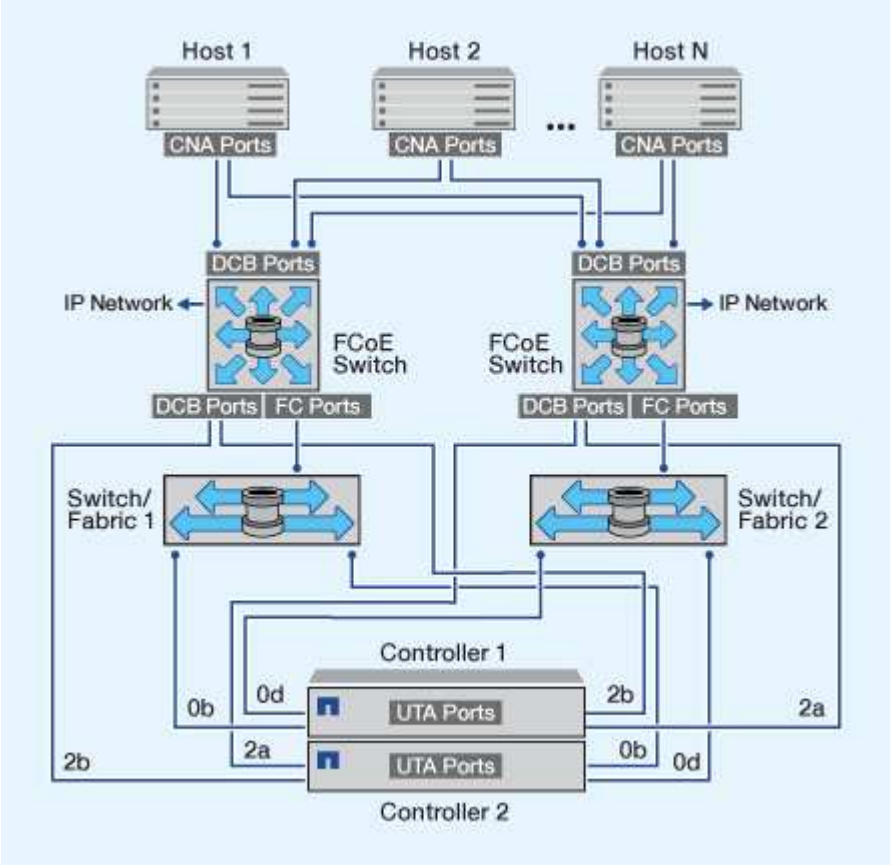
FCoEイニシエータから**FCoE**ターゲット

ホストのFCoEイニシエータ（CNA）を使用すると、FCoEスイッチを介して、ホストをHAペアの両方のコントローラのFCoEターゲットポート（UTAまたはUTA2とも呼ばれる）に接続できます。



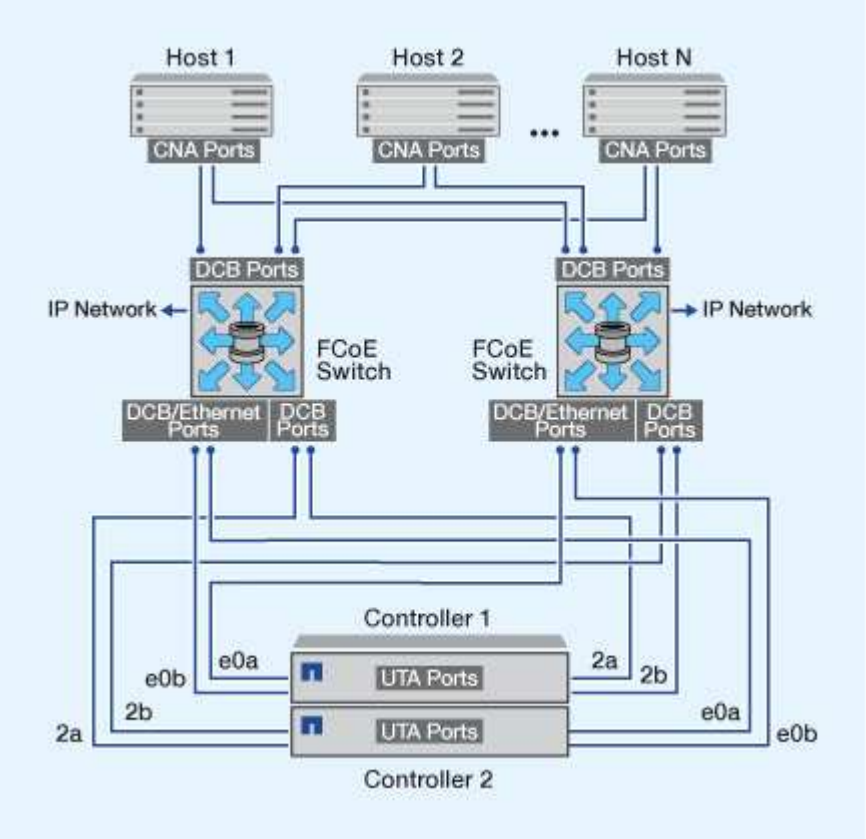
FCoEイニシエータから**FCoE**および**FC**ターゲット

ホストのFCoEイニシエータ（CNA）を使用すると、FCoEスイッチを介して、ホストをHAペアの両方のコントローラのFCoEおよびFCターゲットポート（UTAまたはUTA2とも呼ばれる）に接続できます。



FCoEとIPストレージプロトコルの混在

ホストのFCoEイニシエータ（CNA）を使用すると、FCoEスイッチを介して、ホストをHAペアの両方のコントローラのFCoEターゲットポート（UTAまたはUTA2とも呼ばれる）に接続できます。FCoEポートは、単一のスイッチへの従来のリンクアグリゲーションを使用できません。Ciscoスイッチでは、FCoEをサポートする特殊なタイプのリンクアグリゲーション（仮想ポートチャネル）がサポートされます。仮想ポートチャネルは、2つのスイッチへの個 々 のリンクを集約します。仮想ポートチャネルは、他のイーサネットトラフィックにも使用できます。NFS、SMB、iSCSI、およびその他のイーサネットトラフィックなど、FCoE以外のトラフィックに使用されるポートでは、FCoEスイッチの通常のイーサネットポートを使用できます。



FCoEイニシエータとターゲットの組み合わせ

FCoEと従来のFCのイニシエータとターゲットの特定の組み合わせがサポートされます。

FCoEイニシエータ

ホストコンピュータのFCoEイニシエータは、ストレージコントローラのFCoEターゲットと従来のFCターゲットの両方で使用できます。ホストのFCoEイニシエータはFCoE DCB（Data Center Bridging）スイッチに接続する必要があります。ターゲットに直接接続することはできません。

次の表に、サポートされる組み合わせを示します。

イニシエータ	ターゲット	サポートの有無
FC	FC	○

イニシエータ	ターゲット	サポートの有無
FC	FCoE	○
FCoE	FC	○
FCoE	FCoE	○

FCoEターゲット

ストレージコントローラでFCoEターゲットポートと4Gb、8Gb、または16GbのFCポートを混在させることができます。FCポートがアドインのターゲットアダプタであるかオンボードのポートであるかは関係ありません。FCoEとFCの両方のターゲットアダプタを同じストレージコントローラに搭載できます。

FCのオンボードポートと拡張ポートの組み合わせルールも適用されます。

サポートされる**FCoE**ホップ数

ホストとストレージシステムの間でサポートされるFibre Channel over Ethernet（FCoE）の最大ホップ数は、スイッチベンダーとストレージシステムでのFCoE構成のサポートによって異なります。

ホップ数は、イニシエータ（ホスト）とターゲット（ストレージシステム）の間のパスにあるスイッチの数として定義されます。Cisco Systems のマニュアルでは、この値のことを「 SAN fabric_ の直径」とも呼んでいます。

FCoEでは、FCoEスイッチをFCスイッチに接続できます。

エンドツーエンドのFCoE接続では、イーサネットInter-Switch Link（ISL；スイッチ間リンク）に対応するバージョンのファームウェアがFCoEスイッチで実行されている必要があります。

次の表に、サポートされる最大ホップ数を示します。

スイッチベンダー	サポートされるホップ数
Brocade	FCの場合は7 FCoEの場合は5
Cisco	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。

ファイバチャネルと**FCoE**のゾーニング

ファイバチャネルと**FCoE**のゾーニングの概要

FC ゾーン、 FC-NVMe ゾーン、または FCoE ゾーンは、ファブリック内の 1 つ以上のポートを論理的にグループ化したものです。デバイスがお互いを認識し、接続し、相互にセッションを作成し、通信できるようにするには、両方のポートが共通のゾーンメンバーシップを持っている必要があります。シングルイニシエータゾーニングを推奨します。

ゾーニングを行う理由

- イニシエータ HBA 間のクロストークを削減または解消できます。

  これは小規模な環境でも発生し、ゾーニングを実装する最大の理由の 1 つです。ゾーニングによってファブリックの論理サブセットを作成することで、クロストークの問題が解消されます。

- 特定の FC 、 FC-NVMe 、または FCoE ポートへの使用可能なパスの数と、ホストと特定の LUN の間に認識されるパスの数を減らすことができます。

  たとえば、一部のホスト OS のマルチパスソリューションには、管理できるパスの数に制限があります。ゾーニングを使用すると、 OS のマルチパスドライバで認識されるパスの数を減らすことができます。ホストにマルチパス解決策がインストールされていない場合は、ファブリックのゾーニングまたは SVM の選択的 LUN マッピング（ SLM ）とポートセットの組み合わせを使用して、認識される LUN へのパスが 1 つだけであることを確認する必要があります。

- ゾーンを共有するエンドポイントへのアクセスと接続を制限することで、セキュリティを強化します。

  共通のゾーンがないポート同士が通信することはできません。

- 発生する問題を切り離すことで SAN の信頼性が高まり、問題の範囲を限定することで解決時間を短縮する効果があります。

ゾーニングに関する推奨事項

- 1 つの SAN にホストを 4 つ以上接続する場合や SAN に接続されたノードで SLM が実装されていない場合は、常にゾーニングを実装してください。
- 一部のスイッチベンダーでは World Wide Node Name のゾーニングも使用できますが、特定のポートを正しく定義し、 NPIV を効果的に利用するには、 World Wide Port Name のゾーニングを使用する必要があります。
- 管理性を損なわない範囲でゾーンサイズを制限することを推奨します。

  複数のゾーンを重複させてサイズを制限することができます。ホストまたはホストクラスタごとにゾーンを定義することを推奨します。

- イニシエータ HBA 間のクロストークを解消するために、単一イニシエータのゾーニングを使用してください。

World Wide Nameに基づくゾーニング

World Wide Name（WWN）に基づくゾーニングでは、ゾーンに含めるメンバーのWWNを指定します。ONTAPのゾーニングでは、World Wide Port Name（WWPN）ゾーニン

グを使用する必要があります。

WWPNゾーニングは柔軟性に優れており、デバイスがファブリックに物理的に接続されている場所によってアクセスが決まりません。ゾーンを再設定することなく、1つのポートから別のポートにケーブルを移動できます。

ONTAPを実行するストレージコントローラへのファイバチャネルパスでは、ノードの物理ポートのWWPNではなく、ターゲットの論理インターフェイス（LIF）のWWPNを使用してFCスイッチをゾーニングしてください。LIF の詳細については、『 ONTAP ネットワーク管理ガイド』を参照してください。

"ネットワーク管理"

個 々 のゾーン

推奨されるゾーニング設定では、ゾーンごとに 1 つのホストイニシエータを配置します。ゾーンは、ホストイニシエータポートとストレージノード上の 1 つ以上のターゲット LIF で構成され、ターゲットあたりの希望する数のパスまで LUN へのアクセスを提供します。つまり、同じノードにアクセスする複数のホストはお互いのポートを認識できませんが、各イニシエータはすべてのノードにアクセスできます。

Storage Virtual Machine（SVM）のすべてのLIFを、ホストイニシエータを含むゾーンに追加する必要があります。これにより、既存のゾーンを編集したり、新しいゾーンを作成したりせずに、ボリュームや LUN を移動できます。

ONTAP を実行するノードへのファイバチャネルパスでは、ノードの物理ポートの WWPN ではなく、ターゲットの論理インターフェイス（ LIF ）の WWPN を使用して FC スイッチをゾーニングしてください。物理ポートの WWPN は「 50 」で始まり、 LIF の WWPN は「 20 」で始まります。

単一ファブリックゾーニング

単一ファブリック構成でも、各ホストイニシエータを各ストレージノードに接続できます。複数のパスを管理するには、ホストにマルチパスソフトウェアが必要です。ソリューションの耐障害性を確保するために、マルチパス用に各ホストに2つのイニシエータが必要です。

各イニシエータには、そのイニシエータがアクセスできる各ノードのLIFを少なくとも1つ設定する必要があります。ホストイニシエータからクラスタ内のHAペアのノードへのパスが少なくとも1つあるようにゾーニングを設定して、LUN接続用のパスを提供する必要があります。つまり、ホスト上の各イニシエータには、そのゾーン構成内のノードごとにターゲットLIFが1つだけ割り当てられます。クラスタ内の同じノードまたは複数のノードへのパスが複数必要な場合は、ゾーン構成内の各ノードに複数のLIFが割り当てられます。これにより、ノードに障害が発生した場合や、LUNを含むボリュームが別のノードに移動された場合でも、ホストはLUNに引き続きアクセスできます。また、レポートノードを適切に設定する必要があります。

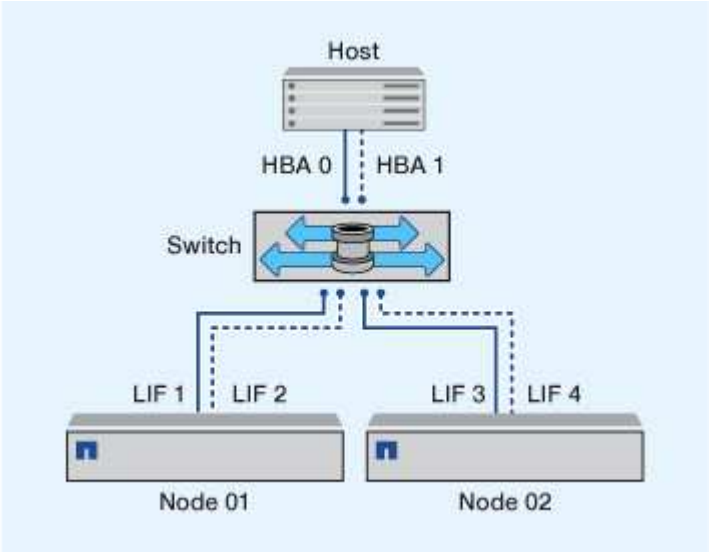
単一ファブリック構成はサポートされていますが、可用性に優れているとはみなされません。1つのコンポーネントの障害が、データ アクセスの中断を招く可能性があります。

次の図では、ホストに2つのイニシエータがあり、マルチパス ソフトウェアを実行しています。次の2つのゾーンがあります。

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

- ゾーン1：HBA 0、LIF_1、およびLIF_3
- ゾーン2：HBA 1、LIF_2、およびLIF_4

構成に追加のノードが含まれている場合は、追加のノードのLIFがこれらのゾーンに含まれます。



この例では、各ゾーンに4つのLIFをすべて配置することもできます。その場合のゾーンは次のようになります。

- ゾーン1：HBA 0、LIF_1、LIF_2、LIF_3、およびLIF_4
- ゾーン2：HBA 1、LIF_1、LIF_2、LIF_3、およびLIF_4

ホストオペレーティングシステムとマルチパスソフトウェアが、ノード上のLUNへのアクセスに使用される数のパスをサポートしている必要があります。ノードのLUNへのアクセスに使用するパスの数については、SAN構成の制限に関するセクションを参照してください。

関連情報

"NetApp Hardware Universe"

デュアルファブリックの**HA**ペアのゾーニング

デュアルファブリック構成では、各ホストイニシエータを各クラスタノードに接続できます。各ホストイニシエータは、異なるスイッチを使用してクラスタノードにアクセスします。複数のパスを管理するには、ホストにマルチパスソフトウェアが必要です。

1つのコンポーネントで障害が発生してもデータへのアクセスが維持されるため、デュアルファブリック構成はハイアベイラビリティとみなされます。

次の図では、ホストに2つのイニシエータがあり、マルチパスソフトウェアを実行しています。2つのゾーンがあります。SLMは、すべてのノードがレポートノードとみなされるように設定されています。

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

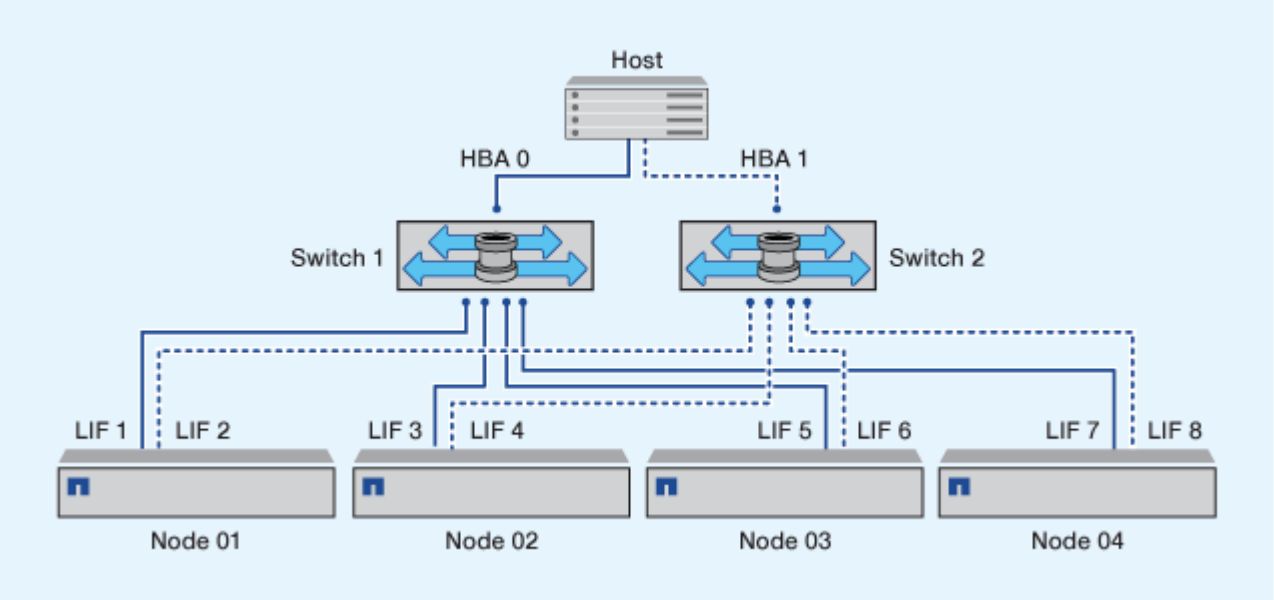
- ゾーン1：HBA 0、LIF_1、LIF_3、LIF_5、およびLIF_7

- ゾーン2：HBA 1、LIF_2、LIF_4、LIF_6、およびLIF_8

各ホストイニシエータは、異なるスイッチを使用してゾーニングされます。ゾーン1にはスイッチ1からアクセスします。ゾーン2にはスイッチ2からアクセスします。

各イニシエータは、すべてのノードのLIFにアクセスできます。これにより、ノードで障害が発生しても、ホストはLUNに引き続きアクセスできます。SVMは、選択的LUNマップ（SLM）とレポートノードの設定に基づいて、クラスタソリューション内のすべてのノードのすべてのiSCSI LIFとFC LIFにアクセスできます。SLM、ポートセット、またはFCスイッチゾーニングを使用して、SVMからホストへのパスの数とSVMからLUNへのパスの数を減らすことができます。

構成に追加のノードが含まれている場合は、追加のノードのLIFがこれらのゾーンに含まれます。



ホストオペレーティングシステムとマルチパスソフトウェアが、ノード上のLUNへのアクセスに使用される数のパスをサポートしている必要があります。

関連情報

"NetApp Hardware Universe"

Cisco FCおよびFCoEスイッチのゾーニング制限

Cisco FC スイッチおよび FCoE スイッチを使用する場合、 1 つのファブリックゾーンに同じ物理ポートのターゲット LIF を複数含めることはできません。同じポートの LIF を同じゾーンに複数配置すると、接続が失われた場合に LIF ポートがリカバリできなくなる可能性があります。

FC-NVMe プロトコルには、通常の FC スイッチが FC プロトコルとまったく同じ方法で使用されます。

- FC および FCoE プロトコルの複数の LIF は、ゾーンが同じでなければノード上の物理ポートを共有することができます。
- FC-NVMe と FCoE は、同じ物理ポートを共有できません。
- FC と FC-NVMe は、同じ 32Gb 物理ポートを共有できます。

- Cisco FC スイッチおよび FCoE スイッチでは、特定のポートの各 LIF をそのポートの他の LIF とは別のゾーンに配置する必要があります。
- 1 つのゾーンに FC と FCoE 両方の LIF を配置することができます。ゾーンにはクラスタ内のすべてのターゲットポートのLIFを含めることができますが、ホストのパス制限を超えないように注意し、SLMの設定を確認してください。
- 物理ポートが異なる LIF は、同じゾーンに配置することもできます。
- Cisco スイッチを使用する場合は、 LIF を分離する必要があります。

  必須ではありませんが、 LIF の分離はすべてのスイッチで推奨されます

共有SAN構成の要件

共有SAN構成とは、ONTAPストレージシステムと他社のストレージシステムの両方に接続されるホストのことです。ONTAPストレージシステムと他のベンダーのストレージシステムに単一のホストからアクセスする場合は、いくつかの要件を満たす必要があります。

すべてのホストオペレーティングシステムで、各ベンダーのストレージシステムへの接続には別 々 のアダプタを使用することを推奨します。別 々 のアダプタを使用すると、ドライバと設定が競合する可能性が低くなります。ONTAPストレージシステムに接続する場合は、NetApp Interoperability Matrix Toolにサポート対象として記載されているアダプタモデル、BIOS、ファームウェア、ドライバを使用する必要があります。

必須または推奨のタイムアウト値や、ホストのその他のストレージパラメータを設定する必要があります。NetAppソフトウェアをインストールするか、NetApp設定を最後に適用する必要があります。

- AIXの場合、構成に対応するAIX Host Utilitiesバージョンの値をInteroperability Matrix Toolで確認して適用します。
- ESXの場合、Virtual Storage Console for VMware vSphereを使用してホスト設定を適用します。
- HP-UXの場合は、HP-UXのデフォルトのストレージ設定を使用する必要があります。
- Linuxの場合、構成に対応するLinux Host Utilitiesバージョンの値をInteroperability Matrix Toolで確認して適用します。
- Solarisの場合、構成に対応するSolaris Host Utilitiesバージョンの値をInteroperability Matrix Toolで確認して適用します。
- Windowsの場合、構成に対応するWindows Host UtilitiesバージョンをInteroperability Matrix Toolで確認してインストールする必要があります。

関連情報

"NetApp Interoperability Matrix Tool"

MetroCluster環境でのSAN構成

MetroCluster環境でのSAN構成

MetroCluster環境でSAN構成を使用する場合は、一定の考慮事項に注意する必要があります。

- MetroCluster 構成では ' フロントエンド FC ファブリックのルーテッド VSAN 構成はサポートされません
- ONTAP 9 .15.1以降では、NVMe/TCPで4ノードのMetroCluster IP構成がサポートされます。
- ONTAP 9.12.1以降では、NVMe / FCで4ノードのMetroCluster IP構成がサポートされます。MetroCluster構成は、ONTAP 9.12.1よりも前のフロントエンドNVMeネットワークではサポートされません。
- MetroCluster構成では、iSCSI、FC、FCoEなどのその他のSANプロトコルがサポートされます。
- SANクライアント構成を使用している場合は、（IMT）に記載されているメモにMetroCluster構成に関する特別な考慮事項がないかどうかを確認する必要があります"NetApp Interoperability Matrix Tool"。
- MetroClusterの自動計画外スイッチオーバーとTiebreakerまたはMediatorで開始されるスイッチオーバーをサポートするには、オペレーティングシステムとアプリケーションで120秒のI/O耐障害性を提供する必要があります。
- MetroCluster構成では、フロントエンドFCファブリックの両側で同じWWNNとWWPNが使用されます。

関連情報

- "MetroClusterのデータ保護とディザスタリカバリの概要"
- "技術情報アーティクル：「What are AIX Host support considerations in a MetroCluster configuration？」"
- "技術情報アーティクル：「Solaris host support considerations in a MetroCluster configuration」"

スイッチオーバーとスイッチバックの間でポートの重複を防止

SAN環境では、古いポートがオフラインになって新しいポートがオンラインになったときに重複しないようにフロントエンドスイッチを設定できます。

スイッチオーバーの実行中、ディザスタサイトのFCポートがオフラインであることがファブリックで検出され、ネームサービスとディレクトリサービスからこのポートが削除される前に、サバイバーサイトのFCポートがファブリックにログインすることがあります。

災害時にFCポートをまだ削除していない場合、WWPNの重複が原因でサバイバーサイトのFCポートのファブリックログイン試行が拒否されることがあります。FCスイッチのこの動作は、既存のデバイスではなく以前のデバイスのログインを維持するように変更できます。この動作が他のファブリックデバイスに与える影響を確認する必要があります。詳細については、スイッチベンダーにお問い合わせください。

スイッチのタイプに応じて、正しい手順を選択します。

例 **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. コンフィギュレーションモードを開始します。

```
switch# config t
switch(config)#
```

3. ネームサーバデータベースの最初のデバイスエントリを新しいデバイスで上書きします。

```
switch(config)# no fcns reject-duplicate-pwwn vsan 1
```

4. NX-OS 8.xを実行しているスイッチで、flogi quiesce timeoutがゼロに設定されていることを確認します。

   a. 休止時間を表示します。

   ```
   switch(config)# show flogi interval info \| i quiesce
   ```

   ```
   Stats:  fs flogi quiesce timerval:  0
   ```

   b. 前の手順の出力でtimervalがゼロであることが示されていない場合は、ゼロに設定します。

   ```
   switch(config)# flogi scale enable
   ```

```
switch(config)$ flogi quiesce timeout 0
```

Brocadeスイッチ

1. スイッチに接続してログインします。
2. コマンドを入力します `switchDisable`。
3. コマンドを入力し `configure`、プロンプトでを押し `y`ます。

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

4. 設定1を選択：

```
- 0: First login take precedence over the second login (default)
- 1: Second login overrides first login.
- 2: the port type determines the behavior
Enforce FLOGI/FDISC login: (0..2) [0] 1
```

5. 残りのプロンプトに応答するか、 * Ctrl+D* を押します。
6. コマンドを入力します `switchEnable`。

関連情報

"テストまたはメンテナンスのためのスイッチオーバーの実行"

ホストでのマルチパスのサポート

ホストでのマルチパスサポートの概要

ONTAPでは、FCとiSCSIの両方のパスに常にAsymmetric Logical Unit Access（ALUA；非対称論理ユニットアクセス）が使用されます。FCプロトコルとiSCSIプロトコルのALUAをサポートするホスト構成を使用してください。

ONTAP 9 .5以降では、Asynchronous Namespace Access（ANA）を使用するNVMe構成でマルチパスHAペアのフェイルオーバー/ギブバックがサポートされます。ONTAP 9 .4では、NVMeでサポートされるホストからターゲットへのパスは1つだけです。アプリケーションホストは、ハイアベイラビリティ（HA）パートナーへのパスフェイルオーバーを管理する必要があります。

ALUAまたはANAをサポートする具体的なホスト構成については、ご使用のホストオペレーティングシステムに対応したおよび "ONTAP SANホスト構成"を参照して "NetApp Interoperability Matrix Tool"ください。

ホストのマルチパスソフトウェアが必要な場合

Storage Virtual Machine（SVM）の論理インターフェイス（LIF）からファブリックへのパスが複数ある場合は、マルチパスソフトウェアが必要です。ホストが複数のパスを介してLUNにアクセスできる場合は、常にホストにマルチパスソフトウェアが必要です。

マルチパスソフトウェアは、LUNへのすべてのパスで単一のディスクをオペレーティングシステムに提供します。マルチパスソフトウェアがないと、各パスがオペレーティングシステムで別 々 のディスクとして扱われ、データが破損する可能性があります。

次のいずれかに該当する場合、ソリューションには複数のパスがあるとみなされます。

- ホストの単一のイニシエータポートをSVMの複数のSAN LIFに接続している場合
- 複数のイニシエータポートをSVMの単一のSAN LIFに接続している場合
- 複数のイニシエータポートをSVMの複数のSAN LIFに接続している場合

HA構成では、マルチパスソフトウェアを推奨します。選択的LUNマップに加えて、FCスイッチのゾーニングまたはポートセットを使用してLUNへのアクセスに使用するパスを制限することを推奨します。

マルチパスソフトウェアは、マルチパスI/O（MPIO）ソフトウェアとも呼ばれます。

ホストからクラスタ内のノードへの推奨されるパス数

ホストからクラスタ内の各ノードへのパスは8個までにする必要があります。ホストOS

やホストで使用されるマルチパスでサポートされるパスの総数に注意してください。

選択的LUNマップ（SLM）を使用して、クラスタ内のStorage Virtual Machine（SVM）が使用する各レポートノードへのパスをLUNごとに少なくとも2つ確保します。これにより、単一点障害（Single Point of Failure）が排除され、コンポーネント障害からシステムを保護できます。

クラスタにノードが4つ以上ある場合、またはいずれかのノードのSVMで5つ以上のターゲットポートを使用している場合は、次の方法でノード上のLUNへのアクセスに使用できるパスの数を制限して、推奨される最大数の8個を超えないようにすることができます。

- SLM

  SLMを使用すると、ホストからLUNへのパスの数が、LUNを所有するノードとそのHAパートナーのパスだけになります。SLMはデフォルトで有効になっています。

- iSCSIのポートセット
- ホストのFC igroupマッピング
- FCスイッチゾーニング

関連情報

"SAN管理"

構成の制限

SAN構成でサポートされるノード数の確認

ONTAPでサポートされるクラスタあたりのノード数は、ONTAPのバージョン、クラスタ内のストレージコントローラのモデル、およびクラスタノードのプロトコルによって異なります。

タスクの内容

FC、FC-NVMe、FCoE、またはiSCSIが設定されたノードがクラスタにある場合、そのクラスタにはSANノードの制限が適用されます。クラスタ内のコントローラに基づくノードの制限については、 _ Hardware Universe _ を参照してください。

手順

1. に進みます "NetApp Hardware Universe"。
2. 左上の [* ホーム] ボタンの横にある [* プラットフォーム] をクリックし、プラットフォームの種類を選択します。
3. 使用しているONTAPのバージョンの横にあるチェックボックスをオンにします。

   プラットフォームを選択するための新しい列が表示されます。

4. ソリューションで使用するプラットフォームの横にあるチェックボックスをオンにします。
5. [仕様を選択] 列の [すべて選択 *] チェックボックスをオフにします。
6. [クラスタあたりの最大ノード数（ NAS / SAN ） *] チェックボックスをオンにします。

7. [結果を表示（ Show Results ）] をクリックする。

関連情報

"NetApp Hardware Universe"

FC構成およびFC-NVMe構成におけるクラスタあたりのサポートされるホスト数を確認する

クラスタに接続できる SAN ホストの最大数は、クラスタの各ノードに接続されるホストの数、ホストあたりのイニシエータ数、ホストあたりのセッション数、クラスタ内のノード数など、クラスタのさまざまな属性の組み合わせによって大きく異なります。

タスクの内容

FC 構成および FC-NVMe 構成では、システムの Initiator-Target Nexus （ ITN ；イニシエータ - ターゲット接続）の数に基づいて、クラスタにホストを追加できるかどうかを判断します。

1 つの ITN は、ホストのイニシエータからストレージシステムのターゲットへの 1 つのパスに該当します。FC 構成および FC-NVMe 構成のノードあたりの最大 ITN 数は 2 、 048 です。ITN がこの最大数を超えない限り、クラスタにホストを追加することができます。

クラスタで使用されている ITN の数を確認するには、クラスタの各ノードで次の手順を実行します。

手順

1. ノードの LIF をすべて特定します。
2. ノードのすべてのLIFに対して次のコマンドを実行します。

   ```
   fcp initiator show -fields wwpn, lif
   ```

   コマンド出力の一番下に表示されたエントリ数が、その LIF の ITN 数です。
3. それぞれの LIF について、表示された ITN 数を記録します。
4. クラスタのすべてのノードの各 LIF の ITN 数を合計します。

   この値がクラスタの ITN の総数になります。

iSCSI構成でサポートされるホスト数の確認

iSCSI 構成で接続できる SAN ホストの最大数は、クラスタの各ノードに接続されるホストの数、ホストあたりのイニシエータ数、ホストあたりのログイン数、クラスタ内のノード数など、クラスタのさまざまな属性の組み合わせによって大きく異なります。

タスクの内容

ノードに直接または 1 つ以上のスイッチを介して接続できるホストの数は、使用可能なイーサネットポートの数で決まります。使用可能なイーサネットポートの数は、コントローラのモデル、およびコントローラにインストールされているアダプタの数とタイプによって決まります。コントローラおよびアダプタでサポートされるイーサネットポートの数は、 _ Hardware Universe _ で確認できます。

マルチノードクラスタ構成の場合は、ノードあたりの iSCSI セッションの数に基づいて、クラスタにホスト

を追加できるかどうかを判断する必要があります。ノードあたりの iSCSI セッションの最大数をクラスタが下回っている場合は、引き続きクラスタにホストを追加できます。ノードあたりの iSCSI セッションの最大数は、クラスタ内のコントローラのタイプによって異なります。

手順

1. ノードのターゲットポータルグループをすべて特定します。
2. ノードのすべてのターゲットポータルグループについて、それぞれ iSCSI セッションの数を確認します。

   `iscsi session show -tpgroup` *`tpgroup`*

   コマンド出力の一番下に表示されたエントリ数が、そのターゲットポータルグループの iSCSI セッション数です。

3. 各ターゲットポータルグループについて、表示された iSCSI セッション数を記録します。
4. ノードの各ターゲットポータルグループの iSCSI セッション数を追加します。

   この値がノードの iSCSI セッションの総数になります。

FCスイッチノコウセイノセイゲン

ファイバチャネルスイッチには、ポート、ポートグループ、ブレード、およびスイッチごとにサポートされるログイン数など、最大構成制限があります。サポートされる制限については、スイッチベンダーのドキュメントを参照してください。

各FC論理インターフェイス（LIF）がFCスイッチポートにログインします。ノード上の1つのターゲットからのログインの総数は、LIFの数に、基盤となる物理ポートへのログイン数1を足した数です。スイッチベンダーが設定しているログインやその他の設定値の制限を超えないようにしてください。これは、NPIVが有効な仮想環境でホスト側で使用されているイニシエータにも当てはまります。ソリューションで使用しているターゲットまたはイニシエータのログインに関して、スイッチベンダーが設定している制限を超えないようにしてください。

Brocadeスイッチの最大数

Brocade スイッチの最大構成数は、 _Brocade 拡張性ガイドライン _ で確認できます。

Ciscoシステムのスイッチ制限

Ciscoスイッチの構成の制限については、使用しているバージョンのCiscoスイッチソフトウェアのガイドを参照して "Cisco設定の制限"ください。

キュー深度の計算の概要

ノードおよびFCポートのファンインあたりのITN数を最大にするために、ホストのFCキュー深度の調整が必要になる場合があります。LUNの最大数と1つのFCポートに接続できるHBAの数は、FCターゲット ポートで使用可能なキューの深度によって制限されます。

タスクの内容

キュー深度は、ストレージコントローラで一度にキューに格納できるI/O要求（SCSIコマンド）の数です。ホ

ストのイニシエータHBAからストレージコントローラのターゲットアダプタへのI/O要求ごとに、キューエントリが1つ作成されます。通常、キュー深度が大きいほどパフォーマンスは向上します。ただし、ストレージコントローラの最大キュー深度に達すると、ストレージコントローラはQFULL応答を返して受信コマンドを拒否します。QFULL状態が発生するとシステムパフォーマンスが大幅に低下し、一部のシステムでエラーが発生する可能性があるため、1台のストレージコントローラに多数のホストがアクセスしている場合は、QFULLが発生しないように慎重に計画する必要があります。

複数のイニシエータ（ホスト）を含む構成では、すべてのホストでキュー深度を同程度に設定する必要があります。同じターゲットポートを介してストレージコントローラに接続されているホスト間でキュー深度が異なるため、キュー深度が小さいホストは、キュー深度が大きいホストからリソースにアクセスできなくなります。

キュー深度を「チューニング」する場合は、次の一般的な推奨事項を考慮してください。

- 小規模から中規模のシステムでは、HBAキュー深度を32にします。
- 大規模なシステムでは、HBAキュー深度を128にします。
- 例外的なケースやパフォーマンステストでは、キュー深度を256にして、キューの問題の可能性を回避します。
- すべてのホストに均等にアクセスできるようにするには、すべてのホストのキュー深度を同じ値に設定する必要があります。
- パフォーマンスの低下やエラーを回避するために、ストレージコントローラのターゲットFCポートのキュー深度を超えないようにする必要があります。

手順

1. 1つのFCターゲットポートに接続しているすべてのホストのFCイニシエータの総数を数えます。
2. 128を掛けます。
   - 2 、 048 より小さい場合は、すべてのイニシエータのキュー深度を 128 に設定します。15台のホストがあり、1つのイニシエータがストレージコントローラ上の2つのターゲットポートのそれぞれに接続されています。15 × 128 = 1 、 920 。これは合計最大キュー深度の 2 、 048 より少ないため、すべてのイニシエータのキュー深度を 128 に設定できます。
   - この値が 2 、 048 よりも大きい場合は、手順 3 に進みます。30台のホストがあり、1つのイニシエータがストレージコントローラ上の2つのターゲットポートのそれぞれに接続されています。30 × 128 = 3 、 840 。これは合計最大キュー深度の 2 、 048 より大きいため、手順 3 に記載されているいずれかのオプションを実行して調整します。
3. 次のいずれかのオプションを選択して、ストレージコントローラにホストを追加します。
   - オプション1：
     i. FCターゲットポートを追加します。
     ii. FCイニシエータを再配置します。
     iii. 手順1と2を繰り返します。+ 必要なキュー深度 3 、 840 は、ポートあたりの使用可能なキュー深度を超えています。これを解決するには、各コントローラに2ポートのFCターゲットアダプタを追加し、30台のホストのうち15台を1つのポートセットに接続し、残りの15台を2つ目のポートセットに接続するようにFCスイッチをゾーニングし直します。これで、ポートあたりのキュー深度は 15 × 128 = 1 、 920 となります。
   - オプション2：
     i. 各ホストを「ラージ」または「モール」として指定します。これは、予想される I/O ニーズに基づいています。

ii. 大規模イニシエータの数に128を掛けます。

iii. 小規模イニシエータの数に32を掛けます。

iv. 2つの結果を足し合わせます。

v. 2 、 048 より小さい場合は、大規模ホストのキュー深度を 128 に、小規模ホストのキュー深度を 32 に設定します。

vi. 2 、 048 よりも大きい場合は、合計キュー深度が 2 、 048 以下になるまで各イニシエータのキュー深度を下げます。

> 特定の1秒あたりのI/Oスループットを達成するために必要なキュー深度を見積もるには、次の式を使用します。
>
> 必要なキュー深度=（1秒あたりのI/O数）×（応答時間）
>
> たとえば、応答時間 3 ミリ秒で 40 、 000 IOPS のスループットに必要なキュー深度は、 40 、 000 × （ .003 ） = 120 です。

基本的な推奨構成に従ってキュー深度を32に制限した場合、ターゲットポートに接続できるホストの最大数は64です。ただし、キュー深度を128にすると、1つのターゲットポートに接続できるホストの最大数は16になります。キュー深度が大きいほど、1つのターゲットポートでサポートできるホストの数が少なくなります。キュー深度を妥協できないような要件の場合は、追加のターゲットポートを用意する必要があります。

必要とされるキュー深度 3 、 840 は、ポートあたりの使用可能なキュー深度を超えています。ストレージ I/O のニーズが高い「大規模」ホストが 10 台あり、 I/O のニーズが低い「モール」ホストが 20 台あります。大規模ホストのイニシエータのキュー深度を128に、小規模ホストのイニシエータのキュー深度を32に設定します。

その結果、合計キュー深度は（ 10 × 128 ） + （ 20 × 32 ） = 1 、 920 になります。

使用可能なキュー深度を、各イニシエータに均等に分配できます。

そのため、イニシエータあたりのキュー深度は 2 、 048 ÷ 30 = 68 となります。

SAN ホストでキュー深度を設定します

ノードあたりおよびFCポートのファンインあたりのITN数を最大にするために、ホストのキュー深度の変更が必要になる場合があります。

AIX ホスト

AIXホストのキュー深度は、コマンドを使用して変更できます `chdev`。コマンドを使用して行った変更 `chdev`はリブート後も維持されます。

例：

- hdisk7デバイスのキュー深度を変更するには、次のコマンドを使用します。

```
chdev -l hdisk7 -a queue_depth=32
```

- fcs0 HBAのキュー深度を変更するには、次のコマンドを使用します。

```
chdev -l fcs0 -a num_cmd_elems=128
```

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

> 場合によっては、コマンドと `makdev -l fcs0 -P`コマンドを使用してHBAをオフラインにして変更後にオンラインに戻し `rmdev -l fcs0 -R`なければならないことがあり `num_cmd_elems`ます。

HP-UX ホスト

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

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

  `scsi_max_qdepth`コマンドのオプションを `kmtune`使用すると、実行中のシステムで動的に変更できます `-u`。この変更は、システム上のすべてのデバイスに有効になります。たとえば、LUNのキュー深度を64に増やすには、次のコマンドを使用します。

  ```
  kmtune -u -s scsi_max_qdepth=64
  ```

  コマンドを使用すると、個 々 のデバイスファイルのキュー深度を変更でき `scsictl`ます。コマンドを使用した変更 `scsictl`は、システムのリブート後は維持されません。特定のデバイスファイルのキュー深度を表示および変更するには、次のコマンドを実行します。

  ```
  scsictl -a /dev/rdsk/c2t2d0
  ```

  ```
  scsictl -m queue_depth=16 /dev/rdsk/c2t2d0
  ```

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

  変更を有効にするには、カーネルを再構築し、システムを再起動する必要があり `max_fcp_reqs`ます。たとえば、HBAのキュー深度を256に変更するには、次のコマンドを使用します。

  ```
  kmtune -u -s max_fcp_reqs=256
  ```

Solaris ホストの場合

SolarisホストのLUNおよびHBAのキュー深度を設定できます。

- LUN のキュー深度の場合：ホストで使用中の LUN の数に LUN あたりのスロットル（ lun-queue-depth ）をかけた値が、ホストの tgt-queue-depth の値以下になる必要があります。
- Sunスタックのキュー深度の場合：標準ドライバでは、LUN単位またはターゲット単位でHBAレベルを設定することはできません `max_throttle`。ネイティブドライバの値は、ファイルおよび `/kernel/drv/ssd.conf`ファイルのデバイスタイプ（`VID_PID`）単位で設定することを `/kernel/drv/sd.conf`推奨します `max_throttle`。ホストユーティリティでは、この値がMPxIO構成では64、Veritas DMP構成では8に設定されます。

手順

1. `# cd/kernel/drv`

2. `# vi lpfc.conf`
3. 検索対象 `/tft-queue (/tgt-queue)`

   `tgt-queue-depth=32`

   デフォルト値はインストール時に32に設定されます。

4. 環境の構成に基づいて、必要な値を設定します。
5. ファイルを保存します。
6. コマンドを使用してホストをリブートし `sync; sync; sync; reboot -- -r`ます。

QLogicHBAヨウノ**VMware**ホスト

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

手順

1. rootユーザとしてサービスコンソールにログオンします。
2. コマンドを使用し `#vmkload_mod -l`て、現在ロードされているQlogic HBAモジュールを確認します。
3. Qlogic HBAの単一インスタンスの場合は、次のコマンドを実行します。

   `#esxcfg-module -s ql2xmaxqdepth=64 qla2300_707`

   この例では、qla2300_707モジュールを使用しています。の出力に基づいて、適切なモジュールを使用し `vmkload_mod -l`ます。

4. 次のコマンドを使用して変更を保存します。

   `#/usr/sbin/esxcfg-boot -b`

5. 次のコマンドを使用してサーバをリブートします。

   `#reboot`

6. 次のコマンドを使用して変更を確認します。
   a. `#esxcfg-module -g qla2300_707`
   b. `qla2300_707 enabled = 1 options = 'ql2xmaxqdepth=64'`

Emulex HBAヨウノ**VMware**ホスト

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

手順

1. rootユーザとしてサービスコンソールにログオンします。
2. コマンドを使用し `#vmkload_mod -l grep lpfc`て、どのEmulex HBAが現在ロードされているかを確認しま

す。

3. Emulex HBAの単一インスタンスの場合は、次のコマンドを入力します。

```
#esxcfg-module -s lpfc0_lun_queue_depth=16 lpfcdd_7xx
```

> HBAのモデルに応じて、モジュールはlpfcdd_7xxまたはlpfcdd_732のいずれかになります。上記のコマンドはlpfcdd_7xxモジュールを使用します。の結果に基づいて、適切なモジュールを使用する必要があります `vmkload_mod -l`。

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

4. Emulex HBAの複数のインスタンスの場合は、次のコマンドを実行します。

```
a esxcfg-module -s "lpfc0_lun_queue_depth=16 lpfc1_lun_queue_depth=16"
lpfcdd_7xx
```

lpfc0のLUNキュー深度とlpfc1のLUNキュー深度が16に設定されます。

5. 次のコマンドを入力します。

```
#esxcfg-boot -b
```

6. を使用してリブートします `#reboot`

Emulex HBAヨウノ**Windows**ホスト

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

手順

1. ディレクトリにあるユーティリティを `C:\WINNT\system32`実行し `LPUTILNT`ます。
2. 右側のメニューから * Drive Parameters * （ドライブパラメータ）を選択します。
3. スクロールダウンして、 [**QueueDepth**] をダブルクリックします。

> 150 より大きい * QueueDepth * を設定する場合は、次の Windows レジストリ値も適切に増やす必要があります。
>
> `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\lpxnds\Parameters\Device\NumberOfRequests`

Qlogic HBA用の**Windows**ホスト

Windowsホストでは、およびHBAマネージャユーティリティを使用してQlogic HBAのキュー深度を更新できます `SANsurfer`。

手順

1. HBAマネージャユーティリティを実行し `SANsurfer`ます。
2. [* HBA ポート **>** 設定] をクリックします。

3. リスト・ボックスの * HBA ポートの詳細設定 * をクリックします。
4. パラメータを更新し `Execution Throttle`ます。

Emulex HBAヨウノ**Linux**ホスト

Linux ホストでは Emulex HBA のキュー深度を更新できます。更新をリブート後も維持するには、新しい RAM ディスクイメージを作成してホストをリブートする必要があります。

手順

1. 変更するキュー深度パラメータを特定します。

   ```
   modinfo lpfc|grep queue_depth
   ```

   キュー深度パラメータとその概要のリストが表示されます。使用しているオペレーティングシステムのバージョンに応じて、次のキュー深度パラメータを 1 つ以上変更できます。

   - `lpfc_lun_queue_depth`：特定のLUNのキューに格納できるFCコマンドの最大数（uint）
   - `lpfc_hba_queue_depth`：lpfc HBAのキューに格納できるFCコマンドの最大数（uint）
   - `lpfc_tgt_queue_depth`：特定のターゲットポートのキューに格納できるFCコマンドの最大数（uint）

     > `lpfc_tgt_queue_depth`パラメータは、`Red Hat Enterprise Linux 7.x`システム、`SUSE Linux Enterprise Server 11 SP4`システム、および`12.x`システムにのみ適用されます。

2. キュー深度を更新するには、Red Hat Enterprise Linux 5.xシステムの場合はファイル、Red Hat Enterprise Linux 6.x / 7.xシステム、またはSUSE Linux Enterprise Server 11.x / 12.xシステムの場合はファイルに、`/etc/modprobe.d/scsi.conf`キュー深度パラメータを追加します `/etc/modprobe.conf`。

   使用しているオペレーティングシステムのバージョンに応じて、次のコマンドを 1 つ以上追加できます。

   - `options lpfc lpfc_hba_queue_depth=new_queue_depth`
   - `options lpfc lpfc_lun_queue_depth=new_queue_depth`
   - `options lpfc_tgt_queue_depth=new_queue_depth`

3. 新しい RAM ディスクイメージを作成し、ホストをリブートして、リブート後も更新内容を維持します。

   詳細については、使用しているLinuxオペレーティングシステムのバージョンに対応したを参照してください"システム管理"。

4. 変更したキュー深度パラメータの値が更新されていることを確認します。

   ```
   root@localhost ~]#cat /sys/class/scsi_host/host5/lpfc_lun_queue_depth
         30
   ```

   キュー深度の現在の値が表示されます。

QLogicHBAヨウノLinuxホスト

Linux ホストでは QLogic ドライバのデバイスキュー深度を更新できます。更新をリブート後も維持するには、新しい RAM ディスクイメージを作成してホストをリブートする必要があります。QLogic HBA のキュー深度を変更するには、 QLogic HBA の管理 GUI またはコマンドラインインターフェイス（ CLI ）を使用します。

このタスクでは、 QLogic HBA の CLI を使用して QLogic HBA のキュー深度を変更する方法を示します

手順

1. 変更するデバイスキュー深度パラメータを特定します。

   ```
   modinfo qla2xxx | grep ql2xmaxqdepth
   ```

   変更できるのはキュー深度パラメータのみ `ql2xmaxqdepth`です。このパラメータは、LUNごとに設定できる最大キュー深度を示します。RHEL 7.5以降のデフォルト値は64です。RHEL 7.4以前のデフォルト値は32です。

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

2. デバイスのキュー深度の値を更新します。

   - 永続的に変更する場合は、次の手順を実行します。

     i. キュー深度を更新するには、Red Hat Enterprise Linux 5.xシステムの場合はファイルに、`/etc/modprobe.d/scsi.conf`Red Hat Enterprise Linux 6.x / 7.xシステムまたはSUSE Linux Enterprise Server 11.x / 12.xシステムの場合はファイルに、キュー深度パラメータを追加し `/etc/modprobe.conf`ます。 `options qla2xxx ql2xmaxqdepth=new_queue_depth`

     ii. 新しい RAM ディスクイメージを作成し、ホストをリブートして、リブート後も更新内容を維持します。

     詳細については、使用しているLinuxオペレーティングシステムのバージョンに対応したを参照してください"システム管理"。

   - 現在のセッションだけでパラメータを変更する場合は、次のコマンドを実行します。

     ```
     echo new_queue_depth > /sys/module/qla2xxx/parameters/ql2xmaxqdepth
     ```

     次の例では、キュー深度を 128 に設定します。

   ```
   echo 128 > /sys/module/qla2xxx/parameters/ql2xmaxqdepth
   ```

3. キュー深度の値が更新されたことを確認します。

   ```
   cat /sys/module/qla2xxx/parameters/ql2xmaxqdepth
   ```

キュー深度の現在の値が表示されます。

4. QLogic HBA BIOSからファームウェアパラメータを更新して、QLogic HBAのキュー深度を変更します `Execution Throttle`。

   a. QLogic HBA管理CLIにログインします。

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

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

      ```
      [root@localhost ~]#
      /opt/QLogic_Corporation/QConvergeConsoleCLI/qaucli
      Using config file:
      /opt/QLogic_Corporation/QConvergeConsoleCLI/qaucli.cfg
      Installation directory: /opt/QLogic_Corporation/QConvergeConsoleCLI
      Working dir: /root

      QConvergeConsole

              CLI - Version 2.2.0 (Build 15)

          Main Menu

          1:  Adapter Information
          **2:  Adapter Configuration**
          3:  Adapter Updates
          4:  Adapter Diagnostics
          5:  Monitoring
          6:  FabricCache CLI
          7:  Refresh
          8:  Help
          9:  Exit


              Please Enter Selection: 2
      ```

   c. アダプタ設定パラメータのリストから、オプションを選択し `HBA Parameters`ます。

```
1:  Adapter Alias
    2:  Adapter Port Alias
    **3:  HBA Parameters**
    4:  Persistent Names (udev)
    5:  Boot Devices Configuration
    6:  Virtual Ports (NPIV)
    7:  Target Link Speed (iiDMA)
    8:  Export (Save) Configuration
    9:  Generate Reports
   10:  Personality
   11:  FEC
(p or 0: Previous Menu; m or 98: Main Menu; ex or 99: Quit)
        Please Enter Selection: 3
```

d. HBA ポートのリストから、必要な HBA ポートを選択します。

```
Fibre Channel Adapter Configuration

    HBA Model QLE2562 SN: BFD1524C78510
      1: Port   1: WWPN: 21-00-00-24-FF-8D-98-E0 Online
      2: Port   2: WWPN: 21-00-00-24-FF-8D-98-E1 Online
    HBA Model QLE2672 SN: RFE1241G81915
      3: Port   1: WWPN: 21-00-00-0E-1E-09-B7-62 Online
      4: Port   2: WWPN: 21-00-00-0E-1E-09-B7-63 Online


        (p or 0: Previous Menu; m or 98: Main Menu; ex or 99: Quit)
        Please Enter Selection: 1
```

HBA ポートの詳細が表示されます。

e. [HBA Parameters]メニューで、オプションの現在の値を表示するオプションを `Execution Throttle`選択します `Display HBA Parameters。

このオプションのデフォルト値 `Execution Throttle`は65535です。

```
HBA Parameters Menu

======================================================
HBA           : 2 Port: 1
SN            : BFD1524C78510
HBA Model     : QLE2562
HBA Desc.     : QLE2562 PCI Express to 8Gb FC Dual Channel
FW Version    : 8.01.02
```

```
WWPN          : 21-00-00-24-FF-8D-98-E0
WWNN          : 20-00-00-24-FF-8D-98-E0
Link          : Online
=====================================================

    1:  Display HBA Parameters
    2:  Configure HBA Parameters
    3:  Restore Defaults


        (p or 0: Previous Menu; m or 98: Main Menu; x or 99: Quit)
        Please Enter Selection: 1
-------------------------------------------------------------------------
--------
HBA Instance 2: QLE2562 Port 1 WWPN 21-00-00-24-FF-8D-98-E0 PortID 03-
07-00
Link: Online
-------------------------------------------------------------------------
--------
Connection Options             : 2 - Loop Preferred, Otherwise Point-to-
Point
Data Rate                      : Auto
Frame Size                     : 2048
Hard Loop ID                   : 0
Loop Reset Delay (seconds)     : 5
Enable Host HBA BIOS           : Enabled
Enable Hard Loop ID            : Disabled
Enable FC Tape Support         : Enabled
Operation Mode                 : 0 - Interrupt for every I/O completion
Interrupt Delay Timer (100us)  : 0
**Execution Throttle             : 65535**
Login Retry Count              : 8
Port Down Retry Count          : 30
Enable LIP Full Login          : Enabled
Link Down Timeout (seconds)    : 30
Enable Target Reset            : Enabled
LUNs Per Target                : 128
Out Of Order Frame Assembly    : Disabled
Enable LR Ext. Credits         : Disabled
Enable Fabric Assigned WWN     : N/A

Press <Enter> to continue:
```

a. Enter * を押して続行します。

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

c. [Configure Parameters]メニューからオプションを選択し `Execute Throttle`、このパラメータの値を更新します。

```
Configure Parameters Menu

=======================================================
HBA           : 2 Port: 1
SN            : BFD1524C78510
HBA Model     : QLE2562
HBA Desc.     : QLE2562 PCI Express to 8Gb FC Dual Channel
FW Version    : 8.01.02
WWPN          : 21-00-00-24-FF-8D-98-E0
WWNN          : 20-00-00-24-FF-8D-98-E0
Link          : Online
=======================================================

    1:  Connection Options
    2:  Data Rate
    3:  Frame Size
    4:  Enable HBA Hard Loop ID
    5:  Hard Loop ID
    6:  Loop Reset Delay (seconds)
    7:  Enable BIOS
    8:  Enable Fibre Channel Tape Support
    9:  Operation Mode
   10:  Interrupt Delay Timer (100 microseconds)
   11:  Execution Throttle
   12:  Login Retry Count
   13:  Port Down Retry Count
   14:  Enable LIP Full Login
   15:  Link Down Timeout (seconds)
   16:  Enable Target Reset
   17:  LUNs per Target
   18:  Enable Receive Out Of Order Frame
   19:  Enable LR Ext. Credits
   20:  Commit Changes
   21:  Abort Changes


        (p or 0: Previous Menu; m or 98: Main Menu; x or 99: Quit)
        Please Enter Selection: 11
Enter Execution Throttle [1-65535] [65535]: 65500
```

d. Enter * を押して続行します。

e. [Configure Parameters]メニューから、変更を保存するオプションを選択し `Commit Changes`ます。

f. メニューを終了します。