



ファブリック接続 **MetroCluster**  
をインストール  
ONTAP MetroCluster

NetApp  
February 13, 2026

# 目次

ファブリック接続 MetroCluster をインストール	1
概要	1
MetroCluster のインストールを準備	1
ONTAP MetroCluster 構成の違い	1
クラスタピアリング	2
ISL に関する考慮事項	5
ファブリック接続 MetroCluster 構成で TDM / WDM 機器を使用する場合の考慮事項	6
Brocade DCX 8510-8 スイッチを使用するための要件	8
ミラーされていないアグリゲートを使用する場合の	9
MetroCluster サイトでのファイアウォールの使用状況	10
ファブリック接続 MetroCluster 構成をケーブル接続	10
ファブリック接続 MetroCluster 構成のケーブル接続	10
ファブリック MetroCluster 構成のコンポーネント	11
必要な MetroCluster FC コンポーネントと命名規則	18
FC スイッチおよび FC-to-SAS ブリッジの設定ワークシート	22
MetroCluster コンポーネントを設置してケーブルを配線します	22
FC スイッチを設定	55
FC-to-SAS ブリッジおよび SAS ディスクシェルフを設置	183
ONTAP で MetroCluster FC ソフトウェアを設定する	197
必要な情報の収集	198
標準クラスタ構成と MetroCluster 構成の類似点 / 相違点	204
メンテナンスモードでコンポーネントの HA 状態を確認および設定する	205
システムのデフォルト設定をリストアし、コントローラモジュールで HBA タイプを設定しています	206
FAS8020 システムでの X1132A-R6 クアッドポートカードの FC-VI ポートの設定	208
メンテナンスモードでの 8 ノードまたは 4 ノード構成のディスク割り当ての検証	210
保守モードでの 2 ノード構成のディスク割り当ての検証	217
ONTAP をセットアップしています	219
クラスタを MetroCluster 構成に設定	224
Config Advisor での MetroCluster 構成エラーの確認	256
ローカル HA の処理を検証しています	256
スイッチオーバー、修復、スイッチバックを検証しています	258
構成バックアップファイルを保護しています	258
MetroCluster 設定で仮想 IP およびボーダーゲートウェイプロトコルを使用する場合の考慮事項	258
ONTAP の制限事項	259
このレイヤ 3 解決策を MetroCluster 設定で使用する場合の注意事項	260
MetroCluster 構成をテストする	261
ネゴシエートスイッチオーバーを検証中	261
修復と手動スイッチバックの検証	263
単一の FC-to-SAS ブリッジの停止	265

電源回線切断後の動作確認	267
スイッチファブリック障害後の動作確認	268
単一のストレージシェルフが停止したあとの動作確認	270
MetroCluster 構成を削除	280
Active IQ Unified Manager と ONTAP System Manager を使用して設定と監視を強化する方法	281
Active IQ Unified Manager および ONTAP システムマネージャを使用して詳細な設定と監視を行う	281
NTP を使用してシステム時刻を同期します	281
MetroCluster 構成で ONTAP を使用する場合の考慮事項	282
MetroCluster 構成での FlexCache のサポート	283
MetroCluster 構成での FabricPool のサポート	284
MetroCluster 構成での FlexGroup のサポート	285
MetroCluster 構成での整合グループのサポート	285
MetroCluster 構成のジョブスケジュール	285
MetroCluster サイトから第 3 のクラスタへのクラスタピアリング	285
MetroCluster 構成での LDAP クライアント設定のレプリケーション	285
MetroCluster 構成用のネットワーク設定および LIF 作成ガイドライン	285
MetroCluster 構成の SVM ディザスタリカバリ	291
MetroCluster スイッチオーバー後に storage aggregate plex show コマンドの出力が確定しない	294
スイッチオーバー発生時に NVFAIL フラグを設定するためのボリュームの変更	294
追加情報の参照先	295
MetroCluster およびその他の情報	295

# ファブリック接続 MetroCluster をインストール

## 概要

ファブリック接続 MetroCluster 構成をインストールするには、いくつかの手順を正しい順序で実行する必要があります。

- "インストールを準備し、すべての要件を理解します"。
- "コンポーネントをケーブル接続します"
- "ソフトウェアを設定します"
- "設定をテストします"

## MetroCluster のインストールを準備

### ONTAP MetroCluster 構成の違い

MetroCluster 構成のタイプごとに、必要なコンポーネントが異なります。

いずれの構成においても、2つの MetroCluster サイトがそれぞれ ONTAP クラスタとして構成されます。2ノード MetroCluster 構成では、各ノードがシングルノードクラスタとして構成されます。

フィーチャー (Feature)	IP 構成	ファブリック接続構成		ストレッチ構成	
		* 4 ノードまたは 8 ノード *	* 2 ノード *	* 2 ノードブリッジ接続 *	* 2 ノード直接接続 *
コントローラ数	4または8 <sup>1</sup>	4 台または 8 台	2 つ	2 つ	2 つ
FC スイッチストレージファブリックを使用します	いいえ	はい。	はい。	いいえ	いいえ
IP スイッチストレージファブリックを使用します	はい。	いいえ	いいえ	いいえ	いいえ
FC-to-SAS ブリッジを使用します	いいえ	はい。	はい。	はい。	いいえ
直接接続型 SAS ストレージを使用します	○ (ローカル接続のみ)	いいえ	いいえ	いいえ	はい。

ADP をサポート します	○ (ONTAP 9.4 以降)	いいえ	いいえ	いいえ	いいえ
ローカル HA を サポートします	はい。	はい。	いいえ	いいえ	いいえ
ONTAP 自動計 画外スイッチオ ーバー (AUSO ) のサポート	いいえ	はい。	はい。	はい。	はい。
ミラーされてい ないアグリゲー トを	○ (ONTAP 9.8 以降)	はい。	はい。	はい。	はい。
ONTAP メディ エーターをサポ ートします	○ (ONTAP 9.7 以降)	いいえ	いいえ	いいえ	いいえ
MetroCluster Tiebreaker をサ ポートします	○ (ONTAP メデ ィエーターとの 併用は不可)	はい。	はい。	はい。	はい。
をサポートしま す <a href="#">すべての SAN アレイ</a>	はい。	はい。	はい。	はい。	はい。

• メモ \*

1. 8ノードMetroCluster IP構成について、次の考慮事項を確認してください。

- ONTAP 9.9.1 以降では、8 ノード構成がサポートされます。
- ネットアップ検証済みの MetroCluster スイッチ（ネットアップから購入したもの）のみがサポートされます。
- IP ルーティング（レイヤ 3）バックエンド接続を使用する設定はサポートされていません。

**MetroCluster** 構成でのオール **SAN** アレイシステムのサポート

All SAN Array（ASA）の一部は、MetroCluster 構成でサポートされています。MetroCluster のドキュメントで、AFF モデルの情報環境対応する ASA システムを確認します。たとえば、すべてのケーブル配線と AFF A400 システムのその他の情報は、ASA AFF A400 システムも環境に接続します。

サポートされるプラットフォーム構成は、に記載されています ["NetApp Hardware Universe の略"](#)。

クラスタピアリング

各 MetroCluster サイトは、パートナーサイトのピアとして設定されます。ピア関係を設定するための前提条件とガイドラインを理解しておく必要があります。これは、それらの関係に共有ポートと専用ポートのどちらを使用するかを決定する際に重要になりま

す。

## 関連情報

### "クラスタと SVM のピアリングの簡単な設定"

#### クラスタピアリングの前提条件

クラスタピアリングを設定する前に、ポート、IP アドレス、サブネット、ファイアウォール、およびクラスタの命名要件の間の接続が満たされていることを確認する必要があります。

#### 接続要件

ローカルクラスタのすべてのクラスタ間 LIF が、リモートクラスタのすべてのクラスタ間 LIF と通信できる必要があります。

必須ではありませんが、一般に、クラスタ間 LIF には同じサブネットの IP アドレスを使用した方が構成がシンプルになります。IP アドレスは、データ LIF と同じサブネット内や、別のサブネット内に存在できます。各クラスタで使用するサブネットは、次の要件を満たしている必要があります。

- サブネットには、各ノードに 1 つのインタークラスタ LIF が割り当てられる十分な数の IP アドレスが必要です。

たとえば、4 ノードクラスタの場合、クラスタ間通信で使用するサブネットには、使用可能な IP アドレスが 4 つ必要です。

クラスタ間ネットワークでは、各ノードにインタークラスタ LIF と IP アドレスが必要です。

クラスタ間 LIF のアドレスには IPv4 または IPv6 のいずれかを使用できます。



ONTAP 9 では、必要に応じて IPv4 プロトコルと IPv6 プロトコルがクラスタ間 LIF に共存することを許可し、IPv4 から IPv6 にピアリングネットワークを移行できます。以前のリリースでは、クラスタ全体のすべてのクラスタ間関係が IPv4 または IPv6 のどちらかだったため、プロトコルの変更はシステム停止を伴うイベントでした。

#### ポート要件

クラスタ間通信には専用のポートを使用することも、データネットワークで使用されているポートを共有することもできます。ポートは、次の要件を満たしている必要があります。

- あるリモートクラスタとの通信に使用するポートは、すべて同じ IPspace に属している必要があります。

複数のクラスタとのピア関係の作成には複数の IPspace を使用できます。ペアワイズのフルメッシュ接続は IPspace 内でのみ必要になります。

- クラスタ間通信で使用されるブロードキャストドメインに、1 ノードあたり最低 2 つのポートがあり、クラスタ間通信で別のポートへのフェイルオーバーが可能になっている。

ブロードキャストドメインに追加できるポートは、物理ネットワークポート、VLAN、インターフェイスグループ (ifgrps) です。

- すべてのポートが接続されている。

- すべてのポートが正常な状態である必要があります。
- ポートの MTU 設定が一貫している。

#### ファイアウォールの要件

ファイアウォールとクラスタ間ファイアウォールポリシーでは、次のプロトコルを許可する必要があります。

- ICMP サービス
- ポート 10000、11104、および 11105 経由でのすべてのインタークラスタ LIF の IP アドレスへの TCP 接続
- クラスタ間 LIF 間の双方向 HTTPS

デフォルトのクラスタ間ファイアウォールポリシーは、HTTPS プロトコル経由のアクセス、およびすべての IP アドレス（0.0.0.0/0）からのアクセスを許可します。ポリシーは必要に応じて変更または置き換えできません。

#### 専用のポートを使用する場合の考慮事項

専用のポートを使用することが適切なクラスタ間ネットワーク解決策であるかどうかを判断するには、LAN のタイプ、利用可能な WAN 帯域幅、レプリケーション間隔、変更率、ポート数などの設定や要件を考慮する必要があります。

専用のポートを使用することがクラスタ間ネットワーク解決策として適切であるかどうかを判断するには、ネットワークについて次の事項を考慮してください。

- 使用できる WAN 帯域幅が LAN ポートの帯域幅とほぼ同じで、レプリケーション間隔の設定により、通常のクライアントアクティビティが実行されている間にレプリケーションが実行される場合は、クラスタ間レプリケーションにイーサネットポートを専用に割り当てて、レプリケーションとデータプロトコルとの競合を回避します。
- データプロトコル（CIFS、NFS、iSCSI）によるネットワーク利用率が 50% を超える場合は、レプリケーションにポートを専用に割り当てて、ノードのフェイルオーバーが発生してもパフォーマンスが低下しないようにします。
- 10GbE 以上の物理ポートがデータとレプリケーションの両方に使用されている場合は、レプリケーション用に VLAN ポートを作成し、論理ポートをクラスタ間レプリケーション専用にすることができます。

ポートの帯域幅は、すべての VLAN とベースポートで共有されます。

- データの変更率とレプリケーション間隔について検討し、間隔ごとにレプリケートする必要があるデータの量に十分な帯域幅が必要かどうかを検討します。データポートを共有すると、原因がデータプロトコルと競合する可能性があります。

#### データポートを共有する場合の考慮事項

クラスタ間レプリケーションのためにデータポートを共有することが、正しいクラスタ間ネットワーク解決策であるかどうかを判断するには、LAN のタイプ、利用可能な WAN 帯域幅、レプリケーション間隔、変更率、ポート数などの設定や要件を考慮する必要があります。

データポートを共有することがクラスタ間接続解決策として適切であるかどうかを判断するには、ネットワークについて次の事項を考慮してください。

- 40 ギガビットイーサネット（40GbE）ネットワークのように高速なネットワークの場合は、データアクセスに使用されるのと同じ 40GbE ポート上に、レプリケーションを実行するためのローカル LAN 帯域幅が十分にあると考えられます。

多くの場合、使用できる WAN 帯域幅は、10GbE の LAN 帯域幅よりもはるかに少なくなります。

- クラスタ内のすべてのノードが、データをレプリケートし、使用できる WAN 帯域幅を共有しなければならない場合、データポートを共有する方法は、比較的許容できる選択肢となります。
- データ用とレプリケーション用のポートを共有すると、ポートをレプリケーション専用にする場合の追加のポート数が不要になります。
- レプリケーションネットワークの最大伝送ユニット（MTU）サイズは、データネットワークで使用されるサイズと同じになります。
- データの変更率とレプリケーション間隔について検討し、間隔ごとにレプリケートする必要があるデータの量に十分な帯域幅が必要かどうかを検討します。データポートを共有すると、原因がデータプロトコルと競合する可能性があります。
- データポートをクラスタ間レプリケーション用に共有すると、同じノード上にある他の任意のクラスタ間対応ポートにクラスタ間 LIF を移行して、レプリケーションに使用する特定のデータポートを制御できます。

## ISL に関する考慮事項

MetroCluster 構成では、各 FC スイッチファブリックに必要な ISL の数を確認する必要があります。ONTAP 9.2 以降では、MetroCluster 構成ごとに専用の FC スイッチと ISL を使用する代わりに、同じ 4 つのスイッチを共有できる場合があります。

### ISL の共有に関する考慮事項（ONTAP 9.2）

ONTAP 9.2 以降では、次の場合に ISL を共有できます。

- 2 ノード MetroCluster 構成 × 1 と 4 ノード 構成 × 1
- 4 ノード MetroCluster 構成 × 2
- 2 ノード MetroCluster 構成 × 2
- 2 つの DR グループを 1 つの 8 ノード MetroCluster 構成に含めます

共有スイッチ間に必要な ISL の数は、共有スイッチに接続されているプラットフォームモデルの帯域幅によって異なります。

構成に必要な ISL の数を決定する際は、次の点を考慮してください。

- バックエンド MetroCluster 接続を提供する FC スイッチに MetroCluster 以外のデバイスを接続しないでください。
- ISL の共有は、Cisco 9250i スイッチと Cisco 9148 スイッチを除くすべてのスイッチでサポートされません。
- すべてのノードで ONTAP 9.2 以降が実行されている必要があります。
- ISL を共有する場合の FC スイッチのケーブル接続は、8 ノード MetroCluster の場合と同じです。
- ISL を共有する場合に使用する RCF ファイルは、8 ノードの MetroCluster ケーブル接続の場合と同じで

す。

- すべてのハードウェアとソフトウェアのバージョンがサポートされていることを確認する必要があります。

#### "NetApp Hardware Universe の略"

- ISL の速度と数は、両方の MetroCluster システムのクライアント負荷に対応できるようにサイジングする必要があります。
- バックエンドの ISL とコンポーネントは、MetroCluster 構成専用にする必要があります。
- サポートされる ISL の速度は、4Gbps、8Gbps、16Gbps、32Gbps です。
- ISL の速度と長さは、1つのファブリックのすべての ISL で同じである必要があります。
- ISL のトポロジは、1つのファブリックのすべての ISL で同じである必要があります。たとえば、すべての ISL を直接リンクにするか、または WDM を使用する場合はすべての ISL で WDM を使用する必要があります。

#### プラットフォーム固有の ISL に関する考慮事項

推奨される ISL の数は、プラットフォームモデルによって異なります。次の表に、ファブリックごとの ISL 要件をプラットフォームモデル別に示します。各 ISL の容量が 16Gbps であると想定しています。

プラットフォームモデル	4 ノードの DR グループ（スイッチファブリック）あたりの推奨される ISL 数
AFF A900およびFAS9500	8
AFF A700	6
FAS9000	6
8080 です	4.
その他すべて	2 つ

8 ノード構成をサポートするスイッチファブリックの場合（単一の 8 ノード MetroCluster 構成の一部である場合、または 2 つの 4 ノード構成で ISL を共有する場合）ファブリックあたりの推奨される ISL 数は、4 ノードの各 DR グループに必要な数の合計になります。例：

- DR グループ 1 に AFF A700 システムが 4 つ含まれている場合は、ISL が 6 つ必要です。
- DR グループ 2 に FAS8200 システムが 4 つ含まれている場合は、ISL が 2 つ必要です。
- スイッチファブリックあたりの推奨される ISL 数は合計 8 個です。

#### ファブリック接続 MetroCluster 構成で TDM / WDM 機器を使用する場合の考慮事項

Hardware Universe ツールには、ファブリック接続 MetroCluster 構成で Time Division Multiplexing（TDM；時分割多重化）または Wavelength Division Multiplexing（WDM；波長分割多重化）機器を使用する場合の要件について、いくつかの注意事項が記載さ

れています。これにはさまざまな構成に関する情報も含まれており、フレームの配信にインオーダー配信（IOD）アウトオブオーダー配信（OOD）のどちらを使用するかを判断するのに役立ちます。

このような要件の例としては、ルーティングポリシーを使用するリンクアグリゲーション（トランキング）機能を TDM / WDM 機器でサポートする必要があります。フレームの配信順序（IOD または OOD）は有効になっているルーティングポリシーによって決まり、スイッチ内で維持されます。

#### "NetApp Hardware Universe の略"

次の表に、Brocade スイッチと Cisco スイッチを含む構成のルーティングポリシーを示します。

スイッチ	MetroCluster 構成を IOD に設定する	OOD の MetroCluster 設定を行います
Brocade	<ul style="list-style-type: none"> <li>• AptPolicy を 1 に設定する必要があります</li> <li>• DLS を off に設定します</li> <li>• IOD を on に設定する必要があります</li> </ul>	<ul style="list-style-type: none"> <li>• AptPolicy を 3 に設定する必要があります</li> <li>• DLS は ON に設定する必要があります</li> <li>• IOD を off に設定する必要があります</li> </ul>
シスコ	<p>FCVI 用 VSAN のポリシー：</p> <ul style="list-style-type: none"> <li>• ロードバランシングポリシー：srcid、dstid</li> <li>• IOD を on に設定する必要があります</li> </ul> <p>ストレージ用 VSAN のポリシー：</p> <ul style="list-style-type: none"> <li>• ロードバランシングポリシー：srcid、dstid、oxid</li> <li>• VSAN で in-order-guarantee オプションを設定しないでください</li> </ul>	該当なし

#### IOD を使用する状況

IOD がリンクでサポートされている場合は、IOD を使用することを推奨します。IOD をサポートする構成は次のとおりです。

- 単一の ISL
- 単一の ISL と単一のリンク（および TDM / WDM などのリンク機器）
- 単一のトランク、および複数の ISL とリンク（および TDM / WDM などのリンク機器）

## OOD を使用する状況

- IOD をサポートしないすべての構成
- トランキング機能をサポートしないすべての構成

## 暗号化デバイスを使用する

MetroCluster 構成で ISL で専用の暗号化デバイスを使用する場合、または WDM デバイスで暗号化を使用する場合は、次の要件を満たす必要があります。

- 該当する FC スイッチのベンダーの認定を受けた外部暗号化デバイスまたは WDM 機器を使用する必要があります。  
動作モード（トランキングや暗号化など）に対応した認定が必要です。
- 暗号化によるレイテンシが 10 マイクロ秒以下である必要があります。

## Brocade DCX 8510-8 スイッチを使用するための要件

MetroCluster の設置を準備するにあたっては、MetroCluster のハードウェアアーキテクチャおよび必要なコンポーネントについて理解しておく必要があります。

- MetroCluster 構成で使用する DCX 8510-8 スイッチは、ネットアップから購入する必要があります。
- 拡張性を確保するために、4x48 ポートモジュールのうち 2 つの MetroCluster しかケーブル接続しない場合は、MetroCluster 構成間にポートチャックを 1 つ残しておくことを推奨します。これにより、ケーブルを再接続することなく MetroCluster 構成でポートの使用を拡張できます。
- MetroCluster 構成内の各 Brocade DCX 8510-8 スイッチは、ISL ポートとストレージ接続が正しく設定されている必要があります。ポートの使用方法については、次のセクションを参照してください。"[FC スイッチのポート割り当て](#)"。
- ISL は共有できず、MetroCluster ごとにファブリックごとに 2 つの ISL が必要です。
- バックエンド MetroCluster 接続に使用する DCX 8510-8 スイッチは、他の接続には使用しないでください。

MetroCluster 以外のデバイスはこれらのスイッチには接続せず、MetroCluster 以外のトラフィックが DCX 8510-8 スイッチを経由しないようにしてください。

- 1 枚のラインカードを、ONTAP MetroClusters \* または ONTAP 7-Mode MetroCluster のいずれかに接続できます。



このスイッチには RCF ファイルはありません。

Brocade DCX 8510-8 スイッチを 2 つ使用する場合は次のとおりです。

- 各サイトに DCX 8510-8 スイッチが 1 つ必要です。
- 16Gb SFP を搭載した 48 ポートブレードをスイッチごとに少なくとも 2 つ使用する必要があります。

MetroCluster 構成の各サイトで DCX 8510-8 スイッチを 4 つ使用する場合は次のとおりです。

- 各サイトに DCX 8510-8 スイッチが 2 つ必要です。
- 48 ポートブレードを DCX 8510-8 スイッチごとに少なくとも 1 つ使用する必要があります。
- 各ブレードは、仮想ファブリックを使用して仮想スイッチとして設定されます。

次のネットアップ製品は、Brocade DCX 8510-8 スイッチではサポートされません。

- Config Advisor
- Fabric Health Monitor の略
- MyAutoSupport（システムリスクが誤検出される可能性がある）
- Active IQ Unified Manager（旧 OnCommand Unified Manager）



この設定に必要なすべてのコンポーネントがあることを確認します "[NetApp Interoperability Matrix Tool](#) で確認できます"。サポートされている構成については、Interoperability Matrix Tool の注意事項のセクションを参照してください。

## ミラーされていないアグリゲートを使用する場合の

### ミラーされていないアグリゲートを使用する場合の

ミラーされていないアグリゲートが構成に含まれている場合、スイッチオーバー処理に関連するアクセスの問題に注意する必要があります。

### 電源のシャットダウンが必要なメンテナンス実施時のミラーされていないアグリゲートに関する考慮事項

サイト全体の電源のシャットダウンが必要なメンテナンスのためにネゴシエートスイッチオーバーを実行する場合は、最初にディザスタサイトが所有するミラーされていないアグリゲートを手動でオフラインにする必要があります。

ミラーされていないアグリゲートをオフラインにしないと、複数のディスクがパニック状態になって、サバイバーサイトのノードが停止する可能性があります。これは、ディザスタサイトのストレージへの接続が失われたために、スイッチオーバーされたミラーされていないアグリゲートがオフラインになるか、または見つからない場合に発生します。これは、電源のシャットダウンまたは ISL の停止が原因です。

### ミラーされていないアグリゲートと階層状のネームスペースに関する考慮事項

階層状のネームスペースを使用している場合は、パス内のすべてのボリュームがミラーされたアグリゲートのみ、またはミラーされていないアグリゲートのみ配置されるようにジャンクションパスを設定する必要があります。ジャンクションパスにミラーされていないアグリゲートとミラーされたアグリゲートが混在していると、スイッチオーバー処理後にミラーされていないアグリゲートにアクセスできなくなる可能性があります。

### ミラーされていないアグリゲート、CRS メタデータボリューム、およびデータ SVM ルートボリュームに関する考慮事項

設定レプリケーションサービス（CRS）メタデータボリュームとデータ SVM ルートボリュームは、ミラーされたアグリゲートに配置する必要があります。これらのボリュームをミラーされていないアグリゲートに移動することはできません。ミラーされていないアグリゲートに配置されている場合、ネゴシエートスイッチオーバー処理とスイッチバック処理が拒否されます。MetroCluster チェックコマンドを使用すると、この場合に警告が表示されます。

## ミラーされていないアグリゲートと **SVM** に関する考慮事項

SVM は、ミラーされたアグリゲートでのみ、またはミラーされていないアグリゲートでのみ設定してください。ミラーされていないアグリゲートとミラーされたアグリゲートが混在しているとスイッチオーバー処理に 2 分以上かかり、ミラーされていないアグリゲートがオンラインにならない場合にデータを利用できなくなることがあります。

## ミラーされていないアグリゲートと **SAN** に関する考慮事項

9.4.1 より前のバージョンの ONTAP では、LUN をミラーされていないアグリゲートに配置しないでください。ミラーされていないアグリゲートに LUN を設定すると、スイッチオーバー処理が 120 秒を超え、データを利用できなくなる可能性があります。

## **MetroCluster** サイトでのファイアウォールの使用状況

### **MetroCluster** サイトでのファイアウォールの使用に関する考慮事項

MetroCluster サイトでファイアウォールを使用している場合は、必要なポートへのアクセスを確保する必要があります。

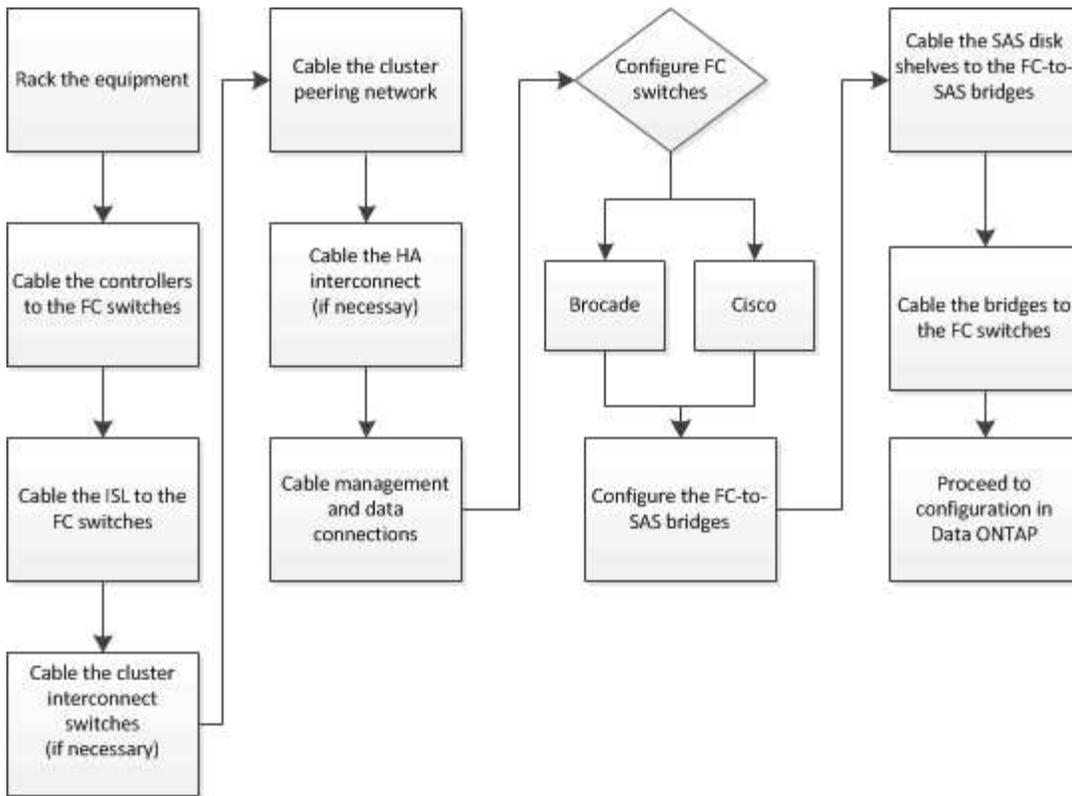
次の表は、2 つの MetroCluster サイト間に配置された外部ファイアウォールでの TCP/UDP ポートの使用状況を示しています。

トラフィックタイプ	ポート / サービス
クラスタピアリング	11104/TCP 11105/TCP
ONTAP システムマネージャ	443 / TCP
MetroCluster IP のクラスタ間 LIF	65200/TCP 10006/TCP および UDP
ハードウェアアシスト	4444/TCP

## ファブリック接続 **MetroCluster** 構成をケーブル接続

### ファブリック接続 **MetroCluster** 構成のケーブル接続

両方の地理的サイトで MetroCluster コンポーネントを物理的に設置し、ケーブル接続して、設定する必要があります。



## ファブリック MetroCluster 構成のコンポーネント

### ファブリック MetroCluster 構成のコンポーネント

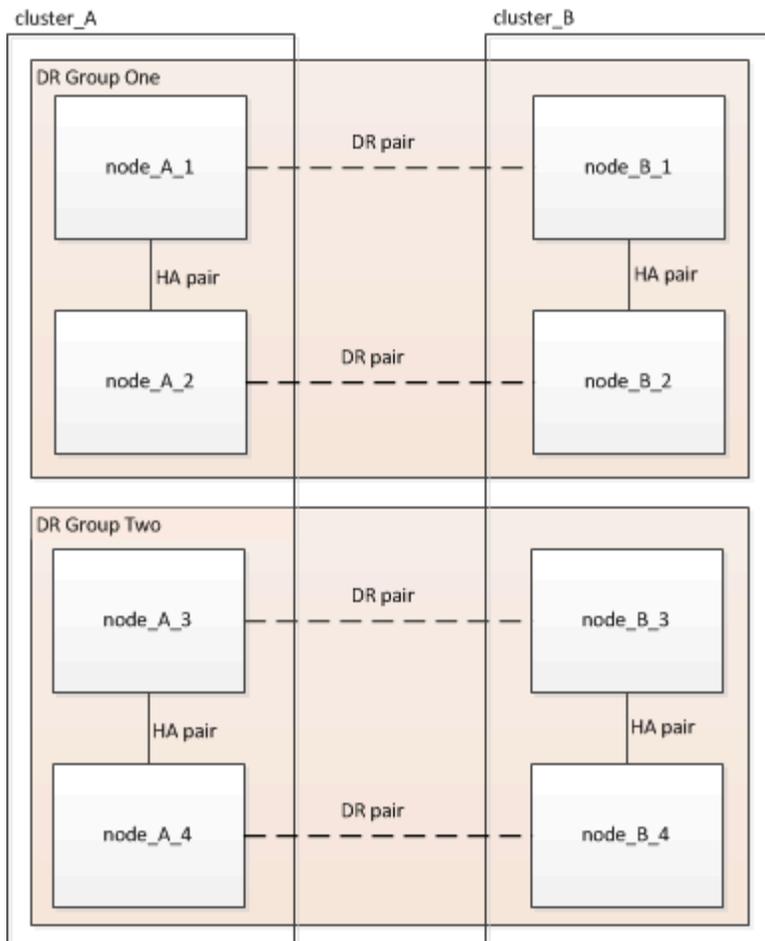
MetroCluster 構成を計画するときは、ハードウェアコンポーネントとその相互接続について理解しておく必要があります。

#### ディザスタリカバリ（DR）グループ

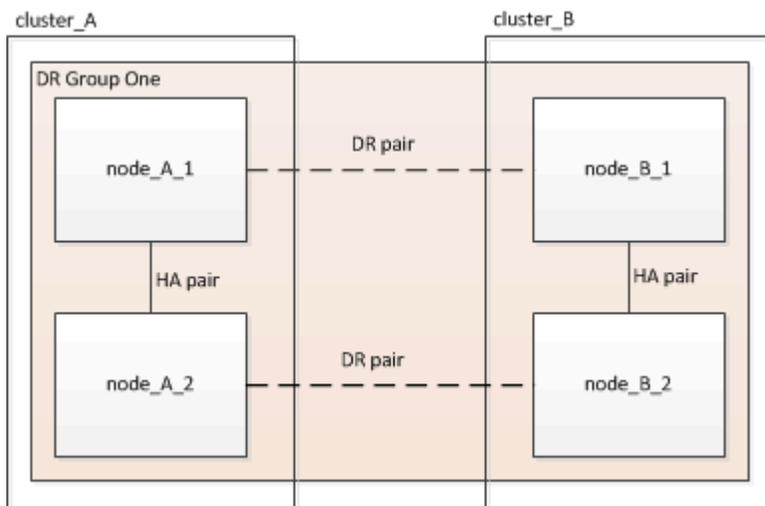
ファブリック MetroCluster 構成は、MetroCluster 構成のノード数に応じて、1つまたは2つの DR グループで構成されます。各 DR グループは4つのノードで構成されます。

- 8 ノードの MetroCluster 構成は、2つの DR グループで構成されます。
- 4 ノード MetroCluster 構成は、1つの DR グループで構成されます。

次の図は、8 ノードの MetroCluster 構成におけるノードの編成を示しています。



次の図は、4 ノード MetroCluster 構成におけるノードの編成を示しています。



主要なハードウェア要素

MetroCluster 構成には、中核をなす次のハードウェアが含まれます。

- ストレージコントローラ

ストレージコントローラはストレージに直接は接続されず、2つの冗長 FC スイッチファブリックに接続されます。

- FC-to-SAS ブリッジ

FC-to-SAS ブリッジは、SAS ストレージスタックを FC スイッチに接続し、2つのプロトコル間のブリッジの役割を果たします。

- FC スイッチ

FC スイッチは、2つのサイト間の長距離基幹 ISL の役割を果たします。FC スイッチが提供する2つのストレージファブリックによって、リモートストレージプールへのデータミラーリングが可能になります。

- クラスタピアリングネットワーク

クラスタピアリングネットワークは、Storage Virtual Machine (SVM) の設定を含むクラスタ構成をミラーするための接続を提供します。一方のクラスタのすべての SVM の設定が、パートナークラスタにミラーされます。

## 8 ノードのファブリック MetroCluster 構成

8 ノードの構成は、地理的に離れたサイトにある2つのクラスタで構成されています。cluster\_A は1つ目の MetroCluster サイトに配置されています。cluster\_B は2つ目の MetroCluster サイトに配置されています。各サイトには、SAS ストレージスタックが1つあります。追加のストレージスタックもサポートされますが、図では各サイトに1つしかありません。HA ペアは、クラスタインターコネクต์スイッチのないスイッチレスクラスタとして構成されています。スイッチを使用する構成もサポートされますが、ここでは使用していません。

8 ノード構成には次の接続が含まれます。

- 各コントローラの HBA アダプタおよび FC-VI アダプタから各 FC スイッチへの FC 接続
- 各 FC-to-SAS ブリッジから FC スイッチへの FC 接続
- 各 SAS シェルフ間および各スタックの上下から FC-to-SAS ブリッジへの SAS 接続
- ローカル HA ペアの各コントローラ間の HA インターコネクต์

コントローラが単一シャーシの HA ペアをサポートしている場合、HA インターコネクต์はバックプレーンを使用して内部で接続されます。つまり、外部のインターコネクต์は必要ありません。

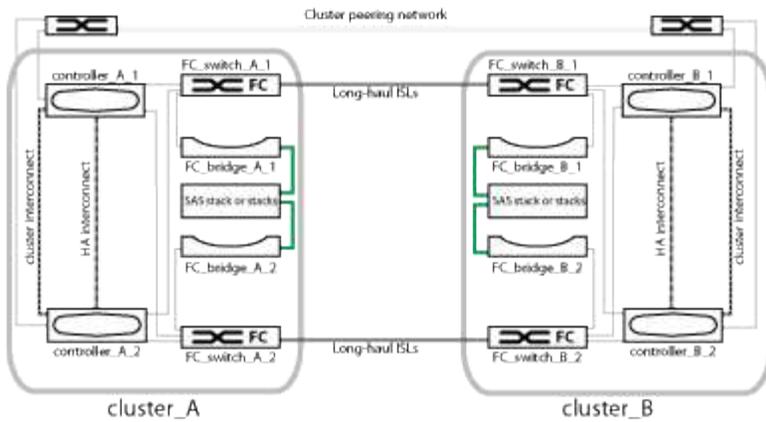
- コントローラからクラスタピアリングに使用されるお客様ネットワークへのイーサネット接続

SVM の設定はクラスタピアリングネットワーク経由でレプリケートされます。

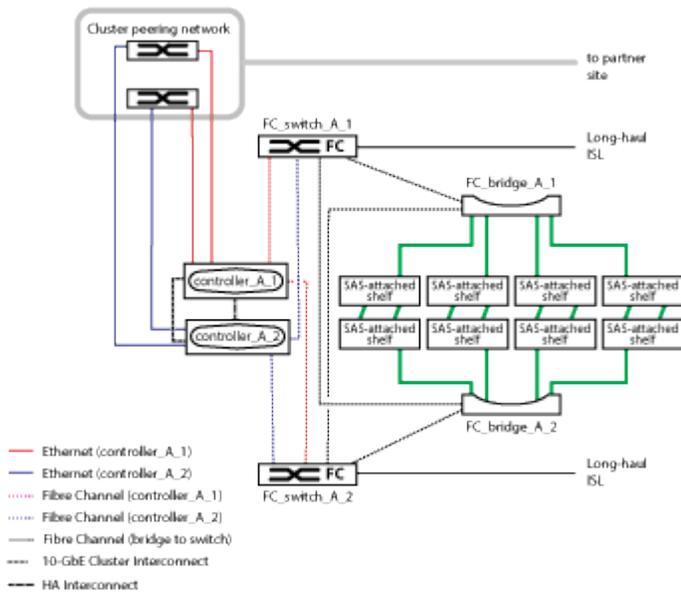
- ローカルクラスタの各コントローラ間のクラスタインターコネクต์

## 4 ノードのファブリック MetroCluster 構成

次の図は、4 ノードのファブリック MetroCluster 構成を単純化したものです。一部の接続では、コンポーネント間の複数の冗長接続を1本の線で表しています。データネットワーク接続と管理ネットワーク接続は表示されません。

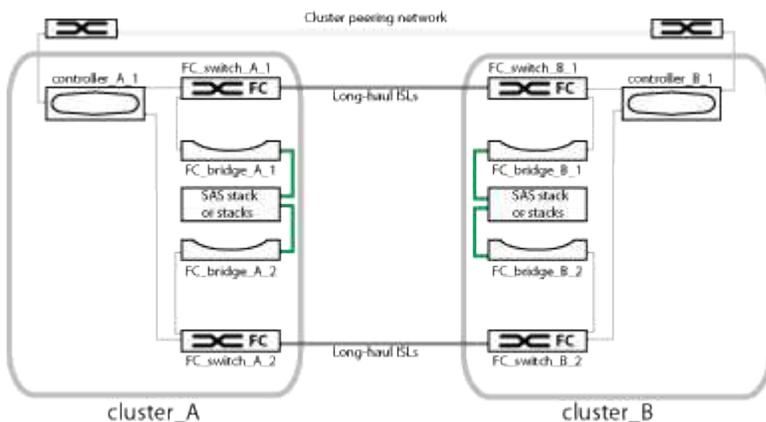


次の図は、単一の MetroCluster クラスタ（両方のクラスタの構成が同じ）内の接続をより詳細に示したものです。



## 2 ノードのファブリック MetroCluster 構成

次の図は、2 ノードのファブリック MetroCluster 構成を単純化したものです。一部の接続では、コンポーネント間の複数の冗長接続を 1 本の線で表しています。データネットワーク接続と管理ネットワーク接続は表示されません。

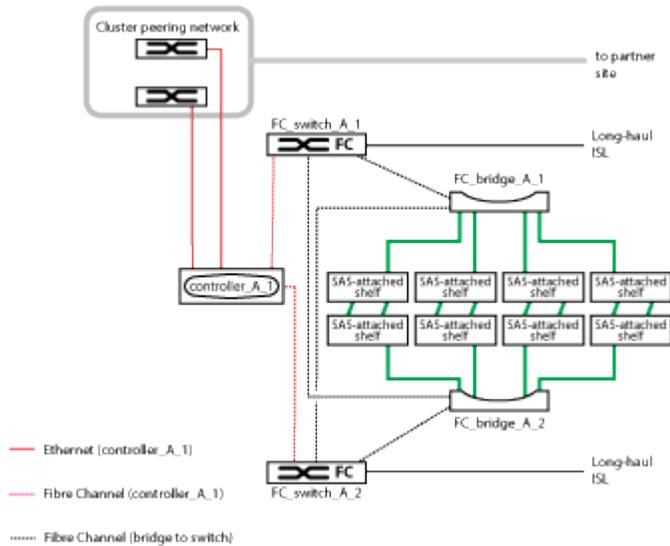


2 ノードの構成は、地理的に離れたサイトにある 2 つのクラスタで構成されています。cluster\_A は 1 つ目の MetroCluster サイトに配置されています。cluster\_B は 2 つ目の MetroCluster サイトに配置されています。各サイトには、SAS ストレージスタックが 1 つあります。追加のストレージスタックもサポートされますが、図では各サイトに 1 つしかありません。



2 ノード構成では、ノードが HA ペアとして構成されません。

次の図は、単一の MetroCluster クラスタ（両方のクラスタの構成が同じ）内の接続をより詳細に示したものです。



2 ノード構成には次の接続が含まれます。

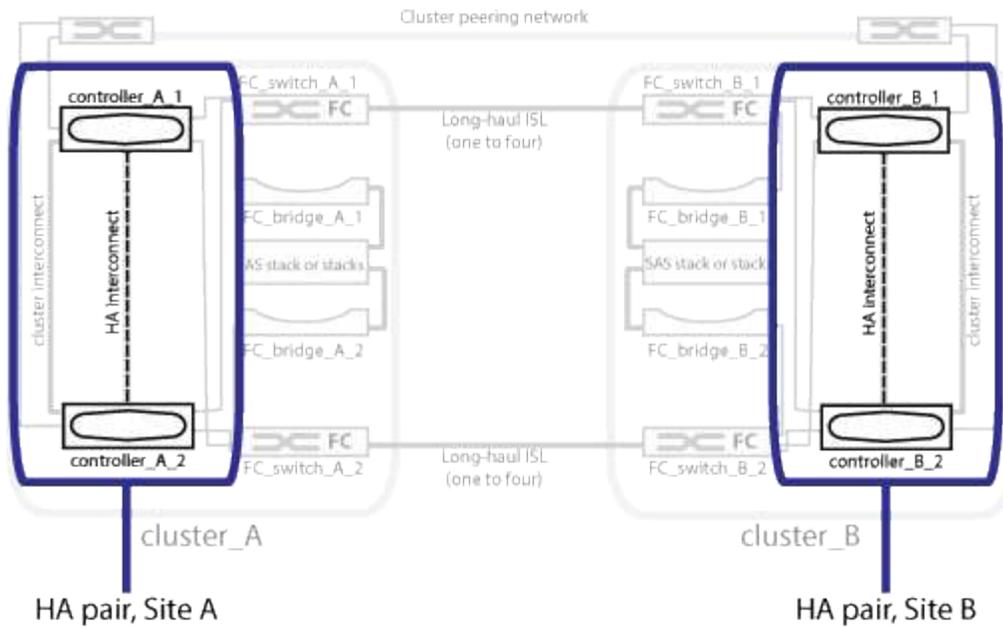
- 各コントローラモジュールの FC-VI アダプタ間の FC 接続
- 各コントローラモジュールの HBA から各 SAS シェルフスタックの FC-to-SAS ブリッジへの FC 接続
- 各 SAS シェルフ間および各スタックの上下から FC-to-SAS ブリッジへの SAS 接続
- コントローラからクラスタピアリングに使用されるお客様ネットワークへのイーサネット接続

SVM の設定はクラスタピアリングネットワーク経由でレプリケートされます。

### MetroCluster 構成のローカル HA ペアの図

8 ノード / 4 ノード MetroCluster 構成では、それぞれのサイトに、1 つまたは 2 つの HA ペアを構成するストレージコントローラが含まれます。これによってローカルでの冗長性が実現し、一方のストレージコントローラに障害が発生した場合はローカルの HA パートナーがテイクオーバーできるようになります。このような障害には、MetroCluster のスイッチオーバー処理は必要ありません。

ローカルの HA フェイルオーバー処理とギブバック処理は、非 MetroCluster 構成と同じように、storage failover コマンドで実行します。



#### 関連情報

"冗長 FC-to-SAS ブリッジの図"

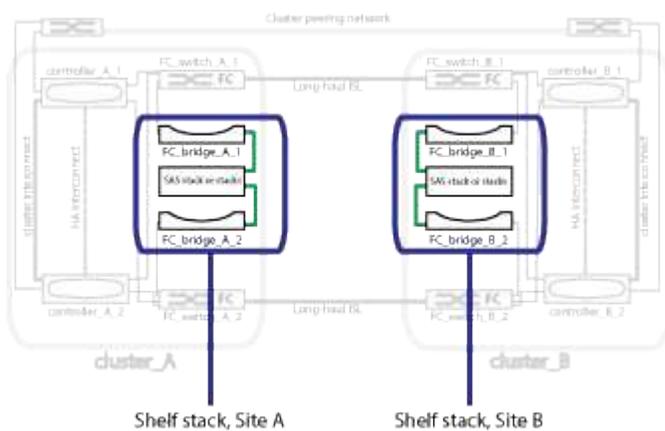
"冗長 FC スイッチファブリック"

"クラスタピアリングネットワークの図"

"ONTAP の概念"

#### 冗長 **FC-to-SAS** ブリッジの図

FC-to-SAS ブリッジは、SAS 接続ディスクと FC スイッチファブリックの間のプロトコルブリッジの役割を果たします。



#### 関連情報

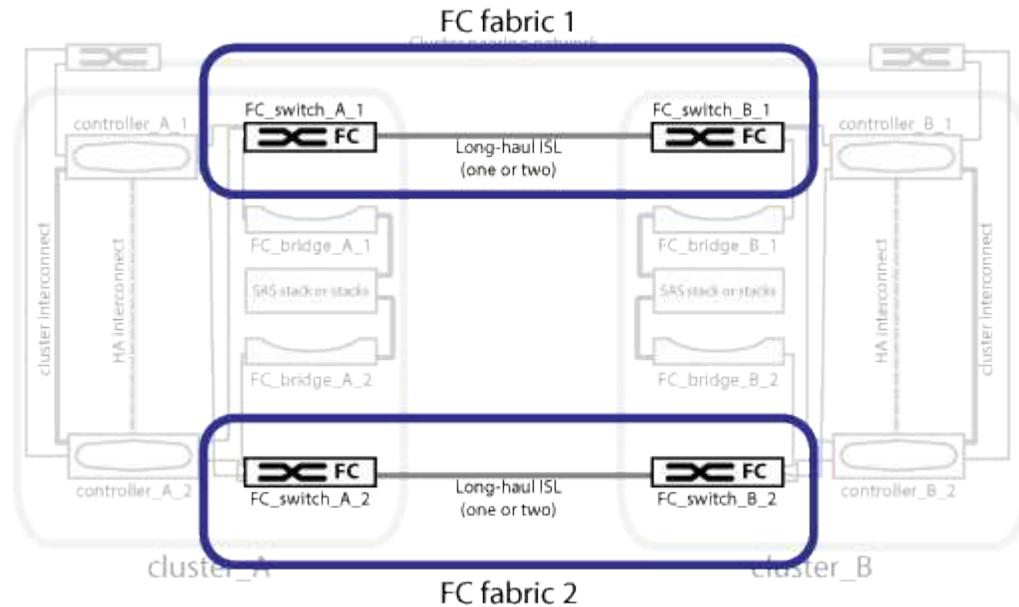
"MetroCluster 構成のローカル HA ペアの図"

"冗長 FC スイッチファブリック"

"クラスタピアリングネットワークの図"

## 冗長 FC スイッチファブリック

各スイッチファブリックには、サイトを接続するスイッチ間リンク（ISL）が含まれています。データは、サイトからサイトへ、ISL 経由でレプリケートされます。冗長性を確保するためには、各スイッチファブリックを異なる物理パスに配置する必要があります。



### 関連情報

["MetroCluster 構成のローカル HA ペアの図"](#)

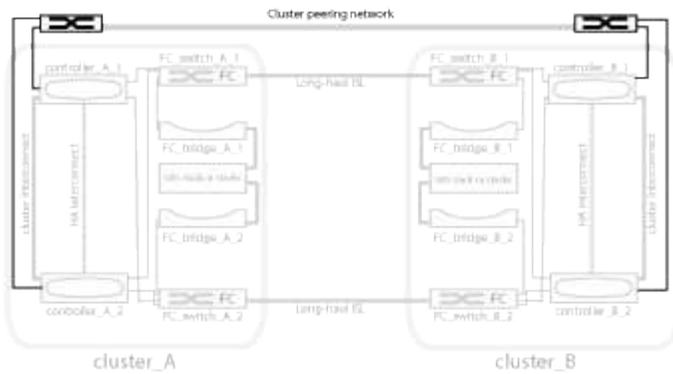
["冗長 FC-to-SAS ブリッジの図"](#)

["クラスタピアリングネットワークの図"](#)

### クラスタピアリングネットワークの図

MetroCluster 構成の 2 つのクラスタは、お客様のクラスタピアリングネットワーク経由でピアリングされています。クラスタピアリングは、サイト間の Storage Virtual Machine（SVM、旧 Vserver）の同期ミラーリングをサポートしています。

MetroCluster 構成の各ノードにインタークラスタ LIF が設定され、クラスタがピアリング用に設定されている必要があります。インタークラスタ LIF が設定されたポートが、お客様のクラスタピアリングネットワークに接続されます。SVM 構成は、このネットワーク経由で、Configuration Replication Service を使用してレプリケートされます。



## 関連情報

["MetroCluster 構成のローカル HA ペアの図"](#)

["冗長 FC-to-SAS ブリッジの図"](#)

["冗長 FC スイッチファブリック"](#)

["クラスタと SVM のピアリングの簡単な設定"](#)

["クラスタピアリングの設定に関する考慮事項"](#)

["クラスタピアリングのケーブル接続"](#)

["クラスタをピアリング"](#)

## 必要な MetroCluster FC コンポーネントと命名規則

MetroCluster FC 構成を計画する際には、サポート対象の必要なハードウェアコンポーネントとソフトウェアコンポーネントを把握しておく必要があります。また、内容を正しく理解するためには、このドキュメントで使用しているコンポーネントの命名規則も確認しておく必要があります。たとえば、一方のサイトをサイト A と呼び、もう一方のサイトをサイト B と呼びます

サポートされているソフトウェアおよびハードウェア

ハードウェアとソフトウェアは、MetroCluster FC 構成でサポートされている必要があります。

["NetApp Hardware Universe の略"](#)

AFF システムを使用する場合は、MetroCluster 構成内のすべてのコントローラモジュールを AFF システムとして構成する必要があります。



MetroCluster ストレージスイッチでは長波 SFP がサポートされません。サポートされる SPF については、MetroCluster テクニカルレポートを参照してください。

## MetroCluster FC 構成でのハードウェアの冗長性

MetroCluster FC 構成ではハードウェアの冗長性が確保されるため、サイトには各コンポーネントが 2 つずつあります。コンポーネントの名前には、サイトを表す A または B、および 2 つあるコンポーネントのうちど

ちらかを表す番号として 1 または 2 を使用します。

## ONTAP クラスタ × 2

ファブリック接続 MetroCluster FC 構成には、MetroCluster サイトごとに 1 つ、計 2 つの ONTAP クラスタが必要です。

名前は MetroCluster 構成内で一意である必要があります。

名前の例：

- サイト A : cluster\_A
- サイト B : cluster\_B

## FC スイッチ × 4

ファブリック接続 MetroCluster FC 構成には、FC スイッチ（サポートされている Brocade または Cisco モデル）が 4 つ必要です。

4 つのスイッチが 2 つのスイッチストレージファブリックを形成し、MetroCluster FC 構成の各クラスタ間の ISL を提供します。

名前は MetroCluster 構成内で一意である必要があります。

## コントローラモジュール × 2、4、または 8

ファブリック接続 MetroCluster FC 構成には、コントローラモジュールが 2 つ、4 つ、または 8 つ必要です。

4 ノードまたは 8 ノードの MetroCluster 構成では、各サイトのコントローラモジュールが 1 つまたは 2 つの HA ペアを形成します。各コントローラモジュールには、もう一方のサイトに DR パートナーがあります。

コントローラモジュールの要件は次のとおりです。

- 名前は MetroCluster 構成内で一意である必要があります。
- MetroCluster 構成のすべてのコントローラモジュールで同じバージョンの ONTAP が実行されている必要があります。
- 1 つの DR グループ内のすべてのコントローラモジュールのモデルが同じであることが必要です。

ただし、2 つの DR グループ構成にする場合は、DR グループごとに異なるモデルのコントローラモジュールで構成してもかまいません。

- 1 つの DR グループのすべてのコントローラモジュールで同じ FC-VI 構成を使用する必要があります。

一部のコントローラモジュールは、次の 2 つのオプションに対応しています。

- オンボードの FC-VI ポート
- スロット 1 の FC-VI カードオンボードの FC-VI ポートを使用するコントローラモジュールとアドオンの FC-VI カードを使用するコントローラモジュールが混在している場合は、サポートされません。たとえば、あるノードでオンボードの FC-VI 構成を使用する場合は、DR グループの他のすべてのノードでもオンボードの FC-VI 構成を使用する必要があります。

名前の例：

- サイト A : controller\_A\_1
- サイト B : controller\_B\_1

#### クラスタインターコネクトスイッチ × 4

ファブリック接続 MetroCluster FC 構成には、クラスタインターコネクトスイッチが 4 つ必要です（2 ノードスイッチレスクラスタを使用している場合は除く）。

これらのスイッチは、各クラスタのコントローラモジュール間のクラスタ通信を提供します。各サイトのコントローラモジュールが 2 ノードスイッチレスクラスタとして設定されている場合、これらのスイッチは必要ありません。

#### FC-to-SAS ブリッジの要件

ファブリック接続 MetroCluster FC 構成には、SAS シェルフのスタックグループごとに FC-to-SAS ブリッジのペアが 1 組必要です。



ONTAP 9.8 以降を実行している構成では、FibreBridge 6500N ブリッジはサポートされません。

- FibreBridge 7600N / 7500N ブリッジでは、最大 4 つの SAS スタックがサポートされます。
- 各スタックで異なる IOM のモデルを使用できます。
- 名前は MetroCluster 構成内で一意である必要があります。

このドキュメントで例として使用されている推奨名には、次のようにブリッジの接続先のコントローラモジュールとスタックが含まれています。

#### プールとドライブの要件（最小サポート）

シェルフ単位でディスク所有権を割り当てられるようにするために、SAS ディスクシェルフを 8 台（各サイトに 4 台）配置することを推奨します。

MetroCluster 構成では、各サイトに最小構成が必要です。

- 各ノードのサイトに少なくとも 1 つのローカルプールと 1 つのリモートプールがあります。  
たとえば、各サイトにノードが 2 つある 4 ノード MetroCluster 構成では、各サイトにプールが 4 つ必要です。
- 各プールに少なくとも 7 本のドライブ。  
各ノードにミラーされたデータアグリゲートが 1 つある 4 ノード MetroCluster 構成では、最小構成として 24 本のディスクがサイトに必要です。

サポートされる最小構成では、各プールのドライブレイアウトは次のようになります。

- ルートドライブ × 3 本

- 3本のデータドライブ
- スペアドライブ x 1本

サポートされる最小構成では、各サイトに少なくとも1台のシェルフが必要です。

MetroCluster 構成では、RAID-DP と RAID 4 がサポートされます。

空きのあるシェルフでのドライブの配置場所に関する考慮事項

収容数が半分（24 ドライブシェルフに 12 本のドライブ）のシェルフを使用している場合にドライブの自動割り当てを正しく行うには、スロット 0~5 および 18~23 にドライブを配置する必要があります。

シェルフに空きがある構成では、シェルフの4つの部分にドライブを均等に配置する必要があります。

ブリッジの命名規則

ブリッジでは、次のような命名規則を使用します。

ペア内の 'bridge\_site\_stack グループ・ロケーション

名前の各部分	特定のインターフェイス	有効な値
サイト	ブリッジペアが物理的に配置されているサイト。	A または B
スタックグループ	ブリッジペアが接続されているスタックグループの番号。  FibreBridge 7600N / 7500N ブリッジでは、スタックグループで最大4個のスタックがサポートされます。  スタックグループに含めることができるストレージシェルフは10個までです。	1、2 など
ペア内の場所	ブリッジペア内のブリッジ。ブリッジのペアは、特定のスタックグループに接続します。	a または b

各サイトの1つのスタックグループのブリッジ名の例：

- bridge\_A\_1a
- bridge\_A\_1b
- bridge\_B\_1a
- bridge\_B\_1b

## FC スイッチおよび FC-to-SAS ブリッジの設定ワークシート

MetroCluster サイトの設定を開始する前に、次のワークシートを使用してサイト情報を記録できます。

["サイト A のワークシート"](#)

["サイト B のワークシート"](#)

### MetroCluster コンポーネントを設置してケーブルを配線します

ラックにハードウェアコンポーネントを配置

納入された機器がキャビネットに設置されていない場合は、コンポーネントをラックに配置する必要があります。

このタスクについて

このタスクは両方の MetroCluster サイトで実行する必要があります。

手順

1. MetroCluster コンポーネントの配置を計画します。

ラックスペースは、コントローラモジュールのプラットフォームモデル、スイッチのタイプ、構成内のディスクシェルフスタック数によって異なります。

2. 自身の適切な接地対策を行います
3. コントローラモジュールをラックまたはキャビネットに設置します。

["ONTAPハードウェアシステムのドキュメント"](#)

4. FC スイッチをラックまたはキャビネットに設置します。
5. ディスクシェルフを設置し、電源を投入して、シェルフ ID を設定します。

- 各ディスクシェルフの電源を再投入する必要があります。
- 各 MetroCluster DR グループ（両サイトを含む）で、各 SAS ディスクシェルフのシェルフ ID が一意である必要があります。

6. 各 FC-to-SAS ブリッジを設置します。

- a. 4 本のネジを使用して、ブリッジ前面の「L」ブラケットをラックの前面に固定します（フラッシュマウント）。

ブリッジ「L」ブラケットの開口部は、19 インチ（482.6 mm）ラックのラック標準 ETA-310-X に準拠しています。

設置の詳細および図については、使用しているブリッジモデルに対応した ATTO FibreBridge Installation and Operation Manual を参照してください。



ポートスペースへのアクセスと FRU の保守性を確保するには、ブリッジペアの下に 1U のスペースを残し、そのスペースを工具が不要なブランクパネルでカバーする必要があります。

- b. 各ブリッジを、適切なアースを提供する電源に接続します。
- c. 各ブリッジの電源をオンにします。



耐障害性を最大限にするために、ディスクシェルフの同じスタックに接続されているブリッジをそれぞれ別々の電源に接続する必要があります。

ブリッジの準備完了を示す LED が点灯し、ブリッジの電源投入時自己診断テストが完了したことを示すまで、30 秒ほどかかる場合があります。

新しいコントローラモジュールの **FC-VI** ポートおよび **HBA** ポートを **FC** スイッチにケーブル接続します

FC-VI ポートと HBA（ホストバスアダプタ）は、MetroCluster 構成の各コントローラモジュール上にあるサイトの FC スイッチにケーブル接続する必要があります。

手順

1. 構成とスイッチモデルの表を使用して、FC-VI ポートと HBA ポートをケーブル接続します。
  - ["FCスイッチのポート割り当て"](#)

**MetroCluster** サイト間での **ISL** のケーブル接続

光ファイバスイッチ間リンク（ISL）を使用して各サイトの FC スイッチを接続し、MetroCluster のコンポーネントに接続するスイッチファブリックを形成する必要があります。

このタスクについて

両方のスイッチファブリックに対して実行する必要があります。

手順

1. 構成およびスイッチのモデルに対応するケーブル接続の表に従って、各サイトの FC スイッチをすべての ISL に接続します。
  - ["FCスイッチのポート割り当て"](#)

関連情報

["ISL に関する考慮事項"](#)

**FC**スイッチのポート割り当て

**MetroCluster** **FC**スイッチのポート割り当て

FCスイッチをケーブル接続するときは、指定のポート割り当てを使用していることを確認する必要があります。

イニシエータポート、FC-VIポート、またはISLの接続に使用されていないポートを、ストレージポートとして再構成できます。ただし、サポートされているRCFを使用している場合は、それに応じてゾーニングを変更する必要があります。

サポートされている RCF を使用する場合、ISL ポートは表示されているポートと同じポートに接続されない可能性があります、手動で再構成する必要がある場合があります。

ONTAP 9のポート割り当てを使用してスイッチが設定されている場合は、引き続き古い割り当てを使用できます。ただし、ONTAP 9.1以降を実行する新しい構成では、ここに示すポート割り当てを使用する必要があります。

## ケーブル接続の全体的なガイドライン

ケーブル接続の表を使用する際は、次の点に注意してください。

- Brocade スイッチと Cisco スイッチでは、ポート番号の付け方が異なります。
  - Brocade スイッチでは、ポート番号は 0 から始まります。
  - Cisco スイッチでは、ポート番号は 1 から始まります。
- ケーブル接続は、スイッチファブリックの各 FC スイッチで同じです。
- AFF A300およびFAS8200ストレージシステムでは、発注時にFC-VI接続のオプションとして次のいずれかを選択できます。
  - FC-VI モードで設定されたオンボードポート 0e および 0f。
  - スロット 1 の FC-VI カードのポート 1a および 1b。
- AFF A700 および FAS9000 ストレージシステムの場合、FC-VI ポートが 4 つ必要です。次の表に、Cisco 9250i スイッチを除く各コントローラに FC-VI ポートが 4 つある FC スイッチのケーブル接続を示します。

他のストレージシステムの場合、表にあるケーブル接続を使用し、FC-VI ポート c および d については無視してください

これらのポートは空にしておくことができます。

- AFF A400 および FAS8300 ストレージシステムは、FC-VI 接続にポート 2a と 2b を使用します。
- 2 つの MetroCluster 構成で ISL を共有する場合は、8 ノード MetroCluster のケーブル接続と同じポート割り当てを使用します。
- ケーブル接続する ISL の数は、サイトの要件に応じて異なります。
- ISL に関する考慮事項についてのセクションを参照してください。

### "ISL に関する考慮事項"

## AFF A900およびFAS9500の配線ガイドライン

- AFF A900またはFAS9500ストレージシステムでは、FC-VIポートが8つ必要です。AFF A900またはFAS9500を使用している場合は、8つのポート構成を使用する必要があります。構成に他のストレージシステムモデルが含まれている場合は、表に示されているケーブル接続を使用し、不要な FC-VI ポートのケーブル接続は無視してください。

2つのイニシエータポートを使用するシステムのポート割り当て

各ファブリックに1つのイニシエータポート、各コントローラに2つのイニシエータポートを使用して、FAS8200およびAFF A300システムを構成できます。

1つのFCポート (FC1 または FC2) のみを使用して、FibreBridge 7600N ブリッジのケーブル接続を実行できます。4つのあるイニシエータのうち2つだけを接続し、スイッチポートに接続されている他の2つのイニシエータは空にしておきます。

ゾーニングを手動で実行する場合は、1つのFCポート (FC1 または FC2) を使用するFibreBridge 7600Nブリッジに使用されるゾーニングに従います。この場合は、各ファブリックのゾーンメンバーごとに2つではなく1つのイニシエータポートが追加されます。

の手順を使用して、ゾーニングを変更したり、FibreBridge 6500NからFibreBridge 7500Nへのアップグレードを実行したりできます。"[FibreBridge 6500N ブリッジと FibreBridge 7600N / 7500N ブリッジのホットスワップ](#)"。

次の表は、ファブリックごとに1つのイニシエータポートを使用し、コントローラごとに2つのイニシエータポートを使用する場合のBrocade FCスイッチのポートの割り当てを示しています。

1つのFCポート (FC1またはFC2) のみを使用するFibreBridge 7500N / 7600Nを使用する構成			
• MetroCluster 1 または DR グループ 1 *	• コンポーネント *	• ポート *	6505、6510、6520、7840、G620、G630、G610、G710、G720、G730、DCX 8510-8
• FC スイッチに接続 *	• スイッチポートに接続 ... *	controller_x_1	FC-VI ポート a
1.	0	FC-VI ポート b	2.
0	FC-VI ポート c	1.	1.
FC-VI ポート d	2.	1.	HBA ポート A
1.	2.	HBA ポート b	2.
2.	HBA ポート c	-	-
HBA ポート d	-	-	スタック 1
bridge_x_1a	1.	8.	bridge_x_1b
2.	8.	スタック y	bridge_x_ya
1.	11.	bridge_x_YB	2.

Brocade FC スイッチをコントローラにケーブル接続するために必要なポートの割り当てについて説明します。

以下の表は、DRグループあたり4つのコントローラモジュールを使用した場合の最大サポート構成を示しています。8それよりも小規模な構成の場合、余分なコントローラモジュールの行は無視してください。このISLは、Brocade 6510、Brocade DCX 8510-8、G620、G630、G620-1、G630-1、G720、およびG730スイッチでのみサポートされることに注意してください。

これらの表を使用する前に、次の情報を確認してください。

- 8 ノードMetroCluster構成におけるBrocade 6505、G610、および G710 スイッチのポート使用状況は表示されません。ポートの数に限りがあるため、コントローラモジュールのモデルや使用しているISLおよびブリッジペアの数に応じて、サイトごとにポートを割り当てる必要があります。
- Brocade DCX 8510-8 スイッチでは、6510 スイッチ \* \_ または \_ \* the 7840 スイッチと同じポートレイアウトを使用できます。
- Brocade 6520、7810、および 7840 スイッチは、8 つの FC-VI ポート (AFF A900およびFAS9500システム) を使用するシステムではサポートされません。
- Brocade 7810 スイッチは 1 つの DR グループのみをサポートします。

### MetroCluster 1またはDRグループ1

次の表は、Brocadeスイッチ上のMetroCluster 1 または DR グループ 1 でサポートされているコントローラ構成を示しています。

* コンポーネント *	* ポート *	* FC スイッチに接続 *	6505、G610、G710 ポート	6510、DCX 8510-8 ポート	6520ポート	7810ポート	7840ポート	G620、G620-1、G630、G630-1 ポート	G720、G730 ポート
controller_x_1	FC-VI ポート a	1.	0	0	0	0	0	0	0
FC-VI ポート b	2.	0	0	0	0	0	0	0	FC-VI ポート c
1.	1.	1.	1.	1.	1.	1.	1.	FC-VI ポート d	2.
1.	1.	1.	1.	1.	1.	1.	FC-VI-2 ポート A	1.	16
20	N/A	N/A	N/A	16	2.	FC-VI-2 ポート b	2.	16	20
N/A	N/A	N/A	16	2.	FC-VI-2 ポート c	1.	17	21	N/A

* コンポー ネント*	*ポート*	*FC スイッチ に接続*	6505、G 610、G7 10ポート	6510、D CX 8510- 8ポート	6520ポー ト	7810ポー ト	7840ポー ト	G620、G 620-1 、G630 、G630-1 ポート	G720、G 730 ポート
N/A	N/A	17	3.	FC-VI-2 ポート d	2.	17	21	N/A	N/A
N/A	17	3.	HBA ポー ト A	1.	2.	2.	2.	2.	2.
2.	8.	HBA ポー ト b	2.	2.	2.	2.	2.	2.	2.
8.	HBA ポー ト c	1.	3.	3.	3.	3.	3.	3.	9.
HBA ポー ト d	2.	3.	3.	3.	3.	3.	3.	9.	controller _x_2
FC-VI ポ ート a	1.	4.	4.	4.	4.	4.	4.	4.	FC-VI ポ ート b
2.	4.	4.	4.	4.	4.	4.	4.	FC-VI ポ ート c	1.
5.	5.	5.	5.	5.	5.	5.	FC-VI ポ ート d	2.	5.
5.	5.	5.	5.	5.	5.	FC-VI-2 ポート A	1.	18	22
N/A	N/A	N/A	20	6.	FC-VI-2 ポート b	2.	18	22	N/A
N/A	N/A	20	6.	FC-VI-2 ポート c	1.	19	23	N/A	N/A
N/A	21	7.	FC-VI-2 ポート d	2.	19	23	N/A	N/A	N/A
21	7.	HBA ポー ト A	1.	6.	6.	6.	6.	6.	6.
12.	HBA ポー ト b	2.	6.	6.	6.	6.	6.	6.	12.

* コンポーネント *	* ポート *	* FC スイッチに接続 *	6505、G610、G710 ポート	6510、DCX 8510-8 ポート	6520ポート	7810ポート	7840ポート	G620、G620-1、G630、G630-1 ポート	G720、G730 ポート
HBA ポート c	1.	7.	7.	7.	7.	7.	7.	13	HBA ポート d

## MetroCluster 2またはDRグループ2

次の表は、Brocadeスイッチ上のMetroCluster 2 または DR グループ 2 でサポートされているコントローラ構成を示しています。

* コンポーネント *	* ポート *	* FC スイッチに接続 *	6505、G610、G710 ポート	6510、DCX 8510-8 ポート	6520ポート	7810ポート	7840ポート	G620、G620-1、G630、G630-1 ポート	G720、G730 ポート
controller_x_3	FC-VI ポート a	1.	N/A	24	48	N/A	12.	18	18
FC-VI ポート b	2.	N/A	24	48	N/A	12.	18	18	FC-VI ポート c
1.	N/A	25	49	N/A	13	19	19	FC-VI ポート d	2.
N/A	25	49	N/A	13	19	19	FC-VI-2 ポート A	1.	N/A
36	N/A	N/A	N/A	36	24	FC-VI-2 ポート b	2.	N/A	36
N/A	N/A	N/A	36	24	FC-VI-2 ポート c	1.	N/A	37	N/A
N/A	N/A	37	25	FC-VI-2 ポート d	2.	N/A	37	N/A	N/A
N/A	37	25	HBA ポート A	1.	N/A	26	50	N/A	14
24	26	HBA ポート b	2.	N/A	26	50	N/A	14	24

* コンポーネント *	* ポート *	* FC スイッチに接続 *	6505、G610、G710 ポート	6510、DCX 8510-8 ポート	6520ポート	7810ポート	7840ポート	G620、G620-1、G630、G630-1 ポート	G720、G730 ポート
26	HBA ポート c	1.	N/A	27	51	N/A	15	25	27
HBA ポート d	2.	N/A	27	51	N/A	15	25	27	controller_x_4
FC-VI ポート a	1.	N/A	28	52	N/A	16	22	22	FC-VI ポート b
2.	N/A	28	52	N/A	16	22	22	FC-VI ポート c	1.
N/A	29	53	N/A	17	23	23	FC-VI ポート d	2.	N/A
29	53	N/A	17	23	23	FC-VI-2 ポート A	1.	N/A	38
N/A	N/A	N/A	38	28	FC-VI-2 ポート b	2.	N/A	38	N/A
N/A	N/A	38	28	FC-VI-2 ポート c	1.	N/A	39	N/A	N/A
N/A	39	29	FC-VI-2 ポート d	2.	N/A	39	N/A	N/A	N/A
39	29	HBA ポート A	1.	N/A	30	54	N/A	18	28
30	HBA ポート b	2.	N/A	30	54	N/A	18	28	30
HBA ポート c	1.	N/A	31.	55	N/A	19	29	31.	HBA ポート d

### MetroCluster 3 または DR グループ 3

次の表は、Brocadeスイッチ上のMetroCluster 3 または DR グループ 3 でサポートされているコントローラ構成を示しています。

* コンポーネント *	* ポート *	* FC スイッチに接続 *	G630、G630-1 ポート	G730 ポート
controller_x_5	FC-VI ポート a	1.	48	48
FC-VI ポート b	2.	48	48	FC-VI ポート c
1.	49	49	FC-VI ポート d	2.
49	49	FC-VI-2 ポート A	1.	64
50	FC-VI-2 ポート b	2.	64	50
FC-VI-2 ポート c	1.	65	51	FC-VI-2 ポート d
2.	65	51	HBA ポート A	1.
50	56	HBA ポート b	2.	50
56	HBA ポート c	1.	51	57
HBA ポート d	2.	51	57	controller_x_6
FC-VI ポート a	1.	52	52	FC-VI ポート b
2.	52	52	FC-VI ポート c	1.
53	53	FC-VI ポート d	2.	53
53	FC-VI-2 ポート A	1.	68	54
FC-VI-2 ポート b	2.	68	54	FC-VI-2 ポート c
1.	69	55	FC-VI-2 ポート d	2.
69	55	HBA ポート A	1.	54
60	HBA ポート b	2.	54	60
HBA ポート c	1.	55	61	HBA ポート d

## MetroCluster 4 または DR グループ 4

次の表は、Brocadeスイッチ上のMetroCluster 4 または DR グループ 4 でサポートされているコントローラ構成を示しています。

* コンポーネント *	* ポート *	* FC スイッチに接続 *	G630、G630-1 ポート	G730 ポート
controller_x_7	FC-VI ポート a	1.	66	66
FC-VI ポート b	2.	66	66	FC-VI ポート c
1.	67	67	FC-VI ポート d	2.
67	67	FC-VI-2 ポート A	1.	84
72	FC-VI-2 ポート b	2.	84	72
FC-VI-2 ポート c	1.	85	73	FC-VI-2 ポート d
2.	85	73	HBA ポート A	1.
72	74	HBA ポート b	2.	72
74	HBA ポート c	1.	73	75
HBA ポート d	2.	73	75	controller_x_8
FC-VI ポート a	1.	70	70	FC-VI ポート b
2.	70	70	FC-VI ポート c	1.
71.	71.	FC-VI ポート d	2.	71.
71.	FC-VI-2 ポート A	1.	86	76
FC-VI-2 ポート b	2.	86	76	FC-VI-2 ポート c
1.	87	77	FC-VI-2 ポート d	2.
87	77	HBA ポート A	1.	76
78	HBA ポート b	2.	76	78

* コンポーネント *	* ポート *	* FC スイッチに接続 *	<b>G630、G630-1</b> ポート	<b>G730</b> ポート
HBA ポート c	1.	77	79	HBA ポート d

#### MetroCluster FC構成におけるFC-SASブリッジのBrocadeポートの使用

Brocade FCスイッチをFC-SASブリッジに接続するために必要なポート割り当てについて説明します。ポート割り当ては、ブリッジが使用するFCポートが1つなのか2つなのかによって異なります。



Brocade 7810 スイッチは 1 つの DR グループのみをサポートします。

両方の FC ポート (FC1 と FC2) を使用する FibreBridge 7500N または 7600N ブリッジを使用したセルフ構成

#### MetroCluster 1またはDRグループ1

以下の表は、BrocadeスイッチのFCポート (FC1とFC2) の両方を使用するFibreBridge 7500Nまたは7600Nブリッジにおいて、MetroCluster 1またはDRグループ1でサポートされるセルフ構成を示しています。この構成表を使用する際は、以下の点にご注意ください。

- Brocade 6505、G610、G710、G620、G620-1、G630、および G630-1 スイッチでは、追加のブリッジをポート 12 ~ 15 にケーブル接続できます。
- Brocade 6510 および DCX 8510-8 スイッチでは、追加のブリッジをポート 12 ~ 19 にケーブル接続できます。
- Brocade 6520 スイッチでは、追加のブリッジをポート 12 ~ 21 および 24 ~ 45 にケーブル接続できます。
- Brocade 7810 および 7840 スイッチでは、MetroCluster 1 または DR グループ 1 は 2 つのブリッジ スタックのみをサポートします。
- Brocade G720 および G730 スイッチでは、追加のブリッジをポート 16 ~ 21 にケーブル接続できます。

* コンポーネント *	* ポート *	* FC スイッチに接続 *	6505、G610、G710 ポート	6510、DCX 8510-8 ポート	6520ポ ート	7810ポ ート	7840ポ ート	G620、G620-1、G630、G630-1 ポート	G720、G730 ポート
スタック 1	bridge_x_1a	fc1	1.	8.	8.	8.	8.	8.	10.
FC2	2.	8.	8.	8.	8.	8.	10.	bridge_x_1b	fc1
1.	9.	9.	9.	9.	9.	11.	FC2	2.	9.

* コンポーネント *	* ポート *	* FC スイッチに接 続 *	6505、 G610、 G710 ポート	6510、 D CX 8510-8 ポート	6520ポ ート	7810ポ ート	7840ポ ート	G620、 G620- 1、 G63 0、 G63 0-1 ポート	G720、 G730 ポート
9.	9.	9.	9.	11.	スタック 2	bridge_x _2a	fc1	1.	10.
10.	10.	10.	10.	14	FC2	2.	10.	10.	10.
10.	10.	10.	14	bridge_x _2b	fc1	1.	11.	11.	11.
11.	11.	15	FC2	2.	11.	11.	11.	11.	11.

## MetroCluster 2またはDRグループ2

以下の表は、BrocadeスイッチのFCポート（FC1とFC2）の両方を使用するFibreBridge 7500Nまたは7600Nブリッジにおいて、MetroCluster 2またはDRグループ2でサポートされるシェルフ構成を示しています。この構成表を使用する際は、以下の点にご注意ください。

- Brocade 6510、DCX 8510-8、および 7840 スイッチでは、MetroCluster 2 または DR グループ 2 は 2 つのブリッジ スタックのみをサポートします。
- Brocade 6520 スイッチでは、追加のブリッジをポート 60 ~ 69 および 72 ~ 93 にケーブル接続できません。
- Brocade G620、G620-1、G630、および G630-1 スイッチでは、追加のブリッジをポート 32 ~ 35 にケーブル接続できます。
- Brocade G720 および G730 スイッチでは、追加のブリッジをポート 36 ~ 39 にケーブル接続できます。
- 8ノードMetroCluster構成におけるBrocade 6505、G610、およびG710スイッチのポート使用状況は示されていません。ポート数が限られているため、コントローラモデル、使用するISLおよびブリッジペアの数に応じて、サイトごとにポートを割り当てます。

* コンポーネント *	* ポート *	* FC スイッチに接 続 *	6505、 G610、 G710 ポート	6510、 D CX 8510-8 ポート	6520ポ ート	7810ポ ート	7840ポ ート	G620、 G620- 1、 G63 0、 G63 0-1 ポート	G720、 G730 ポート	
スタック 1	bridge_x _1a	fc1	1.	N/A	32	56	N/A	20	26	32
FC2	2.	N/A	32	56	N/A	20	26	32	bridge_x _1b	fc1
1.	N/A	33	57	N/A	21	27	33	FC2	2.	N/A

* コンポーネント *	* ポート *	* FC スイッチに接 続 *	6505、 G610、 G710 ポート	6510、 D CX 8510-8 ポート	6520ポ ート	7810ポ ート	7840ポ ート	G620、 G620- 1、 G63 0、 G63 0-1 ポート	G720、 G730 ポート	
33	57	N/A	21	27	33	スタック 2	bridge_x_2a	fc1	1.	N/A
34	58	N/A	22	30	34	FC2	2.	N/A	34	58
N/A	22	30	34	bridge_x_2b	fc1	1.	N/A	35	59	N/A
23	31.	35	FC2	2.	N/A	35	59	N/A	23	31.

### MetroCluster 3 または DR グループ 3

以下の表は、BrocadeスイッチのFCポート（FC1とFC2）の両方を使用するFibreBridge 7500Nまたは7600Nブリッジにおいて、MetroCluster 3またはDRグループ3でサポートされるシェルフ構成を示しています。この構成表を使用する際は、以下の点にご注意ください。

- Brocade G630 および G630-1 スイッチでは、追加のブリッジをポート 60 ～ 63 にケーブル接続できません。
- Brocade G730 スイッチでは、追加のブリッジをポート 64、65、68、および 69 にケーブル接続できません。

* コンポーネント *	* ポート *	* FC スイッチに接 続 *	G630、 G630-1 ポート	G730 ポート	
スタック 1	bridge_x_1a	fc1	1.	56	58
FC2	2.	56	58	bridge_x_1b	fc1
1.	57	59	FC2	2.	57
59	スタック 2	bridge_x_2a	fc1	1.	58
62	FC2	2.	58	62	bridge_x_2b
fc1	1.	59	63	FC2	2.

### MetroCluster 4 または DR グループ 4

以下の表は、BrocadeスイッチのFCポート（FC1とFC2）の両方を使用するFibreBridge 7500Nまたは7600Nブリッジにおいて、MetroCluster 4またはDRグループ4でサポートされるシェルフ構成を示しています。この構成表を使用する際は、以下の点にご注意ください。

- Brocade G630 および G630-1 スイッチでは、追加のブリッジをポート 80 ～ 83 にケーブル接続できます。
- Brocade G730 スイッチでは、追加のブリッジをポート 84 ～ 95 にケーブル接続できます。

* コンポーネント *		* ポート *	* FC スイッチに接続 *	G630、G630-1 ポート	G730 ポート
スタック 1	bridge_x_1a	fc1	1.	74	80
FC2	2.	74	80	bridge_x_1b	fc1
1.	75	81	FC2	2.	75
81	スタック 2	bridge_x_2a	fc1	1.	78
82	FC2	2.	78	82	bridge_x_2b
fc1	1.	79	83	FC2	2.

1つのFCポート（FC1またはFC2）のみを使用するFibreBridge 7500Nまたは7600Nを使用するシェルフ構成

#### MetroCluster 1またはDRグループ1

以下の表は、FibreBridge 7500Nまたは7600NとBrocadeスイッチの1つのFCポート（FC1またはFC2）のみを使用した、MetroCluster 1またはDRグループ1でサポートされるシェルフ構成を示しています。この構成表を使用する際は、以下の点にご注意ください。

- Brocade 6505、G610、G710、G620、G620-1、G630、および G630-1 スイッチでは、追加のブリッジポート 12 ～ 15。
- Brocade 6510 および DCX 8510-8 スイッチでは、追加のブリッジをポート 12 ～ 19 にケーブル接続できます。
- Brocade 6520 スイッチでは、追加のブリッジをポート 16 ～ 21 および 24 ～ 45 にケーブル接続できます。
- Brocade G720 および G730 スイッチでは、追加のブリッジをポート 16 ～ 21 にケーブル接続できます。

* コンポー ネント *	* ポート *	* FC スイッチ に接続 *	6505、G 610、G7 10 ポート	6510、D CX 8510- 8 ポート	6520ポー ト	7810ポー ト	7840ポー ト	G620、G 620-1 、G630 、G630-1 ポート	G720、G 730 ポート
スタック 1	bridge_x _1a	1.	8.	8.	8.	8.	8.	8.	10.
bridge_x _1b	2.	8.	8.	8.	8.	8.	8.	10.	スタック 2

* コンポーネント *	* ポート *	* FC スイッチに接続 *	6505、G610、G710 ポート	6510、DCX 8510-8 ポート	6520ポート	7810ポート	7840ポート	G620、G620-1、G630、G630-1 ポート	G720、G730 ポート
bridge_x_2a	1.	9.	9.	9.	9.	9.	9.	11.	bridge_x_2b
2.	9.	9.	9.	9.	9.	9.	11.	スタック3	bridge_x_3a
1.	10.	10.	10.	10.	10.	10.	14	bridge_x_3b	2.
10.	10.	10.	10.	10.	10.	14	スタック4	bridge_x_4a	1.
11.	11.	11.	11.	11.	11.	15	bridge_x_4b	2.	11.

## MetroCluster 2またはDRグループ2

以下の表は、Brocadeスイッチの1つのFCポート（FC1またはFC2）を使用するFibreBridge 7500Nまたは7600Nブリッジにおいて、MetroCluster 2またはDRグループ2でサポートされるシェルフ構成を示しています。この構成表を使用する際は、以下の点にご注意ください。

- Brocade 6520 スイッチでは、追加のブリッジをポート 60 ~ 69 および 72 ~ 93 にケーブル接続できません。
- Brocade G620、G620-1、G630、G630-1 スイッチでは、追加のブリッジをポート 32 ~ 35 にケーブル接続できます。
- Brocade G720 および G730 スイッチでは、追加のブリッジをポート 36 ~ 39 にケーブル接続できます。
- 8ノードMetroCluster構成におけるBrocade 6505、G610、およびG710スイッチのポート使用状況は示されていません。ポート数が限られているため、コントローラモデル、使用するISLおよびブリッジペアの数に応じて、サイトごとにポートを割り当てます。

* コンポーネント *	* ポート *	* FC スイッチに接続 *	6505、G610、G710 ポート	6510、DCX 8510-8 ポート	6520ポート	7810ポート	7840ポート	G620、G620-1、G630、G630-1 ポート	G720、G730 ポート
スタック1	bridge_x_1a	1.	N/A	32	56	N/A	20	26	32
bridge_x_1b	2.	N/A	32	56	N/A	20	26	32	スタック2

* コンポーネント *	* ポート *	* FC スイッチに接続 *	6505、G610、G710 ポート	6510、DCX 8510-8 ポート	6520ポート	7810ポート	7840ポート	G620、G620-1、G630、G630-1 ポート	G720、G730 ポート
bridge_x_2a	1.	N/A	33	57	N/A	21	27	33	bridge_x_2b
2.	N/A	33	57	N/A	21	27	33	スタック 3	bridge_x_3a
1.	N/A	34	58	N/A	22	30	34	bridge_x_3b	2.
N/A	34	58	N/A	22	30	34	スタック 4	bridge_x_4a	1.
N/A	35	59	N/A	23	31.	35	bridge_x_4b	2.	N/A

### MetroCluster 3 または DR グループ 3

以下の表は、Brocadeスイッチの1つのFCポート（FC1またはFC2）を使用するFibreBridge 7500Nまたは7600Nブリッジにおいて、MetroCluster 3またはDRグループ3でサポートされるシェルフ構成を示しています。この構成表を使用する際は、以下の点にご注意ください。

- Brocade G630 および G630-1 スイッチでは、追加のブリッジをポート 60 ~ 63 にケーブル接続できません。
- Brocade G730 スイッチでは、追加のブリッジをポート 64、65、68、69 にケーブル接続できます。

* コンポーネント *	* ポート *	* FC スイッチに接続 *	G630、G630-1 ポート	G730 ポート
スタック 1	bridge_x_1a	1.	56	58
bridge_x_1b	2.	56	58	スタック 2
bridge_x_2a	1.	57	59	bridge_x_2b
2.	57	59	スタック 3	bridge_x_3a
1.	58	62	bridge_x_3b	2.
58	62	スタック 4	bridge_x_4a	1.
59	63	bridge_x_4b	2.	59

## MetroCluster 4 または DR グループ 4

以下の表は、Brocadeスイッチの1つのFCポート（FC1またはFC2）を使用するFibreBridge 7500Nまたは7600Nブリッジにおいて、MetroCluster 4またはDRグループ4でサポートされるシェルフ構成を示しています。この構成表を使用する際は、以下の点にご注意ください。

- Brocade G630 および G630-1 スイッチでは、追加のブリッジをポート 80 ～ 83 にケーブル接続できます。
- Brocade G730 スイッチでは、追加のブリッジをポート 84 ～ 95 にケーブル接続できます。

* コンポーネント *	* ポート *	* FC スイッチに接続 *	G630、G630-1 ポート	G730 ポート
スタック 1	bridge_x_1a	1.	74	80
bridge_x_1b	2.	74	80	スタック 2
bridge_x_2a	1.	75	81	bridge_x_2b
2.	75	81	スタック 3	bridge_x_3a
1.	78	82	bridge_x_3b	2.
78	82	スタック4	bridge_x_4a	1.
79	83	bridge_x_4b	2.	79

### MetroCluster FC構成におけるISLのBrocadeポートの使用

Brocade FC スイッチを ISL にケーブル接続するために必要なポート割り当てについて説明します。



- AFF A900およびFAS9500システムは8つのISLをサポートします。Brocade G620、G620-1、G630、G630-1、G720、およびG730スイッチでは8つのISLがサポートされます。
- Brocade 6520 スイッチは 8 つの ISL をサポートしますが、AFF A900およびFAS9500システムはサポートしません。

ISLポート	6505、G610 、G710 ポート	6520ポート	7810ポート	7840 (10Gbps) s) ポート	7840 (40Gbps) s) ポート	6510、G620 、G620-1 、G630、G630-1、G720 、G730 ポート
ISL、ポート 1	20	22	ge2	ge2	ge0	40

ISLポート	6505、G610、G710ポート	6520ポート	7810ポート	7840 (10Gbps) ポート	7840 (40Gbps) ポート	6510、G620、G620-1、G630、G630-1、G720、G730ポート
ISL、ポート 2	21	23	ge3	ge3	ge1	41.
ISL、ポート 3	22	46	ge4	ge10	N/A	42
ISL、ポート 4	23	47	ge5	ge11	N/A	43
ISL、ポート 5	N/A	70	ge6	N/A	N/A	44
ISL、ポート 6	N/A	71.	ge7	N/A	N/A	45
ISL、ポート 7	N/A	94	N/A	N/A	N/A	46
ISL ポート 8	N/A	95	N/A	N/A	N/A	47

#### MetroCluster FC構成におけるコントローラのCiscoポートの使用

Cisco 9124V、9148S、9148V、9250i、および 9396S FC スイッチをコントローラにケーブル接続するために必要なポート割り当てについて説明します。

次の表に、2つのDRグループに8つのコントローラモジュールを配置した場合のサポートされる最大構成を示します。それよりも小規模な構成の場合、余分なコントローラモジュールの行は無視してください。



- Cisco 9132Tについては、"[MetroCluster FC構成におけるコントローラのCisco 9132Tポートの使用](#)"。
- Cisco 9124V および 9250i スイッチは、8 ノードMetroCluster構成ではサポートされません。

#### MetroCluster 1またはDRグループ1

次の表は、Ciscoスイッチ (9132T を除く) 上のMetroCluster 1 または DR グループ 1 でサポートされているコントローラ構成を示しています。

* コンポーネント *	* ポート *	* FC スイッチに接続 *	9124Vポート	9148Sポート	9148Vポート	9250iポート	9396Sポート
controller_x_1	FC-VI ポート a	1.	1.	1.	1.	1.	1.
FC-VI ポート b	2.	1.	1.	1.	1.	1.	FC-VI ポート c
1.	2.	2.	2.	2.	2.	FC-VI ポート d	2.
2.	2.	2.	2.	2.	FC-VI-2 ポート A	1.	3.
N/A	3.	N/A	N/A	FC-VI-2 ポート b	2.	3.	N/A
3.	N/A	N/A	FC-VI-2 ポート c	1.	4.	N/A	4.
N/A	N/A	FC-VI-2 ポート d	2.	4.	N/A	4.	N/A
N/A	HBA ポート A	1.	13	3.	13	3.	3.
HBA ポート b	2.	13	3.	13	3.	3.	HBA ポート c
1.	14	4.	14	4.	4.	HBA ポート d	2.
14	4.	14	4.	4.	controller_x_2	FC-VI ポート a	1.
5.	5.	5.	5.	5.	FC-VI ポート b	2.	5.
5.	5.	5.	5.	FC-VI ポート c	1.	6.	6.
6.	6.	6.	FC-VI ポート d	2.	6.	6.	6.

* コンポーネント *	* ポート *	* FC スイッチに接続 *	9124Vポート	9148Sポート	9148Vポート	9250iポート	9396Sポート
6.	6.	FC-VI-2 ポート A	1.	7.	N/A	7.	N/A
N/A	FC-VI-2 ポート b	2.	7.	N/A	7.	N/A	N/A
FC-VI-2 ポート c	1.	8.	N/A	8.	N/A	N/A	FC-VI-2 ポート d
2.	8.	N/A	8.	N/A	N/A	HBA ポート A	1.
15	7.	15	7.	7.	HBA ポート b	2.	15
7.	15	7.	7.	HBA ポート c	1.	16	8.
16	8.	8.	HBA ポート d	2.	16	8.	16

## MetroCluster 2またはDRグループ2

次の表は、Ciscoスイッチ (9132T を除く) 上のMetroCluster 2 または DR グループ 2 でサポートされているコントローラ構成を示しています。

* コンポーネント *	* ポート *	* FC スイッチに接続 *	9124Vポート	9148Sポート	9148Vポート	9250iポート	9396Sポート
controller_x_3	FC-VI ポート a	1.	N/A	25	25	N/A	49
FC-VI ポート b	2.	N/A	25	25	N/A	49	FC-VI ポート c
1.	N/A	26	26	N/A	50	FC-VI ポート d	2.
N/A	26	26	N/A	50	FC-VI-2 ポート A	1.	N/A

* コンポーネント *	* ポート *	* FC スイッチに接続 *	9124Vポート	9148Sポート	9148Vポート	9250iポート	9396Sポート
N/A	27	N/A	N/A	FC-VI-2 ポート b	2.	N/A	N/A
27	N/A	N/A	FC-VI-2 ポート c	1.	N/A	N/A	28
N/A	N/A	FC-VI-2 ポート d	2.	N/A	N/A	28	N/A
N/A	HBA ポート A	1.	N/A	27	37	N/A	51
HBA ポート b	2.	N/A	27	37	N/A	51	HBA ポート c
1.	N/A	28	38	N/A	52	HBA ポート d	2.
N/A	28	38	N/A	52	controller_x_4	FC-VI ポート a	1.
N/A	29	29	N/A	53	FC-VI ポート b	2.	N/A
29	29	N/A	53	FC-VI ポート c	1.	N/A	30
30	N/A	54	FC-VI ポート d	2.	N/A	30	30
N/A	54	FC-VI-2 ポート A	1.	N/A	N/A	31.	N/A
N/A	FC-VI-2 ポート b	2.	N/A	N/A	31.	N/A	N/A
FC-VI-2 ポート c	1.	N/A	N/A	32	N/A	N/A	FC-VI-2 ポート d
2.	N/A	N/A	32	N/A	N/A	HBA ポート A	1.

* コンポーネント *	* ポート *	* FC スイッチに接続 *	9124Vポート	9148Sポート	9148Vポート	9250iポート	9396Sポート
N/A	31.	39	N/A	55	HBA ポート b	2.	N/A
31.	39	N/A	55	HBA ポート c	1.	N/A	32
40	N/A	56	HBA ポート d	1.	N/A	32	40

#### MetroCluster FC構成におけるFC-SASブリッジのCiscoポート使用

Cisco 9124V、9148S、9148V、9250i、および9396S FCスイッチをFC-SASブリッジに接続するために必要なポート割り当てについて説明します。ポート割り当ては、ブリッジが使用するFCポートが1つなのか2つなのかによって異なります。



Cisco 9132Tについては、"[MetroCluster FC構成におけるFC-SASブリッジ用のCisco 9132tポートの使用](#)"。

両方のFCポート（FC1およびFC2）を使用するFibreBridge 7500Nまたは7600Nを使用するシェルフ構成

#### MetroCluster 1またはDRグループ1

以下の表は、FibreBridge 7500Nまたは7600NブリッジとCiscoスイッチ（9132Tを除く）の両方のFCポート（FC1とFC2）を使用した、MetroCluster 1またはDRグループ1でサポートされるシェルフ構成を示しています。この構成表を使用する際は、以下の点にご注意ください。

- Cisco 9250i スイッチでは、追加のMetroCluster 1 または DR グループ 1 ブリッジをポート 17 ~ 40 にケーブル接続できます。
- Cisco 9396S スイッチでは、追加のMetroCluster 1 または DR グループ 1 ブリッジをポート 17 ~ 32 にケーブル接続できます。

* コンポーネント *	* ポート *	* FC スイッチに接続 *	9124Vポート	9148Sポート	9148Vポート	9250iポート	9396Sポート
スタック 1	bridge_x_1a	fc1	1.	17	9.	17	9.
FC2	2.	17	9.	17	9.	9.	bridge_x_1b fc1
1.	18	10.	18	10.	10.	FC2	2.
							18

* コンポーネント *		* ポート *	* FC スイッチ に接続 *	9124Vポ ート	9148Sポ ート	9148Vポ ート	9250i ポート	9396Sポ ート
10.	18	10.	10.	スタック 2	bridge_x_ 2a	fc1	1.	19
11.	19	11.	11.	FC2	2.	19	11.	19
11.	11.	bridge_x_ 2b	fc1	1.	20	12.	20	12.
12.	FC2	2.	20	12.	20	12.	12.	スタック 3
bridge_x_ 3a	fc1	1.	21	13	21	13	13	FC2
2.	21	13	21	13	13	bridge_x_ 3b	fc1	1.
22	14	22	14	14	FC2	2.	22	14
22	14	14	スタック4	bridge_x_ 4a	fc1	1.	23	15
23	15	15	FC2	2.	23	15	23	15
15	bridge_x_ 4b	fc1	1.	24	16	24	16	16

## MetroCluster 2またはDRグループ2

以下の表は、FibreBridge 7500Nまたは7600NとCiscoスイッチ（9132Tを除く）の両方のFCポート（FC1とFC2）を使用した、MetroCluster 2またはDRグループ2でサポートされるシェルフ構成を示しています。ケーブル接続表を使用する際は、以下の点にご注意ください。

- Cisco 9124V および 9250i スイッチは、8 ノードMetroCluster構成ではサポートされません。
- Cisco 9396S スイッチでは、追加のMetroCluster 2 (DR グループ 2) ブリッジをポート 65 ~ 80 にケーブル接続できます。

* コンポーネント *		* ポート *	* FC スイッチ に接続 *	9124Vポ ート	9148Sポ ート	9148Vポ ート	9250i ポート	9396Sポ ート
スタック 1	bridge_x_ 1a	fc1	1.	N/A	33	41.	N/A	57

* コンポーネント *		* ポート *	* FC スイッチ に接続 *	9124Vポ ート	9148Sポ ート	9148Vポ ート	9250i ポート	9396Sポ ート
FC2	2.	N/A	33	41.	N/A	57	bridge_x_ 1b	fc1
1.	N/A	34	42	N/A	58	FC2	2.	N/A
34	42	N/A	58	スタック 2	bridge_x_ 2a	fc1	1.	N/A
35	43	N/A	59	FC2	2.	N/A	35	43
N/A	59	bridge_x_ 2b	fc1	1.	N/A	36	44	N/A
60	FC2	2.	N/A	36	44	N/A	60	スタック 3
bridge_x_ 3a	fc1	1.	N/A	37	45	N/A	61	FC2
2.	N/A	37	45	N/A	61	bridge_x_ 3b	fc1	1.
N/A	38	46	N/A	62	FC2	2.	N/A	38
46	N/A	62	スタック 4	bridge_x_ 4a	fc1	1.	N/A	39
47	N/A	63	FC2	2.	N/A	39	47	N/A
63	bridge_x_ 4b	fc1	1.	N/A	40	48	N/A	64

1つのFCポート（FC1またはFC2）のみを使用するFibreBridge 7500Nまたは7600Nを使用するシェルフ構成

### MetroCluster 1またはDRグループ1

以下の表は、Ciscoスイッチ（9132Tを除く）上の1つのFCポート（FC1またはFC2）を使用するFibreBridge 7500Nまたは7600Nブリッジについて、MetroCluster 1またはDRグループ1でサポートされるシェルフ構成を示しています。リファレンス構成ファイル（RCF）はFibreBridgeブリッジ上の1つのFCポートをサポートしていないため、バックエンドのファイバチャネルスイッチを手動で設定する必要があります。

#### "Cisco FC スイッチを手動で設定"

ケーブルテーブルを使用するときは、次の点に注意してください。

- Cisco 9250i スイッチでは、追加のMetroCluster 1 または DR グループ 1 ブリッジをポート 17 ~ 40 にケーブル接続できます。
- Cisco 9396S スイッチでは、追加のMetroCluster 1 または DR グループ 1 ブリッジをポート 17 ~ 32 にケーブル接続できます。

* コンポーネント *	* ポート *	* FC スイッチに接続 *	9124Vポート	9148Sポート	9148Vポート	9250iポート	9396Sポート
スタック 1	bridge_x_1a	1.	17	9.	17	9.	9.
bridge_x_1b	2.	17	9.	17	9.	9.	スタック 2
bridge_x_2a	1.	18	10.	18	10.	10.	bridge_x_2b
2.	18	10.	18	10.	10.	スタック 3	bridge_x_3a
1.	19	11.	19	11.	11.	bridge_x_3b	2.
19	11.	19	11.	11.	スタック4	bridge_x_4a	1.
20	12.	20	12.	12.	bridge_x_4b	2.	20
12.	20	12.	12.	スタック5	bridge_x_5a	1.	21
13	21	13	13	bridge_x_5b	2.	21	13
21	13	13	スタック6	bridge_x_6a	1.	22	14
22	14	14	bridge_x_6b	2.	22	14	22
14	14	スタック7	bridge_x_7a	1.	23	15	23
15	15	bridge_x_7b	2.	23	15	23	15
15	スタック8	bridge_x_8a	1.	24	16	24	16
16	bridge_x_8b	2.	24	16	24	16	16

## MetroCluster 2またはDRグループ2

以下の表は、Ciscoスイッチ（9132Tを除く）上の1つのFCポート（FC1またはFC2）を使用するFibreBridge 7500Nまたは7600Nブリッジについて、MetroCluster 2またはDRグループ2でサポートされるシェルフ構成を示しています。この構成表を使用する際は、以下の点にご注意ください。

- Cisco 9124V および 9250i スイッチは、8 ノード MetroCluster 構成ではサポートされていません。
- Cisco 9396S スイッチでは、追加の MetroCluster 2 または DR グループ 2 ブリッジをポート 65 ~ 80 にケーブル接続できます。

* コンポーネント *	* ポート *	* FC スイッチに接続 *	9124Vポート	9148Sポート	9148Vポート	9250iポート	9396Sポート
スタック 1	bridge_x_1a	1.	N/A	33	41.	N/A	57
bridge_x_1b	2.	N/A	33	41.	N/A	57	スタック 2
bridge_x_2a	1.	N/A	34	42	N/A	58	bridge_x_2b
2.	N/A	34	42	N/A	58	スタック 3	bridge_x_3a
1.	N/A	35	43	N/A	59	bridge_x_3b	2.
N/A	35	43	N/A	59	スタック 4	bridge_x_4a	1.
N/A	36	44	N/A	60	bridge_x_4b	2.	N/A
36	44	N/A	60	スタック 5	bridge_x_5a	1.	N/A
37	45	N/A	61	bridge_x_5b	2.	N/A	37
45	N/A	61	スタック 6	bridge_x_6a	1.	N/A	38
46	N/A	62	bridge_x_6b	2.	N/A	38	46
N/A	62	スタック 7	bridge_x_7a	1.	N/A	39	47
N/A	63	bridge_x_7b	2.	N/A	39	47	N/A
63	スタック 8	bridge_x_8a	1.	N/A	40	48	N/A
64	bridge_x_8b	2.	N/A	40	48	N/A	64

#### MetroCluster FC構成におけるISLのCiscoポート使用

Cisco 9124V、9148S、9148V、9250i、および 9396S FC スイッチを ISL にケーブル接続するために必要なポート割り当てについて説明します。

次の表に、使用する ISL ポートを示します。ISL ポートの用途は、構成内のすべてのスイッチで同じです。



- Cisco 9132Tについては、"[MetroCluster FC構成におけるISL用のCisco 9132Tポートの使用](#)"。
- Cisco 9250i スイッチには 24 ポート ライセンスが必要です。

ISLポート	9124Vポート	9148Sポート	9148Vポート	9250i ポート	9396Sポート
ISL、ポート 1	9.	20	9.	12.	44
ISL、ポート 2	10.	24	10.	16	48
ISL、ポート 3	11.	44	11.	20	92
ISL、ポート 4	12.	48	12.	24	96
ISL、ポート 5	N/A	N/A	33	N/A	N/A
ISL、ポート 6	N/A	N/A	34	N/A	N/A
ISL、ポート 7	N/A	N/A	35	N/A	N/A
ISL ポート 8	N/A	N/A	36	N/A	N/A

#### MetroCluster FC構成におけるコントローラのCisco 9132Tポートの使用

Cisco 9132T FC スイッチをコントローラにケーブル接続するために必要なポートの割り当てについて説明します。

次の表は、両方のFCポート（FC1およびFC2）を使用するFibreBridge 7500Nまたは7600Nを使用するコントローラ構成を示しています。次の表に、2つのDRグループに4台と8台のコントローラモジュールを含む、サポートされる最大構成を示します。



8ノード構成の場合は、RCFは提供されないため、ゾーニングを手動で実行する必要があります。

#### MetroCluster 1またはDRグループ1

次の表は、Cisco 9132TスイッチのMetroCluster 1またはDRグループ1でサポートされるコントローラ構成を示しています。この構成表を使用する際は、以下の点にご注意ください。

- AFF A900およびFAS9500システムには、8つのFC-VIポート（FC-VI-1およびFC-VI-2の場合はa、b、c、d）があります。

* コンポーネント *		* ポート *	FC_switch に接続します ...	9132T 1x LEM (4ノ ード)	9132T 2x LEM (4ノ ード)	9132T 2x LEM (8ノ ード)
controller_x_1	FC-VI ポート a	1.	LEM1-1.	LEM1-1.	LEM1-1.	FC-VI ポート b
2.	LEM1-1.	LEM1-1.	LEM1-1.	FC-VI ポート c	1.	LEM1-2
LEM1-2	LEM1-2	FC-VI ポート d	2.	LEM1-2	LEM1-2	LEM1-2
FC-VI-2 ポー ト A	1.	LEM1-3	LEM1-3	N/A	FC-VI-2 ポー ト b	2.
LEM1-3	LEM1-3	N/A	FC-VI-2 ポー ト c	1.	LEM1-4.	LEM1-4.
N/A	FC-VI-2 ポー ト d	2.	LEM1-4.	LEM1-4.	N/A	HBA ポート A
1.	LEM1-5.	LEM1-5.	LEM1-3	HBA ポート b	2.	LEM1-5.
LEM1-5.	LEM1-3	HBA ポート c	1.	LEM1-6.	LEM1-6.	LEM1-4.
HBA ポート d	2.	LEM1-6.	LEM1-6.	LEM1-4.	controller_x_2	FC-VI ポート a
1.	LEM1-7.	LEM1-7.	LEM1-5.	FC-VI ポート b	2.	LEM1-7.
LEM1-7.	LEM1-5.	FC-VI ポート c	1.	LEM1-8	LEM1-8	LEM1-6.
FC-VI ポート d	2.	LEM1-8	LEM1-8	LEM1-6.	FC-VI-2 ポー ト A	1.
LEM1-9	LEM1-9	N/A	FC-VI-2 ポー ト b	2.	LEM1-9	LEM1-9
N/A	FC-VI-2 ポー ト c	1.	LEM1-10	LEM1-10	N/A	FC-VI-2 ポー ト d
2.	LEM1-10	LEM1-10	N/A	HBA ポート A	1.	LEM1-11

* コンポーネント *		* ポート *	FC_switch に接続します ...	9132T 1x LEM (4ノ ード)	9132T 2x LEM (4ノ ード)	9132T 2x LEM (8ノ ード)
LEM1-11	LEM1-7.	HBA ポート b	2.	LEM1-11	LEM1-11	LEM1-7.
HBA ポート c	1.	LEM1-12	LEM1-12	LEM1-8	HBA ポート d	2.

## MetroCluster 2またはDRグループ2

次の表は、Cisco 9132Tスイッチ上のMetroCluster 2またはDRグループ2でサポートされるCisco 9132Tコントローラ構成を示しています。この構成表を使用する際は、以下の点にご注意ください。

- AFF A900およびFAS9500システムには、8つのFC-VIポート (FC-VI-1 および FC-VI-2 の場合は a、b、c、d) があります。
- MetroCluster 2 または DR グループ 2 は、AFF A900およびFAS9500システム用のCisco 9132T スイッチではサポートされていません。
- MetroCluster 2またはDRグループ2は、8ノードのMetroCluster構成でのみサポートされます。

* コンポーネント *		* ポート *	FC_switch に接続します ...	9132T 1x LEM (4ノ ード)	9132T 2x LEM (4ノ ード)	9132T 2x LEM (8ノ ード)
controller_x_3	FC-VI ポート a	1.	N/A	N/A	LEM2-1	FC-VI ポート b
2.	N/A	N/A	LEM2-1	FC-VI ポート c	1.	N/A
N/A	LEM2-2	FC-VI ポート d	2.	N/A	N/A	LEM2-2
FC-VI-2 ポー ト A	1.	N/A	N/A	N/A	FC-VI-2 ポー ト b	2.
N/A	N/A	N/A	FC-VI-2 ポー ト c	1.	N/A	N/A
N/A	FC-VI-2 ポー ト d	2.	N/A	N/A	N/A	HBA ポート A
1.	N/A	N/A	LEM2-3	HBA ポート b	2.	N/A
N/A	LEM2-3	HBA ポート c	1.	N/A	N/A	LEM2-4

* コンポーネント *		* ポート *	FC_switch に接続します ...	9132T 1x LEM (4ノ ード)	9132T 2x LEM (4ノ ード)	9132T 2x LEM (8ノ ード)
HBA ポート d	2.	N/A	N/A	LEM2-4	controller_x_4	FC-VI 1 ポ ート a
1.	N/A	N/A	LEM2-5	FC-VI 1 ポ ート b	2.	N/A
N/A	LEM2-5	FC-VI-1 ポ ート c	1.	N/A	N/A	LEM2-6
FC-VI 1 ポ ート d	2.	N/A	N/A	LEM2-6	FC-VI-2 ポ ート A	1.
N/A	N/A	N/A	FC-VI-2 ポ ート b	2.	N/A	N/A
N/A	FC-VI-2 ポ ート c	1.	N/A	N/A	N/A	FC-VI-2 ポ ート d
2.	N/A	N/A	N/A	HBA ポート A	1.	N/A
N/A	LEM2-7	HBA ポート b	2.	N/A	N/A	LEM2-7
HBA ポート c	1.	N/A	N/A	LEM2-8	HBA ポート d	2.

#### MetroCluster FC構成におけるFC-SASブリッジ用のCisco 9132Tポートの使用

両方の FC ポートを使用してCisco 9132T FC スイッチを FC-to-SAS ブリッジにケーブル接続するために必要なポート割り当てについて説明します。



1xLEM モジュールを搭載したCisco 9132T スイッチを使用する場合、1つのブリッジ スタックのみがサポートされます。

#### MetroCluster 1またはDRグループ1

次の表は、Cisco 9132TスイッチのFCポート（FC1とFC2）の両方を使用するFibreBridge 7500Nまたは7600Nブリッジにおいて、MetroCluster 1またはDRグループ1でサポートされるシェルフ構成を示しています。この構成表を使用する際は、以下の点にご注意ください。

- 4 ノード構成では、2xLEM を搭載したCisco 9132T スイッチのポート LEM2-1 ~ LEM2-8 に追加のブリッジをケーブル接続できます。

* コンポーネント *		* ポート *	FC_switch に接続します ...	9132T 1x LEM (4ノ ード)	9132T 2x LEM (4ノ ード)	9132T 2x LEM (8ノ ード)
スタック 1	bridge_x_1a	fc1	1.	LEM1-13	LEM1-13	LEM1-9
FC2	2.	LEM1-13	LEM1-13	LEM1-9	bridge_x_1b	fc1
1.	LEM1-14	LEM1-14	LEM1-10	FC2	2.	LEM1-14
LEM1-14	LEM1-10	スタック 2	bridge_x_2a	fc1	1.	N/A
LEM1-15	LEM1-11	FC2	2.	N/A	LEM1-15	LEM1-11
bridge_x_2b	fc1	1.	N/A	LEM1-16	LEM1-12	FC2

## MetroCluster 2またはDRグループ2

次の表は、Cisco 9132Tスイッチの両方のFCポート（FC1とFC2）を使用するFibreBridge 7500Nまたは7600Nブリッジについて、MetroCluster 2またはDRグループ2でサポートされるシェルフ構成を示しています。この構成表を使用する際は、以下の点にご注意ください。

- 8ノード構成では、2つのLEMを搭載したCisco 9132TスイッチのポートLEM2-13～LEM2-16に追加のブリッジをケーブル接続できます。

* コンポーネント *		* ポート *	FC_switch に接続します ...	9132T 1x LEM (4ノ ード)	9132T 2x LEM (4ノ ード)	9132T 2x LEM (8ノ ード)
スタック 1	bridge_x_1a	fc1	1.	N/A	N/A	LEM1-9
FC2	2.	N/A	N/A	LEM1-9	bridge_x_1b	fc1
1.	N/A	N/A	LEM1-10	FC2	2.	N/A
N/A	LEM1-10	スタック 2	bridge_x_2a	fc1	1.	N/A
N/A	LEM1-11	FC2	2.	N/A	N/A	LEM1-11
bridge_x_2b	fc1	1.	N/A	N/A	LEM1-12	FC2

## MetroCluster FC構成におけるISL用のCisco 9132Tポートの使用

Cisco 9132T FC スイッチを ISL にケーブル接続するために必要なポート割り当てについて説明します。

次の表に、Cisco 9132TスイッチでのISLポートの用途を示します。

ISLポート	9132T 1x LEM (4ノード)	9132T 2x LEM (4ノード)	9132T 2x LEM (8ノード)
ISL、ポート 1	LEM1-15	LEM2-9	LEM1-13
ISL、ポート 2	LEM1-16	LEM2-10	LEM1-14
ISL、ポート 3	N/A	LEM2-11	LEM1-15
ISL、ポート 4	N/A	LEM2-12	LEM1-16
ISL、ポート 5	N/A	LEM2-13	N/A
ISL、ポート 6	N/A	LEM2-14	N/A
ISL、ポート 7	N/A	LEM2-15	N/A
ISL ポート 8	N/A	LEM2-16	N/A

#### 8 ノード / 4 ノード構成でのクラスタインターコネクトのケーブル接続

8ノードまたは4ノードのMetroCluster 構成では、各サイトでローカルコントローラモジュール間のクラスタインターコネクトをケーブル接続する必要があります。

このタスクについて

このタスクは、2 ノード MetroCluster 構成の場合は必要ありません。

このタスクは両方の MetroCluster サイトで実行する必要があります。

ステップ

1. 一方のコントローラモジュールからもう一方のコントローラモジュールへ、またはクラスタインターコネクトスイッチが使用されている場合は、各コントローラモジュールからスイッチへ、クラスタインターコネクトをケーブル接続します。

関連情報

["ONTAPハードウェアシステムのドキュメント"](#)

["ネットワークと LIF の管理"](#)

クラスタピアリングのケーブル接続

クラスタピアリングに使用するコントローラモジュールのポートをケーブル接続して、パートナーサイトのクラスタに接続できるようにする必要があります。

このタスクについて

このタスクは、MetroCluster 構成の各コントローラモジュールで実行する必要があります。

クラスタピアリングには、各コントローラモジュールの少なくとも 2 つのポートを使用します。

ポートおよびネットワーク接続の推奨される最小帯域幅は 1GbE です。

#### ステップ

1. クラスタピアリングに使用する少なくとも 2 つのポートを特定してケーブル接続し、そのポートがパートナークラスタとネットワーク接続されていることを確認します。

クラスタピアリングには、専用のポートとデータポートのどちらも使用できます。専用のポートを使用すると、クラスタピアリングトラフィックのスループットが向上します。

#### 関連情報

##### "クラスタと SVM のピアリングの簡単な設定"

各 MetroCluster サイトは、パートナーサイトのピアとして設定されます。ここでは、ピア関係を設定し、それらの関係に共有ポートと専用ポートのどちらを使用するかを決定する際に理解しておく必要がある前提条件とガイドラインを示します。

##### "クラスタピアリング"

#### HA インターコネクットのケーブル接続

8 ノード / 4 ノードの MetroCluster 構成で、HA ペアのストレージコントローラが別々のシャーシにある場合は、コントローラ間の HA インターコネクットをケーブル接続する必要があります。

#### このタスクについて

- このタスクは、2 ノード MetroCluster 構成には適用されません。
- このタスクは両方の MetroCluster サイトで実行する必要があります。
- HA インターコネクットをケーブル接続する必要があるのは、HA ペアのストレージコントローラが別々のシャーシにある場合のみです。

ストレージコントローラのモデルによっては、1 台のシャーシに 2 台のコントローラを設置でき、その場合は内部の HA インターコネクットが使用されます。

#### 手順

1. ストレージコントローラの HA パートナーが別のシャーシにある場合は、HA インターコネクットをケーブル接続します。

##### "ONTAPハードウェアシステムのドキュメント"

2. MetroCluster サイトに HA ペアが 2 つある場合は、2 つ目の HA ペアについて同じ手順を繰り返します。
3. MetroCluster パートナーサイトでこのタスクを繰り返します。

#### 管理ポートとデータポートのケーブル接続

各ストレージコントローラの管理ポートとデータポートをサイトネットワークにケーブル接続する必要があります。

このタスクについて

このタスクは、両方の MetroCluster サイトで新しいコントローラを配置するときに実行する必要があります。

コントローラおよびクラスタスイッチの管理ポートをネットワーク内の既存のスイッチに接続したり、NetApp CN1601 クラスタ管理スイッチなどの新しい専用ネットワークスイッチに接続したりできます。

ステップ

1. コントローラの管理ポートとデータポートを、ローカルサイトの管理ネットワークとデータネットワークにケーブル接続します。

["ONTAPハードウェアシステムのドキュメント"](#)

## FC スイッチを設定

FCスイッチの設定の概要

RCFファイルを使用してCiscoとBrocadeのFCスイッチを設定できます。また、必要に応じてスイッチを手動で設定することもできます。

状況	使用する手順
要件を満たすRCFを用意する	<ul style="list-style-type: none"><li>• <a href="#">"RCFファイルを使用して Brocade FC スイッチを設定します"</a></li><li>• <a href="#">"RCFファイルによるCisco FCスイッチの設定"</a></li></ul>
RCFがないか、要件を満たしていないRCFがある	<ul style="list-style-type: none"><li>• <a href="#">"Brocade FC スイッチを手動で設定"</a></li><li>• <a href="#">"Cisco FC スイッチを手動で設定"</a></li></ul>

RCF ファイルを使用して **Brocade FC** スイッチを設定します

**Brocade FC** スイッチを工場出荷時のデフォルトにリセット

新しいソフトウェアバージョンと RCF ファイルをインストールする前に、現在のスイッチの設定を消去し、基本的な設定を完了する必要があります。

このタスクについて

この手順は、MetroCluster ファブリック構成内の各 FC スイッチで実行する必要があります。

手順

1. 管理者としてスイッチにログインします。
2. Brocade Virtual Fabric (VF) 機能を無効にします。

「[fosconfig options](#)」を参照してください

```
FC_switch_A_1:admin> fosconfig --disable vf
WARNING: This is a disruptive operation that requires a reboot to take
effect.
Would you like to continue [Y/N]: y
```

3. スイッチのポートから ISL ケーブルを外します。
4. スイッチを無効にします。

```
switchcfgpersistentdisable
```

```
FC_switch_A_1:admin> switchcfgpersistentdisable
```

5. 設定を無効にします。

```
「cfgDisable」
```

```
FC_switch_A_1:admin> cfgDisable
You are about to disable zoning configuration. This action will disable
any previous zoning configuration enabled.
Do you want to disable zoning configuration? (yes, y, no, n): [no] y
Updating flash ...
Effective configuration is empty. "No Access" default zone mode is ON.
```

6. 設定をクリアします。

```
「cfgClear」
```

```
FC_switch_A_1:admin> cfgClear
The Clear All action will clear all Aliases, Zones, FA Zones
and configurations in the Defined configuration.
Run cfgSave to commit the transaction or cfgTransAbort to
cancel the transaction.
Do you really want to clear all configurations? (yes, y, no, n): [no] y
```

7. 設定を保存します。

```
cfgsave
```

```
FC_switch_A_1:admin> cfgSave
You are about to save the Defined zoning configuration. This
action will only save the changes on Defined configuration.
Do you want to save the Defined zoning configuration only? (yes, y, no,
n): [no] y
Updating flash ...
```

8. デフォルトの設定を行います。

「configDefault」

```
FC_switch_A_1:admin> configDefault
WARNING: This is a disruptive operation that requires a switch reboot.
Would you like to continue [Y/N]: y
Executing configdefault...Please wait
2020/10/05-08:04:08, [FCR-1069], 1016, FID 128, INFO, FC_switch_A_1, The
FC Routing service is enabled.
2020/10/05-08:04:08, [FCR-1068], 1017, FID 128, INFO, FC_switch_A_1, The
FC Routing service is disabled.
2020/10/05-08:04:08, [FCR-1070], 1018, FID 128, INFO, FC_switch_A_1, The
FC Routing configuration is set to default.
Committing configuration ... done.
2020/10/05-08:04:12, [MAPS-1113], 1019, FID 128, INFO, FC_switch_A_1,
Policy dflt_conservative_policy activated.
2020/10/05-08:04:12, [MAPS-1145], 1020, FID 128, INFO, FC_switch_A_1,
FPI Profile dflt_fpi_profile is activated for E-Ports.
2020/10/05-08:04:12, [MAPS-1144], 1021, FID 128, INFO, FC_switch_A_1,
FPI Profile dflt_fpi_profile is activated for F-Ports.
The switch has to be rebooted to allow the changes to take effect.
2020/10/05-08:04:12, [CONF-1031], 1022, FID 128, INFO, FC_switch_A_1,
configDefault completed successfully for switch.
```

9. すべてのポートについて、ポートの設定を default に設定します。

```
portcfgdefault_port-number_
```

```
FC_switch_A_1:admin> portcfgdefault <port number>
```

この手順はポートごとに実行する必要があります。

10. FOS 9.0 より前のバージョンを実行している場合は、スイッチが動的ポート オン デマンド (POD) 方式を使用していることを確認します。



Fabric OS 9.0以降では、ライセンス方式はデフォルトで動的です。静的ライセンス方式はサポートされていません。

バージョン 8.0 より前の Brocade Fabric OS では、次のコマンドを admin として実行し、バージョン 8.0 以降では root として実行します。

- a. ライセンスコマンドを実行します。

```
licenseport --show。
```

```
FC_switch_A_1:admin> license --show -port
24 ports are available in this switch
Full POD license is installed
Dynamic POD method is in use
```

- b. Brocade によって root ユーザが無効にされている場合は、有効にします。

```
FC_switch_A_1:admin> userconfig --change root -e yes
FC_switch_A_1:admin> rootaccess --set consoleonly
```

- c. ライセンスコマンドを実行します。

```
licenseport --show。
```

```
FC_switch_A_1:root> license --show -port
24 ports are available in this switch
Full POD license is installed
Dynamic POD method is in use
```

- d. Fabric OS 8.2.x以前を実行している場合は、ライセンス方式をdynamicに変更する必要があります。

```
licenseport — メソッドの動的
```

```
FC_switch_A_1:admin> licenseport --method dynamic
The POD method has been changed to dynamic.
Please reboot the switch now for this change to take effect
```

11. スイッチをリブートします。

「Fastboot」を参照してください

```
FC_switch_A_1:admin> fastboot
Warning: This command would cause the switch to reboot
and result in traffic disruption.
Are you sure you want to reboot the switch [y/n]?y
```

12. デフォルト設定が実装されたことを確認します。

```
'witchshow'
```

13. IP アドレスが正しく設定されていることを確認します。

```
ipAddrShow
```

必要に応じて、次のコマンドで IP アドレスを設定できます。

```
ipAddrSet
```

#### Brocade FC スイッチの RCF ファイルのダウンロード

MetroCluster ファブリック構成内の各スイッチにリファレンス構成ファイル（RCF）をダウンロードする必要があります。

このタスクについて

これらの RCF ファイルを使用するには、システムで ONTAP 9.1 以降を実行している必要があり、ONTAP 9.1 以降のポートレイアウトを使用する必要があります。

FibreBridgeブリッジのFCポートの1つだけを使用する予定の場合は、セクションの指示に従ってバックエンドのファイバチャネルスイッチを手動で構成します。"[FCスイッチのポート割り当て](#)"。

手順

1. Brocade RCF ダウンロードページの RCF ファイルの表を参照し、構成内の各スイッチに対応する正しい RCF ファイルを特定します。

RCF ファイルを正しいスイッチに適用する必要があります。

2. スイッチ用の RCF ファイルをからダウンロードします "[MetroCluster の RCF ダウンロード](#)" ページ

ファイルは、スイッチに転送できる場所に配置する必要があります。2つのスイッチファブリックを構成する4つのスイッチのそれぞれに、個別のファイルがあります。

3. 構成内のスイッチごとに上記の手順を繰り返します。

#### Brocade FC スイッチの RCF ファイルをインストールします

Brocade FC スイッチを設定する際には、特定の構成のスイッチ設定がすべて定義されたスイッチ構成ファイルをインストールできます。

このタスクについて

- この手順は、MetroClusterファブリック構成内の各Brocade FCスイッチで実行する必要があります。

- xWDM構成を使用する場合は、ISLの設定が必要になることがあります。詳細については、xWDMベンダーのドキュメントを参照してください。

## 手順

1. ダウンロードと設定のプロセスを開始します。

「configDownload」

次の例に示すようにプロンプトに応答します。

```
FC_switch_A_1:admin> configDownload
Protocol (scp, ftp, sftp, local) [ftp]:
Server Name or IP Address [host]: <user input>
User Name [user]:<user input>
Path/Filename [<home dir>/config.txt]:path to configuration file
Section (all|chassis|switch [all]): all
.
.
.
Do you want to continue [y/n]: y
Password: <user input>
```

パスワードを入力すると、スイッチはコンフィギュレーションファイルをダウンロードして実行します。

2. 構成ファイルでスイッチドメインが設定されていることを確認します。

'witchshow'

スイッチが使用する構成ファイルに応じて、各スイッチに異なるドメイン番号が割り当てられます。

```
FC_switch_A_1:admin> switchShow
switchName: FC_switch_A_1
switchType: 109.1
switchState: Online
switchMode: Native
switchRole: Subordinate
switchDomain: 5
```

3. 次の表に示すように、スイッチに正しいドメイン値が割り当てられていることを確認します。

ファブリック	スイッチ	スイッチドメイン
1.	A_1	5.
B_1.	7.	2.

A\_2

6.

B\_2

#### 4. ポート速度を変更します。

「portcfgspeed」

```
FC_switch_A_1:admin> portcfgspeed port number port speed
```

デフォルトでは、すべてのポートが 16Gbps で動作するように設定されています。ポート速度は次のような理由で変更される可能性があります。

- 8 Gbps の FC-VI アダプタを使用し、スイッチポート速度を 8Gbps に設定している場合、インターコネクトスイッチポート速度を変更する必要があります。
- ISL が 16Gbps で実行されない場合は、ISL ポートの速度を変更する必要があります。

#### 5. ISL の距離を計算します。

FC-VI の動作により、この距離を 10 (LE) 以上の実際の距離の 1.5 倍に設定する必要があります。ISL の距離は次のように計算され、km 単位に切り上げられます。1.5 × 実際の距離 = 距離です。

距離が 3km の場合は、1.5 × 3 km = 4.5 となります。これは 10 より小さいため、ISL は LE の距離レベルに設定する必要があります。

この距離は 20km の場合は、20km × 1.5 = 30 となり、ISL は LS 距離レベルに設定する必要があります。

#### 6. ISL ポートごとに距離を設定します。

```
longdistance_port level vc_link_init__ distance_ddistance value
```

vc\_link\_init の値が 1 の場合は、デフォルトで fillword 「ARB」が使用されます。0 の値は、fillword "idle" を使用します。必要な値は、使用するリンクによって異なる場合があります。この例では、デフォルトが設定され、距離は 20 km と想定されていますしたがって、設定は「30」で、VC\_link\_init の値は「1」、ISL ポートは「21」です。

例：ls

```
FC_switch_A_1:admin> portcfglongdistance 21 LS 1 -distance 30
```

例：LE

```
FC_switch_A_1:admin> portcfglongdistance 21 LE 1
```

#### 7. スイッチを永続的に有効にします。

'witchcfgpersistentenable

次の例は、FC switch\_A\_1 を永続的に有効にします。

```
FC_switch_A_1:admin> switchcfgpersistentenable
```

8. IP アドレスが正しく設定されていることを確認します。

ipaddrshow

```
FC_switch_A_1:admin> ipAddrshow
```

必要に応じて、IP アドレスを設定できます。

ipAddrSet

9. スイッチのプロンプトでタイムゾーンを設定します。

tstimezone — 対話型

プロンプトに対してと入力します。

```
FC_switch_A_1:admin> tstimezone --interactive
```

10. スイッチをリブートします。

「再起動」

次の例は、FC switch\_A\_1 をリブートします。

```
FC_switch_A_1:admin> reboot
```

11. 距離設定を確認します。

portbuffershow

LE の距離設定は 10 km と表示されます

```
FC_Switch_A_1:admin> portbuffershow
User Port Lx   Max/Resv Buffer Needed  Link      Remaining
Port Type Mode Buffers  Usage  Buffers Distance Buffers
-----
...
21    E    -     8      67     67     30 km
22    E    -     8      67     67     30 km
...
23    -     8     0      -      -      466
```

12. ISL ケーブルを、取り外したスイッチのポートに再接続します。

工場出荷時の設定にリセットすると、ISL ケーブルは切断されています。

"Brocade FC スイッチを工場出荷時のデフォルトにリセット"

13. 構成を検証

a. スイッチが1つのファブリックを形成することを確認します。

'witchshow'

次の例は、ポート 20 とポート 21 上の ISL を使用する構成の出力です。

```
FC_switch_A_1:admin> switchshow
switchName: FC_switch_A_1
switchType: 109.1
switchState:Online
switchMode: Native
switchRole: Subordinate
switchDomain:      5
switchId:   fffc01
switchWwn:  10:00:00:05:33:86:89:cb
zoning:      OFF
switchBeacon: OFF

Index Port Address Media Speed State  Proto
=====
...
20   20   010C00   id    16G  Online FC   LE E-Port
10:00:00:05:33:8c:2e:9a "FC_switch_B_1" (downstream) (trunk master)
21   21   010D00   id    16G  Online FC   LE E-Port (Trunk port,
master is Port 20)
...
```

b. ファブリックの設定を確認します。

「fabricshow」

```
FC_switch_A_1:admin> fabricshow
Switch ID      Worldwide Name      Enet IP Addr FC IP Addr Name
-----
1: fffc01 10:00:00:05:33:86:89:cb 10.10.10.55  0.0.0.0
"FC_switch_A_1"
3: fffc03 10:00:00:05:33:8c:2e:9a 10.10.10.65  0.0.0.0
>"FC_switch_B_1"
```

- c. ISL が機能していることを確認します。

「islshow」

```
FC_switch_A_1:admin> islshow
```

- d. ゾーニングが正しくレプリケートされたことを確認します。

「cfgshow」 + 「zoneshow」と入力します

両方の出力に、両方のスイッチの同じ設定情報とゾーニング情報が表示されます。

- e. トランキングを使用する場合は、トランキングを確認します。

「トラクショー」

```
FC_switch_A_1:admin> trunkshow
```

## RCF ファイルを使用して Cisco FC スイッチを設定します

### Cisco FC スイッチを工場出荷時のデフォルトにリセット

新しいバージョンのソフトウェアと RCF をインストールする前に、Cisco スイッチの設定を消去し、基本的な設定を完了する必要があります。

このタスクについて

この手順は、MetroCluster ファブリック構成内の各 FC スイッチで実行する必要があります。



出力は Cisco IP スイッチについてのものですが、Cisco FC スイッチについても同様です。

手順

1. スイッチを工場出荷時のデフォルトにリセットします。
  - a. 既存の設定を消去します **:write erase**
  - b. スイッチ・ソフトウェアをリロードします **+reload**

システムがリブートし、設定ウィザードが表示されます。起動中に、Abort Auto Provisioning（自動プロビジョニングの中止）というプロンプトが表示され、通常の設定アップを続行する場合（yes/no） [n]、「\*yes\*」と応答して続行します。

- c. 設定ウィザードで、スイッチの基本設定を入力します。
  - 管理パスワード
  - スイッチ名
  - アウトオブバンド管理設定

- デフォルトゲートウェイ
- SSHサービス (Remote Support Agent) 。

設定ウィザードが完了すると、スイッチがリブートします。

- d. プロンプトが表示されたら、ユーザ名とパスワードを入力してスイッチにログインします。

次の例は、スイッチにログインする際のプロンプトおよびシステム応答を示しています。山括弧（「\* <\*>」）は、情報を入力する場所を示します。

```
---- System Admin Account Setup ----
Do you want to enforce secure password standard (yes/no) [y]:y
**<<<*
```

```
    Enter the password for "admin": password  **<<<*
    Confirm the password for "admin": password  **<<<*
```

```
        ---- Basic System Configuration Dialog VDC: 1 ----
```

This setup utility will guide you through the basic configuration of the system. Setup configures only enough connectivity for management of the system.

Please register Cisco Nexus3000 Family devices promptly with your supplier. Failure to register may affect response times for initial service calls. Nexus3000 devices must be registered to receive entitled support services.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime to skip the remaining dialogs.

- e. 次のプロンプトで、スイッチ名、管理アドレス、ゲートウェイなどの基本情報を入力し、SSH キーに「\*rsa\*」と入力します。

```
Would you like to enter the basic configuration dialog (yes/no): yes
Create another login account (yes/no) [n]:
Configure read-only SNMP community string (yes/no) [n]:
Configure read-write SNMP community string (yes/no) [n]:
Enter the switch name : switch-name **<<<
Continue with Out-of-band (mgmt0) management configuration?
(yes/no) [y]:
  Mgmt0 IPv4 address : management-IP-address **<<<
  Mgmt0 IPv4 netmask : management-IP-netmask **<<<
Configure the default gateway? (yes/no) [y]: y **<<<
  IPv4 address of the default gateway : gateway-IP-address **<<<
Configure advanced IP options? (yes/no) [n]:
Enable the telnet service? (yes/no) [n]:
Enable the ssh service? (yes/no) [y]: y **<<<
  Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
**<<<
  Number of rsa key bits <1024-2048> [1024]:
Configure the ntp server? (yes/no) [n]:
Configure default interface layer (L3/L2) [L2]:
Configure default switchport interface state (shut/noshut)
[noshut]: shut **<<<
  Configure CoPP system profile (strict/moderate/lenient/dense)
[strict]:
```

最後の一連のプロンプトで設定が完了します。

The following configuration will be applied:

```
password strength-check
switchname IP_switch_A_1
vrf context management
ip route 0.0.0.0/0 10.10.99.1
exit
no feature telnet
ssh key rsa 1024 force
feature ssh
system default switchport
system default switchport shutdown
copp profile strict
interface mgmt0
ip address 10.10.99.10 255.255.255.0
no shutdown
```

Would you like to edit the configuration? (yes/no) [n]:

Use this configuration and save it? (yes/no) [y]:

```
2017 Jun 13 21:24:43 A1 %$ VDC-1 %$ %COPP-2-COPP_POLICY: Control-Plane
is protected with policy copp-system-p-policy-strict.
```

```
[#####] 100%
Copy complete.
```

```
User Access Verification
IP_switch_A_1 login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
.
.
.
IP_switch_A_1#
```

2. 設定を保存します。

```
IP_switch_A_1# copy running-config startup-config
```

3. スイッチをリブートし、スイッチがリロードされるまで待ちます。

```
IP_switch_A_1# reload
```

4. MetroCluster ファブリック構成の他の 3 つのスイッチについて、上記の手順を繰り返します。

MetroCluster ファブリック構成の各スイッチにスイッチのオペレーティングシステムファイルと RCF ファイルをダウンロードする必要があります。

作業を開始する前に

この作業には、FTP、TFTP、SFTP、SCP などのファイル転送ソフトウェアが必要です。ファイルをスイッチにコピーします。

このタスクについて

この手順は、MetroCluster ファブリック構成の各 FC スイッチで実行する必要があります。

サポートされているバージョンのスイッチソフトウェアを使用する必要があります。

["NetApp Hardware Universe の略"](#)



出力は Cisco IP スイッチについてのものですが、Cisco FC スイッチについても同様です。

手順

1. サポートされている NX-OS ソフトウェアファイルをダウンロードします。

["シスコのダウンロードページ"](#)

2. スイッチソフトウェアをスイッチにコピーします。

```
'copy sftp://root@server-IP-address/tftpboot/NX-OS -file-name bootflash:vrf management'
```

この例では、「nxos.7.0.3.i4.6.bin」ファイルが SFTP サーバ 10.10.99.99 からローカルブートフラッシュにコピーされています。

```
IP_switch_A_1# copy sftp://root@10.10.99.99/tftpboot/nxos.7.0.3.I4.6.bin
bootflash: vrf management
root@10.10.99.99's password: password
sftp> progress
Progress meter enabled
sftp> get /tftpboot/nxos.7.0.3.I4.6.bin
/bootflash/nxos.7.0.3.I4.6.bin
Fetching /tftpboot/nxos.7.0.3.I4.6.bin to /bootflash/nxos.7.0.3.I4.6.bin
/tftpboot/nxos.7.0.3.I4.6.bin          100% 666MB 7.2MB/s
01:32
sftp> exit
Copy complete, now saving to disk (please wait)...
```

3. 各スイッチの bootflash ディレクトリにスイッチの NX-OS ファイルがあることを確認します。

「IR ブートフラッシュ」

次の例は 'ファイルが ip\_switch\_a\_1' に存在することを示しています

```
IP_switch_A_1# dir bootflash:
      .
      .
      .
698629632   Jun 13 21:37:44 2017  nxos.7.0.3.I4.6.bin
      .
      .
      .

Usage for bootflash://sup-local
 1779363840 bytes used
13238841344 bytes free
15018205184 bytes total
IP_switch_A_1#
```

#### 4. スイッチソフトウェアをインストールします。

すべてのシステムブートフラッシュをインストールします。 nxos.version-number.bin キックスタート  
bootflash:nxos.version-kickstart -number.bin

```
IP_switch_A_1# install all system bootflash:nxos.7.0.3.I4.6.bin
kickstart bootflash:nxos.7.0.3.I4.6.bin
Installer will perform compatibility check first. Please wait.

Verifying image bootflash:/nxos.7.0.3.I4.6.bin for boot variable
"kickstart".
[#####] 100% -- SUCCESS

Verifying image bootflash:/nxos.7.0.3.I4.6.bin for boot variable
"system".
[#####] 100% -- SUCCESS

Performing module support checks.
[#####] 100% -- SUCCESS

Verifying image type.
[#####] 100% -- SUCCESS

Extracting "system" version from image bootflash:/nxos.7.0.3.I4.6.bin.
[#####] 100% -- SUCCESS

Extracting "kickstart" version from image
bootflash:/nxos.7.0.3.I4.6.bin.
[#####] 100% -- SUCCESS
...
```

スイッチソフトウェアをインストールすると、スイッチが自動的にリブートします。

5. スイッチがリロードされるまで待ってから、スイッチにログインします。

スイッチがリブートされると、ログインプロンプトが表示されます。

```
User Access Verification
IP_switch_A_1 login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2017, Cisco and/or its affiliates.
All rights reserved.
.
.
.
MDP database restore in progress.
IP_switch_A_1#

The switch software is now installed.
```

6. スイッチソフトウェアがインストールされたことを確認します。

'how version (バージョンの表示) '

次の例は、の出力を示しています。

```

IP_switch_A_1# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2017, Cisco and/or its affiliates.
All rights reserved.
.
.
.

Software
  BIOS: version 04.24
  NXOS: version 7.0(3)I4(6)   **<<< switch software version**
  BIOS compile time: 04/21/2016
  NXOS image file is: bootflash:///nxos.7.0.3.I4.6.bin
  NXOS compile time: 3/9/2017 22:00:00 [03/10/2017 07:05:18]

Hardware
  cisco Nexus 3132QV Chassis
  Intel(R) Core(TM) i3- CPU @ 2.50GHz with 16401416 kB of memory.
  Processor Board ID FOC20123GPS

  Device name: A1
  bootflash: 14900224 kB
  usb1: 0 kB (expansion flash)

Kernel uptime is 0 day(s), 0 hour(s), 1 minute(s), 49 second(s)

Last reset at 403451 usecs after Mon Jun 10 21:43:52 2017

Reason: Reset due to upgrade
System version: 7.0(3)I4(1)
Service:

plugin
  Core Plugin, Ethernet Plugin
IP_switch_A_1#

```

7. MetroCluster ファブリック構成の残りの 3 つの FC スイッチについて、上記の手順を繰り返します。

**Cisco FC RCF** ファイルのダウンロードとインストール

MetroCluster ファブリック構成内の各スイッチに RCF ファイルをダウンロードする必要があります。

作業を開始する前に

この作業では、スイッチにファイルをコピーするために、FTP、Trivial File Transfer Protocol（TFTP；簡易ファイル転送プロトコル）、SFTP、Secure Copy Protocol（SCP）などのファイル転送ソフトウェアが必要です。

このタスクについて

この手順は、MetroCluster ファブリック構成内の各 Cisco FC スイッチで実行する必要があります。

サポートされているバージョンのスイッチソフトウェアを使用する必要があります。

### "NetApp Hardware Universe の略"

RCF ファイルは 4 つあり、それぞれが MetroCluster ファブリック構成の 4 つの各スイッチに対応しています。使用するスイッチのモデルに対応した正しい RCF ファイルを使用する必要があります。

スイッチ	RCF ファイル
FC_switch_A_1 を使用します	「NX3232_v1.80_Switch-A1.txt」というテキストを入力します
FC_switch_A_2	「NX3232_v1.80_Switch-A2.txt」を参照してください
FC_switch_B_1	「NX3232_v1.80_Switch-B1.txt」というテキストを入力します
FC_switch_B_2	NX323232_v1.80_Switch-B2.txt



出力は Cisco IP スイッチについてのものですが、Cisco FC スイッチについても同様です。

手順

1. Cisco FC の RCF ファイルをからダウンロードします "[MetroCluster の RCF ダウンロードページ](#)"。
2. RCF ファイルをスイッチにコピーします。
  - a. RCF ファイルを最初のスイッチにコピーします。

```
'copy sftp://_root@ftp-server-ip-address /tftpboot/switch-specific - rcf_bootflash:vrf management'
```

この例では 'NX32323\_v1.80\_Switch-A1.txt' RCF ファイルが '10.10.99.99' の SFTP サーバからローカルブートフラッシュにコピーされます使用する TFTP / SFTP サーバの IP アドレスと、インストールする必要がある RCF ファイルのファイル名を使用する必要があります。

```

IP_switch_A_1# copy sftp://root@10.10.99.99/tftpboot/NX3232_v1.8T-
X1_Switch-A1.txt bootflash: vrf management
root@10.10.99.99's password: password
sftp> progress
Progress meter enabled
sftp> get /tftpboot/NX3232_v1.80_Switch-A1.txt
/bootflash/NX3232_v1.80_Switch-A1.txt
Fetching /tftpboot/NX3232_v1.80_Switch-A1.txt to
/bootflash/NX3232_v1.80_Switch-A1.txt
/tftpboot/NX3232_v1.80_Switch-A1.txt          100% 5141      5.0KB/s
00:00
sftp> exit
Copy complete, now saving to disk (please wait)...
IP_switch_A_1#

```

a. 残りの3つのスイッチのそれぞれについて、同じ手順を繰り返します。それぞれのスイッチに対応する RCF ファイルをコピーするように注意してください。

3. 各スイッチの「bootflash」ディレクトリに RCF ファイルがあることを確認します。

「IR bootflash:」のように表示されます

次の例は、FC\_switch\_A\_1 にファイルが存在することを示しています。

```

IP_switch_A_1# dir bootflash:
      .
      .
      .
5514   Jun 13 22:09:05 2017  NX3232_v1.80_Switch-A1.txt
      .
      .
      .

Usage for bootflash://sup-local
 1779363840 bytes used
13238841344 bytes free
15018205184 bytes total
IP_switch_A_1#

```

4. 各スイッチで、対応する RCF ファイルをローカルブートフラッシュから実行中の設定にコピーします。

copy bootflash: *switch-specific-RCF.txt* running-config

5. 各スイッチで、実行中の設定からスタートアップ設定に RCF ファイルをコピーします。

'copy running-config startup-config

次のような出力が表示されます。

```
IP_switch_A_1# copy bootflash:NX3232_v1.80_Switch-A1.txt running-config
IP_switch_A_1# copy running-config startup-config
```

6. スイッチをリロードします。

「再ロード」

```
IP_switch_A_1# reload
```

7. MetroCluster IP 構成の他の 3 つのスイッチについて、上記の手順を繰り返します。

### Brocade FC スイッチを手動で設定

MetroCluster 構成内の各 Brocade スイッチファブリックを設定する必要があります。

作業を開始する前に

- Telnet または Secure Shell (SSH) を使用して FC スイッチにアクセス可能な PC または UNIX ワークステーションが必要です。
- 同じバージョンとライセンスの Brocade Fabric Operating System (FOS) を実行している、同じモデルの Brocade スイッチ (サポートされるもの) を 4 つ使用している必要があります。

["NetApp Interoperability Matrix Tool で確認できます"](#)

IMT では、Storage 解決策フィールドを使用して MetroCluster 解決策を選択できます。検索を絞り込むには、\* 構成部品エクスペローラ \* を使用して構成部品と ONTAP バージョンを選択します。[ 結果の表示 (Show Results) ] をクリックすると、条件に一致するサポートされている構成のリストを表示できます。

- サポートされる 4 つの Brocade スイッチがそれぞれ 2 つのスイッチで構成される 2 つのファブリックに接続されます。各ファブリックが両方のサイトにまたがっている必要があります。
- 各ストレージコントローラに、スイッチファブリックに接続可能なイニシエータポートが 4 つ必要です。各ストレージコントローラの 2 つのイニシエータポートを各ファブリックに接続する必要があります。



FAS8020、AFF8020、FAS8200、および AFF A300 のシステムでは、次のすべての条件に該当する場合、コントローラあたりのイニシエータポートを 2 ポート (各ファブリックに 1 つのイニシエータポートを接続) にすることができます。

- ディスクストレージの接続に使用できる FC イニシエータポートが 3 つ以下で、それ以外に FC イニシエータとして設定できるポートがない。
- すべてのスロットが使用中で、FC イニシエータカードを追加できません。

このタスクについて

- スイッチ間リンク (ISL) トランキングがリンクでサポートされている場合、これを有効にする必要があります。

## "ファブリック接続 MetroCluster 構成で TDM / WDM 機器を使用する場合の考慮事項"

- xWDM構成を使用する場合は、ISLの設定が必要になることがあります。詳細については、xWDMベンダーのドキュメントを参照してください。
- 1つのファブリック内のすべての ISL の長さや速度が同じである必要があります。

ISL の長さはファブリックが異なる場合は同じである必要はありませんが、速度はすべてのファブリックで同じである必要があります。

- Metro-E および TDM (SONET / SDH) はサポートされず、FC 以外のネイティブのフレーミングやシグナリングはサポートされていません。

Metro-E とは、長距離 (メトロ距離) 間でネイティブに、または何らかの時分割多重化 (TDM)、Multiprotocol Label Switching (MPLS)、波長分割多重化 (WDM) 経由で行われるイーサネットフレーミングまたはシグナリングを意味します。

- TDM、FCR (ネイティブの FC ルーティング)、または FCIP の拡張機能は、MetroCluster FC スイッチファブリックではサポートされていません。
- 次の Brocade FC スイッチは、MetroCluster FC バックエンドファブリックで WAN ISL 暗号化と圧縮をサポートしています。
  - Brocade G720
  - Brocade G630
  - Brocade G620
  - Brocade 6520
- Brocade Virtual Fabric (VF) 機能はサポートされていません。
- ドメインポートに基づく FC ゾーニングはサポートされていますが、ワールドワイド名 (WWN) に基づくゾーニングはサポートされていません。

### Brocade のライセンス要件を確認する

MetroCluster 構成内のスイッチには所定のライセンスが必要です。これらのライセンスは 4 つのスイッチすべてにインストールする必要があります。

このタスクについて

MetroCluster 構成での Brocade ライセンス要件は次のとおりです。

- 推奨される複数の ISL を使用するシステムのランキングライセンスです。
- Extended Fabric ライセンス (ISL の距離が 6km を超える場合)
- ISL の距離が 6km を超えるサイト用の Enterprise ライセンスです

Enterprise ライセンスには、Brocade Network Advisor と、追加のポートライセンスを除くすべてのライセンスが含まれます。

### ステップ

1. ライセンスがインストールされていることを確認します。

**Fabric OS 8.2.x以前の場合**

コマンドを実行します `licenseshow`。

**Fabric OS 9.0以降の場合**

コマンドを実行します `license --show`。

これらのライセンスをお持ちでない場合は、作業を進める前に営業担当者までお問い合わせください。

**Brocade FCスイッチの値を工場出荷時のデフォルトに設定する**

設定を適切に行うには、スイッチを工場出荷時のデフォルトに設定する必要があります。また、各スイッチに一意的な名前を割り当てる必要があります。

このタスクについて

この手順の例では、ファブリックは BrocadeSwitchA と BrocadeSwitchB で構成されています。

手順

1. コンソールに接続し、1つのファブリック内の両方のスイッチにログインします。
2. スイッチを永続的に無効にします。

```
'witchcfgpersistentdisable
```

これにより、リブート後や高速ブート後もスイッチが無効なままになります。このコマンドが使用できない場合は、「witchDisable」コマンドを使用します。

次の例は、BrocadeSwitchA に対するコマンドを示しています。

```
BrocadeSwitchA:admin> switchcfgpersistentdisable
```

次の例は、BrocadeSwitchB に対するコマンドを示しています。

```
BrocadeSwitchB:admin> switchcfgpersistentdisable
```

3. スイッチ名を設定します。

```
'witchname switch_name
```

スイッチの名前はそれぞれ一意である必要があります。名前を設定すると、プロンプトがそれに応じて変わります。

次の例は、BrocadeSwitchA に対するコマンドを示しています。

```
BrocadeSwitchA:admin> switchname "FC_switch_A_1"  
FC_switch_A_1:admin>
```

次の例は、BrocadeSwitchB に対するコマンドを示しています。

```
BrocadeSwitchB:admin> switchname "FC_Switch_B_1"  
FC_switch_B_1:admin>
```

4. すべてのポートをデフォルト値に設定します。

portcfgdefault

スイッチ上のすべてのポートに対して実行する必要があります。

次の例は、FC\_switch\_A\_1 に対するコマンドを示しています。

```
FC_switch_A_1:admin> portcfgdefault 0  
FC_switch_A_1:admin> portcfgdefault 1  
...  
FC_switch_A_1:admin> portcfgdefault 39
```

次の例は、FC\_switch\_B\_1 に対するコマンドを示しています。

```
FC_switch_B_1:admin> portcfgdefault 0  
FC_switch_B_1:admin> portcfgdefault 1  
...  
FC_switch_B_1:admin> portcfgdefault 39
```

5. ゾーニング情報を消去します。

cfgdisable

cfgclear

cfgsave

次の例は、FC\_switch\_A\_1 に対するコマンドを示しています。

```
FC_switch_A_1:admin> cfgdisable  
FC_switch_A_1:admin> cfgclear  
FC_switch_A_1:admin> cfgsave
```

次の例は、FC\_switch\_B\_1 に対するコマンドを示しています。

```
FC_switch_B_1:admin> cfgdisable  
FC_switch_B_1:admin> cfgclear  
FC_switch_B_1:admin> cfgsave
```

6. スイッチの一般的な設定をデフォルトに設定します。

「configdefault」

次の例は、FC\_switch\_A\_1 に対するコマンドを示しています。

```
FC_switch_A_1:admin> configdefault
```

次の例は、FC\_switch\_B\_1 に対するコマンドを示しています。

```
FC_switch_B_1:admin> configdefault
```

7. すべてのポートを非ランキングモードに設定します。

'switchcfgtrunk 0'

次の例は、FC\_switch\_A\_1 に対するコマンドを示しています。

```
FC_switch_A_1:admin> switchcfgtrunk 0
```

次の例は、FC\_switch\_B\_1 に対するコマンドを示しています。

```
FC_switch_B_1:admin> switchcfgtrunk 0
```

8. Brocade 6510 スイッチで、Brocade Virtual Fabric (VF) 機能を無効にします。

「fosconfig options」を参照してください

次の例は、FC\_switch\_A\_1 に対するコマンドを示しています。

```
FC_switch_A_1:admin> fosconfig --disable vf
```

次の例は、FC\_switch\_B\_1 に対するコマンドを示しています。

```
FC_switch_B_1:admin> fosconfig --disable vf
```

9. Administrative Domain (AD) 設定をクリアします。

次の例は、FC\_switch\_A\_1 に対するコマンドを示しています。

```
FC_switch_A_1:> defzone --noaccess
FC_switch_A_1:> cfgsave
FC_switch_A_1:> exit
```

次の例は、FC\_switch\_B\_1 に対するコマンドを示しています。

```
FC_switch_A_1:> defzone --noaccess
FC_switch_A_1:> cfgsave
FC_switch_A_1:> exit
```

10. スイッチをリブートします。

「再起動」

次の例は、FC\_switch\_A\_1 に対するコマンドを示しています。

```
FC_switch_A_1:admin> reboot
```

次の例は、FC\_switch\_B\_1 に対するコマンドを示しています。

```
FC_switch_B_1:admin> reboot
```

基本的なスイッチ設定を構成する

Brocade スイッチに対して、ドメイン ID を含む基本的なグローバル設定を行う必要があります。

このタスクについて

このタスクには、両方の MetroCluster サイトの各スイッチで実行する必要がある手順が含まれています。

この手順では、次の例に示すように、スイッチごとに一意のドメイン ID を設定します。この例では、ドメイン ID 5 と 7 が fabric\_1 を形成し、ドメイン ID 6 と 8 が fabric\_2 を形成します。

- FC\_switch\_A\_1 をドメイン ID 5 に割り当てます
- FC\_switch\_A\_2 はドメイン ID 6 に割り当てられています
- FC\_switch\_B\_1 をドメイン ID 7 に割り当てます
- FC\_switch\_B\_2 をドメイン ID 8 に割り当て

手順

1. コンフィギュレーションモードを開始します。

「configure」を実行します

2. プロンプトに従って次の手順に進みます。
  - a. スイッチのドメイン ID を設定します。
  - b. 「RDP Polling Cycle」というプロンプトが表示されるまで \*Enter を押し、その値を「0」に設定してポーリングを無効にします。
  - c. スイッチのプロンプトに戻るまで \* Enter キーを押します。

```
FC_switch_A_1:admin> configure
Fabric parameters = y
Domain_id = 5
.
.

RSCN Transmission Mode [yes, y, no, no: [no] y

End-device RSCN Transmission Mode
(0 = RSCN with single PID, 1 = RSCN with multiple PIDs, 2 = Fabric
RSCN): (0..2) [1]
Domain RSCN To End-device for switch IP address or name change
(0 = disabled, 1 = enabled): (0..1) [0] 1
.
.
RDP Polling Cycle(hours) [0 = Disable Polling]: (0..24) [1] 0
```

3. ファブリックごとに2つ以上の ISL を使用している場合は、フレームの配信順序として In-Order Delivery (IOD ; インオーダー配信) または Out-of-Order Delivery (OOD ; アウトオブオーダー配信) のいずれかを設定できます。



標準の IOD 設定を推奨します。OOD を設定するのは必要な場合だけにしてください。

#### "ファブリック接続 MetroCluster 構成で TDM / WDM 機器を使用する場合の考慮事項"

- a. フレームの IOD を設定するには、各スイッチファブリックで次の手順を実行する必要があります。
  - i. IOD を有効にします。  
「iodset」
  - ii. Advanced Performance Tuning (APT ; 高度なパフォーマンスチューニング) ポリシーを 1 に設定します。  
「aptpolicy 1」
  - iii. 動的負荷共有 (DLS) を無効にします。  
「lsreset」と表示されます

iv. `iodshow`、`aptpolicy`、および`dlsshow`の各コマンドを使用してIOD設定を検証します。

たとえば、`FC_switch_A_1`で次のコマンドを問題に実行します。

```
FC_switch_A_1:admin> iodshow
IOD is set

FC_switch_A_1:admin> aptpolicy
Current Policy: 1 0(ap)

3 0(ap) : Default Policy
1: Port Based Routing Policy
3: Exchange Based Routing Policy
    0: AP Shared Link Policy
    1: AP Dedicated Link Policy
command aptpolicy completed

FC_switch_A_1:admin> dlsshow
DLS is not set
```

i. 2つ目のスイッチファブリックで、上記の手順を繰り返します。

b. フレームのOODを設定するには、各スイッチファブリックで次の手順を実行する必要があります。

i. OODを有効にします。

「`iodreset`」

ii. Advanced Performance Tuning (APT ; 高度なパフォーマンスチューニング) ポリシーを3に設定します。

「`aptpolicy 3`」

iii. 動的負荷共有 (DLS) を無効にします。

「`lsreset`」と表示されます

iv. OOD設定を確認します。

「`iodshow`」

「`aptpolicy`」と入力します

「`llsshow`」

たとえば、`FC_switch_A_1`で次のコマンドを問題に実行します。

```

FC_switch_A_1:admin> iodshow
IOD is not set

FC_switch_A_1:admin> aptpolicy
Current Policy: 3 0(ap)
3 0(ap) : Default Policy
1: Port Based Routing Policy
3: Exchange Based Routing Policy
0: AP Shared Link Policy
1: AP Dedicated Link Policy
command aptpolicy completed

FC_switch_A_1:admin> dlsshow
DLS is set by default with current routing policy

```

i. 2つ目のスイッチファブリックで、上記の手順を繰り返します。



コントローラモジュールに ONTAP を設定する場合は、MetroCluster 構成の各コントローラモジュールで OOD を明示的に設定する必要があります。

"ONTAPソフトウェアでフレームの順序どおりの配信または順序どおりでない配信を設定する"

4. FOS 9.0 より前のバージョンを実行している場合は、スイッチが動的ポートオンデマンド (POD) ライセンス方式を使用していることを確認します。



Fabric OS 9.0以降では、ライセンス方式はデフォルトで動的です。静的ライセンス方式はサポートされていません。

a. ライセンスコマンドを実行します。

```
licenseport --show
```

```

FC_switch_A_1:admin> license --show -port
24 ports are available in this switch
Full POD license is installed
Dynamic POD method is in use

```



バージョン 8.0 より前の Brocade FabricOS では、次のコマンドを admin として実行し、バージョン 8.0 以降では root として実行します。

b. root ユーザを有効にします。

Brocade によって root ユーザがすでに無効にされている場合は、次の例に示すように root ユーザを有効にします。

```
FC_switch_A_1:admin> userconfig --change root -e yes
FC_switch_A_1:admin> rootaccess --set consoleonly
```

- c. ライセンスコマンドを実行します。

```
license --show -port
```

```
FC_switch_A_1:root> license --show -port
24 ports are available in this switch
Full POD license is installed
Dynamic POD method is in use
```

- d. Fabric OS 8.2.x以前を実行している場合は、ライセンス方式をdynamicに変更する必要があります。

licenseport — メソッドの動的

```
FC_switch_A_1:admin> licenseport --method dynamic
The POD method has been changed to dynamic.
Please reboot the switch now for this change to take effect
```

5. ONTAP でスイッチの健全性を監視できるように、T11-FC-ZONE-SERVER-MIB のトラップを有効にします。

- a. T11-FC-ZONE-SERVER-MIB を有効にします。

```
'mpconfig — set mibCapability-mib_name T11-FC-ZONE-SERVER-MIB-Bitz-0x3f
```

- b. T11-FC-ZONE-SERVER-MIB トラップを有効にします。

```
「 mpconfig 」 — mibcapability を有効にする - mib_name sw-mib-trap_name
swZoneConfigChangeTrap 」
```

- c. 2つ目のスイッチファブリックで、ここまでの手順を繰り返します。

6. \* オプション \* : コミュニティストリングを「 public 」以外の値に設定した場合は、指定したコミュニティストリングを使用して ONTAP ヘルスマニタを設定する必要があります。

- a. 既存のコミュニティストリングを変更します。

```
'mpconfig — set snmpv1'
```

- b. 「 Community (ro): [public] 」というテキストが表示されるまで \* Enter キーを押します。

- c. 目的のコミュニティストリングを入力します。

FC\_switch\_A\_1 では、次のコマンドを実行します。

```

FC_switch_A_1:admin> snmpconfig --set snmpv1
SNMP community and trap recipient configuration:
Community (rw): [Secret C0de]
Trap Recipient's IP address : [0.0.0.0]
Community (rw): [OrigEquipMfr]
Trap Recipient's IP address : [0.0.0.0]
Community (rw): [private]
Trap Recipient's IP address : [0.0.0.0]
Community (ro): [public] mcchm      <<<<<< change the community string
to the desired value,
Trap Recipient's IP address : [0.0.0.0]      in this example it is set
to "mcchm"
Community (ro): [common]
Trap Recipient's IP address : [0.0.0.0]
Community (ro): [FibreChannel]
Trap Recipient's IP address : [0.0.0.0]
Committing configuration.....done.
FC_switch_A_1:admin>

```

FC\_switch\_B\_1では、次のコマンドを実行します。

```

FC_switch_B_1:admin> snmpconfig --set snmpv1
SNMP community and trap recipient configuration:
Community (rw): [Secret C0de]
Trap Recipient's IP address : [0.0.0.0]
Community (rw): [OrigEquipMfr]
Trap Recipient's IP address : [0.0.0.0]
Community (rw): [private]
Trap Recipient's IP address : [0.0.0.0]
Community (ro): [public] mcchm      <<<<<< change the community string
to the desired value,
Trap Recipient's IP address : [0.0.0.0]      in this example it is set to
"mcchm"
Community (ro): [common]
Trap Recipient's IP address : [0.0.0.0]
Community (ro): [FibreChannel]
Trap Recipient's IP address : [0.0.0.0]
Committing configuration.....done.
FC_switch_B_1:admin>

```

7. スイッチをリブートします。

「再起動」

FC\_switch\_A\_1 では、次のコマンドを実行します。

```
FC_switch_A_1:admin> reboot
```

FC\_switch\_B\_1 では、次のコマンドを実行します。

```
FC_switch_B_1:admin> reboot
```

8. スイッチを永続的に有効にします。

```
'witchcfgpersistentenable
```

FC\_switch\_A\_1 では、次のコマンドを実行します。

```
FC_switch_A_1:admin> switchcfgpersistentenable
```

FC\_switch\_B\_1 では、次のコマンドを実行します。

```
FC_switch_B_1:admin> switchcfgpersistentenable
```

#### Brocade DCX 8510-8 スイッチの基本的なスイッチ設定を構成する

Brocade スイッチに対して、ドメイン ID を含む基本的なグローバル設定を行う必要があります。

このタスクについて

この手順は、両方の MetroCluster サイトの各スイッチで実行する必要があります。この手順では、次の例に示すように、各スイッチのドメイン ID を設定します。

- FC\_switch\_A\_1 をドメイン ID 5 に割り当てます
- FC\_switch\_A\_2 はドメイン ID 6 に割り当てられています
- FC\_switch\_B\_1 をドメイン ID 7 に割り当てます
- FC\_switch\_B\_2 をドメイン ID 8 に割り当て

この例では、ドメイン ID 5 と 7 が fabric\_1 を形成し、ドメイン ID 6 と 8 が fabric\_2 を形成します。



各サイトで DCX 8510-8 スイッチを 1 つだけ使用する場合も、この手順を使用してスイッチを設定できます。

この手順を使用して、各 Brocade DCX 8510-8 スイッチに 2 つの論理スイッチを作成する必要があります。両方の Brocade DCX8510-8 スイッチに作成された 2 つの論理スイッチは、次の例に示すように 2 つの論理ファブリックを形成します。

- 論理ファブリック 1 : スイッチ 1 のブレード 1 とスイッチ 2 のブレード 1

- 論理ファブリック 2 : スイッチ 2 のブレード 2 とスイッチ 2 のブレード 2

#### 手順

1. コマンドモードを開始します。

「configure」を実行します

2. プロンプトに従って次の手順に進みます。
  - a. スイッチのドメイン ID を設定します。
  - b. 「RDP Polling Cycle」というプロンプトが表示されるまで \*Enter を押し続け、値を「0」に設定してポーリングを無効にします。
  - c. スイッチのプロンプトに戻るまで \*Enter を押します。

```
FC_switch_A_1:admin> configure
Fabric parameters = y
Domain_id = `5

RDP Polling Cycle(hours) [0 = Disable Polling]: (0..24) [1] 0
`
```

3. fabric\_1 と fabric\_2 のすべてのスイッチについて、同じ手順を繰り返します。
4. 仮想ファブリックを設定します。

- a. スイッチで仮想ファブリックを有効にします。

fosconfig — 有効な evf

- b. すべての論理スイッチで同じ基本設定を使用するようにシステムを設定します。

「シャーシの設定」を参照してください

次に 'configurechassis コマンドの出力例を示します

```
System (yes, y, no, n): [no] n
cfgload attributes (yes, y, no, n): [no] n
Custom attributes (yes, y, no, n): [no] y
Config Index (0 to ignore): (0..1000) [3]:
```

5. 論理スイッチを作成して設定します。

'cfg — fabricID' を作成します

6. ブレードのすべてのポートを仮想ファブリックに追加します。

lscfg --config fabricID-slot スロットポート lowest-port-highest-port



論理ファブリックを形成するブレード（例 スイッチ 1 のブレード 1 とスイッチ 3 のブレード 1）のファブリック ID が同じである必要があります。

```
setcontext fabricid
switchdisable
configure
<configure the switch per the above settings>
switchname unique switch name
switchenable
```

## 関連情報

### "Brocade DCX 8510-8 スイッチを使用するための要件"

#### FCポートを使用してBrocade FCスイッチのEポートを構成する

FCポートを使用してスイッチ間リンク（ISL）が設定された Brocade スイッチの場合、ISL を接続する各スイッチファブリックのスイッチポートを設定する必要があります。これらの ISL ポートは E ポートとも呼ばれます。

#### 作業を開始する前に

- FC スイッチファブリック内のすべての ISL を、同じ速度、同じ距離で設定する必要があります。
- この速度をサポートするスイッチポートと Small Form-factor Pluggable（SFP）の組み合わせを使用する必要があります。
- サポートされる ISL の距離は FC スイッチのモデルによって異なります。

### "NetApp Interoperability Matrix Tool で確認できます"

IMT では、Storage 解決策フィールドを使用して MetroCluster 解決策を選択できます。検索を絞り込むには、\* 構成部品エクスペローラ \* を使用して構成部品と ONTAP バージョンを選択します。[ 結果の表示（ Show Results ） ] をクリックすると、条件に一致するサポートされている構成のリストを表示できます。

- ISL リンクには専用のラムダが必要であり、Brocade によって距離、スイッチタイプ、および Fabric Operating System（FOS）がサポートされている必要があります。

#### このタスクについて

portCfgLongDistance コマンドを実行する際、L0 設定は使用しないでください。代わりに LE または LS 設定を使用し、Brocade スイッチで LE の距離レベルを最小値とする距離を設定します。

xWDM/TDM 機器で作業をする場合は 'portCfgLongDistance コマンドを実行する際に LD 設定は使用しないでください代わりに LE または LS 設定を使用し、Brocade スイッチで距離を設定します。

このタスクは FC スイッチファブリックごとに行う必要があります。

以下の表は、ONTAP 9.1 または 9.2 を実行している構成の各種スイッチと ISL 数に対応する ISL ポートを示しています。このセクションでは、Brocade 6505 スイッチの例を示しています。スイッチタイプに応じて、該当するポートを使用するように変更してください。

構成に応じて必要な数の ISL を使用する必要があります。

スイッチモデル	ISL ポート	スイッチポート
Brocade 6520	ISL、ポート 1	23
	ISL、ポート 2	47
	ISL、ポート 3	71
	ISL、ポート 4	95
Brocade 6505	ISL、ポート 1	20
	ISL、ポート 2	21
	ISL、ポート 3	22
	ISL、ポート 4	23
Brocade 6510 および Brocade DCX 8510-8	ISL、ポート 1	40
	ISL、ポート 2	41
	ISL、ポート 3	42
	ISL、ポート 4	43
	ISL、ポート 5	44
	ISL、ポート 6	45
	ISL、ポート 7	46
	ISL、ポート 8	47
Brocade 7810	ISL、ポート 1	GE2 ( 10Gbps )
	ISL、ポート 2	GE3 ( 10Gbps )
	ISL、ポート 3	GE4 ( 10Gbps )
	ISL、ポート 4	GE5 ( 10Gbps )
	ISL、ポート 5	ge6 ( 10Gbps )
	ISL、ポート 6	ge7 ( 10Gbps )

Brocade 7840 *注： Brocade 7840 スイッチでは、 FCIP ISL を作成するために、スイッチあたり 2 つの 40Gbps VE ポートまたは最大 4 つの 10Gbps VE ポートがサポートされます。	ISL、ポート 1	ge0 ( 40Gbps ) または ge2 ( 10Gbps )
	ISL、ポート 2	GE1 ( 40Gbps ) または ge3 ( 10Gbps )
	ISL、ポート 3	ge10 ( 10Gbps )
	ISL、ポート 4	ge11 ( 10Gbps )
BrocadeG610、G710	ISL、ポート 1	20
	ISL、ポート 2	21
	ISL、ポート 3	22
	ISL、ポート 4	23
Brocade G620、G620 -1、G630、G630-1、G720	ISL、ポート 1	40
	ISL、ポート 2	41.
	ISL、ポート 3	42
	ISL、ポート 4	43
	ISL、ポート 5	44
	ISL、ポート 6	45
	ISL、ポート 7	46

## 手順

1. ポート速度を設定します。

```
portcfgspeed port-number speed
```

パス内のすべてのコンポーネントでサポートされている最高速度を使用する必要があります。

次の例では、各ファブリックに ISL が 2 つあります。

```
FC_switch_A_1:admin> portcfgspeed 20 16
FC_switch_A_1:admin> portcfgspeed 21 16

FC_switch_B_1:admin> portcfgspeed 20 16
FC_switch_B_1:admin> portcfgspeed 21 16
```

## 2. ISL ごとにトランキングモードを設定します。

`portcfgtrunkport port-number`

- ISL でトランキングを設定する場合（IOD の場合）は、`portcfgtrunk port-number port-number port-number port-number` を 1 に設定します。次に例を示します。

```
FC_switch_A_1:admin> portcfgtrunkport 20 1
FC_switch_A_1:admin> portcfgtrunkport 21 1
FC_switch_B_1:admin> portcfgtrunkport 20 1
FC_switch_B_1:admin> portcfgtrunkport 21 1
```

- ISL でトランキングを設定しない場合（OOD の場合）は、`portcfgtrunkport-number` を 0 に設定します。次に例を示します。

```
FC_switch_A_1:admin> portcfgtrunkport 20 0
FC_switch_A_1:admin> portcfgtrunkport 21 0
FC_switch_B_1:admin> portcfgtrunkport 20 0
FC_switch_B_1:admin> portcfgtrunkport 21 0
```

## 3. ISL ポートごとに QoS トラフィックを有効にします。

`portcfgqos --enable port-number`

次の例では、各スイッチファブリックに ISL が 2 つあります。

```
FC_switch_A_1:admin> portcfgqos --enable 20
FC_switch_A_1:admin> portcfgqos --enable 21

FC_switch_B_1:admin> portcfgqos --enable 20
FC_switch_B_1:admin> portcfgqos --enable 21
```

## 4. 設定を確認します。

`portCfgShow` コマンド

次の例は、2 つの ISL がポート 20 とポート 21 にケーブル接続されている構成の出力を示しています。Trunk Port の設定は、IOD の場合は ON、OOD の場合は OFF になります。

Ports of Slot 0	12	13	14	15	16	17	18	19	20	21	22	23	24
25 26 27													
Speed	AN	AN	AN	AN	AN	AN	8G	AN	AN	AN	16G	16G	
AN AN AN AN													
Fill Word	0	0	0	0	0	0	3	0	0	0	3	3	3
0 0 0													
AL_PA Offset 13	..	..	..	..	..	..	..	..	..	..	..	..	..
.. .. .. ..													
Trunk Port	..	..	..	..	..	..	..	..	ON	ON	..	..	
.. .. .. ..													
Long Distance	..	..	..	..	..	..	..	..	..	..	..	..	
.. .. .. ..													
VC Link Init	..	..	..	..	..	..	..	..	..	..	..	..	
.. .. .. ..													
Locked L_Port	..	..	..	..	..	..	..	..	..	..	..	..	
.. .. .. ..													
Locked G_Port	..	..	..	..	..	..	..	..	..	..	..	..	
.. .. .. ..													
Disabled E_Port	..	..	..	..	..	..	..	..	..	..	..	..	
.. .. .. ..													
Locked E_Port	..	..	..	..	..	..	..	..	..	..	..	..	
.. .. .. ..													
ISL R_RDY Mode	..	..	..	..	..	..	..	..	..	..	..	..	
.. .. .. ..													
RSCN Suppressed	..	..	..	..	..	..	..	..	..	..	..	..	
.. .. .. ..													
Persistent Disable	..	..	..	..	..	..	..	..	..	..	..	..	
.. .. .. ..													
LOS TOV enable	..	..	..	..	..	..	..	..	..	..	..	..	
.. .. .. ..													
NPIV capability	ON												
ON ON ON ON													
NPIV PP Limit	126	126	126	126	126	126	126	126	126	126	126	126	
126 126 126 126													
QOS E_Port	AE												
AE AE AE AE													
Mirror Port	..	..	..	..	..	..	..	..	..	..	..	..	
.. .. .. ..													
Rate Limit	..	..	..	..	..	..	..	..	..	..	..	..	
.. .. .. ..													
Credit Recovery	ON												
ON ON ON ON													
Fport Buffers	..	..	..	..	..	..	..	..	..	..	..	..	

```

.. .. .. ..
Port Auto Disable .. .. .. .. .. .. .. .. .. .. .. .. .. .. .. ..
.. .. .. ..
CSCTL mode .. .. .. .. .. .. .. .. .. .. .. .. .. .. .. ..
.. .. .. ..
Fault Delay 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

```

5. ISL の距離を計算します。

FC-VI の動作により、この距離は、10km（LE の距離レベルを使用）を最小値として、実際の距離の 1.5 倍に設定する必要があります。

ISL の距離は次のように計算され、km 単位に切り上げられます。

実際の距離 × 1.5

距離が 3km の場合は、 $3\text{km} \times 1.5 = 4.5\text{km}$  となりますこの場合、10km より短いため、ISL は LE の距離レベルに設定する必要があります。

距離が 20km の場合は、 $1.5 \times 20\text{ km} = 30\text{ km}$  となります ISL は 30km に設定し、LS の距離レベルを使用する必要があります。

6. ISL ポートごとに距離を設定します。

```
`longdistance_portdistance-level_vc_link_init_ddistance
```

'vc\_link\_init' の値が '1' の場合は 'ARB フィルワード (デフォルト) が使用されます値「0」は IDLE を使用します。必要な値は、使用されているリンクによって異なる場合があります。コマンドは ISL ポートごとに繰り返し実行する必要があります。

前の手順の例で ISL の距離が 3km であるとする、設定は 4.5km で、デフォルトの「vc\_link\_init」の値は「1」です。設定が 4.5km で 10km より短いため、ポートを LE の距離レベルに設定する必要があります。

```

FC_switch_A_1:admin> portcfglongdistance 20 LE 1
FC_switch_B_1:admin> portcfglongdistance 20 LE 1

```

前の手順の例で ISL の距離が 20km であるとする、設定は 30km で、vc\_link\_init はデフォルト値の「1」です。

```

FC_switch_A_1:admin> portcfglongdistance 20 LS 1 -distance 30
FC_switch_B_1:admin> portcfglongdistance 20 LS 1 -distance 30

```

7. 距離設定を確認します。

portbuffershow

LE の距離レベルは 10 km と表示されます

次の例は、ポート 20 とポート 21 上の ISL を使用する構成の出力です。

```
FC_switch_A_1:admin> portbuffershow
```

User Port	Port Type	Lx Mode	Max/Resv Buffers	Buffer Usage	Needed Buffers	Link Distance	Remaining Buffers
...							
20	E	-	8	67	67	30km	
21	E	-	8	67	67	30km	
...							
23		-	8	0	-	-	466

8. 両方のスイッチが 1 つのファブリックを形成することを確認します。

'witchshow'

次の例は、ポート 20 とポート 21 上の ISL を使用する構成の出力です。

```

FC_switch_A_1:admin> switchshow
switchName: FC_switch_A_1
switchType: 109.1
switchState:Online
switchMode: Native
switchRole: Subordinate
switchDomain:      5
switchId:   fffc01
switchWwn:  10:00:00:05:33:86:89:cb
zoning:     OFF
switchBeacon: OFF

Index Port Address Media Speed State Proto
=====
...
20  20  010C00  id    16G  Online FC  LE E-Port
10:00:00:05:33:8c:2e:9a "FC_switch_B_1" (downstream) (trunk master)
21  21  010D00  id    16G  Online FC  LE E-Port (Trunk port, master
is Port 20)
...

FC_switch_B_1:admin> switchshow
switchName: FC_switch_B_1
switchType: 109.1
switchState:Online
switchMode: Native
switchRole: Principal
switchDomain:      7
switchId:   fffc03
switchWwn:  10:00:00:05:33:8c:2e:9a
zoning:     OFF
switchBeacon: OFF

Index Port Address Media Speed State Proto
=====
...
20  20  030C00  id    16G  Online FC  LE E-Port
10:00:00:05:33:86:89:cb "FC_switch_A_1" (downstream) (Trunk master)
21  21  030D00  id    16G  Online FC  LE E-Port (Trunk port, master
is Port 20)
...

```

9. ファブリックの設定を確認します。

「fabricshow」

```

FC_switch_A_1:admin> fabricshow
  Switch ID      Worldwide Name      Enet IP Addr FC IP Addr Name
-----
1: fffc01 10:00:00:05:33:86:89:cb 10.10.10.55  0.0.0.0
"FC_switch_A_1"
3: fffc03 10:00:00:05:33:8c:2e:9a 10.10.10.65  0.0.0.0
>"FC_switch_B_1"

```

```

FC_switch_B_1:admin> fabricshow
  Switch ID      Worldwide Name      Enet IP Addr FC IP Addr      Name
-----
1: fffc01 10:00:00:05:33:86:89:cb 10.10.10.55  0.0.0.0
"FC_switch_A_1"

3: fffc03 10:00:00:05:33:8c:2e:9a 10.10.10.65  0.0.0.0
>"FC_switch_B_1"

```

10. [step10\_brocade\_config] ISL のトランキングを確認します。

「trunkshow」

◦ ISL でトランキングを設定する場合（IOD の場合）は、次のような出力が表示されます。

```

FC_switch_A_1:admin> trunkshow
  1: 20-> 20 10:00:00:05:33:ac:2b:13 3 deskew 15 MASTER
    21-> 21 10:00:00:05:33:8c:2e:9a 3 deskew 16
FC_switch_B_1:admin> trunkshow
  1: 20-> 20 10:00:00:05:33:86:89:cb 3 deskew 15 MASTER
    21-> 21 10:00:00:05:33:86:89:cb 3 deskew 16

```

◦ ISL でトランキングを設定しない場合（OOD の場合）は、次のような出力が表示されます。

```

FC_switch_A_1:admin> trunkshow
  1: 20-> 20 10:00:00:05:33:ac:2b:13 3 deskew 15 MASTER
  2: 21-> 21 10:00:00:05:33:8c:2e:9a 3 deskew 16 MASTER
FC_switch_B_1:admin> trunkshow
  1: 20-> 20 10:00:00:05:33:86:89:cb 3 deskew 15 MASTER
  2: 21-> 21 10:00:00:05:33:86:89:cb 3 deskew 16 MASTER

```

11. 繰り返します 手順 1. から 手順 10 2 つ目の FC スイッチファブリック。

関連情報

## "FCスイッチのポート割り当て"

### Brocade FC 7840 スイッチでの 10Gbps VE ポートの設定

ISL に 10Gbps VE ポート（FCIP を使用）を使用する場合は、各ポートに IP インターフェイスを作成し、FCIP トンネルと各トンネルの回線を設定する必要があります。

このタスクについて

この手順は、MetroCluster 構成の各スイッチファブリックで実行する必要があります。

この手順の例では、2 つの Brocade 7840 スイッチの IP アドレスを次のように想定しています。

- ローカルが FC\_switch\_A\_1。
- リモートが FC\_switch\_B\_1。

### 手順

1. ファブリック内の両方のスイッチに 10Gbps ポートの IP インターフェイス（ipif）アドレスを作成します。

```
'portcfg ipif FC_switch1_namefirst_port_name create FC_switch1_ip_address netmask netmask_number  
vlan 2 mtu auto
```

次のコマンドは、FC\_switch\_A\_1 のポート GE2.dp0 および ge3.dp0 に ipif アドレスを作成します。

```
portcfg ipif ge2.dp0 create 10.10.20.71 netmask 255.255.0.0 vlan 2 mtu  
auto  
portcfg ipif ge3.dp0 create 10.10.21.71 netmask 255.255.0.0 vlan 2 mtu  
auto
```

次のコマンドは、FC\_switch\_B\_1 のポート GE2.dp0 および ge3.dp0 に ipif アドレスを作成します。

```
portcfg ipif ge2.dp0 create 10.10.20.72 netmask 255.255.0.0 vlan 2 mtu  
auto  
portcfg ipif ge3.dp0 create 10.10.21.72 netmask 255.255.0.0 vlan 2 mtu  
auto
```

2. 両方のスイッチに ipif アドレスが作成されたことを確認します。

```
"portShow ipif all"
```

次のコマンドは、スイッチ FC\_switch\_A\_1 の ipif アドレスを表示します。

```
FC_switch_A_1:root> portshow ipif all
```

Port	IP Address	/ Pfx	MTU	VLAN	Flags
ge2.dp0	10.10.20.71	/ 24	AUTO	2	U R M I
ge3.dp0	10.10.21.71	/ 20	AUTO	2	U R M I

Flags: U=Up B=Broadcast D=Debug L=Loopback P=Point2Point R=Running  
I=InUse  
N=NoArp PR=Promisc M=Multicast S=StaticArp LU=LinkUp X=Crossport

次のコマンドは、スイッチ FC\_switch\_B\_1 の ipif アドレスを表示します。

```
FC_switch_B_1:root> portshow ipif all
```

Port	IP Address	/ Pfx	MTU	VLAN	Flags
ge2.dp0	10.10.20.72	/ 24	AUTO	2	U R M I
ge3.dp0	10.10.21.72	/ 20	AUTO	2	U R M I

Flags: U=Up B=Broadcast D=Debug L=Loopback P=Point2Point R=Running  
I=InUse  
N=NoArp PR=Promisc M=Multicast S=StaticArp LU=LinkUp X=Crossport

3. dp0 のポートを使用して、2つの FCIP トンネルのうちの1つ目のトンネルを作成します。

```
"portcfg fciptunnel
```

このコマンドは、単一回線のトンネルを作成します。

次のコマンドは、スイッチ FC\_switch\_A\_1 にトンネルを作成します。

```
portcfg fciptunnel 24 create -S 10.10.20.71 -D 10.10.20.72 -b 10000000  
-B 10000000
```

次のコマンドは、スイッチ FC\_switch\_B\_1 にトンネルを作成します。

```
portcfg fciptunnel 24 create -S 10.10.20.72 -D 10.10.20.71 -b 10000000  
-B 10000000
```

4. FCIP トンネルが作成されたことを確認します。

```
'portShow fciptunnel all
```

次の例は、トンネルが作成され、回線が稼働していることを示しています。

```
FC_switch_B_1:root>

  Tunnel Circuit  OpStatus  Flags      Uptime  TxMBps  RxMBps  ConnCnt
CommRt Met/G
-----
-----
  24    -          Up        -----   2d8m    0.05    0.41    3        -
-----
-----
  Flags (tunnel): i=IPSec f=Fastwrite T=TapePipelining F=FICON
r=ReservedBW
                  a=FastDeflate d=Deflate D=AggrDeflate P=Protocol
                  I=IP-Ext
```

5. DP0 の追加の回線を作成します。

次のコマンドは、スイッチ FC\_switch\_A\_1 に dp0 の回線を作成します。

```
portcfg fcipcircuit 24 create 1 -S 10.10.21.71 -D 10.10.21.72 --min
-comm-rate 5000000 --max-comm-rate 5000000
```

次のコマンドは、スイッチ FC\_switch\_A\_1 に dp0 の回線を作成します。

```
portcfg fcipcircuit 24 create 1 -S 10.10.21.72 -D 10.10.21.71 --min
-comm-rate 5000000 --max-comm-rate 5000000
```

6. すべての回線が正常に作成されたことを確認します。

```
'portShow fcipcircuit all
```

次のコマンドは、回線とそのステータスを表示します。

```

FC_switch_A_1:root> portshow fcipcircuit all

  Tunnel Circuit  OpStatus  Flags      Uptime  TxMBps  RxMBps  ConnCnt
  CommRt Met/G
-----
-----
  24    0 ge2      Up        ---va---4  2d12m   0.02    0.03    3
10000/10000 0/-
  24    1 ge3      Up        ---va---4  2d12m   0.02    0.04    3
10000/10000 0/-
-----
-----
  Flags (circuit): h=HA-Configured v=VLAN-Tagged p=PMTU i=IPSec 4=IPv4
6=IPv6
                        ARL a=Auto r=Reset s=StepDown t=TimedStepDown S=SLA

```

#### Brocade 7810および7840 FCスイッチで40 GbpsのVEポートを構成する

ISLに2つの40GbE VEポート（FCIPを使用）を使用する場合は、各ポートにIPインターフェイスを作成し、FCIPトンネルと各トンネルの回線を設定する必要があります。

このタスクについて

この手順は、MetroCluster構成の各スイッチファブリックで実行する必要があります。

この手順の例では、次の2つのスイッチを使用します。

- ローカルが FC\_switch\_A\_1。
- リモートが FC\_switch\_B\_1。

#### 手順

1. ファブリック内の両方のスイッチに40GbpsポートのIPインターフェイス（ipif）アドレスを作成します。

```
'portcfg ipif FC_switch_nameefirst_port_name create FC_switch_ip_address netmask netmask_number
VLAN 2 mtu auto'
```

次のコマンドは、FC\_switch\_A\_1のポート ge0.dp0 および ge1.dp0 に ipif アドレスを作成します。

```
portcfg ipif ge0.dp0 create 10.10.82.10 netmask 255.255.0.0 vlan 2 mtu
auto
portcfg ipif ge1.dp0 create 10.10.82.11 netmask 255.255.0.0 vlan 2 mtu
auto
```

次のコマンドは、FC\_switch\_B\_1のポート ge0.dp0 および ge1.dp0 に ipif アドレスを作成します。

```
portcfg ipif ge0.dp0 create 10.10.83.10 netmask 255.255.0.0 vlan 2 mtu
auto
portcfg ipif ge1.dp0 create 10.10.83.11 netmask 255.255.0.0 vlan 2 mtu
auto
```

2. 両方のスイッチに ipif アドレスが作成されたことを確認します。

"portShow ipif all"

次の例は、FC\_switch\_A\_1 の IP インターフェイスを示しています。

```
Port                IP Address                / Pfx  MTU   VLAN  Flags
-----
-----
ge0.dp0             10.10.82.10                / 16   AUTO  2     U R M
ge1.dp0             10.10.82.11                / 16   AUTO  2     U R M
-----
Flags: U=Up B=Broadcast D=Debug L=Loopback P=Point2Point R=Running
I=InUse
      N=NoArp PR=Promisc M=Multicast S=StaticArp LU=LinkUp X=Crossport
```

次の例は、FC\_switch\_B\_1 の IP インターフェイスを示しています。

```
Port                IP Address                / Pfx  MTU   VLAN  Flags
-----
-----
ge0.dp0             10.10.83.10                / 16   AUTO  2     U R M
ge1.dp0             10.10.83.11                / 16   AUTO  2     U R M
-----
Flags: U=Up B=Broadcast D=Debug L=Loopback P=Point2Point R=Running
I=InUse
      N=NoArp PR=Promisc M=Multicast S=StaticArp LU=LinkUp X=Crossport
```

3. 両方のスイッチに FCIP トンネルを作成します。

「portconfig fciptunnel」のように入力します

次のコマンドは、FC\_switch\_A\_1 にトンネルを作成します。

```
portcfg fciptunnel 24 create -S 10.10.82.10 -D 10.10.83.10 -b 10000000  
-B 10000000
```

次のコマンドは、FC\_switch\_B\_1 にトンネルを作成します。

```
portcfg fciptunnel 24 create -S 10.10.83.10 -D 10.10.82.10 -b 10000000  
-B 10000000
```

#### 4. FCIP トンネルが作成されたことを確認します。

```
'portShow fciptunnel all
```

次の例は、トンネルが作成され、回線が稼働していることを示しています。

```
FC_switch_A_1:root>  
  
Tunnel Circuit OpStatus  Flags      Uptime  TxMBps  RxMBps  ConnCnt  
CommRt Met/G  
-----  
-----  
24      -          Up      -----    2d8m    0.05    0.41    3        -  
-----  
-----  
Flags (tunnel): i=IPSec f=Fastwrite T=TapePipelining F=FICON  
r=ReservedBW  
                a=FastDeflate d=Deflate D=AggrDeflate P=Protocol  
                I=IP-Ext
```

#### 5. 各スイッチに追加の回線を作成します。

```
'portcfg fcipcircuit 24 create 1-S source-ip-address -D destination-ip-address --min-comm-rate 10000000  
--max-comm-rate 10000000
```

次のコマンドは、スイッチ FC\_switch\_A\_1 に dp0 の回線を作成します。

```
portcfg fcipcircuit 24 create 1 -S 10.10.82.11 -D 10.10.83.11 --min  
-comm-rate 10000000 --max-comm-rate 10000000
```

次のコマンドは、スイッチ FC\_switch\_A\_1 に DP1 の回線を作成します。

```
portcfg fcipcircuit 24 create 1 -S 10.10.83.11 -D 10.10.82.11 --min
-comm-rate 10000000 --max-comm-rate 10000000
```

6. すべての回線が正常に作成されたことを確認します。

```
'portShow fcipcircuit all
```

次の例は、回線をリストしたもので、それぞれの OpStatus が Up であることを示しています。

```
FC_switch_A_1:root> portshow fcipcircuit all

Tunnel Circuit  OpStatus  Flags      Uptime  TxMBps  RxMBps  ConnCnt
CommRt Met/G
-----
-----
 24    0 ge0      Up        ---va---4  2d12m   0.02    0.03    3
10000/10000 0/-
 24    1 ge1      Up        ---va---4  2d12m   0.02    0.04    3
10000/10000 0/-
-----
-----
Flags (circuit): h=HA-Configured v=VLAN-Tagged p=PMTU i=IPSec 4=IPv4
6=IPv6
                    ARL a=Auto r=Reset s=StepDown t=TimedStepDown S=SLA
```

### Brocadeスイッチの非Eポートを構成する

FC スイッチ上の非 E ポートを設定する必要があります。MetroCluster 構成では、これらのポートによって、スイッチと HBA イニシエータ、FC-VI インターコネクト、および FC-to-SAS ブリッジが接続されます。この手順はポートごとに実行する必要があります。

このタスクについて

次の例では、ポートを FC-to-SAS ブリッジに接続します。

- Site\_A の FC\_FC\_switch\_A\_1 のポート 6
- Site\_B の FC\_FC\_switch\_B\_1 のポート 6

手順

1. 非 E ポートの速度を設定します。

```
portcfgspeed portSpeed
```

データパス内のすべてのコンポーネント（SFP、SFP が設置されているスイッチポート、HBA、ブリッジなどの接続デバイス）でサポートされている最高速度を使用する必要があります。

たとえば、各コンポーネントで次の速度がサポートされているとします。

- SFP は 4GB、8GB、16GB に対応
- スイッチポートは 4GB、8GB、16GB に対応
- 接続されている HBA の最高速度は 16GBこの場合の共通最高速度は 16GB であるため、ポート速度は 16GB に設定する必要があります。

```
FC_switch_A_1:admin> portcfgspeed 6 16
```

```
FC_switch_B_1:admin> portcfgspeed 6 16
```

## 2. 設定を確認します。

portcfgshow

```
FC_switch_A_1:admin> portcfgshow
```

```
FC_switch_B_1:admin> portcfgshow
```

この出力例では、ポート 6 に次の設定があり、速度は 16G に設定されています。

Ports of Slot 0	0	1	2	3	4	5	6	7	8
Speed	16G								
AL_PA Offset 13	..	..	..	..	..	..	..	..	..
Trunk Port	..	..	..	..	..	..	..	..	..
Long Distance	..	..	..	..	..	..	..	..	..
VC Link Init	..	..	..	..	..	..	..	..	..
Locked L_Port	-	-	-	-	-	-	-	-	-
Locked G_Port	..	..	..	..	..	..	..	..	..
Disabled E_Port	..	..	..	..	..	..	..	..	..
Locked E_Port	..	..	..	..	..	..	..	..	..
ISL R_RDY Mode	..	..	..	..	..	..	..	..	..
RSCN Suppressed	..	..	..	..	..	..	..	..	..
Persistent Disable	..	..	..	..	..	..	..	..	..
LOS TOV enable	..	..	..	..	..	..	..	..	..
NPIV capability	ON								
NPIV PP Limit	126	126	126	126	126	126	126	126	126
QOS Port	AE	ON							
EX Port	..	..	..	..	..	..	..	..	..
Mirror Port	..	..	..	..	..	..	..	..	..
Rate Limit	..	..	..	..	..	..	..	..	..
Credit Recovery	ON								
Fport Buffers	..	..	..	..	..	..	..	..	..
Eport Credits	..	..	..	..	..	..	..	..	..
Port Auto Disable	..	..	..	..	..	..	..	..	..
CSCTL mode	..	..	..	..	..	..	..	..	..
D-Port mode	..	..	..	..	..	..	..	..	..
D-Port over DWDM	..	..	..	..	..	..	..	..	..
FEC	ON								
Fault Delay	0	0	0	0	0	0	0	0	0
Non-DFE	..	..	..	..	..	..	..	..	..

**Brocade G620**スイッチのISLポートで圧縮を設定する

Brocade G620 スイッチを使用している場合に ISL で圧縮を有効にするには、スイッチの各 E ポートで圧縮を設定する必要があります。

このタスクについて

このタスクは、 ISL を使用する両方のスイッチの ISL ポートで実行する必要があります。

手順

1. 圧縮を設定するポートを無効にします。

```
portdisable port-id`
```

2. ポートで圧縮を有効にします。

portCfgCompress — ポート ID を有効にします

3. ポートを有効にして圧縮の設定をアクティブにします。

```
portEnable port-id`
```

4. 設定が変更されたことを確認します。

```
portcfgshow port-id`
```

次の例は、ポート 0 で圧縮を有効にします。

```
FC_switch_A_1:admin> portdisable 0
FC_switch_A_1:admin> portcfgcompress --enable 0
FC_switch_A_1:admin> portenable 0
FC_switch_A_1:admin> portcfgshow 0
Area Number: 0
Octet Speed Combo: 3(16G,10G)
(output truncated)
D-Port mode: OFF
D-Port over DWDM ..
Compression: ON
Encryption: ON
```

islShow コマンドを使用すると、暗号化または圧縮が設定され、アクティブになった状態で E\_port がオンラインになったことを確認できます。

```
FC_switch_A_1:admin> islshow
 1: 0-> 0 10:00:c4:f5:7c:8b:29:86   5 FC_switch_B_1
sp: 16.000G bw: 16.000G TRUNK QOS CR_RECOV ENCRYPTION COMPRESSION
```

portEncCompShow コマンドを使用すると、アクティブなポートを確認できます。この例では、ポート 0 で暗号化と圧縮が設定され、アクティブになっています。

```
FC_switch_A_1:admin> portenccompshow
User      Encryption      Compression      Config
Port      Configured      Active           Configured      Active  Speed
-----      -
 0         Yes             Yes             Yes             Yes    16G
```

### Brocade FCスイッチのゾーニングを構成する

スイッチポートを別々のゾーンに割り当てて、コントローラとストレージのトラフィックを分離する必要があります。

## FC-VIポートをゾーン分けする

MetroCluster の DR グループごとに、コントローラ間のトラフィックに使用する FC-VI 接続のゾーンを 2 つ 設定する必要があります。これらのゾーンには、コントローラモジュールの FC-VI ポートに接続する FC スイッチポートが含まれます。これらのゾーンは、Quality of Service ( QoS ; サービス品質) ゾーンです。

QoS ゾーンには、通常のゾーンと区別するために、プレフィックス QOSHid\_ から始まる名前を使用します。これらの QoS ゾーンは、使用する FibreBridge ブリッジのモデルに関係なく同じです。

各ゾーンには、各コントローラの FC-VI ケーブルごとに 1 つ、すべての FC-VI ポートが含まれます。これらのゾーンには高い優先度が設定されています。

次の表に、2 つの DR グループの FC-VI ゾーンを示します。

### • DR グループ 1 : FC-VI ポート a / c \* の QOSH1 FC-VI ゾーン

FC スイッチ	サイト	スイッチドメイン	6505 / 6510 ポート	6520 ポート	G620 ポート	接続先
FC_switch_A_1 を使用します	A	5.	0	0	0	controller_A_1 のポート FC-VI a
FC_switch_A_1 を使用します	A	5.	1.	1.	1.	controller_A_1 のポート FC-VI c
FC_switch_A_1 を使用します	A	5.	4.	4.	4.	controller_A_2 、 FC-VI a
FC_switch_A_1 を使用します	A	5.	5.	5.	5.	controller_A_2 、 FC-VI c ポート
FC_switch_B_1	B	7.	0	0	0	controller_B_1 、 ポート FC-VI a
FC_switch_B_1	B	7.	1.	1.	1.	controller_B_1 、 ポート FC-VI c
FC_switch_B_1	B	7.	4.	4.	4.	controller_B_2 、 ポート FC-VI a
FC_switch_B_1	B	7.	5.	5.	5.	controller_B_2 、 ポート FC-VI c

Fabric_1 のゾーン	メンバーポート
QOSH1_MC1_FAB_1_FCVI	5、 0 ; 5、 1 ; 5、 4 ; 5、 5 ; 7、 0 ; 7、 1 ; 7、 4 ; 7、 5

### • DR グループ 1 : FC-VI ポート b / d \* の QOSH1 FC-VI ゾーン

FC スイッチ	サイト	スイッチドメイン	6505 / 6510 ポート	6520 ポート	G620 ポート	接続先
FC_switch_A_2	A	6.	0	0	0	controller_A_1 のポート FC- VI b
			1.	1.	1.	controller_A_1 のポート FC- VI d
			4.	4.	4.	controller_A_2 、 FC-VI b ポ ート
			5.	5.	5.	controller_A_2 、 FC-VI d ポ ート
FC_switch_B_2	B	8.	0	0	0	controller_B_1 、 ポート FC- VI b
			1.	1.	1.	controller_B_1 、 ポート FC- VI d
			4.	4.	4.	controller_B_2 、 ポート FC- VI b
			5.	5.	5.	controller_B_2 、 ポート FC- VI d

Fabric_1 のゾーン	メンバーポート
QOSH1_MC1_FAB_2_FCVI	6、 0 ; 6、 1 ; 6、 4 ; 6、 5 ; 8、 0 ; 8、 1 ; 8、 4 ; 8、 5

• DR グループ 2 : FC-VI ポート a/c\* の QOSH2 FC-VI ゾーン

FC スイッチ	サイト	スイッチドメイン	スイッチポート			接続先
			6510	6520	G620	
FC_switch_A_1 を使用しま す	A	5.	24	48	18	controller_A_1 のポート FC- VI a
			25	49	19	controller_A_1 のポート FC- VI c
			28	52	22	controller_A_2 、 FC-VI a

FC スイッチ	サイト	スイッチドメイン	スイッチポート			接続先
			29	53	23	controller_A_1 のポート FC- VI c
FC_switch_B_1	B	7.	24	48	18	controller_B_2 、ポート FC- VI a
			25	49	19	controller_B_2 、ポート FC- VI c
			28	52	22	controller_B_2 、ポート FC- VI a
			29	53	23	controller_B_2 、ポート FC- VI c

Fabric_1 のゾーン	メンバーポート
QOSH2_MC2_FAB_1_FCVI (6510)	5、24 ; 5、25 ; 5、28 ; 5、29 ; 7、24 ; 7、25 ; 7、28 ; 7、29
QOSH2_MC2_FAB_1_FCVI (6520)	5、48 ; 5、49 ; 5、52 ; 5、53 ; 7、48 ; 7、49 ; 7、52 ; 7、53

• DR グループ 2 : FC-VI ポート b/d\* の QOSH2 FC-VI ゾーン

FC スイッチ	サイト	スイッチドメイン	6510 ポート	6520 ポート	G620 ポート	接続先
FC_switch_A_2	A	6.	24	48	18	controller_A_1 のポート FC- VI b
FC_switch_A_2	A	6.	25	49	19	controller_A_1 のポート FC- VI d
FC_switch_A_2	A	6.	28	52	22	controller_A_1 のポート FC- VI b
FC_switch_A_2	A	6.	29	53	23	controller_A_1 のポート FC- VI d
FC_switch_B_2	B	8.	24	48	18	controller_B_2 、ポート FC- VI b

FC スイッチ	サイト	スイッチドメイン	6510 ポート	6520 ポート	G620 ポート	接続先
FC_switch_B_2	B	8.	25	49	19	controller_B_2、ポート FC-VI d
FC_switch_B_2	B	8.	28	52	22	controller_B_2、ポート FC-VI b
FC_switch_B_2	B	8.	29	53	23	controller_B_2、ポート FC-VI d

Fabric_2 のゾーン	メンバーポート
QOSH2_MC2_FAB_2_FCVI (6510)	6、24、6、25、6、28、6、29、8、24、8、25、8、28、8、29
QOSH2_MC2_FAB_2_FCVI (6520)	6、48、6、49、6、52、6、53、8、48、8、49、8、52、8、53

次の表に、FC-VI ゾーンをまとめます。

ファブリック	ゾーン名	メンバーポート
FC_switch_A_1 および FC_switch_B_1	QOSH1_MC1_FAB_1_FCVI	5、0 ; 5、1 ; 5、4 ; 5、5 ; 7、0 ; 7、1 ; 7、4 ; 7、5
	QOSH2_MC1_FAB_1_FCVI (6510)	5、24 ; 5、25 ; 5、28 ; 5、29 ; 7、24 ; 7、25 ; 7、28 ; 7、29
	QOSH2_MC1_FAB_1_FCVI (6520)	5、48 ; 5、49 ; 5、52 ; 5、53 ; 7、48 ; 7、49 ; 7、52 ; 7、53
FC_switch_A_2 と FC_switch_B_2	QOSH1_MC1_FAB_2_FCVI	6、0 ; 6、1 ; 6、4 ; 6、5 ; 8、0 ; 8、1 ; 8、4 ; 8、5
	QOSH2_MC1_FAB_2_FCVI (6510)	6、24、6、25、6、28、6、29、8、24、8、25、8、28、8、29
	QOSH2_MC1_FAB_2_FCVI (6520)	6、48、6、49、6、52、6、53、8、48、8、49、8、52、8、53

## 1つのFCポートを使用してFibreBridge 7500Nまたは7600Nブリッジをゾーン化する

2つのFCポートのどちらか一方だけを使用するFibreBridge 7500N / 7600Nブリッジを使用する場合は、ブリッジポートのストレージゾーンを作成する必要があります。ゾーンを設定する前に、ゾーンおよび関連するポートについて理解しておく必要があります。

ここでは、DRグループ1のゾーニング例のみを示しています。2つ目のDRグループがある構成の場合は、コントローラとブリッジの対応するポートを使用して、同じ方法で2つ目のDRグループのゾーニングを設定します。

### 必要なゾーン

FC-to-SASブリッジのFCポートごとにゾーンを1つ設定し、各コントローラモジュールのイニシエータとそのFC-to-SASブリッジの間のトラフィックを許可する必要があります。

各ストレージゾーンに9つのポートが含まれます。

- HBA イニシエータポート × 8 (コントローラごとに2つの接続)
- FC-to-SASブリッジのFCポートに接続するポート × 1

ストレージゾーンでは標準のゾーニングを使用します。

例では、各サイトの2つのスタックグループを接続する2組のブリッジのペアを示します。各ブリッジが1つのFCポートを使用するため、ファブリックあたりのストレージゾーン数は4個(合計8個)になります。

### ブリッジ名

ブリッジでは、次の名前前の例を使用します。bridge\_site\_B、スタックグループペア内での指定

名前前の各部分	特定のインターフェイス	有効な値
サイト	ブリッジペアが物理的に配置されているサイト。	A または B
スタックグループ	ブリッジペアが接続されているスタックグループの番号。  FibreBridge 7600N / 7500Nブリッジでは、スタックグループで最大4個のスタックがサポートされます。  スタックグループに含めることができるストレージシェルフは10個までです。	1、2 など
ペア内の場所	ブリッジペア内のブリッジ。ブリッジのペアは、特定のスタックグループに接続します。	a または b

各サイトの1つのスタックグループのブリッジ名の例：

- bridge\_A\_1a
- bridge\_A\_1b
- bridge\_B\_1a
- bridge\_B\_1b

**DR グループ 1 - Site\_A のスタック 1**

- drgroup 1 : MC1\_INIT\_GRP\_1\_SITE\_A\_STK\_GRP\_1\_TOP\_FC1 : \*

FC スイッチ	サイト	スイッチドメイン	Brocade 6505、6510、6520、G620、G610、またはG710 スイッチポート	接続先
FC_switch_A_1 を使用します	A	5.	2.	controller_A_1 のポート 0a
FC_switch_A_1 を使用します	A	5.	3.	controller_A_1 のポート 0c
FC_switch_A_1 を使用します	A	5.	6.	controller_A_2、ポート 0a
FC_switch_A_1 を使用します	A	5.	7.	controller_A_2、ポート 0c
FC_switch_A_1 を使用します	A	5.	8.	bridge_A_1a の FC1
FC_switch_B_1	B	7.	2.	controller_B_1、ポート 0a
FC_switch_B_1	B	7.	3.	controller_B_1、ポート 0c
FC_switch_B_1	B	7.	6.	controller_B_2、ポート 0a
FC_switch_B_1	B	7.	7.	controller_B_2、ポート 0c

Fabric_1 のゾーン	メンバーポート
MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1	5、2 ; 5、3 ; 5、6 ; 5、7 ; 7、2 ; 7、3 ; 7、7 ; 5、8

- drgroup 1 : MC1\_INIT\_GRP\_1\_SITE\_A\_STK\_GRP\_1\_BOT\_FC1 : \*

FC スイッチ	サイト	スイッチドメイン	Brocade 6505、6510、6520、G620、G610、またはG710 スイッチポート	接続先
FC_switch_A_1 を使 用します	A	6.	2.	controller_A_1 のポ ート 0b
FC_switch_A_1 を使 用します	A	6.	3.	controller_A_1 のポ ート 0d
FC_switch_A_1 を使 用します	A	6.	6.	controller_A_2、ポ ート 0b
FC_switch_A_1 を使 用します	A	6.	7.	controller_A_2、ポ ート 0d
FC_switch_A_1 を使 用します	A	6.	8.	bridge_A_1b の FC1
FC_switch_B_1	B	8.	2.	controller_B_1、ポ ート 0b
FC_switch_B_1	B	8.	3.	controller_B_1、ポ ート 0d
FC_switch_B_1	B	8.	6.	controller_B_2、ポ ート 0b
FC_switch_B_1	B	8.	7.	controller_B_2、ポ ート 0d

Fabric_2 のゾーン	メンバーポート
MC1_INIT_GRP_1_SITE_A_STK_GRP_1_BOT_FC1	6、2 ; 6、3 ; 6 ; 6、7 ; 8、2 ; 8、3 ; 8、6 ; 8、7 ; 6、8

## DR グループ 1 - Site\_A のスタック 2

- drgroup 1 : MC1\_INIT\_GRP\_1\_SITE\_A\_STK\_GRP\_2\_TOP\_FC1 : \*

FC スイッチ	サイト	スイッチドメイン	Brocade 6505、6510、6520、G620、G610、またはG710 スイッチポート	接続先
FC_switch_A_1 を使 用します	A	5.	2.	controller_A_1 のポ ート 0a
FC_switch_A_1 を使 用します	A	5.	3.	controller_A_1 のポ ート 0c
FC_switch_A_1 を使 用します	A	5.	6.	controller_A_2、ポ ート 0a
FC_switch_A_1 を使 用します	A	5.	7.	controller_A_2、ポ ート 0c

FC スイッチ	サイト	スイッチドメイン	Brocade 6505 、 6510、 6520、 G62 0、 G610、 または G710 スイッチ ポート	接続先
FC_switch_A_1 を使 用します	A	5.	9.	bridge_A_2a の FC1
FC_switch_B_1	B	7.	2.	controller_B_1、ポ ート 0a
FC_switch_B_1	B	7.	3.	controller_B_1、ポ ート 0c
FC_switch_B_1	B	7.	6.	controller_B_2、ポ ート 0a
FC_switch_B_1	B	7.	7.	controller_B_2、ポ ート 0c

Fabric_1 のゾーン	メンバーポート
MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC1	5、 2 ; 5、 3 ; 5、 6 ; 5、 7 ; 7、 2 ; 7、 3 ; 7、 7 ; 5、 9

• drgroup 1 : MC1\_INIT\_GRP\_1\_SITE\_A\_STK\_GRP\_2\_BOT\_FC1 : \*

FC スイッチ	サイト	スイッチドメイン	Brocade 6505 、 6510、 6520、 G62 0、 G610、 または G710 スイッチ ポート	接続先
FC_switch_A_1 を使 用します	A	6.	2.	controller_A_1 のポ ート 0b
FC_switch_A_1 を使 用します	A	6.	3.	controller_A_1 のポ ート 0d
FC_switch_A_1 を使 用します	A	6.	6.	controller_A_2、ポ ート 0b
FC_switch_A_1 を使 用します	A	6.	7.	controller_A_2、ポ ート 0d
FC_switch_A_1 を使 用します	A	6.	9.	bridge_A_2b の FC1
FC_switch_B_1	B	8.	2.	controller_B_1、ポ ート 0b
FC_switch_B_1	B	8.	3.	controller_B_1、ポ ート 0d
FC_switch_B_1	B	8.	6.	controller_B_2、ポ ート 0b

FC スイッチ	サイト	スイッチドメイン	Brocade 6505 、 6510、 6520、 G62 0、 G610、 または G710 スイッチ ポート	接続先
FC_switch_B_1	B	8.	7.	controller_B_2、ポ ート 0d

Fabric_2 のゾーン	メンバーポート
MC1_INIT_GRP_1_SITE_A_STK_GRP_2_BOT_FC1	6、 2 ; 6、 3 ; 6 ; 6、 7 ; 8、 2 ; 8、 3 ; 8 、 6 ; 8、 7 ; 6、 9

### DR グループ 1 - Site\_B のスタック 1

- MC1\_INIT\_GRP\_1\_SITE\_B\_STK\_GRP\_1\_TOP\_FC1 : \*

FC スイッチ	サイト	スイッチドメイン	Brocade 6505 、 6510、 6520、 G62 0、 G610、 または G710 スイッチ	接続先
FC_switch_A_1 を使 用します	A	5.	2.	controller_A_1 のポ ート 0a
FC_switch_A_1 を使 用します	A	5.	3.	controller_A_1 のポ ート 0c
FC_switch_A_1 を使 用します	A	5.	6.	controller_A_2、ポ ート 0a
FC_switch_A_1 を使 用します	A	5.	7.	controller_A_2、ポ ート 0c
FC_switch_B_1	B	7.	2.	controller_B_1、ポ ート 0a
FC_switch_B_1	B	7.	3.	controller_B_1、ポ ート 0c
FC_switch_B_1	B	7.	6.	controller_B_2、ポ ート 0a
FC_switch_B_1	B	7.	7.	controller_B_2、ポ ート 0c
FC_switch_B_1	B	7.	8.	bridge_B_1a の FC1

Fabric_1 のゾーン	メンバーポート
MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC1	5、 2 ; 5、 3 ; 5、 6 ; 5、 7 ; 7、 2 ; 7、 3 ; 7、 6 ; 7、 8

- drgroup 1 : MC1\_INIT\_GRP\_1\_SITE\_B\_STK\_GRP\_1\_BOT\_FC1 : \*

FC スイッチ	サイト	スイッチドメイン	Brocade 6505 、 6510、 6520、 G62 0、 G610、 または G710 スイッチ	接続先
FC_switch_A_1 を使 用します	A	6.	2.	controller_A_1 のポ ート 0b
FC_switch_A_1 を使 用します	A	6.	3.	controller_A_1 のポ ート 0d
FC_switch_A_1 を使 用します	A	6.	6.	controller_A_2、 ポ ート 0b
FC_switch_A_1 を使 用します	A	6.	7.	controller_A_2、 ポ ート 0d
FC_switch_B_1	B	8.	2.	controller_B_1、 ポ ート 0b
FC_switch_B_1	B	8.	3.	controller_B_1、 ポ ート 0d
FC_switch_B_1	B	8.	6.	controller_B_2、 ポ ート 0b
FC_switch_B_1	B	8.	7.	controller_B_2、 ポ ート 0d
FC_switch_B_1	B	8.	8.	bridge_B_1b の FC1

Fabric_2 のゾーン	メンバーポート
MC1_INIT_GRP_1_SITE_B_STK_GRP_1_BOT_FC1	5、 2 ; 5、 3 ; 5、 6 ; 5、 7 ; 7、 2 ; 7、 3 ; 7、 6 ; 7、 7 ; 8

## DR グループ 1 - Site\_B のスタック 2

• drgroup 1 : MC1\_INIT\_GRP\_1\_SITE\_B\_STK\_GRP\_2\_TOP\_FC1 : \*

FC スイッチ	サイト	スイッチドメイン	Brocade 6505 、 6510、 6520、 G62 0、 G610、 または G710 スイッチ ポート	接続先
FC_switch_A_1 を使 用します	A	5.	2.	controller_A_1 のポ ート 0a
FC_switch_A_1 を使 用します	A	5.	3.	controller_A_1 のポ ート 0c
FC_switch_A_1 を使 用します	A	5.	6.	controller_A_2、 ポ ート 0a
FC_switch_A_1 を使 用します	A	5.	7.	controller_A_2、 ポ ート 0c

FC スイッチ	サイト	スイッチドメイン	Brocade 6505 、 6510、 6520、 G62 0、 G610、 または G710 スイッチ ポート	接続先
FC_switch_B_1	B	7.	2.	controller_B_1、ポ ート 0a
FC_switch_B_1	B	7.	3.	controller_B_1、ポ ート 0c
FC_switch_B_1	B	7.	6.	controller_B_2、ポ ート 0a
FC_switch_B_1	B	7.	7.	controller_B_2、ポ ート 0c
FC_switch_B_1	B	7.	9.	bridge_B_2a の FC1

Fabric_1 のゾーン	メンバーポート
MC1_INIT_GRP_1_SITE_b_STK_GRP_2_TOP_FC1	5、 2 ; 5、 3 ; 5、 6 ; 5、 7 ; 7、 2 ; 7、 3 ; 7、 6 ; 7、 9

• drgroup 1 : MC1\_INIT\_GRP\_1\_SITE\_B\_STK\_GRP\_2\_BOT\_FC1 : \*

FC スイッチ	サイト	スイッチドメイン	Brocade 6505 、 6510、 6520、 G62 0、 G610、 または G710 スイッチ ポート	接続先
FC_switch_A_1 を使 用します	A	6.	2.	controller_A_1 のポ ート 0b
FC_switch_A_1 を使 用します	A	6.	3.	controller_A_1 のポ ート 0d
FC_switch_A_1 を使 用します	A	6.	6.	controller_A_2、ポ ート 0b
FC_switch_A_1 を使 用します	A	6.	7.	controller_A_2、ポ ート 0d
FC_switch_B_1	B	8.	2.	controller_B_1、ポ ート 0b
FC_switch_B_1	B	8.	3.	controller_B_1、ポ ート 0d
FC_switch_B_1	B	8.	6.	controller_B_2、ポ ート 0b
FC_switch_B_1	B	8.	7.	controller_B_2、ポ ート 0d
FC_switch_B_1	B	8.	9.	bridge_B_1b の FC1

Fabric_2 のゾーン	メンバーポート
MC1_INIT_GRP_1_SITE_B_STK_GRP_2_BOT_FC1	6、2、6、6、6、6、7、8、2、8、3、8、6、8、7、8、9

### ストレージゾーンのサマリ

ファブリック	ゾーン名	メンバーポート
FC_switch_A_1 および FC_switch_B_1	MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1	5、2 ; 5、3 ; 5、6 ; 5、7 ; 7、2 ; 7、3 ; 7、7 ; 5、8
	MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC1	5、2 ; 5、3 ; 5、6 ; 5、7 ; 7、2 ; 7、3 ; 7、7 ; 5、9
	MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC1	5、2 ; 5、3 ; 5、6 ; 5、7 ; 7、2 ; 7、3 ; 7、6 ; 7、8
	MC1_INIT_GRP_1_SITE_B_STK_GRP_2_TOP_FC1	5、2 ; 5、3 ; 5、6 ; 5、7 ; 7、2 ; 7、3 ; 7、6 ; 7、9
FC_switch_A_2 と FC_switch_B_2	MC1_INIT_GRP_1_SITE_A_STK_GRP_1_BOT_FC1	6、2 ; 6、3 ; 6 ; 6、7 ; 8、2 ; 8、3 ; 8、6 ; 8、7 ; 6、8
	MC1_INIT_GRP_1_SITE_A_STK_GRP_2_BOT_FC1	6、2 ; 6、3 ; 6 ; 6、7 ; 8、2 ; 8、3 ; 8、6 ; 8、7 ; 6、9
	MC1_INIT_GRP_1_SITE_B_STK_GRP_1_BOT_FC1	6、2 ; 6、3 ; 6 ; 6、7 ; 8、2 ; 8、3 ; 8、6 ; 8、7 ; 8、8
	MC1_INIT_GRP_1_SITE_B_STK_GRP_2_BOT_FC1	6、2、6、6、6、6、7、8、2、8、3、8、6、8、7、8、9

### 両方のFCポートを使用してFibreBridge 7500Nブリッジをゾーン化する

両方の FC ポートを使用する FibreBridge 7500N ブリッジを使用する場合は、ブリッジポートのストレージゾーンを作成する必要があります。ゾーンを設定する前に、ゾーンおよび関連するポートについて理解しておく必要があります。

#### 必要なゾーン

FC-to-SAS ブリッジの FC ポートごとにゾーンを 1 つ設定し、各コントローラモジュールのイニシエータとその FC-to-SAS ブリッジの間のトラフィックを許可する必要があります。

各ストレージゾーンに 5 つのポートが含まれます。

- HBA イニシエータポート × 4 (コントローラごとに 1 つの接続)

- FC-to-SAS ブリッジの FC ポートに接続するポート × 1

ストレージゾーンでは標準のゾーニングを使用します。

例では、各サイトの 2 つのスタックグループを接続する 2 組のブリッジのペアを示します。各ブリッジが 1 つの FC ポートを使用するため、ファブリックあたりのストレージゾーン数は 8 個（合計 16 個）になります。

### ブリッジ名

ブリッジでは、次の名前前の例を使用します。 bridge\_site\_B、スタックグループペア内での指定

名前前の各部分	特定のインターフェイス	有効な値
サイト	ブリッジペアが物理的に配置されているサイト。	A または B
スタックグループ	ブリッジペアが接続されているスタックグループの番号。  FibreBridge 7600N / 7500N ブリッジでは、スタックグループで最大 4 個のスタックがサポートされます。  スタックグループに含めることができるストレージシェルフは 10 個までです。	1、2 など
ペア内の場所	ブリッジペア内のブリッジ。ブリッジのペアは、特定のスタックグループに接続します。	a または b

各サイトの 1 つのスタックグループのブリッジ名の例：

- bridge\_A\_1a
- bridge\_A\_1b
- bridge\_B\_1a
- bridge\_B\_1b

### DR グループ 1 - Site\_A のスタック 1

- drgroup 1 : MC1\_INIT\_GRP\_1\_SITE\_A\_STK\_GRP\_1\_TOP\_FC1 : \*

FC スイッチ	サイト	スイッチドメイン	6505 / 6510 / G610 / G710 / G620 ポート	6520 ポート	接続先

FC_switch_A_1 を使用します	A	5.	2.	2.	controller_A_1 のポート 0a
FC_switch_A_1 を使用します	A	5.	6.	6.	controller_A_2 、ポート 0a
FC_switch_A_1 を使用します	A	5.	8.	8.	bridge_A_1a の FC1
FC_switch_B_1	B	7.	2.	2.	controller_B_1 、ポート 0a
FC_switch_B_1	B	7.	6.	6.	controller_B_2 、ポート 0a

Fabric_1 のゾーン	メンバーポート
MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1	5、 2 ; 5、 6 ; 7、 2 ; 7、 6 ; 5、 8

• drgroup 1 : MC1\_INIT\_GRP\_2\_SITE\_A\_STK\_GRP\_1\_TOP\_FC1 : \*

FC スイッチ	サイト	スイッチドメ イン	6505 / 6510 / G610 / G710 ポート	6520 ポート	G620 ポート	接続先
FC_switch_A_1 を使用しま す	A	5.	3.	3.	3.	controller_A_1 のポート 0c
FC_switch_A_1 を使用しま す	A	5.	7.	7.	7.	controller_A_2 、ポート 0c
FC_switch_A_1 を使用しま す	A	5.	9.	9.	9.	bridge_A_1b の FC1
FC_switch_B_1	B	7.	3.	3.	3.	controller_B_1 、ポート 0c
FC_switch_B_1	B	7.	7.	7.	7.	controller_B_2 、ポート 0c

Fabric_2 のゾーン	メンバーポート
MC1_INIT_GRP_2_SITE_A_STK_GRP_1_BOT_FC1	5、 3 ; 5、 7 ; 7、 3 ; 7、 7 ; 5、 9

• drgroup 1 : MC1\_INIT\_GRP\_1\_SITE\_A\_STK\_GRP\_1\_BOT\_FC1 : \*

FC スイッチ	サイト	スイッチドメイン	6505 / 6510 / G610 / G710	6520	G620	接続先
FC_switch_A_2	A	6.	2.	2.	2.	controller_A_1 のポート 0b
FC_switch_A_2	A	6.	6.	6.	6.	controller_A_2、ポート 0b
FC_switch_A_2	A	6.	8.	8.	8.	bridge_A_1a の FC2
FC_switch_B_2	B	8.	2.	2.	2.	controller_B_1、ポート 0b
FC_switch_B_2	B	8.	6.	6.	6.	controller_B_2、ポート 0b

Fabric_1 のゾーン	メンバーポート
MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC2	6、2、6、8、2、8、6、6、8

• drgroup 1 : MC1\_INIT\_GRP\_2\_SITE\_A\_STK\_GRP\_1\_BOT\_FC2 : \*

FC スイッチ	サイト	スイッチドメイン	6505 / 6510 / G610 / G710	6520	G620	接続先
FC_switch_A_2	A	6.	3.	3.	3.	controller_A_1 のポート 0d
FC_switch_A_2	A	6.	7.	7.	7.	controller_A_2、ポート 0d
FC_switch_A_2	A	6.	9.	9.	9.	bridge_A_1b の FC2
FC_switch_B_2	B	8.	3.	3.	3.	controller_B_1、ポート 0d
FC_switch_B_2	B	8.	7.	7.	7.	controller_B_2、ポート 0d

Fabric_2 のゾーン	メンバーポート
MC1_INIT_GRP_2_SITE_A_STK_GRP_1_BOT_FC2	6、3、6、7、8、3、8、7、6、9

DR グループ 1 - Site\_A のスタック 2

- drgroup 1 : MC1\_INIT\_GRP\_1\_SITE\_A\_STK\_GRP\_2\_TOP\_FC1 : \*

FC スイッチ	サイト	スイッチドメイン	6505 / 6510 / G610 / G710 ポート	6520 ポート	G620 ポート	接続先
FC_switch_A_1 を使用しません	A	5.	2.	2.	2.	controller_A_1 のポート 0a
FC_switch_A_1 を使用しません	A	5.	6.	6.	6.	controller_A_2、ポート 0a
FC_switch_A_1 を使用しません	A	5.	10.	10.	10.	bridge_A_2a の FC1
FC_switch_B_1	B	7.	2.	2.	2.	controller_B_1、ポート 0a
FC_switch_B_1	B	7.	6.	6.	6.	controller_B_2、ポート 0a

Fabric_1 hh のゾーン	メンバーポート
MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC1	5、 2 ; 5、 6 ; 7、 2 ; 7、 6 ; 5、 10

- drgroup 1 : MC1\_INIT\_GRP\_2\_SITE\_A\_STK\_GRP\_2\_TOP\_FC1 : \*

FC スイッチ	サイト	スイッチドメイン	6505 / 6510 / G610 / G710 ポート	6520 ポート	G620 ポート	接続先
FC_switch_A_1 を使用しません	A	5.	3.	3.	3.	controller_A_1 のポート 0c
FC_switch_A_1 を使用しません	A	5.	7.	7.	7.	controller_A_2、ポート 0c
FC_switch_A_1 を使用しません	A	5.	11.	11.	11.	bridge_A_2b の FC1
FC_switch_B_1	B	7.	3.	3.	3.	controller_B_1、ポート 0c

FC_switch_B_1	B	7.	7.	7.	7.	controller_B_2、ポート 0c
---------------	---	----	----	----	----	-----------------------

Fabric_2 のゾーン	メンバーポート
MC1_INIT_GRP_2_SITE_A_STK_GRP_2_BOT_FC1	5、3 ; 5、7 ; 7、3 ; 7、7 ; 5、11

• drgroup 1 : MC1\_INIT\_GRP\_1\_SITE\_A\_STK\_GRP\_2\_BOT\_FC2 : \*

FC スイッチ	サイト	スイッチドメイン	6505 / 6510 / G610 / G710 ポート	6520 ポート	G620 ポート	接続先
FC_switch_A_2	A	6.	2.	0	0	controller_A_1 のポート 0b
FC_switch_A_2	A	6.	6.	4.	4.	controller_A_2、ポート 0b
FC_switch_A_2	A	6.	10.	10.	10.	bridge_A_2a の FC2
FC_switch_B_2	B	8.	2.	2.	2.	controller_B_1、ポート 0b
FC_switch_B_2	B	8.	6.	6.	6.	controller_B_2、ポート 0b

Fabric_1 のゾーン	メンバーポート
MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC2	6、2、6、8、2、8、6、6、10

• drgroup 1 : MC1\_INIT\_GRP\_2\_SITE\_A\_STK\_GRP\_2\_BOT\_FC2 : \*

FC スイッチ	サイト	スイッチドメイン	6505 / 6510 / G610 / G710 ポート	6520 ポート	G620 ポート	接続先
FC_switch_A_2	A	6.	3.	3.	3.	controller_A_1 のポート 0d
FC_switch_A_2	A	6.	7.	7.	7.	controller_A_2、ポート 0d
FC_switch_A_2	A	6.	11.	11.	11.	Bridge_A_2b FC2

FC_switch_B_2	B	8.	3.	3.	3.	controller_B_1、ポート 0d
FC_switch_B_2	B	8.	7.	7.	7.	controller_B_2、ポート 0d

Fabric_2 のゾーン	メンバーポート
MC1_INIT_GRP_2_SITE_A_STK_GRP_2_BOT_FC2	6、3、6、7、8、3、8、7、6、11

### DR グループ 1 - Site\_B のスタック 1

- drgroup 1 : MC1\_INIT\_GRP\_1\_SITE\_B\_STK\_GRP\_1\_TOP\_FC1 : \*

FC スイッチ	サイト	スイッチドメイン	6505 / 6510 / G610 / G710 ポート	6520 ポート	G620 ポート	接続先
FC_switch_A_1 を使用しません	A	5.	2.	2.	2.	controller_A_1 のポート 0a
FC_switch_A_1 を使用しません	A	5.	6.	6.	6.	controller_A_2、ポート 0a
FC_switch_B_1	B	7.	2.	2.	8.	controller_B_1、ポート 0a
FC_switch_B_1	B	7.	6.	6.	2.	controller_B_2、ポート 0a
FC_switch_B_1	B	7.	8.	8.	6.	bridge_B_1a の FC1

Fabric_1 のゾーン	メンバーポート
MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC1	5、2 ; 5、6 ; 7、2 ; 7、6 ; 7、8

- drgroup 1 : MC1\_INIT\_GRP\_2\_SITE\_B\_STK\_GRP\_1\_TOP\_FC1 : \*

FC スイッチ	サイト	スイッチドメイン	6505 / 6510 / G610 / G710 ポート	6520 ポート	G620 ポート	接続先

FC_switch_A_1を使用します	A	5.	3.	3.	3.	controller_A_1のポート 0c
FC_switch_A_1を使用します	A	5.	7.	7.	7.	controller_A_2、ポート 0c
FC_switch_B_1	B	7.	3.	3.	9.	controller_B_1、ポート 0c
FC_switch_B_1	B	7.	7.	7.	3.	controller_B_2、ポート 0c
FC_switch_B_1	B	7.	9.	9.	7.	bridge_B_1bのFC1

Fabric_2 のゾーン	メンバーポート
MC1_INIT_GRP_2_SITE_B_STK_GRP_1_BOT_FC1	5、3 ; 5、7 ; 7、3 ; 7、7 ; 7、9

• drgroup 1 : MC1\_INIT\_GRP\_1\_SITE\_B\_STK\_GRP\_1\_BOT\_FC2 : \*

FC スイッチ	サイト	スイッチドメイン	6505 / 6510 / G610 / G710 ポート	6520 ポート	G620 ポート	接続先
FC_switch_A_2	A	6.	2.	2.	2.	controller_A_1のポート 0b
FC_switch_A_2	A	6.	6.	6.	6.	controller_A_2、ポート 0b
FC_switch_B_2	B	8.	2.	2.	2.	controller_B_1、ポート 0b
FC_switch_B_2	B	8.	6.	6.	6.	controller_B_2、ポート 0b
FC_switch_B_2	B	8.	8.	8.	8.	bridge_B_1aのFC2

Fabric_1 のゾーン	メンバーポート
MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC2	6、2、6、8、2、8、6、8、8

• drgroup 1 : MC1\_INIT\_GRP\_2\_SITE\_B\_STK\_GRP\_1\_BOT\_FC2 : \*

FC スイッチ	サイト	スイッチドメイン	6505 / 6510 / G610 / G710 ポート	6520 ポート	G620 ポート	接続先
FC_switch_A_2	A	6.	3.	3.	3.	controller_A_1 のポート 0d
FC_switch_A_2	A	6.	7.	7.	7.	controller_A_2、ポート 0d
FC_switch_B_2	B	8.	3.	3.	3.	controller_B_1、ポート 0d
FC_switch_B_2	B	8.	7.	7.	7.	controller_B_2、ポート 0d
FC_switch_B_2	B	8.	9.	9.	9.	bridge_A_1b の FC2

Fabric_2 のゾーン	メンバーポート
MC1_INIT_GRP_2_SITE_B_STK_GRP_1_BOT_FC2	6、3、6、7、8、3、8、7、8、9

#### DR グループ 1 - Site\_B のスタック 2

- drgroup 1 : MC1\_INIT\_GRP\_1\_SITE\_B\_STK\_GRP\_2\_TOP\_FC1 : \*

FC スイッチ	サイト	スイッチドメイン	6505 / 6510 / G610 / G710 ポート	6520 ポート	G620 ポート	接続先
FC_switch_A_1 を使用しません	A	5.	2.	2.	2.	controller_A_1 のポート 0a
FC_switch_A_1 を使用しません	A	5.	6.	6.	6.	controller_A_2、ポート 0a
FC_switch_B_1	B	7.	2.	2.	2.	controller_B_1、ポート 0a
FC_switch_B_1	B	7.	6.	6.	6.	controller_B_2、ポート 0a
FC_switch_B_1	B	7.	10.	10.	10.	bridge_B_2a の FC1

Fabric_1 のゾーン	メンバーポート
MC1_INIT_GRP_1_SITE_B_STK_GRP_2_TOP_FC1	5、 2 ; 5、 6 ; 7、 2 ; 7、 6 ; 7、 10

• drgroup 1 : MC1\_INIT\_GRP\_2\_SITE\_B\_STK\_GRP\_2\_TOP\_FC1 : \*

FC スイッチ	サイト	スイッチドメイン	6505 / 6510 / G610 / G710 ポート	6520 ポート	G620 ポート	接続先
FC_switch_A_1 を使用しません	A	5.	3.	3.	3.	controller_A_1 のポート 0c
FC_switch_A_1 を使用しません	A	5.	7.	7.	7.	controller_A_2、ポート 0c
FC_switch_B_1	B	7.	3.	3.	3.	controller_B_1、ポート 0c
FC_switch_B_1	B	7.	7.	7.	7.	controller_B_2、ポート 0c
FC_switch_B_1	B	7.	11.	11.	11.	bridge_B_2b の FC1

Fabric_2 hh のゾーン	メンバーポート
MC1_INIT_GRP_2_SITE_B_STK_GRP_2_BOT_FC1	5、 3 ; 5、 7 ; 7、 3 ; 7、 7 ; 7、 11

• drgroup 1 : MC1\_INIT\_GRP\_1\_SITE\_B\_STK\_GRP\_2\_BOT\_FC2 : \*

FC スイッチ	サイト	スイッチドメイン	6505 / 6510 / G610 / G710 ポート	6520 ポート	G620 ポート	接続先
FC_switch_A_2	A	6.	2.	2.	2.	controller_A_1 のポート 0b
FC_switch_A_2	A	6.	6.	6.	6.	controller_A_2、ポート 0b
FC_switch_B_2	B	8.	2.	2.	2.	controller_B_1、ポート 0b
FC_switch_B_2	B	8.	6.	6.	6.	controller_B_2、ポート 0b

FC_switch_B_2	B	8.	10.	10.	10.	bridge_B_2a の FC2
---------------	---	----	-----	-----	-----	----------------------

Fabric_1 のゾーン	メンバーポート
MC1_INIT_GRP_1_SITE_B_STK_GRP_2_TOP_FC2	6、2、6、8、2、8、6、8、10

• drgroup 1 : MC1\_INIT\_GRP\_2\_SITE\_B\_STK\_GRP\_2\_BOT\_FC2 : \*

FC スイッチ	サイト	スイッチドメイン	6505 / 6510 / G610 / G710 ポート	6520 ポート	G620 ポート	接続先
FC_switch_A_2	A	6.	3.	3.	3.	controller_A_1 のポート 0d
FC_switch_A_2	A	6.	7.	7.	7.	controller_A_2、 ポート 0d
FC_switch_B_2	B	8.	3.	3.	3.	controller_B_1、 ポート 0d
FC_switch_B_2	B	8.	7.	7.	7.	controller_B_2、 ポート 0d
FC_switch_B_2	B	8.	11.	11.	11.	Bridge_B_2b FC2

Fabric_2 のゾーン	メンバーポート
MC1_INIT_GRP_2_SITE_B_STK_GRP_2_BOT_FC2	6、3、6、7、8、3、8、7、8、11

#### ストレージゾーンのサマリ

ファブリック	ゾーン名	メンバーポート
FC_switch_A_1 および FC_switch_B_1	MC1_INIT_GRP_1_SITE_A_STK_ GRP_1_TOP_FC1	5、2 ; 5、6 ; 7、2 ; 7、6 ; 5、8
FC_switch_A_1 および FC_switch_B_1	MC1_INIT_GRP_2_SITE_A_STK_ GRP_1_BOT_FC1	5、3 ; 5、7 ; 7、3 ; 7、7 ; 5、9
FC_switch_A_1 および FC_switch_B_1	MC1_INIT_GRP_1_SITE_A_STK_ GRP_2_TOP_FC1	5、2 ; 5、6 ; 7、2 ; 7、6 ; 5、10

FC_switch_A_1 および FC_switch_B_1	MC1_INIT_GRP_2_SITE_A_STK_ GRP_2_BOT_FC1	5、3 ; 5、7 ; 7、3 ; 7、7 ; 5、11
FC_switch_A_1 および FC_switch_B_1	MC1_INIT_GRP_1_SITE_B_STK_ GRP_1_TOP_FC1	5、2 ; 5、6 ; 7、2 ; 7、6 ; 7、8
FC_switch_A_1 および FC_switch_B_1	MC1_INIT_GRP_2_SITE_B_STK_ GRP_1_BOT_FC1	5、3 ; 5、7 ; 7、3 ; 7、7 ; 7、9
FC_switch_A_1 および FC_switch_B_1	MC1_INIT_GRP_1_SITE_B_STK_ GRP_2_TOP_FC1	5、2 ; 5、6 ; 7、2 ; 7、6 ; 7、10
FC_switch_A_1 および FC_switch_B_1	MC1_INIT_GRP_2_SITE_B_STK_ GRP_2_BOT_FC1	5、3 ; 5、7 ; 7、3 ; 7、7 ; 7、11
FC_switch_A_2 と FC_switch_B_2	MC1_INIT_GRP_1_SITE_A_STK_ GRP_1_TOP_FC2	6、2、6、8、2、8、6、6 、8
FC_switch_A_2 と FC_switch_B_2	MC1_INIT_GRP_2_SITE_A_STK_ GRP_1_BOT_FC2	6、3、6、7、8、3、8、7 、6、9
FC_switch_A_2 と FC_switch_B_2	MC1_INIT_GRP_1_SITE_A_STK_ GRP_2_TOP_FC2	6、2、6、8、2、8、6、6 、10
FC_switch_A_2 と FC_switch_B_2	MC1_INIT_GRP_2_SITE_A_STK_ GRP_2_BOT_FC2	6、3、6、7、8、3、8、7 、6、11
FC_switch_A_2 と FC_switch_B_2	MC1_INIT_GRP_1_SITE_B_STK_ GRP_1_TOP_FC2	6、2、6、8、2、8、6、8 、8
FC_switch_A_2 と FC_switch_B_2	MC1_INIT_GRP_2_SITE_B_STK_ GRP_1_BOT_FC2	6、3、6、7、8、3、8、7 、8、9
FC_switch_A_2 と FC_switch_B_2	MC1_INIT_GRP_1_SITE_B_STK_ GRP_2_TOP_FC2	6、2、6、8、2、8、6、8 、10
FC_switch_A_2 と FC_switch_B_2	MC1_INIT_GRP_2_SITE_B_STK_ GRP_2_BOT_FC2	6、3、6、7、8、3、8、7 、8、11

## Brocade FCスイッチをゾーン分けする

スイッチポートを別々のゾーンに割り当てて、コントローラとストレージのトラフィックを分離する必要があります。また、FC-VIポートのゾーンとストレージポートのゾーンも含める必要があります。

このタスクについて

次の手順では、MetroCluster 構成の標準的なゾーニングを使用します。

## "FC-VI ポートのゾーニング"

### "1つのFCポートを使用するFibreBridge 7500N / 7600Nブリッジのゾーニング"

### "両方の FC ポートを使用する FibreBridge 7500N ブリッジのゾーニング"

#### 手順

1. 各スイッチに FC-VI ゾーンを作成します。

```
zonecreate "QOSH1_FCVI_1"、 member ; member ... ..
```

この例では、ポート 5、 0 ; 5、 1 ; 5、 4 ; 5、 5 ; 7、 0 ; 7、 1 ; 7、 4 ; 7、 5 を含む QOS FCVI ゾーンを作成しています。

```
Switch_A_1:admin> zonecreate "QOSH1_FCVI_1",  
"5,0;5,1;5,4;5,5;7,0;7,1;7,4;7,5"
```

2. 各スイッチにストレージゾーンを設定します。

ファブリックのゾーニングは、ファブリック内の 1 つのスイッチから設定できます。次の例では、Switch\_A\_1 でゾーニングを設定します。

- a. スイッチファブリックの各スイッチドメインのストレージゾーンを作成します。

```
zonecreate name、 member ; member ... ..
```

この例では、両方の FC ポートを使用する FibreBridge 7500N のストレージゾーンを作成します。ゾーンには、ポート 5、 2 ; 5、 6 ; 7、 2 ; 7、 6 ; 5、 16 が含まれます。

```
Switch_A_1:admin> zonecreate  
"MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1", "5,2;5,6;7,2;7,6;5,16"
```

- b. 1 つ目のスイッチファブリックで設定を作成します。

```
cfgcreate config_name、 zone ; zone... を使用します
```

この例では、CFG\_1 という名前、 QOSH1\_MC1\_FAB\_1\_FCVI および GRP\_1\_SITE\_A\_STK\_GRP\_1\_TOP\_FC1 の 2 つのゾーンを含む設定を作成します

```
Switch_A_1:admin> cfgcreate "CFG_1", "QOSH1_MC1_FAB_1_FCVI;  
MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1"
```

- c. 必要に応じて、設定にゾーンを追加します。

```
cfgadd config_name zone ; zone... を使用します
```

- d. 設定を有効にします。

## cfgenable config\_name

```
Switch_A_1:admin> cfgenable "CFG_1"
```

- e. 設定を保存します。

## cfsave

```
Switch_A_1:admin> cfsave
```

- f. ゾーニング設定を検証します。

## zone — 妥当性検査

```
Switch_A_1:admin> zone --validate
Defined configuration:
cfg: CFG_1 QOSH1_MC1_FAB_1_FCVI ;
MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1
zone: QOSH1_MC1_FAB_1_FCVI
5,0;5,1;5,4;5,5;7,0;7,1;7,4;7,5
zone: MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1
5,2;5,6;7,2;7,6;5,16
Effective configuration:
cfg: CFG_1
zone: QOSH1_MC1_FAB_1_FCVI
5,0
5,1
5,4
5,5
7,0
7,1
7,4
7,5
zone: MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1
5,2
5,6
7,2
7,6
5,16
-----
~ - Invalid configuration
* - Member does not exist
# - Invalid usage of broadcast zone
```

## Brocade 6510またはG620スイッチでISL暗号化を設定する

Brocade 6510 または G620 スイッチでは、ISL 接続に対してオプションで Brocade 暗号化機能を使用できます。暗号化機能を使用する場合は、MetroCluster 構成の各スイッチで追加の設定手順を実行する必要があります。

作業を開始する前に

- Brocade 6510 または G620 スイッチが必要です。



Brocade G620 スイッチでの ISL 暗号化の使用は、ONTAP 9.4 以降でのみサポートされません。

- 同じファブリックの 2 つのスイッチを選択しておく必要があります。
- スイッチと Fabric Operating System のバージョンに対応する Brocade のドキュメントを参照して、帯域幅とポートの制限を確認しておく必要があります。

このタスクについて

この手順は、同じファブリック内の両方のスイッチで実行する必要があります。

### 仮想ファブリックを無効にする

ISL 暗号化を設定するには、MetroCluster 構成で使用されている 4 つのスイッチすべてで仮想ファブリックを無効にする必要があります。

手順

1. スイッチコンソールで次のコマンドを入力して、仮想ファブリックを無効にします。

```
fosconfig — VF' を無効にします
```

2. スイッチをリブートします。

### ペイロードを設定します

仮想ファブリックを無効にしたら、ファブリック内の両方のスイッチでペイロードまたはデータフィールドサイズを設定する必要があります。

このタスクについて

データフィールドサイズは 2048 以下にする必要があります。

手順

1. スイッチを無効にします。

```
'witchdisable
```

2. ペイロードを設定します。

「configure」を実行します

3. 次のスイッチパラメータを設定します。

- a. Fabric パラメータを 'y' のように設定します

b. Domain、WWN ベースの persistent PID など、その他のパラメータを設定します。

c. データフィールドのサイズを「2048」に設定します

認証ポリシーを設定します

認証ポリシーおよび関連するパラメータを設定する必要があります。

このタスクについて

コマンドはスイッチコンソールで実行する必要があります。

手順

1. 認証シークレットを設定します。

a. セットアッププロセスを開始します。

```
'ecAuthSecret — セット
```

このコマンドにより、次の手順で応答する一連のプロンプトが開始されます。

a. Enter peer WWN、Domain、or switch name というプロンプトに対して、ファブリック内のもう一方のスイッチの World Wide Name（WWN；ワールドワイド名）を指定します。

b. Enter peer secret というプロンプトに対して、ピアシークレットを指定します。

c. Enter local secret というプロンプトに対して、ローカルシークレットを指定します。

d. 「Are you done」パラメータに「Y」と入力します。

認証シークレットの設定例を以下に示します。

```
brcd> secAuthSecret --set
```

This command is used to set up secret keys for the DH-CHAP authentication.

The minimum length of a secret key is 8 characters and maximum 40 characters. Setting up secret keys does not initiate DH-CHAP authentication. If switch is configured to do DH-CHAP, it is performed whenever a port or a switch is enabled.

Warning: Please use a secure channel for setting secrets. Using an insecure channel is not safe and may compromise secrets.

Following inputs should be specified for each entry.

1. WWN for which secret is being set up.
2. Peer secret: The secret of the peer that authenticates to peer.
3. Local secret: The local secret that authenticates peer.

Press enter to start setting up secrets > <cr>

Enter peer WWN, Domain, or switch name (Leave blank when done):

10:00:00:05:33:76:2e:99

Enter peer secret: <hidden>

Re-enter peer secret: <hidden>

Enter local secret: <hidden>

Re-enter local secret: <hidden>

Enter peer WWN, Domain, or switch name (Leave blank when done):

Are you done? (yes, y, no, n): [no] yes

Saving data to key store... Done.

2. 認証グループを 4 に設定します。

```
authUtil — set-g 4`
```

3. 認証タイプを「dhchap」に設定します。

```
authUtil — set -a dhchap
```

次の出力が表示されます。

```
Authentication is set to dhchap.
```

4. スイッチの認証ポリシーを on に設定します。

authUtil — policy-sw on`

次の出力が表示されます。

```
Warning: Activating the authentication policy requires either DH-CHAP
secrets or PKI certificates depending on the protocol selected.
Otherwise, ISLs will be segmented during next E-port bring-up.
ARE YOU SURE (yes, y, no, n): [no] yes
Auth Policy is set to ON
```

## Brocade スイッチで ISL 暗号化を有効にします

認証ポリシーと認証シークレットを設定したら、ポートで ISL 暗号化を有効にする必要があります。

このタスクについて

- この手順は、一度に 1 つのスイッチファブリックで実行する必要があります。
- コマンドはスイッチコンソールで実行する必要があります。

手順

1. すべての ISL ポートで暗号化を有効にします。

portCfgEncrypt — ポート番号を有効にします

次の例は、ポート 8 とポート 12 で暗号化を有効にします。

portCfgEncrypt — 8 を有効にします

portCfgEncrypt — 12 を有効にします

2. スイッチを有効にします。

「witchenable」

3. ISL が稼働していることを確認します。

「islshow」

4. 暗号化が有効であることを確認します。

portenccompshow`

次の例は、ポート 8 とポート 12 で暗号化が有効であることを示しています。

User Port	Encryption configured	Active
8	yes	yes
9	No	No
10	No	No
11	No	No
12	yes	yes

次に何をするか

MetroCluster 構成の他のファブリック内のスイッチで、すべての手順を実行します。

### Cisco FC スイッチを手動で設定する

MetroCluster 構成の各 Cisco スイッチを ISL 接続とストレージ接続用にそれぞれ設定する必要があります。

作業を開始する前に

Cisco FC スイッチには次の要件が適用されます。

- 同じNX-OSバージョンおよびライセンスの同じモデルの、サポートされている4台のCiscoスイッチを使用する必要があります。
- MetroCluster 構成には4つのスイッチが必要です。

それぞれ2つのスイッチで構成される2つのファブリックに接続されます。各ファブリックが両方のサイトにまたがっている必要があります。

- ATTO FibreBridge モデルへの接続をサポートしている必要があります。
- Cisco FCストレージファブリックでは暗号化や圧縮を使用できません。MetroCluster 構成ではサポートされません。

を参照してください "[ネットアップの Interoperability Matrix Tool \(IMT\)](#)" では、Storage 解決策フィールドを使用して MetroCluster 解決策を選択できます。検索を絞り込むには、\* 構成部品エクスプローラ \* を使用して構成部品と ONTAP バージョンを選択します。[ 結果の表示 ( Show Results ) ] をクリックすると、条件に一致するサポートされている構成のリストを表示できます。

このタスクについて

環境スイッチ間リンク ( ISL ) 接続には次の要件があります。

- 1つのファブリック内のすべての ISL の長さや速度が同じである必要があります。

ISL の長さはファブリックが異なる場合は同じである必要はありませんが、速度はすべてのファブリックで同じである必要があります。

環境 the storage connections には次の要件があります。

- 各ストレージコントローラに、スイッチファブリックに接続可能なイニシエータポートが 4 つ必要です。

各ストレージコントローラの 2 つのイニシエータポートを各ファブリックに接続する必要があります。



FAS8020、AFF8020、FAS8200、および AFF A300 のシステムでは、次のすべての条件に該当する場合、コントローラあたりのイニシエータポートを 2 ポート（各ファブリックに 1 つのイニシエータポートを接続）にすることができます。

- ディスクストレージの接続に使用できる FC イニシエータポートが 3 つ以下で、それ以外に FC イニシエータとして設定できるポートがない。
- すべてのスロットが使用中で、FC イニシエータカードを追加できません。

## 関連情報

["NetApp Interoperability Matrix Tool で確認できます"](#)

## Cisco スイッチのライセンス要件

ファブリック接続 MetroCluster 構成では、Cisco スイッチに一部の機能ベースのライセンスが必要な場合があります。これらのライセンスを使用すると、QoS や長距離モードクレジットなどの機能をスイッチで使用できます。MetroCluster 構成内の 4 つのスイッチすべてに、必要な機能ベースのライセンスをインストールする必要があります。

MetroCluster 構成では、次の機能ベースのライセンスが必要になる場合があります。

- ENTERPRISE\_PKG

Cisco スイッチで QoS 機能を使用できるようになります。

- PORT\_ACTIVATION\_PKG

このライセンスは、Cisco 9148 スイッチに使用できます。スイッチ上のポートをアクティブ化または非アクティブ化できます。ただし、任意の時点でアクティブにできるポートは 16 個のみです。Cisco MDS 9148 スイッチでは 16 個のポートがデフォルトで有効になっています。

- FM\_SERVER\_PKG

複数のファブリックを同時に管理でき、また、Web ブラウザを使用してスイッチを管理できます。

FM\_SERVER\_PKG ライセンスがある場合、パフォーマンスしきい値、しきい値の監視などのパフォーマンス管理機能も使用できるようになります。このライセンスの詳細については、Cisco Fabric Manager Server Package を参照してください。

show license usage コマンドを使用すると、ライセンスがインストールされているかどうかを確認できます。これらのライセンスをお持ちでない場合は、インストールを開始する前に営業担当者にお問い合わせください。



Cisco MDS 9250i スイッチには、固定構成の 1/10GbE IP ストレージサービスポートが 2 つあります。これらのポートには追加のライセンスは必要ありません。Cisco SAN Extension over IP アプリケーションパッケージは、これらのスイッチの標準ライセンスで、FCIP や圧縮などの機能を有効にします。

## Cisco FC スイッチを工場出荷時のデフォルトに設定

正しく設定するには、スイッチを工場出荷時のデフォルトに設定する必要があります。これにより、スイッチがクリーンな設定から開始されます。

このタスクについて

このタスクは、MetroCluster 構成内のすべてのスイッチで実行する必要があります。

手順

1. コンソールに接続し、同じファブリック内の両方のスイッチにログインします。
2. スイッチをデフォルトの設定に戻します。

「write erase」を入力します

コマンドの確認を求められたら、「y」と入力します。これにより、スイッチのライセンスおよび設定情報がすべて消去されます。

3. スイッチをリブートします。

「再ロード」

コマンドの確認を求められたら、「y」と入力します。

4. もう一方のスイッチで 'write erase' コマンドと 'reload コマンドを繰り返します

「reload」コマンドを発行すると、スイッチが再起動し、セットアップのプロンプトが表示されます。この時点で、次のセクションに進みます。

例

次の例は、FC\_switch\_A\_1 と FC\_switch\_B\_1 で構成されるファブリックでの処理を示しています。

```
FC_Switch_A_1# write erase
Warning: This command will erase the startup-configuration.
Do you wish to proceed anyway? (y/n) [n] y
FC_Switch_A_1# reload
This command will reboot the system. (y/n)? [n] y

FC_Switch_B_1# write erase
Warning: This command will erase the startup-configuration.
Do you wish to proceed anyway? (y/n) [n] y
FC_Switch_B_1# reload
This command will reboot the system. (y/n)? [n] y
```

## Cisco FC スイッチの基本設定とコミュニティストリングを設定します

基本設定は 'setup' コマンドを使用して、または 'reload' コマンドを発行した後で指定する必要があります。

手順

1. セットアップのプロンプトがスイッチに表示されない場合は、スイッチの基本設定を実行します。

「セットアップ」

2. SNMP コミュニティストリングのプロンプトが表示されるまで、セットアップの質問に対するデフォルトの応答を受け入れます。
3. コミュニティストリングを「public」（すべて小文字）に設定し、ONTAP ヘルスモニタからのアクセスを許可します。

コミュニティストリングを「public」以外の値に設定することもできますが、指定したコミュニティストリングを使用して ONTAP ヘルスモニタを設定する必要があります。

次の例は、FC\_switch\_A\_1 に対するコマンドを示しています。

```
FC_switch_A_1# setup
  Configure read-only SNMP community string (yes/no) [n]: y
  SNMP community string : public
  Note: Please set the SNMP community string to "Public" or another
value of your choosing.
  Configure default switchport interface state (shut/noshut) [shut]:
noshut
  Configure default switchport port mode F (yes/no) [n]: n
  Configure default zone policy (permit/deny) [deny]: deny
  Enable full zoneset distribution? (yes/no) [n]: yes
```

次の例は、FC\_switch\_B\_1 に対するコマンドを示しています。

```
FC_switch_B_1# setup
  Configure read-only SNMP community string (yes/no) [n]: y
  SNMP community string : public
  Note: Please set the SNMP community string to "Public" or another
value of your choosing.
  Configure default switchport interface state (shut/noshut) [shut]:
noshut
  Configure default switchport port mode F (yes/no) [n]: n
  Configure default zone policy (permit/deny) [deny]: deny
  Enable full zoneset distribution? (yes/no) [n]: yes
```

ポートのライセンスを取得しています

連続する範囲のポートで Cisco スイッチライセンスを使用する必要はありません。代わりに、使用する特定のポートのライセンスを取得し、未使用のポートからライセンスを削除できます。

作業を開始する前に

スイッチ構成内でライセンスが付与されているポートの数を確認し、必要に応じてポート間でライセンスを移動します。

## 手順

1. スイッチファブリックのライセンス使用状況を表示します。

```
'how port-resources module 1'
```

ライセンスが必要なポートを特定します。ライセンスが付与されていないポートがある場合は、ライセンスが付与されている余分なポートがないかを特定し、余分なポートからライセンスを削除することを検討します。

2. コンフィギュレーションモードを開始します。

```
'config t'
```

3. 選択したポートからライセンスを削除します。
  - a. ライセンスを削除するポートを選択します。

```
'interface_name_`
```

- b. ポートからライセンスを削除します。

「 no port-license acquire 」を選択します

- c. ポート設定インターフェイスを終了します。

```
「 exit
```

4. 選択したポートのライセンスを取得します。

- a. ライセンスを削除するポートを選択します。

```
'interface_name_`
```

- b. ポートがライセンスを取得できるようにします。

「ポートライセンス」

- c. ポートのライセンスを取得します。

「ポートライセンス取得」

- d. ポート設定インターフェイスを終了します。

```
「 exit
```

5. 追加のポートがある場合は、この手順を繰り返します

6. 構成モードを終了します。

```
「 exit
```

## ポートのライセンスを削除および取得する

次の例は、ポート fc1/2 からライセンスを削除し、ポート fc1/1 をライセンス取得可能にし、ポート fc1/1 で

ライセンスを取得する手順を示しています。

```
Switch_A_1# conf t
Switch_A_1(config)# interface fc1/2
Switch_A_1(config)# shut
Switch_A_1(config-if)# no port-license acquire
Switch_A_1(config-if)# exit
Switch_A_1(config)# interface fc1/1
Switch_A_1(config-if)# port-license
Switch_A_1(config-if)# port-license acquire
Switch_A_1(config-if)# no shut
Switch_A_1(config-if)# end
Switch_A_1# copy running-config startup-config

Switch_B_1# conf t
Switch_B_1(config)# interface fc1/2
Switch_B_1(config)# shut
Switch_B_1(config-if)# no port-license acquire
Switch_B_1(config-if)# exit
Switch_B_1(config)# interface fc1/1
Switch_B_1(config-if)# port-license
Switch_B_1(config-if)# port-license acquire
Switch_B_1(config-if)# no shut
Switch_B_1(config-if)# end
Switch_B_1# copy running-config startup-config
```

次の例は、ポートライセンスの使用状況を検証する方法を示しています。

```
Switch_A_1# show port-resources module 1
Switch_B_1# show port-resources module 1
```

#### Cisco MDS 9148 または 9148S スイッチでのポートの有効化

Cisco MDS 9148 または 9148S スイッチでは、MetroCluster 構成で必要なポートを手動で有効にする必要があります。

このタスクについて

- Cisco MDS 9148 または 9148S スイッチの 16 個のポートを手動で有効にできます。
- Cisco スイッチを使用すると、POD ライセンスをランダムなポートに適用することができますが、順番に適用することはできません。
- Cisco スイッチでは、12 個を超えるポートが必要な場合を除き、各ポートグループから 1 つのポートを使用する必要があります。

手順

1. Cisco スイッチで使用可能なポートグループを表示します。

```
'how port-resources module_blade_number_`
```

2. ポートグループの必要なポートにライセンスを付与して取得します。

```
'config t`
```

```
'interface_port_number_`
```

「小屋」

「ポートライセンス取得」

「no shut」のようになります

たとえば、次のコマンドシーケンスでは、fc 1/45 ポートがライセンス付与され、取得されます。

```
switch# config t
switch(config)#
switch(config)# interface fc 1/45
switch(config-if)#
switch(config-if)# shut
switch(config-if)# port-license acquire
switch(config-if)# no shut
switch(config-if)# end
```

3. 設定を保存します。

```
'copy running-config startup-config
```

### Cisco FC スイッチでの F ポートの設定

FC スイッチで F ポートを設定する必要があります。

このタスクについて

MetroCluster 構成では、F ポートとは、スイッチを HBA イニシエータ、FC-VI インターコネクト、および FC-to-SAS ブリッジに接続するポートです。

ポートはそれぞれ個別に設定する必要があります。

次のセクションを参照して、構成に応じた F ポート（スイッチからノード）を確認してください。

- ["FCスイッチのポート割り当て"](#)

このタスクは、MetroCluster 構成内のスイッチごとに実行する必要があります。

手順

1. コンフィギュレーションモードを開始します。

'config t'

2. ポートのインターフェイス構成モードに切り替えます。

'interface\_port-ID\_

3. ポートをシャットダウンします。

「ダウンタイム」

4. ポートを F モードに設定します。

「witchport mode F」

5. ポートを固定の速度に設定します。

'witchport speed\_speed - value\_

*speed-value* は '8000' または '16000' です

6. スイッチポートのレートモードを dedicated に設定します。

'witchport rate-mode dedicated (スイッチポートレートモード専用)

7. ポートを再起動します。

「シャットダウンなし」

8. 構成モードを終了します。

「end」と入力します

例

次の例は、2つのスイッチに対するコマンドを示しています。

```

Switch_A_1# config t
FC_switch_A_1(config)# interface fc 1/1
FC_switch_A_1(config-if)# shutdown
FC_switch_A_1(config-if)# switchport mode F
FC_switch_A_1(config-if)# switchport speed 8000
FC_switch_A_1(config-if)# switchport rate-mode dedicated
FC_switch_A_1(config-if)# no shutdown
FC_switch_A_1(config-if)# end
FC_switch_A_1# copy running-config startup-config

FC_switch_B_1# config t
FC_switch_B_1(config)# interface fc 1/1
FC_switch_B_1(config-if)# switchport mode F
FC_switch_B_1(config-if)# switchport speed 8000
FC_switch_B_1(config-if)# switchport rate-mode dedicated
FC_switch_B_1(config-if)# no shutdown
FC_switch_B_1(config-if)# end
FC_switch_B_1# copy running-config startup-config

```

**ISL** と同じポートグループ内の **F** ポートにバッファ間クレジットを割り当てます

F ポートが ISL と同じポートグループに含まれている場合は、バッファ間クレジットを割り当てる必要があります。必要なバッファ間クレジットがポートにない場合、ISL は動作しなくなる可能性があります。

このタスクについて

F ポートが ISL ポートと同じポートグループに含まれていない場合は、このタスクは必要ありません。

F ポートが ISL を含むポートグループに含まれている場合は、MetroCluster 構成内の FC スイッチごとにこのタスクを実行する必要があります。

手順

1. コンフィギュレーションモードを開始します。

```
'config t'
```

2. ポートのインターフェイス構成モードを設定します。

```
'interface port-ID_
```

3. ポートを無効にします。

```
「小屋」
```

4. ポートが F モードになっていない場合は、F モードに設定します。

```
「witchport mode F」
```

5. E ポート以外のバッファ間クレジットを 1 に設定します。

「witchport fcrxbbcredit 1」を参照してください

6. ポートを再度有効にします。

「no shut」のようになります

7. 構成モードを終了します。

「exit

8. 更新された設定をスタートアップ設定にコピーします。

'copy running-config startup-config

9. ポートに割り当てられているバッファ間クレジットを確認します。

'how port-resources module 1'

10. 構成モードを終了します。

「exit

11. ファブリック内のもう一方のスイッチで、上記の手順を繰り返します。

12. 設定を確認します。

'how port-resource module 1'

#### 例

この例では、ポート fc1/40 は ISL です。ポート fc1/37、fc1/38 および fc1/39 は同じポートグループに含まれているため、設定が必要です。

次のコマンドは、ポート範囲を fc1/37~fc1/39 に設定する場合を示しています。

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# interface fc1/37-39
FC_switch_A_1(config-if)# shut
FC_switch_A_1(config-if)# switchport mode F
FC_switch_A_1(config-if)# switchport fcrxbbcredit 1
FC_switch_A_1(config-if)# no shut
FC_switch_A_1(config-if)# exit
FC_switch_A_1# copy running-config startup-config

FC_switch_B_1# conf t
FC_switch_B_1(config)# interface fc1/37-39
FC_switch_B_1(config-if)# shut
FC_switch_B_1(config-if)# switchport mode F
FC_switch_B_1(config-if)# switchport fcrxbbcredit 1
FC_switch_A_1(config-if)# no shut
FC_switch_A_1(config-if)# exit
FC_switch_B_1# copy running-config startup-config
```

次のコマンドおよび出力は、設定が適切に適用されていることを示しています。

```

FC_switch_A_1# show port-resource module 1
...
Port-Group 11
  Available dedicated buffers are 93

-----
Interfaces in the Port-Group          B2B Credit  Bandwidth  Rate Mode
                                   Buffers      (Gbps)
-----
fc1/37                               32          8.0       dedicated
fc1/38                               1           8.0       dedicated
fc1/39                               1           8.0       dedicated
...

FC_switch_B_1# port-resource module
...
Port-Group 11
  Available dedicated buffers are 93

-----
Interfaces in the Port-Group          B2B Credit  Bandwidth  Rate Mode
                                   Buffers      (Gbps)
-----
fc1/37                               32          8.0       dedicated
fc1/38                               1           8.0       dedicated
fc1/39                               1           8.0       dedicated
...

```

### Cisco FC スイッチでの VSAN の作成および設定

MetroCluster 構成内の各 FC スイッチに、FC-VI ポート用の VSAN とストレージポート用の VSAN を 1 つずつ作成する必要があります。

このタスクについて

VSAN の番号と名前は一意である必要があります。フレームのインオーダー配信で 2 つの ISL を使用している場合は、追加の設定が必要です。

このタスクの例では、次の命名規則を使用します。

スイッチファブリック	VSAN 名	ID 番号
1.	FCVI_1_10	10.
STOR_1_20	20	2.

このタスクは FC スイッチファブリックごとに行う必要があります。

#### 手順

1. FC-VI VSAN を設定します。

- a. 構成モードを開始していない場合は、構成モードに切り替えます。

```
'config t'
```

- b. VSAN データベースを編集します。

```
「VSAN データベース」
```

- c. VSAN ID を設定します。

```
'vsan_vsan-ID_'
```

- d. VSAN 名を設定します。

```
'vsan_vsan-ID_VSAN_NAME_NAME_'
```

2. FC-VI VSAN にポートを追加します。

- a. VSAN の各ポートのインターフェイスを追加します。

```
'vsan_vsan-ID_interface_name_'
```

FC-VI VSAN に関しては、ローカル FC-VI ポートを接続するポートが追加されます。

- b. 構成モードを終了します。

```
「end」と入力します
```

- c. running-config を startup-config にコピーします。

```
'copy running-config startup-config'
```

次の例では、該当するポートは fc1/1 と fc1/13 です。

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# vsan database
FC_switch_A_1(config)# vsan 10 interface fc1/1
FC_switch_A_1(config)# vsan 10 interface fc1/13
FC_switch_A_1(config)# end
FC_switch_A_1# copy running-config startup-config
FC_switch_B_1# conf t
FC_switch_B_1(config)# vsan database
FC_switch_B_1(config)# vsan 10 interface fc1/1
FC_switch_B_1(config)# vsan 10 interface fc1/13
FC_switch_B_1(config)# end
FC_switch_B_1# copy running-config startup-config
```

### 3. VSAN のポートメンバーシップを確認します。

'How VSAN member' (VSAN メンバーの仕組み)

```
FC_switch_A_1# show vsan member
FC_switch_B_1# show vsan member
```

### 4. フレームのインオーダー配信またはアウトオブオーダー配信を保証するように VSAN を設定します。



標準の IOD 設定を推奨します。OOD を設定するのは必要な場合だけにしてください。

#### "ファブリック接続 MetroCluster 構成で TDM / WDM 機器を使用する場合の考慮事項"

◦ フレームのインオーダー配信を設定するには、次の手順を実行する必要があります。

i. コンフィギュレーションモードを開始します。

「conf t」

ii. VSAN の交換のインオーダー保証を有効にします。

inorder-guarantee vsan\_vsan-ID\_`



FC-VI VSAN (FCVI\_1\_10 および FCVI\_2\_30) については、フレームと交換のインオーダー保証を VSAN 10 でのみ有効にする必要があります。

iii. VSAN のロードバランシングを有効にします。

'vsan\_vsan-ID\_loadbalancing src-dst-id

iv. 構成モードを終了します。

「end」と入力します

v. running-config を startup-config にコピーします。

```
'copy running-config startup-config
```

FC\_switch\_A\_1 でフレームのインオーダー配信を設定するコマンドは次のとおりです。

```
FC_switch_A_1# config t
FC_switch_A_1(config)# in-order-guarantee vsan 10
FC_switch_A_1(config)# vsan database
FC_switch_A_1(config-vsan-db)# vsan 10 loadbalancing src-dst-id
FC_switch_A_1(config-vsan-db)# end
FC_switch_A_1# copy running-config startup-config
```

FC\_switch\_B\_1 でフレームのインオーダー配信を設定するコマンドは次のとおりです。

```
FC_switch_B_1# config t
FC_switch_B_1(config)# in-order-guarantee vsan 10
FC_switch_B_1(config)# vsan database
FC_switch_B_1(config-vsan-db)# vsan 10 loadbalancing src-dst-id
FC_switch_B_1(config-vsan-db)# end
FC_switch_B_1# copy running-config startup-config
```

◦ フレームのアウトオブオーダー配信を設定するには、次の手順を実行する必要があります。

i. コンフィギュレーションモードを開始します。

```
「conf t」
```

ii. VSAN の交換のインオーダー保証を無効にします。

```
'no in-order-guarantee VSAN_vsan-ID_
```

iii. VSAN のロードバランシングを有効にします。

```
'vsan_vsan-ID_loadbalancing src-dst-id
```

iv. 構成モードを終了します。

```
「end」と入力します
```

v. running-config を startup-config にコピーします。

```
'copy running-config startup-config
```

FC\_switch\_A\_1 でフレームのアウトオブオーダー配信を設定するコマンドは次のとおりです。

```
FC_switch_A_1# config t
FC_switch_A_1(config)# no in-order-guarantee vsan 10
FC_switch_A_1(config)# vsan database
FC_switch_A_1(config-vsan-db)# vsan 10 loadbalancing src-dst-id
FC_switch_A_1(config-vsan-db)# end
FC_switch_A_1# copy running-config startup-config
```

FC\_switch\_B\_1 でフレームのアウトオブオーダー配信を設定するコマンドは次のとおりです。

```
FC_switch_B_1# config t
FC_switch_B_1(config)# no in-order-guarantee vsan 10
FC_switch_B_1(config)# vsan database
FC_switch_B_1(config-vsan-db)# vsan 10 loadbalancing src-dst-id
FC_switch_B_1(config-vsan-db)# end
FC_switch_B_1# copy running-config startup-config
```

+



コントローラモジュールに ONTAP を設定する場合は、MetroCluster 構成の各コントローラモジュールで OOD を明示的に設定する必要があります。

#### "ONTAP ソフトウェアでのフレームのインオーダー配信またはアウトオブオーダー配信の設定"

##### 5. FC-VI VSAN の QoS ポリシーを設定します。

- a. コンフィギュレーションモードを開始します。

「conf t」

- b. 次のコマンドを続けて入力して、QoS をイネーブルにし、クラスマップを作成します。

「qos enable」と入力します

'qos class-map\_class\_name\_match-any'

- c. 前の手順で作成したクラスマップをポリシーマップに追加します。

'class\_class\_name\_`

- d. 優先度を設定します。

「優先度高」

- e. この手順で作成したポリシーマップに VSAN を追加します。

'qos service policy\_policy\_policy\_name\_vsan\_vsan-id\_`

- f. 更新された設定をスタートアップ設定にコピーします。

```
'copy running-config startup-config
```

FC\_switch\_A\_1 で QoS ポリシーを設定するコマンドは次のとおりです。

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# qos enable
FC_switch_A_1(config)# qos class-map FCVI_1_10_Class match-any
FC_switch_A_1(config)# qos policy-map FCVI_1_10_Policy
FC_switch_A_1(config-pmap)# class FCVI_1_10_Class
FC_switch_A_1(config-pmap-c)# priority high
FC_switch_A_1(config-pmap-c)# exit
FC_switch_A_1(config)# exit
FC_switch_A_1(config)# qos service policy FCVI_1_10_Policy vsan 10
FC_switch_A_1(config)# end
FC_switch_A_1# copy running-config startup-config
```

FC\_switch\_B\_1 で QoS ポリシーを設定するコマンドは次のとおりです。

```
FC_switch_B_1# conf t
FC_switch_B_1(config)# qos enable
FC_switch_B_1(config)# qos class-map FCVI_1_10_Class match-any
FC_switch_B_1(config)# qos policy-map FCVI_1_10_Policy
FC_switch_B_1(config-pmap)# class FCVI_1_10_Class
FC_switch_B_1(config-pmap-c)# priority high
FC_switch_B_1(config-pmap-c)# exit
FC_switch_B_1(config)# exit
FC_switch_B_1(config)# qos service policy FCVI_1_10_Policy vsan 10
FC_switch_B_1(config)# end
FC_switch_B_1# copy running-config startup-config
```

6. ストレージ VSAN を設定します。

a. VSAN ID を設定します。

```
'vsan_vsan-ID_`
```

b. VSAN 名を設定します。

```
'vsan_vsan-ID_VSAN_NAME_NAME_`
```

FC\_switch\_A\_1 でストレージ VSAN を設定するコマンドは次のとおりです。

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# vsan database
FC_switch_A_1(config-vsan-db)# vsan 20
FC_switch_A_1(config-vsan-db)# vsan 20 name STOR_1_20
FC_switch_A_1(config-vsan-db)# end
FC_switch_A_1# copy running-config startup-config
```

FC\_switch\_B\_1 でストレージ VSAN を設定するコマンドは次のとおりです。

```
FC_switch_B_1# conf t
FC_switch_B_1(config)# vsan database
FC_switch_B_1(config-vsan-db)# vsan 20
FC_switch_B_1(config-vsan-db)# vsan 20 name STOR_1_20
FC_switch_B_1(config-vsan-db)# end
FC_switch_B_1# copy running-config startup-config
```

#### 7. ストレージ VSAN にポートを追加します。

ストレージ VSAN に関しては、HBA または FC-to-SAS ブリッジを接続するすべてのポートを追加する必要があります。この例では、fc1/5、fc1/9、fc1/17、fc1/21、fc1/25、fc1/29、fc1/33、および fc1/37 が追加されます。

FC\_switch\_A\_1 でストレージ VSAN にポートを追加するコマンドは次のとおりです。

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# vsan database
FC_switch_A_1(config)# vsan 20 interface fc1/5
FC_switch_A_1(config)# vsan 20 interface fc1/9
FC_switch_A_1(config)# vsan 20 interface fc1/17
FC_switch_A_1(config)# vsan 20 interface fc1/21
FC_switch_A_1(config)# vsan 20 interface fc1/25
FC_switch_A_1(config)# vsan 20 interface fc1/29
FC_switch_A_1(config)# vsan 20 interface fc1/33
FC_switch_A_1(config)# vsan 20 interface fc1/37
FC_switch_A_1(config)# end
FC_switch_A_1# copy running-config startup-config
```

FC\_switch\_B\_1 でストレージ VSAN にポートを追加するコマンドは次のとおりです。

```

FC_switch_B_1# conf t
FC_switch_B_1(config)# vsan database
FC_switch_B_1(config)# vsan 20 interface fc1/5
FC_switch_B_1(config)# vsan 20 interface fc1/9
FC_switch_B_1(config)# vsan 20 interface fc1/17
FC_switch_B_1(config)# vsan 20 interface fc1/21
FC_switch_B_1(config)# vsan 20 interface fc1/25
FC_switch_B_1(config)# vsan 20 interface fc1/29
FC_switch_B_1(config)# vsan 20 interface fc1/33
FC_switch_B_1(config)# vsan 20 interface fc1/37
FC_switch_B_1(config)# end
FC_switch_B_1# copy running-config startup-config

```

E ポートを設定しています

ISL を接続するスイッチポート（E ポート）を設定する必要があります。

このタスクについて

使用する手順は、使用するスイッチによって異なります。

- [Cisco FC スイッチでの E ポートの設定](#)
- [Cisco 9250i FC スイッチのシングル ISL に対する FCIP ポートの設定](#)
- [Cisco 9250i FC スイッチのデュアル ISL に対する FCIP ポートの設定](#)

### Cisco FC スイッチでの E ポートの設定

スイッチ間リンク（ISL）を接続する FC スイッチポートを設定する必要があります。

このタスクについて

これらは E ポートであり、設定はポートごとに行う必要があります。そのためには、正しいバッファ間クレジット（BBC）数を計算する必要があります。

ファブリック内のすべての ISL を、同じ速度と同じ距離で設定する必要があります。

このタスクは ISL ポートごとに実行する必要があります。

手順

1. 次の表を使用して、可能なポート速度で調整された 1 km あたりの必要な BBC を確認します。

正しい BBC 数は、必要な調整済み BBC（下記の表で特定）に、スイッチ間の距離（km）を掛けて算出します。FC-VI のフレーミング動作に対応するために、1.5 の調整係数が必要です。

速度（Gbps）	1km あたりの必要な BBC	必要な調整済み BBC（1km あたりの BBC × 1.5）
1.	0.5	0.75

2.	1.	1.5
4.	2.	3.
8.	4.	6.
16	8.	12.

たとえば、4Gbps のリンクで 30km の距離に必要なクレジット数を算出するには、次の計算を行います。

- 「Gbps での速度」は 4 です
- 「必要な調整済み BBC」は 3
- 「スイッチ間の距離 (km)」は 30km です
- $3 \times 30 = 90$

a. コンフィギュレーションモードを開始します。

```
'config t'
```

b. 設定するポートを指定します。

```
'interface port-name_`'
```

c. ポートをシャットダウンします。

```
'ダウンタイム'
```

d. ポートのレートモードを「dedicated」に設定します。

```
'witchport rate-mode dedicated (スイッチポートレートモード専用)
```

e. ポートの速度を設定します。

```
'witchport speed_speed - value_`'
```

f. ポートのバッファ間クレジットを設定します。

```
'witchport fcrxbbcredit number_of_buffers'
```

g. ポートを E モードに設定します。

```
'witchport mode E'
```

h. ポートのトランクモードをイネーブルにします。

```
'witchport trunk mode on `'
```

i. ISL Virtual Storage Area Network (VSAN ; 仮想ストレージエリアネットワーク) をトランクに追加します。

'witchport トランクでは VSAN 10 を許可

```
'witchport trunk allowed vsan add 20'
```

- j. ポートをポートチャンネル 1 に追加します。

「channel-group 1」のようになります

- k. ファブリック内のパートナースイッチ上の対応する ISL ポートに対して、ここまでの手順を繰り返します。

次の例は、ポート fc1/41 を距離 30km、8Gbps で設定する場合を示しています。

```
FC_switch_A_1# conf t
FC_switch_A_1# shutdown
FC_switch_A_1# switchport rate-mode dedicated
FC_switch_A_1# switchport speed 8000
FC_switch_A_1# switchport fcrxbbcredit 60
FC_switch_A_1# switchport mode E
FC_switch_A_1# switchport trunk mode on
FC_switch_A_1# switchport trunk allowed vsan 10
FC_switch_A_1# switchport trunk allowed vsan add 20
FC_switch_A_1# channel-group 1
fc1/36 added to port-channel 1 and disabled

FC_switch_B_1# conf t
FC_switch_B_1# shutdown
FC_switch_B_1# switchport rate-mode dedicated
FC_switch_B_1# switchport speed 8000
FC_switch_B_1# switchport fcrxbbcredit 60
FC_switch_B_1# switchport mode E
FC_switch_B_1# switchport trunk mode on
FC_switch_B_1# switchport trunk allowed vsan 10
FC_switch_B_1# switchport trunk allowed vsan add 20
FC_switch_B_1# channel-group 1
fc1/36 added to port-channel 1 and disabled
```

- l. 問題：両方のスイッチで次のコマンドを実行してポートを再起動します。

「シャットダウンなし」

- m. ファブリック内の他の ISL ポートに対して、ここまでの手順を繰り返します。  
n. 同じファブリック内の両方のスイッチで、ネイティブ VSAN をポートチャンネルインターフェイスに追加します。

```
'interface port-channel_number_
```

```
'witchport トランク許可 VSAN add_native_san_id_
```

o. ポートチャネルの設定を確認します。

```
'show interface port-channel_number
```

ポートチャネルの属性は次のとおりです。

- ポートチャネルの状態は「trunking」です。
- 管理ポートモードは E、トランクモードはオンです。
- 速度は、すべての ISL リンク速度の累積値です。

たとえば、2つの ISL ポートが 4Gbps で動作している場合は 8Gbps です。

- 「Trunk vsans (admin allowed and active)」には、許可されているすべての VSAN が表示されます。
- 「Trunk vsans (up)」は、許可されているすべての VSAN を表示します。
- メンバーリストには、port-channel に追加されたすべての ISL ポートを表示。
- ポート VSAN の番号は、ISL を含む VSAN と同じ（通常はネイティブの vsan 1）。

```

FC_switch_A_1(config-if)# show int port-channel 1
port-channel 1 is trunking
  Hardware is Fibre Channel
  Port WWN is 24:01:54:7f:ee:e2:8d:a0
  Admin port mode is E, trunk mode is on
  snmp link state traps are enabled
  Port mode is TE
  Port vsan is 1
  Speed is 8 Gbps
  Trunk vsans (admin allowed and active) (1,10,20)
  Trunk vsans (up) (1,10,20)
  Trunk vsans (isolated) ()
  Trunk vsans (initializing) ()
  5 minutes input rate 1154832 bits/sec,144354 bytes/sec, 170
frames/sec
  5 minutes output rate 1299152 bits/sec,162394 bytes/sec, 183
frames/sec
  535724861 frames input,1069616011292 bytes
    0 discards,0 errors
    0 invalid CRC/FCS,0 unknown class
    0 too long,0 too short
  572290295 frames output,1144869385204 bytes
    0 discards,0 errors
  5 input OLS,11 LRR,2 NOS,0 loop inits
  14 output OLS,5 LRR, 0 NOS, 0 loop inits
Member[1] : fc1/36
Member[2] : fc1/40
Interface last changed at Thu Oct 16 11:48:00 2014

```

- a. 両方のスイッチでインターフェイス設定を終了します。

「end」と入力します

- b. 両方のファブリックで、更新された設定をスタートアップ設定にコピーします。

'copy running-config startup-config

```

FC_switch_A_1(config-if)# end
FC_switch_A_1# copy running-config startup-config

FC_switch_B_1(config-if)# end
FC_switch_B_1# copy running-config startup-config

```

- a. 2つ目のスイッチファブリックで、ここまでの手順を繰り返します。

## 関連情報

FCスイッチをケーブル接続するときは、指定のポート割り当てを使用していることを確認する必要があります。参照["FCスイッチのポート割り当て"](#)

### Cisco 9250i FC スwitchのシングル ISL に対する FCIP ポートの設定

FCIP プロファイルとインターフェイスを作成して IPStorage1/1 GbE インターフェイスに割り当てることで、ISL を接続する FCIP スwitchポート（E ポート）を設定する必要があります。

このタスクについて

このタスクは、各スイッチが IPStorage1/1 インターフェイスを使用し、スイッチファブリックごとに 1 つの ISL を使用する構成にのみ該当します。

このタスクは FC スwitchごとに行う必要があります。

各スイッチに 2 つの FCIP プロファイルを作成します。

- ファブリック 1
  - FC\_switch\_A\_1 で FCIP プロファイル 11 および 111 を設定します。
  - FC\_switch\_B\_1 で FCIP プロファイル 12 および 121 を設定します。
- ファブリック 2
  - FC\_switch\_A\_2 で FCIP プロファイル 13 および 131 を設定しています。
  - FC\_switch\_B\_2 に FCIP プロファイル 14 および 141 を設定します。

## 手順

1. コンフィギュレーションモードを開始します。

```
'config t'
```

2. FCIP を有効にします。

```
「機能 FCIP」
```

3. IPStorage1/1 GbE インターフェイスを設定します。

- a. コンフィギュレーションモードを開始します。

```
「 conf t」
```

- b. IPStorage1/1 インターフェイスを指定します。

```
インターフェイス IPStorage1/1
```

- c. IP アドレスとサブネットマスクを指定します。

```
'interface_ip-address__subnet-mask_」
```

- d. MTU サイズを 2500 に指定します。

```
'witchport mtu 2500」
```

e. ポートを有効にします。

「シャットダウンなし」

f. 構成モードを終了します。

「 exit

次の例は、 IPStorage1/1 ポートの設定を示しています。

```
conf t
interface IPStorage1/1
  ip address 192.168.1.201 255.255.255.0
  switchport mtu 2500
  no shutdown
exit
```

4. FC-VI トラフィック用の FCIP プロファイルを設定します。

a. FCIP プロファイルを設定し、 FCIP プロファイル構成モードに切り替えます。

FCIP profile\_fcip -profile-name\_`

プロファイル名は、設定するスイッチによって異なります。

b. IPStorage1/1 インターフェイスの IP アドレスを FCIP プロファイルに割り当てます。

「 ip address\_ip-address\_`」

c. FCIP プロファイルを TCP ポート 3227 に割り当てます。

ポート 3227`

d. TCP を設定します。

「 tcp keepalive-timeout 1 」を参照してください

「 tcp max-retransmissions3 」

「 m ax-bandwidth-mbs 5000 minavailable-bandwidth-mbs 4500 round-trip -time-ms 3 」を参照してください

「 tcp min-retransmit-time 200 」

「 tcp keepalive-timeout 1 」を参照してください

tcp pmtu-enable reset-timeout 3600

「 tcp sack -enable 」 「 no tcp cwm 」を選択します

次の例は、FCIP プロファイルの設定を示しています。

```
conf t
fcip profile 11
  ip address 192.168.1.333
  port 3227
  tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-
time-ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
no tcp cwm
```

5. ストレージトラフィック用の FCIP プロファイルを設定します。

a. 111 という名前で FCIP プロファイルを設定し、FCIP プロファイル構成モードに切り替えます。

FCIP プロファイル 111'

b. IPStorage1/1 インターフェイスの IP アドレスを FCIP プロファイルに割り当てます。

「 ip address\_ip-address\_` 」

c. FCIP プロファイルを TCP ポート 3229 に割り当てます。

ポート 3229`

d. TCP を設定します。

「 tcp keepalive-timeout 1 」を参照してください

「 tcp max-retransmissions3 」

「 m ax-bandwidth-mbs 5000 minavailable-bandwidth-mbs 4500 round-trip -time-ms 3 」を参照してください

「 tcp min-retransmit-time 200 」

「 tcp keepalive-timeout 1 」を参照してください

tcp pmtu-enable reset-timeout 3600

「 tcp sack -enable 」 「 no tcp cwm 」を選択します

次の例は、FCIP プロファイルの設定を示しています。

```
conf t
fcip profile 111
  ip address 192.168.1.334
  port 3229
  tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-
time-ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
no tcp cwm
```

6. 2つのうちの1つ目のFCIPインターフェイスを作成します。

インターフェイス fcip 1'

このインターフェイスはFC-IVトラフィックに使用します。

- a. 前の手順で作成したプロファイル 11 を選択します。

「USE - profile 11`」

- b. パートナースイッチのIPStorage1/1 ポートのIPアドレスとポート番号を設定します。

'peer-info ipaddr\_partner-switch-port-ip\_port 3227'

- c. TCP 接続 2 を選択します。

「tcp-connection 2」

- d. 圧縮を無効にします。

「IP 圧縮なし」

- e. インターフェイスを有効にします。

「シャットダウンなし」

- f. 制御TCP接続を48、データ接続を26に設定して、そのDifferentiated Services Code Point (DSCP) 値のすべてのパケットをマークします。

'qos control 48 data 26`

- g. インターフェイスコンフィギュレーションモードを終了します。

「exit

次の例は、FCIP インターフェイスの設定を示しています。

```
interface fcip 1
  use-profile 11
  # the port # listed in this command is the port that the remote switch
  is listening on
  peer-info ipaddr 192.168.32.334 port 3227
  tcp-connection 2
  no ip-compression
  no shutdown
  qos control 48 data 26
exit
```

7. 2つのうちの2つ目のFCIP インターフェイスを作成します。

「interface fcip 2」と入力します

このインターフェイスはストレージトラフィックに使用されます。

a. 前の手順で作成したプロファイル 111 を選択します。

'USE - profile 111'

b. パートナースイッチの IPStorage1/1 ポートの IP アドレスとポート番号を設定します。

'peer-info ipaddr\_partner-switch-port-ip\_port 3229'

c. TCP 接続 2 を選択します。

「tcp-connection 5」

d. 圧縮を無効にします。

「IP 圧縮なし」

e. インターフェイスを有効にします。

「シャットダウンなし」

f. 制御 TCP 接続を 48、データ接続を 26 に設定して、その Differentiated Services Code Point (DSCP) 値のすべてのパケットをマークします。

'qos control 48 data 26'

g. インターフェイスコンフィギュレーションモードを終了します。

「exit」

次の例は、FCIP インターフェイスの設定を示しています。

```
interface fcip 2
  use-profile 11
# the port # listed in this command is the port that the remote switch
is listening on
  peer-info ipaddr 192.168.32.33e port 3229
  tcp-connection 5
  no ip-compression
  no shutdown
  qos control 48 data 26
exit
```

8. FCIP 1 インターフェイスのスイッチポートを設定します。

- a. コンフィギュレーションモードを開始します。

```
'config t'
```

- b. 設定するポートを指定します。

```
インターフェイス fcip 1'
```

- c. ポートをシャットダウンします。

```
「ダウンタイム」
```

- d. ポートを E モードに設定します。

```
'witchport mode E'
```

- e. ポートのトランクモードをイネーブルにします。

```
'witchport trunk mode on `
```

- f. トランクで許可される VSAN を 10 に設定します。

```
'witchport トランクでは VSAN 10 を許可
```

- g. ポートの速度を設定します。

```
'witchport speed_speed - value_
```

9. FCIP 2 インターフェイスのスイッチポートを設定します。

- a. コンフィギュレーションモードを開始します。

```
'config t'
```

- b. 設定するポートを指定します。

```
「 interface fcip 2 」 と入力します
```

c. ポートをシャットダウンします。

「ダウンタイム」

d. ポートを E モードに設定します。

'witchport mode E`

e. ポートのトランクモードをイネーブルにします。

'witchport trunk mode on`

f. トランクで許可される VSAN を 20 に設定します。

「witchport trunk allowed vsan 20`」

g. ポートの速度を設定します。

'witchport speed\_speed - value\_`

10. 2 つ目のスイッチで、上記の手順を繰り返します。

ただし、適切な IP アドレスと一意の FCIP プロファイル名を使用してください。

- 1 つ目のスイッチファブリックの設定では、FC\_switch\_B\_1 で FCIP プロファイル 12 および 121 を設定します。
- 1 つ目のスイッチファブリックの設定では、FC\_switch\_A\_2 で FCIP プロファイル 13 および 131 を設定し、FC\_switch\_B\_2 で FCIP プロファイル 14 および 141 を設定します。

11. 両方のスイッチでポートを再起動します。

「シャットダウンなし」

12. 両方のスイッチでインターフェイス設定を終了します。

「end」と入力します

13. 両方のスイッチで、更新された設定をスタートアップ設定にコピーします。

'copy running-config startup-config

```
FC_switch_A_1(config-if)# end
FC_switch_A_1# copy running-config startup-config

FC_switch_B_1(config-if)# end
FC_switch_B_1# copy running-config startup-config
```

14. 2 つ目のスイッチファブリックで、ここまでの手順を繰り返します。

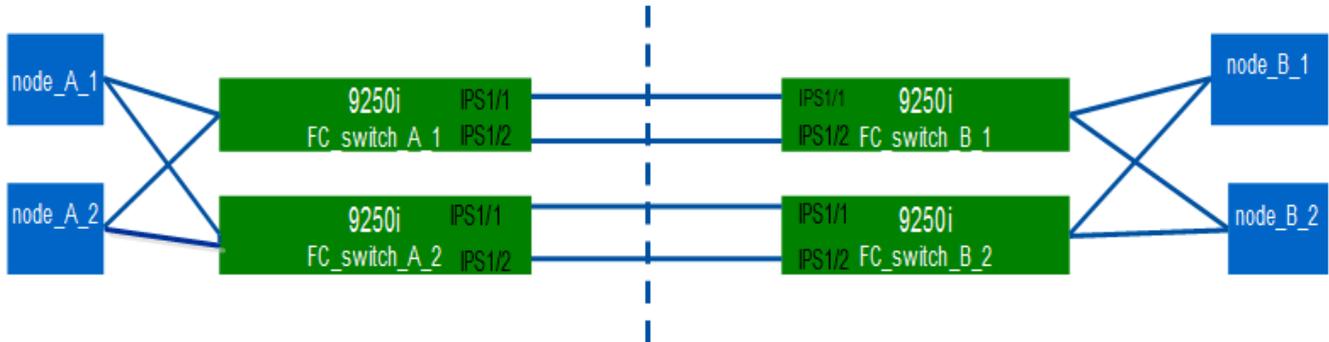
## Cisco 9250i FC スイッチのデュアル ISL に対する FCIP ポートの設定

FCIP プロファイルとインターフェイスを作成して IPStorage1/1 および IPStorage1/2 GbE インターフェイスに割り当てることで、ISL を接続する FCIP スイッチポート（E ポート）を設定する必要があります。

このタスクについて

このタスクは、各スイッチで IPStorage1/1 および IPStorage1/2 GbE インターフェイスを使用し、スイッチファブリックごとに 2 つの ISL を使用する構成にのみ該当します。

このタスクは FC スイッチごとに行う必要があります。



このタスクと例で使用するプロファイル設定の表は次のとおりです。

- [\[fabric1\\_table\]](#)
- [\[fabric2\\_table\]](#)
- ファブリック 1 プロファイル設定表 \*

スイッチ ファブリック	IPStorage インター フェイス	IP アドレ ス	ポートタ イプ	FCIP イン ターフェ イス	FCIP プロ ファイル	ポート	IP/port を ピアリン グします	VSAN ID
FC_switch _A_1 を使 用します	IPStorage 1/1	1. a. a. a.	FC-VI	FCIP 1.	15	3220	1. c. c. c/3230	10.
ストレ ージ	FCIP 2.	20	3221	1. c. c. c/3231	20	IPStorage 1/2	b.b.b.b.b .b.b.b	FC-VI
FCIP 3.	25	3222	1. d d / 3232	10.	ストレ ージ	FCIP 4.	30	3223
1. d d / 3233	20	FC_switch _B_1	IPStorage 1/1	c.c.c	FC-VI	FCIP 1.	15	3230
A.a.a/3220 の例	10.	ストレ ージ	FCIP 2.	20	3231	1. a. a/ 3221	20	IPStorage 1/2
d.d.d.d	FC-VI	FCIP 3.	25	3232	1. b. b. b b/3222	10.	ストレ ージ	FCIP 4.

• ファブリック 2 プロファイル設定表 \*

スイッチ ファブリック	IPStorage インター フェイス	IP アドレ ス	ポートタ イプ	FCIP イン ターフェ イス	FCIP プロ ファイル	ポート	IP/port を ピアリン グします	VSAN ID
FC_switch _A_2	IPStorage 1/1	e.e	FC-VI	FCIP 1.	15	3220	G.G.g/323 0	10.
ストレージ	FCIP 2.	20	3221	G.gg/3231	20	IPStorage 1/2	f.f.f.f.f	FC-VI
FCIP 3.	25	3222	H.H/3232	10.	ストレージ	FCIP 4.	30	3223
H.H/3233	20	FC_switch _B_2	IPStorage 1/1	g.g.g.g.g	FC-VI	FCIP 1.	15	3230
例： /3220	10.	ストレージ	FCIP 2.	20	3231	例： 3221	20	IPStorage 1/2
h.h.h.h	FC-VI	FCIP 3.	25	3232	1. f. f. /3222	10.	ストレージ	FCIP 4.

手順

1. コンフィギュレーションモードを開始します。

```
'config t'
```

2. FCIP を有効にします。

```
「機能 FCIP」
```

3. 各スイッチで、2つの IPStorage インターフェイス（「IPStorage1/1」および「IPStorage1/2」）を設定します。

- a. [a] 構成モードに切り替えます：

```
「 conf t」
```

- b. 作成する IPStorage インターフェイスを指定します。

```
'interface_ipstorage_」
```

*IPstorage* パラメータ値は "IPStorage1/1" または "IPStorage1/2" です

- c. 前の手順で指定した IPStorage インターフェイスの IP アドレスとサブネットマスクを指定します。

```
'interface_ip-address__subnet-mask_」
```



各スイッチで、IPStorage インターフェイス「IPStorage1/1」と「IPStorage1/2」には異なる IP アドレスを指定する必要があります。

- a. MTU サイズを 2500 に指定します。

```
'witchport mtu 2500'
```

- b. ポートを有効にします。

```
「シャットダウンなし」
```

- c. [[suf, 手順 "f"] 構成モードを終了します。

```
「 exit
```

- d. 繰り返します [substep\_a] から [substep\_f] IPStorage1/2 GbE インターフェイスを別の IP アドレスで設定します。

4. プロファイル設定の表に記載されたプロファイル名を使用して、FC-VI トラフィック用とストレージトラフィック用の FCIP プロファイルを設定します。

- a. コンフィギュレーションモードを開始します。

```
「 conf t`
```

- b. 次のプロファイル名で FCIP プロファイルを設定します。

```
FCIP profile_fcip -profile-name_`
```

次に '*fcip -profile-name*' パラメータの値を示します

- IPStorage1/1 の FC-VI : 15
- IPStorage1/1 のストレージ : 20
- IPStorage1/2 上の FC-VI は 25 です
- IPStorage1/2 にストレージを指定した場合は 30 個

- c. プロファイル設定の表に従って、FCIP プロファイルのポートを割り当てます。

```
「 port_port_number_` 」のようになります
```

- d. TCP を設定します。

```
「 tcp keepalive-timeout 1 」を参照してください
```

```
「 tcp max-retransmissions3 」
```

```
「 m ax-bandwidth-mbs 5000 minavailable-bandwidth-mbs 4500 round-trip -time-ms 3 」を参照してください
```

```
「 tcp min-retransmit-time 200 」
```

```
「 tcp keepalive-timeout 1 」を参照してください
```

```
tcp pmtu-enable reset-timeout 3600
```

「 tcp sack-enable 」を入力します

「 no tcp CWM 」

5. FCIP インターフェイスを作成します。

```
interface fcp_fcp_interface_`
```

パラメータの値は '*fcp\_interface*' で ' プロファイル設定テーブルに表示されているように '1' '2' '3' または '4' です

- a. 前の手順で作成したプロファイルにインターフェイスをマッピングします。

```
'use-profile_profile_`
```

- b. ピア IP アドレスとピアプロファイルポート番号を設定します。

```
'peer-info_peer_ipstorage_ipaddr_port_peer_port_port_number_`
```

- c. TCP 接続を選択します。

```
「 tcp-connection_connection-#_ 」
```

パラメータの値は 'FC-VI プロファイルの場合は 2' ストレージ・プロファイルの場合は 5' です

- a. 圧縮を無効にします。

```
「 IP 圧縮なし」
```

- b. インターフェイスを有効にします。

```
「シャットダウンなし」
```

- c. 制御 TCP 接続を 「 48 」 に設定し、データ接続を 「 26 」 に設定して、 DSCP 値が異なるすべてのパケットをマークします。

```
'qos control 48 data 26`
```

- d. 構成モードを終了します。

```
「 exit
```

6. 各 FCIP インターフェイスのスイッチポートを設定します。

- a. コンフィギュレーションモードを開始します。

```
'config t`
```

- b. 設定するポートを指定します。

```
インターフェイス fcp 1'
```

c. ポートをシャットダウンします。

```
「ダウンタイム」
```

d. ポートを E モードに設定します。

```
'witchport mode E'
```

e. ポートのトランクモードをイネーブルにします。

```
'witchport trunk mode on '
```

f. 特定の VSAN で許可されるトランクを指定します。

```
'witchport trunk allowed vsan_vsan_id_'
```

`_vsan_id_parameter` 値は 'FC-VI プロファイルの場合は「VSAN 10」' ストレージ・プロファイルの場合は「VSAN 20」です

a. ポートの速度を設定します。

```
'witchport speed_speed - value_'
```

b. 構成モードを終了します。

```
「exit
```

7. 両方のスイッチで、更新された設定をスタートアップ設定にコピーします。

```
'copy running-config startup-config
```

次の例は、ファブリック 1 のスイッチ FC\_switch\_A\_1 および FC\_switch\_B\_1 で 2 つの ISL を使用する場合の FCIP ポートの設定を示しています。

• FC\_switch\_A\_1 では、次のコマンドを実行します。

```
FC_switch_A_1# config t
FC_switch_A_1(config)# no in-order-guarantee vsan 10
FC_switch_A_1(config-vsan-db)# end
FC_switch_A_1# copy running-config startup-config

# fcip settings

feature fcip

conf t
interface IPStorage1/1
# IP address: a.a.a.a
# Mask: y.y.y.y
ip address <a.a.a.a y.y.y.y>
```

```

switchport mtu 2500
no shutdown
exit
conf t
fcip profile 15
  ip address <a.a.a.a>
  port 3220
  tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm

conf t
fcip profile 20
  ip address <a.a.a.a>
  port 3221
  tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm

conf t
interface IPStorage1/2
# IP address: b.b.b.b
# Mask: y.y.y.y
  ip address <b.b.b.b y.y.y.y>
  switchport mtu 2500
  no shutdown
exit

conf t
fcip profile 25
  ip address <b.b.b.b>
  port 3222
tcp keepalive-timeout 1
tcp max-retransmissions 3

```

```

max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm

conf t
fcip profile 30
  ip address <b.b.b.b>
  port 3223
tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm
interface fcip 1
  use-profile 15
# the port # listed in this command is the port that the remote switch is
listening on
  peer-info ipaddr <c.c.c.c> port 3230
  tcp-connection 2
  no ip-compression
  no shutdown
  qos control 48 data 26
exit

interface fcip 2
  use-profile 20
# the port # listed in this command is the port that the remote switch is
listening on
  peer-info ipaddr <c.c.c.c> port 3231
  tcp-connection 5
  no ip-compression
  no shutdown
  qos control 48 data 26
exit

interface fcip 3
  use-profile 25
# the port # listed in this command is the port that the remote switch is

```

```
listening on
peer-info ipaddr < d.d.d.d > port 3232
tcp-connection 2
no ip-compression
no shutdown
qos control 48 data 26
exit

interface fcip 4
use-profile 30
# the port # listed in this command is the port that the remote switch is
listening on
peer-info ipaddr < d.d.d.d > port 3233
tcp-connection 5
no ip-compression
no shutdown
qos control 48 data 26
exit

conf t
interface fcip 1
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 10
no shutdown
exit

conf t
interface fcip 2
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 20
no shutdown
exit

conf t
interface fcip 3
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 10
no shutdown
exit
```

```
conf t
interface fcip 4
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 20
no shutdown
exit
```

• FC\_switch\_B\_1の場合:

```
FC_switch_A_1# config t
FC_switch_A_1(config)# in-order-guarantee vsan 10
FC_switch_A_1(config-vsan-db)# end
FC_switch_A_1# copy running-config startup-config

# fcip settings

feature fcip

conf t
interface IPStorage1/1
# IP address: c.c.c.c
# Mask: y.y.y.y
ip address <c.c.c.c y.y.y.y>
switchport mtu 2500
no shutdown
exit

conf t
fcip profile 15
ip address <c.c.c.c>
port 3230
tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
tcp min-retransmit-time 200
tcp keepalive-timeout 1
tcp pmtu-enable reset-timeout 3600
tcp sack-enable
no tcp cwm

conf t
fcip profile 20
```

```

ip address <c.c.c.c>
port 3231
tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
tcp min-retransmit-time 200
tcp keepalive-timeout 1
tcp pmtu-enable reset-timeout 3600
tcp sack-enable
no tcp cwm

conf t
interface IPStorage1/2
# IP address: d.d.d.d
# Mask: y.y.y.y
ip address <b.b.b.b y.y.y.y>
switchport mtu 2500
no shutdown
exit

conf t
fcip profile 25
ip address <d.d.d.d>
port 3232
tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
tcp min-retransmit-time 200
tcp keepalive-timeout 1
tcp pmtu-enable reset-timeout 3600
tcp sack-enable
no tcp cwm

conf t
fcip profile 30
ip address <d.d.d.d>
port 3233
tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
tcp min-retransmit-time 200
tcp keepalive-timeout 1
tcp pmtu-enable reset-timeout 3600

```

```

tcp sack-enable
no tcp cwm

interface fcip 1
  use-profile 15
# the port # listed in this command is the port that the remote switch is
listening on
  peer-info ipaddr <a.a.a.a> port 3220
  tcp-connection 2
  no ip-compression
  no shutdown
  qos control 48 data 26
exit

interface fcip 2
  use-profile 20
# the port # listed in this command is the port that the remote switch is
listening on
  peer-info ipaddr <a.a.a.a> port 3221
  tcp-connection 5
  no ip-compression
  no shutdown
  qos control 48 data 26
exit

interface fcip 3
  use-profile 25
# the port # listed in this command is the port that the remote switch is
listening on
  peer-info ipaddr < b.b.b.b > port 3222
  tcp-connection 2
  no ip-compression
  no shutdown
  qos control 48 data 26
exit

interface fcip 4
  use-profile 30
# the port # listed in this command is the port that the remote switch is
listening on
  peer-info ipaddr < b.b.b.b > port 3223
  tcp-connection 5
  no ip-compression
  no shutdown
  qos control 48 data 26
exit

```

```
conf t
interface fcip 1
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 10
no shutdown
exit
```

```
conf t
interface fcip 2
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 20
no shutdown
exit
```

```
conf t
interface fcip 3
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 10
no shutdown
exit
```

```
conf t
interface fcip 4
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 20
no shutdown
exit
```

### Cisco FC スイッチでゾーニングを設定する

スイッチポートを別々のゾーンに割り当てて、ストレージ（HBA）とコントローラ（FC-VI）のトラフィックを分離する必要があります。

このタスクについて

この手順は、両方の FC スイッチファブリックで実行する必要があります。

次の手順では、「4 ノード MetroCluster 構成の FibreBridge 7500N のゾーニング」セクションで説明されているゾーニングを使用します。

## 手順

1. 既存のゾーンとゾーンセットがある場合は消去します。

a. アクティブなゾーンおよびゾーンセットを特定します。

「ゾーンセットのアクティブ化」

```
FC_switch_A_1# show zoneset active  
  
FC_switch_B_1# show zoneset active
```

b. 前の手順で特定したアクティブなゾーンセットを無効にします。

```
'no zoneset activate name_vszone_name_vsan_vsan_id'
```

次の例は、2つのゾーンセットを無効にする方法を示しています。

- VSAN 10 内の FC\_switch\_A\_1 の ZoneSet\_A
- VSAN 20 内の FC\_switch\_B\_1 の ZoneSet\_B

```
FC_switch_A_1# no zoneset activate name ZoneSet_A vsan 10  
  
FC_switch_B_1# no zoneset activate name ZoneSet_B vsan 20
```

c. すべてのゾーンセットが非アクティブになったら、ゾーンデータベースをクリアします。

```
clear zone database-zone-name_`
```

```
FC_switch_A_1# clear zone database 10  
FC_switch_A_1# copy running-config startup-config  
  
FC_switch_B_1# clear zone database 20  
FC_switch_B_1# copy running-config startup-config
```

2. スイッチのワールドワイド名（WWN）を取得します。

```
'How WWN switch`
```

3. ゾーンの基本設定を行います。

a. デフォルトのゾーニング・ポリシーを "permit" に設定します

```
no system default zone default-zone permit
```

b. フルゾーン配信を有効にします。

「システムデフォルトゾーンは完全に配布」

- c. VSAN ごとにデフォルトのゾーニングポリシーを設定します。

```
no zone default-zone permit_vsanId_`
```

- d. VSAN ごとにデフォルトのフルゾーン配信を設定します。

```
zoneset distribute full_vsanId_`
```

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# no system default zone default-zone permit
FC_switch_A_1(config)# system default zone distribute full
FC_switch_A_1(config)# no zone default-zone permit 10
FC_switch_A_1(config)# no zone default-zone permit 20
FC_switch_A_1(config)# zoneset distribute full vsan 10
FC_switch_A_1(config)# zoneset distribute full vsan 20
FC_switch_A_1(config)# end
FC_switch_A_1# copy running-config startup-config

FC_switch_B_1# conf t
FC_switch_B_1(config)# no system default zone default-zone permit
FC_switch_B_1(config)# system default zone distribute full
FC_switch_B_1(config)# no zone default-zone permit 10
FC_switch_B_1(config)# no zone default-zone permit 20
FC_switch_B_1(config)# zoneset distribute full vsan 10
FC_switch_B_1(config)# zoneset distribute full vsan 20
FC_switch_B_1(config)# end
FC_switch_B_1# copy running-config startup-config
```

4. ストレージゾーンを作成し、ストレージポートを追加します。



次の手順は、ファブリックごとに1つのスイッチだけで実行します。

ゾーニングは、使用している FC-to-SAS ブリッジのモデルによって異なります。詳細については、ブリッジのモデルに対応するセクションを参照してください。例では Brocade スイッチポートを使用しているため、適宜ポートを調整してください。

- "1つのFCポートを使用する FibreBridge 7500N / 7600Nブリッジのゾーニング"
- "両方の FC ポートを使用する FibreBridge 7500N ブリッジのゾーニング"

各ストレージゾーンには、すべてのコントローラの HBA イニシエータポートと、FC-to-SAS ブリッジを接続するポートが1つ含まれます。

- a. ストレージゾーンを作成します。

```
'zone name_STOR-zone-name_vsanId_`
```

- b. ストレージポートをゾーンに追加します。

「member-portswitch WWN」というエラーが表示されます

- c. ゾーンセットをアクティブにします。

```
zoneset activate name_STOR-zone-name-setname_vsan_vsan-id_`
```

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# zone name STOR_Zone_1_20_25 vsan 20
FC_switch_A_1(config-zone)# member interface fc1/5 swwn
20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# member interface fc1/9 swwn
20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# member interface fc1/17 swwn
20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# member interface fc1/21 swwn
20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# member interface fc1/5 swwn
20:00:00:05:9b:24:12:99
FC_switch_A_1(config-zone)# member interface fc1/9 swwn
20:00:00:05:9b:24:12:99
FC_switch_A_1(config-zone)# member interface fc1/17 swwn
20:00:00:05:9b:24:12:99
FC_switch_A_1(config-zone)# member interface fc1/21 swwn
20:00:00:05:9b:24:12:99
FC_switch_A_1(config-zone)# member interface fc1/25 swwn
20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# end
FC_switch_A_1# copy running-config startup-config
```

5. ストレージ・ゾーン・セットを作成し'新しいセットにストレージ・ゾーンを追加します



ファブリック内の1つのスイッチだけで、次の手順を実行します。

- a. ストレージゾーンセットを作成します。

```
zoneset name_STOR-zone-set-name_vsan_vsan-id_`
```

- b. ストレージゾーンをゾーンセットに追加します。

「member\_STOR-zone-name\_`」

- c. ゾーンセットをアクティブにします。

```
zoneset activate name_STOR-zone-set-name_vsanId_`
```

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# zoneset name STORI_Zoneset_1_20 vsan 20
FC_switch_A_1(config-zoneset)# member STOR_Zone_1_20_25
...
FC_switch_A_1(config-zoneset)# exit
FC_switch_A_1(config)# zoneset activate name STOR_ZoneSet_1_20 vsan 20
FC_switch_A_1(config)# exit
FC_switch_A_1# copy running-config startup-config
```

## 6. FCVI ゾーンを作成して、FCVI ポートを追加します。

各 FCVI ゾーンには、1つの DR グループのすべてのコントローラから FCVI ポートが含まれます。



ファブリック内の1つのスイッチだけで、次の手順を実行します。

ゾーニングは、使用している FC-to-SAS ブリッジのモデルによって異なります。詳細については、ブリッジのモデルに対応するセクションを参照してください。例では Brocade スイッチポートを使用しているため、適宜ポートを調整してください。

- "1つのFCポートを使用するFibreBridge 7500N / 7600Nブリッジのゾーニング"
- "両方の FC ポートを使用する FibreBridge 7500N ブリッジのゾーニング"

各ストレージゾーンには、すべてのコントローラの HBA イニシエータポートと、FC-to-SAS ブリッジを接続するポートが1つ含まれます。

### a. FCVI ゾーンを作成します。

```
'zone name_FCVI-zone-name_vsanId_`
```

### b. FCVI ポートをゾーンに追加します。

```
「 member_fcvi -zone-name_` 」
```

### c. ゾーンセットをアクティブにします。

```
zoneset activate name_FCVI-zone-name-set-name_vsanId_`
```

```

FC_switch_A_1# conf t
FC_switch_A_1(config)# zone name FCVI_Zone_1_10_25 vsan 10
FC_switch_A_1(config-zone)# member interface fc1/1
swwn20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# member interface fc1/2
swwn20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# member interface fc1/1
swwn20:00:00:05:9b:24:12:99
FC_switch_A_1(config-zone)# member interface fc1/2
swwn20:00:00:05:9b:24:12:99
FC_switch_A_1(config-zone)# end
FC_switch_A_1# copy running-config startup-config

```

7. FCVI ゾーンセットを作成して、FCVI ゾーンを追加します。



ファブリック内の1つのスイッチだけで、次の手順を実行します。

a. FCVI ゾーンセットを作成します。

```
zoneset name_FCVI_zone_set_name_VSAN_vsan-id_`
```

b. FCVI ゾーンをゾーンセットに追加します。

```
「 member_FCVI_zonename_` 」
```

c. ゾーンセットをアクティブにします。

```
zoneset activate name_FCVI_zone_set_name_vsan_vsan-id_`
```

```

FC_switch_A_1# conf t
FC_switch_A_1(config)# zoneset name FCVI_Zoneset_1_10 vsan 10
FC_switch_A_1(config-zoneset)# member FCVI_Zone_1_10_25
FC_switch_A_1(config-zoneset)# member FCVI_Zone_1_10_29
...
FC_switch_A_1(config-zoneset)# exit
FC_switch_A_1(config)# zoneset activate name FCVI_ZoneSet_1_10 vsan 10
FC_switch_A_1(config)# exit
FC_switch_A_1# copy running-config startup-config

```

8. ゾーニングを検証します。

「ゾーンの方法」

9. 2つ目の FC スイッチファブリックで、ここまでの手順を繰り返します。

FC スイッチの設定を保存しておきます

すべてのスイッチで、FC スイッチの設定がスタートアップ設定に保存されたことを確認する必要があります。

ステップ

両方の FC スイッチファブリックに対して次のコマンドを問題で実行します。

```
'copy running-config startup-config
```

```
FC_switch_A_1# copy running-config startup-config  
FC_switch_B_1# copy running-config startup-config
```

## FC-to-SAS ブリッジおよび SAS ディスクシェルフを設置

新しいストレージを構成に追加する際には、ATTO FibreBridge ブリッジおよび SAS ディスクシェルフを設置してケーブル接続します。

このタスクについて

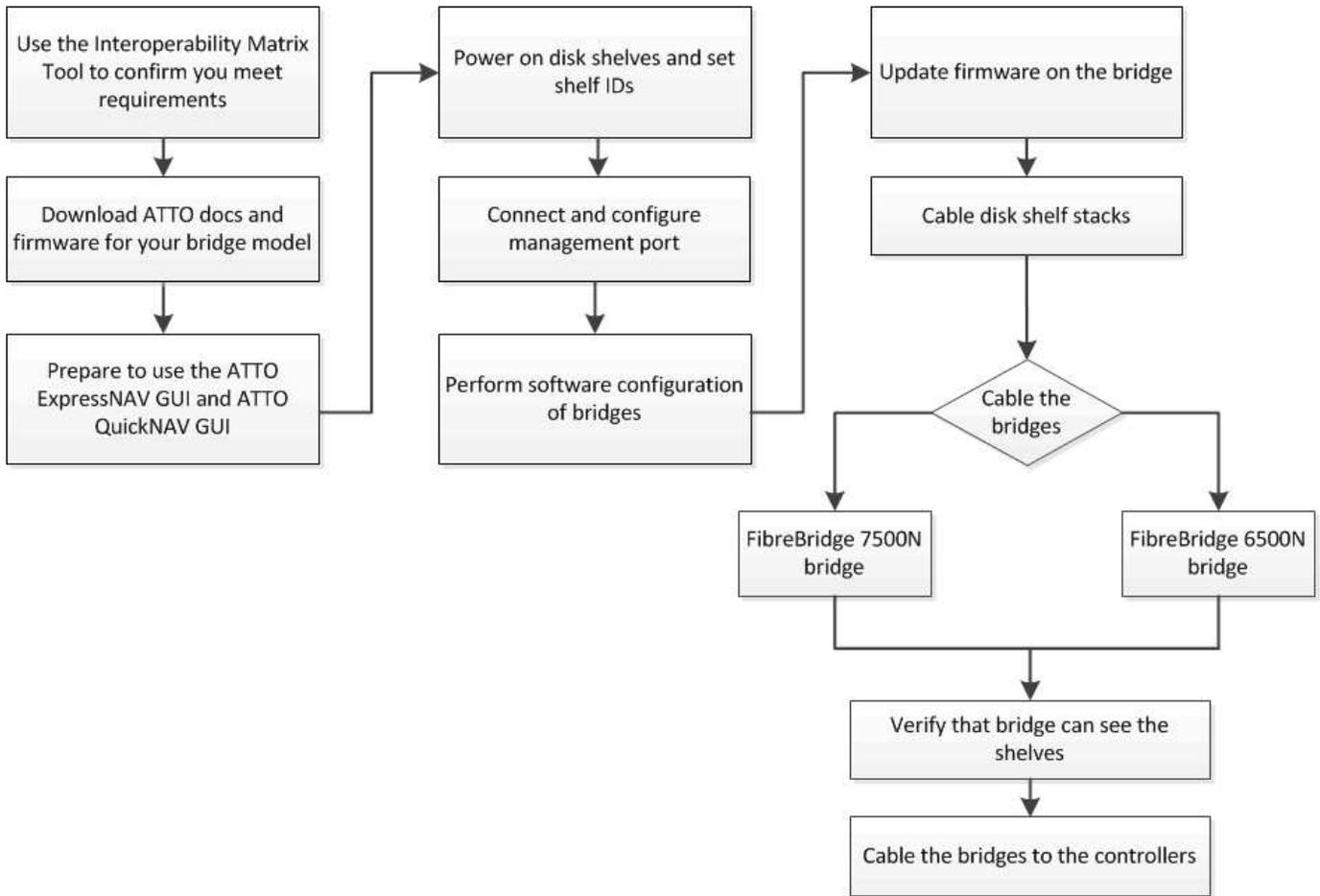
工場出荷状態のシステムの場合は、FC-to-SAS は事前に構成されているため、追加の構成は不要です。

この手順は、推奨されるブリッジ管理インターフェイスである ATTO ExpressNAV GUI と ATTO QuickNAV ユーティリティを使用していることを前提としています。

ATTO ExpressNAV GUI は、ブリッジの設定および管理、ブリッジファームウェアの更新に使用します。ATTO QuickNAV ユーティリティは、ブリッジのイーサネット管理 1 ポートの設定に使用します。

シリアルポートや Telnet を使用してブリッジの設定と管理、イーサネット管理 1 ポートの設定を行ったり、FTP を使用してブリッジファームウェアを更新するなど、必要に応じて他の管理インターフェイスも使用できます。

この手順では次のワークフローを使用します。



## FC-to-SAS ブリッジのインバンド管理

ONTAP 9.5 以降では、FibreBridge 7500N / 7600N ブリッジについて、IP 管理に代わる方法としてインバンド管理\_がサポートされます。ONTAP 9.8 以降では、アウトオブバンド管理は廃止されています。



ONTAP 9.8 以降では 'storage bridge コマンドは 'system bridge コマンドに置き換えられました。次の手順は「storage bridge」コマンドを示していますが、ONTAP 9.8 以降を実行している場合は「system bridge」コマンドが優先されます。

インバンド管理を使用すると、ONTAP CLI からブリッジへの FC 接続を介してブリッジを管理および監視できます。ブリッジのイーサネットポートを介してブリッジに物理的にアクセスする必要がないため、ブリッジのセキュリティの脆弱性が軽減されます。

ブリッジのインバンド管理が可能かどうかは、ONTAP のバージョンによって異なります。

- ONTAP 9.8 以降では、ブリッジはデフォルトでインバンド接続を介して管理され、SNMP を介したブリッジのアウトオブバンド管理は廃止されています。
- ONTAP 9.5 から 9.7 : インバンド管理またはアウトオブバンド管理のどちらかで SNMP 管理がサポートされます。
- ONTAP 9.5 よりも前のバージョンでは、アウトオブバンドの SNMP 管理のみがサポートされます。

ブリッジの CLI コマンドは、ONTAP インターフェイスで実行する ONTAP インターフェイスの「storage bridge run -cli-name\_ bridge\_name\_-command\_ command\_name\_」コマンドから実行できます。



ブリッジへの物理接続を制限してセキュリティを強化するために、IPアクセスを無効にしたインバンド管理を使用することを推奨します。

## FibreBridge 7600N / 7500Nブリッジの制限と接続ルール

FibreBridge 7600N / 7500Nブリッジを接続する際の制限と考慮事項を確認してください。

### FibreBridge 7600N / 7500Nブリッジの制限

- HDDドライブとSSDドライブの組み合わせの最大数は240です。
- SSDドライブの最大数は96です。
- SASポートあたりのSSDの最大数は48です。
- SASポートあたりのシェルフの最大数は10です。

### FibreBridge 7600N / 7500Nブリッジ接続ルール

- 同じSASポートにSSDドライブとHDDドライブを混在させないでください。
- シェルフをSASポートに均等に分散します。
- 他のシェルフタイプ（DS212やDS224シェルフなど）と同じSASポートにDS460シェルフを配置しないでください。

### 設定例

次の例は、SSDドライブを搭載した4台のDS224シェルフとHDDドライブを搭載した6台のDS224シェルフを接続する構成を示しています。

SAS ポート	シェルフとドライブ
SASポートA	SSDを搭載したDS224シェルフ×2
SASポートB	SSDを搭載したDS224シェルフ×2
SASポートC	HDDドライブ搭載のDS224シェルフ×3
SASポートD	HDDドライブ搭載のDS224シェルフ×3

### インストールの準備

新しい MetroCluster システムで使用するブリッジの設置を準備する際には、システムが一定の要件を満たしていることを確認する必要があります。これには、ブリッジのセットアップや構成の要件と、必要なドキュメント、ATTO QuickNAV ユーティリティ、ブリッジファームウェアのダウンロードなどがあります。

### 作業を開始する前に

- システムキャビネットに付属していない場合は、システムをラックに設置しておく必要があります。
- サポートされているハードウェアモデルとソフトウェアバージョンを使用している必要があります。

を参照してください "[ネットアップの Interoperability Matrix Tool \(IMT\)](#)" では、Storage 解決策フィールドを使用して MetroCluster 解決策を選択できます。検索を絞り込むには、\* 構成部品エクスペローラ \* を使用して構成部品と ONTAP バージョンを選択します。[ 結果の表示 ( Show Results ) ] をクリックすると、条件に一致するサポートされている構成のリストを表示できます。

- 各 FC スイッチで、1つの FC ポートを1つのブリッジに接続できる必要があります。

- SAS ケーブルの取り扱い方法、およびディスクシェルフの設置とケーブル接続に関する考慮事項とベストプラクティスを確認しておく必要があります。

考慮事項とベストプラクティスについては、使用しているディスクシェルフモデルの『Installation and Service Guide』を参照してください。

- ブリッジの設定に使用するコンピュータでは、ATTO ExpressNAV GUI を使用するために、ATTO でサポートされている Web ブラウザを実行している必要があります。

ATTO Product Release Notes に、サポートされている Web ブラウザの最新のリストが掲載されています。このドキュメントには、以下の手順で説明する ATTO の Web サイトからアクセスできます。

## 手順

1. 使用しているディスクシェルフモデルの Installation and Service Guide をダウンロードします。
  - a. FibreBridge のモデルに対応するリンクを使用して ATTO の Web サイトにアクセスし、マニュアルと QuickNAV ユーティリティをダウンロードします。



管理インターフェースの詳細については、使用しているモデルブリッジに対応した ATTO FibreBridge Installation and Operation Manual を参照してください。

ATTO FibreBridge の説明ページに記載されているリンクを使用して、このコンテンツや ATTO Web サイト上のその他のコンテンツにアクセスできます。

2. 推奨されるブリッジ管理インターフェイス、ATTO ExpressNAV GUI および ATTO QuickNAV ユーティリティを使用するために必要なハードウェアおよび情報を収集します。
  - a. デフォルト以外のユーザ名とパスワードを決定します（ブリッジへのアクセス用）。  
  
デフォルトのユーザ名とパスワードは変更してください。
  - b. ブリッジの IP 管理を設定する場合は、ブリッジに付属のシールド付きイーサネットケーブル（ブリッジのイーサネット管理 1 ポートとネットワークの接続に使用）が必要です。
  - c. ブリッジの IP 管理を設定する場合は、各ブリッジのイーサネット管理 1 ポートの IP アドレス、サブネットマスク、およびゲートウェイの情報が必要です。
  - d. セットアップに使用するコンピュータで VPN クライアントを無効にします。

アクティブな VPN クライアント原因がブリッジの QuickNAV スキャンに失敗しました。

## FC-to-SASブリッジおよびSASシェルフの設置

システムが「インストールの準備」のすべての要件を満たしていることを確認したら、新しいシステムをインストールできます。

### このタスクについて

- ディスクとシェルフの構成は両方のサイトで同じである必要があります。

ミラーされていないアグリゲートを使用する場合は、各サイトでディスクとシェルフの構成が異なることがあります。



ミラーされたアグリゲートとミラーされていないアグリゲートのどちらに使用されているかに関係なく、ディザスタリカバリグループ内のディスクはすべて同じタイプの接続を使用し、ディザスタリカバリグループ内のすべてのノードから認識する必要があります。

- 50 ミクロンのマルチモード光ファイバケーブルを使用するディスクシェルフ、FC スイッチ、およびバックアップテープデバイスの最大距離に関するシステム接続要件が、FibreBridge ブリッジにも該当します。

#### "NetApp Hardware Universe の略"

次のシェルフと FibreBridge 7500N / 7600N ブリッジでは、追加のケーブル接続なしでインバンド ACP がサポートされます。



- ONTAP 9.2 以降の 7500N または 7600N ブリッジで接続された IOM12 (DS460C)
- ONTAP 9.1 以降の 7500N または 7600N ブリッジで接続された IOM12 (DS212C および DS224C)



MetroCluster 構成の SAS シェルフでは、ACP ケーブル接続はサポートされません。

必要に応じて、**FibreBridge 7600N** ブリッジの IP ポートアクセスを有効にします

9.5 より前のバージョンの ONTAP を使用している場合、または Telnet やその他の IP ポートプロトコルおよびサービス (FTP、ExpressNAV、ICMP、QuickNAV) を使用して FibreBridge 7600N ブリッジへのアウトオブバンドアクセスを使用する場合は、コンソールポート経由でアクセスサービスを有効にできます。

このタスクについて

ATTO FibreBridge 7500Nブリッジとは異なり、FibreBridge 7600Nブリッジは、すべてのIPポートプロトコルおよびサービスが無効になった状態で出荷されます。

ONTAP 9.5 以降では、ブリッジのインバンド管理\_がサポートされます。これは、ONTAP CLI からブリッジへの FC 接続を介してブリッジを設定および監視できることを意味します。ブリッジのイーサネットポートを介してブリッジに物理的にアクセスする必要がなく、ブリッジのユーザインターフェイスも必要ありません。

ONTAP 9.8 以降では、ブリッジの\_帯域内管理\_がデフォルトでサポートされ、アウトオブバンド SNMP 管理は廃止されています。

このタスクは、ブリッジの管理にインバンド管理を使用していない場合に必要です。この場合は、イーサネット管理ポートを介してブリッジを設定する必要があります。

手順

1. FibreBridge 7600Nブリッジのシリアルポートにシリアルケーブルを接続して、ブリッジのコンソールインターフェイスにアクセスします。
2. コンソールを使用してアクセスサービスを有効にし、設定を保存します。

```
'et closePort none'
```

```
'aveConfiguration'
```

'set closePort none' コマンドを使用すると、ブリッジ上のすべてのアクセスサービスがイネーブルになり

ます。

3. 必要に応じて 'set closePort' コマンドを発行し '必要に応じてコマンドを繰り返して '必要なサービスをすべて無効にします

```
'et closePort_service_`
```

'set closePort' コマンドは '一度に 1 つのサービスを無効にします

パラメータ「SERVICE」は、次のいずれかとして指定できます。

- エクプレスナヴ
- FTP
- ICMP
- QuickNAV
- SNMP
- Telnet

特定のプロトコルがイネーブルになっているかディセーブルになっているかを確認するには、get closePort コマンドを使用します。

4. SNMP を有効にする場合は、次の問題コマンドも実行する必要があります。

```
'Set SNMP enabled
```

SNMP は、別個の enable コマンドを必要とする唯一のプロトコルです。

5. 設定を保存します。

```
'aveConfiguration'
```

#### FC-to-SASブリッジを設定

モデルに応じた FC-to-SAS ブリッジのケーブル接続に進む前に、FibreBridge ソフトウェアで設定を行う必要があります。

作業を開始する前に

ブリッジのインバンド管理を使用するかどうかを決めておく必要があります。



ONTAP 9.8 以降では 'storage bridge コマンドは 'system bridge コマンドに置き換えられました。次の手順は「storage bridge」コマンドを示していますが、ONTAP 9.8 以降を実行している場合は「system bridge」コマンドが優先されます。

このタスクについて

IP 管理ではなくブリッジのインバンド管理を使用する場合は、該当する手順に記載されているように、イーサネットポートと IP を設定する手順を省略できます。

手順

1. ATTO FibreBridge のシリアルコンソールポートを設定し、ポート速度を 1、000 詐欺検出用に設定します。

```
get serialportbaudrate
SerialPortBaudRate = 115200

Ready.

set serialportbaudrate 115200

Ready. *
saveconfiguration
Restart is necessary....
Do you wish to restart (y/n) ? y
```

2. インバンド管理用に設定する場合は、FibreBridge RS-232 シリアルポートから PC のシリアル（COM）ポートにケーブルを接続します。

シリアル接続は初期設定と ONTAP によるインバンド管理に使用され、FC ポートを使用してブリッジの監視と管理を行うことができます。

3. IP 管理用に設定する場合は、イーサネットケーブルを使用して、各ブリッジのイーサネット管理 1 ポートをネットワークに接続します。

ONTAP 9.5 以降を実行しているシステムでは、インバンド管理を使用してイーサネットポートではなく FC ポート経由でブリッジにアクセスできます。ONTAP 9.8 以降では、インバンド管理のみがサポートされ、SNMP 管理は廃止されています。

イーサネット管理 1 ポートを使用すると、ブリッジファームウェアを短時間でダウンロードし（ATTO ExpressNAV または FTP 管理インターフェイスを使用）、コアファイルと抽出ログを取得できます。

4. IP 管理用に設定する場合は、使用しているブリッジモデルの ATTO FibreBridge Installation and Operation Manual \_ のセクション 2.0 の手順に従って、各ブリッジのイーサネット管理 1 ポートを設定します。

ONTAP 9.5 以降を実行しているシステムでは、インバンド管理を使用してイーサネットポートではなく FC ポート経由でブリッジにアクセスできます。ONTAP 9.8 以降では、インバンド管理のみがサポートされ、SNMP 管理は廃止されています。

QuickNAV を実行してイーサネット管理ポートを設定すると、イーサネットケーブルで接続されているイーサネット管理ポートのみが設定されます。たとえば、イーサネット管理 2 ポートも設定する場合は、イーサネットケーブルをポート 2 に接続して QuickNAV を実行する必要があります。

5. ブリッジを設定します。

指定するユーザ名とパスワードは必ずメモしてください。



ATTO FibreBridge 7600N または 7500N では時刻同期は設定しないでください。ATTO FibreBridge 7600N または 7500N の時刻は、ONTAP でブリッジが検出されたあとにクラスタ時間に設定されます。また、1 日に 1 回定期的に同期されます。使用されるタイムゾーンは GMT で、変更することはできません。

- a. IP 管理用に設定する場合は、ブリッジの IP 設定を行います。

ONTAP 9.5 以降を実行しているシステムでは、インバンド管理を使用してイーサネットポートではなく FC ポート経由でブリッジにアクセスできます。ONTAP 9.8 以降では、インバンド管理のみがサポートされ、SNMP 管理は廃止されています。

Quicknav ユーティリティなしで IP アドレスを設定するには、FibreBridge に対するシリアル接続が必要です。

CLI を使用する場合は、次のコマンドを実行する必要があります。

```
'set ipaddress mp1 ip-address
```

```
'set ipsubnetmask mp1 subnet-mask
```

```
'set ipgateway mp1x.x'
```

```
'set ipdhcp mp1 disabled
```

```
「 setethernetspeed mp1 1000」
```

b. ブリッジ名を設定します。

ブリッジ名は、MetroCluster 構成内でそれぞれ一意である必要があります。

各サイトの 1 つのスタックグループのブリッジ名の例：

- bridge\_A\_1a
- bridge\_A\_1b
- bridge\_B\_1a
- bridge\_B\_1b

CLI を使用する場合は、次のコマンドを実行する必要があります。

```
'set bridgename _bridgename_bridge_name'
```

c. ONTAP 9.4 以前を実行している場合は、ブリッジで SNMP を有効にします。

```
'Set SNMP enabled
```

ONTAP 9.5 以降を実行しているシステムでは、インバンド管理を使用してイーサネットポートではなく FC ポート経由でブリッジにアクセスできます。ONTAP 9.8 以降では、インバンド管理のみがサポートされ、SNMP 管理は廃止されています。

6. ブリッジの FC ポートを設定します。

a. ブリッジ FC ポートのデータ速度を設定します。

サポートされる FC データ速度は、モデルブリッジによって異なります。

- FibreBridge 7600Nブリッジは、最大32、16、または8Gbpsをサポートします。
- FibreBridge 7500Nブリッジは、最大16、8、または4Gbpsをサポートします。



選択できる FCDataRate の速度は、ブリッジポートを接続するコントローラモジュールのブリッジ / FC ポートの両方でサポートされる最大速度以下です。ケーブルでの接続距離が SFP およびその他のハードウェアの制限を超えないようにしてください。

CLI を使用する場合は、次のコマンドを実行する必要があります。

```
set FCDataRate <port-number> <port-speed>
```

- b. FibreBridge 7500Nブリッジを設定する場合は、ポートで使用する接続モードを「ptp」に設定します。



FibreBridge 7600N ブリッジを設定する場合、 FCConnMode の設定は不要です。

CLI を使用する場合は、次のコマンドを実行する必要があります。

```
set FCConnMode <port-number> ptp
```

- c. FibreBridge 7600N / 7500N ブリッジを設定する場合は、 FC2 ポートを設定または無効にする必要があります。

- 2 番目のポートを使用する場合は、 FC2 ポートについて同じ手順を繰り返す必要があります。
- 2 番目のポートを使用しない場合は、ポートを無効にする必要があります。

```
FCPortDisable <port-number>
```

次に、 FC ポート 2 を無効にする例を示します。

```
FCPortDisable 2  
  
Fibre Channel Port 2 has been disabled.
```

- a. FibreBridge 7600N / 7500N ブリッジを設定する場合は、未使用の SAS ポートを無効にします。

```
'ASPortDisable_SAS-PORT_'
```



SAS ポート A~D はデフォルトで有効になります。使用していない SAS ポートを無効にする必要があります。

SAS ポート A のみを使用している場合は、 SAS ポート B、 C、 および D を無効にする必要があります。次の例は、 SAS ポート B を無効にしています SAS ポート C および D についても、同じように無効にする必要があります。

```
SASPortDisable b  
  
SAS Port B has been disabled.
```

7. ブリッジへのアクセスを保護し、ブリッジの設定を保存します。システムで実行している ONTAP のバー

ジョンに応じて、次のいずれかのオプションを選択します。

ONTAP バージョン	手順
• ONTAP 9.5 以降 *	<p>a. ブリッジのステータスを表示します。</p> <p>「 storage bridge show 」</p> <p>出力には、保護されていないブリッジが表示されます。</p> <p>b. ブリッジを保護します。</p> <p>「 ecurebridge 」</p>
• ONTAP 9.4 以前 *	<p>a. ブリッジのステータスを表示します。</p> <p>「 storage bridge show 」</p> <p>出力には、保護されていないブリッジが表示されます。</p> <p>b. セキュリティ保護されていないブリッジのポートのステータスを確認します。</p> <p>「 info 」 のようになります</p> <p>出力には、イーサネットポート MP1 と MP2 のステータスが表示されません。</p> <p>c. イーサネットポート MP1 がイネーブルの場合、次のコマンドを実行します。</p> <p>「 Set EthernetPort mp1 disabled 」 です</p> <p>イーサネットポート MP2 も有効になっている場合は、ポート MP2 について前の手順を繰り返します。</p> <p>d. ブリッジの設定を保存します。</p> <p>次のコマンドを実行する必要があります。</p> <p>'aveConfiguration'</p> <p>「 FirmwareRestart 」 と入力します</p> <p>ブリッジを再起動するように求められます。</p>

8. MetroCluster の設定が完了したら、「 flashimages 」 コマンドを使用して FibreBridge ファームウェアのバージョンを確認し、ブリッジが最新のサポート対象バージョンを使用していない場合は構成内のすべてのブリッジのファームウェアを更新します。

#### "MetroCluster コンポーネントの保守"

ブリッジを設定したら、新しいシステムのケーブル接続を開始できます。

このタスクについて

ディスクシェルフの場合は、SAS ケーブルのコネクタをプルタブ（コネクタの下側）を下にして挿入します。

手順

1. 各スタックのディスクシェルフをデイジーチェーン接続します。
  - a. スタック内の論理的に最初のシェルフから、IOM Aのポート3を次のシェルフのIOM Aのポート1に接続し、スタック内の各IOM Aを接続します。
  - b. IOM B について、同じ手順を繰り返します
  - c. 各スタックについて、同じ手順を繰り返します。

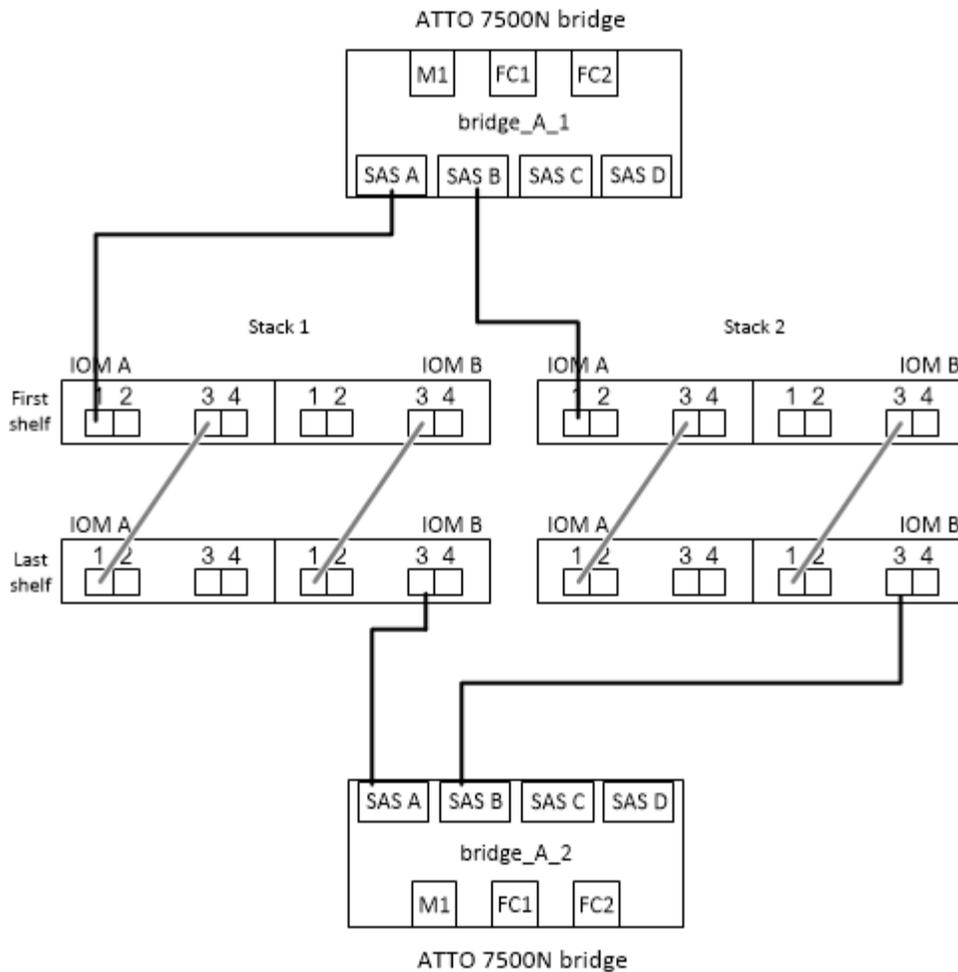
ディスクシェルフのデイジーチェーン接続の詳細については、使用しているディスクシェルフモデルの *Installation and Service Guide* を参照してください。

2. ディスクシェルフの電源をオンにし、シェルフ ID を設定します。
  - 各ディスクシェルフの電源を再投入する必要があります。
  - 各 MetroCluster DR グループ（両サイトを含む）で、各 SAS ディスクシェルフのシェルフ ID が一意である必要があります。
3. ディスクシェルフを FibreBridge ブリッジにケーブル接続します。
  - a. ディスクシェルフの最初のスタックで、最初のシェルフの IOM A を FibreBridge A の SAS ポート A にケーブル接続し、最後のシェルフの IOM B を FibreBridge B の SAS ポート A にケーブル接続します
  - b. 残りのシェルフスタックについて、FibreBridge ブリッジの次に使用可能な SAS ポートを使用して同じ手順を繰り返します。2番目のスタックにはポート B、3番目のスタックにはポート C、4番目のスタックにはポート D を使用します。
  - c. ケーブル接続中、IOM12 モジュールに基づくスタックは、別々の SAS ポートに接続されている限り、同じブリッジに接続します。



それぞれのスタックで異なる IOM モデルを使用できますが、スタック内ではすべてのディスクシェルフで同じモデルを使用する必要があります。

次の図は、1組の FibreBridge 7600N / 7500N ブリッジにディスクシェルフが接続された状態を示しています。



ブリッジの接続を確認し、ブリッジのFCポートをケーブル接続する

各ブリッジですべてのディスクドライブが検出されることを確認してから、各ブリッジをローカルの FC スイッチにケーブル接続します。

手順

1. 各ブリッジが接続されているすべてのディスクドライブとディスクシェルフを検出できることを確認します。

使用する手段	作業
--------	----

ATTO ExpressNAV の GUI	<p>a. サポートされている Web ブラウザで、ブリッジの IP アドレスをブラウザのアドレスバーに入力します。</p> <p>IP アドレスを入力したブリッジの ATTO FibreBridge ホームページに移動し、リンクが表示されます。</p> <p>b. リンクをクリックし、ブリッジを設定するときに指定したユーザ名とパスワードを入力します。</p> <p>ブリッジの ATTO FibreBridge ステータスページが開き、左側にメニューが表示されます。</p> <p>c. 「* 詳細設定 *」をクリックします。</p> <p>d. <code>sastargets</code> コマンドを使用して、接続されているデバイスを表示し、* 送信 * をクリックします。</p>
シリアルポート接続	<p>接続されているデバイスを表示します。</p> <p>「<code>astargets</code>」</p>

出力には、ブリッジが接続されているデバイス（ディスクおよびディスクシェルフ）が表示されます。出力行には行番号が振られているため、デバイスの台数を簡単に把握できます。たとえば、次の出力は、10 本のディスクが接続されていることを示しています。

```

Tgt VendorID ProductID          Type          SerialNumber
  0 NETAPP    X410_S15K6288A15 DISK          3QP1CLE300009940UHJV
  1 NETAPP    X410_S15K6288A15 DISK          3QP1ELF600009940V1BV
  2 NETAPP    X410_S15K6288A15 DISK          3QP1G3EW00009940U2M0
  3 NETAPP    X410_S15K6288A15 DISK          3QP1EWMP00009940U1X5
  4 NETAPP    X410_S15K6288A15 DISK          3QP1FZLE00009940G8YU
  5 NETAPP    X410_S15K6288A15 DISK          3QP1FZLF00009940TZKZ
  6 NETAPP    X410_S15K6288A15 DISK          3QP1CEB400009939MGXL
  7 NETAPP    X410_S15K6288A15 DISK          3QP1G7A900009939FNNTT
  8 NETAPP    X410_S15K6288A15 DISK          3QP1FY0T00009940G8PA
  9 NETAPP    X410_S15K6288A15 DISK          3QP1FXW600009940VERQ

```



出力の先頭に「`response truncated`」というテキストが表示された場合は、Telnet を使用してブリッジに接続し、同じコマンドを入力してすべての出力を確認できます。

2. コマンド出力を確認して、ブリッジがスタック内の想定されるすべてのディスクおよびディスクシェルフに接続していることを確認します。

出力結果	作業
正解です	繰り返します <a href="#">手順 1</a> . 残りの各ブリッジ。

不正解です	<p>a. SAS ケーブルに緩みがないか確認するか、SAS ケーブル接続をやり直します。</p> <p><a href="#">FibreBridge 7600N / 7500NブリッジをIOM12モジュールを使用してディスクシェルフとケーブル接続</a></p> <p>b. 繰り返します <a href="#">手順 1.</a></p>
-------	--

3. 構成およびスイッチのモデルと FC-to-SAS ブリッジのモデルに対応するケーブル接続の表に従って、各ブリッジをローカルの FC スイッチにケーブル接続します。



FibreBridge 7500N ブリッジの 2 つ目の FC ポート接続については、ゾーニングが完了するまでケーブル接続しないでください。

使用している ONTAP のバージョンに対応したポート割り当てを参照してください。

4. パートナーサイトのブリッジに対して同じ手順を繰り返します。

#### 関連情報

FCスイッチをケーブル接続するときは、指定のポート割り当てを使用していることを確認する必要があります。

#### "FCスイッチのポート割り当て"

#### FibreBridge ブリッジをセキュリティ保護または保護解除します

安全性に問題のあるイーサネットプロトコルをブリッジで簡単に無効にできるように、ONTAP 9.5 以降ではブリッジを保護することができます。これにより、ブリッジのイーサネットポートが無効になります。イーサネットアクセスを再度有効にすることもできます。

#### このタスクについて

- ブリッジをセキュリティ保護すると、ブリッジの Telnet とその他の IP ポートプロトコルおよびサービス（FTP、ExpressNAV、ICMP、QuickNAV）が無効になります。
- この手順では、ONTAP 9.5 以降で使用可能な ONTAP プロンプトを使用したアウトオブバンド管理を使用します。

アウトオブバンド管理を使用していない場合は、ブリッジの CLI からコマンドを問題できます。

- 「unsecurebridge」コマンドを使用して、イーサネットポートを再度イネーブルにできます。
- ONTAP 9.7 以前では、ATTO FibreBridge で「ecurebridge」コマンドを実行すると、パートナークラスターでブリッジステータスが正しく更新されない可能性があります。この場合は、パートナークラスターから「ecurebridge」コマンドを実行します。



ONTAP 9.8 以降では 'storage bridge コマンドは 'system bridge コマンドに置き換えられました。次の手順は「storage bridge」コマンドを示していますが、ONTAP 9.8 以降を実行している場合は「system bridge」コマンドが優先されます。

#### 手順

1. ブリッジを含むクラスタの ONTAP プロンプトで、ブリッジのセキュリティ保護を設定または解除します。

- 次のコマンドは、bridge\_A\_1 をセキュリティ保護します。

```
'cluster_a> storage bridge run-cli -bridge bridge_A_1 コマンド securebridge`
```

- 次のコマンドは、bridge\_A\_1 のセキュリティ保護を解除します。

```
'cluster_a> storage bridge run-cli -bridge bridge_A_1 コマンド unsecurebridge`
```

2. ブリッジを含むクラスタの ONTAP プロンプトで、ブリッジの設定を保存します。

```
「 storage bridge run -cli-bridge-name_command savecfigation` 」
```

次のコマンドは、bridge\_A\_1 をセキュリティ保護します。

```
'cluster_a > storage bridge run -cli -bridge bridge_A_1 - コマンド保存構成`
```

3. ブリッジを含むクラスタの ONTAP プロンプトから、ブリッジのファームウェアを再起動します。

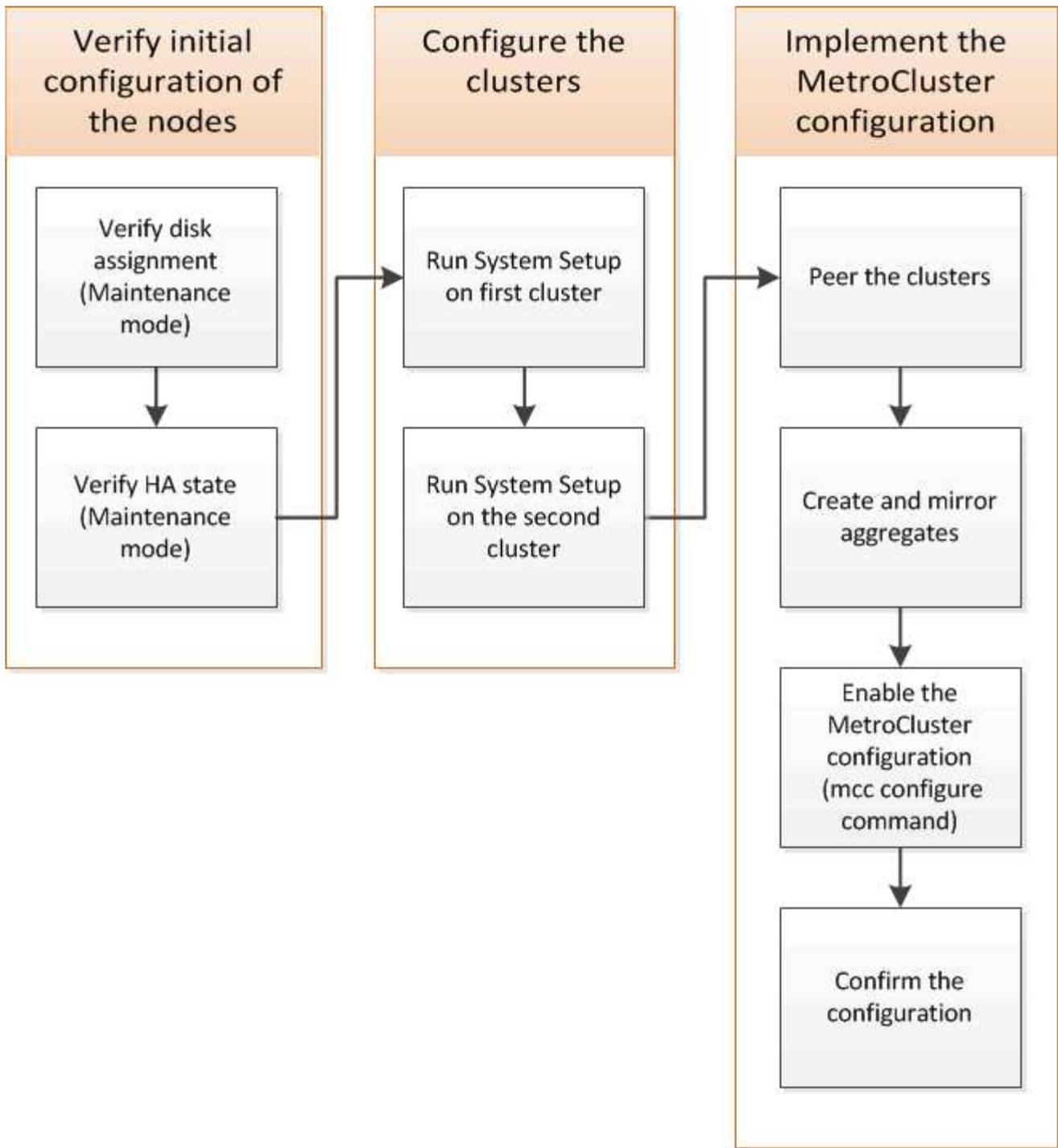
```
「 storage bridge run -cli -bridge_name _ command firmwareerestart` 」
```

次のコマンドは、bridge\_A\_1 をセキュリティ保護します。

```
'cluster_a > storage bridge run-cli -bridge bridge_A_1 - コマンド firmwareerestart`
```

## ONTAP で MetroCluster FC ソフトウェアを設定する

ONTAP の MetroCluster FC 構成で各ノードをセットアップする必要があります。これには、ノードレベルの構成と、2つのサイトへのノードの構成が含まれます。また、2つのサイト間の MetroCluster 関係を実装する必要があります。



## 必要な情報の収集

設定プロセスを開始する前に、コントローラモジュールに必要な IP アドレスを収集する必要があります。

### サイト A の IP ネットワーク情報ワークシート

システムを設定する前に、最初の MetroCluster サイト（サイト A）の IP アドレスその他のネットワーク情報を、ネットワーク管理者から入手する必要があります。

#### スイッチ情報：サイト A（スイッチクラスタ）

システムをケーブル接続するときは、各クラスタスイッチのホスト名と管理 IP アドレスが必要です。この情報は、2 ノードスイッチレスクラスタ構成または 2 ノード MetroCluster 構成（サイトごとに 1 つのノード）を使用している場合は必要ありません。

クラスタスイッチ	ホスト名	IP アドレス	ネットワークマスク	デフォルトゲートウェイ
インターコネクト 1.				
インターコネクト 2				
管理 1				
管理 2.				

#### クラスタ作成情報：サイト A

クラスタを初めて作成するときは、次の情報が必要です。

情報のタイプ	値を入力します
クラスタ名 この手順で使用している例： site_A	
DNS ドメイン	
DNS ネームサーバ	
場所	
管理者パスワード	

#### ノード情報：サイト A

クラスタ内のノードごとに、管理 IP アドレス、ネットワークマスク、およびデフォルトゲートウェイが必要です。

ノード	ポート	IP アドレス	ネットワークマスク	デフォルトゲートウェイ
-----	-----	---------	-----------	-------------

ノード 1  この手順で使用している例： controller_A_1				
ノード 2  2 ノード MetroCluster 構成（サイトごとに1つのノード）を使用している場合は不要  この手順で使用している例： controller_A_2				

クラスタピアリング用の LIF およびポート：サイト A

クラスタ内のノードごとに、2つのクラスタ間 LIF の IP アドレス、ネットワークマスク、およびデフォルトゲートウェイが必要です。クラスタ間 LIF は、クラスタのピアリングに使用されます。

ノード	ポート	クラスタ間 LIF の IP アドレス	ネットワークマスク	デフォルトゲートウェイ
ノード 1 IC LIF 1				
ノード 1 IC LIF 2				
ノード 2 IC LIF 1  2 ノード MetroCluster 構成（サイトごとに1つのノード）の場合は不要				
ノード 2 IC LIF 2  2 ノード MetroCluster 構成（サイトごとに1つのノード）の場合は不要				

タイムサーバ情報：サイト A

時間を同期する必要があります。これには 1 台以上の NTP タイムサーバが必要です。

ノード	ホスト名	IP アドレス	ネットワークマスク	デフォルトゲートウェイ
NTP サーバ 1				
NTP サーバ 2				

#### サイトA nbsp ; AutoSupport 情報

各ノードで AutoSupport を設定する必要があります。これには次の情報が必要です。

情報のタイプ	値を入力します
送信元 E メールアドレス	メールホスト
IP アドレスまたは名前	転送プロトコル
HTTP、HTTPS、または SMTP	プロキシサーバ
	受信者の E メールアドレスまたは 配信リスト
	簡潔なメッセージ

#### サイトA nbsp ; SP情報

トラブルシューティングとメンテナンスのために、各ノードのサービスプロセッサ（SP）へのアクセスを有効にする必要があります。これには、ノードごとに次のネットワーク情報が必要です。

ノード	IP アドレス	ネットワークマスク	デフォルトゲートウェイ
ノード 1			
ノード 2			
2 ノード MetroCluster 構成（サイトごとに 1 つのノード）の場合は不要			

#### サイト B の IP ネットワーク情報ワークシート

システムを設定する前に、2 つ目の MetroCluster サイト（サイト B）の IP アドレスその他のネットワーク情報を、ネットワーク管理者から入手する必要があります。

スイッチ情報：サイト B（スイッチクラスタ）

システムをケーブル接続するときは、各クラスタスイッチのホスト名と管理 IP アドレスが必要です。この情

報は、2 ノードスイッチレスクラスタ構成または2 ノード MetroCluster 構成（サイトごとに1つのノード）を使用している場合は必要ありません。

クラスタスイッチ	ホスト名	IP アドレス	ネットワークマスク	デフォルトゲートウェイ
インターコネクト 1.				
インターコネクト 2				
管理 1				
管理 2.				

クラスタ作成情報：サイト **B**

クラスタを初めて作成するときは、次の情報が必要です。

情報のタイプ	値を入力します
クラスタ名 この手順で使用される例：site_B	
DNS ドメイン	
DNS ネームサーバ	
場所	
管理者パスワード	

ノード情報：サイト **B**

クラスタ内のノードごとに、管理 IP アドレス、ネットワークマスク、およびデフォルトゲートウェイが必要です。

ノード	ポート	IP アドレス	ネットワークマスク	デフォルトゲートウェイ
ノード 1 この手順で使用される例 ： controller_B_1				

ノード 2  2 ノード MetroCluster 構成（サイトごとに 1 つのノード）の場合は不要  この手順で使用される例 : controller_B_2				
---	--	--	--	--

クラスタピアリング用の LIF およびポート：サイト B

クラスタ内のノードごとに、2 つのクラスタ間 LIF の IP アドレス、ネットワークマスク、およびデフォルトゲートウェイが必要です。クラスタ間 LIF は、クラスタのピアリングに使用されます。

ノード	ポート	クラスタ間 LIF の IP アドレス	ネットワークマスク	デフォルトゲートウェイ
ノード 1 IC LIF 1				
ノード 1 IC LIF 2				
ノード 2 IC LIF 1  2 ノード MetroCluster 構成（サイトごとに 1 つのノード）の場合は不要				
ノード 2 IC LIF 2  2 ノード MetroCluster 構成（サイトごとに 1 つのノード）の場合は不要				

タイムサーバ情報：サイト B

時間を同期する必要があります。これには 1 台以上の NTP タイムサーバが必要です。

ノード	ホスト名	IP アドレス	ネットワークマスク	デフォルトゲートウェイ
NTP サーバ 1				

NTP サーバ 2				
-----------	--	--	--	--

#### サイトB nbsp ; AutoSupport情報

各ノードで AutoSupport を設定する必要があります。これには次の情報が必要です。

情報のタイプ	値を入力します	
送信元 E メールアドレス		
メールホスト	IP アドレスまたは名前	
転送プロトコル	HTTP、HTTPS、または SMTP	
プロキシサーバ	受信者の E メールアドレスまたは配信リスト	
メッセージ全文	簡潔なメッセージ	
	パートナー	

#### サイトB nbsp ; SP情報

トラブルシューティングとメンテナンスのために、各ノードのサービスプロセッサ（SP）へのアクセスを有効にする必要があります。これには、ノードごとに次のネットワーク情報が必要です。

ノード	IP アドレス	ネットワークマスク	デフォルトゲートウェイ
ノード 1 (controller_B_1)			
ノード 2 (controller_B_2)			
2 ノード MetroCluster 構成 (サイトごとに 1 つのノード) の場合は不要			

## 標準クラスタ構成と MetroCluster 構成の類似点 / 相違点

MetroCluster 構成の各クラスタのノードの構成は、標準クラスタのノードと似ています。

MetroCluster 構成は、2 つの標準クラスタを基盤としています。構成は物理的に対称な構成である必要があります。各ノードのハードウェア構成が同じで、すべての MetroCluster コンポーネントがケーブル接続され、設定されている必要があります。ただし、MetroCluster 構成のノードの基本的なソフトウェア設定は、標準クラスタのノードと同じです。

設定手順	標準クラスタ構成	MetroCluster の設定
各ノードで管理 LIF、クラスタ LIF、データ LIF を設定。	両方のクラスタタイプで同じです	
ルートアグリゲートを設定	両方のクラスタタイプで同じです	
クラスタ内のノードを HA ペアとして設定	両方のクラスタタイプで同じです	
クラスタ内の一方のノードでクラスタを設定。	両方のクラスタタイプで同じです	
もう一方のノードをクラスタに追加。	両方のクラスタタイプで同じです	
ミラーされたルートアグリゲートを作成	任意。	必須
クラスタをピアリング。	任意。	必須
MetroCluster 設定を有効にします。	該当しません	必須

## メンテナンスモードでコンポーネントの HA 状態を確認および設定する

ストレージシステムを MetroCluster FC 構成で構成する場合は、コントローラモジュールおよびシャーシのコンポーネントのハイアベイラビリティ (HA) 状態が mcc または mcc-2n であることを確認して、これらのコンポーネントが適切にブートするようにする必要があります。工場出荷状態のシステムではこの値を事前に設定しておく必要がありますが、作業を進める前に設定を確認しておく必要があります。

コントローラモジュールとシャーシの HA 状態が正しくない場合は、ノードを再初期化しないと MetroCluster を設定できません。この手順を使用して設定を修正し、次のいずれかの手順を使用してシステムを初期化する必要があります。



- MetroCluster IP 構成では、の手順に従います ["コントローラモジュールのシステムデフォルトの復元"](#)。
- MetroCluster FC 構成では、の手順に従います ["システムをデフォルトに戻し、コントローラモジュールで HBA タイプを設定する"](#)。

作業を開始する前に

システムがメンテナンスモードであることを確認します。

手順

1. メンテナンスモードで、コントローラモジュールとシャーシの HA 状態を表示します。

「 ha-config show 」

HA の正しい状態は、MetroCluster 構成によって異なります。

MetroCluster 構成タイプ	すべてのコンポーネントの HA 状態
--------------------	--------------------

8ノードまたは4ノードのMetroCluster FC構成	MCC
2ノード MetroCluster FC 構成	mcc-2n
8ノードまたは4ノードのMetroCluster IP構成	mccip

2. 表示されたコントローラのシステム状態が正しくない場合は、コントローラモジュールで構成に応じた正しいHA状態を設定します。

MetroCluster構成タイプ	コマンドを実行します
8ノードまたは4ノードのMetroCluster FC構成	「 ha-config modify controller mcc 」
2ノード MetroCluster FC 構成	「 ha-config modify controller mcc-2n 」 という形式で指定します
8ノードまたは4ノードのMetroCluster IP構成	「 ha-config modify controller mccip 」 を参照してください

3. 表示されたシャーシのシステム状態が正しくない場合は、シャーシの構成に応じた正しいHA状態を設定します。

MetroCluster構成タイプ	コマンドを実行します
8ノードまたは4ノードのMetroCluster FC構成	「 ha-config modify chassis mcc 」
2ノード MetroCluster FC 構成	「 ha-config modify chassis mcc-2n 」 というようになりまし
8ノードまたは4ノードのMetroCluster IP構成	「 ha-config modify chassis mccip 」 を参照してください

4. ノードを ONTAP でブートします。

「 boot\_ontap 」

5. この手順をすべて繰り返して、MetroCluster構成の各ノードのHA状態を確認します。

システムのデフォルト設定をリストアし、コントローラモジュールで **HBA** タイプを設定しています

このタスクについて

MetroCluster を正しくインストールするには、コントローラモジュールのデフォルトをリセットしてリストアします。

重要

このタスクを実行する必要があるのは、FC-to-SASブリッジを使用するストレッチ構成のみです。

#### 手順

1. LOADER プロンプトで環境変数をデフォルト設定に戻します。

「デフォルト設定」

2. ノードをメンテナンスモードでブートし、システム内の HBA の設定を行います。

- a. メンテナンスモードでブートします。

「boot\_ontap maint」を使用してください

- b. ポートの現在の設定を確認します。

ucadmin show

- c. 必要に応じてポートの設定を更新します。

HBA のタイプと目的のモード	使用するコマンド
CNA FC	ucadmin modify -m fc -t initiator_adapter_name _`
CNA イーサネット	ucadmin modify -mode cna_adapter_name _`
FC ターゲット	fcadmin config -t target_adapter_name _`
FC イニシエータ	fcadmin config -t initiator_adapter_name _`

3. メンテナンスモードを終了します。

「halt」

コマンドの実行後、ノードが LOADER プロンプトで停止するまで待ちます。

4. ノードをブートしてメンテナンスモードに戻り、設定の変更が反映されるようにします。

「boot\_ontap maint」を使用してください

5. 変更内容を確認します。

HBA のタイプ	使用するコマンド
CNA	ucadmin show
FC	fcadmin show`

6. メンテナンスモードを終了します。

「halt」

コマンドの実行後、ノードが LOADER プロンプトで停止するまで待ちます。

7. ノードをブートメニューでブートします。

```
「 boot_ontap menu
```

コマンドの実行後、ブートメニューが表示されるまで待ちます。

8. ブートメニュープロンプトで「 wipeconfig 」と入力してノード設定をクリアし、 Enter キーを押します。

次の画面はブートメニューのプロンプトを示しています。

```
Please choose one of the following:
```

- ```
(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning.
```

```
Selection (1-9)? wipeconfig
```

```
This option deletes critical system configuration, including cluster membership.
```

```
Warning: do not run this option on a HA node that has been taken over.
```

```
Are you sure you want to continue?: yes
```

```
Rebooting to finish wipeconfig request.
```

## FAS8020 システムでの X1132A-R6 クアッドポートカードの FC-VI ポートの設定

FAS8020 システムで X1132A-R6 クアッドポートカードを使用している場合は、メンテナンスモードに切り替えて、ポート 1a / 1b を FC-VI およびイニシエータ用に使用するように設定できます。工場出荷状態の MetroCluster システムでは、構成に応じて適切にポートが設定されているため、この設定は必要ありません。

このタスクについて

このタスクはメンテナンスモードで実行する必要があります。



ucadmin コマンドを使用した FC ポートの FC-VI ポートへの変換は、FAS8020 および AFF 8020 システムでのみサポートされます。他のプラットフォームでは、FC ポートを FCVI ポートに変換することはできません。

手順

1. ポートを無効にします。

```
「ストレージ無効化アダプタ 1a」
```

## 「ストレージ無効化アダプタ 1b」

```
*> storage disable adapter 1a
Jun 03 02:17:57 [controller_B_1:fc.adapter.offlining:info]: Offlining
Fibre Channel adapter 1a.
Host adapter 1a disable succeeded
Jun 03 02:17:57 [controller_B_1:fc.adapter.offline:info]: Fibre Channel
adapter 1a is now offline.
*> storage disable adapter 1b
Jun 03 02:18:43 [controller_B_1:fc.adapter.offlining:info]: Offlining
Fibre Channel adapter 1b.
Host adapter 1b disable succeeded
Jun 03 02:18:43 [controller_B_1:fc.adapter.offline:info]: Fibre Channel
adapter 1b is now offline.
*>
```

2. ポートが無効になっていることを確認します。

ucadmin show

```
*> ucadmin show
      Current  Current  Pending  Pending  Admin
Adapter Mode    Type     Mode     Type     Status
-----
...
1a    fc     initiator -        -        offline
1b    fc     initiator -        -        offline
1c    fc     initiator -        -        online
1d    fc     initiator -        -        online
```

3. ポート a とポート b を FC-VI モードに設定します。

ucadmin modify -adapter 1a -type FCVI'

このコマンドでは、1a だけを指定した場合でも、ポートペアの両方のポート 1a と 1b のモードが設定されます。

```
*> ucadmin modify -t fcvi 1a
Jun 03 02:19:13 [controller_B_1:ucm.type.changed:info]: FC-4 type has
changed to fcvi on adapter 1a. Reboot the controller for the changes to
take effect.
Jun 03 02:19:13 [controller_B_1:ucm.type.changed:info]: FC-4 type has
changed to fcvi on adapter 1b. Reboot the controller for the changes to
take effect.
```

4. 変更が保留中であることを確認します。

ucadmin show

```
*> ucadmin show
      Current   Current   Pending   Pending   Admin
Adapter Mode     Type      Mode      Type      Status
-----
...
1a    fc       initiator -         fcvi     offline
1b    fc       initiator -         fcvi     offline
1c    fc       initiator -         -        online
1d    fc       initiator -         -        online
```

5. コントローラをシャットダウンし、メンテナンスモードでリブートします。

6. 設定の変更を確認します。

ucadmin show local

```
Node           Adapter  Mode     Type      Mode     Type      Status
-----
...
controller_B_1 1a       fc       fcvi     -        -        online
controller_B_1 1b       fc       fcvi     -        -        online
controller_B_1 1c       fc       initiator -        -        online
controller_B_1 1d       fc       initiator -        -        online
6 entries were displayed.
```

## メンテナンスモードでの 8 ノードまたは 4 ノード構成のディスク割り当ての検証

システムを ONTAP で完全にブートする前に、オプションで、メンテナンスモードでブートしてノードのディスク割り当てを確認することができます。ディスクは、各プールのディスク数が等しい、完全に対称なアクティブ / アクティブ構成を形成するように割り当てられている必要があります。

このタスクについて

新しい MetroCluster システムの場合、出荷前にディスク割り当てが完了しています。

次の表に、MetroCluster 構成のプール割り当ての例を示します。ディスクはシェルフ単位でプールに割り当てられます。

・ サイト A のディスクシェルフ \*

| ディスクシェルフ (sample_shelf_name) | 所属ノード  | 割り当てプール |
|------------------------------|--------|---------|
| ディスクシェルフ 1 (shelf_A_1_1)     | ノード A1 | プール 0   |
| ディスクシェルフ 2 (shelf_A_1_3)     |        |         |
| ディスクシェルフ 3 (shelf_B_1_1)     | ノード B1 | プール 1.  |
| ディスクシェルフ 4 (shelf_B_1_3)     |        |         |
| ディスクシェルフ 5 (shelf_A_2_1)     | ノード A2 | プール 0   |
| ディスクシェルフ 6 (shelf_A_2_3)     |        |         |
| ディスクシェルフ 7 (shelf_B_2_1)     | ノード B2 | プール 1.  |
| ディスクシェルフ 8 (shelf_B_2_3)     |        |         |
| ディスクシェルフ 1 (shelf_A_3_1)     | ノード a3 | プール 0   |
| ディスクシェルフ 2 (shelf_A_3_3)     |        |         |
| ディスクシェルフ 3 (shelf_B_3_1)     | ノード B3 | プール 1.  |
| ディスクシェルフ 4 (shelf_B_3_3)     |        |         |
| ディスクシェルフ 5 (shelf_A_4_1)     | ノード A4 | プール 0   |
| ディスクシェルフ 6 (shelf_A_4_3)     |        |         |
| ディスクシェルフ 7 (shelf_B_4_1)     | ノード B4 | プール 1.  |
| ディスクシェルフ 8 (shelf_B_4_3)     |        |         |

・ サイト B のディスクシェルフ \*

| ディスクシェルフ (sample_shelf_name) | 所属ノード | 割り当てプール |
|------------------------------|-------|---------|
|                              |       |         |

|                           |                           |                           |
|---------------------------|---------------------------|---------------------------|
| ディスクシェルフ 9 (shelf_B_1_2)  | ノード B1                    | プール 0                     |
| ディスクシェルフ 10 (shelf_B_1_4) | ディスクシェルフ 11 (shelf_A_1_2) | ノード A1                    |
| プール 1.                    | ディスクシェルフ 12 (shelf_A_1_4) | ディスクシェルフ 13 (shelf_B_2_2) |
| ノード B2                    | プール 0                     | ディスクシェルフ 14 (shelf_B_2_4) |
| ディスクシェルフ 15 (shelf_A_2_2) | ノード A2                    | プール 1.                    |
| ディスクシェルフ 16 (shelf_A_2_4) | ディスクシェルフ 1 (shelf_B_3_2)  | ノード a 3                   |
| プール 0                     | ディスクシェルフ 2 (shelf_B_3_4)  | ディスクシェルフ 3 (shelf_A_3_2)  |
| ノード B3                    | プール 1.                    | ディスクシェルフ 4 (shelf_A_3_4)  |
| ディスクシェルフ 5 (shelf_B_4_2)  | ノード A4                    | プール 0                     |
| ディスクシェルフ 6 (shelf_B_4_4)  | ディスクシェルフ 7 (shelf_A_4_2)  | ノード B4                    |

## 手順

1. シェルフの割り当てを確認します。

「Disk show -v」のように表示されます

2. 必要に応じて、接続されているディスクシェルフ上のディスクを適切なプールに明示的に割り当てます。

「ディスク割り当て」

ワイルドカードを使用すると、1回のコマンドで1つのディスクシェルフのすべてのディスクを割り当てることができます。「storage show disk --x」コマンドを使用すると、各ディスクのディスクシェルフ ID とベイを識別できます。

## AFF 以外のシステムでディスク所有権を割り当てています

MetroCluster ノードにディスクが正しく割り当てられていない場合、または構成で DS460C ディスクシェルフを使用している場合は、MetroCluster 構成内の各ノードにシェルフ単位でディスクを割り当てる必要があ

ります。構成内の各ノードのローカルディスクプールとリモートディスクプールでディスク数が同じになるように設定します。

作業を開始する前に

ストレージコントローラがメンテナンスモードになっている必要があります。

このタスクについて

構成に DS460C ディスクシェルフが含まれている場合を除き、工場出荷時の状態でディスクが正しく割り当てられていればこのタスクは必要ありません。



プール 0 には、ディスクを所有するストレージシステムと同じサイトにあるディスクを割り当てます。

プール 1 には、ディスクを所有するストレージシステムに対してリモートなディスクを割り当てます。

構成に DS460C ディスクシェルフが含まれている場合は、それぞれの 12 ディスクドロワーについて、次のガイドラインに従ってディスクを手動で割り当てる必要があります。

| ドロワーのディスク | ノードとプール                   |
|-----------|---------------------------|
| 0 ~ 2     | ローカルノードのプール 0             |
| 3-5       | HA パートナーノードのプール 0         |
| 6 ~ 8     | ローカルノードのプール 1 の DR パートナー  |
| 9 ~ 11    | HA パートナーのプール 1 の DR パートナー |

このディスク割り当てパターンに従うことで、ドロワーがオフラインになった場合のアグリゲートへの影響を最小限に抑えることができます。

手順

1. システムをブートしていない場合は、メンテナンスモードでブートします。
2. 最初のサイト（サイト A）にあるノードにディスクシェルフを割り当てます。

ノードと同じサイトにあるディスクシェルフはプール 0 に割り当て、パートナーサイトにあるディスクシェルフはプール 1 に割り当てます。

各プールに同じ数のシェルフを割り当てる必要があります。

- a. 最初のノードで、ローカルディスクシェルフをプール 0 に、リモートディスクシェルフをプール 1 に割り当てます。

```
「 Disk assign-shelf_local-switch-name : shelf-name .port_-p_pool_」
```

ストレージコントローラ Controller\_A\_1 にシェルフが 4 台ある場合は、次のコマンドを問題に設定します。

```
*> disk assign -shelf FC_switch_A_1:1-4.shelf1 -p 0
*> disk assign -shelf FC_switch_A_1:1-4.shelf2 -p 0

*> disk assign -shelf FC_switch_B_1:1-4.shelf1 -p 1
*> disk assign -shelf FC_switch_B_1:1-4.shelf2 -p 1
```

- b. ローカルサイトの 2 番目のノードに対して処理を繰り返し、ローカルディスクシェルフをプール 0 に、リモートディスクシェルフをプール 1 に割り当てます。

「Disk assign-shelf\_local-switch-name : shelf-name .port\_-p\_pool\_」

ストレージコントローラ Controller\_A\_2 にシェルフが 4 台ある場合は、次のコマンドを問題に設定します。

```
*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0
*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1

*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0
*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1
```

3. 2 番目のサイト（サイト B）にあるノードにディスクシェルフを割り当てます。

ノードと同じサイトにあるディスクシェルフはプール 0 に割り当て、パートナーサイトにあるディスクシェルフはプール 1 に割り当てます。

各プールに同じ数のシェルフを割り当てる必要があります。

- a. リモートサイトの最初のノードで、ローカルディスクシェルフをプール 0 に、リモートディスクシェルフをプール 1 に割り当てます。

「ディスク assign -shelf\_local-switch-namesshelf-name -p\_pool\_」

ストレージコントローラ Controller\_B\_1 にシェルフが 4 台ある場合は、次のコマンドを問題にします。

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf1 -p 0
*> disk assign -shelf FC_switch_B_1:1-5.shelf2 -p 0

*> disk assign -shelf FC_switch_A_1:1-5.shelf1 -p 1
*> disk assign -shelf FC_switch_A_1:1-5.shelf2 -p 1
```

- b. リモートサイトの 2 番目のノードに対して処理を繰り返し、ローカルディスクシェルフをプール 0 に、リモートディスクシェルフをプール 1 に割り当てます。

「ディスク assign -shelf\_shelf-name-p\_pool\_」

ストレージコントローラ Controller\_B\_2 にシェルフが 4 台ある場合は、次のコマンドを問題に実行し

ます。

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf3 -p 0
*> disk assign -shelf FC_switch_B_1:1-5.shelf4 -p 0

*> disk assign -shelf FC_switch_A_1:1-5.shelf3 -p 1
*> disk assign -shelf FC_switch_A_1:1-5.shelf4 -p 1
```

4. シェルフの割り当てを確認します。

「storage show shelf

5. メンテナンスモードを終了します。

「halt」

6. ブートメニューを表示します。

「boot\_ontap menu

7. 各ノードで、オプション \* 4 \* を選択してすべてのディスクを初期化します。

#### AFF システムでディスク所有権を割り当てます

アグリゲートがミラーされた AFF システムを使用する構成で、ノードにディスク（SSD）が正しく割り当てられていない場合は、各シェルフの半分のディスクを 1 つのローカルノードに割り当て、残りの半分を対応する HA パートナーノードに割り当てる必要があります。構成内の各ノードのローカルディスクプールとリモートディスクプールでディスク数が同じになるように設定する必要があります。

作業を開始する前に

ストレージコントローラがメンテナンスモードになっている必要があります。

このタスクについて

これは、アグリゲートがミラーされていない構成、アクティブ / パッシブ構成、ローカルプールとリモートプールのディスク数が異なる構成には該当しません。

このタスクは、工場出荷時にディスクが正しく割り当てられている場合は必要ありません。



プール 0 には、ディスクを所有するストレージシステムと同じサイトにあるディスクを割り当てます。

プール 1 には、ディスクを所有するストレージシステムに対してリモートなディスクを割り当てます。

手順

1. システムをブートしていない場合は、メンテナンスモードでブートします。
2. 最初のサイト（サイト A）にあるノードにディスクを割り当てます。

各プールに同じ数のディスクを割り当てる必要があります。

- a. 最初のノードで、各シェルフの半分のディスクをプール 0 に、残りの半分の HA パートナーのプール 0 に割り当てます。

```
disk assign -shelf <shelf-name> -p <pool> -n <number-of-disks>
```

ストレージコントローラ Controller\_A\_1 にシェルフが 4 台あり、各シェルフに SSD が 8 本ある場合は、次のコマンドを問題に設定します。

```
*> disk assign -shelf FC_switch_A_1:1-4.shelf1 -p 0 -n 4
*> disk assign -shelf FC_switch_A_1:1-4.shelf2 -p 0 -n 4

*> disk assign -shelf FC_switch_B_1:1-4.shelf1 -p 1 -n 4
*> disk assign -shelf FC_switch_B_1:1-4.shelf2 -p 1 -n 4
```

- b. ローカルサイトの 2 番目のノードに対して処理を繰り返し、各シェルフの半分のディスクをプール 1 に、残りの半分の HA パートナーのプール 1 に割り当てます。

「disk assign -disk disk-name -p pool」 という名前です

ストレージコントローラ Controller\_A\_1 にシェルフが 4 台あり、各シェルフに SSD が 8 本ある場合は、次のコマンドを問題に設定します。

```
*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1 -n 4

*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1 -n 4
```

### 3. 2 番目のサイト（サイト B）にあるノードにディスクを割り当てます。

各プールに同じ数のディスクを割り当てる必要があります。

- a. リモートサイトの最初のノードで、各シェルフの半分のディスクをプール 0 に、残りの半分の HA パートナーのプール 0 に割り当てます。

「disk assign -disk disk-name-p\_pool\_」

ストレージコントローラ Controller\_B\_1 にシェルフが 4 台あり、各シェルフに SSD が 8 本ある場合は、次のコマンドを問題で実行します。

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf1 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-5.shelf2 -p 0 -n 4

*> disk assign -shelf FC_switch_A_1:1-5.shelf1 -p 1 -n 4
*> disk assign -shelf FC_switch_A_1:1-5.shelf2 -p 1 -n 4
```

- b. リモートサイトの 2 番目のノードに対して処理を繰り返し、各シェルフの半分のディスクをプール 1 に、残りの半分以上 HA パートナーのプール 1 に割り当てます。

「 disk assign -disk disk-name-p\_pool\_` 」

ストレージコントローラ Controller\_B\_2 にシェルフが 4 台あり、各シェルフに SSD が 8 本ある場合は、次のコマンドを問題に設定します。

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf3 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-5.shelf4 -p 0 -n 4

*> disk assign -shelf FC_switch_A_1:1-5.shelf3 -p 1 -n 4
*> disk assign -shelf FC_switch_A_1:1-5.shelf4 -p 1 -n 4
```

4. ディスクの割り当てを確認します。

「 storage show disk 」を参照してください

5. メンテナンスモードを終了します。

「 halt 」

6. ブートメニューを表示します。

「 boot\_ontap menu 」

7. 各ノードで、オプション \* 4 \* を選択してすべてのディスクを初期化します。

## 保守モードでの 2 ノード構成のディスク割り当ての検証

システムを ONTAP で完全にブートする前に、システムをメンテナンスモードでブートして、ノードのディスク割り当てを確認することもできます。ディスクは、両方のサイトが独自のディスクシェルフを所有してデータを提供し、各ノードおよび各プールのミラーディスク数が等しい、完全に対称な構成を形成するように割り当てられている必要があります。

作業を開始する前に

システムをメンテナンスモードにする必要があります。

このタスクについて

新しい MetroCluster システムの場合、出荷前にディスク割り当てが完了しています。

次の表に、MetroCluster 構成のプール割り当ての例を示します。ディスクはシェルフ単位でプールに割り当てられます。

| ディスクシェルフ (名前) | サイト | 所属ノード | 割り当てプール |
|---------------|-----|-------|---------|
|---------------|-----|-------|---------|

|                           |       |        |        |
|---------------------------|-------|--------|--------|
| ディスクシェルフ 1 (shelf_A_1_1)  | サイト A | ノード A1 | プール 0  |
| ディスクシェルフ 2 (shelf_A_1_3)  |       |        |        |
| ディスクシェルフ 3 (shelf_B_1_1)  |       | ノード B1 | プール 1. |
| ディスクシェルフ 4 (shelf_B_1_3)  |       |        |        |
| ディスクシェルフ 9 (shelf_B_1_2)  | サイト B | ノード B1 | プール 0  |
| ディスクシェルフ 10 (shelf_B_1_4) |       |        |        |
| ディスクシェルフ 11 (shelf_A_1_2) |       | ノード A1 | プール 1. |
| ディスクシェルフ 12 (shelf_A_1_4) |       |        |        |

構成に DS460C ディスクシェルフが含まれている場合は、それぞれの 12 ディスクドロワーについて、次のガイドラインに従ってディスクを手動で割り当てる必要があります。

| ドロワーのディスク | ノードとプール        |
|-----------|----------------|
| 1~6       | ローカルノードのプール 0  |
| 7-12      | DR パートナーのプール 1 |

このディスク割り当てパターンに従うことで、ドロワーがオフラインになった場合のアグリゲートへの影響を最小限に抑えることができます。

#### 手順

- 工場出荷状態のシステムの場合は、シェルフの割り当てを確認します。

「Disk show -v」のように表示されます

- 必要に応じて、disk assign コマンドを使用すると、接続されているディスクシェルフ上のディスクを適切なプールに明示的に割り当てることができます。

ノードと同じサイトにあるディスクシェルフはプール 0 に割り当て、パートナーサイトにあるディスクシェルフはプール 1 に割り当てます。各プールに同じ数のシェルフを割り当てる必要があります。

- システムをブートしていない場合は、メンテナンスモードでブートします。
- サイト A のノードで、ローカルディスクシェルフをプール 0 に、リモートディスクシェルフをプール 1 に割り当てます。

「disk assign -shelf\_disk\_shelf\_name\_-p\_pool\_」のようになります

ストレージコントローラ node\_A\_1 にシェルフが 4 台ある場合は、次のコマンドを問題できます。

```
*> disk assign -shelf shelf_A_1_1 -p 0
*> disk assign -shelf shelf_A_1_3 -p 0

*> disk assign -shelf shelf_A_1_2 -p 1
*> disk assign -shelf shelf_A_1_4 -p 1
```

- c. リモートサイト（サイト B）のノードで、ローカルディスクシェルフをプール 0 に、リモートディスクシェルフをプール 1 に割り当てます。

「`disk assign -shelf_disk_shelf_name_-p_pool_``」のようになります

ストレージコントローラ `node_B_1` にシェルフが 4 台ある場合は、次のコマンドを問題に設定します。

```
*> disk assign -shelf shelf_B_1_2 -p 0
*> disk assign -shelf shelf_B_1_4 -p 0

*> disk assign -shelf shelf_B_1_1 -p 1
*> disk assign -shelf shelf_B_1_3 -p 1
```

- a. 各ディスクのディスクシェルフ ID とベイを表示します。

「`Disk show -v`」のように表示されます

## ONTAP をセットアップしています

各コントローラモジュールに ONTAP をセットアップする必要があります。

新しいコントローラをネットブートする必要がある場合は、を参照してください "[新しいコントローラモジュールのネットブート](#)" MetroCluster アップグレード、移行、および拡張ガイドの各ガイドを参照してください。

選択肢

- [2 ノード MetroCluster 構成での ONTAP のセットアップ](#)
- [ONTAP は、8 ノードまたは 4 ノードの MetroCluster 構成でセットアップします](#)

### 2 ノード MetroCluster 構成での ONTAP のセットアップ

2 ノード MetroCluster 構成では、各クラスタでノードをブートし、クラスタセットアップウィザードを終了し、`cluster setup` コマンドを使用してシングルノードクラスタとしてノードを構成する必要があります。

作業を開始する前に

サービスプロセッサが設定されていないことを確認してください。

このタスクについて

このタスクは、ネットアップの標準のストレージを使用した 2 ノード MetroCluster 構成が対象です。

このタスクは、MetroCluster 構成の両方のクラスタで実行する必要があります。

ONTAP の設定の詳細については、を参照してください ["ONTAP をセットアップする"](#)。

#### 手順

1. 最初のノードの電源をオンにします。



この手順はディザスタリカバリ（DR）サイトのノードでも実行する必要があります。

ノードがブートし、コンソールでクラスタセットアップウィザードが起動されて、AutoSupport が自動的に有効になることを示すメッセージが表示されます。

```
::> Welcome to the cluster setup wizard.
```

```
You can enter the following commands at any time:
```

```
"help" or "?" - if you want to have a question clarified,  
"back" - if you want to change previously answered questions, and  
"exit" or "quit" - if you want to quit the cluster setup wizard.  
Any changes you made before quitting will be saved.
```

```
You can return to cluster setup at any time by typing "cluster setup".  
To accept a default or omit a question, do not enter a value.
```

```
This system will send event messages and periodic reports to NetApp  
Technical  
Support. To disable this feature, enter  
autosupport modify -support disable  
within 24 hours.
```

```
Enabling AutoSupport can significantly speed problem determination and  
resolution, should a problem occur on your system.  
For further information on AutoSupport, see:  
http://support.netapp.com/autosupport/
```

```
Type yes to confirm and continue {yes}: yes
```

```
Enter the node management interface port [e0M]:  
Enter the node management interface IP address [10.101.01.01]:
```

```
Enter the node management interface netmask [101.010.101.0]:  
Enter the node management interface default gateway [10.101.01.0]:
```

```
Do you want to create a new cluster or join an existing cluster?  
{create, join}:
```

2. 新しいクラスタを作成します。

「create」

3. ノードをシングルノードクラスタとして使用するかどうかを選択します。

```
Do you intend for this node to be used as a single node cluster? {yes, no} [yes]:
```

4. Enter キーを押してシステムのデフォルト値をそのまま使用するか 'no' と入力してから Enter キーを押して '独自の値を入力します
5. プロンプトに従って \* Cluster Setup \* ウィザードを完了し、Enter キーを押してデフォルト値をそのまま使用するか、独自の値を入力して Enter キーを押します。

デフォルト値は、プラットフォームとネットワークの構成に基づいて自動的に決定されます。

6. クラスタセットアップ \* ウィザードが完了したら、次のコマンドを入力して、クラスタがアクティブで、最初のノードが正常に機能していることを確認します

「cluster show」を参照してください

次の例は、第 1 ノードが含まれるクラスタ（cluster1-01）が正常に機能しており、クラスタへの参加条件を満たしていることを示しています。

```
cluster1::> cluster show
Node                               Health  Eligibility
-----
cluster1-01                        true    true
```

管理 SVM やノード SVM に対する設定に変更が必要になった場合は、cluster setup コマンドを使用してクラスタセットアップウィザードにアクセスできます。

## 8 ノード / 4 ノード MetroCluster 構成での ONTAP のセットアップ

各ノードをブートすると、System Setup ツールを使用してノードおよびクラスタの基本的な設定を実行するよう求めるメッセージが表示されます。クラスタを設定したら、ONTAP CLI に戻ってアグリゲートを作成し、MetroCluster 構成を作成します。

作業を開始する前に

MetroCluster 構成のケーブル接続を完了しておく必要があります。

このタスクについて

このタスクは、ネットアップの標準のストレージを使用した 8 ノード / 4 ノード MetroCluster 構成が対象です。

新規で購入した MetroCluster システムは事前に設定されており、ここで説明する手順を実行する必要はありません。ただし、AutoSupport ツールを設定する必要があります。

このタスクは、MetroCluster 構成の両方のクラスタで実行する必要があります。

この手順では、System Setup ツールを使用します。必要に応じて、CLI クラスタセットアップウィザードを使用することもできます。

#### 手順

1. 各ノードに電源が入っていない場合は、電源を投入してブートします。

システムが保守モードになっている場合は問題、halt コマンドを使用して保守モードを終了し、次に LOADER プロンプトで次のコマンドを問題します。

```
「 boot_ontap 」
```

次のような出力が表示されます。

```
Welcome to node setup

You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the setup wizard.
                Any changes you made before quitting will be saved.

To accept a default or omit a question, do not enter a value.
.
.
.
```

2. システムの指示に従って AutoSupport ツールを有効にします。
3. プロンプトに従ってノード管理インターフェイスを設定します。

次のようなプロンプトが表示されます。

```
Enter the node management interface port: [e0M]:
Enter the node management interface IP address: 10.228.160.229
Enter the node management interface netmask: 225.225.252.0
Enter the node management interface default gateway: 10.228.160.1
```

4. ノードがハイアベイラビリティモードで設定されていることを確認します。

「 storage failover show -fields mode 」を選択します

そうでない場合は、各ノードで次のコマンドを問題処理してノードをリブートする必要があります。

「 storage failover modify -mode ha -node localhost 」を参照してください

このコマンドを実行するとハイアベイラビリティモードが設定されますが、ストレージフェイルオーバー

は有効になりません。ストレージフェイルオーバーは、あとで実行する MetroCluster の設定プロセスで自動的に有効になります。

5. クラスタインターコネクトとして4つのポートが構成されていることを確認します。

「network port show」のように表示されます

次の例は、cluster\_A の出力を示しています。

```
cluster_A::> network port show
```

|             |       |         |           |        |       |       | Speed      |
|-------------|-------|---------|-----------|--------|-------|-------|------------|
| (Mbps)      |       |         |           |        |       |       |            |
| Node        | Port  | IPspace | Broadcast | Domain | Link  | MTU   | Admin/Oper |
| -----       | ----- | -----   | -----     | -----  | ----- | ----- | -----      |
| node_A_1    |       |         |           |        |       |       |            |
|             | **e0a | Cluster | Cluster   |        | up    | 1500  |            |
| auto/1000   | e0b   | Cluster | Cluster   |        | up    | 1500  |            |
| auto/1000** | e0c   | Default | Default   |        | up    | 1500  | auto/1000  |
|             | e0d   | Default | Default   |        | up    | 1500  | auto/1000  |
|             | e0e   | Default | Default   |        | up    | 1500  | auto/1000  |
|             | e0f   | Default | Default   |        | up    | 1500  | auto/1000  |
|             | e0g   | Default | Default   |        | up    | 1500  | auto/1000  |
| node_A_2    |       |         |           |        |       |       |            |
|             | **e0a | Cluster | Cluster   |        | up    | 1500  |            |
| auto/1000   | e0b   | Cluster | Cluster   |        | up    | 1500  |            |
| auto/1000** | e0c   | Default | Default   |        | up    | 1500  | auto/1000  |
|             | e0d   | Default | Default   |        | up    | 1500  | auto/1000  |
|             | e0e   | Default | Default   |        | up    | 1500  | auto/1000  |
|             | e0f   | Default | Default   |        | up    | 1500  | auto/1000  |
|             | e0g   | Default | Default   |        | up    | 1500  | auto/1000  |

14 entries were displayed.

6. 2 ノードスイッチレスクラスタ（クラスタインターコネクトスイッチのないクラスタ）を作成する場合は、switchless-cluster ネットワークモードを有効にします。

- a. advanced 権限レベルに切り替えます。

「advanced」の権限が必要です

advanced モードで続行するかどうかを確認するプロンプトが表示されたら、「y」と入力します。advanced モードのプロンプトが表示されます（\*>）。

- a. switchless-cluster モードを有効にします。

```
network options switchless-cluster modify -enabled true
```

- b. admin 権限レベルに戻ります。

「特権管理者」

7. 最初のブート後にシステムコンソールに表示される情報に従って、System Setup ツールを起動します。
8. System Setup ツールを使用して各ノードを設定し、クラスタを作成します。ただし、アグリゲートは作成しないでください。



後続のタスクでミラーされたアグリゲートを作成します。

完了後

ONTAP のコマンドラインインターフェイスに戻り、後続のタスクを実行して MetroCluster の設定を完了します。

## クラスタを **MetroCluster** 構成に設定

クラスタをピアリングし、ルートアグリゲートをミラーリングし、ミラーリングされたデータアグリゲートを作成し、コマンドを問題して MetroCluster の処理を実装する必要があります。

このタスクについて

を実行する前に `metrocluster configure`、HAモードおよびDRミラーリングが有効になっていないため、この想定動作に関連するエラーメッセージが表示される場合があります。HAモードとDRミラーリングは、あとでコマンドを実行するときに有効にします `metrocluster configure` をクリックして構成を実装してください。

クラスタをピアリング

MetroCluster 構成内のクラスタが相互に通信し、MetroCluster ディザスタリカバリに不可欠なデータミラーリングを実行できるようにするために、クラスタ間にはピア関係が必要です。

クラスタ間 LIF を設定しています

MetroCluster パートナークラスタ間の通信に使用するポートにクラスタ間 LIF を作成する必要があります。専用のポートを使用することも、データトラフィック用を兼ねたポートを使用することもできます。

選択肢

- [専用ポートでのクラスタ間 LIF の設定](#)
- [共有データポートでのクラスタ間 LIF の設定](#)

専用ポートでのクラスタ間 LIF の設定

専用ポートにクラスタ間 LIF を設定できます。通常は、レプリケーショントラフィックに使用できる帯域幅が増加します。

手順

1. クラスタ内のポートの一覧を表示します。

「network port show」のように表示されます

コマンド構文全体については、マニュアルページを参照してください。

次の例は、「cluster01」内のネットワークポートを示しています。

```
cluster01::> network port show
```

| (Mbps)       |      |         |           |        |      |      | Speed      |
|--------------|------|---------|-----------|--------|------|------|------------|
| Node         | Port | IPspace | Broadcast | Domain | Link | MTU  | Admin/Oper |
| -----        |      |         |           |        |      |      |            |
| cluster01-01 |      |         |           |        |      |      |            |
|              | e0a  | Cluster | Cluster   |        | up   | 1500 | auto/1000  |
|              | e0b  | Cluster | Cluster   |        | up   | 1500 | auto/1000  |
|              | e0c  | Default | Default   |        | up   | 1500 | auto/1000  |
|              | e0d  | Default | Default   |        | up   | 1500 | auto/1000  |
|              | e0e  | Default | Default   |        | up   | 1500 | auto/1000  |
|              | e0f  | Default | Default   |        | up   | 1500 | auto/1000  |
| cluster01-02 |      |         |           |        |      |      |            |
|              | e0a  | Cluster | Cluster   |        | up   | 1500 | auto/1000  |
|              | e0b  | Cluster | Cluster   |        | up   | 1500 | auto/1000  |
|              | e0c  | Default | Default   |        | up   | 1500 | auto/1000  |
|              | e0d  | Default | Default   |        | up   | 1500 | auto/1000  |
|              | e0e  | Default | Default   |        | up   | 1500 | auto/1000  |
|              | e0f  | Default | Default   |        | up   | 1500 | auto/1000  |

2. クラスタ間通信専用で使用可能なポートを特定します。

network interface show -fields home-port、 curr -port

コマンド構文全体については、マニュアルページを参照してください。

次の例は、ポート e0e とポート e0f に LIF が割り当てられていないことを示しています。

```

cluster01::> network interface show -fields home-port,curr-port
vserver lif                home-port curr-port
-----
Cluster cluster01-01_clus1 e0a        e0a
Cluster cluster01-01_clus2 e0b        e0b
Cluster cluster01-02_clus1 e0a        e0a
Cluster cluster01-02_clus2 e0b        e0b
cluster01
      cluster_mgmt         e0c        e0c
cluster01
      cluster01-01_mgmt1   e0c        e0c
cluster01
      cluster01-02_mgmt1   e0c        e0c

```

### 3. 専用ポートのフェイルオーバーグループを作成します。

「network interface failover-groups create -vserver\_system\_svm」 -failover-group\_failover\_group\_ -targets\_physical\_or\_logical\_ports\_」

次の例は、ポート「e0e」と「e0f」を、システム「SVMcluster01」上のフェイルオーバーグループ intercluster01 に割り当てます。

```

cluster01::> network interface failover-groups create -vserver cluster01
-failover-group
intercluster01 -targets
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f

```

### 4. フェイルオーバーグループが作成されたことを確認します。

「network interface failover-groups show」と表示されます

コマンド構文全体については、マニュアルページを参照してください。

```

cluster01::> network interface failover-groups show

```

| Vserver   | Group          | Failover Targets                                                                                                                                       |
|-----------|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cluster   | Cluster        | cluster01-01:e0a, cluster01-01:e0b,<br>cluster01-02:e0a, cluster01-02:e0b                                                                              |
| cluster01 | Default        | cluster01-01:e0c, cluster01-01:e0d,<br>cluster01-02:e0c, cluster01-02:e0d,<br>cluster01-01:e0e, cluster01-01:e0f<br>cluster01-02:e0e, cluster01-02:e0f |
|           | intercluster01 | cluster01-01:e0e, cluster01-01:e0f<br>cluster01-02:e0e, cluster01-02:e0f                                                                               |

5. システム SVM にクラスタ間 LIF を作成して、フェイルオーバーグループに割り当てます。

#### ONTAP 9.6 以降

「`network interface create -vserver system_svm _ -lif_lif_name_service-policy default -intercluster -home-node _-home-port _ -port_IP_address _port_ip-netmask netmask _ -failover-group _``」のようになります

#### ONTAP 9.5 以前

「`network interface create -vserver_system_SVM_lif_lif_name — ー ル intercluster -home-node node_name のクラスタ間ホームポートポート _port-address port_ip-netmask netmask_—failover-group_failover_group_name`」

コマンド構文全体については、マニュアルページを参照してください。

次の例は、フェイルオーバーグループ「intercluster01」にクラスタ間 LIF 「cluster01\_icl01」と「cluster01\_icl02」を作成します。

```

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0 -failover-group intercluster01

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0 -failover-group intercluster01

```

6. クラスタ間 LIF が作成されたことを確認します。

**ONTAP 9.6 以降**

次のコマンドを実行します。network interface show -service-policy default-intercluster

**ONTAP 9.5 以前**

次のコマンドを実行します。network interface show -role intercluster

コマンド構文全体については、マニュアルページを参照してください。

```

cluster01::> network interface show -service-policy default-intercluster

```

| Current Is | Logical         | Status     | Network          | Current          |
|------------|-----------------|------------|------------------|------------------|
| Vserver    | Interface       | Admin/Oper | Address/Mask     | Node             |
| Home       |                 |            |                  | Port             |
| cluster01  | cluster01_icl01 | up/up      | 192.168.1.201/24 | cluster01-01 e0e |
| true       | cluster01_icl02 | up/up      | 192.168.1.202/24 | cluster01-02 e0f |
| true       |                 |            |                  |                  |

7. クラスタ間 LIF が冗長構成になっていることを確認します。

### ONTAP 9.6 以降

次のコマンドを実行します。network interface show -service-policy default-intercluster -failover

### ONTAP 9.5 以前

次のコマンドを実行します。network interface show -role intercluster -failover

コマンド構文全体については、マニュアルページを参照してください。

次の例は、SVM 「e0e」ポート上のクラスタ間 LIF 「cluster01\_icl01」と「cluster01\_icl02」が「e0f」ポートにフェイルオーバーされることを示しています。

```
cluster01::> network interface show -service-policy default-intercluster
-failover
          Logical          Home          Failover          Failover
Vserver  Interface          Node:Port      Policy            Group
-----  -
cluster01
          cluster01_icl01 cluster01-01:e0e  local-only
intercluster01
          Failover Targets: cluster01-01:e0e,
                           cluster01-01:e0f
          cluster01_icl02 cluster01-02:e0e  local-only
intercluster01
          Failover Targets: cluster01-02:e0e,
                           cluster01-02:e0f
```

## 関連情報

### "専用のポートを使用する場合の考慮事項"

専用のポートを使用することが適切なクラスタ間ネットワーク解決策であるかどうかを判断するには、LAN のタイプ、利用可能な WAN 帯域幅、レプリケーション間隔、変更率、ポート数などの設定や要件を考慮する必要があります。

### 共有データポートでのクラスタ間 LIF の設定

データネットワークと共有するポートにクラスタ間 LIF を設定できます。これにより、クラスタ間ネットワークに必要なポート数を減らすことができます。

### 手順

1. クラスタ内のポートの一覧を表示します。

「network port show」のように表示されます

コマンド構文全体については、マニュアルページを参照してください。

次の例は、 cluster01 内のネットワークポートを示しています。

```
cluster01::> network port show
```

| (Mbps)       |      | Speed   |                  |      |      |            |
|--------------|------|---------|------------------|------|------|------------|
| Node         | Port | IPspace | Broadcast Domain | Link | MTU  | Admin/Oper |
| -----        |      |         |                  |      |      |            |
| cluster01-01 |      |         |                  |      |      |            |
|              | e0a  | Cluster | Cluster          | up   | 1500 | auto/1000  |
|              | e0b  | Cluster | Cluster          | up   | 1500 | auto/1000  |
|              | e0c  | Default | Default          | up   | 1500 | auto/1000  |
|              | e0d  | Default | Default          | up   | 1500 | auto/1000  |
| cluster01-02 |      |         |                  |      |      |            |
|              | e0a  | Cluster | Cluster          | up   | 1500 | auto/1000  |
|              | e0b  | Cluster | Cluster          | up   | 1500 | auto/1000  |
|              | e0c  | Default | Default          | up   | 1500 | auto/1000  |
|              | e0d  | Default | Default          | up   | 1500 | auto/1000  |

## 2. システム SVM にクラスタ間 LIF を作成します。

### ONTAP 9.6 以降

次のコマンドを実行します。 `network interface create -vserver system_SVM -lif LIF_name -service-policy default-intercluster -home-node node -home-port port -address port_IP -netmask netmask`

### ONTAP 9.5 以前

次のコマンドを実行します。 `network interface create -vserver system_SVM -lif LIF_name -role intercluster -home-node node -home-port port -address port_IP -netmask netmask`

コマンド構文全体については、マニュアルページを参照してください。次の例は、クラスタ間 LIF cluster01\_icl01 と cluster01\_icl02 を作成します。

```

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0

```

### 3. クラスタ間 LIF が作成されたことを確認します。

#### ONTAP 9.6 以降

次のコマンドを実行します。network interface show -service-policy default-intercluster

#### ONTAP 9.5 以前

次のコマンドを実行します。network interface show -role intercluster

コマンド構文全体については、マニュアルページを参照してください。

```

cluster01::> network interface show -service-policy default-intercluster

```

| Current Is | Logical         | Status     | Network          | Current          |
|------------|-----------------|------------|------------------|------------------|
| Vserver    | Interface       | Admin/Oper | Address/Mask     | Node             |
| Home       |                 |            |                  | Port             |
| cluster01  | cluster01_icl01 | up/up      | 192.168.1.201/24 | cluster01-01 e0c |
| true       | cluster01_icl02 | up/up      | 192.168.1.202/24 | cluster01-02 e0c |
| true       |                 |            |                  |                  |

### 4. クラスタ間 LIF が冗長構成になっていることを確認します。

### ONTAP 9.6 以降

次のコマンドを実行します。network interface show -service-policy default-intercluster -failover

### ONTAP 9.5 以前

次のコマンドを実行します。network interface show -role intercluster -failover

コマンド構文全体については、マニュアルページを参照してください。

次の例は、「e0c」ポート上のクラスタ間 LIF 「cluster01\_icl01」と「cluster01\_icl02」が「e0d」ポートにフェイルオーバーされることを示しています。

```
cluster01::> network interface show -service-policy default-intercluster
-failover
          Logical          Home          Failover          Failover
Vserver  Interface          Node:Port      Policy            Group
-----  -
cluster01
          cluster01_icl01 cluster01-01:e0c  local-only
192.168.1.201/24
                                     Failover Targets: cluster01-01:e0c,
   cluster01-01:e0d
          cluster01_icl02 cluster01-02:e0c  local-only
192.168.1.201/24
                                     Failover Targets: cluster01-02:e0c,
   cluster01-02:e0d
```

## 関連情報

["データポートを共有する場合の考慮事項"](#)

## クラスタピア関係を作成

MetroCluster クラスタ間にクラスタピア関係を作成する必要があります。

## このタスクについて

cluster peer create コマンドを使用すると、ローカルクラスタとリモートクラスタ間にピア関係を作成できます。ピア関係が作成されたら 'リモート・クラスタ上で cluster peer create を実行して' ローカル・クラスタに対してピア関係を認証できます

## 作業を開始する前に

- ピア関係にあるクラスタ内の各ノードでクラスタ間 LIF を作成しておく必要があります。
- クラスタで ONTAP 9.3 以降が実行されている必要があります。

## 手順

1. デスティネーションクラスタで、ソースクラスタとのピア関係を作成します。

```
cluster peer create -generate-passphrase -offer-expiration_mm/dd/YYYY HH : MM : SS|1...7days|1...168hours_-peer-addr_ peer_lif_ips_-ipospace_ips_`
```

「-generate-passphrase」と「-peer-addr」の両方を指定した場合、生成されたパスワードを使用できるのは、「-peer-addr」にクラスタ間 LIF が指定されているクラスタだけです。

カスタム IPspace を使用しない場合は、-ipospace オプションを無視してかまいません。コマンド構文全体については、マニュアルページを参照してください。

次の例は、リモートクラスタを指定せずにクラスタピア関係を作成します。

```
cluster02::> cluster peer create -generate-passphrase -offer-expiration
2days

                Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
                Expiration Time: 6/7/2017 08:16:10 EST
Initial Allowed Vserver Peers: -
                Intercluster LIF IP: 192.140.112.101
                Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed again.
```

2. ソースクラスタで、ソースクラスタをデスティネーションクラスタに対して認証します。

```
'cluster peer create -peer-addr_ peer_lif_ips-ipospace ips'
```

コマンド構文全体については、マニュアルページを参照してください。

次の例は、クラスタ間 LIF の IP アドレス「192.140.112.101」および「192.140.112.102」でローカルクラスタをリモートクラスタに対して認証します。

```
cluster01::> cluster peer create -peer-addr
192.140.112.101,192.140.112.102

Notice: Use a generated passphrase or choose a passphrase of 8 or more
characters.

                To ensure the authenticity of the peering relationship, use a
                phrase or sequence of characters that would be hard to guess.

Enter the passphrase:
Confirm the passphrase:

Clusters cluster02 and cluster01 are peered.
```

プロンプトが表示されたら、ピア関係のパスフレーズを入力します。

3. クラスピア関係が作成されたことを確認します。

「cluster peer show -instance」のように表示されます

```
cluster01::> cluster peer show -instance

Peer Cluster Name: cluster02
Remote Intercluster Addresses: 192.140.112.101,
192.140.112.102
Availability of the Remote Cluster: Available
Remote Cluster Name: cluster2
Active IP Addresses: 192.140.112.101,
192.140.112.102

Cluster Serial Number: 1-80-123456
Address Family of Relationship: ipv4
Authentication Status Administrative: no-authentication
Authentication Status Operational: absent
Last Update Time: 02/05 21:05:41
IPspace for the Relationship: Default
```

4. ピア関係にあるノードの接続状態とステータスを確認します。

cluster peer health show

```
cluster01::> cluster peer health show
Node          cluster-Name          Node-Name
          Ping-Status          RDB-Health Cluster-Health Avail...
-----
cluster01-01
          cluster02          cluster02-01
          Data: interface_reachable
          ICMP: interface_reachable true          true          true
          cluster02-02
          Data: interface_reachable
          ICMP: interface_reachable true          true          true
cluster01-02
          cluster02          cluster02-01
          Data: interface_reachable
          ICMP: interface_reachable true          true          true
          cluster02-02
          Data: interface_reachable
          ICMP: interface_reachable true          true          true
```

## クラスタピア関係の作成 ( ONTAP 9.2 以前)

「 cluster peer create 」 コマンドを使用して、ローカルクラスタとリモートクラスタ間のピア関係の要求を開始できます。ピア関係がローカルクラスタによって要求された後、リモートクラスタ上で cluster peer create を実行して、関係を受け入れることができます。

作業を開始する前に

- ピア関係にあるクラスタ内の各ノードでクラスタ間 LIF を作成しておく必要があります。
- クラスタ管理者は、各クラスタが他のクラスタに対して自身を認証する際に使用するパスフレーズに同意しておく必要があります。

手順

1. データ保護のデスティネーションクラスタで、データ保護のソースクラスタとのピア関係を作成します。

```
'cluster peer create -peer-addr _peer_lif_ips_ -ip space_`
```

カスタム IPspace を使用しない場合は、 -ip space オプションを無視してかまいません。コマンド構文全体については、マニュアルページを参照してください。

次の例は、クラスタ間 LIF の IP アドレス「 192.168.2.201 」および「 192.168.2.202 」で、リモートクラスタとのクラスタピア関係を作成します。

```
cluster02::> cluster peer create -peer-addr 192.168.2.201,192.168.2.202
Enter the passphrase:
Please enter the passphrase again:
```

プロンプトが表示されたら、ピア関係のパスフレーズを入力します。

2. データ保護のソースクラスタで、ソースクラスタをデスティネーションクラスタに対して認証します。

```
'cluster peer create -peer-addr _peer_lif_ips_ -ip space_`
```

コマンド構文全体については、マニュアルページを参照してください。

次の例は、クラスタ間 LIF の IP アドレス「 192.140.112.203 」および「 192.140.112.204 」でローカルクラスタをリモートクラスタに対して認証します。

```
cluster01::> cluster peer create -peer-addr 192.168.2.203,192.168.2.204
Please confirm the passphrase:
Please confirm the passphrase again:
```

プロンプトが表示されたら、ピア関係のパスフレーズを入力します。

3. クラスタピア関係が作成されたことを確認します。

```
cluster peer show - instance
```

コマンド構文全体については、マニュアルページを参照してください。

```
cluster01::> cluster peer show -instance
Peer Cluster Name: cluster01
Remote Intercluster Addresses: 192.168.2.201,192.168.2.202
Availability: Available
Remote Cluster Name: cluster02
Active IP Addresses: 192.168.2.201,192.168.2.202
Cluster Serial Number: 1-80-000013
```

#### 4. ピア関係にあるノードの接続状態とステータスを確認します。

```
cluster peer health show
```

コマンド構文全体については、マニュアルページを参照してください。

```
cluster01::> cluster peer health show
Node          cluster-Name          Node-Name
              Ping-Status           RDB-Health Cluster-Health Avail...
-----
-----
cluster01-01
              cluster02          cluster02-01
              Data: interface_reachable
              ICMP: interface_reachable true          true          true
              cluster02-02
              Data: interface_reachable
              ICMP: interface_reachable true          true          true
cluster01-02
              cluster02          cluster02-01
              Data: interface_reachable
              ICMP: interface_reachable true          true          true
              cluster02-02
              Data: interface_reachable
              ICMP: interface_reachable true          true          true
```

### ルートアグリゲートをミラーリング

データ保護を提供するには、ルートアグリゲートをミラーする必要があります。

このタスクについて

デフォルトでは、ルートアグリゲートは RAID-DP タイプのアグリゲートとして作成されます。ルートアグリゲートのタイプは RAID-DP から RAID4 に変更することができます。次のコマンドは、ルートアグリゲートを RAID4 タイプのアグリゲートに変更します。

```
storage aggregate modify -aggregate aggr_name -raidtype raid4
```



ADP 以外のシステムでは、ミラーリングの実行前後に、アグリゲートの RAID タイプをデフォルトの RAID-DP から RAID4 に変更できます。

#### 手順

1. ルートアグリゲートをミラーします。

「storage aggregate mirror aggr\_name」のようになります

次のコマンドでは、controller\_A\_1 のルートアグリゲートがミラーされます。

```
controller_A_1::> storage aggregate mirror aggr0_controller_A_1
```

これによりアグリゲートがミラーされるため、ローカルのプレックスとリモートのプレックスがリモートの MetroCluster サイトに配置されたアグリゲートが作成されます。

2. MetroCluster 構成の各ノードについて、同じ手順を繰り返します。

#### 関連情報

##### "CLI を使用した論理ストレージ管理"

各ノードでミラーされたデータアグリゲートを作成します

DR グループの各ノードに、ミラーされたデータアグリゲートを 1 つ作成する必要があります。

- 新しいアグリゲートで使用するドライブを把握しておく必要があります。
- 複数のドライブタイプを含むシステム（異機種混在ストレージ）の場合は、正しいドライブタイプが選択されるようにする方法を確認しておく必要があります。
- ドライブは特定のノードによって所有されます。アグリゲートを作成する場合、アグリゲート内のすべてのドライブは同じノードによって所有される必要があります。そのノードが、作成するアグリゲートのホームノードになります。
- アグリゲート名は、MetroCluster 構成を計画する際に決定した命名規則に従う必要があります。を参照してください ["ディスクおよびアグリゲートの管理"](#)。
- アグリゲート名は、MetroCluster サイト全体で一意である必要があります。つまり、サイト A とサイト B に同じ名前を持つ 2 つの異なるデータ アグリゲートを持つことはできません。

#### 手順

1. 使用可能なスペアのリストを表示します。

「storage disk show -spare -owner node\_name」という名前になります

2. storage aggregate create -mirror true コマンドを使用して、アグリゲートを作成します。

クラスタ管理インターフェイスでクラスタにログインした場合、クラスタ内の任意のノードにアグリゲートを作成できます。アグリゲートを特定のノード上に作成するには、「-node」パラメータを使用する

か、そのノードが所有するドライブを指定します。

次のオプションを指定できます。

- アグリゲートのホームノード（通常運用時にアグリゲートを所有するノード）
- アグリゲートに追加するドライブのリスト
- 追加するドライブ数



最小サポート構成では、使用可能なドライブ数が制限されていますが、3つのディスク RAID-DP アグリゲートを作成できるようにするには、「force-small-aggregate」オプションを使用する必要があります。

- アグリゲートに使用するチェックサム形式
- 使用するドライブのタイプ
- 使用するドライブのサイズ
- 使用するドライブの速度
- アグリゲート上の RAID グループの RAID タイプ
- RAID グループに含めることができるドライブの最大数
- RPM の異なるドライブが許可されるかどうか

これらのオプションの詳細については 'storage aggregate create のマニュアルページを参照してください

次のコマンドでは、10本のディスクを含むミラーアグリゲートが作成されます。

```
cluster_A::> storage aggregate create aggr1_node_A_1 -diskcount 10 -node
node_A_1 -mirror true
[Job 15] Job is queued: Create aggr1_node_A_1.
[Job 15] The job is starting.
[Job 15] Job succeeded: DONE
```

### 3. 新しいアグリゲートの RAID グループとドライブを確認します。

「storage aggregate show-status -aggregate \_aggregate-name \_」を参照してください

#### ミラーされていないデータアグリゲートの作成

MetroCluster 構成が提供する冗長なミラーリングを必要としないデータについては、必要に応じてミラーされていないデータアグリゲートを作成できます。

#### 作業を開始する前に

- 新しいアグリゲートで使用されるドライブを把握していることを確認します。
- 複数のドライブタイプを含むシステム（異機種混在ストレージ）の場合は、正しいドライブタイプが選択されていることを確認する方法を理解しておく必要があります。



MetroCluster FC 構成では、ミラーされていないアグリゲートがスイッチオーバー後にオンラインになるのは、アグリゲート内のリモートディスクにアクセスできる場合のみです。ISL で障害が発生すると、ミラーされていないリモートディスク内のデータにローカルノードがアクセスできなくなる可能性があります。アグリゲートに障害が発生すると、ローカルノードがリブートされる場合があります。

- ドライブは特定のノードによって所有されます。アグリゲートを作成する場合、アグリゲート内のすべてのドライブは同じノードによって所有される必要があります。そのノードが、作成するアグリゲートのホームノードになります。



ミラーされていないアグリゲートは、そのアグリゲートを所有するノードに対してローカルでなければなりません。

- アグリゲート名は、MetroCluster 構成を計画する際に決定した命名規則に従う必要があります。
- `_Disks and aggregates management_` アグリゲートのミラーリングの詳細については、を参照してください。

## 手順

1. 使用可能なスペアのリストを表示します。

「`storage disk show -spare -owner_node_name _`」というように入力します

2. アグリゲートを作成します。

「`storage aggregate create`」

クラスタ管理インターフェイスでクラスタにログインした場合、クラスタ内の任意のノードにアグリゲートを作成できます。アグリゲートが特定のノード上に作成されていることを確認するには、「`-node`」パラメータを使用するか、そのノードが所有するドライブを指定します。

次のオプションを指定できます。

- アグリゲートのホームノード（通常運用時にアグリゲートを所有するノード）
- アグリゲートに追加するドライブのリスト
- 追加するドライブ数
- アグリゲートに使用するチェックサム形式
- 使用するドライブのタイプ
- 使用するドライブのサイズ
- 使用するドライブの速度
- アグリゲート上の RAID グループの RAID タイプ
- RAID グループに含めることができるドライブの最大数
- RPM の異なるドライブが許可されるかどうか

これらのオプションの詳細については、`storage aggregate create` のマニュアルページを参照してください。

次のコマンドでは、10本のディスクを含むミラーされていないアグリゲートが作成さ

```
controller_A_1::> storage aggregate create aggr1_controller_A_1
-diskcount 10 -node controller_A_1
[Job 15] Job is queued: Create aggr1_controller_A_1.
[Job 15] The job is starting.
[Job 15] Job succeeded: DONE
```

3. 新しいアグリゲートの RAID グループとドライブを確認します。

「storage aggregate show-status -aggregate \_aggregate-name \_」を参照してください

関連情報

["ディスクと階層（アグリゲート）の管理"](#)

### MetroCluster 構成の実装

MetroCluster 構成でデータ保護を開始するに MetroCluster は 'data configure コマンド' を実行する必要があります

作業を開始する前に

- ルート以外のミラーされたデータアグリゲートが各クラスタに少なくとも2つ必要です。

その他のデータアグリゲートはミラーされていてもいなくてもかまいません。

これは「storage aggregate show」コマンドで確認できます。



ミラーされた単一のデータアグリゲートを使用する場合は、を参照してください [手順 1. 手順](#)については、を参照し

- コントローラおよびシャーシの ha-config の状態が「mcc」である必要があります。

このタスクについて

MetroCluster 構成を有効にするには '任意のノードで MetroCluster configure コマンド' を1回実行します問題サイトごとまたはノードごとにコマンドを問題で実行する必要はありません。また、問題するノードまたはサイトはどれでもかまいません。

MetroCluster configure コマンドを実行すると '2つのクラスタそれぞれのシステム ID が最も小さい2つのノードが 'DR（災害復旧）パートナーとして自動的にペア設定されます4ノード MetroCluster 構成の場合は、DR パートナーのペアは2組になります。2つ目の DR ペアは、システム ID が大きい2つのノードで作成されます。



コマンド 'MetroCluster configure' を実行する前に 'Onboard Key Manager（OKM；オンボードキーマネージャ）または外部キー管理を構成しないでください

手順

1. 次の形式で MetroCluster を設定します。

| MetroCluster 構成の内容   | 操作                                                                                                                                                                                                                                                                                                                                                                |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 複数のデータアグリゲート         | <p>いずれかのノードのプロンプトで、MetroCluster を設定します。</p> <p>MetroCluster configure node-name</p>                                                                                                                                                                                                                                                                               |
| ミラーされた 1 つのデータアグリゲート | <p>a. いずれかのノードのプロンプトで、advanced 権限レベルに切り替えます。</p> <p>「advanced」の権限が必要です</p> <p>advanced モードで続行するかどうかを尋ねられたら、「y」と入力して応答する必要があります。advanced モードのプロンプト (*&gt;) が表示されます。</p> <p>b. MetroCluster に -allow-with-one-aggregate true パラメータを設定します。</p> <p>「MetroCluster configure -allow-with-one -aggregate true_node-name_」</p> <p>c. admin 権限レベルに戻ります。</p> <p>「特権管理者」</p> |



複数のデータアグリゲートを使用することを推奨します。最初の DR グループにアグリゲートが 1 つしかなく、1 つのアグリゲートを含む DR グループを追加する場合は、メタデータボリュームを単一のデータアグリゲートから移動する必要があります。この手順の詳細については、を参照してください ["MetroCluster 構成でのメタデータボリュームの移動"](#)。

次のコマンドは、controller\_A\_1 を含む DR グループ内のすべてのノードの MetroCluster 構成を有効にします。

```
cluster_A::*> metrocluster configure -node-name controller_A_1

[Job 121] Job succeeded: Configure is successful.
```

## 2. サイト A のネットワークステータスを確認します。

「network port show」のように表示されます

次の例は、4 ノード MetroCluster 構成でのネットワークポートの用途を示しています。

```

cluster_A::> network port show

```

| Node           | Port | IPspace | Broadcast Domain | Link | MTU  | Speed (Mbps)<br>Admin/Oper |
|----------------|------|---------|------------------|------|------|----------------------------|
| -----          |      |         |                  |      |      |                            |
| controller_A_1 |      |         |                  |      |      |                            |
|                | e0a  | Cluster | Cluster          | up   | 9000 | auto/1000                  |
|                | e0b  | Cluster | Cluster          | up   | 9000 | auto/1000                  |
|                | e0c  | Default | Default          | up   | 1500 | auto/1000                  |
|                | e0d  | Default | Default          | up   | 1500 | auto/1000                  |
|                | e0e  | Default | Default          | up   | 1500 | auto/1000                  |
|                | e0f  | Default | Default          | up   | 1500 | auto/1000                  |
|                | e0g  | Default | Default          | up   | 1500 | auto/1000                  |
| controller_A_2 |      |         |                  |      |      |                            |
|                | e0a  | Cluster | Cluster          | up   | 9000 | auto/1000                  |
|                | e0b  | Cluster | Cluster          | up   | 9000 | auto/1000                  |
|                | e0c  | Default | Default          | up   | 1500 | auto/1000                  |
|                | e0d  | Default | Default          | up   | 1500 | auto/1000                  |
|                | e0e  | Default | Default          | up   | 1500 | auto/1000                  |
|                | e0f  | Default | Default          | up   | 1500 | auto/1000                  |
|                | e0g  | Default | Default          | up   | 1500 | auto/1000                  |

14 entries were displayed.

3. MetroCluster 構成の両方のサイトから MetroCluster 構成を確認します。

a. サイト A から構成を確認します。

「 MetroCluster show 」

```

cluster_A::> metrocluster show

```

| Cluster           | Entry Name          | State            |
|-------------------|---------------------|------------------|
| -----             |                     |                  |
| Local: cluster_A  | Configuration state | configured       |
|                   | Mode                | normal           |
|                   | AUSO Failure Domain | auso-on-cluster- |
| disaster          |                     |                  |
| Remote: cluster_B | Configuration state | configured       |
|                   | Mode                | normal           |
|                   | AUSO Failure Domain | auso-on-cluster- |
| disaster          |                     |                  |

b. サイト B から構成を確認します。

「 MetroCluster show 」

```

cluster_B::> metrocluster show
Cluster                               Entry Name                               State
-----                               -
Local: cluster_B                      Configuration state configured
Mode                                   normal
AUSO Failure Domain                   auso-on-cluster-disaster
Remote: cluster_A                     Configuration state configured
Mode                                   normal
AUSO Failure Domain                   auso-on-cluster-disaster

```

## ONTAP ソフトウェアでのフレームのインオーダー配信またはアウトオブオーダー配信の設定

Fibre Channel（FC）スイッチの設定に応じて、フレームの In-Order Delivery（IOD；インオーダー配信）または Out-of-Order Delivery（OOD；アウトオブオーダー配信）のいずれかを設定する必要があります。

このタスクについて

FC スイッチが IOD に設定されている場合は、ONTAP ソフトウェアを IOD に設定する必要があります。同様に、FC スイッチが OOD に設定されている場合は、ONTAP を OOD に設定する必要があります。



設定を変更するには、コントローラをリブートする必要があります。

ステップ

1. ONTAP でのフレームの処理方法として IOD または OOD のいずれかを設定します。

◦ ONTAP では、デフォルトではフレームの IOD が有効になっています。設定の詳細を確認するには、次の手順を

i. advanced モードに切り替えます。

「高度」

ii. 設定を確認します。

MetroCluster インターコネクト・アダプタ・ショー

```

mcc4-b12_siteB:~*~> metrocluster interconnect adapter show
                        Adapter Link   Is OOD
Node                    Name      Type   Status Enabled? IP Address  Port
Number
-----
mcc4-b1                 fcvi_device_0  FC-VI  Up     false   17.0.1.2
6a
mcc4-b1                 fcvi_device_1  FC-VI  Up     false   18.0.0.2
6b
mcc4-b1                 mlx4_0         IB      Down   false   192.0.5.193
ib2a
mcc4-b1                 mlx4_0         IB      Up     false   192.0.5.194
ib2b
mcc4-b2                 fcvi_device_0  FC-VI  Up     false   17.0.2.2
6a
mcc4-b2                 fcvi_device_1  FC-VI  Up     false   18.0.1.2
6b
mcc4-b2                 mlx4_0         IB      Down   false   192.0.2.9
ib2a
mcc4-b2                 mlx4_0         IB      Up     false   192.0.2.10
ib2b
8 entries were displayed.

```

◦ フレームの OOD を設定するには、各ノードで次の手順を実行する必要があります。

i. advanced モードに切り替えます。

「高度」

ii. MetroCluster 構成の設定を確認します。

MetroCluster インターコネクト・アダプタ・ショー

```

mcc4-b12_siteB:*> metrocluster interconnect adapter show
                Adapter Link   Is OOD
Node            Adapter Name  Type   Status Enabled? IP Address
Port Number
-----
mcc4-b1        fcvi_device_0  FC-VI  Up     false  17.0.1.2
6a
mcc4-b1        fcvi_device_1  FC-VI  Up     false  18.0.0.2
6b
mcc4-b1        mlx4_0         IB     Down   false  192.0.5.193
ib2a
mcc4-b1        mlx4_0         IB     Up     false  192.0.5.194
ib2b
mcc4-b2        fcvi_device_0  FC-VI  Up     false  17.0.2.2
6a
mcc4-b2        fcvi_device_1  FC-VI  Up     false  18.0.1.2
6b
mcc4-b2        mlx4_0         IB     Down   false  192.0.2.9
ib2a
mcc4-b2        mlx4_0         IB     Up     false  192.0.2.10
ib2b
8 entries were displayed.

```

- iii. ノード「m cc4-b1」およびノード「m cc4-b0」で OOD を有効にします。

MetroCluster 相互接続アダプタ modify -Node\_node\_name --is-ood-enabled true

```

mcc4-b12_siteB:*> metrocluster interconnect adapter modify -node
mcc4-b1 -is-ood-enabled true
mcc4-b12_siteB:*> metrocluster interconnect adapter modify -node
mcc4-b2 -is-ood-enabled true

```

- i. 両方向でハイアベイラビリティ (HA) テイクオーバーを実行してコントローラをリブートします。
- ii. 設定を確認します。

MetroCluster インターコネクト・アダプタ・ショー

```

mcc4-b12_siteB::*> metrocluster interconnect adapter show
                        Adapter Link   Is OOD
Node                    Name      Type   Status Enabled? IP Address  Port
Number
-----
mcc4-b1                 fcvi_device_0  FC-VI  Up     true   17.0.1.2   6a
mcc4-b1                 fcvi_device_1  FC-VI  Up     true   18.0.0.2   6b
mcc4-b1                 mlx4_0         IB     Down   false  192.0.5.193  ib2a
mcc4-b1                 mlx4_0         IB     Up     false  192.0.5.194  ib2b
mcc4-b2                 fcvi_device_0  FC-VI  Up     true   17.0.2.2   6a
mcc4-b2                 fcvi_device_1  FC-VI  Up     true   18.0.1.2   6b
mcc4-b2                 mlx4_0         IB     Down   false  192.0.2.9   ib2a
mcc4-b2                 mlx4_0         IB     Up     false  192.0.2.10  ib2b
8 entries were displayed.

```

## MetroCluster 構成での SNMPv3 の設定

作業を開始する前に

認証プロトコルとプライバシープロトコルは、スイッチと ONTAP システムで同じである必要があります。

このタスクについて

ONTAP は現在、AES-128 暗号化をサポートしています。

手順

1. コントローラのプロンプトで各スイッチの SNMP ユーザを作成します。

'securitylogin create (セキュリティログインの作成

```

Controller_A_1::> security login create -user-or-group-name snmpv3user
-application snmp -authentication-method usm -role none -remote-switch
-ipaddress 10.10.10.10

```

2. サイトで必要に応じて、次のプロンプトに回答します。



EngineID の場合は、**ENTER** を押してデフォルト値を割り当てます。

```
Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,
sha2-256) [none]: sha

Enter the authentication protocol password (minimum 8 characters long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128) [none]:
aes128

Enter privacy protocol password (minimum 8 characters long):

Enter privacy protocol password again:
```



同じユーザ名を IP アドレスが異なる別のスイッチに追加できます。

### 3. 残りのスイッチの SNMP ユーザを作成します。

次の例は、IP アドレス 10.10.10.11 のスイッチのユーザ名を作成する方法を示しています。

```
Controller_A_1::> security login create -user-or-group-name snmpv3user
-application snmp -authentication-method usm -role none -remote-switch
-ipaddress 10.
10.10.11
```

### 4. ログインエントリがスイッチごとに 1 つずつあることを確認します。

「securitylogin show」を参照してください

```
Controller_A_1::> security login show -user-or-group-name snmpv3user
-fields remote-switch-ipaddress

vserver      user-or-group-name application authentication-method
remote-switch-ipaddress

-----
-----

node_A_1 SVM 1 snmpv3user      snmp      usm
10.10.10.10

node_A_1 SVM 2 snmpv3user      snmp      usm
10.10.10.11

node_A_1 SVM 3 snmpv3user      snmp      usm
10.10.10.12

node_A_1 SVM 4 snmpv3user      snmp      usm
10.10.10.13

4 entries were displayed.
```

5. スイッチのプロンプトで SNMPv3 を設定します。

### Brocadeスイッチ (FOS 9.0 以降)

```
snmpconfig --add snmpv3 -index <index> -user <user_name> -groupname <rw/ro>
-auth_proto <auth_protocol> -auth_passwd <auth_password> -priv_proto
<priv_protocol> -priv_passwd <priv_password>
```

### Brocadeスイッチ (FOS 8.x 以前)

「mpconfig — set snmpv3」

この例では、読み取り専用ユーザーを構成する方法を示します。必要に応じて RW ユーザーを調整できます。RO アクセスが必要な場合は、「User (ro):」の後に「snmpv3user」を指定します。

```
Switch-A1:admin> snmpconfig --set snmpv3
SNMP Informs Enabled (true, t, false, f): [false] true
SNMPv3 user configuration(snmp user not configured in FOS user
database will have physical AD and admin role as the default):
User (rw): [snmpadmin1]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/AES128(3)/AES256(4)]: (2..2) [2]
Engine ID: [00:00:00:00:00:00:00:00]
User (ro): [snmpuser2] snmpv3user
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [2]
Priv Protocol [DES(1)/noPriv(2)/AES128(3)/AES256(4)]: (2..2) [3]
```

### Cisco スイッチ

```
snmp-server user <user_name> auth [md5/sha/sha-256] <auth_password> priv
(aes-128) <priv_password>
```



また、未使用のアカウントにパスワードを設定して保護し、ONTAP リリースで最適な暗号化機能を使用する必要があります。

- 必要に応じて、残りのスイッチユーザに暗号化とパスワードを設定します。

### 健全性監視用の MetroCluster コンポーネントの設定

MetroCluster 構成のコンポーネントを監視するには、いくつかの特別な設定手順を実行する必要があります。



セキュリティを強化するために、NetAppでは、スイッチのヘルスを監視するようにSNMPv2またはSNMPv3を設定することを推奨します。

このタスクについて

これらのタスクは、FC-to-SAS ブリッジを使用するシステムにのみ適用されます。

Fabric OS 9.0.1以降では、Brocadeスイッチでのヘルス監視でSNMPv2はサポートされていません。代わりにSNMPv3を使用する必要があります。SNMPv3を使用している場合は、次のセクションに進む前に、ONTAPでSNMPv3を設定する必要があります。詳細については、を参照してください [MetroCluster 構成](#)

## での SNMPv3 の設定。



- ブリッジとノード管理 LIF は、他のソースからの干渉を避けるために専用のネットワークに配置する必要があります。
- 健全性監視に専用のネットワークを使用する場合は、各ノードのノード管理LIFをその専用のネットワーク内に配置する必要があります。

NetAppでは、MetroCluster FC構成のコンポーネントを監視するための次のツールのみがサポートされます。

- Brocade Network Advisor (BNA)
- Brocade SANnav
- Active IQ Config Advisor
- NetAppヘルスマモニタリング (ONTAP)
- MetroClusterデータコレクタ (MC\_DC)

### 健全性監視用の MetroCluster FC スイッチの設定

ファブリック接続 MetroCluster 構成の FC スイッチを監視するには、いくつかの設定手順を追加で実行する必要があります。



ONTAP 9.8以降では `storage switch`、コマンドが置き換えられ ``system switch fibre-channel`` ました。以降の手順ではコマンドを使用し ``storage switch`` ますが、ONTAP 9.8以降を実行している場合はコマンドを使用 ``system switch fibre-channel`` することを推奨します。

### 手順

1. 各 MetroCluster ノードに IP アドレスを指定してスイッチを追加します。

実行するコマンドは、SNMPv2とSNMPv3のどちらを使用しているかによって異なります。

**SNMPv3**を使用してスイッチを追加します。

```
storage switch add -address <ip_address> -snmp-version SNMPv3 -snmp  
-community-or-username <SNMP_user_configured_on_the_switch>
```

**SNMPv2**を使用してスイッチを追加します。

「 `storage switch add -address ipaddress` 」と入力します

このコマンドは、MetroCluster 構成の 4 つのスイッチすべてに対して繰り返す必要があります。



健全性監視では、Brocade 7840 FC スイッチと `NoISLPresent_Alert` を除くすべてのアラートがサポートされます

次の例は、IP アドレスが 10.10.10.10 のスイッチを追加するコマンドを示しています。

```
controller_A_1::> storage switch add -address 10.10.10.10
```

2. すべてのスイッチが適切に設定されたことを確認します。

「storage switch show」と表示されます

ポーリング間隔が 15 分であるため、すべてのデータが反映されるまで最大で 15 分かかる場合があります。

次の例は、MetroCluster FC スイッチが設定されたことを検証するコマンドを示しています。

```
controller_A_1::> storage switch show
Fabric          Switch Name      Vendor  Model          Switch WWN
Status
-----
-----
1000000533a9e7a6 brcd6505-fcs40  Brocade Brocade6505    1000000533a9e7a6
OK
1000000533a9e7a6 brcd6505-fcs42  Brocade Brocade6505    1000000533d3660a
OK
1000000533ed94d1 brcd6510-fcs44  Brocade Brocade6510    1000000533eda031
OK
1000000533ed94d1 brcd6510-fcs45  Brocade Brocade6510    1000000533ed94d1
OK
4 entries were displayed.

controller_A_1::>
```

スイッチの World Wide Name (WWN ; ワールドワイド名) が表示される場合は、ONTAP ヘルスマニタを使用して FC スイッチに接続し、監視できます。

## 関連情報

### "システム管理"

#### 健全性監視用の **FC-to-SAS** ブリッジの設定

9.8 より前のバージョンの ONTAP を実行しているシステムでは、MetroCluster 構成の FC-to-SAS ブリッジを監視するには、いくつかの特別な設定手順を実行する必要があります。

#### このタスクについて

- FibreBridge ブリッジでは、サードパーティ製の SNMP 監視ツールはサポートされません。
- ONTAP 9.8 以降では、デフォルトで FC-to-SAS ブリッジがインバンド接続で監視されるため、追加の設定は必要ありません。



ONTAP 9.8 以降では 'storage bridge コマンドは 'system bridge コマンドに置き換えられました。次の手順は「storage bridge」コマンドを示していますが、ONTAP 9.8 以降を実行している場合は「system bridge」コマンドが優先されます。

## 手順

1. ONTAP クラスタのプロンプトで、ブリッジをヘルスマニタの対象に追加します。

a. 使用している ONTAP のバージョンに対応したコマンドを使用して、ブリッジを追加します。

| ONTAP バージョン | コマンドを実行します                                                                   |
|-------------|------------------------------------------------------------------------------|
| 9.5 以降      | 「 storage bridge add -address 0.0.0.0 -managed-by in-band-name_bridge-name_」 |
| 9.4 以前      | 「 storage bridge add -address_bridge-ip-address_-name_bridge-name_」          |

b. ブリッジが追加され、正しく設定されていることを確認します。

「 storage bridge show 」

ポーリング間隔に応じて、すべてのデータが反映されるまで 15 分程度かかる場合があります。「 Status 」列の値が「 ok 」で、World Wide Name ( WWN ; ワールドワイド名) などのその他の情報が表示されていれば、ONTAP ヘルスマニタでブリッジに接続して監視できます。

次の例は、FC-to-SAS ブリッジが設定されていることを示しています。

```
controller_A_1::> storage bridge show

Bridge          Symbolic Name Is Monitored  Monitor Status  Vendor
Model          Bridge WWN
-----
-----
ATTO_10.10.20.10  atto01         true          ok              Atto
FibreBridge 7500N  20000010867038c0
ATTO_10.10.20.11  atto02         true          ok              Atto
FibreBridge 7500N  20000010867033c0
ATTO_10.10.20.12  atto03         true          ok              Atto
FibreBridge 7500N  20000010867030c0
ATTO_10.10.20.13  atto04         true          ok              Atto
FibreBridge 7500N  2000001086703b80

4 entries were displayed

controller_A_1::>
```

### MetroCluster の設定を確認しています

MetroCluster 構成内のコンポーネントおよび関係が正しく機能していることを確認できます。

チェックは、初期設定後と、MetroCluster 設定に変更を加えたあとに実施する必要があります。また、ネゴシエート (計画的) スイッチオーバーやスイッチバックの処理の前にも実施します。

## このタスクについて

いずれかまたは両方のクラスタに対して短時間に MetroCluster check run コマンドを 2 回発行すると '競合が発生し' コマンドがすべてのデータを収集しない場合がありますそれ以降の MetroCluster check show コマンドでは '期待される出力は表示されません'

## 手順

1. 構成を確認します。

「MetroCluster check run」のようになります

このコマンドはバックグラウンドジョブとして実行され、すぐに完了しない場合があります。

```
cluster_A::> metrocluster check run
The operation has been started and is running in the background. Wait
for
it to complete and run "metrocluster check show" to view the results. To
check the status of the running metrocluster check operation, use the
command,
"metrocluster operation history show -job-id 2245"
```

```
cluster_A::> metrocluster check show

Component          Result
-----
nodes              ok
lifs               ok
config-replication ok
aggregates        ok
clusters          ok
connections       ok
volumes           ok
7 entries were displayed.
```

2. 最新の MetroCluster check run コマンドから 'より詳細な結果を表示します'

MetroCluster check aggregate show

MetroCluster check cluster show

MetroCluster check config-replication show

MetroCluster check lif show

MetroCluster check node show



「MetroCluster check show」コマンドは、最新の「MetroCluster check run」コマンドの結果を表示します。MetroCluster check show コマンドを使用する前に、必ず MetroCluster check run コマンドを実行して、表示されている情報が最新であることを確認してください。

次に、正常な 4 ノード MetroCluster 構成の MetroCluster check aggregate show コマンドの出力例を示します。

```
cluster_A::> metrocluster check aggregate show

Last Checked On: 8/5/2014 00:42:58

Node          Aggregate          Check
Result
-----
controller_A_1  controller_A_1_aggr0
ok
ok
ok
controller_A_1  controller_A_1_aggr1
ok
ok
ok
controller_A_1  controller_A_1_aggr2
ok
ok
ok
controller_A_2  controller_A_2_aggr0
ok
ok
ok
controller_A_2  controller_A_2_aggr1
```

```

ok
mirroring-status
disk-pool-allocation
ok
ownership-state
ok
controller_A_2_aggr2
mirroring-status
ok
disk-pool-allocation
ok
ownership-state
ok
18 entries were displayed.

```

次に、正常な 4 ノード MetroCluster 構成の MetroCluster check cluster show コマンドの出力例を示します。この出力は、必要に応じてネゴシエートスイッチオーバーを実行できる状態であることを示しています。

```

Last Checked On: 9/13/2017 20:47:04

Cluster          Check          Result
-----
mccint-fas9000-0102
negotiated-switchover-ready  not-applicable
switchback-ready             not-applicable
job-schedules                 ok
licenses                       ok
periodic-check-enabled        ok

mccint-fas9000-0304
negotiated-switchover-ready  not-applicable
switchback-ready             not-applicable
job-schedules                 ok
licenses                       ok
periodic-check-enabled        ok

10 entries were displayed.

```

#### 関連情報

["ディスクおよびアグリゲートの管理"](#)

["ネットワークと LIF の管理"](#)

## Config Advisor での MetroCluster 構成エラーの確認

一般的な構成エラーの有無を確認する Config Advisor ツールをネットアップサポートサイトからダウンロードできます。

このタスクについて

Config Advisor は、構成の検証や健全性のチェックに使用できるツールです。データ収集とシステム分析のために、セキュアなサイトにもセキュアでないサイトにも導入できます。



Config Advisor のサポートには制限があり、オンラインでしか使用できません。

手順

1. Config Advisor のダウンロードページにアクセスし、ツールをダウンロードします。

["ネットアップのダウンロード： Config Advisor"](#)

2. Config Advisor を実行し、ツールの出力を確認して、問題が検出された場合は出力に表示される推奨事項に従って対処します。

## ローカル HA の処理を検証しています

4 ノード MetroCluster 構成の場合、MetroCluster 構成のローカル HA ペアの処理を検証する必要があります。2 ノード構成の場合は不要です。

このタスクについて

2 ノード MetroCluster 構成ではローカル HA ペアは構成されないため、このタスクは適用されません。

このタスクの例では、次の標準的な命名規則を使用します。

- cluster\_A
  - controller\_A\_1
  - controller\_A\_2
- cluster\_B
  - controller\_B\_1
  - controller\_B\_2

手順

1. cluster\_A で、フェイルオーバーとギブバックを両方向で実行します。
  - a. ストレージフェイルオーバーが有効になっていることを確認します。

「storage failover show」をクリックします

両方のノードでテイクオーバーが可能であることが出力に示されます。

```

cluster_A::> storage failover show
                                Takeover
Node           Partner           Possible State Description
-----
controller_A_1 controller_A_2 true      Connected to controller_A_2

controller_A_2 controller_A_1 true      Connected to controller_A_1
2 entries were displayed.

```

- b. controller\_A\_1 から controller\_A\_2 をテイクオーバーします。

```
'storage failover takeover controller_A_2
```

テイクオーバー処理の進捗は storage failover show-takeover コマンドを使用して監視できます。

- c. テイクオーバーが完了したことを確認します。

「 storage failover show 」をクリックします

出力には、 controller\_A\_1 がテイクオーバー状態であること、 HA パートナーをテイクオーバーしたことが示されます。

```

cluster_A::> storage failover show
                                Takeover
Node           Partner           Possible State Description
-----
controller_A_1 controller_A_2 false     In takeover

controller_A_2 controller_A_1 -         Unknown
2 entries were displayed.

```

- d. controller\_A\_2 をギブバックします。

```
'storage failover giveback controller_A_2
```

「 storage failover show-giveback 」 コマンドを使用すると、ギブバック処理の進捗を監視できます。

- e. ストレージフェイルオーバーが通常の状態に戻ったことを確認します。

「 storage failover show 」をクリックします

両方のノードでテイクオーバーが可能であることが出力に示されます。

```

cluster_A::> storage failover show
                                Takeover
Node           Partner           Possible State Description
-----
controller_A_1 controller_A_2 true      Connected to controller_A_2
controller_A_2 controller_A_1 true      Connected to controller_A_1
2 entries were displayed.

```

a. ここまでの手順を繰り返して、今度は controller\_A\_2 から controller\_A\_1 をテイクオーバーします。

2. cluster\_B に関して、上記の手順を繰り返します

関連情報

["ハイアベイラビリティ構成"](#)

スイッチオーバー、修復、スイッチバックを検証しています

MetroCluster 構成のスイッチオーバー、修復、スイッチバックの処理を検証する必要があります。

ステップ

1. に記載されているネゴシエートスイッチオーバー、修復、スイッチバックの手順を使用します ["災害からリカバリします"](#)。

構成バックアップファイルを保護しています

ローカルクラスタ内のデフォルトの場所に加えて、クラスタ構成バックアップファイルをアップロードするリモート URL（HTTP または FTP）を指定することで、クラスタ構成バックアップファイルの保護を強化できます。

ステップ

1. 構成バックアップファイルのリモートデスティネーションの URL を設定します。

「システム構成のバックアップ設定 MODIT\_URL-of-destination\_」

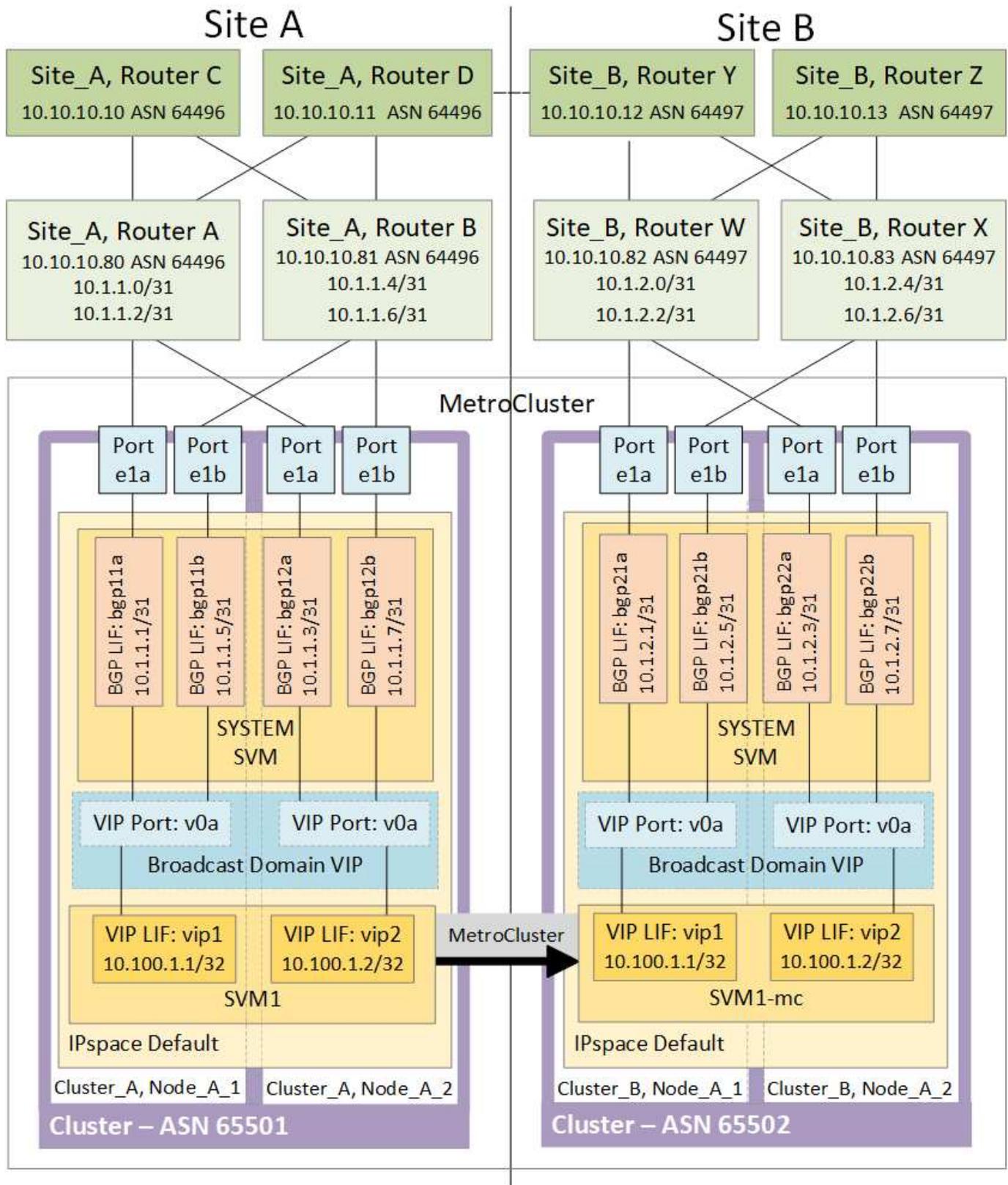
- 。 ["CLI を使用したクラスタ管理"](#) 追加情報が含まれています。

## MetroCluster 設定で仮想 IP およびボーダーゲートウェイプロトコルを使用する場合の考慮事項

ONTAP 9.5 以降では、ONTAP で仮想 IP（VIP）と Border Gateway Protocol（BGP）を使用してレイヤ 3 接続がサポートされます。VIP と BGP を組み合わせることで、フロントエンドネットワークでの冗長性とバックエンド MetroCluster の冗長性が確保され、レイヤ 3 ディザスタリカバリ解決策が実現します。

レイヤ 3 解決策を計画する際は、次のガイドラインと図を確認してください。ONTAP での VIP および BGP

の実装の詳細については、を参照してください ["仮想 IP LIF を設定"](#)。



## ONTAP の制限事項

ONTAP では、MetroCluster 構成の両方のサイトのすべてのノードに BGP ピアリングが設定されていること

は自動的に検証されません。

ONTAP は、ルートアグリゲーションを実行するのではなく、個々の仮想 LIF のすべての IP を一意のホストルートとして常時通知します。

ONTAP は、真のエニーキャストをサポートしません。クラスタ内の 1 つのノードだけが、特定の仮想 LIF の IP を提供します（ただし、物理ポートが正しい IPspace の一部である場合は、BGP LIF であるかどうかに関係なく、すべての物理インターフェイスで許可されます）。異なる LIF は、異なるホストノードに個別に移行できます。

## このレイヤ 3 解決策を MetroCluster 設定で使用する場合の注意事項

必要な冗長性を確保するために、BGP および VIP を正しく設定する必要があります。

よりシンプルな導入シナリオが、より複雑なアーキテクチャよりも推奨されます（たとえば、BGP ピアリングルータは、中間の BGP 以外のルータ経由で到達可能です）。ただし、ONTAP では、ネットワーク設計やトポロジの制限は適用されません。

VIP LIF はフロントエンド / データネットワークのみをカバーします。

ONTAP のバージョンに応じて、システム SVM やデータ SVM ではなく、ノード SVM に BGP ピアリング LIF を設定する必要があります。ONTAP 9.8 では、クラスタ（システム）SVM 内に BGP LIF が表示され、ノード SVM が存在しなくなります。

各データ SVM には、LIF の移行や MetroCluster のフェイルオーバーが発生したときにリターンデータパスを使用できるように、考えられるすべてのファーストホップゲートウェイアドレス（通常は BGP ルータピアリングの IP アドレス）を設定する必要があります。

BGP LIF はクラスタ間 LIF と同様にノード固有で、各ノードは一意の設定を持ちます。DR サイトのノードにレプリケートする必要はありません。

設定が完了すると、v0a（v0bなど）が接続を継続的に検証し、LIFの移行またはフェイルオーバーが成功するかどうかを（停止したあとにのみ構成の分断が認識されるL2とは異なります）チェックします。

アーキテクチャに大きな違いは、クライアントがデータ SVM の VIP と同じ IP サブネットを共有しなくなることです。適切なエンタープライズクラスの復元力と冗長性功能（たとえば、VRRP/HSRP）をイネーブルにした L3 ルータは、VIP が正しく動作するために、ストレージとクライアント間のパス上に配置する必要があります。

BGP の信頼性の高い更新プロセスにより、LIF の移行がわずかに高速化され、一部のクライアントの中断が少なくなるため、円滑な移行が可能になります

ネットワークまたはスイッチの一部の動作を LACP よりも高速に検出するように BGP を設定できます（設定されている場合）。

外部 BGP（EBGP）は、ONTAP ノードとピアリングルータ間で異なる AS 番号を使用し、ルータ上でのルート集約と再配布を容易にするための推奨配置です。内部 BGP（IBGP）およびルートリフレクタの使用は不可能ではありませんが、簡単な VIP 設定の範囲外です。

導入後、関連する仮想 LIF が各サイトのすべてのノード間で移行されたときに（MetroCluster スイッチオーバーを含む）データ SVM にアクセスできることを確認し、同じデータ SVM への静的ルートの正しい設定を確認する必要があります。

VIP は、ほとんどの IP ベースのプロトコル（NFS、SMB、iSCSI）に対応しています。

## MetroCluster 構成をテストする

障害シナリオをテストして、MetroCluster 構成が正しく動作していることを確認できます。

### ネゴシエートスイッチオーバーを検証中

ネゴシエート（計画的）スイッチオーバー処理をテストして、データが中断なく提供されることを確認できます。

このタスクについて

このテストでは、クラスターを 2 番目のデータセンターに切り替えても、データの可用性が影響を受けないこと (SMB およびファイバチャネルプロトコルを除く) を検証します。

このテストには約 30 分かかります。

この手順の想定される結果は次のとおりです。

- MetroCluster switchover コマンドは '警告プロンプトを表示します' プロンプトに「yes」と応答すると、コマンドが発行されたサイトがパートナーサイトを切り替えます。

MetroCluster IP 構成の場合：

- ONTAP 9.4 以前：
  - ミラーアグリゲートはネゴシエートスイッチオーバー後にデグレード状態になります。
- ONTAP 9.5 以降：
  - リモートストレージがアクセス可能である場合、ミラーされたアグリゲートは通常の状態のままになります。
  - リモートストレージへのアクセスが失われると、ネゴシエートスイッチオーバー後にミラーアグリゲートがデグレード状態になります。
- ONTAP 9.8 以降の場合：
  - リモートストレージへのアクセスが失われると、ディザスタサイトにあるミラーされていないアグリゲートは使用できなくなります。これにより、コントローラが停止する可能性があります。

手順

1. すべてのノードが設定済みの状態で通常モードになっていることを確認します。

```
MetroCluster node show
```

```
cluster_A::> metrocluster node show
```

| Cluster           | Configuration State | Mode   |
|-------------------|---------------------|--------|
| -----             | -----               |        |
| -----             |                     |        |
| Local: cluster_A  | configured          | normal |
| Remote: cluster_B | configured          | normal |

2. スイッチオーバー処理を開始します。

#### MetroCluster スイッチオーバー

```
cluster_A::> metrocluster switchover
Warning: negotiated switchover is about to start. It will stop all the
data Vservers on cluster "cluster_B" and
automatically re-start them on cluster "`cluster_A`". It will finally
gracefully shutdown cluster "cluster_B".
```

3. ローカルクラスタが設定済みの状態でスイッチオーバーモードになっていることを確認します。

#### MetroCluster node show

```
cluster_A::> metrocluster node show
```

| Cluster           | Configuration State | Mode       |
|-------------------|---------------------|------------|
| -----             | -----               |            |
| -----             |                     |            |
| Local: cluster_A  | configured          | switchover |
| Remote: cluster_B | not-reachable       | -          |
| configured        | normal              |            |

4. スイッチオーバー処理が成功したことを確認します。

「MetroCluster operation show」を参照してください

```
cluster_A::> metrocluster operation show
Operation: switchover
State: successful
Start Time: 2/6/2016 13:28:50
End Time: 2/6/2016 13:29:41
Errors: -
```

5. 「vserver show」コマンドと「network interface show」コマンドを使用して、DR SVM と LIF がオン

ラインになったことを確認します。

## 修復と手動スイッチバックの検証

修復処理と手動スイッチバック処理をテストするには、ネゴシエートスイッチオーバー後にクラスタを元のデータセンターにスイッチバックして、データの可用性に影響がないことを検証します（SMB および Solaris FC 構成を除く）。

このタスクについて

このテストには約 30 分かかります。

この手順では、想定される結果として、サービスがホームノードにスイッチバックされることを確認します。

手順

1. 修復が完了したことを確認します。

MetroCluster node show

次の例は、コマンドが正常に完了したことを示しています。

```
cluster_A:~> metrocluster node show
DR
Group Cluster Node Configuration State DR Mirroring Mode
-----
-----
1 cluster_A
node_A_1 configured enabled heal roots
completed
cluster_B
node_B_2 unreachable - switched over
42 entries were displayed.
```

2. すべてのアグリゲートがミラーされたことを確認します。

「 storage aggregate show

次の例では、すべてのアグリゲートの RAID ステータスが mirrored になっています。

```

cluster_A::> storage aggregate show
cluster Aggregates:
Aggregate Size      Available Used% State   #Vols  Nodes      RAID
Status
-----
-----
data_cluster
      4.19TB      4.13TB   2% online    8 node_A_1  raid_dp,
mirrored,
normal

root_cluster
      715.5GB    212.7GB  70% online    1 node_A_1  raid4,
mirrored,
normal

cluster_B Switched Over Aggregates:
Aggregate Size      Available Used% State   #Vols  Nodes      RAID
Status
-----
-----
data_cluster_B
      4.19TB      4.11TB   2% online    5 node_A_1  raid_dp,
mirrored,
normal

root_cluster_B    -          -      - unknown    - node_A_1  -

```

3. ディザスタサイトからノードをブートします。
4. スイッチバックリカバリのステータスを確認します。

#### MetroCluster node show

```

cluster_A::> metrocluster node show
DR
Group Cluster Node      Configuration  DR
State          Mirroring Mode
-----
-----
1      cluster_A
      node_A_1      configured    enabled    heal roots
completed
      cluster_B
      node_B_2      configured    enabled    waiting for
switchback                                     recovery

2 entries were displayed.

```

## 5. スイッチバックを実行します。

### MetroCluster スイッチバック

```
cluster_A::> metrocluster switchback
[Job 938] Job succeeded: Switchback is successful.Verify switchback
```

## 6. ノードのステータスを確認します。

### MetroCluster node show

```
cluster_A::> metrocluster node show
DR
Group Cluster Node Configuration State DR Mirroring Mode
-----
1 cluster_A
node_A_1 configured enabled normal
cluster_B
node_B_2 configured enabled normal
2 entries were displayed.
```

## 7. ステータスを確認します。

「MetroCluster operation show」を参照してください

正常に完了したことを示す出力が表示されます。

```
cluster_A::> metrocluster operation show
Operation: switchback
State: successful
Start Time: 2/6/2016 13:54:25
End Time: 2/6/2016 13:56:15
Errors: -
```

## 単一の FC-to-SAS ブリッジの停止

単一の FC-to-SAS ブリッジの障害をテストして、単一点障害がないことを確認できます。

このタスクについて

このテストには約 15 分かかります。

この手順の想定される結果は次のとおりです。

- ブリッジのスイッチがオフになるため、とエラーが生成されます。
- フェイルオーバーやサービスの中断は発生しません。
- コントローラモジュールからブリッジに接続されたドライブへのパスは1つだけになります。



ONTAP 9.8 以降では 'storage bridge コマンドは 'system bridge コマンドに置き換えられました。次の手順は「storage bridge」コマンドを示していますが、ONTAP 9.8 以降を実行している場合は「system bridge」コマンドが優先されます。

#### 手順

1. ブリッジの電源装置をオフにします。
2. ブリッジの監視がエラーを示していることを確認します。

「storage bridge show」

```
cluster_A::> storage bridge show

Monitor
Bridge      Symbolic Name Vendor  Model      Bridge WWN      Monitored
Status
-----
-----
ATTO_10.65.57.145
      bridge_A_1   Atto    FibreBridge 6500N
                                      200000108662d46c true
error
```

3. ブリッジに接続されたドライブに1つのパスでアクセス可能なことを確認します。

「storage disk error show」と表示されます

```

cluster_A::> storage disk error show
Disk              Error Type          Error Text
-----
-----
1.0.0             onedomain           1.0.0 (5000cca057729118): All paths
to this array LUN are connected to the same fault domain. This is a
single point of failure.
1.0.1             onedomain           1.0.1 (5000cca057727364): All paths
to this array LUN are connected to the same fault domain. This is a
single point of failure.
1.0.2             onedomain           1.0.2 (5000cca05772e9d4): All paths
to this array LUN are connected to the same fault domain. This is a
single point of failure.
...
1.0.23            onedomain           1.0.23 (5000cca05772e9d4): All paths
to this array LUN are connected to the same fault domain. This is a
single point of failure.

```

## 電源回線切断後の動作確認

MetroCluster 構成で PDU の障害が発生した場合の対応をテストできます。

このタスクについて

ベストプラクティスとして、コンポーネントの各電源装置（PSU）を別々の電源装置に接続することを推奨します。両方の PSU を同じ配電ユニット（PDU）に接続している場合、停電が発生したときに、サイトが停止したりシェルフ全体が使用できなくなったりする可能性があります。1 本原因の電源回線に障害が発生した場合に、サービスが中断する可能性があるケーブル接続の不一致がないかどうかをテストします。

このテストには約 15 分かかります。

このテストでは、MetroCluster コンポーネントが格納されたすべてのラックで、左側のすべての PDU の電源をオフにしてから、右側のすべての PDU の電源をオフにする必要があります。

この手順の想定される結果は次のとおりです。

- PDU の接続が切断されるため、エラーが生成されます。
- フェイルオーバーやサービスの中断は発生しません。

手順

1. MetroCluster コンポーネントが格納されたラックの左側の PDU の電源をオフにします。
2. コンソールで結果を監視します。

「system environment sensors show -state fault」というエラーが表示されます

「storage shelf show -errors」を参照してください

```

cluster_A::> system environment sensors show -state fault

Node Sensor                               State Value/Units Crit-Low Warn-Low Warn-Hi
Crit-Hi
-----
node_A_1
    PSU1                                   fault
   PSU_OFF
    PSU1 Pwr In OK fault
   FAULT
node_A_2
    PSU1                                   fault
   PSU_OFF
    PSU1 Pwr In OK fault
   FAULT

4 entries were displayed.

cluster_A::> storage shelf show -errors
Shelf Name: 1.1
Shelf UID: 50:0a:09:80:03:6c:44:d5
Serial Number: SHFHU1443000059

Error Type          Description
-----
Power               Critical condition is detected in storage shelf
power supply unit "1". The unit might fail.Reconnect PSU1

```

3. 左側の PDU の電源を再度オンにします。
4. ONTAP がエラー状態をクリアすることを確認します。
5. 右側の PDU で上記の手順を繰り返します。

## スイッチファブリック障害後の動作確認

スイッチファブリックを無効にして、データの可用性に影響がないことを確認できます。

このタスクについて

このテストには約 15 分かかります。

この手順では、想定される結果として、ファブリックを無効にしたあとにクラスインターコネクトとディスクのすべてのトラフィックがもう一方のファブリックに送られることを確認します。

この例では、スイッチファブリック 1 を無効にしています。このファブリックは、各 MetroCluster サイトに 1 つずつ、2 つのスイッチで構成されます。

- cluster\_A の FC\_switch\_A\_1
- cluster\_B の FC\_switch\_B\_1

#### 手順

1. MetroCluster 構成の 2 つのスイッチファブリックの一方への接続を無効にします。

a. ファブリックの 1 つ目のスイッチを無効にします。

'witchdisable

```
FC_switch_A_1::> switchdisable
```

b. ファブリックの 2 つ目のスイッチを無効にします。

'witchdisable

```
FC_switch_B_1::> switchdisable
```

2. コントローラモジュールのコンソールで結果を監視します。

次のコマンドを使用してクラスタノードをチェックし、すべてのデータが引き続き提供されていることを確認できます。コマンドの出力に、ディスクへのパスがないことが示されます。これは想定される状態です。

- vserver show のコマンドです
- network interface show の略
- aggr show のコマンドを入力し
- system node run nodename command storage show disk -p のようになりました
- storage disk error show のコマンドを入力します

3. MetroCluster 構成の 2 つのスイッチファブリックの一方への接続を再度有効にします。

a. ファブリックの 1 つ目のスイッチを再度有効にします。

「 witchenable 」

```
FC_switch_A_1::> switchenable
```

b. ファブリックの 2 つ目のスイッチを再度有効にします。

「 witchenable 」

```
FC_switch_B_1::> switchenable
```

4. 10分以上待ってから、もう一方のスイッチファブリックで上記の手順を繰り返します。

## 単一のストレージシェルフが停止したあとの動作確認

単一のストレージシェルフの障害をテストして、単一点障害がないことを確認できます。

このタスクについて

この手順の想定される結果は次のとおりです。

- 監視ソフトウェアからエラーメッセージが報告されます。
- フェイルオーバーやサービスの中断は発生しません。
- ハードウェア障害がリストアされたあと、ミラーの再同期が自動的に開始されます。

手順

1. ストレージフェイルオーバーのステータスを確認します。

「storage failover show」をクリックします

```
cluster_A::> storage failover show

Node           Partner           Possible State Description
-----
node_A_1       node_A_2           true           Connected to node_A_2
node_A_2       node_A_1           true           Connected to node_A_1
2 entries were displayed.
```

2. アグリゲートのステータスを確認します。

「storage aggregate show」

```
cluster_A::> storage aggregate show
```

```
cluster Aggregates:
```

| Aggregate                  | Size    | Available | Used% | State  | #Vols | Nodes    | RAID |
|----------------------------|---------|-----------|-------|--------|-------|----------|------|
| node_A_1data01_mirrored    | 4.15TB  | 3.40TB    | 18%   | online | 3     | node_A_1 |      |
| raid_dp,                   |         |           |       |        |       |          |      |
| mirrored,                  |         |           |       |        |       |          |      |
| normal                     |         |           |       |        |       |          |      |
| node_A_1root               | 707.7GB | 34.29GB   | 95%   | online | 1     | node_A_1 |      |
| raid_dp,                   |         |           |       |        |       |          |      |
| mirrored,                  |         |           |       |        |       |          |      |
| normal                     |         |           |       |        |       |          |      |
| node_A_2_data01_mirrored   | 4.15TB  | 4.12TB    | 1%    | online | 2     | node_A_2 |      |
| raid_dp,                   |         |           |       |        |       |          |      |
| mirrored,                  |         |           |       |        |       |          |      |
| normal                     |         |           |       |        |       |          |      |
| node_A_2_data02_unmirrored | 2.18TB  | 2.18TB    | 0%    | online | 1     | node_A_2 |      |
| raid_dp,                   |         |           |       |        |       |          |      |
| normal                     |         |           |       |        |       |          |      |
| node_A_2_root              | 707.7GB | 34.27GB   | 95%   | online | 1     | node_A_2 |      |
| raid_dp,                   |         |           |       |        |       |          |      |
| mirrored,                  |         |           |       |        |       |          |      |
| normal                     |         |           |       |        |       |          |      |

3. すべてのデータ SVM とデータボリュームがオンラインで、データを提供していることを確認します。

```
vserver show -type data
```

```
network interface show -fields is-home false
```

volume show ! vol0、! MDV \*

```
cluster_A::> vservers show -type data

cluster_A::> vservers show -type data
Admin      Operational Root
Vserver    Type      Subtype   State     State     Volume
Aggregate
-----
SVM1       data     sync-source   running   SVM1_root
node_A_1_data01_mirrored
SVM2       data     sync-source   running   SVM2_root
node_A_2_data01_mirrored

cluster_A::> network interface show -fields is-home false
There are no entries matching your query.

cluster_A::> volume show !vol0,!MDV*
Vserver    Volume      Aggregate    State     Type     Size
Available Used%
-----
SVM1
    SVM1_root
        node_A_1data01_mirrored
            online    RW        10GB
9.50GB    5%
SVM1
    SVM1_data_vol
        node_A_1data01_mirrored
            online    RW        10GB
9.49GB    5%
SVM2
    SVM2_root
        node_A_2_data01_mirrored
            online    RW        10GB
9.49GB    5%
SVM2
    SVM2_data_vol
        node_A_2_data02_unmirrored
            online    RW        1GB
972.6MB   5%
```

4. ハードウェア障害をシミュレートするために電源をオフにするノード node\_A\_1 のプール 1 内のシェルフ

を特定します。

```
「 storage aggregate show -r -node node_name !!* root
```

ミラーされたデータアグリゲートを構成するドライブが格納されたシェルフを選択する必要があります。

次の例では、停止する対象としてシェルフ ID 31 を選択します。

```
cluster_A::> storage aggregate show -r -node node_A_2 !*root
Owner Node: node_A_2
Aggregate: node_A_2_data01_mirrored (online, raid_dp, mirrored) (block
checksums)
Plex: /node_A_2_data01_mirrored/plex0 (online, normal, active, pool0)
RAID Group /node_A_2_data01_mirrored/plex0/rg0 (normal, block
checksums)
Physical
Position Disk Pool Type RPM Usable
Size Status Size
-----
-----
dparity 2.30.3 0 BSAS 7200 827.7GB
828.0GB (normal)
parity 2.30.4 0 BSAS 7200 827.7GB
828.0GB (normal)
data 2.30.6 0 BSAS 7200 827.7GB
828.0GB (normal)
data 2.30.8 0 BSAS 7200 827.7GB
828.0GB (normal)
data 2.30.5 0 BSAS 7200 827.7GB
828.0GB (normal)
Plex: /node_A_2_data01_mirrored/plex4 (online, normal, active, pool1)
RAID Group /node_A_2_data01_mirrored/plex4/rg0 (normal, block
checksums)
Physical
Position Disk Pool Type RPM Usable
Size Status Size
-----
-----
dparity 1.31.7 1 BSAS 7200 827.7GB
828.0GB (normal)
parity 1.31.6 1 BSAS 7200 827.7GB
828.0GB (normal)
data 1.31.3 1 BSAS 7200 827.7GB
828.0GB (normal)
```

```

    data      1.31.4                1   BSAS      7200  827.7GB
828.0GB (normal)
    data      1.31.5                1   BSAS      7200  827.7GB
828.0GB (normal)

Aggregate: node_A_2_data02_unmirrored (online, raid_dp) (block
checksums)
Plex: /node_A_2_data02_unmirrored/plex0 (online, normal, active,
pool0)
RAID Group /node_A_2_data02_unmirrored/plex0/rg0 (normal, block
checksums)

  Usable
Physical
  Position Disk                               Pool Type    RPM    Size
Size Status
-----
-----
    dparity  2.30.12                0   BSAS      7200  827.7GB
828.0GB (normal)
    parity   2.30.22                0   BSAS      7200  827.7GB
828.0GB (normal)
    data     2.30.21                0   BSAS      7200  827.7GB
828.0GB (normal)
    data     2.30.20                0   BSAS      7200  827.7GB
828.0GB (normal)
    data     2.30.14                0   BSAS      7200  827.7GB
828.0GB (normal)
15 entries were displayed.

```

5. 選択したシェルフの電源を物理的にオフにします。
6. アグリゲートのステータスを再度確認します。

「 storage aggregate show

「 storage aggregate show -r -node node\_name ! \* root」

電源をオフにしたシェルフにドライブがあるアグリゲートの RAID ステータスは「 degraded」になり、影響を受けたプレックスのドライブのステータスは「 failed」になります。次に例を示します。

```

cluster_A::> storage aggregate show
Aggregate      Size Available Used% State   #Vols  Nodes           RAID
Status
-----
-----
node_A_1data01_mirrored
                4.15TB    3.40TB   18% online    3 node_A_1

```

```

raid_dp,

mirrored,

normal
node_A_1root
      707.7GB   34.29GB   95% online      1 node_A_1
raid_dp,

mirrored,

normal
node_A_2_data01_mirrored
      4.15TB    4.12TB    1% online       2 node_A_2
raid_dp,

mirror

degraded
node_A_2_data02_unmirrored
      2.18TB    2.18TB    0% online       1 node_A_2
raid_dp,

normal
node_A_2_root
      707.7GB   34.27GB   95% online      1 node_A_2
raid_dp,

mirror

```

```

degraded
cluster_A::> storage aggregate show -r -node node_A_2 !*root
Owner Node: node_A_2
Aggregate: node_A_2_data01_mirrored (online, raid_dp, mirror degraded)
(block checksums)
Plex: /node_A_2_data01_mirrored/plex0 (online, normal, active, pool0)
RAID Group /node_A_2_data01_mirrored/plex0/rg0 (normal, block
checksums)

```

|                  |        |      |      | Usable |         |
|------------------|--------|------|------|--------|---------|
| Physical         |        |      |      |        |         |
| Position         | Disk   | Pool | Type | RPM    | Size    |
| Size             | Status |      |      |        |         |
| -----            |        |      |      |        |         |
| dparity          | 2.30.3 | 0    | BSAS | 7200   | 827.7GB |
| 828.0GB (normal) |        |      |      |        |         |

```

    parity    2.30.4                0   BSAS    7200   827.7GB
828.0GB (normal)
    data      2.30.6                0   BSAS    7200   827.7GB
828.0GB (normal)
    data      2.30.8                0   BSAS    7200   827.7GB
828.0GB (normal)
    data      2.30.5                0   BSAS    7200   827.7GB
828.0GB (normal)

```

Plex: /node\_A\_2\_data01\_mirrored/plex4 (offline, failed, inactive, pool1)

RAID Group /node\_A\_2\_data01\_mirrored/plex4/rg0 (partial, none checksums)

|            |        |      |      |     | Usable  |
|------------|--------|------|------|-----|---------|
| Physical   |        |      |      |     |         |
| Position   | Disk   | Pool | Type | RPM | Size    |
| Size       | Status |      |      |     |         |
| -----      |        |      |      |     |         |
| dparity    | FAILED | -    | -    | -   | 827.7GB |
| - (failed) |        |      |      |     |         |
| parity     | FAILED | -    | -    | -   | 827.7GB |
| - (failed) |        |      |      |     |         |
| data       | FAILED | -    | -    | -   | 827.7GB |
| - (failed) |        |      |      |     |         |
| data       | FAILED | -    | -    | -   | 827.7GB |
| - (failed) |        |      |      |     |         |
| data       | FAILED | -    | -    | -   | 827.7GB |
| - (failed) |        |      |      |     |         |

Aggregate: node\_A\_2\_data02\_unmirrored (online, raid\_dp) (block checksums)

Plex: /node\_A\_2\_data02\_unmirrored/plex0 (online, normal, active, pool0)

RAID Group /node\_A\_2\_data02\_unmirrored/plex0/rg0 (normal, block checksums)

|                  |         |      |      |      | Usable  |
|------------------|---------|------|------|------|---------|
| Physical         |         |      |      |      |         |
| Position         | Disk    | Pool | Type | RPM  | Size    |
| Size             | Status  |      |      |      |         |
| -----            |         |      |      |      |         |
| dparity          | 2.30.12 | 0    | BSAS | 7200 | 827.7GB |
| 828.0GB (normal) |         |      |      |      |         |
| parity           | 2.30.22 | 0    | BSAS | 7200 | 827.7GB |
| 828.0GB (normal) |         |      |      |      |         |

```
data      2.30.21      0  BSAS  7200  827.7GB
828.0GB (normal)
data      2.30.20      0  BSAS  7200  827.7GB
828.0GB (normal)
data      2.30.14      0  BSAS  7200  827.7GB
828.0GB (normal)
```

15 entries were displayed.

7. データが提供されていること、およびすべてのボリュームがオンラインのままであることを確認します。

```
vserver show -type data
```

```
network interface show -fields is-home false
```

```
volume show ! vol0、! MDV *
```

```

cluster_A::> vservers show -type data

cluster_A::> vservers show -type data
Admin      Operational Root
Vserver    Type      Subtype   State     State     Volume
Aggregate
-----
-----
SVM1       data      sync-source      running    SVM1_root
node_A_1_data01_mirrored
SVM2       data      sync-source      running    SVM2_root
node_A_1_data01_mirrored

cluster_A::> network interface show -fields is-home false
There are no entries matching your query.

cluster_A::> volume show !vol0,!MDV*
Vserver    Volume      Aggregate    State     Type     Size
Available Used%
-----
-----
SVM1
          SVM1_root
                node_A_1data01_mirrored
                        online    RW      10GB
9.50GB    5%
SVM1
          SVM1_data_vol
                node_A_1data01_mirrored
                        online    RW      10GB
9.49GB    5%
SVM2
          SVM2_root
                node_A_1data01_mirrored
                        online    RW      10GB
9.49GB    5%
SVM2
          SVM2_data_vol
                node_A_2_data02_unmirrored
                        online    RW      1GB
972.6MB   5%

```

8. シェルフの電源を物理的にオンにします。

再同期が自動的に開始されます

9. 再同期が開始されたことを確認します。

「 storage aggregate show

次の例に示すように、影響を受けたアグリゲートの RAID ステータスは「resyncing」になります。

```
cluster_A::> storage aggregate show
cluster Aggregates:
Aggregate      Size Available Used% State  #Vols  Nodes      RAID
Status
-----
node_A_1_data01_mirrored
      4.15TB      3.40TB      18% online      3 node_A_1
raid_dp,
mirrored,
normal
node_A_1_root
      707.7GB      34.29GB      95% online      1 node_A_1
raid_dp,
mirrored,
normal
node_A_2_data01_mirrored
      4.15TB      4.12TB      1% online      2 node_A_2
raid_dp,
resyncing
node_A_2_data02_unmirrored
      2.18TB      2.18TB      0% online      1 node_A_2
raid_dp,
normal
node_A_2_root
      707.7GB      34.27GB      95% online      1 node_A_2
raid_dp,
resyncing
```

10. アグリゲートを監視して、再同期が完了したことを確認します。

「 storage aggregate show

次の例に示すように、影響を受けるアグリゲートの RAID ステータスは「normal」になります。

```
cluster_A::> storage aggregate show
cluster Aggregates:
Aggregate      Size Available Used% State  #Vols  Nodes      RAID
Status
-----
-----
node_A_1data01_mirrored
      4.15TB      3.40TB   18% online    3 node_A_1
raid_dp,
mirrored,
normal
node_A_1root
      707.7GB      34.29GB   95% online    1 node_A_1
raid_dp,
mirrored,
normal
node_A_2_data01_mirrored
      4.15TB      4.12TB    1% online    2 node_A_2
raid_dp,
normal
node_A_2_data02_unmirrored
      2.18TB      2.18TB    0% online    1 node_A_2
raid_dp,
normal
node_A_2_root
      707.7GB      34.27GB   95% online    1 node_A_2
raid_dp,
resyncing
```

## MetroCluster 構成を削除

MetroCluster構成を削除する必要がある場合は、テクニカル サポートにお問い合わせください。

NetAppテクニカルサポートに連絡し、構成に適したガイドを参照してください。"[MetroCluster 構成-解決ガイドからノードを削除する方法](#)"



MetroClusterの構成解除を元に戻すことはできません。このプロセスは、テクニカルサポートの支援を受けてのみ実行してください。MetroCluster構成を削除した後、すべてのMetroCluster接続と相互接続をサポート可能な状態に調整する必要があります。

## Active IQ Unified Manager と ONTAP System Manager を使用して設定と監視を強化する方法

**Active IQ Unified Manager**および**ONTAP**システムマネージャを使用して詳細な設定と監視を行う

Active IQ Unified Manager と ONTAP の System Manager は、GUI を使用したクラスタ管理および設定監視に使用できます。

各ノードには ONTAP System Manager が事前にインストールされています。System Manager をロードするには、ノードに接続されている Web ブラウザのアドレスバーにクラスタ管理 LIF アドレスを入力します。

Active IQ Unified Manager を使用して MetroCluster 設定を監視することもできます。

関連情報

["Active IQ Unified Managerのドキュメント"](#)

### NTP を使用してシステム時刻を同期します

ノードとそのクライアントの間で時刻を同期するには、クラスタごとに独自の Network Time Protocol (NTP ; ネットワークタイムプロトコル) サーバが必要です。

このタスクについて

- テイクオーバーの発生後に障害ノードまたはパートナーノードのタイムゾーン設定を変更することはできません。
- MetroCluster FC 構成のクラスタごとに、その MetroCluster サイトのノード、FC スイッチ、および FC-to-SAS ブリッジで使用する独自の NTP サーバをそれぞれ用意する必要があります。
- MetroCluster Tiebreaker ソフトウェアを使用する場合は、それ専用の NTP サーバも必要です。

ONTAPのバージョンに応じて、System Manager UIの\*タブまたは[インサイト]\*タブでNTPを設定できます。

## クラスタ

System Managerでは、ONTAPのバージョンに応じて\*[クラスタ]\*タブから次の2つのオプションを使用してNTPを設定できます。

### ONTAP 9.8以降：

次の手順に従って、ONTAP 9.8以降の\*[クラスタ]\*タブからNTPを同期します。

#### 手順

1. [クラスタ]>[概要]\*に移動します。
2. 次に、オプションを選択し  で\*[編集]\*を選択します。
3. ウィンドウで、[NTPサーバ]の下の+追加\*オプションを選択します。
4. タイムサーバの名前と場所を追加し、IPアドレスを指定します。
5. 次に、\*[保存]\*を選択します。
6. タイムサーバを追加する場合は、この手順を繰り返します。

### ONTAP 9.11.1以降：

次の手順に従って、ONTAP 9.11.1以降の\*[クラスタ]タブの\*[インサイト]\*ウィンドウからNTPを同期します。

#### 手順

1. [クラスタ]>[概要]\*に移動します。
2. ページの\* Insights ウィンドウまで下にスクロールし、 Too few NTP servers are configured (設定されているNTPサーバが少なすぎる) を探して Fix it (修正) \*を選択します。
3. タイムサーバのIPアドレスを指定し、\*[保存]\*を選択します。
4. タイムサーバを追加する場合は、上記の手順を繰り返します。

#### 分析

ONTAP 9.11.1以降では、System Managerの\*[Insights]\*タブを使用してNTPを設定することもできます。

#### 手順

1. System Manager UIの\*[Insights]\*タブに移動します。
2. 下にスクロールして\*を選択し、[Fix it]\*を選択します。
3. タイムサーバのIPアドレスを指定し、\*[保存]\*を選択します。
4. タイムサーバを追加する場合は、上記の手順を繰り返します。

## MetroCluster 構成で ONTAP を使用する場合の考慮事項

MetroCluster 構成で ONTAP を使用する場合は、ライセンス、MetroCluster 構成の外部にあるクラスタとのピアリング、ボリューム処理や NVFAIL 処理などの ONTAP 処理の実行について、一定の考慮事項に注意する必要があります。

## ライセンスに関する考慮事項

- 両方のサイトに、同じサイトライセンスが設定されている必要があります。
- すべてのノードに同じノードロック式ライセンスが設定されている必要があります。

## SnapMirror に関する考慮事項

- SnapMirror SVM ディザスタリカバリは、ONTAP 9.5 以降のバージョンを実行している MetroCluster 構成でのみサポートされます。

## MetroCluster 構成での FlexCache のサポート

ONTAP 9.7 以降では、MetroCluster 構成で FlexCache ボリュームがサポートされます。スイッチオーバーまたはスイッチバック処理後の手動廃止の要件を理解しておく必要があります。

### FlexCache の元のデータとキャッシュが同じ MetroCluster サイト内にある場合のスイッチオーバー後の SVM 削除

ネゴシエートスイッチオーバーまたは計画外スイッチオーバーのあと、クラスタ内の SVM FlexCache ピア関係を手動で設定する必要があります。

たとえば、SVM vs1（キャッシュ）と vs2（元）が site\_A にあるとしますこれらの SVM はピア関係にあります。

スイッチオーバー後、SVM 「vs1-mc」と「vs2-mc」がパートナーサイト（site\_B）でアクティブ化されます。FlexCache が「vserver peer repeer」コマンドを使用して機能するには、これらの機能を手動で廃止する必要があります。

### FlexCache デスティネーションが第 3 のクラスタにあり、切断モードの場合のスイッチオーバーまたはスイッチバック後の SVM 削除

MetroCluster 構成外のクラスタへの FlexCache 関係では、スイッチオーバー中に関連するクラスタが切断モードになっている場合、スイッチオーバー後に常にピアリングを手動で再設定する必要があります。

例：

- FlexCache の一端（vs1 の cache\_1）は、MetroCluster site\_A にあります
- FlexCache のもう一方の端（vs2 の origin\_1）は、site\_A に配置されています（MetroCluster 構成ではありません）。

スイッチオーバーがトリガーされたときに site\_A と site\_B が接続されていない場合は、スイッチオーバー後に「vserver peer repeer」コマンドを使用して site\_B の SVM（スイッチオーバークラスタ）と site\_B の SVM を手動で再ピアリングする必要があります。

スイッチバックが実行された場合は、site\_A（元のクラスタ）と site\_B の SVM のピア関係を再設定する必要があります

## 関連情報

["FlexCache ボリュームの管理には CLI を使用します"](#)

## MetroCluster 構成での FabricPool のサポート

ONTAP 9.7 以降では、MetroCluster 構成で FabricPool ストレージ階層がサポートされます。

FabricPool の使用に関する一般的な情報については、を参照してください ["ディスクと階層（アグリゲート）の管理"](#)。

### FabricPool を使用する際の考慮事項

- クラスタに同じ容量制限の FabricPool ライセンスが必要です。
- 各クラスタに同じ名前の IPspace が必要です。

これは、デフォルト IPspace か管理者が作成した IPspace です。この IPspace は、FabricPool オブジェクトストア設定のセットアップに使用されます。

- 選択したIPspaceについて、外部のオブジェクトストアにアクセスできるクラスタ間LIFが各クラスタで定義されている必要があります。
- ソースまたはデスティネーションがMetroClusterクラスタの場合、FabricPoolでSVMの移行はサポートされません。

["SVMデータモビリティの詳細"](#)です。

### ミラーリングされた FabricPool で使用するアグリゲートを設定する



アグリゲートを設定する前に、の説明に従ってオブジェクトストアを設定する必要があります。 ["MetroCluster 構成で FabricPool のオブジェクトストアを設定する"](#)。

### 手順

FabricPool で使用するアグリゲートを設定するには、次の手順を実行します。

1. アグリゲートを作成するか、既存のアグリゲートを選択します。
2. アグリゲートを MetroCluster 構成内の標準のミラーアグリゲートとしてミラーリングします。
3. の説明に従って、アグリゲートを使用して FabricPool ミラーを作成します ["ディスクとアグリゲートの管理"](#)
  - a. プライマリオブジェクトストアを接続します。

このオブジェクトストアは、クラスタに物理的に近い場所にあります。

- b. ミラーオブジェクトストアを追加します。

このオブジェクトストアは、プライマリオブジェクトストアよりもクラスタから物理的に離れています。



ストレージのパフォーマンスと可用性を最適化するために、ミラーアグリゲートでは少なくとも20%の空きスペースを確保することを推奨します。ミラーされていないアグリゲートでは10%が推奨されますが、追加の10%のスペースはファイルシステムで増分変更に対応するために使用できます。増分変更を行うと、ONTAPのcopy-on-write Snapshotベースのアーキテクチャにより、ミラーされたアグリゲートのスペース使用率が向上します。これらのベストプラクティスに従わないと、パフォーマンスに悪影響を及ぼす可能性があります。

## MetroCluster 構成での FlexGroup のサポート

ONTAP 9.6 以降では、MetroCluster 構成で FlexGroup ボリュームがサポートされます。

## MetroCluster 構成での 整合グループのサポート

ONTAP 9.11.1以降、"整合グループ" MetroCluster 構成でサポートされます。

## MetroCluster 構成のジョブスケジュール

ONTAP 9.3 以降では、ユーザが作成したジョブスケジュールが MetroCluster 構成のクラスタ間で自動的にレプリケートされます。クラスタでジョブスケジュールを作成、変更、または削除すると、Configuration Replication Service (CRS) を使用して同じスケジュールがパートナークラスタに自動的に作成されます。



システムによって作成されたスケジュールはレプリケートされません。両方のクラスタのジョブスケジュールが同じになるように、パートナークラスタで同じ処理を手動で実行する必要があります。

## MetroCluster サイトから第 3 のクラスタへのクラスタピアリング

ピアリング設定はレプリケートされないため、MetroCluster 構成のどちらかのクラスタを構成外の第 3 のクラスタにピアリングする場合は、パートナーの MetroCluster クラスタでもピアリングを設定する必要があります。これにより、スイッチオーバーが発生してもピアリングが維持されます。

MetroCluster 以外のクラスタで ONTAP 8.3 以降が実行されている必要があります。そうでない場合、両方の MetroCluster パートナーでピアリングが設定されていても、スイッチオーバーが発生するとピアリングが失われます。

## MetroCluster 構成での LDAP クライアント設定のレプリケーション

ローカルクラスタの Storage Virtual Machine (SVM) に作成された LDAP クライアント設定は、リモートクラスタのパートナーのデータ SVM にレプリケートされます。たとえば、ローカルクラスタの管理 SVM に LDAP クライアント設定が作成されると、リモートクラスタのすべての管理データ SVM にレプリケートされます。この MetroCluster 機能は、リモートクラスタのすべてのパートナー SVM で LDAP クライアント設定をアクティブにするための意図的なものです。

## MetroCluster 構成用のネットワーク設定および LIF 作成ガイドライン

MetroCluster 構成で LIF がどのように作成およびレプリケートされるかを理解しておく必要があります。また、ネットワーク設定時に適切に判断できるように、こういった整合性が必要とされるかも把握しておく必要があります。

関連情報

- "ネットワークと LIF の管理"

- パートナークラスタに IPspace オブジェクトをレプリケートするための要件、および MetroCluster 構成でサブネットと IPv6 を設定するための要件を理解しておく必要があります。

#### IPspace オブジェクトのレプリケーションとサブネットの設定の要件

- MetroCluster 構成でネットワークを設定するときは、LIF の作成に関する要件に注意する必要があります。

#### MetroCluster 構成での LIF の作成に関する要件

- MetroCluster 構成での LIF のレプリケーションの要件を理解しておく必要があります。また、レプリケートされた LIF がパートナークラスタにどのように配置されるかを把握し、LIF のレプリケーションまたは LIF の配置に失敗した場合に発生する問題について確認しておく必要があります。

#### LIF のレプリケーションおよび配置の要件と問題

### IPspace オブジェクトのレプリケーションとサブネットの設定の要件

パートナークラスタに IPspace オブジェクトをレプリケートするための要件、および MetroCluster 構成でサブネットと IPv6 を設定するための要件を理解しておく必要があります。

#### IPspace レプリケーション

IPspace オブジェクトをパートナークラスタにレプリケートするときは、次のガイドラインを考慮する必要があります。

- 2 つのサイトの IPspace 名が一致している必要があります。
- IPspace オブジェクトは手動でパートナークラスタにレプリケートする必要があります。

IPspace をレプリケートする前に作成されて IPspace に割り当てられた Storage Virtual Machine (SVM) は、パートナークラスタにレプリケートされません。

#### サブネット構成

MetroCluster 構成でサブネットを設定するときは、次のガイドラインを考慮する必要があります。

- MetroCluster 構成の両方のクラスタのサブネットが同じ IPspace にあり、サブネット名、サブネット、ブロードキャストドメイン、ゲートウェイが同じである必要があります。
- 2 つのクラスタの IP 範囲が同じである必要があります。

次の例では、IP 範囲が異なります。

```
cluster_A::> network subnet show
```

```
IPspace: Default
```

| Subnet                    | Broadcast      | Avail/       |             |       |  |
|---------------------------|----------------|--------------|-------------|-------|--|
| Name Subnet               | Domain Gateway | Total Ranges |             |       |  |
| subnet1                   | 192.168.2.0/24 | Default      | 192.168.2.1 | 10/10 |  |
| 192.168.2.11-192.168.2.20 |                |              |             |       |  |

```
cluster_B::> network subnet show
```

```
IPspace: Default
```

| Subnet                    | Broadcast      | Avail/       |             |       |  |
|---------------------------|----------------|--------------|-------------|-------|--|
| Name Subnet               | Domain Gateway | Total Ranges |             |       |  |
| subnet1                   | 192.168.2.0/24 | Default      | 192.168.2.1 | 10/10 |  |
| 192.168.2.21-192.168.2.30 |                |              |             |       |  |

## IPv6 の設定

一方のサイトで IPv6 が設定されている場合は、もう一方のサイトでも IPv6 を設定する必要があります。

## 関連情報

- MetroCluster 構成でネットワークを設定するときは、LIF の作成に関する要件に注意する必要があります。

### MetroCluster 構成での LIF の作成に関する要件

- MetroCluster 構成での LIF のレプリケーションの要件を理解しておく必要があります。また、レプリケートされた LIF がパートナークラスタにどのように配置されるかを把握し、LIF のレプリケーションまたは LIF の配置に失敗した場合に発生する問題について確認しておく必要があります。

### LIF のレプリケーションおよび配置の要件と問題

## MetroCluster 構成での LIF の作成に関する要件

MetroCluster 構成でネットワークを設定するときは、LIF の作成に関する要件に注意する必要があります。

LIF を作成する際は、次のガイドラインを考慮する必要があります。

- Fibre Channel : ストレッチ VSAN またはストレッチファブリックを使用する必要があります
- IP/iSCSI : レイヤ 2 拡張ネットワークを使用する必要があります
- ARP ブロードキャスト : 2 つのクラスタ間で ARP ブロードキャストを有効にする必要があります
- LIF の重複 : 同じ IPspace に同じ IP アドレスを持つ複数の LIF (重複する LIF) を作成することはできません

- NFS および SAN 構成：ミラーされていないアグリゲートとミラーされたアグリゲートの両方に、異なる Storage Virtual Machine (SVM) を使用する必要があります
- LIFを作成する前にサブネットオブジェクトを作成する必要があります。ONTAPにはブロードキャストドメインが関連付けられているため、サブネットオブジェクトを使用してデスティネーションクラスタのフェイルオーバーターゲットを決定できます。

#### LIF の作成を確認

MetroCluster 構成内で LIF が正常に作成されたことを確認するには、「MetroCluster check lif show」コマンドを実行します。LIF の作成中に問題が発生した場合は、「MetroCluster check lif repair-placement」コマンドを使用して問題を修正できます。

#### 関連情報

- パートナークラスタに IPspace オブジェクトをレプリケートするための要件、および MetroCluster 構成でサブネットと IPv6 を設定するための要件を理解しておく必要があります。

#### IPspace オブジェクトのレプリケーションとサブネットの設定の要件

- MetroCluster 構成での LIF のレプリケーションの要件を理解しておく必要があります。また、レプリケートされた LIF がパートナークラスタにどのように配置されるかを把握し、LIF のレプリケーションまたは LIF の配置に失敗した場合に発生する問題について確認しておく必要があります。

#### LIF のレプリケーションおよび配置の要件と問題

#### LIF のレプリケーションおよび配置の要件と問題

MetroCluster 構成での LIF のレプリケーションの要件を理解しておく必要があります。また、レプリケートされた LIF がパートナークラスタにどのように配置されるかを把握し、LIF のレプリケーションまたは LIF の配置に失敗した場合に発生する問題について確認しておく必要があります。

#### パートナークラスタへの LIF のレプリケーション

MetroCluster 構成内の 1 つのクラスタに LIF を作成すると、その LIF はパートナークラスタにレプリケートされます。LIF は名前に基づいて 1 対 1 で配置されるわけではありません。スイッチオーバー処理後に LIF を使用できるようにするため、LIF の配置プロセスは、ポートが LIF をホストできるかどうかを到達可能性とポート属性チェックに基づいて検証します。

LIF をレプリケートしてパートナークラスタに配置するには、システムが次の条件を満たしている必要があります。

| 条件     | LIF タイプ：FC                                                                                               | LIF タイプ：IP/iSCSI                                                                              |
|--------|----------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| ノードの識別 | ONTAP は、LIF を作成したノードのディザスタリカバリ (DR) パートナーに、レプリケートされた LIF を配置します。DR パートナーが使用できない場合は、DR 補助パートナーが配置に使用されます。 | ONTAP は、LIF を作成したノードの DR パートナーに、レプリケートされた LIF を配置します。DR パートナーが使用できない場合は、DR 補助パートナーが配置に使用されます。 |

|                  |                                                                                                                           |                                                                                                                                                                                                                                               |
|------------------|---------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>ポートの識別</p>    | <p>ONTAP は、DR クラスタで接続されている FC ターゲットポートを特定します。</p>                                                                         | <p>ソース LIF と同じ IPspace にある DR クラスタのポートが到達可能性チェックの対象として選択されません。</p> <p>DR クラスタに同じ IPspace のポートがない場合は LIF を配置できません。</p> <p>同じ IPspace とサブネットですすでに LIF をホストしている DR クラスタのポートは自動的に到達可能とマークされ、配置先として使用できます。これらのポートは、到達可能性チェックの対象ではありません。</p>        |
| <p>到達可能性チェック</p> | <p>到達可能性は、DR クラスタのポートのソースファブリック WWN の接続をチェックすることによって判別されます。</p> <p>DR サイトに同じファブリックがない場合、LIF は DR パートナーの任意のポートに配置されます。</p> | <p>上記で特定された DR クラスタの各ポートから配置する LIF のソース IP アドレスに Address Resolution Protocol (ARP) ブロードキャストが送信され、その応答に基づいて到達可能性が判別されます。</p> <p>到達可能性チェックが成功するためには、2つのクラスタ間で ARP ブロードキャストが許可されている必要があります。</p> <p>ソース LIF から応答を受信した各ポートが配置可能なポートとしてマークされます。</p> |

|                  |                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------|---------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>ポートを選択します</p> | <p>ONTAP では、アダプタタイプや速度などの属性に基づいてポートが分類され、属性が一致するポートが選択されます。</p> <p>属性が一致するポートがない場合、LIF は DR パートナーの任意の接続されたポートに配置されます。</p> | <p>到達可能性チェックで到達可能とマークされたポートのうち、ONTAP が優先して LIF のサブネットに関連付けられたブロードキャストドメイン内のポートを選択します。</p> <p>DR クラスタに LIF のサブネットに関連付けられたブロードキャストドメイン内の使用可能なネットワークポートがない場合は、ソース LIF に到達可能なポートが ONTAP によって選択されます。</p> <p>ソース LIF に到達可能なポートがない場合は、ソース LIF のサブネットに関連付けられたブロードキャストドメインからポートが選択され、該当するブロードキャストドメインが存在しない場合は、任意のポートが選択されます。</p> <p>ONTAP は、アダプタタイプ、インターフェイスタイプ、速度などの属性に基づいてポートを分類し、属性が一致するポートを選択します。</p> |
| <p>LIF の配置</p>   | <p>到達可能なポートのうち、ONTAP は最も負荷の少ないポートを配置先として選択します。</p>                                                                        | <p>選択したポートのうち、ONTAP は最も負荷の少ないポートを配置対象として選択します。</p>                                                                                                                                                                                                                                                                                                                                                |

#### DR パートナー停止時のレプリケートされた LIF の配置

あるノードに iSCSI または FC LIF が作成され、そのノードの DR パートナーがテイクオーバーされた場合、LIF がレプリケートされて DR 補助パートナーノードに配置されます。その後ギブバック処理が発生しても、LIF は DR パートナーに自動的に移動されません。そのため、パートナークラスタ内の 1 つのノードに LIF が集中する可能性があります。MetroCluster のスイッチオーバー処理が発生した場合、その後の Storage Virtual Machine (SVM) に属する LUN をマップしようとしても失敗します。

テイクオーバー処理またはギブバック処理のあとに「lif check lif show」コマンドを実行して、MetroCluster の配置が正しいことを確認する必要があります。エラーがある場合は、「MetroCluster check lif replacement」コマンドを実行して問題を解決します。

#### LIF 配置エラー

MetroCluster check lif show コマンドで表示される LIF 配置エラーは、スイッチオーバー操作の後も保持されます。配置エラーがある LIF に対して network interface modify コマンド、network interface rename コマンド MetroCluster、または network interface delete コマンドを実行すると、エラーは削除され、「lif check show」コマンドの出力には表示されません。

## LIF レプリケーションエラーです

また、MetroCluster check lif show コマンドを使用して、LIF のレプリケーションが成功したかどうかを確認することもできます。LIF のレプリケーションが失敗すると、EMS メッセージが表示されます。

レプリケーションの障害を修正するには、正しいポートが見つからなかった LIF に対して「MetroCluster check lif repair-placement」コマンドを実行します。MetroCluster スイッチオーバー処理の際に確実に LIF を使用できるよう、LIF のレプリケーションエラーはできるだけ早く解決する必要があります。



ソース SVM がダウンしている場合でも、デスティネーション SVM で同じ IPspace とネットワークを使用するポートに別の SVM に所属する LIF が設定されていれば、LIF の配置は続行されます。

スイッチオーバー後は LIF にアクセスできなくなります

ソースノードと DR ノードの FC ターゲットポートが接続されている FC スイッチファブリックに何らかの変更を加えると、スイッチオーバー処理のあとに、DR パートナーに配置された FC LIF にホストからアクセスできなくなることがあります。

MetroCluster のホスト接続を確認するには、FC スイッチファブリックに変更を加えたあとに、ソースノードと DR ノードで「lif check life-placement」コマンドを実行する必要があります。スイッチファブリックの変更内容によっては、DR パートナーノードの別のターゲット FC ポートに LIF が配置されることがあります。

## 関連情報

- パートナークラスタに IPspace オブジェクトをレプリケートするための要件、および MetroCluster 構成でサブネットと IPv6 を設定するための要件を理解しておく必要があります。

### [IPspace オブジェクトのレプリケーションとサブネットの設定の要件](#)

- MetroCluster 構成でネットワークを設定するときは、LIF の作成に関する要件に注意する必要があります。

### [MetroCluster 構成での LIF の作成に関する要件](#)

## ルートアグリゲートでのボリューム作成

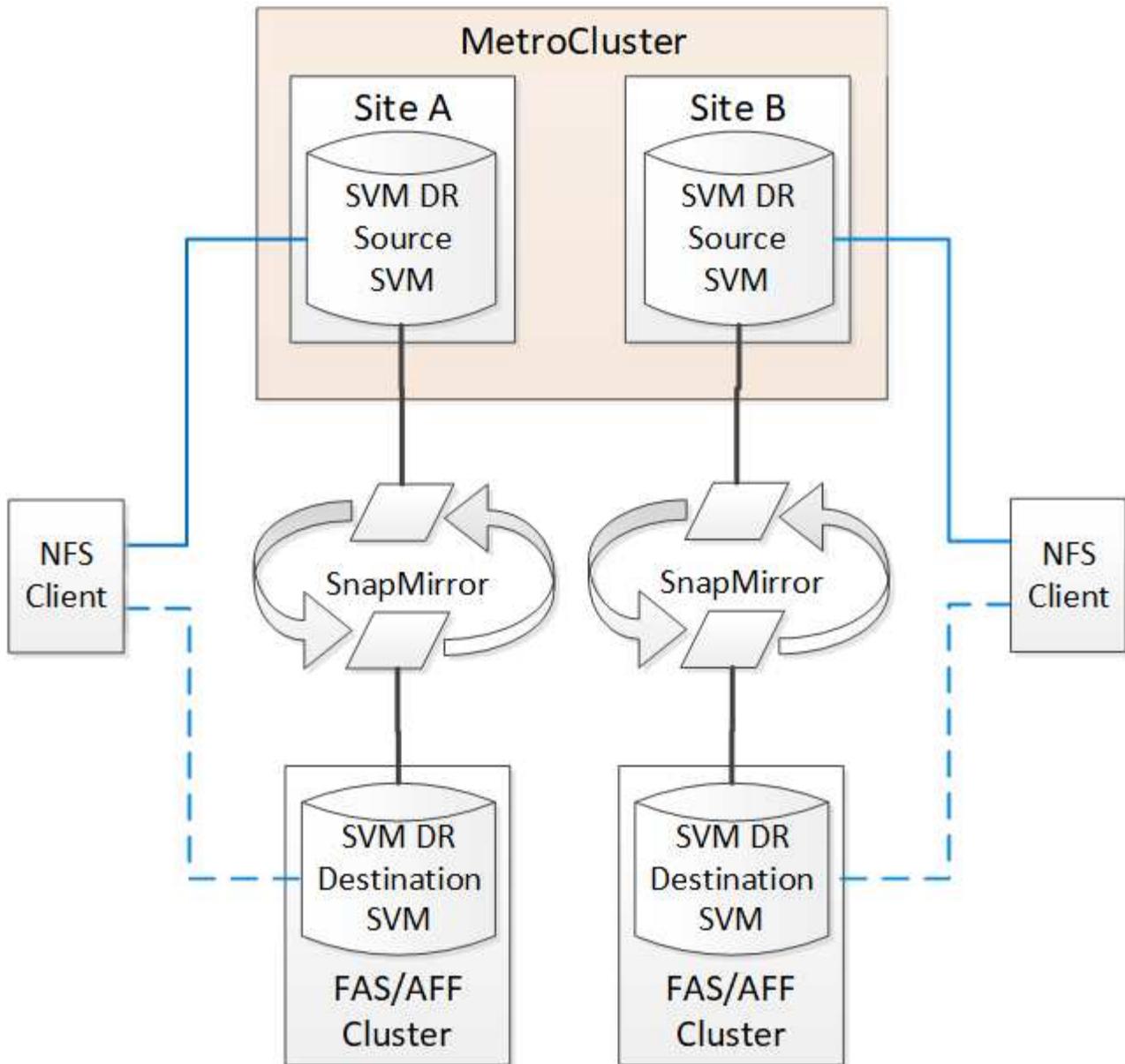
MetroCluster 構成内のノードのルートアグリゲート（HA ポリシーが CFO）に新しいボリュームを作成することはできません。

この制限があるため、ルートアグリゲートを vserver add-aggregates コマンドで SVM に追加することはできません。

## MetroCluster 構成の SVM ディザスタリカバリ

ONTAP 9.5 以降では、MetroCluster 構成のアクティブな Storage Virtual Machine（SVM）を SnapMirror SVM ディザスタリカバリ機能でソースとして使用できます。デスティネーション SVM は、MetroCluster 構成外の第 3 のクラスタに配置する必要があります。

ONTAP 9.11.1以降では、次の図に示すように、MetroCluster 構成内の両方のサイトを、FAS または AFF デスティネーションクラスタを使用した SVM DR関係のソースにすることができます。



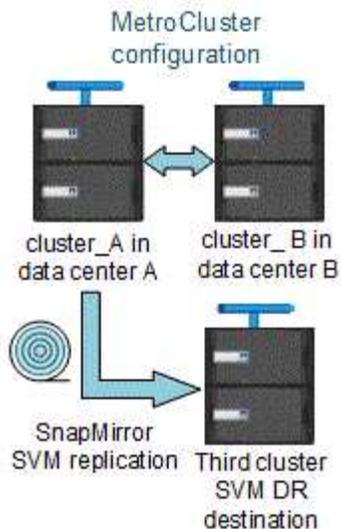
SVM を SnapMirror ディザスタリカバリで使用する場合は、次の要件と制限事項に注意してください。

- SVM ディザスタリカバリ関係のソースとして使用できるのは、MetroCluster 構成内のアクティブな SVM だけです。

スイッチオーバー前の同期元の SVM とスイッチオーバー後の同期先の SVM のどちらもソースに使用できます。

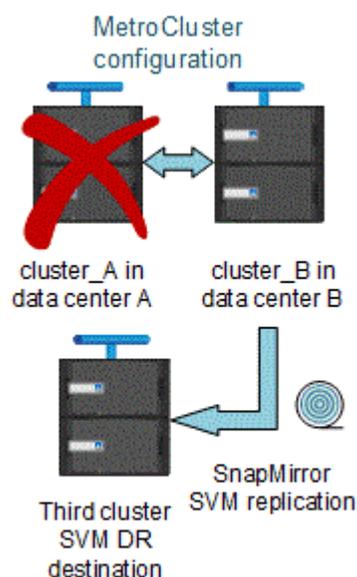
- MetroCluster 構成が安定した状態のときは MetroCluster の同期先の SVM はオンラインでないため、同期先ボリュームを SVM ディザスタリカバリ関係のソースにすることはできません。

次の図は、安定した状態における SVM ディザスタリカバリの動作を示しています。



- SVM DR 関係のソースが同期元の SVM の場合、ソースの SVM DR 関係情報が MetroCluster パートナーにレプリケートされます。

これにより、次の図に示すように、スイッチオーバー後も SVM DR の更新を続行できます。



- スイッチオーバーおよびスイッチバックの実行中に、SVM DR のデスティネーションへのレプリケーションが失敗することがあります。

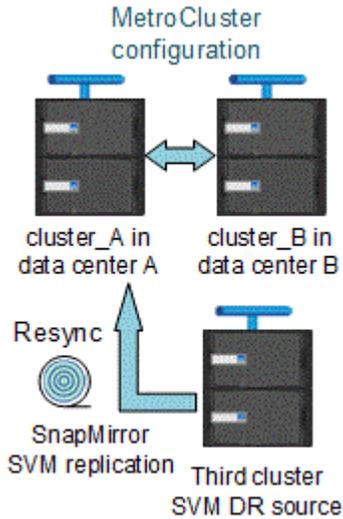
ただし、スイッチオーバーまたはスイッチバックプロセスの完了後、SVM DR の次回のスケジュールされている更新は成功します。

の「SVM の設定のレプリケート」セクションを参照してください "[CLI によるデータ保護](#)" SVM DR 関係の設定の詳細については、[を参照してください](#)。

#### ディザスタリカバリサイトでの SVM の再同期

再同期では、MetroCluster 構成の Storage Virtual Machine (SVM) ディザスタリカバリ (DR) ソースが MetroCluster でないサイトのデスティネーション SVM からリストアされます。

再同期中は、次の図に示すように、ソース SVM（cluster\_A）が一時的にデスティネーション SVM として機能します。



再同期中に計画外スイッチオーバーが発生した場合

再同期中に計画外スイッチオーバーが発生すると、再同期の転送が停止します。計画外スイッチオーバーが発生した場合は次のようになります。

- MetroCluster サイトのデスティネーション SVM（再同期前のソース SVM）は、デスティネーション SVM のままです。パートナークラスタの SVM は、同じサブタイプで非アクティブのままです。
- 同期先の SVM をデスティネーションとする SnapMirror 関係を手動で再作成する必要があります。
- スイッチオーバー後、SnapMirror 作成処理を実行しないかぎり、サバイバーサイトでの SnapMirror show の出力に SnapMirror 関係は表示されません。

再同期中に計画外スイッチオーバーが発生した場合は、スイッチバックを実行

スイッチバックプロセスを正常に実行するには、再同期関係を解除して削除する必要があります。MetroCluster 構成に SnapMirror DR のデスティネーション SVM がある場合、またはクラスタにサブタイプ「d p-destination」の SVM がある場合、スイッチバックは実行できません。

## MetroCluster スイッチオーバー後に **storage aggregate plex show** コマンドの出力が確定しない

MetroCluster のスイッチオーバー後に「storage aggregate plex show」コマンドを実行すると、スイッチオーバーされたルートアグリゲートの plex0 のステータスが確定していないため、「failed」と表示されます。この間、スイッチオーバーされたルートは更新されません。このプレックスの実際のステータスは、MetroCluster 修復フェーズ後に確定します。

## スイッチオーバー発生時に **NVFAIL** フラグを設定するためのボリュームの変更

MetroCluster スイッチオーバーが発生した場合に NVFAIL フラグが設定されるようにボリュームを変更することができます。NVFAIL フラグが設定されたボリュームは、一切変更されなくなります。コミットされた書き込みがスイッチオーバー後に失われたと想定してボリュームを処理する必要がある場合は、この変更が必要となります。

このタスクについて



9.0 よりも前のバージョンの ONTAP では、スイッチオーバーのたびに NVFAIL フラグが設定されます。ONTAP 9.0 以降のバージョンでは、計画外スイッチオーバー（USO）が使用されません。

ステップ

1. スイッチオーバー時に MetroCluster 構成で NVFAIL をトリガーするには、「vol-dr-force-nvfail」パラメータを「on」に設定します。

```
*vol modify -vserver_name _-volume -name _-dr-force-nvfail on *
```

## 追加情報の参照先

MetroCluster の設定と処理の詳細については、[を参照してください](#)。

### MetroCluster およびその他の情報

| 情報                                                                    | 件名                                                                                                                                                                 |
|-----------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">"ONTAP 9 のドキュメント"</a>                                     | <ul style="list-style-type: none"><li>• すべての MetroCluster 情報</li></ul>                                                                                             |
| <a href="#">"NetApp MetroCluster 解決策のアーキテクチャと設計、TR-4705"</a>          | <ul style="list-style-type: none"><li>• MetroCluster FC の構成と運用の技術概要</li><li>• MetroCluster FC 構成のベストプラクティス</li></ul>                                               |
| <a href="#">"MetroCluster IP 解決策のアーキテクチャおよび設計、TR-4689"</a>            | <ul style="list-style-type: none"><li>• MetroCluster IP の構成と運用の技術概要</li><li>• MetroCluster IP 構成のベストプラクティス。</li></ul>                                              |
| <a href="#">"ストレッチ MetroCluster のインストールと設定"</a>                       | <ul style="list-style-type: none"><li>• ストレッチ MetroCluster アーキテクチャ</li><li>• 構成のケーブル接続</li><li>• FC-to-SAS ブリッジの設定</li><li>• ONTAP で MetroCluster を設定します</li></ul> |
| <a href="#">"MetroCluster IP のインストールと設定：ONTAP MetroCluster 構成の違い"</a> | <ul style="list-style-type: none"><li>• MetroCluster IP アーキテクチャ</li><li>• 構成のケーブル接続</li><li>• ONTAP で MetroCluster を設定します</li></ul>                                |
| <a href="#">"MetroCluster の管理とディザスタリカバリ"</a>                          | <ul style="list-style-type: none"><li>• MetroCluster 構成について</li><li>• スイッチオーバー、修復、スイッチバック</li><li>• ディザスタリカバリ</li></ul>                                            |

|                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>"MetroCluster のコンポーネントをメンテナンスしません"</p>                                                | <ul style="list-style-type: none"> <li>• MetroCluster FC 構成のメンテナンスガイドライン</li> <li>• FC-to-SAS ブリッジおよび FC スイッチのハードウェア交換 / アップグレードおよびファームウェアアップグレード手順</li> <li>• ファブリック接続またはストレッチ MetroCluster FC 構成でのディスクシェルフのホットアド</li> <li>• ファブリック接続またはストレッチ MetroCluster FC 構成でのディスクシェルフのホットリムーブ</li> <li>• ファブリック接続またはストレッチ MetroCluster FC 構成のディザスタサイトでのハードウェア交換</li> <li>• 2 ノードのファブリック接続またはストレッチ MetroCluster FC 構成の 4 ノード MetroCluster 構成への拡張</li> <li>• 4 ノードのファブリック接続またはストレッチ MetroCluster FC 構成の 8 ノード MetroCluster FC 構成への拡張</li> </ul> |
| <p>"MetroCluster FC から MetroCluster IP に移行します"</p> <p>"MetroCluster アップグレードおよび拡張ガイド"</p> | <ul style="list-style-type: none"> <li>• MetroCluster 設定をアップグレードまたは更新する</li> <li>• MetroCluster FC 構成から MetroCluster IP 構成への移行</li> <li>• ノードの追加による MetroCluster 構成の拡張</li> </ul>                                                                                                                                                                                                                                                                                                                                                   |
| <p>"MetroCluster Tiebreaker ソフトウェアのインストールおよび設定"</p>                                      | <ul style="list-style-type: none"> <li>• MetroCluster Tiebreaker ソフトウェアを使用して MetroCluster 構成を監視する</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <p>Active IQ デジタルアドバイザーのドキュメント</p> <p>"ネットアップのマニュアル：製品ガイドとリソース"</p>                      | <ul style="list-style-type: none"> <li>• MetroCluster の設定とパフォーマンスを監視する</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <p>"コピーベースの移行"</p>                                                                       | <ul style="list-style-type: none"> <li>• 7-Mode ストレージシステムから clustered Data ONTAP ストレージシステムへデータを移行する</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <p>"ONTAP の概念"</p>                                                                       | <ul style="list-style-type: none"> <li>• ミラーされたアグリゲートの機能</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

## 著作権に関する情報

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および/または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

## 商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。