



ストレッチ **MetroCluster** 構成をインストール ONTAP MetroCluster

NetApp
February 13, 2026

目次

ストレッチ MetroCluster 構成をインストール	1
概要	1
MetroCluster のインストールを準備	1
ONTAP MetroCluster 構成の違い	1
クラスピアリング	3
ミラーされていないアグリゲートを使用する場合の	5
MetroCluster サイトでのファイアウォールの使用状況	6
構成に適したインストール手順の選択	6
2 ノード SAS 接続ストレッチ MetroCluster 構成のケーブル接続	7
2 ノード SAS 接続ストレッチ MetroCluster 構成のケーブル接続	7
2 ノード SAS 接続ストレッチ MetroCluster 構成のコンポーネント	7
2 ノード SAS 接続ストレッチ構成の MetroCluster に必要なハードウェアコンポーネントと命名ガイドライン	8
2 ノード SAS 接続ストレッチ構成の MetroCluster コンポーネントを設置してケーブル接続します	9
2 ノードブリッジ接続ストレッチ MetroCluster 構成をケーブル接続します	13
2 ノードブリッジ接続ストレッチ MetroCluster 構成のケーブル接続	13
2 ノードブリッジ接続ストレッチ MetroCluster 構成のコンポーネント	13
2 ノードブリッジ接続ストレッチ構成の MetroCluster に必要なハードウェアコンポーネントと命名規則	14
FC-to-SAS ブリッジの情報収集ワークシート	17
MetroCluster コンポーネントを設置してケーブルを配線します	18
FC-to-SAS ブリッジおよび SAS ディスクシェルフを設置	20
ONTAP での MetroCluster ソフトウェアの設定	34
サイト A の IP ネットワーク情報ワークシート	35
サイト B の IP ネットワーク情報ワークシート	37
標準クラスタ構成と MetroCluster 構成の類似点 / 相違点	39
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	40
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	42
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	44
コンポーネントの HA 状態の確認	46
2 ノード MetroCluster 構成での ONTAP のセットアップ	47
クラスタを MetroCluster 構成に設定	49
Config Advisor での MetroCluster 構成エラーの確認	72
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	72
構成バックアップファイルを保護しています	73
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	73
MetroCluster 構成をテストする	76
ネゴシエートスイッチオーバーを検証中	76
修復と手動スイッチバックの検証	78

単一の FC-to-SAS ブリッジの停止	80
電源回線切断後の動作確認	82
単一のストレージシェルフが停止したあとの動作確認	83
MetroCluster 構成を削除	94
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	95
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	95
NTP を使用してシステム時刻を同期します	95
MetroCluster 構成で ONTAP を使用する場合の考慮事項	96
ライセンスに関する考慮事項	97
SnapMirror に関する考慮事項	97
MetroCluster 構成での FlexCache のサポート	97
MetroCluster 構成での FabricPool のサポート	97
MetroCluster 構成での FlexGroup のサポート	98
MetroCluster 構成のジョブスケジュール	98
MetroCluster サイトから第 3 のクラスタへのクラスタピアリング	99
MetroCluster 構成での LDAP クライアント設定のレプリケーション	99
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	99
MetroCluster 構成の SVM ディザスタリカバリ	103
2 ノードストレッチ MetroCluster 構成での storage disk show コマンドおよび storage shelf show	105
コマンドの出力	
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	106
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	106
ストレッチからファブリック接続への MetroCluster 構成の移行	106
追加情報の参照先	107
MetroCluster およびその他の情報	107

ストレッチ MetroCluster 構成をインストール

概要

ストレッチ 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"
- "正しいインストール手順を選択します"
- コンポーネントをケーブル接続します
 - "2 ノード SAS 接続構成"
 - "2 ノードブリッジ接続構成"
- "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 ¹	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 すべての SAN アレイ	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わ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。

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で構成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

構成に適したインストール手順の選択

ストレージコントローラがストレージシェルフに接続される方法に基づいて、適切なイ

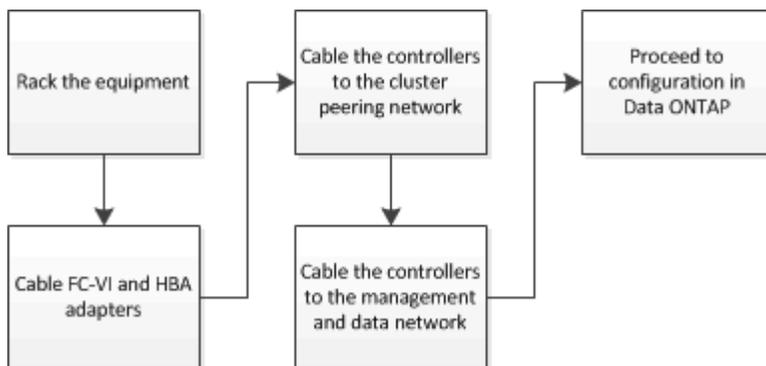
インストール手順を選択する必要があります。

インストールの種類	使用する手順
FC-to SAS ブリッジを使用する 2 ノードストレッチ構成	<ol style="list-style-type: none">1. "2 ノードブリッジ接続ストレッチ MetroCluster 構成のケーブル接続"2. "ONTAP での MetroCluster ソフトウェアの設定"
直接接続型の SAS ケーブル接続を使用する 2 ノードストレッチ構成	<ol style="list-style-type: none">1. "2 ノード SAS 接続ストレッチ MetroCluster 構成のケーブル接続"2. "ONTAP での MetroCluster ソフトウェアの設定"

2 ノード SAS 接続ストレッチ MetroCluster 構成のケーブル接続

2 ノード SAS 接続ストレッチ 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。



2 ノード SAS 接続ストレッチ MetroCluster 構成のコンポーネント

2 ノード MetroCluster SAS 接続構成には、ストレージコントローラを SAS ケーブルでストレージに直接接続した 2 つのシングルノードクラスターなど、さまざまなコンポーネントが必要です。

MetroCluster の設定には、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、SAS ケーブルを使用してストレージに直接接続します。

各ストレージコントローラは、パートナーサイトのストレージコントローラに対する DR パートナーとして構成されます。

- 短い距離には SAS 銅線ケーブルを使用できます。

- 長い距離には SAS 光ケーブルを使用できます。

["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。

- 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を経由して、Storage Virtual Machine (SVM) の設定がミラーされます。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。

2 ノード SAS 接続ストレッチ構成の MetroCluster に必要なハードウェアコンポーネントと命名ガイドライン

MetroCluster 構成にはさまざまなハードウェアコンポーネントが必要です。わかりやすいように、MetroCluster のドキュメント全般をとおして標準的なコンポーネント名を使用します。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 構成でのハードウェアの冗長性

MetroCluster 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。

シングルノード ONTAP クラスタ × 2

SAS 接続ストレッチ MetroCluster 構成には、シングルノード ONTAP クラスタが 2 つ必要です。

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

ストレージコントローラモジュール × 2

SAS 接続ストレッチ MetroCluster 構成には、ストレージコントローラモジュールが 2 つ必要です。

- 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。
- 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は混在できません。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

SAS ディスクシェルフ × 4 台以上 (推奨)

SAS 接続ストレッチ MetroCluster 構成には、SAS ディスクシェルフが少なくとも 2 台必要です。推奨される SAS ディスクシェルフ数は 4 台です。

シェルフ単位でのディスク割り当てを可能にするために、各サイトにシェルフを 2 台配置することを推奨します。各サイトにシェルフ 1 台の最小構成もサポートされます。

名前の例：

- サイト A :
 - shelf_A_1_1
 - shelf_A_1_2
- サイト B :
 - shelf_B_1_1
 - shelf_B_1_2

2 ノード SAS 接続ストレッチ構成の MetroCluster コンポーネントを設置してケーブル接続します

2 ノード SAS 接続ストレッチ構成の MetroCluster コンポーネントの設置とケーブル接続

ストレージコントローラをストレージメディアおよび他のストレージコントローラにケーブル接続する必要があります。ストレージコントローラは、データおよび管理ネットワークにもケーブル接続する必要があります。

本ドキュメントで手順を開始する前に

このタスクを実行するには、次の全体的な要件を満たしている必要があります。

- 設置前に、ディスクシェルフモデルに応じた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。
- すべてのMetroClusterコンポーネントがサポートされ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。

このタスクについて

- 「ノード」と「コントローラ」は同じ意味で使用されます。

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。

必要なラックスペースは、ストレージコントローラ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. 電気機器を扱うための標準的な製造方法を使用して、適切に接地されていることを確認します。
3. ストレージコントローラ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. ディスクシェルフを設置し、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、電源を投入して、シェルフ ID を設定します。

ディスクシェルフのデイジーチェーン接続とシェルフ ID の設定については、ディスクシェルフモデルに対応するガイドを参照してください。



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。シェルフ ID を手動で設定する場合は、ディスクシェルフの電源を再投入する必要があります。

コントローラ間およびコントローラとストレージシェルフのケーブル接続

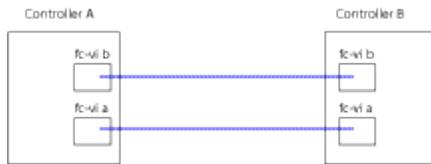
コントローラの FC-VI アダプタどうしを直接ケーブル接続する必要があります。コント

ローラの SAS ポートは、リモートとローカルの両方のストレージスタックにケーブル接続する必要があります。

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. FC-VI ポートをケーブル接続します。

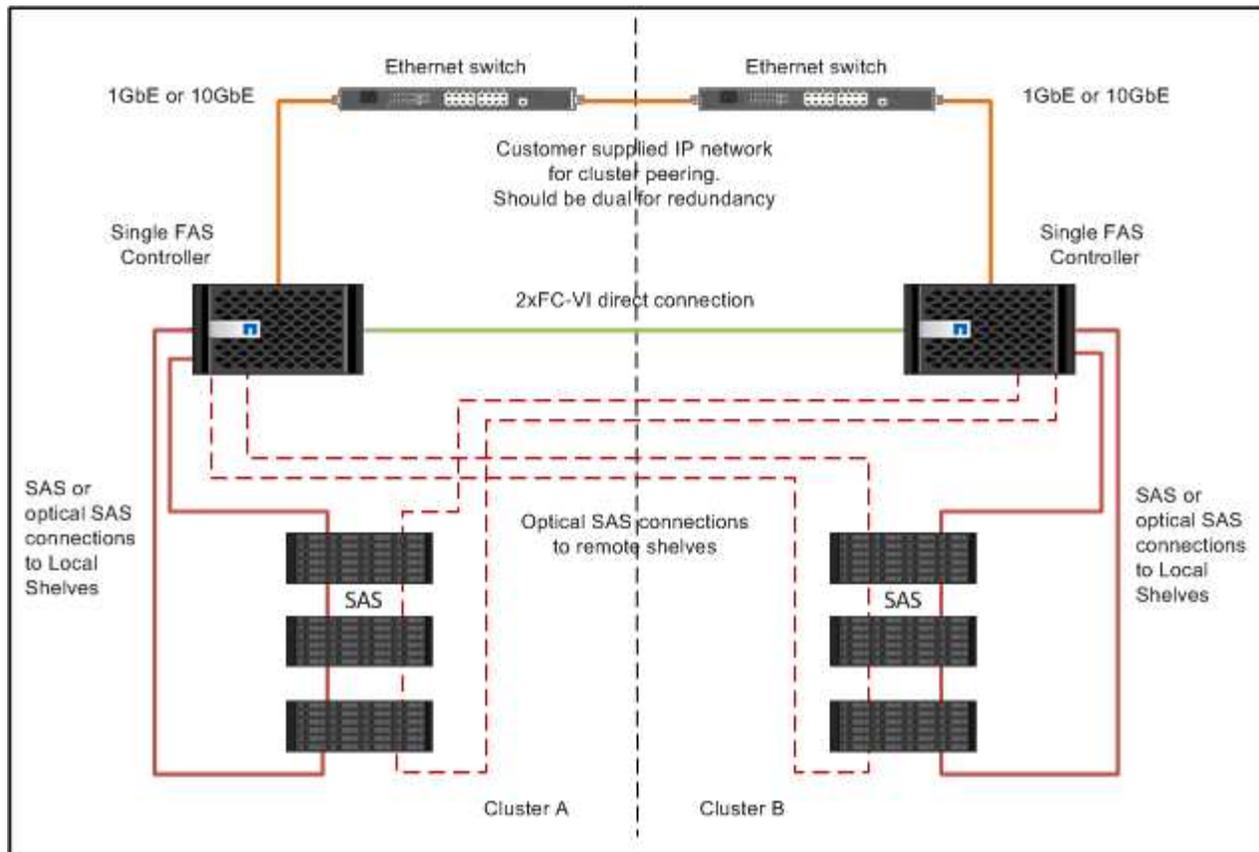


上の図は、一般的なケーブル接続を示しています。FC-VI ポートはコントローラモジュールによって異なります。

- FAS8200 および AFF A300 コントローラモジュールでは、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。
 - オンボードポート 0e と 0f は、FC-VI モードで設定します。
 - FC-VI カードのポート 1a および 1b は、スロット 1 に装着します。
- AFF A700 および FAS9000 ストレージシステムのコントローラモジュールは、それぞれ FC-VI ポートを 4 つ使用します。
- AFF A400 および FAS8300 ストレージシステムコントローラモジュールは、FC-VI ポート 2a および 2b を使用します。

2. SAS ポートをケーブル接続します。

次の図は接続を示しています。使用するポートは、コントローラモジュールの利用可能な SAS ポートと FC-VI ポートによって異なることがあります。



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、それらのポートがパートナーサイトのクラスタに接続されるようにする必要があります。

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。

手順

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。

"クラスタと SVM のピアリングの簡単な設定"

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。

このタスクは、両方の MetroCluster サイトで新しいコントローラを配置するたび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できます。また、NetApp CN1601 クラスタ管理スイッチなど、新しい専用ネットワークスイッチにコントローラを接続することもできます。

手順

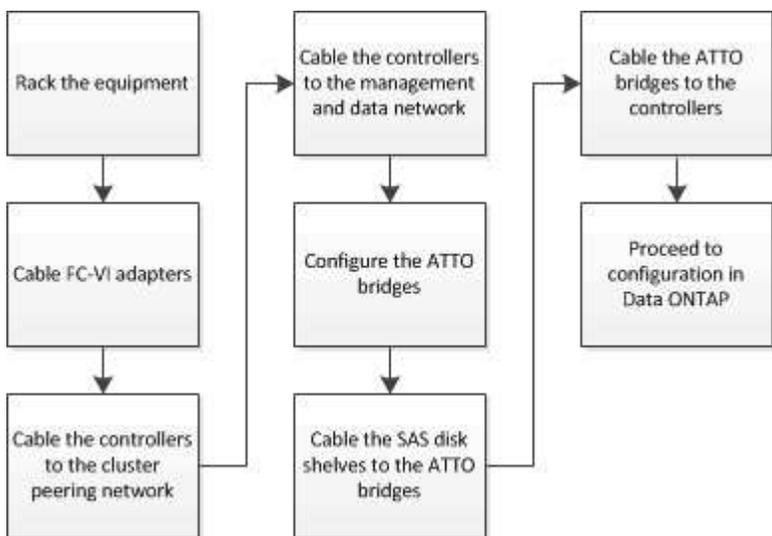
1. コントローラの管理ポートとデータポートを、ローカルサイトの管理ネットワークとデータネットワークにケーブル接続します。

["ONTAPハードウェアシステムのドキュメント"](#)

2 ノードブリッジ接続ストレッチ MetroCluster 構成をケーブル接続します

2 ノードブリッジ接続ストレッチ 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。



2 ノードブリッジ接続ストレッチ MetroCluster 構成のコンポーネント

MetroCluster 構成を計画するときは、構成のコンポーネントとそれらの連携について理解しておく必要があります。

MetroCluster の設定には、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、FC-to-SAS ブリッジに接続されます。ストレージコントローラは、各コントローラの FC-VI アダプタどうしを FC ケーブルで接続することで相互に接続されます。

各ストレージコントローラは、パートナーサイトのストレージコントローラに対する DR パートナーとして構成されます。

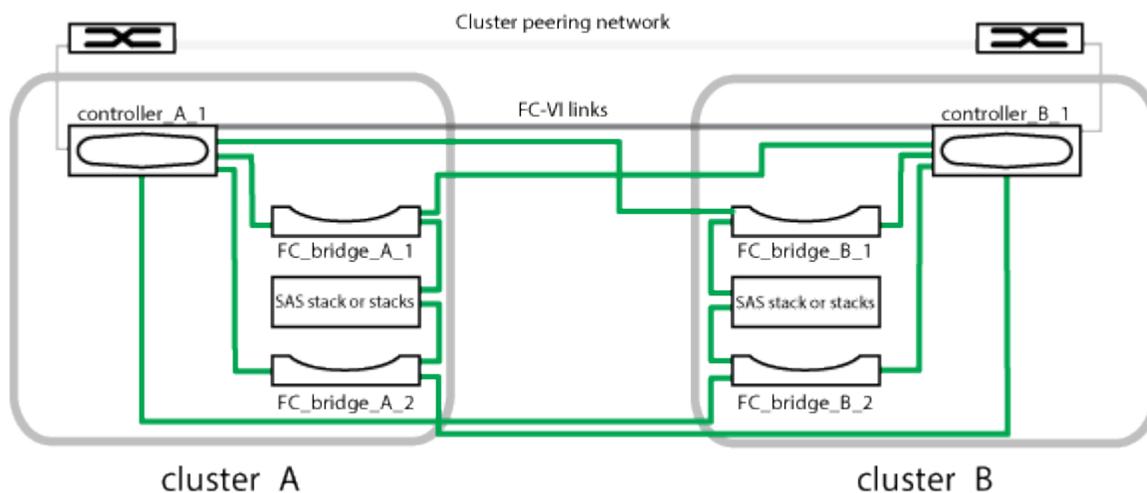
- FC-to-SAS ブリッジ

FC-to-SAS ブリッジは、コントローラ上の FC イニシエータポートに SAS ストレージスタックを接続して、2つのプロトコル間のブリッジの役割を果たします。

- 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を経由して、Storage Virtual Machine (SVM) の設定がミラーされます。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。

次の図は、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つのシングルノードクラスタで構成されます。
- 各サイトには、SAS ストレージスタックが1つ以上あります。



MetroCluster 構成の SAS シェルフは、ACP ケーブル配線ではサポートされていません。

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 ノードブリッジ接続ストレッチ構成の MetroCluster に必要なハードウェアコンポーネントと命名規則

MetroCluster 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 構成でのハードウェアの冗長性

MetroCluster 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。

シングルノード ONTAP クラスタ × 2

ブリッジ接続ストレッチ MetroCluster 構成には、シングルノード ONTAP クラスタが 2 つ必要です。

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

ストレージコントローラモジュール × 2

ブリッジ接続ストレッチ MetroCluster 構成には、ストレージコントローラモジュールが 2 つ必要です。

コントローラ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。
- 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は混在できません。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

FC-to-SAS ブリッジの要件

ブリッジ接続ストレッチ MetroCluster 構成では、各サイトに FC-to-SAS ブリッジが 2 つ以上必要です。

これらのブリッジで SAS ディスクシェルフをコントローラモジュールに接続します。



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。
- 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シェルフで同じモデルを使用する必要があります。

サポートされる IOM モデルは、実行している ONTAP のバージョンによって異なります。

- 名前は MetroCluster 構成内で一意である必要があります。

この手順で例として使用されている推奨名には、ブリッジの接続先コントローラモジュールとポート番号が含まれています。

名前の例：

- サイト A :
 - bridge_A_1__ ポート番号 _
 - bridge_A_2_ ポート番号 `
- サイト B :
 - bridge_B_1__ ポート番号 _
 - Bridge_B_2_ __ ポート番号 _ `

SAS シェルフ × 4 台以上 (推奨)

ブリッジ接続ストレッチ MetroCluster 構成には、SAS シェルフが少なくとも 2 台必要です。ただし、シェルフ単位でのディスク割り当てを可能にするために、各サイトにシェルフを 2 台配置し、合計 4 台の SAS シェルフを使用することを推奨します。

各サイトにシェルフ 1 台の最小構成もサポートされます。

名前の例：

- サイト A :
 - shelf_A_1_1
 - shelf_A_1_2
- サイト B :

- shelf_B_1_1
- shelf_B_1_2

FC-to-SAS ブリッジの情報収集ワークシート

MetroCluster サイトの設定を開始する前に、必要な設定情報を収集する必要があります。

サイト A、FC-to-SAS ブリッジ 1 (FC_bridge_A_1a)

SAS スタックごとに FC-to-SAS ブリッジが少なくとも 2 つ必要です。

各ブリッジは、Controller_A_1_` ` ポート番号 と Controller_B_1_` ` ポート番号 _ に接続します。

サイト A	あなたの値
bridge_A_1a の IP アドレス	
Bridge_A_1a ユーザ名	
Bridge_A_1a のパスワード	

サイト A、FC-to-SAS ブリッジ 2 (FC_bridge_A_1b)

SAS スタックごとに FC-to-SAS ブリッジが少なくとも 2 つ必要です。

各ブリッジは、Controller_A_1_` ` ポート番号 と Controller_B_1_` ` ポート番号 _ に接続します。

サイト A	あなたの値
Bridge_A_1b の IP アドレス	
Bridge_A_1b のユーザ名	
Bridge_A_1b のパスワード	

サイト B、FC-to-SAS ブリッジ 1 (FC_bridge_B_1a)

SAS スタックごとに FC-to-SAS ブリッジが少なくとも 2 つ必要です。

各ブリッジは、Controller_A_1_` ` ポート番号 と Controller_B_1_` ` ポート番号 に接続します。

サイト B	あなたの値
Bridge_B_1a の IP アドレス	

Bridge_B_1a ユーザ名	
Bridge_B_1a のパスワード	

サイト B、FC-to-SASブリッジ 2 (FC_bridge_B_1b)

SAS スタックごとに FC-to-SAS ブリッジが少なくとも 2 つ必要です。

各ブリッジは、Controller_A_1_`ポート番号 と Controller_B_1_`ポート番号 に接続します。

サイト B	あなたの価値
Bridge_B_1b の IP アドレス	
Bridge_B_1b ユーザ名	
Bridge_B_1b のパスワード	

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、ストレージコントローラ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. ストレージコントローラ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. 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。
5. 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、ブリッジモデルに対応する *_ATTO FibreBridge Installation and Operation Manual* を参照してください。

- 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。

コントローラ間のケーブル接続

各コントローラの FC-VI アダプタを対応するパートナーに直接ケーブル接続する必要があります。

手順

1. FC-VI ポートをケーブル接続します。



上の図は、必要なケーブル接続の一般的な例です。FC-VI ポートはコントローラモジュールによって異なります。

- AFF A300 および FAS8200 コントローラモジュールの場合、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コントローラモジュールは、それぞれ FC-VI ポートを 4 つ使用します。

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、それらのポートがパートナーサイトのクラスタに接続されるようにする必要があります。

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。

手順

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。

"クラスタと SVM のピアリングの簡単な設定"

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できます。また、NetApp CN1601 クラスタ管理スイッチなど、新しい専用ネットワークスイッチにコントローラを接続することもできます。

手順

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-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、ATTO FibreBridgeブリッジと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

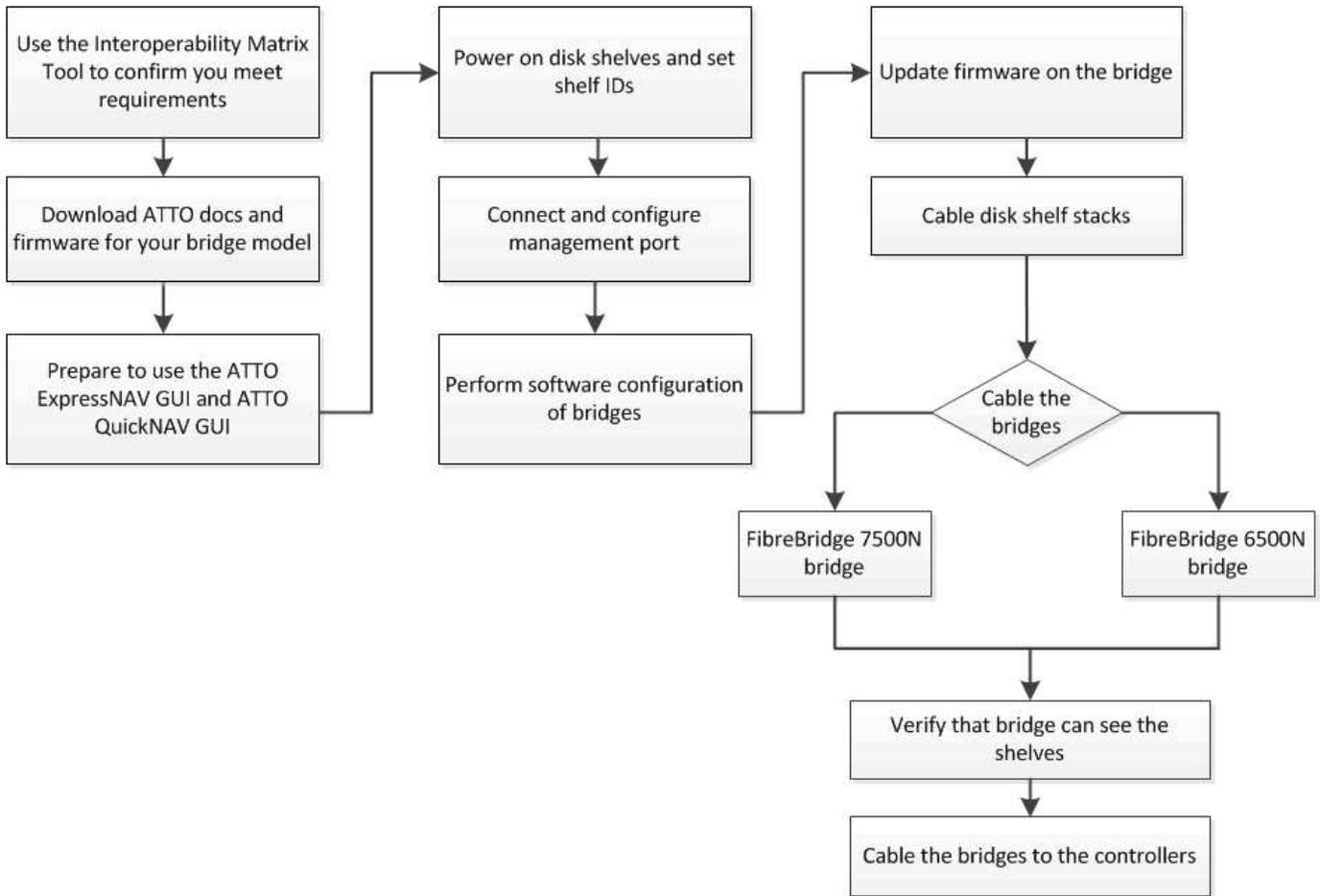
工場出荷状態のシステムの場合は、FC-to-SAS は事前に構成されているため、追加の構成は不要です。

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場合は、ONTAP CLIからブリッジへのFC接続を使用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ていました。

ブリッジCLIコマンドは、ONTAPインターフェイスでONTAP interfaceコマンドを使用して実行でき `storage bridge run-cli -name <bridge_name> -command <bridge_command_name>` ます。



ブリッジの物理接続を制限することでセキュリティを向上させるために、IP アクセスを無効にしたインバンド管理の使用を推奨します。

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準備を行うときは、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設定の要件と、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。

で ["ネットアップの Interoperability Matrix Tool \(IMT\)"](#)、*[Storage Solution]*フィールドを使用してMetroClusterソリューションを選択できます。コンポーネントエクスプローラ*を使用してコンポーネントとONTAPバージョンを選択し、検索を絞り込むことができます。[Show Results]*を選択すると、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コントローラで、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理解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ース、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できる必要があります。

- 50マイ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コントローラ、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も、FibreBridgeブリッジに適用されません。

"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。

- 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。

- 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。

- 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

- 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 <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をに接続し、スタック内の各IOM Aを接続するまで次のシェルフのIOM Aのポート1に接続します。
 - 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。

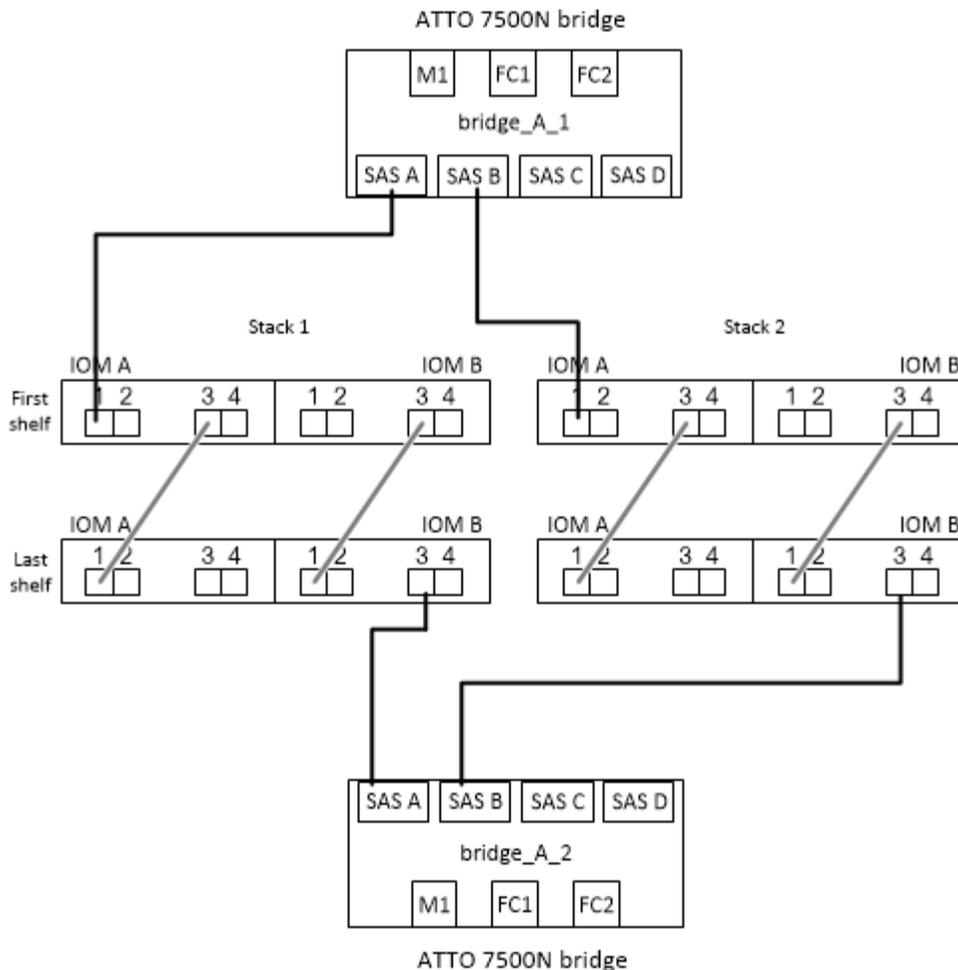
ディスクシェルフのデイジーチェーン接続の詳細については、使用しているディスクシェルフモデルの *Installation and Service Guide* を参照してください。

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、**FC-to-SAS**ブリッジをコントローラの**FC**ポートにケーブル接続します。

2ノードブリッジ接続MetroCluster構成では、ブリッジをコントローラのFCポートにケーブル接続する必要があります。

手順

1. 各ブリッジで、ブリッジが接続されているすべてのディスクドライブおよびディスクシェルフが検出されることを確認します。

「astargets」

「astargets」コマンドの出力には、ブリッジに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。

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	3QP1G7A900009939FNNT
8	NETAPP	X410_S15K6288A15	DISK	3QP1FY0T00009940G8PA
9	NETAPP	X410_S15K6288A15	DISK	3QP1FXW600009940VERQ

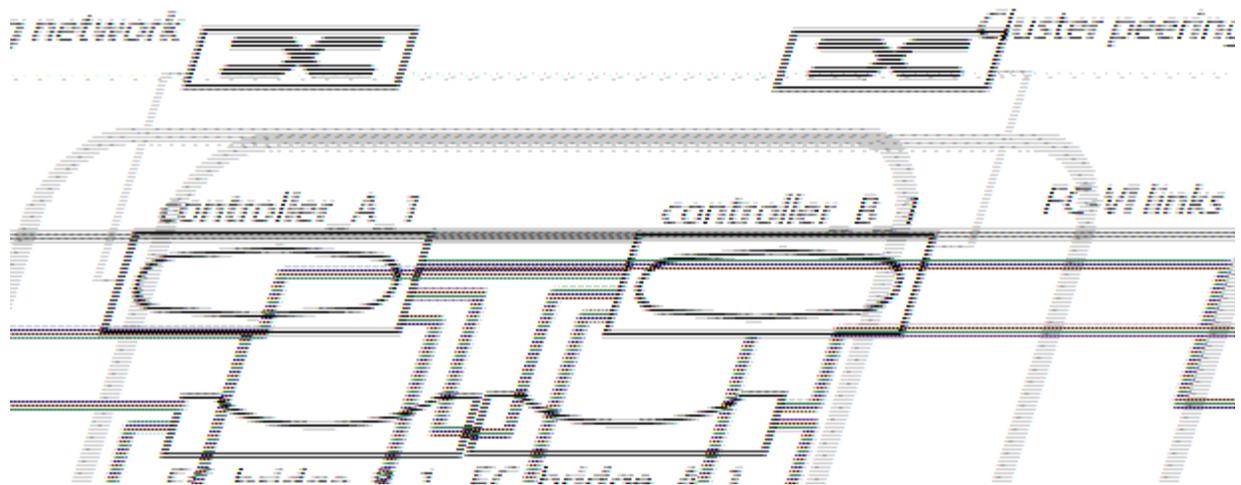
2. コマンド出力で、ブリッジがスタック内の正しいディスクおよびディスクシェルフに接続されていることを確認します。

出力結果	作業
正解です	繰り返します 手順 1 . 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、ディスクシェルフからブリッジへの SAS ケーブル接続をやり直します。</p> <p>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</p> <p>b. 繰り返します 手順 1. 残りの各ブリッジ。</p>

3. `[[step3-cable-each-bridge]`各ブリッジをコントローラのFCポートにケーブル接続します。
- ブリッジのFCポート1をcluster_AのコントローラのFCポートにケーブル接続します。
 - ブリッジのFCポート2をcluster_Bのコントローラ上のFCポートにケーブル接続します。
 - コントローラにクアドポートFCアダプタが設定されている場合は、ストレージスタックの両端にあるブリッジが同じASICの2つのFCポートに接続されていないことを確認してください。例：
 - ポートaとポートbは同じASICを共有します。
 - ポートcとポートdは同じASICを共有します。

この例では、FC_bridge_A_1をポートAに接続し、FC_bridge_A2をポートCに接続します。
 - コントローラに複数のFCアダプタが設定されている場合は、ストレージスタックのどちらかの端にあるブリッジを同じアダプタにケーブル接続しないでください。

このシナリオでは、FC_bridge_A_1をオンボードのFCポートに接続し、FC_bridge_A_2を拡張スロットのアダプタのFCポートに接続します。



4. 繰り返します **手順 3** 他のブリッジについて、すべてのブリッジがケーブル接続されるまで。

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ーの 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
```

- 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 <bridge-name> -command saveconfiguration
```

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
```

- 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。

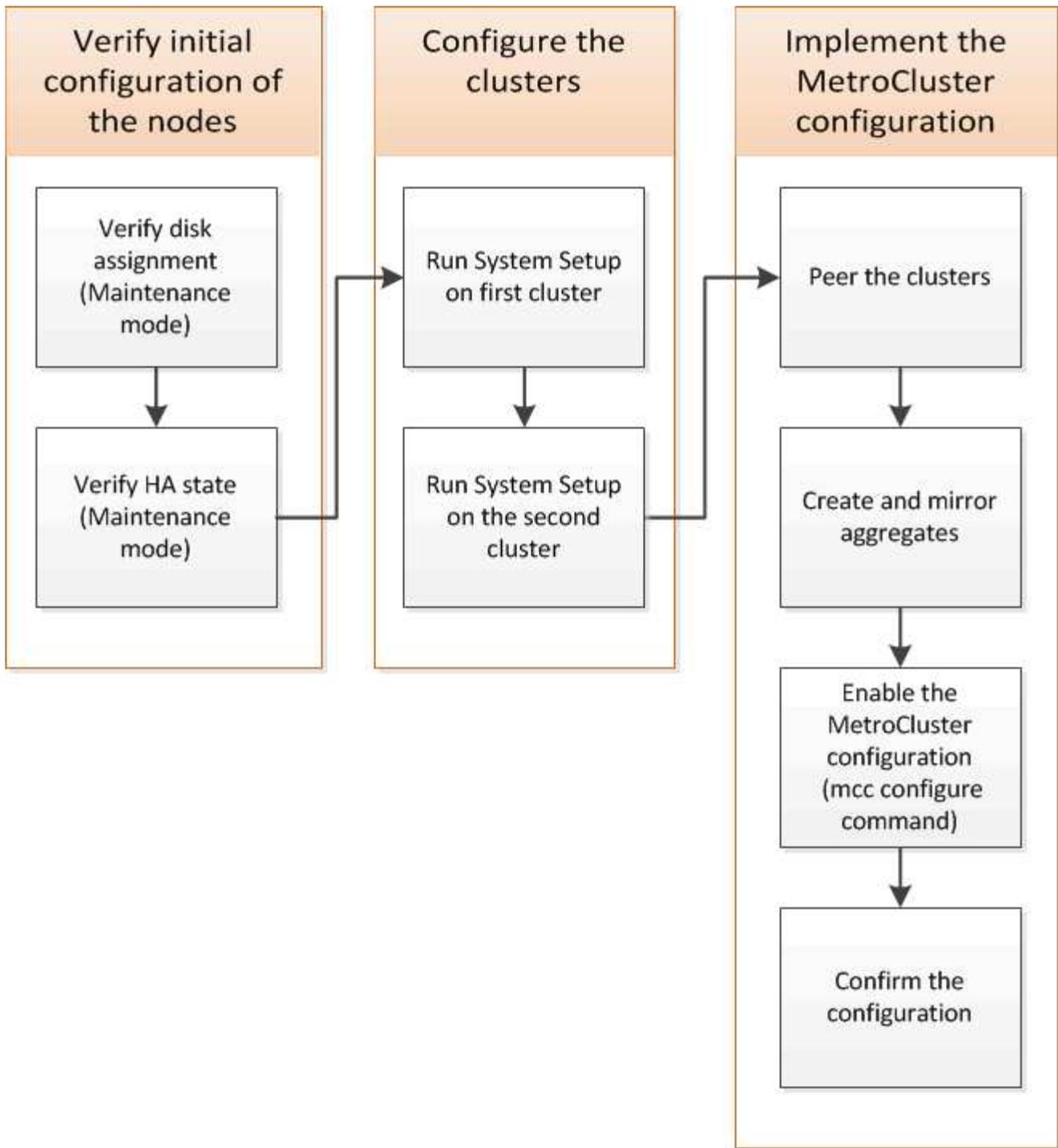
```
storage bridge run-cli -bridge <bridge-name> -command firmwarerestart
```

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 での MetroCluster ソフトウェアの設定

MetroCluster 構成の各ノードは、ノードレベルの設定や 2 つのサイトへのノードの設定を含めて、ONTAP で設定する必要があります。また、2 つのサイト間に MetroCluster 関係を実装する必要があります。



手順

1. 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 アドレスを収集します。
2. サイト A の IP ネットワーク情報ワークシートに記入

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。

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。この情報で使用している例： 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：この情報で 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 この情報で使用して 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				
----------------	--	--	--	--

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

SP 情報：サイト A

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。そのためには、各ノードについて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			

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。

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。この情報で使用している例： 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：この情報で 使用している例： 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 この情報で使用して いる例： 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				
----------------	--	--	--	--

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
	簡潔なメッセージ

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）			

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、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。

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

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	<code>ucadmin modify -m fc -t initiator_adapter_name _`</code>

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.
```

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 (_ 例名 _) ...	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

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、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

「ディスク割り当て」

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_`

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_

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

コンポーネントの HA 状態の確認

工場出荷時に事前設定されていないストレッチ MetroCluster 構成では、コントローラおよびシャーシのコンポーネントの HA の状態が「mcc-2n」に設定されていることを確認し、適切にブートする必要があります。工場出荷状態のシステムでは事前に設定されているため、検証は不要です。

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。

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」

コントローラモジュールとシャーシには「mcc-2n」という値が表示されます。

2. 表示されたコントローラのシステム状態が「mcc-2n」でない場合は、コントローラの HA 状態を設定します。

「ha-config modify controller mcc-2n」という形式で指定します

3. 表示されたシャーシのシステム状態が「mcc-2n」でない場合は、シャーシの HA 状態を設定します。

「ha-config modify chassis mcc-2n」というようになりました

ノードを停止します。

ノードが LOADER プロンプトに戻るまで待ちます。

4. MetroCluster 構成の各ノードで、上記の手順を繰り返します。

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ノードをシングルノードクラスタに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 のセットアップに関するその他の一般的な情報については、を参照してください ["ONTAP をセットアップします"](#)

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、AutoSupport が自動的に有効になることを示すクラスタセットアップウィザードがコンソールで起動されます。

```
::> 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の "yes" をそのまま使用するか、または "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、第 1 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 またはノード SVM に対して入力した設定のいずれかを変更する必要がある場合は '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

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。

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。

関連情報

["クラスタと SVM のピアリングの簡単な設定"](#)

["専用のポートを使用する場合の考慮事項"](#)

["データポートを共有する場合の考慮事項"](#)

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。

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 'cluster0' 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」および「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_`
```

次の例では、ポート「e0e」および「e0f」を、システム SVM 「cluster01」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
                                     Failover
Vserver          Group          Targets
-----
Cluster
cluster01        Cluster
                                     cluster01-01:e0a, cluster01-01:e0b,
                                     cluster01-02:e0a, cluster01-02:e0b
cluster01        Default
                                     cluster01-01:e0c, cluster01-01:e0d,
                                     cluster01-02:e0c, cluster01-02:e0d,
                                     cluster01-01:e0e, cluster01-01:e0f
                                     cluster01-02:e0e, cluster01-02:e0f
cluster01        intercluster01
                                     cluster01-01:e0e, cluster01-01:e0f
                                     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 バージョン	コマンドを実行します
ONTAP 9.6 以降	「 network interface create -vserver system_svm -lif lif_name -policy default -intercluster -home-node node -home-port port -address port_ip -netmask netmask-failover-group failover_group 」という名前のポートを作成します
ONTAP 9.5 以前	network interface create -vserver system_svm -lif lif_name -role intercluster -home-node node -home-port port -address port_ip -netmask netmask-failover-group failover_group を作成します

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、フェイルオーバーグループ「intercluster0」内にクラスタ間 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 バージョン	コマンドを実行します
ONTAP 9.6 以降	「network interface show -service -policy default -intercluster」のように表示されます
ONTAP 9.5 以前	「network interface show -role intercluster」の略

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
      Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper  Address/Mask      Node      Port
Home
-----
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 バージョン	コマンドを実行します
ONTAP 9.6 以降	「network interface show -service -policy default -intercluster-failover」のように入力します

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、SVM ポート「e0e」上のクラスタ間 LIF 「cluster01_icl01」と「cluster01_icl02」がポート「e0f」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"

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 'cluster0' 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 バージョン	コマンドを実行します
ONTAP 9.6 以降	「 <code>network interface create -vserver system_svm _ -lif_lif_name_service -policy default -intercluster -home-node node -home-port port _ -address_port_ip-netmask netmask _</code> 」のようになります
ONTAP 9.5 以前	「 <code>network interface create -vserver system_svm _ -lif LIF_name -role intercluster -home-node _node _ -home-port _ -address_port_ip-netmask netmask _</code> 」のようになります

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、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 バージョン	コマンドを実行します
ONTAP 9.6 以降	「 network interface show -service -policy default -intercluster 」のように表示されます
ONTAP 9.5 以前	「 network interface show -role intercluster 」の略

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
      Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper  Address/Mask      Node      Port
Home
-----
-----
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 バージョン	コマンドを実行します
ONTAP 9.6 以降	「 network interface show - service-policy default-intercluster-failover 」と表示されます
ONTAP 9.5 以前	「 network interface show -role intercluster-failover 」の略

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「e0c」上のクラスタ間 LIF 「cluster01_icl01」と「cluster01_icl02」がポート「e0d」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

```

Vserver	Logical Interface	Home Node:Port	Failover Policy	Failover 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。

クラスタピア関係を作成

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...
168 時間 -peer-addr_peer_lif_ips_ -ip-space_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、-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、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_ -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 192.140.112.101 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. クラスタ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_ -ipospace_`
```

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、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_ -ipospace_`
```

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_name _raidtype raid4 」と表示されます



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

["論理ストレージ管理"](#)

["ONTAP の概念"](#)

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。

作業を開始する前に

- 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。

このタスクについて

- 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。

["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 サイト全体で一貫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 _ 」 というように入力します

2. アグリゲートを作成します。

「storage aggregate create -mirror true」のようになります

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



使用できるドライブ数が限られている最小サポート構成では、force-small-aggregate オプションを使用して、3 ディスクの RAID-DP アグリゲートを作成できるように設定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
- 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 RPM の異なるドライブでも使用できます

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。

例 1. このタスクについて

- 注意 * : 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。



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。

- 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。
- ["ディスクとアグリゲートの管理"](#) 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
- 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 RPM の異なるドライブでも使用できます

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

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。

アグリゲートのタイプを確認します。

「storage aggregate show



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 ["ONTAP で MCC ソフトウェアを設定"](#) 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-2n」である必要があります。

このタスクについて

MetroCluster 構成をイネーブルにするには、任意のノード上で、MetroCluster configure コマンドを1回実行し問題です。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。

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	いずれかのノードのプロンプトで、MetroCluster を設定します。 MetroCluster configure_node-name_` です

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 モードで続け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 (* >) 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。 +set -privilege admin</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で 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、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) 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

```
7 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

```

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 FC-to-SAS ブリッジを使用している場合は、MetroCluster 構成の FC-to-SAS ブリッジを監視するための特別な設定手順を実行する必要があります。

- 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
ONTAP 9.5 以降	「 storage bridge add -address 0.0.0.0 -managed-by in-band-name_bridge-name_」
ONTAP 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。ONTAP ヘルスマニタは、「Status」列の値が「ok」で、ワールドワイド名 (WWN) などのその他の情報が表示されていれば、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。

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、期待される出力が表示されません。

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. より詳細な結果を表示します。

「MetroCluster check run」のようになります

```
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	mirroring-status
ok		disk-pool-allocation
ok		ownership-state

```

ok
        controller_A_1_aggr1
                                mirroring-status
ok
                                disk-pool-allocation
ok
                                ownership-state
ok
        controller_A_1_aggr2
                                mirroring-status
ok
                                disk-pool-allocation
ok
                                ownership-state
ok

controller_A_2        controller_A_2_aggr0
                                mirroring-status
ok
                                disk-pool-allocation
ok
                                ownership-state
ok
        controller_A_2_aggr1
                                mirroring-status
ok
                                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。

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。

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。

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。

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 ["スイッチオーバー、修復、スイッチバックを実行"](#)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。

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は URL-of-destination」を変更します

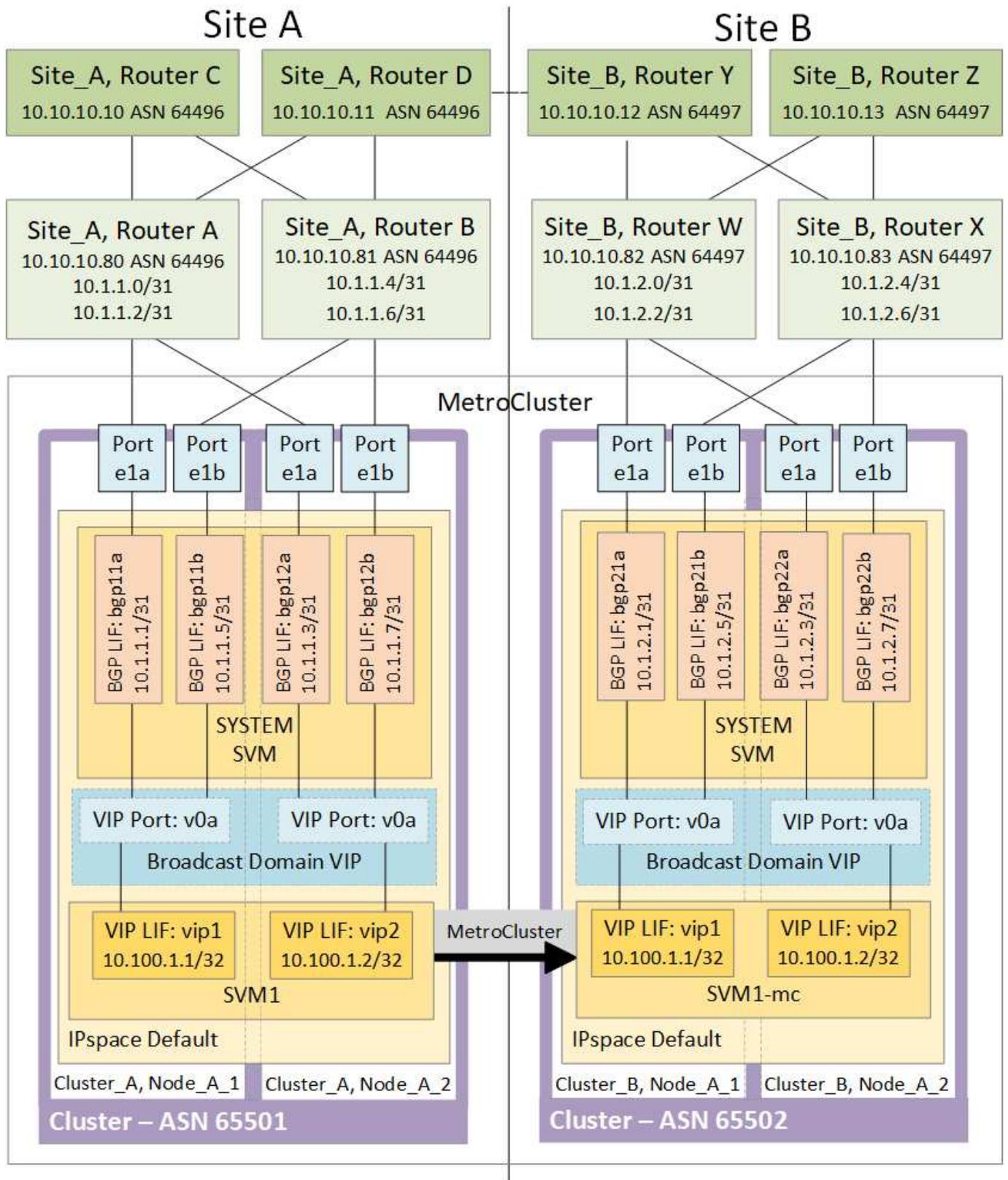
。 ["CLI を使用したクラスタ管理"](#) 追加情報が含まれています。

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、次の項を参照してください。

**** 仮想 IP（VIP）LIF の設定 ****



• ONTAP の制限 *

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 構成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。

v0a（v0b など）が存在することにより、接続が継続的に検証され、LIF の移行またはフェイルオーバーが成功するかどうか保証されます（停止後にはのみ構成の破損が表示される L2 とは異なります）。

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機能（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、コマンドの発行元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  DR
State          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ていることを確認します。

「 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。

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、停電が発生すると、サイトが停止してシェルフ全体が使用できなくな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. 「system environment sensors show -state fault」コマンドと「storage shelf show -errors」コマンドを使用して、コンソールで結果を監視します。

```

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。

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。

「ストレージ・アグリゲート」

「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。
- ストレッチMetroCluster構成のクラスタごとに、そのMetroClusterサイトのノードで使用する独自の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 を使用する場合はの考慮事項

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）でアクティブになります。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：

- MetroCluster（vs1 の cache_1）の一端が FlexCache site_A にある場合は、FlexCache の一端になっています
- 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

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 または管理者が作成した IP スペースです。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。

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、FabricPool の「MetroCluster 用のオブジェクトストアのセットアップ」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 ["ディスクとアグリゲートの管理"](#)。

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せん。

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

["ONTAP の概念"](#)

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
Name      Subnet          Broadcast      Gateway      Avail/      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
Name      Subnet          Broadcast      Gateway      Avail/      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。

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。

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	<p>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。</p> <p>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>	<p>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。</p> <p>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>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す。</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 repair-placement」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witchオーバー処理の際に確実に LIF を使用できるように、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。

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。

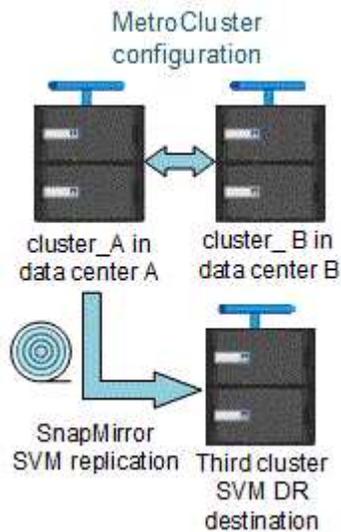
SVM を SnapMirror ディザスタリカバリで使用する場合は、次の要件と制限事項に注意してください。

- 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。

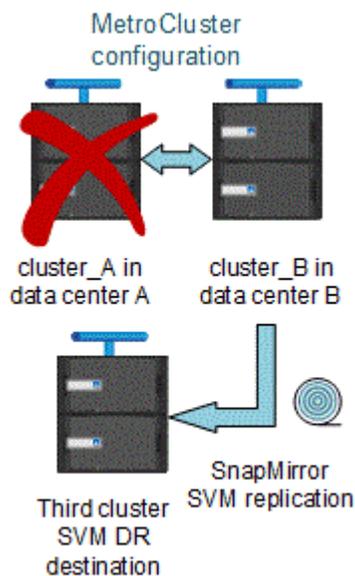
- MetroCluster 構成が安定した状態のときは MetroCluster の同期先の SVM はオンラインでないため、同期先ボリュームを SVM ディザスタリカバリ関係のソースにすることはできません。

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。

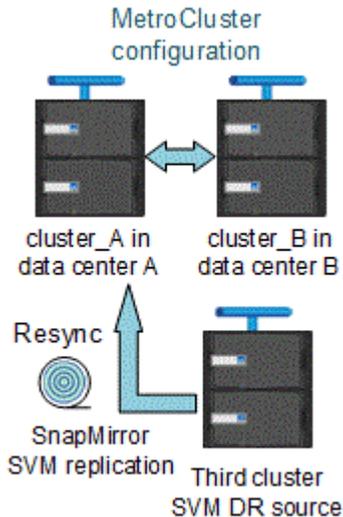
ただし、スイッチオーバーまたはスイッチバックプロセスの完了後、SVM DR の次回のスケジュールされている更新は成功します。

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witch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。

2 ノードストレッチ MetroCluster 構成での storage disk show コマンドおよび storage shelf show コマンドの出力

2 ノードストレッチ MetroCluster 構成では、「storage disk show」コマンドと「storage shelf show」コマンドの「is-local-attach」フィールドに、ディスクとストレージシェルフがどのノードに接続されているかに関係なく、すべてローカルとして表示されます。

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。



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。

手順

1. スイッチオーバー時に MetroCluster 構成が NVFAIL をトリガーできるようにするには、「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`
```

ストレッチからファブリック接続への **MetroCluster** 構成の移行

ファブリック接続 MetroCluster 構成では、ノードが異なる場所に配置されます。この地理的な違いにより、災害からの保護が強化されます。ストレッチからファブリック接続 MetroCluster 構成に移行するには、FC スイッチを追加し、必要に応じて FC-to-SAS ブリッジを追加する必要があります。

- MetroCluster modify -auto-switchover failure-domain auto-disabled コマンドを実行して、両方のクラスターで自動スイッチオーバーを無効にする必要があります。
- ノードをシャットダウンしておく必要があります。

この手順はシステムの停止を伴います。

MetroCluster 構成の移行は両方のサイトで実行する必要があります。MetroCluster 設定をアップグレードしたあと、両方のクラスターで自動スイッチオーバーを有効にする必要があります。また 'MetroCluster check run' コマンドを実行して '構成を検証する必要があります'

この手順では、必要な手順の概要を示します。詳細な手順については、の特定のセクションを参照する必要があります ["ファブリック接続 MetroCluster のインストールと設定"](#)。インストールと設定のすべてを実行する必要はありません。

手順

1. の「MetroCluster のインストールの準備」セクションをよく確認して、アップグレードの準備をします "[ファブリック接続 MetroCluster のインストールと設定](#)"。
2. 必要なスイッチと FC-to-SAS ブリッジの設置、ケーブル接続、設定を行います。



の「ファブリック接続 MetroCluster 構成のケーブル接続」セクションの手順を使用する必要があります "[ファブリック接続 MetroCluster のインストールと設定](#)"。

3. 次の手順に従って、MetroCluster 構成を更新します。

『Configuring the MetroCluster software in ONTAP』の手順は使用しないでください。 "[ファブリック接続 MetroCluster のインストールと設定](#)"。

- a. advanced 権限モードに切り替えます。 `++set -privilege advanced *`
- b. MetroCluster 構成を更新します `:+* MetroCluster configure -refresh true *`

次のコマンドを実行すると、controller_A_1 を含む DR グループのすべてのノードの MetroCluster 構成が更新されます。

```
controller_A_1::*> metrocluster configure -refresh true
[Job 009] Job succeeded: Configure is successful.
```

- a. admin 特権モードに戻ります `:+set -privilege admin`

4. MetroCluster 構成にエラーがないかどうかを確認し、動作していることを確認します。

の次のセクションの手順を使用する必要があります "[ファブリック接続 MetroCluster のインストールと設定](#)" :

- Config Advisor での MetroCluster 構成エラーの確認
- ローカル HA の処理を検証しています
- 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

追加情報の参照先

MetroCluster の設定と処理の詳細を確認できます。

MetroCluster およびその他の情報

情報	件名
"ONTAP 9 のドキュメント"	<ul style="list-style-type: none"> • MetroCluster のすべてのガイド
	<ul style="list-style-type: none"> • MetroCluster FC の構成と運用の技術概要 • MetroCluster FC 構成のベストプラクティス

<p>"ファブリック接続 MetroCluster のインストールと設定"</p>	<ul style="list-style-type: none"> • ファブリック接続 MetroCluster アーキテクチャ • 構成のケーブル接続 • FC-to-SAS ブリッジの設定 • FC スイッチを設定します • ONTAP で MetroCluster を設定します
<p>"MetroCluster IP のインストールと設定： ONTAP MetroCluster 構成の違い"</p>	<ul style="list-style-type: none"> • MetroCluster IP アーキテクチャ • 構成のケーブル接続 • ONTAP で MetroCluster を設定します
<p>"MetroCluster の管理とディザスタリカバリ"</p>	<ul style="list-style-type: none"> • MetroCluster 構成について • スイッチオーバー、修復、スイッチバック • ディザスタリカバリ（DR）
<p>"MetroCluster コンポーネントの保守"</p>	<ul style="list-style-type: none"> • MetroCluster FC 構成のメンテナンスガイドライン • ハードウェアの交換またはアップグレードFC-to-SAS ブリッジおよび FC スイッチのファームウェアアップグレード手順 • 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 • 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 • ファブリック接続またはストレッチ MetroCluster FC 構成のディザスタリカバリサイトでのハードウェア交換 • 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 • 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
<p>"MetroCluster FC から MetroCluster IP に移行します" "MetroCluster アップグレードおよび拡張ガイド"</p>	<ul style="list-style-type: none"> • MetroCluster 設定をアップグレードまたは更新する • MetroCluster FC 構成から MetroCluster IP 構成への移行 • ノードの追加による MetroCluster 構成の拡張
<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"> • MetroCluster Tiebreaker ソフトウェアを使用して MetroCluster 構成を監視する

Active IQ Unified Manager のドキュメント "ネットアップのマニュアル：製品ガイドとリソース"	<ul style="list-style-type: none">• MetroCluster の設定とパフォーマンスを監視する
"コピーベースの移行"	<ul style="list-style-type: none">• 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
"ONTAP の概念"	<ul style="list-style-type: none">• ミラーされたアグリゲートの機能

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。