



# MetroCluster IP 構成をインストール

## ONTAP MetroCluster

NetApp  
February 27, 2026

# 目次

MetroCluster IP 構成をインストール	1
MetroCluster IP インストールワークフロー	1
MetroCluster のインストールを準備	1
ONTAP MetroCluster構成のサポートマトリックス	1
ONTAP メディエーターと MetroCluster Tiebreaker の違い	3
リモートストレージとMetroCluster IP 構成について学習します	3
自動ドライブ割り当てとADPシステムのMetroCluster IP要件	6
MetroCluster IP構成におけるクラスタピアリングの要件	23
ISL の要件	25
MetroCluster 準拠スイッチの使用に関する考慮事項	41
MetroCluster IP構成におけるミラーリングされていないアグリゲートについて学習します	49
MetroCluster IP構成のファイアウォール ポート要件	51
MetroCluster IP構成で仮想 IPとボーダーゲートウェイプロトコルを使用する方法について学習します。	51
MetroCluster ハードウェアコンポーネントを設定します	54
MetroCluster IP構成におけるハードウェアコンポーネントの相互接続について学習します。	54
必要なMetroCluster IP 構成コンポーネントと命名規則	58
MetroCluster IP構成ハードウェアコンポーネントをラックに収納する	62
MetroCluster IP スイッチをケーブル接続します	63
MetroCluster IP構成でONTAPコントローラモジュールポートをケーブル接続する	113
MetroCluster IP スイッチを設定します	114
MetroCluster IPスイッチの健全性を監視する	171
ONTAP で MetroCluster ソフトウェアを設定します	199
CLIを使用したMetroClusterソフトウェアの設定	199
System Managerを使用したMetroClusterソフトウェアの設定	267
計画外の自動スイッチオーバー用に ONTAP Mediator を構成する	271
MetroCluster IP構成のONTAP Mediatorインストール要件	271
MetroCluster IP構成用のONTAPメディエーターを設定する	273
MetroCluster IP構成からONTAPメディエーターを削除する	278
MetroCluster IP構成を別のONTAPメディエーターインスタンスに接続する	279
ONTAPメディエーターがMetroCluster IP構成で計画外の自動スイッチオーバーをサポートする仕組み	279
MetroCluster IP構成でデフォルトのONTAPメディエーターメールボックスのタイムアウトを増やす	281
MetroCluster IP構成でSystem Managerを使用してONTAP Mediatorを管理する	282
MetroCluster IP構成のONTAP ノードスイッチオーバーをテストします	283
ネゴシエートスイッチオーバーを検証中	283
修復と手動スイッチバックの検証	285
電源回線切断後の動作確認	288
単一のストレージシェルフが停止したあとの動作確認	290

MetroCluster 構成を削除 .....	300
MetroCluster IP構成でのONTAP操作の要件と考慮事項 .....	301
ライセンスに関する考慮事項 .....	301
SnapMirror に関する考慮事項 .....	301
ONTAP System Manager での MetroCluster 処理 .....	301
MetroCluster 構成での FlexCache のサポート .....	301
MetroCluster 構成での FabricPool のサポート .....	302
MetroCluster 構成での FlexGroup のサポート .....	303
MetroCluster 構成のジョブスケジュール .....	303
MetroCluster サイトから第 3 のクラスタへのクラスタピアリング .....	303
MetroCluster 構成での LDAP クライアント設定のレプリケーション .....	303
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 .....	304
MetroCluster 構成の SVM ディザスタリカバリ .....	308
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 .....	311
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 .....	311
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 .....	312
MetroCluster IP構成でさらに詳細な構成と監視を行うには、Active IQ Unified ManagerとONTAP System Managerを使用します。 .....	312
MetroCluster IP構成でNTPを使用してシステム時刻を同期する .....	312
MetroCluster IP に関する追加情報の入手先 .....	313
MetroCluster およびその他の情報 .....	314

# MetroCluster IP 構成をインストール

## MetroCluster IP インストールワークフロー

MetroCluster IP 設定をインストールするには、いくつかの手順を正しい順序で実行する必要があります。

- "インストールを準備し、すべての要件を理解します"。
- "コンポーネントをケーブル接続します"
- "ソフトウェアを設定します"
- "ONTAP メディエーターを設定します" (オプション)
- "設定をテストします"

## MetroCluster のインストールを準備

### ONTAP MetroCluster構成のサポートマトリックス

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

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

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

直接接続型 SAS ストレージを使用します	○（ローカル接続のみ）	いいえ	いいえ	いいえ	はい。
ADP をサポートします	○（ONTAP 9.4 以降）	いいえ	いいえ	いいえ	いいえ
ローカル HA をサポートします	はい。	はい。	いいえ	いいえ	いいえ
ONTAP 自動計画外スイッチオーバー（AUSO）のサポート	いいえ	はい。	はい。	はい。	はい。
ミラーされていないアグリゲートを	○（ONTAP 9.8 以降）	はい。	はい。	はい。	はい。
ONTAP メディエーターをサポートします	○（ONTAP 9.7 以降）	いいえ	いいえ	いいえ	いいえ
MetroCluster Tiebreaker をサポートします	○（ONTAP メディエーターとの併用は不可）	はい。	はい。	はい。	はい。
をサポートします <a href="#">すべての SAN アレイ</a>	はい。	はい。	はい。	はい。	はい。

• メモ \*

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

- ONTAP 9.9..1 以降では、8 ノード構成がサポートされます。
- ネットアップ検証済みの MetroCluster スイッチ（ネットアップから購入したもの）のみがサポートされます。
- IP ルーティング（レイヤ 3）バックエンド接続を使用する設定はサポートされていません。

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

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

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

## ONTAP メディエーターと MetroCluster Tiebreaker の違い

ONTAP 9.7 以降では、MetroCluster IP 構成で ONTAP Mediator-Assisted Automatic Unplanned Switchover (MAUSO ; メディエーターアシスト自動計画外スイッチオーバー) を使用するか、MetroCluster Tiebreaker ソフトウェアを使用できます。MAUSO または Tiebreaker ソフトウェアを使用する必要はありませんが、これらのサービスのどちらとも使用しない場合は、["手動リカバリの実行"](#) 災害が発生した場合。

MetroCluster 構成に応じて、異なる状況で自動スイッチオーバーが実行されます。

- \* AUSO 機能を使用した MetroCluster FC 構成 ( MetroCluster IP 構成には含まれません) \*

これらの構成では、コントローラの障害が発生した場合にストレージ (および存在する場合はブリッジ) が動作していれば AUSO が開始されます。

- **ONTAP Mediator** を使用した **MetroCluster IP 構成 (ONTAP 9.7 以降)**

これらの構成では、前述の AUSO と同じ状況に加え、サイト全体 (コントローラ、ストレージ、スイッチ) の障害が発生した場合に MAUSO が開始されます。

["ONTAP メディエーターでの自動計画外スイッチオーバーのサポート"](#)。

- \* アクティブモードで Tiebreaker ソフトウェアを使用した MetroCluster IP または FC 構成 \*

これらの構成では、サイト全体の障害が発生した場合に Tiebreaker で計画外スイッチオーバーが開始されます。

Tiebreaker ソフトウェアを使用する前に、を参照してください ["MetroCluster Tiebreaker ソフトウェアのインストールおよび設定"](#)

## ONTAP メディエーターと他のアプリケーションおよびアプライアンスとの相互運用性

スイッチオーバーをトリガーできるサードパーティのアプリケーションやアプライアンスを ONTAP メディエーターと組み合わせて使用することはできません。また、ONTAP メディエーターを使用した場合、MetroCluster Tiebreaker ソフトウェアでの MetroCluster 構成の監視はサポートされません。

## リモート ストレージと MetroCluster IP 構成について学習します

コントローラがリモートストレージにアクセスする方法と MetroCluster IP アドレスの仕組みを理解しておく必要があります。

### MetroCluster IP 構成のリモートストレージへのアクセス

MetroCluster IP 構成では、ローカルコントローラからリモートストレージプールにアクセスするには、リモートコントローラを使用する必要があります。IP スイッチはコントローラのイーサネットポートに接続され、ディスクシェルフに直接は接続されません。リモートコントローラが停止した場合、ローカルコントローラはリモートストレージプールにアクセスできません。

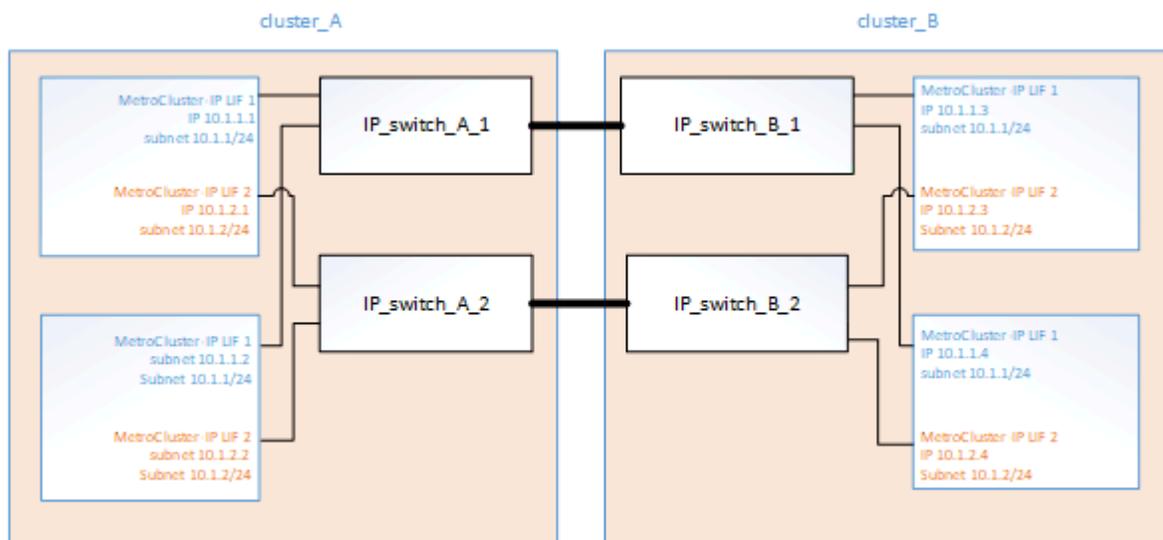
これは、MetroCluster FC 構成とは異なります。FC ファブリックまたは SAS 接続を介してリモートストレージプールがローカルコントローラに接続されます。ローカルコントローラはリモートコントローラが停止し

でもリモートストレージにアクセスできます。

## MetroCluster の IP アドレス

MetroCluster IP 構成での MetroCluster IP アドレスとインターフェイスの実装方法、および関連する要件について理解しておく必要があります。

MetroCluster IP 構成では、HA ペア間および DR パートナー間でのストレージと不揮発性キャッシュのレプリケーションが、MetroCluster IP ファブリック内の広帯域の専用リンクを使用して行われます。ストレージのレプリケーションには iSCSI 接続が使用されます。IP スイッチは、ローカルクラスタ内のすべてのクラスタ内トラフィックにも使用されます。MetroCluster トラフィックは、別の IP サブネットと VLAN を使用することでクラスタ内トラフィックから分離されます。MetroCluster IP ファブリックは、クラスタピアリングネットワークとは別のものです。



MetroCluster IP 構成では、バックエンド MetroCluster IP ファブリック用に予約された IP アドレスが各ノードに 2 つ必要です。予約された IP アドレスは、初期設定時に MetroCluster IP の論理インターフェイス（LIF）に割り当てられます。この IP アドレスの要件は次のとおりです。



MetroCluster の IP アドレスは初期設定後は変更できないため、慎重に選択する必要があります。

- 一意の IP 範囲に属している必要があります。

環境内のどの IP スペースとも重複しないようにしてください。

- 2 つの IP サブネットのいずれかに属し、他のすべてのトラフィックから分離されている必要があります。

たとえば、次のようにノードの IP アドレスを設定できます。

ノード	インターフェイス	IP アドレス	サブネット
node_A_1	MetroCluster IP インターフェイス 1	10.1.1.1	10.1.1/24

node_A_1	MetroCluster IP インターフェイス 2	10.1.2.1	10.1.2/24
Node_a_2	MetroCluster IP インターフェイス 1	10.1.1.2	10.1.1/24
Node_a_2	MetroCluster IP インターフェイス 2	10.1.2.2	10.1.2/24
node_B_1	MetroCluster IP インターフェイス 1	10.1.1.3 の場合	10.1.1/24
node_B_1	MetroCluster IP インターフェイス 2	10.1.2.3	10.1.2/24
node_B_2	MetroCluster IP インターフェイス 1	10.1.1.4	10.1.1/24
node_B_2	MetroCluster IP インターフェイス 2	10.1.2.4	10.1.2/24

### MetroCluster IP インターフェイスの特性

MetroCluster IP インターフェイスは、MetroCluster IP 構成に固有のインターフェイスです。他の ONTAP インターフェイスタイプとは異なる特性があります。

- これらは '初期 MetroCluster 構成の一部として MetroCluster configuration-settings interface create コマンドによって作成されます



ONTAP 9.9..1 以降では、レイヤ 3 設定を使用している場合、MetroCluster IP インターフェイスを作成するときに `-gateway` パラメータも指定する必要があります。を参照してください "[レイヤ 3 ワイドエリアネットワークに関する考慮事項](#)"。

ネットワークインターフェイスのコマンドで作成または変更することはできません。

- これらは 'network interface show コマンドの出力には表示されません
- フェイルオーバーせず、作成時と同じポートに関連付けられたままになります。
- MetroCluster IP 構成では、MetroCluster IP インターフェイスに特定のイーサネットポート（プラットフォームによって異なる）を使用します。



MetroCluster IP インターフェイスを作成するときは、同じ範囲のシステム自動生成インターフェイス IP アドレスとの競合を避けるため、169.254.17.x または 169.254.18.x の IP アドレスを使用しないでください。

## 自動ドライブ割り当てとADPシステムのMetroCluster IP要件

ONTAP 9.4以降のMetroCluster IP構成では、自動ディスク割り当てとアドバンスドドライブパーティショニングを使用した新規インストールがサポートされます。

MetroCluster IP 構成で ADP を使用する場合は、次の点に注意する必要があります。

- AFFおよびASAシステムでMetroCluster IP構成でADPを使用するには、ONTAP 9.4以降が必要です。
- ADPv2は、MetroCluster IP設定でサポートされます。
- ルートアグリゲートは、両方のサイトのすべてのノードのパーティション3に配置する必要があります。
- パーティショニングとディスク割り当ては、MetroClusterサイトの初期設定時に自動的に実行されます。
- プール0のディスクは出荷時点で割り当て済みです。
- ミラーされていないルートが工場出荷時に作成されています。
- データパーティションは、手順のセットアップ時にお客様のサイトで割り当てます。
- ほとんどの場合、ドライブの割り当てとパーティショニングはセットアップ時に自動的に実行されます。
- ディスクとそのすべてのパーティションは、同じハイアベイラビリティ (HA) ペアのノードが所有している必要があります。ローカルHAペアとディザスタリカバリ (DR) パートナーまたはDR補助パートナーと、1つのドライブ内でパーティションまたはドライブの所有権を混在させることはできません。

サポートされる構成の例：

ドライブ/パーティション	オーナー
ドライブ：	ClusterA-Node01
パーティション1：	ClusterA-Node01
パーティション2：	ClusterA-Node02
パーティション3：	ClusterA-Node01



ONTAP 9.4 から 9.5 へのアップグレードでは、既存のディスク割り当てが認識されます。

### 自動パーティショニング

ADPは、システムの初期設定時に自動的に実行されます。



ONTAP 9.5以降では、でディスクの自動割り当てを有効にする必要があります `storage disk option modify -autoassign on` コマンドを実行します

ha-config状態をに設定する必要があります `mccip` 自動プロビジョニングの前に、ルートボリュームのサイズが適切になるように正しいパーティションサイズが選択されていることを確認します。詳細については、を参照してください ["コンポーネントの ha-config 状態の確認"](#)。

インストール中に最大 96 本のドライブを自動的にパーティショニングできます。初期インストール後にドライブを追加することができます。

内蔵ドライブと外付けドライブを使用する場合は、最初にADPを使用する内蔵ドライブのみでMetroClusterを初期化します。その後、設置またはセットアップ作業が完了したら、外付けシェルフを手動で接続します。



の説明に従って、内蔵シェルフに推奨される最小数のドライブが搭載されていることを確認する必要があります。 [ADPとディスク割り当てのシステム別の違い](#)。

内蔵ドライブと外付けドライブの両方について、「」の説明に従って、部分的にフルになったシェルフを取り付ける必要があります。 [部分的にフルになったシェルフの設置方法](#)。

### シェルフ単位の自動割り当ての仕組み

各サイトに4台の外付けシェルフがある場合、次の例に示すように、各シェルフが異なるノードの異なるプールに割り当てられます。

- site\_A-shelf\_1 のすべてのディスクが node\_A\_1 のプール0に自動的に割り当てられます
- site\_A-shelf\_3 のすべてのディスクが node\_A\_1 のプール0に自動的に割り当てられます
- site\_B-shelf\_1 のすべてのディスクが node\_B\_1 のプール0に自動的に割り当てられます
- site\_B-shelf\_3 のすべてのディスクが node\_B\_2 のプール0に自動的に割り当てられます
- site\_B-shelf\_2 のすべてのディスクが node\_A\_1 のプール1に自動的に割り当てられます
- site\_B-shelf\_2 のすべてのディスクが node\_B\_2 のプール1に自動的に割り当てられます
- site\_A-shelf\_2 のすべてのディスクが node\_B\_1 のプール1に自動的に割り当てられます
- site\_A-shelf\_2 のすべてのディスクが node\_B\_2 のプール1に自動的に割り当てられます

### 部分的にフルになったシェルフの設置方法

シェルフに十分な空きドライブベイがない場合は、ディスク割り当てポリシーに応じて、シェルフ全体にドライブを均等に分散する必要があります。ディスク割り当てポリシーは、各 MetroCluster サイトにシェルフがいくつあるかによって異なります。

各サイトでシェルフが1台（またはAFF A800システムの内蔵シェルフのみ）を使用している場合は、クォータシェルフポリシーを使用してディスクが割り当てられます。シェルフに空きがない場合は、すべてのクォータにドライブを均等に付けます。

次の表は、24本のディスクを48本のドライブ内蔵シェルフに配置する方法の例を示しています。ドライブの所有権も表示されます。

48個のドライブベイが4つのクォータに分割されています。	各クォータの最初の6つのベイに6本のドライブを取り付け ...
第1クォータ：ベイ 0~11	ベイ 0~5
第2クォータ：ベイ 12~23	ベイ 12~17
第3四半期：ベイ 24-35	ベイ 24-29

第4クォータ：ベイ36~47	ベイ 36-41
----------------	----------

次の表に、24ドライブ内蔵シェルフに16本のディスクを配置する方法の例を示します。

24個のドライブベイは4つのクォータに分けられます。	四半期ごとに最初の4つのベイに4本のドライブを設置...
第1クォータ：ベイ0~5	ベイ0~3
第2クォータ：ベイ6-11	ベイ6-9
第3クォータ：ベイ12~17	ベイ12~15
第4四半期：ベイ18~23	ベイ18~21

各サイトで外付けシェルフを2台使用している場合は、ハーフシェルフポリシーを使用してディスクが割り当てられます。シェルフにフル装備されていない場合は、シェルフの両端からドライブを均等に取り付けます。

たとえば、24ドライブシェルフに12本のドライブを取り付ける場合は、ベイ0~5および18~23にドライブを取り付けます。

#### ドライブの手動割り当て（ONTAP 9.5）

ONTAP 9.5では、次のシェルフ構成のシステムについては手動でドライブを割り当てる必要があります。

- 各サイトに外付けシェルフが3台ある構成。  
2台のシェルフはハーフシェルフの割り当てポリシーに従って自動的に割り当てられますが、3台目のシェルフは手動で割り当てる必要があります。
- 各サイトにシェルフが5台以上あり、外付けシェルフの総数が4の倍数でない構成。  
4の倍数を超えた分のシェルフは未割り当てとなり、ドライブを手動で割り当てる必要があります。たとえば、サイトに5台の外付けシェルフがある場合は、シェルフ5を手動で割り当てる必要があります。

未割り当てのシェルフのドライブは1本だけ手動で割り当てます。シェルフの残りのドライブは自動的に割り当てられます。

#### ドライブの手動割り当て（ONTAP 9.4）

ONTAP 9.4では、次のシェルフ構成のシステムに対して手動でドライブを割り当てる必要があります。

- 各サイトに外付けシェルフが3台以下の構成。  
ドライブを手動で割り当てる必要があります。各プールのドライブ数が同じになるようにドライブを対称的に割り当てます。
- 各サイトに外付けシェルフが5台以上あり、外付けシェルフの総数が4の倍数でない構成。

4 の倍数を超えた分のシェルフは未割り当てとなり、ドライブを手動で割り当てする必要があります。

ドライブを手動で割り当てるときは、各プールのドライブ数が同じになるようにディスクを対称的に割り当てる必要があります。たとえば、各サイトにストレージシェルフが 2 台ある構成では、1 台のシェルフをローカル HA ペアに使用し、もう 1 台のシェルフをリモート HA ペアに使用します。

- site\_A-shelf\_1 の半分のディスクを node\_A\_1 のプール 0 に割り当てます。
- site\_A-shelf\_1 の半分のディスクを node\_A\_1 のプール 0 に割り当てます。
- site\_A-shelf\_2 の半分のディスクを node\_B\_1 のプール 1 に割り当てます。
- site\_A-shelf\_2 の半分のディスクを node\_B\_2 のプール 1 に割り当てます。
- site\_B-shelf\_1 の半分のディスクを node\_B\_1 のプール 0 に割り当てます。
- site\_B-shelf\_1 の半分のディスクを node\_B\_2 のプール 0 に割り当てます。
- site\_B-shelf\_2 の半分のディスクを node\_A\_1 のプール 1 に割り当てます。
- site\_B-shelf\_2 の半分のディスクを node\_B\_2 のプール 1 に割り当てます。

#### 既存構成へのシェルフの追加

自動ドライブ割り当てでは、既存の構成にシェルフを対称的に追加できます。

新しいシェルフが追加されると、追加されたシェルフに同じ割り当てポリシーが適用されます。たとえば、各サイトにシェルフが 1 台ある構成でシェルフを追加した場合、新しいシェルフにはクォータシェルフの割り当てルールが適用されます。

#### 関連情報

["必要な MetroCluster IP コンポーネントと命名規則"](#)

["ディスクおよびアグリゲートの管理"](#)

#### MetroCluster IP 構成での ADP とディスク割り当てのシステム別の違い

MetroCluster IP 構成でのアドバンスドドライブパーティショニング（ADP）と自動ディスク割り当ての動作は、システムモデルによって異なります。



ADP を使用するシステムではパーティションを使用してアグリゲートが作成され、各ドライブがパーティション P1、P2、P3 に分割されます。ルートアグリゲートは P3 パーティションを使用して作成されます。

テーブルを使用する前に、次の要件を確認してください。

- MetroClusterでサポートされる最大ドライブ数やその他のガイドラインに従う必要があります。参照 ["NetApp Hardware Universe の略"](#)。
- 外部ディスク シェルフを再利用する場合は、コントローラに接続する前に、外部ディスク シェルフのディスク所有権が削除されていることを確認してください。参照 ["ディスクからONTAPの所有権を削除する"](#)。

**AFF A320** システムでの **ADP** とディスクの割り当て

ガイドライン	サイトあたりのドライブ数	ドライブ割り当てルール	ルートパーティションの ADP レイアウト
推奨される最小ドライブ数（サイトあたり）	48 ドライブ	各外付けシェルフのドライブが 2 つのグループに均等に分割されます（ハーフ）。シェルフの各ハーフが自動的に別々のプールに割り当てられます。	<p>1 台のシェルフはローカル HA ペアによって使用されます。2 番目のシェルフはリモート HA ペアによって使用されます。</p> <p>各シェルフのパーティションを使用してルートアグリゲートが作成されます。ルートアグリゲートの 2 つのプレックスには、それぞれ次のパーティションが含まれます。</p> <ul style="list-style-type: none"> <li>• データ用パーティション × 8</li> <li>• パリティパーティション × 2</li> <li>• スペアパーティションが 2 つ必要です</li> </ul>
サポートされる最小ドライブ数（サイトあたり）	24 本のドライブ	ドライブは 4 つのグループに均等に分割されます。各クォータシェルフは、自動的に別々のプールに割り当てられます。	<p>ルートアグリゲートの 2 つのプレックスのそれぞれに、次のパーティションが含まれます。</p> <ul style="list-style-type: none"> <li>• データ用パーティション × 3</li> <li>• パリティパーティション × 2</li> <li>• スペアパーティション × 1</li> </ul>

**AFF A150**、**ASA A150**、および **AFF A220** システムでの **ADP** とディスク割り当て

ガイドライン	サイトあたりのドライブ数	ドライブ割り当てルール	ルートパーティションの ADP レイアウト

<p>推奨される最小ドライブ数（サイトあたり）</p>	<p>内蔵ドライブのみ</p>	<p>内蔵ドライブは4つのグループに均等に分割されます各グループは自動的に別々のプールに割り当てられ、各プールは構成内の別々のコントローラに割り当てられます。</p> <p>*注：*内蔵ドライブの半分は、MetroClusterを構成する前に未割り当てのままになります。</p>	<p>2つのクォータはローカル HA ペアに使用されます。残り2つのクォータはリモート HA ペアに使用されます。</p> <p>ルートアグリゲートの各プレックスには、次のパーティションが含まれます。</p> <ul style="list-style-type: none"> <li>• データ用パーティション × 3</li> <li>• パリティパーティション × 2</li> <li>• スペアパーティション × 1</li> </ul>
-----------------------------	-----------------	---	---

<p>サポートされる最小ドライブ数（サイトあたり）</p>	<p>16 本の内蔵ドライブ</p>	<p>ドライブは 4 つのグループに均等に分割されます。各クォータシェルフは、自動的に別々のプールに割り当てられます。</p> <p>シェルフ上の 2 つのクォータに同じプールを割り当てることができます。プールは、そのクォータを所有するノードに基づいて選択されます。</p> <ul style="list-style-type: none"> <li>ローカルノードが所有している場合は、プール 0 が使用されます。</li> <li>リモートノードが所有している場合は、プール 1 が使用されます。</li> </ul> <p>たとえば、Q1~Q4 に 4 分割されたシェルフでは次のような割り当てが可能です。</p> <ul style="list-style-type: none"> <li>Q1 : node_A_1 のプール 0</li> <li>Q2 : node_A_1 のプール 0</li> <li>Q3 : node_B_1 のプール 1</li> <li>Q4 : node_B_2 のプール 1</li> </ul> <p>*注：*内蔵ドライブの半分は、MetroClusterを構成する前に未割り当てのままになります。</p>	<p>ルートアグリゲートの 2 つのブレッक्सのそれぞれに、次のパーティションが含まれます。</p> <ul style="list-style-type: none"> <li>データ用パーティション×2</li> <li>パリティパーティション×2</li> <li>スペアなし</li> </ul>
-------------------------------	--------------------	--	---

**AFF A250、AFF C250、ASA A250、ASA C250、FAS500f、AFF A20、AFF A30、およびAFF C30システムでのADPとディスク割り当て**

ガイドライン	サイトあたりのドライブ数	ドライブ割り当てルール	ルートパーティションのADP レイアウト
--------	--------------	-------------	----------------------

推奨される最小ドライブ数（サイトあたり）	48ドライブ（外付けドライブのみ、内蔵ドライブなし）	各外付けシェルフのドライブが2つのグループに均等に分割されます（ハーフ）。シェルフの各ハーフが自動的に別々のプールに割り当てられます。	1台のシェルフはローカルHAペアによって使用されます。2番目のシェルフはリモートHAペアによって使用されます。  各シェルフのパーティションは、ルートアグリゲートの作成に使用されます。ルートアグリゲートの各ブックスには、次のパーティションが含まれます。  <ul style="list-style-type: none"> <li>• データ用パーティション × 8</li> <li>• パリティパーティション × 2</li> <li>• スペアパーティションが2つ必要です</li> </ul>
	48ドライブ（外付けドライブと内蔵ドライブ）	内部パーティションは4つのグループ（クォータ）に均等に分割されます。各クォータが自動的に別々のプールに割り当てられます。外付けシェルフのドライブが4つのグループ（クォータ）に均等に分割されます。各クォータシェルフは自動的に別々のプールに割り当てられます。	ルートアグリゲートの2つのブックスのそれぞれに、次のものが含まれます。  <ul style="list-style-type: none"> <li>• データ用パーティション × 8</li> <li>• パリティパーティション × 2</li> <li>• スペアパーティションが2つ必要です</li> </ul>
サポートされる最小ドライブ数（サイトあたり）	16本の内蔵ドライブ	ドライブは4つのグループに均等に分割されます。各クォータシェルフは、自動的に別々のプールに割り当てられます。	ルートアグリゲートの2つのブックスのそれぞれに、次のパーティションが含まれます。  <ul style="list-style-type: none"> <li>• データ用パーティション × 2</li> <li>• パリティパーティション × 2</li> <li>• スペアパーティションがありません</li> </ul>

ガイドライン	サイトあたりのドライブ数	ドライブ割り当てルール	ルートパーティションのADP レイアウト
推奨される最小ドライブ数（サイトあたり）	48ドライブ（外付けドライブのみ、内蔵ドライブなし）	各外付けシェルフのドライブが2つのグループに均等に分割されます（ハーフ）。シェルフの各ハーフが自動的に別々のプールに割り当てられます。	<p>ローカルHAペアは1台のシェルフを使用します。リモートHAペアは2番目のシェルフを使用します。</p> <p>各シェルフのパーティションは、ルートアグリゲートの作成に使用されます。ルートアグリゲートの各プレックスには、次のパーティションが含まれます。</p> <ul style="list-style-type: none"> <li>• データ用パーティション × 8</li> <li>• パリティパーティション × 2</li> <li>• スペアパーティションが2つ必要です</li> </ul>
	48ドライブ（外付けドライブと内蔵ドライブ）	内部パーティションは4つのグループ（クォータ）に均等に分割されます。各クォータが自動的に別々のプールに割り当てられます。外付けシェルフのドライブが4つのグループ（クォータ）に均等に分割されます。各クォータシェルフは自動的に別々のプールに割り当てられます。	<p>ルートアグリゲートの2つのプレックスのそれぞれに、次のものが含まれます。</p> <ul style="list-style-type: none"> <li>• データ用パーティション × 8</li> <li>• パリティパーティション × 2</li> <li>• スペアパーティションが2つ必要です</li> </ul>
サポートされる最小ドライブ数（サイトあたり）	内蔵ドライブ24本	ドライブは4つのグループに均等に分割されます。各クォータシェルフは、自動的に別々のプールに割り当てられます。	<p>ルートアグリゲートの2つのプレックスのそれぞれに、次のパーティションが含まれます。</p> <ul style="list-style-type: none"> <li>• データ用パーティション × 2</li> <li>• パリティパーティション × 2</li> <li>• スペアパーティションがありません</li> </ul>

**AFF A300** システムでの **ADP** とディスク割り当て

ガイドライン	サイトあたりのドライブ数	ドライブ割り当てルール	ルートパーティションの ADP レイアウト
推奨される最小ドライブ数（サイトあたり）	48 ドライブ	各外付けシェルフのドライブが 2 つのグループに均等に分割されます（ハーフ）。シェルフの各ハーフが自動的に別々のプールに割り当てられます。	<p>1 台のシェルフはローカル HA ペアによって使用されます。2 番目のシェルフはリモート HA ペアによって使用されます。</p> <p>各シェルフのパーティションは、ルートアグリゲートの作成に使用されます。ルートアグリゲートの各プレックスには、次のパーティションが含まれます。</p> <ul style="list-style-type: none"> <li>データ用パーティション × 8</li> <li>パリティパーティション × 2</li> <li>スペアパーティションが 2 つ必要です</li> </ul>
サポートされる最小ドライブ数（サイトあたり）	24 本のドライブ	ドライブは 4 つのグループに均等に分割されます。各クォータシェルフは、自動的に別々のプールに割り当てられます。	<p>ルートアグリゲートの 2 つのプレックスのそれぞれに、次のパーティションが含まれます。</p> <ul style="list-style-type: none"> <li>データ用パーティション × 3</li> <li>パリティパーティション × 2</li> <li>スペアパーティション × 1</li> </ul>

**AFF C400、AFF A400、ASA C400、および ASA A400** システムでの **ADP** とディスク割り当て

ガイドライン	サイトあたりのドライブ数	ドライブ割り当てルール	ルートパーティションの ADP レイアウト

推奨される最小ドライブ数（サイトあたり）	96本のドライブ	ドライブはシェルフ単位で自動的に割り当てられます。	<p>ルートアグリゲートの2つのプレックスのそれぞれに、次のものが含まれます。</p> <ul style="list-style-type: none"> <li>• データ用のパーティション × 20</li> <li>• パリティパーティション × 2</li> <li>• スペアパーティションが2つ必要です</li> </ul>
サポートされる最小ドライブ数（サイトあたり）	24本のドライブ	ドライブが4つのグループ（クォータ）に均等に分割されます。各クォータシェルフは、自動的に別々のプールに割り当てられます。	<p>ルートアグリゲートの2つのプレックスのそれぞれに、次のものが含まれます。</p> <ul style="list-style-type: none"> <li>• データ用パーティション × 3</li> <li>• パリティパーティション × 2</li> <li>• スペアパーティション × 1</li> </ul>

ADP とディスク割り当ては **AFF A700** システムでサポートされます

ガイドライン	サイトあたりのドライブ数	ドライブ割り当てルール	ルートパーティションのADPレイアウト
推奨される最小ドライブ数（サイトあたり）	96本のドライブ	ドライブはシェルフ単位で自動的に割り当てられます。	<p>ルートアグリゲートの2つのプレックスのそれぞれに、次のものが含まれます。</p> <ul style="list-style-type: none"> <li>• データ用のパーティション × 20</li> <li>• パリティパーティション × 2</li> <li>• スペアパーティションが2つ必要です</li> </ul>

サポートされる最小ドライブ数（サイトあたり）	24本のドライブ	ドライブが4つのグループ（クォータ）に均等に分割されます。各クォータシェルフは、自動的に別々のプールに割り当てられます。	<p>ルートアグリゲートの2つのブレックスのそれぞれに、次のものが含まれます。</p> <ul style="list-style-type: none"> <li>データ用パーティション × 3</li> <li>パリティパーティション × 2</li> <li>スペアパーティション × 1</li> </ul>
------------------------	----------	--	--

**AFF C800、ASA C800、ASA A800、AFF A800システムでのADPとディスク割り当て**

ガイドライン	サイトあたりのドライブ数	ドライブ割り当てルール	ルートアグリゲートのADPレイアウト
推奨される最小ドライブ数（サイトあたり）	内蔵ドライブと外付けドライブ 96本	内部パーティションは4つのグループ（クォータ）に均等に分割されます。各クォータが自動的に別々のプールに割り当てられます。外付けシェルフのドライブはシェルフ単位で自動的に割り当てられ、各シェルフのすべてのドライブがMetroCluster構成の4つのノードのいずれかに割り当てられます。	<p>ルートアグリゲートの2つのブレックスのそれぞれに、次のものが含まれます。</p> <ul style="list-style-type: none"> <li>データ用パーティション × 8</li> <li>パリティパーティション × 2</li> <li>スペアパーティションが2つ必要です</li> </ul> <p>*注：*ルートアグリゲートは内蔵シェルフの12個のルートパーティションで作成されます。</p>

サポートされる最小ドライブ数（サイトあたり）	内蔵ドライブ24本	内部パーティションは4つのグループ（クォータ）に均等に分割されません。各クォータが自動的に別々のプールに割り当てられます。	<p>ルートアグリゲートの2つのプレックスのそれぞれに、次のものが含まれます。</p> <ul style="list-style-type: none"> <li>データ用パーティション × 3</li> <li>パリティパーティション × 2</li> <li>スペアパーティション × 1</li> </ul> <p>*注：*ルートアグリゲートは内蔵シェルフの12個のルートパーティションで作成されます。</p>
------------------------	-----------	---	---

**AFF A70、AFF A90、AFF C80**システムでのADPとディスク割り当て

ガイドライン	サイトあたりのドライブ数	ドライブ割り当てルール	ルートアグリゲートのADPレイアウト
推奨される最小ドライブ数（サイトあたり）	内蔵ドライブと外付けドライブ 96 本	内部パーティションは4つのグループ（クォータ）に均等に分割されます。各クォータが自動的に別々のプールに割り当てられます。外付けシェルフのドライブはシェルフ単位で自動的に割り当てられ、各シェルフのすべてのドライブがMetroCluster構成の4つのノードのいずれかに割り当てられます。	<p>ルートアグリゲートの2つのプレックスのそれぞれに、次のものが含まれます。</p> <ul style="list-style-type: none"> <li>データ用パーティション × 8</li> <li>パリティパーティション × 2</li> <li>スペアパーティションが2つ必要です</li> </ul>
サポートされる最小ドライブ数（サイトあたり）	内蔵ドライブ24本	内部パーティションは4つのグループ（クォータ）に均等に分割されません。各クォータが自動的に別々のプールに割り当てられます。	<p>ルートアグリゲートの2つのプレックスのそれぞれに、次のものが含まれます。</p> <ul style="list-style-type: none"> <li>データ用パーティション × 3</li> <li>パリティパーティション × 2</li> <li>スペアパーティション × 1</li> </ul>

**AFF A900、ASA A900、およびAFF A1KシステムでのADPとディスク割り当て**

ガイドライン	サイトあたりのシェルフ数	ドライブ割り当てルール	ルートパーティションのADP レイアウト
推奨される最小ドライブ数（サイトあたり）	96 本のドライブ	ドライブはシェルフ単位で自動的に割り当てられます。	<p>ルートアグリゲートの 2 つのプレックスのそれぞれに、次のものが含まれます。</p> <ul style="list-style-type: none"> <li>データ用のパーティション × 20</li> <li>パリティパーティション × 2</li> <li>スペアパーティションが 2 つ必要です</li> </ul>
サポートされる最小ドライブ数（サイトあたり）	24 本のドライブ	ドライブが 4 つのグループ（クォータ）に均等に分割されます。各クォータシェルフは、自動的に別々のプールに割り当てられます。	<p>ルートアグリゲートの 2 つのプレックスのそれぞれに、次のものが含まれます。</p> <ul style="list-style-type: none"> <li>データ用パーティション × 3</li> <li>パリティパーティション × 2</li> <li>スペアパーティション × 1</li> </ul>

**FAS2750 システムでのディスク割り当て**

ガイドライン	サイトあたりのドライブ数	ドライブ割り当てルール	ルートパーティションのADP レイアウト
推奨される最小ドライブ数（サイトあたり）	内蔵ドライブ 24 本、外付けドライブ 24 本	内蔵シェルフと外付けシェルフは、2 つに均等に分割されます。各ハーフが自動的に別々のプールに割り当てられます	該当なし
サポートされる最小ドライブ数（サイトあたり） （アクティブ / パッシブ HA 構成）	内蔵ドライブのみ	手動で割り当てる必要があります	該当なし

**FAS8200 システムでのディスク割り当て**

ガイドライン	サイトあたりのドライブ数	ドライブ割り当てルール	ルートパーティションのADP レイアウト
推奨される最小ドライブ数（サイトあたり）	48 ドライブ	外付けシェルフのドライブが2つのグループ（ハーフ）に均等に分割されます。シェルフの各ハーフが自動的に別々のプールに割り当てられます。	該当なし
サポートされる最小ドライブ数（サイトあたり） （アクティブ/パッシブHA構成）	24本のドライブ	手動で割り当てる必要があります。	該当なし

#### FAS500f システムでのディスク割り当て

AFF C250システムとAFF A250システムで同じディスク割り当てガイドラインとルールがFAS500fシステムにも適用されます。FAS500fシステムでのディスク割り当てについては、[を参照してください。](#)

[\[ADP\\_FAS500f\]](#) 表。

#### FAS9000、FAS9500、FAS70、およびFAS90システムでのディスク割り当て

ガイドライン	サイトあたりのドライブ数	ドライブ割り当てルール	ルートパーティションのADP レイアウト
推奨される最小ドライブ数（サイトあたり）	96本のドライブ	ドライブはシェルフ単位で自動的に割り当てられます。	該当なし
サポートされる最小ドライブ数（サイトあたり）	24本のドライブ	ドライブが4つのグループ（クォータ）に均等に分割されます。各クォータシェルフは、自動的に別々のプールに割り当てられます。	該当なし

#### FAS50システムでのディスク割り当て

ガイドライン	サイトあたりのドライブ数	ドライブ割り当てルール	ルートパーティションのADP レイアウト

推奨される最小ドライブ数（サイトあたり）	48ドライブ（外付けドライブのみ、内蔵ドライブなし）	各外付けシェルフのドライブが2つのグループに均等に分割されます（ハーフ）。シェルフの各ハーフが自動的に別々のプールに割り当てられません。	該当なし
	48ドライブ（外付けドライブと内蔵ドライブ）	内部パーティションは4つのグループ（クォータ）に均等に分割されます。各クォータが自動的に別々のプールに割り当てられます。外付けシェルフのドライブが4つのグループ（クォータ）に均等に分割されます。各クォータシェルフは自動的に別々のプールに割り当てられます。	該当なし
サポートされる最小ドライブ数（サイトあたり）	24本のドライブ	ドライブは4つのグループに均等に分割されます。各クォータシェルフは、自動的に別々のプールに割り当てられます。	該当なし

フラッシュキャッシュを搭載した**FAS50**システムでのディスク割り当て

ONTAP 9.18.1 以降、MetroCluster IP 構成の FAS50 システムで Flash Cache がサポートされるようになりました。



- 内部シェルフに、データ アグリゲートと、フラッシュ キャッシュ ドライブを備えたルート アグリゲートの両方を配置することはできません。
- スロット 0 と 23 は、Flash Cache ドライブに使用されます。
- 外部ディスク シェルフを再利用する場合は、コントローラに接続する前に、外部ディスク シェルフのディスク所有権が削除されていることを確認してください。参照["ディスクからONTAPの所有権を削除する"](#)。

ガイドライン	サイトあたりのドライブ数	ドライブ割り当てルール	ルートパーティションのADP レイアウト
--------	--------------	-------------	----------------------

<p>推奨される最小ドライブ数（サイトあたり）</p>	<p>48ドライブ（外付けドライブのみ、内蔵ドライブなし）</p>	<p>各外付けシェルフのドライブが2つのグループに均等に分割されます（ハーフ）。シェルフの各ハーフが自動的に別々のプールに割り当てられません。</p>	<p>該当なし</p>
	<p>36台のドライブ（内部ドライブ12台と外部ドライブ24台 - データアグリゲートは外部シェルフに、ルートアグリゲートは内部シェルフに配置）</p>	<p>内部ドライブは4つの均等なグループ（四半期）に分割されます。各クォータが自動的に別々のプールに割り当てられます。外部シェルフ上のドライブは4つの均等なグループ（四半期）に分割されます。シェルフの各クォータが自動的に別々のプールに割り当てられます。</p> <p>注記:</p> <ul style="list-style-type: none"> <li>内部ドライブと外部ドライブを使用している場合は、まずONTAPをインストールし、内部ドライブのみを使用してローカルクラスタを構成する必要があります。その後、インストールまたはセットアップのタスクが完了したら、外付けシェルフを手動で接続します。</li> <li>ルートアグリゲートには少なくとも12台の内部ドライブが必要です。ルート内部ドライブはスロット1から配置する必要があります。たとえば、内部ドライブが12台の場合、スロット1～3、6～8、12～14、および18～20を使用します。</li> </ul>	<p>該当なし</p>

サポートされる最小ドライブ数（サイトあたり）	外付けドライブ24台	ドライブは4つのグループに均等に分割されます。各クォータシェルフは、自動的に別々のプールに割り当てられます。	該当なし
------------------------	------------	--	------

## MetroCluster IP構成におけるクラスタピアリングの要件

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

### 関連情報

["クラスタと SVM のピアリングの簡単な設定"](#)

### クラスタピアリングの前提条件

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

### 接続要件

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

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

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

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

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

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



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

### ポート要件

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

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

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

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

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

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

#### ファイアウォールの要件

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

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

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

#### 専用のポートを使用する場合の考慮事項

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

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

- 使用できる WAN 帯域幅が LAN ポートの帯域幅とほぼ同じで、レプリケーション間隔の設定により、通常のクライアントアクティビティが実行されている間にレプリケーションが実行される場合は、クラスタ間レプリケーションにイーサネットポートを専用割り当てて、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せん。

## ISL の要件

### MetroCluster IP構成のスイッチ間リンク要件

MetroCluster IP構成とネットワークがスイッチ間リンク（ISL）の要件をすべて満たしていることを確認する必要があります。一部の要件が該当しない構成もありますが、構成全体の理解を深めるためには、ISLのすべての要件を把握しておく必要があります。

次の表に、このセクションで説明するトピックの概要を示します。

タイトル	説明
"ネットアップが検証したMetroCluster準拠スイッチ"	に、スイッチの要件を示します。 環境バックエンドスイッチを含む、MetroCluster構成で使用されるすべてのスイッチ。

タイトル	説明
"ISL に関する考慮事項"	に、ISLの要件を示します。  ネットワークトポロジ、およびネットアップ検証済みスイッチとMetroCluster準拠スイッチのどちらを使用しているかに関係なく、環境All MetroCluster構成。
"共有レイヤ2またはレイヤ3ネットワークにMetroClusterを導入する際の考慮事項"	共有レイヤ2またはレイヤ3ネットワークの要件について説明します。  環境：ネットアップ検証済みのスイッチを使用し、直接接続されたISLを使用するMetroCluster構成を除くすべての構成。
"MetroCluster準拠スイッチを使用する場合の考慮事項"	MetroCluster準拠スイッチの要件について説明します。  ネットアップ検証済みスイッチを使用していない環境All MetroCluster構成。
"MetroCluster ネットワークトポロジの例"	に、さまざまなMetroClusterネットワークトポロジの例を示します。  環境All MetroCluster構成

## MetroCluster IP 構成におけるNetApp認定およびMetroCluster準拠のスイッチ

バックエンドスイッチを含め、構成で使用するすべてのスイッチが、ネットアップ検証済みまたはMetroCluster準拠のいずれかである必要があります。

### ネットアップ検証済みスイッチ

スイッチが次の要件を満たしている場合、ネットアップで検証されます。

- スwitchは、MetroCluster IP構成の一部としてネットアップから提供されます
- スwitchは、"[NetApp Hardware Universe の略](#)" MetroCluster-over-IP-connections\_でサポートされるスイッチとして使用
- このスイッチは、MetroCluster IPコントローラと、一部の構成ではNS224ドライブシェルフへの接続にのみ使用します
- スwitchは、NetAppが提供するリファレンス構成ファイル（RCF）を使用して設定します。

これらの要件を満たしていないスイッチは、ネットアップの検証済みスイッチではありません。

### MetroCluster準拠のスイッチ

MetroCluster準拠スイッチはネットアップでは検証されていませんが、一定の要件および構成ガイドラインを満たしていれば、MetroCluster IP構成で使用できます。



NetAppでは、MetroCluster準拠の検証が行われていないスイッチについては、トラブルシューティングや構成のサポートサービスは提供していません。

## MetroCluster IP構成におけるスイッチ間リンク（ISL）の要件

すべてのMetroCluster IP構成およびネットワークトポロジでMetroClusterトラフィックを伝送するスイッチ間リンク（ISL）には、一定の要件があります。これらの要件は、お客様のスイッチ間でISLを直接接続するか共有するかに関係なく、MetroClusterトラフィ

ックを伝送するすべてのISLに適用されます。

#### MetroCluster ISL要件

すべてのMetroCluster IP構成の次の環境ISL：

- ISLの数は両方のファブリックで同じである必要があります。
- 1つのファブリックのISLは、速度と長さがすべて同じである必要があります。
- ISLの速度と長さは、両方のファブリックで同じである必要があります。
- サポートされるファブリック1とファブリック2の距離の最大差は20km（0.2ms）です。
- ISLのトポロジは同じである必要があります。たとえば、すべてのリンクを直接リンクにするか、WDMを使用する場合はすべてのリンクでWDMを使用する必要があります。
- 必要な最小 ISL 速度はプラットフォーム モデルによって異なります。
  - ONTAP 9.18.1以降、MetroCluster IPバックエンドポート速度が100Gbpsのプラットフォームでは、最小ISLリンク速度が100Gbps必要です。異なるISL速度を使用するには、Feature Product Variance Request (FPVR) が必要です。FPVRを提出するには、NetApp営業チームにお問い合わせください。



現在 100Gbps ISL 要件を満たしていないプラットフォームでの ONTAP 9.18.1 以降へのアップグレードはブロックされず、続行できます。ただし、NetApp は、期待されるパフォーマンスと可用性のレベルを維持するために、お客様が 100Gbps ISL 接続に移行することを強く推奨します。

- その他のすべてのプラットフォームでは、サポートされる最小 ISL リンク速度は 10 Gbps です。
- ファブリックごとに少なくとも 1 つの 10Gbps ISL ポートが必要です。

#### ISL のレイテンシとパケット損失の制限

安定した状態でのMetroCluster構成でのsite\_Aとsite\_BのMetroCluster IPスイッチ間の次の環境ラウンドトリップトラフィック。

- 2 つの MetroCluster サイト間の距離が長くなるとレイテンシが増加します。通常、ラウンドトリップ遅延時間は 100km（62 マイル）ごとに 1 ミリ秒程度です。レイテンシは、ネットワーク上のISLリンクの帯域幅、パケットドロップレート、およびジッタに関して、ネットワークのService Level Agreement (SLA ; サービスレベルアグリーメント) にも左右されます。低帯域幅、高ジッタ、およびランダムなパケットドロップは、パケット配信を成功させるために、スイッチまたはコントローラモジュール上のTCPエンジンによって異なるリカバリメカニズムをもたらします。このようなりカバリメカニズムによって、全体的なレイテンシが増加することがあり構成のラウンドトリップレイテンシおよび最大距離の要件の詳細については、を参照してください "[Hardware Universe の略。](#)"
- レイテンシに影響するすべてのデバイスについて考慮する必要があります。
- "[Hardware Universe の略。](#)" 距離 (km) を提供します。100kmごとに1ミリ秒を割り当てる必要があります。最大距離は、最初に到達した距離によって定義されます。最大ラウンドトリップ時間 (RTT) (ms) または距離 (km) です。たとえば、-the\_listsの距離が300km (3ミリ秒) の場合、ISLは300km以下にすることができ、最大Hardware Universe時間は3ミリ秒のいずれか先に達した方を超えることはできません。
- パケット損失は0.01%以下でなければなりません。最大パケット損失は、MetroClusterノード間のパス上のすべてのリンクの損失と、ローカルMetroCluster IPインターフェイス上の損失の合計です。

- サポートされるジッタ値は、ラウンドトリップの場合は3ミリ秒（一方向の場合は1.5ミリ秒）です。
- ネットワークは、トラフィックのマイクロバーストや急増に関係なく、MetroClusterトラフィックに必要な帯域幅のSLAを割り当て、維持する必要があります。
- ONTAP 9.7以降を使用している場合は、2つのサイト間の中間ネットワークでMetroCluster IP構成用に4.5Gbps以上の帯域幅が確保されている必要があります。

#### トランシーバとケーブルに関する考慮事項

MetroCluster ISL では、機器のベンダーがサポートしている SFP または QSFP がサポートされます。NetApp または機器ベンダーから提供されたSFPおよびQSFPが、スイッチおよびスイッチのファームウェアでサポートされている必要があります。

コントローラをスイッチおよびローカルクラスタのISLに接続するときは、NetAppとMetroClusterが提供するトランシーバとケーブルを使用する必要があります。

QSFP-SFPアダプタを使用する場合、ポートをブレイクアウトモードとネイティブモードのどちらで設定するかは、スイッチのモデルとファームウェアによって異なります。たとえば、NX-OSファームウェア9.xまたは10.xを実行するCisco 9336CスイッチでQSFP-SFPアダプタを使用するには、ポートをネイティブ速度モードで設定する必要があります。



RCFを設定する場合は、正しい速度モードを選択するか、適切な速度モードのポートを使用してください。

#### xWDM、TDM、および外部暗号化デバイスの使用

MetroCluster IP構成でxWDM / TDMデバイスまたは暗号化を提供するデバイスを使用する場合は、次の要件を満たす必要があります。

- MetroCluster IPスイッチをxWDM / TDMに接続する場合は、スイッチとファームウェアについてベンダーが認定した外部暗号化デバイスまたはxWDM / TDM機器を使用する必要があります。動作モード（トランキングや暗号化など）に対応している必要があります。
- 暗号化を含むエンドツーエンドの全体的な遅延とジッタは、IMTおよびこのマニュアルに記載されている最大値を超えることはできません。

#### サポートされるISL数とブレイクアウトケーブル数

次の表に、リファレンス構成ファイル（RCF）構成を使用してMetroCluster IPスイッチに設定できる、サポートされるISLの最大数を示します。

MetroCluster IP スwitchのモデル	ポートタイプ	ISLの最大数
Broadcom 対応 BES-53248 スイッチ	ネイティブポート	ISL×4（10Gbpsまたは25Gbpsを使用）
Broadcom 対応 BES-53248 スイッチ	ネイティブポート（注1）	ISL×2、40Gbpsまたは100Gbpsを使用
Cisco 3132Q-V の設定	ネイティブポート	ISL×6、40Gbpsを使用

Cisco 3132Q-V の設定	ブレイクアウトケーブル	ISL×16 (10Gbpsを使用)
Cisco 3232C	ネイティブポート	ISL×6、40Gbpsまたは100Gbpsを使用
Cisco 3232C	ブレイクアウトケーブル	ISL×16、10Gbpsまたは25Gbpsを使用
Cisco 9336C-FX2 (NS224シェルフは接続しない)	ネイティブポート	ISL×6、40Gbpsまたは100Gbpsを使用
Cisco 9336C-FX2 (NS224シェルフは接続しない)	ブレイクアウトケーブル	ISL×16、10Gbpsまたは25Gbpsを使用
Cisco 9336C-FX2 (NS224シェルフの接続)	ネイティブポート (注2)	ISL×4、40Gbpsまたは100Gbpsを使用
Cisco 9336C-FX2 (NS224シェルフの接続)	ブレイクアウトケーブル (注2)	ISL×16、10Gbpsまたは25Gbpsを使用
NVIDIA SN2100	ネイティブポート (注2)	ISL×2、40Gbpsまたは100Gbpsを使用
NVIDIA SN2100	ブレイクアウトケーブル (注2)	ISL×8、10Gbpsまたは25Gbpsを使用

\*注1 \* : BES-53248スイッチで40Gbpsまたは100GbpsのISLを使用するには、追加のライセンスが必要です。

\*注2 \* : 同じポートがネイティブ速度とブレイクアウトモードに使用されます。RCFファイルを作成するときは、ポートを標準の速度モードとブレイクアウトモードのどちらで使用するかを選択する必要があります。

- 1つのMetroCluster IPスイッチのISLは、すべて同じ速度である必要があります。速度が異なるISLポートを同時に使用することはできません。
- 最適なパフォーマンスを実現するには、ネットワークごとに40GbpsのISLを少なくとも1つ使用する必要があります。FAS9000、AFF A700、またはその他の大容量プラットフォームでは、ネットワークごとに1つの10Gbps ISLを使用しないでください。



NetAppでは、広帯域幅のISLを多数使用するのではなく、広帯域幅のISLを少数使用することを推奨しています。たとえば、4つの10Gbps ISLではなく、40Gbps ISLを1つ設定することを推奨します。複数のISLを使用する場合は、統計的なロードバランシングが最大スループットに影響する可能性があります。負荷分散が均等でないと、単一ISLのスループットまで低下する可能性があります。

共有レイヤー2またはレイヤー3ネットワークに**MetroCluster IP**構成を導入するための要件

要件に応じて、共有レイヤ2またはレイヤ3ネットワークを使用してMetroClusterを導入できます。

ONTAP 9.6以降では、サポート対象のスイッチを使用するMetroCluster IP構成で、専用のMetroCluster ISLを使用する代わりに、既存のネットワークをスイッチ間リンク（ISL）で共有できます。このトポロジは\_共有レイヤ2ネットワーク\_と呼ばれます。

ONTAP 9.9.1以降では、MetroCluster IP設定をIPルーテッド（レイヤ3）バックエンド接続で実装できます。このトポロジは\_共有レイヤ3ネットワーク\_と呼ばれます。



- すべての機能がすべてのネットワークトポロジでサポートされているわけではありません。
- ネットワーク容量が十分であり、ISLサイズが構成に適していることを確認する必要があります。MetroCluster サイト間でのデータのレプリケーションでは、レイテンシを低く抑えることが重要になります。これらの接続にレイテンシの問題があると、クライアント I/O に影響する可能性があります
- MetroClusterバックエンドスイッチとは、いずれもネットアップが検証したスイッチ、またはMetroClusterに準拠しているスイッチを指します。を参照してください "[ネットアップが検証したMetroCluster準拠スイッチ](#)" 詳細：

#### レイヤ2およびレイヤ3ネットワークのISL要件

次の環境レイヤ2およびレイヤ3ネットワーク：

- MetroClusterスイッチと中間ネットワークスイッチ間で、ISLの速度と数が一致している必要はありません。同様に、中間ネットワークスイッチ間で速度が一致している必要はありません。

たとえば、1つの40Gbps ISLを使用してMetroClusterスイッチを中間スイッチに接続し、2つの100Gbps ISLを使用して中間スイッチを相互に接続できます。

- ISLの使用状況、エラー（ドロップ、リンクフラップ、破損など）を監視するには、中間ネットワークでネットワーク監視を設定する必要があります。そして失敗。
- MetroClusterエンドツーエンドトラフィックを伝送するすべてのポートで、MTUサイズを9216に設定する必要があります。
- 他のトラフィックには、Class of Service（COS;サービスクラス）5よりも高いプライオリティを設定することはできません。
- エンドツーエンドMetroClusterトラフィックを伝送するすべてのパスで、Explicit Congestion Notification（ECN;明示的輻輳通知）を設定する必要があります。
- MetroCluster トラフィックを伝送する ISL は、スイッチ間のネイティブリンクである必要があります。

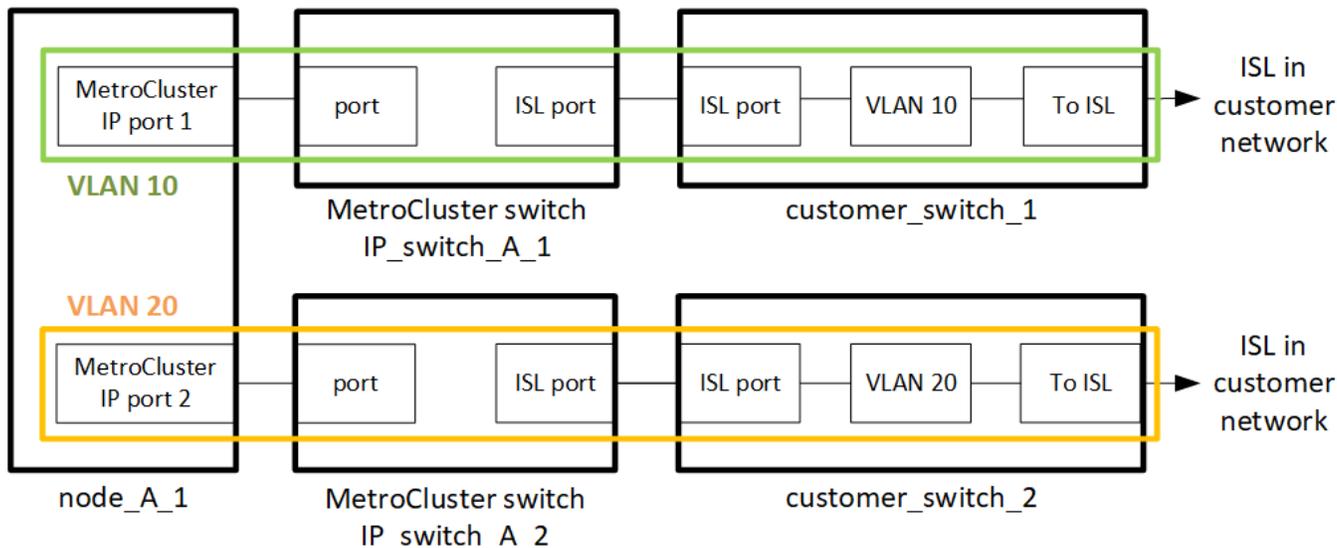
マルチプロトコルラベルスイッチング（MPLS）リンクなどのリンク共有サービスはサポートされません。

- レイヤ2 VLANは、ネイティブに複数のサイトにまたがっている必要があります。Virtual Extensible LAN（VXLAN）などのVLAN オーバーレイはサポートされていません。
- 中間スイッチの数に制限はありません。ただし、NetAppでは、スイッチの数を必要な最小数に保つことを推奨しています。
- MetroClusterスイッチのISLは次のように設定されます。
  - LACPポートチャネルの一部としてのスイッチポートモード「trunk」
  - MTUサイズは9216

- ネイティブVLANが設定されていない
- サイト間のMetroClusterトラフィックを伝送するVLANのみが許可されます。
- スイッチのデフォルトVLANは許可されていません。

#### レイヤ2ネットワークに関する考慮事項

MetroClusterバックエンドスイッチがお客様のネットワークに接続されている。



お客様側で用意する中間スイッチは、次の要件を満たしている必要があります。

- 中間ネットワークは、サイト間で同じVLANを提供する必要があります。これは、RCFファイルに設定されているMetroCluster VLANと一致している必要があります。
- RcfFileGenerator では、プラットフォームでサポートされていない VLAN を使用して RCF ファイルを作成することはできません。
- RcfFileGeneratorは、将来の使用を想定している場合など、特定のVLAN IDの使用を制限することがあります。一般的に、予約済み VLAN は最大で 100 です。
- MetroCluster VLAN ID と ID が一致するレイヤ 2 VLAN で共有ネットワークを構成する必要があります。

#### ONTAPでのVLANの設定

VLANはインターフェイスの作成時にのみ指定できます。デフォルトのVLAN 10および20、または101~4096（またはスイッチベンダーがサポートする番号のいずれか小さい方の番号）の範囲内のVLANを設定できます。MetroClusterインターフェイスの作成後にVLAN IDを変更することはできません。



一部のスイッチベンダーでは、特定のVLANの使用を予約する場合があります。

次のシステムでは、ONTAP内でVLANを設定する必要はありません。VLANは、スイッチポートの設定によって指定されます。

- FAS8200 と AFF A300
- AFF A320
- FAS9000およびAFF A700

- AFF A800、ASA A800、AFF C800、およびASA C800



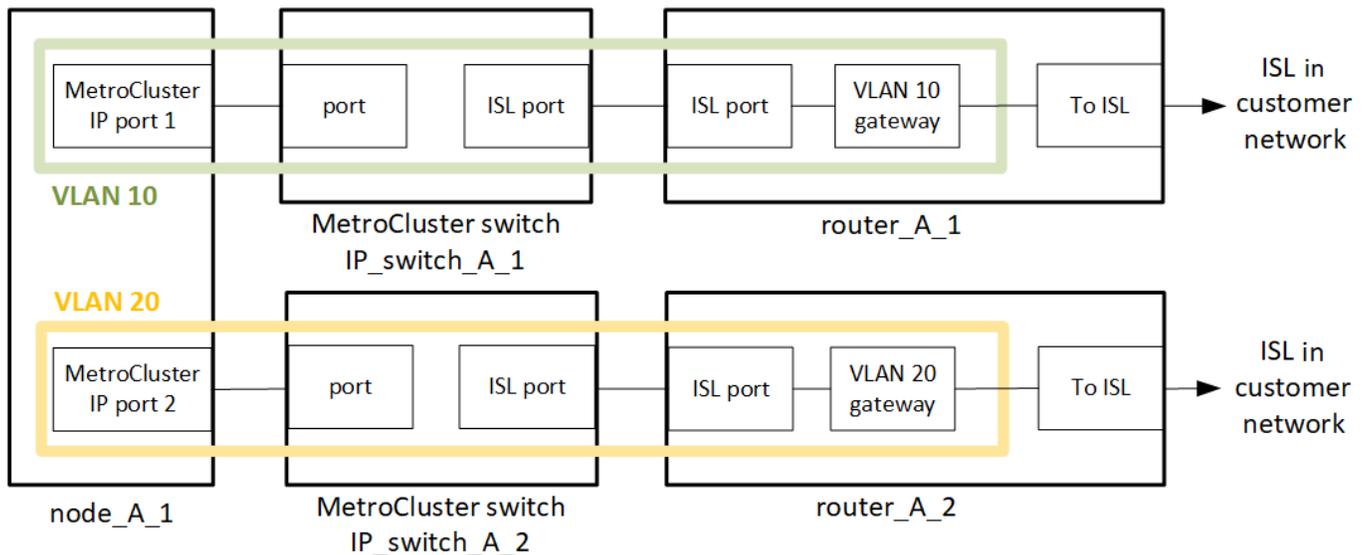
上記のシステムは、VLAN 100以下を使用して設定できます。ただし、この範囲の一部のVLANは、他の用途や将来の用途に予約されている可能性があります。

他のすべてのシステムでは、ONTAPでMetroClusterインターフェイスを作成するときにVLANを設定する必要があります。次の制限事項が適用されます。

- デフォルトのVLANは10および20です。
- ONTAP 9.7以前を実行している場合は、デフォルトのVLAN 10およびVLAN 20のみを使用できます。
- ONTAP 9.8以降を実行している場合は、デフォルトのVLAN 10および20を使用できます。また、100を超えるVLAN（101以上）も使用できます。

#### レイヤ3ネットワークに関する考慮事項

MetroCluster バックエンドスイッチは、ルータに直接接続するか（次の簡単な例を参照）、または他の介在するスイッチを介してルーティングされた IP ネットワークに接続されます。



MetroCluster 環境は、の説明に従って標準的な MetroCluster IP 構成で構成およびケーブル接続されます ["MetroCluster ハードウェアコンポーネントを設定します"](#)。手順のインストールとケーブル接続を実行する場合は、レイヤ3構成に固有の手順を実行する必要があります。次の環境レイヤ3設定

- MetroClusterスイッチは、ルータに直接接続することも、介入する1つ以上のスイッチに接続することもできます。
- MetroCluster IPインターフェイスは、ルータに直接接続することも、介入するスイッチの1つに接続することもできます。
- VLAN をゲートウェイデバイスに拡張する必要があります。
- を使用します `-gateway parameter` MetroCluster IPインターフェイスアドレスにIPゲートウェイアドレスを設定するには、次の手順を実行します。
- MetroCluster VLAN の VLAN ID は、各サイトで同じである必要があります。ただし、サブネットは異なる場合があります。

- ダイナミックルーティングは、MetroCluster トラフィックではサポートされていません。
- 次の機能はサポートされません。
  - 8 ノード MetroCluster 構成
  - 4 ノード MetroCluster 構成の更新
  - MetroCluster FC から MetroCluster IP に移行します
- 各 MetroCluster サイトには、ネットワークごとに 1 つ、合計 2 つのサブネットが必要です。
- 自動 IP 割り当てはサポートされていません。

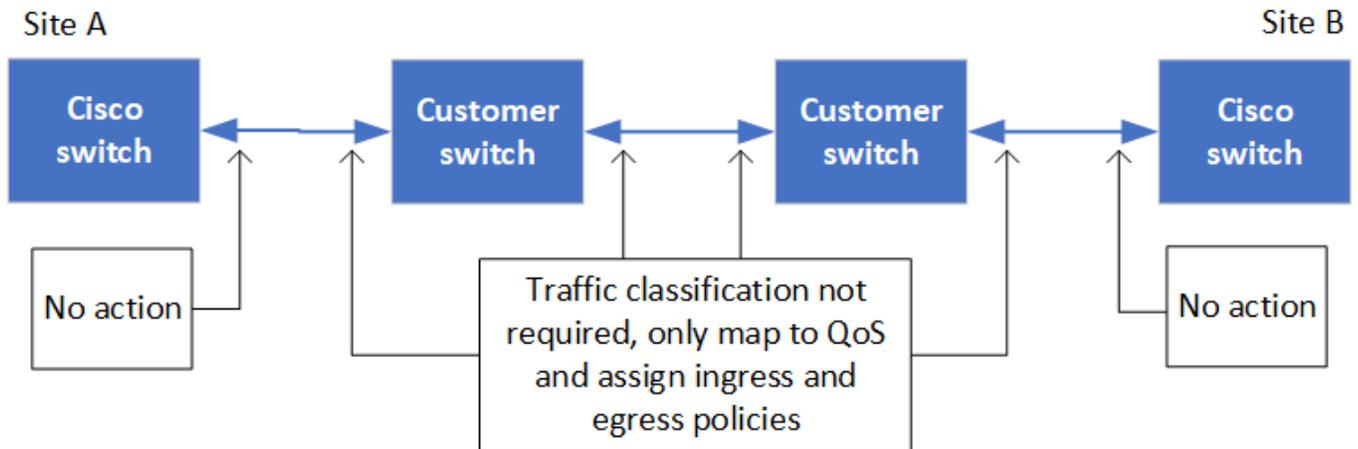
ルータおよびゲートウェイのIPアドレスを設定する場合は、次の要件を満たす必要があります。

- 一方のノードの2つのインターフェイスに同じゲートウェイIPアドレスを設定することはできません。
- 各サイトの HA ペアの対応するインターフェイスには、同じゲートウェイ IP アドレスが必要です。
- ノードとその DR パートナーおよび AUX パートナーの対応するインターフェイスは、同じゲートウェイ IP アドレスを持つことはできません。
- ノードとその DR パートナーおよび AUX パートナーの対応するインターフェイスは、同じ VLAN ID を持つ必要があります。

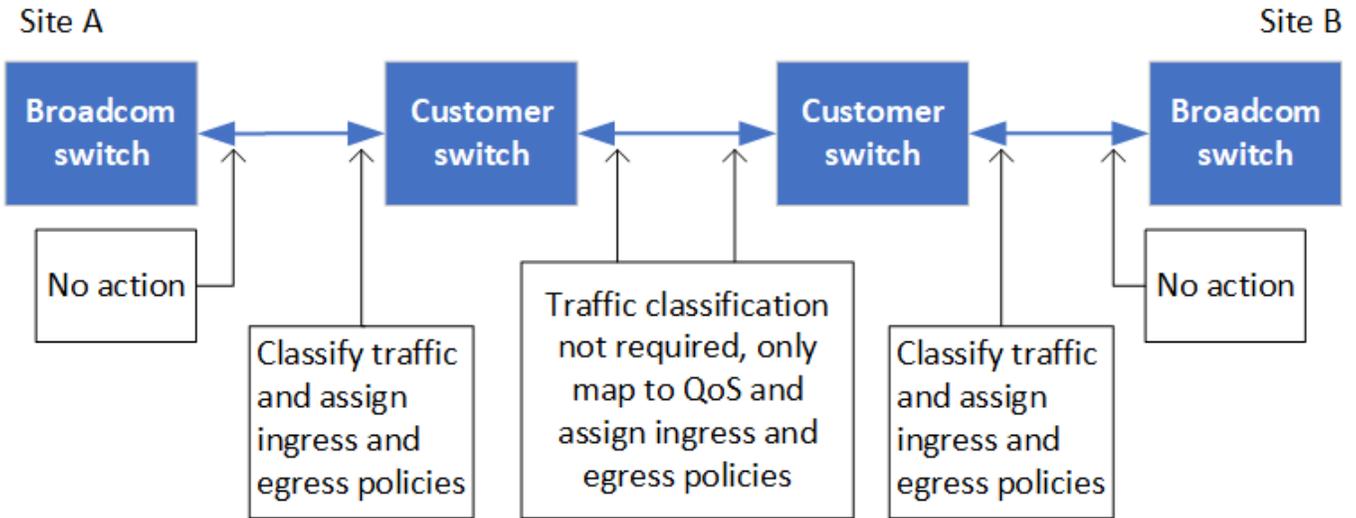
#### 中間スイッチに必要な設定

MetroClusterトラフィックが中間ネットワークのISLを経由する場合は、中間スイッチの設定によって、MetroClusterサイト間のパス全体でMetroClusterトラフィック（RDMAおよびストレージ）が必要なサービスレベルを満たしていることを確認する必要があります。

次の図に、NetApp検証済みCiscoスイッチを使用する場合に必要な設定の概要を示します。



次の図は、外部スイッチがBroadcom IPスイッチの場合の共有ネットワークに必要な設定の概要を示しています。



この例では、MetroCluster トラフィックに対して次のポリシーとマップが作成されます。

- MetroClusterIP\_ISL\_Ingress ポリシーは、MetroCluster IPスイッチに接続する中間スイッチのポートに適用されます。
- MetroClusterIP\_ISL\_Ingress ポリシーは、着信タグ付きトラフィックを中間スイッチの適切なキューにマッピングします。
- AMetroClusterIP\_ISL\_Egress ポリシーは、中間スイッチ間のISLに接続する中間スイッチのポートに適用されます。
- MetroCluster IP スイッチ間のパスに沿って、一致する QoS アクセスマップ、クラスマップ、およびポリシーマップを使用して中間スイッチを設定する必要があります。中間スイッチは、RDMA トラフィックを COS5 にマッピングし、ストレージトラフィックを COS4 にマッピングします。

次に、Cisco Nexus 3232Cおよび9336C-FX2スイッチの例を示します。スイッチのベンダーとモデルに応じて、中間スイッチの構成が適切であることを確認する必要があります。

中間スイッチISLポートのクラスマップを設定する

次に、入力でトラフィックを分類する必要があるか一致させる必要があるかに応じたクラスマップ定義の例を示します。

入力時のトラフィックの分類：

```
ip access-list rdma
  10 permit tcp any eq 10006 any
  20 permit tcp any any eq 10006
ip access-list storage
  10 permit tcp any eq 65200 any
  20 permit tcp any any eq 65200

class-map type qos match-all rdma
  match access-group name rdma
class-map type qos match-all storage
  match access-group name storage
```

入力のトラフィックを照合します。

```
class-map type qos match-any c5
  match cos 5
  match dscp 40
class-map type qos match-any c4
  match cos 4
  match dscp 32
```

中間スイッチの**ISL**ポートに入力ポリシーマップを作成します。

次に、入力でトラフィックを分類する必要があるか照合する必要があるかに応じて、入力ポリシーマップを作成する例を示します。

入力時にトラフィックを分類します。

```
policy-map type qos MetroClusterIP_ISL_Ingress_Classify
  class rdma
    set dscp 40
    set cos 5
    set qos-group 5
  class storage
    set dscp 32
    set cos 4
    set qos-group 4
  class class-default
    set qos-group 0
```

入力のトラフィックを照合します。

```
policy-map type qos MetroClusterIP_ISL_Ingress_Match
  class c5
    set dscp 40
    set cos 5
    set qos-group 5
  class c4
    set dscp 32
    set cos 4
    set qos-group 4
  class class-default
    set qos-group 0
```

**ISL**ポートの出力キューイングポリシーを設定する

次に、出力キューイングポリシーを設定する例を示します。

```

policy-map type queuing MetroClusterIP_ISL_Egress
  class type queuing c-out-8q-q7
    priority level 1
  class type queuing c-out-8q-q6
    priority level 2
  class type queuing c-out-8q-q5
    priority level 3
    random-detect threshold burst-optimized ecn
  class type queuing c-out-8q-q4
    priority level 4
    random-detect threshold burst-optimized ecn
  class type queuing c-out-8q-q3
    priority level 5
  class type queuing c-out-8q-q2
    priority level 6
  class type queuing c-out-8q-q1
    priority level 7
  class type queuing c-out-8q-q-default
    bandwidth remaining percent 100
    random-detect threshold burst-optimized ecn

```

これらの設定は、MetroClusterトラフィックを伝送するすべてのスイッチおよびISLに適用する必要があります。

この例では、Q4とQ5は random-detect threshold burst-optimized ecn。構成によっては、次の例に示すように、最小しきい値と最大しきい値の設定が必要になる場合があります。

```

class type queuing c-out-8q-q5
  priority level 3
  random-detect minimum-threshold 3000 kbytes maximum-threshold 4000
  kbytes drop-probability 0 weight 0 ecn
class type queuing c-out-8q-q4
  priority level 4
  random-detect minimum-threshold 2000 kbytes maximum-threshold 3000
  kbytes drop-probability 0 weight 0 ecn

```



最小値と最大値は、スイッチと要件によって異なります。

#### 例1：Cisco

構成にCiscoスイッチが含まれている場合は、中間スイッチの最初の入力ポートで分類する必要はありません。次に、次のマップとポリシーを設定します。

- class-map type qos match-any c5
- class-map type qos match-any c4

- MetroClusterIP\_ISL\_Ingress\_Match

ユーザーは、MetroClusterIP\_ISL\_Ingress\_Match MetroClusterトラフィックを伝送するISLポートへのポリシーマップ。

## 例2：Broadcom

Broadcomスイッチを使用する構成の場合は、中間スイッチの最初の入力ポートで分類する必要があります。次に、次のマップとポリシーを設定します。

- ip access-list rdma
- ip access-list storage
- class-map type qos match-all rdma
- class-map type qos match-all storage
- MetroClusterIP\_ISL\_Ingress\_Classify
- MetroClusterIP\_ISL\_Ingress\_Match

割り当て the MetroClusterIP\_ISL\_Ingress\_Classify Broadcomスイッチに接続する中間スイッチのISLポートへのポリシーマップ

ユーザーは、MetroClusterIP\_ISL\_Ingress\_Match MetroClusterトラフィックを伝送しているがBroadcomスイッチを接続していない中間スイッチのISLポートへのポリシーマップ。

## MetroCluster IP構成ネットワークトポロジの例

ONTAP 9.6以降では、MetroCluster IP構成で追加のネットワーク設定がサポートされません。ここでは、サポートされるネットワーク構成の例をいくつか示します。サポートされているトポロジの一部がリストされていません。

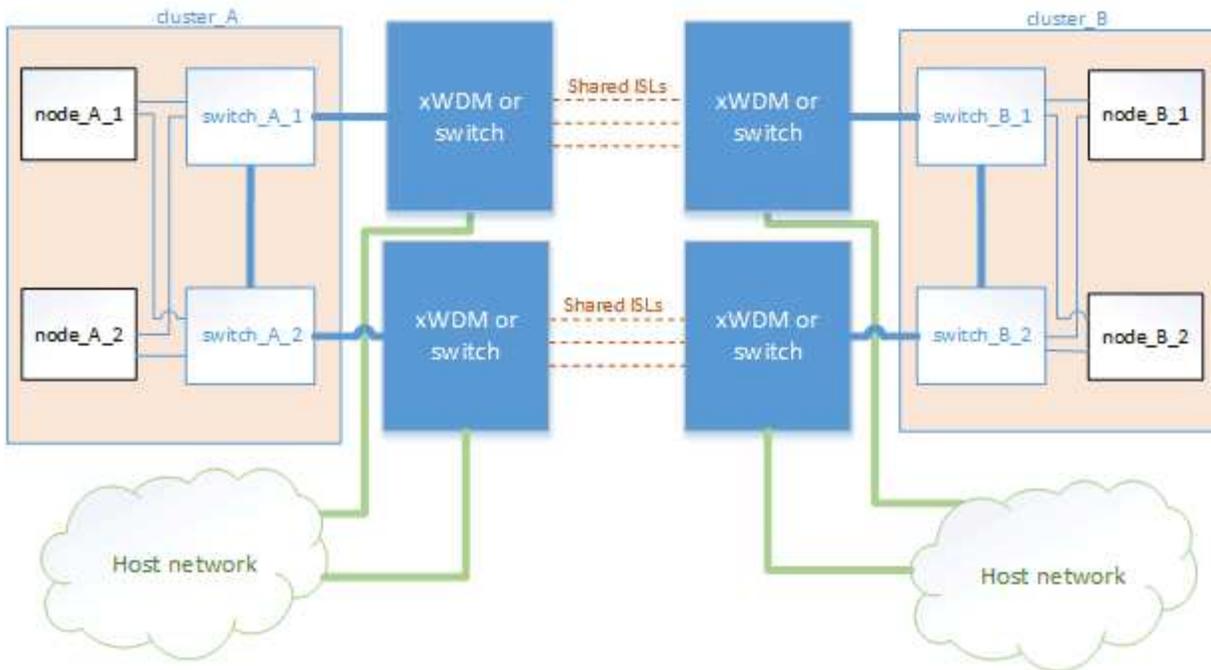
これらのトポロジでは、に記載されている要件に従ってISLと中間ネットワークが設定されていることを前提としています。"[ISLに関する考慮事項](#)"。



MetroCluster以外のトラフィックでISLを共有する場合は、MetroClusterに最小限必要な帯域幅が常に確保されていることを確認する必要があります。

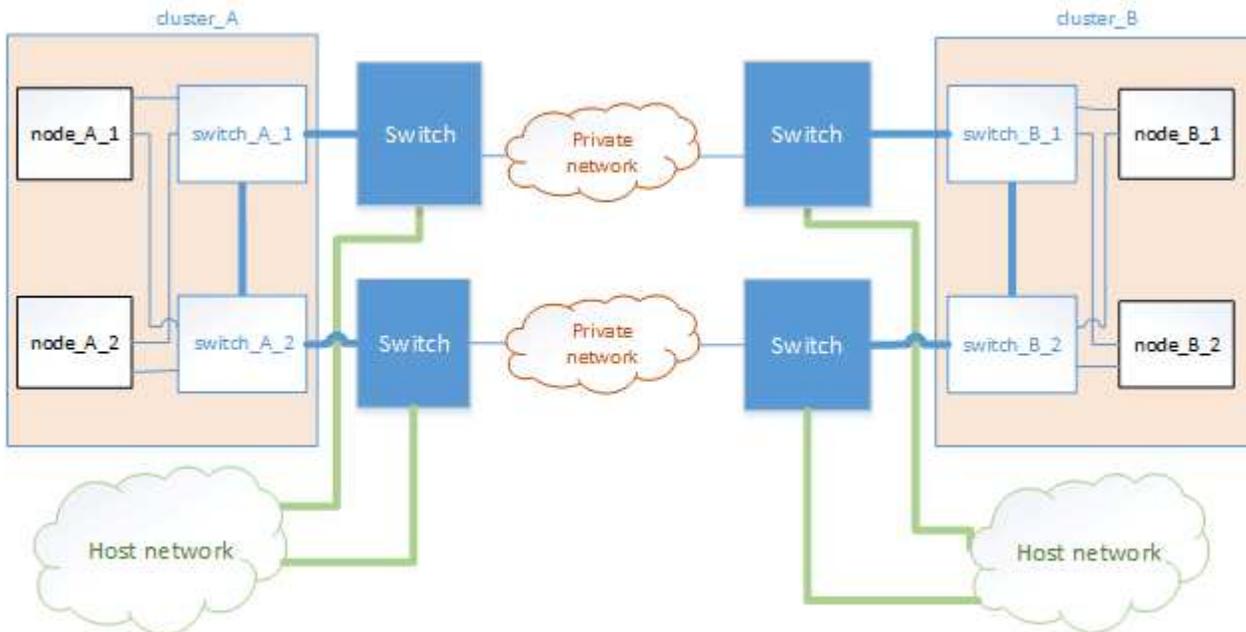
### 直接リンクを使用した共有ネットワーク構成

このトポロジでは、2つのサイトが直接リンクで接続されます。これらのリンクは、xWDMとTDMデバイスまたはスイッチ間に設定できます。ISLの容量はMetroClusterトラフィック専用ではなく、MetroCluster以外の他のトラフィックと共有されます。



中間ネットワークを使用する共有インフラ

このトポロジでは、MetroClusterサイトは直接接続されませんが、MetroClusterとホストトラフィックはネットワークを経由します。ネットワークは一連のxWDMおよびTDMとスイッチで構成できますが、直接ISLを使用した共有構成とは異なり、サイト間のリンクは直接接続ではありません。サイト間のインフラによっては、ネットワーク構成を任意に組み合わせて設定できます。

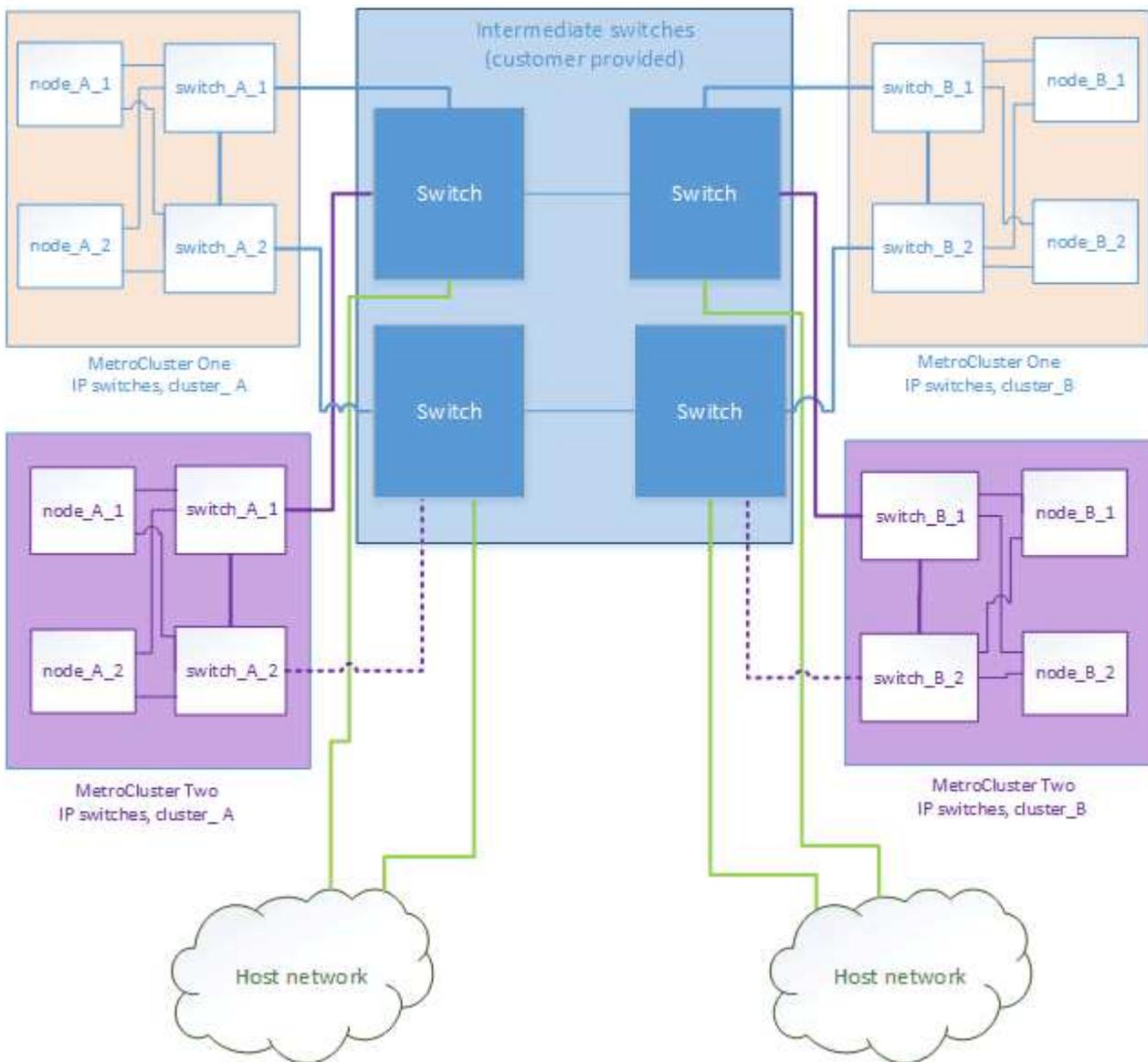


複数のMetroCluster構成で中間ネットワークを共有

このトポロジでは、2つの異なるMetroCluster構成が同じ中間ネットワークを共有しています。この例では、MetroCluster 1のswitch\_A\_1とMetroCluster 2のswitch\_A\_1が同じ中間スイッチに接続されています。

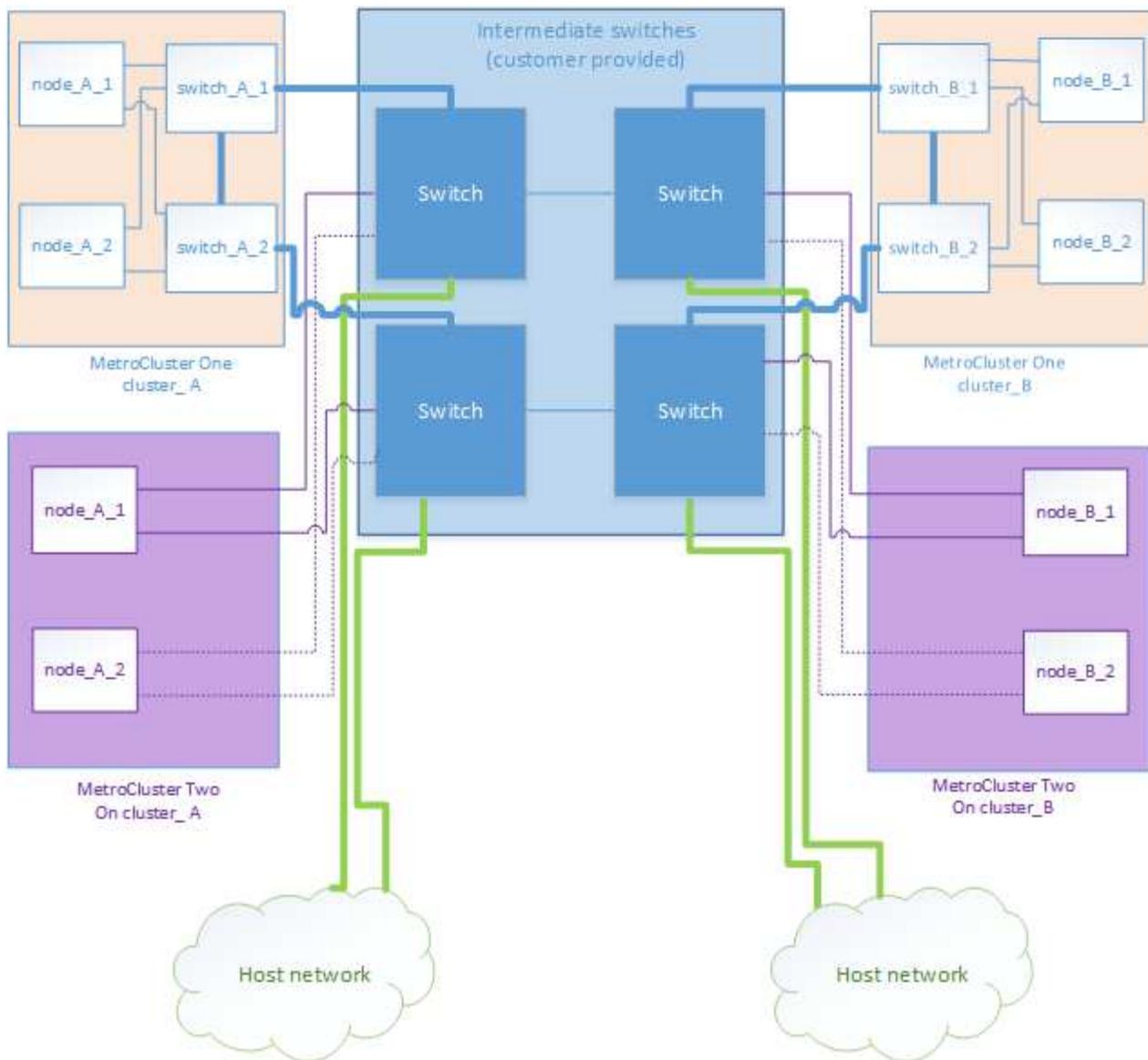


「MetroCluster 1」または「MetroCluster 2」は、どちらも8ノードMetroCluster構成の場合と4ノードMetroCluster構成の場合があります。



#### NetApp検証済みスイッチを使用するMetroCluster構成とMetroCluster準拠スイッチを使用する構成の組み合わせ

2つの異なるMetroCluster構成で同じ中間スイッチを共有します。1つのMetroClusterは共有レイヤ2構成のNetApp検証済みスイッチ（MetroCluster 1）を使用して構成され、もう1つのMetroClusterは、中間スイッチに直接接続されたMetroCluster準拠スイッチ（MetroCluster 2）を使用して構成されます。



## MetroCluster 準拠スイッチの使用に関する考慮事項

### MetroCluster準拠スイッチの要件と制限

ONTAP 9.7以降では、MetroCluster IP構成でMetroClusterに準拠したスイッチを使用できます。ネットアップ検証は実施されていないが、ネットアップの仕様に準拠しているスイッチです。ただし、NetAppでは、検証されていないスイッチのトラブルシューティングサービスや設定サポートサービスは提供されていません。MetroCluster準拠スイッチを使用する場合は、一般的な要件と制限事項を確認しておく必要があります。

### MetroCluster準拠スイッチとネットアップ検証済みスイッチの比較

スイッチが次の要件を満たしている場合、ネットアップで検証されます。

- スイッチは、MetroCluster IP構成の一部としてネットアップから提供されます
- スイッチは、"[NetApp Hardware Universe の略](#)" MetroCluster-over-IP-connections\_でサポートされるスイッチとして使用

- このスイッチは、MetroCluster IPコントローラと、一部の構成ではNS224ドライブシェルフへの接続にのみ使用します
- スイッチは、NetAppが提供するリファレンス構成ファイル（RCF）を使用して設定します。

これらの要件を満たしていないスイッチは、ネットアップの検証済みスイッチではありません。

MetroCluster準拠スイッチはネットアップでは検証されていませんが、一定の要件および構成ガイドラインを満たしていれば、MetroCluster IP構成で使用できます。



NetAppでは、MetroCluster準拠の検証が行われていないスイッチについては、トラブルシューティングや構成のサポートサービスは提供していません。

#### MetroCluster準拠スイッチの一般的な要件

MetroCluster IPインターフェイスを接続するスイッチは、次の一般的な要件を満たしている必要があります。

- スイッチでQuality of Service（QoS；サービス品質）とトラフィック分類がサポートされている必要があります。
- スイッチで Explicit Congestion Notification（ECN；明示的輻輳通知）がサポートされている必要
- パスで順序が維持されるように、スイッチでロードバランシングポリシーがサポートされている必要があります。
- スイッチで L2 Flow Control（L2FC；L2 フロー制御）がサポートされている必要があります。
- スイッチポートは専用のレートを提供する必要があり、過剰に割り当てられないようにする必要があります。
- ノードをスイッチに接続するケーブルとトランシーバは、NetAppから提供する必要があります。これらのケーブルは、スイッチベンダーがサポートしている必要があります。光ケーブルを使用している場合は、スイッチのトランシーバがNetAppから提供されていない可能性があります。コントローラのトランシーバと互換性があることを確認する必要があります。
- MetroClusterノードを接続するスイッチは、MetroCluster以外のトラフィックを伝送できます。
- MetroCluster準拠のスイッチで使用できるのは、スイッチレスクラスインターコネクト専用ポートを提供するプラットフォームのみです。FAS2750やAFF A220などのプラットフォームは、MetroCluster トラフィックとMetroCluster インターコネクトトラフィックが同じネットワークポートを共有しているため使用できません。
- MetroCluster準拠のスイッチをローカルクラスタ接続に使用しないでください。
- MetroCluster IP インターフェイスは、要件を満たすように設定できる任意のスイッチポートに接続できます。
- スイッチファブリックごとに2つ、計4つのIPスイッチが必要です。ダイレクタを使用する場合は'各側で1つのダイレクタを使用できますが' MetroCluster IPインタフェースは'そのダイレクタ上の2つの異なる障害ドメインにある2つの異なるブレードに接続する必要があります
- 1つのノードのMetroClusterインターフェイスは、2つのネットワークスイッチまたはブレードに接続する必要があります。1つのノードのMetroClusterインターフェイスを同じネットワーク、スイッチ、またはブレードに接続することはできません。
- ネットワークは、次のセクションで説明する要件を満たしている必要があります。
  - ["ISL に関する考慮事項"](#)
  - ["共有レイヤ2またはレイヤ3ネットワークにMetroClusterを導入する際の考慮事項"](#)

- MetroCluster IPトラフィックを伝送するすべてのスイッチで、Maximum Transmission Unit (MTU;最大伝送ユニット) 9216を設定する必要があります。
- ONTAP 9.6以前へのリポートはサポートされていません。

両方のサイトのMetroCluster IPインターフェイスを接続するスイッチ間で使用する中間スイッチは、要件を満たし、に記載されているように設定する必要があります。"[共有レイヤ2またはレイヤ3ネットワークにMetroClusterを導入する際の考慮事項](#)"。

#### MetroCluster準拠スイッチを使用する場合の制限事項

ローカルクラスタ接続をスイッチに接続する必要がある設定や機能は使用できません。たとえば、MetroCluster準拠スイッチでは、次の構成や手順を使用できません。

- 8 ノード MetroCluster 構成
- MetroCluster FC から MetroCluster IP 構成への移行
- 4 ノード MetroCluster IP 設定の更新
- ローカルクラスタとMetroClusterトラフィックで物理インターフェイスを共有するプラットフォーム。を参照してください "[MetroCluster準拠スイッチのプラットフォーム固有のネットワーク速度とスイッチポートモード](#)" サポートされている速度の場合。

#### MetroCluster準拠スイッチのONTAPプラットフォーム固有のネットワーク速度とスイッチポートモード

MetroCluster準拠のスイッチを使用している場合は、プラットフォーム固有のネットワーク速度とスイッチポートモードの要件を確認しておく必要があります。

次の表に、MetroCluster準拠スイッチのネットワーク速度とスイッチポートモードをプラットフォーム別に示します。表に従ってスイッチポートモードを設定する必要があります。



- 値がない場合は、プラットフォームをMetroCluster準拠のスイッチで使用できないことを示しています。
- AFF A30、AFF C30、AFF C60、およびFAS50のシステムで25Gbpsのネットワーク速度をサポートするには、コントローラのカードにQSFP-SFP+アダプタが必要です。

Platform	Network Speed (Gbps)	Switch port mode
FAS9500 AFF A900 ASA A900	100Gbps 40Gbps when upgrade PCM from FAS9000 / AFF A700	trunk mode
AFF C800 ASA C800 AFF A800 ASA A800	40Gbps or 100Gbps	access mode
FAS9000 AFF A700	40Gbps	access mode
FAS8300 AFF C400 ASA C400 AFF A400 ASA A400	40Gbps or 100Gbps	trunk mode
AFF A320	40Gbps or 100Gbps	access mode
FAS8200 AFF A300	25Gbps	access mode
FAS500f AFF C250 ASA C250 AFF A250 ASA A250	-	-
FAS2750 AFF A220	-	-
AFF A150 ASA A150	-	-
AFF A20	25Gbps	trunk mode
AFF A30	25Gbps or 100Gbps	trunk mode
AFF C30	25Gbps or 100Gbps	trunk mode
AFF C60	25Gbps or 100Gbps	trunk mode
FAS50	25Gbps or 100Gbps	trunk mode
AFF A50	100Gbps	trunk mode
AFF A70	100Gbps	trunk mode
AFF A90	100Gbps	trunk mode
AFF A1K	100Gbps	trunk mode
AFF C80	100Gbps	trunk mode
FAS70	100Gbps	trunk mode
FAS90	100Gbps	trunk mode

## MetroCluster IPスイッチの構成例

さまざまなスイッチポートの構成について説明します。



次の例では、10進数の値を使用して、環境Ciscoスイッチの表に従っています。スイッチベンダーによっては、DSCPに異なる値が必要になる場合があります。値が正しいことを確認するには、スイッチベンダーに対応する表を参照してください。

DSCP値	10進数	16進	意味
101、000	16	0x10	CS2
011、000	24	0x18	CS3
100、000	32	0x20	CS4
101、000	40	0x28	CS5

### MetroClusterインターフェイスを接続するスイッチポート

- リモートダイレクトメモリアクセス (RDMA) トラフィックの分類：
  - 一致：TCPポート10006、送信元、宛先、またはその両方
  - オプションマッチ：COS 5
  - オプション照合：DSCP 40
  - DSCP 40の設定
  - COS 5の設定
  - オプション：20Gbpsへのレートシェーピング
- iSCSIトラフィックの分類：
  - 一致：TCPポート62500、送信元、宛先、またはその両方
  - オプションマッチ：COS 4
  - オプション照合:DSCP 32
  - DSCP 32の設定
  - COS 4の設定
- L2FlowControl (PAUSE) 、RXおよびTX

### ISL ポート数

- 分類：
  - COS 5またはDSCP 40と一致
    - DSCP 40の設定
    - COS 5の設定
  - COS 4またはDSCP 32と一致

- DSCP 32の設定
- COS 4の設定
- 出力キューイング
  - CoSグループ4の最小設定しきい値は2000、最大しきい値は3000です。
  - CoSグループ5の最小設定しきい値は3500、最大しきい値は6500です。



構成のしきい値は環境によって異なります。構成のしきい値は個々の環境に基づいて評価する必要があります。

- Q4およびQ5でECNが有効
- 第4四半期と第5四半期に赤が有効

帯域幅の割り当て（MetroClusterインターフェイスとISLポートを接続するスイッチポート）

- RDMA、COS 5 / DSCP 40：60%
- iSCSI、COS 4 / DSCP 32：40%
- MetroCluster構成およびネットワークごとの最小容量要件：10Gbps



レート制限を使用する場合は、トラフィックを損失なしに\*シェーピング\*する必要があります。

**MetroCluster**コントローラを接続するスイッチポートの設定例

ここに示すコマンド例は、Cisco NX3232スイッチまたはCisco NX9336スイッチに有効です。コマンドは、スイッチタイプによって異なります。

例に示されている機能または同等の機能がスイッチで使用できない場合、スイッチは最小要件を満たしておらず、MetroCluster構成の導入に使用することはできません。これは、MetroCluster構成に接続するすべてのスイッチ、およびすべての中間スイッチに当てはまります。



次の例では、1つのネットワークの構成しか表示されていません。

キホンセツテイ

各ネットワークに仮想LAN（VLAN）を設定する必要があります。次に、ネットワーク10にVLANを設定する例を示します。

- 例：\*

```
# vlan 10
The load balancing policy should be set so that order is preserved.
```

- 例：\*

```
# port-channel load-balance src-dst ip-l4port-vlan
```

## 分類の設定例

RDMAおよびiSCSIトラフィックを適切なクラスにマッピングするには、アクセスマップとクラスマップを設定する必要があります。

次の例では、ポート65200との間のすべてのTCPトラフィックをストレージ (iSCSI) クラスにマッピングします。ポート 10006 を経由するすべての TCP トラフィックを RDMA クラスにマッピングします。これらのポリシーマップは、MetroClusterインターフェイスを接続するスイッチポートで使用されます。

- 例： \*

```
ip access-list storage
  10 permit tcp any eq 65200 any
  20 permit tcp any any eq 65200
ip access-list rdma
  10 permit tcp any eq 10006 any
  20 permit tcp any any eq 10006

class-map type qos match-all storage
  match access-group name storage
class-map type qos match-all rdma
  match access-group name rdma
```

入力ポリシーを設定する必要があります。入力ポリシーは、異なるCOSグループに分類されたトラフィックをマッピングします。この例では、RDMAトラフィックをCOSグループ5にマッピングし、iSCSIトラフィックをCOSグループ4にマッピングしています。入力ポリシーは、MetroClusterインターフェイスを接続するスイッチポートおよびMetroClusterトラフィックを伝送するISLポートで使用されます。

- 例： \*

```
policy-map type qos MetroClusterIP_Node_Ingress
class rdma
  set dscp 40
  set cos 5
  set qos-group 5
class storage
  set dscp 32
  set cos 4
  set qos-group 4
```

NetAppでは、次の例に示すように、MetroClusterインターフェイスを接続するスイッチポートでトラフィックをシェーピングすることを推奨しています。

- 例： \*

```
policy-map type queuing MetroClusterIP_Node_Egress
class type queuing c-out-8q-q7
  priority level 1
class type queuing c-out-8q-q6
  priority level 2
class type queuing c-out-8q-q5
  priority level 3
  shape min 0 gbps max 20 gbps
class type queuing c-out-8q-q4
  priority level 4
class type queuing c-out-8q-q3
  priority level 5
class type queuing c-out-8q-q2
  priority level 6
class type queuing c-out-8q-q1
  priority level 7
class type queuing c-out-8q-q-default
  bandwidth remaining percent 100
  random-detect threshold burst-optimized ecn
```

#### ノードポートの設定例

ノードポートをブレイクアウトモードで設定しなければならない場合があります。次の例では、ポート25と26が4つの25Gbpsブレイクアウトモードで設定されています。

- 例： \*

```
interface breakout module 1 port 25-26 map 25g-4x
```

MetroCluster インターフェイスポート速度の設定が必要になる場合があります。次に、速度を\*auto\*または40Gbpsモードに設定する例を示します。

- 例： \*

```
speed auto

speed 40000
```

次の例は、MetroClusterインターフェイスを接続するように設定されたスイッチポートを示しています。VLAN 10のアクセスモードポートで、MTUは9216で、ネイティブ速度で動作しています。対称（送受信）フロー制御（PAUSE）がイネーブルで、MetroCluster入力および出力ポリシーが割り当てられています。

- 例： \*

```
interface eth1/9
description MetroCluster-IP Node Port
speed auto
switchport access vlan 10
spanning-tree port type edge
spanning-tree bpduguard enable
mtu 9216
flowcontrol receive on
flowcontrol send on
service-policy type qos input MetroClusterIP_Node_Ingress
service-policy type queuing output MetroClusterIP_Node_Egress
no shutdown
```

25Gbpsポートでは、次の例に示すように、前方誤り訂正（FEC）設定を「off」に設定する必要があります。

• 例：\*

```
fec off
```

ネットワーク全体でのISLポートの設定例

MetroCluster準拠スイッチは、MetroClusterインターフェイスを直接接続するスイッチであっても、中間スイッチとみなされます。MetroCluster準拠スイッチでMetroClusterトラフィックを伝送するISLポートは、中間スイッチのISLポートと同じように設定する必要があります。を参照してください "[中間スイッチに必要な設定](#)" を参照してください。



一部のポリシーマップは、MetroClusterインターフェイスを接続するスイッチポートと、MetroClusterトラフィックを伝送するISLで同じです。これらの両方のポート使用に同じポリシーマップを使用できます。

## MetroCluster IP構成におけるミラーリングされていないアグリゲートについて学習します

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後にアクセスに関する問題が発生する可能性があります。

### ミラーリングされていない集約と階層型名前空間

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

### ミラーリングされていないアグリゲートと電源シャットダウンを必要とするメンテナンス

サイト全体の電源シャットダウンを必要とする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、まず災害サイトが所有するミラーリング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。

ディザスタサイトが所有するミラーリングされていないアグリゲートをオフラインにしないと、マルチディスクパニックにより、サバイバルサイトのノードがダウンする可能性があります。これは、電源のシャットダウンやISLの損失により、スイッチオーバーされたミラーリングされていないアグリゲートがオフラインになったり、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欠落したりした場合に発生する可能性があります。

ミラーリング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

構成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、ミラーリングされたアグリゲート上に配置する必要があります。ミラーリング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。されていないアグリゲート上に配置されている場合、ネゴシエートされたスイッチオーバーおよびスイッチバック操作は拒否され、`metrocluster check` コマンドは警告を返します。

ミラーリングされていないアグリゲートと**SVM**

SVMは、ミラーリングされたアグリゲートのみ、またはミラーリングされていないアグリゲートだけに設定する必要があります。ミラーリングされていないアグリゲートとミラーリングされたアグリゲートの両方にSVMを設定すると、スイッチオーバー処理に120秒を超える時間がかかる場合があります。ミラーリング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、データ障害が発生する可能性があります。

ミラーリングされていないアグリゲートと**SAN**

ONTAP 9.9.1より前のバージョンでは、LUNをミラーリングされていないアグリゲート上に配置しないでください。ミラーリングされていないアグリゲート上にLUNを設定すると、スイッチオーバー処理に120秒以上かかり、データが停止する可能性があります。

ミラーリングされていないアグリゲート用のストレージシェルフを追加する

シェルフを追加し、MetroCluster IP 構成内のミラーリングされていないアグリゲートに使用する場合は、次の手順を実行する必要があります。

1. 手順を開始してシェルフを追加する前に、次のコマンドを問題に設定します。

```
MetroCluster modify -enable -ミラー されていない -aggr-deployment true
```

2. ディスクの自動割り当てが無効になっていることを確認します。

「ディスクオプション表示」

3. 手順の手順に従ってシェルフを追加します。
4. 新しいシェルフのすべてのディスクを、ミラーされていないアグリゲートまたはアグリゲートを所有するノードに手動で割り当てます。
5. アグリゲートを作成します。

```
「 storage aggregate create 」
```

6. 手順が完了したら、次のコマンドを問題に設定します。

MetroCluster modify -enable -ミラー されていない -aggr-deployment false

7. ディスクの自動割り当てが有効になっていることを確認します。

「ディスクオプション表示」

## MetroCluster IP構成のファイアウォール ポート要件

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

### 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。

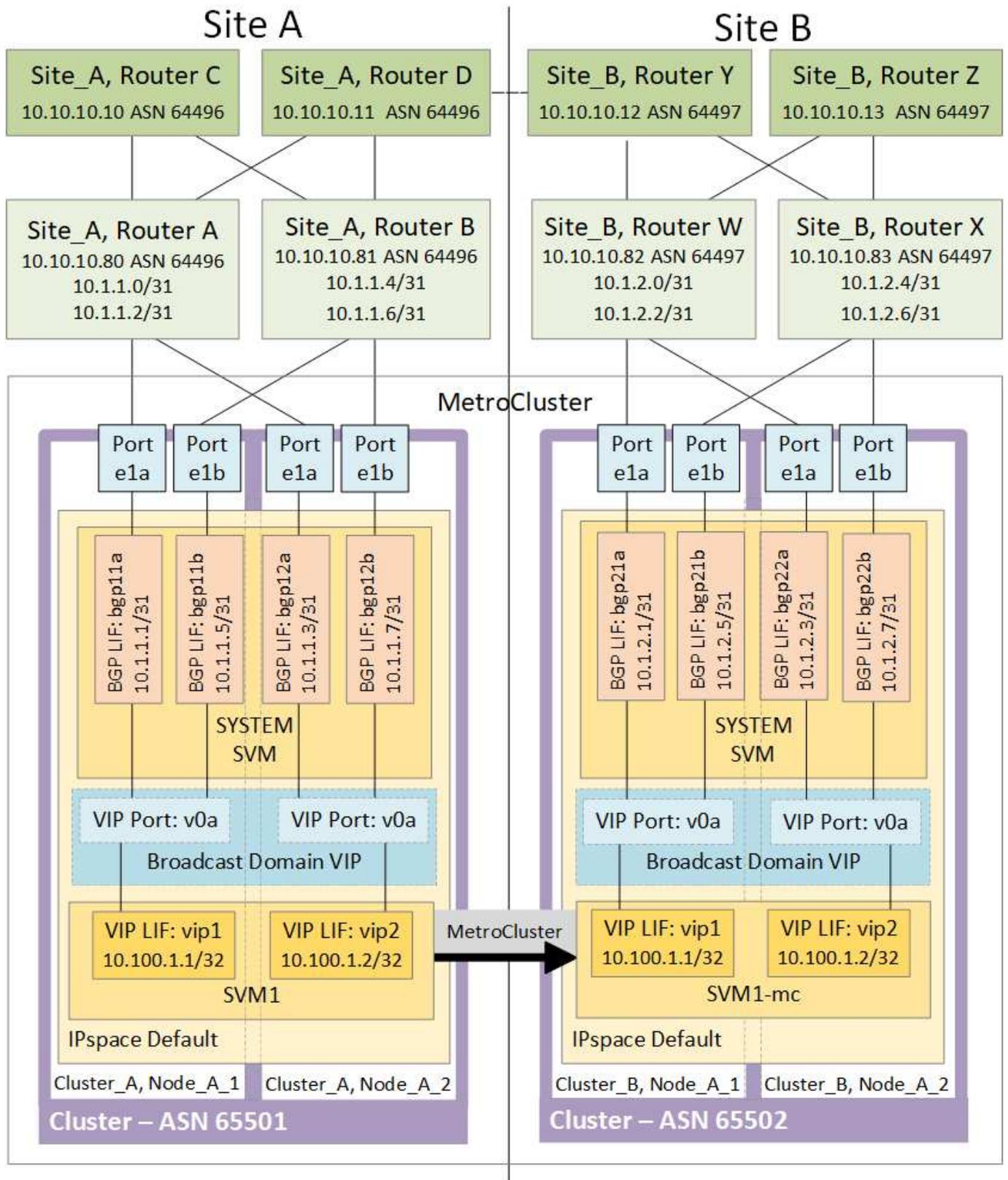
トラフィックタイプ	ポート / サービス
クラスタピアリング	11104/TCP
	11105/TCP
ONTAP システムマネージャ	443 / TCP
MetroCluster IP のクラスタ間 LIF	65200/TCP
	10006/TCP および UDP
ハードウェアアシスト	4444/TCP

**MetroCluster IP構成で仮想IPとボーダーゲートウェイプロトコルを使用する方法について学習します。**

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。9.8 では、BGP LIF がクラスタ（システム）SVM 内で認識され、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）が存在することで接続が継続的に検証され、LIFの移行やフェイルオーバーが正常に実行されます（L2では、破損した構成がシステム停止後にしか認識されません）。

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 ハードウェアコンポーネントを設定します

**MetroCluster IP**構成におけるハードウェアコンポーネントの相互接続について学習します。

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

## 主要なハードウェア要素

MetroCluster IP の設定には、次の主要なハードウェア要素が含まれます。

- ストレージコントローラ

ストレージコントローラは 2 つの 2 ノードクラスタとして構成されます。

- IP ネットワーク

このバックエンド IP ネットワークは、次の 2 つの用途に接続を提供します。

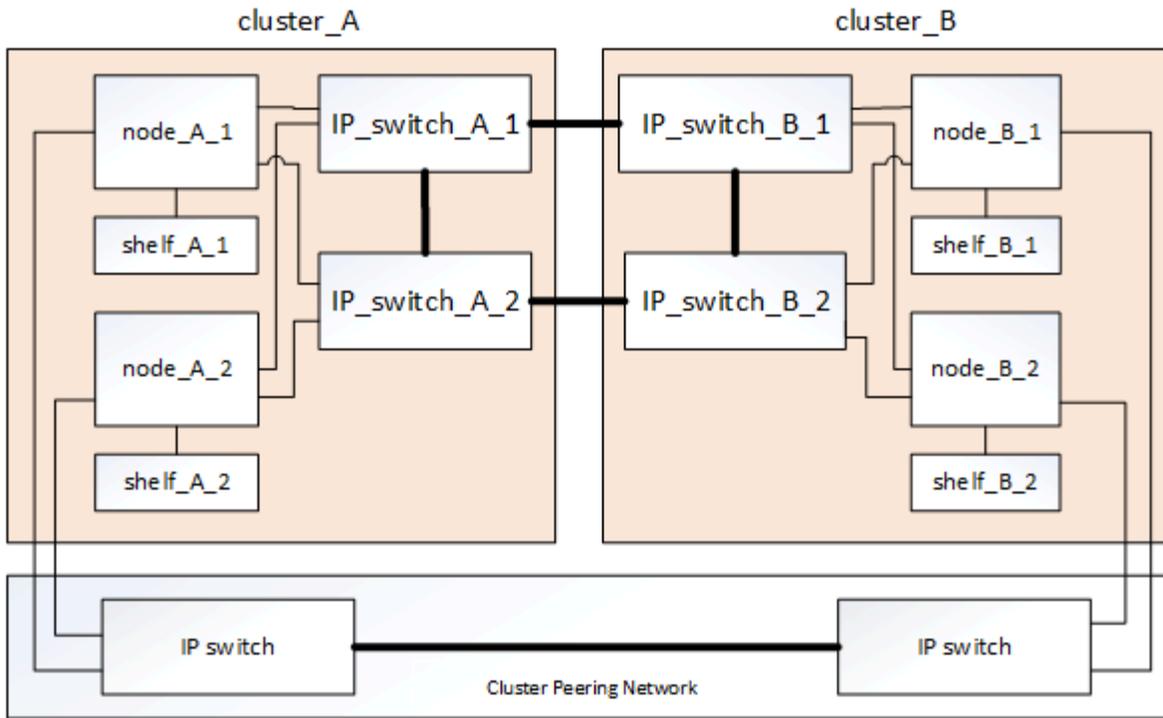
- クラスタ内通信用の標準クラスタ接続。

これは、MetroCluster 以外の ONTAP スイッチクラスタで使用されるクラスタスイッチ機能と同じです。

- ストレージデータと不揮発性キャッシュのレプリケーション用の MetroCluster バックエンド接続。

- クラスタピアリングネットワーク

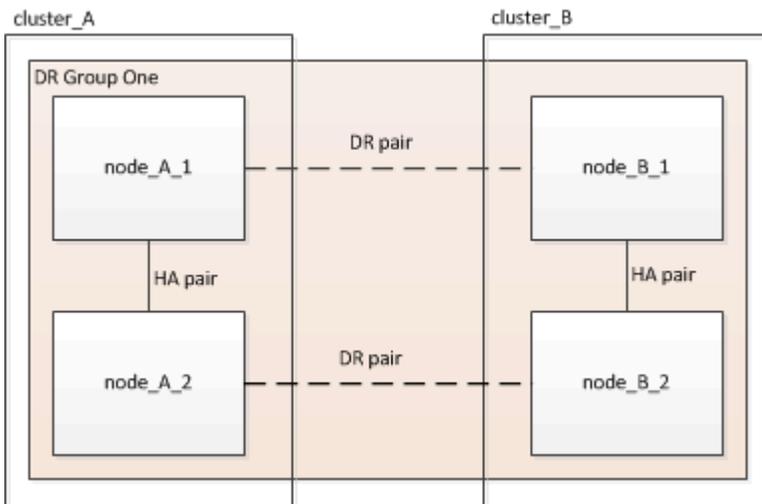
クラスタピアリングネットワークは、Storage Virtual Machine (SVM) の設定を含むクラスタ構成をミラーするための接続を提供します。一方のクラスタのすべての SVM の設定が、パートナークラスタにミラーされます。



### ディザスタリカバリ（DR）グループ

MetroCluster IP 構成は、4 つのノードからなる 1 つの DR グループで構成されます。

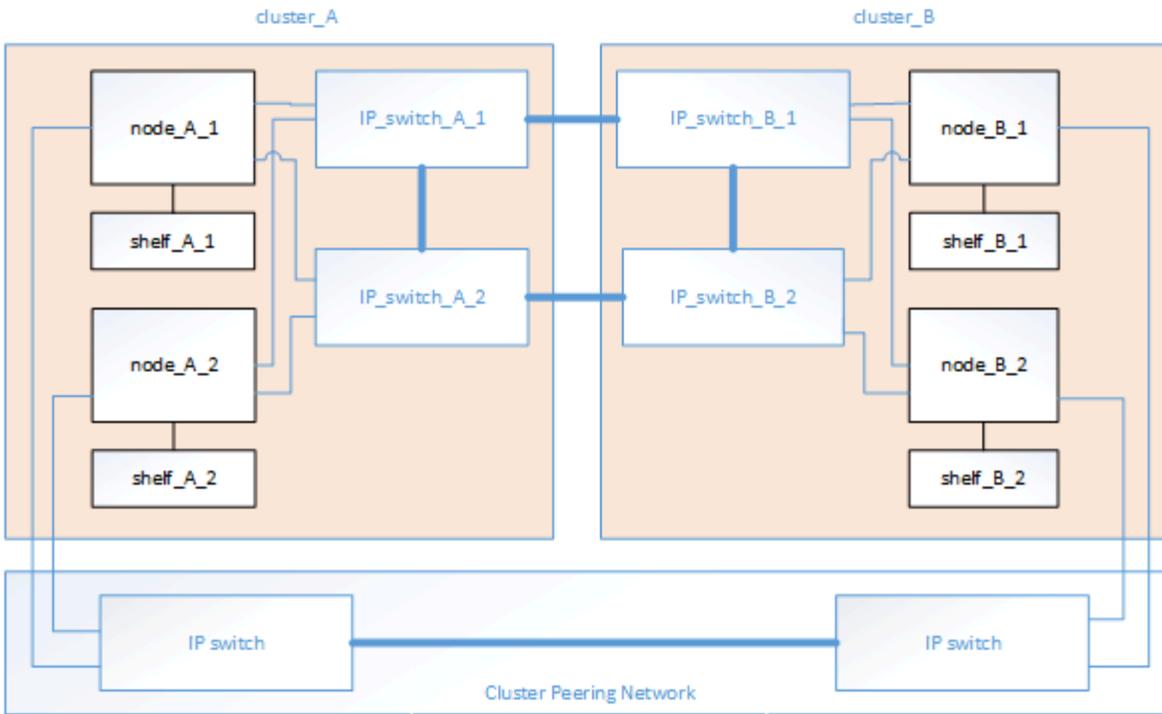
次の図は、4 ノード MetroCluster 構成におけるノードの編成を示しています。



### MetroCluster 構成のローカル HA ペアの図

各 MetroCluster サイトは、HA ペアとして構成されているストレージコントローラで構成されています。これによってローカルでの冗長性が実現し、一方のストレージコントローラに障害が発生した場合はローカルの HA パートナーがテイクオーバーできるようになります。このような障害には、MetroCluster のスイッチオーバー処理は必要ありません。

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

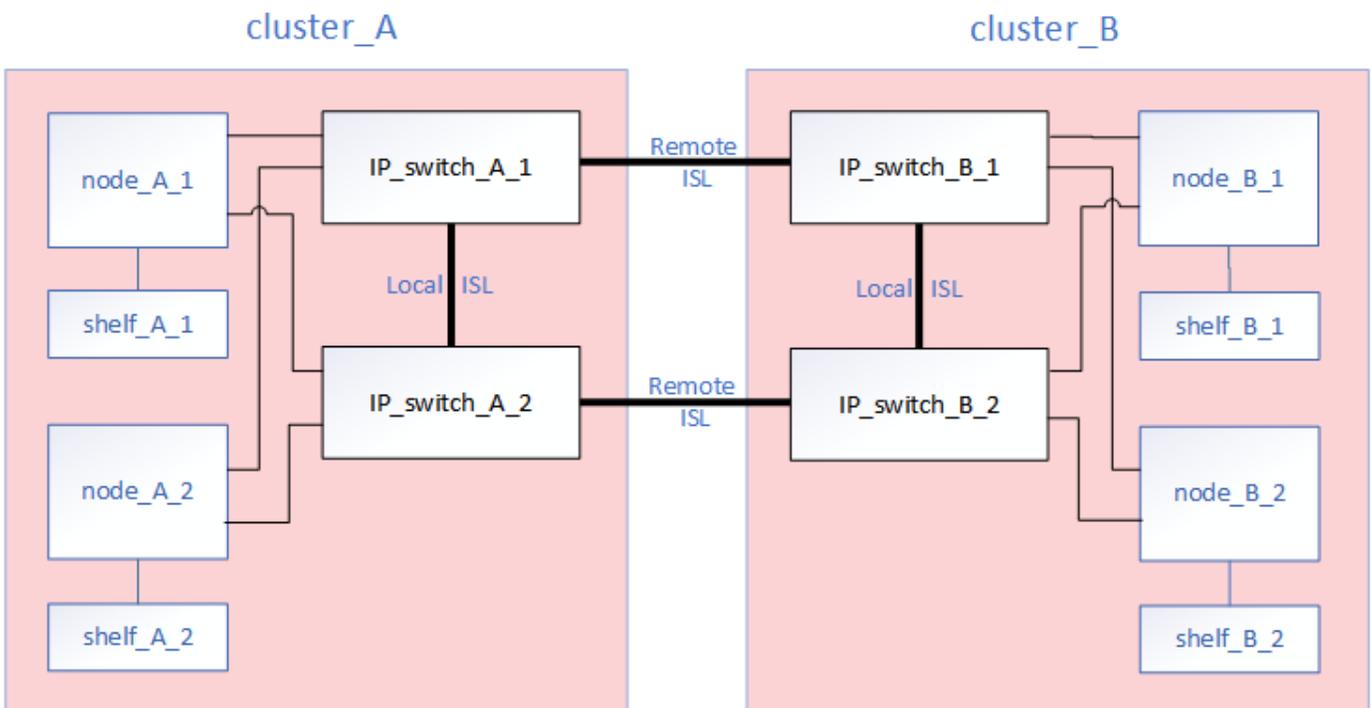


関連情報

"ONTAP の概念"

### MetroCluster IP およびクラスターインターコネクトネットワークの図

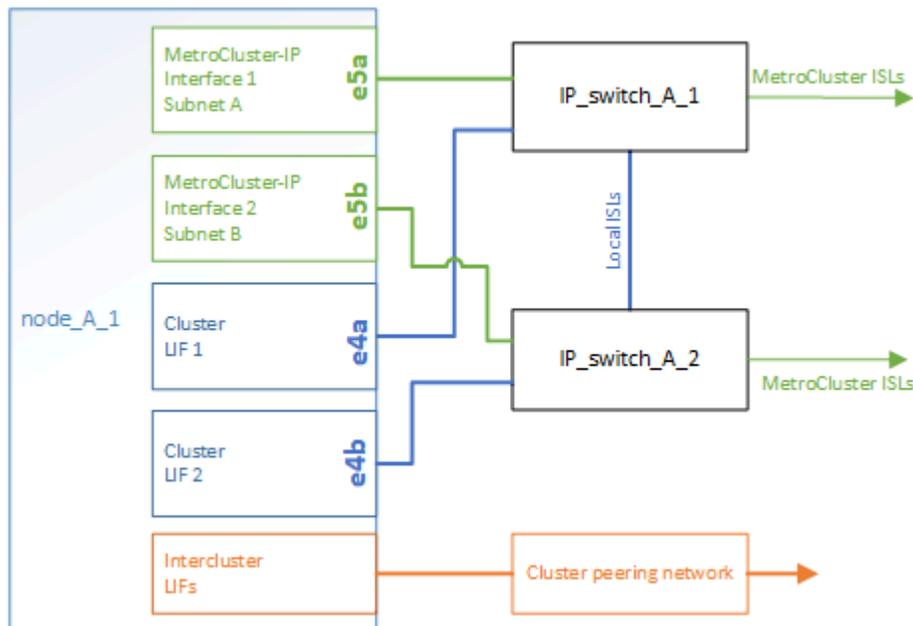
ONTAP クラスタには、通常、クラスター内のノード間のトラフィック用にクラスターインターコネクトネットワークが含まれています。MetroCluster IP 構成では、MetroCluster サイト間のデータレプリケーショントラフィックにもこのネットワークが使用されます。



MetroCluster IP構成の各ノードには、バックエンドIPネットワークに接続するための専用のインターフェイスがあります。

- 2つの MetroCluster IP インターフェイス
- 2つのローカルクラスタインターフェイス

これらのインターフェイスを次の図に示します。ポートの用途はAFF A700 または FAS9000 システムの場合のものです。



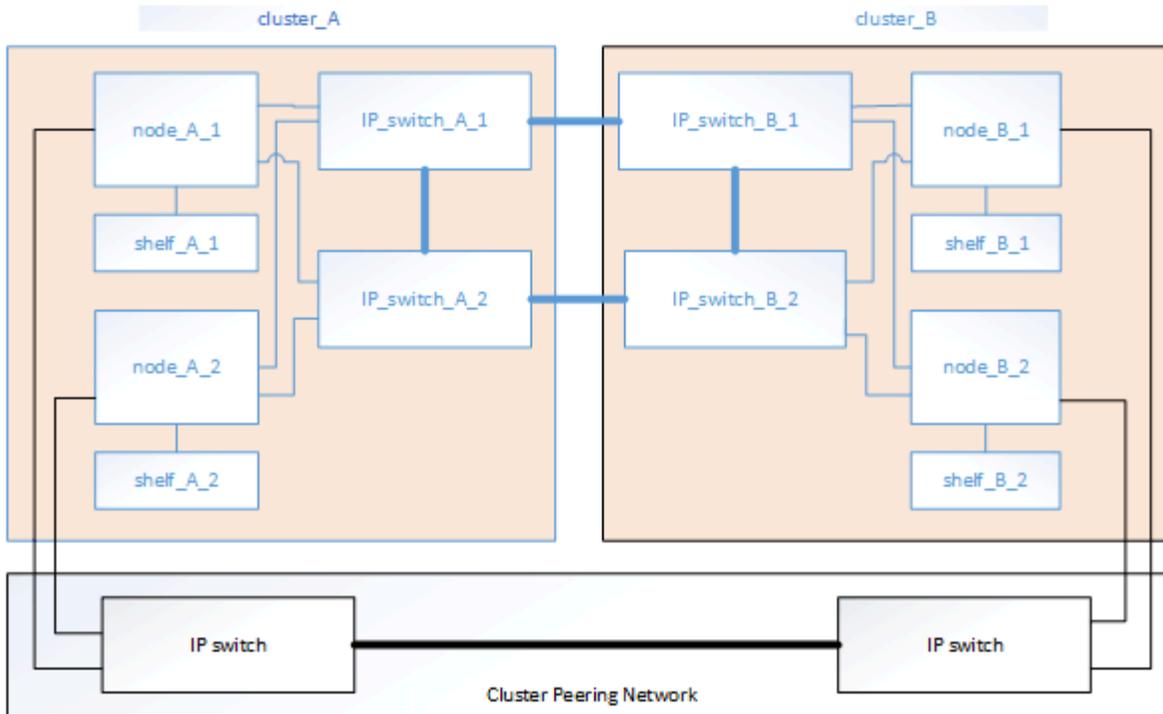
#### 関連情報

["MetroCluster IP 構成に関する考慮事項"](#)

#### クラスタピアリングネットワークの図

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

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



## 関連情報

"クラスタと SVM のピアリングの簡単な設定"

"クラスタピアリングの設定に関する考慮事項"

"クラスタピアリングのケーブル接続"

"クラスタをピアリング"

## 必要なMetroCluster IP 構成コンポーネントと命名規則

MetroCluster IP 構成に必要な、サポートされているハードウェアおよびソフトウェア コンポーネントを特定します。ドキュメントの例でコンポーネントに使用されている命名規則を確認します。

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 IP 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 IP 構成でのハードウェアの冗長性要件

MetroCluster IP 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。

## MetroCluster IP 構成での ONTAP クラスタの要件

MetroCluster IP 構成には、MetroCluster サイトごとに 1 つ、計 2 つの ONTAP クラスタが必要です。

名前は MetroCluster 構成内で一意である必要があります。

名前の例：

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

## MetroCluster IP 構成での IP スイッチの要件

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

IP スイッチは、各クラスタのコントローラモジュール間のクラスタ内通信も提供します。

名前は MetroCluster 構成内で一意である必要があります。

名前の例：

- サイト A : cluster\_A
  - IP\_switch\_A\_1
  - IP\_switch\_a\_2
- サイト B : cluster\_B
  - IP\_switch\_B\_1
  - IP\_switch\_B\_2

## MetroCluster IP 構成でのコントローラモジュールの要件

MetroCluster IP 構成には、コントローラモジュールが 4 つまたは 8 つ必要です。

各サイトのコントローラモジュールが HA ペアを形成します。各コントローラモジュールには、もう一方のサイトに DR パートナーがあります。

各コントローラモジュールが同じバージョンの ONTAP を実行している必要があります。サポートされるプラットフォームモデルは ONTAP のバージョンによって異なります。

- FAS システムへの MetroCluster IP の新規インストールは、ONTAP 9.4 ではサポートされません。  
FAS システムの既存の MetroCluster IP 構成を ONTAP 9.4 にアップグレードすることはできます。
- ONTAP 9.5 以降では、FAS システムへの MetroCluster IP の新規インストールがサポートされます。
- ONTAP 9.4 以降では、ADP 用に設定されたコントローラモジュールがサポートされます。

名前の例

このドキュメントでは、次のような名前を使用しています。

- サイト A : cluster\_A
  - controller\_A\_1
  - controller\_A\_2
- サイト B : cluster\_B
  - controller\_B\_1
  - controller\_B\_2

### MetroCluster IP 構成でのギガビットイーサネットアダプタの要件

MetroCluster IP 構成では、MetroCluster IP ファブリックに使用される IP スイッチへの IP インターフェイスに 40/100Gbps または 10/25Gbps のイーサネットアダプタを使用します。



オンボードポートはコントローラハードウェア（スロット0）に組み込まれており、交換できないため、アダプタに必要なスロットは使用できません。

プラットフォームモデル	必要なギガビットイーサネットアダプタ	アダプタに必要なスロット	ポート
AFF A900、ASA A900、およびFAS9500	X91146A	スロット 5、スロット 7	e5b、e7b  注: ポートe5aとe7aはクラスタ間LIFにのみ使用できます。これらのポートをデータLIFに使用することはできません。
AFF A700 および FAS9000	X91146A-C	スロット 5	e5b、e5b
AFF A800、AFF C800、ASAA800、およびASA C800	X1146A / オンボードポート	スロット1/オンボードポートには適用されません。	e0be1b
FAS8300、AFF A400、ASAA400、ASA C400、AFF C400	X1146A	スロット 1	e1A、e1b
AFF A300、FAS8200	X1116A	スロット 1	e1A、e1b
FAS2750、AFF A150、ASAA150、AFF A220	オンボードポート	該当なし	e0a、e0b
FAS500f、AFF A250、ASAA250、ASA C250、AFF C250	オンボードポート	該当なし	e0c、e0d

AFF A320	オンボードポート	該当なし	e0g、e0h
AFF A70、FAS70、AFF C80	X50132A	スロット2	e2a、e2b
AFF A90、AFF A1K、FAS90	X50132A	スロット2、スロット3	e2b、e3b  *注：*ポートe2aおよびe3aは未使用のままにする必要があります。これらのポートをフロントエンドネットワークまたはピアリングに使用することはできません。
AFF A50用	X60134A	スロット2	e2a、e2b
AFF A30、AFF C30、AFF C60、FAS50	X60134A	スロット2	e2a、e2b
AFF A20用	X60132A	スロット4、スロット2	e2b、e4b

#### "MetroCluster IP構成での自動ドライブ割り当てとADPシステムの概要"。

#### プールとドライブの要件（最小サポート）

4 ノード MetroCluster IP 構成では、各サイトに次の最小構成が必要です。

- 各ノードのサイトに少なくとも 1 つのローカルプールと 1 つのリモートプールがあります。
- 各プールに少なくとも 7 本のドライブ。

各ノードにミラーされたデータアグリゲートが 1 つある 4 ノード MetroCluster 構成では、最小構成として 24 本のディスクがサイトに必要です。



アグリゲート名は、MetroClusterサイト全体で一意である必要があります。つまり、サイト A とサイト B に同じ名前を持つ 2 つの異なるデータアグリゲートを持つことはできません。

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

- ルートドライブ × 3 本
- 3 本のデータドライブ
- スペアドライブ × 1 本

サポートされる最小構成では、各サイトに少なくとも 1 台のシェルフが必要です。

MetroCluster 構成は、RAID-DP、RAID4、および RAID-TEC をサポートします。



ONTAP 9.4以降のMetroCluster IP構成では、自動ディスク割り当てとアドバンスドドライブパーティショニングを使用した新規インストールがサポートされます。詳細については、を参照してください "[自動ドライブ割り当てとADPシステムに関する考慮事項](#)"。

### 空きのあるシェルフでのドライブの配置場所に関する考慮事項

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

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

### AFF A800 内蔵ドライブの場所に関する考慮事項

ADP 機能を正しく実装するためには、AFF A800 システムのディスクスロットを 4 分割し、それぞれにディスクを対称的に配置する必要があります。

AFF A800 システムには 48 個のドライブベイがあります。ベイは 4 分の 1 に分割できます。

- 第 1 クォータ：
  - ベイ 0~5
  - ベイ 24-29
- 第 2 クォータ：
  - ベイ 6-11
  - ベイ 30-35
- 第 3 クォータ：
  - ベイ 12~17
  - ベイ 36-41
- 第 4 クォータ：
  - ベイ 18-23
  - ベイ 42-47

このシステムに 16 本のドライブを搭載する場合、各クォータに次のように対称的にドライブを配置する必要があります。

- 第 1 クォータに 4 本のドライブ： 0、 1、 2、 3
- 第 2 クォータに 4 本のドライブ： 6、 7、 8、 9
- 第 3 クォータに 4 本のドライブ： 12、 13、 14、 15
- 第 4 クォータに 4 本のドライブ： 18、 19、 20、 21

### MetroCluster IP構成ハードウェアコンポーネントをラックに収納する

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

このタスクについて

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

手順

1. MetroCluster コンポーネントの配置を計画します。

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

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

インストールとセットアップの手順に従って、プラットフォームモデルのハードウェアのインストールを実行してください。"[ONTAPハードウェア システムのドキュメント](#)"。

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

- 各ディスクシェルフの電源を再投入する必要があります。
- トラブルシューティングに役立てるため、各 MetroCluster DR グループ内の各 SAS ディスクシェルフには、シェルフ ID を一意にすることを強く推奨します。



ミラーされていないアグリゲートが含まれるディスクシェルフは、この時点ではケーブル接続しないでください。MetroCluster 構成が完了するまで、ミラーされていないアグリゲート用のシェルフを配置し、「MetroCluster modify -enable -munSHELved-aggr -deployment true」コマンドを使用した後にのみ配置する必要があります。

## MetroCluster IP スwitchをケーブル接続します

複数のMetroCluster IP構成でポートテーブルを使用する方法

RCF ファイルを正しく生成するためには、ポートテーブル内の情報の使用方法を理解しておく必要があります。

作業を開始する前に

表を使用する前に、次の考慮事項を確認してください。

- 次の表は、サイト A で使用するポートを示しています。サイト B でも同じケーブル接続が使用されます。
- 異なる速度のポート (たとえば、100 Gbps ポートと 40 Gbps ポートの混在) を持つスイッチを構成することはできません。
- MetroClusterポートグループ (MetroCluster 1、MetroCluster 2など) を記録しておいてください。この設定手順の後半で説明するRcfFileGeneratorツールを使用する際に、この情報が必要になります。
- すべてのノードを同じ方法でケーブル接続する必要があります。ノードのケーブル接続に使用できるポートの組み合わせオプションが異なる場合は、すべてのノードで同じポートの組み合わせを使用する必要があります。たとえば、node1のe1aとnode2のe1aを1つのスイッチに接続する必要があります。同様に、両方のノードの2番目のポートを2番目のスイッチに接続する必要があります。
- "[MetroCluster IP 用の RcfFileGenerator](#)" また、各スイッチのポート単位のケーブル接続の概要についても

説明しています。ケーブル接続の概要を使用して、ケーブル接続を確認します。

## 2 つの MetroCluster 構成とスイッチのケーブル接続

複数の MetroCluster 構成をスイッチにケーブル接続する場合は、各 MetroCluster を適切な表に従ってケーブル接続します。例えば、FAS2750 と AFF A700 を同じスイッチにケーブル接続する場合、FAS2750 は表1の「MetroCluster 1」に従ってケーブル接続し、AFF A700 は表2の「MetroCluster 2」または「MetroCluster 3」に従ってケーブル接続します。FAS2750 と AFF A700 の両方を「MetroCluster 1」として物理的にケーブル接続することはできません。

## 8 ノード MetroCluster 構成のケーブル接続

ONTAP 9.8 以前を実行している MetroCluster 構成でアップグレードを移行する場合、一時的な 8 ノード構成にするには、2 つ目の 4 ノード DR グループを構成に追加する必要があります。ONTAP 9.9.1 以降では、永続的な 8 ノード MetroCluster 構成がサポートされます。

このタスクについて

8 ノード構成の場合も、上記と同じ方法を使用します。2 つ目の MetroCluster の代わりに、追加の 4 ノード DR グループをケーブル接続します。

たとえば、次のような構成になります。

- Cisco 3132Q-V スイッチ
- MetroCluster 1 : FAS2750 プラットフォーム
- MetroCluster 2 : AFF A700 プラットフォーム (これらのプラットフォームは 2 つ目の 4 ノード DR グループとして追加)

手順

1. MetroCluster 1 では、FAS2750 プラットフォームの表と MetroCluster 1 インターフェイスの行を使用して、Cisco 3132Q-V スイッチをケーブル接続します。
2. MetroCluster 2 (2 つ目の DR グループ) の場合は、AFF A700 プラットフォームの表と MetroCluster 2 インターフェイスの行を使用して、Cisco 3132Q-V スイッチをケーブル接続します。

## MetroCluster IP 構成における Cisco 3132Q-V スイッチのプラットフォームポート割り当て

MetroCluster IP 構成で使用するポートは、スイッチのモデルとプラットフォームのタイプによって異なります。

表を使用する前に、次のガイドラインを確認してください。

- スイッチを MetroCluster FC から IP へ移行するように設定した場合は、ポート 5、ポート 6、ポート 13、またはポート 14 を使用して MetroCluster FC ノードのローカル クラスター インターフェイスを接続できます。を参照してください ["RcfFileGenerator の順にクリックします"](#) および生成されたケーブル接続 ファイルを参照してください。それ以外のすべての接続では、表に記載されているポート使用量の割り当てを使用できます。

構成に適したケーブル接続テーブルを選択

次の表を使用して、必要なケーブル接続の表を特定します。

システムの状態	使用するケーブル接続テーブル
FAS2750、AFF A220	Cisco 3132Q-Vプラットフォームのポート割り当て（グループ1）
FAS9000、AFF A700	Cisco 3132Q-Vプラットフォームのポート割り当て（グループ2）
AFF A800、ASA A800向け	Cisco 3132Q-Vプラットフォームのポート割り当て（グループ3）

#### Cisco 3132Q-Vプラットフォームのポート割り当て（グループ1）

プラットフォームポート割り当てを確認し、FAS2750またはAFF A220システムをCisco 3132Q-Vスイッチにケーブル接続します。

Switch Port	Port use	FAS2750 AFF A220	
		IP_Switch_x_1	IP_Switch_x_2
1 - 6	Unused	disabled	
7	ISL, Local Cluster native speed / 40G / 100G	ISL, Local Cluster	
8			
9/1	MetroCluster 1, Shared Cluster and MetroCluster interface	e0a	e0b
9/2-4		disabled	
10/1		e0a	e0b
10/2-4		disabled	
11/1	MetroCluster 2, Shared Cluster and MetroCluster interface	e0a	e0b
11/2-4		disabled	
12/1		e0a	e0b
12/2-4		disabled	
13/1	MetroCluster 3, Shared Cluster and MetroCluster interface	e0a	e0b
13/2-4		disabled	
14/1		e0a	e0b
14/2-4		disabled	
15	ISL, MetroCluster native speed 40G	ISL, MetroCluster	
16			
17			
18			
19			
20			
21/1-4	ISL, MetroCluster breakout mode 10G	ISL, MetroCluster	
22/1-4			
23/1-4			
24/1-4			
25 - 32	Unused	disabled	

#### Cisco 3132Q-Vプラットフォームのポート割り当て（グループ2）

プラットフォームポート割り当てを確認し、FAS9000またはAFF A700システムをCisco 3132Q-Vスイッチにケーブル接続します。

Switch Port	Port use	FAS9000 AFF A700	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4e / e8a
2			
3	MetroCluster 2, Local Cluster interface	e4a	e4e / e8a
4			
5	MetroCluster 3, Local Cluster interface	e4a	e4e / e8a
6			
7	ISL, Local Cluster native speed 40G	ISL, Local Cluster	
8			
9	MetroCluster 1, MetroCluster interface	e5a	e5b
10			
11	MetroCluster 2, MetroCluster interface	e5a	e5b
12			
13	MetroCluster 3, MetroCluster interface	e5a	e5b
14			
15	ISL, MetroCluster native speed 40G	ISL, MetroCluster	
16			
17			
18			
19			
20			
21/1-4	ISL, MetroCluster breakout mode 10G	ISL, MetroCluster	
22/1-4			
23/1-4			
24/1-4			
25 - 32	Unused	disabled	

### Cisco 3132Q-Vプラットフォームのポート割り当て（グループ3）

プラットフォームポートの割り当てを確認して、AFF A800またはASA A800システムをCisco 3132Q-Vスイッチにケーブル接続します。

Switch Port	Port use	AFF A800 ASA A800	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0a	e1a
2			
3	MetroCluster 2, Local Cluster interface	e0a	e1a
4			
5	MetroCluster 3, Local Cluster interface	e0a	e1a
6			
7	ISL, Local Cluster native speed 40G	ISL, Local Cluster	
8			
9	MetroCluster 1, MetroCluster interface	e0b	e1b
10			
11	MetroCluster 2, MetroCluster interface	e0b	e1b
12			
13	MetroCluster 3, MetroCluster interface	e0b	e1b
14			
15	ISL, MetroCluster native speed 40G	ISL, MetroCluster	
16			
17			
18			
19			
20			
21/1-4	ISL, MetroCluster breakout mode 10G	ISL, MetroCluster	
22/1-4			
23/1-4			
24/1-4			
25 - 32	Unused	disabled	

**MetroCluster IP** 構成における**Cisco 3232C** または **36** ポート**Cisco 9336C** スイッチのプラットフォーム ポート割り当て

MetroCluster IP 構成で使用するポートは、スイッチのモデルとプラットフォームのタイプによって異なります。

構成テーブルを使用する前に、次の考慮事項を確認してください。

- このセクションの表は、NS224 ストレージに接続されていない Cisco 3232C スイッチまたは 36 ポート Cisco 9336C-FX2 スイッチ用です。

12ポートのCisco 9336C-FX2スイッチをお持ちの場合は、"[12ポートCisco 9336C-FX2スイッチのプラットフォームポート割り当て](#)"。

36ポートのCisco 9336C-FX2スイッチがあり、少なくとも1つのMetroCluster構成またはDRグループがNS224シェルフをMetroClusterスイッチに接続している場合は、"[NS224ストレージを接続する36ポートCisco 9336C-FX2スイッチのプラットフォームポート割り当て](#)"。

- 次の表は、サイト A で使用するポートを示しています。サイト B でも同じケーブル接続が使用されます。

- 異なる速度のポート (たとえば、100 Gbps ポートと 40 Gbps ポートの混在) を持つスイッチを構成することはできません。
- スイッチを使用して 1 つの MetroCluster を設定する場合は、\* MetroCluster 1 \* ポートグループを使用します。

MetroClusterポートグループ (MetroCluster 1、MetroCluster 2、MetroCluster 3、またはMetroCluster 4) を追跡します。RcfFileGenerator ツールを使用する場合は、この設定手順で後述するように、このツールが必要になります。

- また、RcfFileGenerator for MetroCluster IP では、各スイッチのポートごとのケーブル配線の概要についても説明します。

ケーブル接続の概要を使用して、ケーブル接続を検証します。

- MetroCluster ISLの25Gブレイクアウトモードには、バージョンv2.10以降のRCFファイルが必要です。
- 「MetroCluster 4」グループでFAS8200またはAFF A300以外のプラットフォームを使用するには、ONTAP 9.13.1以降およびRCFファイルバージョン2.00が必要です。



RCFファイルのバージョンは、ファイルの生成に使用されるRCFfilegeneratorツールのバージョンとは異なります。たとえば、RCFファイルジェネレータv1.6cを使用してバージョン2.00のRCFファイルを生成できます。

構成に適したケーブル接続テーブルを選択

次の表を使用して、必要なケーブル接続の表を特定します。

システムの状態	使用するケーブル接続テーブル
AFF A150、ASA A150 FAS2750、AFF A220 FAS500f、AFF C250 、ASA C250 AFF A250 、ASA A250	Cisco 3232CまたはCisco 9336C-FX2プラットフォームのポート割り当て (グループ1)
AFF A20用	Cisco 3232CまたはCisco 9336C-FX2プラットフォームのポート割り当て (グループ2)
AFF A30、AFF C30 FAS50 AFF C60	次の表は、25G (グループ3a) と100G (グループ3b) のどちらのイーサネットカードを使用しているかによって異なります。 <ul style="list-style-type: none"> <li>Cisco 3232CまたはCisco 9336C-FX2プラットフォームのポート割り当て (グループ3a-25G)</li> <li>Cisco 3232CまたはCisco 9336C-FX2プラットフォームのポート割り当て (グループ3b-100G)</li> </ul>
FAS8200、AFF A300	Cisco 3232CまたはCisco 9336C-FX2プラットフォームのポート割り当て (グループ4)
AFF A320 FAS8300、AFF C400、ASA C400 、FAS8700 AFF A400 、ASA A400	Cisco 3232CまたはCisco 9336C-FX2プラットフォームのポート割り当て (グループ5)

システムの状態	使用するケーブル接続テーブル
AFF A50用	Cisco 3232CまたはCisco 9336C-FX2プラットフォームのポート割り当て（グループ6）
FAS9000、AFF A700 AFF C800、ASA C800、AFF A800、ASAA800 FAS9500、AFF A900、ASA A900	Cisco 3232CまたはCisco 9336C-FX2プラットフォームのポート割り当て（グループ7）
FAS70、AFF A70 AFF C80 FAS90、AFF A90 AFF A1K	Cisco 3232CまたはCisco 9336C-FX2プラットフォームのポート割り当て（グループ8）

**Cisco 3232C**または**Cisco 9336C-FX2**プラットフォームのポート割り当て（グループ1）

プラットフォームポート割り当てを確認して、AFF A150、ASAA150、FAS2750、AFF A220、FAS500f、AFF C250、ASA C250、AFF A250、またはASA A250システムからCisco 3232Cまたは9336C-FX2スイッチへの接続：

Switch Port	Port use	AFF A150 ASA A150 FAS2750 AFF A220		FAS500f AFF C250 ASA C250 AFF A250 ASA A250	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1 - 6	Unused	disabled		disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster	
8					
9/1	MetroCluster 1, Shared Cluster and MetroCluster interface	e0a	e0b	e0c	e0d
9/2-4		disabled		disabled	
10/1		e0a	e0b	e0c	e0d
10/2-4		disabled		disabled	
11/1	MetroCluster 2, Shared Cluster and MetroCluster interface	e0a	e0b	e0c	e0d
11/2-4		disabled		disabled	
12/1		e0a	e0b	e0c	e0d
12/2-4		disabled		disabled	
13/1	MetroCluster 3, Shared Cluster and MetroCluster interface	e0a	e0b	e0c	e0d
13/2-4		disabled		disabled	
14/1		e0a	e0b	e0c	e0d
14/2-4		disabled		disabled	
15	ISL, MetroCluster native speed 40G / 100G				
16					
17		ISL, MetroCluster		ISL, MetroCluster	
18					
19					
20					
21/1-4	ISL, MetroCluster breakout mode 10G / 25G				
22/1-4		ISL, MetroCluster		ISL, MetroCluster	
23/1-4					
24/1-4					
25/1	MetroCluster 1, Shared Cluster and MetroCluster interface	e0a	e0b	e0c	e0d
25/2-4		disabled		disabled	
26/1		e0a	e0b	e0c	e0d
26/2-4		disabled		disabled	
27 - 32	Unused	disabled		disabled	
33 - 36	Unused (Cisco 9336C-FX2 only)	disabled		disabled	

### Cisco 3232CまたはCisco 9336C-FX2プラットフォームのポート割り当て（グループ2）

プラットフォームポート割り当てを確認し、AFF A20システムをCisco 3232Cまたは9336C-FX2スイッチにケーブル接続します。

Switch Port	Port use	AFF A20	
		IP_Switch_x_1	IP_Switch_x_2
1/1	MetroCluster 1, Local Cluster interface	e2a	e4a
1/2-4		disabled	
2/1		e2a	e4a
2/2-4		disabled	
3/1	MetroCluster 2, Local Cluster interface	e2a	e4a
3/2-4		disabled	
4/1		e2a	e4a
4/2-4		disabled	
5/1	MetroCluster 3, Local Cluster interface	e2a	e4a
5/2-4		disabled	
6/1		e2a	e4a
6/2-4		disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9/1	MetroCluster 1, MetroCluster interface	e2b	e4b
9/2-4		disabled	
10/1		e2b	e4b
10/2-4		disabled	
11/1	MetroCluster 2, MetroCluster interface	e2b	e4b
11/2-4		disabled	
12/1		e2b	e4b
12/2-4		disabled	
13/1	MetroCluster 3, MetroCluster interface	e2b	e4b
13/2-4		disabled	
14/1		e2b	e4b
14/2-4		disabled	
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster	
16			
17			
18			
19			
20			
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster	
22/1-4			
23/1-4			
24/1-4			
25/1	MetroCluster 4, MetroCluster interface	e2b	e4b
25/2-4		disabled	
26/1		e2b	e4b
26/2-4		disabled	
27 - 28	Unused	disabled	
29/1	MetroCluster 4, Local Cluster interface	e2a	e4a
29/2-4		disabled	
30/1		e2a	e4a
30/2-4		disabled	
25 - 32	Unused	disabled	
33 - 36	Unused (Cisco 9336C-FX2 only)	disabled	

### Cisco 3232CまたはCisco 9336C-FX2プラットフォームのポート割り当て（グループ3a）

プラットフォームポートの割り当てを確認し、4ポートの25Gイーサネットカードを使用してAFF A30、AFF C30、AFF C60、またはFAS50システムをCisco 3232Cまたは9336C-FX2スイッチにケーブル接続します。



この構成では、ローカルクラスタとHAインターフェイスを接続するために、スロット4に4ポートの25Gイーサネットカードが必要です。

Switch Port	Port use	AFF C30 (25G Cluster/HA) AFF A30 (25G Cluster/HA)		FAS50 (25G Cluster/HA)		AFF C60 (25G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1/1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
1/2-4		disabled		disabled		disabled	
2/1		e4a	e4b	e4a	e4b	e4a	e4b
2/2-4		disabled		disabled		disabled	
3/1	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
3/2-4		disabled		disabled		disabled	
4/1		e4a	e4b	e4a	e4b	e4a	e4b
4/2-4		disabled		disabled		disabled	
5/1	MetroCluster 3, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
5/2-4		disabled		disabled		disabled	
6/1		e4a	e4b	e4a	e4b	e4a	e4b
6/2-4		disabled		disabled		disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
10	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
11	MetroCluster 3, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
12	MetroCluster 4, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
13	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
14	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
16							
17							
18							
19							
20							
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
22/1-4							
23/1-4							
24/1-4							
25	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
26		e2a	e2b	e2a	e2b	e2a	e2b
27 - 28	Unused	disabled		disabled		disabled	
29/1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
29/2-4		disabled		disabled		disabled	
30/1		e4a	e4b	e4a	e4b	e4a	e4b
30/2-4		disabled		disabled		disabled	
25 - 32	Unused	disabled		disabled		disabled	
33 - 36	Unused (Cisco 9336C-FX2 only)	disabled		disabled		disabled	

### Cisco 3232CまたはCisco 9336C-FX2プラットフォームのポート割り当て（グループ3b）

プラットフォームポートの割り当てを確認し、2ポートの100Gイーサネットカードを使用してAFF A30、AFF C30、AFF C60、またはFAS50システムをCisco 3232Cまたは9336C-FX2スイッチにケーブル接続します。



この構成では、ローカルクラスタとHAインターフェイスを接続するために、スロット4に2ポートの100Gイーサネットカードが必要です。

Switch Port	Port use	AFF C30 (100G Cluster/HA) AFF A30 (100G Cluster/HA)		FAS50 (100G Cluster/HA)		AFF C60 (100G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
		1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b
2		e4a	e4b	e4a	e4b	e4a	e4b
3	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
4		e4a	e4b	e4a	e4b	e4a	e4b
5	MetroCluster 3, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
6		e4a	e4b	e4a	e4b	e4a	e4b
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
10		e2a	e2b	e2a	e2b	e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
12		e2a	e2b	e2a	e2b	e2a	e2b
13	MetroCluster 3, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
14		e2a	e2b	e2a	e2b	e2a	e2b
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
16							
17							
18							
19							
20							
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
22/1-4							
23/1-4							
24/1-4							
25	MetroCluster 4, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
26		e2a	e2b	e2a	e2b	e2a	e2b
27 - 28	Unused	disabled		disabled		disabled	
29	MetroCluster 4, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
30		e4a	e4b	e4a	e4b	e4a	e4b
25 - 32	Unused	disabled		disabled		disabled	
33 - 36	Unused (Cisco 9336C-FX2 only)	disabled		disabled		disabled	

**Cisco 3232C**または**Cisco 9336C-FX2**プラットフォームのポート割り当て（グループ4）

プラットフォームポート割り当てを確認し、FAS8200またはAFF A300システムをCisco 3232Cまたは9336C-FX2スイッチにケーブル接続します。

Switch Port	Port use	FAS8200 AFF A300	
		IP_Switch_x_1	IP_Switch_x_2
1/1	MetroCluster 1, Local Cluster interface	e0a	e0b
1/2-4		disabled	
2/1		e0a	e0b
2/2-4		disabled	
3/1	MetroCluster 2, Local Cluster interface	e0a	e0b
3/2-4		disabled	
4/1		e0a	e0b
4/2-4		disabled	
5/1	MetroCluster 3, Local Cluster interface	e0a	e0b
5/2-4		disabled	
6/1		e0a	e0b
6/2-4		disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9/1	MetroCluster 1, MetroCluster interface	e1a	e1b
9/2-4		disabled	
10/1		e1a	e1b
10/2-4		disabled	
11/1	MetroCluster 2, MetroCluster interface	e1a	e1b
11/2-4		disabled	
12/1		e1a	e1b
12/2-4		disabled	
13/1	MetroCluster 3, MetroCluster interface	e1a	e1b
13/2-4		disabled	
14/1		e1a	e1b
14/2-4		disabled	
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster	
16			
17			
18			
19			
20			
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster	
22/1-4			
23/1-4			
24/1-4			
25/1	MetroCluster 4, MetroCluster interface	e1a	e1b
25/2-4		disabled	
26/1		e1a	e1b
26/2-4		disabled	
27 - 28	Unused	disabled	
29/1	MetroCluster 4, Local Cluster interface	e0a	e0b
29/2-4		disabled	
30/1		e0a	e0b
30/2-4		disabled	
25 - 32	Unused	disabled	
33 - 36	Unused (Cisco 9336C-FX2 only)	disabled	

古いRCFファイルからアップグレードする場合は、「MetroCluster 4」グループのポート（ポート25 / 26および29 / 30）をケーブル接続構成で使用している可能性があります。

**Cisco 3232CまたはCisco 9336C-FX2プラットフォームのポート割り当て（グループ5）**

AFF A320、FAS8300、AFF C400、ASA C400、FAS8700をケーブル接続するためのプラットフォームポート割り当ての確認 AFF A400またはASA A400システムからCisco 3232Cまたは9336C-FX2スイッチへの接続：

Switch Port	Port use	AFF A320		FAS8300 AFF C400 ASA C400 FAS8700		AFF A400 ASA A400	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b
2							
3	MetroCluster 2, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b
4							
5	MetroCluster 3, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b
6							
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b
10							
11	MetroCluster 2, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b
12							
13	MetroCluster 3, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b
14							
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
16							
17							
18							
19							
20							
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
22/1-4							
23/1-4							
24/1-4							
25	MetroCluster 4, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b
26							
27 - 28	Unused	disabled		disabled		disabled	
29	MetroCluster 4, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b
30							
31 - 32	Unused	disabled		disabled		disabled	
33 - 34	Unused (Cisco 9336C-FX2 only)	disabled		disabled		disabled	



「MetroCluster 4」グループのポートを使用するには、ONTAP 9.13.1以降が必要です。

**Cisco 3232CまたはCisco 9336C-FX2プラットフォームのポート割り当て（グループ6）**

プラットフォームポート割り当てを確認し、AFF A50システムをCisco 3232Cまたは9336C-FX2スイッチにケーブル接続します。

Switch Port	Port use	AFF A50	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4b
2		e4a	e4b
3	MetroCluster 2, Local Cluster interface	e4a	e4b
4		e4a	e4b
5	MetroCluster 3, Local Cluster interface	e4a	e4b
6		e4a	e4b
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9	MetroCluster 1, MetroCluster interface	e2a	e2b
10		e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b
12		e2a	e2b
13	MetroCluster 3, MetroCluster interface	e2a	e2b
14		e2a	e2b
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster	
16			
17			
18			
19			
20			
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster	
22/1-4			
23/1-4			
24/1-4			
25	MetroCluster 4, MetroCluster interface	e2a	e2b
26		e2a	e2b
27 - 28	Unused	disabled	
29	MetroCluster 4, Local Cluster interface	e4a	e4b
30		e4a	e4b
25 - 32	Unused	disabled	
33 - 36	Unused (Cisco 9336C-FX2 only)	disabled	

**Cisco 3232C**または**Cisco 9336C-FX2**プラットフォームのポート割り当て（グループ7）

FAS9000、AFF A700、AFF C800、ASA C800、AFF A800をケーブル接続するためのプラットフォームポート割り当ての確認 ASA A800、FAS9500、AFF A900、またはASA A900システムからCisco 3232Cまたは9336C-FX2スイッチへの接続：

Switch Port	Port use	FAS9000 AFF A700		AFF C800 ASA C800 AFF A800 ASA A800		FAS9500 AFF A900 ASA A900	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
2							
3	MetroCluster 2, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
4							
5	MetroCluster 3, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
6							
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b
10							
11	MetroCluster 2, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b
12							
13	MetroCluster 3, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b
14							
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
16							
17							
18							
19							
20							
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
22/1-4							
23/1-4							
24/1-4							
25	MetroCluster 4, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b
26							
27 - 28	Unused	disabled		disabled		disabled	
29	MetroCluster 4, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
30							
31 - 32	Unused	disabled		disabled		disabled	
33 - 34	Unused (Cisco 9336C-FX2 only)	disabled		disabled		disabled	

\*注1 \* : X91440Aアダプタ (40Gbps) を使用している場合は、ポートe4aとe4e、またはe4aとe8aのいずれかを使用します。ポートe4aとe4b、またはX91153Aアダプタ (100Gbps) を使用している場合はe4aとe8aのいずれかを使用します。



「MetroCluster 4」グループのポートを使用するには、ONTAP 9.13.1以降が必要です。

#### Cisco 3232CまたはCisco 9336C-FX2プラットフォームのポート割り当て (グループ8)

プラットフォームポート割り当てを確認し、AFF A70、FAS70、AFF C80、FAS90、AFF A90、またはAFF A1KシステムをCisco 3232Cまたは9336C-FX2スイッチにケーブル接続します。

Switch Port	Port use	FAS70 AFF A70		AFF C80		FAS90 AFF A90		AFF A1K	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
2									
3									
4	MetroCluster 2, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
5									
6									
7	MetroCluster 3, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
8									
9									
10	ISL, Local Cluster native speed / 100G	ISL, Local Cluster							
11									
12									
13	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
14									
15									
16	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
17									
18									
19	MetroCluster 3, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
20									
21									
22	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
23									
24									
25									
26	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
27									
28									
29									
30	MetroCluster 4, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
31									
32									
33	Unused	disabled		disabled		disabled		disabled	
34									
35									
36	MetroCluster 4, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
37									
38									
39	Unused (Cisco 9336C-FX2 only)	disabled		disabled		disabled		disabled	
40									
41									

## MetroCluster IP構成における12ポートCisco 9336C-FX2スイッチのプラットフォームポート割り当て

MetroCluster IP 構成で使用するポートは、スイッチのモデルとプラットフォームのタイプによって異なります。

構成テーブルを使用する前に、次の考慮事項を確認してください。

- このセクションの表は、12ポートのCisco 9336C-FX2スイッチ用です。

NS224シェルフに接続していない36ポートのCisco 9336C-FX2スイッチがある場合は、"[Cisco 3232C または 36ポート Cisco 9336C-FX2スイッチのプラットフォームポート割り当て](#)"。

36ポートのCisco 9336C-FX2スイッチがあり、少なくとも1つのMetroCluster構成またはDRグループがNS224シェルフをMetroClusterスイッチに接続している場合は、"[NS224ストレージを接続する36ポートCisco 9336C-FX2スイッチのプラットフォームポート割り当て](#)"。



12ポートのCisco 9336C-FX2スイッチは、NS224シェルフをMetroClusterスイッチに接続することをサポートしていません。

- 次の表は、サイトAで使用するポートを示しています。サイトBでも同じケーブル接続が使用されます。
- 異なる速度のポート（たとえば、100 Gbpsポートと40 Gbpsポートの混在）を持つスイッチを構成することはできません。
- スイッチを使用して1つのMetroClusterを設定する場合は、\* MetroCluster 1 \* ポートグループを使用します。

MetroClusterポートグループ（MetroCluster 1、MetroCluster 2）を把握しておいてください。この設定手順の後半で説明するRcfFileGeneratorツールを使用する際に必要になります。

- また、RcfFileGenerator for MetroCluster IP では、各スイッチのポートごとのケーブル配線の概要についても説明します。

構成に適したケーブル接続テーブルを選択

次の表を使用して、必要なケーブル接続の表を特定します。

システムの状態	使用するケーブル接続テーブル
AFF A150、ASAA150 FAS500f AFF C250、ASA C250 AFF A250、ASA A250	Cisco 9336C-FX2 12 ポート プラットフォームのポート割り当て (グループ 1)
AFF A20用	Cisco 9336C-FX2 12ポート プラットフォームのポート割り当て (グループ2)
AFF A30、AFF C30 FAS50 AFF C60	次の表は、25G (グループ3a) と100G (グループ3b) のどちらのイーサネットカードを使用しているかによって異なります。 <ul style="list-style-type: none"> <li>• Cisco 9336C-FX2 12 ポート プラットフォームのポート割り当て (グループ 3a - 25G)</li> <li>• Cisco 9336C-FX2 12 ポート プラットフォームのポート割り当て (グループ 3b - 100G)</li> </ul>
FAS8300、AFF C400 、ASA C400、FAS8700 AFF A400、ASAA400	Cisco 9336C-FX2 12 ポート プラットフォームのポート割り当て (グループ 4)
AFF A50用	Cisco 9336C-FX2 12ポート プラットフォームのポート割り当て (グループ5)
AFF C800、ASA C800 、AFF A800、ASAA800 FAS9500、AFF A900 、ASAA900	Cisco 9336C-FX2 12ポート プラットフォームのポート割り当て (グループ 6)
FAS70、AFF A70 AFF C80 FAS90、AFF A90 AFF A1K	Cisco 9336C-FX2 12ポート プラットフォームのポート割り当て (グループ7)

#### Cisco 9336C-FX2 12 ポート プラットフォームのポート割り当て (グループ 1)

AFF A150、ASAA150、FAS500f、AFF C250、ASA C250、AFF A250、または ASA A250 システムを 12 ポートの Cisco 9336C-FX2 スイッチにケーブル接続するには、プラットフォーム ポートの割り当てを確認します。

Switch Port	Port use	AFF A150 ASA A150		FAS500f AFF C250 ASA C250 AFF A250 ASA A250	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1-4	Unused	disabled		disabled	
5-6	Ports disallowed to use	blocked		blocked	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster	
8					
9/1	MetroCluster 1, Shared Cluster and MetroCluster interface	e0a	e0b	e0c	e0d
9/2-4		disabled		disabled	
10/1		e0a	e0b	e0c	e0d
10/2-4		disabled		disabled	
11/1	MetroCluster 2, Shared Cluster and MetroCluster interface	e0a	e0b	e0c	e0d
11/2-4		disabled		disabled	
12/1		e0a	e0b	e0c	e0d
12/2-4		disabled		disabled	
13-18	Ports disallowed to use	blocked		blocked	
19	ISL, MetroCluster native speed 40G / 100G (note 1)	ISL, MetroCluster		ISL, MetroCluster	
20					
21/1-4	ISL, MetroCluster breakout mode 10G / 25G (note 1)	ISL, MetroCluster		ISL, MetroCluster	
22/1-4					
23-36	Ports disallowed to use	blocked		blocked	

注 1: 設定できるのはポート 19 と 20、またはポート 21 と 22 のみです。ポート 19 と 20 を先に使用した場合、ポート 21 と 22 はブロックされます。ポート 21 と 22 を先に使用した場合、ポート 19 と 20 はブロックされます。

#### Cisco 9336C-FX2 12ポート プラットフォームのポート割り当て (グループ2)

AFF A20 システムを 12 ポートの Cisco 9336C-FX2 スイッチにケーブル接続するためのプラットフォーム ポートの割り当てを確認します。

Switch Port	Port use	AFF A20	
		IP_Switch_x_1	IP_Switch_x_2
1/1	MetroCluster 1, Local Cluster interface	e2a	e4a
1/2-4		disabled	
2/1		e2a	e4a
2/2-4		disabled	
3/1	MetroCluster 2, Local Cluster interface	e2a	e4a
3/2-4		disabled	
4/1		e2a	e4a
4/2-4		disabled	
5-6	Ports disallowed to use	blocked	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9/1	MetroCluster 1, MetroCluster interface	e2b	e4b
9/2-4		disabled	
10/1		e2b	e4b
10/2-4		disabled	
11/1	MetroCluster 2, MetroCluster interface	e2b	e4b
11/2-4		disabled	
12/1		e2b	e4b
12/2-4		disabled	
13-18	Ports disallowed to use	blocked	
19	ISL, MetroCluster native speed 40G / 100G (note 1)	ISL, MetroCluster	
20			
21/1-4	ISL, MetroCluster breakout mode 10G / 25G (note 1)	ISL, MetroCluster	
22/1-4			
23-36	Ports disallowed to use	blocked	

注 1: 設定できるのはポート 19 と 20、またはポート 21 と 22 のみです。ポート 19 と 20 を先に使用した場合、ポート 21 と 22 はブロックされます。ポート 21 と 22 を先に使用した場合、ポート 19 と 20 はブロックされます。

#### Cisco 9336C-FX2 12ポート プラットフォームのポート割り当て (グループ3a)

4 ポート 25G イーサネット カードを使用して、AFF A30、AFF C30、AFF C60、または FAS50 システムを 12 ポートの Cisco 9336C-FX2 スイッチにケーブル接続するためのプラットフォーム ポートの割り当てを確認します。



この構成では、ローカルクラスターとHAインターフェイスを接続するために、スロット4に4ポートの25Gイーサネットカードが必要です。

Switch Port	Port use	AFF C30 (25G Cluster/HA) AFF A30 (25G Cluster/HA)		FAS50 (25G Cluster/HA)		AFF C60 (25G Cluster/HA)		
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	
1/1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b	
1/2-4		disabled		disabled		disabled		
2/1		e4a	e4b	e4a	e4b	e4a	e4b	
2/2-4		disabled		disabled		disabled		
3/1	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b	
3/2-4		disabled		disabled		disabled		
4/1		e4a	e4b	e4a	e4b	e4a	e4b	
4/2-4		disabled		disabled		disabled		
5-6	Ports disallowed to use	blocked		blocked		blocked		
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster		
8								
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b	
10		e2a	e2b	e2a	e2b	e2a	e2b	
11		MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
12			e2a	e2b	e2a	e2b	e2a	e2b
13-18	Ports disallowed to use	blocked		blocked		blocked		
19	ISL, MetroCluster native speed 40G / 100G (note 1)	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		
20								
21/1-4	ISL, MetroCluster breakout mode 10G / 25G (note 1)	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		
22/1-4								
23-36	Ports disallowed to use	blocked		blocked		blocked		

注 1: 設定できるのはポート 19 と 20、またはポート 21 と 22 のみです。ポート 19 と 20 を先に使用した場合、ポート 21 と 22 はブロックされます。ポート 21 と 22 を先に使用した場合、ポート 19 と 20 はブロックされます。

### Cisco 9336C-FX2 12ポート プラットフォームのポート割り当て (グループ3b)

2 ポート 100G イーサネット カードを使用して、AFF A30、AFF C30、AFF C60、または FAS50 システムを 12 ポートの Cisco 9336C-FX2 スイッチにケーブル接続するためのプラットフォーム ポートの割り当てを確認します。



この構成では、ローカルクラスターとHAインターフェイスを接続するために、スロット4に2ポートの100Gイーサネットカードが必要です。

Switch Port	Port use	AFF C30 (100G Cluster/HA) AFF A30 (100G Cluster/HA)		FAS50 (100G Cluster/HA)		AFF C60 (100G Cluster/HA)		
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	
1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b	
2		e4a	e4b	e4a	e4b	e4a	e4b	
3	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b	
4		e4a	e4b	e4a	e4b	e4a	e4b	
5-6	Ports disallowed to use	blocked		blocked		blocked		
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster		
8								
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b	
10		e2a	e2b	e2a	e2b	e2a	e2b	
11		MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
12			e2a	e2b	e2a	e2b	e2a	e2b
13-18	Ports disallowed to use	blocked		blocked		blocked		
19	ISL, MetroCluster native speed 40G / 100G (note 1)	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		
20								
21/1-4	ISL, MetroCluster breakout mode 10G / 25G (note 1)	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		
22/1-4								
23-36	Ports disallowed to use	blocked		blocked		blocked		

注 1: 設定できるのはポート 19 と 20、またはポート 21 と 22 のみです。ポート 19 と 20 を先に使用した場合、ポート 21 と 22 はブロックされます。ポート 21 と 22 を先に使用した場合、ポート 19 と 20 はブロックされます。

**Cisco 9336C-FX2 12 ポート プラットフォームのポート割り当て (グループ 4)**

FAS8300、AFF C400、ASA C400、FAS8700、AFF A400、または ASAA400 システムを 12 ポートの Cisco 9336C-FX2 スイッチにケーブル接続するには、プラットフォーム ポートの割り当てを確認します。

Switch Port	Port use	FAS8300 AFF C400 ASA C400 FAS8700		AFF A400 ASA A400	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0c	e0d	e3a	e3b
2					
3	MetroCluster 2, Local Cluster interface	e0c	e0d	e3a	e3b
4					
5-6	Ports disallowed to use	blocked		blocked	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster	
8					
9	MetroCluster 1, MetroCluster interface	e1a	e1b	e1a	e1b
10					
11	MetroCluster 2, MetroCluster interface	e1a	e1b	e1a	e1b
12					
13-18	Ports disallowed to use	blocked		blocked	
19	ISL, MetroCluster native speed 40G / 100G (note 1)	ISL, MetroCluster		ISL, MetroCluster	
20					
21/1-4	ISL, MetroCluster breakout mode 10G / 25G (note 1)	ISL, MetroCluster		ISL, MetroCluster	
22/1-4					
23-36	Ports disallowed to use	blocked		blocked	

注 1: 設定できるのはポート 19 と 20、またはポート 21 と 22 のみです。ポート 19 と 20 を先に使用した場合、ポート 21 と 22 はブロックされます。ポート 21 と 22 を先に使用した場合、ポート 19 と 20 はブロックされます。

**Cisco 9336C-FX2 12 ポート プラットフォームのポート割り当て (グループ 5)**

AFF A50 システムを 12 ポートの Cisco 9336C-FX2 スイッチにケーブル接続するためのプラットフォーム ポートの割り当てを確認します。

Switch Port	Port use	AFF A50	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4b
2		e4a	e4b
3	MetroCluster 2, Local Cluster interface	e4a	e4b
4		e4a	e4b
5-6	Ports disallowed to use	blocked	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9	MetroCluster 1, MetroCluster interface	e2a	e2b
10		e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b
12		e2a	e2b
13-18	Ports disallowed to use	blocked	
19	ISL, MetroCluster native speed 40G / 100G (note 1)	ISL, MetroCluster	
20			
21/1-4	ISL, MetroCluster breakout mode 10G / 25G (note 1)	ISL, MetroCluster	
22/1-4			
23-36	Ports disallowed to use	blocked	

注 1: 設定できるのはポート 19 と 20、またはポート 21 と 22 のみです。ポート 19 と 20 を先に使用した場合、ポート 21 と 22 はブロックされます。ポート 21 と 22 を先に使用した場合、ポート 19 と 20 はブロックされます。

#### Cisco 9336C-FX2 12ポート プラットフォームのポート割り当て (グループ 6)

AFF C800、ASA C800、AFF A800、ASAA800、FAS9500、AFF A900、または ASAA900 システムを 12 ポートの Cisco 9336C-FX2 スイッチにケーブル接続するためのプラットフォーム ポートの割り当てを確認します。

Switch Port	Port use	AFF C800 ASA C800 AFF A800 ASA A800		FAS9500 AFF A900 ASA A900	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0a	e1a	e4a	e4b(e) / e8a (note 2)
2					
3	MetroCluster 2, Local Cluster interface	e0a	e1a	e4a	e4b(e) / e8a (note 2)
4					
5-6	Ports disallowed to use	blocked		blocked	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster	
8					
9	MetroCluster 1, MetroCluster interface	e0b	e1b	e5b	e7b
10					
11	MetroCluster 2, MetroCluster interface	e0b	e1b	e5b	e7b
12					
13-18	Ports disallowed to use	blocked		blocked	
19	ISL, MetroCluster native speed 40G / 100G (note 1)	ISL, MetroCluster		ISL, MetroCluster	
20					
21/1-4	ISL, MetroCluster breakout mode 10G / 25G (note 1)	ISL, MetroCluster		ISL, MetroCluster	
22/1-4					
23-36	Ports disallowed to use	blocked		blocked	

注 1: 設定できるのはポート 19 と 20、またはポート 21 と 22 のみです。ポート 19 と 20 を先に使用した場合、ポート 21 と 22 はブロックされます。ポート 21 と 22 を先に使用した場合、ポート 19 と 20 はブロックされます。

注 2: X91440A アダプタ (40Gbps) を使用している場合は、ポート e4a と e4e、またはポート e4a と e8a のいずれかを使用します。ポート e4a と e4b、または X91153A アダプタ (100Gbps) を使用している場合は e4a と e8a のいずれかを使用します。

### Cisco 9336C-FX2 12ポート プラットフォームのポート割り当て (グループ7)

AFF A70、FAS70、AFF C80、FAS90、AFF A90、または AFF A1K システムを 12 ポートの Cisco 9336C-FX2 スイッチにケーブル接続するには、プラットフォーム ポートの割り当てを確認します。

Switch Port	Port use	FAS70 AFF A70		AFF C80		FAS90 AFF A90		AFF A1K	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
2									
3	MetroCluster 2, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
4									
5-6	Ports disallowed to use	blocked		blocked		blocked		blocked	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster							
8									
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
10									
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
12									
13-18	Ports disallowed to use	blocked		blocked		blocked		blocked	
19	ISL, MetroCluster native speed 40G / 100G (note 1)	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
20									
21/1-4	ISL, MetroCluster breakout mode 10G / 25G (note 1)	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
22/1-4									
23-36	Ports disallowed to use	blocked		blocked		blocked		blocked	

注 1: 設定できるのはポート 19 と 20、またはポート 21 と 22 のみです。ポート 19 と 20 を先に使用した場合、ポート 21 と 22 はブロックされます。ポート 21 と 22 を先に使用した場合、ポート 19 と 20 はブロックされます。

## MetroCluster IP構成でNS224ストレージを接続する36ポートCisco 9336C-FX2スイッチのプラットフォームポート割り当て

MetroCluster IP 構成で使用するポートは、スイッチのモデルとプラットフォームのタイプによって異なります。

構成テーブルを使用する前に、次の考慮事項を確認してください。

- このセクションの表は、少なくとも1つのMetroCluster構成またはDRグループがNS224シェルフをMetroClusterスイッチに接続している場合の36ポートCisco 9336C-FX2スイッチ用です。

36ポートCisco 9336C-FX2スイッチをお持ちで、NS224ストレージをスイッチに接続する予定がない場合は、"[Cisco 3232C または 36 ポート Cisco 9336C-FX2 スwitchのプラットフォーム ポート割り当て](#)"の表を使用してください。

12ポートのCisco 9336C-FX2スイッチをお持ちの場合は、"[12ポートCisco 9336C-FX2スイッチのプラットフォームポート割り当て](#)"。



12ポートのCisco 9336C-FX2スイッチは、NS224シェルフをMetroClusterスイッチに接続することをサポートしていません。

- NS224ストレージを接続するCisco 9336C-FX2スイッチをケーブル接続する場合、最大2つのMetroCluster構成またはDRグループしか使用できません。少なくとも1つのMetroCluster構成またはDRグループは、NS224シェルフをMetroClusterスイッチに接続する必要があります。

MetroCluster構成またはDRグループのいずれかでNS224シェルフがMetroClusterスイッチに接続されていない場合は、[スイッチ接続NS224シェルフに接続しないコントローラの配線表](#)に従ってください。

- RcfFileGeneratorでは、最初のプラットフォームが選択されている場合にのみ、対象となるプラットフォームが表示されます。
- スイッチ接続NS224ストレージをサポートしていない通常のMetroCluster構成を拡張し、スイッチ接続NS224ストレージを備えたMetroCluster構成を追加する場合は、次の情報を確認してください：
  - "[RcfFileGenerator の順にクリックします](#)"ツールでは、最初にスイッチ接続NS224ストレージをサポートするプラットフォームを選択し、次にスイッチ接続NS224ストレージをサポートしないプラットフォームを選択する必要があります。

つまり、新しい構成のRCFを生成するとき、RcfFileGeneratorツールで次の順序でプラットフォームを選択する必要がある場合があります：

- i. 2番目のドロップダウンフィールドから、スイッチ接続NS224ストレージをサポートするプラットフォームを選択します。
  - ii. \*最初のドロップダウンフィールド\*から、スイッチ接続NS224ストレージをサポートしていないプラットフォームを選択します。
- 1つの8ノードまたは2つの4ノードMetroCluster構成を接続するには、ONTAP 9.14.1以降が必要です。

構成に適したケーブル接続テーブルを選択

構成に適したポート割り当ての表を確認します。このセクションには、2組のケーブルテーブルがあります。

- [スイッチ接続NS224シェルフを接続するコントローラのケーブル接続表](#)

・ スイッチ接続NS224シェルフを接続しないコントローラのケーブル接続表

スイッチ接続**NS224**シェルフを接続するコントローラ

スイッチ接続NS224シェルフを接続するコントローラのポート割り当て表を確認します。

プラットフォーム	使用するケーブル接続テーブル
AFF C30、AFF A30 AFF C60	次の表は、25G（グループ1a）と100G（グループ1b）のどちらのイーサネットカードを使用しているかによって異なります。 <ul style="list-style-type: none"> <li>NS224ストレージプラットフォームのポート割り当てを接続するCisco 9336C-FX2スイッチ（グループ1a-25G）</li> <li>NS224ストレージプラットフォームのポート割り当てを接続するCisco 9336C-FX2スイッチ（グループ1b-100G）</li> </ul>
AFF A320 AFF C400、ASA C400 AFF A400、ASA A400	NS224ストレージプラットフォームのポート割り当て（グループ2）を接続するCisco 9336C-FX2スイッチ
AFF A50用	NS224ストレージプラットフォームのポート割り当てを接続するCisco 9336C-FX2スイッチ（グループ3）
AFF A700 AFF C800、ASA C800、AFF A800 AFF A900、ASA A900	NS224ストレージプラットフォームのポート割り当てを接続するCisco 9336C-FX2スイッチ（グループ4）
AFF A70 AFF C80 AFF A90 AFF A1K	NS224ストレージプラットフォームのポート割り当てを接続するCisco 9336C-FX2スイッチ（グループ5）

**NS224**ストレージプラットフォームのポート割り当てを接続する**Cisco 9336C-FX2**スイッチ（グループ1a）

プラットフォームポートの割り当てを確認し、4ポートの25Gイーサネットカードを使用してスイッチ接続NS224シェルフをCisco 9336C-FX2スイッチに接続するAFF A30、AFF C30、またはAFF C60システムをケーブル接続します。



この構成では、ローカルクラスタとHAインターフェイスを接続するために、スロット4に4ポートの25Gイーサネットカードが必要です。

Controllers connecting switch-attached shelves					
Switch Port	Port Use	AFF C30 (25G Cluster/HA) AFF A30 (25G Cluster/HA)		AFF C60 (25G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1/1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b
1/2-4		disabled		disabled	
2/1		e4a	e4b	e4a	e4b
2/2-4		disabled		disabled	
3/1	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b
3/2-4		disabled		disabled	
4/1		e4a	e4b	e4a	e4b
4/2-4		disabled		disabled	
5	Storage shelf 1 (9)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
6		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster	
8					
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b
10		e2a	e2b	e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b
12		e2a	e2b	e2a	e2b
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster	
14					
15					
16					
17	MetroCluster 1, Ethernet Storage Interface	e3a	e3b	e3a	e3b
18					
19	MetroCluster 2, Ethernet Storage Interface	e3a	e3b	e3a	e3b
20					
21	Storage shelf 2 (8)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
22		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
23	Storage shelf 3 (7)				
24					
25	Storage shelf 4 (6)				
26					
27	Storage shelf 5 (5)				
28					
29	Storage shelf 6 (4)				
30					
31	Storage shelf 7 (3)				
32					
33	Storage shelf 8 (2)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
34		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
35	Storage shelf 9 (1)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
36		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b

### NS224ストレージプラットフォームのポート割り当てを接続するCisco 9336C-FX2スイッチ（グループ1b）

プラットフォームポートの割り当てを確認し、2ポート100Gイーサネットカードを使用してスイッチ接続NSS24シェルフをCisco 9336C-FX2スイッチに接続するAFF A30、AFF C30、またはAFF C60システムをケーブル接続します。



この構成では、ローカルクラスターとHAインターフェイスを接続するために、スロット4に2ポートの100Gイーサネットカードが必要です。

Controllers connecting switch-attached shelves					
Switch Port	Port Use	AFF C30 (100G Cluster/HA) AFF A30 (100G Cluster/HA)		AFF C60 (100G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b
2		e4a	e4b	e4a	e4b
3	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b
4		e4a	e4b	e4a	e4b
5	Storage shelf 1 (9)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
6		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster	
8					
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b
10		e2a	e2b	e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b
12		e2a	e2b	e2a	e2b
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster	
14					
15					
16					
17	MetroCluster 1, Ethernet Storage Interface	e3a	e3b	e3a	e3b
18		e3a	e3b	e3a	e3b
19	MetroCluster 2, Ethernet Storage Interface	e3a	e3b	e3a	e3b
20		e3a	e3b	e3a	e3b
21	Storage shelf 2 (8)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
22		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
23	Storage shelf 3 (7)				
24					
25	Storage shelf 4 (6)				
26					
27	Storage shelf 5 (5)				
28					
29	Storage shelf 6 (4)				
30					
31	Storage shelf 7 (3)				
32					
33	Storage shelf 8 (2)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
34		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
35	Storage shelf 9 (1)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
36		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b

**NS224**ストレージプラットフォームのポート割り当て（グループ2）を接続する**Cisco 9336C-FX2**スイッチ

プラットフォームポート割り当てを確認し、スイッチ接続NSS24シェルフをCisco 9336C-FX2スイッチに接続するAFF A320、AFF C400、ASA C400、AFF A400、またはASA A400システムをケーブル接続します。

Controllers connecting switch-attached shelves							
Switch Port	Port Use	AFF A320		AFF C400 ASA C400		AFF A400 ASA A400	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b
2							
3	MetroCluster 2, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b
4							
5	Storage shelf 1 (9)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
6		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b
10							
11	MetroCluster 2, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b
12							
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14							
15							
16							
17	MetroCluster 1, Ethernet Storage Interface	e0c	e0f	e4a	e4b / e5b	e0c	e0d / e5b
18							
19	MetroCluster 2, Ethernet Storage Interface	e0c	e0f	e4a	e4b / e5b	e0c	e0d / e5b
20							
21	Storage shelf 2 (8)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
22		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
23	Storage shelf 3 (7)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
24		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
25	Storage shelf 4 (6)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
26		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
27	Storage shelf 5 (5)	NSM-1, e0a	NSM-1, e0b				
28		NSM-2, e0a	NSM-2, e0b				
29	Storage shelf 6 (4)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
30		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
31	Storage shelf 7 (3)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
32		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
33	Storage shelf 8 (2)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
34		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
35	Storage shelf 9 (1)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
36		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b

**NS224ストレージプラットフォームのポート割り当てを接続するCisco 9336C-FX2スイッチ（グループ3）**

プラットフォームポート割り当てを確認し、スイッチ接続NSS24シェルフをCisco 9336C-FX2スイッチに接続するAFF A50システムをケーブル接続します。

Controllers connecting switch-attached shelves			
Switch Port	Port Use	AFF A50	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4b
2		e4a	e4b
3	MetroCluster 2, Local Cluster interface	e4a	e4b
4		e4a	e4b
5	Storage shelf 1 (9)	NSM-1, e0a	NSM-1, e0b
6		NSM-2, e0a	NSM-2, e0b
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9	MetroCluster 1, MetroCluster interface	e2a	e2b
10		e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b
12		e2a	e2b
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster	
14			
15			
16			
17	MetroCluster 1, Ethernet Storage Interface	e3a	e3b
18			
19	MetroCluster 2, Ethernet Storage Interface	e3a	e3b
20			
21	Storage shelf 2 (8)	NSM-1, e0a	NSM-1, e0b
22		NSM-2, e0a	NSM-2, e0b
23	Storage shelf 3 (7)	NSM-1, e0a	NSM-1, e0b
24		NSM-2, e0a	NSM-2, e0b
25	Storage shelf 4 (6)	NSM-1, e0a	NSM-1, e0b
26		NSM-2, e0a	NSM-2, e0b
27	Storage shelf 5 (5)		
28			
29	Storage shelf 6 (4)	NSM-1, e0a	NSM-1, e0b
30		NSM-2, e0a	NSM-2, e0b
31	Storage shelf 7 (3)	NSM-1, e0a	NSM-1, e0b
32		NSM-2, e0a	NSM-2, e0b
33	Storage shelf 8 (2)	NSM-1, e0a	NSM-1, e0b
34		NSM-2, e0a	NSM-2, e0b
35	Storage shelf 9 (1)	NSM-1, e0a	NSM-1, e0b
36		NSM-2, e0a	NSM-2, e0b

## NS224ストレージプラットフォームのポート割り当てを接続するCisco 9336C-FX2スイッチ（グループ4）

プラットフォームポート割り当てを確認し、スイッチ接続のNSS24シェルフをCisco 9336C-FX2スイッチに接続するAFF A700、AFF A900、ASA C800、AFF A800、AFF C800、またはASA A900システムをケーブル接続します。

Controllers connecting switch-attached shelves							
Switch Port	Port Use	AFF A700		AFF C800 ASA C800 AFF A800		AFF A900 ASA A900	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
2							
3	MetroCluster 2, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
4							
5	Storage shelf 1 (9)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
6		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b
10							
11	MetroCluster 2, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b
12							
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14							
15							
16							
17	MetroCluster 1, Ethernet Storage Interface	e3a	e3b / e7b	e5a	e5b / e3b	e3a (option 1)	e3b (option 1)
18						e2a (option 2)	e10b (option 2)
19	MetroCluster 2, Ethernet Storage Interface	e3a	e3b / e7b	e5a	e5b / e3b	e3a (option 1)	e3b (option 1)
20						e2a (option 2)	e10b (option 2)
21	Storage shelf 2 (8)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
22		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
23	Storage shelf 3 (7)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
24		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
25	Storage shelf 4 (6)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
26		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
27	Storage shelf 5 (5)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
28		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
29	Storage shelf 6 (4)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
30		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
31	Storage shelf 7 (3)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
32		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
33	Storage shelf 8 (2)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
34		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
35	Storage shelf 9 (1)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
36		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b

\*注1\* : X91440Aアダプタ（40Gbps）を使用している場合は、ポートe4aとe4e、またはe4aとe8aのいずれかを使用します。ポートe4aとe4b、またはX91153Aアダプタ（100Gbps）を使用している場合はe4aとe8aのいずれかを使用します。

## NS224ストレージプラットフォームのポート割り当てを接続するCisco 9336C-FX2スイッチ（グループ5）

プラットフォームポート割り当てを確認し、スイッチ接続NSS24シェルフをCisco 9336C-FX2スイッチに接続するAFF A70、AFF C80、AFF A90、またはAFF A1Kシステムをケーブル接続します。

Controllers connecting switch-attached shelves									
Switch Port	Port Use	AFF A70		AFF C80		AFF A90		AFF A1K	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
2									
3	MetroCluster 2, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
4									
5	Storage shelf 1 (9)	NSM-1, e0a	NSM-1, e0b						
6		NSM-2, e0a	NSM-2, e0b						
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster							
8									
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
10									
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
12									
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14									
15									
16									
17	MetroCluster 1, Ethernet Storage Interface	e8a (option 1)	e8b (option 1)						
18		e11a (option 2)	e11b (option 2)						
19	MetroCluster 2, Ethernet Storage Interface	e8a (option 1)	e8b (option 1)						
20		e11a (option 2)	e11b (option 2)						
21	Storage shelf 2 (8)	NSM-1, e0a	NSM-1, e0b						
22		NSM-2, e0a	NSM-2, e0b						
23	Storage shelf 3 (7)	NSM-1, e0a	NSM-1, e0b						
24		NSM-2, e0a	NSM-2, e0b						
25	Storage shelf 4 (6)	NSM-1, e0a	NSM-1, e0b						
26		NSM-2, e0a	NSM-2, e0b						
27	Storage shelf 5 (5)	NSM-1, e0a	NSM-1, e0b						
28		NSM-2, e0a	NSM-2, e0b						
29	Storage shelf 6 (4)	NSM-1, e0a	NSM-1, e0b						
30		NSM-2, e0a	NSM-2, e0b						
31	Storage shelf 7 (3)	NSM-1, e0a	NSM-1, e0b						
32		NSM-2, e0a	NSM-2, e0b						
33	Storage shelf 8 (2)	NSM-1, e0a	NSM-1, e0b						
34		NSM-2, e0a	NSM-2, e0b						
35	Storage shelf 9 (1)	NSM-1, e0a	NSM-1, e0b						
36		NSM-2, e0a	NSM-2, e0b						

コントローラがスイッチ接続NS224シェルフを接続しない

スイッチ接続NS224シェルフを接続しないコントローラのポート割り当て表を確認します。

プラットフォーム	使用するケーブル接続テーブル
AFF A150、ASA A150 FAS2750、AFF A220	Cisco 9336C-FX2スイッチがNS224ストレージプラットフォームのポート割り当てを接続しない (グループ6)
AFF A20用	Cisco 9336C-FX2スイッチがNS224ストレージプラットフォームのポート割り当てを接続しない (グループ7)
FAS500f AFF C250、ASA C250 AFF A250、ASA A250	Cisco 9336C-FX2スイッチがNS224ストレージプラットフォームのポート割り当てを接続しない (グループ8)

プラットフォーム	使用するケーブル接続テーブル
AFF C30、AFF A30 FAS50 AFF C60	次の表は、25G（グループ9a）と100G（グループ9b）のどちらのイーサネットカードを使用しているかによって異なります。 <ul style="list-style-type: none"> <li>• Cisco 9336C-FX2スイッチでNS224ストレージプラットフォームのポート割り当てが接続されない（グループ9a）</li> <li>• Cisco 9336C-FX2スイッチがNS224ストレージプラットフォームのポート割り当てを接続しない（グループ9b）</li> </ul>
FAS8200、AFF A300	Cisco 9336C-FX2スイッチがNS224ストレージプラットフォームのポート割り当てを接続しない（グループ10）
AFF A320 FAS8300、AFF C400、ASA C400 、FAS8700 AFF A400 、ASA A400	Cisco 9336C-FX2スイッチがNS224ストレージプラットフォームのポート割り当てを接続しない（グループ11）
AFF A50用	Cisco 9336C-FX2スイッチがNS224ストレージプラットフォームのポート割り当てを接続しない（グループ12）
FAS9000、AFF A700 AFF C800、ASA C800、AFF A800、ASA A800 FAS9500、AFF A900、 ASA A900	Cisco 9336C-FX2スイッチがNS224ストレージプラットフォームのポート割り当てを接続しない（グループ13）
FAS70、AFF A70 AFF C80 FAS90、AFF A90 AFF A1K	Cisco 9336C-FX2スイッチがNS224ストレージプラットフォームのポート割り当てを接続しない（グループ14）

**Cisco 9336C-FX2スイッチがNS224ストレージプラットフォームのポート割り当てを接続しない（グループ6）**

プラットフォームポート割り当てを確認し、スイッチ接続NSS24シェルフをCisco 9336C-FX2スイッチに接続していないAFF A150、ASA A150、FAS2750、またはAFF A220システムをケーブル接続します。

Controllers not connecting switch-attached shelves			
Switch Port	Port Use	AFF A150 ASA A150 FAS2750 AFF A220	
		IP_Switch_x_1	IP_Switch_x_2
1 - 6	Unused	disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9/1	MetroCluster 1, Shared Cluster and MetroCluster interface	e0a	e0b
9/2-4		disabled	
10/1		e0a	e0b
10/2-4		disabled	
11/1	MetroCluster 2, Shared Cluster and MetroCluster interface	e0a	e0b
11/2-4		disabled	
12/1		e0a	e0b
12/2-4		disabled	
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster	
14			
15			
16			
17-36	Unused	disabled	

**Cisco 9336C-FX2**スイッチが**NS224**ストレージプラットフォームのポート割り当てを接続しない（グループ7）プラットフォームポート割り当てを確認し、スイッチ接続NSS24シェルフをCisco 9336C-FX2スイッチに接続していないAFF A20システムをケーブル接続します。

Controllers not connecting switch-attached shelves			
Switch Port	Port Use	AFF A20	
		IP_Switch_x_1	IP_Switch_x_2
1/1	MetroCluster 1, Local Cluster interface	e2a	e4a
1/2-4		disabled	
2/1		e2a	e4a
2/2-4		disabled	
3/1	MetroCluster 2, Local Cluster interface	e2a	e4a
3/2-4		disabled	
4/1		e2a	e4a
4/2-4		disabled	
5-6	Unused	disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9/1	MetroCluster 1, MetroCluster interface	e2b	e4b
9/2-4		disabled	
10/1		e2b	e4b
10/2-4		disabled	
11/1	MetroCluster 2, MetroCluster interface	e2b	e4b
11/2-4		disabled	
12/1		e2b	e4b
12/2-4		disabled	
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster	
14			
15			
16			
17-36	Unused	disabled	

**Cisco 9336C-FX2**スイッチが**NS224**ストレージプラットフォームのポート割り当てを接続しない（グループ8）

プラットフォームポート割り当てを確認し、スイッチ接続NSS24シェルフをCisco 9336C-FX2スイッチに接続していないFAS500f、AFF C250、ASA C250、AFF A250、またはASAA250システムをケーブル接続します。

Controllers not connecting switch-attached shelves			
Switch Port	Port Use	FAS500f AFF C250 ASA C250 AFF A250 ASA A250	
		IP_Switch_x_1	IP_Switch_x_2
1 - 6	Unused	disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9/1	MetroCluster 1, Shared Cluster and MetroCluster interface	e0c	e0d
9/2-4		disabled	
10/1		e0c	e0d
10/2-4		disabled	
11/1	MetroCluster 2, Shared Cluster and MetroCluster interface	e0c	e0d
11/2-4		disabled	
12/1		e0c	e0d
12/2-4		disabled	
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster	
14			
15			
16			
17-36	Unused	disabled	

**Cisco 9336C-FX2**スイッチで**NS224**ストレージプラットフォームのポート割り当てが接続されない（グループ**9a**）プラットフォームポート割り当てを確認し、4ポート25Gイーサネットカードを使用してスイッチ接続NSS24シェルフをCisco 9336C-FX2スイッチに接続していないAFF A30、AFF C30、AFF C60、またはFAS50システムをケーブル接続します。



この構成では、ローカルクラスタとHAインターフェイスを接続するために、スロット4に4ポートの25Gイーサネットカードが必要です。

Controllers not connecting switch-attached shelves							
Switch Port	Port use	AFF C30 (25G Cluster/HA) AFF A30 (25G Cluster/HA)		FAS50 (25G Cluster/HA)		AFF C60 (25G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1/1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
1/2-4		disabled		disabled		disabled	
2/1		e4a	e4b	e4a	e4b	e4a	e4b
2/2-4		disabled		disabled		disabled	
3/1	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
3/2-4		disabled		disabled		disabled	
4/1		e4a	e4b	e4a	e4b	e4a	e4b
4/2-4		disabled		disabled		disabled	
5-6	Unused	disabled		disabled		disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
9	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
10	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
12	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
15		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
16		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
17-36	Unused	disabled		disabled		disabled	

**Cisco 9336C-FX2**スイッチが**NS224**ストレージプラットフォームのポート割り当てを接続しない（グループ**9b**）プラットフォームポート割り当てを確認し、2ポート100Gイーサネットカードを使用してスイッチ接続NSS24シェルフをCisco 9336C-FX2スイッチに接続していないAFF A30、AFF C30、AFF C60、またはFAS50システムをケーブル接続します。



この構成では、ローカルクラスターとHAインターフェイスを接続するために、スロット4に2ポートの100Gイーサネットカードが必要です。

Controllers not connecting switch-attached shelves							
Switch Port	Port use	AFF C30 (100G Cluster/HA) AFF A30 (100G Cluster/HA)		FAS50 (100G Cluster/HA)		AFF C60 (100G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
2	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
3	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
4	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
5-6	Unused	disabled		disabled		disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
9	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
10	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
12	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
15		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
16		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
17-36	Unused	disabled		disabled		disabled	

**Cisco 9336C-FX2**スイッチが**NS224**ストレージプラットフォームのポート割り当てを接続しない（グループ**10**）プラットフォームポート割り当てを確認し、スイッチ接続NSS24シェルフをCisco 9336C-FX2スイッチに接続していないFAS8200またはAFF A300システムをケーブル接続します。

Controllers not connecting switch-attached shelves			
Switch Port	Port Use	FAS8200 AFF A300	
		IP_Switch_x_1	IP_Switch_x_2
1/1	MetroCluster 1, Local Cluster interface	e0a	e0b
1/2-4		disabled	
2/1		e0a	e0b
2/2-4		disabled	
3/1	MetroCluster 2, Local Cluster interface	e0a	e0b
3/2-4		disabled	
4/1		e0a	e0b
4/2-4		disabled	
5-6	Unused	disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9/1	MetroCluster 1, MetroCluster interface	e1a	e1b
9/2-4		disabled	
10/1		e1a	e1b
10/2-4		disabled	
11/1	MetroCluster 2, MetroCluster interface	e1a	e1b
11/2-4		disabled	
12/1		e1a	e1b
12/2-4		disabled	
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster	
14			
15			
16			
17-36	Unused	disabled	

**Cisco 9336C-FX2**スイッチが**NS224**ストレージプラットフォームのポート割り当てを接続しない（グループ11）

プラットフォームポート割り当てを確認し、スイッチ接続NSS24シェルフをFAS8300 Cisco 9336C-FX2スイッチに接続していないAFF A320 ASAA400、FAS8700、AFF C400 AFF A400、またはASA C400システムをケーブル接続します。

Controllers not connecting switch-attached shelves							
Switch Port	Port Use	AFF A320		FAS8300 AFF C400 ASA C400 FAS8700		AFF A400 ASA A400	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b
2							
3	MetroCluster 2, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b
4							
5-6	Unused	disabled		disabled		disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b
10							
11	MetroCluster 2, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b
12							
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14							
15							
16							
17-36	Unused	disabled		disabled		disabled	

**Cisco 9336C-FX2**スイッチが**NS224**ストレージプラットフォームのポート割り当てを接続しない（グループ12）  
プラットフォームポート割り当てを確認し、スイッチ接続NSS24シェルフをCisco 9336C-FX2スイッチに接続していないAFF A50システムをケーブル接続します。

Controllers not connecting switch-attached shelves			
Switch Port	Port use	AFF A50	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4b
2			
3	MetroCluster 2, Local Cluster interface	e4a	e4b
4			
5-6	Unused	disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9	MetroCluster 1, MetroCluster interface	e2a	e2b
10			
11	MetroCluster 2, MetroCluster interface	e2a	e2b
12			
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster	
14			
15			
16			
17-36	Unused	disabled	

**Cisco 9336C-FX2**スイッチが**NS224**ストレージプラットフォームのポート割り当てを接続しない（グループ13）  
プラットフォームポート割り当てを確認し、スイッチ接続NSS24シェルフをASA C800 Cisco 9336C-FX2スイッチに接続していないFAS9000、AFF A800 AFF A900、ASA A800 ASA A900、FAS9500、AFF A700、またはAFF C800システムをケーブル接続します。

Controllers not connecting switch-attached shelves							
Switch Port	Port Use	FAS9000 AFF A700		AFF C800 ASA C800 AFF A800 ASA A800		FAS9500 AFF A900 ASA A900	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
2							
3	MetroCluster 2, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
4							
5-6	Unused	disabled		disabled		disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b
10							
11	MetroCluster 2, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b
12							
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14							
15							
16							
17-36	Unused	disabled		disabled		disabled	

\*注1\* : X91440Aアダプタ (40Gbps) を使用している場合は、ポートe4aとe4e、またはe4aとe8aのいずれかを使用します。ポートe4aとe4b、またはX91153Aアダプタ (100Gbps) を使用している場合はe4aとe8aのいずれかを使用します。

**Cisco 9336C-FX2**スイッチが**NS224**ストレージプラットフォームのポート割り当てを接続しない (グループ**14**)

プラットフォームポート割り当てを確認し、スイッチ接続**NSS24**シェルフをCisco 9336C-FX2スイッチに接続していない**AFF A70**、**FAS70**、**AFF C80**、**FAS90**、**AFF A90**、または**AFF A1K**システムをケーブル接続します。

Controllers not connecting switch-attached shelves									
Switch Port	Port Use	FAS70 AFF A70		AFF C80		FAS90 AFF A90		AFF A1K	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
2									
3	MetroCluster 2, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
4									
5-6	Unused	disabled		disabled		disabled		disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster							
8									
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
10									
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
12									
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14									
15									
16									
17-36	Unused	disabled		disabled		disabled		disabled	

**MetroCluster IP**構成における**Broadcom**対応**BES-53248 IP**スイッチのプラットフォームポート割り当て

**MetroCluster IP**構成で使用するポートは、スイッチのモデルとプラットフォームのタイプによって異なります。

構成テーブルを使用する前に、次の考慮事項を確認してください。

- 速度が異なるリモートISLポート (25Gbpsポートを10Gbps ISLポートに接続した場合など) のスイッチは使用できません。

- スイッチをMetroCluster FCからIPへの移行用に設定する場合は、選択したターゲットプラットフォームに応じて次のポートが使用されます。

ターゲットプラットフォーム	ポート
FAS500f、AFF C250、ASA C250、AFF A250、ASA A250、FAS8300、AFF C400、ASA C400、AFF A400、ASA A400、またはFAS8700プラットフォーム	ポート1~6、10Gbps
FAS8200またはAFF A300プラットフォーム	ポート3 <sub>4</sub> および9 <sub>12</sub> 、10Gbps

- AFF A320 システムが Broadcom BES-53248 スイッチで構成されている場合、一部の機能がサポートされないことがあります。

ローカルクラスタ接続を必要とする設定または機能がスイッチに接続されていても、サポートされていません。たとえば、次の設定と手順はサポートされていません。

- 8 ノード MetroCluster 構成
- MetroCluster FC から MetroCluster IP 構成への移行
- 4 ノード MetroCluster IP 構成の更新（ONTAP 9.8 以降）

構成に適したケーブル接続テーブルを選択

次の表を使用して、必要なケーブル接続の表を特定します。

システムの状態	使用するケーブル接続テーブル
AFF A150、ASA A150向け FAS2750 AFF A220	<a href="#">Broadcom BES-53248プラットフォームのポート割り当て（グループ1）</a>
FAS500f、AFF C250、ASA C250、AFF A250、ASA A250	<a href="#">Broadcom BES-53248プラットフォームのポート割り当て（グループ2）</a>
AFF A20用	<a href="#">Broadcom BES-53248プラットフォームのポート割り当て（グループ3）</a>
AFF C30、AFF A30 FAS50、AFF C60	<a href="#">Broadcom BES-53248プラットフォームのポート割り当て（グループ4）</a>
FAS8200、AFF A300	<a href="#">Broadcom BES-53248プラットフォームのポート割り当て（グループ5）</a>
AFF A320	<a href="#">Broadcom BES-53248プラットフォームのポート割り当て（グループ6）</a>
FAS8300、AFF C400、ASA C400、AFF A400、ASA A400、FAS8700	<a href="#">Broadcom BES-53248プラットフォームのポート割り当て（グループ7）</a>

#### **Broadcom BES-53248プラットフォームのポート割り当て（グループ1）**

プラットフォームポート割り当てを確認し、AFF A150、ASA A150、FAS2750、またはAFF A220システムをBroadcom BES-53248スイッチにケーブル接続します。

Physical Port	Port use	AFF A150 ASA A150 FAS2750 AFF A220	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Shared Cluster and MetroCluster interface	e0a	e0b
2			
3	MetroCluster 2, Shared Cluster and MetroCluster interface	e0a	e0b
4			
5-8	Unused	disabled	
9	MetroCluster 3, Shared Cluster and MetroCluster interface	e0a	e0b
10			
11	MetroCluster 4, Shared Cluster and MetroCluster interface	e0a	e0b
12			
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster	
14			
15			
16			
..	Ports not licensed (17 - 54)		
53	ISL, MetroCluster, native speed 40G / 100G (Note 1)	ISL, MetroCluster	
54			
55	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
56			

- \*注1\*：これらのポートを使用するには、追加ライセンスが必要です。
- 両方のMetroCluster構成で同じプラットフォームを使用している場合、NetAppは一方の構成にグループ「MetroCluster 3」を、もう一方の構成にグループ「MetroCluster 4」を選択することを推奨します。プラットフォームが異なる場合は、最初の構成で「MetroCluster 3」または「MetroCluster 4」を選択し、2つ目の構成で「MetroCluster 1」または「MetroCluster 2」を選択する必要があります。

#### Broadcom BES-53248プラットフォームのポート割り当て（グループ2）

プラットフォームポート割り当てを確認し、FAS500f、AFF C250、ASA C250、AFF A250、またはASA A250システムをBroadcom BES-53248スイッチにケーブル接続します。

Physical Port	Port use	FAS500f AFF C250 ASA C250 AFF A250 ASA A250	
		IP_Switch_x_1	IP_Switch_x_2
1 - 4	Unused	disabled	
5	MetroCluster 1, Shared Cluster and MetroCluster interface	e0c	e0d
6			
7	MetroCluster 2, Shared Cluster and MetroCluster interface	e0c	e0d
8			
9	MetroCluster 3, Shared Cluster and MetroCluster interface	e0c	e0d
10			
11	MetroCluster 4, Shared Cluster and MetroCluster interface	e0c	e0d
12			
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster	
14			
15			
16			
..	Ports not licensed (17 - 54)		
53	ISL, MetroCluster, native speed 40G / 100G (Note 1)	ISL, MetroCluster	
54			
55	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
56			

- \*注1\*：これらのポートを使用するには、追加ライセンスが必要です。
- 両方のMetroCluster構成で同じプラットフォームを使用している場合、NetAppは一方の構成にグループ「MetroCluster 3」を、もう一方の構成にグループ「MetroCluster 4」を選択することを推奨します。プラットフォームが異なる場合は、最初の構成で「MetroCluster 3」または「MetroCluster 4」を選択し、2つ目の構成で「MetroCluster 1」または「MetroCluster 2」を選択する必要があります。

#### Broadcom BES-53248プラットフォームのポート割り当て（グループ3）

プラットフォームポートの割り当てを確認し、AFF A20システムをBroadcom BES-53248スイッチにケーブル接続します。

Physical Port	Port use	AFF A20	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e2a	e4a
2			
3	MetroCluster 2, Local Cluster interface	e2a	e4a
4			
5	MetroCluster 1, MetroCluster interface	e2b	e4b
6			
7	MetroCluster 2, MetroCluster interface	e2b	e4b
8			
9 - 12	Unused	disabled	
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster	
14			
15			
16			
17	MetroCluster 3, Local Cluster interface (note 1)	e2a	e4a
18			
19	MetroCluster 3, MetroCluster interface (note 1)	e2b	e4b
20			
21	MetroCluster 4, Local Cluster interface (note 1)	e2a	e4a
22			
23	MetroCluster 4, MetroCluster interface (note 1)	e2b	e4b
24			
..	Ports not licensed (25 - 54)		
53	ISL, MetroCluster, native speed 40G / 100G (note 1)	ISL, MetroCluster	
54			
55	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
56			

• \*注1\* : これらのポートを使用するには、追加ライセンスが必要です。

#### Broadcom BES-53248プラットフォームのポート割り当て (グループ4)

プラットフォームポートの割り当てを確認し、4ポートの25Gイーサネットカードを使用してAFF A30、AFF C30、AFF C60、またはFAS50システムをBroadcom BES-53248スイッチにケーブル接続します。



- この構成では、ローカルクラスターとHAインターフェイスを接続するために、スロット4に4ポートの25Gイーサネットカードが必要です。
- この構成では、25Gbpsのネットワーク速度をサポートするために、コントローラのカードにQSFP / SFP+アダプタが必要です。

Physical Port	Port use	AFF C30 (25G Cluster/HA) AFF A30 (25G Cluster/HA)		FAS50 (25G Cluster/HA)		AFF C60 (25G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
2							
3	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
4							
5	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
6							
7	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
8							
9 - 12	Unused	disabled		disabled		disabled	
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14							
15							
16							
17	MetroCluster 3, Local Cluster interface (note 1)	e4a	e4b	e4a	e4b	e4a	e4b
18							
19	MetroCluster 3, MetroCluster interface (note 1)	e2a	e2b	e2a	e2b	e2a	e2b
20							
21	MetroCluster 4, Local Cluster interface (note 1)	e4a	e4b	e4a	e4b	e4a	e4b
22							
23	MetroCluster 4, MetroCluster interface (note 1)	e2a	e2b	e2a	e2b	e2a	e2b
24							
..	Ports not licensed (25 - 54)						
53	ISL, MetroCluster, native speed 40G / 100G (note 1)	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
54							
55	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
56							

• \*注1\* : これらのポートを使用するには、追加ライセンスが必要です。

#### Broadcom BES-53248プラットフォームのポート割り当て（グループ5）

プラットフォームポート割り当てを確認し、FAS8200またはAFF A300システムをBroadcom BES-53248スイッチにケーブル接続します。

Physical Port	Port use	FAS8200 AFF A300	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0a	e0b
2			
3	MetroCluster 2, Local Cluster interface	e0a	e0b
4			
5	MetroCluster 1, MetroCluster interface	e1a	e1b
6			
7	MetroCluster 2, MetroCluster interface	e1a	e1b
8			
9 - 12	Unused	disabled	
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster	
14			
15			
16			
..	Ports not licensed (17 - 54)		
53	ISL, MetroCluster, native speed 40G / 100G (note 1)	ISL, MetroCluster	
54			
55	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
56			

- \*注1\*：これらのポートを使用するには、追加ライセンスが必要です。

#### Broadcom BES-53248プラットフォームのポート割り当て（グループ6）

プラットフォームポートの割り当てを確認し、AFF A320システムをBroadcom BES-53248スイッチにケーブル接続します。

Physical Port	Port use	AFF A320	
		IP_Switch_x_1	IP_Switch_x_2
1 - 12	Ports not used (Note 2)	disabled	
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster	
14			
15			
16			
..	Ports not licensed (17 - 54)		
53	ISL, MetroCluster, native speed 40G / 100G (see Note 1)	ISL, MetroCluster	
54			
55	MetroCluster 1, MetroCluster interface (Note 2)	e0g	e0h
56			

- \*注1\*：これらのポートを使用するには、追加ライセンスが必要です。
- \*注2\*：AFF A320システムを使用する単一の4ノードMetroClusterのみをスイッチに接続できます。

この構成では、スイッチクラスタを必要とする機能はサポートされません。これには、MetroClusterのFCからIPへの移行と機器更改の手順が含まれます。

#### Broadcom BES-53248プラットフォームのポート割り当て（グループ7）

FAS8300、AFF C400、ASA C400、AFF A400、ASA A400をケーブル接続するためのプラットフォームポート割り当てを確認します。またはFAS8700システムからBroadcom BES-53248スイッチへの接続：

Physical Port	Port use	FAS8300 AFF C400 ASA C400 FAS8700		AFF A400 ASA A400	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1 - 12	Ports not used (see Note 2)	disabled		disabled	
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster		ISL, MetroCluster	
14					
15					
16					
..	Ports not licensed (17 - 48)				
49	MetroCluster 5, Local Cluster interface (Note 1)	e0c	e0d	e3a	e3b
50					
51	MetroCluster 5, MetroCluster interface (Note 1)	e1a	e1b	e1a	e1b
52					
53	ISL, MetroCluster, native speed 40G / 100G (Note 1)	ISL, MetroCluster		ISL, MetroCluster	
54					
55	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster	
56					

- \*注1\*：これらのポートを使用するには、追加ライセンスが必要です。
- \*注2\*：AFF A320システムを使用する単一の4ノードMetroClusterのみをスイッチに接続できます。

この構成では、スイッチクラスタを必要とする機能はサポートされません。これには、MetroClusterのFCからIPへの移行と機器更改の手順が含まれます。

## MetroCluster IP構成におけるNVIDIA対応SN2100 IPスイッチのプラットフォームポート割り当て

MetroCluster IP 構成で使用するポートは、スイッチのモデルとプラットフォームのタイプによって異なります。

構成テーブルを使用する前に、次の考慮事項を確認してください。

- 8ノードまたは2つの4ノードMetroCluster構成を接続するには、ONTAP 9.14.1以降とRCFファイルバージョン2.00以降が必要です。



RCFファイルのバージョンは、ファイルの生成に使用されるRCFfilegeneratorツールのバージョンとは異なります。たとえば、RCFファイルジェネレータv1.6cを使用してバージョン2.00のRCFファイルを生成できます。

- 複数のMetroCluster 構成をケーブル接続する場合は、該当する表に従ってください。例：
  - タイプがAFF A700の2つの4ノードMetroCluster 構成をケーブル接続する場合は、AFF A700の表で「MetroCluster 1」と表示されている最初のMetroCluster と「MetroCluster 2」と表示されている2つ目のMetroCluster を接続します。



ポート13と14は、40Gbpsと100Gbpsをサポートするネイティブ速度モードまたは4×25Gbpsをサポートするブレイクアウトモードで使用できます。ネイティブ速度モードを使用している場合は、ポート13と14として表されます。ブレイクアウトモード（4×25Gbpsまたは4×10Gbps）を使用する場合、ポート13s0-3および14s0-3として表されます。

以降の各セクションでは、物理的なケーブル接続の概要について説明します。を参照することもできます ["RcfFileGenerator の順にクリックします"](#) ケーブル接続の詳細については、を参照して

構成に適したケーブル接続テーブルを選択

次の表を使用して、必要なケーブル接続の表を特定します。

システムの状態	使用するケーブル接続テーブル
AFF A150、ASA A150向け FAS500f AFF C250、ASA C250向け AFF A250、ASA A250向け	NVIDIA SN2100プラットフォームのポート割り当て (グループ1)

システムの状態	使用するケーブル接続テーブル
AFF A20用	NVIDIA SN2100プラットフォームのポート割り当て (グループ2)
AFF C30、AFF A30 FAS50 AFF C60	次の表は、25G (グループ3a) と100G (グループ3b) のどちらのイーサネットカードを使用しているかによって異なります。  <ul style="list-style-type: none"> <li>• NVIDIA SN2100プラットフォームのポート割り当て (グループ3a-25G)</li> <li>• NVIDIA SN2100プラットフォームのポート割り当て (グループ3b-100G)</li> </ul>
FAS8300 AFF C400 、ASA C400 AFF A400 、ASA A400 FAS8700 FAS9000、AFF A700	NVIDIA SN2100プラットフォームのポート割り当て (グループ4)
AFF A50用	NVIDIA SN2100プラットフォームのポート割り当て (グループ5)
AFF C800、ASA C800 AFF A800、ASA A800 FAS9500 AFF A900 、ASA A900	NVIDIA SN2100プラットフォームのポート割り当て (グループ6)
FAS70、AFF A70 AFF C80 FAS90、AFF A90 AFF A1K	NVIDIA SN2100プラットフォームのポート割り当て (グループ7)

#### NVIDIA SN2100プラットフォームのポート割り当て (グループ1)

プラットフォームポートの割り当てを確認して、AFF A150、ASA A150、FAS500f、AFF C250、ASA C250、AFF A250またはASA A250システムからNVIDIA SN2100スイッチへの接続：

Switch Port	Port use	AFF A150 ASA A150		FAS500F AFF C250 ASA C250 AFF A250 ASA A250	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1 - 6	Unused	disabled		disabled	
7s0	MetroCluster 1, Shared Cluster and MetroCluster interface	e0c	e0d	e0c	e0d
7s1-3		disabled		disabled	
8s0		e0c	e0d	e0c	e0d
8s1-3		disabled		disabled	
9s0	MetroCluster 2, Shared Cluster and MetroCluster interface	e0c	e0d	e0c	e0d
9s1-3		disabled		disabled	
10s0		e0c	e0d	e0c	e0d
10s1-3		disabled		disabled	
11s0	MetroCluster 3, Shared Cluster and MetroCluster interface	e0c	e0d	e0c	e0d
11s1-3		disabled		disabled	
12s0		e0c	e0d	e0c	e0d
12s1-3		disabled		disabled	
13 / 13s0-3	MetroCluster ISL 40/100G or 4x25G or 4x10G	ISL, MetroCluster		ISL, MetroCluster	
14 / 14s0-3		ISL, MetroCluster		ISL, MetroCluster	
15	ISL, Local Cluster	ISL, Local Cluster		ISL, Local Cluster	
16	100G	ISL, Local Cluster		ISL, Local Cluster	

#### NVIDIA SN2100プラットフォームのポート割り当て (グループ2)

プラットフォームポートの割り当てを確認して、AFF A20システムをNVIDIA SN2100スイッチにケーブル接続します。

Switch Port	Port use	AFF A20	
		IP_Switch_x_1	IP_Switch_x_2
1s0	MetroCluster 1, Local Cluster interface	e2a	e4a
s1s1-3		disabled	
2s0		e2a	e4a
2s1-3		disabled	
3s0	MetroCluster 2, Local Cluster interface	e2a	e4a
3s1-3		disabled	
4s0		e2a	e4a
4s1-3		disabled	
5s0	MetroCluster 3, Local Cluster interface	e2a	e4a
5s1-3		disabled	
6s0		e2a	e4a
6s1-3		disabled	
7	MetroCluster 1, MetroCluster interface	e2b	e4b
8			
9	MetroCluster 2, MetroCluster interface	e2b	e4b
10			
11	MetroCluster 3, MetroCluster interface	e2b	e4b
12			
13 / 13s0-3	MetroCluster ISL 40/100G or 4x25G or 4x10G	ISL, MetroCluster	
14 / 14s0-3			
15	ISL, Local Cluster 100G	ISL, Local Cluster	
16			

### NVIDIA SN2100プラットフォームのポート割り当て（グループ3a）

プラットフォームポート割り当てを確認し、4ポートの25Gイーサネットカードを使用してAFF A30、AFF C30、AFF C60、またはFAS50システムをNVIDIA SN2100スイッチにケーブル接続します。



この構成では、ローカルクラスターとHAインターフェイスを接続するために、スロット4に4ポートの25Gイーサネットカードが必要です。

Switch Port	Port use	AFF C30 (25G Cluster/HA) AFF A30 (25G Cluster/HA)		FAS50 (25G Cluster/HA)		AFF C60 (25G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1s0	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
s1s1-3		disabled		disabled		disabled	
2s0		e4a	e4b	e4a	e4b	e4a	e4b
2s1-3		disabled		disabled		disabled	
3s0	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
3s1-3		disabled		disabled		disabled	
4s0		e4a	e4b	e4a	e4b	e4a	e4b
4s1-3		disabled		disabled		disabled	
5s0	MetroCluster 3, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
5s1-3		disabled		disabled		disabled	
6s0		e4a	e4b	e4a	e4b	e4a	e4b
6s1-3		disabled		disabled		disabled	
7	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
8	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
9	MetroCluster 3, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
10	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
12	MetroCluster 3, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
13 / 13s0-3	MetroCluster ISL	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14 / 14s0-3	40/100G or 4x25G or 4x10G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
15	ISL, Local Cluster	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
16	100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	

### NVIDIA SN2100プラットフォームのポート割り当て (グループ3b)

プラットフォームポート割り当てを確認し、2ポート100Gイーサネットカードを使用してAFF A30、AFF C30、AFF C60、またはFAS50システムをNVIDIA SN2100スイッチにケーブル接続します。



この構成では、ローカルクラスターとHAインターフェイスを接続するために、スロット4に2ポートの100Gイーサネットカードが必要です。

Switch Port	Port use	AFF C30 (100G Cluster/HA) AFF A30 (100G Cluster/HA)		FAS50 (100G Cluster/HA)		AFF C60 (100G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
2	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
3	MetroCluster 3, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
4	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
5	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
6	MetroCluster 3, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
7	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
8	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
9	MetroCluster 3, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
10	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
12	MetroCluster 3, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
13 / 13s0-3	MetroCluster ISL	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14 / 14s0-3	40/100G or 4x25G or 4x10G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
15	ISL, Local Cluster	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
16	100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	

### NVIDIA SN2100プラットフォームのポート割り当て (グループ4)

FAS8300、AFF C400、ASA C400、AFF A400、ASA A400をケーブル接続するためのプラットフォームポート割り当てを確認します。FAS8700、FAS9000、またはAFF A700システムからNVIDIA SN2100スイッチへの接続：

Switch Port	Port use	FAS8300 AFF C400 ASA C400 FAS8700		AFF A400 ASA A400		FAS9000 AFF A700	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0c	e0d	e3a	e3b	e4a	e4e / e8a Note 1
2							
3	MetroCluster 2, Local Cluster interface	e0c	e0d	e3a	e3b	e4a	e4e / e8a Note 1
4							
5	MetroCluster 3, Local Cluster interface	e0c	e0d	e3a	e3b	e4a	e4e / e8a Note 1
6							
7	MetroCluster 1, MetroCluster interface	e1a	e1b	e1a	e1b	e5a	e5b
8							
9	MetroCluster 2, MetroCluster interface	e1a	e1b	e1a	e1b	e5a	e5b
10							
11	MetroCluster 3, MetroCluster interface	e1a	e1b	e1a	e1b	e5a	e5b
12							
13 / 13s0-3	MetroCluster ISL 40/100G or 4x25G or 4x10G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14 / 14s0-3							
15	ISL, Local Cluster 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
16							

\*注1\* : X91440Aアダプタ (40Gbps) を使用している場合は、ポートe4aとe4e、またはe4aとe8aのいずれかを使用します。ポートe4aとe4b、またはX91153Aアダプタ (100Gbps) を使用している場合はe4aとe8aのいずれかを使用します。

#### NVIDIA SN2100プラットフォームのポート割り当て (グループ5)

プラットフォームポートの割り当てを確認して、AFF A50システムをNVIDIA SN2100スイッチにケーブル接続します。

Switch Port	Port use	AFF A50	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4b
2			
3	MetroCluster 2, Local Cluster interface	e4a	e4b
4			
5	MetroCluster 3, Local Cluster interface	e4a	e4b
6			
7	MetroCluster 1, MetroCluster interface	e2a	e2b
8			
9	MetroCluster 2, MetroCluster interface	e2a	e2b
10			
11	MetroCluster 3, MetroCluster interface	e2a	e2b
12			
13 / 13s0-3	MetroCluster ISL 40/100G or 4x25G or 4x10G	ISL, MetroCluster	
14 / 14s0-3			
15	ISL, Local Cluster 100G	ISL, Local Cluster	
16			

#### NVIDIA SN2100プラットフォームのポート割り当て (グループ6)

AFF C800、ASA C800、AFF A800、ASA A800、FAS9500をケーブル接続するためのプラットフォームポート割り当ての確認 AFF A900またはASA A900システムからNVIDIA SN2100スイッチへの接続：

Switch Port	Port use	AFF C800 ASA C800 AFF A800 ASA A800		FAS9500 AFF A900 ASA A900	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0a	e1a	e4a	e4b(e) / e8a Note 1
2					
3	MetroCluster 2, Local Cluster interface	e0a	e1a	e4a	e4b(e) / e8a Note 1
4					
5	MetroCluster 3, Local Cluster interface	e0a	e1a	e4a	e4b(e) / e8a Note 1
6					
7	MetroCluster 1, MetroCluster interface	e0b	e1b	e5b	e7b
8					
9	MetroCluster 2, MetroCluster interface	e0b	e1b	e5b	e7b
10					
11	MetroCluster 3, MetroCluster interface	e0b	e1b	e5b	e7b
12					
13 / 13s0-3	MetroCluster ISL 40/100G or 4x25G or 4x10G	ISL, MetroCluster		ISL, MetroCluster	
14 / 14s0-3					
15	ISL, Local Cluster 100G	ISL, Local Cluster		ISL, Local Cluster	
16					

\*注1\* : X91440Aアダプタ (40Gbps) を使用している場合は、ポートe4aとe4e、またはe4aとe8aのいずれかを使用します。ポートe4aとe4b、またはX91153Aアダプタ (100Gbps) を使用している場合はe4aとe8aのいずれかを使用します。

#### NVIDIA SN2100プラットフォームのポート割り当て (グループ7)

プラットフォームポート割り当てを確認し、FAS70、AFF A70、AFF C80、FAS90、AFF A90、またはAFF A1KシステムをNVIDIA SN2100スイッチにケーブル接続します。

Switch Port	Port use	FAS70 AFF A70		AFF C80		FAS90 AFF A90		AFF A1K	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
2									
3	MetroCluster 2, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
4									
5	MetroCluster 3, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
6									
7	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e3b	e2b	e3b	e2b	e3b
8									
9	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e3b	e2b	e3b	e2b	e3b
10									
11	MetroCluster 3, MetroCluster interface	e2a	e2b	e2a	e3b	e2b	e3b	e2b	e3b
12									
13 / 13s0-3	MetroCluster ISL 40/100G or 4x25G or 4x10G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14 / 14s0-3									
15	ISL, Local Cluster 100G	ISL, Local Cluster							
16									

### MetroCluster IP構成でONTAPコントローラモジュールポートをケーブル接続する

クラスタピアリング、管理、データ接続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。

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

ネットワーク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"

2. 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。

使用しているプラットフォームに対応したインストール手順をで使します ["ONTAPハードウェアシステムのドキュメント"](#)。



MetroCluster IPシステムには、専用のハイアベイラビリティ (HA) ポートはありません。プラットフォームに応じて、HAトラフィックはMetroClusterインターフェイス、ローカルクラスタインターフェイス、または共有クラスタ/MetroClusterインターフェイスを使用して処理されます。ONTAPハードウェアシステムのドキュメント\_を使用してプラットフォームを設置する場合は、手順に従ってクラスタポートとHAポートをケーブル接続しないでください。

## MetroCluster IP スイッチを設定します

適切なMetroCluster IPスイッチ構成手順を選択する

バックエンドMetroCluster IP接続を提供するには、IPスイッチを設定する必要があります。手順はスイッチベンダーによって異なります。

- ["Broadcom IP スイッチを設定します"](#)
- ["Cisco IP スイッチを設定する"](#)
- ["NVIDIA IPスイッチを設定します"](#)

クラスタ相互接続とバックエンドMetroCluster IP 接続用に **Broadcom IP** スイッチを構成する

クラスタインターコネクトおよびバックエンド MetroCluster IP 接続用に **Broadcom IP** スイッチを設定する必要があります。



次のような場合は、構成に追加のライセンス (100Gbポートライセンス×6) が必要になります。

- ポート53および54を40Gbpsまたは100GbpsのMetroCluster ISLとして使用します。
- ローカルクラスタインターフェイスとMetroCluster インターフェイスをポート49-52に接続するプラットフォームを使用します。

**Broadcom IP** スイッチを工場出荷時のデフォルトにリセット

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

このタスクについて

- この手順は、MetroCluster IP 構成の各 IP スイッチで実行する必要があります。
- シリアルコンソールを使用してスイッチに接続する必要があります。
- このタスクでは、管理ネットワークの設定をリセットします。

#### 手順

1. 昇格されたコマンドプロンプト (#):'enable' に変更します

```
(IP_switch_A_1)> enable
(IP_switch_A_1) #
```

2. スタートアップコンフィギュレーションを消去し、バナーを削除します

- a. スタートアップ設定を消去します。

**\*`erase startup-config`\***

```
(IP_switch_A_1) #erase startup-config

Are you sure you want to clear the configuration? (y/n) y

(IP_switch_A_1) #
```

このコマンドでは、バナーは消去されません。

- b. バナーを削除します。

**no set clibanner**

```
(IP_switch_A_1) #configure
(IP_switch_A_1) (Config) # no set clibanner
(IP_switch_A_1) (Config) #
```

3. スイッチを再起動します **\*(IP\_switch\_A\_1) #reload \***

```
Are you sure you would like to reset the system? (y/n) y
```



スイッチをリロードする前に、未保存または変更された設定を保存するかどうかを確認するメッセージが表示された場合は、**No** を選択します。

4. スイッチがリロードされるまで待ってから、スイッチにログインします。

デフォルトのユーザは「admin」で、パスワードは設定されていません。次のようなプロンプトが表示されます。

```
(Routing) >
```

5. 管理者特権のコマンドプロンプトに切り替えます。

「enable」を選択します

```
Routing) > enable  
(Routing) #
```

6. サービスポートプロトコルを「none」に設定します。

「サービスポートプロトコルなし」

```
(Routing) #serviceport protocol none  
Changing protocol mode will reset ip configuration.  
Are you sure you want to continue? (y/n) y  
  
(Routing) #
```

7. サービスポートに IP アドレスを割り当てます。

serviceport IP\_address netmask gateway\_

次の例では、サービスポートに IP アドレス「10.10.10.10」が割り当てられています。サブネットは「255.255.255.0」、ゲートウェイは「10.10.10.1」です。

```
(Routing) #serviceport ip 10.10.10.10 255.255.255.0 10.10.10.1
```

8. サービスポートが正しく設定されていることを確認します。

How serviceport

次の例は、ポートが稼働しており、正しいアドレスが割り当てられていることを示しています。

```
(Routing) #show serviceport

Interface Status..... Up
IP Address..... 10.10.10.10
Subnet Mask..... 255.255.255.0
Default Gateway..... 10.10.10.1
IPv6 Administrative Mode..... Enabled
IPv6 Prefix is .....
fe80::dac4:97ff:fe56:87d7/64
IPv6 Default Router..... fe80::222:bdf8:19ff
Configured IPv4 Protocol..... None
Configured IPv6 Protocol..... None
IPv6 AutoConfig Mode..... Disabled
Burned In MAC Address..... D8:C4:97:56:87:D7

(Routing) #
```

## 9. SSH サーバーを構成します。



- RCF ファイルで Telnet プロトコルが無効になります。SSH サーバを設定しない場合は、シリアルポート接続を使用してブリッジにアクセスする必要があります。
- ログ収集やその他の外部ツールを使用するには、SSH サーバーを構成する必要があります。

### a. RSA キーを生成します。

```
(Routing) #configure
(Routing) (Config)#crypto key generate rsa
```

### b. DSA キーの生成 (オプション)

```
(Routing) #configure
(Routing) (Config)#crypto key generate dsa
```

### c. FIPS 準拠バージョンの EFOS を使用している場合は、ECDSA キーを生成します。次の例では、長さ521のキーを作成します。有効な値は、256、384、または 521 です。

```
(Routing) #configure
(Routing) (Config)#crypto key generate ecdsa 521
```

### d. SSH サーバを有効にします。

必要に応じて、設定コンテキストを終了します。

```
(Routing) (Config) #end
(Routing) #ip ssh server enable
```

+



キーがすでに存在する場合は、それらを上書きするように求められることがあります。

10. 必要に応じて、ドメインとネームサーバを設定します。

「configure」を実行します

次に 'ip domain' コマンドと 'ip name server' コマンドの例を示します

```
(Routing) # configure
(Routing) (Config) #ip domain name lab.netapp.com
(Routing) (Config) #ip name server 10.99.99.1 10.99.99.2
(Routing) (Config) #exit
(Routing) (Config) #
```

11. 必要に応じて、タイムゾーンと時刻の同期 (SNTP) を設定します。

次に 'ntp' コマンドの例を示しますこの例では 'sntp' サーバの IP アドレスと相対タイム・ゾーンを指定します

```
(Routing) #
(Routing) (Config) #sntp client mode unicast
(Routing) (Config) #sntp server 10.99.99.5
(Routing) (Config) #clock timezone -7
(Routing) (Config) #exit
(Routing) (Config) #
```

EFOSバージョン3.10.0.3以降の場合は、ntp 次の例に示すように、コマンドを実行します。

```
> (Config)# ntp ?

authenticate          Enables NTP authentication.
authentication-key    Configure NTP authentication key.
broadcast             Enables NTP broadcast mode.
broadcastdelay        Configure NTP broadcast delay in microseconds.
server               Configure NTP server.
source-interface      Configure the NTP source-interface.
trusted-key           Configure NTP authentication key number for
trusted time source.
vrf                   Configure the NTP VRF.

>(Config)# ntp server ?

ip-address|ipv6-address|hostname  Enter a valid IPv4/IPv6 address or
hostname.

>(Config)# ntp server 10.99.99.5
```

12. スイッチ名を設定します。

```
'hostname ip_switch_a_1'
```

スイッチのプロンプトに新しい名前が表示されます。

```
(Routing) # hostname IP_switch_A_1

(IP_switch_A_1) #
```

13. 設定を保存します。

「メモリの書き込み」

次の例のようなプロンプトと出力が表示されます。

```
(IP_switch_A_1) #write memory
```

```
This operation may take a few minutes.
```

```
Management interfaces will not be available during this time.
```

```
Are you sure you want to save? (y/n) y
```

```
Config file 'startup-config' created successfully .
```

```
Configuration Saved!
```

```
(IP_switch_A_1) #
```

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

#### **Broadcom** スイッチの **EFOS** ソフトウェアのダウンロードとインストール

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

このタスクについて

このタスクは、MetroCluster IP 構成内のスイッチごとに実行する必要があります。

- 次の点に注意してください。 \*
- EFOS 3.x.x から EFOS 3.x.x 以降にアップグレードするときは、スイッチが EFOS 3.4.4.6（または 3.4.x.x 以降のリリース）を実行している必要があります。それよりも前のリリースを実行している場合は、まずスイッチを EFOS 3.4.4.6（または 3.4.x.x 以降のリリース）にアップグレードしてから、スイッチを EFOS 3.x.x 以降にアップグレードします。
- EFOS 3.x.x と 3.7.x.x 以降の設定は異なります。EFOS バージョンを 3.4.x.x から 3.7.x.x 以降、またはその逆に変更する場合は、スイッチを工場出荷時のデフォルトにリセットする必要があります。対応する EFOS バージョンの RCF ファイルが適用される（再適用される）必要があります。この手順には、シリアルコンソールポート経由でアクセスする必要があります。
- EFOS バージョン 3.7.x.x 以降では、FIPS に準拠していないバージョンと FIPS に準拠したバージョンが提供されています。FIPS に準拠していないバージョンから FIPS に準拠したバージョンに移行する場合とその逆に移行する場合は、さまざまな手順があります。EFOS を FIPS 非準拠バージョンから FIPS 準拠バージョンに変更するか、その逆に変更すると、スイッチが工場出荷時のデフォルトにリセットされます。この手順には、シリアルコンソールポート経由でアクセスする必要があります。

手順

1. からスイッチファームウェアをダウンロードし["Broadcomサポートサイト"](#)ます。
2. 「show fips status」コマンドを使用して、EFOSのバージョンがFIPSに準拠しているか、FIPSに準拠していないかを確認します。次の例では'ip\_switch\_a\_1'はFIPS準拠のEFOSを使用しており'ip\_switch\_a\_2'はFIPS非準拠のEFOSを使用しています

\*例1\*

```
IP_switch_A_1 #show fips status

System running in FIPS mode

IP_switch_A_1 #
```

\*例2\*

```
IP_switch_A_2 #show fips status
      ^
% Invalid input detected at ``^` marker.

IP_switch_A_2 #
```

3. 次の表を参照して、実行する必要がある方法を確認してください。

* 手順 *	* 現在の EFOS バージョン *	* 新しい EFOS バージョン *	* 高レベルステップ *
FIPS に準拠している 2 つのバージョン間で EFOS をアップグレードする手順	3.4.x.x	3.4.x.x	方法 1) 設定とライセンスの情報は保持されています
3.4.4.6 (または 3.4.x.x 以降)	3.7.x.x 以降の非 FIPS 準拠	方法 1 を使用して EFOS をアップグレードします。スイッチを工場出荷時のデフォルトにリセットして、EFOS 3.x.x 以降の RCF ファイルを適用します	3.7.x.x 以降の非 FIPS 準拠
3.4.4.6 (または 3.4.x.x 以降)	方法 1 を使用して EFOS をダウングレードします。スイッチを工場出荷時のデフォルトにリセットして、EFOS 3.x.x の RCF ファイルを適用します	3.7.x.x 以降の非 FIPS 準拠	
方法 1 を使用して新しい EFOS イメージをインストールします。構成とライセンスの情報は保持されます	3.7.x.x 以降の FIPS に準拠しています	3.7.x.x 以降の FIPS に準拠しています	方法 1 を使用して新しい EFOS イメージをインストールします。構成とライセンスの情報は保持されます

FIPS 準拠の EFOS バージョンへのアップグレード手順	FIPS に準拠していません	FIPS に準拠している	方法 2 を使用した EFOS イメージのインストールスイッチの設定とライセンス情報が失われます。
--------------------------------	----------------	--------------	---

- 方法 1 : ソフトウェアイメージをバックアップブートパーティションにダウンロードして EFOS をアップグレードする手順
- 方法 2 : ONIE OS インストールを使用して EFOS をアップグレードする手順

ソフトウェアイメージをバックアップブートパーティションにダウンロードして **EFOS** をアップグレードする手順

次の手順を実行できるのは、両方の EFOS バージョンが FIPS 非準拠であるか、両方の EFOS バージョンが FIPS 準拠である場合のみです。



FIPS に準拠したバージョンで、もう一方のバージョンが FIPS に準拠していない場合は、次の手順を使用しないでください。

手順

1. スイッチソフトウェアをスイッチにコピーします `:+copy sftp://user@50.50.50.50 /switchsoftware/efos-3.4.6.stk backup+`

この例では、efos-3.4.6.stk オペレーティングシステムファイルが SFTP サーバ（50.50.50）からバックアップパーティションにコピーされています。使用する TFTP / SFTP サーバの IP アドレスを指定し、インストールする必要がある RCF ファイルのファイル名を指定する必要があります。

```
(IP_switch_A_1) #copy sftp://user@50.50.50.50/switchsoftware/efos-3.4.4.6.stk backup
Remote Password:*****

Mode..... SFTP
Set Server IP..... 50.50.50.50
Path..... /switchsoftware/
Filename..... efos-3.4.4.6.stk
Data Type..... Code
Destination Filename..... backup

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y

File transfer in progress. Management access will be blocked for the
duration of the transfer. Please wait...
SFTP Code transfer starting...

File transfer operation completed successfully.

(IP_switch_A_1) #
```

2. 次回リブート時にスイッチをバックアップパーティションからブートするように設定します。

「ブート・システム・バックアップ」を参照してください

```
(IP_switch_A_1) #boot system backup
Activating image backup ..

(IP_switch_A_1) #
```

3. 次回ブート時に新しいブートイメージがアクティブになることを確認します。

'How bootvar'

```
(IP_switch_A_1) #show bootvar
```

```
Image Descriptions
```

```
active :
```

```
backup :
```

```
Images currently available on Flash
```

unit	active	backup	current-active	next-active
1	3.4.4.2	3.4.4.6	3.4.4.2	3.4.4.6

```
(IP_switch_A_1) #
```

#### 4. 設定を保存します。

「メモリの書き込み」

```
(IP_switch_A_1) #write memory
```

```
This operation may take a few minutes.
```

```
Management interfaces will not be available during this time.
```

```
Are you sure you want to save? (y/n) y
```

```
Configuration Saved!
```

```
(IP_switch_A_1) #
```

#### 5. スイッチをリブートします。

「再ロード」

```
(IP_switch_A_1) #reload
```

```
Are you sure you would like to reset the system? (y/n) y
```

#### 6. スイッチがリブートするまで待ちます。



まれに、スイッチが起動しないことがあります。に従ってください [ONIE OS インストール](#) を使用して [EFOS をアップグレードする手順](#) 新しいイメージをインストールします。

7. スイッチを EFOS 3.x.x から EFOS 3.x.x に変更した場合、またはその逆の場合は、次の 2 つの手順に従って正しい設定（RCF）を適用します。
  - a. [Broadcom IP スイッチを工場出荷時のデフォルトにリセット](#)
  - b. [Broadcom の RCF ファイルのダウンロードとインストール](#)
8. MetroCluster IP 構成の残りの 3 つの IP スイッチについて、上記の手順を繰り返します。

### ONIE OS インストールを使用して EFOS をアップグレードする手順

一方の EFOS バージョンが FIPS に準拠していて、もう一方の EFOS バージョンが FIPS に準拠していない場合は、次の手順を実行できます。次の手順は、スイッチがブートに失敗した場合に、ONIE から FIPS 非準拠または FIPS 準拠の EFOS 3.x.x イメージをインストールするために使用できます。

#### 手順

1. スイッチを ONIE インストールモードで起動します。

起動中に、次の画面が表示されたら ONIE を選択します。

```
+-----+
| EFOS                                     |
| *ONIE                                   |
|                                         |
|                                         |
|                                         |
|                                         |
|                                         |
|                                         |
|                                         |
|                                         |
|                                         |
|                                         |
|                                         |
+-----+
```

「ONIE」を選択すると、スイッチがロードされ、次の選択肢が表示されます。

```

+-----+
|*ONIE: Install OS
| ONIE: Rescue
| ONIE: Uninstall OS
| ONIE: Update ONIE
| ONIE: Embed ONIE
| DIAG: Diagnostic Mode
| DIAG: Burn-In Mode
|
|
|
|
|
+-----+

```

スイッチが ONIE インストールモードで起動します。

## 2. ONIE の検出を停止し、イーサネットインターフェイスを設定します

次のメッセージが表示されたら、<ENTER> を押して ONIE コンソールを起動します。

```

Please press Enter to activate this console. Info: eth0: Checking
link... up.
ONIE:/ #

```



ONIE の検出は続行され、メッセージがコンソールに出力されます。

```

Stop the ONIE discovery
ONIE:/ # onie-discovery-stop
discover: installer mode detected.
Stopping: discover... done.
ONIE:/ #

```

## 3. イーサネットインターフェイスを設定し、「ifconfig eth0 <ipAddress> netmask <netmask> up」および「route add default gw <gatewayAddress>」を使用してルートを追加します

```

ONIE:/ # ifconfig eth0 10.10.10.10 netmask 255.255.255.0 up
ONIE:/ # route add default gw 10.10.10.1

```

## 4. ONIE インストールファイルをホストしているサーバにアクセスできることを確認します。

```

ONIE:/ # ping 50.50.50.50
PING 50.50.50.50 (50.50.50.50): 56 data bytes
64 bytes from 50.50.50.50: seq=0 ttl=255 time=0.429 ms
64 bytes from 50.50.50.50: seq=1 ttl=255 time=0.595 ms
64 bytes from 50.50.50.50: seq=2 ttl=255 time=0.369 ms
^C
--- 50.50.50.50 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.369/0.464/0.595 ms
ONIE:/ #

```

## 5. 新しいスイッチソフトウェアをインストールします

```

ONIE:/ # onie-nos-install http:// 50.50.50.50/Software/onie-installer-
x86_64
discover: installer mode detected.
Stopping: discover... done.
Info: Fetching http:// 50.50.50.50/Software/onie-installer-3.7.0.4 ...
Connecting to 50.50.50.50 (50.50.50.50:80)
installer          100% |*****| 48841k
0:00:00 ETA
ONIE: Executing installer: http:// 50.50.50.50/Software/onie-installer-
3.7.0.4
Verifying image checksum ... OK.
Preparing image archive ... OK.

```

ソフトウェアがスイッチをインストールし、リブートします。スイッチを通常どおりにリブートして新しいEFOSバージョンにします。

## 6. 新しいスイッチソフトウェアがインストールされていることを確認します

### 'How bootvar'

```

(Routing) #show bootvar
Image Descriptions
active :
backup :
Images currently available on Flash
----
unit   active      backup      current-active  next-active
----
1      3.7.0.4      3.7.0.4     3.7.0.4         3.7.0.4
(Routing) #

```

## 7. インストールを完了します

設定を適用せずにスイッチがリブートし、工場出荷時のデフォルトにリセットされます。2つの手順に従ってスイッチの基本設定を行い、次の2つのドキュメントに記載されているように RCF ファイルを適用します。

- a. スwitchの基本設定を行います。手順4以降を実行します。 [Broadcom IP スwitchを工場出荷時のデフォルトにリセット](#)
- b. の説明に従って、RCF ファイルを作成して適用します [Broadcom の RCF ファイルのダウンロードとインストール](#)

### Broadcom の RCF ファイルのダウンロードとインストール

MetroCluster IP構成の各スイッチにスイッチのRCFファイルを生成してインストールする必要があります。

作業を開始する前に

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

このタスクについて

この手順は、MetroCluster IP 構成の各 IP スwitchで実行する必要があります。

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

スイッチ	RCF ファイル
IP_switch_A_1	v1.32_Switch-A1.txt
IP_switch_a_2	v1.32_Switch-A2.txt
IP_switch_B_1	v1.32_Switch-B1.txt
IP_switch_B_2	v1.32_Switch-B2.txt



EFOS バージョン 3.4.4.6 以降の 3.4.x.x の RCF ファイルリリースと EFOS バージョン 3.7.0.4 は異なります。スイッチが実行されている EFOS バージョンの正しい RCF ファイルを作成したことを確認する必要があります。

EFOS バージョン	RCF ファイルのバージョン
3.4.x.x	V1.3 倍、V1.4 倍
3.7.x.x	v2.x

手順

1. MetroCluster IP 用の Broadcom RCF ファイルを生成します。
  - a. ダウンロード "[MetroCluster IP 用の RcfFileGenerator](#)"

b. RcfFileGenerator for MetroCluster IPを使用して、設定用のRCFファイルを生成します。



ダウンロード後にRCFファイルを変更することはできません。

2. RCF ファイルをスイッチにコピーします。

a. RCFファイルを最初のスイッチにコピーします。'copy sftp://user@ftp-server-ip-address/RcfFiles/switch-specific -RCF / BES-53248\_v1.32\_Switch-A1.txt nvram : script BES-53248\_v1.32\_Switch-A1.SCR

この例では、「BES-53248\_v1.32\_Switch-A1.txt」RCF ファイルを、SFTP サーバの「0.50.50.50」からローカルブートフラッシュにコピーしています。使用する TFTP / SFTP サーバの IP アドレスを指定し、インストールする必要がある RCF ファイルのファイル名を指定する必要があります。

```
(IP_switch_A_1) #copy sftp://user@50.50.50.50/RcfFiles/BES-53248_v1.32_Switch-A1.txt nvram:script BES-53248_v1.32_Switch-A1.scr
```

```
Remote Password:*****
```

```
Mode..... SFTP
Set Server IP..... 50.50.50.50
Path..... /RcfFiles/
Filename..... BES-53248_v1.32_Switch-A1.txt
Data Type..... Config Script
Destination Filename..... BES-53248_v1.32_Switch-A1.scr
```

```
Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y
```

```
File transfer in progress. Management access will be blocked for the
duration of the transfer. Please wait...
File transfer operation completed successfully.
```

```
Validating configuration script...
```

```
config
```

```
set clibanner
```

```
*****
*****
```

```
* NetApp Reference Configuration File (RCF)
```

```
*
```

```
* Switch : BES-53248
```

```
...
```

```
The downloaded RCF is validated. Some output is being logged here.
```

```
...
```

```
Configuration script validated.
```

```
File transfer operation completed successfully.
```

```
(IP_switch_A_1) #
```

b. RCF ファイルがスクリプトとして保存されたことを確認します。

「原稿リスト」

```
(IP_switch_A_1) #script list

Configuration Script Name          Size(Bytes)  Date of Modification
-----
BES-53248_v1.32_Switch-A1.scr      852         2019 01 29 18:41:25

1 configuration script(s) found.
2046 Kbytes free.
(IP_switch_A_1) #
```

c. RCF スクリプトを適用します。

「script apply BES-53248 v1.32\_Switch-A1.scr」を参照してください

```
(IP_switch_A_1) #script apply BES-53248_v1.32_Switch-A1.scr

Are you sure you want to apply the configuration script? (y/n) y

config

set clibanner
*****
*****

* NetApp Reference Configuration File (RCF)

*

* Switch      : BES-53248

...
The downloaded RCF is validated. Some output is being logged here.
...

Configuration script 'BES-53248_v1.32_Switch-A1.scr' applied.

(IP_switch_A_1) #
```

d. 設定を保存します。

## 「メモリの書き込み」

```
(IP_switch_A_1) #write memory

This operation may take a few minutes.
Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) y

Configuration Saved!

(IP_switch_A_1) #
```

- e. スイッチをリブートします。

## 「再ロード」

```
(IP_switch_A_1) #reload

Are you sure you would like to reset the system? (y/n) y
```

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

3. スイッチをリロードします。

## 「再ロード」

```
IP_switch_A_1# reload
```

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

未使用のISLポートとポートチャネルを無効にする

NetAppでは、不要なヘルスアラートを回避するために、未使用のISLポートとポートチャネルを無効にすることを推奨します

1. RCFファイルのバナーを使用して、未使用のISLポートとポートチャネルを特定します。



ポートがブレイクアウトモードの場合は、コマンドで指定するポート名がRCFバナーに表示される名前と異なることがあります。RCFケーブル接続ファイルを使用してポート名を検索することもできます。

### ISLホオトノシヨウサイ

コマンドを実行します `show port all`。

ポートチャネルの詳細

コマンドを実行します `show port-channel all`。

## 2. 未使用のISLポートとポートチャネルを無効にします。

特定された未使用のポートまたはポートチャネルごとに、次のコマンドを実行する必要があります。

```
(SwtichA_1)> enable
(SwtichA_1)# configure
(SwtichA_1)(Config)# <port_name>
(SwtichA_1)(Interface 0/15)# shutdown
(SwtichA_1)(Interface 0/15)# end
(SwtichA_1)# write memory
```

## Cisco IP スイッチを設定する

クラスタ相互接続とバックエンドMetroCluster IP 接続用にCisco IP スイッチを構成する

クラスターインターコネクトおよびバックエンド MetroCluster IP 接続用に Cisco IP スイッチを設定する必要があります。

このタスクについて

このセクションの手順のいくつかは独立した手順であり、実行する必要があるのは自分がタスクに指示された手順、またはタスクに関連する手順のみです。

## Cisco IP スイッチを工場出荷時のデフォルトにリセットする

RCF ファイルをインストールする前に、Cisco スイッチの設定を消去し、基本的な設定を完了する必要があります。この手順は、以前のインストールに失敗したあとに同じ RCF ファイルを再インストールする場合、または新しいバージョンのファイルをインストールする場合に必要です。

このタスクについて

- この手順は、MetroCluster IP 構成の各 IP スイッチで実行する必要があります。
- シリアルコンソールを使用してスイッチに接続する必要があります。
- このタスクでは、管理ネットワークの設定をリセットします。

手順

1. スイッチを工場出荷時のデフォルトにリセットします。
  - a. 既存の設定を消去します。

「 write erase 」を入力します

- b. スイッチソフトウェアをリロードします。

「再ロード」

システムがリブートし、設定ウィザードが表示されます。起動中に「Abort Auto Provisioning and continue with normal setup ?」というプロンプトが表示された場合は、(yes/no)[n]"、続行するには 'yes' と応答する必要があります。

- c. 設定ウィザードで、スイッチの基本設定を入力します。

- 管理パスワード
- スイッチ名
- アウトオブバンド管理設定
- デフォルトゲートウェイ
- SSH サービス (RSA)

設定ウィザードが完了すると、スイッチがリブートします。

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

次の例は、スイッチを設定する際のプロンプトとシステム応答を示しています。山括弧 (「<<<」) は、情報を入力する場所を示します。

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

    Enter the password for "admin": password
    Confirm the password for "admin": password
        ---- Basic System Configuration Dialog VDC: 1 ----

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

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

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

次の一連のプロンプトで、スイッチ名、管理アドレス、ゲートウェイなどの基本情報を入力し、SSH with RSA を選択します。



この例は、RCFの設定に必要な最小限の情報を示しています。RCFの適用後に追加オプションを設定できます。たとえば、RCFを適用したあとにSNMPv3、NTP、またはSCP/SFTPを設定できます。

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

最後の一連のプロンプトで設定が完了します。

The following configuration will be applied:

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

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

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

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

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

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

## 2. 設定を保存します。

```
IP_switch-A-1# copy running-config startup-config
```

## 3. スイッチをリブートし、スイッチがリロードされるまで待ちます。

```
IP_switch-A-1# reload
```

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

## Cisco スイッチの NX-OS ソフトウェアのダウンロードとインストール

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

このタスクについて

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

この手順は、MetroCluster IP 構成の各 IP スイッチで実行する必要があります。

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

["NetApp Hardware Universe の略"](#)

手順

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

["シスコソフトウェアのダウンロード"](#)

2. スイッチソフトウェアをスイッチにコピーします。

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

この例では、nxos.7.0.3.l4.6.bin ファイルと EPLD イメージが SFTP サーバ 10.10.99.99 からローカルブートフラッシュにコピーされます。

```

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

IP_switch_A_1# copy sftp://root@10.10.99.99/tftpboot/n9000-
epld.9.3.5.img bootflash: vrf management
root@10.10.99.99's password: password
sftp> progress
Progress meter enabled
sftp> get /tftpboot/n9000-epld.9.3.5.img /bootflash/n9000-
epld.9.3.5.img
Fetching /tftpboot/n9000-epld.9.3.5.img to /bootflash/n9000-
epld.9.3.5.img
/tftpboot/n9000-epld.9.3.5.img          161MB 9.5MB/s 00:16
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.

```

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

「IR bootflash:」のように表示されます

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

```

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

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

```

#### 4. スイッチソフトウェアをインストールします。

すべての nxos bootflash:nxos.version-number.bin をインストールします

スイッチソフトウェアがインストールされると、スイッチは自動的にリロード（リブート）します。

次の例は、FC\_switch\_A\_1 へのソフトウェアのインストールを示しています。

```

IP_switch_A_1# install all nxos bootflash:nxos.7.0.3.I4.6.bin
Installer will perform compatibility check first. Please wait.
Installer is forced disruptive

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

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

Preparing "nxos" version info using image
bootflash:/nxos.7.0.3.I4.6.bin.
[#####] 100% -- SUCCESS

Preparing "bios" version info using image
bootflash:/nxos.7.0.3.I4.6.bin.
[#####] 100% -- SUCCESS          [#####] 100%
-- SUCCESS

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

```

```

Notifying services about system upgrade.      [#####] 100%
-- SUCCESS

Compatibility check is done:
Module  bootable          Impact  Install-type  Reason
-----  -----  -----  -----  -----
      1      yes      disruptive      reset  default upgrade is not
hitless

Images will be upgraded according to following table:
Module      Image  Running-Version(pri:alt)      New-Version  Upg-
Required
-----  -----  -----  -----  -----
      1      nxos      7.0(3)I4(1)      7.0(3)I4(6)  yes
      1      bios      v04.24(04/21/2016)  v04.24(04/21/2016)  no

Switch will be reloaded for disruptive upgrade.
Do you want to continue with the installation (y/n)?  [n] y

Install is in progress, please wait.

Performing runtime checks.      [#####] 100%  --
SUCCESS

Setting boot variables.
[#####] 100% -- SUCCESS

Performing configuration copy.
[#####] 100% -- SUCCESS

Module 1: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[#####] 100% -- SUCCESS

Finishing the upgrade, switch will reboot in 10 seconds.
IP_switch_A_1#

```

5. スイッチがリロードされるまで待ってから、スイッチにログインします。

スイッチがリブートされると、ログインプロンプトが表示されます。

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

The switch software is now installed.
```

6. スイッチソフトウェアがインストールされていることを確認します :+show version

次の例は、の出力を示しています。

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

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

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

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

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

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

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

plugin
  Core Plugin, Ethernet Plugin
IP_switch_A_1#
```

7. EPLD イメージをアップグレードし、スイッチを再起動します。

```

IP_switch_A_1# install epld bootflash:n9000-epld.9.3.5.img module 1
Compatibility check:
Module          Type          Upgradable    Impact        Reason
-----
1              SUP              Yes           disruptive    Module Upgradable

Retrieving EPLD versions.... Please wait.
Images will be upgraded according to following table:
Module  Type  EPLD          Running-Version  New-Version  Upg-
Required
-----
1  SUP  MI FPGA      0x07            0x07        No
1  SUP  IO FPGA      0x17            0x19        Yes
1  SUP  MI FPGA2     0x02            0x02        No

The above modules require upgrade.
The switch will be reloaded at the end of the upgrade
Do you want to continue (y/n) ? [n] y

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

Module 1 : IO FPGA [Programming] : 100.00% (      64 of      64 sectors)
Module 1 EPLD upgrade is successful.
Module  Type  Upgrade-Result
-----
1  SUP  Success

EPLDs upgraded.

Module 1 EPLD upgrade is successful.

```

8. [[step8] スイッチのリブート後に再度ログインし、新しいバージョンの EPLD が正常にロードされたことを確認します。

```
show version module 1 epld
```

9. MetroCluster IP 構成の残りの 3 つの IP スイッチについて、上記の手順を繰り返します。

### Cisco IP RCF ファイルのダウンロードとインストール

MetroCluster IP構成の各スイッチにRCFファイルを生成してインストールする必要があります。

このタスクについて

この作業には、FTP、TFTP、SFTP、SCP などのファイル転送ソフトウェアが必要です。ファイルをス

イッチにコピーします。

この手順は、MetroCluster IP 構成の各 IP スイッチで実行する必要があります。

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

### "NetApp Hardware Universe の略"

QSFP / SFP+アダプタを使用している場合は、ISLポートをブレイクアウト速度モードではなくネイティブ速度モードで設定する必要があります。ISLポートの速度モードについては、スイッチベンダーのドキュメントを参照してください。

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

スイッチ	RCF ファイル
IP_switch_A_1	NX3232_v1.80_Switch-A1.txt
IP_switch_a_2	NX3232_v1.80_Switch-A2.txt
IP_switch_B_1	NX3232_v1.80_Switch-B1.txt
IP_switch_B_2	NX3232_v1.80_Switch-B2.txt

### 手順

1. MetroCluster IP用のCisco RCFファイルを生成します。
  - a. ダウンロード "[MetroCluster IP 用の RcfFileGenerator](#)"
  - b. RcfFileGenerator for MetroCluster IPを使用して、設定用のRCFファイルを生成します。



ダウンロード後にRCFファイルを変更することはできません。

2. RCF ファイルをスイッチにコピーします。
  - a. RCF ファイルを最初のスイッチにコピーします。

```
'copy sftp://root@ftp-server-ip-address /tftpboot/switch-specific -RCF bootflash:vrf management'
```

この例では、NX3232\_v1.80\_Switch-A1.txt RCF ファイルを SFTP サーバの 10.10.99.99 からローカルブートフラッシュにコピーしています。使用する TFTP / SFTP サーバの IP アドレスと、インストールする必要がある RCF ファイルのファイル名を使用する必要があります。

```

IP_switch_A_1# copy
sftp://root@10.10.99.99/tftpboot/NX3232_v1.80_Switch-A1.txt bootflash:
vrf management
root@10.10.99.99's password: password
sftp> progress
Progress meter enabled
sftp> get /tftpboot/NX3232_v1.80_Switch-A1.txt
/bootflash/NX3232_v1.80_Switch-A1.txt
Fetching /tftpboot/NX3232_v1.80_Switch-A1.txt to
/bootflash/NX3232_v1.80_Switch-A1.txt
/tftpboot/NX3232_v1.80_Switch-A1.txt          100% 5141      5.0KB/s
00:00
sftp> exit
Copy complete, now saving to disk (please wait)...
IP_switch_A_1#

```

- a. 残りの3つのスイッチのそれぞれについて、同じ手順を繰り返します。それぞれのスイッチに対応するRCFファイルをコピーするように注意してください。
3. 各スイッチのbootflashディレクトリにRCFファイルがあることを確認します。

「IR bootflash:」のように表示されます

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

```

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

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

```

4. Cisco 3132Q-V および Cisco 3232C スイッチのTCAMリージョンを設定します。



Cisco 3132Q-V または Cisco 3232C スイッチを使用していない場合は、この手順を省略します。

- a. Cisco 3132Q-V スイッチで、次の TCAM リージョンを設定します。

```
conf t
hardware access-list tcam region span 0
hardware access-list tcam region racl 256
hardware access-list tcam region e-racl 256
hardware access-list tcam region qos 256
```

- b. Cisco 3232C スイッチで、次の TCAM リージョンを設定します。

```
conf t
hardware access-list tcam region span 0
hardware access-list tcam region racl-lite 0
hardware access-list tcam region racl 256
hardware access-list tcam region e-racl 256
hardware access-list tcam region qos 256
```

- c. TCAM リージョンを設定したら、設定を保存してスイッチをリロードします。

```
copy running-config startup-config
reload
```

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

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

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

```
'copy running-config startup-config
```

次のような出力が表示されます。

```
IP_switch_A_1# copy bootflash:NX3232_v1.80_Switch-A1.txt running-config
IP_switch-A-1# copy running-config startup-config
```

7. スイッチをリロードします。

「再ロード」

```
IP_switch_A_1# reload
```

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

## 25Gbps 接続を使用するシステムの前方誤り訂正の設定

25Gbps 接続を使用してシステムが設定されている場合は、RCF ファイルの適用後に前方誤り訂正 (fec) パラメータを手動で off に設定する必要があります。この設定は RCF ファイルでは適用されません。

このタスクについて

この手順を実行する前に、25Gbps ポートがケーブル接続されている必要があります。

"Cisco 3232C スイッチまたは Cisco 9336C スイッチのプラットフォームポートの割り当て"

このタスクでは、25Gbps 接続を使用する環境 プラットフォームのみを使用します。

- AFF A300
- FAS 8200
- FAS 500f
- AFF A250

このタスクは、MetroCluster IP 構成の 4 つのスイッチすべてで実行する必要があります。

手順

1. コントローラモジュールに接続されている各 25Gbps ポートで fec パラメータを off に設定し、実行中の設定をスタートアップ設定にコピーします。
  - a. 構成モードを開始します :`config t`
  - b. 設定する 25Gbps インターフェイスを「`interface interface-Id`」と指定します
  - c. fec を off に設定します
  - d. スイッチの各 25Gbps ポートについて、上記の手順を繰り返します。
  - e. 構成モードを終了します :`exit`

次の例は、スイッチ IP\_switch\_A\_1 のインターフェイス Ethernet1/25/1 に対するコマンドを示しています。

```
IP_switch_A_1# conf t
IP_switch_A_1(config)# interface Ethernet1/25/1
IP_switch_A_1(config-if)# fec off
IP_switch_A_1(config-if)# exit
IP_switch_A_1(config-if)# end
IP_switch_A_1# copy running-config startup-config
```

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

未使用の ISL ポートとポートチャネルを無効にする

NetApp では、不要なヘルスアラートを回避するために、未使用の ISL ポートとポートチャネルを無効にすることを推奨します

1. 未使用のISLポートとポートチャネルを特定します。

「インターフェイスの概要」

2. 未使用のISLポートとポートチャネルを無効にします。

特定された未使用のポートまたはポートチャネルごとに、次のコマンドを実行する必要があります。

```
SwitchA_1# config t
Enter configuration commands, one per line. End with CNTL/Z.
SwitchA_1(config)# int Eth1/14
SwitchA_1(config-if)# shutdown
SwitchA_12(config-if)# exit
SwitchA_1(config-if)# copy running-config startup-config
[#####] 100%
Copy complete, now saving to disk (please wait)...
Copy complete.
```

#### MetroCluster IPサイト内のCisco 9336CスイッチでMACsec暗号化を構成する



MACsec 暗号化は、WAN ISL ポートにのみ適用できます。

#### Cisco 9336C スイッチに MACsec 暗号化を設定します

サイト間で実行される WAN ISL ポートにのみ MACsec 暗号化を設定する必要があります。正しい RCF ファイルを適用したあとに MACsec を設定する必要があります。

#### MACsec のライセンス要件

MACsec にはセキュリティライセンスが必要です。Cisco NX-OS ライセンス方式の詳細およびライセンスの取得方法と適用方法については、を参照してください "『[Cisco NX-OS Licensing Guide](#)』"

#### MetroCluster IP構成でCisco MACsec暗号化WAN ISLを有効にします

MetroCluster IP 構成では、WAN ISL 上の Cisco 9336C スイッチに対して MACsec 暗号化をイネーブルにできます。

#### 手順

1. グローバルコンフィギュレーションモードを開始します。

「configure terminal」をクリックします

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. デバイスで MACsec と MKA を有効にします。

「 feature MACsec

```
IP_switch_A_1(config)# feature macsec
```

3. 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

'copy running-config startup-config

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

## MACsecキーチェーンとキーを設定します

MACsec キーチェーンまたはキーをコンフィギュレーションに作成できます。

- キーライフタイムと Hitless Key Rollover \*

MACsec キーチェーンには、複数の Pre-Shared Key (PSK; 事前共有キー) を設定できます。各 PSKs には、キー ID とオプションのライフタイムが設定されています。キーの有効期間は、キーがアクティブになって有効期限が切れるタイミングを指定します。ライフタイム設定がない場合、デフォルトのライフタイムは無制限です。ライフタイムが設定されている場合、ライフタイムが期限切れになると、MKA はキーチェーン内で設定されている次の事前共有キーにロールオーバーします。キーのタイムゾーンは、local または UTC です。デフォルトのタイムゾーンは UTC です。キーを同じキーチェーン内の 2 番目のキー (キーチェーン内) にロールオーバーして、最初のキーのライフタイムを設定することができます。最初のキーの有効期間が終了すると、自動的にリスト内の次のキーにロールオーバーされます。リンクの両側で同じキーが同時に設定されている場合、キーのロールオーバーはヒットレスになります (つまり、キーはトラフィックを中断することなくロールオーバーされます)。

手順

1. グローバルコンフィギュレーションモードを開始します。

「configure terminal」をクリックします

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. 暗号化されたキーオクテット文字列を非表示にするには、「show running-config」コマンドと「show startup-config」コマンドの出力で、文字列をワイルドカード文字に置き換えます。

```
IP_switch_A_1(config)# key-chain macsec-psk no-show
```



オクテット文字列は、コンフィギュレーションをファイルに保存するときにも非表示になります。

デフォルトでは、PSK キーは暗号化形式で表示され、簡単に復号化できます。このコマンドは、MACsec キーチェーンにのみ適用されます。

- MACsec キーチェーンを作成して一連の MACsec キーを保持し、MACsec キーチェーンコンフィギュレーションモードを開始します。

キーチェーン名 MACsec

```
IP_switch_A_1(config)# key chain 1 macsec
IP_switch_A_1(config-macseckeychain)#
```

- MACsec キーを作成し、MACsec キーコンフィギュレーションモードを開始します。

「key key-id」

指定できる 16 進数のキー文字列の範囲は 1 ~ 32 で、最大サイズは 64 文字です。

```
IP_switch_A_1 switch(config-macseckeychain)# key 1000
IP_switch_A_1 (config-macseckeychain-macseckey)#
```

- キーのオクテット文字列を設定します。

「key-octet-string octet-string octet-string cryptographic-algorithm ae\_128\_CMAC | aes-256\_CMAC」という形式で指定します

```
IP_switch_A_1(config-macseckeychain-macseckey)# key-octet-string
abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789
cryptographic-algorithm AES_256_CMAC
```



octet-string 引数には、最大 64 個の 16 進文字を含めることができます。オクテットキーは内部でエンコードされるため、クリアテキストのキーは、「show running-config macsec」コマンドの出力には表示されません。

- キーの送信ライフタイムを設定します (秒単位)。

「send-lifetime start-time duration」

```
IP_switch_A_1(config-macseckeychain-macseckey)# send-lifetime 00:00:00
Oct 04 2020 duration 100000
```

デフォルトでは、デバイスは開始時間を UTC として処理します。start-time 引数には、キーがアクティブになる時刻と日付を指定します。duration 引数は、ライフタイムの秒単位の長さです。最大値は 2147483646 秒 (約 68 年) です。

- 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

'copy running-config startup-config

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

8. キーチェーン設定を表示します。

「鍵チェーン名」

```
IP_switch_A_1(config-macseckeychain-macseckey)# show key chain 1
```

## MACsecポリシーを設定します

### 手順

1. グローバルコンフィギュレーションモードを開始します。

「configure terminal」をクリックします

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. MACsec ポリシーを作成します。

「ACSEC ポリシー名」

```
IP_switch_A_1(config)# macsec policy abc
IP_switch_A_1(config-macsec-policy)#
```

3. 次のいずれかの暗号、gcm-aes-128、gcm-aes-256、gcm-aes-xpN-128、またはgcm-aes-xpN-256を設定します。

「cipher-site name」

```
IP_switch_A_1(config-macsec-policy)# cipher-suite GCM-AES-256
```

4. キー交換時にピア間の接続を解除するために、キーサーバの優先度を設定します。

「key-server -priority number」と入力します

```
switch(config-macsec-policy)# key-server-priority 0
```

5. データおよび制御パケットの処理を定義するセキュリティポリシーを設定します。

「セキュリティ・ポリシー・セキュリティ・ポリシー」を参照してください

次のオプションからセキュリティポリシーを選択します。

- must-secure — MACsec ヘッダーを伝送していないパケットはドロップされます
- must-secure — MACsec ヘッダーを伝送しないパケットは許可されます (これがデフォルト値です)
- 

```
IP_switch_A_1(config-macsec-policy)# security-policy should-secure
```

6. リプレイ保護ウィンドウを設定して、セキュアインターフェイスが設定されたウィンドウサイズより小さいパケットを受け入れないようにします。「window-size number」



リプレイ保護ウィンドウのサイズは、MACsec が受信して破棄されない最大アウトオブオーダーフレーム数を表します。指定できる範囲は 0 ~ 596000000 です。

```
IP_switch_A_1(config-macsec-policy)# window-size 512
```

7. SAK キーの再生成を強制する時間を秒単位で設定します。

「SAK-expiry-date time」

このコマンドを使用して、予測可能な時間間隔にセッションキーを変更できます。デフォルトは 0 です。

```
IP_switch_A_1(config-macsec-policy)# sak-expiry-time 100
```

8. 暗号化を開始するレイヤ 2 フレームで、次の機密性オフセットのいずれかを設定します。

「conf-offsetconfidentiality offset」を参照してください

次のいずれかのオプションを選択します。

- conf-offset-0。
- conf-offset-30。
- conf -offset-50。

```
IP_switch_A_1(config-macsec-policy)# conf-offset CONF-OFFSET-0
```



このコマンドは、中間スイッチが MPLS タグのようなパケットヘッダー (DMAC、smac、type) を使用するために必要な場合があります。

9. 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

```
'copy running-config startup-config
```

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

10. MACsec ポリシー設定を表示します。

「MACsec ポリシー」

```
IP_switch_A_1(config-macsec-policy)# show macsec policy
```

インターフェイス上で**Cisco MACsec**暗号化をイネーブルにします

1. グローバルコンフィギュレーションモードを開始します。

「configure terminal」をクリックします

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. MACsec暗号化で設定したインターフェイスを選択します。

インターフェイスのタイプと ID を指定できます。イーサネットポートの場合は、イーサネットスロット / ポートを使用します。

```
IP_switch_A_1(config)# interface ethernet 1/15
switch(config-if)#
```

3. インターフェイスに設定するキーチェーンとポリシーを追加して、MACsec設定を追加します。

「MACsec keychain -name policy policy-name」という名前のキーチェーンがあります

```
IP_switch_A_1(config-if)# macsec keychain 1 policy abc
```

4. MACsec暗号化を設定するすべてのインターフェイスで、ステップ1と2を繰り返します。
5. 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

'copy running-config startup-config

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

## MetroCluster IP構成でCisco MACsec暗号化WAN ISLをディセーブルにします

MetroCluster IP 構成では、WAN ISL 上の Cisco 9336C スイッチに対して MACsec 暗号化を無効にする必要がある場合があります。

手順

1. グローバルコンフィギュレーションモードを開始します。

「configure terminal」をクリックします

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. デバイスの MACsec 設定を無効にします。

「ACSEC SHUTDOWN」のようになります

```
IP_switch_A_1(config)# macsec shutdown
```



「no」オプションを選択すると、MACsec 機能が復元されます。

3. MACsec で設定済みのインターフェイスを選択します。

インターフェイスのタイプと ID を指定できます。イーサネットポートの場合は、イーサネットスロット / ポートを使用します。

```
IP_switch_A_1(config)# interface ethernet 1/15
switch(config-if)#
```

4. インターフェイスに設定されているキーチェーンとポリシーを削除して、MACsec設定を削除します。

「no MACsec keychain keychain -name policy policy-name」

```
IP_switch_A_1(config-if)# no macsec keychain 1 policy abc
```

5. MACsec が設定されているすべてのインターフェイスで、ステップ 3 と 4 を繰り返します。
6. 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

'copy running-config startup-config

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

## MACsec 構成の確認

### 手順

1. コンフィギュレーション内の 2 番目のスイッチで上記の手順 \* すべて \* を繰り返して、MACsec セッションを確立します。
2. 次のコマンドを実行して、両方のスイッチが正常に暗号化されたことを確認します。
  - a. 「How MACsec mka summary」を実行します
  - b. 実行 : 'How MACsec mka session'
  - c. 実行 : 'How MACsec mka statistics (MACsec mka 統計情報)

MACsec 設定を確認するには、次のコマンドを使用します。

コマンドを実行します	表示される情報
'How MACsec mka session interface types/port number	特定のインターフェイスまたはすべてのインターフェイスの MACsec MKA セッション
「鍵チェーン名」	キーチェーン設定
「MACsec mka の概要」を参照してください	MACsec MKA 設定
'How MACsec policy policy-name'」を参照してください	特定の MACsec ポリシーまたはすべての MACsec ポリシーの設定

## NVIDIA IPスイッチを設定します

クラスター相互接続とバックエンド MetroCluster IP 接続用に NVIDIA IP SN2100 スイッチを構成する

クラスターインターコネクトおよびバックエンド MetroCluster IP 接続用に NVIDIA SN2100 IP スイッチを設定する必要があります。

**[[Reset-The switch]]** NVIDIA IP SN2100 スイッチを工場出荷時のデフォルトにリセットします

スイッチを工場出荷時のデフォルト設定にリセットするには、次のいずれかの方法を選択します。

- [RCFファイルオプションを使用してスイッチをリセットします](#)
- [Cumulusソフトウェアのダウンロードとインストール](#)

**[RCFファイルオプション]]** RCFファイルオプションを使用してスイッチをリセットします

新しいRCF設定をインストールする前に、NVIDIAスイッチ設定をリポートする必要があります。

### このタスクについて

スイッチをデフォルト設定に戻すには、「restoreDefaults」オプションを指定してRCFファイルを実行します。このオプションを選択すると、元のバックアップファイルが元の場所にコピーされ、スイッチがリポートされます。リポート後、スイッチを設定するためにRCFファイルを最初に行ったときに使用していた元の設

定がスイッチにオンラインになります。

次の設定の詳細はリセットされません。

- ユーザおよびクレデンシャルの設定
- 管理ネットワークポートeth0の設定



RCFファイルの適用中に発生するその他の設定変更は、すべて元の設定にリバートされます。

作業を開始する前に

- に従ってスイッチを設定する必要があります [NVIDIAのRCFファイルをダウンロードしてインストールします](#)。この方法で設定していない場合やRCFファイルを実行する前に追加機能を設定している場合は、この手順を使用できません。
- この手順は、MetroCluster IP 構成の各 IP スイッチで実行する必要があります。
- シリアルコンソール接続を使用してスイッチに接続する必要があります。
- このタスクでは、管理ネットワークの設定をリセットします。

手順

1. 同じバージョンまたは互換性のあるRCFファイルを使用してRCF設定が正常に適用され、バックアップファイルが存在することを確認します。



出力には、バックアップファイル、保持されたファイル、またはその両方が表示されます。バックアップファイルまたは保存されたファイルが出力に表示されない場合は、この手順を使用できません。

```

cumulus@IP_switch_A_1:mgmt:~$ sudo python3
SN2100_v2.0.0_IP_switch_A_1.py
[sudo] password for cumulus:
>>> Opened RcfApplyLog
A RCF configuration has been successfully applied.
Backup files exist.
Preserved files exist.
Listing completion of the steps:
    Success: Step: 1: Performing Backup and Restore
    Success: Step: 2: updating MOTD file
    Success: Step: 3: Disabling apt-get
    Success: Step: 4: Disabling cdp
    Success: Step: 5: Adding lldp config
    Success: Step: 6: Creating interfaces
    Success: Step: 7: Configuring switch basic settings: Hostname,
SNMP
    Success: Step: 8: Configuring switch basic settings: bandwidth
allocation
    Success: Step: 9: Configuring switch basic settings: ecn
    Success: Step: 10: Configuring switch basic settings: cos and
dscp remark
    Success: Step: 11: Configuring switch basic settings: generic
egress cos mappings
    Success: Step: 12: Configuring switch basic settings: traffic
classification
    Success: Step: 13: Configuring LAG load balancing policies
    Success: Step: 14: Configuring the VLAN bridge
    Success: Step: 15: Configuring local cluster ISL ports
    Success: Step: 16: Configuring MetroCluster ISL ports
    Success: Step: 17: Configuring ports for MetroCluster-1, local
cluster and MetroCluster interfaces
    Success: Step: 18: Configuring ports for MetroCluster-2, local
cluster and MetroCluster interfaces
    Success: Step: 19: Configuring ports for MetroCluster-3, local
cluster and MetroCluster interfaces
    Success: Step: 20: Configuring L2FC for MetroCluster interfaces
    Success: Step: 21: Configuring the interface to UP
    Success: Step: 22: Final commit
    Success: Step: 23: Final reboot of the switch
Exiting ...
<<< Closing RcfApplyLog
cumulus@IP_switch_A_1:mgmt:~$

```

2. デフォルトに戻すオプションを指定してRCFファイルを実行します。'restoreDefaults'

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3
SN2100_v2.0.0_IP_switch_A_2.py restoreDefaults
[sudo] password for cumulus:
>>> Opened RcfApplyLog
Can restore from backup directory. Continuing.
This will reboot the switch !!!
Enter yes or no: yes
```

3. プロンプトに「yes」と入力します。スイッチが元の設定に戻り、リブートします。
4. スイッチがリブートするまで待ちます。

スイッチがリセットされ、RCFファイルを適用する前の既存の管理ネットワーク設定や現在のクレデンシャルなどの初期設定が保持されます。リブート後、同じバージョンまたは別のバージョンのRCFファイルを使用して新しい設定を適用できます。

## Cumulusソフトウェアのダウンロードとインストール

このタスクについて

Cumulus画像を適用してスイッチを完全にリセットするには、次の手順を実行します。

作業を開始する前に

- シリアルコンソール接続を使用してスイッチに接続する必要があります。
- Cumulusスイッチソフトウェアイメージには、HTTP経由でアクセスできます。



Cumulus Linuxのインストールの詳細については、を参照してください。"[NVIDIA SN2100 スイッチのインストールと設定の概要](#)"

- コマンドへの「sudo」アクセス用のrootパスワードが必要です。

手順

1. Cumulusコンソールから、スイッチ・ソフトウェアのインストールを「ONIE-install-A-i」コマンドに続けてスイッチ・ソフトウェアへのファイル・パスを指定して、ダウンロードしてキューに入れます。

この例では、ファームウェアファイル `cumulus-linux-4.4.3-mlx-amd64.bin` HTTPサーバ「50.50.50.50」からローカルスイッチにコピーされます。

```
cumulus@IP_switch_A_1:mgmt:~$ sudo onie-install -a -i
http://50.50.50.50/switchsoftware/cumulus-linux-4.4.3-mlx-amd64.bin
Fetching installer: http://50.50.50.50/switchsoftware/cumulus-linux-
4.4.3-mlx-amd64.bin
Downloading URL: http://50.50.50.50/switchsoftware/cumulus-linux-4.4.3-
mlx-amd64.bin
#####
# 100.0%
Success: HTTP download complete.
```

```
tar: ./sysroot.tar: time stamp 2021-01-30 17:00:58 is 53895092.604407122
s in the future
tar: ./kernel: time stamp 2021-01-30 17:00:58 is 53895092.582826352 s in
the future
tar: ./initrd: time stamp 2021-01-30 17:00:58 is 53895092.509682557 s in
the future
tar: ./embedded-installer/bootloader/grub: time stamp 2020-12-10
15:25:16 is 49482950.509433937 s in the future
tar: ./embedded-installer/bootloader/init: time stamp 2020-12-10
15:25:16 is 49482950.509336507 s in the future
tar: ./embedded-installer/bootloader/uboot: time stamp 2020-12-10
15:25:16 is 49482950.509213637 s in the future
tar: ./embedded-installer/bootloader: time stamp 2020-12-10 15:25:16 is
49482950.509153787 s in the future
tar: ./embedded-installer/lib/init: time stamp 2020-12-10 15:25:16 is
49482950.509064547 s in the future
tar: ./embedded-installer/lib/logging: time stamp 2020-12-10 15:25:16 is
49482950.508997777 s in the future
tar: ./embedded-installer/lib/platform: time stamp 2020-12-10 15:25:16
is 49482950.508913317 s in the future
tar: ./embedded-installer/lib/utility: time stamp 2020-12-10 15:25:16 is
49482950.508847367 s in the future
tar: ./embedded-installer/lib/check-onie: time stamp 2020-12-10 15:25:16
is 49482950.508761477 s in the future
tar: ./embedded-installer/lib: time stamp 2020-12-10 15:25:47 is
49482981.508710647 s in the future
tar: ./embedded-installer/storage/blk: time stamp 2020-12-10 15:25:16 is
49482950.508631277 s in the future
tar: ./embedded-installer/storage/gpt: time stamp 2020-12-10 15:25:16 is
49482950.508523097 s in the future
tar: ./embedded-installer/storage/init: time stamp 2020-12-10 15:25:16
is 49482950.508437507 s in the future
tar: ./embedded-installer/storage/mbr: time stamp 2020-12-10 15:25:16 is
49482950.508371177 s in the future
tar: ./embedded-installer/storage/mtd: time stamp 2020-12-10 15:25:16 is
49482950.508293856 s in the future
tar: ./embedded-installer/storage: time stamp 2020-12-10 15:25:16 is
49482950.508243666 s in the future
tar: ./embedded-installer/platforms.db: time stamp 2020-12-10 15:25:16
is 49482950.508179456 s in the future
tar: ./embedded-installer/install: time stamp 2020-12-10 15:25:47 is
49482981.508094606 s in the future
tar: ./embedded-installer: time stamp 2020-12-10 15:25:47 is
49482981.508044066 s in the future
tar: ./control: time stamp 2021-01-30 17:00:58 is 53895092.507984316 s
in the future
```

```
tar: .: time stamp 2021-01-30 17:00:58 is 53895092.507920196 s in the
future
Staging installer image...done.
WARNING:
WARNING: Activating staged installer requested.
WARNING: This action will wipe out all system data.
WARNING: Make sure to back up your data.
WARNING:
Are you sure (y/N)? y
Activating staged installer...done.
Reboot required to take effect.
cumulus@IP_switch_A_1:mgmt:~$
```

2. イメージのダウンロードおよび確認時に'プロンプトにyと応答してインストールを確認します
3. 新しいソフトウェア「sudo reboot」をインストールするには、スイッチを再起動します

```
cumulus@IP_switch_A_1:mgmt:~$ sudo reboot
```



スイッチがリブートし、スイッチソフトウェアのインストールが開始されます。この処理にはしばらく時間がかかります。インストールが完了すると、スイッチがリブートし、「log-in」プロンプトが表示されたままになります。

4. スwitchの基本設定を行います

- a. スwitchがブートされ、ログインプロンプトでログインし、パスワードを変更します。



ユーザ名は「cumulus」で、デフォルトのパスワードは「cumulus」です。

```
Debian GNU/Linux 10 cumulus ttyS0

cumulus login: cumulus
Password:
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password:
New password:
Retype new password:
Linux cumulus 4.19.0-cl-1-amd64 #1 SMP Cumulus 4.19.206-1+cl4.4.3u1
(2021-12-18) x86_64

Welcome to NVIDIA Cumulus (R) Linux (R)

For support and online technical documentation, visit
http://www.cumulusnetworks.com/support

The registered trademark Linux (R) is used pursuant to a sublicense from
LMI,
the exclusive licensee of Linus Torvalds, owner of the mark on a world-
wide
basis.

cumulus@cumulus:mgmt:~$
```

## 5. 管理ネットワークインターフェイスを設定

使用するコマンドは、実行しているスイッチファームウェアのバージョンによって異なります。



次に、ホスト名をIP\_switch\_A\_1、IPアドレスを10.10.10.10、ネットマスクを255.255.255.0 (24)、ゲートウェイアドレスを10.10.10.1に設定する例を示します。

#### クムルス4.4.x

次に、Cumulus 4.4.xを実行しているスイッチにホスト名、IPアドレス、ネットマスク、およびゲートウェイを設定する例を示します。

```
cumulus@cumulus:mgmt:~$ net add hostname IP_switch_A_1
cumulus@cumulus:mgmt:~$ net add interface eth0 ip address
10.0.10.10/24
cumulus@cumulus:mgmt:~$ net add interface eth0 ip gateway 10.10.10.1
cumulus@cumulus:mgmt:~$ net pending
```

```
.
.
.
```

```
cumulus@cumulus:mgmt:~$ net commit
```

```
.
.
.
```

```
net add/del commands since the last "net commit"
```

User Timestamp Command

```
cumulus 2021-05-17 22:21:57.437099 net add hostname Switch-A-1
cumulus 2021-05-17 22:21:57.538639 net add interface eth0 ip address
10.10.10.10/24
cumulus 2021-05-17 22:21:57.635729 net add interface eth0 ip gateway
10.10.10.1
```

```
cumulus@cumulus:mgmt:~$
```

#### Cumulus 5.4.x以降

次に、Cumulus 5.4.xを実行しているスイッチにホスト名、IPアドレス、ネットマスク、およびゲートウェイを設定する例を示します。以降が必要です。

```
cumulus@cumulus:mgmt:~$ nv set system hostname IP_switch_A_1

cumulus@cumulus:mgmt:~$ nv set interface eth0 ip address
10.0.10.10/24

cumulus@cumulus:mgmt:~$ nv set interface eth0 ip gateway 10.10.10.1

cumulus@cumulus:mgmt:~$ nv config apply

cumulus@cumulus:mgmt:~$ nv config save
```

6. `sudo reboot`コマンドを使用してスイッチをリブートします。

```
cumulus@cumulus:~$ sudo reboot
```

スイッチがリブートしたら、の手順に従って新しい設定を適用できます [NVIDIAのRCFファイルをダウンロードしてインストールします](#)。

### NVIDIA RCFファイルをダウンロードしてインストールします

MetroCluster IP構成の各スイッチにスイッチのRCFファイルを生成してインストールする必要があります。

作業を開始する前に

- コマンドへの「`sudo`」アクセス用のrootパスワードが必要です。
- スイッチソフトウェアがインストールされ、管理ネットワークが設定されている。
- 方法1または方法2のいずれかを使用して、スイッチを最初に設置する手順を実行しました。
- 初期インストール後に追加の設定を適用しなかった場合。



RCFファイルを適用する前にスイッチをリセットしたあとに以降の設定を実行する場合は、この手順を使用できません。

このタスクについて

この手順は、MetroCluster IP構成（新規の設置）または交換用スイッチ（スイッチの交換）の各IPスイッチで実行する必要があります。

QSFP / SFP+アダプタを使用している場合は、ISLポートをブレイクアウト速度モードではなくネイティブ速度モードで設定する必要があります。ISLポートの速度モードについては、スイッチベンダーのドキュメントを参照してください。

手順

1. MetroCluster IP用のNVIDIA RCFファイルを生成します。
  - a. をダウンロードします "["MetroCluster IP 用の RcfFileGenerator"](#)。

- b. RcfFileGenerator for MetroCluster IPを使用して、設定用のRCFファイルを生成します。
- c. ホームディレクトリに移動します。「cumulus」として記録されている場合、ファイルパスは「/home/cumulus」です。

```
cumulus@IP_switch_A_1:mgmt:~$ cd ~
cumulus@IP_switch_A_1:mgmt:~$ pwd
/home/cumulus
cumulus@IP_switch_A_1:mgmt:~$
```

- d. このディレクトリにRCFファイルをダウンロードします。次に、SCPを使用してファイルをダウンロードする例を示します。SN2100\_v2.0.0\_IP\_switch\_A\_1.txt サーバ「50.50.50.50」からホームディレクトリに保存します。SN2100\_v2.0.0\_IP\_switch\_A\_1.py:

```
cumulus@Switch-A-1:mgmt:~$ scp
username@50.50.50.50:/RcfFiles/SN2100_v2.0.0_IP_switch_A_1.txt
./SN2100_v2.0.0_IP_switch-A1.py
The authenticity of host '50.50.50.50 (50.50.50.50)' can't be
established.
RSA key fingerprint is
SHA256:B5gBtOmNZvdKiY+dPhh8=ZK9DaKG7g6sv+2gFlGVF8E.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '50.50.50.50' (RSA) to the list of known
hosts.
*****
**
Banner of the SCP server
*****
**
username@50.50.50.50's password:
SN2100_v2.0.0_IP_switch_A1.txt 100% 55KB 1.4MB/s 00:00
cumulus@IP_switch_A_1:mgmt:~$
```

- 2. RCFファイルを実行します。RCFファイルでは、1つ以上の手順を適用するためのオプションが必要です。テクニカルサポートから指示がないかぎり、コマンドラインオプションを指定せずにRCFファイルを実行します。RCFファイルのさまざまな手順の完了ステータスを確認するには、オプション「-1」または「all」を使用してすべての（保留中の）手順を適用します。

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3
SN2100_v2.0.0_IP_switch_A_1.py
all
[sudo] password for cumulus:
The switch will be rebooted after the step(s) have been run.
Enter yes or no: yes

... the steps will apply - this is generating a lot of output ...

Running Step 24: Final reboot of the switch

... The switch will reboot if all steps applied successfully ...
```

3. 構成でDACケーブルを使用する場合は、スイッチポートでDACオプションを有効にします。

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3 SN2100_v2.0.0-X10_Switch-
A1.py runCmd <switchport> DacOption [enable | disable]
```

次に、ポートのDACオプションをイネーブルにする例を示します。 swp7 :

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3 SN2100_v2.00_Switch-A1.py
runCmd swp7 DacOption enable
Running cumulus version : 5.4.0
Running RCF file version : v2.00
Running command: Enabling the DacOption for port swp7
runCmd: 'nv set interface swp7 link fast-linkup on', ret: 0
runCmd: committed, ret: 0
Completion: SUCCESS
cumulus@IP_switch_A_1:mgmt:~$
```

4. スイッチポートでDACオプションを有効にしたら、スイッチをリブートします。

```
sudo reboot
```



複数のスイッチポートにDACオプションを設定する場合は、スイッチをリブートするだけで済みます。

## 25Gbps接続を使用するシステムの前方エラー修正の設定

25Gbps接続を使用するシステムの場合は、RCFの適用後に前方誤り訂正（FEC）パラメータを手動でoffに設定します。この設定はRCFでは適用されません。

このタスクについて

- このタスクは、25Gbps接続を使用するプラットフォームにのみ該当します。を参照してください ["NVIDIAがサポートするSN2100 IPスイッチのプラットフォームポート割り当て"](#)。
- このタスクは、MetroCluster IP 構成の4つのスイッチすべてで実行する必要があります。
- 各スイッチポートは個別に更新する必要があります。コマンドで複数のポートまたはポート範囲を指定することはできません。

手順

1. 25Gbps接続を使用する最初のスイッチポートのパラメータをoffに設定し `fec` ます。

```
sudo python3 SN2100_v2.0_Switch-A1.py runCmd <switchport> fec off
```

2. コントローラモジュールに接続されている25Gbpsスイッチポートごとに、この手順を繰り返します。

## MetroCluster IP インターフェイスのスイッチポート速度の設定

このタスクについて

- 次の手順を使用して、スイッチポート速度を100Gに設定します。
  - AFF A70、AFF A90、AFF A1K、AFF C80
  - AFF A30、AFF C30、AFF A50、AFF C60
  - FAS50、FAS70、FAS90
- 各スイッチポートは個別に更新する必要があります。コマンドで複数のポートまたはポート範囲を指定することはできません。

ステップ

1. 速度を設定するには、オプションを指定してRCFファイルを使用し runCmd ます。これにより、設定が適用され、設定が保存されます。

次のコマンドは、MetroClusterインターフェイスおよびの速度を設定し swp7 `swp8` ます。

```
sudo python3 SN2100_v2.20 _Switch-A1.py runCmd swp7 speed 100
```

```
sudo python3 SN2100_v2.20 _Switch-A1.py runCmd swp8 speed 100
```

- 例 \*

```
cumulus@Switch-A-1:mgmt:~$ sudo python3 SN2100_v2.20_Switch-A1.py runCmd
swp7 speed 100
[sudo] password for cumulus: <password>
Running cumulus version : 5.4.0
Running RCF file version : v2.20
Running command: Setting switchport swp7 to 100G speed
runCmd: 'nv set interface swp7 link auto-negotiate off', ret: 0
runCmd: 'nv set interface swp7 link speed 100G', ret: 0
runCmd: committed, ret: 0
Completion: SUCCESS
cumulus@Switch-A-1:mgmt:~$
```

## 未使用のISLポートとポートチャネルを無効にする

NetAppでは、不要なヘルスアラートを回避するために、未使用のISLポートとポートチャネルを無効にすることを推奨します各ポートまたはポートチャネルを個別にディセーブルにする必要があります。コマンドで複数のポートまたはポート範囲を指定することはできません。

### 手順

1. RCFファイルのバナーを使用して、未使用のISLポートとポートチャネルを特定します。



ポートがブレイクアウトモードの場合は、コマンドで指定するポート名がRCFバナーに表示される名前と異なることがあります。RCFケーブル接続ファイルを使用してポート名を検索することもできます。

```
net show interface
```

2. RCFファイルを使用して、未使用のISLポートとポートチャネルを無効にします。

```

cumulus@mcc1-integrity-a1:mgmt:~$ sudo python3 SN2100_v2.0_IP_Switch-
A1.py runCmd
[sudo] password for cumulus:
    Running cumulus version   : 5.4.0
    Running RCF file version  : v2.0
Help for runCmd:
    To run a command execute the RCF script as follows:
    sudo python3 <script> runCmd <option-1> <option-2> <option-x>
    Depending on the command more or less options are required. Example
to 'up' port 'swp1'
    sudo python3 SN2100_v2.0_IP_Switch-A1.py runCmd swp1 up
Available commands:
    UP / DOWN the switchport
        sudo python3 SN2100_v2.0_IP_Switch-A1.py runCmd <switchport>
state <up | down>
    Set the switch port speed
        sudo python3 SN2100_v2.0_Switch-A1.py runCmd <switchport>
speed <10 | 25 | 40 | 100 | AN>
    Set the fec mode on the switch port
        sudo python3 SN2100_v2.0_Switch-A1.py runCmd <switchport>
fec <default | auto | rs | baser | off>
    Set the [localISL | remoteISL] to 'UP' or 'DOWN' state
        sudo python3 SN2100_v2.0_Switch-A1.py runCmd [localISL |
remoteISL] state [up | down]
    Set the option on the port to support DAC cables. This option
does not support port ranges.
    You must reload the switch after changing this option for
the required ports. This will disrupt traffic.
    This setting requires Cumulus 5.4 or a later 5.x release.
        sudo python3 SN2100_v2.0_Switch-A1.py runCmd <switchport>
DacOption [enable | disable]
cumulus@mcc1-integrity-a1:mgmt:~$

```

次の例では、ポート「swp14」を無効にします。

```
sudo python3 SN2100_v2.0_Switch-A1.py runCmd swp14 state down
```

特定された未使用のポートまたはポートチャンネルごとに、この手順を繰り返します。

**NVIDIA SN2100 MetroCluster IP**スイッチ用のイーサネットスイッチヘルスマニター構成ファイルをインストールします。

**NVIDIA イーサネット スイッチ**でイーサネット スイッチのヘルス モニタリングを構成するには、次の手順に従います。

これらの手順は、NVIDIA X190006-PEおよびX190006-PIスイッチが正しく検出されない場合に適用されます。これは、実行することで確認できます。system switch ethernet show`お使いのモデル

に\*OTHER\*が表示されているかどうかを確認してください。NVIDIAスイッチのモデルを確認するには、コマンドで部品番号を検索してください。`nv show platform hardware NVIDIA CL 5.8以前または`nv show platform`それ以降のバージョンの場合。



以下のONTAPリリースでNVIDIA CL 5.11.xを使用する際に、ヘルスマモニタリングとログ収集を意図したとおりに動作させたい場合にも、これらの手順を実行することをお勧めします。これらの手順を実行しなくてもヘルスマモニタリングとログ収集は機能する可能性がありますが、実行することですべてが正しく動作することが保証されます。

- 9.10.1P20、9.11.1P18、9.12.1P16、9.13.1P8、9.14.1、9.15.1以降のパッチリリース

作業を開始する前に

- ONTAP クラスタが起動し、実行中であることを確認します。
- CSHM で利用可能なすべての機能を使用するには、スイッチで SSH を有効にします。
- すべてのノードでディレクトリをクリアし `/mroot/etc/cshm\_nod/nod\_sign/` ます。

- a. ノードシェルに切り替えます。

```
system node run -node <name>
```

- b. advanced権限に切り替えます。

```
priv set advanced
```

- c. ディレクトリ内の構成ファイルを一覧表示します /etc/cshm\_nod/nod\_sign。ディレクトリが存在し、構成ファイルが含まれている場合は、ファイル名がリストされます。

```
ls /etc/cshm_nod/nod_sign
```

- d. 接続されているスイッチモデルに対応する構成ファイルをすべて削除します。

不明な場合は、上記のサポートされているモデルのすべての構成ファイルを削除してから、それらの同じモデルの最新の構成ファイルをダウンロードしてインストールしてください。

```
rm /etc/cshm_nod/nod_sign/<filename>
```

- a. 削除した構成ファイルがディレクトリに存在しないことを確認します。

```
ls /etc/cshm_nod/nod_sign
```

手順

1. 対応するONTAPリリースバージョンに基づいて、イーサネットスイッチヘルスマモニタ構成のzipファイルをダウンロードします。このファイルは、ページから入手でき **"NVIDIAイーサネットスイッチ"** ます。
  - a. NVIDIA SN2100ソフトウェアのダウンロードページで、\*Nvidia CSHMファイル\*を選択します。
  - b. [注意/必ずお読みください]ページで、同意するチェックボックスをオンにします。
  - c. [End User License Agreement]ページで、同意するチェックボックスを選択し、\*[Accept & Continue]\* をクリックします。
  - d. Nvidia CSHM File - Download (Nvidia CSHMファイル-ダウンロード) ページで、適切な設定ファイル

を選択します。次のファイルを使用できます。

#### ONTAP 9.15.1以降

- MSN2100-CB2FC-v1.4.zip
- MSN2100-CB2RC-v1.4.zip
- X190006-PE-v1.4.zip
- X190006-PI-v1.4.zip

#### ONTAP 9.11.1~9.14.1

- MSN2100-CB2FC\_PRIOR\_R9.15.1-v1.4.zip
- MSN2100-CB2RC\_PRIOR\_R9.15.1-v1.4.zip
- X190006-PE\_PRIOR\_9.15.1-v1.4.zip
- X190006-PI\_PRIOR\_9.15.1-v1.4.zip

1. 該当するzipファイルを内部Webサーバにアップロードします。
2. クラスタ内のいずれかのONTAPシステムからadvancedモード設定にアクセスします。

「advanced」の権限が必要です

3. switch health monitor configureコマンドを実行します。

```
cluster1::> system switch ethernet configure-health-monitor
```

4. 使用しているONTAPのバージョンに応じて、コマンド出力の末尾が次のテキストになっていることを確認します。

#### ONTAP 9.15.1以降

イーサネットスイッチヘルスマニタに構成ファイルがインストールされました。

#### ONTAP 9.11.1~9.14.1

SHMは設定ファイルをインストールしました。

#### ONTAP 9.10.1

CSHMダウンロードパッケージが正常に処理されました。

エラーが発生した場合は、NetAppサポートにお問い合わせください。

1. を実行すると検出されたイーサネットスイッチヘルスマニタのポーリング間隔が最大2倍になるまで待つて `system switch ethernet polling-interval show` から、次の手順を完了します。
2. コマンドを実行する `system switch ethernet configure-health-monitor show` ONTAPシステムで、監視対象フィールドが **True** に設定され、シリアル番号フィールドに **Unknown** が表示されていない状態でクラスタスイッチが検出されていることを確認します。

```
cluster1::> system switch ethernet configure-health-monitor show
```



構成ファイルを適用してもモデルに\*その他\*が表示される場合は、NetAppサポートにお問い合わせください。

参照 ["システムスイッチイーサネットヘルスマニターの設定"](#) 詳細についてはコマンドを参照してください。

次の手順

["スイッチヘルス監視の設定"](#)です。

## MetroCluster IPスイッチの健全性を監視する

MetroCluster IP構成におけるスイッチヘルスマニタリングについて学習します

イーサネットスイッチヘルスマニタ (CSHM) は、クラスタネットワークスイッチとストレージネットワークスイッチの動作の健全性を確認し、デバッグ用にスイッチのログを収集します。

MetroCluster IP構成でCSHMを構成する際の重要な注意事項

このセクションでは、Cisco、Broadcom、NVIDIA SN2100スイッチでSNMPv3とログ収集を設定するための一般的な手順について説明します。MetroCluster構成でサポートされているスイッチファームウェアバージョンに応じた手順に従う必要があります。"[Hardware Universe](#)"サポートされているファームウェアのバージョンを確認します。

MetroCluster 構成では、ローカル クラスタ スイッチに対してのみヘルス モニタリングを構成します。

BroadcomおよびCiscoスイッチでログ収集を行う場合、ログ収集が有効になっているクラスタごとに、スイッチ上に新しいユーザーを作成する必要があります。MetroCluster構成では、MetroCluster 1、MetroCluster 2、MetroCluster 3、およびMetroCluster 4のそれぞれについて、スイッチ上に個別のユーザーを設定する必要があります。これらのスイッチは、同じユーザーに対して複数のSSHキーをサポートしません。追加のログ収集設定を実行すると、そのユーザーの既存のSSHキーが上書きされます。

CSHM を設定する前に、不要な ISL アラートを回避するために、使用されていない ISL を無効にする必要があります。

MetroCluster IPスイッチの健全性を監視するためにSNMPv3を構成する

MetroCluster IP構成では、IPスイッチのヘルスを監視するようにSNMPv3を設定できません。

この手順は、スイッチ上で SNMPv3 を構成するための一般的な手順を示しています。記載されているスイッチファームウェアバージョンの一部は、MetroCluster IP構成ではサポートされない可能性があります。

MetroCluster IP構成でサポートされているスイッチファームウェアバージョンに応じた手順に従う必要があります。"[Hardware Universe](#)"サポートされているファームウェアのバージョンを確認します。



- SNMPv3は、ONTAP 9.12.1以降でのみサポートされます。
- ONTAP 9.13.1P12、9.14.1P9、9.15.1P5、9.16.1 以降のバージョンでは、次の2つの問題が修正されています。
  - "CiscoスイッチのONTAPヘルスマニタリングでは、モニタリングをSNMPv3に切り替えた後もSNMPv2トラフィックが引き続き表示されることがあります。"
  - "SNMP障害発生時にスイッチファンと電源の誤検知アラートを通知"

このタスクについて

Broadcom、**Cisco** \*、および NVIDIA \*スイッチでSNMPv3ユーザ名を設定するには、次のコマンドを使用します。

## Broadcomスイッチ

Broadcom BES-53248スイッチでSNMPv3ユーザ名network-operatorを設定します。

- 認証なし\*の場合：

```
snmp-server user SNMPv3UserNoAuth NETWORK-OPERATOR noauth
```

- MD5/SHA認証の場合\*：

```
snmp-server user SNMPv3UserAuth NETWORK-OPERATOR [auth-md5|auth-sha]
```

- AES/DES暗号化を使用した\* MD5/SHA認証の場合\*：

```
snmp-server user SNMPv3UserAuthEncrypt NETWORK-OPERATOR [auth-  
md5|auth-sha] [priv-aes128|priv-des]
```

次のコマンドは、ONTAP側でSNMPv3ユーザ名を設定します。

```
security login create -user-or-group-name SNMPv3_USER -application snmp  
-authentication-method usm -remote-switch-ipaddress ADDRESS
```

次のコマンドは、CSHMでSNMPv3ユーザ名を確立します。

```
cluster1::*> system switch ethernet modify -device DEVICE -snmp-version  
SNMPv3 -community-or-username SNMPv3_USER
```

## 手順

1. 認証と暗号化を使用するようにスイッチのSNMPv3ユーザを設定します。

```
show snmp status
```

```
(sw1) (Config)# snmp-server user <username> network-admin auth-md5
<password> priv-aes128 <password>
```

```
(cs1) (Config)# show snmp user snmp
```

Name	Group Name	Auth Meth	Priv Meth	Remote Engine ID
<username>	network-admin	MD5	AES128	8000113d03d8c497710bee

## 2. ONTAP 側でSNMPv3ユーザをセットアップします。

```
security login create -user-or-group-name <username> -application
snmp -authentication-method usm -remote-switch-ipaddress
10.231.80.212
```

```
cluster1::*> security login create -user-or-group-name <username>
-application snmp -authentication-method usm -remote-switch
-ipaddress 10.231.80.212
```

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha, sha2-256)

[none]: **md5**

Enter the authentication protocol password (minimum 8 characters long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)

[none]: **aes128**

Enter privacy protocol password (minimum 8 characters long):

Enter privacy protocol password again:

## 3. 新しいSNMPv3ユーザで監視するようにCSHMを設定します。

```
system switch ethernet show-all -device "sw1" -instance
```

```

cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance

Device Name: sw1
IP Address: 10.228.136.24
SNMP Version: SNMPv2c
Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
Community String or SNMPv3 Username: cshml!
Model Number: BES-53248
Switch Network: cluster-network
Software Version: 3.9.0.2
Reason For Not Monitoring: None <---- should
display this if SNMP settings are valid
Source Of Switch Version: CDP/ISDP
Is Monitored ?: true
Serial Number of the Device: QTFCU3826001C
RCF Version: v1.8X2 for

Cluster/HA/RDMA

cluster1::*>
cluster1::*> system switch ethernet modify -device "sw1" -snmp
-version SNMPv3 -community-or-username <username>

```

4. CSHM ポーリング期間を待った後、イーサネットスイッチのシリアル番号が入力されていることを確認します。

```

system switch ethernet polling-interval show

```

```

cluster1::*> system switch ethernet polling-interval show
Polling Interval (in minutes): 5

cluster1::*> system switch ethernet show-all -device "sw1" -instance
Device Name: sw1
IP Address: 10.228.136.24
SNMP Version: SNMPv3
Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
Community String or SNMPv3 Username: <username>
Model Number: BES-53248
Switch Network: cluster-network
Software Version: 3.9.0.2
Reason For Not Monitoring: None <---- should
display this if SNMP settings are valid
Source Of Switch Version: CDP/ISDP
Is Monitored?: true
Serial Number of the Device: QTFCU3826001C
RCF Version: v1.8X2 for

Cluster/HA/RDMA

```

## Cisco スイッチ

Cisco 9336C-FX2スイッチでSNMPv3ユーザ名SNMPv3\_userを設定します。

- 認証なし\*の場合：

```
snmp-server user SNMPv3_USER NoAuth
```

- MD5/SHA認証の場合\*：

```
snmp-server user SNMPv3_USER auth [md5|sha] AUTH-PASSWORD
```

- AES/DES暗号化を使用した\* MD5/SHA認証の場合\*：

```
snmp-server user SNMPv3_USER AuthEncrypt auth [md5|sha] AUTH-
PASSWORD priv aes-128 PRIV-PASSWORD
```

次のコマンドは、ONTAP側でSNMPv3ユーザ名を設定します。

```
security login create -user-or-group-name SNMPv3_USER -application snmp
-authentication-method usm -remote-switch-ipaddress ADDRESS
```

次のコマンドは、CSHMでSNMPv3ユーザ名を確立します。

```
system switch ethernet modify -device DEVICE -snmp-version SNMPv3
-community-or-username SNMPv3_USER
```

手順

1. 認証と暗号化を使用するようにスイッチのSNMPv3ユーザを設定します。

```
show snmp user
```

```
(sw1) (Config) # snmp-server user SNMPv3User auth md5 <auth_password>
priv aes-128 <priv_password>
```

```
(sw1) (Config) # show snmp user
```

```
-----
-----
                                SNMP USERS
-----
-----
```

User	Auth	Priv(enforce)	Groups
acl_filter			
admin	md5	des(no)	network-admin
SNMPv3User	md5	aes-128(no)	network-operator

```
-----
-----
NOTIFICATION TARGET USERS (configured for sending V3 Inform)
-----
-----
```

User	Auth	Priv
------	------	------

```
(sw1) (Config) #
```

2. ONTAP 側でSNMPv3ユーザをセットアップします。

```
security login create -user-or-group-name <username> -application  
snmp -authentication-method usm -remote-switch-ipaddress  
10.231.80.212
```

```
cluster1::*> system switch ethernet modify -device "sw1  
(b8:59:9f:09:7c:22)" -is-monitoring-enabled-admin true
```

```
cluster1::*> security login create -user-or-group-name <username>  
-application snmp -authentication-method usm -remote-switch  
-ipaddress 10.231.80.212
```

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,  
sha2-256)

[none]: **md5**

Enter the authentication protocol password (minimum 8 characters  
long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)

[none]: **aes128**

Enter privacy protocol password (minimum 8 characters long):

Enter privacy protocol password again:

3. 新しいSNMPv3ユーザで監視するようにCSHMを設定します。

```
system switch ethernet show-all -device "sw1" -instance
```

```

cluster1::*> system switch ethernet show-all -device "sw1" -instance

                Device Name: sw1
                IP Address: 10.231.80.212
                SNMP Version: SNMPv2c
                Is Discovered: true
                SNMPv2c Community String or SNMPv3 Username: cshml!
                Model Number: N9K-C9336C-FX2
                Switch Network: cluster-network
                Software Version: Cisco Nexus
Operating System (NX-OS) Software, Version 9.3(7)
                Reason For Not Monitoring: None <---- displays
when SNMP settings are valid
                Source Of Switch Version: CDP/ISDP
                Is Monitored?: true
                Serial Number of the Device: QTFCU3826001C
                RCF Version: v1.8X2 for

Cluster/HA/RDMA

cluster1::*>
cluster1::*> system switch ethernet modify -device "sw1" -snmp
-version SNMPv3 -community-or-username <username>
cluster1::*>

```

4. 新しく作成したSNMPv3ユーザで照会するシリアル番号が、CSHMポーリング期間の完了後に前の手順で説明したものと同一であることを確認します。

```

system switch ethernet polling-interval show

```

```

cluster1::*> system switch ethernet polling-interval show
Polling Interval (in minutes): 5

cluster1::*> system switch ethernet show-all -device "sw1" -instance

Device Name: sw1
IP Address: 10.231.80.212
SNMP Version: SNMPv3
Is Discovered: true
SNMPv2c Community String or SNMPv3 Username: SNMPv3User
Model Number: N9K-C9336C-FX2
Switch Network: cluster-network
Software Version: Cisco Nexus
Operating System (NX-OS) Software, Version 9.3(7)
Reason For Not Monitoring: None <---- displays
when SNMP settings are valid
Source Of Switch Version: CDP/ISDP
Is Monitored?: true
Serial Number of the Device: QTFCU3826001C
RCF Version: v1.8X2 for
Cluster/HA/RDMA

cluster1::*>

```

## NVIDIA - CL 5.4.0

CLI 5.4.0 を実行している NVIDIA SN2100 スイッチで SNMPv3 ユーザー名 SNMPv3\_USER を設定します。

- 認証なし\*の場合：

```
nv set service snmp-server username SNMPv3_USER auth-none
```

- MD5/SHA認証の場合\*：

```
nv set service snmp-server username SNMPv3_USER [auth-md5|auth-sha]
AUTH-PASSWORD
```

- AES/DES暗号化を使用した\* MD5/SHA認証の場合\*：

```
nv set service snmp-server username SNMPv3_USER [auth-md5|auth-sha]
AUTH-PASSWORD [encrypt-aes|encrypt-des] PRIV-PASSWORD
```

次のコマンドは、ONTAP側でSNMPv3ユーザ名を設定します。

```
security login create -user-or-group-name SNMPv3_USER -application snmp
-authentication-method usm -remote-switch-ipaddress ADDRESS
```

次のコマンドは、CSHMでSNMPv3ユーザ名を確立します。

```
system switch ethernet modify -device DEVICE -snmp-version SNMPv3
-community-or-username SNMPv3_USER
```

手順

1. 認証と暗号化を使用するようにスイッチのSNMPv3ユーザを設定します。

```
net show snmp status
```

```
cumulus@sw1:~$ net show snmp status
Simple Network Management Protocol (SNMP) Daemon.
-----
Current Status          active (running)
Reload Status           enabled
Listening IP Addresses  all vrf mgmt
Main snmpd PID          4318
Version 1 and 2c Community String Configured
Version 3 Usernames     Not Configured
-----

cumulus@sw1:~$
cumulus@sw1:~$ net add snmp-server username SNMPv3User auth-md5
<password> encrypt-aes <password>
cumulus@sw1:~$ net commit
--- /etc/snmp/snmpd.conf      2020-08-02 21:09:34.686949282 +0000
+++ /run/nclu/snmp/snmpd.conf 2020-08-11 00:13:51.826126655 +0000
@@ -1,26 +1,28 @@
# Auto-generated config file: do not edit. #
agentaddress udp:@mgmt:161
agentxperms 777 777 snmp snmp
agentxsocket /var/agentx/master
createuser _snmptrapusernameX
+createuser SNMPv3User MD5 <password> AES <password>
ifmib_max_num_ifaces 500
iquerysecname _snmptrapusernameX
master agentx
monitor -r 60 -o laNames -o laErrorMessage "laTable" laErrorFlag != 0
```

```

pass -p 10 1.3.6.1.2.1.1.1 /usr/share/snmp/sysDescr_pass.py
pass_persist 1.2.840.10006.300.43
/usr/share/snmp/ieee8023_lag_pp.py
pass_persist 1.3.6.1.2.1.17 /usr/share/snmp/bridge_pp.py
pass_persist 1.3.6.1.2.1.31.1.1.1.18
/usr/share/snmp/snmpifAlias_pp.py
pass_persist 1.3.6.1.2.1.47 /usr/share/snmp/entity_pp.py
pass_persist 1.3.6.1.2.1.99 /usr/share/snmp/entity_sensor_pp.py
pass_persist 1.3.6.1.4.1.40310.1 /usr/share/snmp/resq_pp.py
pass_persist 1.3.6.1.4.1.40310.2
/usr/share/snmp/cl_drop_cntrs_pp.py
pass_persist 1.3.6.1.4.1.40310.3 /usr/share/snmp/cl_poe_pp.py
pass_persist 1.3.6.1.4.1.40310.4 /usr/share/snmp/bgpun_pp.py
pass_persist 1.3.6.1.4.1.40310.5 /usr/share/snmp/cumulus-status.py
pass_persist 1.3.6.1.4.1.40310.6 /usr/share/snmp/cumulus-sensor.py
pass_persist 1.3.6.1.4.1.40310.7 /usr/share/snmp/vrf_bgpun_pp.py
+rocommunity cshml! default
rouser _snmptrapusernameX
+rouser SNMPv3User priv
sysobjectid 1.3.6.1.4.1.40310
syssservices 72
-rocommunity cshml! default

```

net add/del commands since the last "net commit"

User	Timestamp	Command
SNMPv3User	2020-08-11 00:13:51.826987	net add snmp-server username SNMPv3User auth-md5 <password> encrypt-aes <password>

```

cumulus@sw1:~$
cumulus@sw1:~$ net show snmp status
Simple Network Management Protocol (SNMP) Daemon.
-----
Current Status          active (running)
Reload Status           enabled
Listening IP Addresses  all vrf mgmt
Main snmpd PID          24253
Version 1 and 2c Community String Configured
Version 3 Usernames     Configured    <---- Configured
here
-----

```

```

cumulus@sw1:~$

```

## 2. ONTAP 側でSNMPv3ユーザをセットアップします。

```
security login create -user-or-group-name SNMPv3User -application  
snmp -authentication-method usm -remote-switch-ipaddress  
10.231.80.212
```

```
cluster1::*> security login create -user-or-group-name SNMPv3User  
-application snmp -authentication-method usm -remote-switch  
-ipaddress 10.231.80.212
```

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,  
sha2-256)

[none]: **md5**

Enter the authentication protocol password (minimum 8 characters  
long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)

[none]: **aes128**

Enter privacy protocol password (minimum 8 characters long):

Enter privacy protocol password again:

## 3. 新しいSNMPv3ユーザで監視するようにCSHMを設定します。

```
system switch ethernet show-all -device "sw1 (b8:59:9f:09:7c:22)"  
-instance
```

```

cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance
Device Name: sw1
(b8:59:9f:09:7c:22)
IP Address: 10.231.80.212
SNMP Version: SNMPv2c
Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
Community String or SNMPv3 Username: cshml!
Model Number: MSN2100-CB2FC
Switch Network: cluster-network
Software Version: Cumulus Linux
version 5.4.0 running on Mellanox Technologies Ltd. MSN2100
Reason For Not Monitoring: None
Source Of Switch Version: LLDP
Is Monitored?: true
Serial Number of the Device: MT2110X06399 <----
serial number to check
RCF Version: MSN2100-RCF-v1.9X6-
Cluster-LLDP Aug-18-2022

cluster1::*>
cluster1::*> system switch ethernet modify -device "sw1
(b8:59:9f:09:7c:22)" -snmp-version SNMPv3 -community-or-username
SNMPv3User

```

4. 新しく作成したSNMPv3ユーザで照会するシリアル番号が、CSHMポーリング期間の完了後に前の手順で説明したものと同一であることを確認します。

```
system switch ethernet polling-interval show
```

```

cluster1::*> system switch ethernet polling-interval show
Polling Interval (in minutes): 5

cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance
Device Name: sw1
IP Address: 10.231.80.212
SNMP Version: SNMPv3
Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
Community String or SNMPv3 Username: SNMPv3User
Model Number: MSN2100-CB2FC
Switch Network: cluster-network
Software Version: Cumulus Linux
version 5.4.0 running on Mellanox Technologies Ltd. MSN2100
Reason For Not Monitoring: None
Source Of Switch Version: LLDP
Is Monitored?: true
Serial Number of the Device: MT2110X06399 <----
serial number to check
RCF Version: MSN2100-RCF-v1.9X6-
Cluster-LLDP Aug-18-2022

```

### NVIDIA - CL 5.11.0

CLI 5.11.0 を実行している NVIDIA SN2100 スイッチで SNMPv3 ユーザー名 SNMPv3\_USER を設定します。

- 認証なし\*の場合：

```
nv set system snmp-server username SNMPv3_USER auth-none
```

- MD5/SHA認証の場合\*：

```
nv set system snmp-server username SNMPv3_USER [auth-md5|auth-sha]
AUTH-PASSWORD
```

- AES/DES暗号化を使用した\* MD5/SHA認証の場合\*：

```
nv set system snmp-server username SNMPv3_USER [auth-md5|auth-sha]
AUTH-PASSWORD [encrypt-aes|encrypt-des] PRIV-PASSWORD
```

次のコマンドは、ONTAP側でSNMPv3ユーザ名を設定します。

```
security login create -user-or-group-name SNMPv3_USER -application snmp
-authentication-method usm -remote-switch-ipaddress ADDRESS
```

次のコマンドは、CSHMでSNMPv3ユーザ名を確立します。

```
system switch ethernet modify -device DEVICE -snmp-version SNMPv3
-community-or-username SNMPv3_USER
```

手順

1. 認証と暗号化を使用するようにスイッチのSNMPv3ユーザを設定します。

```
nv show system snmp-server
```

```
cumulus@sw1:~$ nv show system snmp-server
                                applied
-----
[username]                       SNMPv3_USER
[username]                       limiteduser1
[username]                       testuserauth
[username]                       testuserauthaes
[username]                       testusernoauth
trap-link-up
  check-frequency                 60
trap-link-down
  check-frequency                 60
[listening-address]              all
[readonly-community]             $nvsec$94d69b56e921aec1790844eb53e772bf
state                             enabled
cumulus@sw1:~$
```

2. ONTAP 側でSNMPv3ユーザをセットアップします。

```
security login create -user-or-group-name SNMPv3User -application
snmp -authentication-method usm -remote-switch-ipaddress
10.231.80.212
```

```
cluster1::*> security login create -user-or-group-name SNMPv3User
-application snmp -authentication-method usm -remote-switch
-ipaddress 10.231.80.212
```

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha, sha2-256)

[none]: **md5**

Enter the authentication protocol password (minimum 8 characters long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)

[none]: **aes128**

Enter privacy protocol password (minimum 8 characters long):

Enter privacy protocol password again:

### 3. 新しいSNMPv3ユーザで監視するようにCSHMを設定します。

```
system switch ethernet show-all -device "sw1 (b8:59:9f:09:7c:22)"
-instance
```

```

cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance
Device Name: sw1
(b8:59:9f:09:7c:22)
IP Address: 10.231.80.212
SNMP Version: SNMPv2c
Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
Community String or SNMPv3 Username: cshml!
Model Number: MSN2100-CB2FC
Switch Network: cluster-network
Software Version: Cumulus Linux
version 5.11.0 running on Mellanox Technologies Ltd. MSN2100
Reason For Not Monitoring: None
Source Of Switch Version: LLDP
Is Monitored?: true
Serial Number of the Device: MT2110X06399 <----
serial number to check
RCF Version: MSN2100-RCF-v1.9X6-
Cluster-LLDP Aug-18-2022

cluster1::*>
cluster1::*> system switch ethernet modify -device "sw1
(b8:59:9f:09:7c:22)" -snmp-version SNMPv3 -community-or-username
SNMPv3User

```

4. 新しく作成したSNMPv3ユーザで照会するシリアル番号が、CSHMポーリング期間の完了後に前の手順で説明したものと同一であることを確認します。

```
system switch ethernet polling-interval show
```

```

cluster1::*> system switch ethernet polling-interval show
Polling Interval (in minutes): 5

cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance
Device Name: sw1
IP Address: 10.231.80.212
SNMP Version: SNMPv3
Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
Community String or SNMPv3 Username: SNMPv3User
Model Number: MSN2100-CB2FC
Switch Network: cluster-network
Software Version: Cumulus Linux
version 5.11.0 running on Mellanox Technologies Ltd. MSN2100
Reason For Not Monitoring: None
Source Of Switch Version: LLDP
Is Monitored?: true
Serial Number of the Device: MT2110X06399 <----
serial number to check
RCF Version: MSN2100-RCF-v1.9X6-
Cluster-LLDP Aug-18-2022

```

## MetroCluster IPスイッチでログ収集を構成する

MetroCluster IP 構成では、デバッグの目的でスイッチ ログを収集するようにログ収集を設定できます。



BroadcomおよびCiscoスイッチでは、ログ収集を行うクラスタごとに新しいユーザーが必要です。例えば、MetroCluster 1、MetroCluster 2、MetroCluster 3、MetroCluster 4のそれぞれについて、スイッチ上で個別のユーザーを設定する必要があります。同一ユーザーに対して複数のSSHキーを設定することはサポートされていません。

### このタスクについて

イーサネットスイッチヘルスマニタ (CSHM) は、クラスタネットワークスイッチとストレージネットワークスイッチの動作の健全性を確認し、デバッグ用にスイッチのログを収集します。この手順では、収集を設定し、詳細な\*サポート\*ログを要求し、AutoSupportによって収集される\*定期的\*データの1時間ごとの収集を有効にするプロセスをガイドします。

注： FIPSモードを有効にする場合は、次の手順を実行する必要があります。



1. ベンダーの指示に従って、スイッチでSSHキーを再生成します。
2. を使用したONTAPでのSSHキーの再生成 `debug system regenerate-systemshell-key-pair`
3. ``system switch ethernet log setup-password`` コマンドを使用してログ収集セットアップルーチンを再実行します。

作業を開始する前に

- ユーザはスイッチコマンドにアクセスできる必要があります `show`。これらが使用できない場合は、新しいユーザを作成し、必要な権限をユーザに付与します。
- スwitchのヘルスマニタが有効になっている必要があります。これを確かめるためには、``Is Monitored:`` フィールドが`*true*`に設定されている場合は、``system switch ethernet show`` 指示。
- BroadcomおよびCiscoスイッチを使用したログ収集の場合：
  - ローカル ユーザーにはネットワーク管理者権限が必要です。
  - ログ収集を有効にして、クラスタセットアップごとにスイッチに新しいユーザを作成する必要があります。これらのスイッチは、同じユーザに対して複数のSSHキーをサポートしません。追加のログ収集設定を実行すると、そのユーザの既存のSSHキーが上書きされます。
- NVIDIAスイッチを使用したログ収集をサポートするには、``cl-support`` パスワードを入力せずにコマンドを実行できる `_user_for` ログ収集を許可する必要があります。この使用を許可するには、次のコマンドを実行します。

```
echo '<user> ALL = NOPASSWD: /usr/cumulus/bin/cl-support' | sudo EDITOR='tee  
-a' visudo -f /etc/sudoers.d/cumulus
```

手順

## ONTAP 9.15.1以降

1. ログ収集を設定するには、スイッチごとに次のコマンドを実行します。ログ収集用のスイッチ名、ユーザ名、およびパスワードの入力を求められます。

注意: ユーザー指定プロンプトに「y」と答える場合は、ユーザーが以下の必要な権限を持っていることを確認してください。 [\[作業を開始する前に\]](#)。

```
system switch ethernet log setup-password
```

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs1
Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs2

Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>
```



CL 5.11.1 の場合、ユーザー **cumulus** を作成し、次のプロンプトに **y** と応答します: ログ収集に admin 以外のユーザーを指定しますか? {y|n}: **y**

1. 定期的なログ収集を有効にする:

```
system switch ethernet log modify -device <switch-name> -periodic
-enabled true
```

```
cluster1::*> system switch ethernet log modify -device cs1 -periodic
-enabled true
```

Do you want to modify the cluster switch log collection configuration? {y|n}: [n] **y**

**cs1:** Periodic log collection has been scheduled to run every hour.

```
cluster1::*> system switch ethernet log modify -device cs2 -periodic
-enabled true
```

Do you want to modify the cluster switch log collection configuration? {y|n}: [n] **y**

**cs2:** Periodic log collection has been scheduled to run every hour.

```
cluster1::*> system switch ethernet log show
```

	Periodic	Periodic
Support		
Switch	Log Enabled	Log State
Log State		
cs1	true	scheduled
never-run		
cs2	true	scheduled
never-run		

2 entries were displayed.

## 2. サポートログ収集のリクエスト：

```
system switch ethernet log collect-support-log -device <switch-name>
```

```
cluster1::*> system switch ethernet log collect-support-log -device
cs1
```

```
cs1: Waiting for the next Ethernet switch polling cycle to begin
support collection.
```

```
cluster1::*> system switch ethernet log collect-support-log -device
cs2
```

```
cs2: Waiting for the next Ethernet switch polling cycle to begin
support collection.
```

```
cluster1::*> *system switch ethernet log show
```

	Periodic	Periodic
Support		
Switch	Log Enabled	Log State
Log State		
cs1	false	halted
initiated		
cs2	true	scheduled
initiated		

2 entries were displayed.

3. イネーブルメント、ステータスメッセージ、前回のタイムスタンプと定期収集のファイル名、要求ステータス、ステータスメッセージ、前回のタイムスタンプとサポート収集のファイル名など、ログ収集のすべての詳細を表示するには、次のコマンドを使用します。

```
system switch ethernet log show -instance
```

```
cluster1::*> system switch ethernet log show -instance

                Switch Name: cs1
    Periodic Log Enabled: true
        Periodic Log Status: Periodic log collection has been
scheduled to run every hour.
    Last Periodic Log Timestamp: 3/11/2024 11:02:59
        Periodic Log Filename: cluster1:/mroot/etc/log/shm-
cluster-info.tgz
    Support Log Requested: false
        Support Log Status: Successfully gathered support logs
- see filename for their location.
    Last Support Log Timestamp: 3/11/2024 11:14:20
        Support Log Filename: cluster1:/mroot/etc/log/shm-
cluster-log.tgz

                Switch Name: cs2
    Periodic Log Enabled: false
        Periodic Log Status: Periodic collection has been
halted.
    Last Periodic Log Timestamp: 3/11/2024 11:05:18
        Periodic Log Filename: cluster1:/mroot/etc/log/shm-
cluster-info.tgz
    Support Log Requested: false
        Support Log Status: Successfully gathered support logs
- see filename for their location.
    Last Support Log Timestamp: 3/11/2024 11:18:54
        Support Log Filename: cluster1:/mroot/etc/log/shm-
cluster-log.tgz
2 entries were displayed.
```

#### ONTAP 9.14.1以前

1. ログ収集を設定するには、スイッチごとに次のコマンドを実行します。ログ収集用のスイッチ名、ユーザ名、およびパスワードの入力を求められます。

\*注：\*ユーザー指定プロンプトに回答する場合は y、で説明されているように、ユーザーに必要な権限があることを確認してください[作業を開始する前に]。

```
system switch ethernet log setup-password
```

```
cluster1::*> system switch ethernet log setup-password
```

```
Enter the switch name: <return>
```

```
The switch name entered is not recognized.
```

```
Choose from the following list:
```

```
cs1
```

```
cs2
```

```
cluster1::*> system switch ethernet log setup-password
```

```
Enter the switch name: cs1
```

```
Would you like to specify a user other than admin for log  
collection? {y|n}: n
```

```
Enter the password: <enter switch password>
```

```
Enter the password again: <enter switch password>
```

```
cluster1::*> system switch ethernet log setup-password
```

```
Enter the switch name: cs2
```

```
Would you like to specify a user other than admin for log  
collection? {y|n}: n
```

```
Enter the password: <enter switch password>
```

```
Enter the password again: <enter switch password>
```



CL 5.11.1 の場合、ユーザー **cumulus** を作成し、次のプロンプトに **y** と応答します: ログ収集に admin 以外のユーザーを指定しますか? {y|n}: **y**

1. サポートログの収集を要求し、定期的な収集を有効にするには、次のコマンドを実行します。これにより、詳細なログと1時間ごとのデータ収集の両方のタイプのログ収集が開始されます。 Support Periodic

```
system switch ethernet log modify -device <switch-name> -log-request  
true
```

```
cluster1::*> system switch ethernet log modify -device cs1 -log
-request true
```

```
Do you want to modify the cluster switch log collection
configuration? {y|n}: [n] y
```

```
Enabling cluster switch log collection.
```

```
cluster1::*> system switch ethernet log modify -device cs2 -log
-request true
```

```
Do you want to modify the cluster switch log collection
configuration? {y|n}: [n] y
```

```
Enabling cluster switch log collection.
```

10分待ってから、ログ収集が完了したことを確認します。

```
system switch ethernet log show
```



ログ収集機能によってエラーステータスが報告された場合（の出力に表示され `system switch ethernet log show` ます）、詳細については、[を参照してください "ログ収集のトラブルシューティング"](#)。

## MetroCluster IP構成におけるイーサネットスイッチの監視を管理する

ほとんどの場合、イーサネットスイッチはONTAPによって自動的に検出され、CSHMによって監視されます。スイッチに適用されるリファレンス構成ファイル（RCF）では、特にCisco検出プロトコル（CDP）やリンク層検出プロトコル（LLDP）が有効になります。ただし、検出されなかったスイッチを手動で追加したり、使用されなくなったスイッチを削除したりしなければならない場合があります。また、メンテナンス中など、スイッチを構成内に残したまま、アクティブな監視を停止することもできます。

ONTAPで監視できるようにスイッチエントリを作成します。

このタスクについて

指定したイーサネットスイッチの監視を手動で設定してイネーブルにするには、コマンドを使用し `system switch ethernet create` ます。これは、ONTAPでスイッチが自動的に追加されない場合、または以前にスイッチを削除してから再度追加する場合に役立ちます。

```
system switch ethernet create -device DeviceName -address 1.2.3.4 -snmp
-version SNMPv2c -community-or-username cshml! -model NX3132V -type
cluster-network
```

典型的な例としては、IPアドレスが1.2.3.4、SNMPv2cクレデンシャルが\*cshml!\*に設定された[DeviceName]という名前のスイッチを追加します。ストレージスイッチを設定する場合は、の代わりにを`-type cluster-network`使用し`-type storage-network`ます。

スイッチを削除せずに監視を無効にする

特定のスイッチの監視を一時停止または停止し、今後の監視用に残しておく場合は、パラメータを削除するのではなく変更します `is-monitoring-enabled-admin`。

例：

```
system switch ethernet modify -device DeviceName -is-monitoring-enabled
-admin false
```

これにより、新しいアラートを生成したり再検出したりすることなく、スイッチの詳細と設定を保持できます。

不要になったスイッチを削除

切断されたスイッチまたは不要になったスイッチを削除する場合に使用し`system switch ethernet delete`ます。

```
system switch ethernet delete -device DeviceName
```

デフォルトでは、このコマンドが成功するのは、ONTAPがCDPまたはLLDPを介して現在スイッチを検出していない場合だけです。検出されたスイッチを削除するには、パラメータを使用し`-force`ます。

```
system switch ethernet delete -device DeviceName -force
```

を使用している場合、`-force`ONTAPがスイッチを再度検出すると、スイッチが自動的に再追加されることがあります。

### MetroCluster IP構成におけるイーサネットスイッチの監視を確認する

イーサネットスイッチヘルスマニタ（CSHM）は、検出したスイッチの監視を自動的に試みます。ただし、スイッチが正しく設定されていないと、監視が自動的に行われなことがあります。ヘルスマニタが使用中のスイッチを監視するように適切に設定されていることを確認してください。

接続されているイーサネットスイッチの監視を確認する

このタスクについて

接続されたイーサネットスイッチが監視されていることを確認するには、次のコマンドを実行します。

```
system switch ethernet show
```

列に「\* other」と表示されているか、**IS Monitored** フィールドに「**false**」と表示されている場合、**Model**、**ONTAP**はスイッチを監視できません。通常、値 other \*は、ONTAPがヘルスマニタでそのスイッチをサポートしていないことを示します。

IS Monitored フィールドに指定された理由により、フィールドは \* false \* に設定され、Reason 。



コマンド出力にスイッチがリストされていない場合は、ONTAPによってそのスイッチが検出されていない可能性があります。スイッチのケーブルが正しく接続されていることを確認します。必要に応じて、スイッチを手動で追加できます。 ["イーサネットスイッチの監視を管理します。"](#) 詳細についてはこちらをご覧ください。

ファームウェアとRCFのバージョンが最新であることを確認する

スイッチがサポートされている最新のファームウェアを実行しており、互換性があるリファレンス構成ファイル (RCF) が適用されていることを確認してください。詳細については、[を参照して](#) <https://mysupport.netapp.com/site/downloads/>["ネットアップサポートのダウンロードページ"]をご覧ください。

デフォルトでは、ヘルスマニタはコミュニティストリング \* cshm1 ! \* を含むSNMPv2cを監視に使用しますが、SNMPv3も設定できます。

デフォルトのSNMPv2cコミュニティストリングを変更する必要がある場合は、スイッチに適切なSNMPv2cコミュニティストリングが設定されていることを確認してください。

```
system switch ethernet modify -device SwitchA -snmp-version SNMPv2c  
-community-or-username newCommunity!
```



SNMPv3を使用するための設定の詳細については、[を参照してください](#) ["オプション：SNMPv3を設定する"](#)。

管理ネットワーク接続の確認

スイッチの管理ポートが管理ネットワークに接続されていることを確認します。

ONTAPでSNMPクエリとログ収集を実行するには、適切な管理ポート接続が必要です。

関連情報

- ["アラートのトラブルシューティング"](#)

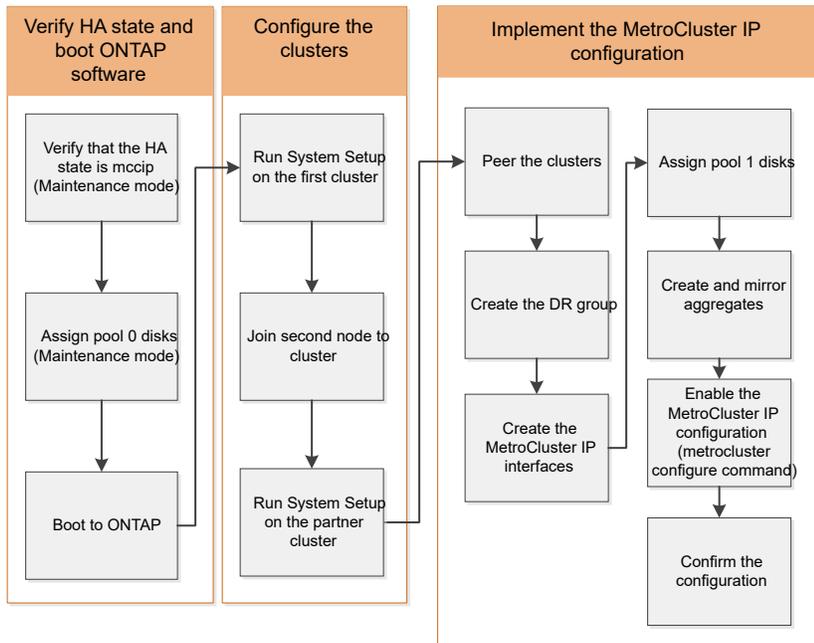
# ONTAP で MetroCluster ソフトウェアを設定します

## CLIを使用したMetroClusterソフトウェアの設定

### MetroCluster IP構成でONTAPノードとクラスタを設定する

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。

設定中にコントローラモジュールに障害が発生した場合は、を参照してください "[MetroCluster のインストール中のコントローラモジュールの障害のシナリオ](#)"。



### 8ノードのMetroCluster IP構成を構成する

8ノードのMetroCluster構成は2つのDRグループで構成されます。最初のDRグループを設定するには、このセクションのタスクを完了してください。最初のDRグループを設定したら、以下の手順に従ってください。 "[4ノードのMetroCluster IP構成を8ノード構成に拡張する](#)"。

### MetroCluster IP構成に必要な情報を収集します

設定プロセスを開始する前に、コントローラモジュールに必要な IP アドレスを収集する必要があります。

これらのリンクを使用して CSV ファイルをダウンロードし、サイト固有の情報を表に入力できます。

["MetroCluster IP セットアップワークシート site\\_A"](#)

["MetroCluster IP セットアップワークシート site\\_B"](#)

## ONTAP標準クラスタとMetroCluster構成の比較

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せん。

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 設定を有効にしません。	該当しません	必須

**MetroCluster IP**構成のコントローラとシャーシコンポーネントの**HA**構成状態を確認します。

MetroCluster IP構成では、コントローラとシャーシのコンポーネントのha-configの状態が「mccip」に設定され、適切にブートされるようにする必要があります。工場出荷状態のシステムではこの値を事前に設定しておく必要がありますが、作業を進める前に設定を確認しておく必要があります。



コントローラモジュールとシャーシのHA状態が正しくない場合は、ノードを再初期化しないとMetroClusterを設定できません。この手順を使用して設定を修正し、次のいずれかの手順を使用してシステムを初期化する必要があります。

- MetroCluster IP構成では、の手順に従います"[コントローラモジュールのシステムデフォルトの復元](#)"。
- MetroCluster FC構成では、の手順に従います"[システムをデフォルトに戻し、コントローラモジュールでHBAタイプを設定する](#)"。

作業を開始する前に

システムがメンテナンスモードであることを確認します。

手順

1. メンテナンスモードで、コントローラモジュールとシャーシの HA 状態を表示します。

「 ha-config show 」

HA の正しい状態は、 MetroCluster 構成によって異なります。

MetroCluster構成タイプ	すべてのコンポーネントのHA状態
8ノードまたは4ノードのMetroCluster FC構成	MCC
2ノード MetroCluster FC 構成	mcc-2n
8ノードまたは4ノードのMetroCluster IP構成	mccip

2. 表示されたコントローラのシステム状態が正しくない場合は、コントローラモジュールで構成に応じた正しいHA状態を設定します。

MetroCluster構成タイプ	コマンドを実行します
8ノードまたは4ノードのMetroCluster FC構成	「 ha-config modify controller mcc 」
2ノード MetroCluster FC 構成	「 ha-config modify controller mcc-2n 」 という形式で指定します
8ノードまたは4ノードのMetroCluster IP構成	「 ha-config modify controller mccip 」 を参照してください

3. 表示されたシャーシのシステム状態が正しくない場合は、シャーシの構成に応じた正しいHA状態を設定します。

MetroCluster構成タイプ	コマンドを実行します
8ノードまたは4ノードのMetroCluster FC構成	「 ha-config modify chassis mcc 」
2ノード MetroCluster FC 構成	「 ha-config modify chassis mcc-2n 」 というようになりまし
8ノードまたは4ノードのMetroCluster IP構成	「 ha-config modify chassis mccip 」 を参照してください

4. ノードを ONTAP でブートします。

「 boot\_ontap 」

5. この手順をすべて繰り返して、MetroCluster構成の各ノードのHA状態を確認します。

**MetroCluster IP**構成を設定する前に、コントローラモジュールのシステムデフォルトを復元します。

コントローラモジュールのデフォルトをリセットおよびリストアする。

1. LOADER プロンプトで、環境変数をデフォルト設定「set-defaults」に戻します
2. ノードをブートメニュー「boot\_ontap menu」からブートします

このコマンドを実行したあと、ブートメニューが表示されるまで待ちます。

3. ノードの設定をクリアします。

- ADP用に設定されたシステムを使用している場合は、オプションを選択します 9a ブートメニューから、と入力します no プロンプトが表示されたら、



このプロセスはシステムの停止を伴います。

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.
- (10) Set Onboard Key Manager recovery secrets.
- (11) Configure node for external key management.

Selection (1-11)? 9a

...

```
##### WARNING: AGGREGATES WILL BE DESTROYED #####
This is a disruptive operation that applies to all the disks
that are attached and visible to this node.
```

Before proceeding further, make sure that:

The aggregates visible from this node do not contain data that needs to be preserved.

This option (9a) has been executed or will be executed on the HA partner node (and DR/DR-AUX partner nodes if applicable), prior to reinitializing any system in the HA-pair or MetroCluster configuration.

The HA partner node (and DR/DR-AUX partner nodes if applicable) is currently waiting at the boot menu.

Do you want to abort this operation (yes/no)? no

- システムがADP用に設定されていない場合は、ブートメニュープロンプトで「wipeconfig」と入力し、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.

## MetroCluster IP構成でプール0にドライブを手動で割り当てる

工場出荷状態のシステムでない場合は、プール0のドライブを手動で割り当てる必要があります。プラットフォームモデルおよびADPを使用しているシステムかどうかに応じて、MetroCluster IP構成の各ノードのプール0にドライブを手動で割り当てる必要があります。使用する手順は、使用するONTAPのバージョンによって異なります。

プール0ドライブの手動割り当て（ONTAP 9.4以降）

工場出荷時に事前設定されておらず、自動ドライブ割り当ての要件を満たしていないシステムでは、プール0のドライブを手動で割り当てる必要があります。

このタスクについて

この手順環境構成はONTAP 9.4以降を実行しています。

手動でディスクを割り当てる必要があるかどうかを確認するには、を参照してください ["ONTAP 9.4以降での自動ドライブ割り当てとADPシステムに関する考慮事項"](#)。

この手順はメンテナンスモードで実行します。手順は、構成内の各ノードで実行する必要があります。

このセクションの例は、次の前提に基づいています。

- node\_A\_1 と node\_A\_1 の所有ドライブ：
  - site\_A-shelf\_1（ローカル）
  - site\_B-shelf\_2（リモート）
- node\_B\_1 と node\_B\_2 のドライブ：
  - site\_B-shelf\_1（ローカル）

◦ site\_A-shelf\_2 (リモート)

手順

1. ブートメニューを表示します。

「boot\_ontap menu

2. オプション9aを選択して応答します no プロンプトが表示されたら、

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.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? 9a

...

##### WARNING: AGGREGATES WILL BE DESTROYED #####
This is a disruptive operation that applies to all the disks
that are attached and visible to this node.

Before proceeding further, make sure that:

The aggregates visible from this node do not contain
data that needs to be preserved.
This option (9a) has been executed or will be executed
on the HA partner node (and DR/DR-AUX partner nodes if
applicable), prior to reinitializing any system in the
HA-pair or MetroCluster configuration.
The HA partner node (and DR/DR-AUX partner nodes if
applicable) is currently waiting at the boot menu.
Do you want to abort this operation (yes/no)? no
```

3. ノードが再起動したら、プロンプトが表示されたら Ctrl+C キーを押してブートメニューを表示し、 \* Maintenance mode boot \* オプションを選択します。

4. メンテナンスモードで、ノードのローカルアグリゲートのドライブを手動で割り当てます。

```
「ディスク assign_disk-id_-p 0 -s local-node-sysid」
```

各ノードのドライブ数が同じになるよう、ドライブは対称的に割り当てる必要があります。次の手順は、各サイトにストレージシェルフが 2 台ある構成のものです。

- a. node\_A\_1 の設定では、スロット 0~11 のドライブを site\_A-shelf\_1 のノード A1 のプール 0 に手動で割り当てます。
  - b. node\_A\_1 の設定では、スロット 12~23 のドライブを site\_A-shelf\_1 のノード A2 のプール 0 に手動で割り当てます。
  - c. node\_B\_1 の設定では、スロット 0~11 のドライブを site\_B-shelf\_1 のノード B1 のプール 0 に手動で割り当てます。
  - d. node\_B\_2 を設定する場合は、スロット 12~23 のドライブを site\_B-shelf\_1 のノード B2 のプール 0 に手動で割り当てます。
5. メンテナンスモードを終了します。

```
「halt」
```

6. ブートメニューを表示します。

```
「boot_ontap menu」
```

7. MetroCluster IP 構成の他のノードに対して上記の手順を繰り返します。
8. 両方のノードのブートメニューからオプション\* 4を選択し、システムをブートします。
9. に進みます **"ONTAP をセットアップしています"**。

#### プール 0 ドライブの手動割り当て (ONTAP 9.3)

各ノードにディスクシェルフが複数ある場合は、ONTAP の自動割り当て機能を使用してローカル (プール 0) のディスクを自動的に割り当てます。

#### このタスクについて

ノードをメンテナンスモードにした状態で、最初にシェルフの 1 つのディスクをプール 0 に割り当てる必要があります。シェルフの残りのディスクは ONTAP によって同じプールに自動的に割り当てられます。このタスクは、プール 0 に事前設定されたルートアグリゲートが含まれる、工場出荷状態のシステムでは必要ありません。

これは、ONTAP 9.3 を実行している手順環境構成です。

この手順は、工場出荷状態の MetroCluster 構成では必要ありません。工場出荷状態のノードには、プール 0 のディスクとルートアグリゲートが設定されています。

この手順は、各ノードにディスクシェルフが少なくとも 2 台あり、シェルフレベルのディスクの自動割り当てが可能な場合にのみ使用できます。シェルフレベルの自動割り当てを使用できない場合は、ローカルディスクを手動で割り当てて、各ノードにディスクのローカルプール (プール 0) を構成する必要があります。

この手順はメンテナンスモードで実行する必要があります。

このセクションの例では、次のディスクシェルフを使用します。

- node\_A\_1 の所有ディスク：
  - site\_A-shelf\_1 (ローカル)
  - site\_B-shelf\_2 (リモート)
- Node\_a\_2 の接続先：
  - site\_A-shelf\_3 (ローカル)
  - site\_B-shelf\_4 (リモート)
- node\_B\_1 の接続先：
  - site\_B-shelf\_1 (ローカル)
  - site\_A-shelf\_2 (リモート)
- node\_B\_2 の接続先：
  - site\_B-shelf\_3 (ローカル)
  - site\_A-shelf\_4 (リモート)

## 手順

1. 各ノードでルートアグリゲートに 1 つのディスクを手動で割り当てます。

「ディスク assign\_disk-id\_p 0 -s local-node-sysid」

これらのディスクを手動で割り当てると、ONTAP の自動割り当て機能によって、各シェルフの残りのディスクが割り当てられます。

- a. node\_A\_1 で、ローカルの site\_A-shelf\_1 のいずれかのディスクをプール 0 に手動で割り当てます。
  - b. node\_A\_1 で、ローカルの site\_A-shelf\_3 のいずれかのディスクをプール 0 に手動で割り当てます。
  - c. node\_B\_1 で、ローカルの site\_B-shelf\_1 のいずれかのディスクをプール 0 に手動で割り当てます。
  - d. node\_B\_2 で、ローカルの site\_B-shelf\_3 のいずれかのディスクをプール 0 に手動で割り当てます。
2. ブートメニューのオプション 4 を使用して、サイト A の各ノードをブートします。

この手順は、次のノードに進む前に各ノードで実行する必要があります。

- a. メンテナンスモードを終了します。

「halt」

- b. ブートメニューを表示します。

「boot\_ontap menu」

- c. ブートメニューからオプション 4 を選択して次に進みます。

3. ブートメニューのオプション 4 を使用して、サイト B の各ノードをブートします。

この手順は、次のノードに進む前に各ノードで実行する必要があります。

- a. メンテナンスモードを終了します。

「halt」

- b. ブートメニューを表示します。

「boot\_ontap menu」

- c. ブートメニューからオプション 4 を選択して次に進みます。

### MetroCluster IP構成でONTAPノードを設定する

各ノードをブートすると、ノードおよびクラスタの基本的な設定を実行するよう求めるプロンプトが表示されます。クラスタを設定したら、ONTAP CLI に戻ってアグリゲートを作成し、MetroCluster 構成を作成します。

作業を開始する前に

- MetroCluster 構成のケーブル接続を完了しておく必要があります。

新しいコントローラをネットブートする必要がある場合は、を参照してください ["新しいコントローラモジュールをネットブート"](#)。

このタスクについて

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。

手順

1. ローカルサイトの各ノードに電源が入っていない場合は電源を投入し、すべてのノードを完全にブートします。

システムが保守モードになっている場合は、halt コマンドを問題して保守モードを終了し、次に「boot\_ontap」コマンドを問題してシステムをブートし、クラスタセットアップを開始する必要があります。

2. 各クラスタの最初のノードで、プロンプトに従ってクラスタを設定します

- a. システムの指示に従って AutoSupport ツールを有効にします。

次のような出力が表示されます。

Welcome to the cluster setup wizard.

You can enter the following commands at any time:

"help" or "?" - if you want to have a question clarified,  
"back" - if you want to change previously answered questions, and  
"exit" or "quit" - if you want to quit the cluster setup wizard.  
Any changes you made before quitting will be saved.

You can return to cluster setup at any time by typing "cluster setup".

To accept a default or omit a question, do not enter a value.

This system will send event messages and periodic reports to NetApp Technical

Support. To disable this feature, enter  
autosupport modify -support disable  
within 24 hours.

Enabling AutoSupport can significantly speed problem determination and

resolution should a problem occur on your system.

For further information on AutoSupport, see:

<http://support.netapp.com/autosupport/>

Type yes to confirm and continue {yes}: yes

.  
.  
.

- b. プロンプトに従ってノード管理インターフェイスを設定します。

次のようなプロンプトが表示されます。

```
Enter the node management interface port [e0M]:
Enter the node management interface IP address: 172.17.8.229
Enter the node management interface netmask: 255.255.254.0
Enter the node management interface default gateway: 172.17.8.1
A node management interface on port e0M with IP address 172.17.8.229
has been created.
```

- c. プロンプトに従ってクラスタを作成します。

次のようなプロンプトが表示されます。

```
Do you want to create a new cluster or join an existing cluster?
{create, join}:
create
```

```
Do you intend for this node to be used as a single node cluster?
{yes, no} [no]:
no
```

```
Existing cluster interface configuration found:
```

```
Port MTU IP Netmask
e0a 1500 169.254.18.124 255.255.0.0
e1a 1500 169.254.184.44 255.255.0.0
```

```
Do you want to use this configuration? {yes, no} [yes]: no
```

```
System Defaults:
```

```
Private cluster network ports [e0a,e1a].
Cluster port MTU values will be set to 9000.
Cluster interface IP addresses will be automatically generated.
```

```
Do you want to use these defaults? {yes, no} [yes]: no
```

```
Enter the cluster administrator's (username "admin") password:
```

```
Retype the password:
```

```
Step 1 of 5: Create a Cluster
```

```
You can type "back", "exit", or "help" at any question.
```

```
List the private cluster network ports [e0a,e1a]:
Enter the cluster ports' MTU size [9000]:
Enter the cluster network netmask [255.255.0.0]: 255.255.254.0
Enter the cluster interface IP address for port e0a: 172.17.10.228
Enter the cluster interface IP address for port e1a: 172.17.10.229
Enter the cluster name: cluster_A
```

```
Creating cluster cluster_A
```

```
Starting cluster support services ...
```

```
Cluster cluster_A has been created.
```

- d. ライセンスを追加し、クラスタ管理 SVM をセットアップします。プロンプトに従って DNS 情報を入力します。

次のようなプロンプトが表示されます。

```
Step 2 of 5: Add Feature License Keys
You can type "back", "exit", or "help" at any question.

Enter an additional license key []:

Step 3 of 5: Set Up a Vserver for Cluster Administration
You can type "back", "exit", or "help" at any question.

Enter the cluster management interface port [e3a]:
Enter the cluster management interface IP address: 172.17.12.153
Enter the cluster management interface netmask: 255.255.252.0
Enter the cluster management interface default gateway: 172.17.12.1

A cluster management interface on port e3a with IP address
172.17.12.153 has been created. You can use this address to connect
to and manage the cluster.

Enter the DNS domain names: lab.netapp.com
Enter the name server IP addresses: 172.19.2.30
DNS lookup for the admin Vserver will use the lab.netapp.com domain.

Step 4 of 5: Configure Storage Failover (SFO)
You can type "back", "exit", or "help" at any question.

SFO will be enabled when the partner joins the cluster.

Step 5 of 5: Set Up the Node
You can type "back", "exit", or "help" at any question.

Where is the controller located []: svl
```

- e. プロンプトに従って、ストレージフェイルオーバーを有効にし、ノードをセットアップします。

次のようなプロンプトが表示されます。

```
Step 4 of 5: Configure Storage Failover (SFO)
You can type "back", "exit", or "help" at any question.

SFO will be enabled when the partner joins the cluster.

Step 5 of 5: Set Up the Node
You can type "back", "exit", or "help" at any question.

Where is the controller located []: site_A
```

- f. ノードの設定を完了します。ただし、データアグリゲートは作成しません。

ONTAPシステムマネージャを使用して、Webブラウザでクラスタ管理IPアドレス (<https://172.17.12.153>).

"[System Managerを使用したクラスタ管理 \(ONTAP 9.7以前\)](#) "

"[ONTAP システムマネージャ \(バージョン 9.7 以降\)](#) "

- g. サービスプロセッサ (SP) を設定します。

"[SP / BMC ネットワークを設定する](#)"

"[System Manager - ONTAP 9.7 以前のバージョンでサービスプロセッサを使用します](#)"

3. 次のコントローラをブートし、プロンプトに従ってクラスタに追加します。
4. ノードがハイアベイラビリティモードで設定されていることを確認します。

「storage failover show -fields mode」を選択します

そうでない場合は、各ノードで HA モードを設定し、ノードをリブートする必要があります。

「storage failover modify -mode ha -node localhost」を参照してください



HAとストレージフェイルオーバーの想定される構成状態は次のとおりです。

- HAモードが設定されていますが、ストレージフェイルオーバーが有効になっていません。
- HAテイクオーバー機能が無効になっています。
- HAインターフェイスがオフラインです。
- HAモード、ストレージフェイルオーバー、およびインターフェイスは、あとで設定します。

5. クラスタインターコネクトとして4つのポートが構成されていることを確認します。

「network port show」のように表示されます

この時点では MetroCluster IP インターフェイスは設定されておらず、コマンド出力に表示されません。

次の例は、node\_A\_1 の 2 つのクラスタポートを示しています。

```
cluster_A::*> network port show -role cluster
```

```
Node: node_A_1
```

```
Ignore
```

							Speed (Mbps)	Health
Health								
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status	
Status								
-----								
e4a	Cluster	Cluster		up	9000	auto/40000	healthy	
false								
e4e	Cluster	Cluster		up	9000	auto/40000	healthy	
false								

```
Node: node_A_2
```

```
Ignore
```

							Speed (Mbps)	Health
Health								
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status	
Status								
-----								
e4a	Cluster	Cluster		up	9000	auto/40000	healthy	
false								

```
e4e      Cluster      Cluster      up    9000  auto/40000 healthy
false

4 entries were displayed.
```

6. パートナークラスタで同じ手順を繰り返します。

次に何をするか

ONTAP のコマンドラインインターフェイスに戻り、後続のタスクを実行して MetroCluster の設定を完了します。

### MetroCluster IP構成でONTAPクラスタを構成する

クラスタをピアリングし、ルートアグリゲートをミラーリングし、ミラーリングされたデータアグリゲートを作成し、コマンドを問題して MetroCluster の処理を実装する必要があります。

このタスクについて

を実行する前に `metrocluster configure`、HAモードおよびDRミラーリングが有効になっていないため、この想定動作に関連するエラーメッセージが表示される場合があります。HAモードとDRミラーリングは、あとでコマンドを実行するときに有効にします `metrocluster configure` をクリックして構成を実装してください。

自動ドライブ割り当ての無効化（ONTAP 9.4 で手動で割り当てを行う場合）

ONTAP 9.4 では、MetroCluster IP 構成の各サイトに外付けストレージシェルフが 3 台以下しかない場合、すべてのノードで自動ドライブ割り当てを無効にし、ドライブを手動で割り当てる必要があります。

このタスクについて

このタスクは ONTAP 9.5 以降では必要ありません。

このタスクは、内蔵シェルフおよび外付けシェルフのない AFF A800 システムには該当しません。

### "ONTAP 9.4 以降での自動ドライブ割り当てと ADP システムに関する考慮事項"

手順

1. 自動ドライブ割り当てを無効にします。

```
storage disk option modify -node <node_name> -autoassign off
```

2. MetroCluster IP 構成のすべてのノードでこのコマンドを問題に設定する必要があります。

プール 0 ドライブのドライブ割り当てを確認しています

リモートドライブがノードに認識され、正しく割り当てられていることを確認する必要があります。

このタスクについて

自動割り当ては、ストレージシステムのプラットフォームモデルとドライブシェルフの配置によって異なります。

## "ONTAP 9.4 以降での自動ドライブ割り当てと ADP システムに関する考慮事項"

### 手順

1. プール 0 のドライブが自動的に割り当てられていることを確認します。

「ディスクショー」

次の例は、外付けシェルフがない AFF A800 システムの cluster\_A についての出力を示しています。

4 分の 1（8 ドライブ）が「node\_A\_1」に自動的に割り当てられ、4 分の 1 が「node\_A\_2」に自動的に割り当てられています。残りのドライブは、「node\_B\_1」と「node\_B\_2」のリモート（プール 1）のドライブになります。

```
cluster_A::*> disk show
Disk Owner Usable Size Disk Shelf Bay Container Type Container Name
-----
node_A_1:0n.12 1.75TB 0 12 SSD-NVM shared aggr0
node_A_1
node_A_1:0n.13 1.75TB 0 13 SSD-NVM shared aggr0
node_A_1
node_A_1:0n.14 1.75TB 0 14 SSD-NVM shared aggr0
node_A_1
node_A_1:0n.15 1.75TB 0 15 SSD-NVM shared aggr0
node_A_1
node_A_1:0n.16 1.75TB 0 16 SSD-NVM shared aggr0
node_A_1
node_A_1:0n.17 1.75TB 0 17 SSD-NVM shared aggr0
node_A_1
node_A_1:0n.18 1.75TB 0 18 SSD-NVM shared aggr0
node_A_1
node_A_1:0n.19 1.75TB 0 19 SSD-NVM shared -
node_A_1
node_A_2:0n.0 1.75TB 0 0 SSD-NVM shared
aggr0_node_A_2_0 node_A_2
node_A_2:0n.1 1.75TB 0 1 SSD-NVM shared
aggr0_node_A_2_0 node_A_2
node_A_2:0n.2 1.75TB 0 2 SSD-NVM shared
aggr0_node_A_2_0 node_A_2
node_A_2:0n.3 1.75TB 0 3 SSD-NVM shared
aggr0_node_A_2_0 node_A_2
node_A_2:0n.4 1.75TB 0 4 SSD-NVM shared
```

```

aggr0_node_A_2_0 node_A_2
node_A_2:0n.5      1.75TB      0      5      SSD-NVM shared
aggr0_node_A_2_0 node_A_2
node_A_2:0n.6      1.75TB      0      6      SSD-NVM shared
aggr0_node_A_2_0 node_A_2
node_A_2:0n.7      1.75TB      0      7      SSD-NVM shared      -
node_A_2
node_A_2:0n.24     -            0      24     SSD-NVM unassigned  -      -
node_A_2:0n.25     -            0      25     SSD-NVM unassigned  -      -
node_A_2:0n.26     -            0      26     SSD-NVM unassigned  -      -
node_A_2:0n.27     -            0      27     SSD-NVM unassigned  -      -
node_A_2:0n.28     -            0      28     SSD-NVM unassigned  -      -
node_A_2:0n.29     -            0      29     SSD-NVM unassigned  -      -
node_A_2:0n.30     -            0      30     SSD-NVM unassigned  -      -
node_A_2:0n.31     -            0      31     SSD-NVM unassigned  -      -
node_A_2:0n.36     -            0      36     SSD-NVM unassigned  -      -
node_A_2:0n.37     -            0      37     SSD-NVM unassigned  -      -
node_A_2:0n.38     -            0      38     SSD-NVM unassigned  -      -
node_A_2:0n.39     -            0      39     SSD-NVM unassigned  -      -
node_A_2:0n.40     -            0      40     SSD-NVM unassigned  -      -
node_A_2:0n.41     -            0      41     SSD-NVM unassigned  -      -
node_A_2:0n.42     -            0      42     SSD-NVM unassigned  -      -
node_A_2:0n.43     -            0      43     SSD-NVM unassigned  -      -
32 entries were displayed.

```

次の例は、cluster\_B についての出力を示しています。

```

cluster_B::> disk show

          Usable      Disk          Container      Container
Disk      Size      Shelf Bay Type      Type      Name
Owner
-----
-----

Info: This cluster has partitioned disks. To get a complete list of
spare disk
capacity use "storage aggregate show-spare-disks".
node_B_1:0n.12  1.75TB      0      12     SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.13  1.75TB      0      13     SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.14  1.75TB      0      14     SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.15  1.75TB      0      15     SSD-NVM shared      aggr0
node_B_1

```

```

node_B_1:0n.16  1.75TB  0  16  SSD-NVM shared  aggr0
node_B_1
node_B_1:0n.17  1.75TB  0  17  SSD-NVM shared  aggr0
node_B_1
node_B_1:0n.18  1.75TB  0  18  SSD-NVM shared  aggr0
node_B_1
node_B_1:0n.19  1.75TB  0  19  SSD-NVM shared  -
node_B_1
node_B_2:0n.0   1.75TB  0  0   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.1   1.75TB  0  1   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.2   1.75TB  0  2   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.3   1.75TB  0  3   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.4   1.75TB  0  4   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.5   1.75TB  0  5   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.6   1.75TB  0  6   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.7   1.75TB  0  7   SSD-NVM shared  -
node_B_2
node_B_2:0n.24  -        0  24  SSD-NVM unassigned - -
node_B_2:0n.25  -        0  25  SSD-NVM unassigned - -
node_B_2:0n.26  -        0  26  SSD-NVM unassigned - -
node_B_2:0n.27  -        0  27  SSD-NVM unassigned - -
node_B_2:0n.28  -        0  28  SSD-NVM unassigned - -
node_B_2:0n.29  -        0  29  SSD-NVM unassigned - -
node_B_2:0n.30  -        0  30  SSD-NVM unassigned - -
node_B_2:0n.31  -        0  31  SSD-NVM unassigned - -
node_B_2:0n.36  -        0  36  SSD-NVM unassigned - -
node_B_2:0n.37  -        0  37  SSD-NVM unassigned - -
node_B_2:0n.38  -        0  38  SSD-NVM unassigned - -
node_B_2:0n.39  -        0  39  SSD-NVM unassigned - -
node_B_2:0n.40  -        0  40  SSD-NVM unassigned - -
node_B_2:0n.41  -        0  41  SSD-NVM unassigned - -
node_B_2:0n.42  -        0  42  SSD-NVM unassigned - -
node_B_2:0n.43  -        0  43  SSD-NVM unassigned - -

```

32 entries were displayed.

cluster\_B::>

## 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"](#)

クラスタピアリング用のクラスタ間 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、「cluster01」内のネットワークポートを示しています。

```
cluster01::> network port show
```

						Speed
(Mbps)						
Node	Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper
-----						
cluster01-01						
	e0a	Cluster	Cluster	up	1500	auto/1000
	e0b	Cluster	Cluster	up	1500	auto/1000
	e0c	Default	Default	up	1500	auto/1000
	e0d	Default	Default	up	1500	auto/1000
	e0e	Default	Default	up	1500	auto/1000
	e0f	Default	Default	up	1500	auto/1000
cluster01-02						
	e0a	Cluster	Cluster	up	1500	auto/1000
	e0b	Cluster	Cluster	up	1500	auto/1000
	e0c	Default	Default	up	1500	auto/1000
	e0d	Default	Default	up	1500	auto/1000
	e0e	Default	Default	up	1500	auto/1000
	e0f	Default	Default	up	1500	auto/1000

2. クラスタ間通信専用で使用可能なポートを特定します。

```
network interface show -fields home-port、 curr -port
```

コマンド構文全体については、マニュアルページを参照してください。

次の例は、ポート e0e とポート e0f に LIF が割り当てられていないことを示しています。

```
cluster01::> network interface show -fields home-port,curr-port
```

vserver	lif	home-port	curr-port
-----			
Cluster	cluster01-01_clus1	e0a	e0a
Cluster	cluster01-01_clus2	e0b	e0b
Cluster	cluster01-02_clus1	e0a	e0a
Cluster	cluster01-02_clus2	e0b	e0b
cluster01			
	cluster_mgmt	e0c	e0c
cluster01			
	cluster01-01_mgmt1	e0c	e0c
cluster01			
	cluster01-02_mgmt1	e0c	e0c

3. 専用ポートのフェイルオーバーグループを作成します。

```
network interface failover-groups create -vserver <system_svm> -failover-group
<failover_group> -targets <physical_or_logical_ports>
```

次の例は、ポート「e0e」と「e0f」を、システム「SVMcluster01」上のフェイルオーバーグループ「intercluster01」に割り当てます。

```
cluster01::> network interface failover-groups create -vserver cluster01
-failover-group
intercluster01 -targets
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

4. フェイルオーバーグループが作成されたことを確認します。

「network interface failover-groups show」と表示されます

コマンド構文全体については、マニュアルページを参照してください。

```
cluster01::> network interface failover-groups show
                                     Failover
Vserver          Group                Targets
-----
Cluster
Cluster
cluster01        Cluster
                                     cluster01-01:e0a, cluster01-01:e0b,
                                     cluster01-02:e0a, cluster01-02:e0b
Default
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
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 9.6**以降では、次のコマンドを実行します。

```
network interface create -vserver <system_svm> -lif <lif_name> -service
-policy default-intercluster -home-node <node_name> -home-port <port_name>
-address <port_ip_address> -netmask <netmask_address> -failover-group
<failover_group>
```

**ONTAP 9.5**以前では、次のコマンドを実行します。

```
network interface create -vserver <system_svm> -lif <lif_name> -role
intercluster -home-node <node_name> -home-port <port_name> -address
<port_ip_address> -netmask <netmask_address> -failover-group
<failover_group>
```

コマンド構文全体については、マニュアルページを参照してください。

次の例は、フェイルオーバーグループ「intercluster01」にクラスタ間 LIF 「cluster01\_icl01」と「cluster01\_icl02」を作成します。

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0 -failover-group intercluster01

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0 -failover-group intercluster01
```

6. クラスタ間 LIF が作成されたことを確認します。

**ONTAP 9.6**以降では、次のコマンドを実行します。

「network interface show -service -policy default -intercluster」のように表示されます

**ONTAP 9.5**以前では、次のコマンドを実行します。

「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 9.6**以降では、次のコマンドを実行します。

「network interface show -service -policy default -intercluster-failover」のように入力します

**ONTAP 9.5**以前では、次のコマンドを実行します。

「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、「SVM0e」ポートのクラスタ間 LIF 「cluster01\_icl01」と「cluster01\_icl02」が「e0f」ポートにフェイルオーバーされることを示しています。

```

cluster01::> network interface show -service-policy default-intercluster
-failover
          Logical      Home      Failover      Failover
Vserver   Interface  Node:Port  Policy      Group
-----
-----
cluster01
          cluster01_icl01  cluster01-01:e0e  local-only
intercluster01
                                Failover Targets:  cluster01-01:e0e,
                                cluster01-01:e0f
          cluster01_icl02  cluster01-02:e0e  local-only
intercluster01
                                Failover Targets:  cluster01-02:e0e,
                                cluster01-02:e0f

```

## 関連情報

### "専用のポートを使用する場合の考慮事項"

#### 共有データポートでのクラスタ間 LIF の設定

データネットワークと共有するポートにクラスタ間 LIF を設定できます。これにより、クラスタ間ネットワークに必要なポート数を減らすことができます。

#### 手順

1. クラスタ内のポートの一覧を表示します。

「network port show」のように表示されます

コマンド構文全体については、マニュアルページを参照してください。

次の例は、「cluster01」内のネットワークポートを示しています。

```
cluster01::> network port show
```

						Speed	
(Mbps)	Node	Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper
-----							
cluster01-01							
		e0a	Cluster	Cluster	up	1500	auto/1000
		e0b	Cluster	Cluster	up	1500	auto/1000
		e0c	Default	Default	up	1500	auto/1000
		e0d	Default	Default	up	1500	auto/1000
cluster01-02							
		e0a	Cluster	Cluster	up	1500	auto/1000
		e0b	Cluster	Cluster	up	1500	auto/1000
		e0c	Default	Default	up	1500	auto/1000
		e0d	Default	Default	up	1500	auto/1000

2. システム SVM にクラスタ間 LIF を作成します。

**ONTAP 9.6**以降では、次のコマンドを実行します。

```
network interface create -vserver <system_svm> -lif <lif_name> -service  
-policy default-intercluster -home-node <node_name> -home-port <port_name>  
-address <port_ip_address> -netmask <netmask>
```

**ONTAP 9.5**以前では、次のコマンドを実行します。

```
network interface create -vserver <system_svm> -lif <lif_name> -role  
intercluster -home-node <node_name> -home-port <port_name> -address  
<port_ip_address> -netmask <netmask>
```

コマンド構文全体については、マニュアルページを参照してください。

次の例は、クラスタ間 LIF 「cluster01\_icl01」と「cluster01\_icl02」を作成します。

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

### 3. クラスタ間 LIF が作成されたことを確認します。

**ONTAP 9.6**以降では、次のコマンドを実行します。

「network interface show -service-policy default-intercluster」のように表示されます

**ONTAP 9.5**以前では、次のコマンドを実行します。

「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 9.6以降では、次のコマンドを実行します。

「network interface show – service-policy default-intercluster-failover」 と表示されます

ONTAP 9.5以前では、次のコマンドを実行します。

「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、「e0c」ポート上のクラスタ間 LIF 「cluster01\_icl01」と「cluster01\_icl02」が「e0d」ポートにフェイルオーバーされることを示しています。

```
cluster01::> network interface show -service-policy default-intercluster
-failover
          Logical          Home          Failover          Failover
Vserver  Interface         Node:Port      Policy            Group
-----
cluster01
          cluster01_icl01 cluster01-01:e0c  local-only
192.168.1.201/24
                                Failover Targets: cluster01-01:e0c,
                                                cluster01-01:e0d
          cluster01_icl02 cluster01-02:e0c  local-only
192.168.1.201/24
                                Failover Targets: cluster01-02:e0c,
                                                cluster01-02:e0d
```

## 関連情報

### "データポートを共有する場合の考慮事項"

#### クラスタピア関係を作成

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の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。

#### このタスクについて

- ピア関係にあるクラスタ内の各ノードでクラスタ間 LIF を作成しておく必要があります。
- クラスタで ONTAP 9.3 以降が実行されている必要があります。

#### 手順

1. デスティネーションクラスタで、ソースクラスタとのピア関係を作成します。

```
cluster peer create -generate-passphrase -offer-expiration <MM/DD/YYYY
HH:MM:SS|1...7days|1...168hours> -peer-addr <peer_lif_ip_addresses> -ipspace
<ipspace>
```

「-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_ip_addresses> -ip-space <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
Cluster UUID: b07036f2-7d1c-11f0-bedb-
d039ea48b059
Remote Intercluster Addresses: 192.140.112.101,
192.140.112.102
Availability of the Remote Cluster: Available
Remote Cluster Name: cluster02
Active IP Addresses: 192.140.112.101,
192.140.112.102
Cluster Serial Number: 1-80-123456
Remote Cluster Nodes: cluster02-01, cluster02-02,
Remote Cluster Health: true
Unreachable Local Nodes: -
Operation Timeout (seconds): 60
Address Family of Relationship: ipv4
Authentication Status Administrative: use-authentication
Authentication Status Operational: ok
Timeout for RPC Connect: 10
Timeout for Update Pings: 5
Last Update Time: 10/9/2025 10:15:29
IPspace for the Relationship: Default
Proposed Setting for Encryption of Inter-Cluster Communication: -
Encryption Protocol For Inter-Cluster Communication: tls-psk
Algorithm By Which the PSK Was Derived: jpake
```

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

```

#### DR グループを作成します

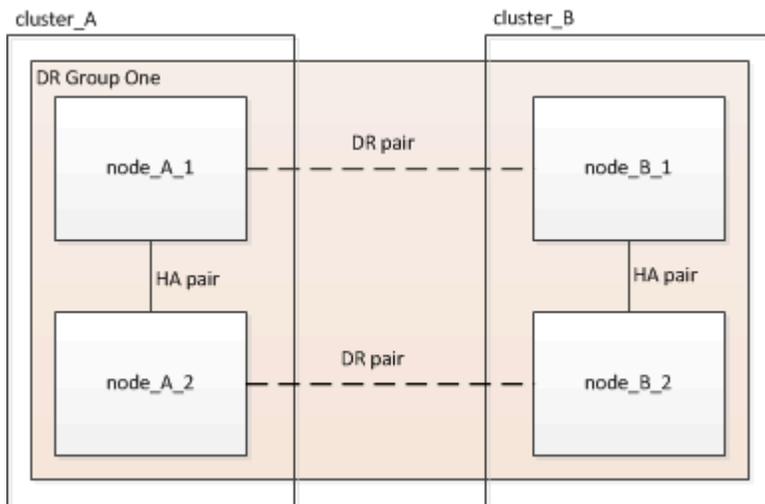
クラスタ間にディザスタリカバリ（DR）グループ関係を作成する必要があります。

このタスクについて

この手順は、MetroCluster 構成の一方のクラスタで実行します。これにより、両方のクラスタのノード間に DR 関係が作成されます。



DR グループを作成したあとに DR 関係を変更することはできません。



手順

1. 各ノードで次のコマンドを入力して、DR グループを作成する準備ができていることを確認します。

MetroCluster の構成設定はステータスを表示します

コマンドの出力に、ノードの準備が完了していることが示されます。

```
cluster_A::> metrocluster configuration-settings show-status
Cluster          Node          Configuration Settings Status
-----
cluster_A       node_A_1     ready for DR group create
                node_A_2     ready for DR group create
2 entries were displayed.
```

```
cluster_B::> metrocluster configuration-settings show-status
Cluster          Node          Configuration Settings Status
-----
cluster_B       node_B_1     ready for DR group create
                node_B_2     ready for DR group create
2 entries were displayed.
```

2. DR グループを作成します。

```
metrocluster configuration-settings dr-group create -partner-cluster
<partner_cluster_name> -local-node <local_node_name> -remote-node
<remote_node_name>
```

このコマンドは 1 回だけ実行します。パートナークラスタで繰り返す必要はありません。コマンドでは、リモートクラスタの名前、および 1 つのローカルノードとパートナークラスタの 1 つのノードの名前を指定します。

指定した 2 つのノードが DR パートナーとして設定され、他の 2 つのノード（コマンドで指定していないノード）が DR グループの 2 つ目の DR ペアとして設定されます。このコマンドの入力後にこれらの関係を変更することはできません。

次のコマンドでは、次の DR ペアが作成されます。

- node\_A\_1 と node\_B\_1
- Node\_a\_2 と Node\_B\_2

```
Cluster_A::> metrocluster configuration-settings dr-group create
-partner-cluster cluster_B -local-node node_A_1 -remote-node node_B_1
[Job 27] Job succeeded: DR Group Create is successful.
```

各ノードのストレージと不揮発性キャッシュのレプリケーションに使用する MetroCluster IP インターフェイスを設定する必要があります。その後、MetroCluster IP インターフェイスを使用して接続を確立します。これにより、ストレージレプリケーション用の iSCSI 接続が作成されます。



MetroCluster IP および接続されているスイッチポートは、MetroCluster IP インターフェイスを作成するまでオンラインになりません。

このタスクについて

- ノードごとに 2 つのインターフェイスを作成する必要があります。インターフェイスは、MetroCluster RCF ファイルで定義されている VLAN に関連付ける必要があります。
- すべての MetroCluster IP インターフェイス「A」ポートを同じ VLAN に作成し、すべての MetroCluster IP インターフェイス「B」ポートをもう一方の VLAN に作成する必要があります。を参照してください ["MetroCluster IP 構成に関する考慮事項"](#)。
- ONTAP 9.9.1 以降では、レイヤ 3 設定を使用している場合、MetroCluster IP インターフェイスを作成するときに `-gateway` パラメータも指定する必要があります。を参照してください ["レイヤ 3 ワイドエリアネットワークに関する考慮事項"](#)。

特定のプラットフォームでは、MetroCluster IP インターフェイスに VLAN が使用されます。デフォルトでは、2 つのポートでそれぞれ 10 と 20 の異なる VLAN が使用されます。

サポートされている場合は、コマンドのパラメータを使用して、100 より大きい別の（デフォルト以外の）VLAN（101 ~ 4095）を指定することもできます `-vlan-id metrocluster configuration-settings interface create`。

次のプラットフォームでは、パラメーターは\*サポートされていません\* `-vlan-id`。

- FAS8200 と AFF A300
- AFF A320
- FAS9000 および AFF A700
- AFF C800、ASA C800、AFF A800、および ASA A800

他のすべてのプラットフォームでは、パラメーターがサポートされ `-vlan-id` ます。

デフォルトおよび有効な VLAN 割り当ては、プラットフォームがパラメータをサポートしているかどうかによって異なり `-vlan-id` ます。

**vlan-vlan-id </code>をサポートするプラットフォーム<code>**

デフォルトVLAN：

- パラメータを指定しない場合、`-vlan-id` インターフェイスは「A」ポートにVLAN 10、「B」ポートにVLAN 20で作成されます。
- 指定するVLANは、RCFで選択したVLANと一致する必要があります。

有効なVLAN範囲：

- デフォルトVLAN 10および20
- VLAN 101以上（101～4095）

**vlan-vlan-id </code>をサポートしないプラットフォーム<code>**

デフォルトVLAN：

- 該当なし。このインターフェイスでは、MetroClusterインターフェイスでVLANを指定する必要はありません。スイッチポートによって、使用されるVLANが定義されます。

有効なVLAN範囲：

- RCFの生成時にすべてのVLANが明示的に除外されていない。VLANが無効な場合は、RCFから警告が表示されます。

- MetroCluster IPインターフェイスで使用される物理ポートは、プラットフォームモデルによって異なります。お使いのシステムで使用するポートについては、[を参照してください "MetroCluster IP スイッチをケーブル接続します"](#)。
- この例では、次の IP アドレスとサブネットを使用しています。

ノード	インターフェイス	IP アドレス	サブネット
node_A_1	MetroCluster IP インターフェイス 1	10.1.1.1	10.1.1/24
MetroCluster IP インターフェイス 2	10.1.2.1	10.1.2/24	Node_a_2
MetroCluster IP インターフェイス 1	10.1.1.2	10.1.1/24	MetroCluster IP インターフェイス 2
10.1.2.2	10.1.2/24	node_B_1	MetroCluster IP インターフェイス 1
10.1.1.3 の場合	10.1.1/24	MetroCluster IP インターフェイス 2	10.1.2.3

10.1.2/24	node_B_2	MetroCluster IP インターフェイス 1	10.1.1.4
10.1.1/24	MetroCluster IP インターフェイス 2	10.1.2.4	10.1.2/24

- この手順では、次の例を使用します。

AFF A700またはFAS9000システムのポート（e5aおよびe5b）。

AFF A220システムのポート。サポートされているプラットフォームでパラメータを使用する方法を示します。 -vlan-id

プラットフォームモデルに応じた正しいポートでインターフェイスを設定します。

#### 手順

1. 各ノードでディスクの自動割り当てが有効になっていることを確認します。

「 storage disk option show 」をクリックします

ディスクの自動割り当てでは、シェルフ単位でプール 0 とプール 1 のディスクが割り当てられます。

Auto Assign 列は、ディスクの自動割り当てが有効になっているかどうかを示します。

Node	BKg. FW. Upd.	Auto Copy	Auto Assign	Auto Assign Policy
node_A_1	on	on	on	default
node_A_2	on	on	on	default
2 entries were displayed.				

2. ノードに MetroCluster IP インターフェイスを作成できることを確認します。

MetroCluster の構成設定はステータスを表示します

すべてのノードの準備が完了していることを確認

Cluster	Node	Configuration Settings Status
cluster_A	node_A_1	ready for interface create
	node_A_2	ready for interface create
cluster_B	node_B_1	ready for interface create
	node_B_2	ready for interface create
4 entries were displayed.		

3. node\_A\_1 にインターフェイスを作成します。

a. 「node\_A\_1」のポート「e5a」にインターフェイスを設定します。



MetroCluster IPインターフェイスを作成するときは、同じ範囲のシステム自動生成インターフェイスIPアドレスとの競合を避けるため、169.254.17.xまたは169.254.18.xのIPアドレスを使用しないでください。

```
metrocluster configuration-settings interface create -cluster-name
<cluster_name> -home-node <node_name> -home-port e5a -address <ip_address>
-netmask <netmask>
```

次の例は、「node\_A\_1」のポート「e5a」にIPアドレスが「10.1.1.1」のインターフェイスを作成する例を示しています。

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_1 -home-port e5a -address
10.1.1.1 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.
cluster_A::>
```

MetroCluster IP インターフェイスの VLAN をサポートするプラットフォームモデルでは、デフォルトの VLAN ID を使用しない場合に `-vlan-id` パラメータを指定できます。次の例は、VLAN ID が 120 の AFF A220 システムに対するコマンドを示しています。

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_2 -home-port e0a -address
10.1.1.2 -netmask 255.255.255.0 -vlan-id 120
[Job 28] Job succeeded: Interface Create is successful.
cluster_A::>
```

b. 「node\_A\_1」のポート「e5b」にインターフェイスを設定します。

```
metrocluster configuration-settings interface create -cluster-name
<cluster_name> -home-node <node_name> -home-port e5b -address <ip_address>
-netmask <netmask>
```

次の例は、「node\_A\_1」のポート「e5b」にIPアドレスが「10.1.2.1」のインターフェイスを作成する例を示しています。

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_1 -home-port e5b -address
10.1.2.1 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.
cluster_A::>
```



これらのインターフェイスが存在することを確認するには、「MetroCluster configuration-settings interface show」コマンドを使用します。

#### 4. node\_A\_1 にインターフェイスを作成します。

- a. 「node\_A\_2」のポート「e5a」にインターフェイスを設定します。

```
metrocluster configuration-settings interface create -cluster-name  
<cluster_name> -home-node <node_name> -home-port e5a -address <ip_address>  
-netmask <netmask>
```

次の例は、「node\_A\_2」のポート「e5a」に IP アドレスが「10.1.1.2」のインターフェイスを作成する例を示しています。

```
cluster_A::> metrocluster configuration-settings interface create  
-cluster-name cluster_A -home-node node_A_2 -home-port e5a -address  
10.1.1.2 -netmask 255.255.255.0  
[Job 28] Job succeeded: Interface Create is successful.  
cluster_A::>
```

- b. 「node\_A\_2」のポート「e5b」にインターフェイスを設定します。

```
metrocluster configuration-settings interface create -cluster-name  
<cluster_name> -home-node <node_name> -home-port e5b -address <ip_address>  
-netmask <netmask>
```

次の例は、「node\_A\_2」のポート「e5b」に IP アドレスが「10.1.2.2」のインターフェイスを作成する例を示しています。

```
cluster_A::> metrocluster configuration-settings interface create  
-cluster-name cluster_A -home-node node_A_2 -home-port e5b -address  
10.1.2.2 -netmask 255.255.255.0  
[Job 28] Job succeeded: Interface Create is successful.  
cluster_A::>
```

MetroCluster IP インターフェイスの VLAN をサポートするプラットフォームモデルでは、デフォルトの VLAN ID を使用しない場合に `-vlan-id` パラメータを指定できます。次の例は、VLAN ID が 220 の AFF A220 システムに対するコマンドを示しています。

```
cluster_A::> metrocluster configuration-settings interface create  
-cluster-name cluster_A -home-node node_A_2 -home-port e0b -address  
10.1.2.2 -netmask 255.255.255.0 -vlan-id 220  
[Job 28] Job succeeded: Interface Create is successful.  
cluster_A::>
```

5. 「node\_B\_1」にインターフェイスを作成します。

a. 「node\_B\_1」のポート「e5a」にインターフェイスを設定します。

```
metrocluster configuration-settings interface create -cluster-name  
<cluster_name> -home-node <node_name> -home-port e5a -address <ip_address>  
-netmask <netmask>
```

次の例は、「node\_B\_1」のポート「e5a」にIPアドレスが「10.1.1.3」のインターフェイスを作成する例を示しています。

```
cluster_A::> metrocluster configuration-settings interface create  
-cluster-name cluster_B -home-node node_B_1 -home-port e5a -address  
10.1.1.3 -netmask 255.255.255.0  
[Job 28] Job succeeded: Interface Create is successful.cluster_B::>
```

b. 「node\_B\_1」のポート「e5b」にインターフェイスを設定します。

```
metrocluster configuration-settings interface create -cluster-name  
<cluster_name> -home-node <node_name> -home-port e5b -address <ip_address>  
-netmask <netmask>
```

次の例は、「node\_B\_1」のポート「e5b」にIPアドレスが「10.1.2.3」のインターフェイスを作成する例を示しています。

```
cluster_A::> metrocluster configuration-settings interface create  
-cluster-name cluster_B -home-node node_B_1 -home-port e5b -address  
10.1.2.3 -netmask 255.255.255.0  
[Job 28] Job succeeded: Interface Create is successful.cluster_B::>
```

6. 「node\_B\_2」にインターフェイスを作成

a. node\_B\_2 のポート e5a でインターフェイスを設定します。

```
metrocluster configuration-settings interface create -cluster-name  
<cluster_name> -home-node <node_name> -home-port e5a -address <ip_address>  
-netmask <netmask>
```

次の例は、「node\_B\_2」のポート「e5a」にIPアドレスが「10.1.1.4」のインターフェイスを作成する例を示しています。

```
cluster_B::> metrocluster configuration-settings interface create  
-cluster-name cluster_B -home-node node_B_2 -home-port e5a -address  
10.1.1.4 -netmask 255.255.255.0  
[Job 28] Job succeeded: Interface Create is successful.cluster_A::>
```

- b. 「node\_B\_2」のポート「e5b」にインターフェイスを設定します。

```
metrocluster configuration-settings interface create -cluster-name  
<cluster_name> -home-node <node_name> -home-port e5b -address <ip_address>  
-netmask <netmask>
```

次の例は、「node\_B\_2」のポート「e5b」にIPアドレスが「10.1.2.4」のインターフェイスを作成する例を示しています。

```
cluster_B::> metrocluster configuration-settings interface create  
-cluster-name cluster_B -home-node node_B_2 -home-port e5b -address  
10.1.2.4 -netmask 255.255.255.0  
[Job 28] Job succeeded: Interface Create is successful.  
cluster_A::>
```

7. インターフェイスが設定されたことを確認します。

「MetroCluster configuration-settings interface show」を参照してください

次に、各インターフェイスの設定状態が completed になっている例を示します。



## 9. 接続を確立します MetroCluster 設定 - 接続接続接続

ONTAP 9.10.1より前のバージョンを実行している場合、このコマンドの実行後にIPアドレスを変更することはできません。

次の例は、 cluster\_A が正常に接続されたことを示しています。

```
cluster_A::> metrocluster configuration-settings connection connect
[Job 53] Job succeeded: Connect is successful.
cluster_A::>
```

## 10. 接続が確立されたことを確認します。

MetroCluster の構成設定はステータスを表示します

すべてのノードの構成設定ステータスが completed になっていることを確認します。

```
Cluster          Node          Configuration Settings Status
-----
cluster_A
                node_A_1      completed
                node_A_2      completed
cluster_B
                node_B_1      completed
                node_B_2      completed
4 entries were displayed.
```

## 11. iSCSI 接続が確立されたことを確認します。

### a. advanced 権限レベルに切り替えます。

「advanced」の権限が必要です

アドバンス・モードに進むかどうかを確認するプロンプトが表示されたら 'y' で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

### b. 接続を表示します。

「storage iscsi-initiator show」のように表示されます

ONTAP 9.5 を実行しているシステムでは、クラスタごとに 8 つの MetroCluster IP イニシエータが出力に表示されます。

ONTAP 9.4 以前を実行しているシステムでは、各クラスタに MetroCluster IP イニシエータが 4 つあり、出力に表示されます。

次の例は、ONTAP 9.5 を実行しているクラスタの 8 つの MetroCluster IP イニシエータを示しています。

```

cluster_A::*> storage iscsi-initiator show
Node Type Label      Target Portal      Target Name
Admin/Op
-----
-----

cluster_A-01
  dr_auxiliary
    mccip-aux-a-initiator
      10.227.16.113:65200      prod506.com.company:abab44
up/up
    mccip-aux-a-initiator2
      10.227.16.113:65200      prod507.com.company:abab44
up/up
    mccip-aux-b-initiator
      10.227.95.166:65200      prod506.com.company:abab44
up/up
    mccip-aux-b-initiator2
      10.227.95.166:65200      prod507.com.company:abab44
up/up
  dr_partner
    mccip-pri-a-initiator
      10.227.16.112:65200      prod506.com.company:cdcd88
up/up
    mccip-pri-a-initiator2
      10.227.16.112:65200      prod507.com.company:cdcd88
up/up
    mccip-pri-b-initiator
      10.227.95.165:65200      prod506.com.company:cdcd88
up/up
    mccip-pri-b-initiator2
      10.227.95.165:65200      prod507.com.company:cdcd88
up/up
cluster_A-02
  dr_auxiliary
    mccip-aux-a-initiator
      10.227.16.112:65200      prod506.com.company:cdcd88
up/up
    mccip-aux-a-initiator2
      10.227.16.112:65200      prod507.com.company:cdcd88
up/up
    mccip-aux-b-initiator
      10.227.95.165:65200      prod506.com.company:cdcd88
up/up
    mccip-aux-b-initiator2

```

```

10.227.95.165:65200      prod507.com.company:cdcd88
up/up
  dr_partner
    mccip-pri-a-initiator
      10.227.16.113:65200      prod506.com.company:abab44
up/up
    mccip-pri-a-initiator2
      10.227.16.113:65200      prod507.com.company:abab44
up/up
    mccip-pri-b-initiator
      10.227.95.166:65200      prod506.com.company:abab44
up/up
    mccip-pri-b-initiator2
      10.227.95.166:65200      prod507.com.company:abab44
up/up
16 entries were displayed.

```

a. admin 権限レベルに戻ります。

「特権管理者」

12. ノードで MetroCluster 構成の最終的な実装準備が完了していることを確認します。

MetroCluster node show

```

cluster_A::> metrocluster node show
DR
Group Cluster Node          Configuration  DR
State          Mirroring Mode
-----
-   cluster_A
      node_A_1      ready to configure -   -
      node_A_2      ready to configure -   -
2 entries were displayed.
cluster_A::>

```

```

cluster_B::> metrocluster node show
DR
Group Cluster Node          Configuration  DR
State          Mirroring Mode
-----
-   cluster_B
      node_B_1      ready to configure -   -
      node_B_2      ready to configure -   -
2 entries were displayed.
cluster_B::>

```

プール 1 ドライブの割り当てを検証または手動で実行する

ストレージ構成に応じて、MetroCluster IP 構成の各ノードのプール 1 のドライブ割り当てを確認するか、ドライブを手動で割り当てる必要があります。使用する手順は、使用する ONTAP のバージョンによって異なります。

構成タイプ	手順
自動ドライブ割り当ての要件を満たしているシステム、または ONTAP 9.3 を実行している工場出荷時の状態のシステム	プール 1 ディスクのディスク割り当てを確認しています
3 台のシェルフ、またはそれ以上の 4 の倍数でない奇数個（7 台など）のシェルフを含む、ONTAP 9.5 を実行している構成。	プール 1 のドライブの手動割り当て（ONTAP 9.4 以降）
各サイトにストレージシェルフが 4 台ない構成で ONTAP 9.4 を実行している	プール 1 のドライブの手動割り当て（ONTAP 9.4 以降）
工場出荷時の状態ではないシステムで、工場出荷時に割り当てられたドライブが搭載された ONTAP 9.3 システムを実行しています。	プール 1 のディスクの手動割り当て（ONTAP 9.3）

プール 1 ディスクのディスク割り当てを確認しています

リモートディスクがノードに認識され、正しく割り当てられていることを確認する必要があります。

作業を開始する前に

MetroCluster IP インタフェースと接続を MetroCluster configuration-settings connection connect コマンドで作成した後、ディスクの自動割り当てが完了するまで 10 分以上待つ必要があります

コマンドの出力には、ディスク名が： node-name : 0m.i1.0L1 の形式で表示されます

#### "ONTAP 9.4 以降での自動ドライブ割り当てと ADP システムに関する考慮事項"

手順

1. プール 1 のディスクが自動で割り当てられていることを確認します。

「ディスクショー」

次の出力は、外付けシェルフがない AFF A800 システムについての出力を示しています。

ドライブの自動割り当てにより、4 分の 1（8 ドライブ）が「node\_A\_1」に、4 分の 1 が「node\_A\_2」に割り当てられています。残りのドライブは、「node\_B\_1」と「node\_B\_2」のリモート（プール 1）のディスクになります。

```
cluster_B::> disk show -host-adapter 0m -owner node_B_2
          Usable      Disk              Container      Container
Disk      Size      Shelf Bay Type      Type          Name
```

Owner

```
-----
-----
node_B_2:0m.i0.2L4 894.0GB 0 29 SSD-NVM shared -
node_B_2
node_B_2:0m.i0.2L10 894.0GB 0 25 SSD-NVM shared -
node_B_2
node_B_2:0m.i0.3L3 894.0GB 0 28 SSD-NVM shared -
node_B_2
node_B_2:0m.i0.3L9 894.0GB 0 24 SSD-NVM shared -
node_B_2
node_B_2:0m.i0.3L11 894.0GB 0 26 SSD-NVM shared -
node_B_2
node_B_2:0m.i0.3L12 894.0GB 0 27 SSD-NVM shared -
node_B_2
node_B_2:0m.i0.3L15 894.0GB 0 30 SSD-NVM shared -
node_B_2
node_B_2:0m.i0.3L16 894.0GB 0 31 SSD-NVM shared -
node_B_2
8 entries were displayed.
```

```
cluster_B::> disk show -host-adapter 0m -owner node_B_1
```

Disk Owner	Usable Size	Disk Shelf	Bay	Type	Container Type	Container Name
node_B_1:0m.i2.3L19 node_B_1	1.75TB	0	42	SSD-NVM	shared	-
node_B_1:0m.i2.3L20 node_B_1	1.75TB	0	43	SSD-NVM	spare	Pool1
node_B_1:0m.i2.3L23 node_B_1	1.75TB	0	40	SSD-NVM	shared	-
node_B_1:0m.i2.3L24 node_B_1	1.75TB	0	41	SSD-NVM	spare	Pool1
node_B_1:0m.i2.3L29 node_B_1	1.75TB	0	36	SSD-NVM	shared	-
node_B_1:0m.i2.3L30 node_B_1	1.75TB	0	37	SSD-NVM	shared	-
node_B_1:0m.i2.3L31 node_B_1	1.75TB	0	38	SSD-NVM	shared	-
node_B_1:0m.i2.3L32 node_B_1	1.75TB	0	39	SSD-NVM	shared	-

8 entries were displayed.

```
cluster_B::> disk show
```

Disk Owner	Usable Size	Disk Shelf	Bay	Type	Container Type	Container Name
node_B_1:0m.i1.0L6	1.75TB	0	1	SSD-NVM	shared	-
node_A_2						
node_B_1:0m.i1.0L8	1.75TB	0	3	SSD-NVM	shared	-
node_A_2						
node_B_1:0m.i1.0L17	1.75TB	0	18	SSD-NVM	shared	-
node_A_1						
node_B_1:0m.i1.0L22	1.75TB	0	17	SSD-NVM	shared	- node_A_1
node_B_1:0m.i1.0L25	1.75TB	0	12	SSD-NVM	shared	- node_A_1
node_B_1:0m.i1.2L2	1.75TB	0	5	SSD-NVM	shared	- node_A_2
node_B_1:0m.i1.2L7	1.75TB	0	2	SSD-NVM	shared	- node_A_2
node_B_1:0m.i1.2L14	1.75TB	0	7	SSD-NVM	shared	- node_A_2
node_B_1:0m.i1.2L21	1.75TB	0	16	SSD-NVM	shared	- node_A_1
node_B_1:0m.i1.2L27	1.75TB	0	14	SSD-NVM	shared	- node_A_1
node_B_1:0m.i1.2L28	1.75TB	0	15	SSD-NVM	shared	- node_A_1
node_B_1:0m.i2.1L1	1.75TB	0	4	SSD-NVM	shared	- node_A_2
node_B_1:0m.i2.1L5	1.75TB	0	0	SSD-NVM	shared	- node_A_2
node_B_1:0m.i2.1L13	1.75TB	0	6	SSD-NVM	shared	- node_A_2
node_B_1:0m.i2.1L18	1.75TB	0	19	SSD-NVM	shared	- node_A_1
node_B_1:0m.i2.1L26	1.75TB	0	13	SSD-NVM	shared	- node_A_1
node_B_1:0m.i2.3L19	1.75TB	0	42	SSD-NVM	shared	- node_B_1
node_B_1:0m.i2.3L20	1.75TB	0	43	SSD-NVM	shared	- node_B_1
node_B_1:0m.i2.3L23	1.75TB	0	40	SSD-NVM	shared	- node_B_1
node_B_1:0m.i2.3L24	1.75TB	0	41	SSD-NVM	shared	- node_B_1
node_B_1:0m.i2.3L29	1.75TB	0	36	SSD-NVM	shared	- node_B_1
node_B_1:0m.i2.3L30	1.75TB	0	37	SSD-NVM	shared	- node_B_1
node_B_1:0m.i2.3L31	1.75TB	0	38	SSD-NVM	shared	- node_B_1
node_B_1:0m.i2.3L32	1.75TB	0	39	SSD-NVM	shared	- node_B_1
node_B_1:0n.12	1.75TB	0	12	SSD-NVM	shared	aggr0 node_B_1
node_B_1:0n.13	1.75TB	0	13	SSD-NVM	shared	aggr0 node_B_1
node_B_1:0n.14	1.75TB	0	14	SSD-NVM	shared	aggr0 node_B_1
node_B_1:0n.15	1.75TB	0	15	SSD-NVM	shared	aggr0 node_B_1
node_B_1:0n.16	1.75TB	0	16	SSD-NVM	shared	aggr0 node_B_1
node_B_1:0n.17	1.75TB	0	17	SSD-NVM	shared	aggr0 node_B_1
node_B_1:0n.18	1.75TB	0	18	SSD-NVM	shared	aggr0 node_B_1
node_B_1:0n.19	1.75TB	0	19	SSD-NVM	shared	- node_B_1
node_B_1:0n.24	894.0GB	0	24	SSD-NVM	shared	- node_A_2
node_B_1:0n.25	894.0GB	0	25	SSD-NVM	shared	- node_A_2
node_B_1:0n.26	894.0GB	0	26	SSD-NVM	shared	- node_A_2
node_B_1:0n.27	894.0GB	0	27	SSD-NVM	shared	- node_A_2
node_B_1:0n.28	894.0GB	0	28	SSD-NVM	shared	- node_A_2
node_B_1:0n.29	894.0GB	0	29	SSD-NVM	shared	- node_A_2

```

node_B_1:0n.30      894.0GB 0 30 SSD-NVM shared - node_A_2
node_B_1:0n.31      894.0GB 0 31 SSD-NVM shared - node_A_2
node_B_1:0n.36      1.75TB 0 36 SSD-NVM shared - node_A_1
node_B_1:0n.37      1.75TB 0 37 SSD-NVM shared - node_A_1
node_B_1:0n.38      1.75TB 0 38 SSD-NVM shared - node_A_1
node_B_1:0n.39      1.75TB 0 39 SSD-NVM shared - node_A_1
node_B_1:0n.40      1.75TB 0 40 SSD-NVM shared - node_A_1
node_B_1:0n.41      1.75TB 0 41 SSD-NVM shared - node_A_1
node_B_1:0n.42      1.75TB 0 42 SSD-NVM shared - node_A_1
node_B_1:0n.43      1.75TB 0 43 SSD-NVM shared - node_A_1
node_B_2:0m.i0.2L4  894.0GB 0 29 SSD-NVM shared - node_B_2
node_B_2:0m.i0.2L10 894.0GB 0 25 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L3  894.0GB 0 28 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L9  894.0GB 0 24 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L11 894.0GB 0 26 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L12 894.0GB 0 27 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L15 894.0GB 0 30 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L16 894.0GB 0 31 SSD-NVM shared - node_B_2
node_B_2:0n.0       1.75TB 0 0 SSD-NVM shared aggr0_rha12_b1_cm_02_0
node_B_2
node_B_2:0n.1 1.75TB 0 1 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.2 1.75TB 0 2 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.3 1.75TB 0 3 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.4 1.75TB 0 4 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.5 1.75TB 0 5 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.6 1.75TB 0 6 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.7 1.75TB 0 7 SSD-NVM shared - node_B_2
64 entries were displayed.

```

```
cluster_B::>
```

```
cluster_A::> disk show
```

```
Usable Disk Container Container
```

```
Disk Size Shelf Bay Type Type Name Owner
```

```

-----
-----
node_A_1:0m.i1.0L2 1.75TB 0 5 SSD-NVM shared - node_B_2
node_A_1:0m.i1.0L8 1.75TB 0 3 SSD-NVM shared - node_B_2
node_A_1:0m.i1.0L18 1.75TB 0 19 SSD-NVM shared - node_B_1
node_A_1:0m.i1.0L25 1.75TB 0 12 SSD-NVM shared - node_B_1
node_A_1:0m.i1.0L27 1.75TB 0 14 SSD-NVM shared - node_B_1
node_A_1:0m.i1.2L1 1.75TB 0 4 SSD-NVM shared - node_B_2
node_A_1:0m.i1.2L6 1.75TB 0 1 SSD-NVM shared - node_B_2
node_A_1:0m.i1.2L7 1.75TB 0 2 SSD-NVM shared - node_B_2
node_A_1:0m.i1.2L14 1.75TB 0 7 SSD-NVM shared - node_B_2

```

```
node_A_1:0m.i1.2L17 1.75TB 0 18 SSD-NVM shared - node_B_1
node_A_1:0m.i1.2L22 1.75TB 0 17 SSD-NVM shared - node_B_1
node_A_1:0m.i2.1L5 1.75TB 0 0 SSD-NVM shared - node_B_2
node_A_1:0m.i2.1L13 1.75TB 0 6 SSD-NVM shared - node_B_2
node_A_1:0m.i2.1L21 1.75TB 0 16 SSD-NVM shared - node_B_1
node_A_1:0m.i2.1L26 1.75TB 0 13 SSD-NVM shared - node_B_1
node_A_1:0m.i2.1L28 1.75TB 0 15 SSD-NVM shared - node_B_1
node_A_1:0m.i2.3L19 1.75TB 0 42 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L20 1.75TB 0 43 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L23 1.75TB 0 40 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L24 1.75TB 0 41 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L29 1.75TB 0 36 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L30 1.75TB 0 37 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L31 1.75TB 0 38 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L32 1.75TB 0 39 SSD-NVM shared - node_A_1
node_A_1:0n.12 1.75TB 0 12 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.13 1.75TB 0 13 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.14 1.75TB 0 14 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.15 1.75TB 0 15 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.16 1.75TB 0 16 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.17 1.75TB 0 17 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.18 1.75TB 0 18 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.19 1.75TB 0 19 SSD-NVM shared - node_A_1
node_A_1:0n.24 894.0GB 0 24 SSD-NVM shared - node_B_2
node_A_1:0n.25 894.0GB 0 25 SSD-NVM shared - node_B_2
node_A_1:0n.26 894.0GB 0 26 SSD-NVM shared - node_B_2
node_A_1:0n.27 894.0GB 0 27 SSD-NVM shared - node_B_2
node_A_1:0n.28 894.0GB 0 28 SSD-NVM shared - node_B_2
node_A_1:0n.29 894.0GB 0 29 SSD-NVM shared - node_B_2
node_A_1:0n.30 894.0GB 0 30 SSD-NVM shared - node_B_2
node_A_1:0n.31 894.0GB 0 31 SSD-NVM shared - node_B_2
node_A_1:0n.36 1.75TB 0 36 SSD-NVM shared - node_B_1
node_A_1:0n.37 1.75TB 0 37 SSD-NVM shared - node_B_1
node_A_1:0n.38 1.75TB 0 38 SSD-NVM shared - node_B_1
node_A_1:0n.39 1.75TB 0 39 SSD-NVM shared - node_B_1
node_A_1:0n.40 1.75TB 0 40 SSD-NVM shared - node_B_1
node_A_1:0n.41 1.75TB 0 41 SSD-NVM shared - node_B_1
node_A_1:0n.42 1.75TB 0 42 SSD-NVM shared - node_B_1
node_A_1:0n.43 1.75TB 0 43 SSD-NVM shared - node_B_1
node_A_2:0m.i2.3L3 894.0GB 0 28 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L4 894.0GB 0 29 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L9 894.0GB 0 24 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L10 894.0GB 0 25 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L11 894.0GB 0 26 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L12 894.0GB 0 27 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L15 894.0GB 0 30 SSD-NVM shared - node_A_2
```

```

node_A_2:0m.i2.3L16 894.0GB 0 31 SSD-NVM shared - node_A_2
node_A_2:0n.0 1.75TB 0 0 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.1 1.75TB 0 1 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.2 1.75TB 0 2 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.3 1.75TB 0 3 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.4 1.75TB 0 4 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.5 1.75TB 0 5 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.6 1.75TB 0 6 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.7 1.75TB 0 7 SSD-NVM shared - node_A_2
64 entries were displayed.

cluster_A::>

```

### プール 1 のドライブの手動割り当て（ONTAP 9.4 以降）

工場出荷時に事前設定されておらず、自動ドライブ割り当ての要件を満たしていないシステムでは、リモートのプール 1 ドライブを手動で割り当てる必要があります。

このタスクについて

この手順環境構成は ONTAP 9.4 以降を実行しています。

手動でディスクを割り当てる必要があるかどうかの詳細については、を参照してください ["ONTAP 9.4 以降での自動ドライブ割り当てと ADP システムに関する考慮事項"](#)。

外付けシェルフがサイトごとに 2 台しかない場合は、次の例に示すように、各サイトのプール 1 で同じシェルフのドライブを共有する必要があります。

- node\_A\_1 に site\_B-shelf\_2（リモート）のベイ 0~11 のドライブを割り当て
- node\_A\_2 に site\_B-shelf\_2（リモート）のベイ 12~23 のドライブを割り当て

手順

1. MetroCluster IP 構成の各ノードで、リモートドライブをプール 1 に割り当てます。
  - a. 未割り当てドライブのリストを表示します。

「 Disk show -host-adapter 0m -container-type unassigned 」

```

cluster_A::> disk show -host-adapter 0m -container-type unassigned
              Usable          Disk   Container   Container
Disk          Size Shelf Bay Type      Type        Name
Owner
-----
-----
6.23.0         -    23   0 SSD      unassigned  -          -
6.23.1         -    23   1 SSD      unassigned  -          -
.
.
.
node_A_2:0m.i1.2L51  -    21  14 SSD      unassigned  -          -
node_A_2:0m.i1.2L64  -    21  10 SSD      unassigned  -          -
.
.
.
48 entries were displayed.

cluster_A::>

```

- b. リモートドライブ（0m）の所有権を最初のノード（例：node\_A\_1）のプール1に割り当てます。

```
disk assign -disk <disk-id> -pool 1 -owner <owner_node_name>
```

disk-idのリモートシェルフのドライブを特定する必要があります owner\_node\_name。

- c. ドライブがプール1に割り当てられたことを確認します。

「Disk show -host-adapter 0m -container-type unassigned」



リモートドライブへのアクセスに使用される iSCSI 接続は、デバイス「0m」と表示されます。

次の出力では、シェルフ23のドライブが割り当てられ、未割り当てドライブのリストに表示されていません。

```

cluster_A::> disk show -host-adapter 0m -container-type unassigned
                Usable          Disk      Container  Container
Disk           Size Shelf Bay Type      Type      Name
Owner
-----
node_A_2:0m.i1.2L51      -    21  14 SSD      unassigned -
node_A_2:0m.i1.2L64      -    21  10 SSD      unassigned -
.
.
.
node_A_2:0m.i2.1L90      -    21  19 SSD      unassigned -
24 entries were displayed.

cluster_A::>

```

- a. 同じ手順を繰り返して、サイト A の 2 つ目のノード（「Node\_a\_2」など）にプール 1 のドライブを割り当てます。
- b. サイト B で同じ手順を繰り返します

### プール 1 のディスクの自動割り当て（ONTAP 9.3）

各ノードにディスクシェルフが複数ある場合は、ONTAP の自動割り当て機能を使用してリモート（プール 1）のディスクを自動的に割り当てます。

作業を開始する前に

最初に、シェルフのディスクを 1 つプール 1 に割り当てる必要があります。シェルフの残りのディスクは ONTAP によって同じプールに自動的に割り当てられます。

このタスクについて

これは、ONTAP 9.3 を実行している手順環境構成です。

この手順は、各ノードにディスクシェルフが少なくとも 2 台あり、それによってシェルフレベルでディスクの自動割り当てが可能の場合にのみ使用できます。

シェルフレベルの自動割り当てを使用できない場合は、リモートディスクを手動で割り当てて、各ノードにディスクのリモートプール（プール 1）を構成する必要があります。

ONTAP の自動ディスク割り当て機能は、シェルフ単位でディスクを割り当てます。例：

- site\_B-shelf\_2 のすべてのディスクが node\_A\_1 のプール 1 に自動的に割り当てられます
- site\_B-shelf\_2 のすべてのディスクが node\_B\_2 のプール 1 に自動的に割り当てられます
- site\_A-shelf\_2 のすべてのディスクが node\_B\_1 のプール 1 に自動的に割り当てられます
- site\_A-shelf\_2 のすべてのディスクが node\_B\_2 のプール 1 に自動的に割り当てられます

各シェルフでディスクを 1 つ指定して、自動割り当てを「開始」する必要があります。

## 手順

1. MetroCluster IP 構成の各ノードで、リモートディスクを 1 つプール 1 に割り当てます。

a. 未割り当てディスクのリストを表示します。

「 Disk show -host-adapter 0m -container-type unassigned 」

```
cluster_A::> disk show -host-adapter 0m -container-type unassigned
          Usable          Disk      Container      Container
Disk      Size Shelf Bay Type      Type          Name
Owner
-----
-----
6.23.0          -    23    0 SSD      unassigned    -            -
6.23.1          -    23    1 SSD      unassigned    -            -
.
.
.
node_A_2:0m.i1.2L51      -    21   14 SSD      unassigned    -            -
node_A_2:0m.i1.2L64      -    21   10 SSD      unassigned    -            -
.
.
.
48 entries were displayed.

cluster_A::>
```

b. リモートディスク（0m）を選択し、ディスクの所有権を最初のノード（「node\_A\_1」など）のプール 1 に割り当てます。

```
disk assign -disk <disk_id> -pool 1 -owner <owner_node_name>
```

には disk-id、のリモートシェルフのディスクを指定する必要があります owner\_node\_name。

ONTAP ディスクの自動割り当て機能により、指定したディスクを含むリモートシェルフのすべてのディスクが割り当てられます。

c. ディスクの自動割り当てが開始されるまで少なくとも 60 秒待ってから、シェルフのリモートディスクがプール 1 に自動的に割り当てられたことを確認します。

「 Disk show -host-adapter 0m -container-type unassigned 」



リモートディスクへのアクセスに使用される iSCSI 接続は、デバイス「0m」と表示されます。

次の出力は、シェルフ 23 のディスクが割り当てられ、表示されていないことを示しています。

```

cluster_A::> disk show -host-adapter 0m -container-type unassigned
                Usable          Disk      Container      Container
Disk            Size Shelf Bay Type      Type          Name
Owner
-----
node_A_2:0m.i1.2L51      -      21  14 SSD      unassigned  -      -
node_A_2:0m.i1.2L64      -      21  10 SSD      unassigned  -      -
node_A_2:0m.i1.2L72      -      21  23 SSD      unassigned  -      -
node_A_2:0m.i1.2L74      -      21   1 SSD      unassigned  -      -
node_A_2:0m.i1.2L83      -      21  22 SSD      unassigned  -      -
node_A_2:0m.i1.2L90      -      21   7 SSD      unassigned  -      -
node_A_2:0m.i1.3L52      -      21   6 SSD      unassigned  -      -
node_A_2:0m.i1.3L59      -      21  13 SSD      unassigned  -      -
node_A_2:0m.i1.3L66      -      21  17 SSD      unassigned  -      -
node_A_2:0m.i1.3L73      -      21  12 SSD      unassigned  -      -
node_A_2:0m.i1.3L80      -      21   5 SSD      unassigned  -      -
node_A_2:0m.i1.3L81      -      21   2 SSD      unassigned  -      -
node_A_2:0m.i1.3L82      -      21  16 SSD      unassigned  -      -
node_A_2:0m.i1.3L91      -      21   3 SSD      unassigned  -      -
node_A_2:0m.i2.0L49      -      21  15 SSD      unassigned  -      -
node_A_2:0m.i2.0L50      -      21   4 SSD      unassigned  -      -
node_A_2:0m.i2.1L57      -      21  18 SSD      unassigned  -      -
node_A_2:0m.i2.1L58      -      21  11 SSD      unassigned  -      -
node_A_2:0m.i2.1L59      -      21  21 SSD      unassigned  -      -
node_A_2:0m.i2.1L65      -      21  20 SSD      unassigned  -      -
node_A_2:0m.i2.1L72      -      21   9 SSD      unassigned  -      -
node_A_2:0m.i2.1L80      -      21   0 SSD      unassigned  -      -
node_A_2:0m.i2.1L88      -      21   8 SSD      unassigned  -      -
node_A_2:0m.i2.1L90      -      21  19 SSD      unassigned  -      -
24 entries were displayed.

cluster_A::>

```

- a. 同じ手順を繰り返して、サイト A の 2 つ目のノード（「Node\_a\_2」など）にプール 1 のディスクを割り当てます。
- b. サイト B で同じ手順を繰り返します

#### ONTAP 9.4 での自動ドライブ割り当ての有効化

このタスクについて

ONTAP 9.4 で手順は、自動ドライブ割り当てを前述の手順に従って無効にした場合、すべてのノードで再度有効にする必要があります。

["ONTAP 9.4 以降での自動ドライブ割り当てと ADP システムに関する考慮事項"](#)

## 手順

1. 自動ドライブ割り当てを有効にします。

```
storage disk option modify -node <node_name> -autoassign on
```

このコマンドは、MetroCluster IP 構成のすべてのノードで問題設定する必要があります。

## ルートアグリゲートをミラーリング

データ保護を提供するには、ルートアグリゲートをミラーする必要があります。

### このタスクについて

デフォルトでは、ルートアグリゲートは RAID-DP タイプのアグリゲートとして作成されます。ルートアグリゲートのタイプは RAID-DP から RAID4 に変更することができます。次のコマンドは、ルートアグリゲートを RAID4 タイプのアグリゲートに変更します。

```
storage aggregate modify -aggregate <aggr_name> -raidtype raid4
```



ADP 以外のシステムでは、ミラーリングの実行前後に、アグリゲートの RAID タイプをデフォルトの RAID-DP から RAID4 に変更できます。

## 手順

1. ルートアグリゲートをミラーします。

```
storage aggregate mirror <aggr_name>
```

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"

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。

### このタスクについて

- 新しいアグリゲートで使用するドライブを把握しておく必要があります。
- 複数のドライブタイプを含むシステム（異機種混在ストレージ）の場合は、正しいドライブタイプが選択されるようにする方法を確認しておく必要があります。
- ドライブは特定のノードによって所有されます。アグリゲートを作成する場合、アグリゲート内のすべてのドライブは同じノードによって所有される必要があります。そのノードが、作成するアグリゲートのホ

ームノードになります。

ADP を使用するシステムではパーティションを使用してアグリゲートが作成され、各ドライブがパーティション P1、P2、P3 に分割されます。

- 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 サイト全体で一意である必要があります。つまり、サイト A とサイト B に同じ名前を持つ 2 つの異なるデータ アグリゲートを持つことはできません。

#### 手順

1. 使用可能なスペアのリストを表示します。

```
storage disk show -spare -owner <node_name>
```

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。

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>
```

## 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

このタスクについて

- 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。

これは「storage aggregate show」コマンドで確認できます。



ミラーされた単一のデータアグリゲートを使用する場合は、を参照してください [手順 1](#). 手順については、を参照し

- コントローラおよびシャーシの ha-config の状態が「mccip」である必要があります。

MetroCluster 構成を有効にするには '任意のノードで MetroCluster configure コマンドを 1 回実行します問題サイトごとまたはノードごとにコマンドを問題で実行する必要はありません。また、問題するノードまたはサイトはどれでもかまいません。

MetroCluster configure コマンドを実行すると '2 つのクラスタそれぞれのシステム ID が最も小さい 2 つのノードが 'DR (災害復旧) パートナーとして自動的にペア設定されます4 ノード MetroCluster 構成の場合は、DR パートナーのペアは 2 組になります。2 つ目の DR ペアは、システム ID が大きい 2 つのノードで作成されます。



コマンド MetroCluster configure'を実行する前に'Onboard Key Manager (OKM ; オンボードキーマネージャ) または外部キー管理を構成しないでください

手順

1. 次の形式で MetroCluster を構成します。

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>

ミラーされた 1 つのデータアグリゲート

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。

「 advanced 」の権限が必要です

advanced モードで続行するかどうかを尋ねられたら、「 y 」と入力して応答する必要があります。 advanced モードのプロンプト ( \* > ) が表示されます。

b. MetroCluster に -allow-with-one-aggregate true パラメータを設定します。

```
metrocluster configure -allow-with-one-aggregate true <node_name>
```

c. admin 権限レベルに戻ります。

「特権管理者」



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、 4 ノード MetroCluster 構成でのネットワークポートの用途を示しています。

```

cluster_A::> network port show

```

Node	Port	IPspace	Broadcast Domain	Link	MTU	Speed (Mbps) Admin/Oper
-----						
controller_A_1						
	e0a	Cluster	Cluster	up	9000	auto/1000
	e0b	Cluster	Cluster	up	9000	auto/1000
	e0c	Default	Default	up	1500	auto/1000
	e0d	Default	Default	up	1500	auto/1000
	e0e	Default	Default	up	1500	auto/1000
	e0f	Default	Default	up	1500	auto/1000
	e0g	Default	Default	up	1500	auto/1000
controller_A_2						
	e0a	Cluster	Cluster	up	9000	auto/1000
	e0b	Cluster	Cluster	up	9000	auto/1000
	e0c	Default	Default	up	1500	auto/1000
	e0d	Default	Default	up	1500	auto/1000
	e0e	Default	Default	up	1500	auto/1000
	e0f	Default	Default	up	1500	auto/1000
	e0g	Default	Default	up	1500	auto/1000

14 entries were displayed.

3. MetroCluster 構成の両方のサイトから MetroCluster 構成を確認します。

a. サイト A から構成を確認します。

「 MetroCluster show 」

```

cluster_A::> metrocluster show

```

Configuration: IP fabric

Cluster	Entry Name	State
-----		
Local: cluster_A	Configuration state	configured
	Mode	normal
Remote: cluster_B	Configuration state	configured
	Mode	normal

b. サイト B から構成を確認します。

「 MetroCluster show 」

```
cluster_B::> metrocluster show
```

```
Configuration: IP fabric
```

Cluster	Entry Name	State
-----	-----	-----
Local: cluster_B	Configuration state	configured
	Mode	normal
Remote: cluster_A	Configuration state	configured
	Mode	normal

4. 不揮発性メモリミラーリングの問題を回避するには、4つのノードのそれぞれをリブートします。

```
node reboot -node <node_name> -inhibit-takeover true
```

5. 構成を再度確認するには、両方のクラスタ上で MetroCluster show コマンドを実行します。

## 8 ノード構成での2つ目のDRグループの設定

同じ手順を繰り返して、2つ目のDRグループのノードを設定します。

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。

このタスクについて

- 新しいアグリゲートで使用されるドライブを把握していることを確認します。
- 複数のドライブタイプを含むシステム（異機種混在ストレージ）の場合は、正しいドライブタイプが選択されていることを確認する方法を理解しておく必要があります。



MetroCluster IP 構成では、スイッチオーバー後にミラーされていないリモートアグリゲートにアクセスできません



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。
- `_Disks and aggregates management_` アグリゲートのミラーリングの詳細については、を参照してください。

手順

1. ミラーされていないアグリゲートの導入を

MetroCluster modify -enable -ミラー されていない -aggr-deployment true

2. ディスクの自動割り当てが無効になったことを確認します。

「ディスクオプション表示」

3. ミラーされていないアグリゲートを格納するディスクシェルフを設置してケーブル接続します。

使用するプラットフォームとディスクシェルフに対応した設置とセットアップのドキュメントに記載されている手順を使用できます。

#### "ONTAPハードウェアシステムのドキュメント"

4. 新しいシェルフのすべてのディスクを適切なノードに手動で割り当てます。

```
disk assign -disk <disk_id> -owner <owner_node_name>
```

5. 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。特定のノードにアグリゲートが作成された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。

また、ミラーされていないシェルフのドライブだけをアグリゲートに追加する必要があります。

次のオプションを指定できます。

- アグリゲートのホームノード（通常運用時にアグリゲートを所有するノード）
- アグリゲートに追加するドライブのリスト
- 追加するドライブ数
- アグリゲートに使用するチェックサム形式
- 使用するドライブのタイプ
- 使用するドライブのサイズ
- 使用するドライブの速度
- アグリゲート上の RAID グループの RAID タイプ
- RAID グループに含めることができるドライブの最大数
- RPM の異なるドライブが許可されるかどうか

これらのオプションの詳細については、 storage aggregate create のマニュアルページを参照してください。

次のコマンドでは、10本のディスクを含むミラーされていないアグリゲートが作成さ

```
controller_A_1::> storage aggregate create aggr1_controller_A_1
-diskcount 10 -node controller_A_1
[Job 15] Job is queued: Create aggr1_controller_A_1.
[Job 15] The job is starting.
[Job 15] Job succeeded: DONE
```

6. 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>
```

7. ミラーされていないアグリゲートの導入を

```
MetroCluster modify -enable -ミラー されていない -aggr-deployment false
```

8. ディスク自動割り当てが有効になっていることを確認します。

「ディスクオプション表示」

## 関連情報

["ディスクおよびアグリゲートの管理"](#)

**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。

このタスクについて

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。

## 手順

1. 構成を確認します。

「MetroCluster check run」のようになります

このコマンドはバックグラウンドジョブとして実行され、すぐに完了しない場合があります。

```
cluster_A::> metrocluster check run
The operation has been started and is running in the background. Wait
for
it to complete and run "metrocluster check show" to view the results. To
check the status of the running metrocluster check operation, use the
command,
"metrocluster operation history show -job-id 2245"
```

```
cluster_A::> metrocluster check show
```

Component	Result
nodes	ok
lifs	ok
config-replication	ok
aggregates	ok
clusters	ok
connections	ok
volumes	ok

7 entries were displayed.

## 2. 最新の MetroCluster check run コマンドから、より詳細な結果を表示します。

MetroCluster check aggregate show

MetroCluster check cluster show

MetroCluster check config-replication show

MetroCluster check lif show

MetroCluster check node show



「 MetroCluster check show 」 コマンドは、最新の 「 MetroCluster check run 」 コマンドの結果を表示します。 MetroCluster check show コマンドを使用する前に ' 必ず MetroCluster check run コマンドを実行して ' 表示されている情報が最新であることを確認してください

次に、正常な 4 ノード MetroCluster 構成の MetroCluster check aggregate show コマンドの出力例を示します。

```
cluster_A::> metrocluster check aggregate show
```

Node	Aggregate	Check
Result		

```

-----
controller_A_1      controller_A_1_aggr0
ok
ok
ok
controller_A_1_aggr1
ok
ok
ok
controller_A_1_aggr2
ok
ok
ok

controller_A_2      controller_A_2_aggr0
ok
ok
ok
controller_A_2_aggr1
ok
ok
ok
controller_A_2_aggr2
ok
ok
ok

mirroring-status
disk-pool-allocation
ownership-state

```

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。

```
cluster_A::> metrocluster check cluster show

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"](#)

ONTAP 設定を完了しています

MetroCluster 構成の設定、有効化、確認が完了したら、必要に応じて SVM、ネットワークインターフェイス、およびその他の ONTAP 機能を追加してクラスタの設定を完了します。

## MetroCluster IP 構成でのエンドツーエンドの暗号化の設定

ONTAP 9.15.1 以降では、サポートされているシステムでエンドツーエンドの暗号化を設定して、MetroCluster IP 構成内のサイト間の NVlog やストレージ レプリケーション データなどのバックエンド トラフィックを暗号化できます。

このタスクについて

- このタスクを実行するには、クラスタ管理者である必要があります。
- エンドツーエンドの暗号化を設定する前に、次の手順を実行する必要があります。 ["外部キー管理を設定"](#)。

- MetroCluster IP構成でエンドツーエンドの暗号化を設定するために必要な、サポートされているシステムおよび最小ONTAPリリースを確認します。

最小ONTAPリリース	サポートされるシステム
ONTAP 9.17.1	<ul style="list-style-type: none"> <li>• AFF A800、AFF C800</li> <li>• AFF A20、AFF A30、AFF C30、AFF A50、AFF C60</li> <li>• AFF A70、AFF A90、AFF A1K、AFF C80</li> <li>• FAS50、FAS70、FAS90</li> </ul>
ONTAP 9.15.1	<ul style="list-style-type: none"> <li>• AFF A400</li> <li>• AFF C400用</li> <li>• FAS8300</li> <li>• FAS8700 の場合</li> </ul>

エンドツーエンドの暗号化を実現

エンドツーエンドの暗号化を有効にするには、次の手順を実行します。

手順

1. MetroCluster 構成の健全性を確認

- a. MetroCluster コンポーネントが正常であることを確認します。

```
metrocluster check run
```

```
cluster_A::*> metrocluster check run
```

この処理はバックグラウンドで実行されます。

- b. のあとに入力します metrocluster check run 処理が完了しました。run :

```
metrocluster check show
```

約 5 分後に、次の結果が表示されます。

```
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.

- a. 実行中の MetroCluster チェック処理のステータスを確認します。

```
metrocluster operation history show -job-id <id>
```

- b. ヘルスアラートがないことを確認します。

```
system health alert show
```

2. 両方のクラスタで外部キー管理が設定されていることを確認します。

```
security key-manager external show-status
```

3. DRグループごとにエンドツーエンドの暗号化を有効にします。

```
metrocluster modify -is-encryption-enabled true -dr-group-id  
<dr_group_id>
```

◦ 例 \*

```
cluster_A:::*> metrocluster modify -is-encryption-enabled true -dr-group  
-id 1  
Warning: Enabling encryption for a DR Group will secure NVLog and  
Storage  
        replication data sent between MetroCluster nodes and have an  
impact on  
        performance. Do you want to continue? {y|n}: y  
[Job 244] Job succeeded: Modify is successful.
```

+ 構成内のDRグループごとにこの手順を繰り返します。

#### 4. エンドツーエンドの暗号化が有効になっていることを確認します。

```
metrocluster node show -fields is-encryption-enabled
```

◦ 例 \*

```
cluster_A::*> metrocluster node show -fields is-encryption-enabled

dr-group-id cluster      node      configuration-state is-encryption-
enabled
-----
1           cluster_A   node_A_1  configured         true
1           cluster_A   node_A_2  configured         true
1           cluster_B   node_B_1  configured         true
1           cluster_B   node_B_2  configured         true
4 entries were displayed.
```

エンドツーエンドの暗号化を無効にする

エンドツーエンドの暗号化を無効にするには、次の手順を実行します。

手順

##### 1. MetroCluster 構成の健全性を確認

a. MetroCluster コンポーネントが正常であることを確認します。

```
metrocluster check run
```

```
cluster_A::*> metrocluster check run
```

この処理はバックグラウンドで実行されます。

b. のあとに入力します metrocluster check run 処理が完了しました。run :

```
metrocluster check show
```

約 5 分後に、次の結果が表示されます。

```
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.

- a. 実行中の MetroCluster チェック処理のステータスを確認します。

```
metrocluster operation history show -job-id <id>
```

- b. ヘルスアラートがないことを確認します。

```
system health alert show
```

2. 両方のクラスタで外部キー管理が設定されていることを確認します。

```
security key-manager external show-status
```

3. 各DRグループでエンドツーエンドの暗号化を無効にします。

```
metrocluster modify -is-encryption-enabled false -dr-group-id  
<dr_group_id>
```

◦ 例 \*

```
cluster_A:::*> metrocluster modify -is-encryption-enabled false -dr-group  
-id 1  
[Job 244] Job succeeded: Modify is successful.
```

+ 構成内のDRグループごとにこの手順を繰り返します。

4. エンドツーエンドの暗号化が無効になっていることを確認します。

```
metrocluster node show -fields is-encryption-enabled
```

◦ 例 \*

```
cluster_A::*> metrocluster node show -fields is-encryption-enabled

dr-group-id cluster      node      configuration-state is-encryption-
enabled
-----
1           cluster_A    node_A_1  configured         false
1           cluster_A    node_A_2  configured         false
1           cluster_B    node_B_1  configured         false
1           cluster_B    node_B_2  configured         false
4 entries were displayed.
```

## MetroCluster IP構成用にMetroCluster TiebreakerまたはONTAP Mediatorを設定する

MetroCluster Tiebreaker ソフトウェアまたは ONTAP 9.7 以降の ONTAP メディエーターは、第 3 のサイトにダウンロードしてインストールできます。

作業を開始する前に

MetroCluster 構成の両方のクラスタにネットワークで接続された Linux ホストが必要です。具体的な要件については、MetroCluster Tiebreaker または ONTAP メディエーターのドキュメントを参照してください。

既存の Tiebreaker または ONTAP Mediator インスタンスに接続する場合は、Tiebreaker または Mediator のユーザー名、パスワード、および IP アドレスが必要です。

ONTAP メディエーターの新しいインスタンスをインストールする必要がある場合は、指示に従ってソフトウェアをインストールおよび設定します。

["計画外の自動スイッチオーバー用に ONTAP Mediator を構成する"](#)

Tiebreaker ソフトウェアの新しいインスタンスをインストールする必要がある場合は、に従います ["ソフトウェアのインストールと設定の手順"](#)。

このタスクについて

MetroCluster Tiebreaker ソフトウェアと ONTAP メディエーターの両方を同じ MetroCluster 構成で使用することはできません。

["ONTAP メディエーターまたは MetroCluster Tiebreaker を使用する場合の考慮事項"](#)

ステップ

1. ONTAP Mediator または Tiebreaker ソフトウェアを構成します。
  - ONTAP Mediator の既存のインスタンスを使用している場合は、ONTAP Mediator を ONTAP に追加します。

MetroCluster の構成設定メディアーターの追加メディアーターのアドレス IP-addressof mediator-host`

- Tiebreaker ソフトウェアを使用している場合は、を参照してください "[Tiebreaker のドキュメント](#)"。

## MetroCluster IP 構成のクラスタ構成ファイルをバックアップする

ローカルクラスタ内のデフォルトの場所に加えて、クラスタ構成バックアップファイルをアップロードするリモート URL（HTTP または FTP）を指定することで、クラスタ構成バックアップファイルの保護を強化できます。

### ステップ

1. 構成バックアップファイルのリモートデスティネーションの URL を設定します。

「システム構成のバックアップ設定は 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。

## System Managerを使用したMetroClusterソフトウェアの設定

### ONTAP System Managerを使用してMetroCluster IPサイトをセットアップする

ONTAP 9.8以降では、System Managerを使用してMetroCluster IPサイトをセットアップできます。

MetroClusterサイトは2つのクラスタで構成されます。通常、クラスタは地理的に異なる場所に配置されま

す。

作業を開始する前に

- システムに付属のに従って、システムの設置とケーブル接続が完了している必要があります "[セットアップガイド](#)"。
- クラスタ内通信用に、各クラスタの各ノードにクラスタネットワークインターフェイスが設定されている必要があります。

ノード管理IPアドレスを割り当てる

### Windowsシステム

Windowsコンピュータをコントローラと同じサブネットに接続する必要があります。これにより、システムにノード管理IPアドレスが自動的に割り当てられます。

手順

1. Windowsシステムで\*[ネットワーク]\*ドライブを開き、ノードを検出します。
2. ノードをダブルクリックしてクラスタセットアップウィザードを起動します。

### その他のシステム

クラスタのいずれかのノードのノード管理IPアドレスを設定する必要があります。そのノード管理IPアドレスを使用してクラスタ セットアップ ウィザードを起動できます。

ノード管理IPアドレスの割り当てについては、を参照してください"[第1ノードでのクラスタの作成](#)".

#### クラスタの初期化と設定

クラスタを初期化するには、クラスタの管理パスワードを設定し、クラスタ管理ネットワークとノード管理ネットワークを設定します。また、ホスト名を解決するためのドメインネームサーバ（DNS）や時刻を同期するためのNTPサーバなどのサービスを設定することもできます。

#### 手順

1. Webブラウザで、設定したノード管理IPアドレスを入力します。 "<a href="https://node-management-IP" class="bare">https://node-management-IP</a>

クラスタの残りのノードはSystem Managerで自動的に検出されます。

2. Initialize Storage System\*（ストレージシステムの初期化）ウィンドウで、次の手順を実行します。
  - a. クラスタ管理ネットワークの設定データを入力します。
  - b. すべてのノードのノード管理IPアドレスを入力します。
  - c. DNSの詳細を指定します。
  - d. [\* その他\*（\* Other\*）]セクションで、[タイムサービス（NTP）を使用（Use time service（NTP）\*]というラベルの付いたチェックボックスを選択してタイムサーバを追加します。

Submit\*をクリックすると、クラスタが作成および構成されるまで待機します。その後、検証プロセスが実行されます。

#### 次の手順

両方のクラスタのセットアップ、初期化、および設定が完了したら、手順を実行します"[MetroCluster IPピアリングをセットアップする](#)".

新しいクラスタでのONTAPの設定に関するビデオ



## ONTAP System ManagerでMetroCluster IPピアリングを設定する

ONTAP 9.8以降では、MetroCluster IPの設定処理をSystem Managerで管理できます。2つのクラスタをセットアップしたら、クラスタ間のピアリングをセットアップします。

作業を開始する前に

2つのクラスタをセットアップする。手順を参照してください"[MetroCluster IPサイトのセットアップ](#)"。

このプロセスの一部の手順は、各クラスタの地理的なサイトに配置された異なるシステム管理者によって実行されます。このプロセスを説明するために、クラスタを「サイトAクラスタ」および「サイトBクラスタ」と呼びます。

サイトAからピアリングプロセスを実行

このプロセスは、サイトAのシステム管理者が実行します。

手順

1. サイトAのクラスタにログインします。
2. System Manager で、左側のナビゲーション列から「\* Dashboard \*」を選択してクラスタの概要を表示します。

ダッシュボードには、このクラスタ（サイトA）の詳細が表示されます。「\* MetroCluster \*」セクションの左側には、サイトAのクラスタが表示されています。

3. [Attach Partner Cluster] をクリックします。
4. サイトAのクラスタのノードとサイトBのクラスタのノードとの通信に使用するネットワークインターフェイスの詳細を入力します。

5. [保存して続行] をクリックします。
6. ウィンドウで、[パズフレーズがありません]\*を選択します。これにより、パズフレーズを生成できます。
7. 生成されたパズフレーズをコピーし、サイトBのシステム管理者と共有します。
8. [閉じる (Close) ] を選択します。

サイトBからピアリングプロセスを実行

このプロセスは、サイトBのシステム管理者が実行します。

手順

1. サイトBのクラスタにログインします。
2. System Manager で、 \* Dashboard \* を選択してクラスタの概要を表示します。  
  
ダッシュボードには、このクラスタ（サイトB）の詳細が表示されます。MetroClusterセクションでは、左側にサイトBのクラスタが表示されています。
3. [Attach Partner Cluster] をクリックしてピアリングプロセスを開始します。
4. サイトBのクラスタのノードとサイトAのクラスタのノードとの通信に使用するネットワークインターフェイスの詳細を入力します。
5. [保存して続行] をクリックします。
6. ウィンドウで、[パズフレーズを使用]\*を選択します。これにより、サイトAのシステム管理者から受け取ったパズフレーズを入力できます。
7. ピア \* を選択してピアリングプロセスを完了します。

次の手順

ピアリングプロセスが正常に完了したら、クラスタを設定します。を参照して "[MetroCluster IPサイトの設定](#)"

**ONTAP System Manager**を使用して**MetroCluster IP**サイトを構成する

ONTAP 9.8以降では、MetroCluster IPの設定処理をSystem Managerで管理できます。この作業には、2つのクラスタのセットアップ、クラスタピアリングの実行、およびクラスタの設定が含まれます。

作業を開始する前に

次の手順を実行します。

- "[MetroCluster IPサイトのセットアップ](#)"
- "[MetroCluster IPピアリングをセットアップする](#)"

クラスタ間の接続を設定

手順

1. いずれかのサイトで System Manager にログインし、 \* Dashboard \* を選択します。

「 \* MetroCluster \* 」セクションの図は、 MetroCluster サイト用にセットアップしてピアリングした 2 つのクラスタを示しています。作業中のクラスタ（ローカルクラスタ）が左側に表示されます。

2. MetroCluster の設定 \* をクリックします。このウィンドウで、次の手順を実行します。
  - a. MetroCluster構成の各クラスタのノードが表示されています。ドロップダウンリストを使用して、リモートクラスタのノードとディザスタリカバリパートナーとなるローカルクラスタ内のノードを選択します。
  - b. ONTAP Mediator を設定する場合は、チェックボックスをクリックします。を参照して ["ONTAPメディアーターの設定"](#)
  - c. 両方のクラスタに暗号化を有効にするライセンスがある場合は、\* Encryption \* セクションが表示されます。  
  
暗号化を有効にするには、パスフレーズを入力します。
  - d. MetroClusterを共有レイヤ3ネットワークで設定する場合は、このチェックボックスをオンにします。



ノードに接続するHAパートナーノードとネットワークスイッチの構成が一致している必要があります。

3. 保存 \* をクリックして、MetroCluster サイトを設定します。

ダッシュボード \* の \* MetroCluster \* セクションでは、2つのクラスタ間のリンクにチェックマークが表示され、正常な接続を示しています。

## 計画外の自動スイッチオーバー用に ONTAP Mediator を構成する

### MetroCluster IP構成のONTAP Mediatorインストール要件

ご使用の環境が特定の要件を満たしている必要があります

1つのディザスタリカバリグループ（DRグループ）に次の要件が適用されます。の詳細を確認してください ["DRグループ"](#)。

- Linux バージョンを更新する予定がある場合は、最新バージョンの ONTAP Mediator をインストールする前に更新してください。
- ONTAP Mediator と MetroCluster Tiebreaker ソフトウェアの両方を同じ MetroCluster 構成で使用しないでください。
- ONTAP Mediator は、MetroCluster サイトとは別の場所にある Linux ホストにインストールする必要があります。

ONTAP メディエーターと各サイトの間の接続には、2つの異なる障害ドメインが必要です。

- ONTAP 9.7 以降では、自動計画外スイッチオーバーがサポートされます。
- ONTAP 9.18.1 およびONTAP Mediator 1.11 以降では、1つのONTAP Mediator インスタンスで最大 10 個のMetroCluster構成を同時に管理できます。以前のリリースでは、ONTAP Mediator は最大 5 つのMetroCluster構成を同時にサポートできました。
- ONTAP 9.18.1 以降では、MetroCluster IP 構成のONTAP Mediator 1.11 以降で IPv6 がサポートされません。

## MetroCluster構成でONTAP Mediatorを使用するためのネットワーク要件

MetroCluster 構成に ONTAP Mediator をインストールするには、構成がいくつかのネットワーク要件を満たしていることを確認する必要があります。

- レイテンシ

最大レイテンシは75ms (RTT) 未満

ジッターは5ミリ秒以下である必要があります。

- MTU

MTU サイズは 1400 以上にする必要があります。

- パケット損失

Internet Control Message Protocol (ICMP) とTCPトラフィックの両方で、パケット損失は0.01%未満でなければなりません。

- 帯域幅

ONTAP Mediator と 1 つの DR グループ間のリンクには、少なくとも 20 Mbps の帯域幅が必要です。

- 独立した接続性

各サイトとONTAP メディエーターは個別に接続する必要があります。一方のサイトで障害が発生しても、影響を受けない他の2つのサイト間のIP接続は中断しないでください。

## MetroCluster構成におけるONTAP Mediatorのホスト要件

構成が複数のホスト要件を満たしていることを確認する必要があります。

- ONTAP メディエーターは、2つのONTAP クラスタから物理的に分離された外部サイトにインストールする必要があります。
- ONTAP メディエーターでは、ホストオペレーティングシステムの最小要件であるCPUおよびメモリ (RAM) は必要ありません。
- ホストオペレーティングシステムの最小要件に加えて、使用可能なディスクスペースが少なくとも30GB 必要です。
  - 各DRグループには、最大200MBのディスクスペースが必要です。

## ONTAP メディエーターのファイアウォール要件

ONTAP メディエーターは、複数のポートを使用して特定のサービスと通信します。

サードパーティのファイアウォールを使用している場合は、次の手順を実行します。

- HTTPS アクセスが有効になっている必要があります。
- ポート 31784 および 3260 でアクセスを許可するように設定されている必要があります。

Red Hat または CentOS のデフォルトのファイアウォールを使用している場合は、メディアエーターのインストール時に自動的に設定されます。

次の表に、ファイアウォールで許可する必要があるポートを示します。



- iSCSIポートは、MetroCluster IP構成でのみ必要です。
- 22/TCPポートは通常の動作には必要ありませんが、メンテナンスのために一時的に有効にし、メンテナンスセッションの終了後に無効にすることができます。

ポート / サービス	ソース	方向	宛先	目的
22 / TCP	管理ホスト	インバウンド	ONTAPメディアエーター	SSH / ONTAPメディアエーターの管理
31784/TCP	クラスタ管理およびノード管理LIF	インバウンド	ONTAPメディアエーター Web サーバ	REST API (HTTPS)
3260 TCP	ノード管理LIF	インバウンド	ONTAPメディアエーターの iSCSI ターゲット	メールボックス用の iSCSI データ接続

## MetroCluster構成でONTAP Mediatorをアップグレードするためのガイドライン

ONTAP Mediator をアップグレードする場合は、Linux バージョンの要件を満たし、アップグレードのガイドラインに従う必要があります。

- ONTAP Mediator は、直前のバージョンから現在のバージョンにアップグレードできます。
- MetroCluster 9.7 以降を実行する ONTAP IP 構成では、すべてのメディアエーターのバージョンがサポートされます。

### "ONTAPメディアエーターをインストールまたはアップグレードする"

#### アップグレード後

メディアエーターとオペレーティングシステム問題のアップグレードが完了したら、「storage iscsi-initiator show」コマンドを実行して、メディアエーター接続が稼働していることを確認する必要があります。

## MetroCluster IP構成用のONTAPメディアエーターを設定する

MetroCluster IP 構成で ONTAP Mediator を使用するには、ONTAPノードでONTAP Mediator を構成する必要があります。

#### 作業を開始する前に

- ONTAP Mediator は、両方の MetroCluster サイトからアクセスできるネットワークの場所に正常にインストールされている必要があります。

### "ONTAPメディアエーターをインストールまたはアップグレードする"

- ONTAP Mediator を実行しているホストの IP アドレスが必要です。
- ONTAP Mediator のユーザー名とパスワードが必要です。
- MetroCluster IP 構成のすべてのノードがオンラインになっている必要があります。



ONTAP 9.12.1以降では、MetroCluster IP設定でMetroCluster 自動強制スイッチオーバー機能をイネーブルにできます。この機能は、メディエーターアシスト計画外スイッチオーバーの拡張機能です。この機能を有効にする前に、"[MetroCluster 自動強制スイッチオーバーを使用する場合のリスクと制限事項](#)"。

#### このタスクについて

- このタスクでは、自動計画外スイッチオーバーをデフォルトで有効にします。
- このタスクは、MetroCluster IP 構成の任意のノードの ONTAP インターフェイスで実行できます。
- ONTAP 9.18.1 およびONTAP Mediator 1.11 以降では、1 つのONTAP Mediator インスタンスで最大 10 個のMetroCluster構成を同時に管理できます。以前のリリースでは、ONTAP Mediator は最大 5 つのMetroCluster構成を同時にサポートできました。

#### 手順

1. ONTAPにONTAP Mediator を追加します。手順は、IPv4 アドレスを使用するか、IPv6 アドレスを使用するかによって異なります。



- IPv6 を使用するには、ONTAP 9.18.1 以降およびONTAP Mediator 1.11 以降を実行している必要があります。
- クラスタで IPv6 を有効にすると、後で無効にすることはできません。

### IPv4を使用する

- a. 次のコマンドを実行して、ONTAPメディエーターを追加します。

```
metrocluster configuration-settings mediator add -mediator-address  
<mediator_host_ip_address>
```



Mediator 管理者ユーザー アカウントのユーザー名とパスワードの入力を求められます。

### IPv6を使用する

- a. 両方のクラスターで次のコマンドを実行します。

```
network options ipv6 modify -enabled true
```

- b. 4つのノードすべてで、IPv6 アドレスを使用してノード管理 IP アドレスを設定します。
- c. ONTAPメディエーターを追加します。

```
metrocluster configuration-settings mediator add -mediator-address  
<mediator_host_ipv6_ip_address>
```



Mediator 管理者ユーザー アカウントのユーザー名とパスワードの入力を求められます。

2. 自動スイッチオーバー機能が有効になっていることを確認します。

「MetroCluster show」

3. メディエーターが実行されたことを確認します。

- a. メディエーターの仮想ディスクを表示します。

「storage disk show -container-type mediator」のように表示されます

```

cluster_A::> storage disk show -container-type mediator
                Usable          Disk      Container
Container
Disk           Size Shelf Bay Type      Type      Name
Owner
-----
NET-1.5        -      -   - VMDISK  mediator  -
node_A_2
NET-1.6        -      -   - VMDISK  mediator  -
node_B_1
NET-1.7        -      -   - VMDISK  mediator  -
node_B_2
NET-1.8        -      -   - VMDISK  mediator  -
node_A_1

```

b. 権限モードを advanced に設定します。

「高度」

```
cluster_A::> set advanced
```

c. mediator というラベルのイニシエータを表示します。

「storage iscsi-initiator show -label mediator」という名前のストレージがあります

```

cluster_A::*> storage iscsi-initiator show -label mediator
(storage iscsi-initiator show)
+
Status
Node Type Label      Target Portal      Target Name
Admin/Op
-----
node_A_1
  mailbox
      mediator 1.1.1.1      iqn.2012-
05.local:mailbox.target.6616cd3f-9ef1-11e9-aada-
00a098ccf5d8:a05e1ffb-9ef1-11e9-8f68- 00a098cbca9e:1 up/up
node_A_2
  mailbox
      mediator 1.1.1.1      iqn.2012-
05.local:mailbox.target.6616cd3f-9ef1-11e9-aada-
00a098ccf5d8:a05e1ffb-9ef1-11e9-8f68-00a098cbca9e:1 up/up

```

- d. Automatic Unplanned Switchover (AUSO ; 自動計画外スイッチオーバー) 障害ドメインの状態を確認します。

「 MetroCluster show 」



次の例は、環境 ONTAP 9.13.1以降の出力を示しています。ONTAP 9.12.1以前では、AUSO障害ドメインの状態は `auso-on-cluster-disaster`。

```

cluster_A:::> metrocluster show
Cluster                               Entry Name                               State
-----
Local: cluster_A                       Configuration state configured
Mode                                    normal
AUSO Failure Domain auso-on-dr-group-disaster
Remote: cluster_B                      Configuration state configured
Mode                                    normal
AUSO Failure Domain auso-on-dr-group-disaster

```

4. 必要に応じて、MetroClusterの自動強制スイッチオーバーを設定します。

次のコマンドはadvanced権限レベルでのみ使用できます。



このコマンドを使用する前に、"[MetroCluster 自動強制スイッチオーバーを使用する場合のリスクと制限事項](#)"。

```
metrocluster modify -allow-auto-forced-switchover true
```

```
cluster_A::*> metrocluster modify -allow-auto-forced-switchover true
```

## MetroCluster IP構成からONTAPメディアエーターを削除する

MetroCluster IP 構成から ONTAP Mediator の構成を解除できます。

作業を開始する前に

両方の MetroCluster サイトからアクセスできるネットワークの場所に ONTAP Mediator を正常にインストールして構成しておく必要があります。

手順

1. 次のコマンドを使用して、ONTAP Mediator の構成を解除します。

MetroCluster 構成設定のメディアエーターが削除されました

ONTAPメディアエーターの管理者ユーザアカウントのユーザ名とパスワードの入力を求められます。



ONTAPメディアエーターがダウンしている場合は、`metrocluster configuration-settings mediator remove`コマンドを実行すると、引き続き ONTAP Mediator 管理者ユーザー アカウントのユーザー名とパスワードの入力が求められ、MetroCluster 構成から ONTAP Mediator が削除されます。

- a. 次のコマンドを使用して、破損ディスクがないかどうかを確認します。

「disk show -broken」

- 例 \*

```
There are no entries matching your query.
```

2. 両方のクラスタで次のコマンドを実行して、ONTAP Mediator が MetroCluster 構成から削除されていることを確認します。

- a. `metrocluster configuration-settings mediator show`

- 例 \*

```
This table is currently empty.
```

- b. 「storage iscsi-initiator show -label mediator」 という名前のストレージがあります

- 例 \*

```
There are no entries matching your query.
```

## MetroCluster IP構成を別のONTAPメディアーターインスタンスに接続する

MetroCluster ノードを別の ONTAP メディアーターインスタンスに接続する場合は、ONTAP ソフトウェアでメディアーター接続の設定を解除して設定し直す必要があります。

作業を開始する前に

新しい ONTAP メディアーターインスタンスのユーザ名、パスワード、および IP アドレスが必要です。

このタスクについて

これらのコマンドは、MetroCluster 構成の任意のノードから実行できます。

手順

1. MetroCluster 構成から現在の ONTAP メディアーターを削除します。

MetroCluster 構成設定のメディアーターが削除されました

2. MetroCluster 構成への新しい ONTAP メディアーター接続を確立します。

MetroCluster の構成設定メディアーターの追加 mediator-address\_ip-address-bmediator-host\_`

## ONTAPメディアーターがMetroCluster IP構成で計画外の自動スイッチオーバーをサポートする仕組み

ONTAP Mediatorは、MetroCluster IPノードの状態情報を保存するためのメールボックスLUNを提供します。これらのLUNは、MetroClusterサイトとは物理的に分離されたLinuxホスト上で実行されるONTAP Mediatorと同じ場所に配置されます。MetroClusterIPノードは、メールボックス情報を使用してディザスタリカバリ（DR）パートナーの状態を監視し、災害発生時にMediator-assisted Unplanned Switchover（MAUSO）を実装できます。



MetroCluster FC 構成では、MAUSO はサポートされません。

スイッチオーバーが必要なサイト障害がノードで検出されると、スイッチオーバーに該当する状況であることを確認したうえでスイッチオーバーが実行されます。デフォルトでは、次のシナリオでMAUSOが開始されます。

- 各ノードの不揮発性キャッシュの SyncMirror ミラーリングと DR ミラーリングはどちらも動作しており、障害発生時にキャッシュとミラーが同期されます。
- サバイバーサイトのいずれのノードもテイクオーバー状態ではありません。
- サイト災害が発生した場合。サイトディザスタとは、同じサイトで\_all\_nodesの障害です。

次のシャットダウンシナリオでは、MAUSOは\_not\_initiatedです。

- シャットダウンを開始した場合。たとえば、次のような場合です。
  - ノードを停止する

- 。ノードをリブート

各ONTAP 9リリースで使用できるMAUSO機能について説明します。

先頭のドキュメント	説明
ONTAP 9.13.1	<ul style="list-style-type: none"> <li>MAUSOが開始されるのは、<a href="#">デフォルトのシナリオ</a> ファンまたはハードウェアの障害が発生し、環境シャットダウンが開始されます。ハードウェア障害には、高温または低温、電源装置、NVRAMバッテリー、サービスプロセッサのハートビート障害などがあります。</li> <li>MetroCluster IP構成では、障害ドメインのデフォルト値は「auso-on-dr-group」に設定されます。ONTAP 9.12.1以前では、デフォルト値は「auso-on-cluster-disaster」に設定されています。</li> </ul> <p>8ノードMetroCluster IP構成では、クラスタまたは1つのDRグループのHAペアに障害が発生すると、「auso-on-dr-group」によってMAUSOがトリガーされます。HAペアの場合は、両方のノードで同時に障害が発生する必要があります。</p> <p>必要に応じて、障害ドメインの設定を「auso-on-cluster-disaster」ドメインに変更できます。metrocluster modify -auto-switchover-failure-domain auso-on-cluster-disaster 両方のDRグループでHAノードペアに障害が発生した場合のみ、MAUSOをトリガーするコマンド。</p> <ul style="list-style-type: none"> <li>障害発生時にNVRAMが同期されていない場合でも、強制的にMAUSOを実行するように動作を変更できます。</li> </ul>
ONTAP 9.12.1	<p>MetroCluster IP構成でMetroCluster自動強制スイッチオーバー機能を有効にするには、<code>metrocluster modify -allow-auto-forced-switchover true</code> コマンドを実行します</p> <p>サイト障害検出時のスイッチオーバーは、MetroCluster の自動強制スイッチオーバー機能を有効にすると自動的に実行されます。この機能は、MetroCluster IP自動スイッチオーバー機能を補完するために使用できます。</p> <p><b>MetroCluster</b> 自動強制スイッチオーバーを使用する場合のリスクと制限事項</p> <p>MetroCluster IP構成を自動強制スイッチオーバーモードで動作させると、次の既知の問題によってデータが失われる可能性があります。</p> <ul style="list-style-type: none"> <li>ストレージコントローラの不揮発性メモリは、パートナーサイトのリモートDRパートナーにミラーされません。</li> </ul> <p>注意：記載されていないシナリオが発生する場合があります。ネットアップは、MetroCluster の自動強制スイッチオーバー機能を有効にした場合に発生する可能性があるデータの破損、データの損失、その他の破損について責任を負いません。リスクと制限を許容できない場合は、MetroCluster の自動強制スイッチオーバー機能を使用しないでください。</p>

## MetroCluster IP構成でデフォルトのONTAPメディアーターメールボックスのタイムアウトを増やす

MetroCluster IP ノードは、iSCSI セッションを使用して ONTAP Mediator メールボックスディスクにアクセスできます。デフォルトの接続タイムアウトは 10 秒で、5 秒後に 1 回の再試行が含まれます。ONTAP のバージョンと環境によっては、Mediator 支援による計画外のスイッチオーバー (MAUSO) の中断を回避するために、メールボックスのタイムアウトを最大 60 秒まで増やすことができます。

NetAppでは、ネットワーク冗長プロトコル (HSRPやVRRPなど)、ループ回避プロトコル (STPなど) を使用している場合、または環境内のネットワーク遅延がデフォルトのタイムアウトである10秒を超える場合は、デフォルトのメールボックス接続タイムアウトを増やすことを推奨します。

作業を開始する前に

停止期間、つまりMetroCluster IPノードをONTAP Mediatorに再接続するのにかかる時間を評価する必要があります。10秒以上かかる場合は、MetroCluster IPノードの再接続にかかる時間よりも数秒長くタイムアウト値を設定する必要があります。

各サイトから接続が独立して維持され、一方のサイトでの停止が存続サイトからONTAP Mediatorへの接続に影響しない場合は、デフォルト値の10秒で十分であり、メールボックスタイムアウトを変更する必要はありません。

このタスクについて

- 次のONTAPバージョンでは、ONTAPメディアーターメールボックスのタイムアウトの増加がサポートされています：
  - ONTAP 9.18.1GA以降
  - ONTAP 9.17.1P3以降のONTAP 9.17.1のパッチリリース
  - ONTAP 9.16.1P10以降のONTAP 9.16.1のパッチリリース
  - ONTAP 9.15.1P16以降のONTAP 9.15.1のパッチリリース
- メールボックスのタイムアウトを増やすことは、すべてのバージョンのONTAP Mediatorでサポートされています。
- タイムアウト値のサポート範囲は 10 ~ 60 秒です。範囲外の値を指定した場合、ONTAP は自動的にデフォルト値の 10 秒に戻ります。
- MetroClusterノードがONTAP Mediatorに再接続するのに10秒以上かかる場合は、タイムアウト値をノードが接続するのにかかる時間よりも数秒長く設定する必要があります。

ステップ

1. デフォルトの ONTAP Mediator メールボックスのタイムアウトを増やすには、"[NetApp ナレッジベースの記事：ネットワーク遅延が 10 秒を超える環境で Mediator メールボックスのタイムアウトを増やす方法](#)" を参照してください。

関連情報

"[ONTAP Mediator が MetroCluster IP 構成で計画外の自動切り替えをサポートする方法の詳細については、こちらをご覧ください。](#)"

## MetroCluster IP構成でSystem Managerを使用してONTAP Mediatorを管理する

System Manager を使用して、ONTAP Mediator を管理するタスクを実行できます。

タスクについて

ONTAP 9.8以降では、System Managerを4ノードのMetroCluster IP構成を管理するためのシンプルなインターフェイスとして使用できます。これには、3番目の場所にインストールされたONTAPメディアーターも含まれます。

ONTAP 9.14.1以降では、System Managerを使用して8ノードMetroCluster IPサイトに対してもこれらの処理を実行できます。System Managerでは8ノードシステムをセットアップまたは拡張することはできませんが、8ノードMetroCluster IPシステムがすでにセットアップされている場合はこれらの処理を実行できます。

ONTAP Mediator を管理するには、次のタスクを実行します。

このタスクを実行します。	対処方法
ONTAPメディアーターの設定	<p>MetroClusterサイトの両方のクラスタが稼働し、ピア関係が確立されている必要があります。</p> <p>手順</p> <ol style="list-style-type: none"><li>1. ONTAP 9.8 の System Manager で、 * Cluster &gt; Settings * を選択します。</li><li>2. [Mediator]*セクションで、をクリックします .</li><li>3. Configure Mediator*（メディアーターの設定）ウィンドウで、 * Add+*（追加 + *）をクリックします。</li><li>4. ONTAP Mediator の設定詳細を入力します。</li></ol> <p>System Manager を使用して ONTAP Mediator を設定するときに、次の詳細を入力できます。</p> <ul style="list-style-type: none"><li>◦ ONTAP Mediator の IP アドレス。</li><li>◦ ユーザ名。</li><li>◦ パスワード。</li></ul>

<p>Mediator-Assisted Automatic Switchover (MAUSO ; メディエーターアシスト自動スイッチオーバー) の有効化または無効化</p>	<p>手順</p> <ol style="list-style-type: none"> <li>1. System Manager で、 * ダッシュボード * をクリックします。</li> <li>2. MetroClusterセクションまでスクロールします。</li> <li>3. MetroClusterサイト名の横にあるをクリックします 。</li> <li>4. または[無効化]*を選択します。</li> <li>5. 管理者のユーザ名とパスワードを入力し、[有効化]*または[無効化]*をクリックします。</li> </ol> <div style="border: 1px solid gray; padding: 10px; margin-top: 10px;">  <p>ONTAP Mediator にアクセスでき、両サイトが「通常」モードの場合、ONTAP Mediator を有効または無効にすることができます。MAUSOが有効または無効であっても、MetroCluster システムが正常な場合は ONTAP Mediator にアクセスできます。</p> </div>
<p>MetroCluster構成からONTAPメディエーターを削除します</p>	<p>手順</p> <ol style="list-style-type: none"> <li>1. System Manager で、 * ダッシュボード * をクリックします。</li> <li>2. MetroClusterセクションまでスクロールします。</li> <li>3. MetroClusterサイト名の横にあるをクリックします 。</li> <li>4. [メディエーターの削除]*を選択します。</li> <li>5. 管理者のユーザ名とパスワードを入力し、*[削除]*をクリックします。</li> </ol>
<p>ONTAPメディエーターの健全性を確認する</p>	<p>のSystem Manager固有の手順を実行します"<a href="#">MetroCluster構成の健全性の確認</a>"。</p>
<p>スイッチオーバーとスイッチバックの実行</p>	<p>の手順を実行します"<a href="#">System Mangerを使用してスイッチオーバーとスイッチバックを実行する (MetroCluster IP構成のみ)</a>"。</p>

## MetroCluster IP構成のONTAPノードスイッチオーバーをテストします

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witchオーバー処理をテストして、データが中断なく提供されることを確認できます。

#### このタスクについて

このテストでは、クラスターを 2 番目のデータ センターに切り替えても、データの可用性が影響を受けないこと (SMB およびファイバチャネル プロトコルを除く) を検証します。

このテストには約 30 分かかります。

この手順の想定される結果は次のとおりです。

- MetroCluster switchover コマンドは ' 警告プロンプトを表示します

プロンプトに「 yes 」と応答すると、コマンドが発行されたサイトがパートナーサイトを切り替えます。

MetroCluster IP 構成の場合：

- ONTAP 9.4 以前：
  - ミラーアグリゲートはネゴシエートスイッチオーバー後にデグレード状態になります。
- ONTAP 9.5 以降：
  - リモートストレージがアクセス可能である場合、ミラーされたアグリゲートは通常の状態のままになります。
  - リモートストレージへのアクセスが失われると、ネゴシエートスイッチオーバー後にミラーアグリゲートがデグレード状態になります。
- ONTAP 9.8 以降の場合：
  - リモートストレージへのアクセスが失われると、ディザスタサイトにあるミラーされていないアグリゲートは使用できなくなります。これにより、コントローラが停止する可能性があります。

手順

1. すべてのノードが設定済みの状態で通常モードになっていることを確認します。

MetroCluster node show

```
cluster_A::> metrocluster node show

Cluster                               Configuration State      Mode
-----
Local: cluster_A                       configured                normal
Remote: cluster_B                       configured                normal
```

2. スイッチオーバー処理を開始します。

MetroCluster スイッチオーバー

```
cluster_A::> metrocluster switchover
Warning: negotiated switchover is about to start. It will stop all the
data Vservers on cluster "cluster_B" and
automatically re-start them on cluster "cluster_A". It will finally
gracefully shutdown cluster "cluster_B".
```

- 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
```

- 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: -
```

- 「vserver show」コマンドと「network interface show」コマンドを使用して、DR SVM と LIF がオンラインになったことを確認します。

## 修復と手動スイッチバックの検証

修復処理と手動スイッチバック処理をテストするには、ネゴシエートスイッチオーバー後にクラスタを元のデータセンターにスイッチバックして、データの可用性に影響がないことを検証します（SMB および Solaris FC 構成を除く）。

このタスクについて

このテストには約 30 分かかります。

この手順では、想定される結果として、サービスがホームノードにスイッチバックされることを確認します。

ONTAP 9.5 以降を実行しているシステムでは、ネゴシエートスイッチオーバー後に自動的に修復が実行されるため、修復の手順は必要ありません。ONTAP 9.6 以降を実行するシステムでは、計画外のスイッチオーバー後にも自動的に修復が実行されます。

手順

- ONTAP 9.4 以前を実行しているシステムの場合は、データアグリゲートを修復します。

MetroCluster はアグリゲートを修復します

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 heal aggregates
[Job 936] Job succeeded: Heal Aggregates is successful.
```

2. ONTAP 9.4 以前を実行しているシステムの場合は、ルートアグリゲートを修復します。

MetroCluster はルートアグリゲートを修復します

この手順は、次の構成が必要です。

- MetroCluster FC 構成
- ONTAP 9.4 以前を実行している MetroCluster IP 構成次の例は、コマンドが正常に完了したことを示しています。

```
cluster_A::> metrocluster heal root-aggregates
[Job 937] Job succeeded: Heal Root Aggregates is successful.
```

3. 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                               Configuration  DR
Group Cluster Node              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.
```

何らかの理由で自動修復操作が失敗した場合は、ONTAP 9.5 より前のバージョンの ONTAP の場合と同様に、MetroCluster heal コマンドを手動で問題する必要があります。修復のステータスを監視し、障害の原因を判別するには、MetroCluster operation show および MetroCluster operation history show -instance コマンドを使用します。

4. すべてのアグリゲートがミラーされたことを確認します。

「 storage aggregate show

次の例では、すべてのアグリゲートの RAID ステータスが mirrored になっています。

```

cluster_A::> storage aggregate show
cluster Aggregates:
Aggregate Size      Available Used% State   #Vols  Nodes      RAID
Status
-----
-----
data_cluster
      4.19TB      4.13TB   2% online    8 node_A_1  raid_dp,
mirrored,
normal

root_cluster
      715.5GB     212.7GB  70% online    1 node_A_1  raid4,
mirrored,
normal

cluster_B Switched Over Aggregates:
Aggregate Size      Available Used% State   #Vols  Nodes      RAID
Status
-----
-----
data_cluster_B
      4.19TB      4.11TB   2% online    5 node_A_1  raid_dp,
mirrored,
normal

root_cluster_B    -          -      - unknown    - node_A_1  -

```

5. 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                               Configuration  DR
Group Cluster Node              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.

```

6. 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
```

### 7. ノードのステータスを確認します。

#### MetroCluster node show

```
cluster_A::> metrocluster node show
DR                               Configuration  DR
Group Cluster Node              State          Mirroring Mode
-----
1      cluster_A
      node_A_1      configured    enabled      normal
      cluster_B
      node_B_2      configured    enabled      normal

2 entries were displayed.
```

### 8. MetroCluster 処理の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: -
```

## 電源回線切断後の動作確認

MetroCluster 構成で PDU の障害が発生した場合の対応をテストできます。

このタスクについて

ベストプラクティスとして、コンポーネントの各電源装置（PSU）を別々の電源装置に接続することを推奨します。両方の PSU を同じ配電ユニット（PDU）に接続している場合、停電が発生したときに、サイトが停止したりシェルフ全体が使用できなくなったりする可能性があります。1 本原因の電源回線に障害が発生した場合に、サービスが中断する可能性があるケーブル接続の不一致がないかどうかをテストします。

このテストには約 15 分かかります。

このテストでは、MetroCluster コンポーネントが格納されたすべてのラックで、左側のすべての PDU の電源をオフにしてから、右側のすべての PDU の電源をオフにする必要があります。

この手順の想定される結果は次のとおりです。

- PDU の接続が切断されるため、エラーが生成されます。
- フェイルオーバーやサービスの中断は発生しません。

#### 手順

1. MetroCluster コンポーネントが格納されたラックの左側の PDU の電源をオフにします。
2. コンソールで結果を監視します。

「system environment sensors show -state fault」というエラーが表示されます

「storage shelf show -errors」を参照してください

```
cluster_A::> system environment sensors show -state fault

Node Sensor                State Value/Units Crit-Low Warn-Low Warn-Hi
Crit-Hi
-----
-----
node_A_1
    PSU1                    fault
                               PSU_OFF
    PSU1 Pwr In OK          fault
                               FAULT
node_A_2
    PSU1                    fault
                               PSU_OFF
    PSU1 Pwr In OK          fault
                               FAULT

4 entries were displayed.

cluster_A::> storage shelf show -errors
    Shelf Name: 1.1
    Shelf UID: 50:0a:09:80:03:6c:44:d5
    Serial Number: SHFHU1443000059

Error Type                Description
-----
Power                    Critical condition is detected in storage shelf
power supply unit "1". The unit might fail.Reconnect PSU1
```

3. 左側の PDU の電源を再度オンにします。
4. ONTAP がエラー状態をクリアすることを確認します。
5. 右側の PDU で上記の手順を繰り返します。

## 単一のストレージシェルフが停止したあとの動作確認

単一のストレージシェルフの障害をテストして、単一点障害がないことを確認できます。

このタスクについて

この手順の想定される結果は次のとおりです。

- 監視ソフトウェアからエラーメッセージが報告されます。
- フェイルオーバーやサービスの中断は発生しません。
- ハードウェア障害がリストアされたあと、ミラーの再同期が自動的に開始されます。

手順

1. ストレージフェイルオーバーのステータスを確認します。

「storage failover show」をクリックします

```
cluster_A::> storage failover show
```

Node	Partner	Possible	State Description
node_A_1	node_A_2	true	Connected to node_A_2
node_A_2	node_A_1	true	Connected to node_A_1

2 entries were displayed.

2. アグリゲートのステータスを確認します。

「storage aggregate show」

```
cluster_A::> storage aggregate show
```

```
cluster Aggregates:
```

Aggregate	Size	Available	Used%	State	#Vols	Nodes	RAID
-----							
node_A_1data01_mirrored	4.15TB	3.40TB	18%	online	3	node_A_1	
raid_dp,							
mirrored,							
normal							
node_A_1root	707.7GB	34.29GB	95%	online	1	node_A_1	
raid_dp,							
mirrored,							
normal							
node_A_2_data01_mirrored	4.15TB	4.12TB	1%	online	2	node_A_2	
raid_dp,							
mirrored,							
normal							
node_A_2_data02_unmirrored	2.18TB	2.18TB	0%	online	1	node_A_2	
raid_dp,							
normal							
node_A_2_root	707.7GB	34.27GB	95%	online	1	node_A_2	
raid_dp,							
mirrored,							
normal							

3. すべてのデータ SVM とデータボリュームがオンラインで、データを提供していることを確認します。

```
vserver show -type data
```

```
network interface show -fields is-home false
```

volume show ! vol0、 ! MDV \*

```
cluster_A::> vserver show -type data
Vserver      Type      Subtype      Admin      Operational  Root
Aggregate
-----
SVM1         data      sync-source  State      running      SVM1_root
node_A_1_data01_mirrored
SVM2         data      sync-source  State      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
-----
-----
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
-----
-----
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
```



```

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 ステータスが「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 ステータスが「normal」になっている必要があります。

```
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](#)



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。

## MetroCluster IP構成でのONTAP操作の要件と考慮事項

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。

2つのクラスタの ONTAP 構成は、ネットワークも含めて同一である必要があります。MetroCluster 機能は、スイッチオーバーの発生時にクラスタがパートナーにデータをシームレスに提供できるかどうかによって依存します。

### 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。

## ONTAP System Manager での MetroCluster 処理

ONTAP のバージョンに応じて、ONTAP System Manager を使用して実行できる MetroCluster 固有の処理もあります。

詳細については、"[System Manager を使用して MetroCluster サイトを管理する](#)" ドキュメント

## 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。vserver peer repeer コマンドを使用して FlexCache を機能させるには、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

関連情報

["FlexCache ボリュームの管理には CLI を使用します"](#)

## MetroCluster 構成での FabricPool のサポート

ONTAP 9.7 以降では、MetroCluster 構成で FabricPool ストレージ階層がサポートされます。

FabricPool の使用に関する一般的な情報については、を参照してください ["ディスクと階層 \(アグリゲート\) の管理"](#)。

**FabricPool** を使用する際の考慮事項

- クラスタに同じ容量制限の FabricPool ライセンスが必要です。
- 各クラスタに同じ名前の IPspace が必要です。

これは、デフォルト IPspace 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。
- ソースまたはデスティネーションがMetroClusterクラスタの場合、FabricPoolでSVMの移行はサポートされません。

["SVMデータモビリティの詳細"](#)です。

ミラーリングされた **FabricPool** で使用するアグリゲートを設定する



アグリゲートを設定する前に、の「MetroCluster 構成での FabricPool 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 ["ディスクおよびアグリゲートの管理"](#)。

## 手順

FabricPool で使用するアグリゲートを設定するには、次の手順を実行します。

1. アグリゲートを作成するか、既存のアグリゲートを選択します。
2. アグリゲートを MetroCluster 構成内の標準のミラーアグリゲートとしてミラーリングします。
3. の説明に従って、アグリゲートを含む FabricPool ミラーを作成します ["ディスクおよび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、どのような整合性が必要とされるかも把握しておく必要があります。

### 関連情報

["ネットワークと LIF の管理"](#)

["IPspace オブジェクトのレプリケーションとサブネットの設定の要件"](#)

["MetroCluster 構成での LIF の作成に関する要件"](#)

["LIF のレプリケーションおよび配置の要件と問題"](#)

### IPspace オブジェクトのレプリケーションとサブネットの設定の要件

パートナークラスタに IPspace オブジェクトをレプリケートするための要件、および MetroCluster 構成でサブネットと IPv6 を設定するための要件を理解しておく必要があります。

#### IPspace レプリケーション

IPspace オブジェクトをパートナークラスタにレプリケートするときは、次のガイドラインを考慮する必要があります。

- 2 つのサイトの IPspace 名が一致している必要があります。
- IPspace オブジェクトは手動でパートナークラスタにレプリケートする必要があります。

IPspace をレプリケートする前に作成されて IPspace に割り当てられた Storage Virtual Machine (SVM) は、パートナークラスタにレプリケートされません。

#### サブネット構成

MetroCluster 構成でサブネットを設定するときは、次のガイドラインを考慮する必要があります。

- MetroCluster 構成の両方のクラスタのサブネットが同じ IPspace にあり、サブネット名、サブネット、ブロードキャストドメイン、ゲートウェイが同じである必要があります。
- 2 つのクラスタの IP 範囲が同じである必要があります。

次の例では、IP 範囲が異なります。

```
cluster_A::> network subnet show
```

```
IPspace: Default
```

Subnet	Broadcast	Avail/			
Name	Subnet	Domain	Gateway	Total	Ranges
subnet1	192.168.2.0/24	Default	192.168.2.1	10/10	
192.168.2.11-192.168.2.20					

```
cluster_B::> network subnet show
```

```
IPspace: Default
```

Subnet	Broadcast	Avail/			
Name	Subnet	Domain	Gateway	Total	Ranges
subnet1	192.168.2.0/24	Default	192.168.2.1	10/10	
192.168.2.21-192.168.2.30					

## IPv6 の設定

一方のサイトで IPv6 が設定されている場合は、もう一方のサイトでも IPv6 を設定する必要があります。

## 関連情報

["MetroCluster 構成での LIF の作成に関する要件"](#)

["LIF のレプリケーションおよび配置の要件と問題"](#)

## MetroCluster 構成での LIF の作成に関する要件

MetroCluster 構成でネットワークを設定するときは、LIF の作成に関する要件に注意する必要があります。

LIF を作成する際は、次のガイドラインを考慮する必要があります。

- Fibre Channel : ストレッチ VSAN またはストレッチファブリックを使用する必要があります
- IP / iSCSI : レイヤ 2 拡張ネットワークを使用する必要があります
- ARP ブロードキャスト : 2 つのクラスタ間で ARP ブロードキャストを有効にする必要があります
- LIF の重複 : 同じ IPspace に同じ IP アドレスを持つ複数の LIF (重複する LIF) を作成することはできません
- NFS および SAN 構成 : ミラーされていないアグリゲートとミラーされたアグリゲートの両方に、異なる Storage Virtual Machine (SVM) を使用する必要があります
- LIFを作成する前にサブネットオブジェクトを作成する必要があります。ONTAPにはブロードキャストドメインが関連付けられているため、サブネットオブジェクトを使用してデスティネーションクラスタのフェイルオーバーターゲットを決定できます。

## LIF の作成を確認

MetroCluster 構成内に 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 の check lif repair-placement コマンドを使用して問題を修正できます。

## 関連情報

["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"](#)

["LIF のレプリケーションおよび配置の要件と問題"](#)

## LIF のレプリケーションおよび配置の要件と問題

MetroCluster 構成での LIF のレプリケーションの要件を理解しておく必要があります。また、レプリケートされた LIF がパートナークラスタにどのように配置されるかを把握し、LIF のレプリケーションまたは LIF の配置に失敗した場合に発生する問題について確認しておく必要があります。

### パートナークラスタへの LIF のレプリケーション

MetroCluster 構成内の 1 つのクラスタに LIF を作成すると、その LIF はパートナークラスタにレプリケートされます。LIF は名前に基づいて 1 対 1 で配置されるわけではありません。スイッチオーバー処理後に LIF を使用できるようにするため、LIF の配置プロセスは、ポートが LIF をホストできるかどうかを到達可能性とポート属性チェックに基づいて検証します。

LIF をレプリケートしてパートナークラスタに配置するには、システムが次の条件を満たしている必要があります。

条件	LIF タイプ：FC	LIF タイプ：IP/iSCSI
ノードの識別	ONTAP は、LIF を作成したノードのディザスタリカバリ（DR）パートナーに、レプリケートされた LIF を配置します。DR パートナーが使用できない場合は、DR 補助パートナーが配置に使用されます。	ONTAP は、LIF を作成したノードの DR パートナーに、レプリケートされた LIF を配置します。DR パートナーが使用できない場合は、DR 補助パートナーが配置に使用されます。
ポートの識別	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。	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。DR クラスタに同じ IPspace にポートがない場合、LIF は配置できません。  同じ IPspace とサブネットですでに 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。

到達可能性 チェック	到達可能性は、DR クラスタのポート上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。同じファブリックが DR サイトにない場合、LIF は DR パートナー上の任意のポートに配置されます。	到達可能性は、DR クラスタで以前に識別された各ポートから配置する LIF のソース IP アドレスへの Address Resolution Protocol (ARP) ブロードキャストへの応答に基づいて決定されます。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 ブロードキャストを許可する必要があります。  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。
ポートを選択 します	ONTAP は、アダプタタイプや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。属性が一致するポートが見つからない場合、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。	到達可能性チェックで到達可能とマークされたポートから、ONTAP では、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が優先されます。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 DR クラスタにない場合は、次に、ONTAP がソース LIF に到達可能なポートを選択します。  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。  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。
LIF の配置	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。	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。

#### 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 スイッチオーバー処理の際に確実に LIF を使用できるよう、LIF のレプリケーションエラーはできるだけ早く解決する必要があります。



ソース SVM がダウンしている場合でも、デスティネーション SVM で同じ IPspace とネットワークを使用するポートに別の SVM に所属する LIF が設定されていれば、LIF の配置は続行されます。

## 関連情報

["IPspace オブジェクトのレプリケーションとサブネットの設定の要件"](#)

["MetroCluster 構成での LIF の作成に関する要件"](#)

## ルートアグリゲートでのボリューム作成

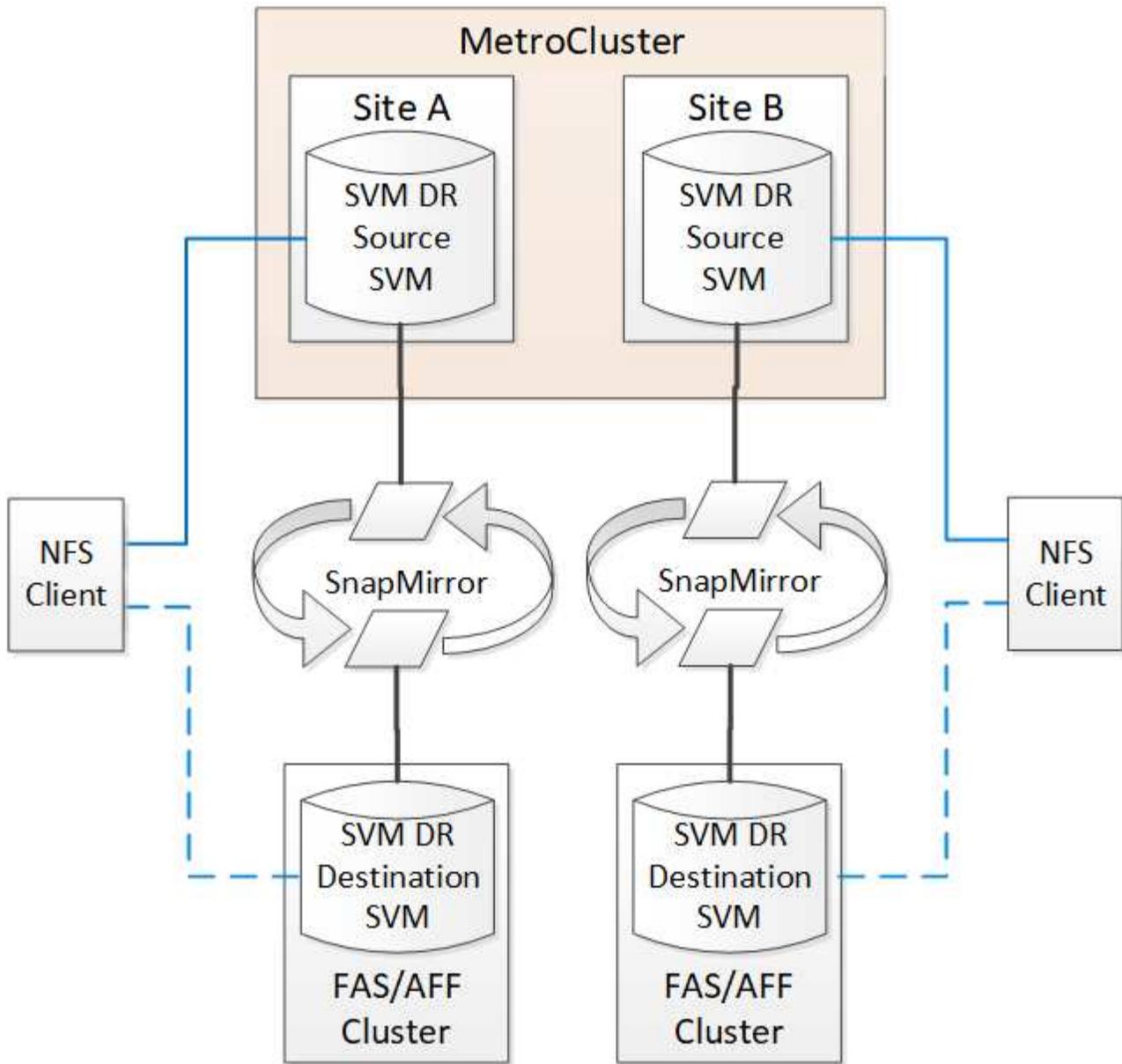
MetroCluster 構成内のノードのルートアグリゲート（HA ポリシーが CFO）に新しいボリュームを作成することはできません。

この制限があるため、ルートアグリゲートを vserver add-aggregates コマンドで SVM に追加することはできません。

## MetroCluster 構成の SVM ディザスタリカバリ

ONTAP 9.5 以降では、MetroCluster 構成のアクティブな Storage Virtual Machine（SVM）を SnapMirror SVM ディザスタリカバリ機能でソースとして使用できます。デスティネーション SVM は、MetroCluster 構成外の第 3 のクラスタに配置する必要があります。

ONTAP 9.11.1以降では、次の図に示すように、MetroCluster 構成内の両方のサイトを、FAS またはAFF デスティネーションクラスタを使用したSVM DR関係のソースにすることができます。



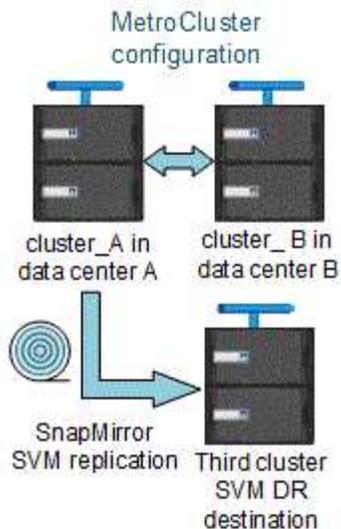
SVM を SnapMirror ディザスタリカバリで使用する場合は、次の要件と制限事項に注意してください。

- SVM ディザスタリカバリ関係のソースとして使用できるのは、MetroCluster 構成内のアクティブな SVM だけです。

スイッチオーバー前の同期元の SVM とスイッチオーバー後の同期先の SVM のどちらもソースに使用できます。

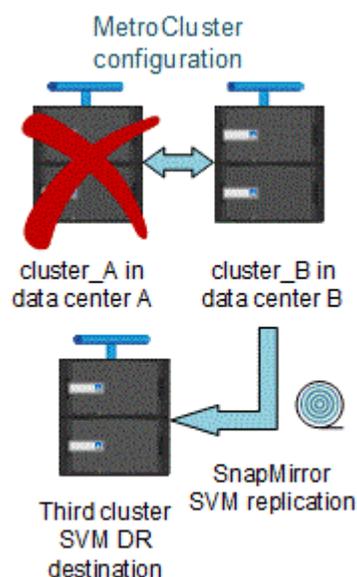
- MetroCluster 構成が安定した状態のときは MetroCluster の同期先の SVM はオンラインでないため、同期先ボリュームを SVM ディザスタリカバリ関係のソースにすることはできません。

次の図は、安定した状態における SVM ディザスタリカバリの動作を示しています。



- SVM DR 関係のソースが同期元の SVM の場合、ソースの SVM DR 関係情報が MetroCluster パートナーにレプリケートされます。

これにより、次の図に示すように、スイッチオーバー後も SVM DR の更新を続行できます。



- スイッチオーバーおよびスイッチバックの実行中に、SVM DR のデスティネーションへのレプリケーションが失敗することがあります。

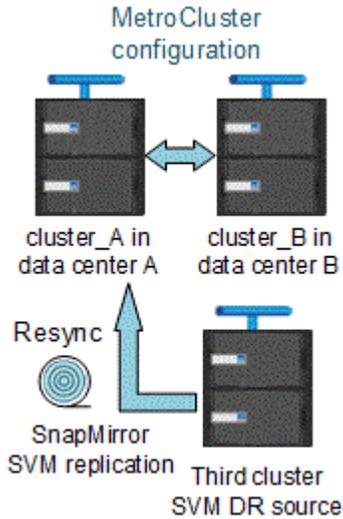
ただし、スイッチオーバーまたはスイッチバックプロセスの完了後、SVM DR の次回のスケジュールされている更新は成功します。

の「SVM 設定のレプリケート」を参照してください ["データ保護" SVM DR 関係の設定の詳細](#)については、を参照してください。

#### ディザスタリカバリサイトでの SVM の再同期

再同期では、MetroCluster 構成の Storage Virtual Machine (SVM) ディザスタリカバリ (DR) ソースが MetroCluster でないサイトのデスティネーション SVM からリストアされます。

再同期中は、次の図に示すように、ソース SVM ( cluster\_A ) が一時的にデスティネーション SVM として機能します。



再同期中に計画外スイッチオーバーが発生した場合

再同期中に計画外スイッチオーバーが発生すると、再同期の転送が停止します。計画外スイッチオーバーが発生した場合は次のようになります。

- MetroCluster サイトのデスティネーション SVM (再同期前のソース SVM) は、デスティネーション SVM のままです。パートナークラスタの SVM は、同じサブタイプで非アクティブのままです。
- 同期先の SVM をデスティネーションとする SnapMirror 関係を手動で再作成する必要があります。
- スイッチオーバー後、SnapMirror 作成処理を実行しないかぎり、サバイバーサイトでの SnapMirror show の出力に SnapMirror 関係は表示されません。

再同期中に計画外スイッチオーバーが発生した場合は、スイッチバックを実行

スイッチバックプロセスを正常に実行するには、再同期関係を解除して削除する必要があります。MetroCluster 構成に SnapMirror DR のデスティネーション SVM がある場合、またはクラスタにサブタイプ「d p-destination」の SVM がある場合、スイッチバックは実行できません。

## MetroCluster スイッチオーバー後に **storage aggregate plex show** コマンドの出力が確定しない

MetroCluster のスイッチオーバー後に **storage aggregate plex show** コマンドを実行すると、スイッチオーバーされたルートアグリゲートの plex0 のステータスが確定していないため、失敗と表示されます。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。

#### ステップ

1. スwitchオーバー時に MetroCluster 構成で NVFAIL をトリガーするには、「vol-dr-force-nvfail」パラメータを on に設定します。

```
vol modify -vserver vserver-name -volume volume-name -dr-force-nvfail on`
```

## 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

**MetroCluster IP**構成でさらに詳細な構成と監視を行うには、**Active IQ Unified Manager**と**ONTAP System Manager**を使用します。

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"](#)

### MetroCluster IP構成でNTPを使用してシステム時刻を同期する

ノードとそのクライアントの間で時刻を同期するには、クラスタごとに独自の Network Time Protocol（NTP；ネットワークタイムプロトコル）サーバが必要です。

#### このタスクについて

- テイクオーバーの発生後に障害ノードまたはパートナーノードのタイムゾーン設定を変更することはできません。
- MetroCluster IP構成のクラスタごとに、そのMetroClusterサイトのノードとIPスイッチで使用する独自のNTPサーバをそれぞれ用意する必要があります。
- MetroCluster TiebreakerまたはONTAPメディアエーターを使用する場合は、独自のNTPサーバも必要です。
- この手順では、MetroCluster IPクラスタのセットアップ後にNTPを設定する方法を示します。System Managerを使用してクラスタを設定した場合は、クラスタセットアップの一環としてNTPサーバをすでに設定しておく必要があります。詳細は、を参照してください ["MetroCluster IPサイトのセットアップ"](#)。

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 IP に関する追加情報の入手先

MetroCluster 設定の詳細については、[こちら](#)を参照してください。

## MetroCluster およびその他の情報

情報	件名
"MetroCluster IP 解決策のアーキテクチャおよび設計、 TR-4689"	<ul style="list-style-type: none"><li>• MetroCluster IP の構成と運用の技術概要</li><li>• MetroCluster IP 構成のベスト プラクティス。</li></ul>
"ファブリック接続 MetroCluster のインストールと設定"	<ul style="list-style-type: none"><li>• ファブリック接続 MetroCluster アーキテクチャ</li><li>• 構成のケーブル接続</li><li>• FC-to-SAS ブリッジの設定</li><li>• FC スイッチを設定します</li><li>• ONTAP で MetroCluster を設定します</li></ul>
"ストレッチ MetroCluster のインストールと設定"	<ul style="list-style-type: none"><li>• ストレッチ MetroCluster アーキテクチャ</li><li>• 構成のケーブル接続</li><li>• FC-to-SAS ブリッジの設定</li><li>• ONTAP で MetroCluster を設定します</li></ul>
"MetroCluster の管理"	<ul style="list-style-type: none"><li>• MetroCluster 構成について</li><li>• スイッチオーバー、修復、スイッチバック</li></ul>
"ディザスタリカバリ"	<ul style="list-style-type: none"><li>• ディザスタリカバリ</li><li>• 強制スイッチオーバー</li><li>• 複数のコントローラまたはストレージの障害からのリカバリ</li></ul>

<p>"MetroCluster メンテナンス"</p>	<ul style="list-style-type: none"> <li>• MetroCluster FC 構成のメンテナンスガイドライン</li> <li>• FC-to-SAS ブリッジおよび FC スイッチのハードウェア交換 / アップグレードおよびファームウェアアップグレード手順</li> <li>• ファブリック接続またはストレッチ MetroCluster FC 構成でのディスクシェルフのホットアド</li> <li>• ファブリック接続またはストレッチ MetroCluster FC 構成でのディスクシェルフのホットリムーブ</li> <li>• ファブリック接続またはストレッチ MetroCluster FC 構成のディザスタサイトでのハードウェア交換</li> <li>• 2 ノードのファブリック接続またはストレッチ MetroCluster FC 構成の 4 ノード MetroCluster 構成への拡張</li> <li>• 4 ノードのファブリック接続またはストレッチ MetroCluster FC 構成の 8 ノード MetroCluster FC 構成への拡張</li> </ul>
<p>"MetroCluster のアップグレードと拡張"</p>	<ul style="list-style-type: none"> <li>• MetroCluster 設定をアップグレードまたは更新する</li> <li>• ノードの追加による MetroCluster 構成の拡張</li> </ul>
<p>"MetroCluster の移行"</p>	<ul style="list-style-type: none"> <li>• MetroCluster FC 構成から MetroCluster IP 構成への移行</li> </ul>
<p>"MetroCluster のアップグレード、移行、拡張"</p>	<ul style="list-style-type: none"> <li>• MetroCluster Tiebreaker ソフトウェアを使用して MetroCluster 構成を監視する</li> </ul>
<p>"ONTAPハードウェアシステムのドキュメント"</p> <ul style="list-style-type: none"> <li>• 注： MetroCluster IP 構成では、標準的なストレージ・シェルフ保守手順を使用できます。</li> </ul>	<ul style="list-style-type: none"> <li>• ディスクシェルフのホットアド</li> <li>• ディスクシェルフのホットリムーブ</li> </ul>
<p>"コピーベースの移行"</p>	<ul style="list-style-type: none"> <li>• 7-Mode ストレージシステムから clustered Data ONTAP ストレージシステムへデータを移行する</li> </ul>
<p>"ONTAP の概念"</p>	<ul style="list-style-type: none"> <li>• ミラーされたアグリゲートの機能</li> </ul>

## 著作権に関する情報

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および/または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

## 商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。