MetroCluster のドキュメント

ONTAP MetroCluster

NetApp
February 27, 2026

This PDF was generated from https://docs.netapp.com/ja-jp/ontap-metrocluster/index.html on February 27, 2026. Always check docs.netapp.com for the latest.

目次

MetroCluster のドキュメント 1
MetroClusterリリースノート 2
MetroClusterの機能の新機能 2
MetroCluster IPプラットフォームおよびスイッチのサポートの新機能 7
プラットフォームのサポート 7
スイッチのサポート 8
MetroCluster FCプラットフォームとスイッチのサポートの新機能 9
プラットフォームのサポート 9
スイッチのサポート 9
MetroCluster IP に対するONTAP Mediator サポートの新機能 10
MetroCluster Tiebreakerのサポートの新機能 10
拡張機能 10
OSサポートマトリックス 11
ファブリック接続 MetroCluster をインストール 13
概要 13
MetroCluster のインストールを準備 13
ONTAP MetroCluster 構成の違い 13
クラスタピアリング 14
ISL に関する考慮事項 17
ファブリック接続 MetroCluster 構成で TDM / WDM 機器を使用する場合の考慮事項 18
Brocade DCX 8510-8 スイッチを使用するための要件 20
ミラーされていないアグリゲートを使用する場合の 21
MetroCluster サイトでのファイアウォールの使用状況 22
ファブリック接続 MetroCluster 構成をケーブル接続 22
ファブリック接続 MetroCluster 構成のケーブル接続 22
ファブリック MetroCluster 構成のコンポーネント 23
必要な MetroCluster FC コンポーネントと命名規則 30
FC スイッチおよび FC-to-SAS ブリッジの設定ワークシート 34
MetroCluster コンポーネントを設置してケーブルを配線します 34
FC スイッチを設定 67
FC-to-SAS ブリッジおよび SAS ディスクシェルフを設置 195
ONTAP で MetroCluster FC ソフトウェアを設定する 209
必要な情報の収集 210
標準クラスタ構成と MetroCluster 構成の類似点 / 相違点 216
メンテナンスモードでコンポーネントの HA 状態を確認および設定する 217
システムのデフォルト設定をリストアし、コントローラモジュールで HBA タイプを設定しています 218
FAS8020 システムでの X1132A-R6 クアッドポートカードの FC-VI ポートの設定 220
メンテナンスモードでの 8 ノードまたは 4 ノード構成のディスク割り当ての検証 222
保守モードでの 2 ノード構成のディスク割り当ての検証 229

ONTAP をセットアップしています 231
クラスタを MetroCluster 構成に設定 236
Config Advisor での MetroCluster 構成エラーの確認 268
ローカル HA の処理を検証しています 268
スイッチオーバー、修復、スイッチバックを検証しています 270
構成バックアップファイルを保護しています 270
MetroCluster 設定で仮想 IP およびボーダーゲートウェイプロトコルを使用する場合の考慮事項 270
ONTAP の制限事項 271
このレイヤ 3 解決策を MetroCluster 設定で使用する場合の注意事項 272
MetroCluster 構成をテストする 273
ネゴシエートスイッチオーバーを検証中 273
修復と手動スイッチバックの検証 275
単一の FC-to-SAS ブリッジの停止 277
電源回線切断後の動作確認 279
スイッチファブリック障害後の動作確認 280
単一のストレージシェルフが停止したあとの動作確認 282
MetroCluster 構成を削除 292
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 293
Active IQ Unified ManagerおよびONTAPシステムマネージャを使用して詳細な設定と監視を行う 293
NTP を使用してシステム時刻を同期します 293
MetroCluster 構成で ONTAP を使用する場合の考慮事項 294
MetroCluster 構成での FlexCache のサポート 295
MetroCluster 構成での FabricPool のサポート 296
MetroCluster 構成での FlexGroup のサポート 297
MetroCluster 構成での整合グループのサポート 297
MetroCluster 構成のジョブスケジュール 297
MetroCluster サイトから第 3 のクラスタへのクラスタピアリング 297
MetroCluster 構成での LDAP クライアント設定のレプリケーション 297
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 297
MetroCluster 構成の SVM ディザスタリカバリ 303
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 306
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 306
追加情報の参照先 307
MetroCluster およびその他の情報 307
MetroCluster IP 構成をインストール 309
MetroCluster IP インストールワークフロー 309
MetroCluster のインストールを準備 309
ONTAP MetroCluster構成のサポートマトリックス 309
ONTAP メディエーターと MetroCluster Tiebreaker の違い 311
リモート ストレージとMetroCluster IP 構成について学習します 311
自動ドライブ割り当てとADPシステムのMetroCluster IP要件 314

MetroCluster IP構成におけるクラスタピアリングの要件 331
ISL の要件 333
MetroCluster 準拠スイッチの使用に関する考慮事項 349
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 357
MetroCluster IP構成のファイアウォール ポート要件 359
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。 359
MetroCluster ハードウェアコンポーネントを設定します 362
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。 362
必要なMetroCluster IP 構成コンポーネントと命名規則 366
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 370
MetroCluster IP スイッチをケーブル接続します 371
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 421
MetroCluster IP スイッチを設定します 422
MetroCluster IPスイッチの健全性を監視する 479
ONTAP で MetroCluster ソフトウェアを設定します 507
CLIを使用したMetroClusterソフトウェアの設定 507
System Managerを使用したMetroClusterソフトウェアの設定 575
計画外の自動スイッチオーバー用に ONTAP Mediator を構成する 579
MetroCluster IP構成のONTAP Mediatorインストール要件 579
MetroCluster IP構成用のONTAPメディエーターを設定する 581
MetroCluster IP構成からONTAPメディエーターを削除する 586
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 587
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 587
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 589
MetroCluster IP構成でSystem Managerを使用してONTAP Mediatorを管理する 590
MetroCluster IP構成のONTAPノードスイッチオーバーをテストします 591
ネゴシエートスイッチオーバーを検証中 591
修復と手動スイッチバックの検証 593
電源回線切断後の動作確認 596
単一のストレージシェルフが停止したあとの動作確認 598
MetroCluster 構成を削除 608
MetroCluster IP構成でのONTAP操作の要件と考慮事項 609
ライセンスに関する考慮事項 609
SnapMirror に関する考慮事項 609
ONTAP System Manager での MetroCluster 処理 609
MetroCluster 構成での FlexCache のサポート 609
MetroCluster 構成での FabricPool のサポート 610
MetroCluster 構成での FlexGroup のサポート 611
MetroCluster 構成のジョブスケジュール 611

MetroCluster サイトから第 3 のクラスタへのクラスタピアリング . . . 611
MetroCluster 構成での LDAP クライアント設定のレプリケーション . . . 611
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 . . . 612
MetroCluster 構成の SVM ディザスタリカバリ . . . 616
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 . . . 619
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 . . . 619
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 . . . 620
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。 . . . 620
MetroCluster IP構成でNTPを使用してシステム時刻を同期する . . . 620
MetroCluster IP に関する追加情報の入手先 . . . 621
MetroCluster およびその他の情報 . . . 622
ストレッチ MetroCluster 構成をインストール . . . 624
概要 . . . 624
MetroCluster のインストールを準備 . . . 624
ONTAP MetroCluster 構成の違い . . . 624
クラスタピアリング . . . 626
ミラーされていないアグリゲートを使用する場合の . . . 628
MetroCluster サイトでのファイアウォールの使用状況 . . . 629
構成に適したインストール手順の選択 . . . 629
2 ノード SAS 接続ストレッチ MetroCluster 構成のケーブル接続 . . . 630
2 ノード SAS 接続ストレッチ MetroCluster 構成のケーブル接続 . . . 630
2 ノード SAS 接続ストレッチ MetroCluster 構成のコンポーネント . . . 630
2 ノード SAS 接続ストレッチ構成の MetroCluster に必要なハードウェアコンポーネントと命名ガイドライン . . . 631
2 ノード SAS 接続ストレッチ構成の MetroCluster コンポーネントを設置してケーブル接続します . . . 632
2 ノードブリッジ接続ストレッチ MetroCluster 構成をケーブル接続します . . . 636
2 ノードブリッジ接続ストレッチ MetroCluster 構成のケーブル接続 . . . 636
2 ノードブリッジ接続ストレッチ MetroCluster 構成のコンポーネント . . . 636
2 ノードブリッジ接続ストレッチ構成の MetroCluster に必要なハードウェアコンポーネントと命名規則 . . . 637
FC-to-SAS ブリッジの情報収集ワークシート . . . 640
MetroCluster コンポーネントを設置してケーブルを配線します . . . 641
FC-to-SAS ブリッジおよび SAS ディスクシェルフを設置 . . . 643
ONTAP での MetroCluster ソフトウェアの設定 . . . 657
サイト A の IP ネットワーク情報ワークシート . . . 658
サイト B の IP ネットワーク情報ワークシート . . . 660
標準クラスタ構成と MetroCluster 構成の類似点 / 相違点 . . . 662
システムのデフォルト設定をリストアし、コントローラモジュールで HBA タイプを設定しています . . . 663
FAS8020 システムでの X1132A-R6 クアッドポートカードの FC-VI ポートの設定 . . . 665
保守モードでの 2 ノード構成のディスク割り当ての検証 . . . 667

コンポーネントの HA 状態の確認 669
2 ノード MetroCluster 構成での ONTAP のセットアップ 670
クラスタを MetroCluster 構成に設定 672
Config Advisor での MetroCluster 構成エラーの確認 695
スイッチオーバー、修復、スイッチバックを検証しています 695
構成バックアップファイルを保護しています 696
MetroCluster 設定で仮想 IP およびボーダーゲートウェイプロトコルを使用する場合の考慮事項 696
MetroCluster 構成をテストする 699
ネゴシエートスイッチオーバーを検証中 699
修復と手動スイッチバックの検証 701
単一の FC-to-SAS ブリッジの停止 703
電源回線切断後の動作確認 705
単一のストレージシェルフが停止したあとの動作確認 706
MetroCluster 構成を削除 717
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 718
Active IQ Unified ManagerおよびONTAPシステムマネージャを使用して詳細な設定と監視を行う 718
NTP を使用してシステム時刻を同期します 718
MetroCluster 構成で ONTAP を使用する場合の考慮事項 719
ライセンスに関する考慮事項 720
SnapMirror に関する考慮事項 720
MetroCluster 構成での FlexCache のサポート 720
MetroCluster 構成での FabricPool のサポート 720
MetroCluster 構成での FlexGroup のサポート 721
MetroCluster 構成のジョブスケジュール 721
MetroCluster サイトから第 3 のクラスタへのクラスタピアリング 722
MetroCluster 構成での LDAP クライアント設定のレプリケーション 722
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 722
MetroCluster 構成の SVM ディザスタリカバリ 726
2 ノードストレッチ MetroCluster 構成での storage disk show コマンドおよび storage shelf show コマンドの出力 728
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 729
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 729
ストレッチからファブリック接続への MetroCluster 構成の移行 729
追加情報の参照先 730
MetroCluster およびその他の情報 730
MetroCluster Tiebreakerのインストールと設定 733
MetroCluster Tiebreakerのサポートの新機能 733
拡張機能 733
OSサポートマトリックス 733
Tiebreaker ソフトウェアの概要 734
NetApp MetroCluster Tiebreaker ソフトウェアによる障害の検出 734

Tiebreaker ソフトウェアでサイト障害を検出する方法 735
Tiebreaker ソフトウェアでサイト間接続障害を検出する方法 736
災害のタイプが Tiebreaker ソフトウェアの検出時間に与える影響 736
Tiebreaker の CLI とマニュアルページについて 737
Tiebreaker ソフトウェアをインストールします 738
Tiebreakerのインストールワークフロー 738
Tiebreakerソフトウェアをインストールする準備 738
Tiebreakerのホストとデータベースのインストールを保護する 740
Tiebreakerソフトウェアパッケージのインストール 743
Tiebreakerモニタが実行されているホストをアップグレードする 840
MetroCluster Tiebreakerソフトウェアを構成する 840
TiebreakerソフトウェアCLIを起動する 840
MetroCluster 構成を追加 840
証明書をインポートする 844
MetroCluster Tiebreaker 構成を変更するためのコマンド 849
MetroCluster 構成を削除 850
Tiebreaker ソフトウェアの SNMP 設定 851
MetroCluster 設定を監視する 853
AutoSupport を設定しています 853
監視処理のステータスを表示する 855
MetroCluster の設定情報を表示する 857
ダンプ・ファイルの作成 857
タイブレーカーオブザーバーモードを無効にする 858
MetroCluster Tiebreaker をアクティブモードで使用する場合のリスクと制限事項 858
MetroCluster Tiebreaker のファイアウォール要件 859
MetroCluster Tiebreakerを使用してスイッチオーバーをシミュレートする 860
MetroCluster Tiebreakerのイベントログファイル 862
追加情報の参照先 862
MetroCluster およびその他の情報 862
MetroCluster のデータ保護とディザスタリカバリを理解する 864
MetroCluster のデータ保護とディザスタリカバリについて理解する 864
8 ノード / 4 ノード MetroCluster 構成でのローカルフェイルオーバーとスイッチオーバー 864
MetroCluster 構成でのデータと設定のレプリケーション 865
災害の種類とリカバリ方法 872
8 ノード / 4 ノード MetroCluster 構成でのノンストップオペレーションの実現 874
2 ノード MetroCluster 構成でのノンストップオペレーションの実現 875
スイッチオーバープロセスの概要 875
修復時の動作（ MetroCluster FC 構成） 882
修復時の動作（ MetroCluster IP 構成） 883
スイッチオーバー後の MetroCluster IP 構成でのアグリゲートの自動修復 884
MetroCluster 構成用の SVM の作成 886

スイッチバック時の動作 888
スイッチオーバー、修復、スイッチバックを実行 889
テストやメンテナンスのためにスイッチオーバーを実行 889
テストまたはメンテナンスのためのスイッチオーバーの実行 889
MetroCluster構成がスイッチオーバー状態の場合の制限事項 889
スイッチオーバーに向けたシステムの事前チェック 890
カスタム AutoSupport メッセージの送信 - ネゴシエートスイッチオーバー前 891
ネゴシエートスイッチオーバーの実行 891
SVMが実行されていて、アグリゲートがオンラインになっていることを確認してください 893
構成を修復 894
スイッチバックを実行しています 898
スイッチバックが成功したことを確認する 901
スイッチオーバー、修復、スイッチバック用のコマンドです 902
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） 903
スイッチオーバーとスイッチバックの概要 903
ONTAP 9.6または9.7のSystem Managerを使用してスイッチオーバーとスイッチバックを実行 904
ONTAP 9.8以降のSystem Managerを使用してスイッチオーバーとスイッチバックを行う 904
MetroCluster 設定を監視する 906
MetroCluster の設定を確認しています 906
MetroCluster 設定を確認および監視するためのコマンド 908
MetroCluster Tiebreaker または ONTAP メディエーターを使用して設定を監視する 909
NetApp MetroCluster Tiebreaker ソフトウェアで障害を検出する方法 909
NVFAIL を使用したファイルシステム整合性の監視および保護 911
NFS ボリュームまたは LUN へのアクセスに対する NVFAIL の影響 912
データ損失イベントを監視するコマンド 913
スイッチオーバー後に NVFAIL 状態のボリュームにアクセスする場合 914
スイッチオーバー後の NVFAIL 状態にある LUN のリカバリ 914
追加情報の参照先 914
MetroCluster およびその他の情報 915
MetroCluster のコンポーネントをメンテナンスします 916
MetroClusterメンテナンスの詳細 916
メンテナンスタスクの準備 916
各種のMetroCluster構成のメンテナンス手順 916
その他のすべてのメンテナンス手順 916
MetroClusterのメンテナンスの準備 917
メンテナンスタスクを実行する前にコンソールログを有効にする 917
メンテナンス作業を実行する前に、 ONTAP メディエーターまたは Tiebreaker の監視を削除します 918
MetroCluster の障害とリカバリのシナリオ 919
Interoperability Matrix Tool を使用した MetroCluster 情報の検索 920
MetroCluster FC構成のメンテナンス手順 920
健常性監視用に、スイッチまたはATTOブリッジのIPアドレスを変更します 920

FC-to-SAS ブリッジのメンテナンス 922
FC スイッチのメンテナンスと交換 983
ファブリック接続 MetroCluster 構成のシェルフを無停止で交換する 1034
MetroCluster FC 構成へのストレージのホットアド 1039
MetroCluster FC 構成からのストレージのホットリムーブ 1061
MetroCluster FC構成での単一サイトの電源オフと電源オン 1065
MetroCluster FC 構成全体の電源をオフにします 1079
MetroCluster IP構成のメンテナンス手順 1081
IP スイッチのメンテナンスと交換 1081
MetroCluster IP 構成でのストレージの特定 1107
共有ストレージ MetroCluster スイッチを使用した MetroCluster IP へのシェルフの追加 1111
MetroCluster IP構成でのエンドツーエンドの暗号化の設定 1127
MetroCluster IP構成での単一サイトの電源オフと電源オン 1131
MetroCluster IP 構成全体の電源をオフにします 1138
すべてのMetroCluster構成のメンテナンス手順 1140
ストレッチ MetroCluster 構成のシェルフの無停止での交換 1140
ルートボリュームを新しいデスティネーションに移行するタイミング 1142
MetroCluster 構成でのメタデータボリュームの移動 1143
MetroCluster 構成のクラスタの名前変更 1146
MetroCluster構成の健全性の確認 1148
追加情報の参照先 1151
MetroCluster FC から MetroCluster IP に移行します 1152
移行する手順を選択 1152
サポートされるプラットフォームの組み合わせ 1152
移行する手順を選択 1154
MetroCluster FC から MetroCluster IP 構成への無停止での移行（ ONTAP 9.8 以降） 1155
MetroCluster FC から MetroCluster IP 構成への無停止での移行（ ONTAP 9.8 以降） 1155
MetroCluster FC 構成から MetroCluster IP 構成への移行を準備 1157
MetroCluster FC から MetroCluster IP 構成への移行 1168
メンテナンス後にカスタム AutoSupport メッセージを送信する 1223
Tiebreaker またはメディエーターの監視をリストアしています 1223
2 ノード MetroCluster FC から 4 ノード MetroCluster IP 構成への無停止での移行（ ONTAP 9.8 以降） 1224
2 ノード MetroCluster FC から 4 ノード MetroCluster IP 構成への無停止での移行（ ONTAP 9.8 以降） 1224
この手順での命名例 1225
FC から IP への移行を停止させる準備をしています 1225
MetroCluster FC ノードを移行します 1234
MetroCluster IP コントローラモジュールを接続します 1243
新しいノードの設定と移行の完了 1259
システムを通常動作に戻します 1266
ストレージシェルフを撤去する際の、 MetroCluster FC から MetroCluster IP への停止を伴う移行（

ONTAP 9.8 以降） 1267
コンソールログを有効にする 1268
古いシェルフを撤去する場合の移行要件 1268
データを移動する場合や古いストレージシェルフを撤去する場合の、停止を伴う移行ワークフロー 1269
構成を移行しています 1269
ルートアグリゲートを移行します 1270
データアグリゲートを移行する 1271
撤去するシェルフは node_A_1 から FC 、 node_A_1 から FC を移行 1271
移行を完了しています 1273
新しいコントローラで既存シェルフを使用できない場合の停止を伴う移行（ ONTAP 9.8 以降） 1273
コンソールログを有効にする 1273
新しいノードでシェルフがサポートされていない場合の移行の要件 1274
新しいコントローラでシェルフがサポートされない場合の停止を伴う移行のワークフロー 1275
新しいコントローラモジュールの準備を行います 1275
新しいディスクシェルフを既存の MetroCluster FC コントローラに接続 1276
ルートアグリゲートを移行して、新しいディスクシェルフにデータを移動します 1276
構成を移行しています 1282
FC SAN ワークロードを MetroCluster FC ノードから MetroCluster IP ノードに移動する 1283
FC SAN ワークロードを MetroCluster FC ノードから MetroCluster IP ノードに移動する 1283
Linux iSCSI ホストを MetroCluster FC ノードから MetroCluster IP ノードに移動 1290
手順1：新しいiSCSI接続をセットアップする 1290
手順2：新しいノードをレポートノードとして追加する 1294
手順3：レポートノードを削除してパスを再スキャンする 1299
追加情報の参照先 1301
MetroCluster およびその他の情報 1301
MetroCluster 構成をアップグレード、更新、または拡張します 1304
まずはこちらから-手順 を選択してください 1304
はじめに：コントローラのアップグレード、システムの更新、拡張のいずれかを選択してください 1304
コントローラのアップグレード手順 を選択します 1305
システムの更新方法を選択する 1311
拡張手順 を選択します 1315
「system controller replace」コマンドを使用したスイッチオーバーとスイッチバックを使用して、4ノードMetroCluster IPのコントローラをアップグレードする（ONTAP 9.13.1以降） 1316
system controller replaceコマンドを使用したMetroCluster IPコントローラのアップグレードワークフロー（ONTAP 9.13.1以降） 1316
アップグレードを準備 1317
コントローラのアップグレード 1330
MetroCluster IPコントローラのアップグレードの完了 1357
スイッチオーバーとスイッチバックを使用したMetroCluster IPのコントローラのアップグレード（ONTAP 9.8以降） 1359
スイッチオーバーとスイッチバックを使用したMetroCluster

IPコントローラのアップグレードのワークフロー（ONTAP 9.8以降） 1359
アップグレードを準備 1360
コントローラのアップグレード 1374
MetroCluster IPコントローラのアップグレードの完了 1402
スイッチオーバーとスイッチバックを使用して、MetroCluster IP構成のAFF A700 / FAS9000からAFF A900 / FAS9500にコントローラをアップグレードする（ONTAP 9.10.1以降） 1404
コンソールログを有効にする 1405
MetroCluster IP 構成のコントローラをアップグレードするためのワークフロー 1405
アップグレードを準備 1406
MetroCluster 構成をスイッチオーバーします 1412
AFF A700またはFAS9000プラットフォームのコントローラモジュールとNVSを取り外します 1414
AFF A900またはFAS9500 NVSとコントローラモジュールを取り付けます 1415
新しいプラットフォームに対応できるようにスイッチの RCF ファイルを更新します 1422
新しいコントローラを設定します 1422
MetroCluster 構成をスイッチバックします 1431
MetroCluster 構成の健全性を確認します 1433
site_A でノードをアップグレードします 1434
Tiebreaker またはメディエーターの監視をリストアします 1434
カスタム AutoSupport メッセージをメンテナンス後に送信します 1434
スイッチオーバーとスイッチバックを使用して、MetroCluster FC構成のコントローラをアップグレードします 1435
サポートされるプラットフォームの組み合わせ 1435
このタスクについて 1435
コンソールログを有効にする 1436
アップグレードを準備 1437
MetroCluster 構成をスイッチオーバーします 1443
古いコントローラのネットワーク構成を準備 1445
古いプラットフォームを削除する 1447
新しいコントローラを設定します 1447
MetroCluster 構成をスイッチバックします 1459
MetroCluster 構成の健全性を確認します 1461
cluster_Aのノードをアップグレードします。 1462
カスタム AutoSupport メッセージをメンテナンス後に送信します 1462
Tiebreaker による監視をリストアします 1462
スイッチオーバーとスイッチバックを使用して、MetroCluster FC構成のAFF A700 / FAS9000からAFF A900/ FAS9500にコントローラをアップグレード（ONTAP 9.10.1以降） 1462
コンソールログを有効にする 1464
アップグレードを準備 1464
AFF A700 コントローラのスロット 7 をクリアします 1464
MetroCluster 構成をスイッチオーバーします 1471
site_BまたはAFF A700コントローラモジュールとNVSをsite_Bで取り外します 1473

site_B の両方のノードからコントローラモジュールと NVS を取り外します 1473
AFF A900またはFAS9500 NVSとコントローラモジュールを取り付けます 1475
MetroCluster 構成をスイッチバックします 1488
MetroCluster 構成の健全性を確認します 1489
site_A でノードをアップグレードします 1490
カスタム AutoSupport メッセージをメンテナンス後に送信します 1490
Tiebreaker による監視をリストアします 1490
「system controller replace」コマンドを使用したスイッチオーバーとスイッチバックを使用した4ノードMetroCluster FC構成のコントローラのアップグレード（ONTAP 9.10.1以降） 1491
サポートされるプラットフォームの組み合わせ 1491
このタスクについて 1491
コンソールログを有効にする 1492
アップグレードを準備 1492
古いコントローラを交換して新しいコントローラをブート 1496
アップグレードを完了します 1508
cluster_Aのノードをアップグレードします。 1509
4 ノード MetroCluster FC 構成を更新しています 1509
コンソールログを有効にする 1509
更新手順の実行 1509
4ノードまたは8ノードのMetroCluster IP構成を更新（ONTAP 9.8以降） 1511
コンソールログを有効にする 1514
更新手順の実行 1514
2 ノード MetroCluster FC 構成を 4 ノード構成に拡張 1523
2 ノード MetroCluster FC 構成から 4 ノード構成への拡張 1523
コンソールログを有効にする 1525
MetroCluster 構成の状態の確認 1525
AutoSupport 構成にノードを追加する前にカスタム MetroCluster メッセージを送信する 1527
ファブリック接続 MetroCluster 構成でコントローラモジュールを追加する際の新しいコントローラポートのゾーニング 1528
各クラスタに新しいコントローラモジュールを追加します 1528
新しいコントローラで MetroCluster 設定を更新しています 1561
両方のコントローラモジュールでのストレージフェイルオーバーの有効化およびクラスタ HA の有効化 1564
SVM を再起動しています 1565
4 ノード MetroCluster FC 構成を 8 ノード構成に拡張 1565
4 ノード MetroCluster FC 構成から 8 ノード構成への拡張 1566
コンソールログを有効にする 1568
新しいケーブルレイアウトの決定 1568
新しい機器をラックに設置 1569
MetroCluster 構成の健全性の確認 1569
Config Advisor での MetroCluster 構成エラーの確認 1571

カスタム AutoSupport メッセージの送信 - MetroCluster 構成へのノードの追加前 1571
新しいノードのスイッチファブリックにケーブルを再接続してゾーニングします 1572
新しいコントローラで ONTAP を設定します 1573
Config Advisor での MetroCluster 構成エラーの確認 1603
カスタム AutoSupport メッセージは、 MetroCluster 構成へのノードの追加後に送信します 1603
スイッチオーバー、修復、スイッチバックを検証しています 1604
MetroCluster IP設定を展開します 1604
コンソールログを有効にする 1606
この手順での命名例 1606
2つ目のDRグループを追加する際にサポートされるプラットフォームの組み合わせ 1606
カスタム AutoSupport メッセージをメンテナンス前に送信する 1609
新しいDRグループを追加する際のVLANに関する考慮事項 1610
MetroCluster 構成の健全性の確認 1611
監視アプリケーションから構成を削除します 1615
新しいコントローラモジュールの準備を行います 1616
RCF ファイルをアップグレードします 1616
新しいノードをクラスタに追加 1618
クラスタ間 LIF の設定、 MetroCluster インターフェイスの作成、およびルートアグリゲートのミラーリングを行います 1620
新しいノードの追加を完了しています 1632
MetroCluster構成からDRグループを削除する 1638
コンソールログを有効にする 1638
各クラスタからDRグループノードを削除します 1639
追加情報の参照先 1646
MetroCluster およびその他の情報 1646
災害からリカバリします 1648
ディザスタリカバリのワークフロー 1648
災害後の強制スイッチオーバーの実行 1648
ディザスタサイトのフェンシング 1648
強制スイッチオーバーの実行 1649
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 1650
スイッチオーバー後に NVFAIL 状態のボリュームにアクセスする場合 1650
正しいリカバリ手順の選択 1651
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 1652
MetroCluster FC-to-IP移行時のコントローラモジュールの障害のシナリオ 1652
8 ノード MetroCluster 構成でのコントローラモジュールの障害のシナリオ 1652
2 ノード MetroCluster 構成でのコントローラモジュールの障害のシナリオ 1656
マルチコントローラまたはストレージの障害からリカバリする 1657
マルチコントローラまたはストレージの障害からのリカバリ 1657
コンソールログを有効にする 1658
ハードウェアを交換し、新しいコントローラをブート 1658

MetroCluster IP 構成でスイッチバックを準備 1671
MetroCluster FC 構成でスイッチバックを準備 1716
混在構成でのスイッチバックの準備（移行中のリカバリ） 1744
リカバリを完了しています 1747
コントローラ以外の障害からのリカバリ 1761
コンソールログを有効にする 1761
MetroCluster構成での構成の修復 1762
スイッチバックに向けたシステムの事前チェック 1764
スイッチバックを実行しています 1766
スイッチバックが成功したことを確認する 1768
スイッチバック後の古いアグリゲートリストの削除 1770
法的通知 1773
著作権 1773
商標 1773
特許 1773
プライバシーポリシー 1773
安全に関する情報と規制に関する通知 1773

MetroCluster のドキュメント

MetroClusterリリースノート

MetroClusterの機能の新機能

ONTAP 9データ管理ソフトウェアの各リリースには、ONTAP MetroCluster構成の機能、管理性、パフォーマンスを向上させる新機能と強化された機能が搭載されています。

ONTAP MetroCluster構成に影響する既知の問題、制限事項、およびアップグレードに関する注意事項の詳細については、『 "ONTAP 9 リリースノート"。リリースノートにアクセスするには、NetAppアカウントでサインインするか、アカウントを作成する必要があります。

MetroCluster構成でサポートされる機能	概要 と詳細情報の入手方法	最初から利用可能です
MetroCluster FlexGroup ボリュームの SnapMirror クラウドサポート	SnapMirror cloudは、MetroCluster構成のFlexGroupボリュームに対するバックアップおよびリストア操作をサポートします。 "ONTAP SnapMirrorを使用してクラウドにデータをバックアップ"	ONTAP 9.18.1GA
`system controller replace`コマンドを使用したMetroCluster IPコントローラのアップグレードでサポートされる新しいアップグレードの組み合わせ	MetroCluster IP 構成で `system controller replace`コマンドを使用した AFF A70 から AFF A90 および FAS70 から FAS90 へのシステムアップグレードのサポート。 "「system controller replace」コマンドを使用したスイッチオーバーとスイッチバックを使用して、4ノードMetroCluster IPのコントローラをアップグレードする（ONTAP 9.13.1以降）"	ONTAP 9.18.1GA
MetroCluster IP構成におけるFAS50システムのフラッシュキャッシュサポート	Flash Cache は、 MetroCluster IP 構成の FAS50 システムでサポートされます。 "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

MetroCluster構成でサポートされる機能	概要 と詳細情報の入手方法	最初から利用可能です
エンドツーエンドの暗号化のためのMetroCluster IPサポート	次のシステムでは、 MetroCluster IP 構成のサイト間の 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するためのエンドツーエンドの暗号化がサポートされています。 • AFF A800、AFF C800 • AFF A20、 AFF A30、 AFF C30、 AFF A50、 AFF C60 • AFF A70、AFF A90、AFF A1K、AFF C80 • FAS50、FAS70、FAS90 "MetroCluster IP構成でのエンドツーエンドの暗号化の設定"	ONTAP 9.17.1
MetroCluster IP構成の変更を制限する	ONTAP 9.17.1 には、4 ノードMetroCluster IP 構成の次の制限の更新が含まれています。 • AFF C800、 AFF A800、 AFF A900、 AFF A90、およびAFF A1K システムには、次の更新された制限があります。 ◦ ノードあたりのFlexVol volume制限: 1250 ◦ SVM の制限: クラスターあたり 64 SVM ◦ LIF数: クラスタあたり256個のLIF • AFF A400、 AFF C400、 ASA A400、 ASA C400、 AFF C80、 AFF A70、およびAFF A50 システムには、次の更新された制限があります。 ◦ アグリゲートあたりのFlexVol volume制限（単一または複数）: 625 ◦ ノードあたりのFlexVol volume制限: 1250 ◦ 高可用性（HA）ペアあたりのFlexVol volume制限：2500 ◦ クラスタあたりのFlexVol volume制限: 5000 ◦ SVM の制限: クラスターあたり 64 SVM ◦ LIF数: クラスタあたり256個のLIF 参照"Hardware Universe"詳細についてはこちらをご覧ください。	ONTAP 9.17.1
資格情報を使用したFibreBridgeファームウェアのアップデート	サーバーがファームウェア パッケージをダウンロードするために資格情報を必要とする場合は、資格情報を使用して FibreBridge ブリッジのファームウェアを更新できます。 "FibreBridge ブリッジのファームウェアを更新します"	ONTAP 9 .16.1

MetroCluster構成でサポートされる機能	概要 と詳細情報の入手方法	最初から利用可能です
MetroCluster構成の移行におけるSVMデータ移動のサポート	ONTAPでサポートされるMetroCluster SVMの移行は次のとおりです。 • MetroCluster以外のHAペアとMetroCluster IP構成間でのSVMの移行 • 2つのMetroCluster IP構成間でのSVMの移行 • MetroCluster FC構成とMetroCluster IP構成間でのSVMの移行 "SVMのデータ移動"	ONTAP 9 .16.1
BGPピアグループのMD5認証サポート	ONTAPはBGPピアグループでMD5認証をサポートして、BGPセッションを保護します。MD5がイネーブルの場合、BGPセッションは許可されたピア間でのみ確立および処理されるため、許可されていないアクターによるセッションの中断を防ぐことができます。 "仮想IP（VIP）LIFの設定"	ONTAP 9 .16.1
エンドツーエンドの暗号化のためのMetroCluster IPサポート	AFF A400、 AFF C400、 FAS8300、およびFAS8700システムでは、エンドツーエンドの暗号化がサポートされており、 MetroCluster IP構成のサイト間の 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
AFF A800およびAFF C800システムでの4ノードMetroCluster IP構成のボリューム制限の拡張	4ノードMetroCluster IP構成では、AFF A800およびAFF C800システムの次のボリューム制限が拡張されました。 • アグリゲートあたりのFlexVolの最大数が200から625に増加しました。 • ノードあたりのFlexVolの最大ボリューム数が800から1250に増加しました。 • HA ペアあたりのFlexVolボリュームの最大数が 1600 から 2500 に増加しました。	ONTAP 9.15.1
MetroCluster IPでのNVMeのサポート	NVMe/TCPフロントエンドホストプロトコルは、4ノードMetroCluster IP構成でサポートされます。 "MetroCluster 環境のSAN構成"	ONTAP 9.15.1

MetroCluster構成でサポートされる機能	概要 と詳細情報の入手方法	最初から利用可能です
AFF A900システムでの4ノードMetroCluster IP構成のボリューム制限の拡張	4ノードMetroCluster IP構成では、AFF A900システムの次のボリューム制限が引き上げられました。 • アグリゲートあたりのFlexVolの最大数が200から625に増加しました。 • ノードあたりのFlexVolの最大ボリューム数が800から1250に増加しました。 • HA ペアあたりのFlexVolボリュームの最大数が 1600 から 2500 に増加しました。	ONTAP 9.14.1
ミラーアグリゲートとミラーされていないアグリゲートでのS3オブジェクトストレージのサポート	MetroCluster IPおよびFC構成では、ミラーされたアグリゲートまたはミラーされていないアグリゲート内のSVMでS3オブジェクトストレージサーバを有効にすることができます。 "MetroClusterによるS3のサポート"	ONTAP 9.14.1
MetroClusterクラスタ内のミラーされたアグリゲートとミラーされていないアグリゲートでのS3バケットのプロビジョニングのサポート	MetroCluster構成では、ミラーされたアグリゲートまたはミラーされていないアグリゲートにバケットを作成できます。 "MetroCluster構成のミラーされたアグリゲートまたはミラーされていないアグリゲートにONTAP S3バケットを作成する"	ONTAP 9.14.1
MetroCluster IPおよびイーサネット接続ストレージ用の共有スイッチを使用したMetroCluster FCからMetroCluster IPへの移行	共有ストレージスイッチを使用して、MetroCluster FC構成からMetroCluster IP構成に無停止で移行できます。 "MetroCluster FC から MetroCluster IP 構成への無停止での移行（ONTAP 9.8 以降）"	ONTAP 9.13.1
8ノードMetroCluster FC構成からMetroCluster IP構成への無停止での移行	既存の8ノードMetroCluster FC構成から新しいMetroCluster IP構成に、ワークロードとデータを無停止で移行できます。 "MetroCluster FC構成からMetroCluster IP構成への無停止での移行"	ONTAP 9.13.1
スイッチオーバーとスイッチバックを使用した4ノードMetroCluster IP構成のアップグレード	スイッチオーバーとスイッチバックを使用して、4ノードMetroCluster IP構成のコントローラをアップグレードできます。 `system controller replace` コマンド "4ノードMetroCluster IP構成でのコントローラのアップグレード"	ONTAP 9.13.1

MetroCluster構成でサポートされる機能	概要 と詳細情報の入手方法	最初から利用可能です
環境のシャットダウン時にメディエーターアシスト自動計画外スイッチオーバー（MAUSO）がトリガーされる	環境のシャットダウンにより一方のサイトが正常にシャットダウンすると、MAUSOがトリガーされます。 "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"	ONTAP 9.13.1
8ノードMetroCluster IP構成のサポート	8ノードMetroCluster IP構成のコントローラとストレージをアップグレードするには、構成を拡張して一時的な12ノード構成にし、古いDRグループを削除します。 "4 ノード MetroCluster IP 構成を更新"	ONTAP 9.13.1
MetroCluster IP構成から共有ストレージMetroClusterスイッチ構成への変換	MetroCluster IP構成を共有ストレージMetroClusterスイッチ構成に変換できます。 "IP スイッチを交換します"	ONTAP 9.13.1
MetroCluster IP構成でのMetroCluster自動強制スイッチオーバー機能	MetroClusterの自動強制スイッチオーバー機能は、MetroCluster IP構成で有効にすることができます。この機能は、Mediator-Assisted Unplanned Switchover（MAUSO；メディエーターアシスト計画外スイッチオーバー）機能の拡張です。 "自動スイッチオーバーの制限事項"	ONTAP 9.12.1
MetroCluster IP構成のミラーされていないアグリゲート上のSVM上のS3	MetroCluster IP構成のミラーされていないアグリゲート上のSVMで、ONTAP Simple Storage Service（S3）オブジェクトストレージサーバを有効にすることができます。 "MetroClusterによるS3のサポート"	ONTAP 9.12.1
MetroCluster IPでのNVMeのサポート	NVMe/FCプロトコルは、4ノードMetroCluster IP構成でサポートされます。 "MetroCluster 環境のSAN構成"	ONTAP 9.12.1
MetroCluster IPおよびMetroClusterファブリック接続構成でのフロントエンドホストプロトコルのIPSecサポート	フロントエンドホストプロトコル（NFSやiSCSIなど）のIPSecサポートは、MetroCluster IPおよびMetroClusterファブリック接続構成で使用できます。 "ワイヤ暗号化を介した IP セキュリティ（ IPsec ）を設定します"	ONTAP 9.12.1

MetroCluster構成でサポートされる機能	概要 と詳細情報の入手方法	最初から利用可能です
MetroCluster FC構成からAFF A250またはFAS500f MetroCluster IP構成への移行	MetroCluster FC構成からAFF A250またはFAS500f MetroCluster IP構成に移行できます。 "ローカルクラスタ接続を移動します"	ONTAP 9.11.1
整合グループ	MetroCluster構成では整合グループがサポートされます。 "MetroCluster構成の整合グループ"	ONTAP 9.11.1
MetroCluster FC構成でのノードのコントローラアップグレードの簡易化	スイッチオーバーとスイッチバックを使用するアップグレードプロセスのアップグレード手順が簡易化されました。 "スイッチオーバーとスイッチバックを使用して、 MetroCluster FC 構成のコントローラをアップグレードします"	ONTAP 9.10.1
レイヤ3での共有リンクのIPサポート	MetroCluster IP設定は、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。 "レイヤ 3 ワイドエリアネットワークに関する考慮事項"	ONTAP 9.9.1
8ノードMetroCluster構成のサポート	永続的な8ノードクラスタは、IPおよびファブリック接続MetroCluster構成でサポートされます。 "MetroCluster コンポーネントを設置してケーブルを配線します"	ONTAP 9.9.1

MetroCluster IPプラットフォームおよびスイッチのサポートの新機能

MetroCluster IP プラットフォームとスイッチ サポートの新機能について説明します。

プラットフォームのサポート

MetroCluster IP構成でサポートされるプラットフォーム	最初から利用可能です
FAS50	ONTAP 9.16.1GA
AFF A20、AFF A30、AFF A50、AFF C30、AFF C60、AFF C80	ONTAP 9 .16.1
FAS70、FAS90	ONTAP 9.15.1P3
AFF A70、AFF A90、AFF A1K	ONTAP 9.15.1

MetroCluster IP構成でサポートされるプラットフォーム	最初から利用可能です
ASA A150、ASA A250、ASA A400、ASA A800 、ASA A900、 ASA C250、ASA C400、ASA C800	ONTAP 9.14.1
AFF A150	ONTAP 9.13.1 ONTAP 9.12.1P1 ONTAP 9.11.1P8 ONTAP 9.10.1P12
AFF C250、AFF C400、AFF C800	ONTAP 9.12.1P1 ONTAP 9 .13.1 GA
AFF A900 の略	ONTAP 9.10.1
AFF A250	ONTAP 9.8
FAS500f	ONTAP 9.8
ASA AFF A220 、 ASA AFF A250 、 ASA AFF A400 、 ASA AFF A700 、 ASA AFF A800	ONTAP 9.7
AFF A320	ONTAP 9.6P3
AFF A220、FAS2750	ONTAP 9.6
AFF A300、FAS8200	ONTAP 9.5

スイッチのサポート

BroadcomIPスイツチ	最初から利用可能です
BES-53248	ONTAP 9.6

Cisco IPスイッチ	最初から利用可能です
9336C-FX2 (12ポート)	ONTAP 9.14.1
9336C-FX2 (36ポート)	ONTAP 9.8
3132Q-V	ONTAP 9.6

Cisco IPスイッチ	最初から利用可能です
3232C	ONTAP 9.6

NVIDIAスイッチ	最初から利用可能です
同じNVIDIA SN2100スイッチ上の複数のMetroCluster IP構成	ONTAP 9.14.1
SN2100	ONTAP 9.12.1

MetroCluster FCプラットフォームとスイッチのサポートの新機能

MetroCluster FC プラットフォームとスイッチ サポートの新機能について説明します。

プラットフォームのサポート

MetroCluster FC構成でサポートされるプラットフォーム	最初から利用可能です
AFF A900 の略	ONTAP 9.10.1
ASA AFF A700およびASA AFF A400	ONTAP 9.7P5
AFF A400およびFAS8300	ONTAP 9.7
AFF A300 および FAS8200	ONTAP 9.5

スイッチのサポート

Brocade FCスイッチ	最初から利用可能です
G710	ONTAP 9.17.1
G720	ONTAP 9.8
G620-1、G630-1	ONTAP 9.8
G630	ONTAP 9.6

MetroCluster IP に対するONTAP Mediator サポートの新機能

ONTAP Mediator サポートの新しいMetroCluster IP 機能と拡張機能について説明します。

ONTAPメディエーターの各リリースの機能と拡張機能の詳細については、"ONTAPメディエーターの新機能"。

ONTAPメディエーター機能	最初から利用可能です
MetroCluster IP 構成では、 ONTAP Mediator 1.11 以降で IPv6 がサポートされます。 "MetroCluster IP構成用のONTAPメディエーターを設定する"	ONTAP 9.18.1
ONTAP Mediator 1.11 では、単一のONTAP Mediator インスタンスを使用して最大 10 個のMetroCluster IP 構成を管理するためのサポートが追加されました。 "MetroCluster IP構成にONTAPメディエーターをインストールする準備"	ONTAP 9.18.1
環境がシャットダウンした場合は、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）がサポートされます。 環境のシャットダウンにより一方のサイトが正常にシャットダウンすると、MAUSOがトリガーされます。 "ONTAPメディエーターが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 9.13.1
MetroCluster IP構成におけるONTAP Mediatorの初期サポート	ONTAP 9.7

MetroCluster Tiebreakerのサポートの新機能

MetroCluster Tiebreakerソフトウェアの機能拡張は、リリースごとに提供されます。MetroCluster Tiebreakerの最近のリリースの新機能は次のとおりです。

拡張機能

ONTAP Tiebreakerのバージョン	拡張機能
1.7	• バグ修正 • CLIを使用したスイッチオーバーシミュレーションのサポートを追加

1.6P1	• サポートライブラリの更新 • セキュリティの機能拡張
1.6	• インストールの容易さの向上 • サポートライブラリの更新 • セキュリティの機能拡張
1.5	• サポートライブラリの更新 • セキュリティの機能拡張
1.4	• サポートライブラリの更新

OSサポートマトリックス

次の表に、Tiebreakerの各バージョンでサポートされるオペレーティングシステムを示します。

TiebreakerノOS	1.7	1.6P1	1.6	1.5	1.4
Rocky Linux 9.4	はい。	はい。	いいえ	いいえ	いいえ
Rocky Linux 9.0	いいえ	いいえ	はい。	いいえ	いいえ
Rocky Linux 8.10	はい。	はい。	いいえ	いいえ	いいえ
Red Hat Enterprise Linux (RHEL) 9.6	はい。	はい。	いいえ	いいえ	いいえ
RHEL 9.5	はい。	はい。	いいえ	いいえ	いいえ
RHEL 9.4	はい。	はい。	いいえ	いいえ	いいえ
RHEL 9.3	いいえ	いいえ	いいえ	いいえ	いいえ
RHEL 9.2	はい。	はい。	はい。	いいえ	いいえ
RHEL 9.1	いいえ	いいえ	はい。	いいえ	いいえ
RHEL 9.0	いいえ	いいえ	はい。	いいえ	いいえ
RHEL 8.11～9.0	いいえ	いいえ	はい。	いいえ	いいえ

RHEL 8.10	はい。	はい。	はい。	いいえ	いいえ
RHEL 8.9	いいえ	いいえ	はい。	いいえ	いいえ
RHEL 8.8	はい。	はい。	はい。	いいえ	いいえ
RHEL 8.1～8.7	いいえ	いいえ	はい。	はい。	はい。
RHEL 7～7.9	いいえ	いいえ	いいえ	いいえ	はい。
CentOS 7-7.9	いいえ	いいえ	いいえ	いいえ	はい。

ファブリック接続 MetroCluster をインストール

概要

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

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

MetroCluster のインストールを準備

ONTAP MetroCluster 構成の違い

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

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

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

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

- メモ *

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

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

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

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

クラスタピアリング

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

す。

関連情報

"クラスタと SVM のピアリングの簡単な設定"

クラスタピアリングの前提条件

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

接続要件

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

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

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

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

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

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

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

ポート要件

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

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

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

- クラスタ間通信で使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す。

専用のポートを使用する場合の考慮事項

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

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

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

  ポートの帯域幅は、すべての VLAN とベースポートで共有されます。

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

データポートを共有する場合の考慮事項

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

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

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

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

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

ISL に関する考慮事項

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

ISL の共有に関する考慮事項（ **ONTAP 9.2** ）

ONTAP 9.2 以降では、次の場合に ISL を共有できます。

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

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

構成に必要な ISL の数を決定する際は、次の点を考慮してください。

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

す。

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

  "NetApp Hardware Universe の略"

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

プラットフォーム固有の **ISL** に関する考慮事項

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

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

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

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

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

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

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

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

"NetApp Hardware Universe の略"

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

スイッチ	MetroCluster 構成を IOD に設定する	OOD の MetroCluster 設定を行います
Brocade	• AptPolicy を 1 に設定する必要があります • DLS を off に設定します • IOD を on に設定する必要があります	• AptPolicy を 3 に設定する必要があります • DLS は ON に設定する必要があります • IOD を off に設定する必要があります
シスコ	FCVI 用 VSAN のポリシー： • ロードバランシングポリシー： srcid 、 dstid • IOD を on に設定する必要があります ストレージ用 VSAN のポリシー： • ロードバランシングポリシー： srcid 、 dstid 、 oxid • VSAN で in-order-guarantee オプションを設定しないでください	該当なし

IOD を使用する状況

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

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

OOD を使用する状況

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

暗号化デバイスを使用する

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

- 該当する FC スイッチのベンダーの認定を受けた外部暗号化デバイスまたは WDM 機器を使用する必要があります。

  動作モード（トランキングや暗号化など）に対応した認定が必要です。

- 暗号化によるレイテンシが 10 マイクロ秒以下である必要があります。

Brocade DCX 8510-8 スイッチを使用するための要件

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

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

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

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



このスイッチには RCF ファイルはありません。

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

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

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

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

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

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

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

ミラーされていないアグリゲートを使用する場合の

ミラーされていないアグリゲートを使用する場合の

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

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

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

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

ミラーされていないアグリゲートと階層状のネームスペースに関する考慮事項

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

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

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

ミラーされていないアグリゲートと **SVM** に関する考慮事項

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

ミラーされていないアグリゲートと **SAN** に関する考慮事項

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

MetroCluster サイトでのファイアウォールの使用状況

MetroCluster サイトでのファイアウォールの使用に関する考慮事項

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

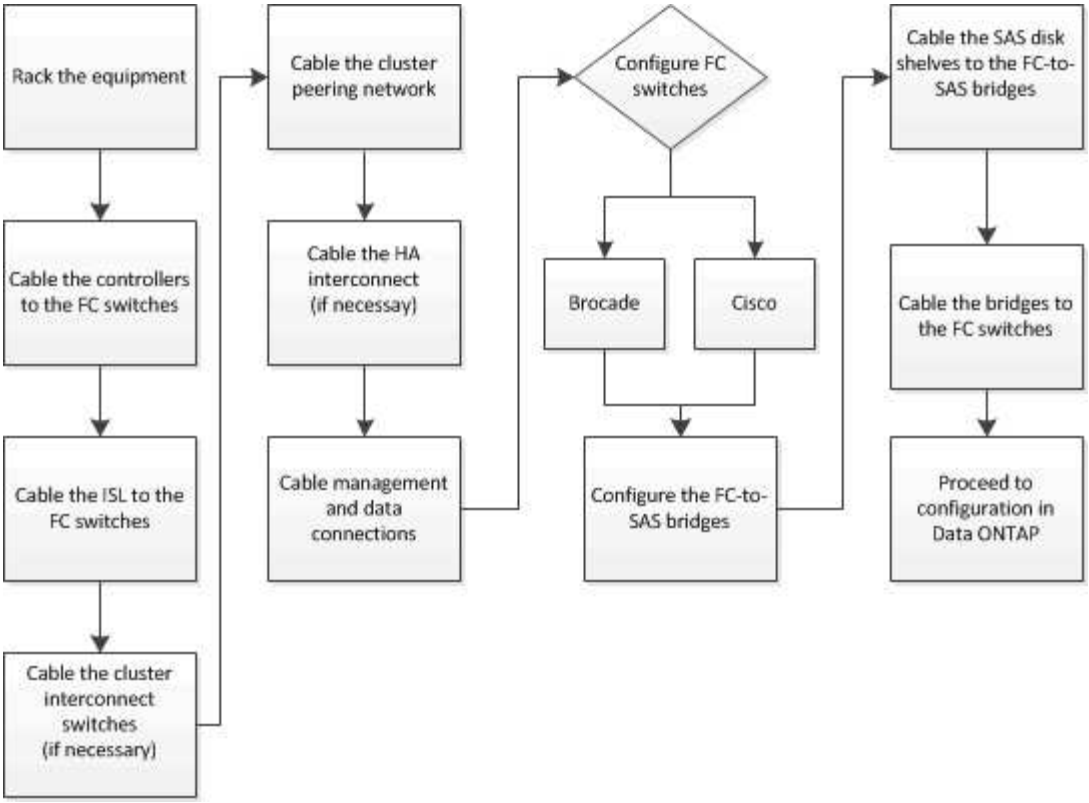
次の表は、 2 つの MetroCluster サイト間に配置された外部ファイアウォールでの TCP/UDP ポートの使用状況を示しています。

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

ファブリック接続 **MetroCluster** 構成をケーブル接続

ファブリック接続 **MetroCluster** 構成のケーブル接続

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



ファブリック **MetroCluster** 構成のコンポーネント

ファブリック **MetroCluster** 構成のコンポーネント

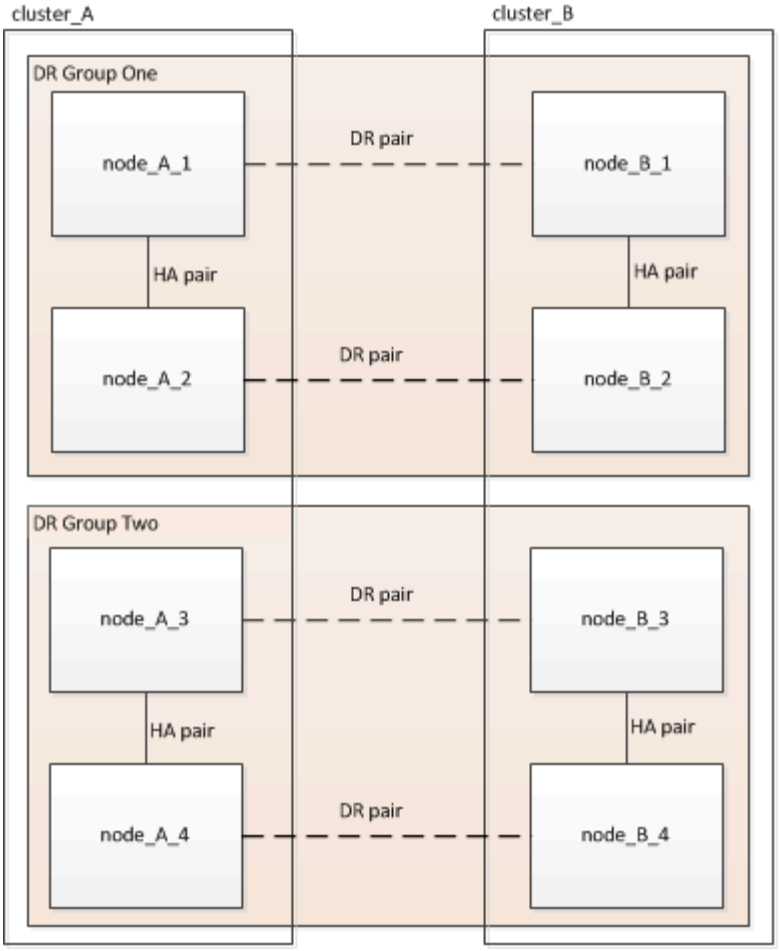
MetroCluster 構成を計画するときは、ハードウェアコンポーネントとその相互接続について理解しておく必要があります。

ディザスタリカバリ（ **DR** ）グループ

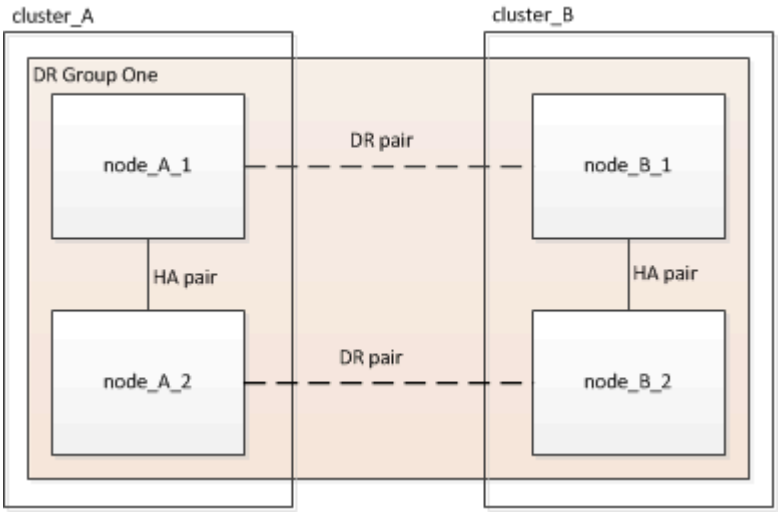
ファブリック MetroCluster 構成は、 MetroCluster 構成のノード数に応じて、 1 つまたは 2 つの DR グループで構成されます。各 DR グループは 4 つのノードで構成されます。

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

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



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



主要なハードウェア要素

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

- ストレージコントローラ

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

- FC-to-SAS ブリッジ

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

- FC スイッチ

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

- クラスタピアリングネットワーク

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

8 ノードのファブリック **MetroCluster** 構成

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

8 ノード構成には次の接続が含まれます。

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

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

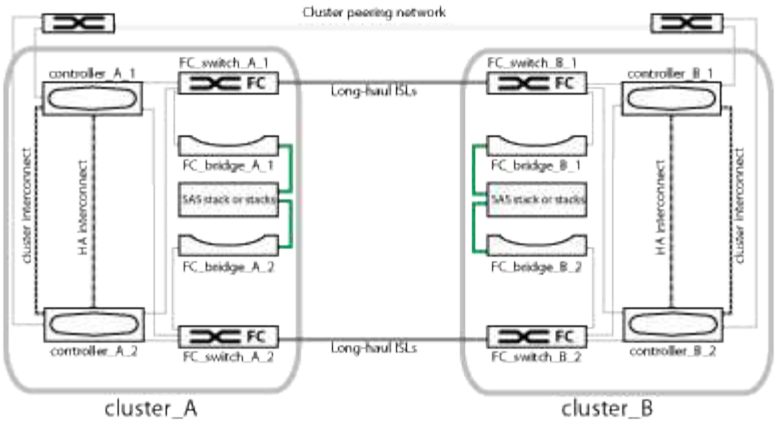
- コントローラからクラスタピアリングに使用されるお客様ネットワークへのイーサネット接続

  SVM の設定はクラスタピアリングネットワーク経由でレプリケートされます。

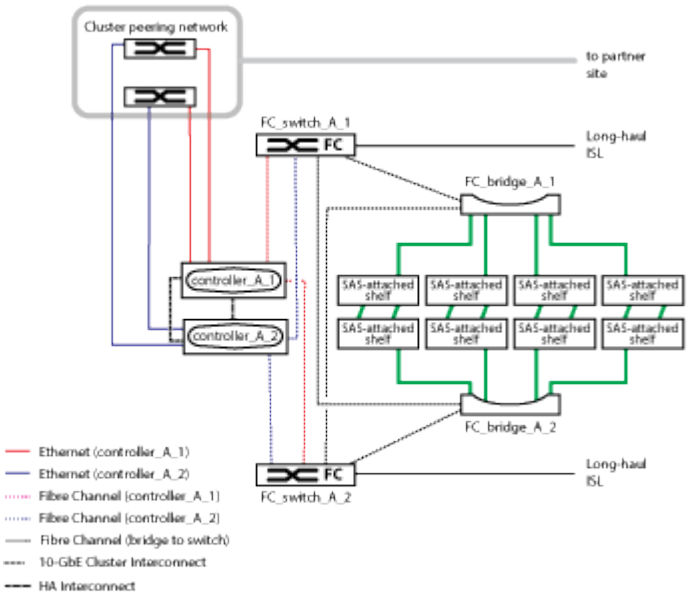
- ローカルクラスタの各コントローラ間のクラスタインターコネクト

4 ノードのファブリック **MetroCluster** 構成

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

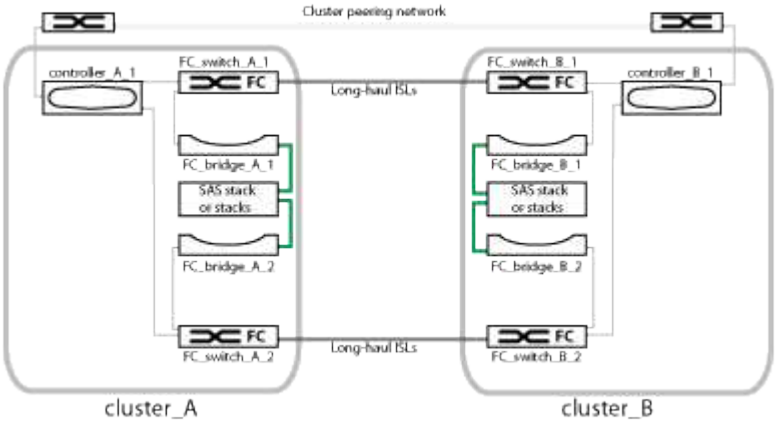


次の図は、単一の MetroCluster クラスタ（両方のクラスタの構成が同じ）内の接続をより詳細に示したものです。



2 ノードのファブリック **MetroCluster** 構成

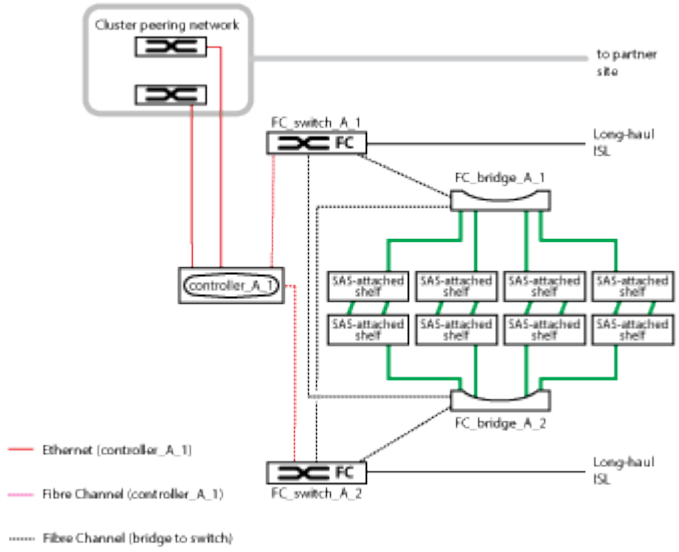
次の図は、 2 ノードのファブリック MetroCluster 構成を単純化したものです。一部の接続では、コンポーネント間の複数の冗長接続を 1 本の線で表しています。データネットワーク接続と管理ネットワーク接続は表示されません。



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

2 ノード構成では、ノードが HA ペアとして構成されません。

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



2 ノード構成には次の接続が含まれます。

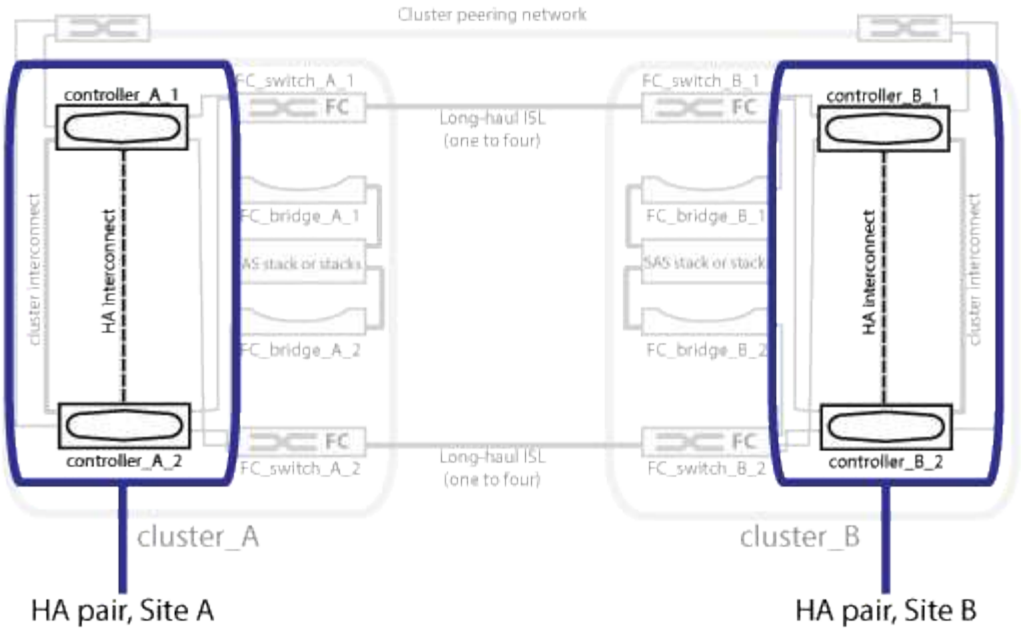
- 各コントローラモジュールの FC-VI アダプタ間の FC 接続
- 各コントローラモジュールの HBA から各 SAS シェルフスタックの FC-to-SAS ブリッジへの FC 接続
- 各 SAS シェルフ間および各スタックの上下から FC-to-SAS ブリッジへの SAS 接続
- コントローラからクラスタピアリングに使用されるお客様ネットワークへのイーサネット接続

  SVM の設定はクラスタピアリングネットワーク経由でレプリケートされます。

MetroCluster 構成のローカル **HA** ペアの図

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

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



関連情報

"冗長 FC-to-SAS ブリッジの図"

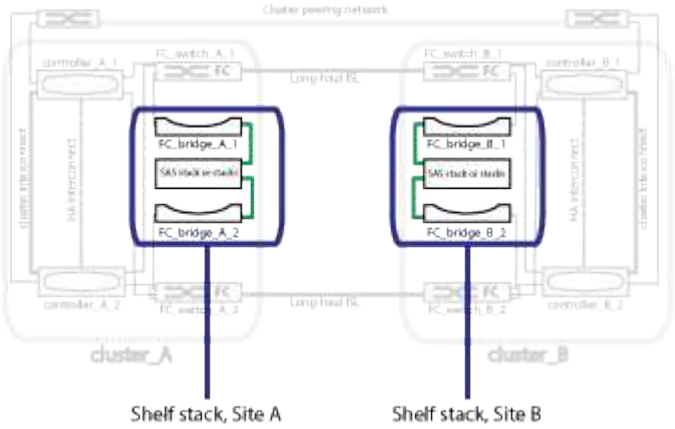
"冗長 FC スイッチファブリック"

"クラスタピアリングネットワークの図"

"ONTAP の概念"

冗長 **FC-to-SAS** ブリッジの図

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



関連情報

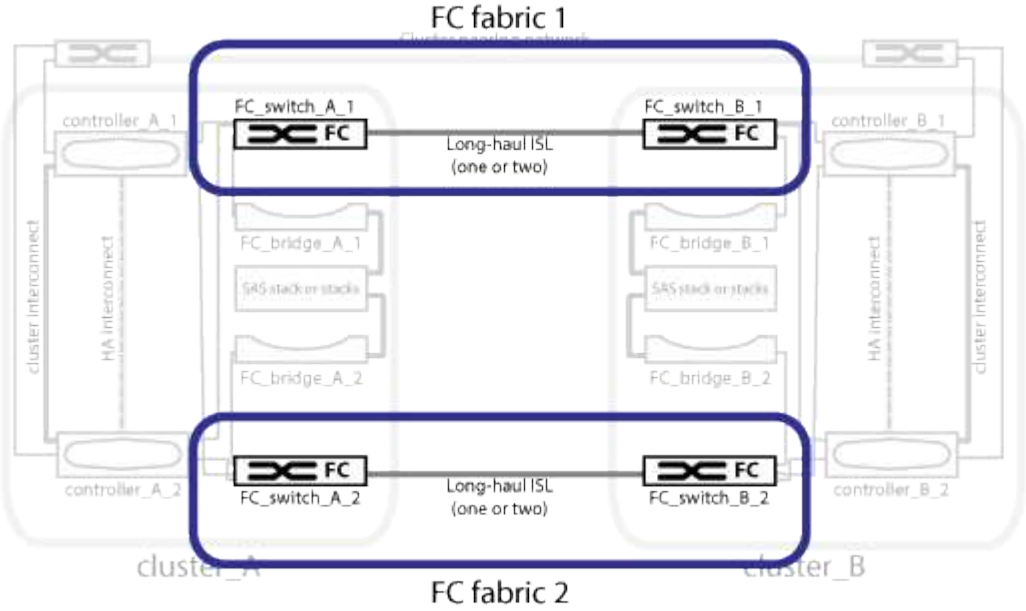
"MetroCluster 構成のローカル HA ペアの図"

"冗長 FC スイッチファブリック"

"クラスタピアリングネットワークの図"

冗長 **FC** スイッチファブリック

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



関連情報

"MetroCluster 構成のローカル HA ペアの図"

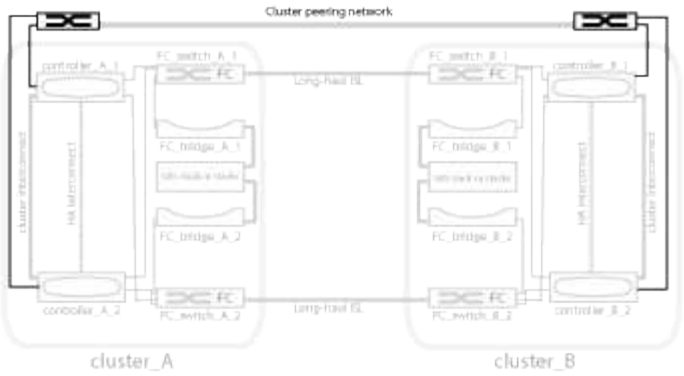
"冗長 FC-to-SAS ブリッジの図"

"クラスタピアリングネットワークの図"

クラスタピアリングネットワークの図

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

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



関連情報

"MetroCluster 構成のローカル HA ペアの図"

"冗長 FC-to-SAS ブリッジの図"

"冗長 FC スイッチファブリック"

"クラスタと SVM のピアリングの簡単な設定"

"クラスタピアリングの設定に関する考慮事項"

"クラスタピアリングのケーブル接続"

"クラスタをピアリング"

必要な **MetroCluster FC** コンポーネントと命名規則

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

サポートされているソフトウェアおよびハードウェア

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

"NetApp Hardware Universe の略"

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

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

MetroCluster FC 構成でのハードウェアの冗長性

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

ちらかを表す番号として 1 または 2 を使用します。

ONTAP クラスタ **× 2**

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

名前は MetroCluster 構成内で一意である必要があります。

名前の例：

- サイト A ： cluster_A
- サイト B ： cluster_B

FC スイッチ **× 4**

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

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

名前は MetroCluster 構成内で一意である必要があります。

コントローラモジュール **× 2** 、 **4** 、または **8**

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

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

コントローラモジュールの要件は次のとおりです。

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

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

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

  一部のコントローラモジュールは、次の 2 つのオプションに対応しています。

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

名前の例：

- サイト A ： controller_A_1
- サイト B ： controller_B_1

クラスタインターコネクトスイッチ **× 4**

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

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

FC-to-SAS ブリッジの要件

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

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

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

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

プールとドライブの要件（最小サポート）

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

MetroCluster 構成では、各サイトに最小構成が必要です。

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

  たとえば、各サイトにノードが 2 つある 4 ノード MetroCluster 構成では、各サイトにプールが 4 つ必要です。

- 各プールに少なくとも 7 本のドライブ。

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

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

- ルートドライブ × 3 本

- 3 本のデータドライブ
- スペアドライブ x 1 本

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

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

空きのあるシェルフでのドライブの配置場所に関する考慮事項

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

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

ブリッジの命名規則

ブリッジでは、次のような命名規則を使用します。

ペア内の 'bridge_site_stack グループ・ロケーション

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

各サイトの 1 つのスタックグループのブリッジ名の例：

- bridge_A_1a
- bridge_A_1b
- bridge_B_1a
- bridge_B_1b

FC スイッチおよび FC-to-SAS ブリッジの設定ワークシート

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

"サイト A のワークシート"

"サイト B のワークシート"

MetroCluster コンポーネントを設置してケーブルを配線します

ラックにハードウェアコンポーネントを配置

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

このタスクについて

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

手順

1. MetroCluster コンポーネントの配置を計画します。

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

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

   "ONTAPハードウェアシステムのドキュメント"

4. FC スイッチをラックまたはキャビネットに設置します。
5. ディスクシェルフを設置し、電源を投入して、シェルフ ID を設定します。
   - 各ディスクシェルフの電源を再投入する必要があります。
   - 各 MetroCluster DR グループ（両サイトを含む）で、各 SAS ディスクシェルフのシェルフ ID が一意である必要があります。
6. 各 FC-to-SAS ブリッジを設置します。

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

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

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

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

b. 各ブリッジを、適切なアースを提供する電源に接続します。

c. 各ブリッジの電源をオンにします。

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

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

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

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

手順

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

MetroCluster サイト間での **ISL** のケーブル接続

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

このタスクについて

両方のスイッチファブリックに対して実行する必要があります。

手順

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

関連情報

"ISL に関する考慮事項"

FCスイッチのポート割り当て

MetroCluster FCスイッチのポート割り当て

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

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

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

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

ケーブル接続の全体的なガイドライン

ケーブル接続の表を使用する際は、次の点に注意してください。

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

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

  これらのポートは空にしておくことができます。

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

  "ISL に関する考慮事項"

AFF A900および**FAS9500**の配線ガイドライン

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

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

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

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

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

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

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

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

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

これらの表を使用する前に、次の情報を確認してください。

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

MetroCluster 1またはDRグループ1

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

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

* コンポーネント *	* ポート *	* FC スイッチに接続 *	6505、G610、G710 ポート	6510、DCX 8510-8 ポート	6520ポート	7810ポート	7840ポート	G620、G620-1、G630、G630-1 ポート	G720、G730 ポート
N/A	N/A	17	3.	FC-VI-2 ポート d	2.	17	21	N/A	N/A
N/A	17	3.	HBA ポート A	1.	2.	2.	2.	2.	2.
2.	8.	HBA ポート b	2.	2.	2.	2.	2.	2.	2.
8.	HBA ポート c	1.	3.	3.	3.	3.	3.	3.	9.
HBA ポート d	2.	3.	3.	3.	3.	3.	3.	9.	controller_x_2
FC-VI ポート a	1.	4.	4.	4.	4.	4.	4.	4.	FC-VI ポート b
2.	4.	4.	4.	4.	4.	4.	4.	FC-VI ポート c	1.
5.	5.	5.	5.	5.	5.	5.	FC-VI ポート d	2.	5.
5.	5.	5.	5.	5.	5.	FC-VI-2 ポート A	1.	18	22
N/A	N/A	N/A	20	6.	FC-VI-2 ポート b	2.	18	22	N/A
N/A	N/A	20	6.	FC-VI-2 ポート c	1.	19	23	N/A	N/A
N/A	21	7.	FC-VI-2 ポート d	2.	19	23	N/A	N/A	N/A
21	7.	HBA ポート A	1.	6.	6.	6.	6.	6.	6.
12.	HBA ポート b	2.	6.	6.	6.	6.	6.	6.	12.

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

MetroCluster 2または**DR**グループ**2**

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

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

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

MetroCluster 3 または **DR** グループ **3**

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

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

MetroCluster 4 または **DR** グループ **4**

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

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

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

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

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

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

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

MetroCluster 1または**DR**グループ**1**

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

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

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

* コンポーネント *		* ポート *	* FC スイッチに接続 *	6505、G610、G710 ポート	6510、DCX 8510-8 ポート	6520ポート	7810ポート	7840ポート	G620、G620-1、G630、G630-1 ポート	G720、G730 ポート
9.	9.	9.	9.	9.	11.	スタック 2	bridge_x_2a	fc1	1.	10.
10.	10.	10.	10.	10.	14	FC2	2.	10.	10.	10.
10.	10.	10.	14	bridge_x_2b	fc1	1.	11.	11.	11.	11.
11.	11.	15	FC2	2.	11.	11.	11.	11.	11.	11.

MetroCluster 2またはDRグループ2

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

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

* コンポーネント *		* ポート *	* FC スイッチに接続 *	6505、G610、G710 ポート	6510、DCX 8510-8 ポート	6520ポート	7810ポート	7840ポート	G620、G620-1、G630、G630-1 ポート	G720、G730 ポート
スタック 1	bridge_x_1a	fc1	1.	N/A	32	56	N/A	20	26	32
FC2	2.	N/A	32	56	N/A	20	26	32	bridge_x_1b	fc1
1.	N/A	33	57	N/A	21	27	33	FC2	2.	N/A

* コンポーネント *		* ポート *	* FC スイッチに接続 *	6505、G610、G710 ポート	6510、DCX 8510-8 ポート	6520ポート	7810ポート	7840ポート	G620、G620-1、G630、G630-1 ポート	G720、G730 ポート
33	57	N/A	21	27	33	スタック 2	bridge_x_2a	fc1	1.	N/A
34	58	N/A	22	30	34	FC2	2.	N/A	34	58
N/A	22	30	34	bridge_x_2b	fc1	1.	N/A	35	59	N/A
23	31.	35	FC2	2.	N/A	35	59	N/A	23	31.

MetroCluster 3 または **DR** グループ **3**

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

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

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

MetroCluster 4 または **DR** グループ **4**

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

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

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

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

MetroCluster 1または**DR**グループ**1**

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

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

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

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

MetroCluster 2またはDRグループ2

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

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

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

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

MetroCluster 3 または **DR** グループ **3**

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

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

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

MetroCluster 4 または **DR** グループ **4**

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

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

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

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

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

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

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

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

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

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

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

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

MetroCluster 1またはDRグループ1

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

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

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

MetroCluster 2または**DR**グループ**2**

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

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

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

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

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

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

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

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

MetroCluster 1または**DR**グループ**1**

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

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

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

* コンポーネント *		* ポート *	* FC スイッチに接続 *	9124Vポート	9148Sポート	9148Vポート	9250i ポート	9396Sポート
10.	18	10.	10.	スタック 2	bridge_x_2a	fc1	1.	19
11.	19	11.	11.	FC2	2.	19	11.	19
11.	11.	bridge_x_2b	fc1	1.	20	12.	20	12.
12.	FC2	2.	20	12.	20	12.	12.	スタック 3
bridge_x_3a	fc1	1.	21	13	21	13	13	FC2
2.	21	13	21	13	13	bridge_x_3b	fc1	1.
22	14	22	14	14	FC2	2.	22	14
22	14	14	スタック4	bridge_x_4a	fc1	1.	23	15
23	15	15	FC2	2.	23	15	23	15
15	bridge_x_4b	fc1	1.	24	16	24	16	16

MetroCluster 2または**DR**グループ**2**

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

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

* コンポーネント *		* ポート *	* FC スイッチに接続 *	9124Vポート	9148Sポート	9148Vポート	9250i ポート	9396Sポート
スタック 1	bridge_x_1a	fc1	1.	N/A	33	41.	N/A	57

* コンポーネント *		* ポート *	* FC スイッチに接続 *	9124Vポート	9148Sポート	9148Vポート	9250i ポート	9396Sポート
FC2	2.	N/A	33	41.	N/A	57	bridge_x_1b	fc1
1.	N/A	34	42	N/A	58	FC2	2.	N/A
34	42	N/A	58	スタック 2	bridge_x_2a	fc1	1.	N/A
35	43	N/A	59	FC2	2.	N/A	35	43
N/A	59	bridge_x_2b	fc1	1.	N/A	36	44	N/A
60	FC2	2.	N/A	36	44	N/A	60	スタック 3
bridge_x_3a	fc1	1.	N/A	37	45	N/A	61	FC2
2.	N/A	37	45	N/A	61	bridge_x_3b	fc1	1.
N/A	38	46	N/A	62	FC2	2.	N/A	38
46	N/A	62	スタック4	bridge_x_4a	fc1	1.	N/A	39
47	N/A	63	FC2	2.	N/A	39	47	N/A
63	bridge_x_4b	fc1	1.	N/A	40	48	N/A	64

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

MetroCluster 1または**DR**グループ**1**

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

"Cisco FC スイッチを手動で設定"

ケーブルテーブルを使用するときは、次の点に注意してください。

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

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

MetroCluster 2または**DR**グループ**2**

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

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

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

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

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

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

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

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

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

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

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

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

MetroCluster 1またはDRグループ1

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

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

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

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

MetroCluster 2または**DR**グループ**2**

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

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

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

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

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

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

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

MetroCluster 1またはDRグループ1

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

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

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

MetroCluster 2または**DR**グループ**2**

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

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

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

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

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

次の表に、Cisco 9132TスイッチでのISLポートの用途を示します。

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

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

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

このタスクについて

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

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

ステップ

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

関連情報

"ONTAPハードウェアシステムのドキュメント"

"ネットワークと LIF の管理"

クラスタピアリングのケーブル接続

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

このタスクについて

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

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

ポートおよびネットワーク接続の推奨される最小帯域幅は 1GbE です。

ステップ

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

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

関連情報

"クラスタと SVM のピアリングの簡単な設定"

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

"クラスタピアリング"

HA インターコネクトのケーブル接続

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

このタスクについて

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

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

手順

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

   "ONTAPハードウェアシステムのドキュメント"

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

管理ポートとデータポートのケーブル接続

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

このタスクについて

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

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

ステップ

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

   "ONTAPハードウェアシステムのドキュメント"

FC スイッチを設定

FCスイッチの設定の概要

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

状況	使用する手順
要件を満たすRCFを用意する	• "RCF ファイルを使用して Brocade FC スイッチを設定します" • "RCFファイルによるCisco FCスイッチの設定"
RCFがないか、要件を満たしていないRCFがある	• "Brocade FC スイッチを手動で設定" • "Cisco FC スイッチを手動で設定"

RCF ファイルを使用して Brocade FC スイッチを設定します

Brocade FC スイッチを工場出荷時のデフォルトにリセット

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

このタスクについて

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

手順

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

   「 fosconfig options 」を参照してください

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

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

   'witchcfgpersistentdisable

```
FC_switch_A_1:admin> switchcfgpersistentdisable
```

5. 設定を無効にします。

   「 cfgDisable 」

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

6. 設定をクリアします。

   「 cfgClear 」

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

7. 設定を保存します。

   cfgsave

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

8. デフォルトの設定を行います。

   「 configDefault 」

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

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

   `portcfgdefault_port-number_`

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

   この手順はポートごとに実行する必要があります。

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

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

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

a. ライセンスコマンドを実行します。

`licenseport --show`。

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

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

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

c. ライセンスコマンドを実行します。

`licenseport --show`。

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

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

licenseport — メソッドの動的

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

11. スイッチをリブートします。

「 Fastboot 」を参照してください

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

12. デフォルト設定が実装されたことを確認します。

    'witchshow'

13. IP アドレスが正しく設定されていることを確認します。

    ipAddrShow

    必要に応じて、次のコマンドで IP アドレスを設定できます。

    ipAddrSet

Brocade FC スイッチの RCF ファイルのダウンロード

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

このタスクについて

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

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

手順

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

   RCF ファイルを正しいスイッチに適用する必要があります。

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

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

3. 構成内のスイッチごとに上記の手順を繰り返します。

Brocade FC スイッチの RCF ファイルをインストールします

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

このタスクについて

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

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

手順

1. ダウンロードと設定のプロセスを開始します。

   「 configDownload 」

   次の例に示すようにプロンプトに応答します。

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

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

2. 構成ファイルでスイッチドメインが設定されていることを確認します。

   'witchshow'

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

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

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

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

A_2	6.	B_2

4. ポート速度を変更します。

   「 portcfgspeed 」

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

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

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

5. ISL の距離を計算します。

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

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

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

6. ISL ポートごとに距離を設定します。

   `longdistance_port level vc_link_init__ distance_ddistance` *`value`*

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

   例： ls

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

   例： LE

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

7. スイッチを永続的に有効にします。

   'witchcfgpersistentenable

   次の例は、 FC switch_A_1 を永続的に有効にします。

```
FC_switch_A_1:admin> switchcfgpersistentenable
```

8. IP アドレスが正しく設定されていることを確認します。

   ipaddrshow

```
FC_switch_A_1:admin> ipAddrshow
```

   必要に応じて、 IP アドレスを設定できます。

   ipAddrSet

9. スイッチのプロンプトでタイムゾーンを設定します。

   tstimezone — 対話型

   プロンプトに対してと入力します。

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

10. スイッチをリブートします。

    「再起動」

    次の例は、 FC switch_A_1 をリブートします。

```
FC_switch_A_1:admin> reboot
```

11. 距離設定を確認します。

    portbuffershow

    LE の距離設定は 10 km と表示されます

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

12. ISL ケーブルを、取り外したスイッチのポートに再接続します。

    工場出荷時の設定にリセットすると、 ISL ケーブルは切断されています。

    "Brocade FC スイッチを工場出荷時のデフォルトにリセット"

13. 構成を検証

    a. スイッチが 1 つのファブリックを形成することを確認します。

       'witchshow'

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

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

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

    b. ファブリックの設定を確認します。

       「 fabricshow` 」

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

c. ISL が機能していることを確認します。

「 islshow` 」

```
FC_switch_A_1:admin> islshow
```

d. ゾーニングが正しくレプリケートされたことを確認します。

「 cfgshow 」＋「 zoneshow 」と入力します

両方の出力に、両方のスイッチの同じ設定情報とゾーニング情報が表示されます。

e. トランキングを使用する場合は、トランキングを確認します。

「トラクショー」

```
FC_switch_A_1:admin> trunkshow
```

RCF ファイルを使用して Cisco FC スイッチを設定します

Cisco FC スイッチを工場出荷時のデフォルトにリセット

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

このタスクについて

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

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

手順

1. スイッチを工場出荷時のデフォルトにリセットします。

   a. 既存の設定を消去します :**+write erase**

   b. スイッチ・ソフトウェアをリロードします **+reload**

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

   c. 設定ウィザードで、スイッチの基本設定を入力します。

      - 管理パスワード
      - スイッチ名
      - アウトオブバンド管理設定

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

  設定ウィザードが完了すると、スイッチがリブートします。

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

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

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

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

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

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

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

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

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

最後の一連のプロンプトで設定が完了します。

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

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

Use this configuration and save it? (yes/no) [y]:
2017 Jun 13 21:24:43 A1 %$ VDC-1 %$ %COPP-2-COPP_POLICY: Control-Plane
is protected with policy copp-system-p-policy-strict.

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

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

2. 設定を保存します。

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

3. スイッチをリブートし、スイッチがリロードされるまで待ちます。

```
IP_switch_A_1# reload
```

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

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

作業を開始する前に

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

このタスクについて

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

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

"NetApp Hardware Universe の略"

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

手順

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

   "シスコのダウンロードページ"

2. スイッチソフトウェアをスイッチにコピーします。

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

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

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

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

   「 IR ブートフラッシュ」

   次の例は ' ファイルが ip_switch _a_1' に存在することを示しています

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

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

4. スイッチソフトウェアをインストールします。

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

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

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

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

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

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

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

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

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

5. スイッチがリロードされるまで待ってから、スイッチにログインします。

   スイッチがリブートされると、ログインプロンプトが表示されます。

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

The switch software is now installed.
```

6. スイッチソフトウェアがインストールされたことを確認します。

   'how version （バージョンの表示）'

   次の例は、の出力を示しています。

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

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


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

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

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

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

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

plugin
  Core Plugin, Ethernet Plugin
IP_switch_A_1#
```

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

Cisco FC RCF ファイルのダウンロードとインストール

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

作業を開始する前に

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

このタスクについて

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

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

"NetApp Hardware Universe の略"

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

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

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

手順

1. Cisco FC の RCF ファイルをからダウンロードします "MetroCluster の RCF ダウンロードページ"。
2. RCF ファイルをスイッチにコピーします。

   a. RCF ファイルを最初のスイッチにコピーします。

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

      この例では 'NX32323_v1.80_Switch-A1.txt 'RCF ファイルが '10.10.99.99' の SFTP サーバからローカルブートフラッシュにコピーされます使用する TFTP / SFTP サーバの IP アドレスと、インストールする必要がある RCF ファイルのファイル名を使用する必要があります。

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

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

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

「 IR bootflash: 」のように表示されます

次の例は、 FC_switch_A_1 にファイルが存在することを示しています。

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

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

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

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

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

'copy running-config startup-config

次のような出力が表示されます。

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

6. スイッチをリロードします。

「再ロード」

```
IP_switch_A_1# reload
```

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

Brocade FC スイッチを手動で設定

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

作業を開始する前に

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

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

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

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

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

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

このタスクについて

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

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

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

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

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

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

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

Brocade のライセンス要件を確認する

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

このタスクについて

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

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

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

ステップ

1. ライセンスがインストールされていることを確認します。

Fabric OS 8.2.x以前の場合

コマンドを実行します `licenseshow`。

Fabric OS 9.0以降の場合

コマンドを実行します `license --show`。

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

Brocade FCスイッチの値を工場出荷時のデフォルトに設定する

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

このタスクについて

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

手順

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

   'witchcfgpersistentdisable

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

   次の例は、 BrocadeSwitchA に対するコマンドを示しています。

   ```
   BrocadeSwitchA:admin> switchcfgpersistentdisable
   ```

   次の例は、 BrocadeSwitchB に対するコマンドを示しています。

   ```
   BrocadeSwitchB:admin> switchcfgpersistentdisable
   ```

3. スイッチ名を設定します。

   'witchname switch_name

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

   次の例は、 BrocadeSwitchA に対するコマンドを示しています。

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

次の例は、 BrocadeSwitchB に対するコマンドを示しています。

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

4. すべてのポートをデフォルト値に設定します。

   portcfgdefault

   スイッチ上のすべてのポートに対して実行する必要があります。

   次の例は、 FC_switch_A_1 に対するコマンドを示しています。

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

   次の例は、 FC_switch_B_1 に対するコマンドを示しています。

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

5. ゾーニング情報を消去します。

   cfgdisable

   cfgclear

   cfgsave

   次の例は、 FC_switch_A_1 に対するコマンドを示しています。

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

   次の例は、 FC_switch_B_1 に対するコマンドを示しています。

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

6. スイッチの一般的な設定をデフォルトに設定します。

   「 configdefault 」

   次の例は、 FC_switch_A_1 に対するコマンドを示しています。

```
FC_switch_A_1:admin> configdefault
```

   次の例は、 FC_switch_B_1 に対するコマンドを示しています。

```
FC_switch_B_1:admin> configdefault
```

7. すべてのポートを非トランキングモードに設定します。

   'witchcfgtrunk 0`

   次の例は、 FC_switch_A_1 に対するコマンドを示しています。

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

   次の例は、 FC_switch_B_1 に対するコマンドを示しています。

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

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

   「 fosconfig options 」を参照してください

   次の例は、 FC_switch_A_1 に対するコマンドを示しています。

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

   次の例は、 FC_switch_B_1 に対するコマンドを示しています。

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

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

次の例は、 FC_switch_A_1 に対するコマンドを示しています。

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

次の例は、 FC_switch_B_1 に対するコマンドを示しています。

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

10. スイッチをリブートします。

「再起動」

次の例は、 FC_switch_A_1 に対するコマンドを示しています。

```
FC_switch_A_1:admin> reboot
```

次の例は、 FC_switch_B_1 に対するコマンドを示しています。

```
FC_switch_B_1:admin> reboot
```

基本的なスイッチ設定を構成する

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

このタスクについて

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

この手順では、次の例に示すように、スイッチごとに一意のドメイン ID を設定します。この例では、ドメイン ID 5 と 7 が fabric_1 を形成し、ドメイン ID 6 と 8 が fabric_2 を形成します。

- FC_switch_A_1 をドメイン ID 5 に割り当てます
- FC_switch_A_2 はドメイン ID 6 に割り当てられています
- FC_switch_B_1 をドメイン ID 7 に割り当てます
- FC_switch_B_2 をドメイン ID 8 に割り当て

手順

1. コンフィギュレーションモードを開始します。

「 configure 」を実行します

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

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

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

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

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

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

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

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

   a. フレームの IOD を設定するには、各スイッチファブリックで次の手順を実行する必要があります。
      i. IOD を有効にします。

         「 iodset 」

      ii. Advanced Performance Tuning （ APT ；高度なパフォーマンスチューニング）ポリシーを 1 に設定します。

         「 aptpolicy 1 」

      iii. 動的負荷共有（ DLS ）を無効にします。

         「 lsreset 」と表示されます

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

たとえば、 FC_switch_A_1 で次のコマンドを問題に実行します。

```
FC_switch_A_1:admin> iodshow
    IOD is set

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

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

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

i. 2 つ目のスイッチファブリックで、上記の手順を繰り返します。

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

i. OOD を有効にします。

「 iodreset 」

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

「 aptpolicy 3 」

iii. 動的負荷共有（ DLS ）を無効にします。

「 lsreset 」と表示されます

iv. OOD 設定を確認します。

「 iodshow 」

「 aptpolicy 」と入力します

「 llsshow 」

たとえば、 FC_switch_A_1 で次のコマンドを問題に実行します。

```
FC_switch_A_1:admin> iodshow
    IOD is not set

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


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

i. 2 つ目のスイッチファブリックで、上記の手順を繰り返します。

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

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

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

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

a. ライセンスコマンドを実行します。

```
licenseport --show
```

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

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

b. root ユーザを有効にします。

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

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

c. ライセンスコマンドを実行します。

`license --show -port`

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

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

licenseport — メソッドの動的

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

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

a. T11-FC-ZONE-SERVER-MIB を有効にします。

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

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

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

c. 2 つ目のスイッチファブリックで、ここまでの手順を繰り返します。

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

a. 既存のコミュニティストリングを変更します。

'mpconfig — set snmpv1'

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

c. 目的のコミュニティストリングを入力します。

FC_switch_A_1 では、次のコマンドを実行します。

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

FC_switch_B_1 では、次のコマンドを実行します。

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

7. スイッチをリブートします。

「再起動」

FC_switch_A_1 では、次のコマンドを実行します。

```
FC_switch_A_1:admin> reboot
```

FC_switch_B_1 では、次のコマンドを実行します。

```
FC_switch_B_1:admin> reboot
```

8. スイッチを永続的に有効にします。

'witchcfgpersistentenable

FC_switch_A_1 では、次のコマンドを実行します。

```
FC_switch_A_1:admin> switchcfgpersistentenable
```

FC_switch_B_1 では、次のコマンドを実行します。

```
FC_switch_B_1:admin> switchcfgpersistentenable
```

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

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

このタスクについて

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

- FC_switch_A_1 をドメイン ID 5 に割り当てます
- FC_switch_A_2 はドメイン ID 6 に割り当てられています
- FC_switch_B_1 をドメイン ID 7 に割り当てます
- FC_switch_B_2 をドメイン ID 8 に割り当て

この例では、ドメイン ID 5 と 7 が fabric_1 を形成し、ドメイン ID 6 と 8 が fabric_2 を形成します。

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

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

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

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

手順

1. コマンドモードを開始します。

   「 configure 」を実行します

2. プロンプトに従って次の手順に進みます。

   a. スイッチのドメイン ID を設定します。

   b. 「 RDP Polling Cycle 」というプロンプトが表示されるまで *Enter を押し続け、値を「 0 」に設定してポーリングを無効にします。

   c. スイッチのプロンプトに戻るまで *Enter を押します。

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


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

3. fabric_1 と fabric_2 のすべてのスイッチについて、同じ手順を繰り返します。
4. 仮想ファブリックを設定します。

   a. スイッチで仮想ファブリックを有効にします。

      fosconfig — 有効な evf`

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

      「シャーシの設定」を参照してください

      次に 'configurechassis コマンドの出力例を示します

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

5. 論理スイッチを作成して設定します。

   'cfg — fabricID' を作成します

6. ブレードのすべてのポートを仮想ファブリックに追加します。

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

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

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

関連情報

"Brocade DCX 8510-8 スイッチを使用するための要件"

FCポートを使用してBrocade FCスイッチのEポートを構成する

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

作業を開始する前に

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

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

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

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

このタスクについて

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

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

このタスクは FC スイッチファブリックごとに行う必要があります。

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

構成に応じて必要な数の ISL を使用する必要があります。

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

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

手順

1. ポート速度を設定します。

   portcfgspeed port-number speed

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

   次の例では、各ファブリックに ISL が 2 つあります。

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

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

2. ISL ごとにトランキングモードを設定します。

   'portcfgtrunkport port-number

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

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

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

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

3. ISL ポートごとに QoS トラフィックを有効にします。

   portcfgqos --enable port-number

   次の例では、各スイッチファブリックに ISL が 2 つあります。

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

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

4. 設定を確認します。

   portCfgShow コマンド

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

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

```
..  ..  ..  ..
Port Auto Disable ..  ..  ..  ..    ..  ..  ..  ..   ..  ..  ..  ..
..  ..  ..  ..
CSCTL mode        ..  ..  ..  ..    ..  ..  ..  ..   ..  ..  ..  ..
..  ..  ..  ..

Fault Delay       0  0  0  0    0  0  0  0   0  0  0  0    0  0  0  0
```

5. ISL の距離を計算します。

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

   ISL の距離は次のように計算され、 km 単位に切り上げられます。

   実際の距離 × 1.5

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

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

6. ISL ポートごとに距離を設定します。

   `longdistance_portdistance-level_vc_link_init_ddistance

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

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

```
FC_switch_A_1:admin> portcfglongdistance 20 LE 1

FC_switch_B_1:admin> portcfglongdistance 20 LE 1
```

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

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

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

7. 距離設定を確認します。

portbuffershow

LE の距離レベルは 10 km と表示されます

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

```
FC_switch_A_1:admin> portbuffershow

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

8. 両方のスイッチが 1 つのファブリックを形成することを確認します。

'witchshow'

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

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

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

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

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

9. ファブリックの設定を確認します。

「 fabricshow` 」

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

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

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

10. [step10_brocade_config]] ISL のトランキングを確認します。

    「 trunkshow 」

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

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

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

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

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

関連情報

"FCスイッチのポート割り当て"

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

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

このタスクについて

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

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

- ローカルが FC_switch_A_1 。
- リモートが FC_switch_B_1 。

手順

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

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

   次のコマンドは、 FC_switch_A_1 のポート GE2.dp0 および ge3.dp0 に ipif アドレスを作成します。

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

   次のコマンドは、 FC_switch_B_1 のポート GE2.dp0 および ge3.dp0 に ipif アドレスを作成します。

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

2. 両方のスイッチに ipif アドレスが作成されたことを確認します。

   "portShow ipif all`

   次のコマンドは、スイッチ FC_switch_A_1 の ipif アドレスを表示します。

```
FC_switch_A_1:root> portshow ipif all

 Port         IP Address                      / Pfx  MTU   VLAN  Flags
-------------------------------------------------------------------------
--------
 ge2.dp0      10.10.20.71                     / 24   AUTO  2     U R M I
 ge3.dp0      10.10.21.71                     / 20   AUTO  2     U R M I
-------------------------------------------------------------------------
--------
Flags: U=Up B=Broadcast D=Debug L=Loopback P=Point2Point R=Running
I=InUse
       N=NoArp PR=Promisc M=Multicast S=StaticArp LU=LinkUp X=Crossport
```

次のコマンドは、スイッチ FC_switch_B_1 の ipif アドレスを表示します。

```
FC_switch_B_1:root> portshow ipif all

 Port         IP Address                      / Pfx  MTU   VLAN  Flags
-------------------------------------------------------------------------
--------
 ge2.dp0      10.10.20.72                     / 24   AUTO  2     U R M I
 ge3.dp0      10.10.21.72                     / 20   AUTO  2     U R M I
-------------------------------------------------------------------------
--------
Flags: U=Up B=Broadcast D=Debug L=Loopback P=Point2Point R=Running
I=InUse
       N=NoArp PR=Promisc M=Multicast S=StaticArp LU=LinkUp X=Crossport
```

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

   "portcfg fciptunnel

   このコマンドは、単一回線のトンネルを作成します。

   次のコマンドは、スイッチ FC_switch_A_1 にトンネルを作成します。

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

   次のコマンドは、スイッチ FC_switch_B_1 にトンネルを作成します。

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

4. FCIP トンネルが作成されたことを確認します。

   'portShow fciptunnel all

   次の例は、トンネルが作成され、回線が稼働していることを示しています。

```
FC_switch_B_1:root>

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

5. DP0 の追加の回線を作成します。

   次のコマンドは、スイッチ FC_switch_A_1 に dp0 の回線を作成します。

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

   次のコマンドは、スイッチ FC_switch_A_1 に dp0 の回線を作成します。

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

6. すべての回線が正常に作成されたことを確認します。

   'portShow fcipcircuit all

   次のコマンドは、回線とそのステータスを表示します。

```
FC_switch_A_1:root> portshow fcipcircuit all

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

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

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

このタスクについて

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

この手順の例では、次の 2 つのスイッチを使用します。

- ローカルが FC_switch_A_1 。
- リモートが FC_switch_B_1 。

手順

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

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

   次のコマンドは、 FC_switch_A_1 のポート ge0.dp0 および ge1.dp0 に ipif アドレスを作成します。

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

   次のコマンドは、 FC_switch_B_1 のポート ge0.dp0 および ge1.dp0 に ipif アドレスを作成します。

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

2. 両方のスイッチに ipif アドレスが作成されたことを確認します。

   "portShow ipif all`

   次の例は、 FC_switch_A_1 の IP インターフェイスを示しています。

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

   次の例は、 FC_switch_B_1 の IP インターフェイスを示しています。

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

3. 両方のスイッチに FCIP トンネルを作成します。

   「 portconfig fciptunnel 」のように入力します

   次のコマンドは、 FC_switch_A_1 にトンネルを作成します。

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

次のコマンドは、 FC_switch_B_1 にトンネルを作成します。

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

4. FCIP トンネルが作成されたことを確認します。

   'portShow fciptunnel all

   次の例は、トンネルが作成され、回線が稼働していることを示しています。

```
FC_switch_A_1:root>

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

5. 各スイッチに追加の回線を作成します。

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

   次のコマンドは、スイッチ FC_switch_A_1 に dp0 の回線を作成します。

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

   次のコマンドは、スイッチ FC_switch_A_1 に DP1 の回線を作成します。

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

6. すべての回線が正常に作成されたことを確認します。

   'portShow fcipcircuit all

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

```
FC_switch_A_1:root> portshow fcipcircuit all

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

Brocadeスイッチの非**E**ポートを構成する

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

このタスクについて

次の例では、ポートを FC-to-SAS ブリッジに接続します。

- Site_A の FC_FC_switch_A_1 のポート 6
- Site_B の FC_FC_switch_B_1 のポート 6

手順

1. 非 E ポートの速度を設定します。

   portcfgspeed portSpeed

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

   たとえば、各コンポーネントで次の速度がサポートされているとします。

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

```
FC_switch_A_1:admin> portcfgspeed 6 16

FC_switch_B_1:admin> portcfgspeed 6 16
```

2. 設定を確認します。

   portcfgshow

```
FC_switch_A_1:admin> portcfgshow

FC_switch_B_1:admin> portcfgshow
```

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

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

Brocade G620スイッチのISLポートで圧縮を設定する

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

このタスクについて

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

手順

1. 圧縮を設定するポートを無効にします。

   portdisable port-id`

2. ポートで圧縮を有効にします。

portCfgCompress — ポート ID を有効にします

3. ポートを有効にして圧縮の設定をアクティブにします。

   portEnable port-id`

4. 設定が変更されたことを確認します。

   portcfgshow port-id`

次の例は、ポート 0 で圧縮を有効にします。

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

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

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

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

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

Brocade FCスイッチのゾーニングを構成する

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

FC-VIポートをゾーン分けする

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

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

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

次の表に、 2 つの DR グループの FC-VI ゾーンを示します。

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

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

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

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

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

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

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

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

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

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

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

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

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

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

次の表に、 FC-VI ゾーンをまとめます。

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

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

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

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

必要なゾーン

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

各ストレージゾーンに 9 つのポートが含まれます。

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

ストレージゾーンでは標準のゾーニングを使用します。

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

ブリッジ名

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

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

各サイトの 1 つのスタックグループのブリッジ名の例：

- bridge_A_1a
- bridge_A_1b
- bridge_B_1a
- bridge_B_1b

DR グループ **1 - Site_A** のスタック **1**

- drgroup 1 ： MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1 ： *

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

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

- drgroup 1 ： MC1_INIT_GRP_1_SITE_A_STK_GRP_1_BOT_FC1 ： *

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

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

DR グループ **1 - Site_A** のスタック **2**

- drgroup 1 ： MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC1 ： *

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

FC スイッチ	サイト	スイッチドメイン	**Brocade 6505** 、**6510**、**6520**、**G620**、**G610**、または **G710** スイッチポート	接続先
FC_switch_A_1 を使用します	A	5.	9.	bridge_A_2a の FC1
FC_switch_B_1	B	7.	2.	controller_B_1 、ポート 0a
FC_switch_B_1	B	7.	3.	controller_B_1 、ポート 0c
FC_switch_B_1	B	7.	6.	controller_B_2 、ポート 0a
FC_switch_B_1	B	7.	7.	controller_B_2 、ポート 0c

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

- drgroup 1 ： MC1_INIT_GRP_1_SITE_A_STK_GRP_2_BOT_FC1 ： *

FC スイッチ	サイト	スイッチドメイン	**Brocade 6505** 、**6510**、**6520**、**G620**、**G610**、または **G710** スイッチポート	接続先
FC_switch_A_1 を使用します	A	6.	2.	controller_A_1 のポート 0b
FC_switch_A_1 を使用します	A	6.	3.	controller_A_1 のポート 0d
FC_switch_A_1 を使用します	A	6.	6.	controller_A_2 、ポート 0b
FC_switch_A_1 を使用します	A	6.	7.	controller_A_2 、ポート 0d
FC_switch_A_1 を使用します	A	6.	9.	bridge_A_2b の FC1
FC_switch_B_1	B	8.	2.	controller_B_1 、ポート 0b
FC_switch_B_1	B	8.	3.	controller_B_1 、ポート 0d
FC_switch_B_1	B	8.	6.	controller_B_2 、ポート 0b

FC スイッチ	サイト	スイッチドメイン	Brocade 6505 、6510、6520、G620、G610、または G710 スイッチポート	接続先
FC_switch_B_1	B	8.	7.	controller_B_2 、ポート 0d

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

DR グループ **1 - Site_B** のスタック **1**

- MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC1 ： *

FC スイッチ	サイト	スイッチドメイン	Brocade 6505 、6510、6520、G620、G610、または G710 スイッチ	接続先
FC_switch_A_1 を使用します	A	5.	2.	controller_A_1 のポート 0a
FC_switch_A_1 を使用します	A	5.	3.	controller_A_1 のポート 0c
FC_switch_A_1 を使用します	A	5.	6.	controller_A_2 、ポート 0a
FC_switch_A_1 を使用します	A	5.	7.	controller_A_2 、ポート 0c
FC_switch_B_1	B	7.	2.	controller_B_1 、ポート 0a
FC_switch_B_1	B	7.	3.	controller_B_1 、ポート 0c
FC_switch_B_1	B	7.	6.	controller_B_2 、ポート 0a
FC_switch_B_1	B	7.	7.	controller_B_2 、ポート 0c
FC_switch_B_1	B	7.	8.	bridge_B_1a の FC1

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

- drgroup 1 ： MC1_INIT_GRP_1_SITE_B_STK_GRP_1_BOT_FC1 ： *

FC スイッチ	サイト	スイッチドメイン	**Brocade 6505**、**6510**、**6520**、**G620**、**G610**、または **G710** スイッチ	接続先
FC_switch_A_1 を使用します	A	6.	2.	controller_A_1 のポート 0b
FC_switch_A_1 を使用します	A	6.	3.	controller_A_1 のポート 0d
FC_switch_A_1 を使用します	A	6.	6.	controller_A_2 、ポート 0b
FC_switch_A_1 を使用します	A	6.	7.	controller_A_2 、ポート 0d
FC_switch_B_1	B	8.	2.	controller_B_1 、ポート 0b
FC_switch_B_1	B	8.	3.	controller_B_1 、ポート 0d
FC_switch_B_1	B	8.	6.	controller_B_2 、ポート 0b
FC_switch_B_1	B	8.	7.	controller_B_2 、ポート 0d
FC_switch_B_1	B	8.	8.	bridge_B_1b の FC1

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

DR グループ **1 - Site_B** のスタック **2**

- drgroup 1 ： MC1_INIT_GRP_1_SITE_B_STK_GRP_2_TOP_FC1 ： *

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

FC スイッチ	サイト	スイッチドメイン	**Brocade 6505** 、**6510**、**6520**、**G620**、**G610**、または **G710** スイッチポート	接続先
FC_switch_B_1	B	7.	2.	controller_B_1 、ポート 0a
FC_switch_B_1	B	7.	3.	controller_B_1 、ポート 0c
FC_switch_B_1	B	7.	6.	controller_B_2 、ポート 0a
FC_switch_B_1	B	7.	7.	controller_B_2 、ポート 0c
FC_switch_B_1	B	7.	9.	bridge_B_2a の FC1

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

- drgroup 1 ： MC1_INIT_GRP_1_SITE_B_STK_GRP_2_BOT_FC1 ： *

FC スイッチ	サイト	スイッチドメイン	**Brocade 6505** 、**6510**、**6520**、**G620**、**G610**、または **G710** スイッチポート	接続先
FC_switch_A_1 を使用します	A	6.	2.	controller_A_1 のポート 0b
FC_switch_A_1 を使用します	A	6.	3.	controller_A_1 のポート 0d
FC_switch_A_1 を使用します	A	6.	6.	controller_A_2 、ポート 0b
FC_switch_A_1 を使用します	A	6.	7.	controller_A_2 、ポート 0d
FC_switch_B_1	B	8.	2.	controller_B_1 、ポート 0b
FC_switch_B_1	B	8.	3.	controller_B_1 、ポート 0d
FC_switch_B_1	B	8.	6.	controller_B_2 、ポート 0b
FC_switch_B_1	B	8.	7.	controller_B_2 、ポート 0d
FC_switch_B_1	B	8.	9.	bridge_B_1b の FC1

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

ストレージゾーンのサマリ

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

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

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

必要なゾーン

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

各ストレージゾーンに 5 つのポートが含まれます。

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

- FC-to-SAS ブリッジの FC ポートに接続するポート × 1

ストレージゾーンでは標準のゾーニングを使用します。

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

ブリッジ名

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

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

各サイトの 1 つのスタックグループのブリッジ名の例：

- bridge_A_1a
- bridge_A_1b
- bridge_B_1a
- bridge_B_1b

DR グループ **1 - Site_A** のスタック **1**

- drgroup 1 ： MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1 ： *

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

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

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

- drgroup 1 ： MC1_INIT_GRP_2_SITE_A_STK_GRP_1_TOP_FC1 ： *

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

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

- drgroup 1 ： MC1_INIT_GRP_1_SITE_A_STK_GRP_1_BOT_FC1 ： *

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

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

- drgroup 1 ： MC1_INIT_GRP_2_SITE_A_STK_GRP_1_BOT_FC2 ： *

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

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

DR グループ 1 - Site_A のスタック 2

- drgroup 1 ： MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC1 ： *

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

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

- drgroup 1 ： MC1_INIT_GRP_2_SITE_A_STK_GRP_2_TOP_FC1 ： *

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

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

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

- drgroup 1 ： MC1_INIT_GRP_1_SITE_A_STK_GRP_2_BOT_FC2 ： *

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

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

- drgroup 1 ： MC1_INIT_GRP_2_SITE_A_STK_GRP_2_BOT_FC2 ： *

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

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

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

DR グループ **1 - Site_B** のスタック **1**

- drgroup 1 ： MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC1 ： *

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

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

- drgroup 1 ： MC1_INIT_GRP_2_SITE_B_STK_GRP_1_TOP_FC1 ： *

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

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

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

- drgroup 1 ： MC1_INIT_GRP_1_SITE_B_STK_GRP_1_BOT_FC2 ： *

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

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

- drgroup 1 ： MC1_INIT_GRP_2_SITE_B_STK_GRP_1_BOT_FC2 ： *

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

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

DR グループ **1 - Site_B** のスタック **2**

- drgroup 1 ： MC1_INIT_GRP_1_SITE_B_STK_GRP_2_TOP_FC1 ： *

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

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

- drgroup 1 ： MC1_INIT_GRP_2_SITE_B_STK_GRP_2_TOP_FC1 ： *

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

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

- drgroup 1 ： MC1_INIT_GRP_1_SITE_B_STK_GRP_2_BOT_FC2 ： *

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

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

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

- drgroup 1 ： MC1_INIT_GRP_2_SITE_B_STK_GRP_2_BOT_FC2 ： *

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

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

ストレージゾーンのサマリ

ファブリック	ゾーン名	メンバーポート
FC_switch_A_1 および FC_switch_B_1	MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1	5 、 2 ； 5 、 6 ； 7 、 2 ； 7 、 6 ； 5 、 8
FC_switch_A_1 および FC_switch_B_1	MC1_INIT_GRP_2_SITE_A_STK_GRP_1_BOT_FC1	5 、 3 ； 5 、 7 ； 7 、 3 ； 7 、 7 ； 5 、 9
FC_switch_A_1 および FC_switch_B_1	MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC1	5 、 2 ； 5 、 6 ； 7 、 2 ； 7 、 6 ； 5 、 10

FC_switch_A_1 および FC_switch_B_1	MC1_INIT_GRP_2_SITE_A_STK_GRP_2_BOT_FC1	5 、 3 ； 5 、 7 ； 7 、 3 ； 7 、 7 ； 5 、 11
FC_switch_A_1 および FC_switch_B_1	MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC1	5 、 2 ； 5 、 6 ； 7 、 2 ； 7 、 6 ； 7 、 8
FC_switch_A_1 および FC_switch_B_1	MC1_INIT_GRP_2_SITE_B_STK_GRP_1_BOT_FC1	5 、 3 ； 5 、 7 ； 7 、 3 ； 7 、 7 ； 7 、 9
FC_switch_A_1 および FC_switch_B_1	MC1_INIT_GRP_1_SITE_B_STK_GRP_2_TOP_FC1	5 、 2 ； 5 、 6 ； 7 、 2 ； 7 、 6 ； 7 、 10
FC_switch_A_1 および FC_switch_B_1	MC1_INIT_GRP_2_SITE_B_STK_GRP_2_BOT_FC1	5 、 3 ； 5 、 7 ； 7 、 3 ； 7 、 7 ； 7 、 11
FC_switch_A_2 と FC_switch_B_2	MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC2	6 、 2 、 6 、 8 、 2 、 8 、 6 、 6 、 8
FC_switch_A_2 と FC_switch_B_2	MC1_INIT_GRP_2_SITE_A_STK_GRP_1_BOT_FC2	6 、 3 、 6 、 7 、 8 、 3 、 8 、 7 、 6 、 9
FC_switch_A_2 と FC_switch_B_2	MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC2	6 、 2 、 6 、 8 、 2 、 8 、 6 、 6 、 10
FC_switch_A_2 と FC_switch_B_2	MC1_INIT_GRP_2_SITE_A_STK_GRP_2_BOT_FC2	6 、 3 、 6 、 7 、 8 、 3 、 8 、 7 、 6 、 11
FC_switch_A_2 と FC_switch_B_2	MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC2	6 、 2 、 6 、 8 、 2 、 8 、 6 、 8 、 8
FC_switch_A_2 と FC_switch_B_2	MC1_INIT_GRP_2_SITE_B_STK_GRP_1_BOT_FC2	6 、 3 、 6 、 7 、 8 、 3 、 8 、 7 、 8 、 9
FC_switch_A_2 と FC_switch_B_2	MC1_INIT_GRP_1_SITE_B_STK_GRP_2_TOP_FC2	6 、 2 、 6 、 8 、 2 、 8 、 6 、 8 、 10
FC_switch_A_2 と FC_switch_B_2	MC1_INIT_GRP_2_SITE_B_STK_GRP_2_BOT_FC2	6 、 3 、 6 、 7 、 8 、 3 、 8 、 7 、 8 、 11

Brocade FCスイッチをゾーン分けする

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

このタスクについて

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

"FC-VI ポートのゾーニング"

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

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

手順

1. 各スイッチに FC-VI ゾーンを作成します。

   zonecreate "QOSH1_FCVI_1" 、 member ； member … ..

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

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

2. 各スイッチにストレージゾーンを設定します。

   ファブリックのゾーニングは、ファブリック内の 1 つのスイッチから設定できます。次の例では、 Switch_A_1 でゾーニングを設定します。

   a. スイッチファブリックの各スイッチドメインのストレージゾーンを作成します。

      zonecreate name 、 member ； member … ..

      この例では、両方の FC ポートを使用する FibreBridge 7500N のストレージゾーンを作成します。ゾーンには、ポート 5 、 2 ； 5 、 6 ； 7 、 2 ； 7 、 6 ； 5 、 16 が含まれます。

      ```
      Switch_A_1:admin> zonecreate
      "MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1", "5,2;5,6;7,2;7,6;5,16"
      ```

   b. 1 つ目のスイッチファブリックで設定を作成します。

      cfgcreate config_name 、 zone ； zone… を使用します

      この例では、 CFG_1 という名前で、 QOSH1_MC1_FAB_1_FCVI および GRP_1_SITE_A_STK_GRP_1_TOP_FC1 の 2 つのゾーンを含む設定を作成します

      ```
      Switch_A_1:admin> cfgcreate "CFG_1", "QOSH1_MC1_FAB_1_FCVI;
      MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1"
      ```

   c. 必要に応じて、設定にゾーンを追加します。

      cfgadd config_name zone ； zone… を使用します

   d. 設定を有効にします。

cfgenable config_name

```
Switch_A_1:admin> cfgenable "CFG_1"
```

e. 設定を保存します。

cfgsave

```
Switch_A_1:admin> cfgsave
```

f. ゾーニング設定を検証します。

zone — 妥当性検査

```
Switch_A_1:admin> zone --validate
Defined configuration:
cfg: CFG_1 QOSH1_MC1_FAB_1_FCVI ;
MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1
zone: QOSH1_MC1_FAB_1_FCVI
5,0;5,1;5,4;5,5;7,0;7,1;7,4;7,5
zone: MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1
5,2;5,6;7,2;7,6;5,16
Effective configuration:
cfg: CFG_1
zone: QOSH1_MC1_FAB_1_FCVI
5,0
5,1
5,4
5,5
7,0
7,1
7,4
7,5
zone: MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1
5,2
5,6
7,2
7,6
5,16
----------------------------------
~ - Invalid configuration
* - Member does not exist
# - Invalid usage of broadcast zone
```

Brocade 6510またはG620スイッチでISL暗号化を設定する

Brocade 6510 または G620 スイッチでは、 ISL 接続に対してオプションで Brocade 暗号化機能を使用できます。暗号化機能を使用する場合は、 MetroCluster 構成の各スイッチで追加の設定手順を実行する必要があります。

作業を開始する前に

- Brocade 6510 または G620 スイッチが必要です。

> Brocade G620 スイッチでの ISL 暗号化の使用は、 ONTAP 9.4 以降でのみサポートされます。

- 同じファブリックの 2 つのスイッチを選択しておく必要があります。
- スイッチと Fabric Operating System のバージョンに対応する Brocade のドキュメントを参照して、帯域幅とポートの制限を確認しておく必要があります。

このタスクについて

この手順は、同じファブリック内の両方のスイッチで実行する必要があります。

仮想ファブリックを無効にする

ISL 暗号化を設定するには、 MetroCluster 構成で使用されている 4 つのスイッチすべてで仮想ファブリックを無効にする必要があります。

手順

1. スイッチコンソールで次のコマンドを入力して、仮想ファブリックを無効にします。

   fosconfig — VF' を無効にします

2. スイッチをリブートします。

ペイロードを設定します

仮想ファブリックを無効にしたら、ファブリック内の両方のスイッチでペイロードまたはデータフィールドサイズを設定する必要があります。

このタスクについて

データフィールドサイズは 2048 以下にする必要があります。

手順

1. スイッチを無効にします。

   'witchdisable

2. ペイロードを設定します。

   「 configure 」を実行します

3. 次のスイッチパラメータを設定します。

   a. Fabric パラメータを 'y' のように設定します

b. Domain 、 WWN ベースの persistent PID など、その他のパラメータを設定します。
c. データフィールドのサイズを「 2048 」に設定します

認証ポリシーを設定します

認証ポリシーおよび関連するパラメータを設定する必要があります。

このタスクについて
コマンドはスイッチコンソールで実行する必要があります。

手順
1. 認証シークレットを設定します。
   a. セットアッププロセスを開始します。

      'ecAuthSecret — セット

   このコマンドにより、次の手順で応答する一連のプロンプトが開始されます。

   a. Enter peer WWN 、 Domain 、 or switch name というプロンプトに対して、ファブリック内のもう一方のスイッチの World Wide Name （ WWN ；ワールドワイド名）を指定します。
   b. Enter peer secret というプロンプトに対して、ピアシークレットを指定します。
   c. Enter local secret というプロンプトに対して、ローカルシークレットを指定します。
   d. 「 Are you done 」パラメータに「 Y 」と入力します。

      認証シークレットの設定例を以下に示します。

```
brcd> secAuthSecret --set

This command is used to set up secret keys for the DH-CHAP
authentication.
The minimum length of a secret key is 8 characters and maximum 40
characters. Setting up secret keys does not initiate DH-CHAP
authentication. If switch is configured to do DH-CHAP, it is
performed
whenever a port or a switch is enabled.

Warning: Please use a secure channel for setting secrets. Using
an insecure channel is not safe and may compromise secrets.

Following inputs should be specified for each entry.

1. WWN for which secret is being set up.
2. Peer secret: The secret of the peer that authenticates to peer.
3. Local secret: The local secret that authenticates peer.

Press enter to start setting up secrets > <cr>

Enter peer WWN, Domain, or switch name (Leave blank when done):
10:00:00:05:33:76:2e:99
Enter peer secret: <hidden>
Re-enter peer secret: <hidden>
Enter local secret: <hidden>
Re-enter local secret: <hidden>

Enter peer WWN, Domain, or switch name (Leave blank when done):
Are you done? (yes, y, no, n): [no] yes
Saving data to key store... Done.
```

2. 認証グループを 4 に設定します。

   authUtil — set-g 4`

3. 認証タイプを「 dhchap 」に設定します。

   authUtil — set -a dhchap

   次の出力が表示されます。

   ```
   Authentication is set to dhchap.
   ```

4. スイッチの認証ポリシーを on に設定します。

authUtil — policy-sw on `

次の出力が表示されます。

```
Warning: Activating the authentication policy requires either DH-CHAP
secrets or PKI certificates depending on the protocol selected.
Otherwise, ISLs will be segmented during next E-port bring-up.
ARE YOU SURE  (yes, y, no, n): [no] yes
Auth Policy is set to ON
```

Brocade スイッチで **ISL** 暗号化を有効にします

認証ポリシーと認証シークレットを設定したら、ポートで ISL 暗号化を有効にする必要があります。

このタスクについて

- この手順は、一度に 1 つのスイッチファブリックで実行する必要があります。
- コマンドはスイッチコンソールで実行する必要があります。

手順

1. すべての ISL ポートで暗号化を有効にします。

   portCfgEncrypt — ポート番号を有効にします

   次の例は、ポート 8 とポート 12 で暗号化を有効にします。

   portCfgEncrypt — 8 を有効にします

   portCfgEncrypt — 12 を有効にします

2. スイッチを有効にします。

   「 witchenable 」

3. ISL が稼働していることを確認します。

   「 islshow` 」

4. 暗号化が有効であることを確認します。

   portenccompshow`

   次の例は、ポート 8 とポート 12 で暗号化が有効であることを示しています。

```
User Encryption
Port  configured     Active
----   ----------    ------
 8      yes           yes
 9      No            No
 10     No            No
 11     No            No
 12     yes           yes
```

次に何をするか

MetroCluster 構成の他のファブリック内のスイッチで、すべての手順を実行します。

Cisco FC スイッチを手動で設定する

MetroCluster 構成の各 Cisco スイッチを ISL 接続とストレージ接続用にそれぞれ設定する必要があります。

作業を開始する前に

Cisco FC スイッチには次の要件が適用されます。

- 同じNX-OSバージョンおよびライセンスの同じモデルの、サポートされている4台のCiscoスイッチを使用する必要があります。
- MetroCluster 構成には 4 つのスイッチが必要です。

  それぞれ 2 つのスイッチで構成される 2 つのファブリックに接続されます。各ファブリックが両方のサイトにまたがっている必要があります。

- ATTO FibreBridge モデルへの接続をサポートしている必要があります。
- Cisco FCストレージファブリックでは暗号化や圧縮を使用できません。MetroCluster 構成ではサポートされません。

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

このタスクについて

環境スイッチ間リンク（ ISL ）接続には次の要件があります。

- 1 つのファブリック内のすべての ISL の長さと速度が同じである必要があります。

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

環境 the storage connections には次の要件があります。

- 各ストレージコントローラに、スイッチファブリックに接続可能なイニシエータポートが 4 つ必要です。

  各ストレージコントローラの 2 つのイニシエータポートを各ファブリックに接続する必要があります。

> FAS8020 、 AFF8020 、 FAS8200 、および AFF A300 のシステムでは、次のすべての条件に該当する場、コントローラあたりのイニシエータポートを 2 ポート（各ファブリックに 1 つのイニシエータポートを接続）にすることができます。
>
> - ディスクストレージの接続に使用できる FC イニシエータポートが 3 つ以下で、それ以外に FC イニシエータとして設定できるポートがない。
> - すべてのスロットが使用中で、 FC イニシエータカードを追加できません。

関連情報

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

Cisco スイッチのライセンス要件

ファブリック接続 MetroCluster 構成では、 Cisco スイッチに一部の機能ベースのライセンスが必要な場合があります。これらのライセンスを使用すると、 QoS や長距離モードクレジットなどの機能をスイッチで使用できます。MetroCluster 構成内の 4 つのスイッチすべてに、必要な機能ベースのライセンスをインストールする必要があります。

MetroCluster 構成では、次の機能ベースのライセンスが必要になる場合があります。

- ENTERPRISE_PKG

  Cisco スイッチで QoS 機能を使用できるようになります。

- PORT_ACTIVATION_PKG

  このライセンスは、 Cisco 9148 スイッチに使用できます。スイッチ上のポートをアクティブ化または非アクティブ化できます。ただし、任意の時点でアクティブにできるポートは 16 個のみです。Cisco MDS 9148 スイッチでは 16 個のポートがデフォルトで有効になっています。

- FM_SERVER_PKG

  複数のファブリックを同時に管理でき、また、 Web ブラウザを使用してスイッチを管理できます。

  FM_SERVER_PKG ライセンスがある場合、パフォーマンスしきい値、しきい値の監視などのパフォーマンス管理機能も使用できるようになります。このライセンスの詳細については、 Cisco Fabric Manager Server Package を参照してください。

show license usage コマンドを使用すると、ライセンスがインストールされているかどうかを確認できます。これらのライセンスをお持ちでない場合は、インストールを開始する前に営業担当者にお問い合わせください。

> Cisco MDS 9250i スイッチには、固定構成の 1/10GbE IP ストレージサービスポートが 2 つあります。これらのポートには追加のライセンスは必要ありません。Cisco SAN Extension over IP アプリケーションパッケージは、これらのスイッチの標準ライセンスで、 FCIP や圧縮などの機能を有効にします。

Cisco FC スイッチを工場出荷時のデフォルトに設定

正しく設定するには、スイッチを工場出荷時のデフォルトに設定する必要があります。これにより、スイッチがクリーンな設定から開始されます。

このタスクについて

このタスクは、 MetroCluster 構成内のすべてのスイッチで実行する必要があります。

手順

1. コンソールに接続し、同じファブリック内の両方のスイッチにログインします。
2. スイッチをデフォルトの設定に戻します。

   「 write erase 」を入力します

   コマンドの確認を求められたら、「 y 」と入力します。これにより、スイッチのライセンスおよび設定情報がすべて消去されます。

3. スイッチをリブートします。

   「再ロード」

   コマンドの確認を求められたら、「 y 」と入力します。

4. もう一方のスイッチで 'write erase' コマンドと 'reload コマンドを繰り返します

   「 reload 」コマンドを発行すると、スイッチが再起動し、セットアップのプロンプトが表示されます。この時点で、次のセクションに進みます。

例

次の例は、 FC_switch_A_1 と FC_switch_B_1 で構成されるファブリックでの処理を示しています。

```
FC_Switch_A_1# write erase
    Warning: This command will erase the startup-configuration.
    Do you wish to proceed anyway? (y/n)  [n] y
    FC_Switch_A_1# reload
    This command will reboot the system. (y/n)?  [n] y

FC_Switch_B_1# write erase
    Warning: This command will erase the startup-configuration.
    Do you wish to proceed anyway? (y/n)  [n] y
    FC_Switch_B_1# reload
    This command will reboot the system. (y/n)?  [n] y
```

Cisco FC スイッチの基本設定とコミュニティストリングを設定します

基本設定は 'setup' コマンドを使用して、または 'reload ' コマンドを発行した後で指定する必要があります。

手順

1. セットアップのプロンプトがスイッチに表示されない場合は、スイッチの基本設定を実行します。

   「セットアップ」

2. SNMP コミュニティストリングのプロンプトが表示されるまで、セットアップの質問に対するデフォルトの応答を受け入れます。
3. コミュニティストリングを「 public 」（すべて小文字）に設定し、 ONTAP ヘルスモニタからのアクセスを許可します。

   コミュニティストリングを「 public 」以外の値に設定することもできますが、指定したコミュニティストリングを使用して ONTAP ヘルスモニタを設定する必要があります。

   次の例は、 FC_switch_A_1 に対するコマンドを示しています。

```
FC_switch_A_1# setup
    Configure read-only SNMP community string (yes/no) [n]: y
    SNMP community string : public
    Note:  Please set the SNMP community string to "Public" or another
value of your choosing.
    Configure default switchport interface state (shut/noshut) [shut]:
noshut
    Configure default switchport port mode F (yes/no) [n]: n
    Configure default zone policy (permit/deny) [deny]: deny
    Enable full zoneset distribution? (yes/no) [n]: yes
```

   次の例は、 FC_switch_B_1 に対するコマンドを示しています。

```
FC_switch_B_1# setup
    Configure read-only SNMP community string (yes/no) [n]: y
    SNMP community string : public
    Note:  Please set the SNMP community string to "Public" or another
value of your choosing.
    Configure default switchport interface state (shut/noshut) [shut]:
noshut
    Configure default switchport port mode F (yes/no) [n]: n
    Configure default zone policy (permit/deny) [deny]: deny
    Enable full zoneset distribution? (yes/no) [n]: yes
```

ポートのライセンスを取得しています

連続する範囲のポートで Cisco スイッチライセンスを使用する必要はありません。代わりに、使用する特定のポートのライセンスを取得し、未使用のポートからライセンスを削除できます。

作業を開始する前に

スイッチ構成内でライセンスが付与されているポートの数を確認し、必要に応じてポート間でライセンスを移動します。

手順

1. スイッチファブリックのライセンス使用状況を表示します。

   'how port-resources module 1'

   ライセンスが必要なポートを特定します。ライセンスが付与されていないポートがある場合は、ライセンスが付与されている余分なポートがないかを特定し、余分なポートからライセンスを削除することを検討します。

2. コンフィギュレーションモードを開始します。

   'config t`

3. 選択したポートからライセンスを削除します。
   a. ライセンスを削除するポートを選択します。

      'interface_name_`

   b. ポートからライセンスを削除します。

      「 no port-license acquire 」を選択します

   c. ポート設定インターフェイスを終了します。

      「 exit

4. 選択したポートのライセンスを取得します。
   a. ライセンスを削除するポートを選択します。

      'interface_name_`

   b. ポートがライセンスを取得できるようにします。

      「ポートライセンス」

   c. ポートのライセンスを取得します。

      「ポートライセンス取得」

   d. ポート設定インターフェイスを終了します。

      「 exit

5. 追加のポートがある場合は、この手順を繰り返します
6. 構成モードを終了します。

   「 exit

ポートのライセンスを削除および取得する

次の例は、ポート fc1/2 からライセンスを削除し、ポート fc1/1 をライセンス取得可能にし、ポート fc1/1 で

ライセンスを取得する手順を示しています。

```
Switch_A_1# conf t
    Switch_A_1(config)# interface fc1/2
    Switch_A_1(config)# shut
    Switch_A_1(config-if)# no port-license acquire
    Switch_A_1(config-if)# exit
    Switch_A_1(config)# interface fc1/1
    Switch_A_1(config-if)# port-license
    Switch_A_1(config-if)# port-license acquire
    Switch_A_1(config-if)# no shut
    Switch_A_1(config-if)# end
    Switch_A_1# copy running-config startup-config

    Switch_B_1# conf t
    Switch_B_1(config)# interface fc1/2
    Switch_B_1(config)# shut
    Switch_B_1(config-if)# no port-license acquire
    Switch_B_1(config-if)# exit
    Switch_B_1(config)# interface fc1/1
    Switch_B_1(config-if)# port-license
    Switch_B_1(config-if)# port-license acquire
    Switch_B_1(config-if)# no shut
    Switch_B_1(config-if)# end
    Switch_B_1# copy running-config startup-config
```

次の例は、ポートライセンスの使用状況を検証する方法を示しています。

```
Switch_A_1# show port-resources module 1
    Switch_B_1# show port-resources module 1
```

Cisco MDS 9148 または 9148S スイッチでのポートの有効化

Cisco MDS 9148 または 9148S スイッチでは、 MetroCluster 構成で必要なポートを手動で有効にする必要があります。

このタスクについて

- Cisco MDS 9148 または 9148S スイッチの 16 個のポートを手動で有効にできます。
- Cisco スイッチを使用すると、 POD ライセンスをランダムなポートに適用することができますが、順番に適用することはできません。
- Cisco スイッチでは、 12 個を超えるポートが必要な場合を除き、各ポートグループから 1 つのポートを使用する必要があります。

手順

1. Cisco スイッチで使用可能なポートグループを表示します。

   'how port-resources module_blade_number_`

2. ポートグループの必要なポートにライセンスを付与して取得します。

   'config t`

   'interface_port_number_`

   「小屋」

   「ポートライセンス取得」

   「 no shut 」のようになります

   たとえば、次のコマンドシーケンスでは、 fc 1/45 ポートがライセンス付与され、取得されます。

   ```
   switch# config t
   switch(config)#
   switch(config)# interface fc 1/45
   switch(config-if)#
   switch(config-if)# shut
   switch(config-if)# port-license acquire
   switch(config-if)# no shut
   switch(config-if)# end
   ```

3. 設定を保存します。

   'copy running-config startup-config

Cisco FC スイッチでの F ポートの設定

FC スイッチで F ポートを設定する必要があります。

このタスクについて

MetroCluster 構成では、 F ポートとは、スイッチを HBA イニシエータ、 FC-VI インターコネクト、および FC-to-SAS ブリッジに接続するポートです。

ポートはそれぞれ個別に設定する必要があります。

次のセクションを参照して、構成に応じた F ポート（スイッチからノード）を確認してください。

- "FCスイッチのポート割り当て"

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

手順

1. コンフィギュレーションモードを開始します。

'config t`

2. ポートのインターフェイス構成モードに切り替えます。

   'interface_port-ID_

3. ポートをシャットダウンします。

   「ダウンタイム」

4. ポートを F モードに設定します。

   「 witchport mode F 」

5. ポートを固定の速度に設定します。

   'witchport speed_speed - value_

   `speed-value` は '8000` または '16000` です

6. スイッチポートのレートモードを dedicated に設定します。

   'witchport rate-mode dedicated （スイッチポートレートモード専用）

7. ポートを再起動します。

   「シャットダウンなし」

8. 構成モードを終了します。

   「 end 」と入力します

例
次の例は、 2 つのスイッチに対するコマンドを示しています。

```
Switch_A_1# config  t
FC_switch_A_1(config)# interface fc 1/1
FC_switch_A_1(config-if)# shutdown
FC_switch_A_1(config-if)# switchport mode F
FC_switch_A_1(config-if)# switchport speed 8000
FC_switch_A_1(config-if)# switchport rate-mode dedicated
FC_switch_A_1(config-if)# no shutdown
FC_switch_A_1(config-if)# end
FC_switch_A_1# copy running-config startup-config

FC_switch_B_1# config  t
FC_switch_B_1(config)# interface fc 1/1
FC_switch_B_1(config-if)# switchport mode F
FC_switch_B_1(config-if)# switchport speed 8000
FC_switch_B_1(config-if)# switchport rate-mode dedicated
FC_switch_B_1(config-if)# no shutdown
FC_switch_B_1(config-if)# end
FC_switch_B_1# copy running-config startup-config
```

ISL と同じポートグループ内の **F** ポートにバッファ間クレジットを割り当てます

F ポートが ISL と同じポートグループに含まれている場合は、バッファ間クレジットを割り当てる必要があります。必要なバッファ間クレジットがポートにない場合、 ISL は動作しなくなる可能性があります。

このタスクについて

F ポートが ISL ポートと同じポートグループに含まれていない場合は、このタスクは必要ありません。

F ポートが ISL を含むポートグループに含まれている場合は、 MetroCluster 構成内の FC スイッチごとにこのタスクを実行する必要があります。

手順

1. コンフィギュレーションモードを開始します。

   'config t`

2. ポートのインターフェイス構成モードを設定します。

   'interface_port-ID_

3. ポートを無効にします。

   「小屋」

4. ポートが F モードになっていない場合は、 F モードに設定します。

   「 witchport mode F 」

5. E ポート以外のバッファ間クレジットを 1 に設定します。

「 witchport fcrxbbcredit 1 」を参照してください

6. ポートを再度有効にします。

   「 no shut 」のようになります

7. 構成モードを終了します。

   「 exit

8. 更新された設定をスタートアップ設定にコピーします。

   'copy running-config startup-config

9. ポートに割り当てられているバッファ間クレジットを確認します。

   'how port-resources module 1'

10. 構成モードを終了します。

    「 exit

11. ファブリック内のもう一方のスイッチで、上記の手順を繰り返します。
12. 設定を確認します。

    'how port-resource module 1'

例

この例では、ポート fc1/40 は ISL です。ポート fc1/37 、 fc1/38 および fc1/39 は同じポートグループに含まれているため、設定が必要です。

次のコマンドは、ポート範囲を fc1/37~fc1/39 に設定する場合を示しています。

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# interface fc1/37-39
FC_switch_A_1(config-if)# shut
FC_switch_A_1(config-if)# switchport mode F
FC_switch_A_1(config-if)# switchport fcrxbbcredit 1
FC_switch_A_1(config-if)# no shut
FC_switch_A_1(config-if)# exit
FC_switch_A_1# copy running-config startup-config

FC_switch_B_1# conf t
FC_switch_B_1(config)# interface fc1/37-39
FC_switch_B_1(config-if)# shut
FC_switch_B_1(config-if)# switchport mode F
FC_switch_B_1(config-if)# switchport fcrxbbcredit 1
FC_switch_A_1(config-if)# no shut
FC_switch_A_1(config-if)# exit
FC_switch_B_1# copy running-config startup-config
```

次のコマンドおよび出力は、設定が適切に適用されていることを示しています。

```
FC_switch_A_1# show port-resource module 1
...
Port-Group 11
 Available dedicated buffers are 93

--------------------------------------------------------------------------
Interfaces in the Port-Group       B2B Credit  Bandwidth  Rate Mode
                                      Buffers     (Gbps)

--------------------------------------------------------------------------
fc1/37                                    32        8.0  dedicated
fc1/38                                     1        8.0  dedicated
fc1/39                                     1        8.0  dedicated
...

FC_switch_B_1# port-resource module
...
Port-Group 11
 Available dedicated buffers are 93

--------------------------------------------------------------------------
Interfaces in the Port-Group       B2B Credit  Bandwidth  Rate Mode
                                    Buffers     (Gbps)

--------------------------------------------------------------------------
fc1/37                                    32        8.0  dedicated
fc1/38                                     1        8.0  dedicated
fc1/39                                     1        8.0 dedicated
...
```

Cisco FC スイッチでの **VSAN** の作成および設定

MetroCluster 構成内の各 FC スイッチに、 FC-VI ポート用の VSAN とストレージポート用の VSAN を 1 つずつ作成する必要があります。

このタスクについて

VSAN の番号と名前は一意である必要があります。フレームのインオーダー配信で 2 つの ISL を使用している場合は、追加の設定が必要です。

このタスクの例では、次の命名規則を使用します。

スイッチファブリック	VSAN 名	ID 番号
1.	FCVI_1_10	10.
STOR_1_20	20	2.

FCVI_2_30	30	STOR_2_20

このタスクは FC スイッチファブリックごとに行う必要があります。

手順

1. FC-VI VSAN を設定します。
   a. 構成モードを開始していない場合は、構成モードに切り替えます。

      'config t`

   b. VSAN データベースを編集します。

      「 VSAN データベース」

   c. VSAN ID を設定します。

      'vsan_vsan-ID_`

   d. VSAN 名を設定します。

      'vsan_vsan-ID_VSAN_NAME_NAME_`
2. FC-VI VSAN にポートを追加します。
   a. VSAN の各ポートのインターフェイスを追加します。

      'vsan_vsan-ID_interface_name_`

      FC-VI VSAN に関しては、ローカル FC-VI ポートを接続するポートが追加されます。

   b. 構成モードを終了します。

      「 end 」と入力します

   c. running-config を startup-config にコピーします。

      'copy running-config startup-config

      次の例では、該当するポートは fc1/1 と fc1/13 です。

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# vsan database
FC_switch_A_1(config)# vsan 10 interface fc1/1
FC_switch_A_1(config)# vsan 10 interface fc1/13
FC_switch_A_1(config)# end
FC_switch_A_1# copy running-config startup-config
FC_switch_B_1# conf t
FC_switch_B_1(config)# vsan database
FC_switch_B_1(config)# vsan 10 interface fc1/1
FC_switch_B_1(config)# vsan 10 interface fc1/13
FC_switch_B_1(config)# end
FC_switch_B_1# copy running-config startup-config
```

3. VSAN のポートメンバーシップを確認します。

   'How VSAN member' （ VSAN メンバーの仕組み

```
FC_switch_A_1# show vsan member
FC_switch_B_1# show vsan member
```

4. フレームのインオーダー配信またはアウトオブオーダー配信を保証するように VSAN を設定します。

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

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

   - フレームのインオーダー配信を設定するには、次の手順を実行する必要があります。

     i. コンフィギュレーションモードを開始します。

        「 conf t`

     ii. VSAN の交換のインオーダー保証を有効にします。

        inorder-guarantee vsan_vsan-ID_`

        FC-VI VSAN （ FCVI_1_10 および FCVI_2_30 ）については、フレームと交換のインオーダー保証を VSAN 10 でのみ有効にする必要があります。

     iii. VSAN のロードバランシングを有効にします。

        'vsan_vsan-ID_loadbalancing src-dst-id

     iv. 構成モードを終了します。

        「 end 」と入力します

v. running-config を startup-config にコピーします。

'copy running-config startup-config

FC_switch_A_1 でフレームのインオーダー配信を設定するコマンドは次のとおりです。

```
FC_switch_A_1# config t
FC_switch_A_1(config)# in-order-guarantee vsan 10
FC_switch_A_1(config)# vsan database
FC_switch_A_1(config-vsan-db)# vsan 10 loadbalancing src-dst-id
FC_switch_A_1(config-vsan-db)# end
FC_switch_A_1# copy running-config startup-config
```

FC_switch_B_1 でフレームのインオーダー配信を設定するコマンドは次のとおりです。

```
FC_switch_B_1# config t
FC_switch_B_1(config)# in-order-guarantee vsan 10
FC_switch_B_1(config)# vsan database
FC_switch_B_1(config-vsan-db)# vsan 10 loadbalancing src-dst-id
FC_switch_B_1(config-vsan-db)# end
FC_switch_B_1# copy running-config startup-config
```

◦ フレームのアウトオブオーダー配信を設定するには、次の手順を実行する必要があります。

i. コンフィギュレーションモードを開始します。

「 conf t`

ii. VSAN の交換のインオーダー保証を無効にします。

'no in-order-guarantee VSAN_vsan-ID_

iii. VSAN のロードバランシングを有効にします。

'vsan_vsan-ID_loadbalancing src-dst-id

iv. 構成モードを終了します。

「 end 」と入力します

v. running-config を startup-config にコピーします。

'copy running-config startup-config

FC_switch_A_1 でフレームのアウトオブオーダー配信を設定するコマンドは次のとおりです。

```
FC_switch_A_1# config t
FC_switch_A_1(config)# no in-order-guarantee vsan 10
FC_switch_A_1(config)# vsan database
FC_switch_A_1(config-vsan-db)# vsan 10 loadbalancing src-dst-id
FC_switch_A_1(config-vsan-db)# end
FC_switch_A_1# copy running-config startup-config
```

FC_switch_B_1 でフレームのアウトオブオーダー配信を設定するコマンドは次のとおりです。

```
FC_switch_B_1# config t
FC_switch_B_1(config)# no in-order-guarantee vsan 10
FC_switch_B_1(config)# vsan database
FC_switch_B_1(config-vsan-db)# vsan 10 loadbalancing src-dst-id
FC_switch_B_1(config-vsan-db)# end
FC_switch_B_1# copy running-config startup-config
```

+

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

"ONTAP ソフトウェアでのフレームのインオーダー配信またはアウトオブオーダー配信の設定"

5. FC-VI VSAN の QoS ポリシーを設定します。
   a. コンフィギュレーションモードを開始します。

      「 conf t`

   b. 次のコマンドを続けて入力して、 QoS をイネーブルにし、クラスマップを作成します。

      「 qos enable 」と入力します

      'qos class-map_class_name_match-any'

   c. 前の手順で作成したクラスマップをポリシーマップに追加します。

      'class_class_name_`

   d. 優先度を設定します。

      「優先度高」

   e. この手順で作成したポリシーマップに VSAN を追加します。

      'qos service policy_policy_policy_name_vsan_vsan-id_`

   f. 更新された設定をスタートアップ設定にコピーします。

'copy running-config startup-config

FC_switch_A_1 で QoS ポリシーを設定するコマンドは次のとおりです。

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# qos enable
FC_switch_A_1(config)# qos class-map FCVI_1_10_Class match-any
FC_switch_A_1(config)# qos policy-map FCVI_1_10_Policy
FC_switch_A_1(config-pmap)# class FCVI_1_10_Class
FC_switch_A_1(config-pmap-c)# priority high
FC_switch_A_1(config-pmap-c)# exit
FC_switch_A_1(config)# exit
FC_switch_A_1(config)# qos service policy FCVI_1_10_Policy vsan 10
FC_switch_A_1(config)# end
FC_switch_A_1# copy running-config startup-config
```

FC_switch_B_1 で QoS ポリシーを設定するコマンドは次のとおりです。

```
FC_switch_B_1# conf t
FC_switch_B_1(config)# qos enable
FC_switch_B_1(config)# qos class-map FCVI_1_10_Class match-any
FC_switch_B_1(config)# qos policy-map FCVI_1_10_Policy
FC_switch_B_1(config-pmap)# class FCVI_1_10_Class
FC_switch_B_1(config-pmap-c)# priority high
FC_switch_B_1(config-pmap-c)# exit
FC_switch_B_1(config)# exit
FC_switch_B_1(config)# qos service policy FCVI_1_10_Policy vsan 10
FC_switch_B_1(config)# end
FC_switch_B_1# copy running-config startup-config
```

6. ストレージ VSAN を設定します。

   a. VSAN ID を設定します。

      'vsan_vsan-ID_`

   b. VSAN 名を設定します。

      'vsan_vsan-ID_VSAN_NAME_NAME_`

FC_switch_A_1 でストレージ VSAN を設定するコマンドは次のとおりです。

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# vsan database
FC_switch_A_1(config-vsan-db)# vsan 20
FC_switch_A_1(config-vsan-db)# vsan 20 name STOR_1_20
FC_switch_A_1(config-vsan-db)# end
FC_switch_A_1# copy running-config startup-config
```

FC_switch_B_1 でストレージ VSAN を設定するコマンドは次のとおりです。

```
FC_switch_B_1# conf t
FC_switch_B_1(config)# vsan database
FC_switch_B_1(config-vsan-db)# vsan 20
FC_switch_B_1(config-vsan-db)# vsan 20 name STOR_1_20
FC_switch_B_1(config-vsan-db)# end
FC_switch_B_1# copy running-config startup-config
```

7. ストレージ VSAN にポートを追加します。

   ストレージ VSAN に関しては、 HBA または FC-to-SAS ブリッジを接続するすべてのポートを追加する必要があります。この例では、 fc1/5 、 fc1/9 、 fc1/17 、 fc1/21 、fc1/25 、 fc1/29 、 fc1/33 、および fc1/37 が追加されます。

   FC_switch_A_1 でストレージ VSAN にポートを追加するコマンドは次のとおりです。

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# vsan database
FC_switch_A_1(config)# vsan 20 interface fc1/5
FC_switch_A_1(config)# vsan 20 interface fc1/9
FC_switch_A_1(config)# vsan 20 interface fc1/17
FC_switch_A_1(config)# vsan 20 interface fc1/21
FC_switch_A_1(config)# vsan 20 interface fc1/25
FC_switch_A_1(config)# vsan 20 interface fc1/29
FC_switch_A_1(config)# vsan 20 interface fc1/33
FC_switch_A_1(config)# vsan 20 interface fc1/37
FC_switch_A_1(config)# end
FC_switch_A_1# copy running-config startup-config
```

   FC_switch_B_1 でストレージ VSAN にポートを追加するコマンドは次のとおりです。

```
FC_switch_B_1# conf t
FC_switch_B_1(config)# vsan database
FC_switch_B_1(config)# vsan 20 interface fc1/5
FC_switch_B_1(config)# vsan 20 interface fc1/9
FC_switch_B_1(config)# vsan 20 interface fc1/17
FC_switch_B_1(config)# vsan 20 interface fc1/21
FC_switch_B_1(config)# vsan 20 interface fc1/25
FC_switch_B_1(config)# vsan 20 interface fc1/29
FC_switch_B_1(config)# vsan 20 interface fc1/33
FC_switch_B_1(config)# vsan 20 interface fc1/37
FC_switch_B_1(config)# end
FC_switch_B_1# copy running-config startup-config
```

E ポートを設定しています

ISL を接続するスイッチポート（ E ポート）を設定する必要があります。

このタスクについて

使用する手順は、使用するスイッチによって異なります。

- Cisco FC スイッチでの E ポートの設定
- Cisco 9250i FC スイッチのシングル ISL に対する FCIP ポートの設定
- Cisco 9250i FC スイッチのデュアル ISL に対する FCIP ポートの設定

Cisco FC スイッチでの E ポートの設定

スイッチ間リンク（ ISL ）を接続する FC スイッチポートを設定する必要があります。

このタスクについて

これらは E ポートであり、設定はポートごとに行う必要があります。そのためには、正しいバッファ間クレジット（ BBC ）数を計算する必要があります。

ファブリック内のすべての ISL を、同じ速度と同じ距離で設定する必要があります。

このタスクは ISL ポートごとに実行する必要があります。

手順

1. 次の表を使用して、可能なポート速度で調整された 1 km あたりの必要な BBC を確認します。

   正しい BBC 数は、必要な調整済み BBC （下記の表で特定）に、スイッチ間の距離（ km ）を掛けて算出します。FC-VI のフレーミング動作に対応するために、 1.5 の調整係数が必要です。

速度（ Gbps ）	1km あたりの必要な BBC	必要な調整済み BBC （ 1km あたりの BBC × 1.5 ）
1.	0.5	0.75

2.	1.	1.5
4.	2.	3.
8.	4.	6.
16	8.	12.

たとえば、 4Gbps のリンクで 30km の距離に必要なクレジット数を算出するには、次の計算を行います。

- 「 Gbps での速度」は 4 です
- 「必要な調整済み BBC 」は 3
- 「スイッチ間の距離（ km ）」は 30km です
- 3 x 30 = 90

a. コンフィギュレーションモードを開始します。

'config t`

b. 設定するポートを指定します。

「 interface_port-name_` 」

c. ポートをシャットダウンします。

「ダウンタイム」

d. ポートのレートモードを「 dedicated 」に設定します。

'witchport rate-mode dedicated （スイッチポートレートモード専用）

e. ポートの速度を設定します。

'witchport speed_speed - value_

f. ポートのバッファ間クレジットを設定します。

'witchport fcrxbbcredit *number_of_buffers*'

g. ポートを E モードに設定します。

'witchport mode E`

h. ポートのトランクモードをイネーブルにします。

'witchport trunk mode on `

i. ISL Virtual Storage Area Network （ VSAN ；仮想ストレージエリアネットワーク）をトランクに追加します。

'witchport トランクでは VSAN 10 を許可

'witchport trunk allowed vsan add 20`

j. ポートをポートチャネル 1 に追加します。

「 channel-group 1 」のようになります

k. ファブリック内のパートナースイッチ上の対応する ISL ポートに対して、ここまでの手順を繰り返します。

次の例は、ポート fc1/41 を距離 30km 、 8Gbps で設定する場合を示しています。

```
FC_switch_A_1# conf t
FC_switch_A_1# shutdown
FC_switch_A_1# switchport rate-mode dedicated
FC_switch_A_1# switchport speed 8000
FC_switch_A_1# switchport fcrxbbcredit 60
FC_switch_A_1# switchport mode E
FC_switch_A_1# switchport trunk mode on
FC_switch_A_1# switchport trunk allowed vsan 10
FC_switch_A_1# switchport trunk allowed vsan add 20
FC_switch_A_1# channel-group 1
fc1/36 added to port-channel 1 and disabled

FC_switch_B_1# conf t
FC_switch_B_1# shutdown
FC_switch_B_1# switchport rate-mode dedicated
FC_switch_B_1# switchport speed 8000
FC_switch_B_1# switchport fcrxbbcredit 60
FC_switch_B_1# switchport mode E
FC_switch_B_1# switchport trunk mode on
FC_switch_B_1# switchport trunk allowed vsan 10
FC_switch_B_1# switchport trunk allowed vsan add 20
FC_switch_B_1# channel-group 1
fc1/36 added to port-channel 1 and disabled
```

l. 問題：両方のスイッチで次のコマンドを実行してポートを再起動します。

「シャットダウンなし」

m. ファブリック内の他の ISL ポートに対して、ここまでの手順を繰り返します。

n. 同じファブリック内の両方のスイッチで、ネイティブ VSAN をポートチャネルインターフェイスに追加します。

'interface port-channel_number_

'witchport トランク許可 VSAN add_native_san_id_

o. ポートチャネルの設定を確認します。

'how interface port-channel_number

ポートチャネルの属性は次のとおりです。

- ポートチャネルの状態は「 trunking 」です。
- 管理ポートモードは E 、トランクモードはオンです。
- 速度は、すべての ISL リンク速度の累積値です。

  たとえば、 2 つの ISL ポートが 4Gbps で動作している場合は 8Gbps です。

- 「 Trunk vsans (admin allowed and active) 」には、許可されているすべての VSAN が表示されます。
- 「 Trunk vsans (up) 」は、許可されているすべての VSAN を表示します。
- メンバーリストには、 port-channel に追加されたすべての ISL ポートを表示。
- ポート VSAN の番号は、 ISL を含む VSAN と同じ（通常はネイティブの vsan 1 ）。

```
FC_switch_A_1(config-if)# show int port-channel 1
port-channel 1 is trunking
    Hardware is Fibre Channel
    Port WWN is 24:01:54:7f:ee:e2:8d:a0
    Admin port mode is E, trunk mode is on
    snmp link state traps are enabled
    Port mode is TE
    Port vsan is 1
    Speed is 8 Gbps
    Trunk vsans (admin allowed and active) (1,10,20)
    Trunk vsans (up)                       (1,10,20)
    Trunk vsans (isolated)                 ()
    Trunk vsans (initializing)             ()
    5 minutes input rate 1154832 bits/sec,144354 bytes/sec, 170
frames/sec
    5 minutes output rate 1299152 bits/sec,162394 bytes/sec, 183
frames/sec
      535724861 frames input,1069616011292 bytes
        0 discards,0 errors
        0 invalid CRC/FCS,0 unknown class
        0 too long,0 too short
      572290295 frames output,1144869385204 bytes
        0 discards,0 errors
      5 input OLS,11  LRR,2 NOS,0 loop inits
      14 output OLS,5 LRR, 0 NOS, 0 loop inits
    Member[1] : fc1/36
    Member[2] : fc1/40
    Interface last changed at Thu Oct 16 11:48:00 2014
```

a. 両方のスイッチでインターフェイス設定を終了します。

「 end 」と入力します

b. 両方のファブリックで、更新された設定をスタートアップ設定にコピーします。

'copy running-config startup-config

```
FC_switch_A_1(config-if)# end
FC_switch_A_1# copy running-config startup-config

FC_switch_B_1(config-if)# end
FC_switch_B_1# copy running-config startup-config
```

a. 2 つ目のスイッチファブリックで、ここまでの手順を繰り返します。

関連情報

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

Cisco 9250i FC スイッチのシングル ISL に対する FCIP ポートの設定

FCIP プロファイルとインターフェイスを作成して IPStorage1/1 GbE インターフェイスに割り当てることで、 ISL を接続する FCIP スイッチポート（ E ポート）を設定する必要があります。

このタスクについて

このタスクは、各スイッチが IPStorage1/1 インターフェイスを使用し、スイッチファブリックごとに 1 つの ISL を使用する構成にのみ該当します。

このタスクは FC スイッチごとに行う必要があります。

各スイッチに 2 つの FCIP プロファイルを作成します。

- ファブリック 1
  - FC_switch_A_1 で FCIP プロファイル 11 および 111 を設定します。
  - FC_switch_B_1 で FCIP プロファイル 12 および 121 を設定します。
- ファブリック 2
  - FC_switch_A_2 で FCIP プロファイル 13 および 131 を設定しています。
  - FC_switch_B_2 に FCIP プロファイル 14 および 141 を設定します。

手順

1. コンフィギュレーションモードを開始します。

   'config t`

2. FCIP を有効にします。

   「機能 FCIP`

3. IPStorage1/1 GbE インターフェイスを設定します。

   a. コンフィギュレーションモードを開始します。

      「 conf t`

   b. IPStorage1/1 インターフェイスを指定します。

      インターフェイス IPStorage1/1

   c. IP アドレスとサブネットマスクを指定します。

      'interface_ip-address__subnet-mask_`

   d. MTU サイズを 2500 に指定します。

      'witchport mtu 2500`

e. ポートを有効にします。

「シャットダウンなし」

f. 構成モードを終了します。

「 exit

次の例は、 IPStorage1/1 ポートの設定を示しています。

```
conf t
interface IPStorage1/1
  ip address 192.168.1.201 255.255.255.0
  switchport mtu 2500
  no shutdown
exit
```

4. FC-VI トラフィック用の FCIP プロファイルを設定します。

a. FCIP プロファイルを設定し、 FCIP プロファイル構成モードに切り替えます。

FCIP profile_fcip -profile-name_`

プロファイル名は、設定するスイッチによって異なります。

b. IPStorage1/1 インターフェイスの IP アドレスを FCIP プロファイルに割り当てます。

「 ip address_ip-address_` 」

c. FCIP プロファイルを TCP ポート 3227 に割り当てます。

ポート 3227`

d. TCP を設定します。

「 tcp keepalive-timeout 1 」を参照してください

「 tcp max-retransmissions3 」

「 m ax-bandwidth-mbs 5000 minavailable-bandwidth-mbs 4500 round-trip -time-ms 3 」を参照してください

「 tcp min-retransmit-time 200 」

「 tcp keepalive-timeout 1 」を参照してください

tcp pmtu-enable reset-timeout 3600

「 tcp sack -enable 」「 no tcp cwm 」を選択します

次の例は、 FCIP プロファイルの設定を示しています。

```
conf t
fcip profile 11
  ip address 192.168.1.333
  port 3227
  tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-
time-ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm
```

5. ストレージトラフィック用の FCIP プロファイルを設定します。

   a. 111 という名前で FCIP プロファイルを設定し、 FCIP プロファイル構成モードに切り替えます。

      FCIP プロファイル 111'

   b. IPStorage1/1 インターフェイスの IP アドレスを FCIP プロファイルに割り当てます。

      「 ip address_ip-address_` 」

   c. FCIP プロファイルを TCP ポート 3229 に割り当てます。

      ポート 3229`

   d. TCP を設定します。

      「 tcp keepalive-timeout 1 」を参照してください

      「 tcp max-retransmissions3 」

      「 m ax-bandwidth-mbs 5000 minavailable-bandwidth-mbs 4500 round-trip -time-ms 3 」を参照してください

      「 tcp min-retransmit-time 200 」

      「 tcp keepalive-timeout 1 」を参照してください

      tcp pmtu-enable reset-timeout 3600

      「 tcp sack -enable 」「 no tcp cwm 」を選択します

次の例は、 FCIP プロファイルの設定を示しています。

```
conf t
fcip profile 111
  ip address 192.168.1.334
  port 3229
  tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-
time-ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm
```

6. 2 つのうちの 1 つ目の FCIP インターフェイスを作成します。

   インターフェイス fcip 1'

   このインターフェイスは FC-IV トラフィックに使用します。

   a. 前の手順で作成したプロファイル 11 を選択します。

      「 USE - profile 11` 」

   b. パートナースイッチの IPStorage1/1 ポートの IP アドレスとポート番号を設定します。

      'peer-info ipaddr_partner-switch-port-ip_port 3227'

   c. TCP 接続 2 を選択します。

      「 tcp-connection 2 」

   d. 圧縮を無効にします。

      「 IP 圧縮なし」

   e. インターフェイスを有効にします。

      「シャットダウンなし」

   f. 制御 TCP 接続を 48 、データ接続を 26 に設定して、その Differentiated Services Code Point （ DSCP ）値のすべてのパケットをマークします。

      'qos control 48 data 26`

   g. インターフェイスコンフィギュレーションモードを終了します。

      「 exit

次の例は、 FCIP インターフェイスの設定を示しています。

```
interface fcip  1
  use-profile 11
# the port # listed in this command is the port that the remote switch
is listening on
 peer-info ipaddr 192.168.32.334   port 3227
  tcp-connection 2
  no ip-compression
  no shutdown
  qos control 48 data 26
exit
```

7. 2 つのうちの 2 つ目の FCIP インターフェイスを作成します。

「 interface fcip 2 」と入力します

このインターフェイスはストレージトラフィックに使用されます。

a. 前の手順で作成したプロファイル 111 を選択します。

'USE - profile 111'

b. パートナースイッチの IPStorage1/1 ポートの IP アドレスとポート番号を設定します。

'peer-info ipaddr_partner-switch-port-ip_port 3229

c. TCP 接続 2 を選択します。

「 tcp-connection 5 」

d. 圧縮を無効にします。

「 IP 圧縮なし」

e. インターフェイスを有効にします。

「シャットダウンなし」

f. 制御 TCP 接続を 48 、データ接続を 26 に設定して、その Differentiated Services Code Point （ DSCP ）値のすべてのパケットをマークします。

'qos control 48 data 26`

g. インターフェイスコンフィギュレーションモードを終了します。

「 exit

次の例は、 FCIP インターフェイスの設定を示しています。

```
interface fcip  2
  use-profile 11
# the port # listed in this command is the port that the remote switch
is listening on
 peer-info ipaddr 192.168.32.33e  port 3229
  tcp-connection 5
  no ip-compression
  no shutdown
  qos control 48 data 26
exit
```

8. FCIP 1 インターフェイスのスイッチポートを設定します。
   a. コンフィギュレーションモードを開始します。

      'config t`

   b. 設定するポートを指定します。

      インターフェイス fcip 1'

   c. ポートをシャットダウンします。

      「ダウンタイム」

   d. ポートを E モードに設定します。

      'witchport mode E`

   e. ポートのトランクモードをイネーブルにします。

      'witchport trunk mode on `

   f. トランクで許可される VSAN を 10 に設定します。

      'witchport トランクでは VSAN 10 を許可

   g. ポートの速度を設定します。

      'witchport speed_speed - value_

9. FCIP 2 インターフェイスのスイッチポートを設定します。
   a. コンフィギュレーションモードを開始します。

      'config t`

   b. 設定するポートを指定します。

      「 interface fcip 2 」と入力します

c. ポートをシャットダウンします。

「ダウンタイム」

d. ポートを E モードに設定します。

'witchport mode E`

e. ポートのトランクモードをイネーブルにします。

'witchport trunk mode on `

f. トランクで許可される VSAN を 20 に設定します。

「 witchport trunk allowed vsan 20` 」

g. ポートの速度を設定します。

'witchport speed_speed - value_

10. 2 つ目のスイッチで、上記の手順を繰り返します。

ただし、適切な IP アドレスと一意の FCIP プロファイル名を使用してください。

- 1 つ目のスイッチファブリックの設定では、 FC_switch_B_1 で FCIP プロファイル 12 および 121 を設定します。
- 1 つ目のスイッチファブリックの設定では、 FC_switch_A_2 で FCIP プロファイル 13 および 131 を設定し、 FC_switch_B_2 で FCIP プロファイル 14 および 141 を設定します。

11. 両方のスイッチでポートを再起動します。

「シャットダウンなし」

12. 両方のスイッチでインターフェイス設定を終了します。

「 end 」と入力します

13. 両方のスイッチで、更新された設定をスタートアップ設定にコピーします。

'copy running-config startup-config

```
FC_switch_A_1(config-if)# end
FC_switch_A_1# copy running-config startup-config

FC_switch_B_1(config-if)# end
FC_switch_B_1# copy running-config startup-config
```

14. 2 つ目のスイッチファブリックで、ここまでの手順を繰り返します。

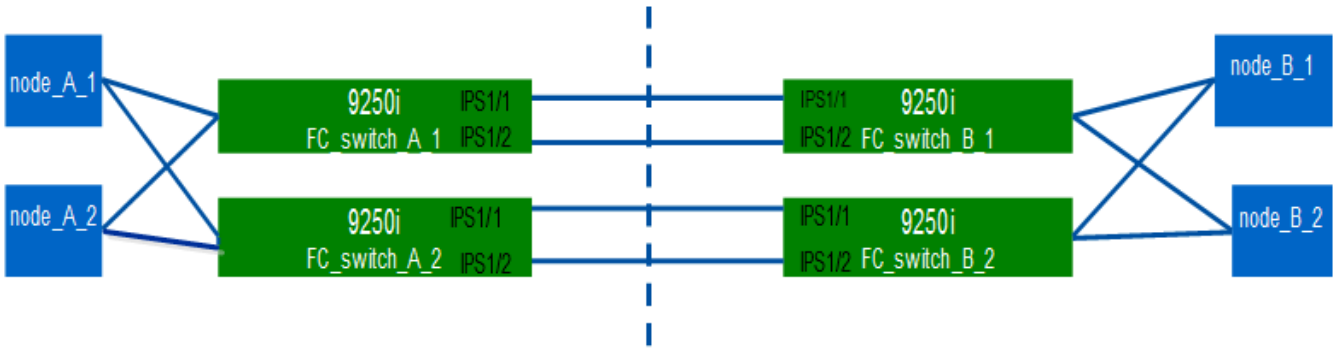
Cisco 9250i FC スイッチのデュアル **ISL** に対する **FCIP** ポートの設定

FCIP プロファイルとインターフェイスを作成して IPStorage1/1 および IPStorage1/2 GbE インターフェイスに割り当てることで、 ISL を接続する FCIP スイッチポート（ E ポート）を設定する必要があります。

このタスクについて

このタスクは、各スイッチで IPStorage1/1 および IPStorage1/2 GbE インターフェイスを使用し、スイッチファブリックごとに 2 つの ISL を使用する構成にのみ該当します。

このタスクは FC スイッチごとに行う必要があります。



このタスクと例で使用するプロファイル設定の表は次のとおりです。

- [fabric1_table]
- [fabric2_table]
- ファブリック 1 プロファイル設定表 *

スイッチファブリック	IPStorage インターフェイス	IP アドレス	ポートタイプ	FCIP インターフェイス	FCIP プロファイル	ポート	IP/port をピアリングします	VSAN ID
FC_switch_A_1 を使用します	IPStorage 1/1	1. a. a. a.	FC-VI	FCIP 1.	15	3220	1. c. c. c/3230	10.
ストレージ	FCIP 2.	20	3221	1. c. c. c/3231	20	IPStorage 1/2	b.b.b.b.b.b .b.b.b	FC-VI
FCIP 3.	25	3222	1. d d / 3232	10.	ストレージ	FCIP 4.	30	3223
1. d d / 3233	20	FC_switch_B_1	IPStorage 1/1	c.c.c	FC-VI	FCIP 1.	15	3230
A.a.a/3220 の例	10.	ストレージ	FCIP 2.	20	3231	1. a. a/ 3221	20	IPStorage 1/2
d.d.d.d.d	FC-VI	FCIP 3.	25	3232	1. b. b. b b/3222	10.	ストレージ	FCIP 4.

• ファブリック 2 プロファイル設定表 *

スイッチファブリック	IPStorage インターフェイス	IP アドレス	ポートタイプ	FCIP インターフェイス	FCIP プロファイル	ポート	IP/port をピアリングします	VSAN ID
FC_switch_A_2	IPStorage 1/1	e.e	FC-VI	FCIP 1.	15	3220	G.G.g/3230	10.
ストレージ	FCIP 2.	20	3221	G.gg/3231	20	IPStorage 1/2	f.f.f.f.f	FC-VI
FCIP 3.	25	3222	H.H/3232	10.	ストレージ	FCIP 4.	30	3223
H.H/3233	20	FC_switch_B_2	IPStorage 1/1	g.g.g.g.g	FC-VI	FCIP 1.	15	3230
例： /3220	10.	ストレージ	FCIP 2.	20	3231	例： 3221	20	IPStorage 1/2
h.h.h.h	FC-VI	FCIP 3.	25	3232	1. f. f. /3222	10.	ストレージ	FCIP 4.

手順

1. コンフィギュレーションモードを開始します。

   'config t`

2. FCIP を有効にします。

   「機能 FCIP`

3. 各スイッチで、 2 つの IPStorage インターフェイス（「 IPStorage1/1 」および「 IPStorage1/2 」）を設定します。

   a. [[[[[['['a ']] 構成モードに切り替えます :

      「 conf t`

   b. 作成する IPStorage インターフェイスを指定します。

      'interface_ipstorage_`

      IPstorage パラメータ値は "`IPStorage1/1 `" または "IPStorage1/2 `" です

   c. 前の手順で指定した IPStorage インターフェイスの IP アドレスとサブネットマスクを指定します。

      'interface_ip-address__subnet-mask_`

各スイッチで、 IPStorage インターフェイス「 IPStorage1/1 」と「 IPStorage1/2 」には異なる IP アドレスを指定する必要があります。

a. MTU サイズを 2500 に指定します。

'witchport mtu 2500`

b. ポートを有効にします。

「シャットダウンなし」

c. [[suf, 手順 "f`"] 構成モードを終了します。

「 exit

d. 繰り返します [substep_a] から [substep_f] IPStorage1/2 GbE インターフェイスを別の IP アドレスで設定します。

4. プロファイル設定の表に記載されたプロファイル名を使用して、 FC-VI トラフィック用とストレージトラフィック用の FCIP プロファイルを設定します。

a. コンフィギュレーションモードを開始します。

「 conf t`

b. 次のプロファイル名で FCIP プロファイルを設定します。

FCIP profile_fcip -profile-name_`

次に '*fcip -profile-name*' パラメータの値を示します

- IPStorage1/1 の FC-VI ： 15
- IPStorage1/1 のストレージ： 20
- IPStorage1/2 上の FC-VI は 25 です
- IPStorage1/2 にストレージを指定した場合は 30 個

c. プロファイル設定の表に従って、 FCIP プロファイルのポートを割り当てます。

「 port_port_number_` 」のようになります

d. TCP を設定します。

「 tcp keepalive-timeout 1 」を参照してください

「 tcp max-retransmissions3 」

「 m ax-bandwidth-mbs 5000 minavailable-bandwidth-mbs 4500 round-trip -time-ms 3 」を参照してください

「 tcp min-retransmit-time 200 」

「 tcp keepalive-timeout 1 」を参照してください

tcp pmtu-enable reset-timeout 3600

「 tcp sack-enable 」を入力します

「 no tcp CWM 」

5. FCIP インターフェイスを作成します。

interface fcp_fcp_interface_`

パラメータの値は '*fcp_interface*' で ' プロファイル設定テーブルに表示されているように '1"2'3' または 4` です

a. 前の手順で作成したプロファイルにインターフェイスをマッピングします。

'use-profile_profile_

b. ピア IP アドレスとピアプロファイルポート番号を設定します。

'peer-info_peer_ipstorage_ipaddr_port_peer_port_port_number_`

c. TCP 接続を選択します。

「 tcp-connection_connection-#_ 」

パラメータの値は 'FC-VI プロファイルの場合は 2" ストレージ・プロファイルの場合は 5' です

a. 圧縮を無効にします。

「 IP 圧縮なし」

b. インターフェイスを有効にします。

「シャットダウンなし」

c. 制御 TCP 接続を「 48 」に設定し、データ接続を「 26 」に設定して、 DSCP 値が異なるすべてのパケットをマークします。

'qos control 48 data 26`

d. 構成モードを終了します。

「 exit

6. 各 FCIP インターフェイスのスイッチポートを設定します。

a. コンフィギュレーションモードを開始します。

'config t`

b. 設定するポートを指定します。

インターフェイス fcip 1'

c. ポートをシャットダウンします。

「ダウンタイム」

d. ポートを E モードに設定します。

'witchport mode E`

e. ポートのトランクモードをイネーブルにします。

'witchport trunk mode on `

f. 特定の VSAN で許可されるトランクを指定します。

'witchport trunk allowed vsan_vsan_id_`

_vsan_id_parameter 値は 'FC-VI プロファイルの場合は「 VSAN 10 」 ' ストレージ・プロファイルの場合は「 VSAN 20 」です

a. ポートの速度を設定します。

'witchport speed_speed - value_

b. 構成モードを終了します。

「 exit

7. 両方のスイッチで、更新された設定をスタートアップ設定にコピーします。

'copy running-config startup-config

次の例は、ファブリック 1 のスイッチ FC_switch_A_1 および FC_switch_B_1 で 2 つの ISL を使用する場合の FCIP ポートの設定を示しています。

- FC_switch_A_1 では、次のコマンドを実行します。

```
FC_switch_A_1# config t
FC_switch_A_1(config)# no in-order-guarantee vsan 10
FC_switch_A_1(config-vsan-db)# end
FC_switch_A_1# copy running-config startup-config

# fcip settings

feature  fcip

conf t
interface IPStorage1/1
#  IP address:  a.a.a.a
#  Mask:  y.y.y.y
  ip address <a.a.a.a   y.y.y.y>
```

```
  switchport mtu 2500
  no shutdown
exit
conf t
fcip profile 15
  ip address <a.a.a.a>
  port 3220
  tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm

conf t
fcip profile 20
  ip address <a.a.a.a>
  port 3221
  tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm

conf t
interface IPStorage1/2
#  IP address:  b.b.b.b
#  Mask:  y.y.y.y
  ip address <b.b.b.b   y.y.y.y>
  switchport mtu 2500
  no shutdown
exit

conf t
fcip profile 25
  ip address <b.b.b.b>
  port 3222
tcp keepalive-timeout 1
tcp max-retransmissions 3
```

```
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm

conf t
fcip profile 30
  ip address <b.b.b.b>
  port 3223
tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm
interface fcip  1
  use-profile 15
# the port # listed in this command is the port that the remote switch is
listening on
 peer-info ipaddr <c.c.c.c>  port 3230
  tcp-connection 2
  no ip-compression
  no shutdown
  qos control 48 data 26
exit

interface fcip  2
  use-profile 20
# the port # listed in this command is the port that the remote switch is
listening on
 peer-info ipaddr <c.c.c.c>  port 3231
  tcp-connection 5
  no ip-compression
  no shutdown
  qos control 48 data 26
exit

interface fcip  3
  use-profile 25
# the port # listed in this command is the port that the remote switch is
```

```
listening on
 peer-info ipaddr < d.d.d.d >  port 3232
  tcp-connection 2
  no ip-compression
  no shutdown
  qos control 48 data 26
exit

interface fcip  4
  use-profile 30
# the port # listed in this command is the port that the remote switch is
listening on
 peer-info ipaddr < d.d.d.d >  port 3233
  tcp-connection 5
  no ip-compression
  no shutdown
  qos control 48 data 26
exit

conf t
interface fcip  1
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 10
no shutdown
exit

conf t
interface fcip  2
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 20
no shutdown
exit

conf t
interface fcip  3
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 10
no shutdown
exit
```

```
conf t
interface fcip  4
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 20
no shutdown
exit
```

- FC_switch_B_1 の場合：

```
FC_switch_A_1# config t
FC_switch_A_1(config)# in-order-guarantee vsan 10
FC_switch_A_1(config-vsan-db)# end
FC_switch_A_1# copy running-config startup-config

# fcip settings

feature  fcip

conf t
interface IPStorage1/1
#  IP address:  c.c.c.c
#  Mask:  y.y.y.y
  ip address <c.c.c.c   y.y.y.y>
  switchport mtu 2500
  no shutdown
exit

conf t
fcip profile 15
  ip address <c.c.c.c>
  port 3230
  tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm

conf t
fcip profile 20
```

```
  ip address <c.c.c.c>
  port 3231
  tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm

conf t
interface IPStorage1/2
#  IP address:  d.d.d.d
#  Mask:  y.y.y.y
  ip address <b.b.b.b   y.y.y.y>
  switchport mtu 2500
  no shutdown
exit

conf t
fcip profile 25
  ip address <d.d.d.d>
  port 3232
tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm

conf t
fcip profile 30
  ip address <d.d.d.d>
  port 3233
tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
```

```
  tcp sack-enable
  no tcp cwm

interface fcip  1
  use-profile 15
# the port # listed in this command is the port that the remote switch is
listening on
 peer-info ipaddr <a.a.a.a>  port 3220
  tcp-connection 2
  no ip-compression
  no shutdown
  qos control 48 data 26
exit

interface fcip  2
  use-profile 20
# the port # listed in this command is the port that the remote switch is
listening on
 peer-info ipaddr <a.a.a.a>  port 3221
  tcp-connection 5
  no ip-compression
  no shutdown
  qos control 48 data 26
exit

interface fcip  3
  use-profile 25
# the port # listed in this command is the port that the remote switch is
listening on
 peer-info ipaddr < b.b.b.b >  port 3222
  tcp-connection 2
  no ip-compression
  no shutdown
  qos control 48 data 26
exit

interface fcip  4
  use-profile 30
# the port # listed in this command is the port that the remote switch is
listening on
 peer-info ipaddr < b.b.b.b >  port 3223
  tcp-connection 5
  no ip-compression
  no shutdown
  qos control 48 data 26
exit
```

```
conf t
interface fcip  1
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 10
no shutdown
exit

conf t
interface fcip  2
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 20
no shutdown
exit

conf t
interface fcip  3
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 10
no shutdown
exit

conf t
interface fcip  4
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 20
no shutdown
exit
```

Cisco FC スイッチでゾーニングを設定する

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

このタスクについて

この手順は、両方の FC スイッチファブリックで実行する必要があります。

次の手順では、「4 ノードMetroCluster構成の FibreBridge 7500N のゾーニング」セクションで説明されているゾーニングを使用します。

手順

1. 既存のゾーンとゾーンセットがある場合は消去します。

   a. アクティブなゾーンおよびゾーンセットを特定します。

      「ゾーンセットのアクティブ化」

      ```
      FC_switch_A_1# show zoneset active

      FC_switch_B_1# show zoneset active
      ```

   b. 前の手順で特定したアクティブなゾーンセットを無効にします。

      'no zoneset activate name_vszone_name_vsan_vsan_id'

      次の例は、 2 つのゾーンセットを無効にする方法を示しています。

      - VSAN 10 内の FC_switch_A_1 の ZoneSet_A
      - VSAN 20 内の FC_switch_B_1 の ZoneSet_B

      ```
      FC_switch_A_1# no zoneset activate name ZoneSet_A vsan 10

      FC_switch_B_1# no zoneset activate name ZoneSet_B vsan 20
      ```

   c. すべてのゾーンセットが非アクティブになったら、ゾーンデータベースをクリアします。

      clear zone database-zone-name_`

   ```
   FC_switch_A_1# clear zone database 10
   FC_switch_A_1# copy running-config startup-config

   FC_switch_B_1# clear zone database 20
   FC_switch_B_1# copy running-config startup-config
   ```

2. スイッチのワールドワイド名（ WWN ）を取得します。

   'How WWN switch`

3. ゾーンの基本設定を行います。

   a. デフォルトのゾーニング・ポリシーを "permit" に設定します

      no system default zone default-zone permit

   b. フルゾーン配信を有効にします。

「システムデフォルトゾーンは完全に配布」

c. VSAN ごとにデフォルトのゾーニングポリシーを設定します。

no zone default-zone permit_vsanId_`

d. VSAN ごとにデフォルトのフルゾーン配信を設定します。

zoneset distribute full_vsanId_`

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# no system default zone default-zone permit
FC_switch_A_1(config)# system default zone distribute full
FC_switch_A_1(config)# no zone default-zone permit 10
FC_switch_A_1(config)# no zone default-zone permit 20
FC_switch_A_1(config)# zoneset distribute full vsan 10
FC_switch_A_1(config)# zoneset distribute full vsan 20
FC_switch_A_1(config)# end
FC_switch_A_1# copy running-config startup-config

FC_switch_B_1# conf t
FC_switch_B_1(config)# no system default zone default-zone permit
FC_switch_B_1(config)# system default zone distribute full
FC_switch_B_1(config)# no zone default-zone permit 10
FC_switch_B_1(config)# no zone default-zone permit 20
FC_switch_B_1(config)# zoneset distribute full vsan 10
FC_switch_B_1(config)# zoneset distribute full vsan 20
FC_switch_B_1(config)# end
FC_switch_B_1# copy running-config startup-config
```

4. ストレージゾーンを作成し、ストレージポートを追加します。



次の手順は、ファブリックごとに 1 つのスイッチだけで実行します。

ゾーニングは、使用している FC-to-SAS ブリッジのモデルによって異なります。詳細については、ブリッジのモデルに対応するセクションを参照してください。例では Brocade スイッチポートを使用しているため、適宜ポートを調整してください。

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

各ストレージゾーンには、すべてのコントローラの HBA イニシエータポートと、 FC-to-SAS ブリッジを接続するポートが 1 つ含まれます。

a. ストレージゾーンを作成します。

'zone name_STOR-zone-name_vsanId_`

b. ストレージポートをゾーンに追加します。

「 member-portswitch WWN 」というエラーが表示されます

c. ゾーンセットをアクティブにします。

zoneset activate name_STOR-zone-name-setname_vsan_vsan-id_`

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# zone name STOR_Zone_1_20_25 vsan 20
FC_switch_A_1(config-zone)# member interface fc1/5 swwn
20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# member interface fc1/9 swwn
20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# member interface fc1/17 swwn
20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# member interface fc1/21 swwn
20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# member interface fc1/5 swwn
20:00:00:05:9b:24:12:99
FC_switch_A_1(config-zone)# member interface fc1/9 swwn
20:00:00:05:9b:24:12:99
FC_switch_A_1(config-zone)# member interface fc1/17 swwn
20:00:00:05:9b:24:12:99
FC_switch_A_1(config-zone)# member interface fc1/21 swwn
20:00:00:05:9b:24:12:99
FC_switch_A_1(config-zone)# member interface fc1/25 swwn
20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# end
FC_switch_A_1# copy running-config startup-config
```

5. ストレージ・ゾーン・セットを作成し ' 新しいセットにストレージ・ゾーンを追加します

ファブリック内の 1 つのスイッチだけで、次の手順を実行します。

a. ストレージゾーンセットを作成します。

zoneset name_STOR-zone-set-name_vsan_vsan-id_`

b. ストレージゾーンをゾーンセットに追加します。

「 member_STOR-zone-name_` 」

c. ゾーンセットをアクティブにします。

zoneset activate name_STOR-zone-set-name_vsanId_`

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# zoneset name STORI_Zoneset_1_20 vsan 20
FC_switch_A_1(config-zoneset)# member STOR_Zone_1_20_25
...
FC_switch_A_1(config-zoneset)# exit
FC_switch_A_1(config)# zoneset activate name STOR_ZoneSet_1_20 vsan 20
FC_switch_A_1(config)# exit
FC_switch_A_1# copy running-config startup-config
```

6. FCVI ゾーンを作成して、 FCVI ポートを追加します。

   各 FCVI ゾーンには、 1 つの DR グループのすべてのコントローラから FCVI ポートが含まれます。

   ファブリック内の 1 つのスイッチだけで、次の手順を実行します。

   ゾーニングは、使用している FC-to-SAS ブリッジのモデルによって異なります。詳細については、ブリッジのモデルに対応するセクションを参照してください。例では Brocade スイッチポートを使用しているため、適宜ポートを調整してください。

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

   各ストレージゾーンには、すべてのコントローラの HBA イニシエータポートと、 FC-to-SAS ブリッジを接続するポートが 1 つ含まれます。

   a. FCVI ゾーンを作成します。

      'zone name_FCVI-zone-name_vsanId_`

   b. FCVI ポートをゾーンに追加します。

      「 member_fcvi -zone-name_` 」

   c. ゾーンセットをアクティブにします。

      zoneset activate name_FCVI-zone-name-set-name_vsanId_`

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# zone name FCVI_Zone_1_10_25 vsan 10
FC_switch_A_1(config-zone)# member interface fc1/1
swwn20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# member interface fc1/2
swwn20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# member interface fc1/1
swwn20:00:00:05:9b:24:12:99
FC_switch_A_1(config-zone)# member interface fc1/2
swwn20:00:00:05:9b:24:12:99
FC_switch_A_1(config-zone)# end
FC_switch_A_1# copy running-config startup-config
```

7. FCVI ゾーンセットを作成して、 FCVI ゾーンを追加します。

   ファブリック内の 1 つのスイッチだけで、次の手順を実行します。

   a. FCVI ゾーンセットを作成します。

      zoneset name_FCVI_zone_set_name_VSAN_vsan-id_`

   b. FCVI ゾーンをゾーンセットに追加します。

      「 member_FCVI_zonename_` 」

   c. ゾーンセットをアクティブにします。

      zoneset activate name_FCVI_zone_set_name_vsan_vsan-id_`

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# zoneset name FCVI_Zoneset_1_10 vsan 10
FC_switch_A_1(config-zoneset)# member FCVI_Zone_1_10_25
FC_switch_A_1(config-zoneset)# member FCVI_Zone_1_10_29
    ...
FC_switch_A_1(config-zoneset)# exit
FC_switch_A_1(config)# zoneset activate name FCVI_ZoneSet_1_10 vsan 10
FC_switch_A_1(config)# exit
FC_switch_A_1# copy running-config startup-config
```

8. ゾーニングを検証します。

   「ゾーンの方法」

9. 2 つ目の FC スイッチファブリックで、ここまでの手順を繰り返します。

すべてのスイッチで、 FC スイッチの設定がスタートアップ設定に保存されたことを確認する必要があります。

ステップ

両方の FC スイッチファブリックに対して次のコマンドを問題で実行します。

'copy running-config startup-config

```
FC_switch_A_1# copy running-config startup-config

FC_switch_B_1# copy running-config startup-config
```

FC-to-SAS ブリッジおよび SAS ディスクシェルフを設置

新しいストレージを構成に追加する際には、 ATTO FibreBridge ブリッジおよび SAS ディスクシェルフを設置してケーブル接続します。

このタスクについて

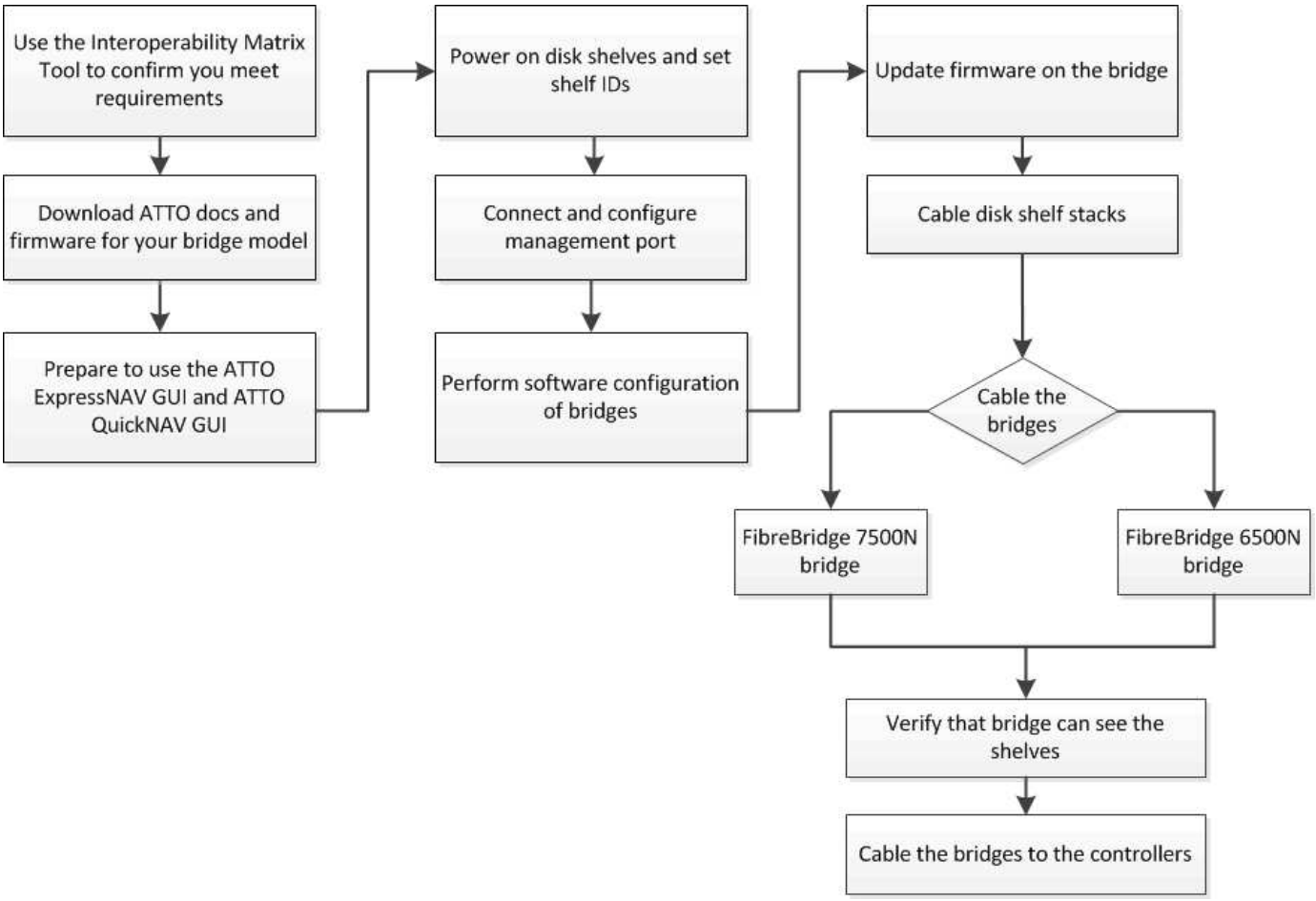
工場出荷状態のシステムの場合は、 FC-to-SAS は事前に構成されているため、追加の構成は不要です。

この手順は、推奨されるブリッジ管理インターフェイスである ATTO ExpressNAV GUI と ATTO QuickNAV ユーティリティを使用していることを前提としています。

ATTO ExpressNAV GUI は、ブリッジの設定および管理、ブリッジファームウェアの更新に使用します。ATTO QuickNAV ユーティリティは、ブリッジのイーサネット管理 1 ポートの設定に使用します。

シリアルポートや Telnet を使用してブリッジの設定と管理、イーサネット管理 1 ポートの設定を行ったり、 FTP を使用してブリッジファームウェアを更新するなど、必要に応じて他の管理インターフェイスも使用できます。

この手順では次のワークフローを使用します。



FC-to-SAS ブリッジのインバンド管理

ONTAP 9.5 以降では、 FibreBridge 7500N / 7600N ブリッジについて、 IP 管理に代わる方法としてインバンド管理 _ がサポートされます。ONTAP 9.8 以降では、アウトオブバンド管理は廃止されています。

ONTAP 9.8 以降では 'storage bridge コマンドは 'system bridge コマンドに置き換えられました次の手順は「 storage bridge 」コマンドを示していますが、 ONTAP 9.8 以降を実行している場合は「 system bridge 」コマンドが優先されます。

インバンド管理を使用すると、 ONTAP CLI からブリッジへの FC 接続を介してブリッジを管理および監視できます。ブリッジのイーサネットポートを介してブリッジに物理的にアクセスする必要がないため、ブリッジのセキュリティの脆弱性が軽減されます。

ブリッジのインバンド管理が可能かどうかは、 ONTAP のバージョンによって異なります。

- ONTAP 9.8 以降では、ブリッジはデフォルトでインバンド接続を介して管理され、 SNMP を介したブリッジのアウトオブバンド管理は廃止されています。
- ONTAP 9.5 から 9.7 ：インバンド管理またはアウトオブバンド管理のどちらかで SNMP 管理がサポートされます。
- ONTAP 9.5 よりも前のバージョンでは、アウトオブバンドの SNMP 管理のみがサポートされます。

ブリッジの CLI コマンドは、 ONTAP インターフェイスで実行する ONTAP インターフェイスの「 storage bridge run -cli-name_bridge_name_-command_command_name_ 」コマンドから実行できます。

ブリッジへの物理接続を制限してセキュリティを強化するために、IPアクセスを無効にしたインバンド管理を使用することを推奨します。

FibreBridge 7600N / 7500Nブリッジの制限と接続ルール

FibreBridge 7600N / 7500Nブリッジを接続する際の制限と考慮事項を確認してください。

FibreBridge 7600N / 7500Nブリッジの制限

- HDDドライブとSSDドライブの組み合わせの最大数は240です。
- SSDドライブの最大数は96です。
- SASポートあたりのSSDの最大数は48です。
- SASポートあたりのシェルフの最大数は10です。

FibreBridge 7600N / 7500Nブリッジ接続ルール

- 同じSASポートにSSDドライブとHDDドライブを混在させないでください。
- シェルフをSASポートに均等に分散します。
- 他のシェルフタイプ（DS212やDS224シェルフなど）と同じSASポートにDS460シェルフを配置しないでください。

設定例

次の例は、SSDドライブを搭載した4台のDS224シェルフとHDDドライブを搭載した6台のDS224シェルフを接続する構成を示しています。

SAS ポート	シェルフとドライブ
SASポートA	SSDを搭載したDS224シェルフ×2
SASポートB	SSDを搭載したDS224シェルフ×2
SASポートC	HDDドライブ搭載のDS224シェルフ×3
SASポートD	HDDドライブ搭載のDS224シェルフ×3

インストールの準備

新しい MetroCluster システムで使用するブリッジの設置を準備する際には、システムが一定の要件を満たしていることを確認する必要があります。これには、ブリッジのセットアップや構成の要件と、必要なドキュメント、 ATTO QuickNAV ユーティリティ、ブリッジファームウェアのダウンロードなどがあります。

作業を開始する前に

- システムキャビネットに付属していない場合は、システムをラックに設置しておく必要があります。
- サポートされているハードウェアモデルとソフトウェアバージョンを使用している必要があります。

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

- 各 FC スイッチで、 1 つの FC ポートを 1 つのブリッジに接続できる必要があります。

- SAS ケーブルの取り扱い方法、およびディスクシェルフの設置とケーブル接続に関する考慮事項とベストプラクティスを確認しておく必要があります。

  考慮事項とベストプラクティスについては、使用しているディスクシェルフモデルの『 Installation and Service Guide 』を参照してください。

- ブリッジの設定に使用するコンピュータでは、 ATTO ExpressNAV GUI を使用するために、 ATTO でサポートされている Web ブラウザを実行している必要があります。

  ATTO Product Release Notes に、サポートされている Web ブラウザの最新のリストが掲載されています。このドキュメントには、以下の手順で説明する ATTO の Web サイトからアクセスできます。

手順

1. 使用しているディスクシェルフモデルの Installation and Service Guide をダウンロードします。
   a. FibreBridge のモデルに対応するリンクを使用して ATTO の Web サイトにアクセスし、マニュアルと QuickNAV ユーティリティをダウンロードします。

      管理インターフェイスの詳細については、使用しているモデルブリッジに対応した ATTO FibreBridge Installation and Operation Manual を参照してください。

      ATTO FibreBridge の説明ページに記載されているリンクを使用して、このコンテンツや ATTO Web サイト上のその他のコンテンツにアクセスできます。

2. 推奨されるブリッジ管理インターフェイス、 ATTO ExpressNAV GUI および ATTO QuickNAV ユーティリティを使用するために必要なハードウェアおよび情報を収集します。
   a. デフォルト以外のユーザ名とパスワードを決定します（ブリッジへのアクセス用）。

      デフォルトのユーザ名とパスワードは変更してください。

   b. ブリッジの IP 管理を設定する場合は、ブリッジに付属のシールド付きイーサネットケーブル（ブリッジのイーサネット管理 1 ポートとネットワークの接続に使用）が必要です。
   c. ブリッジの IP 管理を設定する場合は、各ブリッジのイーサネット管理 1 ポートの IP アドレス、サブネットマスク、およびゲートウェイの情報が必要です。
   d. セットアップに使用するコンピュータで VPN クライアントを無効にします。

      アクティブな VPN クライアント原因がブリッジの QuickNAV スキャンに失敗しました。

FC-to-SASブリッジおよび**SAS**シェルフの設置

システムが「インストールの準備」のすべての要件を満たしていることを確認したら、新しいシステムをインストールできます。

このタスクについて

- ディスクとシェルフの構成は両方のサイトで同じである必要があります。

  ミラーされていないアグリゲートを使用する場合は、各サイトでディスクとシェルフの構成が異なることがあります。

ミラーされたアグリゲートとミラーされていないアグリゲートのどちらに使用されているかに関係なく、ディザスタリカバリグループ内のディスクはすべて同じタイプの接続を使用し、ディザスタリカバリグループ内のすべてのノードから認識できる必要があります。

- 50 ミクロンのマルチモード光ファイバケーブルを使用するディスクシェルフ、 FC スイッチ、およびバックアップテープデバイスの最大距離に関するシステム接続要件が、 FibreBridge ブリッジにも該当します。

  "NetApp Hardware Universe の略"

次のシェルフと FibreBridge 7500N / 7600N ブリッジでは、追加のケーブル接続なしでインバンド ACP がサポートされます。

- ONTAP 9.2 以降の 7500N または 7600N ブリッジで接続された IOM12 （ DS460C ）
- ONTAP 9.1 以降の 7500N または 7600N ブリッジで接続された IOM12 （ DS212C および DS224C ）

MetroCluster 構成の SAS シェルフでは、 ACP ケーブル接続はサポートされません。

必要に応じて、 **FibreBridge 7600N** ブリッジの **IP** ポートアクセスを有効にします

9.5 より前のバージョンの ONTAP を使用している場合、または Telnet やその他の IP ポートプロトコルおよびサービス（ FTP 、 ExpressNAV 、 ICMP 、 QuickNAV ）を使用して FibreBridge 7600N ブリッジへのアウトオブバンドアクセスを使用する場合は、コンソールポート経由でアクセスサービスを有効にできます。

このタスクについて

ATTO FibreBridge 7500Nブリッジとは異なり、FibreBridge 7600Nブリッジは、すべてのIPポートプロトコルおよびサービスが無効になった状態で出荷されます。

ONTAP 9.5 以降では、ブリッジのインバンド管理 _ がサポートされます。これは、 ONTAP CLI からブリッジへの FC 接続を介してブリッジを設定および監視できることを意味します。ブリッジのイーサネットポートを介してブリッジに物理的にアクセスする必要がなく、ブリッジのユーザインターフェイスも必要ありません。

ONTAP 9.8 以降では、ブリッジの _ 帯域内管理 _ がデフォルトでサポートされ、アウトオブバンド SNMP 管理は廃止されています。

このタスクは、ブリッジの管理にインバンド管理を使用していない場合に必要です。この場合は、イーサネット管理ポートを介してブリッジを設定する必要があります。

手順

1. FibreBridge 7600Nブリッジのシリアルポートにシリアルケーブルを接続して、ブリッジのコンソールインターフェイスにアクセスします。
2. コンソールを使用してアクセスサービスを有効にし、設定を保存します。

   'et closePort none`

   'aveConfiguration'

   'set closePort none' コマンドを使用すると、ブリッジ上のすべてのアクセスサービスがイネーブルになり

ます。

3. 必要に応じて 'set closePort' コマンドを発行し ' 必要に応じてコマンドを繰り返して ' 必要なサービスをすべて無効にします

   'et closePort_service_`

   'set closePort' コマンドは ' 一度に 1 つのサービスを無効にします

   パラメータ「 *SERVICE*` 」は、次のいずれかとして指定できます。

   - エクプレスナヴ
   - FTP
   - ICMP
   - QuickNAV
   - SNMP
   - Telnet

   特定のプロトコルがイネーブルになっているかディセーブルになっているかを確認するには、 get closePort コマンドを使用します。

4. SNMP を有効にする場合は、次の問題コマンドも実行する必要があります。

   'Set SNMP enabled

   SNMP は、別個の enable コマンドを必要とする唯一のプロトコルです。

5. 設定を保存します。

   'aveConfiguration'

FC-to-SASブリッジを設定

モデルに応じた FC-to-SAS ブリッジのケーブル接続に進む前に、 FibreBridge ソフトウェアで設定を行う必要があります。

作業を開始する前に

ブリッジのインバンド管理を使用するかどうかを決めておく必要があります。

> ONTAP 9.8 以降では 'storage bridge コマンドは 'system bridge コマンドに置き換えられました 次の手順は「 storage bridge 」コマンドを示していますが、 ONTAP 9.8 以降を実行している場合は「 system bridge 」コマンドが優先されます。

このタスクについて

IP 管理ではなくブリッジのインバンド管理を使用する場合は、該当する手順に記載されているように、イーサネットポートと IP を設定する手順を省略できます。

手順

1. ATTO FibreBridge のシリアルコンソールポートを設定し、ポート速度を 1 、 000 詐欺検出用に設定します。

```
get serialportbaudrate
SerialPortBaudRate = 115200

Ready.

set serialportbaudrate 115200

Ready. *
saveconfiguration
Restart is necessary....
Do you wish to restart (y/n) ? y
```

2. インバンド管理用に設定する場合は、 FibreBridge RS-232 シリアルポートから PC のシリアル（ COM ）ポートにケーブルを接続します。

   シリアル接続は初期設定と ONTAP によるインバンド管理に使用され、 FC ポートを使用してブリッジの監視と管理を行うことができます。

3. IP 管理用に設定する場合は、イーサネットケーブルを使用して、各ブリッジのイーサネット管理 1 ポートをネットワークに接続します。

   ONTAP 9.5 以降を実行しているシステムでは、インバンド管理を使用してイーサネットポートではなく FC ポート経由でブリッジにアクセスできます。ONTAP 9.8 以降では、インバンド管理のみがサポートされ、 SNMP 管理は廃止されています。

   イーサネット管理 1 ポートを使用すると、ブリッジファームウェアを短時間でダウンロードし（ ATTO ExpressNAV または FTP 管理インターフェイスを使用）、コアファイルと抽出ログを取得できます。

4. IP 管理用に設定する場合は、使用しているブリッジモデルの ATTO FibreBridge Installation and Operation Manual _ のセクション 2.0 の手順に従って、各ブリッジのイーサネット管理 1 ポートを設定します。

   ONTAP 9.5 以降を実行しているシステムでは、インバンド管理を使用してイーサネットポートではなく FC ポート経由でブリッジにアクセスできます。ONTAP 9.8 以降では、インバンド管理のみがサポートされ、 SNMP 管理は廃止されています。

   QuickNAV を実行してイーサネット管理ポートを設定すると、イーサネットケーブルで接続されているイーサネット管理ポートのみが設定されます。たとえば、イーサネット管理 2 ポートも設定する場合は、イーサネットケーブルをポート 2 に接続して QuickNAV を実行する必要があります。

5. ブリッジを設定します。

   指定するユーザ名とパスワードは必ずメモしてください。

   > ATTO FibreBridge 7600N または 7500N では時刻同期は設定しないでください。ATTO FibreBridge 7600N または 7500N の時刻は、 ONTAP でブリッジが検出されたあとにクラスタ時間に設定されます。また、 1 日に 1 回定期的に同期されます。使用されるタイムゾーンは GMT で、変更することはできません。

   a. IP 管理用に設定する場合は、ブリッジの IP 設定を行います。

ONTAP 9.5 以降を実行しているシステムでは、インバンド管理を使用してイーサネットポートではなく FC ポート経由でブリッジにアクセスできます。ONTAP 9.8 以降では、インバンド管理のみがサポートされ、 SNMP 管理は廃止されています。

Quicknav ユーティリティなしで IP アドレスを設定するには、 FibreBridge に対するシリアル接続が必要です。

CLI を使用する場合は、次のコマンドを実行する必要があります。

'set ipaddress mp1 ip-address

'set ipsubnetmask mp1 subnet-mask

'set ipgateway mp1x.x'

'set ipdhcp mp1 disabled

「 setethernetspeed mp1 1000」

b. ブリッジ名を設定します。

ブリッジ名は、 MetroCluster 構成内でそれぞれ一意である必要があります。

各サイトの 1 つのスタックグループのブリッジ名の例：

- bridge_A_1a
- bridge_A_1b
- bridge_B_1a
- bridge_B_1b

CLI を使用する場合は、次のコマンドを実行する必要があります。

'set bridgename _bridgename_bridge_name'

c. ONTAP 9.4 以前を実行している場合は、ブリッジで SNMP を有効にします。

'Set SNMP enabled

ONTAP 9.5 以降を実行しているシステムでは、インバンド管理を使用してイーサネットポートではなく FC ポート経由でブリッジにアクセスできます。ONTAP 9.8 以降では、インバンド管理のみがサポートされ、 SNMP 管理は廃止されています。

6. ブリッジの FC ポートを設定します。

a. ブリッジ FC ポートのデータ速度を設定します。

サポートされる FC データ速度は、モデルブリッジによって異なります。

- FibreBridge 7600Nブリッジは、最大32、16、または8Gbpsをサポートします。
- FibreBridge 7500Nブリッジは、最大16、8、または4Gbpsをサポートします。

選択できる FCDataRate の速度は、ブリッジポートを接続するコントローラモジュールのブリッジ / FC ポートの両方でサポートされる最大速度以下です。ケーブルでの接続距離が SFP およびその他のハードウェアの制限を超えないようにしてください。

CLI を使用する場合は、次のコマンドを実行する必要があります。

```
set FCDataRate <port-number> <port-speed>
```

b. FibreBridge 7500Nブリッジを設定する場合は、ポートで使用する接続モードを「ptp」に設定します。

FibreBridge 7600N ブリッジを設定する場合、 FCConnMode の設定は不要です。

CLI を使用する場合は、次のコマンドを実行する必要があります。

```
set FCConnMode <port-number> ptp
```

c. FibreBridge 7600N / 7500N ブリッジを設定する場合は、 FC2 ポートを設定または無効にする必要があります。

- 2 番目のポートを使用する場合は、 FC2 ポートについて同じ手順を繰り返す必要があります。
- 2 番目のポートを使用しない場合は、ポートを無効にする必要があります。

```
FCPortDisable <port-number>
```

次に、 FC ポート 2 を無効にする例を示します。

```
FCPortDisable 2

Fibre Channel Port 2 has been disabled.
```

a. FibreBridge 7600N / 7500N ブリッジを設定する場合は、未使用の SAS ポートを無効にします。

'ASPortDisable_SAS-PORT_'

SAS ポート A~D はデフォルトで有効になります。使用していない SAS ポートを無効にする必要があります。

SAS ポート A のみを使用している場合は、 SAS ポート B 、 C 、および D を無効にする必要があります。次の例は、 SAS ポート B を無効にしていますSAS ポート C および D についても、同じように無効にする必要があります。

```
SASPortDisable b

SAS Port B has been disabled.
```

7. ブリッジへのアクセスを保護し、ブリッジの設定を保存します。システムで実行している ONTAP のバー

ジョンに応じて、次のいずれかのオプションを選択します。

ONTAP バージョン	手順
• ONTAP 9.5 以降 *	a. ブリッジのステータスを表示します。 「 storage bridge show 」 出力には、保護されていないブリッジが表示されます。 b. ブリッジを保護します。 「 ecurebridge 」
• ONTAP 9.4 以前 *	a. ブリッジのステータスを表示します。 「 storage bridge show 」 出力には、保護されていないブリッジが表示されます。 b. セキュリティ保護されていないブリッジのポートのステータスを確認します。 「 info 」のようになります 出力には、イーサネットポート MP1 と MP2 のステータスが表示されます。 c. イーサネットポート MP1 がイネーブルの場合、次のコマンドを実行します。 「 Set EthernetPort mp1 disabled 」です イーサネットポート MP2 も有効になっている場合は、ポート MP2 について前の手順を繰り返します。 d. ブリッジの設定を保存します。 次のコマンドを実行する必要があります。 'aveConfiguration' 「 FirmwareRestart 」と入力します ブリッジを再起動するように求められます。

8. MetroCluster の設定が完了したら、「 flashimages 」コマンドを使用して FibreBridge ファームウェアのバージョンを確認し、ブリッジが最新のサポート対象バージョンを使用していない場合は構成内のすべてのブリッジのファームウェアを更新します。

   "MetroCluster コンポーネントの保守"

ブリッジを設定したら、新しいシステムのケーブル接続を開始できます。

このタスクについて

ディスクシェルフの場合は、 SAS ケーブルのコネクタをプルタブ（コネクタの下側）を下にして挿入します。

手順

1. 各スタックのディスクシェルフをデイジーチェーン接続します。

   a. スタック内の論理的に最初のシェルフから、IOM Aのポート3を次のシェルフのIOM Aのポート1に接続し、スタック内の各IOM Aを接続します。

   b. IOM B について、同じ手順を繰り返します

   c. 各スタックについて、同じ手順を繰り返します。

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

2. ディスクシェルフの電源をオンにし、シェルフ ID を設定します。

   ◦ 各ディスクシェルフの電源を再投入する必要があります。

   ◦ 各 MetroCluster DR グループ（両サイトを含む）で、各 SAS ディスクシェルフのシェルフ ID が一意である必要があります。

3. ディスクシェルフを FibreBridge ブリッジにケーブル接続します。

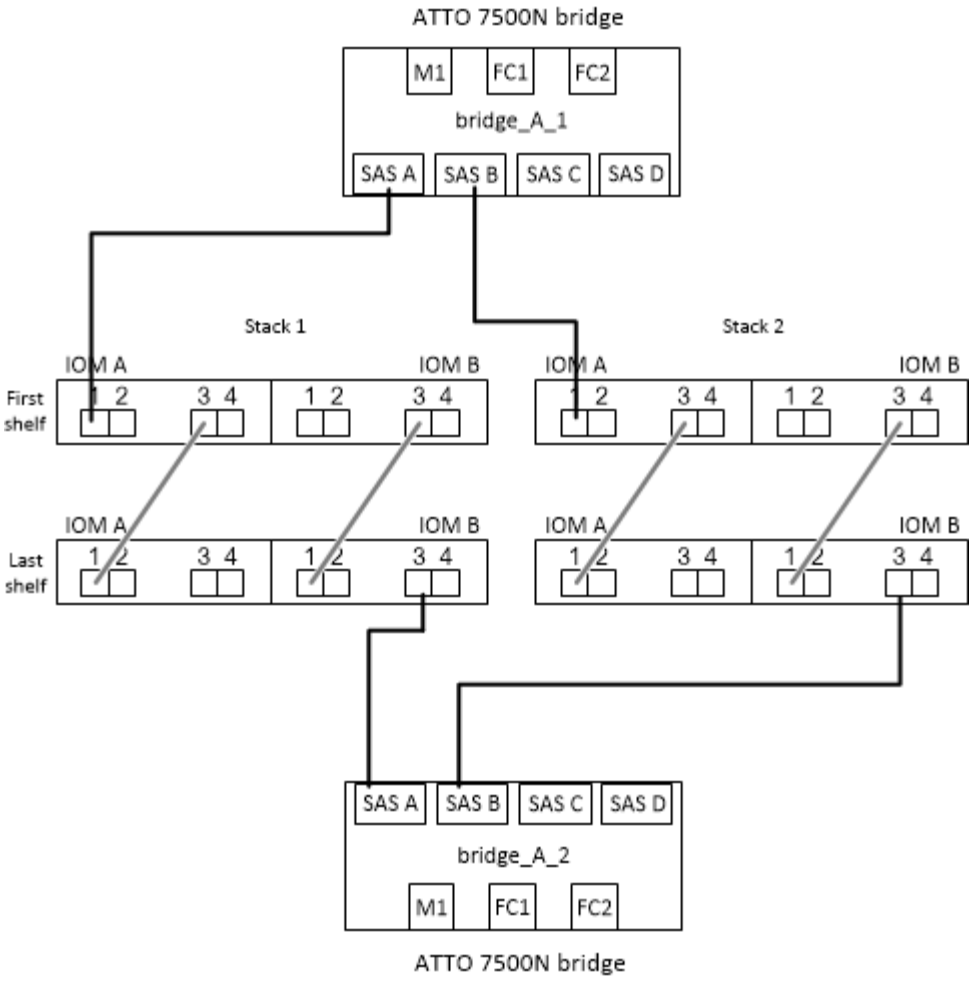
   a. ディスクシェルフの最初のスタックで、最初のシェルフの IOM A を FibreBridge A の SAS ポート A にケーブル接続し、最後のシェルフの IOM B を FibreBridge B の SAS ポート A にケーブル接続します

   b. 残りのシェルフスタックについて、 FibreBridge ブリッジの次に使用可能な SAS ポートを使用して同じ手順を繰り返します。 2 番目のスタックにはポート B 、 3 番目のスタックにはポート C 、 4 番目のスタックにはポート D を使用します。

   c. ケーブル接続中、IOM12 モジュールに基づくスタックは、別々の SAS ポートに接続されている限り、同じブリッジに接続します。

      それぞれのスタックで異なる IOM モデルを使用できますが、スタック内ではすべてのディスクシェルフで同じモデルを使用する必要があります。

      次の図は、 1 組の FibreBridge 7600N / 7500N ブリッジにディスクシェルフが接続された状態を示しています。



ブリッジの接続を確認し、ブリッジの**FC**ポートをケーブル接続する

各ブリッジですべてのディスクドライブが検出されることを確認してから、各ブリッジをローカルの FC スイッチにケーブル接続します。

手順

1. 各ブリッジが接続されているすべてのディスクドライブとディスクシェルフを検出できることを確認します。

使用する手段	作業

ATTO ExpressNAV の GUI	a. サポートされている Web ブラウザで、ブリッジの IP アドレスをブラウザのアドレスバーに入力します。 IP アドレスを入力したブリッジの ATTO FibreBridge ホームページに移動し、リンクが表示されます。 b. リンクをクリックし、ブリッジを設定するときに指定したユーザ名とパスワードを入力します。 ブリッジの ATTO FibreBridge ステータスページが開き、左側にメニューが表示されます。 c. 「 * 詳細設定 * 」をクリックします。 d. sastargets コマンドを使用して、接続されているデバイスを表示し、 * 送信 * をクリックします。
シリアルポート接続	接続されているデバイスを表示します。 「 astargets 」

出力には、ブリッジが接続されているデバイス（ディスクおよびディスクシェルフ）が表示されます。出力行には行番号が振られているため、デバイスの台数を簡単に把握できます。たとえば、次の出力は、10 本のディスクが接続されていることを示しています。

```
Tgt VendorID ProductID         Type        SerialNumber
  0 NETAPP   X410_S15K6288A15 DISK        3QP1CLE300009940UHJV
  1 NETAPP   X410_S15K6288A15 DISK        3QP1ELF600009940V1BV
  2 NETAPP   X410_S15K6288A15 DISK        3QP1G3EW00009940U2M0
  3 NETAPP   X410_S15K6288A15 DISK        3QP1EWMP00009940U1X5
  4 NETAPP   X410_S15K6288A15 DISK        3QP1FZLE00009940G8YU
  5 NETAPP   X410_S15K6288A15 DISK        3QP1FZLF00009940TZKZ
  6 NETAPP   X410_S15K6288A15 DISK        3QP1CEB400009939MGXL
  7 NETAPP   X410_S15K6288A15 DISK        3QP1G7A900009939FNTT
  8 NETAPP   X410_S15K6288A15 DISK        3QP1FY0T00009940G8PA
  9 NETAPP   X410_S15K6288A15 DISK        3QP1FXW600009940VERQ
```

出力の先頭に「response truncated」というテキストが表示された場合は、Telnetを使用してブリッジに接続し、同じコマンドを入力してすべての出力を確認できます。

2. コマンド出力を確認して、ブリッジがスタック内の想定されるすべてのディスクおよびディスクシェルフに接続していることを確認します。

出力結果	作業
正解です	繰り返します 手順 1. 残りの各ブリッジ。

不正解です	a. SAS ケーブルに緩みがないか確認するか、 SAS ケーブル接続をやり直します。 FibreBridge 7600N / 7500NブリッジをIOM12モジュールを使用してディスクシェルフとケーブル接続 b. 繰り返します 手順 1.。

3. 構成およびスイッチのモデルと FC-to-SAS ブリッジのモデルに対応するケーブル接続の表に従って、各ブリッジをローカルの FC スイッチにケーブル接続します。

   FibreBridge 7500N ブリッジの 2 つ目の FC ポート接続については、ゾーニングが完了するまでケーブル接続しないでください。

   使用している ONTAP のバージョンに対応したポート割り当てを参照してください。

4. パートナーサイトのブリッジに対して同じ手順を繰り返します。

関連情報

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

"FCスイッチのポート割り当て"

FibreBridge ブリッジをセキュリティ保護または保護解除します

安全性に問題のあるイーサネットプロトコルをブリッジで簡単に無効にできるように、 ONTAP 9.5 以降ではブリッジを保護することができます。これにより、ブリッジのイーサネットポートが無効になります。イーサネットアクセスを再度有効にすることもできます。

このタスクについて

- ブリッジをセキュリティ保護すると、ブリッジの Telnet とその他の IP ポートプロトコルおよびサービス（ FTP 、 ExpressNAV 、 ICMP 、 QuickNAV ）が無効になります。
- この手順では、 ONTAP 9.5 以降で使用可能な ONTAP プロンプトを使用したアウトオブバンド管理を使用します。

  アウトオブバンド管理を使用していない場合は、ブリッジの CLI からコマンドを問題できます。

- 「 unsecurebridge 」コマンドを使用して、イーサネットポートを再度イネーブルにできます。
- ONTAP 9.7 以前では、 ATTO FibreBridge で「 ecurebridge 」コマンドを実行すると、パートナークラスタでブリッジステータスが正しく更新されない可能性がありました。この場合は、パートナークラスタから「 ecurebridge 」コマンドを実行します。

ONTAP 9.8 以降では 'storage bridge コマンドは 'system bridge コマンドに置き換えられました次の手順は「 storage bridge 」コマンドを示していますが、 ONTAP 9.8 以降を実行している場合は「 system bridge 」コマンドが優先されます。

手順

1. ブリッジを含むクラスタの ONTAP プロンプトで、ブリッジのセキュリティ保護を設定または解除します。
   - 次のコマンドは、 bridge_A_1 をセキュリティ保護します。

     'cluster_a> storage bridge run-cli -bridge bridge_A_1 コマンド securebridge `

   - 次のコマンドは、 bridge_A_1 のセキュリティ保護を解除します。

     'cluster_a> storage bridge run-cli -bridge bridge_A_1 コマンド unsecurebridge

2. ブリッジを含むクラスタの ONTAP プロンプトで、ブリッジの設定を保存します。

   「 storage bridge run -cli-bridge-name_command savecfigation` 」

   次のコマンドは、 bridge_A_1 をセキュリティ保護します。

   'cluster_a > storage bridge run -cli -bridge bridge_A_1 - コマンド保存構成

3. ブリッジを含むクラスタの ONTAP プロンプトから、ブリッジのファームウェアを再起動します。

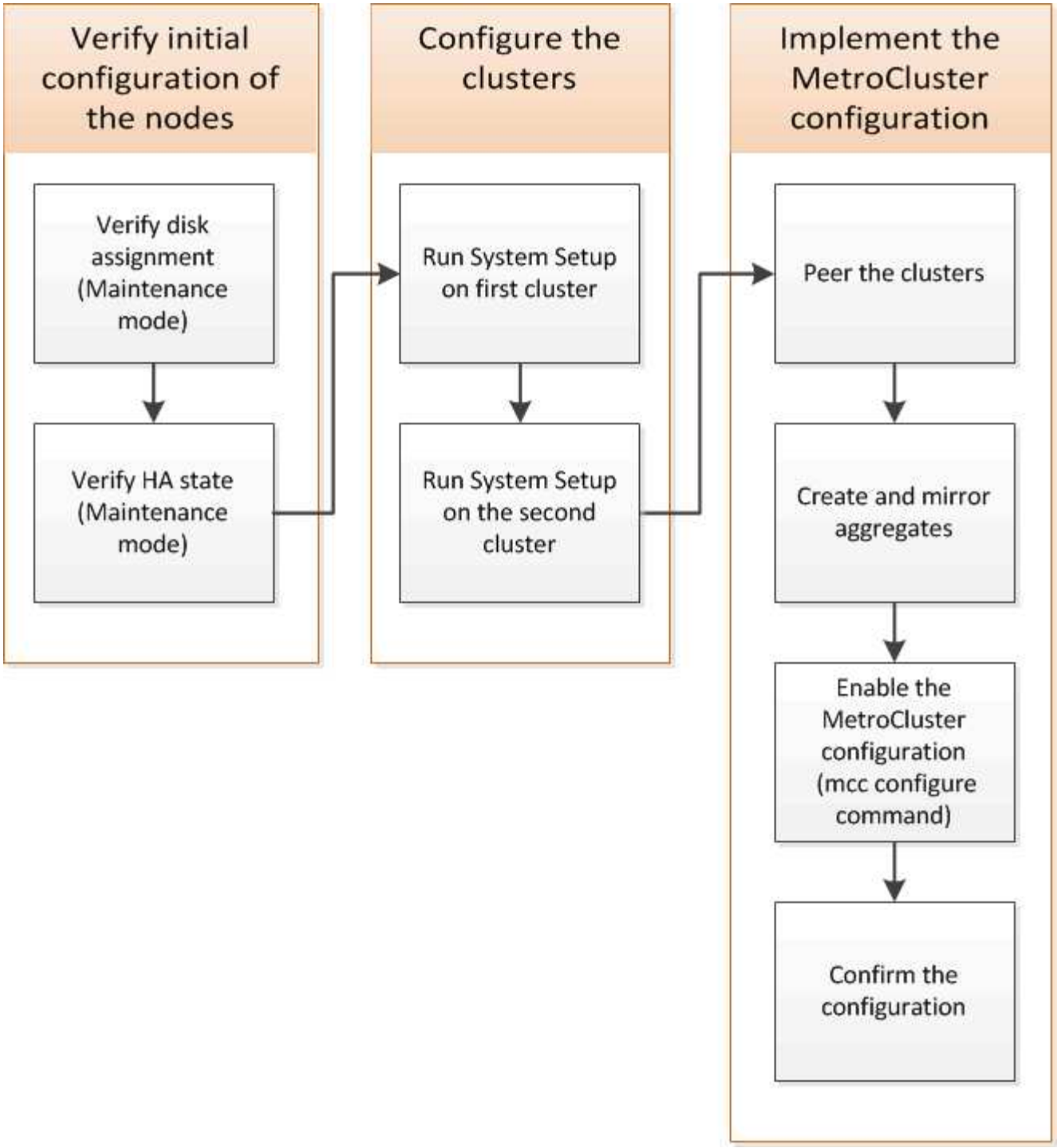
   「 storage bridge run -cli -bridge_name _ command firmwareerestart 」

   次のコマンドは、 bridge_A_1 をセキュリティ保護します。

   'cluster_a > storage bridge run-cli -bridge bridge_A_1 - コマンド firmwareerestart'

ONTAP で MetroCluster FC ソフトウェアを設定する

ONTAP の MetroCluster FC 構成で各ノードをセットアップする必要があります。これには、ノード レベルの構成と、2 つのサイトへのノードの構成が含まれます。また、2 つのサイト間の MetroCluster 関係を実装する必要があります。



必要な情報の収集

設定プロセスを開始する前に、コントローラモジュールに必要な IP アドレスを収集する必要があります。

サイト **A** の **IP** ネットワーク情報ワークシート

システムを設定する前に、最初の MetroCluster サイト（サイト A ）の IP アドレスその他のネットワーク情報を、ネットワーク管理者から入手する必要があります。

スイッチ情報：サイト **A**（スイッチクラスタ）

システムをケーブル接続するときは、各クラスタスイッチのホスト名と管理 IP アドレスが必要です。この情報は、 2 ノードスイッチレスクラスタ構成または 2 ノード MetroCluster 構成（サイトごとに 1 つのノード）を使用している場合は必要ありません。

クラスタスイッチ	ホスト名	IP アドレス	ネットワークマスク	デフォルトゲートウェイ
インターコネクト 1.				
インターコネクト 2				
管理 1				
管理 2.				

クラスタ作成情報：サイト **A**

クラスタを初めて作成するときは、次の情報が必要です。

情報のタイプ	値を入力します
クラスタ名 この手順で使用している例： site_A	
DNS ドメイン	
DNS ネームサーバ	
場所	
管理者パスワード	

ノード情報：サイト **A**

クラスタ内のノードごとに、管理 IP アドレス、ネットワークマスク、およびデフォルトゲートウェイが必要です。

ノード	ポート	IP アドレス	ネットワークマスク	デフォルトゲートウェイ

ノード 1 この手順で使用している例： controller_A_1				
ノード 2 2 ノード MetroCluster 構成（サイトごとに 1 つのノード）を使用している場合は不要 この手順で使用している例： controller_A_2				

クラスタピアリング用の **LIF** およびポート：サイト **A**

クラスタ内のノードごとに、 2 つのクラスタ間 LIF の IP アドレス、ネットワークマスク、およびデフォルトゲートウェイが必要です。クラスタ間 LIF は、クラスタのピアリングに使用されます。

ノード	ポート	クラスタ間 LIF の IP アドレス	ネットワークマスク	デフォルトゲートウェイ
ノード 1 IC LIF 1				
ノード 1 IC LIF 2				
ノード 2 IC LIF 1 2 ノード MetroCluster 構成（サイトごとに 1 つのノード）の場合は不要				
ノード 2 IC LIF 2 2 ノード MetroCluster 構成（サイトごとに 1 つのノード）の場合は不要				

タイムサーバ情報：サイト **A**

時間を同期する必要があります。これには 1 台以上の NTP タイムサーバが必要です。

ノード	ホスト名	IP アドレス	ネットワークマスク	デフォルトゲートウェイ
NTP サーバ 1				
NTP サーバ 2				

サイト**A nbsp**；**AutoSupport** 情報

各ノードで AutoSupport を設定する必要があります。これには次の情報が必要です。

情報のタイプ		値を入力します
送信元 E メールアドレス		メールホスト
IP アドレスまたは名前		転送プロトコル
HTTP 、 HTTPS 、または SMTP		プロキシサーバ
	受信者の E メールアドレスまたは配信リスト	メッセージ全文
	簡潔なメッセージ	

サイト**A nbsp**；**SP**情報

トラブルシューティングとメンテナンスのために、各ノードのサービスプロセッサ（ SP ）へのアクセスを有効にする必要があります。これには、ノードごとに次のネットワーク情報が必要です。

ノード	IP アドレス	ネットワークマスク	デフォルトゲートウェイ
ノード 1			
ノード 2 2 ノード MetroCluster 構成（サイトごとに 1 つのノード）の場合は不要			

サイト **B** の **IP** ネットワーク情報ワークシート

システムを設定する前に、 2 つ目の MetroCluster サイト（サイト B ）の IP アドレスその他のネットワーク情報を、ネットワーク管理者から入手する必要があります。

スイッチ情報：サイト **B** （スイッチクラスタ）

システムをケーブル接続するときは、各クラスタスイッチのホスト名と管理 IP アドレスが必要です。この情

報は、 2 ノードスイッチレスクラスタ構成または 2 ノード MetroCluster 構成（サイトごとに 1 つのノード）を使用している場合は必要ありません。

クラスタスイッチ	ホスト名	IP アドレス	ネットワークマスク	デフォルトゲートウェイ
インターコネクト 1.				
インターコネクト 2				
管理 1				
管理 2.				

クラスタ作成情報：サイト **B**

クラスタを初めて作成するときは、次の情報が必要です。

情報のタイプ	値を入力します
クラスタ名 この手順で使用される例：site_B	
DNS ドメイン	
DNS ネームサーバ	
場所	
管理者パスワード	

ノード情報：サイト **B**

クラスタ内のノードごとに、管理 IP アドレス、ネットワークマスク、およびデフォルトゲートウェイが必要です。

ノード	ポート	IP アドレス	ネットワークマスク	デフォルトゲートウェイ
ノード 1 この手順で使用される例 ：controller_B_1				

ノード 2 2 ノード MetroCluster 構成（サイトごとに 1 つのノード）の場合は不要 この手順で使用される例：controller_B_2				

クラスタピアリング用の **LIF** およびポート：サイト **B**

クラスタ内のノードごとに、 2 つのクラスタ間 LIF の IP アドレス、ネットワークマスク、およびデフォルトゲートウェイが必要です。クラスタ間 LIF は、クラスタのピアリングに使用されます。

ノード	ポート	クラスタ間 LIF の IP アドレス	ネットワークマスク	デフォルトゲートウェイ
ノード 1 IC LIF 1				
ノード 1 IC LIF 2				
ノード 2 IC LIF 1 2 ノード MetroCluster 構成（サイトごとに 1 つのノード）の場合は不要				
ノード 2 IC LIF 2 2 ノード MetroCluster 構成（サイトごとに 1 つのノード）の場合は不要				

タイムサーバ情報：サイト **B**

時間を同期する必要があります。これには 1 台以上の NTP タイムサーバが必要です。

ノード	ホスト名	IP アドレス	ネットワークマスク	デフォルトゲートウェイ
NTP サーバ 1				

NTP サーバ 2				

サイト**B nbsp**；**AutoSupport**情報

各ノードで AutoSupport を設定する必要があります。これには次の情報が必要です。

情報のタイプ		値を入力します
送信元 E メールアドレス		
メールホスト	IP アドレスまたは名前	
転送プロトコル	HTTP 、 HTTPS 、または SMTP	
プロキシサーバ		受信者の E メールアドレスまたは配信リスト
メッセージ全文		簡潔なメッセージ
	パートナー	

サイト**B nbsp**；**SP**情報

トラブルシューティングとメンテナンスのために、各ノードのサービスプロセッサ（ SP ）へのアクセスを有効にする必要があります。これには、ノードごとに次のネットワーク情報が必要です。

ノード	IP アドレス	ネットワークマスク	デフォルトゲートウェイ
ノード 1 （ controller_B_1 ）			
ノード 2 （ controller_B_2 ） 2 ノード MetroCluster 構成（サイトごとに 1 つのノード）の場合は不要			

標準クラスタ構成と **MetroCluster** 構成の類似点 **/** 相違点

MetroCluster 構成の各クラスタのノードの構成は、標準クラスタのノードと似ています。

MetroCluster 構成は、 2 つの標準クラスタを基盤としています。構成は物理的に対称な構成である必要があり、各ノードのハードウェア構成が同じで、すべての MetroCluster コンポーネントがケーブル接続され、設定されている必要があります。ただし、 MetroCluster 構成のノードの基本的なソフトウェア設定は、標準クラスタのノードと同じです。

設定手順	標準クラスタ構成	MetroCluster の設定
各ノードで管理 LIF 、クラスタ LIF 、データ LIF を設定。	両方のクラスタタイプで同じです	
ルートアグリゲートを設定	両方のクラスタタイプで同じです	
クラスタ内のノードを HA ペアとして設定	両方のクラスタタイプで同じです	
クラスタ内の一方のノードでクラスタを設定。	両方のクラスタタイプで同じです	
もう一方のノードをクラスタに追加。	両方のクラスタタイプで同じです	
ミラーされたルートアグリゲートを作成	任意。	必須
クラスタをピアリング。	任意。	必須
MetroCluster 設定を有効にします。	該当しません	必須

メンテナンスモードでコンポーネントの HA 状態を確認および設定する

ストレージシステムをMetroCluster FC構成で構成する場合は、コントローラモジュールおよびシャーシのコンポーネントのハイアベイラビリティ（HA）状態がmccまたはmcc-2nであることを確認して、これらのコンポーネントが適切にブートするようにする必要があります。工場出荷状態のシステムではこの値を事前に設定しておく必要がありますが、作業を進める前に設定を確認しておく必要があります。

コントローラモジュールとシャーシのHA状態が正しくない場合は、ノードを再初期化しないとMetroClusterを設定できません。この手順を使用して設定を修正し、次のいずれかの手順を使用してシステムを初期化する必要があります。

- MetroCluster IP構成では、の手順に従います"コントローラモジュールのシステムデフォルトの復元"。
- MetroCluster FC構成では、の手順に従います"システムをデフォルトに戻し、コントローラモジュールでHBAタイプを設定する"。

作業を開始する前に

システムがメンテナンスモードであることを確認します。

手順

1. メンテナンスモードで、コントローラモジュールとシャーシの HA 状態を表示します。

   「 ha-config show 」

   HA の正しい状態は、 MetroCluster 構成によって異なります。

MetroCluster構成タイプ	すべてのコンポーネントのHA状態

8ノードまたは4ノードのMetroCluster FC構成	MCC
2 ノード MetroCluster FC 構成	mcc-2n
8ノードまたは4ノードのMetroCluster IP構成	mccip

2. 表示されたコントローラのシステム状態が正しくない場合は、コントローラモジュールで構成に応じた正しいHA状態を設定します。

MetroCluster構成タイプ	コマンドを実行します
8ノードまたは4ノードのMetroCluster FC構成	「 ha-config modify controller mcc 」
2 ノード MetroCluster FC 構成	「 ha-config modify controller mcc-2n 」という形式で指定します
8ノードまたは4ノードのMetroCluster IP構成	「 ha-config modify controller mccip 」を参照してください

3. 表示されたシャーシのシステム状態が正しくない場合は、シャーシの構成に応じた正しいHA状態を設定します。

MetroCluster構成タイプ	コマンドを実行します
8ノードまたは4ノードのMetroCluster FC構成	「 ha-config modify chassis mcc 」
2 ノード MetroCluster FC 構成	「 ha-config modify chassis mcc-2n 」というようになりました
8ノードまたは4ノードのMetroCluster IP構成	「 ha-config modify chassis mccip 」を参照してください

4. ノードを ONTAP でブートします。

   「 boot_ontap 」

5. この手順をすべて繰り返して、MetroCluster構成の各ノードのHA状態を確認します。

システムのデフォルト設定をリストアし、コントローラモジュールで **HBA** タイプを設定しています

このタスクについて

MetroCluster を正しくインストールするには、コントローラモジュールのデフォルトをリセットしてリストアします。

重要

このタスクを実行する必要があるのは、 FC-to-SAS ブリッジを使用するストレッチ構成のみです。

手順

1. LOADER プロンプトで環境変数をデフォルト設定に戻します。

   「デフォルト設定」

2. ノードをメンテナンスモードでブートし、システム内の HBA の設定を行います。

   a. メンテナンスモードでブートします。

      「 boot_ontap maint 」を使用してください

   b. ポートの現在の設定を確認します。

      ucadmin show

   c. 必要に応じてポートの設定を更新します。

HBA のタイプと目的のモード	使用するコマンド
CNA FC	ucadmin modify -m fc -t initiator_adapter_name _ `
CNA イーサネット	ucadmin modify -mode cna_adapter_name _ `
FC ターゲット	fcadmin config -t target_adapter_name _`
FC イニシエータ	fcadmin config -t initiator_adapter_name_`

3. メンテナンスモードを終了します。

   「 halt 」

   コマンドの実行後、ノードが LOADER プロンプトで停止するまで待ちます。

4. ノードをブートしてメンテナンスモードに戻り、設定の変更が反映されるようにします。

   「 boot_ontap maint 」を使用してください

5. 変更内容を確認します。

HBA のタイプ	使用するコマンド
CNA	ucadmin show
FC	fcadmin show`

6. メンテナンスモードを終了します。

   「 halt 」

コマンドの実行後、ノードが LOADER プロンプトで停止するまで待ちます。

7. ノードをブートメニューでブートします。

「 boot_ontap menu

コマンドの実行後、ブートメニューが表示されるまで待ちます。

8. ブートメニュープロンプトで「 wipeconfig 」と入力してノード設定をクリアし、 Enter キーを押します。

次の画面はブートメニューのプロンプトを示しています。

```
Please choose one of the following:

     (1) Normal Boot.
     (2) Boot without /etc/rc.
     (3) Change password.
     (4) Clean configuration and initialize all disks.
     (5) Maintenance mode boot.
     (6) Update flash from backup config.
     (7) Install new software first.
     (8) Reboot node.
     (9) Configure Advanced Drive Partitioning.
     Selection (1-9)?  wipeconfig
 This option deletes critical system configuration, including cluster
membership.
 Warning: do not run this option on a HA node that has been taken over.
 Are you sure you want to continue?: yes
 Rebooting to finish wipeconfig request.
```

FAS8020 システムでの X1132A-R6 クアッドポートカードの FC-VI ポートの設定

FAS8020 システムで X1132A-R6 クアッドポートカードを使用している場合は、メンテナンスモードに切り替えて、ポート 1a / 1b を FC-VI およびイニシエータ用に使用するように設定できます。工場出荷状態の MetroCluster システムでは、構成に応じて適切にポートが設定されているため、この設定は必要ありません。

このタスクについて

このタスクはメンテナンスモードで実行する必要があります。

ucadmin コマンドを使用した FC ポートの FC-VI ポートへの変換は、 FAS8020 および AFF 8020 システムでのみサポートされます。他のプラットフォームでは、 FC ポートを FCVI ポートに変換することはできません。

手順

1. ポートを無効にします。

「ストレージ無効化アダプタ 1a 」

「ストレージ無効化アダプタ 1b'

```
*> storage disable adapter 1a
Jun 03 02:17:57 [controller_B_1:fci.adapter.offlining:info]: Offlining
Fibre Channel adapter 1a.
Host adapter 1a disable succeeded
Jun 03 02:17:57 [controller_B_1:fci.adapter.offline:info]: Fibre Channel
adapter 1a is now offline.
*> storage disable adapter 1b
Jun 03 02:18:43 [controller_B_1:fci.adapter.offlining:info]: Offlining
Fibre Channel adapter 1b.
Host adapter 1b disable succeeded
Jun 03 02:18:43 [controller_B_1:fci.adapter.offline:info]: Fibre Channel
adapter 1b is now offline.
*>
```

2. ポートが無効になっていることを確認します。

   ucadmin show

```
*> ucadmin show
         Current  Current    Pending  Pending    Admin
Adapter  Mode     Type       Mode     Type       Status
-------  -------  ---------  -------  ---------  -------
  ...
  1a     fc       initiator  -        -          offline
  1b     fc       initiator  -        -          offline
  1c     fc       initiator  -        -          online
  1d     fc       initiator  -        -          online
```

3. ポート a とポート b を FC-VI モードに設定します。

   ucadmin modify -adapter 1a -type FCVI`

   このコマンドでは、 1a だけを指定した場合でも、ポートペアの両方のポート 1a と 1b のモードが設定されます。

```
*> ucadmin modify -t fcvi 1a
Jun 03 02:19:13 [controller_B_1:ucm.type.changed:info]: FC-4 type has
changed to fcvi on adapter 1a. Reboot the controller for the changes to
take effect.
Jun 03 02:19:13 [controller_B_1:ucm.type.changed:info]: FC-4 type has
changed to fcvi on adapter 1b. Reboot the controller for the changes to
take effect.
```

4. 変更が保留中であることを確認します。

   ucadmin show

```
*> ucadmin show
          Current  Current    Pending  Pending    Admin
Adapter   Mode     Type       Mode     Type       Status
-------   -------  ---------  -------  ---------  -------
  ...
  1a      fc       initiator  -        fcvi       offline
  1b      fc       initiator  -        fcvi       offline
  1c      fc       initiator  -        -          online
  1d      fc       initiator  -        -          online
```

5. コントローラをシャットダウンし、メンテナンスモードでリブートします。
6. 設定の変更を確認します。

   ucadmin show local

```
Node            Adapter  Mode     Type       Mode     Type       Status
------------    -------  -------  ---------  -------  ---------
-----------
...
controller_B_1
                1a       fc       fcvi       -        -          online
controller_B_1
                1b       fc       fcvi       -        -          online
controller_B_1
                1c       fc       initiator  -        -          online
controller_B_1
                1d       fc       initiator  -        -          online
6 entries were displayed.
```

メンテナンスモードでの 8 ノードまたは 4 ノード構成のディスク割り当ての検証

システムを ONTAP で完全にブートする前に、オプションで、メンテナンスモードでブートしてノードのディスク割り当てを確認することができます。ディスクは、各プールのディスク数が等しい、完全に対称なアクティブ / アクティブ構成を形成するように割り当てられている必要があります。

このタスクについて

新しい MetroCluster システムの場合、出荷前にディスク割り当てが完了しています。

次の表に、 MetroCluster 構成のプール割り当ての例を示します。ディスクはシェルフ単位でプールに割り当てられます。

・サイト A のディスクシェルフ *

ディスクシェルフ（ sample_shelf_name ）	所属ノード	割り当てプール
ディスクシェルフ 1 （ shelf_A_1_1 ）	ノード A1	プール 0
ディスクシェルフ 2 （ shelf_A_1_3 ）		
ディスクシェルフ 3 （ shelf_B_1_1 ）	ノード B1	プール 1.
ディスクシェルフ 4 （ shelf_B_1_3 ）		
ディスクシェルフ 5 （ shelf_A_2_1 ）	ノード A2	プール 0
ディスクシェルフ 6 （ shelf_A_2_3 ）		
ディスクシェルフ 7 （ shelf_B_2_1 ）	ノード B2	プール 1.
ディスクシェルフ 8 （ shelf_B_2_3 ）		
ディスクシェルフ 1 （ shelf_A_3_1 ）	ノード a 3	プール 0
ディスクシェルフ 2 （ shelf_A_3_3 ）		
ディスクシェルフ 3 （ shelf_B_3_1 ）	ノード B3	プール 1.
ディスクシェルフ 4 （ shelf_B_3_3 ）		
ディスクシェルフ 5 （ shelf_A_4_1 ）	ノード A4	プール 0
ディスクシェルフ 6 （ shelf_A_4_3 ）		
ディスクシェルフ 7 （ shelf_B_4_1 ）	ノード B4	プール 1.
ディスクシェルフ 8 （ shelf_B_4_3 ）		

・サイト B のディスクシェルフ *

ディスクシェルフ（ sample_shelf_name ）	所属ノード	割り当てプール

ディスクシェルフ 9 （ shelf_B_1_2 ）	ノード B1	プール 0
ディスクシェルフ 10 （ shelf_B_1_4 ）	ディスクシェルフ 11 （ shelf_A_1_2 ）	ノード A1
プール 1.	ディスクシェルフ 12 （ shelf_A_1_4 ）	ディスクシェルフ 13 （ shelf_B_2_2 ）
ノード B2	プール 0	ディスクシェルフ 14 （ shelf_B_2_4 ）
ディスクシェルフ 15 （ shelf_A_2_2 ）	ノード A2	プール 1.
ディスクシェルフ 16 （ shelf_A_2_4 ）	ディスクシェルフ 1 （ shelf_B_3_2 ）	ノード a 3
プール 0	ディスクシェルフ 2 （ shelf_B_3_4 ）	ディスクシェルフ 3 （ shelf_A_3_2 ）
ノード B3	プール 1.	ディスクシェルフ 4 （ shelf_A_3_4 ）
ディスクシェルフ 5 （ shelf_B_4_2 ）	ノード A4	プール 0
ディスクシェルフ 6 （ shelf_B_4_4 ）	ディスクシェルフ 7 （ shelf_A_4_2 ）	ノード B4

手順

1. シェルフの割り当てを確認します。

   「 Disk show – v 」のように表示されます

2. 必要に応じて、接続されているディスクシェルフ上のディスクを適切なプールに明示的に割り当てます。

   「ディスク割り当て」

   ワイルドカードを使用すると、 1 回のコマンドで 1 つのディスクシェルフのすべてのディスクを割り当てることができます。「 storage show disk --x 」コマンドを使用すると、各ディスクのディスクシェルフ ID とベイを識別できます。

AFF 以外のシステムでディスク所有権を割り当てています

MetroCluster ノードにディスクが正しく割り当てられていない場合、または構成で DS460C ディスクシェルフを使用している場合は、 MetroCluster 構成内の各ノードにシェルフ単位でディスクを割り当てる必要があ

ります。構成内の各ノードのローカルディスクプールとリモートディスクプールでディスク数が同じになるように設定します。

作業を開始する前に

ストレージコントローラがメンテナンスモードになっている必要があります。

このタスクについて

構成に DS460C ディスクシェルフが含まれている場合を除き、工場出荷時の状態でディスクが正しく割り当てられていればこのタスクは必要ありません。

> プール 0 には、ディスクを所有するストレージシステムと同じサイトにあるディスクを割り当てます。
>
> プール 1 には、ディスクを所有するストレージシステムに対してリモートなディスクを割り当てます。

構成に DS460C ディスクシェルフが含まれている場合は、それぞれの 12 ディスクドロワーについて、次のガイドラインに従ってディスクを手動で割り当てる必要があります。

ドロワーのディスク	ノードとプール
0 ～ 2	ローカルノードのプール 0
3-5	HA パートナーノードのプール 0
6 ~ 8	ローカルノードのプール 1 の DR パートナー
9 ~ 11	HA パートナーのプール 1 の DR パートナー

このディスク割り当てパターンに従うことで、ドロワーがオフラインになった場合のアグリゲートへの影響を最小限に抑えることができます。

手順

1. システムをブートしていない場合は、メンテナンスモードでブートします。
2. 最初のサイト（サイト A ）にあるノードにディスクシェルフを割り当てます。

   ノードと同じサイトにあるディスクシェルフはプール 0 に割り当て、パートナーサイトにあるディスクシェルフはプール 1 に割り当てます。

   各プールに同じ数のシェルフを割り当てる必要があります。

   a. 最初のノードで、ローカルディスクシェルフをプール 0 に、リモートディスクシェルフをプール 1 に割り当てます。

      「 Disk assign-shelf_local-switch-name ： shelf-name .port_-p_pool_`

      ストレージコントローラ Controller_A_1 にシェルフが 4 台ある場合は、次のコマンドを問題に設定します。

```
*> disk assign -shelf FC_switch_A_1:1-4.shelf1 -p 0
*> disk assign -shelf FC_switch_A_1:1-4.shelf2 -p 0

*> disk assign -shelf FC_switch_B_1:1-4.shelf1 -p 1
*> disk assign -shelf FC_switch_B_1:1-4.shelf2 -p 1
```

b. ローカルサイトの 2 番目のノードに対して処理を繰り返し、ローカルディスクシェルフをプール 0 に、リモートディスクシェルフをプール 1 に割り当てます。

「 Disk assign-shelf_local-switch-name ： shelf-name .port_-p_pool_`

ストレージコントローラ Controller_A_2 にシェルフが 4 台ある場合は、次のコマンドを問題に設定します。

```
*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0
*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1

*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0
*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1
```

3. 2 番目のサイト（サイト B ）にあるノードにディスクシェルフを割り当てます。

ノードと同じサイトにあるディスクシェルフはプール 0 に割り当て、パートナーサイトにあるディスクシェルフはプール 1 に割り当てます。

各プールに同じ数のシェルフを割り当てる必要があります。

a. リモートサイトの最初のノードで、ローカルディスクシェルフをプール 0 に、リモートディスクシェルフをプール 1 に割り当てます。

「ディスク assign -shelf_local-switch-namesshelf-name -*p_pool*` 」

ストレージコントローラ Controller_B_1 にシェルフが 4 台ある場合は、次のコマンドを問題します。

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf1 -p 0
*> disk assign -shelf FC_switch_B_1:1-5.shelf2 -p 0

*> disk assign -shelf FC_switch_A_1:1-5.shelf1 -p 1
*> disk assign -shelf FC_switch_A_1:1-5.shelf2 -p 1
```

b. リモートサイトの 2 番目のノードに対して処理を繰り返し、ローカルディスクシェルフをプール 0 に、リモートディスクシェルフをプール 1 に割り当てます。

「ディスク assign -shelf_shelf-name-p_pool_` 」

ストレージコントローラ Controller_B_2 にシェルフが 4 台ある場合は、次のコマンドを問題に実行し

ます。

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf3 -p 0
*> disk assign -shelf FC_switch_B_1:1-5.shelf4 -p 0

*> disk assign -shelf FC_switch_A_1:1-5.shelf3 -p 1
*> disk assign -shelf FC_switch_A_1:1-5.shelf4 -p 1
```

4. シェルフの割り当てを確認します。

   「 storage show shelf

5. メンテナンスモードを終了します。

   「 halt 」

6. ブートメニューを表示します。

   「 boot_ontap menu

7. 各ノードで、オプション * 4 * を選択してすべてのディスクを初期化します。

AFF システムでディスク所有権を割り当てます

アグリゲートがミラーされた AFF システムを使用する構成で、ノードにディスク（ SSD ）が正しく割り当てられていない場合は、各シェルフの半分のディスクを 1 つのローカルノードに割り当て、残りの半分を対応する HA パートナーノードに割り当てる必要があります。構成内の各ノードのローカルディスクプールとリモートディスクプールでディスク数が同じになるように設定する必要があります。

作業を開始する前に

ストレージコントローラがメンテナンスモードになっている必要があります。

このタスクについて

これは、アグリゲートがミラーされていない構成、アクティブ / パッシブ構成、ローカルプールとリモートプールのディスク数が異なる構成には該当しません。

このタスクは、工場出荷時にディスクが正しく割り当てられている場合は必要ありません。



プール 0 には、ディスクを所有するストレージシステムと同じサイトにあるディスクを割り当てます。

プール 1 には、ディスクを所有するストレージシステムに対してリモートなディスクを割り当てます。

手順

1. システムをブートしていない場合は、メンテナンスモードでブートします。
2. 最初のサイト（サイト A ）にあるノードにディスクを割り当てます。

   各プールに同じ数のディスクを割り当てる必要があります。

a. 最初のノードで、各シェルフの半分のディスクをプール 0 に、残りの半分を HA パートナーのプール 0 に割り当てます。

```
disk assign -shelf <shelf-name> -p <pool> -n <number-of-disks>
```

ストレージコントローラ Controller_A_1 にシェルフが 4 台あり、各シェルフに SSD が 8 本ある場合は、次のコマンドを問題に設定します。

```
*> disk assign -shelf FC_switch_A_1:1-4.shelf1 -p 0 -n 4
*> disk assign -shelf FC_switch_A_1:1-4.shelf2 -p 0 -n 4

*> disk assign -shelf FC_switch_B_1:1-4.shelf1 -p 1 -n 4
*> disk assign -shelf FC_switch_B_1:1-4.shelf2 -p 1 -n 4
```

b. ローカルサイトの 2 番目のノードに対して処理を繰り返し、各シェルフの半分のディスクをプール 1 に、残りの半分を HA パートナーのプール 1 に割り当てます。

「 disk assign -disk disk-name -p pool 」という名前です

ストレージコントローラ Controller_A_1 にシェルフが 4 台あり、各シェルフに SSD が 8 本ある場合は、次のコマンドを問題に設定します。

```
*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1 -n 4

*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1 -n 4
```

3. 2 番目のサイト（サイト B ）にあるノードにディスクを割り当てます。

各プールに同じ数のディスクを割り当てる必要があります。

a. リモートサイトの最初のノードで、各シェルフの半分のディスクをプール 0 に、残りの半分を HA パートナーのプール 0 に割り当てます。

「 disk assign -disk disk-name-p_pool_` 」

ストレージコントローラ Controller_B_1 にシェルフが 4 台あり、各シェルフに SSD が 8 本ある場合は、次のコマンドを問題で実行します。

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf1 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-5.shelf2 -p 0 -n 4

*> disk assign -shelf FC_switch_A_1:1-5.shelf1 -p 1 -n 4
*> disk assign -shelf FC_switch_A_1:1-5.shelf2 -p 1 -n 4
```

b. リモートサイトの 2 番目のノードに対して処理を繰り返し、各シェルフの半分のディスクをプール 1 に、残りの半分を HA パートナーのプール 1 に割り当てます。

「 disk assign -disk disk-name-p_pool_` 」

ストレージコントローラ Controller_B_2 にシェルフが 4 台あり、各シェルフに SSD が 8 本ある場合は、次のコマンドを問題に設定します。

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf3 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-5.shelf4 -p 0 -n 4

*> disk assign -shelf FC_switch_A_1:1-5.shelf3 -p 1 -n 4
*> disk assign -shelf FC_switch_A_1:1-5.shelf4 -p 1 -n 4
```

4. ディスクの割り当てを確認します。

「 storage show disk 」を参照してください

5. メンテナンスモードを終了します。

「 halt 」

6. ブートメニューを表示します。

「 boot_ontap menu

7. 各ノードで、オプション * 4 * を選択してすべてのディスクを初期化します。

保守モードでの 2 ノード構成のディスク割り当ての検証

システムを ONTAP で完全にブートする前に、システムをメンテナンスモードでブートして、ノードのディスク割り当てを確認することもできます。ディスクは、両方のサイトが独自のディスクシェルフを所有してデータを提供し、各ノードおよび各プールのミラーディスク数が等しい、完全に対称な構成を形成するように割り当てられている必要があります。

作業を開始する前に

システムをメンテナンスモードにする必要があります。

このタスクについて

新しい MetroCluster システムの場合、出荷前にディスク割り当てが完了しています。

次の表に、 MetroCluster 構成のプール割り当ての例を示します。ディスクはシェルフ単位でプールに割り当てられます。

ディスクシェルフ（名前）	サイト	所属ノード	割り当てプール

ディスクシェルフ 1 （ shelf_A_1_1 ）	サイト A	ノード A1	プール 0
ディスクシェルフ 2 （ shelf_A_1_3 ）			
ディスクシェルフ 3 （ shelf_B_1_1 ）		ノード B1	プール 1.
ディスクシェルフ 4 （ shelf_B_1_3 ）			
ディスクシェルフ 9 （ shelf_B_1_2 ）	サイト B	ノード B1	プール 0
ディスクシェルフ 10 （ shelf_B_1_4 ）			
ディスクシェルフ 11 （ shelf_A_1_2 ）		ノード A1	プール 1.
ディスクシェルフ 12 （ shelf_A_1_4 ）			

構成に DS460C ディスクシェルフが含まれている場合は、それぞれの 12 ディスクドロワーについて、次のガイドラインに従ってディスクを手動で割り当てる必要があります。

ドロワーのディスク	ノードとプール
1 ~ 6	ローカルノードのプール 0
7-12	DR パートナーのプール 1

このディスク割り当てパターンに従うことで、ドロワーがオフラインになった場合のアグリゲートへの影響を最小限に抑えることができます。

手順

1. 工場出荷状態のシステムの場合は、シェルフの割り当てを確認します。

   「 Disk show – v 」のように表示されます

2. 必要に応じて、 disk assign コマンドを使用すると、接続されているディスクシェルフ上のディスクを適切なプールに明示的に割り当てることができます。

   ノードと同じサイトにあるディスクシェルフはプール 0 に割り当て、パートナーサイトにあるディスクシェルフはプール 1 に割り当てます。各プールに同じ数のシェルフを割り当てる必要があります。

   a. システムをブートしていない場合は、メンテナンスモードでブートします。
   b. サイト A のノードで、ローカルディスクシェルフをプール 0 に、リモートディスクシェルフをプール 1 に割り当てます。

      「 disk assign -shelf_disk_shelf_name_-p_pool_` 」のようになります

      ストレージコントローラ node_A_1 にシェルフが 4 台ある場合は、次のコマンドを問題できます。

```
*> disk assign -shelf shelf_A_1_1 -p 0
*> disk assign -shelf shelf_A_1_3 -p 0

*> disk assign -shelf shelf_A_1_2 -p 1
*> disk assign -shelf shelf_A_1_4 -p 1
```

c. リモートサイト（サイト B ）のノードで、ローカルディスクシェルフをプール 0 に、リモートディスクシェルフをプール 1 に割り当てます。

「 disk assign -shelf_disk_shelf_name_-p_pool_` 」のようになります

ストレージコントローラ node_B_1 にシェルフが 4 台ある場合は、次のコマンドを問題に設定します。

```
*> disk assign -shelf shelf_B_1_2   -p 0
*> disk assign -shelf shelf_B_1_4  -p 0

*> disk assign -shelf shelf_B_1_1 -p 1
 *> disk assign -shelf shelf_B_1_3 -p 1
```

a. 各ディスクのディスクシェルフ ID とベイを表示します。

「 Disk show – v 」のように表示されます

ONTAP をセットアップしています

各コントローラモジュールに ONTAP をセットアップする必要があります。

新しいコントローラをネットブートする必要がある場合は、を参照してください "新しいコントローラモジュールのネットブート" MetroCluster アップグレード、移行、および拡張ガイドの各ガイドを参照してください。

選択肢

- 2 ノード MetroCluster 構成での ONTAP のセットアップ
- ONTAP は、 8 ノードまたは 4 ノードの MetroCluster 構成でセットアップします

2 ノード MetroCluster 構成での ONTAP のセットアップ

2 ノード MetroCluster 構成では、各クラスタでノードをブートし、クラスタセットアップウィザードを終了し、 cluster setup コマンドを使用してシングルノードクラスタとしてノードを構成する必要があります。

作業を開始する前に

サービスプロセッサが設定されていないことを確認してください。

このタスクについて

このタスクは、ネットアップの標準のストレージを使用した 2 ノード MetroCluster 構成が対象です。

このタスクは、 MetroCluster 構成の両方のクラスタで実行する必要があります。

ONTAP の設定の詳細については、を参照してください "ONTAP をセットアップする"。

手順

1. 最初のノードの電源をオンにします。

   この手順はディザスタリカバリ（ DR ）サイトのノードでも実行する必要があります。

   ノードがブートし、コンソールでクラスタセットアップウィザードが起動されて、 AutoSupport が自動的に有効になることを示すメッセージが表示されます。

```
::> Welcome to the cluster setup wizard.

You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the cluster setup wizard.
     Any changes you made before quitting will be saved.

You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.

This system will send event messages and periodic reports to NetApp
Technical
Support. To disable this feature, enter
autosupport modify -support disable
within 24 hours.

Enabling AutoSupport can significantly speed problem determination and
resolution, should a problem occur on your system.
For further information on AutoSupport, see:
http://support.netapp.com/autosupport/

Type yes to confirm and continue {yes}: yes

Enter the node management interface port [e0M]:
Enter the node management interface IP address [10.101.01.01]:

Enter the node management interface netmask [101.010.101.0]:
Enter the node management interface default gateway [10.101.01.0]:



Do you want to create a new cluster or join an existing cluster?
{create, join}:
```

2. 新しいクラスタを作成します。

   「 create 」

3. ノードをシングルノードクラスタとして使用するかどうかを選択します。

   ```
   Do you intend for this node to be used as a single node cluster? {yes,
   no} [yes]:
   ```

4. Enter キーを押してシステムのデフォルト値をそのまま使用するか 'no' と入力してから Enter キーを押して ' 独自の値を入力します
5. プロンプトに従って * Cluster Setup * ウィザードを完了し、 Enter キーを押してデフォルト値をそのまま使用するか、独自の値を入力して Enter キーを押します。

   デフォルト値は、プラットフォームとネットワークの構成に基づいて自動的に決定されます。

6. クラスタセットアップ * ウィザードが完了したら、次のコマンドを入力して、クラスタがアクティブで、最初のノードが正常に機能していることを確認します

   「 cluster show 」を参照してください

   次の例は、第 1 ノードが含まれるクラスタ（ cluster1-01 ）が正常に機能しており、クラスタへの参加条件を満たしていることを示しています。

   ```
   cluster1::> cluster show
   Node                  Health  Eligibility
   --------------------- ------- ------------
   cluster1-01           true    true
   ```

   管理 SVM やノード SVM に対する設定に変更が必要になった場合は、 cluster setup コマンドを使用してクラスタセットアップウィザードにアクセスできます。

8 ノード / 4 ノード MetroCluster 構成での ONTAP のセットアップ

各ノードをブートすると、 System Setup ツールを使用してノードおよびクラスタの基本的な設定を実行するよう求めるメッセージが表示されます。クラスタを設定したら、 ONTAP CLI に戻ってアグリゲートを作成し、 MetroCluster 構成を作成します。

作業を開始する前に

MetroCluster 構成のケーブル接続を完了しておく必要があります。

このタスクについて

このタスクは、ネットアップの標準のストレージを使用した 8 ノード / 4 ノード MetroCluster 構成が対象です。

新規で購入した MetroCluster システムは事前に設定されており、ここで説明する手順を実行する必要はありません。ただし、 AutoSupport ツールを設定する必要があります。

このタスクは、 MetroCluster 構成の両方のクラスタで実行する必要があります。

この手順では、 System Setup ツールを使用します。必要に応じて、 CLI クラスタセットアップウィザードを使用することもできます。

手順

1. 各ノードに電源が入っていない場合は、電源を投入してブートします。

   システムが保守モードになっている場合は問題、 halt コマンドを使用して保守モードを終了し、次に LOADER プロンプトで次のコマンドを問題します。

   「 boot_ontap 」

   次のような出力が表示されます。

   ```
   Welcome to node setup

   You can enter the following commands at any time:
     "help" or "?" - if you want to have a question clarified,
     "back" - if you want to change previously answered questions, and
     "exit" or "quit" - if you want to quit the setup wizard.
                   Any changes you made before quitting will be saved.

   To accept a default or omit a question, do not enter a value.
   .
   .
   .
   ```

2. システムの指示に従って AutoSupport ツールを有効にします。
3. プロンプトに従ってノード管理インターフェイスを設定します。

   次のようなプロンプトが表示されます。

   ```
   Enter the node management interface port: [e0M]:
   Enter the node management interface IP address: 10.228.160.229
   Enter the node management interface netmask: 225.225.252.0
   Enter the node management interface default gateway: 10.228.160.1
   ```

4. ノードがハイアベイラビリティモードで設定されていることを確認します。

   「 storage failover show -fields mode 」を選択します

   そうでない場合は、各ノードで次のコマンドを問題処理してノードをリブートする必要があります。

   「 storage failover modify -mode ha -node localhost 」を参照してください

   このコマンドを実行するとハイアベイラビリティモードが設定されますが、ストレージフェイルオーバー

は有効になりません。ストレージフェイルオーバーは、あとで実行する MetroCluster の設定プロセスで自動的に有効になります。

5. クラスタインターコネクトとして 4 つのポートが構成されていることを確認します。

   「 network port show 」のように表示されます

   次の例は、 cluster_A の出力を示しています。

```
cluster_A::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
node_A_1
       **e0a       Cluster      Cluster          up       1500
auto/1000
       e0b       Cluster      Cluster          up       1500
auto/1000**
       e0c       Default      Default          up       1500  auto/1000
       e0d       Default      Default          up       1500  auto/1000
       e0e       Default      Default          up       1500  auto/1000
       e0f       Default      Default          up       1500  auto/1000
       e0g       Default      Default          up       1500  auto/1000
node_A_2
       **e0a       Cluster      Cluster          up       1500
auto/1000
       e0b       Cluster      Cluster          up       1500
auto/1000**
       e0c       Default      Default          up       1500  auto/1000
       e0d       Default      Default          up       1500  auto/1000
       e0e       Default      Default          up       1500  auto/1000
       e0f       Default      Default          up       1500  auto/1000
       e0g       Default      Default          up       1500  auto/1000
14 entries were displayed.
```

6. 2 ノードスイッチレスクラスタ（クラスタインターコネクトスイッチのないクラスタ）を作成する場合は、 switchless-cluster ネットワークモードを有効にします。

   a. advanced 権限レベルに切り替えます。

      「 advanced 」の権限が必要です

   advanced モードで続行するかどうかを確認するプロンプトが表示されたら、「 y 」と入力します。advanced モードのプロンプトが表示されます（ * > ）。

a. switchless-cluster モードを有効にします。

network options switchless-cluster modify -enabled true

b. admin 権限レベルに戻ります。

「特権管理者」

7. 最初のブート後にシステムコンソールに表示される情報に従って、 System Setup ツールを起動します。
8. System Setup ツールを使用して各ノードを設定し、クラスタを作成します。ただし、アグリゲートは作成しないでください。

後続のタスクでミラーされたアグリゲートを作成します。

完了後

ONTAP のコマンドラインインターフェイスに戻り、後続のタスクを実行して MetroCluster の設定を完了します。

クラスタを **MetroCluster** 構成に設定

クラスタをピアリングし、ルートアグリゲートをミラーリングし、ミラーリングされたデータアグリゲートを作成し、コマンドを問題して MetroCluster の処理を実装する必要があります。

このタスクについて

を実行する前に `metrocluster configure`、HAモードおよびDRミラーリングが有効になっていないため、この想定動作に関連するエラーメッセージが表示される場合があります。HAモードとDRミラーリングは、あとでコマンドを実行するときに有効にします `metrocluster configure` をクリックして構成を実装してください。

クラスタをピアリング

MetroCluster 構成内のクラスタが相互に通信し、 MetroCluster ディザスタリカバリに不可欠なデータミラーリングを実行できるようにするために、クラスタ間にはピア関係が必要です。

クラスタ間 **LIF** を設定しています

MetroCluster パートナークラスタ間の通信に使用するポートにクラスタ間 LIF を作成する必要があります。専用のポートを使用することも、データトラフィック用を兼ねたポートを使用することもできます。

選択肢

- 専用ポートでのクラスタ間 LIF の設定
- 共有データポートでのクラスタ間 LIF の設定

専用ポートでのクラスタ間 **LIF** の設定

専用ポートにクラスタ間 LIF を設定できます。通常は、レプリケーショントラフィックに使用できる帯域幅が増加します。

手順

1. クラスタ内のポートの一覧を表示します。

   「 network port show 」のように表示されます

   コマンド構文全体については、マニュアルページを参照してください。

   次の例は、「 cluster01 」内のネットワークポートを示しています。

```
cluster01::> network port show
                                                                  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に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
                                  cluster01-01:e0a, cluster01-01:e0b,
                                  cluster01-02:e0a, cluster01-02:e0b
cluster01
                 Default
                                  cluster01-01:e0c, cluster01-01:e0d,
                                  cluster01-02:e0c, cluster01-02:e0d,
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
                 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

「 network interface create -vserver *system_svm _ -lif_lif_name_service-policy default -intercluster -home-node _-home-port _ -port_IP_address _port_ip*-netmask netmask _ -failover-group _` 」のようになります

ONTAP 9.5 以前

「 network interface create -vserver_system_SVM_lif_lif_name — ロール intercluster -home-node *node_name* のクラスタ間ホームポートポート *_port*-address *port_ip*-netmask netmask_—failover-group_failover_group_name 」

コマンド構文全体については、マニュアルページを参照してください。

次の例は、フェイルオーバーグループ「 intercluster01 」にクラスタ間 LIF 「 cluster01_icl01 」と「 cluster01_icl02 」を作成します。

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0 -failover-group intercluster01

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0 -failover-group intercluster01
```

6. クラスタ間 LIF が作成されたことを確認します。

ONTAP 9.6 以降

次のコマンドを実行します。 `network interface show -service-policy default-intercluster`

ONTAP 9.5 以前

次のコマンドを実行します。 `network interface show -role intercluster`

コマンド構文全体については、マニュアルページを参照してください。

```
cluster01::> network interface show -service-policy default-intercluster
            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

次のコマンドを実行します。 `network interface show -service-policy default-intercluster -failover`

ONTAP 9.5 以前

次のコマンドを実行します。 `network interface show -role intercluster -failover`

コマンド構文全体については、マニュアルページを参照してください。

次の例は、 SVM 「 e0e 」ポート上のクラスタ間 LIF 「 cluster01_icl01 」と「 cluster01_icl02 」が「 e0f 」ポートにフェイルオーバーされることを示しています。

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

関連情報

"専用のポートを使用する場合の考慮事項"

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

共有データポートでのクラスタ間 **LIF** の設定

データネットワークと共有するポートにクラスタ間 LIF を設定できます。これにより、クラスタ間ネットワークに必要なポート数を減らすことができます。

手順

1. クラスタ内のポートの一覧を表示します。

   「 network port show 」のように表示されます

   コマンド構文全体については、マニュアルページを参照してください。

次の例は、 cluster01 内のネットワークポートを示しています。

```
cluster01::> network port show
                                                                  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

次のコマンドを実行します。 `network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-service-policy default-intercluster -home-node` *`node`* `-home-port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*

ONTAP 9.5 以前

次のコマンドを実行します。

```
network interface create -vserver system_SVM -lif LIF_name -role
intercluster -home-node node -home-port port -address port_IP -netmask
netmask
```

コマンド構文全体については、マニュアルページを参照してください。次の例は、クラスタ間 LIF cluster01_icl01 と cluster01_icl02 を作成します。

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. クラスタ間 LIF が作成されたことを確認します。

ONTAP 9.6 以降

次のコマンドを実行します。 `network interface show -service-policy default-intercluster`

ONTAP 9.5 以前

次のコマンドを実行します。 `network interface show -role intercluster`

コマンド構文全体については、マニュアルページを参照してください。

```
cluster01::> network interface show -service-policy default-intercluster
            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

次のコマンドを実行します。 `network interface show -service-policy default-intercluster -failover`

ONTAP 9.5 以前

次のコマンドを実行します。
`network interface show -role intercluster -failover`

コマンド構文全体については、マニュアルページを参照してください。

次の例は、「 e0c 」ポート上のクラスタ間 LIF 「 cluster01_icl01 」と「 cluster01_icl02 」が「 e0d 」ポートにフェイルオーバーされることを示しています。

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-01:e0c,
                                              cluster01-01:e0d
         cluster01_icl02 cluster01-02:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-02:e0c,
                                              cluster01-02:e0d
```

関連情報

"データポートを共有する場合の考慮事項"

クラスタピア関係を作成

MetroCluster クラスタ間にクラスタピア関係を作成する必要があります。

このタスクについて

cluster peer create コマンドを使用すると、ローカルクラスタとリモートクラスタ間にピア関係を作成できます。ピア関係が作成されたら ' リモート・クラスタ上で cluster peer create を実行して ' ローカル・クラスタに対してピア関係を認証できます

作業を開始する前に

- ピア関係にあるクラスタ内の各ノードでクラスタ間 LIF を作成しておく必要があります。
- クラスタで ONTAP 9.3 以降が実行されている必要があります。

手順

1. デスティネーションクラスタで、ソースクラスタとのピア関係を作成します。

   cluster peer create -generate-passphrase -offer-expiration_mm/dd/YYYY HH ： MM ： SS|1…7days | 1…168hours_-peer-addrs_peer_lif_ips_-ipspace_ips_`

   「 -generate-passphrase 」と「 -peer-addrs 」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-addrs 」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、 -ipspace 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-addrs peer_lif_ips-ipspace ips'

   コマンド構文全体については、マニュアルページを参照してください。

   次の例は、クラスタ間 LIF の IP アドレス「 192.140.112.101 」および「 192.140.112.102 」でローカルクラスタをリモートクラスタに対して認証します。

   ```
   cluster01::> cluster peer create -peer-addrs
   192.140.112.101,192.140.112.102

   Notice: Use a generated passphrase or choose a passphrase of 8 or more
   characters.
           To ensure the authenticity of the peering relationship, use a
   phrase or sequence of characters that would be hard to guess.

   Enter the passphrase:
   Confirm the passphrase:

   Clusters cluster02 and cluster01 are peered.
   ```

   プロンプトが表示されたら、ピア関係のパスフレーズを入力します。

3. クラスタピア関係が作成されたことを確認します。

「 cluster peer show -instance 」のように表示されます

```
cluster01::> cluster peer show -instance

                                Peer Cluster Name: cluster02
                    Remote Intercluster Addresses: 192.140.112.101,
192.140.112.102
               Availability of the Remote Cluster: Available
                             Remote Cluster Name: cluster2
                             Active IP Addresses: 192.140.112.101,
192.140.112.102
                           Cluster Serial Number: 1-80-123456
                  Address Family of Relationship: ipv4
             Authentication Status Administrative: no-authentication
                Authentication Status Operational: absent
                                 Last Update Time: 02/05 21:05:41
                     IPspace for the Relationship: Default
```

4. ピア関係にあるノードの接続状態とステータスを確認します。

cluster peer health show

```
cluster01::> cluster peer health show
Node       cluster-Name                Node-Name
             Ping-Status               RDB-Health Cluster-Health  Avail…
---------- --------------------------- ---------  ---------------
--------
cluster01-01
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
cluster01-02
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
```

「 cluster peer create 」コマンドを使用して、ローカルクラスタとリモートクラスタ間のピア関係の要求を開始できます。ピア関係がローカルクラスタによって要求された後 ' リモートクラスタ上で cluster peer create を実行して ' 関係を受け入れることができます

作業を開始する前に

- ピア関係にあるクラスタ内の各ノードでクラスタ間 LIF を作成しておく必要があります。
- クラスタ管理者は、各クラスタが他のクラスタに対して自身を認証する際に使用するパスフレーズに同意しておく必要があります。

手順

1. データ保護のデスティネーションクラスタで、データ保護のソースクラスタとのピア関係を作成します。

   'cluster peer create -peer-addrs_peer_lif_ips_-ipspace_`

   カスタム IPspace を使用しない場合は、 -ipspace オプションを無視してかまいません。コマンド構文全体については、マニュアルページを参照してください。

   次の例は、クラスタ間 LIF の IP アドレス「 192.168.2.201 」および「 192.168.2.202 」で、リモートクラスタとのクラスタピア関係を作成します。

   ```
   cluster02::> cluster peer create -peer-addrs 192.168.2.201,192.168.2.202
   Enter the passphrase:
   Please enter the passphrase again:
   ```

   プロンプトが表示されたら、ピア関係のパスフレーズを入力します。

2. データ保護のソースクラスタで、ソースクラスタをデスティネーションクラスタに対して認証します。

   'cluster peer create -peer-addrs_peer_lif_ips_-ipspace_`

   コマンド構文全体については、マニュアルページを参照してください。

   次の例は、クラスタ間 LIF の IP アドレス「 192.140.112.203 」および「 192.140.112.204 」でローカルクラスタをリモートクラスタに対して認証します。

   ```
   cluster01::> cluster peer create -peer-addrs 192.168.2.203,192.168.2.204
   Please confirm the passphrase:
   Please confirm the passphrase again:
   ```

   プロンプトが表示されたら、ピア関係のパスフレーズを入力します。

3. クラスタピア関係が作成されたことを確認します。

   cluster peer show – instance

   コマンド構文全体については、マニュアルページを参照してください。

```
cluster01::> cluster peer show -instance
Peer Cluster Name: cluster01
Remote Intercluster Addresses: 192.168.2.201,192.168.2.202
Availability: Available
Remote Cluster Name: cluster02
Active IP Addresses: 192.168.2.201,192.168.2.202
Cluster Serial Number: 1-80-000013
```

4. ピア関係にあるノードの接続状態とステータスを確認します。

   cluster peer health show

   コマンド構文全体については、マニュアルページを参照してください。

```
cluster01::> cluster peer health show
Node       cluster-Name                Node-Name
             Ping-Status               RDB-Health Cluster-Health  Avail…
---------- --------------------------- ---------  ---------------
--------
cluster01-01
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
cluster01-02
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
```

ルートアグリゲートをミラーリング

データ保護を提供するには、ルートアグリゲートをミラーする必要があります。

このタスクについて

デフォルトでは、ルートアグリゲートは RAID-DP タイプのアグリゲートとして作成されます。ルートアグリゲートのタイプは RAID-DP から RAID4 に変更することができます。次のコマンドは、ルートアグリゲートを RAID4 タイプのアグリゲートに変更します。

```
storage aggregate modify -aggregate aggr_name -raidtype raid4
```

ADP 以外のシステムでは、ミラーリングの実行前後に、アグリゲートの RAID タイプをデフォルトの RAID-DP から RAID4 に変更できます。

手順

1. ルートアグリゲートをミラーします。

   「 storage aggregate mirror aggr_name 」のようになります

   次のコマンドでは、 controller_A_1 のルートアグリゲートがミラーされます。

   ```
   controller_A_1::> storage aggregate mirror aggr0_controller_A_1
   ```

   これによりアグリゲートがミラーされるため、ローカルのプレックスとリモートのプレックスがリモートの MetroCluster サイトに配置されたアグリゲートが作成されます。

2. MetroCluster 構成の各ノードについて、同じ手順を繰り返します。

関連情報

"CLI を使用した論理ストレージ管理"

各ノードでミラーされたデータアグリゲートを作成します

DR グループの各ノードに、ミラーされたデータアグリゲートを 1 つ作成する必要があります。

- 新しいアグリゲートで使用するドライブを把握しておく必要があります。
- 複数のドライブタイプを含むシステム（異機種混在ストレージ）の場合は、正しいドライブタイプが選択されるようにする方法を確認しておく必要があります。
- ドライブは特定のノードによって所有されます。アグリゲートを作成する場合、アグリゲート内のすべてのドライブは同じノードによって所有される必要があります。そのノードが、作成するアグリゲートのホームノードになります。
- アグリゲート名は、 MetroCluster 構成を計画する際に決定した命名規則に従う必要があります。を参照してください "ディスクおよびアグリゲートの管理"。
- アグリゲート名は、MetroClusterサイト全体で一意である必要があります。つまり、サイト A とサイト B に同じ名前を持つ 2 つの異なるデータ アグリゲートを持つことはできません。

手順

1. 使用可能なスペアのリストを表示します。

   「 storage disk show -spare -owner node_name 」という名前になります

2. storage aggregate create -mirror true コマンドを使用して、アグリゲートを作成します。

   クラスタ管理インターフェイスでクラスタにログインした場合、クラスタ内の任意のノードにアグリゲートを作成できます。アグリゲートを特定のノード上に作成するには、「 -node 」パラメータを使用する

か、そのノードが所有するドライブを指定します。

次のオプションを指定できます。

- アグリゲートのホームノード（通常運用時にアグリゲートを所有するノード）
- アグリゲートに追加するドライブのリスト
- 追加するドライブ数

> 最小サポート構成では、使用可能なドライブ数が制限されていますが、 3 つのディスク RAID-DP アグリゲートを作成できるようにするには、「 force-small-aggregate 」オプションを使用する必要があります。

- アグリゲートに使用するチェックサム形式
- 使用するドライブのタイプ
- 使用するドライブのサイズ
- 使用するドライブの速度
- アグリゲート上の RAID グループの RAID タイプ
- RAID グループに含めることができるドライブの最大数
- RPM の異なるドライブが許可されるかどうか

これらのオプションの詳細については 'storage aggregate create のマニュアルページを参照してください

次のコマンドでは、 10 本のディスクを含むミラーアグリゲートが作成されます。

```
cluster_A::> storage aggregate create aggr1_node_A_1 -diskcount 10 -node
node_A_1 -mirror true
[Job 15] Job is queued: Create aggr1_node_A_1.
[Job 15] The job is starting.
[Job 15] Job succeeded: DONE
```

3. 新しいアグリゲートの RAID グループとドライブを確認します。

   「 storage aggregate show-status -aggregate _aggregate-name _ 」を参照してください

ミラーされていないデータアグリゲートの作成

MetroCluster 構成が提供する冗長なミラーリングを必要としないデータについては、必要に応じてミラーされていないデータアグリゲートを作成できます。

作業を開始する前に

- 新しいアグリゲートで使用されるドライブを把握していることを確認します。
- 複数のドライブタイプを含むシステム（異機種混在ストレージ）の場合は、正しいドライブタイプが選択されていることを確認する方法を理解しておく必要があります。

MetroCluster FC 構成では、ミラーされていないアグリゲートがスイッチオーバー後にオンラインになるのは、アグリゲート内のリモートディスクにアクセスできる場合のみです。ISL で障害が発生すると、ミラーされていないリモートディスク内のデータにローカルノードがアクセスできなくなる可能性があります。アグリゲートに障害が発生すると、ローカルノードがリブートされる場合があります。

- ドライブは特定のノードによって所有されます。アグリゲートを作成する場合、アグリゲート内のすべてのドライブは同じノードによって所有される必要があります。そのノードが、作成するアグリゲートのホームノードになります。

ミラーされていないアグリゲートは、そのアグリゲートを所有するノードに対してローカルでなければなりません。

- アグリゲート名は、 MetroCluster 構成を計画する際に決定した命名規則に従う必要があります。
- _Disks and aggregates management _ アグリゲートのミラーリングの詳細については、を参照してください。

手順

1. 使用可能なスペアのリストを表示します。

   「 storage disk show -spare -owner_node_name _ 」というように入力します

2. アグリゲートを作成します。

   「 storage aggregate create 」

   クラスタ管理インターフェイスでクラスタにログインした場合、クラスタ内の任意のノードにアグリゲートを作成できます。アグリゲートが特定のノード上に作成されていることを確認するには、「 -node 」パラメータを使用するか、そのノードが所有するドライブを指定します。

   次のオプションを指定できます。

   - アグリゲートのホームノード（通常運用時にアグリゲートを所有するノード）
   - アグリゲートに追加するドライブのリスト
   - 追加するドライブ数
   - アグリゲートに使用するチェックサム形式
   - 使用するドライブのタイプ
   - 使用するドライブのサイズ
   - 使用するドライブの速度
   - アグリゲート上の RAID グループの RAID タイプ
   - RAID グループに含めることができるドライブの最大数
   - RPM の異なるドライブが許可されるかどうか

   これらのオプションの詳細については、 storage aggregate create のマニュアルページを参照してください。

次のコマンドでは、 10 本のディスクを含むミラーされていないアグリゲートが作成さ

```
controller_A_1::> storage aggregate create aggr1_controller_A_1
-diskcount 10 -node controller_A_1
[Job 15] Job is queued: Create aggr1_controller_A_1.
[Job 15] The job is starting.
[Job 15] Job succeeded: DONE
```

3. 新しいアグリゲートの RAID グループとドライブを確認します。

   「 storage aggregate show-status -aggregate _aggregate-name _ 」を参照してください

関連情報

"ディスクと階層（アグリゲート）の管理"

MetroCluster 構成の実装

MetroCluster 構成でデータ保護を開始するに MetroCluster は 'data configure コマンドを実行する必要があります

作業を開始する前に

- ルート以外のミラーされたデータアグリゲートが各クラスタに少なくとも 2 つ必要です。

  その他のデータアグリゲートはミラーされていてもいなくてもかまいません。

  これは「 storage aggregate show 」コマンドで確認できます。

  ミラーされた単一のデータアグリゲートを使用する場合は、を参照してください 手順 1. 手順については、を参照し

- コントローラおよびシャーシの ha-config の状態が「 mcc 」である必要があります。

このタスクについて

MetroCluster 構成を有効にするには ' 任意のノードで MetroCluster configure コマンドを 1 回実行します問題サイトごとまたはノードごとにコマンドを問題で実行する必要はありません。また、問題するノードまたはサイトはどれでもかまいません。

MetroCluster configure コマンドを実行すると '2 つのクラスタそれぞれのシステム ID が最も小さい 2 つのノードが 'DR （災害復旧）パートナーとして自動的にペア設定されます4 ノード MetroCluster 構成の場合は、DR パートナーのペアは 2 組になります。2 つ目の DR ペアは、システム ID が大きい 2 つのノードで作成されます。

コマンドMetroCluster configure'を実行する前に'Onboard Key Manager（OKM；オンボードキーマネージャ）または外部キー管理を構成しないでください

手順

1. 次の形式で MetroCluster を設定します。

MetroCluster 構成の内容	操作
複数のデータアグリゲート	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 グループ内のすべてのノードの MetroCluster 構成を有効にします。

```
cluster_A::*> metrocluster configure -node-name controller_A_1

[Job 121] Job succeeded: Configure is successful.
```

2. サイト A のネットワークステータスを確認します。

「 network port show 」のように表示されます

次の例は、 4 ノード MetroCluster 構成でのネットワークポートの用途を示しています。

```
cluster_A::> network port show
                                                            Speed (Mbps)
Node   Port      IPspace   Broadcast Domain Link   MTU    Admin/Oper
------ --------- --------- ---------------- ----- ------- ------------
controller_A_1
       e0a       Cluster   Cluster          up     9000  auto/1000
       e0b       Cluster   Cluster          up     9000  auto/1000
       e0c       Default   Default          up     1500  auto/1000
       e0d       Default   Default          up     1500  auto/1000
       e0e       Default   Default          up     1500  auto/1000
       e0f       Default   Default          up     1500  auto/1000
       e0g       Default   Default          up     1500  auto/1000
controller_A_2
       e0a       Cluster   Cluster          up     9000  auto/1000
       e0b       Cluster   Cluster          up     9000  auto/1000
       e0c       Default   Default          up     1500  auto/1000
       e0d       Default   Default          up     1500  auto/1000
       e0e       Default   Default          up     1500  auto/1000
       e0f       Default   Default          up     1500  auto/1000
       e0g       Default   Default          up     1500  auto/1000
14 entries were displayed.
```

3. MetroCluster 構成の両方のサイトから MetroCluster 構成を確認します。

   a. サイト A から構成を確認します。

      「 MetroCluster show 」

```
cluster_A::> metrocluster show

Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
Remote: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
```

   b. サイト B から構成を確認します。

      「 MetroCluster show 」

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-disaster
Remote: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-disaster
```

ONTAP ソフトウェアでのフレームのインオーダー配信またはアウトオブオーダー配信の設定

Fibre Channel （ FC ）スイッチの設定に応じて、フレームの In-Order Delivery （ IOD ；インオーダー配信）または Out-of-Order Delivery （ OOD ；アウトオブオーダー配信）のいずれかを設定する必要があります。

このタスクについて

FC スイッチが IOD に設定されている場合は、 ONTAP ソフトウェアを IOD に設定する必要があります。同様に、 FC スイッチが OOD に設定されている場合は、 ONTAP を OOD に設定する必要があります。

設定を変更するには、コントローラをリブートする必要があります。

ステップ

1. ONTAP でのフレームの処理方法として IOD または OOD のいずれかを設定します。
   - ONTAP では、デフォルトではフレームの IOD が有効になっています。設定の詳細を確認するには、次の手順を
     i. advanced モードに切り替えます。

        「高度」

     ii. 設定を確認します。

        MetroCluster インターコネクト・アダプタ・ショー

```
mcc4-b12_siteB::*> metrocluster interconnect adapter show
                             Adapter Link   Is OOD
Node          Adapter Name    Type    Status Enabled? IP Address  Port
Number
------------ --------------- ------- ------ -------- -----------
-----------
mcc4-b1       fcvi_device_0   FC-VI    Up    false    17.0.1.2
6a
mcc4-b1       fcvi_device_1   FC-VI    Up    false    18.0.0.2
6b
mcc4-b1       mlx4_0          IB       Down  false    192.0.5.193
ib2a
mcc4-b1       mlx4_0          IB       Up    false    192.0.5.194
ib2b
mcc4-b2       fcvi_device_0   FC-VI    Up    false    17.0.2.2
6a
mcc4-b2       fcvi_device_1   FC-VI    Up    false    18.0.1.2
6b
mcc4-b2       mlx4_0          IB       Down  false    192.0.2.9
ib2a
mcc4-b2       mlx4_0          IB       Up    false    192.0.2.10
ib2b
8 entries were displayed.
```

- フレームの OOD を設定するには、各ノードで次の手順を実行する必要があります。
  i. advanced モードに切り替えます。

     「高度」

  ii. MetroCluster 構成の設定を確認します。

     MetroCluster インターコネクト・アダプタ・ショー

```
mcc4-b12_siteB::*> metrocluster interconnect adapter show
                             Adapter Link   Is OOD
Node          Adapter Name    Type    Status Enabled? IP Address
Port Number
------------ --------------- ------- ------ -------- -----------
-----------
mcc4-b1       fcvi_device_0   FC-VI    Up    false    17.0.1.2
6a
mcc4-b1       fcvi_device_1   FC-VI    Up    false    18.0.0.2
6b
mcc4-b1       mlx4_0          IB       Down  false    192.0.5.193
ib2a
mcc4-b1       mlx4_0          IB       Up    false    192.0.5.194
ib2b
mcc4-b2       fcvi_device_0   FC-VI    Up    false    17.0.2.2
6a
mcc4-b2       fcvi_device_1   FC-VI    Up    false    18.0.1.2
6b
mcc4-b2       mlx4_0          IB       Down  false    192.0.2.9
ib2a
mcc4-b2       mlx4_0          IB       Up    false    192.0.2.10
ib2b
8 entries were displayed.
```

iii. ノード「`m cc4-b1'` 」およびノード「 `m cc4-b0` 」で OOD を有効にします。

MetroCluster 相互接続アダプタ modify -Node_node_name --is-ood-enabled true

```
mcc4-b12_siteB::*> metrocluster interconnect adapter modify -node
mcc4-b1 -is-ood-enabled true
mcc4-b12_siteB::*> metrocluster interconnect adapter modify -node
mcc4-b2 -is-ood-enabled true
```

i. 両方向でハイアベイラビリティ（HA）テイクオーバーを実行してコントローラをリブートします。

ii. 設定を確認します。

MetroCluster インターコネクト・アダプタ・ショー

```
mcc4-b12_siteB::*> metrocluster interconnect adapter show
                             Adapter Link   Is OOD
Node         Adapter Name    Type    Status Enabled? IP Address  Port
Number
------------ --------------- ------- ------ -------- -----------
-----------
mcc4-b1      fcvi_device_0   FC-VI   Up     true      17.0.1.2       6a
mcc4-b1      fcvi_device_1   FC-VI   Up     true      18.0.0.2      6b
mcc4-b1      mlx4_0          IB      Down   false     192.0.5.193   ib2a
mcc4-b1      mlx4_0          IB      Up     false     192.0.5.194   ib2b
mcc4-b2      fcvi_device_0   FC-VI   Up     true      17.0.2.2      6a
mcc4-b2      fcvi_device_1   FC-VI   Up     true      18.0.1.2      6b
mcc4-b2      mlx4_0          IB      Down   false     192.0.2.9     ib2a
mcc4-b2      mlx4_0          IB      Up     false     192.0.2.10    ib2b
8 entries were displayed.
```

MetroCluster 構成での **SNMPv3** の設定

作業を開始する前に

認証プロトコルとプライバシープロトコルは、スイッチと ONTAP システムで同じである必要があります。

このタスクについて

ONTAP は現在、 AES-128 暗号化をサポートしています。

手順

1. コントローラのプロンプトで各スイッチの SNMP ユーザを作成します。

   'securitylogin create （セキュリティログインの作成

```
Controller_A_1::> security login create -user-or-group-name snmpv3user
-application snmp -authentication-method usm -role none -remote-switch
-ipaddress 10.10.10.10
```

2. サイトで必要に応じて、次のプロンプトに応答します。

   EngineID の場合は、**ENTER** を押してデフォルト値を割り当てます。

```
Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,
sha2-256) [none]: sha

Enter the authentication protocol password (minimum 8 characters long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128) [none]:
aes128

Enter privacy protocol password (minimum 8 characters long):

Enter privacy protocol password again:
```

同じユーザ名を IP アドレスが異なる別のスイッチに追加できます。

3. 残りのスイッチの SNMP ユーザを作成します。

   次の例は、 IP アドレス 10.10.10.11 のスイッチのユーザ名を作成する方法を示しています。

```
Controller_A_1::> security login create -user-or-group-name snmpv3user
-application snmp -authentication-method usm -role none -remote-switch
-ipaddress 10.
10.10.11
```

4. ログインエントリがスイッチごとに 1 つずつあることを確認します。

   「 securitylogin show 」を参照してください

```
Controller_A_1::> security login show -user-or-group-name snmpv3user
-fields remote-switch-ipaddress

vserver      user-or-group-name application authentication-method
remote-switch-ipaddress

------------ ------------------ ----------- ---------------------
-----------------------

node_A_1 SVM 1 snmpv3user     snmp        usm
10.10.10.10

node_A_1 SVM 2 snmpv3user     snmp        usm
10.10.10.11

node_A_1 SVM 3 snmpv3user    snmp        usm
10.10.10.12

node_A_1 SVM 4 snmpv3user     snmp        usm
10.10.10.13

4 entries were displayed.
```

5. スイッチのプロンプトで SNMPv3 を設定します。

Brocadeスイッチ **(FOS 9.0** 以降**)**

```
snmpconfig --add snmpv3 -index <index> -user <user_name> -groupname <rw/ro>
-auth_proto <auth_protocol> -auth_passwd <auth_password> -priv_proto
<priv_protocol> -priv_passwd <priv_password>
```

Brocadeスイッチ **(FOS 8.x** 以前**)**

「 mpconfig — set snmpv3 」

この例では、読み取り専用ユーザーを構成する方法を示します。必要に応じて RW ユーザーを調整できます。 RO アクセスが必要な場合は、「User (ro):」の後に「snmpv3user」を指定します。

```
Switch-A1:admin> snmpconfig --set snmpv3
SNMP Informs Enabled (true, t, false, f): [false] true
SNMPv3 user configuration(snmp user not configured in FOS user
database will have physical AD and admin role as the default):
User (rw): [snmpadmin1]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/AES128(3)/AES256(4)]): (2..2) [2]
Engine ID: [00:00:00:00:00:00:00:00:00:00]
User (ro): [snmpuser2] snmpv3user
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [2]
Priv Protocol [DES(1)/noPriv(2)/AES128(3)/AES256(4)]): (2..2) [3]
```

Cisco スイッチ

```
snmp-server user <user_name> auth [md5/sha/sha-256] <auth_password> priv
(aes-128) <priv_password>
```

また、未使用のアカウントにパスワードを設定して保護し、 ONTAP リリースで最適な暗号化機能を使用する必要があります。

6. 必要に応じて、残りのスイッチユーザに暗号化とパスワードを設定します。

健常性監視用の **MetroCluster** コンポーネントの設定

MetroCluster 構成のコンポーネントを監視するには、いくつかの特別な設定手順を実行する必要があります。

セキュリティを強化するために、NetAppでは、スイッチのヘルスを監視するようにSNMPv2またはSNMPv3を設定することを推奨します。

このタスクについて

これらのタスクは、 FC-to-SAS ブリッジを使用するシステムにのみ適用されます。

Fabric OS 9.0.1以降では、Brocadeスイッチでのヘルス監視でSNMPv2はサポートされていません。代わりにSNMPv3を使用する必要があります。SNMPv3を使用している場合は、次のセクションに進む前に、ONTAPでSNMPv3を設定する必要があります。詳細については、を参照してください MetroCluster 構成

での SNMPv3 の設定。

- ブリッジとノード管理 LIF は、他のソースからの干渉を避けるために専用のネットワークに配置する必要があります。
- 健全性監視に専用のネットワークを使用する場合は、各ノードのノード管理LIFをその専用のネットワーク内に配置する必要があります。

NetAppでは、MetroCluster FC構成のコンポーネントを監視するための次のツールのみがサポートされます。

- Brocade Network Advisor （ BNA ）
- Brocade SANnav
- Active IQ Config Advisor
- NetAppヘルスモニタリング（ONTAP）
- MetroClusterデータコレクタ（MC_DC）

健常性監視用の **MetroCluster FC** スイッチの設定

ファブリック接続 MetroCluster 構成の FC スイッチを監視するには、いくつかの設定手順を追加で実行する必要があります。

ONTAP 9.8以降では `storage switch`、コマンドがに置き換えられ `system switch fibre-channel`ました。以降の手順ではコマンドを使用し `storage switch`ますが、ONTAP 9.8以降を実行している場合はコマンドを使用 `system switch fibre-channel`することを推奨します。

手順

1. 各 MetroCluster ノードに IP アドレスを指定してスイッチを追加します。

   実行するコマンドは、SNMPv2とSNMPv3のどちらを使用しているかによって異なります。

   SNMPv3を使用してスイッチを追加します。

   ```
   storage switch add -address <ip_adddress> -snmp-version SNMPv3 -snmp
   -community-or-username <SNMP_user_configured_on_the_switch>
   ```

   SNMPv2を使用してスイッチを追加します。

   「 storage switch add -address ipaddress 」と入力します

   このコマンドは、 MetroCluster 構成の 4 つのスイッチすべてに対して繰り返す必要があります。

   健常性監視では、 Brocade 7840 FC スイッチと NoISLPresent_Alert を除くすべてのアラートがサポートされます

   次の例は、 IP アドレスが 10.10.10.10 のスイッチを追加するコマンドを示しています。

   ```
   controller_A_1::> storage switch add -address 10.10.10.10
   ```

2. すべてのスイッチが適切に設定されたことを確認します。

   「 storage switch show 」と表示されます

   ポーリング間隔が 15 分であるため、すべてのデータが反映されるまで最大で 15 分かかる場合があります。

   次の例は、 MetroCluster FC スイッチが設定されたことを検証するコマンドを示しています。

```
controller_A_1::> storage switch show
Fabric            Switch Name     Vendor  Model         Switch WWN
Status
---------------- --------------- ------- ------------ ----------------
------
1000000533a9e7a6 brcd6505-fcs40  Brocade Brocade6505  1000000533a9e7a6
OK
1000000533a9e7a6 brcd6505-fcs42  Brocade Brocade6505  1000000533d3660a
OK
1000000533ed94d1 brcd6510-fcs44  Brocade Brocade6510  1000000533eda031
OK
1000000533ed94d1 brcd6510-fcs45  Brocade Brocade6510  1000000533ed94d1
OK
4 entries were displayed.

controller_A_1::>
```

   スイッチの World Wide Name （ WWN ；ワールドワイド名）が表示される場合は、 ONTAP ヘルスモニタを使用して FC スイッチに接続し、監視できます。

関連情報

"システム管理"

健常性監視用の **FC-to-SAS** ブリッジの設定

9.8 より前のバージョンの ONTAP を実行しているシステムでは、 MetroCluster 構成の FC-to-SAS ブリッジを監視するには、いくつかの特別な設定手順を実行する必要があります。

このタスクについて

- FibreBridge ブリッジでは、サードパーティ製の SNMP 監視ツールはサポートされません。
- ONTAP 9.8 以降では、デフォルトで FC-to-SAS ブリッジがインバンド接続で監視されるため、追加の設定は必要ありません。

> ONTAP 9.8 以降では 'storage bridge コマンドは 'system bridge コマンドに置き換えられました 次の手順は「 storage bridge 」コマンドを示していますが、 ONTAP 9.8 以降を実行している場合は「 system bridge 」コマンドが優先されます。

手順

1. ONTAP クラスタのプロンプトで、ブリッジをヘルスモニタの対象に追加します。

   a. 使用している ONTAP のバージョンに対応したコマンドを使用して、ブリッジを追加します。

ONTAP バージョン	コマンドを実行します
9.5 以降	「 storage bridge add -address 0.0.0.0 -managed-by in-band-name_bridge-name_`
9.4 以前	「 storage bridge add -address_bridge-ip-address_-name_bridge-name_` 」

   b. ブリッジが追加され、正しく設定されていることを確認します。

      「 storage bridge show 」

      ポーリング間隔に応じて、すべてのデータが反映されるまで 15 分程度かかる場合があります。「 Status 」列の値が「 ok 」で、 World Wide Name （ WWN ；ワールドワイド名）などのその他の情報が表示されていれば、 ONTAP ヘルスモニタでブリッジに接続して監視できます。

      次の例は、 FC-to-SAS ブリッジが設定されていることを示しています。

```
controller_A_1::> storage bridge show

Bridge              Symbolic Name Is Monitored  Monitor Status  Vendor
Model                Bridge WWN
------------------  ------------ ------------  --------------  ------
-----------------    ----------
ATTO_10.10.20.10  atto01        true          ok              Atto
FibreBridge 7500N      20000010867038c0
ATTO_10.10.20.11  atto02        true          ok              Atto
FibreBridge 7500N      20000010867033c0
ATTO_10.10.20.12  atto03        true          ok              Atto
FibreBridge 7500N      20000010867030c0
ATTO_10.10.20.13  atto04        true          ok              Atto
FibreBridge 7500N      2000001086703b80

4 entries were displayed

 controller_A_1::>
```

MetroCluster の設定を確認しています

MetroCluster 構成内のコンポーネントおよび関係が正しく機能していることを確認できます。

チェックは、初期設定後と、 MetroCluster 設定に変更を加えたあとに実施する必要があります。また、ネゴシエート（計画的）スイッチオーバーやスイッチバックの処理の前にも実施します。

このタスクについて

いずれかまたは両方のクラスタに対して短時間に MetroCluster check run コマンドを 2 回発行すると ' 競合が発生し ' コマンドがすべてのデータを収集しない場合がありますそれ以降の MetroCluster check show コマンドでは ' 期待される出力は表示されません

手順

1. 構成を確認します。

   「 MetroCluster check run 」のようになります

   このコマンドはバックグラウンドジョブとして実行され、すぐに完了しない場合があります。

```
cluster_A::> metrocluster check run
The operation has been started and is running in the background. Wait
for
it to complete and run "metrocluster check show" to view the results. To
check the status of the running metrocluster check operation, use the
command,
"metrocluster operation history show -job-id 2245"
```

```
cluster_A::> metrocluster check show

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         ok
volumes             ok
7 entries were displayed.
```

2. 最新の MetroCluster check run コマンドから ' より詳細な結果を表示します

   MetroCluster check aggregate show

   MetroCluster check cluster show

   MetroCluster check config-replication show

   MetroCluster check lif show

   MetroCluster check node show

「 MetroCluster check show 」コマンドは、最新の「 MetroCluster check run 」コマンドの結果を表示します。MetroCluster check show コマンドを使用する前に ' 必ず MetroCluster check run コマンドを実行して ' 表示されている情報が最新であることを確認してください

次に、正常な 4 ノード MetroCluster 構成の MetroCluster check aggregate show コマンドの出力例を示します。

```
cluster_A::> metrocluster check aggregate show

Last Checked On: 8/5/2014 00:42:58

Node                  Aggregate                 Check
Result
---------------       --------------------      ----------------------
---------
controller_A_1        controller_A_1_aggr0
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
ok
                      controller_A_1_aggr1
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
ok
                      controller_A_1_aggr2
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
ok


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

```
                                                    mirroring-status
ok
                                                    disk-pool-allocation
ok
                                                    ownership-state
ok
                      controller_A_2_aggr2
                                                    mirroring-status
ok
                                                    disk-pool-allocation
ok
                                                    ownership-state
ok

18 entries were displayed.
```

次に、正常な 4 ノード MetroCluster 構成の MetroCluster check cluster show コマンドの出力例を示します。この出力は、必要に応じてネゴシエートスイッチオーバーを実行できる状態であることを示しています。

```
Last Checked On: 9/13/2017 20:47:04

Cluster               Check                          Result
--------------------- ------------------------------ ---------
mccint-fas9000-0102
                      negotiated-switchover-ready    not-applicable
                      switchback-ready               not-applicable
                      job-schedules                  ok
                      licenses                       ok
                      periodic-check-enabled         ok
mccint-fas9000-0304
                      negotiated-switchover-ready    not-applicable
                      switchback-ready               not-applicable
                      job-schedules                  ok
                      licenses                       ok
                      periodic-check-enabled         ok
10 entries were displayed.
```

関連情報

"ディスクおよびアグリゲートの管理"

"ネットワークと LIF の管理"

Config Advisor での MetroCluster 構成エラーの確認

一般的な構成エラーの有無を確認する Config Advisor ツールをネットアップサポートサイトからダウンロードできます。

このタスクについて

Config Advisor は、構成の検証や健常性のチェックに使用できるツールです。データ収集とシステム分析のために、セキュアなサイトにもセキュアでないサイトにも導入できます。

Config Advisor のサポートには制限があり、オンラインでしか使用できません。

手順

1. Config Advisor のダウンロードページにアクセスし、ツールをダウンロードします。

   "ネットアップのダウンロード： Config Advisor"

2. Config Advisor を実行し、ツールの出力を確認して、問題が検出された場合は出力に表示される推奨事項に従って対処します。

ローカル HA の処理を検証しています

4 ノード MetroCluster 構成の場合、 MetroCluster 構成のローカル HA ペアの処理を検証する必要があります。2 ノード構成の場合は不要です。

このタスクについて

2 ノード MetroCluster 構成ではローカル HA ペアは構成されないため、このタスクは適用されません。

このタスクの例では、次の標準的な命名規則を使用します。

- cluster_A
  - controller_A_1
  - controller_A_2
- cluster_B
  - controller_B_1
  - controller_B_2

手順

1. cluster_A で、フェイルオーバーとギブバックを両方向で実行します。

   a. ストレージフェイルオーバーが有効になっていることを確認します。

      「 storage failover show 」をクリックします

      両方のノードでテイクオーバーが可能であることが出力に示されます。

```
cluster_A::> storage failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- -------- -------------------------
controller_A_1 controller_A_2 true     Connected to controller_A_2

controller_A_2 controller_A_1 true     Connected to controller_A_1
2 entries were displayed.
```

b. controller_A_1 から controller_A_2 をテイクオーバーします。

'storage failover takeover controller_A_2

テイクオーバー処理の進捗は storage failover show-takeover コマンドを使用して監視できます。

c. テイクオーバーが完了したことを確認します。

「 storage failover show 」をクリックします

出力には、 controller_A_1 がテイクオーバー状態であること、 HA パートナーをテイクオーバーしたことが示されます。

```
cluster_A::> storage failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- -------- -----------------
controller_A_1 controller_A_2 false    In takeover

controller_A_2 controller_A_1 -        Unknown
2 entries were displayed.
```

d. controller_A_2 をギブバックします。

'storage failover giveback controller_A_2

「 storage failover show-giveback 」コマンドを使用すると、ギブバック処理の進捗を監視できます。

e. ストレージフェイルオーバーが通常の状態に戻ったことを確認します。

「 storage failover show 」をクリックします

両方のノードでテイクオーバーが可能であることが出力に示されます。

```
cluster_A::> storage failover show
                                Takeover
Node            Partner         Possible State Description
--------------- --------------- -------- --------------------------
controller_A_1 controller_A_2 true     Connected to controller_A_2

controller_A_2 controller_A_1 true     Connected to controller_A_1
2 entries were displayed.
```

a. ここまでの手順を繰り返して、今度は controller_A_2 から controller_A_1 をテイクオーバーします。

2. cluster_B に関して、上記の手順を繰り返します

関連情報

"ハイアベイラビリティ構成"

スイッチオーバー、修復、スイッチバックを検証しています

MetroCluster 構成のスイッチオーバー、修復、スイッチバックの処理を検証する必要があります。

ステップ

1. に記載されているネゴシエートスイッチオーバー、修復、スイッチバックの手順を使用します "災害からリカバリします"。

構成バックアップファイルを保護しています

ローカルクラスタ内のデフォルトの場所に加えて、クラスタ構成バックアップファイルをアップロードするリモート URL （ HTTP または FTP ）を指定することで、クラスタ構成バックアップファイルの保護を強化できます。

ステップ

1. 構成バックアップファイルのリモートデスティネーションの URL を設定します。

「システム構成のバックアップ設定 MODIT_URL-of-destination_ 」

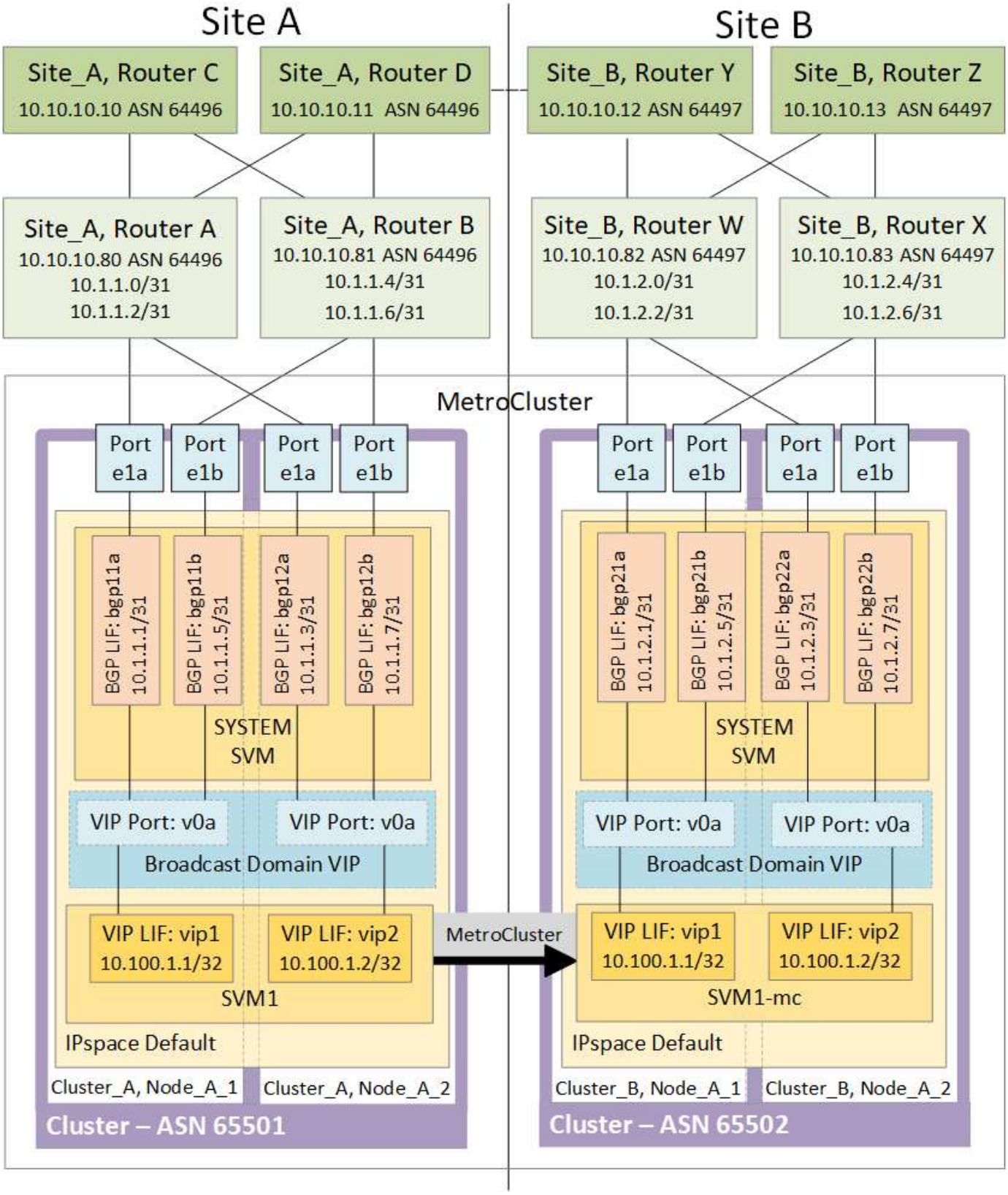
。 "CLI を使用したクラスタ管理" 追加情報が含まれています。

MetroCluster 設定で仮想 IP およびボーダーゲートウェイプロトコルを使用する場合の考慮事項

ONTAP 9.5 以降では、 ONTAP で仮想 IP （ VIP ）と Border Gateway Protocol （ BGP ）を使用してレイヤ 3 接続がサポートされます。VIP と BGP を組み合わせることで、フロントエンドネットワークでの冗長性とバックエンド MetroCluster の冗長性が確保され、レイヤ 3 ディザスタリカバリ解決策が実現します。

レイヤ 3 解決策を計画する際は、次のガイドラインと図を確認してください。ONTAP での VIP および BGP

の実装の詳細については、を参照してください "仮想 IP LIF を設定"。



ONTAP の制限事項

ONTAP では、 MetroCluster 構成の両方のサイトのすべてのノードに BGP ピアリングが設定されていること

は自動的には検証されません。

ONTAP は、ルートアグリゲーションを実行するのではなく、個々の仮想 LIF のすべての IP を一意のホストルートとして常時通知します。

ONTAP は、真のエニーキャストをサポートしません。クラスタ内の 1 つのノードだけが、特定の仮想 LIF の IP を提供します（ただし、物理ポートが正しい IPspace の一部である場合は、 BGP LIF であるかどうかに関係なく、すべての物理インターフェイスで許可されます）。異なる LIF は、異なるホストノードに個別に移行できます。

このレイヤ 3 解決策を MetroCluster 設定で使用する場合の注意事項

必要な冗長性を確保するために、 BGP および VIP を正しく設定する必要があります。

よりシンプルな導入シナリオが、より複雑なアーキテクチャよりも推奨されます（たとえば、 BGP ピアリングルータは、中間の BGP 以外のルータ経由で到達可能です）。ただし、 ONTAP では、ネットワーク設計やトポロジの制限は適用されません。

VIP LIF はフロントエンド / データネットワークのみをカバーします。

ONTAP のバージョンに応じて、システム SVM やデータ SVM ではなく、ノード SVM に BGP ピアリング LIF を設定する必要があります。ONTAP 9.8 では、クラスタ（システム） SVM 内に BGP LIF が表示され、ノード SVM が存在しなくなります。

各データ SVM には、 LIF の移行や MetroCluster のフェイルオーバーが発生したときにリターンデータパスを使用できるように、考えられるすべてのファーストホップゲートウェイアドレス（通常は BGP ルータピアリングの IP アドレス）を設定する必要があります。

BGP LIF はクラスタ間 LIF と同様にノード固有で、各ノードは一意の設定を持ちます。 DR サイトのノードにレプリケートする必要はありません。

設定が完了すると、v0a（v0bなど）が接続を継続的に検証し、LIFの移行またはフェイルオーバーが成功するかどうかを（停止したあとにのみ構成の分断が認識されるL2とは異なります）チェックします。

アーキテクチャに大きな違いは、クライアントがデータ SVM の VIP と同じ IP サブネットを共有しなくなることです。適切なエンタープライズクラスの復元力と冗長性機能（たとえば、 VRRP/HSRP ）をイネーブルにした L3 ルータは、 VIP が正しく動作するために、ストレージとクライアント間のパス上に配置する必要があります。

BGP の信頼性の高い更新プロセスにより、 LIF の移行がわずかに高速化され、一部のクライアントの中断が少なくなるため、円滑な移行が可能になります

ネットワークまたはスイッチの一部の動作を LACP よりも高速に検出するように BGP を設定できます（設定されている場合）。

外部 BGP （ EBGP ）は、 ONTAP ノードとピアリングルータ間で異なる AS 番号を使用し、ルータ上でのルート集約と再配布を容易にするための推奨配置です。内部 BGP （ IBGP ）およびルートリフレクタの使用は不可能ではありませんが、簡単な VIP 設定の範囲外です。

導入後、関連する仮想 LIF が各サイトのすべてのノード間で移行されたときに（ MetroCluster スイッチオーバーを含む）データ SVM にアクセスできることを確認し、同じデータ SVM への静的ルートの正しい設定を確認する必要があります。

VIP は、ほとんどの IP ベースのプロトコル（ NFS 、 SMB 、 iSCSI ）に対応しています。

MetroCluster 構成をテストする

障害シナリオをテストして、 MetroCluster 構成が正しく動作していることを確認できます。

ネゴシエートスイッチオーバーを検証中

ネゴシエート（計画的）スイッチオーバー処理をテストして、データが中断なく提供されることを確認できます。

このタスクについて

このテストでは、クラスターを 2 番目のデータ センターに切り替えても、データの可用性が影響を受けないこと (SMB およびファイバ チャネル プロトコルを除く) を検証します。

このテストには約 30 分かかります。

この手順の想定される結果は次のとおりです。

- MetroCluster switchover コマンドは ' 警告プロンプトを表示します

  プロンプトに「 yes 」と応答すると、コマンドが発行されたサイトがパートナーサイトを切り替えます。

MetroCluster IP 構成の場合：

- ONTAP 9.4 以前：
  - ミラーアグリゲートはネゴシエートスイッチオーバー後にデグレード状態になります。
- ONTAP 9.5 以降：
  - リモートストレージがアクセス可能である場合、ミラーされたアグリゲートは通常の状態のままになります。
  - リモートストレージへのアクセスが失われると、ネゴシエートスイッチオーバー後にミラーアグリゲートがデグレード状態になります。
- ONTAP 9.8 以降の場合：
  - リモートストレージへのアクセスが失われると、ディザスタサイトにあるミラーされていないアグリゲートは使用できなくなります。これにより、コントローラが停止する可能性があります。

手順

1. すべてのノードが設定済みの状態で通常モードになっていることを確認します。

   MetroCluster node show

```
cluster_A::>  metrocluster node show

Cluster                           Configuration State    Mode
--------------------------------- ---------------------
------------------------
 Local: cluster_A                  configured             normal
Remote: cluster_B                  configured             normal
```

2. スイッチオーバー処理を開始します。

   MetroCluster スイッチオーバー

```
cluster_A::> metrocluster switchover
Warning: negotiated switchover is about to start. It will stop all the
data Vservers on cluster "cluster_B" and
automatically re-start them on cluster "`cluster_A`". It will finally
gracefully shutdown cluster "cluster_B".
```

3. ローカルクラスタが設定済みの状態でスイッチオーバーモードになっていることを確認します。

   MetroCluster node show

```
cluster_A::>  metrocluster node show

Cluster                           Configuration State    Mode
--------------------------------- ---------------------
------------------------
Local: cluster_A                   configured             switchover
Remote: cluster_B                  not-reachable          -
              configured             normal
```

4. スイッチオーバー処理が成功したことを確認します。

   「 MetroCluster operation show 」を参照してください

```
cluster_A::> metrocluster operation show
  Operation: switchover
      State: successful
 Start Time: 2/6/2016 13:28:50
   End Time: 2/6/2016 13:29:41
     Errors: -
```

5. 「 vserver show 」コマンドと「 network interface show 」コマンドを使用して、 DR SVM と LIF がオン

ラインになったことを確認します。

修復と手動スイッチバックの検証

修復処理と手動スイッチバック処理をテストするには、ネゴシエートスイッチオーバー後にクラスタを元のデータセンターにスイッチバックして、データの可用性に影響がないことを検証します（ SMB および Solaris FC 構成を除く）。

このタスクについて

このテストには約 30 分かかります。

この手順では、想定される結果として、サービスがホームノードにスイッチバックされることを確認します。

手順

1. 修復が完了したことを確認します。

   MetroCluster node show

   次の例は、コマンドが正常に完了したことを示しています。

```
cluster_A::> metrocluster node show
DR                               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.
```

2. すべてのアグリゲートがミラーされたことを確認します。

   「 storage aggregate show

   次の例では、すべてのアグリゲートの RAID ステータスが mirrored になっています。

```
cluster_A::> storage aggregate show
cluster Aggregates:
Aggregate Size     Available Used% State   #Vols  Nodes       RAID
Status
--------- -------- --------- ----- ------- ------ ----------
------------
data_cluster
            4.19TB    4.13TB    2% online       8 node_A_1    raid_dp,
                                                               mirrored,
                                                               normal
root_cluster
           715.5GB   212.7GB   70% online       1 node_A_1    raid4,
                                                               mirrored,
                                                               normal
cluster_B Switched Over Aggregates:
Aggregate Size     Available Used% State   #Vols  Nodes       RAID
Status
--------- -------- --------- ----- ------- ------ ----------
------------
data_cluster_B
            4.19TB    4.11TB    2% online       5 node_A_1    raid_dp,
                                                               mirrored,
                                                               normal
root_cluster_B    -         -     - unknown      - node_A_1   -
```

3. ディザスタサイトからノードをブートします。
4. スイッチバックリカバリのステータスを確認します。

   MetroCluster node show

```
cluster_A::> metrocluster node show
DR                              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.
```

5. スイッチバックを実行します。

   MetroCluster スイッチバック

```
cluster_A::> metrocluster switchback
[Job 938] Job succeeded: Switchback is successful.Verify switchback
```

6. ノードのステータスを確認します。

   MetroCluster node show

```
cluster_A::> metrocluster node show
DR                               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.
```

7. ステータスを確認します。

   「 MetroCluster operation show 」を参照してください

   正常に完了したことを示す出力が表示されます。

```
cluster_A::> metrocluster operation show
  Operation: switchback
      State: successful
 Start Time: 2/6/2016 13:54:25
   End Time: 2/6/2016 13:56:15
     Errors: -
```

単一の FC-to-SAS ブリッジの停止

単一の FC-to-SAS ブリッジの障害をテストして、単一点障害がないことを確認できます。

このタスクについて
このテストには約 15 分かかります。

この手順の想定される結果は次のとおりです。

- ブリッジのスイッチがオフになるため、とエラーが生成されます。
- フェイルオーバーやサービスの中断は発生しません。
- コントローラモジュールからブリッジに接続されたドライブへのパスは 1 つだけになります。

ONTAP 9.8 以降では 'storage bridge コマンドは 'system bridge コマンドに置き換えられました 次の手順は「 storage bridge 」コマンドを示していますが、 ONTAP 9.8 以降を実行している場合は「 system bridge 」コマンドが優先されます。

手順

1. ブリッジの電源装置をオフにします。
2. ブリッジの監視がエラーを示していることを確認します。

   「 storage bridge show 」

```
cluster_A::> storage bridge show

                                                                  Is
Monitor
Bridge     Symbolic Name Vendor  Model     Bridge WWN       Monitored
Status
---------- ------------- ------- --------- ---------------- ---------
-------
ATTO_10.65.57.145
         bridge_A_1    Atto    FibreBridge 6500N
                                           200000108662d46c true
error
```

3. ブリッジに接続されたドライブに 1 つのパスでアクセス可能なことを確認します。

   「 storage disk error show 」と表示されます

```
cluster_A::> storage disk error show
Disk              Error Type        Error Text
----------------- -----------------
-------------------------------------------
1.0.0             onedomain         1.0.0 (5000cca057729118): All paths
to this array LUN are connected to the same fault domain. This is a
single point of failure.
1.0.1             onedomain         1.0.1 (5000cca057727364): All paths
to this array LUN are connected to the same fault domain. This is a
single point of failure.
1.0.2             onedomain         1.0.2 (5000cca05772e9d4): All paths
to this array LUN are connected to the same fault domain. This is a
single point of failure.
...
1.0.23            onedomain         1.0.23 (5000cca05772e9d4): All paths
to this array LUN are connected to the same fault domain. This is a
single point of failure.
```

電源回線切断後の動作確認

MetroCluster 構成で PDU の障害が発生した場合の対応をテストできます。

このタスクについて

ベストプラクティスとして、コンポーネントの各電源装置（ PSU ）を別々の電源装置に接続することを推奨します。両方の PSU を同じ配電ユニット（ PDU ）に接続している場合、停電が発生したときに、サイトが停止したりシェルフ全体が使用できなくなったりする可能性があります。1 本原因の電源回線に障害が発生した場合に、サービスが中断する可能性があるケーブル接続の不一致がないかどうかをテストします。

このテストには約 15 分かかります。

このテストでは、 MetroCluster コンポーネントが格納されたすべてのラックで、左側のすべての PDU の電源をオフにしてから、右側のすべての PDU の電源をオフにする必要があります。

この手順の想定される結果は次のとおりです。

- PDU の接続が切断されるため、エラーが生成されます。
- フェイルオーバーやサービスの中断は発生しません。

手順

1. MetroCluster コンポーネントが格納されたラックの左側の PDU の電源をオフにします。
2. コンソールで結果を監視します。

   「 system environment sensors show -state fault 」というエラーが表示されます

   「 storage shelf show -errors 」を参照してください

```
cluster_A::> system environment sensors show -state fault

Node Sensor             State Value/Units Crit-Low Warn-Low Warn-Hi
Crit-Hi
---- -------------------- ------ ----------- -------- -------- -------
-------
node_A_1
        PSU1            fault
                            PSU_OFF
        PSU1 Pwr In OK  fault
                            FAULT
node_A_2
        PSU1            fault
                            PSU_OFF
        PSU1 Pwr In OK  fault
                            FAULT
4 entries were displayed.

cluster_A::> storage shelf show -errors
    Shelf Name: 1.1
     Shelf UID: 50:0a:09:80:03:6c:44:d5
 Serial Number: SHFHU1443000059

Error Type          Description
------------------  ---------------------------
Power               Critical condition is detected in storage shelf
power supply unit "1". The unit might fail.Reconnect PSU1
```

3. 左側の PDU の電源を再度オンにします。
4. ONTAP がエラー状態をクリアすることを確認します。
5. 右側の PDU で上記の手順を繰り返します。

スイッチファブリック障害後の動作確認

スイッチファブリックを無効にして、データの可用性に影響がないことを確認できます。

このタスクについて

このテストには約 15 分かかります。

この手順では、想定される結果として、ファブリックを無効にしたあとにクラスタインターコネクトとディスクのすべてのトラフィックがもう一方のファブリックに送られることを確認します。

この例では、スイッチファブリック 1 を無効にしています。このファブリックは、各 MetroCluster サイトに 1 つずつ、 2 つのスイッチで構成されます。

- cluster_A の FC_switch_A_1
- cluster_B の FC_switch_B_1

手順

1. MetroCluster 構成の 2 つのスイッチファブリックの一方への接続を無効にします。

   a. ファブリックの 1 つ目のスイッチを無効にします。

      'witchdisable

      ```
      FC_switch_A_1::> switchdisable
      ```

   b. ファブリックの 2 つ目のスイッチを無効にします。

      'witchdisable

   ```
   FC_switch_B_1::> switchdisable
   ```

2. コントローラモジュールのコンソールで結果を監視します。

   次のコマンドを使用してクラスタノードをチェックし、すべてのデータが引き続き提供されていることを確認できます。コマンドの出力に、ディスクへのパスがないことが示されます。これは想定される状態です。

   - vserver show のコマンドです
   - network interface show の略
   - aggr show のコマンドを入力し
   - system node run nodename command storage show disk -p のようになりました
   - storage disk error show のコマンドを入力します

3. MetroCluster 構成の 2 つのスイッチファブリックの一方への接続を再度有効にします。

   a. ファブリックの 1 つ目のスイッチを再度有効にします。

      「 witchenable 」

      ```
      FC_switch_A_1::> switchenable
      ```

   b. ファブリックの 2 つ目のスイッチを再度有効にします。

      「 witchenable 」

   ```
   FC_switch_B_1::> switchenable
   ```

4. 10 分以上待ってから、もう一方のスイッチファブリックで上記の手順を繰り返します。

単一のストレージシェルフが停止したあとの動作確認

単一のストレージシェルフの障害をテストして、単一点障害がないことを確認できます。

このタスクについて

この手順の想定される結果は次のとおりです。

- 監視ソフトウェアからエラーメッセージが報告されます。
- フェイルオーバーやサービスの中断は発生しません。
- ハードウェア障害がリストアされたあと、ミラーの再同期が自動的に開始されます。

手順

1. ストレージフェイルオーバーのステータスを確認します。

   「 storage failover show 」をクリックします

   ```
   cluster_A::> storage failover show

   Node            Partner         Possible State Description
   --------------- --------------- --------
   -------------------------------------
   node_A_1        node_A_2        true     Connected to node_A_2
   node_A_2        node_A_1        true     Connected to node_A_1
   2 entries were displayed.
   ```

2. アグリゲートのステータスを確認します。

   「 storage aggregate show

```
cluster_A::> storage aggregate show

cluster Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
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,

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

cluster_A::> vserver show -type data
                                Admin      Operational Root
Vserver     Type    Subtype    State      State       Volume
Aggregate
----------- ------- ---------- ---------- ----------- ----------
----------
SVM1        data    sync-source           running     SVM1_root
node_A_1_data01_mirrored
SVM2        data    sync-source           running     SVM2_root
node_A_2_data01_mirrored

cluster_A::> network interface show -fields is-home false
There are no entries matching your query.

cluster_A::> volume show !vol0,!MDV*
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
SVM1
          SVM1_root
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.50GB    5%
SVM1
          SVM1_data_vol
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_root
                       node_A_2_data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_data_vol
                       node_A_2_data02_unmirrored
                                    online     RW          1GB
972.6MB    5%
```

4. ハードウェア障害をシミュレートするために電源をオフにするノード node_A_1 のプール 1 内のシェルフ

を特定します。

「 storage aggregate show -r -node node_name !!* root

ミラーされたデータアグリゲートを構成するドライブが格納されたシェルフを選択する必要があります。

次の例では、停止する対象としてシェルフ ID 31 を選択します。

```
cluster_A::> storage aggregate show -r -node node_A_2 !*root
Owner Node: node_A_2
 Aggregate: node_A_2_data01_mirrored (online, raid_dp, mirrored) (block
checksums)
  Plex: /node_A_2_data01_mirrored/plex0 (online, normal, active, pool0)
   RAID Group /node_A_2_data01_mirrored/plex0/rg0 (normal, block
checksums)
                                                                   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 (online, normal, active, pool1)
   RAID Group /node_A_2_data01_mirrored/plex4/rg0 (normal, block
checksums)
                                                                   Usable
Physical
     Position Disk                       Pool Type     RPM     Size
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
828.0GB (normal)

 Aggregate: node_A_2_data02_unmirrored (online, raid_dp) (block
checksums)
  Plex: /node_A_2_data02_unmirrored/plex0 (online, normal, active,
pool0)
   RAID Group /node_A_2_data02_unmirrored/plex0/rg0 (normal, block
checksums)
                                                                   Usable
Physical
     Position Disk                       Pool Type     RPM     Size
Size Status
     -------- -------------------------- ---- ----- ------ --------
-------- ----------
     dparity  2.30.12                     0   BSAS    7200  827.7GB
828.0GB (normal)
     parity   2.30.22                     0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.21                     0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.20                     0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.14                     0   BSAS    7200  827.7GB
828.0GB (normal)
15 entries were displayed.
```

5. 選択したシェルフの電源を物理的にオフにします。
6. アグリゲートのステータスを再度確認します。

   「 storage aggregate show

   「 storage aggregate show -r -node node_name ！ * root 」

   電源をオフにしたシェルフにドライブがあるアグリゲートの RAID ステータスは「 degraded 」になり、影響を受けたプレックスのドライブのステータスは「 failed 」になります。次に例を示します。

```
cluster_A::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_A_1data01_mirrored
            4.15TB    3.40TB   18% online       3 node_A_1
```

```
raid_dp,

mirrored,

normal
node_A_1root
           707.7GB   34.29GB   95% online       1 node_A_1
raid_dp,

mirrored,

normal
node_A_2_data01_mirrored
            4.15TB    4.12TB    1% online       2 node_A_2
raid_dp,

mirror

degraded
node_A_2_data02_unmirrored
            2.18TB    2.18TB    0% online       1 node_A_2
raid_dp,

normal
node_A_2_root
           707.7GB   34.27GB   95% online       1 node_A_2
raid_dp,

mirror

degraded
cluster_A::> storage aggregate show -r -node node_A_2 !*root
Owner Node: node_A_2
 Aggregate: node_A_2_data01_mirrored (online, raid_dp, mirror degraded)
(block checksums)
  Plex: /node_A_2_data01_mirrored/plex0 (online, normal, active, pool0)
   RAID Group /node_A_2_data01_mirrored/plex0/rg0 (normal, block
checksums)
                                                                   Usable
Physical
     Position Disk                       Pool Type     RPM     Size
Size Status
     -------- -------------------------- ---- ----- ------ --------
-------- ----------
     dparity  2.30.3                      0   BSAS    7200  827.7GB
828.0GB (normal)
```

```
     parity   2.30.4                     0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.6                     0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.8                     0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.5                     0   BSAS    7200  827.7GB
828.0GB (normal)

  Plex: /node_A_2_data01_mirrored/plex4 (offline, failed, inactive,
pool1)
   RAID Group /node_A_2_data01_mirrored/plex4/rg0 (partial, none
checksums)
                                                                  Usable
Physical
     Position Disk                      Pool Type     RPM     Size
Size Status
     -------- ------------------------- ---- ----- ------ --------
-------- ----------
     dparity  FAILED                     -   -          -  827.7GB
-  (failed)
     parity   FAILED                     -   -          -  827.7GB
-  (failed)
     data     FAILED                     -   -          -  827.7GB
-  (failed)
     data     FAILED                     -   -          -  827.7GB
-  (failed)
     data     FAILED                     -   -          -  827.7GB
-  (failed)

 Aggregate: node_A_2_data02_unmirrored (online, raid_dp) (block
checksums)
  Plex: /node_A_2_data02_unmirrored/plex0 (online, normal, active,
pool0)
   RAID Group /node_A_2_data02_unmirrored/plex0/rg0 (normal, block
checksums)
                                                                  Usable
Physical
     Position Disk                      Pool Type     RPM     Size
Size Status
     -------- ------------------------- ---- ----- ------ --------
-------- ----------
     dparity  2.30.12                    0   BSAS    7200  827.7GB
828.0GB (normal)
     parity   2.30.22                    0   BSAS    7200  827.7GB
828.0GB (normal)
```

```
     data     2.30.21                    0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.20                    0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.14                    0   BSAS    7200  827.7GB
828.0GB (normal)
15 entries were displayed.
```

7. データが提供されていること、およびすべてのボリュームがオンラインのままであることを確認します。

   vserver show -type data

   network interface show -fields is-home false

   volume show ！ vol0 、 ！ MDV *

```
cluster_A::> vserver show -type data

cluster_A::> vserver show -type data
                                Admin      Operational Root
Vserver     Type    Subtype    State      State       Volume
Aggregate
----------- ------- ---------- ---------- ----------- ----------
----------
SVM1        data    sync-source           running     SVM1_root
node_A_1_data01_mirrored
SVM2        data    sync-source           running     SVM2_root
node_A_1_data01_mirrored

cluster_A::> network interface show -fields is-home false
There are no entries matching your query.

cluster_A::> volume show !vol0,!MDV*
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
SVM1
          SVM1_root
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.50GB    5%
SVM1
          SVM1_data_vol
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_root
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_data_vol
                       node_A_2_data02_unmirrored
                                    online     RW          1GB
972.6MB    5%
```

8. シェルフの電源を物理的にオンにします。

   再同期が自動的に開始されます

9. 再同期が開始されたことを確認します。

「 storage aggregate show

次の例に示すように、影響を受けたアグリゲートの RAID ステータスは「 resyncing 」になります。

```
cluster_A::> storage aggregate show
cluster Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_A_1_data01_mirrored
            4.15TB    3.40TB   18% online       3 node_A_1
raid_dp,

mirrored,

normal
node_A_1_root
           707.7GB   34.29GB   95% online       1 node_A_1
raid_dp,

mirrored,

normal
node_A_2_data01_mirrored
            4.15TB    4.12TB    1% online       2 node_A_2
raid_dp,

resyncing
node_A_2_data02_unmirrored
            2.18TB    2.18TB    0% online       1 node_A_2
raid_dp,

normal
node_A_2_root
           707.7GB   34.27GB   95% online       1 node_A_2
raid_dp,

resyncing
```

10. アグリゲートを監視して、再同期が完了したことを確認します。

「 storage aggregate show

次の例に示すように、影響を受けるアグリゲートの RAID ステータスは「 normal 」になります。

```
cluster_A::> storage aggregate show
cluster Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_A_1data01_mirrored
            4.15TB    3.40TB   18% online       3 node_A_1
raid_dp,

mirrored,

normal
node_A_1root
           707.7GB   34.29GB   95% online       1 node_A_1
raid_dp,

mirrored,

normal
node_A_2_data01_mirrored
            4.15TB    4.12TB    1% online       2 node_A_2
raid_dp,

normal
node_A_2_data02_unmirrored
            2.18TB    2.18TB    0% online       1 node_A_2
raid_dp,

normal
node_A_2_root
           707.7GB   34.27GB   95% online       1 node_A_2
raid_dp,

resyncing
```

MetroCluster 構成を削除

MetroCluster構成を削除する必要がある場合は、テクニカル サポートにお問い合わせください。

NetAppテクニカルサポートに連絡し、構成に適したガイドを参照してください。 "MetroCluster 構成-解決ガイドからノードを削除する方法"

MetroClusterの構成解除を元に戻すことはできません。このプロセスは、テクニカルサポートの支援を受けてのみ実行してください。MetroCluster構成を削除した後、すべてのMetroCluster接続と相互接続をサポート可能な状態に調整する必要があります。

Active IQ Unified Manager と ONTAP System Manager を使用して設定と監視を強化する方法

Active IQ Unified ManagerおよびONTAPシステムマネージャを使用して詳細な設定と監視を行う

Active IQ Unified Manager と ONTAP の System Manager は、 GUI を使用したクラスタ管理および設定監視に使用できます。

各ノードには ONTAP System Manager が事前にインストールされています。System Manager をロードするには、ノードに接続されている Web ブラウザのアドレスバーにクラスタ管理 LIF アドレスを入力します。

Active IQ Unified Manager を使用して MetroCluster 設定を監視することもできます。

関連情報

"Active IQ Unified Managerのドキュメント"

NTP を使用してシステム時刻を同期します

ノードとそのクライアントの間で時刻を同期するには、クラスタごとに独自の Network Time Protocol （ NTP ；ネットワークタイムプロトコル）サーバが必要です。

このタスクについて

- テイクオーバーの発生後に障害ノードまたはパートナーノードのタイムゾーン設定を変更することはできません。
- MetroCluster FC 構成のクラスタごとに、その MetroCluster サイトのノード、 FC スイッチ、および FC-to-SAS ブリッジで使用する独自の NTP サーバをそれぞれ用意する必要があります。
- MetroCluster Tiebreaker ソフトウェアを使用する場合は、それ専用の NTP サーバも必要です。

ONTAPのバージョンに応じて、System Manager UIの*タブまたは[インサイト]*タブでNTPを設定できます。

クラスタ

System Managerでは、ONTAPのバージョンに応じて*[クラスタ]*タブから次の2つのオプションを使用してNTPを設定できます。

ONTAP 9.8以降：

次の手順に従って、ONTAP 9.8以降の*[クラスタ]*タブからNTPを同期します。

手順

1. [クラスタ]>[概要]*に移動します。
2. 次に、オプションを選択し 

て*[編集]*を選択します。
3. ウィンドウで、**[NTP**サーバ**]**の下の+追加*オプションを選択します。
4. タイムサーバの名前と場所を追加し、IPアドレスを指定します。
5. 次に、*[保存]*を選択します。
6. タイムサーバを追加する場合は、この手順を繰り返します。

ONTAP 9.11.1以降：

次の手順に従って、ONTAP 9.11.1以降の*[クラスタ]タブの*[インサイト]*ウィンドウからNTPを同期します。

手順

1. [クラスタ]>[概要]*に移動します。
2. ページの* Insights ウィンドウまで下にスクロールし、 Too few NTP servers are configured（設定されているNTPサーバが少なすぎる）を探して Fix it（修正）*を選択します。
3. タイムサーバのIPアドレスを指定し、*[保存]*を選択します。
4. タイムサーバを追加する場合は、上記の手順を繰り返します。

分析

ONTAP 9.11.1以降では、System Managerの*[Insights]*タブを使用してNTPを設定することもできます。

手順

1. System Manager UIの*[Insights]*タブに移動します。
2. 下にスクロールして*を選択し、[Fix it]*を選択します。
3. タイムサーバのIPアドレスを指定し、*[保存]*を選択します。
4. タイムサーバを追加する場合は、上記の手順を繰り返します。

MetroCluster 構成で ONTAP を使用する場合の考慮事項

MetroCluster 構成で ONTAP を使用する場合は、ライセンス、 MetroCluster 構成の外部にあるクラスタとのピアリング、ボリューム処理や NVFAIL 処理などの ONTAP 処理の実行について、一定の考慮事項に注意する必要があります。

ライセンスに関する考慮事項

- 両方のサイトに、同じサイトライセンスが設定されている必要があります。
- すべてのノードに同じノードロック式ライセンスが設定されている必要があります。

SnapMirror に関する考慮事項

- SnapMirror SVM ディザスタリカバリは、 ONTAP 9.5 以降のバージョンを実行している MetroCluster 構成でのみサポートされます。

MetroCluster 構成での FlexCache のサポート

ONTAP 9.7 以降では、 MetroCluster 構成で FlexCache ボリュームがサポートされます。スイッチオーバーまたはスイッチバック処理後の手動廃止の要件を理解しておく必要があります。

FlexCache の元のデータとキャッシュが同じ **MetroCluster** サイト内にある場合のスイッチオーバー後の **SVM** 削除

ネゴシエートスイッチオーバーまたは計画外スイッチオーバーのあと、クラスタ内の SVM FlexCache ピア関係を手動で設定する必要があります。

たとえば、 SVM vs1 （キャッシュ）と vs2 （元）が site_A にあるとしますこれらの SVM はピア関係にあります。

スイッチオーバー後、 SVM 「 vs1-mc 」と「 vs2-mc 」がパートナーサイト（ site_B ）でアクティブ化されます。FlexCache が「 vserver peer repeer 」コマンドを使用して機能するには、これらの機能を手動で廃止する必要があります。

FlexCache デスティネーションが第 **3** のクラスタにあり、切断モードの場合のスイッチオーバーまたはスイッチバック後の **SVM** 削除

MetroCluster 構成外のクラスタへの FlexCache 関係では、スイッチオーバー中に関連するクラスタが切断モードになっている場合、スイッチオーバー後に常にピアリングを手動で再設定する必要があります。

例：

- FlexCache の一端（ vs1 の cache_1 ）は、 MetroCluster site_A にあります
- FlexCache のもう一方の端（ vs2 の origin_1 ）は、 site_A に配置されています（ MetroCluster 構成ではありません）。

スイッチオーバーがトリガーされたときに site_A と site_B が接続されていない場合は、スイッチオーバー後に「 vserver peer repeer 」コマンドを使用して site_B の SVM （スイッチオーバークラスタ）と site_B の SVM を手動で再ピアリングする必要があります。

スイッチバックが実行された場合は、 site_A （元のクラスタ）と site_B の SVM のピア関係を再設定する必要があります

関連情報

"FlexCache ボリュームの管理には CLI を使用します"

MetroCluster 構成での FabricPool のサポート

ONTAP 9.7 以降では、 MetroCluster 構成で FabricPool ストレージ階層がサポートされます。

FabricPool の使用に関する一般的な情報については、を参照してください "ディスクと階層（アグリゲート）の管理"。

FabricPool を使用する際の考慮事項

- クラスタに同じ容量制限の FabricPool ライセンスが必要です。
- 各クラスタに同じ名前の IPspace が必要です。

  これは、デフォルト IPspace か管理者が作成した IPspace です。この IPspace は、 FabricPool オブジェクトストア設定のセットアップに使用されます。

- 選択したIPspaceについて、外部のオブジェクトストアにアクセスできるクラスタ間LIFが各クラスタで定義されている必要があります。
- ソースまたはデスティネーションがMetroClusterクラスタの場合、FabricPoolでSVMの移行はサポートされません。

  "SVMデータモビリティの詳細"です。

ミラーリングされた FabricPool で使用するアグリゲートを設定する

アグリゲートを設定する前に、の説明に従ってオブジェクトストアを設定する必要があります。 "MetroCluster 構成で FabricPool のオブジェクトストアを設定する"。

手順

FabricPool で使用するアグリゲートを設定するには、次の手順を実行します。

1. アグリゲートを作成するか、既存のアグリゲートを選択します。
2. アグリゲートを MetroCluster 構成内の標準のミラーアグリゲートとしてミラーリングします。
3. の説明に従って、アグリゲートを使用して FabricPool ミラーを作成します "ディスクとアグリゲートの管理"
   a. プライマリオブジェクトストアを接続します。

      このオブジェクトストアは、クラスタに物理的に近い場所にあります。

   b. ミラーオブジェクトストアを追加します。

      このオブジェクトストアは、プライマリオブジェクトストアよりもクラスタから物理的に離れています。

ストレージのパフォーマンスと可用性を最適化するために、ミラーアグリゲートでは少なくとも20%の空きスペースを確保することを推奨します。ミラーされていないアグリゲートでは10%が推奨されますが、追加の10%のスペースはファイルシステムで増分変更に対応するために使用できます。増分変更を行うと、ONTAPのcopy-on-write Snapshotベースのアーキテクチャにより、ミラーされたアグリゲートのスペース使用率が向上します。これらのベストプラクティスに従わないと、パフォーマンスに悪影響を及ぼす可能性があります。

MetroCluster 構成での FlexGroup のサポート

ONTAP 9.6 以降では、 MetroCluster 構成で FlexGroup ボリュームがサポートされます。

MetroCluster 構成での整合グループのサポート

ONTAP 9.11.1以降、 "整合グループ" MetroCluster 構成でサポートされます。

MetroCluster 構成のジョブスケジュール

ONTAP 9.3 以降では、ユーザが作成したジョブスケジュールが MetroCluster 構成のクラスタ間で自動的にレプリケートされます。クラスタでジョブスケジュールを作成、変更、または削除すると、 Configuration Replication Service （ CRS ）を使用して同じスケジュールがパートナークラスタに自動的に作成されます。

システムによって作成されたスケジュールはレプリケートされません。両方のクラスタのジョブスケジュールが同じになるように、パートナークラスタで同じ処理を手動で実行する必要があります。

MetroCluster サイトから第 3 のクラスタへのクラスタピアリング

ピアリング設定はレプリケートされないため、 MetroCluster 構成のどちらかのクラスタを構成外の第 3 のクラスタにピアリングする場合は、パートナーの MetroCluster クラスタでもピアリングを設定する必要があります。これにより、スイッチオーバーが発生してもピアリングが維持されます。

MetroCluster 以外のクラスタで ONTAP 8.3 以降が実行されている必要があります。そうでない場合、両方の MetroCluster パートナーでピアリングが設定されていても、スイッチオーバーが発生するとピアリングが失われます。

MetroCluster 構成での LDAP クライアント設定のレプリケーション

ローカルクラスタの Storage Virtual Machine （ SVM ）に作成された LDAP クライアント設定は、リモートクラスタのパートナーのデータ SVM にレプリケートされます。たとえば、ローカルクラスタの管理 SVM に LDAP クライアント設定が作成されると、リモートクラスタのすべての管理データ SVM にレプリケートされます。この MetroCluster 機能は、リモートクラスタのすべてのパートナー SVM で LDAP クライアント設定をアクティブにするための意図的なものです。

MetroCluster 構成用のネットワーク設定および LIF 作成ガイドライン

MetroCluster 構成で LIF がどのように作成およびレプリケートされるかを理解しておく必要があります。また、ネットワーク設定時に適切に判断できるように、どういった整合性が必要とされるかも把握しておく必要があります。

関連情報

- "ネットワークと LIF の管理"
- パートナークラスタに IPspace オブジェクトをレプリケートするための要件、および MetroCluster 構成でサブネットと IPv6 を設定するための要件を理解しておく必要があります。

  IPspace オブジェクトのレプリケーションとサブネットの設定の要件

- MetroCluster 構成でネットワークを設定するときは、 LIF の作成に関する要件に注意する必要があります。

  MetroCluster 構成での LIF の作成に関する要件

- MetroCluster 構成での LIF のレプリケーションの要件を理解しておく必要があります。また、レプリケートされた LIF がパートナークラスタにどのように配置されるかを把握し、 LIF のレプリケーションまたは LIF の配置に失敗した場合に発生する問題について確認しておく必要があります。

  LIF のレプリケーションおよび配置の要件と問題

IPspace オブジェクトのレプリケーションとサブネットの設定の要件

パートナークラスタに IPspace オブジェクトをレプリケートするための要件、および MetroCluster 構成でサブネットと IPv6 を設定するための要件を理解しておく必要があります。

IPspace レプリケーション

IPspace オブジェクトをパートナークラスタにレプリケートするときは、次のガイドラインを考慮する必要があります。

- 2 つのサイトの IPspace 名が一致している必要があります。
- IPspace オブジェクトは手動でパートナークラスタにレプリケートする必要があります。

  IPspace をレプリケートする前に作成されて IPspace に割り当てられた Storage Virtual Machine （ SVM ）は、パートナークラスタにレプリケートされません。

サブネット構成

MetroCluster 構成でサブネットを設定するときは、次のガイドラインを考慮する必要があります。

- MetroCluster 構成の両方のクラスタのサブネットが同じ IPspace にあり、サブネット名、サブネット、ブロードキャストドメイン、ゲートウェイが同じである必要があります。
- 2 つのクラスタの IP 範囲が同じである必要があります。

  次の例では、 IP 範囲が異なります。

```
cluster_A::> network subnet show

IPspace: Default
Subnet                       Broadcast                    Avail/
Name      Subnet             Domain    Gateway            Total    Ranges
--------- ----------------- --------- ------------      -------
---------------
subnet1   192.168.2.0/24   Default   192.168.2.1       10/10
192.168.2.11-192.168.2.20

cluster_B::> network subnet show
 IPspace: Default
Subnet                       Broadcast                    Avail/
Name      Subnet             Domain    Gateway            Total    Ranges
--------- ----------------- --------- ------------     --------
---------------
subnet1   192.168.2.0/24   Default   192.168.2.1       10/10
192.168.2.21-192.168.2.30
```

IPv6 の設定

一方のサイトで IPv6 が設定されている場合は、もう一方のサイトでも IPv6 を設定する必要があります。

関連情報

- MetroCluster 構成でネットワークを設定するときは、 LIF の作成に関する要件に注意する必要があります。

  MetroCluster 構成での LIF の作成に関する要件

- MetroCluster 構成での LIF のレプリケーションの要件を理解しておく必要があります。また、レプリケートされた LIF がパートナークラスタにどのように配置されるかを把握し、 LIF のレプリケーションまたは LIF の配置に失敗した場合に発生する問題について確認しておく必要があります。

  LIF のレプリケーションおよび配置の要件と問題

MetroCluster 構成での LIF の作成に関する要件

MetroCluster 構成でネットワークを設定するときは、 LIF の作成に関する要件に注意する必要があります。

LIF を作成する際は、次のガイドラインを考慮する必要があります。

- Fibre Channel ：ストレッチ VSAN またはストレッチファブリックを使用する必要があります
- IP / iSCSI ：レイヤ 2 拡張ネットワークを使用する必要があります
- ARP ブロードキャスト： 2 つのクラスタ間で ARP ブロードキャストを有効にする必要があります
- LIF の重複：同じ IPspace に同じ IP アドレスを持つ複数の LIF （重複する LIF ）を作成することはできません

- NFS および SAN 構成：ミラーされていないアグリゲートとミラーされたアグリゲートの両方に、異なる Storage Virtual Machine （ SVM ）を使用する必要があります
- LIFを作成する前にサブネットオブジェクトを作成する必要があります。ONTAPにはブロードキャストドメインが関連付けられているため、サブネットオブジェクトを使用してデスティネーションクラスタのフェイルオーバーターゲットを決定できます。

LIF の作成を確認

MetroCluster 構成内で LIF が正常に作成されたことを確認するには、「 MetroCluster check lif show 」コマンドを実行します。LIF の作成中に問題が発生した場合は、「 MetroCluster check lif repair-placement 」コマンドを使用して問題を修正できます。

関連情報

- パートナークラスタに IPspace オブジェクトをレプリケートするための要件、および MetroCluster 構成でサブネットと IPv6 を設定するための要件を理解しておく必要があります。

  IPspace オブジェクトのレプリケーションとサブネットの設定の要件

- MetroCluster 構成での LIF のレプリケーションの要件を理解しておく必要があります。また、レプリケートされた LIF がパートナークラスタにどのように配置されるかを把握し、 LIF のレプリケーションまたは LIF の配置に失敗した場合に発生する問題について確認しておく必要があります。

  LIF のレプリケーションおよび配置の要件と問題

LIF のレプリケーションおよび配置の要件と問題

MetroCluster 構成での LIF のレプリケーションの要件を理解しておく必要があります。また、レプリケートされた LIF がパートナークラスタにどのように配置されるかを把握し、 LIF のレプリケーションまたは LIF の配置に失敗した場合に発生する問題について確認しておく必要があります。

パートナークラスタへの LIF のレプリケーション

MetroCluster 構成内の 1 つのクラスタに LIF を作成すると、その LIF はパートナークラスタにレプリケートされます。LIF は名前に基づいて 1 対 1 で配置されるわけではありません。スイッチオーバー処理後に LIF を使用できるようにするため、 LIF の配置プロセスは、ポートが LIF をホストできるかどうかを到達可能性とポート属性チェックに基づいて検証します。

LIF をレプリケートしてパートナークラスタに配置するには、システムが次の条件を満たしている必要があります。

条件	LIF タイプ： FC	LIF タイプ： IP / iSCSI
ノードの識別	ONTAP は、 LIF を作成したノードのディザスタリカバリ（ DR ）パートナーに、レプリケートされた LIF を配置します。DR パートナーが使用できない場合は、 DR 補助パートナーが配置に使用されます。	ONTAP は、 LIF を作成したノードの DR パートナーに、レプリケートされた LIF を配置します。DR パートナーが使用できない場合は、 DR 補助パートナーが配置に使用されます。

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 のポートがない場合は LIF を配置できません。 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。 DR サイトに同じファブリックがない場合、 LIF は DR パートナーの任意のポートに配置されます。	上記で特定された DR クラスタの各ポートから配置する LIF のソース IP アドレスに Address Resolution Protocol （ ARP ）ブロードキャストが送信され、その応答に基づいて到達可能性が判別されます。 到達可能性チェックが成功するためには、 2 つのクラスタ間で ARP ブロードキャストが許可されている必要があります。 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 では、アダプタタイプや速度などの属性に基づいてポートが分類され、属性が一致するポートが選択されます。 属性が一致するポートがない場合、 LIF は DR パートナーの任意の接続されたポートに配置されます。	到達可能性チェックで到達可能とマークされたポートのうち、 ONTAP が優先して LIF のサブネットに関連付けられたブロードキャストドメイン内のポートを選択します。 DR クラスタに LIF のサブネットに関連付けられたブロードキャストドメイン内の使用可能なネットワークポートがない場合は、ソース LIF に到達可能なポートが ONTAP によって選択されます。 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は移動されません。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。

スイッチオーバー後は **LIF** にアクセスできなくなります

ソースノードと DR ノードの FC ターゲットポートが接続されている FC スイッチファブリックに何らかの変更を加えると、スイッチオーバー処理のあとに、 DR パートナーに配置された FC LIF にホストからアクセスできなくなることがあります。

MetroCluster のホスト接続を確認するには、 FC スイッチファブリックに変更を加えたあとに、ソースノードと DR ノードで「 lif check life-placement 」コマンドを実行する必要があります。スイッチファブリックの変更内容によっては、 DR パートナーノードの別のターゲット FC ポートに LIF が配置されることがあります。

関連情報

- パートナークラスタに IPspace オブジェクトをレプリケートするための要件、および MetroCluster 構成でサブネットと IPv6 を設定するための要件を理解しておく必要があります。

  IPspace オブジェクトのレプリケーションとサブネットの設定の要件

- MetroCluster 構成でネットワークを設定するときは、 LIF の作成に関する要件に注意する必要があります。

  MetroCluster 構成での LIF の作成に関する要件

ルートアグリゲートでのボリューム作成

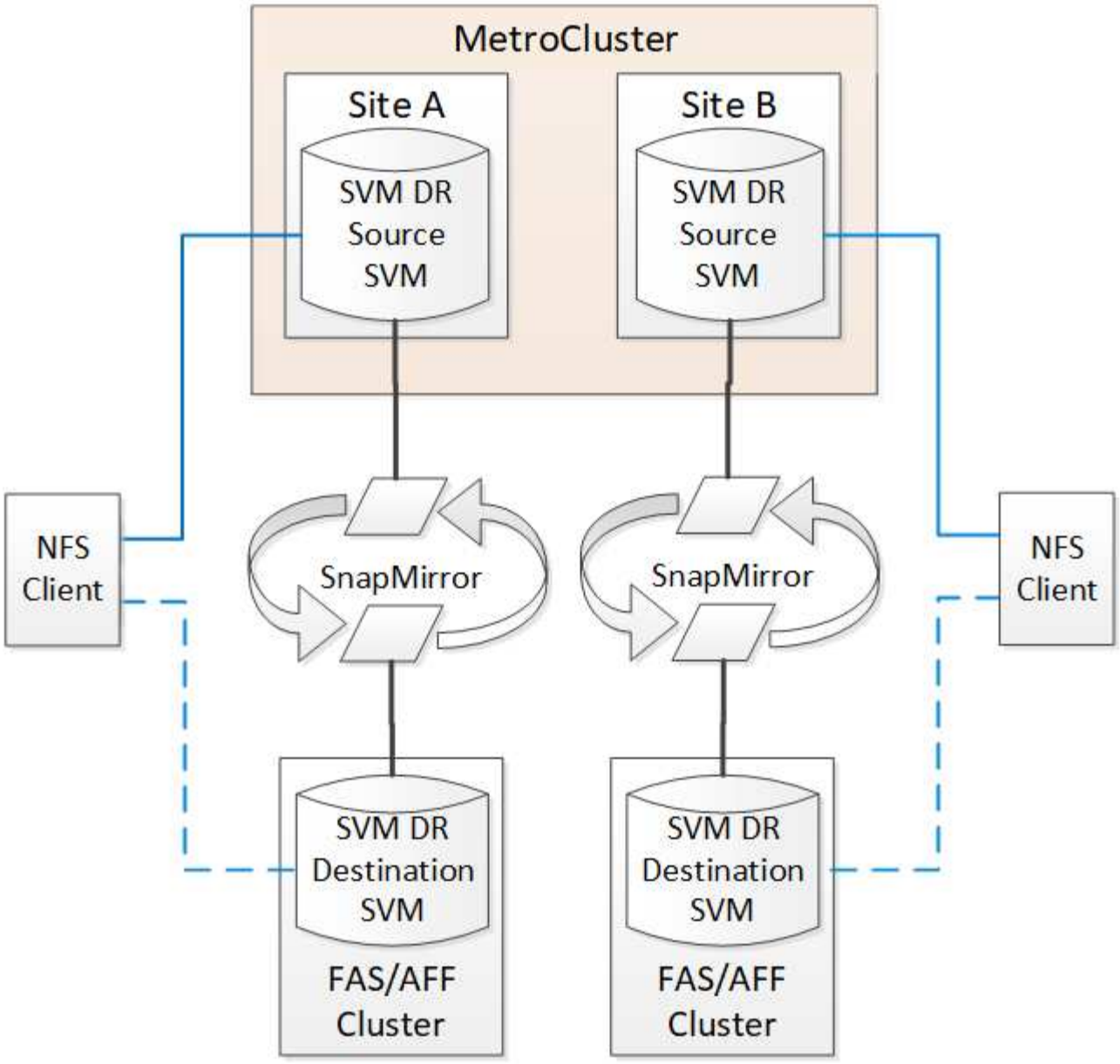
MetroCluster 構成内のノードのルートアグリゲート（ HA ポリシーが CFO ）に新しいボリュームを作成することはできません。

この制限があるため、ルートアグリゲートを vserver add-aggregates コマンドで SVM に追加することはできません。

MetroCluster 構成の SVM ディザスタリカバリ

ONTAP 9.5 以降では、 MetroCluster 構成のアクティブな Storage Virtual Machine （ SVM ）を SnapMirror SVM ディザスタリカバリ機能でソースとして使用できます。デスティネーション SVM は、 MetroCluster 構成外の第 3 のクラスタに配置する必要があります。

ONTAP 9.11.1以降では、次の図に示すように、MetroCluster 構成内の両方のサイトを、FAS またはAFF デスティネーションクラスタを使用したSVM DR関係のソースにすることができます。



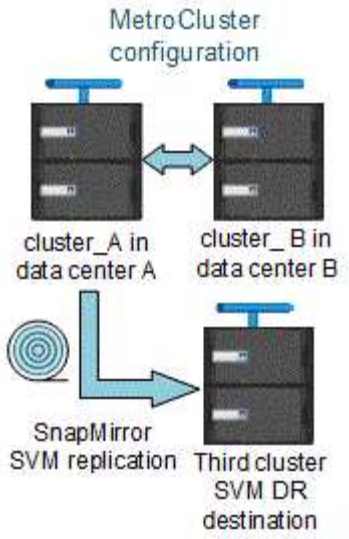
SVM を SnapMirror ディザスタリカバリで使用する場合は、次の要件と制限事項に注意してください。

- SVM ディザスタリカバリ関係のソースとして使用できるのは、 MetroCluster 構成内のアクティブな SVM だけです。

  スイッチオーバー前の同期元の SVM とスイッチオーバー後の同期先の SVM のどちらもソースに使用できます。

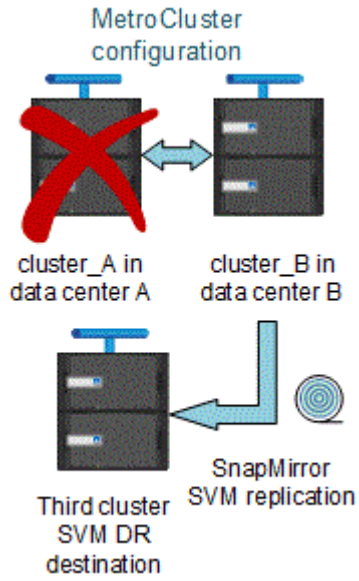
- MetroCluster 構成が安定した状態のときは MetroCluster の同期先の SVM はオンラインでないため、同期先ボリュームを SVM ディザスタリカバリ関係のソースにすることはできません。

  次の図は、安定した状態における SVM ディザスタリカバリの動作を示しています。



- SVM DR 関係のソースが同期元の SVM の場合、ソースの SVM DR 関係情報が MetroCluster パートナーにレプリケートされます。

  これにより、次の図に示すように、スイッチオーバー後も SVM DR の更新を続行できます。



- スイッチオーバーおよびスイッチバックの実行中に、 SVM DR のデスティネーションへのレプリケーションが失敗することがあります。

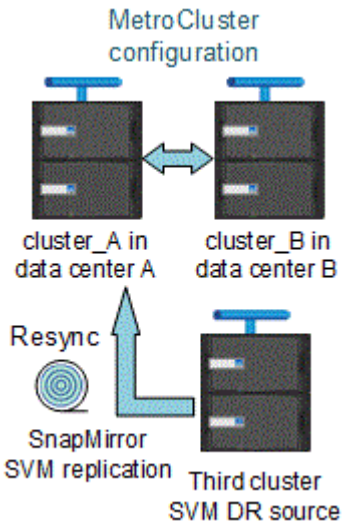
  ただし、スイッチオーバーまたはスイッチバックプロセスの完了後、 SVM DR の次回のスケジュールされている更新は成功します。

の「 SVM の設定のレプリケート」セクションを参照してください "CLI によるデータ保護" SVM DR 関係の設定の詳細については、を参照してください。

ディザスタリカバリサイトでの **SVM** の再同期

再同期では、 MetroCluster 構成の Storage Virtual Machine （ SVM ）ディザスタリカバリ（ DR ）ソースが MetroCluster でないサイトのデスティネーション SVM からリストアされます。

再同期中は、次の図に示すように、ソース SVM （ cluster_A ）が一時的にデスティネーション SVM として機能します。



再同期中に計画外スイッチオーバーが発生した場合

再同期中に計画外スイッチオーバーが発生すると、再同期の転送が停止します。計画外スイッチオーバーが発生した場合は次のようになります。

- MetroCluster サイトのデスティネーション SVM （再同期前のソース SVM ）は、デスティネーション SVM のままです。パートナークラスタの SVM は、同じサブタイプで非アクティブのままです。
- 同期先の SVM をデスティネーションとする SnapMirror 関係を手動で再作成する必要があります。
- スイッチオーバー後、 SnapMirror 作成処理を実行しないかぎり、サバイバーサイトでの SnapMirror show の出力に SnapMirror 関係は表示されません。

再同期中に計画外スイッチオーバーが発生した場合は、スイッチバックを実行

スイッチバックプロセスを正常に実行するには、再同期関係を解除して削除する必要があります。MetroCluster 構成に SnapMirror DR のデスティネーション SVM がある場合、またはクラスタにサブタイプ「 `d p-destination` 」の SVM がある場合、スイッチバックは実行できません。

MetroCluster スイッチオーバー後に storage aggregate plex show コマンドの出力が確定しない

MetroCluster のスイッチオーバー後に「 storage aggregate plex show 」コマンドを実行すると、スイッチオーバーされたルートアグリゲートの plex0 のステータスが確定していないため、「 failed 」と表示されます。この間、スイッチオーバーされたルートは更新されません。このプレックスの実際のステータスは、MetroCluster 修復フェーズ後に確定します。

スイッチオーバー発生時に NVFAIL フラグを設定するためのボリュームの変更

MetroCluster スイッチオーバーが発生した場合に NVFAIL フラグが設定されるようにボリュームを変更することができます。NVFAIL フラグが設定されたボリュームは、一切変更されなくなります。コミットされた書き込みがスイッチオーバー後に失われたと想定してボリュームを処理する必要がある場合は、この変更が必要となります。

このタスクについて

9.0 よりも前のバージョンの ONTAP では、スイッチオーバーのたびに NVFAIL フラグが設定されます。ONTAP 9.0 以降のバージョンでは、計画外スイッチオーバー（ USO ）が使用されます。

ステップ

1. スイッチオーバー時に MetroCluster 構成で NVFAIL をトリガーするには、「 vol-dr-force-nvfail 」パラメータを「 on 」に設定します。

```
*vol modify -vserver_name_-volume -name_-dr-force-nvfail on *
```

追加情報の参照先

MetroCluster の設定と処理の詳細については、を参照してください。

MetroCluster およびその他の情報

情報	件名
"ONTAP 9 のドキュメント"	• すべての MetroCluster 情報
"NetApp MetroCluster 解決策のアーキテクチャと設計、 TR-4705"	• MetroCluster FC の構成と運用の技術概要 • MetroCluster FC 構成のベストプラクティス
"MetroCluster IP 解決策のアーキテクチャおよび設計、 TR-4689"	• MetroCluster IP の構成と運用の技術概要 • MetroCluster IP 構成のベスト プラクティス。
"ストレッチ MetroCluster のインストールと設定"	• ストレッチ MetroCluster アーキテクチャ • 構成のケーブル接続 • FC-to-SAS ブリッジの設定 • ONTAP で MetroCluster を設定します
"MetroCluster IP のインストールと設定： ONTAP MetroCluster 構成の違い"	• MetroCluster IP アーキテクチャ • 構成のケーブル接続 • ONTAP で MetroCluster を設定します
"MetroCluster の管理とディザスタリカバリ"	• MetroCluster 構成について • スイッチオーバー、修復、スイッチバック • ディザスタリカバリ

"MetroCluster のコンポーネントをメンテナンスします"	• MetroCluster FC 構成のメンテナンスガイドライン • 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 • ファブリック接続またはストレッチ MetroCluster FC 構成でのディスクシェルフのホットアド • ファブリック接続またはストレッチ MetroCluster FC 構成でのディスクシェルフのホットリムーブ • ファブリック接続またはストレッチ MetroCluster FC 構成のディザスタサイトでのハードウェア交換 • 2 ノードのファブリック接続またはストレッチ MetroCluster FC 構成の 4 ノード MetroCluster 構成への拡張 • 4 ノードのファブリック接続またはストレッチ MetroCluster FC 構成の 8 ノード MetroCluster FC 構成への拡張
"MetroCluster FC から MetroCluster IP に移行します" "MetroCluster アップグレードおよび拡張ガイド"	• MetroCluster 設定をアップグレードまたは更新する • MetroCluster FC 構成から MetroCluster IP 構成への移行 • ノードの追加による MetroCluster 構成の拡張
"MetroCluster Tiebreaker ソフトウェアのインストールおよび設定"	• MetroCluster Tiebreaker ソフトウェアを使用して MetroCluster 構成を監視する
Active IQ デジタルアドバイザのドキュメント "ネットアップのマニュアル：製品ガイドとリソース"	• MetroCluster の設定とパフォーマンスを監視する
"コピーベースの移行"	• 7-Mode ストレージシステムから clustered Data ONTAP ストレージシステムへデータを移行する
"ONTAP の概念"	• ミラーされたアグリゲートの機能

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 [1]	4 台または 8 台	2 つ	2 つ	2 つ
FC スイッチストレージファブリックを使用します	いいえ	はい。	はい。	いいえ	いいえ
IP スイッチストレージファブリックを使用します	はい。	いいえ	いいえ	いいえ	いいえ
FC-to-SAS ブリッジを使用します	いいえ	はい。	はい。	はい。	いいえ

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

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

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

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

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

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。

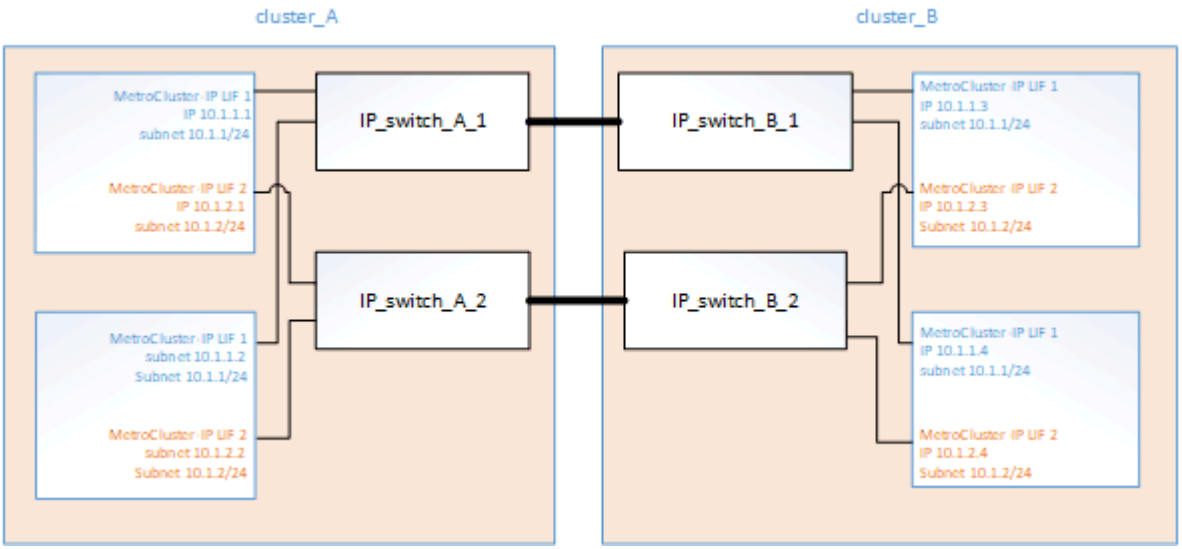
これは、 MetroCluster FC 構成とは異なります。 FC ファブリックまたは SAS 接続を介してリモートストレージプールがローカルコントローラに接続されます。ローカルコントローラはリモートコントローラが停止し

て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 configurion-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ト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取り付けます。

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ト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。	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。 • データ用パーティション × 8 • パリティパーティション × 2 • スペアパーティションが 2 つ必要です
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。	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。 • データ用パーティション × 3 • パリティパーティション × 2 • スペアパーティション × 1

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

推奨される最小ドライブ数（サイトあたり）	内蔵ドライブのみ	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。 *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。	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。 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。 • データ用パーティション × 3 • パリティパーティション × 2 • スペアパーティション × 1

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。 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。 • 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。 • 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。 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。 • Q1 ： node_A_1 のプール 0 • Q2 ： node_A_1 のプール 0 • Q3 ： node_B_1 のプール 1 • Q4 ： node_B_2 のプール 1 *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。	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。 • データ用パーティション×2 • パリティパーティション × 2 • スペアなし

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プレックスには、次のパーティションが含まれます。 • データ用パーティション × 8 • パリティパーティション × 2 • スペアパーティションが 2 つ必要です
	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 つのプレックスのそれぞれに、次のものが含まれます。 • データ用パーティション × 8 • パリティパーティション × 2 • スペアパーティションが 2 つ必要です
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。 • データ用パーティション×2 • パリティパーティション × 2 • スペアパーティションがありません

AFF A50および**AFF C60**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。	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。 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。 • データ用パーティション × 8 • パリティパーティション × 2 • スペアパーティションが 2 つ必要です
	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 つのプレックスのそれぞれに、次のものが含まれます。 • データ用パーティション × 8 • パリティパーティション × 2 • スペアパーティションが 2 つ必要です
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。	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。 • データ用パーティション×2 • パリティパーティション × 2 • スペアパーティションがありません

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。	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プレックスには、次のパーティションが含まれます。 • データ用パーティション × 8 • パリティパーティション × 2 • スペアパーティションが 2 つ必要です
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。	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。 • データ用パーティション × 3 • パリティパーティション × 2 • スペアパーティション × 1

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。	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。 • データ用のパーティション × 20 • パリティパーティション × 2 • スペアパーティションが 2 つ必要です
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。	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。 • データ用パーティション × 3 • パリティパーティション × 2 • スペアパーティション × 1

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。	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。 • データ用のパーティション × 20 • パリティパーティション × 2 • スペアパーティションが 2 つ必要です

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。	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。 • データ用パーティション × 3 • パリティパーティション × 2 • スペアパーティション × 1

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。	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。 • データ用パーティション × 8 • パリティパーティション × 2 • スペアパーティションが 2 つ必要です *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。

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。	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。 • データ用パーティション × 3 • パリティパーティション × 2 • スペアパーティション × 1 *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。

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。	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。 • データ用パーティション × 8 • パリティパーティション × 2 • スペアパーティションが 2 つ必要です
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。	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。 • データ用パーティション × 3 • パリティパーティション × 2 • スペアパーティション × 1

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。	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。 • データ用のパーティション × 20 • パリティパーティション × 2 • スペアパーティションが 2 つ必要です
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。	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。 • データ用パーティション × 3 • パリティパーティション × 2 • スペアパーティション × 1

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す。	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

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。	該当なし
	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)	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。 注記: • 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。 • 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。	該当なし

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す。

専用のポートを使用する場合の考慮事項

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

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

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

  ポートの帯域幅は、すべての VLAN とベースポートで共有されます。

- データの変更率とレプリケーション間隔について検討し、間隔ごとにレプリケートする必要があるデータ

の量に十分な帯域幅が必要かどうかを検討します。データポートを共有すると、原因がデータプロトコルと競合する可能性があります。

データポートを共有する場合の考慮事項

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

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

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

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

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

ISL 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。このようなリ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、ポートをブレー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**数とブレー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 スイッチのモデル	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	ブレークアウトケーブル	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	ブレークアウトケーブル	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）	ブレークアウトケーブル	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）	ブレークアウトケーブル（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	ブレークアウトケーブル（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ー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ー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。

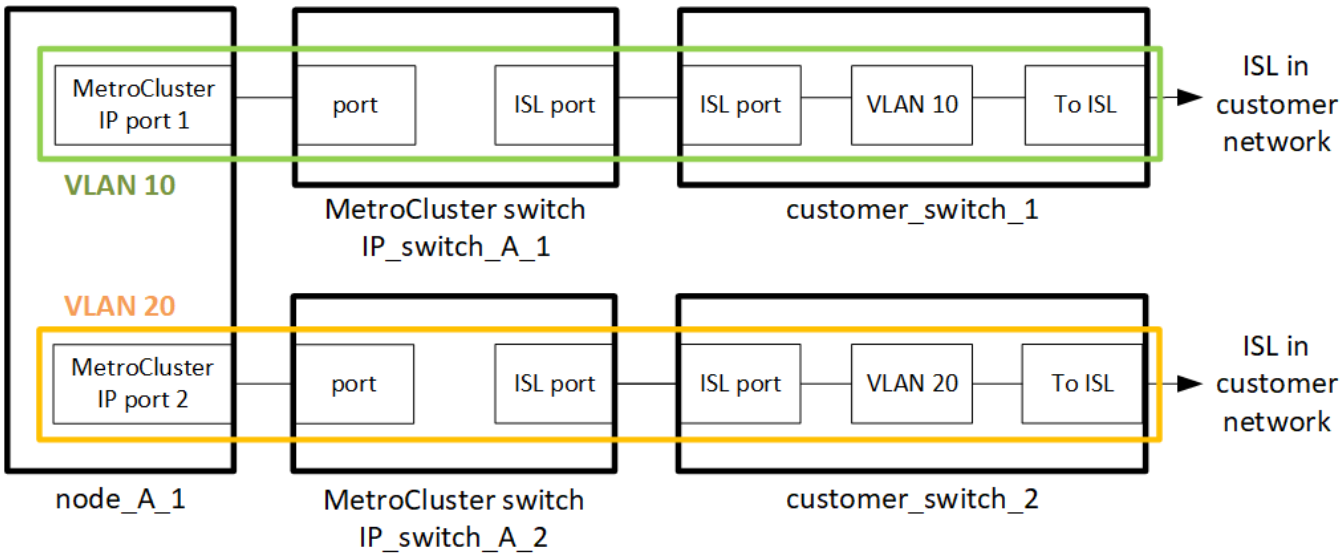
  マルチプロトコルラベルスイッチング（ MPLS ）リンクなどのリンク共有サービスはサポートされません。

- 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

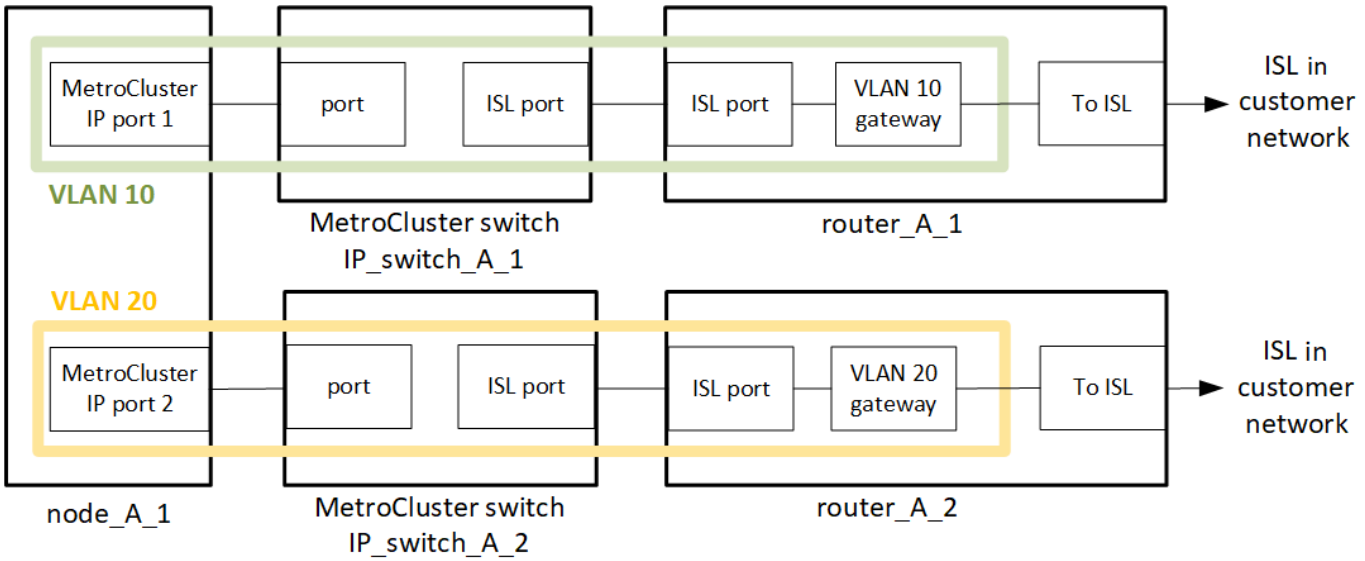
> 上記のシステムは、VLAN 100以下を使用して設定できます。ただし、この範囲の一部のVLANは、他の用途や将来の用途に予約されている可能性があります。

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、介在するスイッチの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。

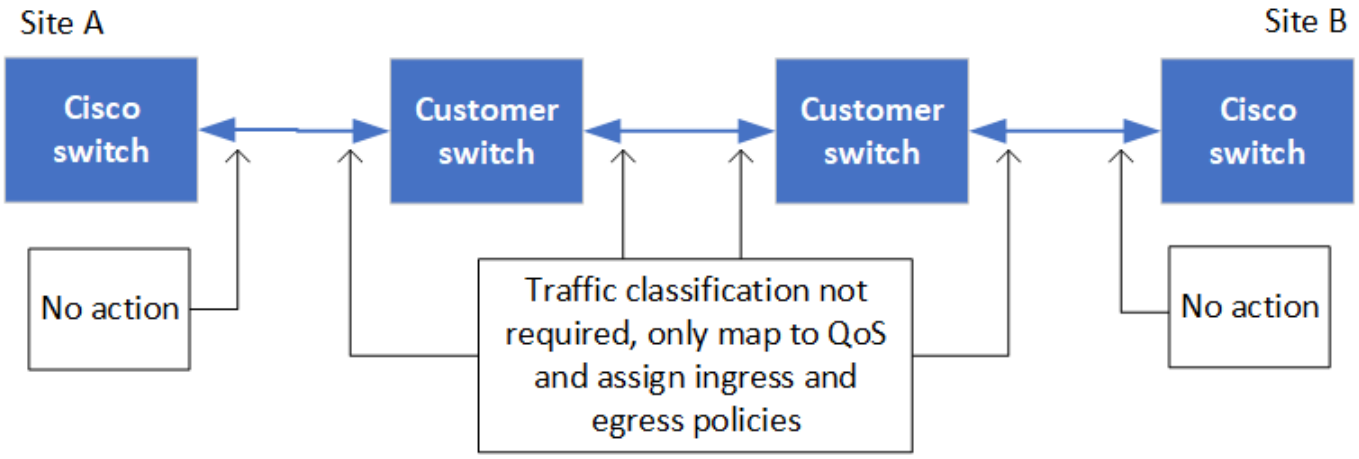
ルータおよびゲートウェイのIPアドレスを設定する場合は、次の要件を満たす必要があります。

- 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。

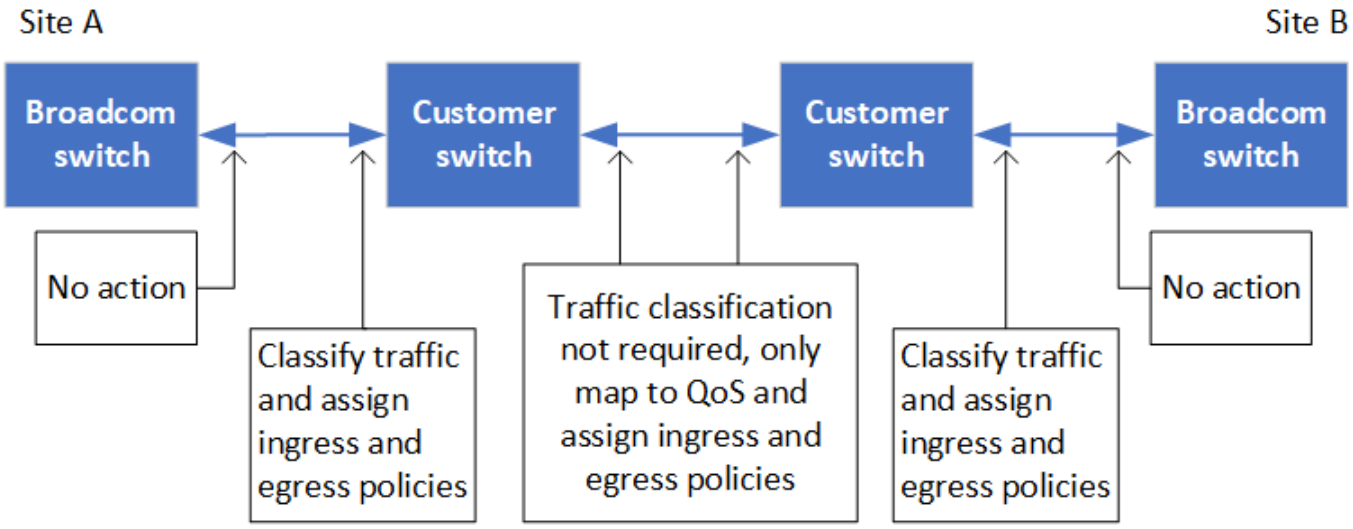
中間スイッチに必要な設定

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の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。

- A `MetroClusterIP_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

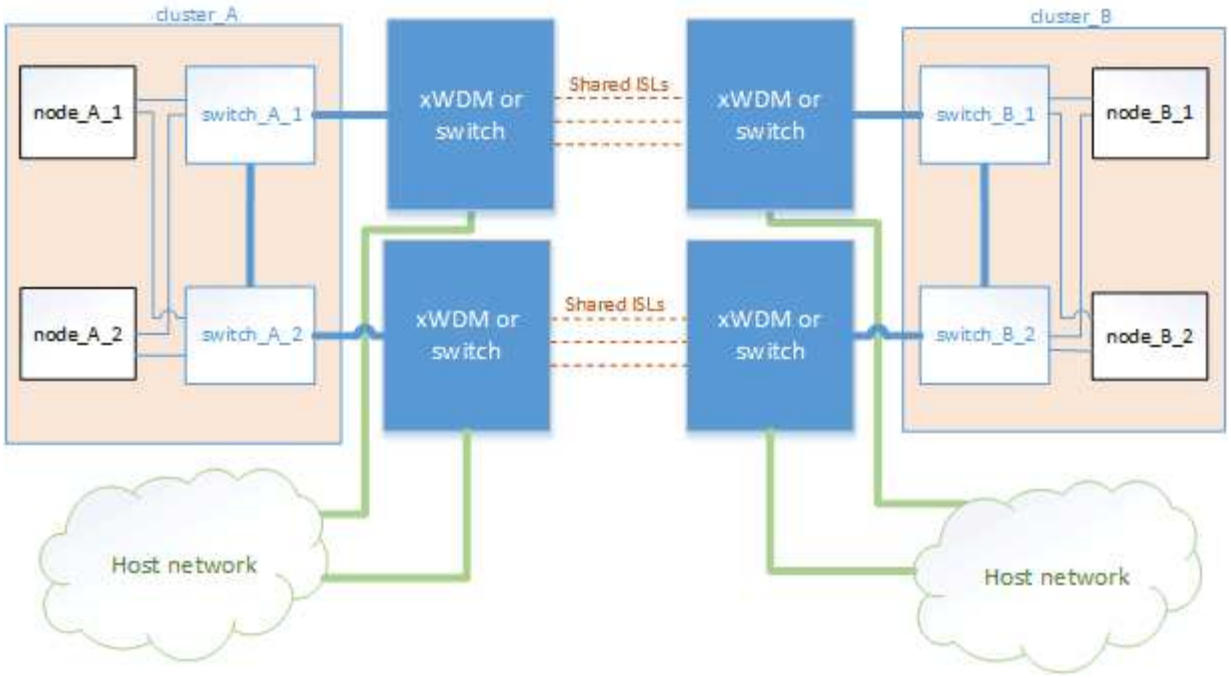
ONTAP 9.6以降では、MetroCluster IP構成で追加のネットワーク設定がサポートされます。ここでは、サポートされるネットワーク構成の例をいくつか示します。サポートされているトポロジの一部がリストされていません。

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。

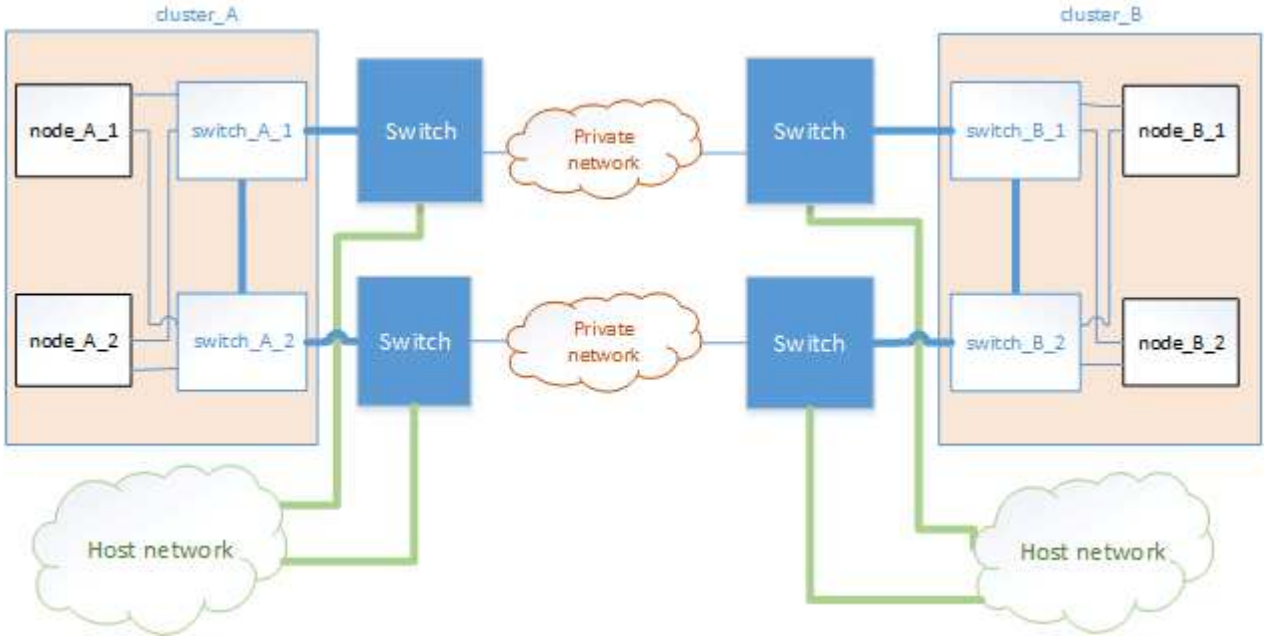
直接リンクを使用した共有ネットワーク構成

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

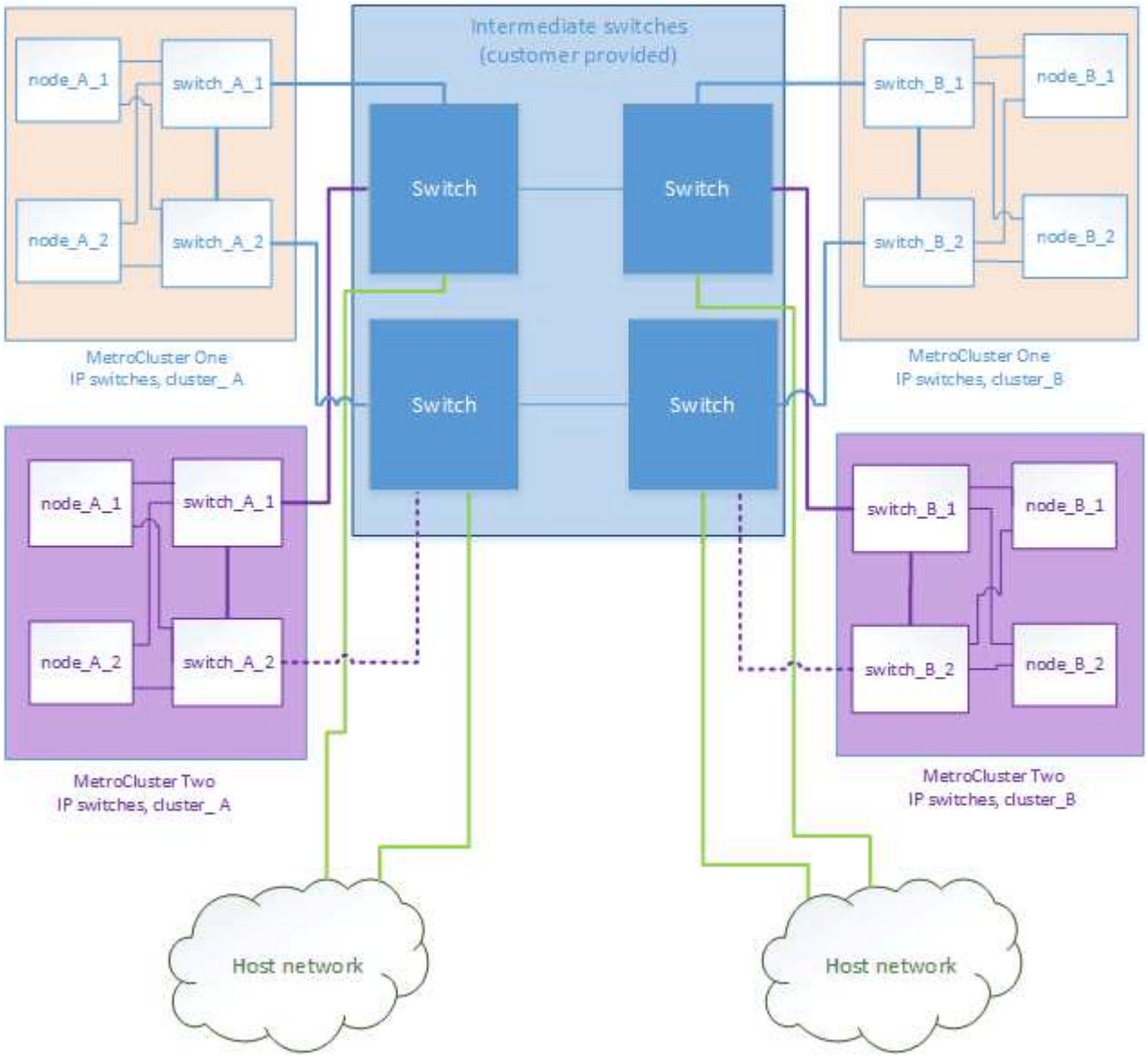
このトポロジでは、MetroClusterサイトは直接接続されませんが、MetroClusterとホストトラフィックはネットワークを経由します。
ネットワークは一連のxWDMおよびTDMとスイッチで構成できますが、直接ISLを使用した共有構成とは異なり、サイト間のリンクは直接接続ではありません。サイト間のインフラによっては、ネットワーク構成を任意に組み合わせて設定できます。



複数の**MetroCluster**構成で中間ネットワークを共有

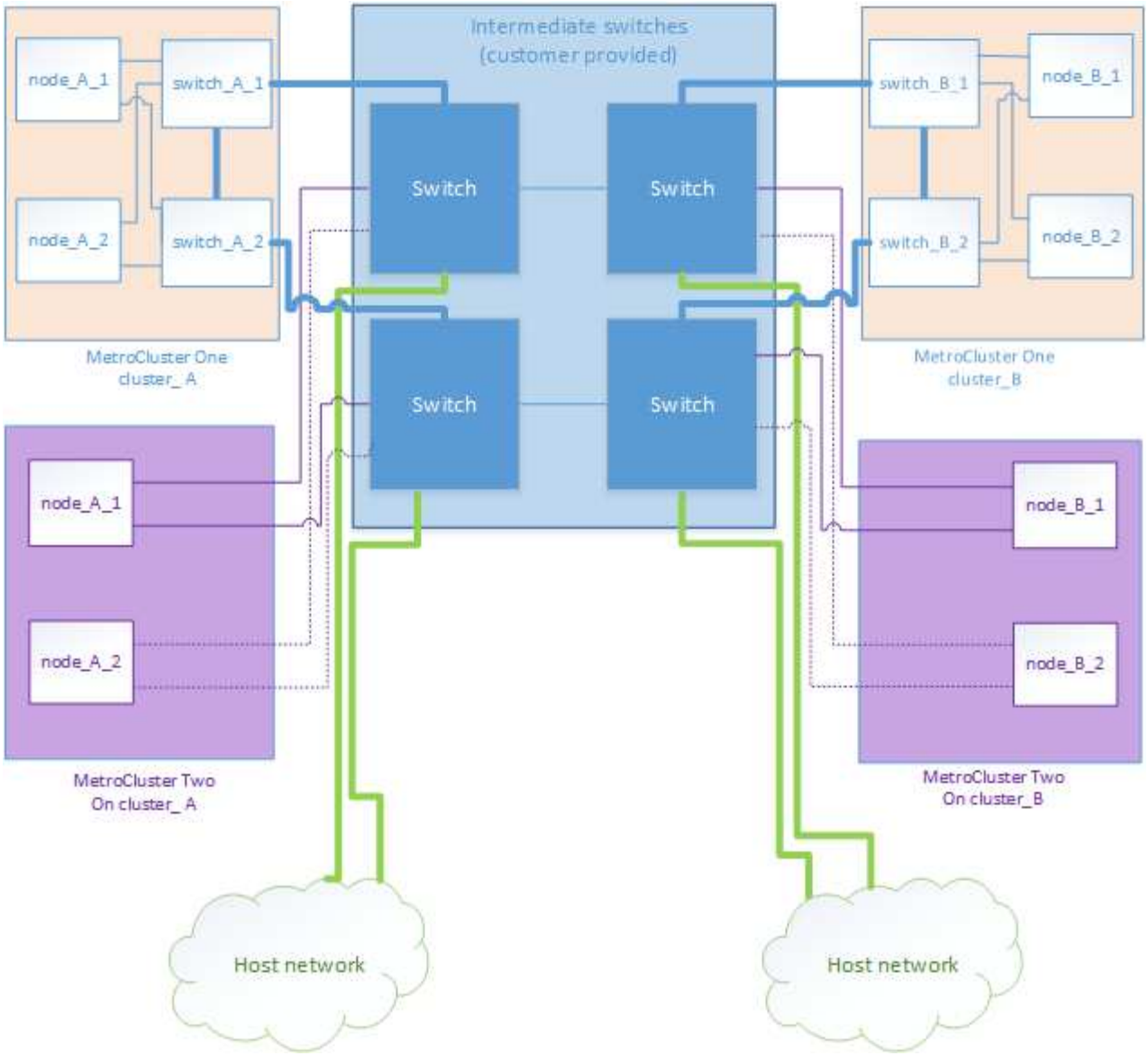
このトポロジでは、 2 つの異なる MetroCluster 構成が同じ中間ネットワークを共有しています。この例では、MetroCluster 1のswitch_A_1とMetroCluster 2のswitch_A_1が同じ中間スイッチに接続されています。

「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タ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以前へのリバ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
```

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ー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ブレー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に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のみ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。

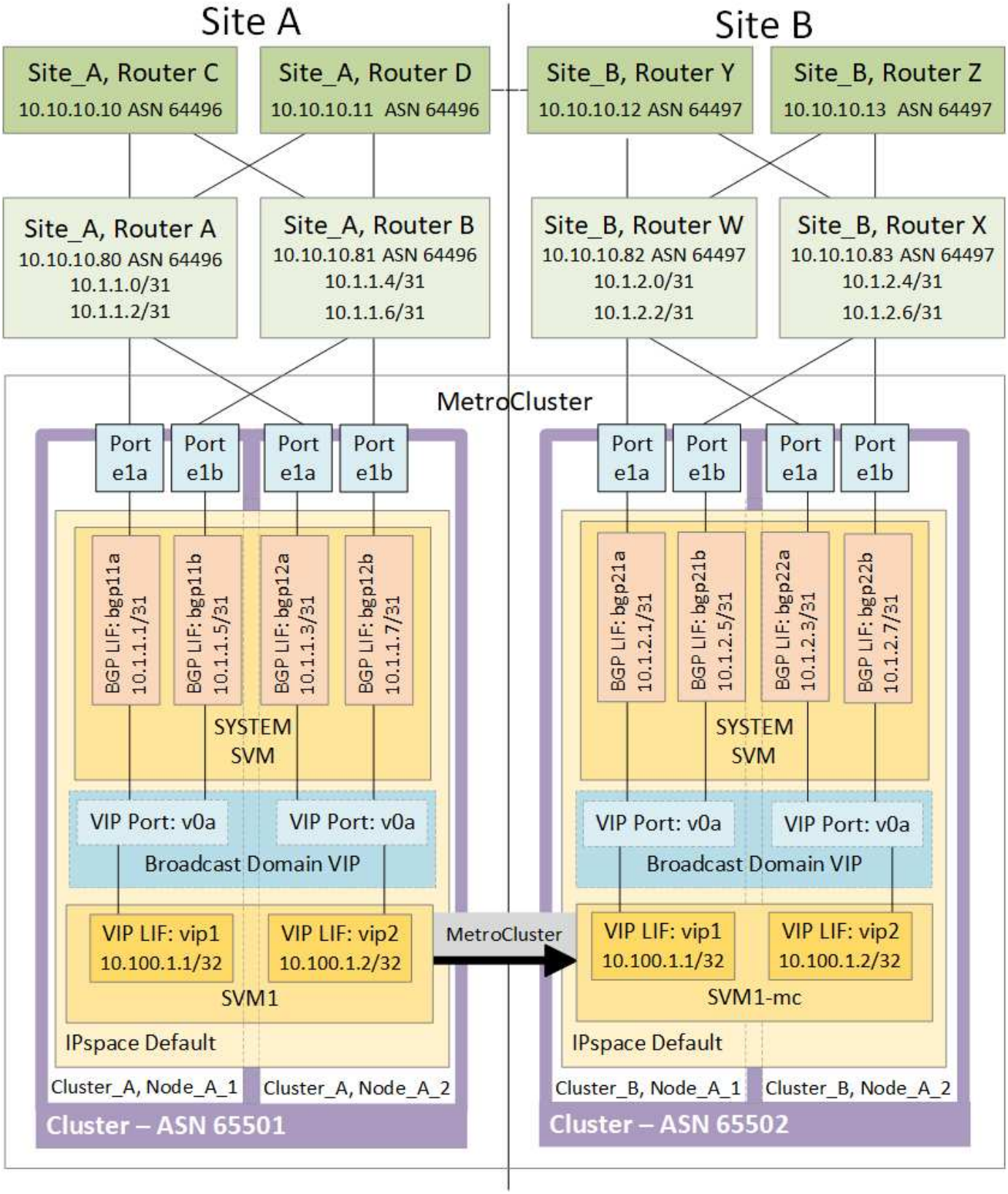
トラフィックタイプ	ポート / サービス
クラスタピアリング	11104/TCP 11105/TCP
ONTAP システムマネージャ	443 / TCP
MetroCluster IP のクラスタ間 LIF	65200/TCP 10006/TCP および UDP
ハードウェアアシスト	4444/TCP

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は検証されません。

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 ）およびルートリフレクタの使用は不可能ではありませんが、簡単な VIP 設定の範囲外です。

導入後、関連する仮想 LIF が各サイトのすべてのノード間で移行されたときに（ MetroCluster スイッチオーバーを含む）データ SVM にアクセスできることを確認し、同じデータ SVM への静的ルートの正しい設定を確認する必要があります。

VIP は、ほとんどの IP ベースのプロトコル（ NFS 、 SMB 、 iSCSI ）に対応しています。

MetroCluster 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。

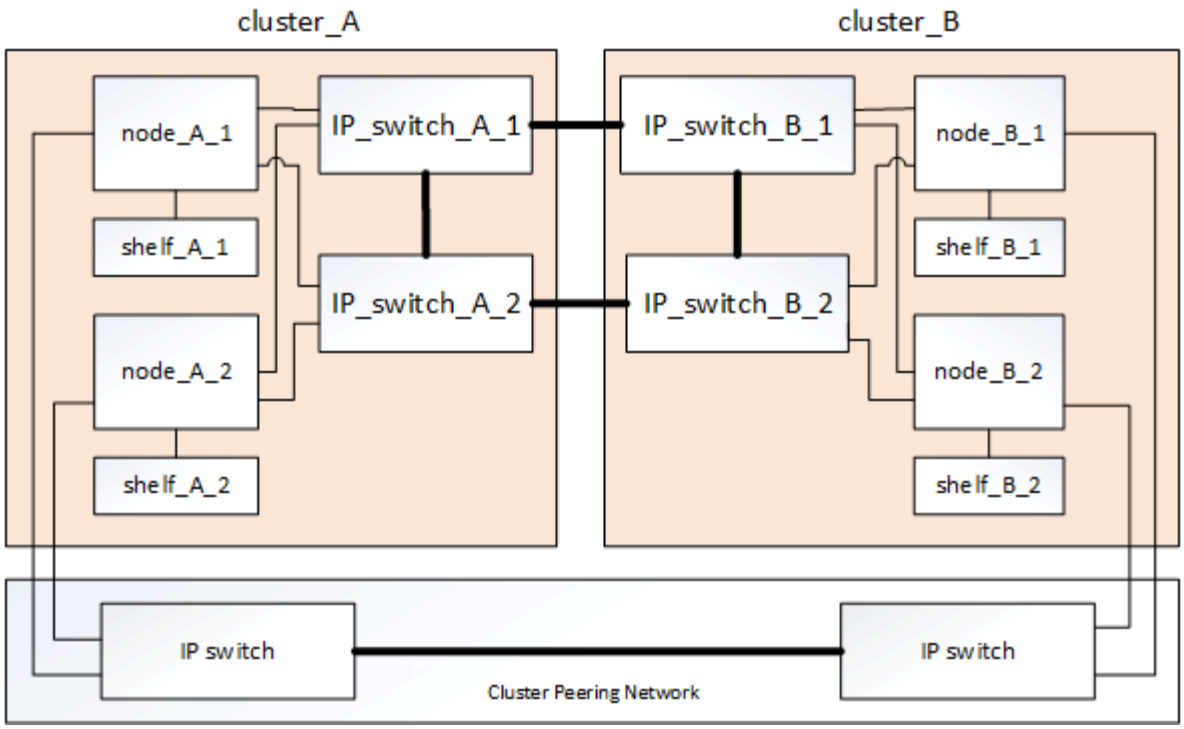
  - クラスタ内通信用の標準クラスタ接続。

    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

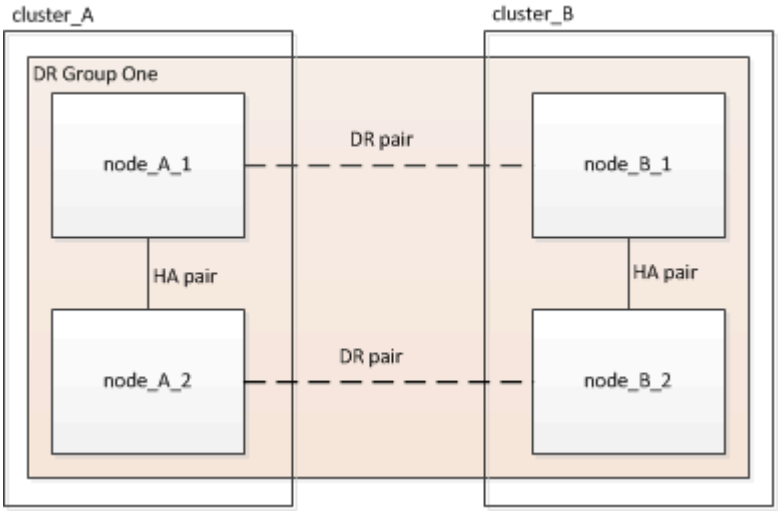
  クラスタピアリングネットワークは、 Storage Virtual Machine （ SVM ）の設定を含むクラスタ構成をミラーするための接続を提供します。一方のクラスタのすべての SVM の設定が、パートナークラスタにミラーされます。



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。

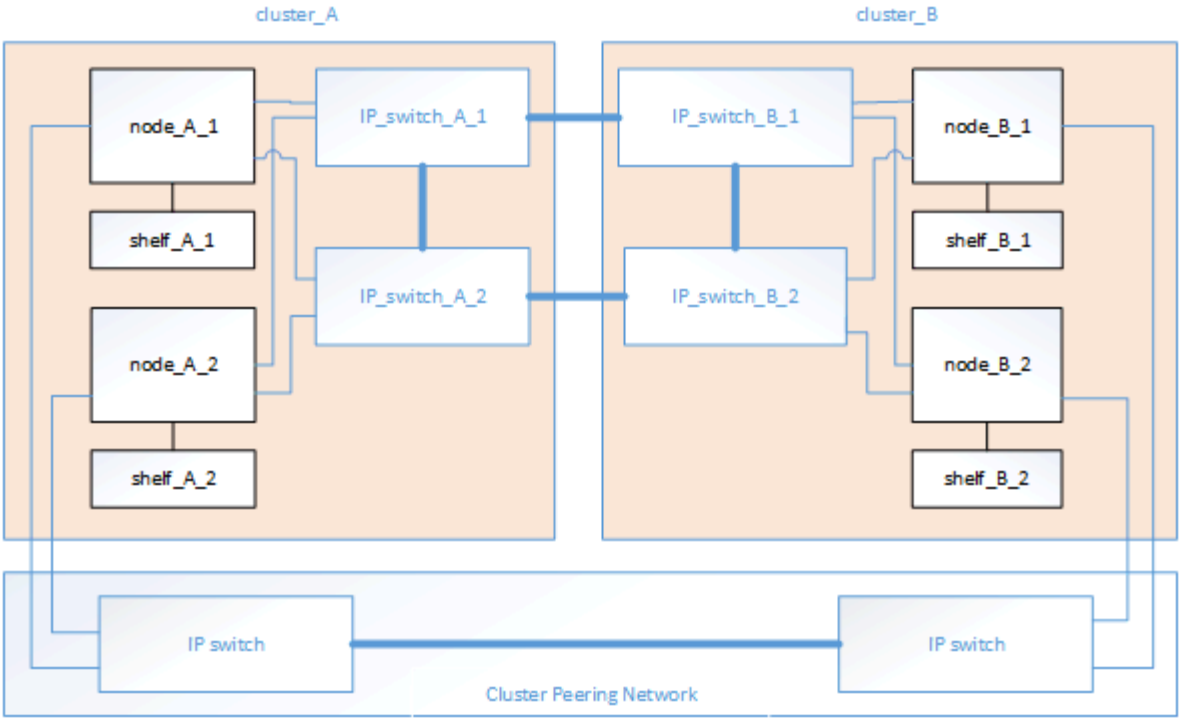
次の図は、 4 ノード MetroCluster 構成におけるノードの編成を示しています。



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。

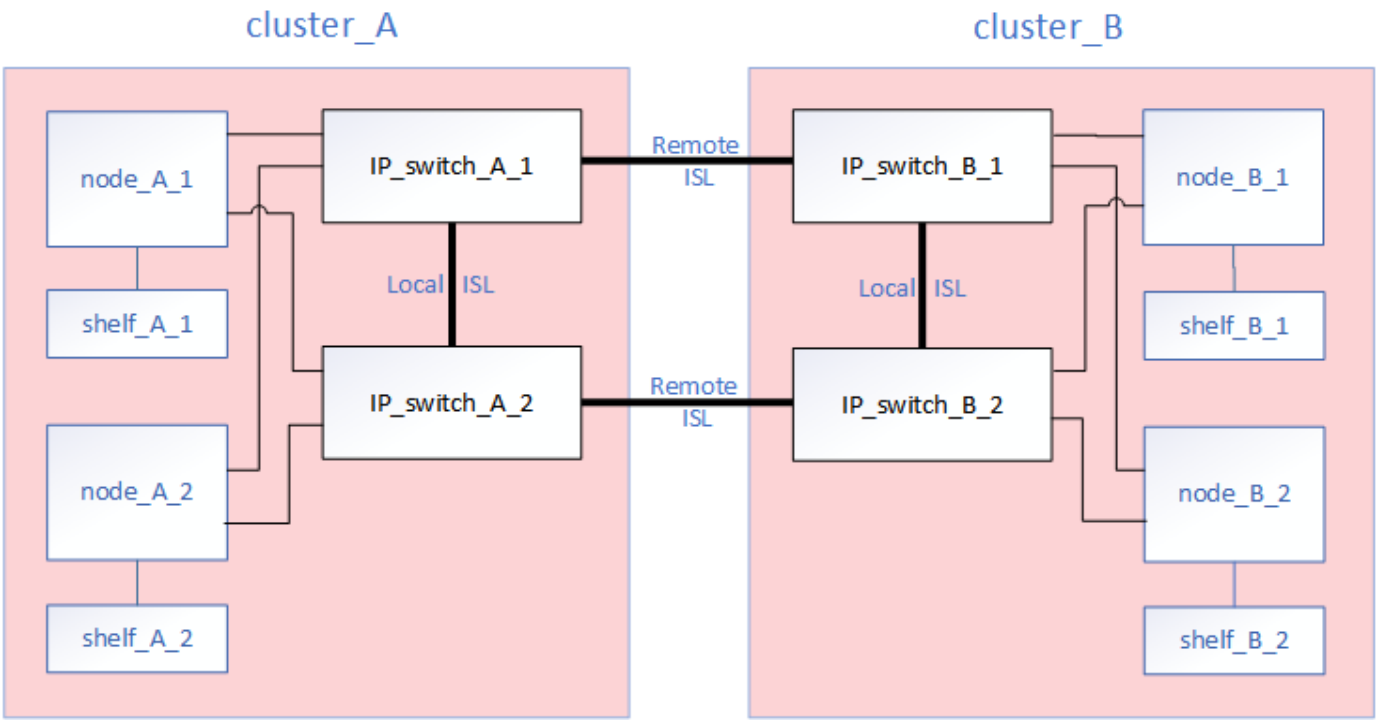


関連情報

"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

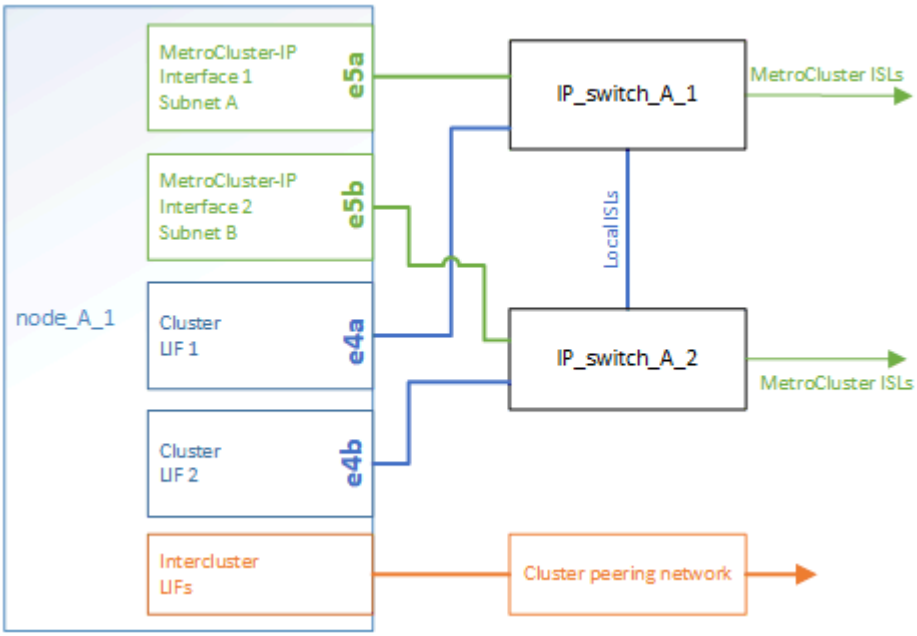
ONTAP クラスタには、通常、クラスタ内のノード間のトラフィック用にクラスタインターコネクトネットワークが含まれています。MetroCluster IP 構成では、 MetroCluster サイト間のデータレプリケーショントラフィックにもこのネットワークが使用されます。



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。



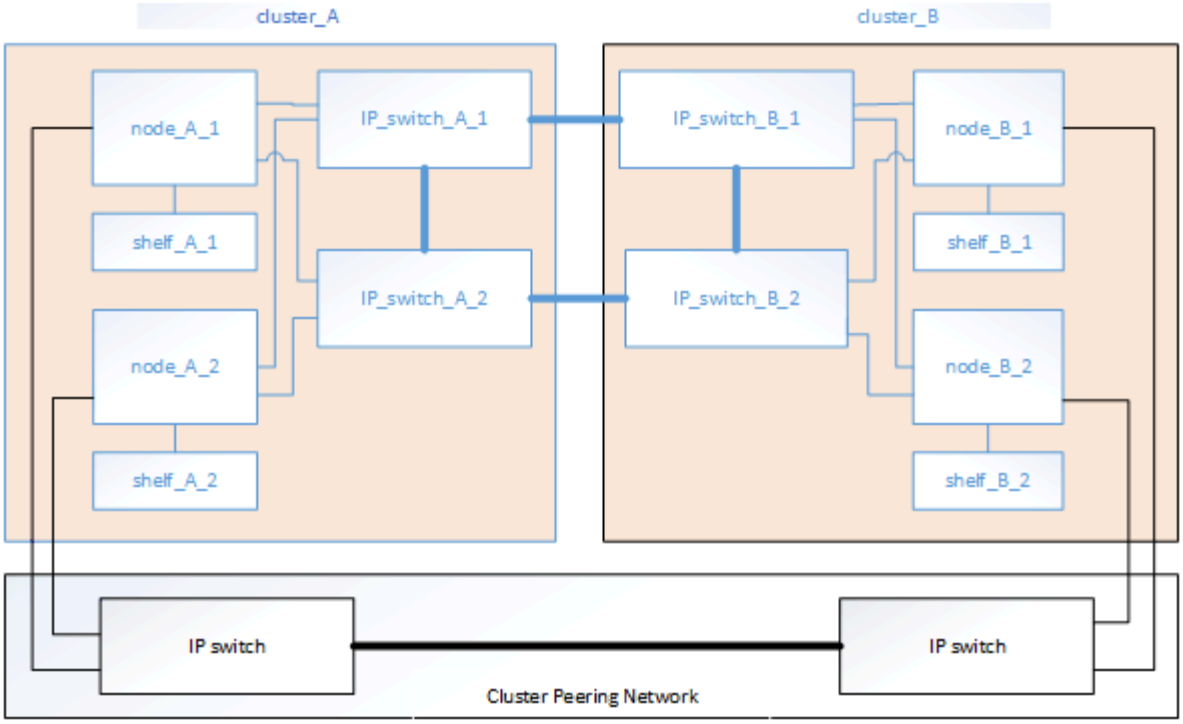
関連情報

"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 、ASA A800、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、 ASA A400、 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、 ASA A150、 AFF A220	オンボードポート	該当なし	e0a 、 e0b
FAS500f、 AFF A250、 ASA A250、 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 x 1 本

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

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

   - 各ディスクシェルフの電源を再投入する必要があります。
   - 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 スイッチ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ブレー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。 • 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） • 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）
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、ASA A800 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、ASA A150、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	ISL, MetroCluster		ISL, MetroCluster	
16					
17					
18					
19					
20					
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster	
22/1-4					
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を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。

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		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	
29/1	MetroCluster 4, 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を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。

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	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	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	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster		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	MetroCluster 3, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
14									
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster		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		ISL, MetroCluster	
22/1-4									
23/1-4									
24/1-4									
25	MetroCluster 4, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
26									
27 - 28	Unused	disabled		disabled		disabled		disabled	
29	MetroCluster 4, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
30									
31 - 32	Unused	disabled		disabled		disabled		disabled	
33 - 36	Unused (Cisco 9336C-FX2 only)	disabled		disabled		disabled		disabled	

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、ASA A150 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。 • 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) • 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)
FAS8300、AFF C400 、ASA C400、FAS8700 AFF A400、ASA A400	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、ASA A800 FAS9500、AFF A900 、ASA A900	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、ASA A150、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 ASA A400 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、ASA A800、FAS9500、AFF A900、または ASA A900 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 2	MetroCluster 1, Local Cluster interface	e0a	e1a	e4a	e4b(e) / e8a (note 2)
3 4	MetroCluster 2, Local Cluster interface	e0a	e1a	e4a	e4b(e) / e8a (note 2)
5-6	Ports disallowed to use	blocked		blocked	
7 8	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster	
9 10	MetroCluster 1, MetroCluster interface	e0b	e1b	e5b	e7b
11 12	MetroCluster 2, MetroCluster interface	e0b	e1b	e5b	e7b
13-18	Ports disallowed to use	blocked		blocked	
19 20	ISL, MetroCluster native speed 40G / 100G (note 1)	ISL, MetroCluster		ISL, MetroCluster	
21/1-4 22/1-4	ISL, MetroCluster breakout mode 10G / 25G (note 1)	ISL, MetroCluster		ISL, MetroCluster	
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 2	MetroCluster 1, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
3 4	MetroCluster 2, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
5-6	Ports disallowed to use	blocked		blocked		blocked		blocked	
7 8	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
9 10	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
11 12	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
13-18	Ports disallowed to use	blocked		blocked		blocked		blocked	
19 20	ISL, MetroCluster native speed 40G / 100G (note 1)	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
21/1-4 22/1-4	ISL, MetroCluster breakout mode 10G / 25G (note 1)	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
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 スイッチ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スイッチに接続している必要があります。

  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を生成するときに、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。 • 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） • 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）
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					
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（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 2	MetroCluster 1, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
3 4	MetroCluster 2, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
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 8	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
9 10	MetroCluster 1, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b
11 12	MetroCluster 2, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b
13 14 15 16	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
17 18	MetroCluster 1, Ethernet Storage Interface	e3a	e3b / e7b	e5a	e5b / e3b	e3a (option 1) e2a (option 2)	e3b (option 1) e10b (option 2)
19 20	MetroCluster 2, Ethernet Storage Interface	e3a	e3b / e7b	e5a	e5b / e3b	e3a (option 1) e2a (option 2)	e3b (option 1) 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 2	MetroCluster 1, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
3 4	MetroCluster 2, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
5	Storage shelf 1 (9)	NSM-1, e0a	NSM-1, e0b	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	NSM-2, e0a	NSM-2, e0b
7 8	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
9 10	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
11 12	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
13 14 15 16	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
17 18	MetroCluster 1, Ethernet Storage Interface	e8a (option 1) e11a (option 2) e8b (option 3)	e8b (option 1) e11b (option 2) e11a (option 3)	e8a (option 1) e11a (option 2) e8b (option 3)	e8b (option 1) e11b (option 2) e11a (option 3)	e8a (option 1) e11a (option 2) e8b (option 3)	e8b (option 1) e11b (option 2) e11a (option 3)	e8a (option 1) e9a (option 2) e10a (option 3) e11a (option 4) e8b (option 5) e10b (option 6)	e8b (option 1) e9b (option 2) e10b (option 3) e11b (option 4) e9a (option 5) e11a (option 6)
19 20	MetroCluster 2, Ethernet Storage Interface	e8a (option 1) e11a (option 2) e8b (option 3)	e8b (option 1) e11b (option 2) e11a (option 3)	e8a (option 1) e11a (option 2) e8b (option 3)	e8b (option 1) e11b (option 2) e11a (option 3)	e8a (option 1) e11a (option 2) e8b (option 3)	e8b (option 1) e11b (option 2) e11a (option 3)	e8a (option 1) e9a (option 2) e10a (option 3) e11a (option 4) e8b (option 5) e10b (option 6)	e8b (option 1) e9b (option 2) e10b (option 3) e11b (option 4) e9a (option 5) e11a (option 6)
21	Storage shelf 2 (8)	NSM-1, e0a	NSM-1, e0b	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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。 • 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） • 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）
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ASA A250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							
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	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**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		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	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	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	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**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 ASA A400、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 2	MetroCluster 1, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b
3 4	MetroCluster 2, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b
5-6	Unused	disabled		disabled		disabled	
7 8	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
9 10	MetroCluster 1, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b
11 12	MetroCluster 2, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b
13 14 15 16	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	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**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		e4a	e4b
3	MetroCluster 2, Local Cluster interface	e4a	e4b
4		e4a	e4b
5-6	Unused	disabled	
7 8	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
9	MetroCluster 1, MetroCluster interface	e2a	e2b
10		e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b
12		e2a	e2b
13 14 15 16	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster	
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 2	MetroCluster 1, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
3 4	MetroCluster 2, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
5-6	Unused	disabled		disabled		disabled	
7 8	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
9 10	MetroCluster 1, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b
11 12	MetroCluster 2, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b
13 14 15 16	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
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 2	MetroCluster 1, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
3 4	MetroCluster 2, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
5-6	Unused	disabled		disabled		disabled		disabled	
7 8	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
9 10	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
11 12	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
13 14 15 16	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
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 4および9 12 、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	Broadcom BES-53248プラットフォームのポート割り当て（グループ1）
FAS500f AFF C250、ASA C250 AFF A250、ASA A250	Broadcom BES-53248プラットフォームのポート割り当て（グループ2）
AFF A20用	Broadcom BES-53248プラットフォームのポート割り当て（グループ3）
AFF C30、AFF A30 FAS50 AFF C60	Broadcom BES-53248プラットフォームのポート割り当て（グループ4）
FAS8200、AFF A300	Broadcom BES-53248プラットフォームのポート割り当て（グループ5）
AFF A320	Broadcom BES-53248プラットフォームのポート割り当て（グループ6）
FAS8300 AFF C400 、ASA C400 AFF A400 、ASA A400 FAS8700	Broadcom BES-53248プラットフォームのポート割り当て（グループ7）

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ー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。ブレークアウトモード（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。 • NVIDIA SN2100プラットフォームのポート割り当て（グループ3a-25G） • NVIDIA SN2100プラットフォームのポート割り当て（グループ3b-100G）
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					
15	ISL, Local Cluster 100G	ISL, Local Cluster		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**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							
9	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
10							
11	MetroCluster 3, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
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							

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NVIDIA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	MetroCluster 3, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
6		e4a	e4b	e4a	e4b	e4a	e4b
7	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
8							
9	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
10							
11	MetroCluster 3, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
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							

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		ISL, Local Cluster		ISL, Local Cluster		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

ナークラスタとネットワーク接続されていることを確認します。

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

"クラスタと SVM のピアリングの簡単な設定"

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用します "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。

   'erviceport 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:bdff:fef8:19ff
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、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. スイッチの基本設定を行います。手順 4 以降を実行します。 Broadcom IP スイッチを工場出荷時のデフォルトにリセット

   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 スイッチ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。

ポートがブレー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.I4.6.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ポートをブレー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。

3. 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)#
```

4. 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)#
```

5. 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。

6. 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。

7. 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シーケンス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スイッチ設定をリバ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、スイッチがリブートされます。リブート後、スイッチを設定するためにRCFファイルを最初に実行し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. スイッチの基本設定を行います
   a. スイッチがブートされ、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ポートをブレー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。

   ポートがブレー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モ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モ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モニタのポーリング間隔が最大2倍になるまで待って `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モニターの設定"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モ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モニタ（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。

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を設定できます。

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ヘルスモニタリングでは、モニタリングをSNMPv3に切り替えた後でも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 Priv
                                     Meth 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: cshm1!
                                 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: cshm1!
                                   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じ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 laErrMessage "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 cshm1! default
 rouser _snmptrapusernameX
+rouser SNMPv3User priv
 sysobjectid 1.3.6.1.4.1.40310
 sysservices 72
-rocommunity cshm1! 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: cshm1!
                                 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じ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
(b8:59:9f:09:7c:22)
                                   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: cshm1!
                                 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じ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
(b8:59:9f:09:7c:22)
                                   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モニタ（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。
- スイッチのヘルスモ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応答する場合は `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 cshm1! -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*cshm1!*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-admim`。

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モニタ（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いことがあります。ヘルスモ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がヘルスモ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 *`に設定されます`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"^]ください。

デフォルトでは、ヘルスモ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"

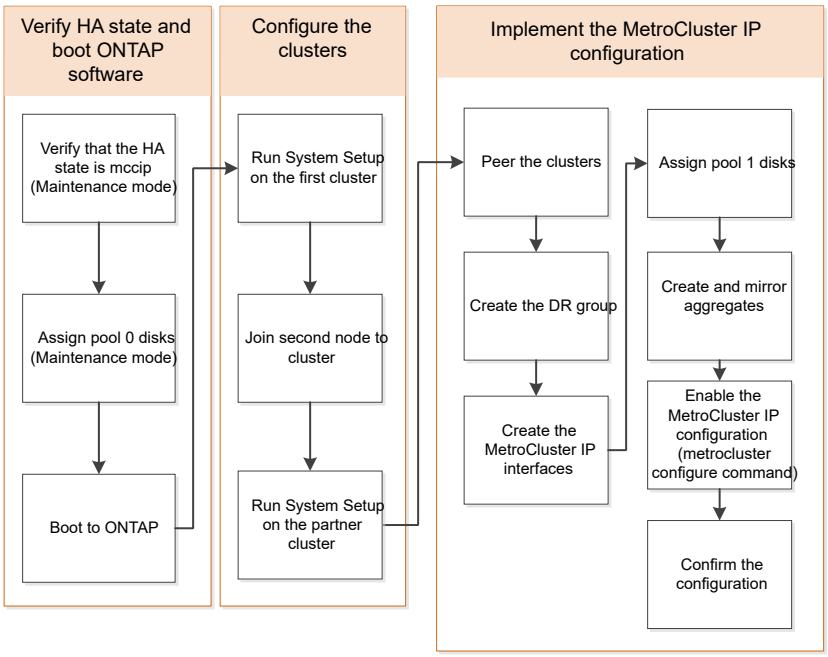
ONTAP で MetroCluster ソフトウェアを設定します

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"

MetroCluster 構成の各クラスタのノードの構成は、標準クラスタのノードと似ています。

MetroCluster 構成は、 2 つの標準クラスタを基盤としています。構成は物理的に対称な構成である必要があり、各ノードのハードウェア構成が同じで、すべての MetroCluster コンポーネントがケーブル接続され、設定されている必要があります。ただし、 MetroCluster 構成のノードの基本的なソフトウェア設定は、標準クラスタのノードと同じです。

設定手順	標準クラスタ構成	MetroCluster の設定
各ノードで管理 LIF 、クラスタ LIF 、データ LIF を設定。	両方のクラスタタイプで同じです	
ルートアグリゲートを設定	両方のクラスタタイプで同じです	
クラスタ内の一方のノードでクラスタを設定。	両方のクラスタタイプで同じです	
もう一方のノードをクラスタに追加。	両方のクラスタタイプで同じです	
ミラーされたルートアグリゲートを作成	任意。	必須
クラスタをピアリング。	任意。	必須
MetroCluster 設定を有効にします。	該当しません	必須

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た
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
                  Usable      Disk      Container           Container
Disk              Size        Shelf Bay Type    Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
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::>
```

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に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
                                  cluster01-01:e0a, cluster01-01:e0b,
                                  cluster01-02:e0a, cluster01-02:e0b
cluster01
                 Default
                                  cluster01-01:e0c, cluster01-01:e0d,
                                  cluster01-02:e0c, cluster01-02:e0d,
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
                 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-addrs <peer_lif_ip_addresses> -ipspace
<ipspace>
```

「 -generate-passphrase 」と「 -peer-addrs 」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-addrs 」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、 -ipspace 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-addrs <peer_lif_ip_addresses> -ipspace <ipspace>
```

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-addrs
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
```

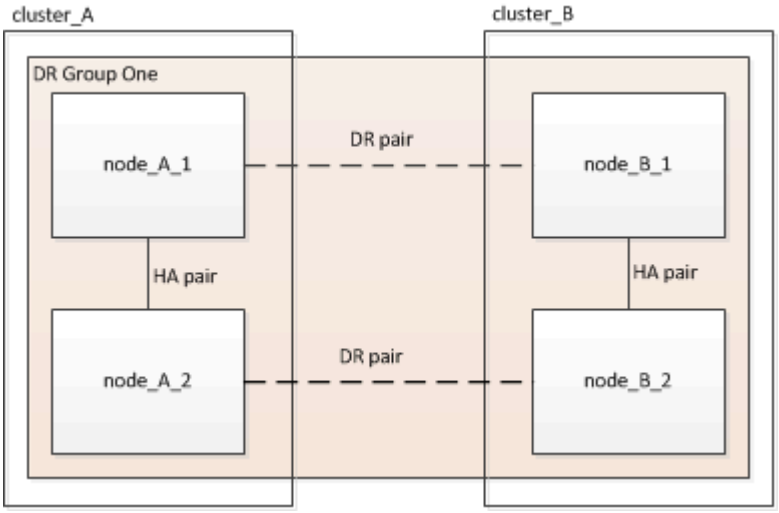
DR グループを作成します

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 configurion-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 configurion-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。

```
cluster_A::> metrocluster configuration-settings interface show
DR                                                                 Config
Group Cluster Node    Network Address Netmask         Gateway   State
----- ------- ------- --------------- --------------- ---------
----------
1     cluster_A  node_A_1
                 Home Port: e5a
                      10.1.1.1     255.255.255.0   -         completed
                 Home Port: e5b
                      10.1.2.1     255.255.255.0   -         completed
                 node_A_2
                 Home Port: e5a
                      10.1.1.2     255.255.255.0   -         completed
                 Home Port: e5b
                      10.1.2.2     255.255.255.0   -         completed
      cluster_B  node_B_1
                 Home Port: e5a
                      10.1.1.3     255.255.255.0   -         completed
                 Home Port: e5b
                      10.1.2.3     255.255.255.0   -         completed
                 node_B_2
                 Home Port: e5a
                      10.1.1.4     255.255.255.0   -         completed
                 Home Port: e5b
                      10.1.2.4     255.255.255.0   -         completed
8 entries were displayed.
cluster_A::>
```

8. ノードで MetroCluster インターフェイスの接続準備が完了し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

   次の例は、「 ready for connection 」状態のすべてのノードを示しています。

```
Cluster       Node         Configuration Settings Status
----------    -----------  ---------------------------------
cluster_A
              node_A_1     ready for connection connect
              node_A_2     ready for connection connect
cluster_B
              node_B_1     ready for connection connect
              node_B_2     ready for connection connect
4 entries were displayed.
```

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                               Configuration  DR
Group Cluster Node               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                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- --------- ----
-     cluster_B
              node_B_1           ready to configure -     -
              node_B_2           ready to configure -     -
2 entries were displayed.
cluster_B::>
```

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 configurion-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
                     Usable     Disk               Container   Container
Disk                 Size       Shelf Bay Type     Type        Name
Owner
----------------    ---------- ----- --- ------- ----------- ---------
--------
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 spare       Pool1
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 spare       Pool1
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
8 entries were displayed.

cluster_B::> disk show
```

```
                    Usable     Disk              Container   Container
Disk                Size       Shelf Bay Type    Type        Name
Owner
----------------    ---------- ----- --- ------- ----------- ---------
--------
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、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
                                                            Speed (Mbps)
Node   Port      IPspace   Broadcast Domain Link   MTU    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問題

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


controller_A_2        controller_A_2_aggr0
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
ok
                      controller_A_2_aggr1
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
ok
                      controller_A_2_aggr2
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
ok
```

```
18 entries were displayed.
```

次に、正常な 4 ノード MetroCluster 構成の MetroCluster check cluster show コマンドの出力例を示します。この出力は、必要に応じてネゴシエートスイッチオーバーを実行できる状態であることを示しています。

```
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	• AFF A800、AFF C800 • AFF A20、 AFF A30、 AFF C30、 AFF A50、 AFF C60 • AFF A70、 AFF A90、 AFF A1K、 AFF C80 • FAS50、FAS70、FAS90
ONTAP 9.15.1	• AFF A400 • AFF C400用 • FAS8300 • FAS8700 の場合

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 の構成設定メディエーターの追加メディエーターのアドレス 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。"https://node-management-IP"

   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、[パスフレーズがありません]*を選択します。これにより、パスフレーズを生成できます。
7. 生成されたパス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、[パスフレーズを使用]*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ス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メディエーターの設定"
   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

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 がサポートされます。

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メディエーター	SSH / ONTAPメディエーターの管理
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、すべてのメディエーターのバージョンがサポートされます。

"ONTAPメディ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。
   - クラスターで 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 構成設定のメディエーターが削除されました

   ONTAPメディ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メディエーターインスタンスに接続する

MetroCluster ノードを別の ONTAP メディエ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エ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 メディエ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 メディエーターを削除します。

   MetroCluster 構成設定のメディエーターが削除されました

2. MetroCluster 構成への新しい ONTAP メディエーター接続を確立します。

   MetroCluster の構成設定メディエーターの追加 mediator-address_ip-address-bmediator-host_`

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

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	• MAUSOが開始されるのは、 デフォルトのシナリオ 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、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。 • 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。 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。 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にのみ、MAUSOをトリガーするコマンド。 • 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。
ONTAP 9.12.1	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、 `metrocluster modify -allow-auto-forced-switchover true` コマンドを実行します 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。 **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 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。 • 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。 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。

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

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メディエ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メディエ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メディエーターの設定	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。 手順 1. ONTAP 9.8 の System Manager で、 * Cluster > Settings * を選択します。 2. [Mediator]*セクションで、をクリックします。 3. Configure Mediator* （メディエーターの設定）ウィンドウで、 * Add+* （追加 + * ）をクリックします。 4. ONTAP Mediator の設定詳細を入力します。 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。 ◦ ONTAP Mediator の IP アドレス。 ◦ ユーザ名。 ◦ パスワード。

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	手順 1. System Manager で、 * ダッシュボード * をクリックします。 2. MetroClusterセクションまでスクロールします。 3. MetroClusterサイト名の横にあるをクリックします ⋮ 。 4. または[無効化]*を選択します。 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。 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。
MetroCluster構成からONTAPメディエーターを削除します	手順 1. System Manager で、 * ダッシュボード * をクリックします。 2. MetroClusterセクションまでスクロールします。 3. MetroClusterサイト名の横にあるをクリックします ⋮ 。 4. [メディエーターの削除]*を選択します。 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。
ONTAPメディエーターの健全性を確認する	のSystem Manager固有の手順を実行します"MetroCluster構成の健全性の確認"。
スイッチオーバーとスイッチバックの実行	の手順を実行します"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）"。

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）スイッチオーバー処理をテストして、データが中断なく提供されることを確認できます。

このタスクについて

このテストでは、クラスターを 2 番目のデータ センターに切り替えても、データの可用性が影響を受けないこと (SMB およびファイバ チャネル プロトコルを除く) を検証します。

このテストには約 30 分かかります。

この手順の想定される結果は次のとおりです。

- MetroCluster switchover コマンドは ' 警告プロンプトを表示します

  プロンプトに「 yes 」と応答すると、コマンドが発行されたサイトがパートナーサイトを切り替えます。

MetroCluster IP 構成の場合：

- ONTAP 9.4 以前：
  - ミラーアグリゲートはネゴシエートスイッチオーバー後にデグレード状態になります。
- ONTAP 9.5 以降：
  - リモートストレージがアクセス可能である場合、ミラーされたアグリゲートは通常の状態のままになります。
  - リモートストレージへのアクセスが失われると、ネゴシエートスイッチオーバー後にミラーアグリゲートがデグレード状態になります。
- ONTAP 9.8 以降の場合：
  - リモートストレージへのアクセスが失われると、ディザスタサイトにあるミラーされていないアグリゲートは使用できなくなります。これにより、コントローラが停止する可能性があります。

手順

1. すべてのノードが設定済みの状態で通常モードになっていることを確認します。

   MetroCluster node show

```
cluster_A::>  metrocluster node show

Cluster                           Configuration State    Mode
--------------------------------- ----------------------
-------------------------
 Local: cluster_A                  configured             normal
Remote: cluster_B                  configured             normal
```

2. スイッチオーバー処理を開始します。

   MetroCluster スイッチオーバー

```
cluster_A::> metrocluster switchover
Warning: negotiated switchover is about to start. It will stop all the
data Vservers on cluster "cluster_B" and
automatically re-start them on cluster "cluster_A". It will finally
gracefully shutdown cluster "cluster_B".
```

3. ローカルクラスタが設定済みの状態でスイッチオーバーモードになっていることを確認します。

   MetroCluster node show

```
cluster_A::>  metrocluster node show

Cluster                           Configuration State    Mode
--------------------------------- ---------------------
------------------------
Local: cluster_A                   configured             switchover
Remote: cluster_B                  not-reachable          -
              configured             normal
```

4. スイッチオーバー処理が成功したことを確認します。

   「 MetroCluster operation show 」を参照してください

```
cluster_A::> metrocluster operation show
  Operation: switchover
      State: successful
 Start Time: 2/6/2016 13:28:50
   End Time: 2/6/2016 13:29:41
     Errors: -
```

5. 「 vserver show 」コマンドと「 network interface show 」コマンドを使用して、 DR SVM と LIF がオンラインになったことを確認します。

修復と手動スイッチバックの検証

修復処理と手動スイッチバック処理をテストするには、ネゴシエートスイッチオーバー後にクラスタを元のデータセンターにスイッチバックして、データの可用性に影響がないことを検証します（ SMB および Solaris FC 構成を除く）。

このタスクについて

このテストには約 30 分かかります。

この手順では、想定される結果として、サービスがホームノードにスイッチバックされることを確認します。

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

1. 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、次の構成で必要です。

   - 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
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,

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
                                 Admin      Operational Root
Vserver     Type    Subtype    State      State       Volume
Aggregate
----------- ------- ---------- ---------- ----------- ----------
----------
SVM1        data    sync-source           running     SVM1_root
node_A_1_data01_mirrored
SVM2        data    sync-source           running     SVM2_root
node_A_2_data01_mirrored

cluster_A::> network interface show -fields is-home false
There are no entries matching your query.

cluster_A::> volume show !vol0,!MDV*
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
SVM1
          SVM1_root
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.50GB    5%
SVM1
          SVM1_data_vol
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_root
                       node_A_2_data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_data_vol
                       node_A_2_data02_unmirrored
                                    online     RW          1GB
972.6MB    5%
```

4. ハードウェア障害をシミュレートするために電源をオフにするノード node_A_1 のプール 1 内のシェルフを特定します。

「 storage aggregate show -r -node node_name !!* root

ミラーされたデータアグリゲートを構成するドライブが格納されたシェルフを選択する必要があります。

次の例では、停止する対象としてシェルフ ID 31 を選択します。

```
cluster_A::> storage aggregate show -r -node node_A_2 !*root
Owner Node: node_A_2
 Aggregate: node_A_2_data01_mirrored (online, raid_dp, mirrored) (block
checksums)
  Plex: /node_A_2_data01_mirrored/plex0 (online, normal, active, pool0)
   RAID Group /node_A_2_data01_mirrored/plex0/rg0 (normal, block
checksums)
                                                                   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 (online, normal, active, pool1)
   RAID Group /node_A_2_data01_mirrored/plex4/rg0 (normal, block
checksums)
                                                                   Usable
Physical
     Position Disk                       Pool Type     RPM     Size
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
```

```
828.0GB (normal)

 Aggregate: node_A_2_data02_unmirrored (online, raid_dp) (block
checksums)
  Plex: /node_A_2_data02_unmirrored/plex0 (online, normal, active,
pool0)
   RAID Group /node_A_2_data02_unmirrored/plex0/rg0 (normal, block
checksums)
                                                                   Usable
Physical
     Position Disk                       Pool Type     RPM     Size
Size Status
     -------- -------------------------- ---- ----- ------ --------
-------- ----------
     dparity  2.30.12                     0   BSAS    7200  827.7GB
828.0GB (normal)
     parity   2.30.22                     0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.21                     0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.20                     0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.14                     0   BSAS    7200  827.7GB
828.0GB (normal)
15 entries were displayed.
```

5. 選択したシェルフの電源を物理的にオフにします。
6. アグリゲートのステータスを再度確認します。

「 storage aggregate show

「 storage aggregate show -r -node node_name ！ * root 」

次の例に示すように、電源をオフにしたシェルフにドライブがあるアグリゲートの RAID ステータスが「 degraded 」になり、影響を受けたプレックスのドライブのステータスが「 failed 」になります。

```
cluster_A::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_A_1data01_mirrored
            4.15TB    3.40TB   18% online       3 node_A_1
raid_dp,

mirrored,
```

```
normal
node_A_1root
           707.7GB   34.29GB   95% online       1 node_A_1
raid_dp,

mirrored,

normal
node_A_2_data01_mirrored
            4.15TB    4.12TB    1% online       2 node_A_2
raid_dp,

mirror

degraded
node_A_2_data02_unmirrored
            2.18TB    2.18TB    0% online       1 node_A_2
raid_dp,

normal
node_A_2_root
           707.7GB   34.27GB   95% online       1 node_A_2
raid_dp,

mirror

degraded
cluster_A::> storage aggregate show -r -node node_A_2 !*root
Owner Node: node_A_2
 Aggregate: node_A_2_data01_mirrored (online, raid_dp, mirror degraded)
(block checksums)
  Plex: /node_A_2_data01_mirrored/plex0 (online, normal, active, pool0)
   RAID Group /node_A_2_data01_mirrored/plex0/rg0 (normal, block
checksums)
                                                                   Usable
Physical
     Position Disk                        Pool Type     RPM     Size
Size Status
     -------- --------------------------- ---- ----- ------ --------
-------- ----------
     dparity  2.30.3                       0   BSAS    7200  827.7GB
828.0GB (normal)
     parity   2.30.4                       0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.6                       0   BSAS    7200  827.7GB
```

```
828.0GB (normal)
     data     2.30.8                        0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.5                        0   BSAS    7200  827.7GB
828.0GB (normal)

  Plex: /node_A_2_data01_mirrored/plex4 (offline, failed, inactive,
pool1)
   RAID Group /node_A_2_data01_mirrored/plex4/rg0 (partial, none
checksums)
                                                                  Usable
Physical
     Position Disk                        Pool Type     RPM     Size
Size Status
     -------- --------------------------- ---- ----- ------ --------
-------- ----------
     dparity  FAILED                       -   -          -  827.7GB
-  (failed)
     parity   FAILED                       -   -          -  827.7GB
-  (failed)
     data     FAILED                       -   -          -  827.7GB
-  (failed)
     data     FAILED                       -   -          -  827.7GB
-  (failed)
     data     FAILED                       -   -          -  827.7GB
-  (failed)

 Aggregate: node_A_2_data02_unmirrored (online, raid_dp) (block
checksums)
  Plex: /node_A_2_data02_unmirrored/plex0 (online, normal, active,
pool0)
   RAID Group /node_A_2_data02_unmirrored/plex0/rg0 (normal, block
checksums)
                                                                  Usable
Physical
     Position Disk                        Pool Type     RPM     Size
Size Status
     -------- --------------------------- ---- ----- ------ --------
-------- ----------
     dparity  2.30.12                      0   BSAS    7200  827.7GB
828.0GB (normal)
     parity   2.30.22                      0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.21                      0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.20                      0   BSAS    7200  827.7GB
```

```
828.0GB (normal)
     data     2.30.14                       0   BSAS    7200  827.7GB
828.0GB (normal)
15 entries were displayed.
```

7. データが提供されていること、およびすべてのボリュームがオンラインのままであることを確認します。

   vserver show -type data

   network interface show -fields is-home false

   volume show ！ vol0 、 ！ MDV *

```
cluster_A::> vserver show -type data

cluster_A::> vserver 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

イドからノードを削除する方法"

MetroClusterの構成解除を元に戻すことはできません。このプロセスは、テクニカルサポートの支援を受けてのみ実行してください。MetroCluster構成を削除した後、すべてのMetroCluster接続と相互接続をサポート可能な状態に調整する必要があります。

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す。

MetroCluster 構成での FlexGroup のサポート

ONTAP 9.6 以降では、 MetroCluster 構成で FlexGroup ボリュームがサポートされます。

MetroCluster 構成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、どういった整合性が必要とされるかも把握しておく必要があります。

関連情報

"ネットワークと LIF の管理"

"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は移動されません。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。

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

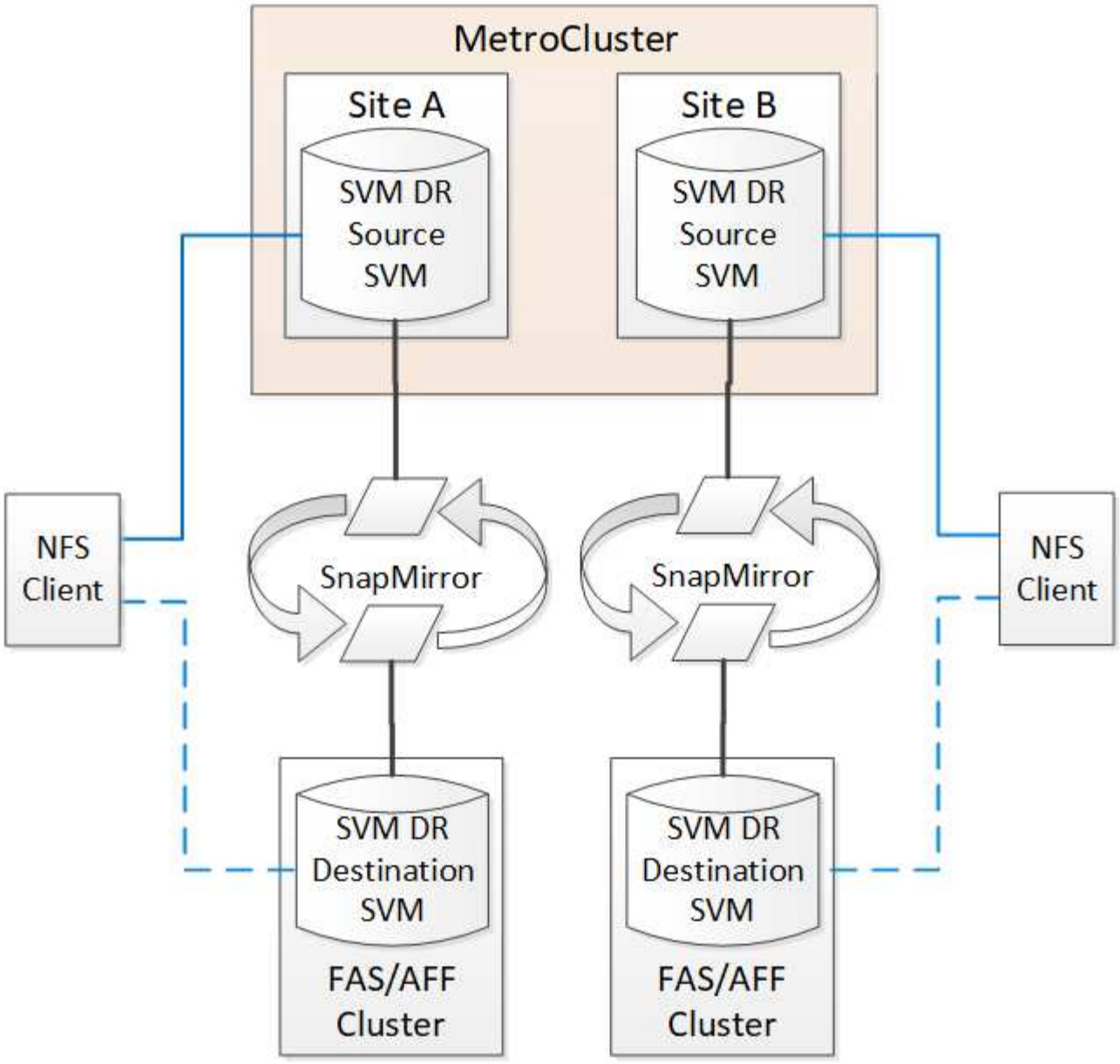
MetroCluster 構成内のノードのルートアグリゲート（ HA ポリシーが CFO ）に新しいボリュームを作成することはできません。

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。



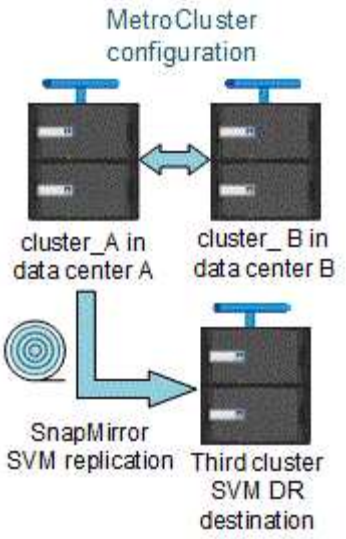
SVM を SnapMirror ディザスタリカバリで使用する場合は、次の要件と制限事項に注意してください。

- 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。

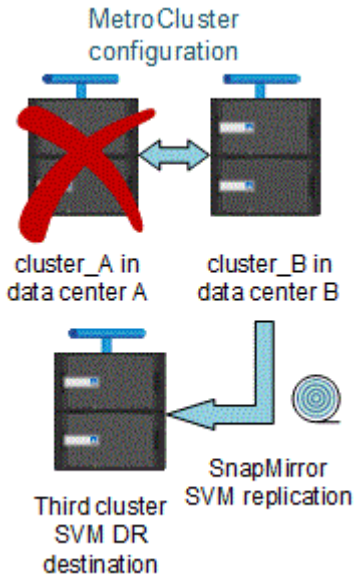
- MetroCluster 構成が安定した状態のときは MetroCluster の同期先の SVM はオンラインでないため、同期先ボリュームを SVM ディザスタリカバリ関係のソースにすることはできません。

  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。

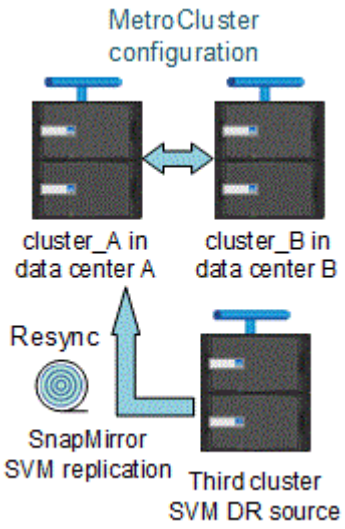
  ただし、スイッチオーバーまたはスイッチバックプロセスの完了後、 SVM DR の次回のスケジュールされている更新は成功します。

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 ）が使用されます。

ステップ

1. スイッチオーバー時に MetroCluster 構成で NVFAIL をトリガーするには、「 vol-dr-force-nvfail 」パラメータを on に設定します。

   vol modify -vserver 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 

て*[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、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"	• MetroCluster IP の構成と運用の技術概要 • MetroCluster IP 構成のベスト プラクティス。
"ファブリック接続 MetroCluster のインストールと設定"	• ファブリック接続 MetroCluster アーキテクチャ • 構成のケーブル接続 • FC-to-SAS ブリッジの設定 • FC スイッチを設定します • ONTAP で MetroCluster を設定します
"ストレッチ MetroCluster のインストールと設定"	• ストレッチ MetroCluster アーキテクチャ • 構成のケーブル接続 • FC-to-SAS ブリッジの設定 • ONTAP で MetroCluster を設定します
"MetroCluster の管理"	• MetroCluster 構成について • スイッチオーバー、修復、スイッチバック
"ディザスタリカバリ"	• ディザスタリカバリ • 強制スイッチオーバー • 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

"MetroCluster メンテナンス"	• MetroCluster FC 構成のメンテナンスガイドライン • 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 • ファブリック接続またはストレッチ MetroCluster FC 構成でのディスクシェルフのホットアド • ファブリック接続またはストレッチ MetroCluster FC 構成でのディスクシェルフのホットリムーブ • ファブリック接続またはストレッチ MetroCluster FC 構成のディザスタサイトでのハードウェア交換 • 2 ノードのファブリック接続またはストレッチ MetroCluster FC 構成の 4 ノード MetroCluster 構成への拡張 • 4 ノードのファブリック接続またはストレッチ MetroCluster FC 構成の 8 ノード MetroCluster FC 構成への拡張
"MetroCluster のアップグレードと拡張"	• MetroCluster 設定をアップグレードまたは更新する • ノードの追加による MetroCluster 構成の拡張
"MetroCluster の移行"	• MetroCluster FC 構成から MetroCluster IP 構成への移行
"MetroCluster のアップグレード、移行、拡張"	• MetroCluster Tiebreaker ソフトウェアを使用して MetroCluster 構成を監視する
"ONTAPハードウェアシステムのドキュメント" • 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。	• ディスクシェルフのホットアド • ディスクシェルフのホットリムーブ
"コピーベースの移行"	• 7-Mode ストレージシステムから clustered Data ONTAP ストレージシステムへデータを移行する
"ONTAP の概念"	• ミラーされたアグリゲートの機能

ストレッチ MetroCluster 構成をインストール

概要

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

- "インストールを準備し、すべての要件を理解します"
- "正しいインストール手順を選択します"
- コンポーネントをケーブル接続します
  - "2 ノード SAS 接続構成"
  - "2 ノードブリッジ接続構成"
- "ソフトウェアを設定します"
- "設定をテストします"

MetroCluster のインストールを準備

ONTAP MetroCluster 構成の違い

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

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

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

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

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

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

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

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

クラスタピアリング

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

関連情報

"クラスタと SVM のピアリングの簡単な設定"

クラスタピアリングの前提条件

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

接続要件

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

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

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

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

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

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

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

ポート要件

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

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

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

- クラスタ間通信で使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す。

専用のポートを使用する場合の考慮事項

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

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

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

  ポートの帯域幅は、すべての VLAN とベースポートで共有されます。

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

データポートを共有する場合の考慮事項

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

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

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

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

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

ミラーされていないアグリゲートを使用する場合の

ミラーされていないアグリゲートを使用する場合の

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

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

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

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

ミラーされていないアグリゲートと階層状のネームスペースに関する考慮事項

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

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

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

ミラーされていないアグリゲートと **SVM** に関する考慮事項

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

ミラーされていないアグリゲートと **SAN** に関する考慮事項

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

MetroCluster サイトでのファイアウォールの使用状況

MetroCluster サイトでのファイアウォールの使用に関する考慮事項

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

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

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

構成に適したインストール手順の選択

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

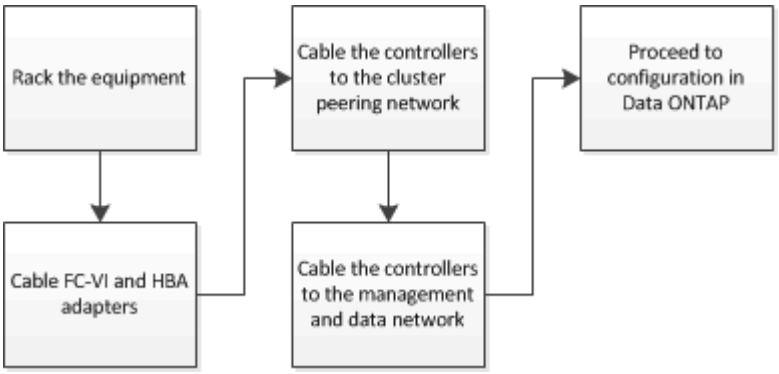
ンストール手順を選択する必要があります。

インストールの種類	使用する手順
FC-to SAS ブリッジを使用する 2 ノードストレッチ構成	1. "2 ノードブリッジ接続ストレッチ MetroCluster 構成のケーブル接続" 2. "ONTAP での MetroCluster ソフトウェアの設定"
直接接続型の SAS ケーブル接続を使用する 2 ノードストレッチ構成	1. "2 ノード SAS 接続ストレッチ MetroCluster 構成のケーブル接続" 2. "ONTAP での MetroCluster ソフトウェアの設定"

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

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

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



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

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

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

- ストレージコントローラ

  ストレージコントローラは、 SAS ケーブルを使用してストレージに直接接続します。

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

  - 短い距離には SAS 銅線ケーブルを使用できます。

◦ 長い距離には SAS 光ケーブルを使用できます。

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

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

- クラスタピアリングネットワーク

  クラスタピアリングネットワークを経由して、 Storage Virtual Machine （ SVM ）の設定がミラーされます。一方のクラスタのすべての SVM の設定が、パートナークラスタにミラーされます。

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

MetroCluster 構成にはさまざまなハードウェアコンポーネントが必要です。わかりやすいように、 MetroCluster のドキュメント全般をとおして標準的なコンポーネント名を使用します。一方のサイトをサイト A と呼び、もう一方のサイトをサイト B と呼びます

サポートされているソフトウェアおよびハードウェア

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

"NetApp Hardware Universe の略"

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

MetroCluster 構成でのハードウェアの冗長性

MetroCluster 構成ではハードウェアの冗長性が確保されるため、サイトには各コンポーネントが 2 つずつあります。コンポーネントの名前には、サイトを表す A または B 、および 2 つあるコンポーネントのうちどちらかを表す番号として 1 または 2 を使用します。

シングルノード **ONTAP** クラスタ **× 2**

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

名前は MetroCluster 構成内で一意である必要があります。

名前の例：

- サイト A ： cluster_A
- サイト B ： cluster_B

ストレージコントローラモジュール **× 2**

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

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

  一部のコントローラモジュールは、次の 2 つのオプションに対応しています。

  - オンボードの FC-VI ポート
  - スロット 1 の FC-VI カード

    オンボードの FC-VI ポートを使用するコントローラモジュールとアドオンの FC-VI カードを使用するコントローラモジュールは混在できません。たとえば、あるノードでオンボードの FC-VI 構成を使用する場合は、 DR グループの他のすべてのノードでもオンボードの FC-VI 構成を使用する必要があります。

名前の例：

- サイト A ： controller_A_1
- サイト B ： controller_B_1

SAS ディスクシェルフ **× 4** 台以上（推奨）

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

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

名前の例：

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

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

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

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

本ドキュメントで手順を開始する前に

このタスクを実行するには、次の全体的な要件を満たしている必要があります。

- 設置前に、ディスクシェルフモデルに応じたディスクシェルフの設置とケーブル接続に関する考慮事項とベストプラクティスを確認しておく必要があります。
- すべてのMetroClusterコンポーネントがサポートされている必要があります。

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

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

このタスクについて

- 「ノード」と「コントローラ」は同じ意味で使用されます。

ラックにハードウェアコンポーネントを配置

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

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

手順

1. MetroCluster コンポーネントの配置を計画します。

   必要なラックスペースは、ストレージコントローラのプラットフォームモデル、スイッチのタイプ、構成内のディスクシェルフスタック数によって異なります。

2. 電気機器を扱うための標準的な製造方法を使用して、適切に接地されていることを確認します。
3. ストレージコントローラをラックまたはキャビネットに設置します。

   "ONTAPハードウェアシステムのドキュメント"

4. ディスクシェルフを設置し、各スタックのディスクシェルフをデイジーチェーン接続し、電源を投入して、シェルフ ID を設定します。

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

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

コントローラ間およびコントローラとストレージシェルフのケーブル接続

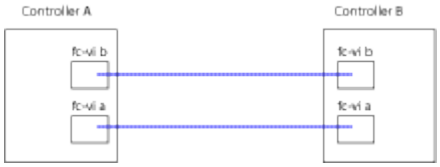
コントローラの FC-VI アダプタどうしを直接ケーブル接続する必要があります。コント

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

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

手順

1. FC-VI ポートをケーブル接続します。

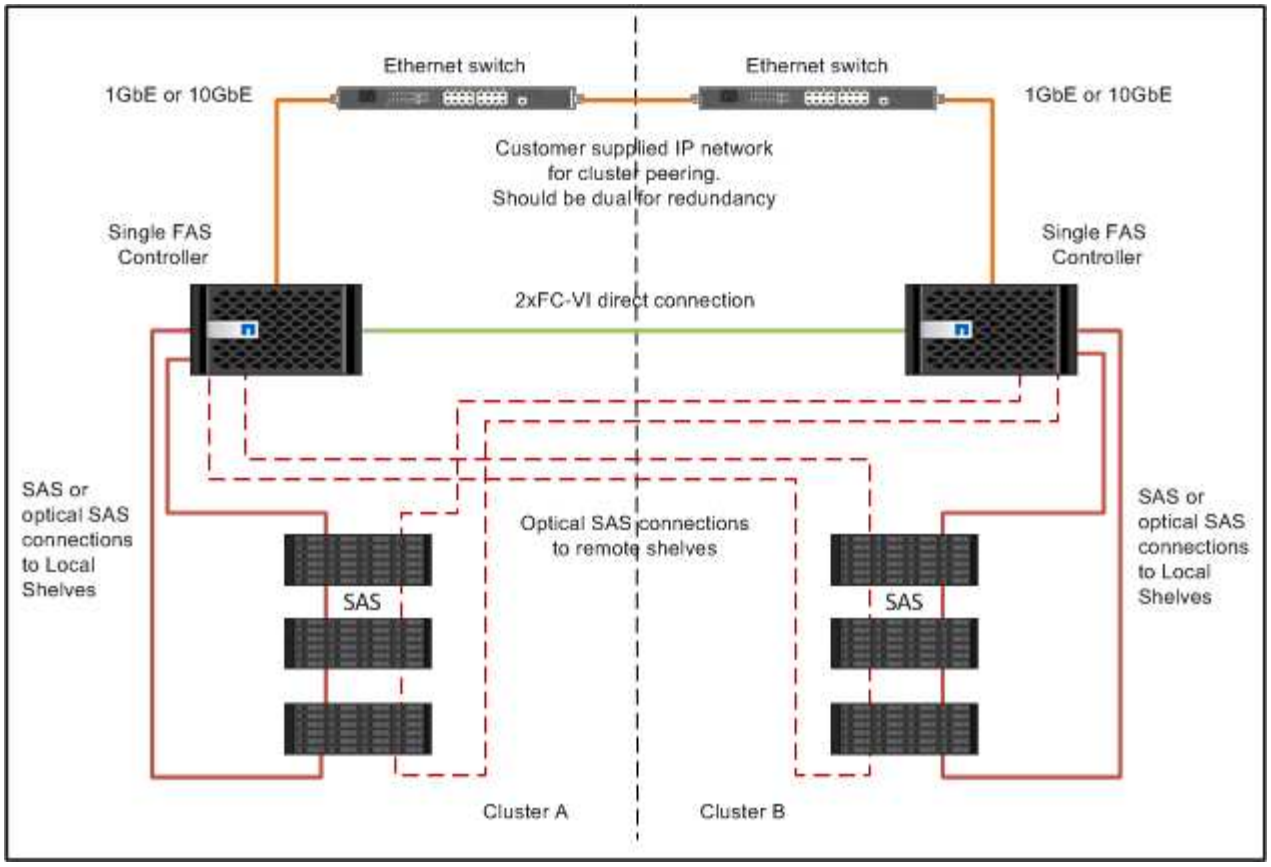


上の図は、一般的なケーブル接続を示しています。FC-VI ポートはコントローラモジュールによって異なります。

- FAS8200 および AFF A300 コントローラモジュールでは、発注時に FC-VI 接続のオプションとして次のいずれかを選択できます。
  - オンボードポート 0e と 0f は、 FC-VI モードで設定します。
  - FC-VI カードのポート 1a および 1b は、スロット 1 に装着します。
- AFF A700 および FAS9000 ストレージシステムのコントローラモジュールは、それぞれ FC-VI ポートを 4 つ使用します。
- AFF A400 および FAS8300 ストレージシステムコントローラモジュールは、 FC-VI ポート 2a および 2b を使用します。

2. SAS ポートをケーブル接続します。

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



クラスタピアリングのケーブル接続

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

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

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

ポートおよびネットワーク接続の推奨される最小帯域幅は 1GbE です。

手順

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

   クラスタピアリングには、専用のポートとデータポートのどちらも使用できます。専用のポートを使用すると、クラスタピアリングトラフィックのスループットが向上します。

   "クラスタと SVM のピアリングの簡単な設定"

管理ポートとデータポートのケーブル接続

各ストレージコントローラの管理ポートとデータポートをサイトネットワークにケーブル接続する必要があります。

このタスクは、両方の MetroCluster サイトで新しいコントローラを配置するたびに実行する必要があります。

コントローラおよびクラスタスイッチの管理ポートをネットワーク内の既存のスイッチに接続できます。また、 NetApp CN1601 クラスタ管理スイッチなど、新しい専用ネットワークスイッチにコントローラを接続することもできます。

手順

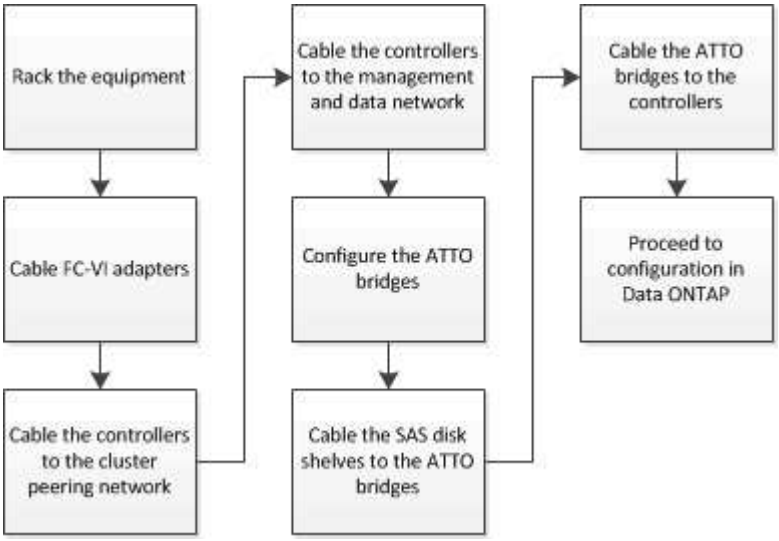
1. コントローラの管理ポートとデータポートを、ローカルサイトの管理ネットワークとデータネットワークにケーブル接続します。

   "ONTAPハードウェアシステムのドキュメント"

2 ノードブリッジ接続ストレッチ MetroCluster 構成をケーブル接続します

2 ノードブリッジ接続ストレッチ MetroCluster 構成のケーブル接続

両方の地理的サイトで MetroCluster コンポーネントを物理的に設置し、ケーブル接続して、設定する必要があります。



2 ノードブリッジ接続ストレッチ MetroCluster 構成のコンポーネント

MetroCluster 構成を計画するときは、構成のコンポーネントとそれらの連携について理解しておく必要があります。

MetroCluster の設定には、中核をなす次のハードウェアが含まれます。

- ストレージコントローラ

  ストレージコントローラはストレージに直接は接続されず、 FC-to-SAS ブリッジに接続されます。ストレージコントローラは、各コントローラの FC-VI アダプタどうしを FC ケーブルで接続することで相互に接続されます。

各ストレージコントローラは、パートナーサイトのストレージコントローラに対する DR パートナーとして構成されます。

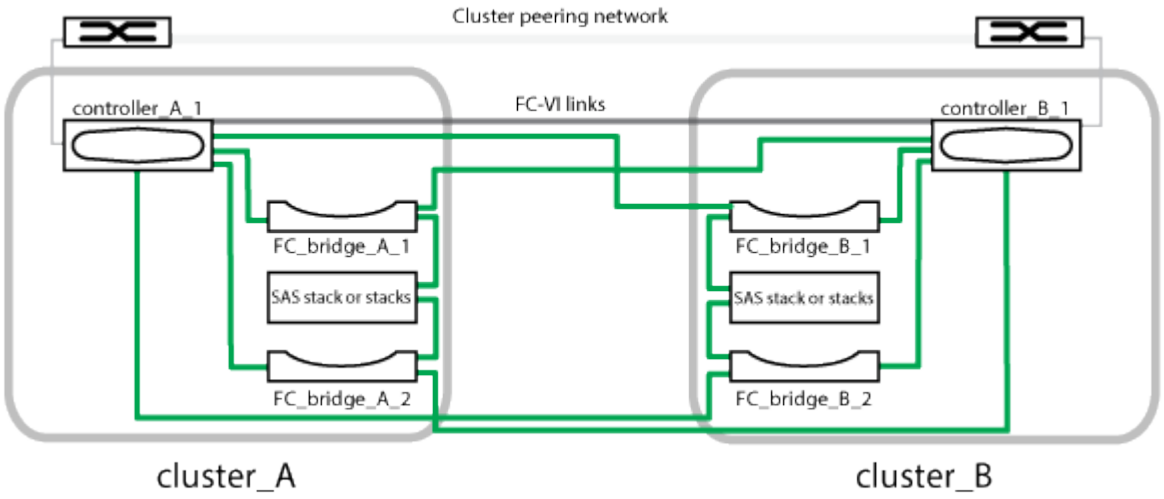
- FC-to-SAS ブリッジ

  FC-to-SAS ブリッジは、コントローラ上の FC イニシエータポートに SAS ストレージスタックを接続して、 2 つのプロトコル間のブリッジの役割を果たします。

- クラスタピアリングネットワーク

  クラスタピアリングネットワークを経由して、 Storage Virtual Machine （ SVM ）の設定がミラーされます。一方のクラスタのすべての SVM の設定が、パートナークラスタにミラーされます。

次の図は、 MetroCluster 構成を単純化したものです。一部の接続では、コンポーネント間の複数の冗長接続を 1 本の線で表しています。データネットワーク接続と管理ネットワーク接続は表示されません。



- 2 つのシングルノードクラスタで構成されます。
- 各サイトには、 SAS ストレージスタックが 1 つ以上あります。

  MetroCluster 構成の SAS シェルフは、 ACP ケーブル配線ではサポートされていません。

  追加のストレージスタックもサポートされますが、図では各サイトに 1 つしかありません。

2 ノードブリッジ接続ストレッチ構成の MetroCluster に必要なハードウェアコンポーネントと命名規則

MetroCluster 構成を計画する際には、サポート対象の必要なハードウェアコンポーネントとソフトウェアコンポーネントを把握しておく必要があります。また、内容を正しく理解するためには、このドキュメントで使用しているコンポーネントの命名規則も確認しておく必要があります。たとえば、一方のサイトをサイト A と呼び、もう一方のサイトをサイト B と呼びます

サポートされているソフトウェアおよびハードウェア

ハードウェアとソフトウェアは、 MetroCluster FC 構成でサポートされている必要があります。

"NetApp Hardware Universe の略"

AFF システムを使用する場合は、 MetroCluster 構成内のすべてのコントローラモジュールを AFF システムとして構成する必要があります。

MetroCluster 構成でのハードウェアの冗長性

MetroCluster 構成ではハードウェアの冗長性が確保されるため、サイトには各コンポーネントが 2 つずつあります。コンポーネントの名前には、サイトを表す A または B 、および 2 つあるコンポーネントのうちどちらかを表す番号として 1 または 2 を使用します。

シングルノード **ONTAP** クラスタ **× 2**

ブリッジ接続ストレッチ MetroCluster 構成には、シングルノード ONTAP クラスタが 2 つ必要です。

名前は MetroCluster 構成内で一意である必要があります。

名前の例：

- サイト A ： cluster_A
- サイト B ： cluster_B

ストレージコントローラモジュール **× 2**

ブリッジ接続ストレッチ MetroCluster 構成には、ストレージコントローラモジュールが 2 つ必要です。

コントローラの要件は次のとおりです。

- 名前は MetroCluster 構成内で一意である必要があります。
- MetroCluster 構成のすべてのコントローラモジュールで同じバージョンの ONTAP が実行されている必要があります。
- 1 つの DR グループ内のすべてのコントローラモジュールのモデルが同じであることが必要です。
- 1 つの DR グループのすべてのコントローラモジュールで同じ FC-VI 構成を使用する必要があります。

  一部のコントローラモジュールは、次の 2 つのオプションに対応しています。

  - オンボードの FC-VI ポート
  - スロット 1 の FC-VI カード

    オンボードの FC-VI ポートを使用するコントローラモジュールとアドオンの FC-VI カードを使用するコントローラモジュールは混在できません。たとえば、あるノードでオンボードの FC-VI 構成を使用する場合は、 DR グループの他のすべてのノードでもオンボードの FC-VI 構成を使用する必要があります。

名前の例：

- サイト A ： controller_A_1
- サイト B ： controller_B_1

FC-to-SAS ブリッジの要件

ブリッジ接続ストレッチ MetroCluster 構成では、各サイトに FC-to-SAS ブリッジが 2 つ以上必要です。

これらのブリッジで SAS ディスクシェルフをコントローラモジュールに接続します。

ONTAP 9.8 以降を実行している構成では、 FibreBridge 6500N ブリッジはサポートされません。

- FibreBridge 7600N / 7500N ブリッジでは、最大 4 つの SAS スタックがサポートされます。
- それぞれのスタックで異なる IOM モデルを使用できますが、スタック内ではすべてのシェルフで同じモデルを使用する必要があります。

  サポートされる IOM モデルは、実行している ONTAP のバージョンによって異なります。

- 名前は MetroCluster 構成内で一意である必要があります。

この手順で例として使用されている推奨名には、ブリッジの接続先コントローラモジュールとポート番号が含まれています。

名前の例：

- サイト A ：
  - bridge_A_1___ ポート番号 _
  - bridge_A_2_ ポート番号 `
- サイト B ：
  - bridge_B_1___ ポート番号 _
  - Bridge_B_2_ ___ ポート番号 _`

SAS シェルフ **× 4** 台以上（推奨）

ブリッジ接続ストレッチ MetroCluster 構成には、 SAS シェルフが少なくとも 2 台必要です。ただし、シェルフ単位でのディスク割り当てを可能にするために、各サイトにシェルフを 2 台配置し、合計 4 台の SAS シェルフを使用することを推奨します。

各サイトにシェルフ 1 台の最小構成もサポートされます。

名前の例：

- サイト A ：
  - shelf_A_1_1
  - shelf_A_1_2
- サイト B ：

- shelf_B_1_1
- shelf_B_1_2

FC-to-SAS ブリッジの情報収集ワークシート

MetroCluster サイトの設定を開始する前に、必要な設定情報を収集する必要があります。

サイト **A** 、 **FC-to-SAS** ブリッジ **1** （ **FC_bridge_A_1a** ）

SAS スタックごとに FC-to-SAS ブリッジが少なくとも 2 つ必要です。

各ブリッジは、 Controller_A_1_`` ポート番号　と `Controller_B_1_` ポート番号 _ に接続します。

サイト A	あなたの価値
bridge_A_1a の IP アドレス	
Bridge_A_1a ユーザ名	
Bridge_A_1a のパスワード	

サイト **A** 、 **FC-to-SAS** ブリッジ **2** （ **FC_bridge_A_1b** ）

SAS スタックごとに FC-to-SAS ブリッジが少なくとも 2 つ必要です。

各ブリッジは、 Controller_A_1_`` ポート番号　と `Controller_B_1_` ポート番号 _ に接続します。

サイト A	あなたの価値
Bridge_A_1b の IP アドレス	
Bridge_A_1b のユーザ名	
Bridge_A_1b のパスワード	

サイト **B** 、 **FC-to-SAS** ブリッジ **1** （ **FC_bridge_B_1a** ）

SAS スタックごとに FC-to-SAS ブリッジが少なくとも 2 つ必要です。

各ブリッジは、 Controller_A_1_` ポート番号 と Controller_B_1_` ポート番号 に接続します。

サイト B	あなたの価値
Bridge_B_1a の IP アドレス	

Bridge_B_1a ユーザ名	
Bridge_B_1a のパスワード	

サイト **B** 、 **FC-to-SAS** ブリッジ **2** （ **FC_bridge_B_1b** ）

SAS スタックごとに FC-to-SAS ブリッジが少なくとも 2 つ必要です。

各ブリッジは、 Controller_A_1_` ポート番号 と Controller_B_1_` ポート番号 に接続します。

サイト B	あなたの価値
Bridge_B_1b の IP アドレス	
Bridge_B_1b ユーザ名	
Bridge_B_1b のパスワード	

MetroCluster コンポーネントを設置してケーブルを配線します

ラックにハードウェアコンポーネントを配置

納入された機器がキャビネットに設置されていない場合は、コンポーネントをラックに配置する必要があります。

このタスクは両方の MetroCluster サイトで実行する必要があります。

手順

1. MetroCluster コンポーネントの配置を計画します。

   ラックスペースは、ストレージコントローラのプラットフォームモデル、スイッチのタイプ、構成内のディスクシェルフスタック数によって異なります。

2. 自身の適切な接地対策を行います
3. ストレージコントローラをラックまたはキャビネットに設置します。

   "ONTAPハードウェアシステムのドキュメント"

4. ディスクシェルフを設置し、電源を投入して、シェルフ ID を設定します。
   - 各ディスクシェルフの電源を再投入する必要があります。
   - 各 MetroCluster DR グループ（両サイトを含む）で、各 SAS ディスクシェルフのシェルフ ID が一意である必要があります。
5. 各 FC-to-SAS ブリッジを設置します。

   a. 4 本のネジを使用して、ブリッジ前面の「 L 」ブラケットをラックの前面に固定します（フラッシュマウント）。

ブリッジ「 L 」ブラケットの開口部は、 19 インチ（ 482.6 mm ）ラックのラック標準 ETA-310-X に準拠しています。

設置の詳細および図については、ブリッジモデルに対応する _ATTO FibreBridge Installation and Operation Manual を参照してください。

b. 各ブリッジを、適切なアースを提供する電源に接続します。

c. 各ブリッジの電源をオンにします。

耐障害性を最大限にするために、ディスクシェルフの同じスタックに接続されているブリッジをそれぞれ別々の電源に接続する必要があります。

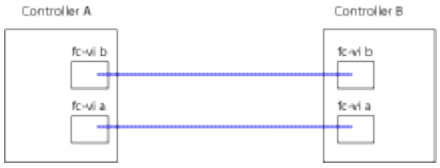
ブリッジの準備完了を示す LED が点灯し、ブリッジの電源投入時自己診断テストが完了したことを示すまで、 30 秒ほどかかる場合があります。

コントローラ間のケーブル接続

各コントローラの FC-VI アダプタを対応するパートナーに直接ケーブル接続する必要があります。

手順

1. FC-VI ポートをケーブル接続します。



上の図は、必要なケーブル接続の一般的な例です。FC-VI ポートはコントローラモジュールによって異なります。

- AFF A300 および FAS8200 コントローラモジュールの場合、発注時に FC-VI 接続のオプションとして次のいずれかを選択できます。
  - FC-VI モードで設定されたオンボードポート 0e および 0f 。
  - スロット 1 の FC-VI カードのポート 1a および 1b 。
- AFF A700 および FAS9000 ストレージシステムのコントローラモジュールは、それぞれ FC-VI ポートを 4 つ使用します。

クラスタピアリングのケーブル接続

クラスタピアリングに使用するコントローラモジュールのポートをケーブル接続して、それらのポートがパートナーサイトのクラスタに接続されるようにする必要があります。

このタスクは、 MetroCluster 構成の各コントローラモジュールで実行する必要があります。

クラスタピアリングには、各コントローラモジュールの少なくとも 2 つのポートを使用します。

ポートおよびネットワーク接続の推奨される最小帯域幅は 1GbE です。

手順

1. クラスタピアリングに使用する少なくとも 2 つのポートを特定してケーブル接続し、そのポートがパートナークラスタとネットワーク接続されていることを確認します。

   クラスタピアリングには、専用のポートとデータポートのどちらも使用できます。専用のポートを使用すると、クラスタピアリングトラフィックのスループットが向上します。

   "クラスタと SVM のピアリングの簡単な設定"

管理ポートとデータポートのケーブル接続

各ストレージコントローラの管理ポートとデータポートをサイトネットワークにケーブル接続する必要があります。

このタスクは、両方の MetroCluster サイトで新しいコントローラを配置するたびに実行する必要があります。

コントローラおよびクラスタスイッチの管理ポートをネットワーク内の既存のスイッチに接続できます。また、 NetApp CN1601 クラスタ管理スイッチなど、新しい専用ネットワークスイッチにコントローラを接続することもできます。

手順

1. コントローラの管理ポートとデータポートを、ローカルサイトの管理ネットワークとデータネットワークにケーブル接続します。

   "ONTAPハードウェアシステムのドキュメント"

FC-to-SAS ブリッジおよび SAS ディスクシェルフを設置

新しいストレージを構成に追加する際に、ATTO FibreBridgeブリッジとSASディスクシェルフを設置してケーブル接続します。

このタスクについて

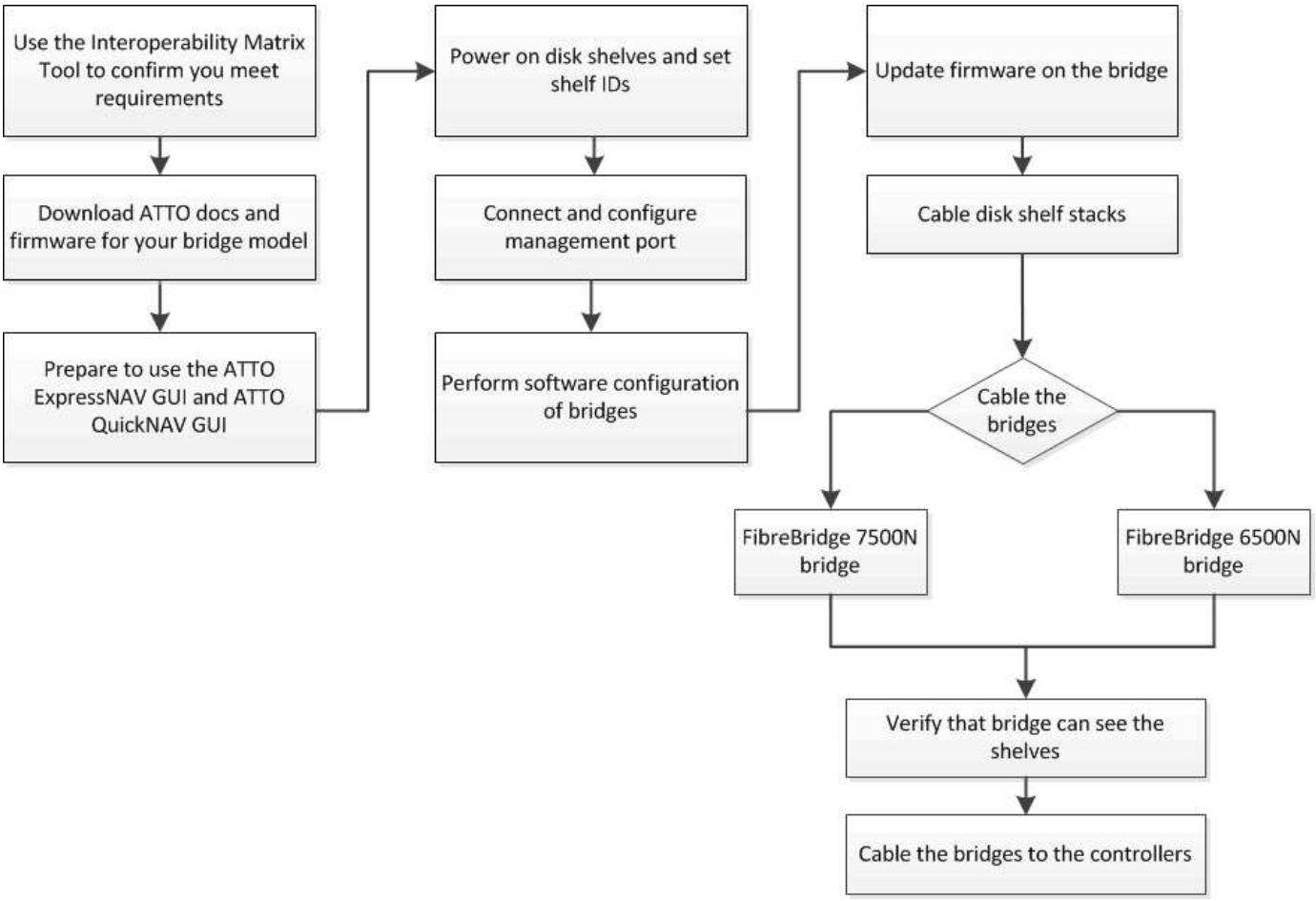
工場出荷状態のシステムの場合は、 FC-to-SAS は事前に構成されているため、追加の構成は不要です。

この手順は、推奨されるブリッジ管理インターフェイスである ATTO ExpressNAV GUI と ATTO QuickNAV ユーティリティを使用していることを前提としています。

ATTO ExpressNAV GUI は、ブリッジの設定および管理、ブリッジファームウェアの更新に使用します。ATTO QuickNAV ユーティリティは、ブリッジのイーサネット管理 1 ポートの設定に使用します。

シリアルポートや Telnet を使用してブリッジの設定と管理、イーサネット管理 1 ポートの設定を行ったり、FTP を使用してブリッジファームウェアを更新するなど、必要に応じて他の管理インターフェイスも使用できます。

この手順では次のワークフローを使用します。



FC-to-SAS ブリッジのインバンド管理

ONTAP 9.5 以降では、 FibreBridge 7500N / 7600N ブリッジについて、 IP 管理に代わる方法としてインバンド管理 _ がサポートされます。ONTAP 9.8 以降では、アウトオブバンド管理は廃止されています。

ONTAP 9.8 以降では 'storage bridge コマンドは 'system bridge コマンドに置き換えられました次の手順は「 storage bridge 」コマンドを示していますが、 ONTAP 9.8 以降を実行している場合は「 system bridge 」コマンドが優先されます。

インバンド管理を使用する場合は、ONTAP CLIからブリッジへのFC接続を使用してブリッジを管理および監視できます。ブリッジのイーサネットポートを介してブリッジに物理的にアクセスする必要がないため、ブリッジのセキュリティの脆弱性が軽減されます。

ブリッジのインバンド管理が可能かどうかは、 ONTAP のバージョンによって異なります。

- ONTAP 9.8 以降では、ブリッジはデフォルトでインバンド接続を介して管理され、 SNMP を介したブリッジのアウトオブバンド管理は廃止されています。
- ONTAP 9.5 から 9.7 ：インバンド管理またはアウトオブバンド管理のどちらかで SNMP 管理がサポートされます。
- ONTAP 9.5よりも前のバージョンでは、アウトオブバンドのSNMP管理のみがサポートされていました。

ブリッジCLIコマンドは、ONTAPインターフェイスでONTAP interfaceコマンドを使用して実行でき `storage bridge run-cli -name <bridge_name> -command <bridge_command_name>`ます。

ブリッジの物理接続を制限することでセキュリティを向上させるために、 IP アクセスを無効にしたインバンド管理の使用を推奨します。

FibreBridge 7600N / 7500Nブリッジの制限と接続ルール

FibreBridge 7600N / 7500Nブリッジを接続する際の制限と考慮事項を確認してください。

FibreBridge 7600N / 7500Nブリッジの制限

- HDDドライブとSSDドライブの組み合わせの最大数は240です。
- SSDドライブの最大数は96です。
- SASポートあたりのSSDの最大数は48です。
- SASポートあたりのシェルフの最大数は10です。

FibreBridge 7600N / 7500Nブリッジ接続ルール

- 同じSASポートにSSDドライブとHDDドライブを混在させないでください。
- シェルフをSASポートに均等に分散します。
- 他のシェルフタイプ（DS212やDS224シェルフなど）と同じSASポートにDS460シェルフを配置しないでください。

設定例

次の例は、SSDドライブを搭載した4台のDS224シェルフとHDDドライブを搭載した6台のDS224シェルフを接続する構成を示しています。

SAS ポート	シェルフとドライブ
SASポートA	SSDを搭載したDS224シェルフ×2
SASポートB	SSDを搭載したDS224シェルフ×2
SASポートC	HDDドライブ搭載のDS224シェルフ×3
SASポートD	HDDドライブ搭載のDS224シェルフ×3

インストールの準備

新しいMetroClusterシステムで使用するブリッジの設置準備を行うときは、システムが一定の要件を満たしていることを確認する必要があります。これには、ブリッジのセットアップや設定の要件と、必要なドキュメント、 ATTO QuickNAV ユーティリティ、ブリッジファームウェアのダウンロードなどがあります。

作業を開始する前に

- システムキャビネットに付属していない場合は、システムをラックに設置しておく必要があります。
- サポートされているハードウェアモデルとソフトウェアバージョンを使用している必要があります。

  で "ネットアップの Interoperability Matrix Tool （ IMT ）"、*[Storage Solution]*フィールドを使用してMetroClusterソリューションを選択できます。コンポーネントエクスプローラ*を使用してコンポーネントとONTAPバージョンを選択し、検索を絞り込むことができます。[Show Results]*を選択すると、条件に一致するサポートされている構成のリストを表示できます。

- 各FCコントローラで、1つのFCポートを1つのブリッジに接続できる必要があります。

- SASケーブルの取り扱い方法、およびディスクシェルフの設置とケーブル接続に関する考慮事項とベストプラクティスを理解しておく必要があります。

  考慮事項とベストプラクティスについては、使用しているディスクシェルフモデルの『 Installation and Service Guide 』を参照してください。

- ブリッジの設定に使用するコンピュータでは、 ATTO ExpressNAV GUI を使用するために、 ATTO でサポートされている Web ブラウザを実行している必要があります。

  ATTO Product Release Notes に、サポートされている Web ブラウザの最新のリストが掲載されています。このドキュメントには、以下の手順で説明する ATTO の Web サイトからアクセスできます。

手順

1. 使用しているディスクシェルフモデルの Installation and Service Guide をダウンロードします。
   a. FibreBridge のモデルに対応するリンクを使用して ATTO の Web サイトにアクセスし、マニュアルと QuickNAV ユーティリティをダウンロードします。

      管理インターフェイスの詳細については、使用しているモデルブリッジに対応した ATTO FibreBridge Installation and Operation Manual を参照してください。

      ATTO FibreBridge の説明ページに記載されているリンクを使用して、このコンテンツや ATTO Web サイト上のその他のコンテンツにアクセスできます。

2. 推奨されるブリッジ管理インターフェイス、 ATTO ExpressNAV GUI および ATTO QuickNAV ユーティリティを使用するために必要なハードウェアおよび情報を収集します。
   a. デフォルト以外のユーザ名とパスワードを決定します（ブリッジへのアクセス用）。

      デフォルトのユーザ名とパスワードは変更してください。

   b. ブリッジの IP 管理を設定する場合は、ブリッジに付属のシールド付きイーサネットケーブル（ブリッジのイーサネット管理 1 ポートとネットワークの接続に使用）が必要です。
   c. ブリッジの IP 管理を設定する場合は、各ブリッジのイーサネット管理 1 ポートの IP アドレス、サブネットマスク、およびゲートウェイの情報が必要です。
   d. セットアップに使用するコンピュータで VPN クライアントを無効にします。

      アクティブな VPN クライアント原因がブリッジの QuickNAV スキャンに失敗しました。

FC-to-SASブリッジおよびSASシェルフの設置

システムが「インストールの準備」のすべての要件を満たしていることを確認したら、新しいシステムをインストールできます。

このタスクについて

- ディスクとシェルフの構成は両方のサイトで同じである必要があります。

  ミラーされていないアグリゲートを使用する場合は、各サイトでディスクとシェルフの構成が異なることがあります。

ミラーされたアグリゲートとミラーされていないアグリゲートのどちらに使用されているかに関係なく、ディザスタリカバリグループ内のディスクはすべて同じタイプの接続を使用し、ディザスタリカバリグループ内のすべてのノードから認識できる必要があります。

- 50ミクロンのマルチモード光ファイバケーブルを使用するディスクシェルフ、FCコントローラ、およびバックアップテープデバイスの最大距離に関するシステム接続要件も、FibreBridgeブリッジに適用されます。

  "NetApp Hardware Universe の略"

次のシェルフと FibreBridge 7500N / 7600N ブリッジでは、追加のケーブル接続なしでインバンド ACP がサポートされます。

- ONTAP 9.2 以降の 7500N または 7600N ブリッジで接続された IOM12 （ DS460C ）
- ONTAP 9.1 以降の 7500N または 7600N ブリッジで接続された IOM12 （ DS212C および DS224C ）

MetroCluster 構成の SAS シェルフでは、 ACP ケーブル接続はサポートされません。

必要に応じて、 **FibreBridge 7600N** ブリッジの **IP** ポートアクセスを有効にします

9.5 より前のバージョンの ONTAP を使用している場合、または Telnet やその他の IP ポートプロトコルおよびサービス（ FTP 、 ExpressNAV 、 ICMP 、 QuickNAV ）を使用して FibreBridge 7600N ブリッジへのアウトオブバンドアクセスを使用する場合は、コンソールポート経由でアクセスサービスを有効にできます。

このタスクについて

ATTO FibreBridge 7500Nブリッジとは異なり、FibreBridge 7600Nブリッジは、すべてのIPポートプロトコルおよびサービスが無効になった状態で出荷されます。

ONTAP 9.5 以降では、ブリッジのインバンド管理 _ がサポートされます。これは、 ONTAP CLI からブリッジへの FC 接続を介してブリッジを設定および監視できることを意味します。ブリッジのイーサネットポートを介してブリッジに物理的にアクセスする必要がなく、ブリッジのユーザインターフェイスも必要ありません。

ONTAP 9.8 以降では、ブリッジの _ 帯域内管理 _ がデフォルトでサポートされ、アウトオブバンド SNMP 管理は廃止されています。

このタスクは、ブリッジの管理にインバンド管理を使用していない場合に必要です。この場合は、イーサネット管理ポートを介してブリッジを設定する必要があります。

手順

1. FibreBridge 7600Nブリッジのシリアルポートにシリアルケーブルを接続して、ブリッジのコンソールインターフェイスにアクセスします。
2. コンソールを使用してアクセスサービスを有効にし、設定を保存します。

   'et closePort none`

   'aveConfiguration'

   'set closePort none' コマンドを使用すると、ブリッジ上のすべてのアクセスサービスがイネーブルになり

ます。

3. 必要に応じて 'set closePort' コマンドを発行し ' 必要に応じてコマンドを繰り返して ' 必要なサービスをすべて無効にします

   'et closePort_service_`

   'set closePort' コマンドは ' 一度に 1 つのサービスを無効にします

   パラメータ「 *SERVICE*` 」は、次のいずれかとして指定できます。

   - エクプレスナヴ
   - FTP
   - ICMP
   - QuickNAV
   - SNMP
   - Telnet

   特定のプロトコルがイネーブルになっているかディセーブルになっているかを確認するには、 get closePort コマンドを使用します。

4. SNMP を有効にする場合は、次の問題コマンドも実行する必要があります。

   'Set SNMP enabled

   SNMP は、別個の enable コマンドを必要とする唯一のプロトコルです。

5. 設定を保存します。

   'aveConfiguration'

FC-to-SASブリッジを設定

モデルに応じた FC-to-SAS ブリッジのケーブル接続に進む前に、 FibreBridge ソフトウェアで設定を行う必要があります。

作業を開始する前に

ブリッジのインバンド管理を使用するかどうかを決めておく必要があります。

> ONTAP 9.8 以降では 'storage bridge コマンドは 'system bridge コマンドに置き換えられました 次の手順は「 storage bridge 」コマンドを示していますが、 ONTAP 9.8 以降を実行している場合は「 system bridge 」コマンドが優先されます。

このタスクについて

IP 管理ではなくブリッジのインバンド管理を使用する場合は、該当する手順に記載されているように、イーサネットポートと IP を設定する手順を省略できます。

手順

1. ATTO FibreBridge のシリアルコンソールポートを設定し、ポート速度を 1 、 000 詐欺検出用に設定します。

```
get serialportbaudrate
SerialPortBaudRate = 115200

Ready.

set serialportbaudrate 115200

Ready. *
saveconfiguration
Restart is necessary....
Do you wish to restart (y/n) ? y
```

2. インバンド管理用に設定する場合は、 FibreBridge RS-232 シリアルポートから PC のシリアル（ COM ）ポートにケーブルを接続します。

   シリアル接続は初期設定と ONTAP によるインバンド管理に使用され、 FC ポートを使用してブリッジの監視と管理を行うことができます。

3. IP 管理用に設定する場合は、イーサネットケーブルを使用して、各ブリッジのイーサネット管理 1 ポートをネットワークに接続します。

   ONTAP 9.5 以降を実行しているシステムでは、インバンド管理を使用してイーサネットポートではなく FC ポート経由でブリッジにアクセスできます。ONTAP 9.8 以降では、インバンド管理のみがサポートされ、 SNMP 管理は廃止されています。

   イーサネット管理 1 ポートを使用すると、ブリッジファームウェアを短時間でダウンロードし（ ATTO ExpressNAV または FTP 管理インターフェイスを使用）、コアファイルと抽出ログを取得できます。

4. IP 管理用に設定する場合は、使用しているブリッジモデルの ATTO FibreBridge Installation and Operation Manual _ のセクション 2.0 の手順に従って、各ブリッジのイーサネット管理 1 ポートを設定します。

   ONTAP 9.5 以降を実行しているシステムでは、インバンド管理を使用してイーサネットポートではなく FC ポート経由でブリッジにアクセスできます。ONTAP 9.8 以降では、インバンド管理のみがサポートされ、 SNMP 管理は廃止されています。

   QuickNAV を実行してイーサネット管理ポートを設定すると、イーサネットケーブルで接続されているイーサネット管理ポートのみが設定されます。たとえば、イーサネット管理 2 ポートも設定する場合は、イーサネットケーブルをポート 2 に接続して QuickNAV を実行する必要があります。

5. ブリッジを設定します。

   指定するユーザ名とパスワードは必ずメモしてください。

   > ATTO FibreBridge 7600N または 7500N では時刻同期は設定しないでください。ATTO FibreBridge 7600N または 7500N の時刻は、 ONTAP でブリッジが検出されたあとにクラスタ時間に設定されます。また、 1 日に 1 回定期的に同期されます。使用されるタイムゾーンは GMT で、変更することはできません。

   a. IP 管理用に設定する場合は、ブリッジの IP 設定を行います。

ONTAP 9.5 以降を実行しているシステムでは、インバンド管理を使用してイーサネットポートではなく FC ポート経由でブリッジにアクセスできます。ONTAP 9.8 以降では、インバンド管理のみがサポートされ、 SNMP 管理は廃止されています。

Quicknav ユーティリティなしで IP アドレスを設定するには、 FibreBridge に対するシリアル接続が必要です。

CLI を使用する場合は、次のコマンドを実行する必要があります。

'set ipaddress mp1 ip-address

'set ipsubnetmask mp1 subnet-mask

'set ipgateway mp1x.x'

'set ipdhcp mp1 disabled

「 setethernetspeed mp1 1000」

b. ブリッジ名を設定します。

ブリッジ名は、 MetroCluster 構成内でそれぞれ一意である必要があります。

各サイトの 1 つのスタックグループのブリッジ名の例：

- bridge_A_1a
- bridge_A_1b
- bridge_B_1a
- bridge_B_1b

CLI を使用する場合は、次のコマンドを実行する必要があります。

```
set bridgename <bridge_name>
```

c. ONTAP 9.4 以前を実行している場合は、ブリッジで SNMP を有効にします。

'Set SNMP enabled

ONTAP 9.5 以降を実行しているシステムでは、インバンド管理を使用してイーサネットポートではなく FC ポート経由でブリッジにアクセスできます。ONTAP 9.8 以降では、インバンド管理のみがサポートされ、 SNMP 管理は廃止されています。

6. ブリッジの FC ポートを設定します。

a. ブリッジ FC ポートのデータ速度を設定します。

サポートされる FC データ速度は、モデルブリッジによって異なります。

- FibreBridge 7600Nブリッジは、最大32、16、または8Gbpsをサポートします。
- FibreBridge 7500Nブリッジは、最大16、8、または4Gbpsをサポートします。

選択できる FCDataRate の速度は、ブリッジポートを接続するコントローラモジュールのブリッジ / FC ポートの両方でサポートされる最大速度以下です。ケーブルでの接続距離が SFP およびその他のハードウェアの制限を超えないようにしてください。

CLI を使用する場合は、次のコマンドを実行する必要があります。

```
set FCDataRate <port-number> <port-speed>
```

b. FibreBridge 7500Nブリッジを設定する場合は、ポートで使用する接続モードを「ptp」に設定します。

FibreBridge 7600N ブリッジを設定する場合、 FCConnMode の設定は不要です。

CLI を使用する場合は、次のコマンドを実行する必要があります。

```
set FCConnMode <port-number> ptp
```

c. FibreBridge 7600N / 7500N ブリッジを設定する場合は、 FC2 ポートを設定または無効にする必要があります。

- 2 番目のポートを使用する場合は、 FC2 ポートについて同じ手順を繰り返す必要があります。
- 2 番目のポートを使用しない場合は、ポートを無効にする必要があります。

```
FCPortDisable <port-number>
```

次に、 FC ポート 2 を無効にする例を示します。

```
FCPortDisable 2

Fibre Channel Port 2 has been disabled.
```

a. FibreBridge 7600N / 7500N ブリッジを設定する場合は、未使用の SAS ポートを無効にします。

'ASPortDisable_SAS-PORT_'

SAS ポート A~D はデフォルトで有効になります。使用していない SAS ポートを無効にする必要があります。

SAS ポート A のみを使用している場合は、 SAS ポート B 、 C 、および D を無効にする必要があります。次の例は、 SAS ポート B を無効にしていますSAS ポート C および D についても、同じように無効にする必要があります。

```
SASPortDisable b

SAS Port B has been disabled.
```

7. ブリッジへのアクセスを保護し、ブリッジの設定を保存します。システムで実行している ONTAP のバー

ジョンに応じて、次のいずれかのオプションを選択します。

ONTAP バージョン	手順
• ONTAP 9.5 以降 *	a. ブリッジのステータスを表示します。 「 storage bridge show 」 出力には、保護されていないブリッジが表示されます。 b. ブリッジを保護します。 「 ecurebridge 」
• ONTAP 9.4 以前 *	a. ブリッジのステータスを表示します。 「 storage bridge show 」 出力には、保護されていないブリッジが表示されます。 b. セキュリティ保護されていないブリッジのポートのステータスを確認します。 「 info 」のようになります 出力には、イーサネットポート MP1 と MP2 のステータスが表示されます。 c. イーサネットポート MP1 がイネーブルの場合、次のコマンドを実行します。 「 Set EthernetPort mp1 disabled 」です イーサネットポート MP2 も有効になっている場合は、ポート MP2 について前の手順を繰り返します。 d. ブリッジの設定を保存します。 次のコマンドを実行する必要があります。 'aveConfiguration' 「 FirmwareRestart 」と入力します ブリッジを再起動するように求められます。

8. MetroCluster の設定が完了したら、「 flashimages 」コマンドを使用して FibreBridge ファームウェアのバージョンを確認し、ブリッジが最新のサポート対象バージョンを使用していない場合は構成内のすべてのブリッジのファームウェアを更新します。

   "MetroCluster コンポーネントの保守"

ブリッジを設定したら、新しいシステムのケーブル接続を開始できます。

このタスクについて

ディスクシェルフの場合は、 SAS ケーブルのコネクタをプルタブ（コネクタの下側）を下にして挿入します。

手順

1. 各スタックのディスクシェルフをデイジーチェーン接続します。

   a. スタック内の論理的に最初のシェルフから、IOM Aのポート3をに接続し、スタック内の各IOM Aを接続するまで次のシェルフのIOM Aのポート1に接続します。

   b. IOM B について、同じ手順を繰り返します

   c. 各スタックについて、同じ手順を繰り返します。

   ディスクシェルフのデイジーチェーン接続の詳細については、使用しているディスクシェルフモデルの Installation and Service Guide を参照してください。

2. ディスクシェルフの電源をオンにし、シェルフ ID を設定します。

   ◦ 各ディスクシェルフの電源を再投入する必要があります。

   ◦ 各 MetroCluster DR グループ（両サイトを含む）で、各 SAS ディスクシェルフのシェルフ ID が一意である必要があります。

3. ディスクシェルフを FibreBridge ブリッジにケーブル接続します。

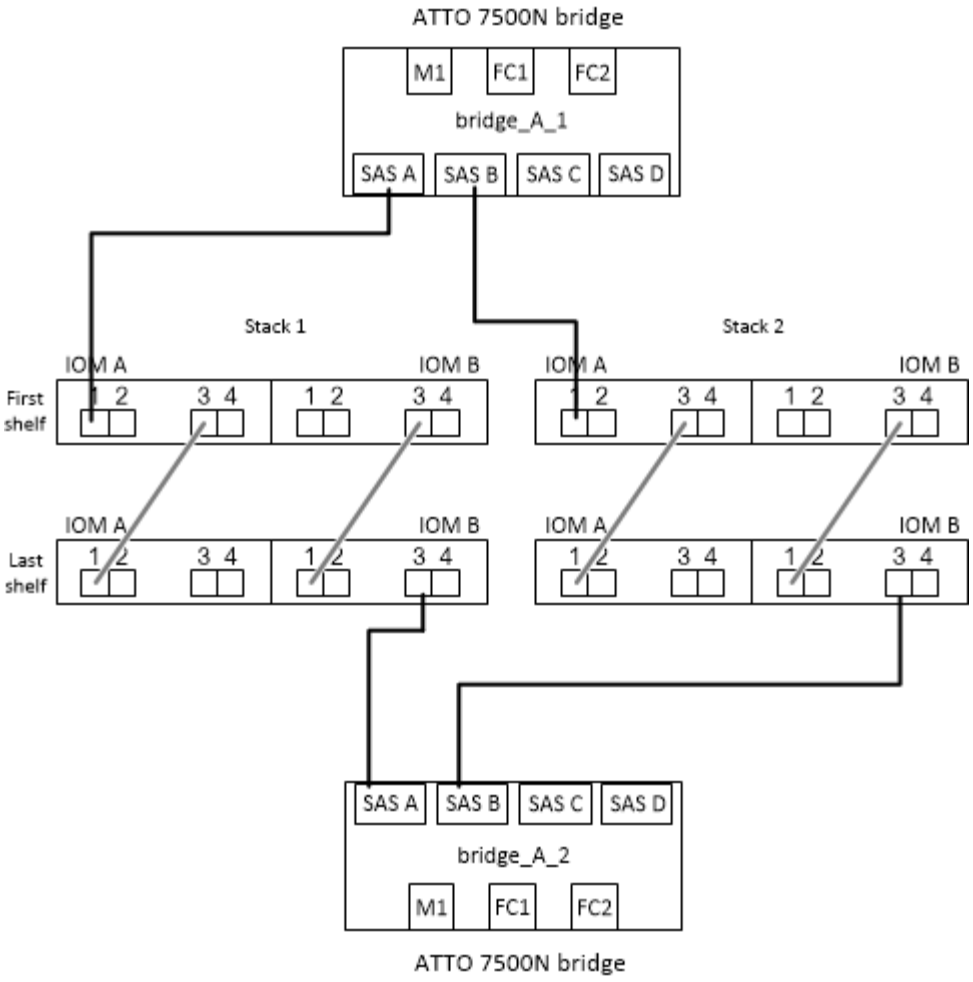
   a. ディスクシェルフの最初のスタックで、最初のシェルフの IOM A を FibreBridge A の SAS ポート A にケーブル接続し、最後のシェルフの IOM B を FibreBridge B の SAS ポート A にケーブル接続します

   b. 残りのシェルフスタックについて、 FibreBridge ブリッジの次に使用可能な SAS ポートを使用して同じ手順を繰り返します。 2 番目のスタックにはポート B 、 3 番目のスタックにはポート C 、 4 番目のスタックにはポート D を使用します。

   c. ケーブル接続中、IOM12 モジュールに基づくスタックは、別々の SAS ポートに接続されている限り、同じブリッジに接続します。

   それぞれのスタックで異なる IOM モデルを使用できますが、スタック内ではすべてのディスクシェルフで同じモデルを使用する必要があります。

   次の図は、 1 組の FibreBridge 7600N / 7500N ブリッジにディスクシェルフが接続された状態を示しています。



ブリッジの接続を確認し、**FC-to-SAS**ブリッジをコントローラの**FC**ポートにケーブル接続します。

2ノードブリッジ接続MetroCluster構成では、ブリッジをコントローラのFCポートにケーブル接続する必要があります。

手順

1. 各ブリッジで、ブリッジが接続されているすべてのディスクドライブおよびディスクシェルフが検出されることを確認します。

   「 astargets 」

   「 astargets 」コマンドの出力には、ブリッジに接続されているデバイス（ディスクおよびディスクシェルフ）が表示されます。出力行には行番号が振られているため、デバイスの台数を簡単に把握できます。

   次の出力は、 10 本のディスクが接続されていることを示します。

```
Tgt VendorID ProductID         Type        SerialNumber
  0 NETAPP   X410_S15K6288A15 DISK        3QP1CLE300009940UHJV
  1 NETAPP   X410_S15K6288A15 DISK        3QP1ELF600009940V1BV
  2 NETAPP   X410_S15K6288A15 DISK        3QP1G3EW00009940U2M0
  3 NETAPP   X410_S15K6288A15 DISK        3QP1EWMP00009940U1X5
  4 NETAPP   X410_S15K6288A15 DISK        3QP1FZLE00009940G8YU
  5 NETAPP   X410_S15K6288A15 DISK        3QP1FZLF00009940TZKZ
  6 NETAPP   X410_S15K6288A15 DISK        3QP1CEB400009939MGXL
  7 NETAPP   X410_S15K6288A15 DISK        3QP1G7A900009939FNTT
  8 NETAPP   X410_S15K6288A15 DISK        3QP1FY0T00009940G8PA
  9 NETAPP   X410_S15K6288A15 DISK        3QP1FXW600009940VERQ
```

2. コマンド出力で、ブリッジがスタック内の正しいディスクおよびディスクシェルフに接続されていることを確認します。

出力結果	作業
正解です	繰り返します 手順 1. 残りの各ブリッジ。
不正解です	a. SAS ケーブルに緩みがないか確認するか、ディスクシェルフからブリッジへの SAS ケーブル接続をやり直します。 FibreBridge 7600N / 7500Nブリッジを IOM12モジュールを使用してディスクシェルフとケーブル接続 b. 繰り返します 手順 1. 残りの各ブリッジ。

3. [[step3-cable-each-bridge]各ブリッジをコントローラのFCポートにケーブル接続します。

   a. ブリッジのFCポート1をcluster_Aのコントローラの FCポートにケーブル接続します。

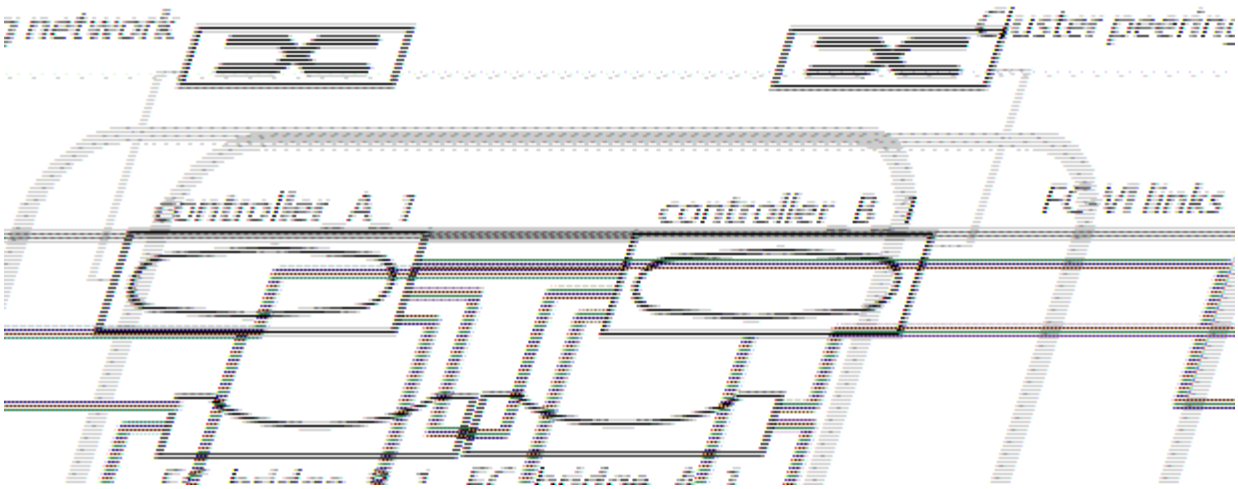
   b. ブリッジのFCポート2をcluster_Bのコントローラ上の FCポートにケーブル接続します。

      - コントローラにクアッドポートFCアダプタが設定されている場合は、ストレージスタックの両端にあるブリッジが同じASICの2つのFCポートに接続されていないことを確認してください。例：
        - ポートaとポートbは同じASICを共有します。
        - ポートcとポートdは同じASICを共有します。

          この例では、FC_bridge_A_1をポートAに接続し、FC_bridge_A2をポートCに接続します。

      - コントローラに複数のFCアダプタが設定されている場合は、ストレージスタックのどちらかの端にあるブリッジを同じアダプタにケーブル接続しないでください。

        このシナリオでは、FC_bridge_A_1をオンボードのFCポートに接続し、FC_bridge_A_2を拡張スロットのアダプタのFCポートに接続します。



4. 繰り返します 手順 3 他のブリッジについて、すべてのブリッジがケーブル接続されるまで。

FibreBridge ブリッジをセキュリティ保護または保護解除します

安全性に問題のあるイーサネットプロトコルをブリッジで簡単に無効にできるように、 ONTAP 9.5 以降ではブリッジを保護することができます。これにより、ブリッジのイーサネットポートが無効になります。イーサネットアクセスを再度有効にすることもできます。

このタスクについて

- ブリッジをセキュリティ保護すると、ブリッジの Telnet とその他の IP ポートプロトコルおよびサービス（ FTP 、 ExpressNAV 、 ICMP 、 QuickNAV ）が無効になります。
- この手順では、 ONTAP 9.5 以降で使用可能な ONTAP プロンプトを使用したアウトオブバンド管理を使用します。

  アウトオブバンド管理を使用していない場合は、ブリッジの CLI からコマンドを問題できます。

- 「 unsecurebridge 」コマンドを使用して、イーサネットポートを再度イネーブルにできます。
- ONTAP 9.7 以前では、 ATTO FibreBridge で「 ecurebridge 」コマンドを実行すると、パートナークラスタでブリッジステータスが正しく更新されない可能性がありました。この場合は、パートナークラスタから「 ecurebridge 」コマンドを実行します。

ONTAP 9.8 以降では 'storage bridge コマンドは 'system bridge コマンドに置き換えられました次の手順は「 storage bridge 」コマンドを示していますが、 ONTAP 9.8 以降を実行している場合は「 system bridge 」コマンドが優先されます。

手順

1. ブリッジを含むクラスタの ONTAP プロンプトで、ブリッジのセキュリティ保護を設定または解除します。
   - 次のコマンドは、 bridge_A_1 をセキュリティ保護します。

     'cluster_a> storage bridge run-cli -bridge bridge_A_1 コマンド securebridge `

   - 次のコマンドは、 bridge_A_1 のセキュリティ保護を解除します。

'cluster_a> storage bridge run-cli -bridge bridge_A_1 コマンド unsecurebridge

2. ブリッジを含むクラスタの ONTAP プロンプトで、ブリッジの設定を保存します。

   `storage bridge run-cli -bridge <bridge-name> -command saveconfiguration`

   次のコマンドは、 bridge_A_1 をセキュリティ保護します。

   'cluster_a > storage bridge run -cli -bridge bridge_A_1 - コマンド保存構成

3. ブリッジを含むクラスタの ONTAP プロンプトから、ブリッジのファームウェアを再起動します。

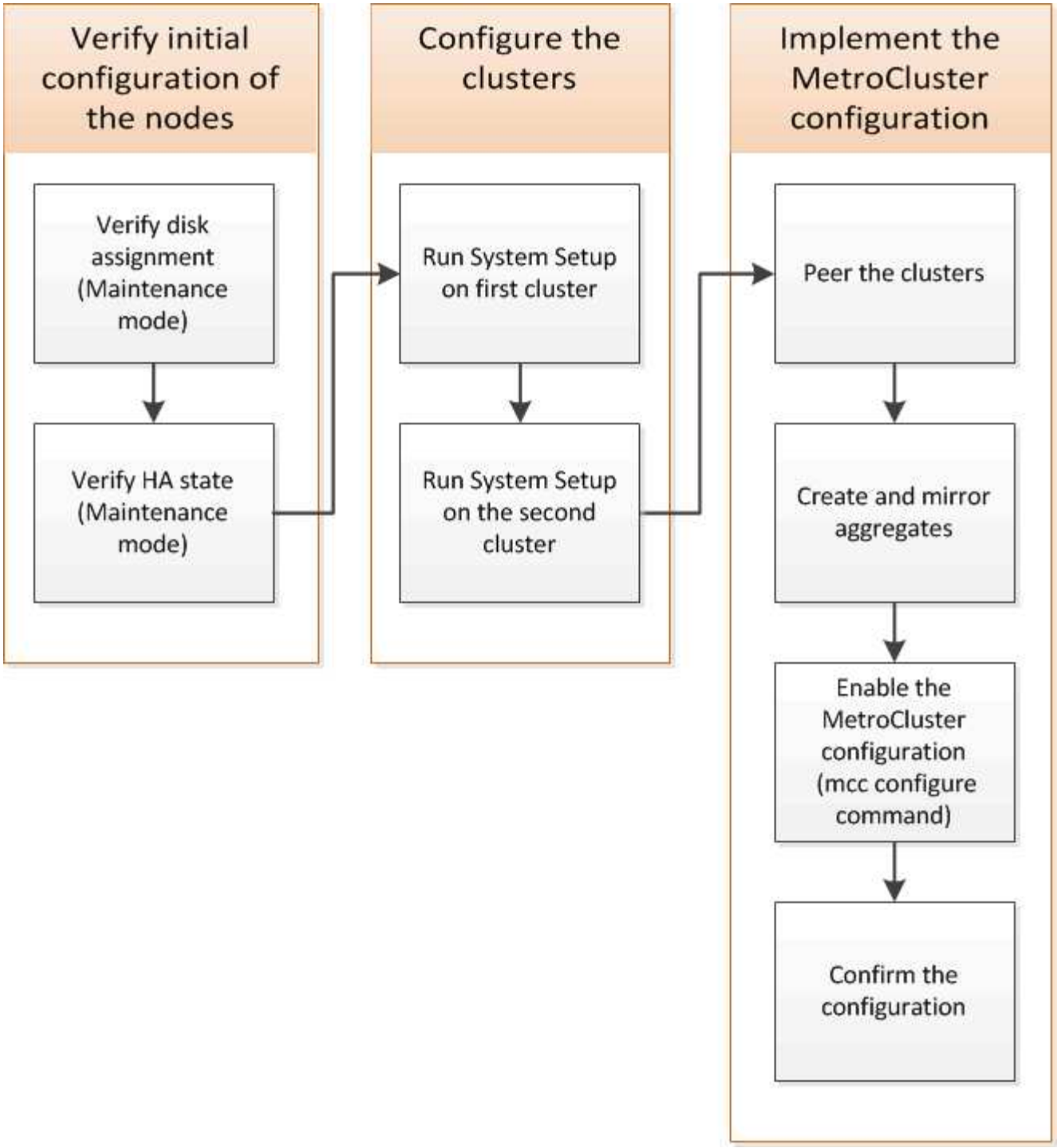
   `storage bridge run-cli -bridge <bridge-name> -command firmwarerestart`

   次のコマンドは、 bridge_A_1 をセキュリティ保護します。

   'cluster_a > storage bridge run-cli -bridge bridge_A_1 - コマンド firmwareerestart'

ONTAP での MetroCluster ソフトウェアの設定

MetroCluster 構成の各ノードは、ノードレベルの設定や 2 つのサイトへのノードの設定を含めて、 ONTAP で設定する必要があります。また、 2 つのサイト間に MetroCluster 関係を実装する必要があります。



手順

1. 設定プロセスを開始する前に、コントローラモジュールに必要な IP アドレスを収集します。
2. サイト A の IP ネットワーク情報ワークシートに記入

サイト **A** の **IP** ネットワーク情報ワークシート

システムを設定する前に、最初の MetroCluster サイト（サイト A ）の IP アドレスその他のネットワーク情報を、ネットワーク管理者から入手する必要があります。

クラスタ作成情報：サイト **A**

クラスタを初めて作成するときは、次の情報が必要です。

情報のタイプ	値を入力します
クラスタ名。この情報で使用している例： site_A	
DNS ドメイン	
DNS ネームサーバ	
場所	
管理者パスワード	

ノード情報：サイト **A**

クラスタ内のノードごとに、管理 IP アドレス、ネットワークマスク、およびデフォルトゲートウェイが必要です。

ノード	ポート	IP アドレス	ネットワークマスク	デフォルトゲートウェイ
ノード 1 ：この情報で使用している例： controller_A_1				
ノード 2 ：2 ノード MetroCluster 構成（サイトごとに 1 つのノード）を使用している場合は不要 この情報で使用している例： controller_A_2				

クラスタピアリング用の **LIF** およびポート：サイト **A**

クラスタ内のノードごとに、 2 つのクラスタ間 LIF の IP アドレス、ネットワークマスク、およびデフォルトゲートウェイが必要です。クラスタ間 LIF は、クラスタのピアリングに使用されます。

ノード	ポート	クラスタ間 LIF の IP アドレス	ネットワークマスク	デフォルトゲートウェイ
ノード 1 IC LIF 1				

ノード 1 IC LIF 2				

タイムサーバ情報：サイト **A**

時間を同期する必要があります。これには 1 台以上の NTP タイムサーバが必要です。

ノード	ホスト名	IP アドレス	ネットワークマスク	デフォルトゲートウェイ
NTP サーバ 1				
NTP サーバ 2				

サイト**A nbsp；AutoSupport** 情報

各ノードで AutoSupport を設定する必要があります。これには次の情報が必要です。

情報のタイプ		値を入力します
送信元 E メールアドレス		メールホスト
IP アドレスまたは名前		転送プロトコル
HTTP 、 HTTPS 、または SMTP		プロキシサーバ
	受信者の E メールアドレスまたは配信リスト	メッセージ全文
	簡潔なメッセージ	

SP 情報：サイト **A**

トラブルシューティングとメンテナンスのために、各ノードのサービスプロセッサ（ SP ）へのアクセスを有効にする必要があります。そのためには、各ノードについて次のネットワーク情報が必要です。

ノード	IP アドレス	ネットワークマスク	デフォルトゲートウェイ
ノード 1			

サイト **B** の **IP** ネットワーク情報ワークシート

システムを設定する前に、 2 つ目の MetroCluster サイト（サイト B ）の IP アドレスその他のネットワーク情報を、ネットワーク管理者から入手する必要があります。

クラスタ作成情報：サイト **B**

クラスタを初めて作成するときは、次の情報が必要です。

情報のタイプ	値を入力します
クラスタ名。この情報で使用している例： site_B	
DNS ドメイン	
DNS ネームサーバ	
場所	
管理者パスワード	

ノード情報：サイト **B**

クラスタ内のノードごとに、管理 IP アドレス、ネットワークマスク、およびデフォルトゲートウェイが必要です。

ノード	ポート	IP アドレス	ネットワークマスク	デフォルトゲートウェイ
ノード 1 ：この情報で使用している例： controller_B_1				
ノード 2 ：2 ノード MetroCluster 構成（サイトごとに 1 つのノード）の場合は不要 この情報で使用している例： controller_B_2				

クラスタピアリング用の **LIF** およびポート：サイト **B**

クラスタ内のノードごとに、 2 つのクラスタ間 LIF の IP アドレス、ネットワークマスク、およびデフォルトゲートウェイが必要です。クラスタ間 LIF は、クラスタのピアリングに使用されます。

ノード	ポート	クラスタ間 LIF の IP アドレス	ネットワークマスク	デフォルトゲートウェイ
ノード 1 IC LIF 1				

ノード 1 IC LIF 2				

タイムサーバ情報：サイト **B**

時間を同期する必要があります。これには 1 台以上の NTP タイムサーバが必要です。

ノード	ホスト名	IP アドレス	ネットワークマスク	デフォルトゲートウェイ
NTP サーバ 1				
NTP サーバ 2				

サイト**B nbsp；AutoSupport** 情報

各ノードで AutoSupport を設定する必要があります。これには次の情報が必要です。

情報のタイプ		値を入力します
送信元 E メールアドレス		メールホスト
IP アドレスまたは名前		転送プロトコル
HTTP 、 HTTPS 、または SMTP		プロキシサーバ
	受信者の E メールアドレスまたは配信リスト	メッセージ全文
	簡潔なメッセージ	

サイト**B nbsp；SP**情報

トラブルシューティングとメンテナンスのために、各ノードのサービスプロセッサ（ SP ）へのアクセスを有効にする必要があります。これには、ノードごとに次のネットワーク情報が必要です。

ノード	IP アドレス	ネットワークマスク	デフォルトゲートウェイ
ノード 1 （ controller_B_1 ）			

標準クラスタ構成と **MetroCluster** 構成の類似点 **/** 相違点

MetroCluster 構成の各クラスタのノードの構成は、標準クラスタのノードと似ています。

MetroCluster 構成は、 2 つの標準クラスタを基盤としています。構成は物理的に対称な構成である必要があり、各ノードのハードウェア構成が同じで、すべての MetroCluster コンポーネントがケーブル接続され、設

定されている必要があります。ただし、 MetroCluster 構成のノードの基本的なソフトウェア設定は、標準クラスタのノードと同じです。

設定手順	標準クラスタ構成	MetroCluster の設定
各ノードで管理 LIF 、クラスタ LIF 、データ LIF を設定。	両方のクラスタタイプで同じです	ルートアグリゲートを設定
両方のクラスタタイプで同じです	クラスタ内の一方のノードでクラスタを設定。	両方のクラスタタイプで同じです
もう一方のノードをクラスタに追加。	両方のクラスタタイプで同じです	ミラーされたルートアグリゲートを作成
任意。	必須	クラスタをピアリング。
任意。	必須	MetroCluster 設定を有効にします。

システムのデフォルト設定をリストアし、コントローラモジュールで **HBA** タイプを設定しています

MetroCluster を正しくインストールするには、コントローラモジュールのデフォルトをリセットしてリストアします。

重要

このタスクを実行する必要があるのは、 FC-to-SAS ブリッジを使用するストレッチ構成のみです。

手順

1. LOADER プロンプトで環境変数をデフォルト設定に戻します。

   「デフォルト設定」

2. ノードをメンテナンスモードでブートし、システム内の HBA の設定を行います。

   a. メンテナンスモードでブートします。

      「 boot_ontap maint 」を使用してください

   b. ポートの現在の設定を確認します。

      ucadmin show

   c. 必要に応じてポートの設定を更新します。

HBA のタイプと目的のモード	使用するコマンド
CNA FC	ucadmin modify -m fc -t initiator_adapter_name _ `

CNA イーサネット	ucadmin modify -mode cna_adapter_name _ `
FC ターゲット	fcadmin config -t target_adapter_name _`
FC イニシエータ	fcadmin config -t initiator_adapter_name_`

3. メンテナンスモードを終了します。

   「 halt 」

   コマンドの実行後、ノードが LOADER プロンプトで停止するまで待ちます。

4. ノードをブートしてメンテナンスモードに戻り、設定の変更が反映されるようにします。

   「 boot_ontap maint 」を使用してください

5. 変更内容を確認します。

HBA のタイプ	使用するコマンド
CNA	ucadmin show
FC	fcadmin show`

6. メンテナンスモードを終了します。

   「 halt 」

   コマンドの実行後、ノードが LOADER プロンプトで停止するまで待ちます。

7. ノードをブートメニューでブートします。

   「 boot_ontap menu

   コマンドの実行後、ブートメニューが表示されるまで待ちます。

8. ブートメニュープロンプトで「 wipeconfig 」と入力してノード設定をクリアし、 Enter キーを押します。

   次の画面はブートメニューのプロンプトを示しています。

```
Please choose one of the following:

     (1) Normal Boot.
     (2) Boot without /etc/rc.
     (3) Change password.
     (4) Clean configuration and initialize all disks.
     (5) Maintenance mode boot.
     (6) Update flash from backup config.
     (7) Install new software first.
     (8) Reboot node.
     (9) Configure Advanced Drive Partitioning.
     Selection (1-9)?  wipeconfig
 This option deletes critical system configuration, including cluster
membership.
 Warning: do not run this option on a HA node that has been taken over.
 Are you sure you want to continue?: yes
 Rebooting to finish wipeconfig request.
```

FAS8020 システムでの X1132A-R6 クアッドポートカードの FC-VI ポートの設定

FAS8020 システムで X1132A-R6 クアッドポートカードを使用している場合は、メンテナンスモードに切り替えて、ポート 1a / 1b を FC-VI およびイニシエータ用に使用するように設定できます。工場出荷状態の MetroCluster システムでは、構成に応じて適切にポートが設定されているため、この設定は必要ありません。

このタスクについて

このタスクはメンテナンスモードで実行する必要があります。

ucadmin コマンドを使用した FC ポートの FC-VI ポートへの変換は、 FAS8020 および AFF 8020 システムでのみサポートされます。他のプラットフォームでは、 FC ポートを FCVI ポートに変換することはできません。

手順

1. ポートを無効にします。

   「ストレージ無効化アダプタ 1a 」

   「ストレージ無効化アダプタ 1b'

```
*> storage disable adapter 1a
Jun 03 02:17:57 [controller_B_1:fci.adapter.offlining:info]: Offlining
Fibre Channel adapter 1a.
Host adapter 1a disable succeeded
Jun 03 02:17:57 [controller_B_1:fci.adapter.offline:info]: Fibre Channel
adapter 1a is now offline.
*> storage disable adapter 1b
Jun 03 02:18:43 [controller_B_1:fci.adapter.offlining:info]: Offlining
Fibre Channel adapter 1b.
Host adapter 1b disable succeeded
Jun 03 02:18:43 [controller_B_1:fci.adapter.offline:info]: Fibre Channel
adapter 1b is now offline.
*>
```

2. ポートが無効になっていることを確認します。

   ucadmin show

```
*> ucadmin show
         Current  Current    Pending  Pending    Admin
Adapter  Mode     Type       Mode     Type       Status
-------  -------  ---------  -------  ---------  -------
  ...
  1a     fc       initiator  -        -          offline
  1b     fc       initiator  -        -          offline
  1c     fc       initiator  -        -          online
  1d     fc       initiator  -        -          online
```

3. ポート a とポート b を FC-VI モードに設定します。

   ucadmin modify -adapter 1a -type FCVI`

   このコマンドでは、 1a だけを指定した場合でも、ポートペアの両方のポート 1a と 1b のモードが設定されます。

```
*> ucadmin modify -t fcvi 1a
Jun 03 02:19:13 [controller_B_1:ucm.type.changed:info]: FC-4 type has
changed to fcvi on adapter 1a. Reboot the controller for the changes to
take effect.
Jun 03 02:19:13 [controller_B_1:ucm.type.changed:info]: FC-4 type has
changed to fcvi on adapter 1b. Reboot the controller for the changes to
take effect.
```

4. 変更が保留中であることを確認します。

ucadmin show

```
*> ucadmin show
         Current  Current    Pending  Pending    Admin
Adapter  Mode     Type       Mode     Type       Status
-------  -------  ---------  -------  ---------  -------
  ...
  1a     fc       initiator  -        fcvi       offline
  1b     fc       initiator  -        fcvi       offline
  1c     fc       initiator  -        -          online
  1d     fc       initiator  -        -          online
```

5. コントローラをシャットダウンし、メンテナンスモードでリブートします。
6. 設定の変更を確認します。

ucadmin show local

```
Node           Adapter  Mode     Type       Mode     Type       Status
------------   -------  -------  ---------  -------  ---------
-----------
...
controller_B_1
               1a       fc       fcvi       -        -          online
controller_B_1
               1b       fc       fcvi       -        -          online
controller_B_1
               1c       fc       initiator  -        -          online
controller_B_1
               1d       fc       initiator  -        -          online
6 entries were displayed.
```

保守モードでの 2 ノード構成のディスク割り当ての検証

システムを ONTAP で完全にブートする前に、システムをメンテナンスモードでブートして、ノードのディスク割り当てを確認することもできます。ディスクは、両方のサイトが独自のディスクシェルフを所有してデータを提供し、各ノードおよび各プールのミラーディスク数が等しい、完全に対称な構成を形成するように割り当てられている必要があります。

作業を開始する前に

システムをメンテナンスモードにする必要があります。

このタスクについて

新しい MetroCluster システムの場合、出荷前にディスク割り当てが完了しています。

次の表に、 MetroCluster 構成のプール割り当ての例を示します。ディスクはシェルフ単位でプールに割り当

てられます。

ディスクシェルフ（ _ 例名 _ ） …	サイト	所属ノード	割り当てプール
ディスクシェルフ 1 （ shelf_A_1_1 ）	サイト A	ノード A1	プール 0
ディスクシェルフ 2 （ shelf_A_1_3 ）	ディスクシェルフ 3 （ shelf_B_1_1 ）	ノード B1	プール 1.
ディスクシェルフ 4 （ shelf_B_1_3 ）	ディスクシェルフ 9 （ shelf_B_1_2 ）	サイト B	ノード B1
プール 0	ディスクシェルフ 10 （ shelf_B_1_4 ）	ディスクシェルフ 11 （ shelf_A_1_2 ）	ノード A1

構成に DS460C ディスクシェルフが含まれている場合は、それぞれの 12 ディスクドロワーについて、次のガイドラインに従ってディスクを手動で割り当てる必要があります。

ドロワーのディスク	ノードとプール
1 ~ 6	ローカルノードのプール 0
7-12	DR パートナーのプール 1

このディスク割り当てパターンに従うことで、ドロワーがオフラインになった場合のアグリゲートへの影響を最小限に抑えることができます。

手順

1. 工場出荷状態のシステムの場合は、シェルフの割り当てを確認します。

   「 Disk show – v 」のように表示されます

2. 必要に応じて、接続されているディスクシェルフ上のディスクを適切なプールに明示的に割り当てることができます

   「ディスク割り当て」

   ノードと同じサイトにあるディスクシェルフはプール 0 に割り当て、パートナーサイトにあるディスクシェルフはプール 1 に割り当てます。各プールに同じ数のシェルフを割り当てる必要があります。

   a. システムをブートしていない場合は、メンテナンスモードでブートします。
   b. サイト A のノードで、ローカルディスクシェルフをプール 0 に、リモートディスクシェルフをプール 1 に割り当てます。 `+disk assign -shelf_disk_shelf_name_-p_pool_`

      ストレージコントローラ node_A_1 にシェルフが 4 台ある場合は、次のコマンドを問題できます。

```
*> disk assign -shelf shelf_A_1_1 -p 0
*> disk assign -shelf shelf_A_1_3 -p 0

*> disk assign -shelf shelf_A_1_2 -p 1
*> disk assign -shelf shelf_A_1_4 -p 1
```

c. リモートサイト（サイト B ）のノードで、ローカルディスクシェルフをプール 0 に、リモートディスクシェルフをプール 1 に割り当てます。 +disk assign -shelf_disk_shelf_name_-p_pool_

ストレージコントローラ node_B_1 にシェルフが 4 台ある場合は、次のコマンドを問題に設定します。

```
*> disk assign -shelf shelf_B_1_2   -p 0
*> disk assign -shelf shelf_B_1_4  -p 0

*> disk assign -shelf shelf_B_1_1 -p 1
 *> disk assign -shelf shelf_B_1_3 -p 1
```

a. 各ディスクのディスク・シェルフ ID とベイを表示します +disk show – v

コンポーネントの HA 状態の確認

工場出荷時に事前設定されていないストレッチ MetroCluster 構成では、コントローラおよびシャーシのコンポーネントの HA の状態が「 mcc-2n 」に設定されていることを確認し、適切にブートする必要があります。工場出荷状態のシステムでは事前に設定されているため、検証は不要です。

作業を開始する前に

システムをメンテナンスモードにする必要があります。

手順

1. メンテナンスモードで、コントローラモジュールとシャーシの HA 状態を表示します。

「 ha-config show 」

コントローラモジュールとシャーシには「 mcc-2n 」という値が表示されます。

2. 表示されたコントローラのシステム状態が「 mcc-2n 」でない場合は、コントローラの HA 状態を設定します。

「 ha-config modify controller mcc-2n 」という形式で指定します

3. 表示されたシャーシのシステム状態が「 mcc-2n 」でない場合は、シャーシの HA 状態を設定します。

「 ha-config modify chassis mcc-2n 」というようになりました

ノードを停止します。

ノードが LOADER プロンプトに戻るまで待ちます。

4. MetroCluster 構成の各ノードで、上記の手順を繰り返します。

2 ノード MetroCluster 構成での ONTAP のセットアップ

2 ノード MetroCluster 構成では、各クラスタでノードをブートし、クラスタセットアップウィザードを終了し、「 cluster setup 」コマンドを使用してノードをシングルノードクラスタに構成する必要があります。

作業を開始する前に

サービスプロセッサが設定されていないことを確認してください。

このタスクについて

このタスクは、ネットアップの標準のストレージを使用した 2 ノード MetroCluster 構成が対象です。

このタスクは、 MetroCluster 構成の両方のクラスタで実行する必要があります。

ONTAP のセットアップに関するその他の一般的な情報については、を参照してください "ONTAP をセットアップします"

手順

1. 最初のノードの電源をオンにします。

   この手順はディザスタリカバリ（ DR ）サイトのノードでも実行する必要があります。

   ノードがブートし、 AutoSupport が自動的に有効になることを示すクラスタセットアップウィザードがコンソールで起動されます。

```
::> Welcome to the cluster setup wizard.

You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the cluster setup wizard.
     Any changes you made before quitting will be saved.

You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.

This system will send event messages and periodic reports to NetApp
Technical
Support. To disable this feature, enter
autosupport modify -support disable
within 24 hours.

Enabling AutoSupport can significantly speed problem determination and
resolution, should a problem occur on your system.
For further information on AutoSupport, see:
http://support.netapp.com/autosupport/

Type yes to confirm and continue {yes}: yes

Enter the node management interface port [e0M]:
Enter the node management interface IP address [10.101.01.01]:

Enter the node management interface netmask [101.010.101.0]:
Enter the node management interface default gateway [10.101.01.0]:



Do you want to create a new cluster or join an existing cluster?
{create, join}:
```

2. 新しいクラスタを作成します。

   「 create 」

3. ノードをシングルノードクラスタとして使用するかどうかを選択します。

```
Do you intend for this node to be used as a single node cluster? {yes,
no} [yes]:
```

4. Enter キーを押してシステムのデフォルトの "yes" をそのまま使用するか ' または "no`" と入力してから

Enter キーを押して独自の値を入力します

5. プロンプトに従って * Cluster Setup * ウィザードを完了し、 Enter キーを押してデフォルト値をそのまま使用するか、独自の値を入力して Enter キーを押します。

   デフォルト値は、プラットフォームとネットワークの構成に基づいて自動的に決定されます。

6. クラスタセットアップ * ウィザードが完了したら、次のコマンドを入力して、クラスタがアクティブで、第 1 ノードが正常に機能していることを確認します。

   「 cluster show 」を参照してください

   次の例は、第 1 ノードが含まれるクラスタ（ cluster1-01 ）が正常に機能しており、クラスタへの参加条件を満たしていることを示しています。

```
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
cluster1-01           true    true
```

   管理 SVM またはノード SVM に対して入力した設定のいずれかを変更する必要がある場合は 'cluster setup コマンドを使用してクラスタセットアップ * ウィザードにアクセスできます

クラスタを MetroCluster 構成に設定

クラスタをピアリングし、ルートアグリゲートをミラーリングし、ミラーリングされたデータアグリゲートを作成し、コマンドを問題して MetroCluster の処理を実装する必要があります。

クラスタをピアリング

MetroCluster 構成内のクラスタが相互に通信し、 MetroCluster ディザスタリカバリに不可欠なデータミラーリングを実行できるようにするために、クラスタ間にはピア関係が必要です。

関連情報

"クラスタと SVM のピアリングの簡単な設定"

"専用のポートを使用する場合の考慮事項"

"データポートを共有する場合の考慮事項"

クラスタ間 LIF を設定しています

MetroCluster パートナークラスタ間の通信に使用するポートにクラスタ間 LIF を作成する必要があります。専用のポートを使用することも、データトラフィック用を兼ねたポートを使用することもできます。

専用ポートでのクラスタ間 LIF の設定

専用ポートにクラスタ間 LIF を設定できます。通常は、レプリケーショントラフィックに使用できる帯域幅が増加します。

手順

1. クラスタ内のポートの一覧を表示します。

   「 network port show 」のように表示されます

   コマンド構文全体については、マニュアルページを参照してください。

   次の例は 'cluster0' 内のネットワーク・ポートを示しています

```
cluster01::> network port show
                                                                  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に使用可能なポートを特定します。

   network interface show -fields home-port 、 curr -port

   コマンド構文全体については、マニュアルページを参照してください。

   次の例は、ポート「 e0e 」および「 e0f 」に LIF が割り当てられていないことを示しています。

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                  home-port curr-port

Cluster cluster01-01_clus1   e0a       e0a
Cluster cluster01-01_clus2   e0b       e0b
Cluster cluster01-02_clus1   e0a       e0a
Cluster cluster01-02_clus2   e0b       e0b
cluster01
        cluster_mgmt         e0c       e0c
cluster01
        cluster01-01_mgmt1   e0c       e0c
cluster01
        cluster01-02_mgmt1   e0c       e0c
```

3. 専用ポートのフェイルオーバーグループを作成します。

   「 network interface failover-groups create -vserver_system_svm 」 -failover-group_failover_group_ -targets_physical_or_logical_ports_`

   次の例では、ポート「 e0e 」および「 e0f 」を、システム SVM 「 cluster01 」上のフェイルオーバーグループ「 intercluster01 」に割り当てます。

```
cluster01::> network interface failover-groups create -vserver cluster01
-failover-group
intercluster01 -targets
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

4. フェイルオーバーグループが作成されたことを確認します。

   「 network interface failover-groups show 」と表示されます

   コマンド構文全体については、マニュアルページを参照してください。

```
cluster01::> network interface failover-groups show
                                  Failover
Vserver          Group            Targets
---------------- ----------------
--------------------------------------------
Cluster
                 Cluster
                                  cluster01-01:e0a, cluster01-01:e0b,
                                  cluster01-02:e0a, cluster01-02:e0b
cluster01
                 Default
                                  cluster01-01:e0c, cluster01-01:e0d,
                                  cluster01-02:e0c, cluster01-02:e0d,
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
                 intercluster01
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
```

5. システム SVM にクラスタ間 LIF を作成して、フェイルオーバーグループに割り当てます。

ONTAP バージョン	コマンドを実行します
ONTAP 9.6 以降	「 network interface create -vserver system_svm -lif lif_name -policy default -intercluster -home-node node -home-port port -address port_ip -netmask netmask-failover-group failover_group 」という名前のポートを作成します
ONTAP 9.5 以前	network interface create -vserver system_svm -lif lif_name -role intercluster -home-node node -home-port port -address port_ip -netmask netmask-failover-group failover_group を作成します

コマンド構文全体については、マニュアルページを参照してください。

次の例は、フェイルオーバーグループ「 intercluster0` 」内にクラスタ間 LIF 「 cluster01_icl01 」と「 cluster01_icl02 」を作成します。

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0 -failover-group intercluster01

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0 -failover-group intercluster01
```

6. クラスタ間 LIF が作成されたことを確認します。

ONTAP バージョン	コマンドを実行します
ONTAP 9.6 以降	「 network interface show -service -policy default -intercluster 」のように表示されます
ONTAP 9.5 以前	「 network interface show -role intercluster 」の略

コマンド構文全体については、マニュアルページを参照してください。

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node           Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01   e0e
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02   e0f
true
```

7. クラスタ間 LIF が冗長構成になっていることを確認します。

ONTAP バージョン	コマンドを実行します
ONTAP 9.6 以降	「 network interface show -service -policy default -intercluster-failover 」のように入力します

ONTAP 9.5 以前	「 network interface show -role intercluster-failover 」の略

コマンド構文全体については、マニュアルページを参照してください。

次の例は、 SVM ポート「 e0e 」上のクラスタ間 LIF 「 cluster01_icl01 」と「 cluster01_icl02 」がポート「 e0f 」にフェイルオーバーされることを示しています。

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

関連情報

"専用のポートを使用する場合の考慮事項"

共有データポートでのクラスタ間 **LIF** の設定

データネットワークと共有するポートにクラスタ間 LIF を設定できます。これにより、クラスタ間ネットワークに必要なポート数を減らすことができます。

手順

1. クラスタ内のポートの一覧を表示します。

   「 network port show 」のように表示されます

   コマンド構文全体については、マニュアルページを参照してください。

   次の例は 'cluster0' 内のネットワーク・ポートを示しています

```
cluster01::> network port show
                                                                  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 バージョン	コマンドを実行します
ONTAP 9.6 以降	「 network interface create -vserver *system_svm _ -lif_lif_name_service -policy default -intercluster -home-node node -home-port port _-address _port_ip*-netmask netmask _ 」のようになります
ONTAP 9.5 以前	「 network interface create -vserver *system_svm _ -lif LIF_name -role intercluster -home-node _node _-home-port _ -address_port_ip*-netmask netmask _ 」のようになります

コマンド構文全体については、マニュアルページを参照してください。

次の例は、クラスタ間 LIF 「 cluster01_icl01 」と「 cluster01_icl02 」を作成します。

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. クラスタ間 LIF が作成されたことを確認します。

ONTAP バージョン	コマンドを実行します
ONTAP 9.6 以降	「 network interface show -service -policy default -intercluster 」のように表示されます
ONTAP 9.5 以前	「 network interface show -role intercluster 」の略

コマンド構文全体については、マニュアルページを参照してください。

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node           Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01   e0c
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02   e0c
true
```

4. クラスタ間 LIF が冗長構成になっていることを確認します。

ONTAP バージョン	コマンドを実行します
ONTAP 9.6 以降	「 network interface show – service-policy default-intercluster-failover 」と表示されます
ONTAP 9.5 以前	「 network interface show -role intercluster-failover 」の略

コマンド構文全体については、マニュアルページを参照してください。

次の例は、ポート「 e0c 」上のクラスタ間 LIF 「 cluster01_icl01 」と「 cluster01_icl02 」がポート「 e0d 」にフェイルオーバーされることを示しています。

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-01:e0c,
                                              cluster01-01:e0d
         cluster01_icl02 cluster01-02:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-02:e0c,
                                              cluster01-02:e0d
```

関連情報

"データポートを共有する場合の考慮事項"

クラスタピア関係を作成

MetroCluster クラスタ間にクラスタピア関係を作成する必要があります。

クラスタピア関係を作成

cluster peer create コマンドを使用すると、ローカルクラスタとリモートクラスタ間にピア関係を作成できます。ピア関係が作成されたら ' リモート・クラスタ上で cluster peer create を実行して ' ローカル・クラスタに対してピア関係を認証できます

作業を開始する前に

- ピア関係にあるクラスタ内の各ノードでクラスタ間 LIF を作成しておく必要があります。
- クラスタで ONTAP 9.3 以降が実行されている必要があります。

手順

1. デスティネーションクラスタで、ソースクラスタとのピア関係を作成します。

   cluster peer create -generate-passphrase -offer-expiration_mm/dd/YYYY HH ： MM ： SS_|1…7days | 1…168 時間 -peer-addrs_peer_lif_ips_-ipspace_ips_`

   「 -generate-passphrase 」と「 -peer-addrs 」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-addrs 」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、 -ipspace 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-addrs_peer_lif_ips_-ipspace_`

   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-addrs
192.140.112.101,192.140.112.102

Notice: Use a generated passphrase or choose a passphrase of 8 or more
characters.
        To ensure the authenticity of the peering relationship, use a
phrase or sequence of characters that would be hard to guess.

Enter the passphrase:
Confirm the passphrase:

Clusters cluster02 and cluster01 are peered.
```

   プロンプトが表示されたら、ピア関係のパスフレーズを入力します。

3. クラスタピア関係が作成されたことを確認します。

   「 cluster peer show -instance 」のように表示されます

```
cluster01::> cluster peer show -instance

                                Peer Cluster Name: cluster02
                    Remote Intercluster Addresses: 192.140.112.101,
192.140.112.102
               Availability of the Remote Cluster: Available
                             Remote Cluster Name: cluster2
                             Active IP Addresses: 192.140.112.101,
192.140.112.102
                           Cluster Serial Number: 1-80-123456
                  Address Family of Relationship: ipv4
             Authentication Status Administrative: no-authentication
                Authentication Status Operational: absent
                                 Last Update Time: 02/05 21:05:41
                     IPspace for the Relationship: Default
```

4. ピア関係にあるノードの接続状態とステータスを確認します。

   cluster peer health show

```
cluster01::> cluster peer health show
Node       cluster-Name                Node-Name
             Ping-Status               RDB-Health Cluster-Health  Avail…
---------- --------------------------- ---------  ---------------
--------
cluster01-01
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
cluster01-02
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
```

クラスタピア関係の作成（ **ONTAP 9.2** 以前）

「 cluster peer create 」コマンドを使用して、ローカルクラスタとリモートクラスタ間のピア関係の要求を開始できます。ピア関係がローカルクラスタによって要求された後 ' リモートクラスタ上で cluster peer create

を実行して ' 関係を受け入れることができます

作業を開始する前に

- ピア関係にあるクラスタ内の各ノードでクラスタ間 LIF を作成しておく必要があります。
- クラスタ管理者は、各クラスタが他のクラスタに対して自身を認証する際に使用するパスフレーズに同意しておく必要があります。

手順

1. データ保護のデスティネーションクラスタで、データ保護のソースクラスタとのピア関係を作成します。

   'cluster peer create -peer-addrs_peer_lif_ips_-ipspace_`

   カスタム IPspace を使用しない場合は、 -ipspace オプションを無視してかまいません。コマンド構文全体については、マニュアルページを参照してください。

   次の例は、クラスタ間 LIF の IP アドレス 192.168.2.201 および 192.168.2.202 で、リモートクラスタとのクラスタピア関係を作成します。

   ```
   cluster02::> cluster peer create -peer-addrs 192.168.2.201,192.168.2.202
   Enter the passphrase:
   Please enter the passphrase again:
   ```

   プロンプトが表示されたら、ピア関係のパスフレーズを入力します。

2. データ保護のソースクラスタで、ソースクラスタをデスティネーションクラスタに対して認証します。

   'cluster peer create -peer-addrs_peer_lif_ips_-ipspace_`

   コマンド構文全体については、マニュアルページを参照してください。

   次の例は、クラスタ間 LIF の IP アドレス 192.140.112.203 および 192.140.112.204 でローカルクラスタをリモートクラスタに対して認証します。

   ```
   cluster01::> cluster peer create -peer-addrs 192.168.2.203,192.168.2.204
   Please confirm the passphrase:
   Please confirm the passphrase again:
   ```

   プロンプトが表示されたら、ピア関係のパスフレーズを入力します。

3. クラスタピア関係が作成されたことを確認します。

   cluster peer show – instance

   コマンド構文全体については、マニュアルページを参照してください。

```
cluster01::> cluster peer show -instance
Peer Cluster Name: cluster01
Remote Intercluster Addresses: 192.168.2.201,192.168.2.202
Availability: Available
Remote Cluster Name: cluster02
Active IP Addresses: 192.168.2.201,192.168.2.202
Cluster Serial Number: 1-80-000013
```

4. ピア関係にあるノードの接続状態とステータスを確認します。

   cluster peer health show

   コマンド構文全体については、マニュアルページを参照してください。

```
cluster01::> cluster peer health show
Node       cluster-Name                Node-Name
             Ping-Status               RDB-Health Cluster-Health  Avail…
---------- --------------------------- ---------  ---------------
--------
cluster01-01
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
cluster01-02
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
```

ルートアグリゲートをミラーリング

データ保護を提供するには、ルートアグリゲートをミラーする必要があります。

このタスクについて

デフォルトでは、ルートアグリゲートは RAID-DP タイプのアグリゲートとして作成されます。ルートアグリゲートのタイプは RAID-DP から RAID4 に変更することができます。次のコマンドは、ルートアグリゲートを RAID4 タイプのアグリゲートに変更します。

「 storage aggregate modify – aggregate_name _raidtype raid4 」と表示されます

ADP 以外のシステムでは、ミラーリングの実行前後に、アグリゲートの RAID タイプをデフォルトの RAID-DP から RAID4 に変更できます。

手順

1. ルートアグリゲートをミラーします。

   「 storage aggregate mirror _aggr_name _ 」のようになります

   次のコマンドでは 'controller_A_1 のルートアグリゲートがミラーされます

   ```
   controller_A_1::> storage aggregate mirror aggr0_controller_A_1
   ```

   これによりアグリゲートがミラーされるため、ローカルのプレックスとリモートのプレックスがリモートの MetroCluster サイトに配置されたアグリゲートが作成されます。

2. MetroCluster 構成の各ノードについて、同じ手順を繰り返します。

関連情報

"論理ストレージ管理"

"ONTAP の概念"

各ノードでミラーされたデータアグリゲートを作成します

DR グループの各ノードに、ミラーされたデータアグリゲートを 1 つ作成する必要があります。

作業を開始する前に

- 新しいアグリゲートで使用するドライブを把握しておく必要があります。
- 複数のドライブタイプを含むシステム（異機種混在ストレージ）の場合は、正しいドライブタイプが選択されるようにする方法を確認しておく必要があります。

このタスクについて

- ドライブは特定のノードによって所有されます。アグリゲートを作成する場合、アグリゲート内のすべてのドライブは同じノードによって所有される必要があります。そのノードが、作成するアグリゲートのホームノードになります。
- アグリゲート名は、 MetroCluster 構成を計画する際に決定した命名規則に従う必要があります。

  "ディスクおよびアグリゲートの管理"

- アグリゲート名は、MetroClusterサイト全体で一意である必要があります。つまり、サイト A とサイト B に同じ名前を持つ 2 つの異なるデータ アグリゲートを持つことはできません。

手順

1. 使用可能なスペアのリストを表示します。

   「 storage disk show -spare -owner_node_name _ 」というように入力します

2. アグリゲートを作成します。

「 storage aggregate create -mirror true 」のようになります

クラスタ管理インターフェイスでクラスタにログインした場合、クラスタ内の任意のノードにアグリゲートを作成できます。アグリゲートを特定のノード上に作成するには、「 -node 」パラメータを使用するか、そのノードが所有するドライブを指定します。

次のオプションを指定できます。

- アグリゲートのホームノード（通常運用時にアグリゲートを所有するノード）
- アグリゲートに追加するドライブのリスト
- 追加するドライブ数

> 使用できるドライブ数が限られている最小サポート構成では、 force-small-aggregate オプションを使用して、 3 ディスクの RAID-DP アグリゲートを作成できるように設定する必要があります。

- アグリゲートに使用するチェックサム形式
- 使用するドライブのタイプ
- 使用するドライブのサイズ
- 使用するドライブの速度
- アグリゲート上の RAID グループの RAID タイプ
- RAID グループに含めることができるドライブの最大数
- これらのオプションの詳細については 'storage aggregate create のマニュアル・ページを参照してください RPM の異なるドライブでも使用できます

  次のコマンドでは、 10 本のディスクを含むミラーアグリゲートが作成されます。

```
cluster_A::> storage aggregate create aggr1_node_A_1 -diskcount 10 -node
node_A_1 -mirror true
[Job 15] Job is queued: Create aggr1_node_A_1.
[Job 15] The job is starting.
[Job 15] Job succeeded: DONE
```

3. 新しいアグリゲートの RAID グループとドライブを確認します。

   「 storage aggregate show-status -aggregate _aggregate-name _ 」を参照してください

ミラーされていないデータアグリゲートの作成

MetroCluster 構成が提供する冗長なミラーリングを必要としないデータについては、必要に応じてミラーされていないデータアグリゲートを作成できます。

作業を開始する前に

- 新しいアグリゲートで使用するドライブを把握しておく必要があります。

- 複数のドライブタイプを含むシステム（異機種混在ストレージ）の場合は、正しいドライブタイプが選択されていることを確認する方法を理解しておく必要があります。

例 **1.** このタスクについて

- 注意 * ： MetroCluster FC 構成では、ミラーされていないアグリゲートがスイッチオーバー後にオンラインになるのは、アグリゲート内のリモートディスクにアクセスできる場合のみです。ISL で障害が発生すると、ミラーされていないリモートディスク内のデータにローカルノードがアクセスできなくなる可能性があります。アグリゲートに障害が発生すると、ローカルノードがリブートされる場合があります。

ミラーされていないアグリゲートは、そのアグリゲートを所有するノードに対してローカルでなければなりません。

- ドライブは特定のノードによって所有されます。アグリゲートを作成する場合、アグリゲート内のすべてのドライブは同じノードによって所有される必要があります。そのノードが、作成するアグリゲートのホームノードになります。
- アグリゲート名は、 MetroCluster 構成を計画する際に決定した命名規則に従う必要があります。
- 。 "ディスクとアグリゲートの管理" アグリゲートのミラーリングの詳細については、を参照してください

手順

1. 使用可能なスペアのリストを表示します。

   「 storage disk show -spare -owner_node_name _ 」というように入力します

2. アグリゲートを作成します。

   「 storage aggregate create 」

   クラスタ管理インターフェイスでクラスタにログインした場合、クラスタ内の任意のノードにアグリゲートを作成できます。アグリゲートが特定のノード上に作成されていることを確認するには、「 -node 」パラメータを使用するか、そのノードが所有するドライブを指定します。

   次のオプションを指定できます。

   - アグリゲートのホームノード（通常運用時にアグリゲートを所有するノード）
   - アグリゲートに追加するドライブのリスト
   - 追加するドライブ数
   - アグリゲートに使用するチェックサム形式
   - 使用するドライブのタイプ
   - 使用するドライブのサイズ
   - 使用するドライブの速度
   - アグリゲート上の RAID グループの RAID タイプ
   - RAID グループに含めることができるドライブの最大数
   - これらのオプションの詳細については 'storage aggregate create のマニュアル・ページを参照してく

ださい RPM の異なるドライブでも使用できます

次のコマンドでは、 10 本のディスクを含むミラーされていないアグリゲートが作成さ

```
controller_A_1::> storage aggregate create aggr1_controller_A_1
-diskcount 10 -node controller_A_1
[Job 15] Job is queued: Create aggr1_controller_A_1.
[Job 15] The job is starting.
[Job 15] Job succeeded: DONE
```

3. 新しいアグリゲートの RAID グループとドライブを確認します。

「 storage aggregate show-status -aggregate _aggregate-name _ 」を参照してください

MetroCluster 構成の実装

MetroCluster 構成でデータ保護を開始するに MetroCluster は 'data configure コマンドを実行する必要があります

作業を開始する前に

- ルート以外のミラーされたデータアグリゲートが各クラスタに少なくとも 2 つ必要です。

  その他のデータアグリゲートはミラーされていてもいなくてもかまいません。

  アグリゲートのタイプを確認します。

  「 storage aggregate show

  ミラーされた単一のデータアグリゲートを使用する場合は、を参照してください "ONTAP で MCC ソフトウェアを設定" 手順については、を参照し

- コントローラおよびシャーシの ha-config の状態が「 mcc-2n 」である必要があります。

このタスクについて

MetroCluster 構成をイネーブルにするには、任意のノード上で、 MetroCluster configure コマンドを 1 回実行し問題ます。サイトごとまたはノードごとにコマンドを問題で実行する必要はありません。また、問題するノードまたはサイトはどれでもかまいません。

手順

1. 次の形式で MetroCluster を設定します。

MetroCluster 構成の内容	操作
複数のデータアグリゲート	いずれかのノードのプロンプトで、 MetroCluster を設定します。 MetroCluster configure_node-name_` です

ミラーされた 1 つのデータアグリゲート	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 モードで続けるかどうかを尋ねられたら、「 y 」と入力して応答する必要があります。 advanced モードのプロンプト（ * > ）が表示されます。 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。 `+set -privilege admin`

複数のデータアグリゲートを使用することを推奨します。最初の DR グループにアグリゲートが 1 つしかなく、 1 つのアグリゲートを含む DR グループを追加する場合は、メタデータボリュームを単一のデータアグリゲートから移動する必要があります。この手順の詳細については、を参照してください "MetroCluster 構成でのメタデータボリュームの移動"。

次のコマンドは 'controller_A_1 を含む DR グループ内のすべてのノードで MetroCluster 構成を有効にします

```
cluster_A::*> metrocluster configure -node-name controller_A_1

[Job 121] Job succeeded: Configure is successful.
```

2. サイト A のネットワークステータスを確認します。

「 network port show 」のように表示されます

次の例は、ネットワークポートの用途を示しています。

```
cluster_A::> network port show
                                                              Speed (Mbps)
Node   Port      IPspace   Broadcast Domain Link   MTU    Admin/Oper
------ --------- --------- ---------------- ----- ------- ------------
controller_A_1
       e0a       Cluster   Cluster          up     9000  auto/1000
       e0b       Cluster   Cluster          up     9000  auto/1000
       e0c       Default   Default          up     1500  auto/1000
       e0d       Default   Default          up     1500  auto/1000
       e0e       Default   Default          up     1500  auto/1000
       e0f       Default   Default          up     1500  auto/1000
       e0g       Default   Default          up     1500  auto/1000

7 entries were displayed.
```

3. MetroCluster 構成の両方のサイトから MetroCluster 構成を確認します。

   a. サイト A から構成を確認します :+`MetroCluster show`

```
cluster_A::> metrocluster show

Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
Remote: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
```

   b. サイト B から構成を確認します + MetroCluster show

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
Remote: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
```

健常性監視用の **FC-to-SAS** ブリッジの設定

9.8 より前のバージョンの ONTAP を実行しているシステムで FC-to-SAS ブリッジを使用している場合は、MetroCluster 構成の FC-to-SAS ブリッジを監視するための特別な設定手順を実行する必要があります。

- FibreBridge ブリッジでは、サードパーティ製の SNMP 監視ツールはサポートされません。
- ONTAP 9.8 以降では、デフォルトで FC-to-SAS ブリッジがインバンド接続で監視されるため、追加の設定は必要ありません。

ONTAP 9.8 以降では 'storage bridge コマンドは 'system bridge コマンドに置き換えられました 次の手順は「 storage bridge 」コマンドを示していますが、 ONTAP 9.8 以降を実行している場合は「 system bridge 」コマンドが優先されます。

手順

1. ONTAP クラスタのプロンプトで、ブリッジをヘルスモニタの対象に追加します。

   a. 使用している ONTAP のバージョンに対応したコマンドを使用して、ブリッジを追加します。

ONTAP バージョン	コマンドを実行します
ONTAP 9.5 以降	「 storage bridge add -address 0.0.0.0 -managed-by in-band-name_bridge-name_`
ONTAP 9.4 以前	「 storage bridge add -address_bridge-ip-address_-name_bridge -name_` 」

   b. ブリッジが追加され、正しく設定されていることを確認します。

      「 storage bridge show 」

      ポーリング間隔に応じて、すべてのデータが反映されるまで 15 分程度かかる場合があります。ONTAP ヘルスモニタは、「 Status 」列の値が「 ok 」で、ワールドワイド名（ WWN ）などのその他の情報が表示されていれば、ブリッジに接続して監視できます。

次の例は、 FC-to-SAS ブリッジが設定されていることを示しています。

```
controller_A_1::> storage bridge show

Bridge              Symbolic Name Is Monitored  Monitor Status  Vendor
Model                Bridge WWN
------------------  ------------ ------------  --------------  ------
-----------------    ----------
ATTO_10.10.20.10  atto01        true          ok              Atto
FibreBridge 7500N      20000010867038c0
ATTO_10.10.20.11  atto02        true          ok              Atto
FibreBridge 7500N      20000010867033c0
ATTO_10.10.20.12  atto03        true          ok              Atto
FibreBridge 7500N      20000010867030c0
ATTO_10.10.20.13  atto04        true          ok              Atto
FibreBridge 7500N      2000001086703b80

4 entries were displayed

 controller_A_1::>
```

MetroCluster の設定を確認しています

MetroCluster 構成内のコンポーネントおよび関係が正しく機能していることを確認できます。チェックは、初期設定後と、 MetroCluster 設定に変更を加えたあとに実施する必要があります。また、ネゴシエート（計画的）スイッチオーバーやスイッチバックの処理の前にも実施します。

いずれかまたは両方のクラスタに対して短時間に MetroCluster check run コマンドを 2 回発行すると ' 競合が発生し ' コマンドがすべてのデータを収集しない場合がありますそれ以降の「 MetroCluster check show 」コマンドでは、期待される出力が表示されません。

1. 構成を確認します。

   「 MetroCluster check run 」のようになります

   このコマンドはバックグラウンドジョブとして実行され、すぐに完了しない場合があります。

```
cluster_A::> metrocluster check run
The operation has been started and is running in the background. Wait
for
it to complete and run "metrocluster check show" to view the results. To
check the status of the running metrocluster check operation, use the
command,
"metrocluster operation history show -job-id 2245"
```

```
cluster_A::> metrocluster check show

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         ok
volumes             ok
7 entries were displayed.
```

2. より詳細な結果を表示します。

「 MetroCluster check run 」のようになります

MetroCluster check aggregate show

MetroCluster check cluster show

MetroCluster check config-replication show

MetroCluster check lif show

MetroCluster check node show

「 MetroCluster check show 」コマンドは、最新の「 MetroCluster check run 」コマンドの結果を表示します。MetroCluster check show コマンドを使用する前に ' 必ず MetroCluster check run コマンドを実行して ' 表示されている情報が最新であることを確認してください

次に、正常な 4 ノード MetroCluster 構成の MetroCluster check aggregate show コマンドの出力例を示します。

```
cluster_A::> metrocluster check aggregate show

Last Checked On: 8/5/2014 00:42:58

Node                  Aggregate                 Check
Result
---------------       --------------------      ---------------------
---------
controller_A_1        controller_A_1_aggr0
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
```

```
ok
                      controller_A_1_aggr1
                                                  mirroring-status
ok
                                                  disk-pool-allocation
ok
                                                  ownership-state
ok
                      controller_A_1_aggr2
                                                  mirroring-status
ok
                                                  disk-pool-allocation
ok
                                                  ownership-state
ok


controller_A_2        controller_A_2_aggr0
                                                  mirroring-status
ok
                                                  disk-pool-allocation
ok
                                                  ownership-state
ok
                      controller_A_2_aggr1
                                                  mirroring-status
ok
                                                  disk-pool-allocation
ok
                                                  ownership-state
ok
                      controller_A_2_aggr2
                                                  mirroring-status
ok
                                                  disk-pool-allocation
ok
                                                  ownership-state
ok

18 entries were displayed.
```

次に、正常な 4 ノード MetroCluster 構成の MetroCluster check cluster show コマンドの出力例を示します。この出力は、必要に応じてネゴシエートスイッチオーバーを実行できる状態であることを示しています。

```
Last Checked On: 9/13/2017 20:47:04

Cluster                 Check                             Result
---------------------- ------------------------------- ---------
mccint-fas9000-0102
                        negotiated-switchover-ready     not-applicable
                        switchback-ready                not-applicable
                        job-schedules                   ok
                        licenses                        ok
                        periodic-check-enabled          ok
mccint-fas9000-0304
                        negotiated-switchover-ready     not-applicable
                        switchback-ready                not-applicable
                        job-schedules                   ok
                        licenses                        ok
                        periodic-check-enabled          ok
10 entries were displayed.
```

関連情報

"ディスクおよびアグリゲートの管理"

"ネットワークと LIF の管理"

Config Advisor での MetroCluster 構成エラーの確認

一般的な構成エラーの有無を確認する Config Advisor ツールをネットアップサポートサイトからダウンロードできます。

Config Advisor は、構成の検証や健常性のチェックに使用できるツールです。データ収集とシステム分析のために、セキュアなサイトにもセキュアでないサイトにも導入できます。

Config Advisor のサポートには制限があり、オンラインでしか使用できません。

1. Config Advisor のダウンロードページにアクセスし、ツールをダウンロードします。

   "ネットアップのダウンロード： Config Advisor"

2. Config Advisor を実行し、ツールの出力を確認して、問題が検出された場合は出力に表示される推奨事項に従って対処します。

スイッチオーバー、修復、スイッチバックを検証しています

MetroCluster 構成のスイッチオーバー、修復、スイッチバックの処理を検証する必要があります。

1. に記載されているネゴシエートスイッチオーバー、修復、スイッチバックの手順を使用し "スイッチオーバー、修復、スイッチバックを実行"ます。

構成バックアップファイルを保護しています

ローカルクラスタ内のデフォルトの場所に加えて、クラスタ構成バックアップファイルをアップロードするリモート URL （ HTTP または FTP ）を指定することで、クラスタ構成バックアップファイルの保護を強化できます。

1. 構成バックアップファイルのリモートデスティネーションの URL を設定します。

   「システム構成のバックアップ設定は URL-of-destination 」を変更します

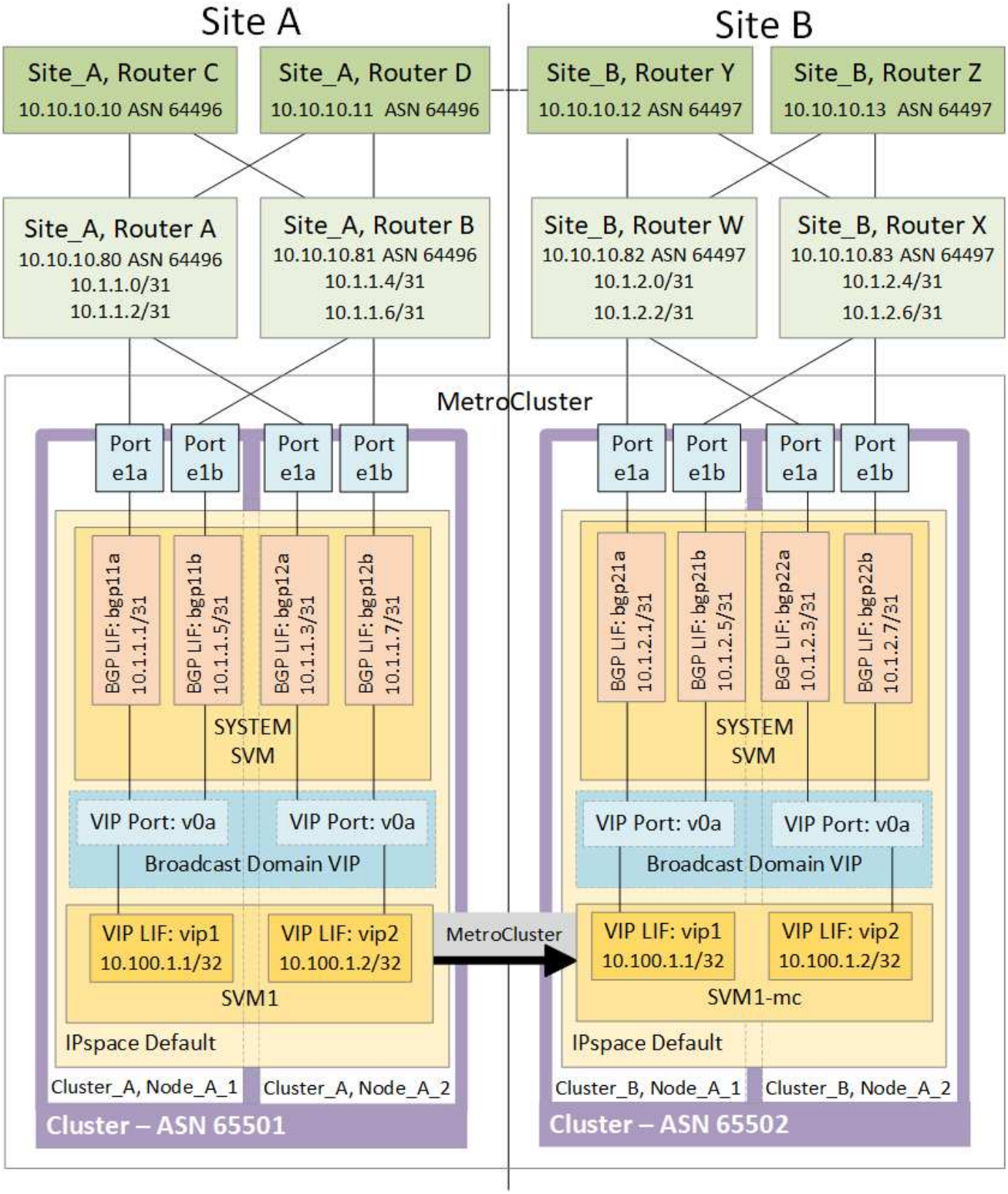
   。 "CLI を使用したクラスタ管理" 追加情報が含まれています。

MetroCluster 設定で仮想 IP およびボーダーゲートウェイプロトコルを使用する場合の考慮事項

ONTAP 9.5 以降では、 ONTAP で仮想 IP （ VIP ）と Border Gateway Protocol （ BGP ）を使用してレイヤ 3 接続がサポートされます。VIP と BGP を組み合わせることで、フロントエンドネットワークでの冗長性とバックエンド MetroCluster の冗長性が確保され、レイヤ 3 ディザスタリカバリ解決策が実現します。

レイヤ 3 解決策を計画する際は、次のガイドラインと図を確認してください。ONTAP での VIP および BGP の実装の詳細については、次の項を参照してください。

"* 仮想 IP （ VIP ） LIF の設定 *"



- ONTAP の制限 *

ONTAP では、 MetroCluster 構成の両方のサイトのすべてのノードに BGP ピアリングが設定されていることは自動的には検証されません。

ONTAP は、ルートアグリゲーションを実行するのではなく、個々の仮想 LIF のすべての IP を一意のホストルートとして常時通知します。

ONTAP は、真のエニーキャストをサポートしません。クラスタ内の 1 つのノードだけが、特定の仮想 LIF の IP を提供します（ただし、物理ポートが正しい IPspace の一部である場合は、 BGP LIF であるかどうかに関係なく、すべての物理インターフェイスで許可されます）。異なる LIF は、異なるホストノードに個別に移行できます。

- このレイヤ 3 解決策を MetroCluster 構成で使用する場合の注意事項 *

必要な冗長性を確保するために、 BGP および VIP を正しく設定する必要があります。

よりシンプルな導入シナリオが、より複雑なアーキテクチャよりも推奨されます（たとえば、 BGP ピアリングルータは、中間の BGP 以外のルータ経由で到達可能です）。ただし、 ONTAP では、ネットワーク設計やトポロジの制限は適用されません。

VIP LIF はフロントエンド / データネットワークのみをカバーします。

ONTAP のバージョンに応じて、システム SVM やデータ SVM ではなく、ノード SVM に BGP ピアリング LIF を設定する必要があります。ONTAP 9.8 では、クラスタ（システム） SVM 内に BGP LIF が表示され、ノード SVM が存在しなくなります。

各データ SVM には、 LIF の移行や MetroCluster のフェイルオーバーが発生したときにリターンデータパスを使用できるように、考えられるすべてのファーストホップゲートウェイアドレス（通常は BGP ルータピアリングの IP アドレス）を設定する必要があります。

BGP LIF はクラスタ間 LIF と同様にノード固有で、各ノードは一意の設定を持ちます。 DR サイトのノードにレプリケートする必要はありません。

v0a （ v0b など）が存在することにより、接続が継続的に検証され、 LIF の移行またはフェイルオーバーが成功するかどうかが保証されます（停止後にのみ構成の破損が表示される L2 とは異なります）。

アーキテクチャに大きな違いは、クライアントがデータ SVM の VIP と同じ IP サブネットを共有しなくなることです。適切なエンタープライズクラスの復元力と冗長性機能（たとえば、 VRRP/HSRP ）をイネーブルにした L3 ルータは、 VIP が正しく動作するために、ストレージとクライアント間のパス上に配置する必要があります。

BGP の信頼性の高い更新プロセスにより、 LIF の移行がわずかに高速化され、一部のクライアントの中断が少なくなるため、円滑な移行が可能になります

ネットワークまたはスイッチの一部の動作を LACP よりも高速に検出するように BGP を設定できます（設定されている場合）。

外部 BGP （ EBGP ）は、 ONTAP ノードとピアリングルータ間で異なる AS 番号を使用し、ルータ上でのルート集約と再配布を容易にするための推奨配置です。内部 BGP （ IBGP ）およびルートリフレクタの使用は不可能ではありませんが、簡単な VIP 設定の範囲外です。

導入後、関連する仮想 LIF が各サイトのすべてのノード間で移行されたときに（ MetroCluster スイッチオーバーを含む）データ SVM にアクセスできることを確認し、同じデータ SVM への静的ルートの正しい設定を確認する必要があります。

VIP は、ほとんどの IP ベースのプロトコル（ NFS 、 SMB 、 iSCSI ）に対応しています。

MetroCluster 構成をテストする

障害シナリオをテストして、 MetroCluster 構成が正しく動作していることを確認できます。

ネゴシエートスイッチオーバーを検証中

ネゴシエート（計画的）スイッチオーバー処理をテストして、データが中断なく提供されることを確認できます。

このテストでは、クラスターを 2 番目のデータ センターに切り替えても、データの可用性が影響を受けないこと (SMB およびファイバ チャネル プロトコルを除く) を検証します。

このテストには約 30 分かかります。

この手順の想定される結果は次のとおりです。

- MetroCluster switchover コマンドは ' 警告プロンプトを表示します

  プロンプトに「 * yes * 」と応答すると、コマンドの発行元サイトがパートナーサイトを切り替えます。

MetroCluster IP 構成の場合：

- ONTAP 9.4 以前：
  - ミラーアグリゲートはネゴシエートスイッチオーバー後にデグレード状態になります。
- ONTAP 9.5 以降：
  - リモートストレージがアクセス可能である場合、ミラーされたアグリゲートは通常の状態のままになります。
  - リモートストレージへのアクセスが失われると、ネゴシエートスイッチオーバー後にミラーアグリゲートがデグレード状態になります。
- ONTAP 9.8 以降の場合：
  - リモートストレージへのアクセスが失われると、ディザスタサイトにあるミラーされていないアグリゲートは使用できなくなります。これにより、コントローラが停止する可能性があります。

手順

1. すべてのノードが設定済みの状態で通常モードになっていることを確認します。

   MetroCluster node show

```
cluster_A::>  metrocluster node show

Cluster                           Configuration State    Mode
--------------------------------- ---------------------
------------------------
 Local: cluster_A                  configured             normal
Remote: cluster_B                  configured             normal
```

2. スイッチオーバー処理を開始します。

   MetroCluster スイッチオーバー

```
cluster_A::> metrocluster switchover
Warning: negotiated switchover is about to start. It will stop all the
data Vservers on cluster "cluster_B" and
automatically re-start them on cluster "cluster_A". It will finally
gracefully shutdown cluster "cluster_B".
```

3. ローカルクラスタが設定済みの状態でスイッチオーバーモードになっていることを確認します。

   MetroCluster node show

```
cluster_A::>  metrocluster node show

Cluster                           Configuration State    Mode
--------------------------------- ---------------------
------------------------
Local: cluster_A                   configured             switchover
Remote: cluster_B                  not-reachable          -
              configured             normal
```

4. スイッチオーバー処理が成功したことを確認します。

   「 MetroCluster operation show 」を参照してください

```
cluster_A::> metrocluster operation show
  Operation: switchover
      State: successful
 Start Time: 2/6/2016 13:28:50
   End Time: 2/6/2016 13:29:41
     Errors: -
```

5. 「 vserver show 」コマンドと「 network interface show 」コマンドを使用して、 DR SVM と LIF がオン

ラインになったことを確認します。

修復と手動スイッチバックの検証

修復処理と手動スイッチバック処理をテストするには、ネゴシエートスイッチオーバー後にクラスタを元のデータセンターにスイッチバックして、データの可用性に影響がないことを検証します（ SMB および Solaris FC 構成を除く）。

このテストには約 30 分かかります。

この手順では、想定される結果として、サービスがホームノードにスイッチバックされることを確認します。

手順

1. 修復が完了したことを確認します。

   MetroCluster node show

   次の例は、コマンドが正常に完了したことを示しています。

```
cluster_A::> metrocluster node show
DR                               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.
```

2. すべてのアグリゲートがミラーされていることを確認します。

   「 storage aggregate show

   次の例では、すべてのアグリゲートの RAID ステータスが mirrored になっています。

```
cluster_A::> storage aggregate show
cluster Aggregates:
Aggregate Size     Available Used% State   #Vols  Nodes       RAID
Status
--------- -------- --------- ----- ------- ------ ----------
------------
data_cluster
            4.19TB    4.13TB    2% online       8 node_A_1    raid_dp,
                                                               mirrored,
                                                               normal
root_cluster
           715.5GB   212.7GB   70% online       1 node_A_1    raid4,
                                                               mirrored,
                                                               normal
cluster_B Switched Over Aggregates:
Aggregate Size     Available Used% State   #Vols  Nodes       RAID
Status
--------- -------- --------- ----- ------- ------ ----------
------------
data_cluster_B
            4.19TB    4.11TB    2% online       5 node_A_1    raid_dp,
                                                               mirrored,
                                                               normal
root_cluster_B    -         -     - unknown      - node_A_1   -
```

3. ディザスタサイトからノードをブートします。
4. スイッチバックリカバリのステータスを確認します。

   MetroCluster node show

```
cluster_A::> metrocluster node show
DR                              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.
```

5. スイッチバックを実行します。

   MetroCluster スイッチバック

```
cluster_A::> metrocluster switchback
[Job 938] Job succeeded: Switchback is successful.Verify switchback
```

6. ノードのステータスを確認します。

   MetroCluster node show

```
cluster_A::> metrocluster node show
DR                               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.
```

7. ステータスを確認します。

   「 MetroCluster operation show 」を参照してください

   正常に完了したことを示す出力が表示されます。

```
cluster_A::> metrocluster operation show
  Operation: switchback
      State: successful
 Start Time: 2/6/2016 13:54:25
   End Time: 2/6/2016 13:56:15
     Errors: -
```

単一の FC-to-SAS ブリッジの停止

単一の FC-to-SAS ブリッジの障害をテストして、単一点障害がないことを確認できます。

このテストには約 15 分かかります。

この手順の想定される結果は次のとおりです。

- ブリッジのスイッチがオフになるため、とエラーが生成されます。
- フェイルオーバーやサービスの中断は発生しません。
- コントローラモジュールからブリッジに接続されたドライブへのパスは 1 つだけになります。

ONTAP 9.8 以降では 'storage bridge コマンドは 'system bridge コマンドに置き換えられました 次の手順は「 storage bridge 」コマンドを示していますが、 ONTAP 9.8 以降を実行している場合は「 system bridge 」コマンドが優先されます。

手順

1. ブリッジの電源装置をオフにします。
2. ブリッジの監視がエラーを示していることを確認します。

   「 storage bridge show 」

```
cluster_A::> storage bridge show

                                                                  Is
Monitor
Bridge     Symbolic Name Vendor  Model     Bridge WWN       Monitored
Status
---------- ------------- ------- --------- ---------------- ---------
-------
ATTO_10.65.57.145
         bridge_A_1    Atto    FibreBridge 6500N
                                           200000108662d46c true
error
```

3. ブリッジに接続されたドライブに 1 つのパスでアクセス可能なことを確認します。

   「 storage disk error show 」と表示されます

```
cluster_A::> storage disk error show
Disk              Error Type        Error Text
----------------- -----------------
-------------------------------------------
1.0.0             onedomain         1.0.0 (5000cca057729118): All paths
to this array LUN are connected to the same fault domain. This is a
single point of failure.
1.0.1             onedomain         1.0.1 (5000cca057727364): All paths
to this array LUN are connected to the same fault domain. This is a
single point of failure.
1.0.2             onedomain         1.0.2 (5000cca05772e9d4): All paths
to this array LUN are connected to the same fault domain. This is a
single point of failure.
...
1.0.23            onedomain         1.0.23 (5000cca05772e9d4): All paths
to this array LUN are connected to the same fault domain. This is a
single point of failure.
```

電源回線切断後の動作確認

MetroCluster 構成で PDU の障害が発生した場合の対応をテストできます。

ベストプラクティスとして、コンポーネントの各電源装置（ PSU ）を別々の電源装置に接続することを推奨します。両方の PSU を同じ配電ユニット（ PDU ）に接続している場合、停電が発生すると、サイトが停止してシェルフ全体が使用できなくなる可能性があります。1 本原因の電源回線に障害が発生した場合に、サービスが中断する可能性があるケーブル接続の不一致がないかどうかをテストします。

このテストには約 15 分かかります。

このテストでは、 MetroCluster コンポーネントが格納されたすべてのラックで、左側のすべての PDU の電源をオフにしてから、右側のすべての PDU の電源をオフにする必要があります。

この手順の想定される結果は次のとおりです。

- PDU の接続が切断されるため、エラーが生成されます。
- フェイルオーバーやサービスの中断は発生しません。

手順

1. MetroCluster コンポーネントが格納されたラックの左側の PDU の電源をオフにします。
2. 「 system environment sensors show -state fault 」コマンドと「 storage shelf show -errors 」コマンドを使用して、コンソールで結果を監視します。

```
cluster_A::> system environment sensors show -state fault

Node Sensor              State Value/Units Crit-Low Warn-Low Warn-Hi
Crit-Hi
---- -------------------- ------ ----------- -------- -------- -------
-------
node_A_1
        PSU1             fault
                             PSU_OFF
        PSU1 Pwr In OK   fault
                             FAULT
node_A_2
        PSU1             fault
                             PSU_OFF
        PSU1 Pwr In OK   fault
                             FAULT
4 entries were displayed.

cluster_A::> storage shelf show -errors
    Shelf Name: 1.1
     Shelf UID: 50:0a:09:80:03:6c:44:d5
 Serial Number: SHFHU1443000059

Error Type          Description
------------------  ---------------------------
Power               Critical condition is detected in storage shelf
power supply unit "1". The unit might fail.Reconnect PSU1
```

3. 左側の PDU の電源を再度オンにします。
4. ONTAP がエラー状態をクリアすることを確認します。
5. 右側の PDU で上記の手順を繰り返します。

単一のストレージシェルフが停止したあとの動作確認

単一のストレージシェルフの障害をテストして、単一点障害がないことを確認できます。

この手順の想定される結果は次のとおりです。

- 監視ソフトウェアからエラーメッセージが報告されます。
- フェイルオーバーやサービスの中断は発生しません。
- ハードウェア障害がリストアされたあと、ミラーの再同期が自動的に開始されます。

手順

1. ストレージフェイルオーバーのステータスを確認します。

「 storage failover show 」をクリックします

```
cluster_A::> storage failover show

Node           Partner        Possible State Description
-------------- -------------- --------
-------------------------------------
node_A_1       node_A_2       true     Connected to node_A_2
node_A_2       node_A_1       true     Connected to node_A_1
2 entries were displayed.
```

2. アグリゲートのステータスを確認します。

「 storage aggregate show

```
cluster_A::> storage aggregate show

cluster Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
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,

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

cluster_A::> vserver show -type data
                                Admin      Operational Root
Vserver     Type    Subtype    State      State       Volume
Aggregate
----------- ------- ---------- ---------- ----------- ----------
----------
SVM1        data    sync-source           running     SVM1_root
node_A_1_data01_mirrored
SVM2        data    sync-source           running     SVM2_root
node_A_2_data01_mirrored

cluster_A::> network interface show -fields is-home false
There are no entries matching your query.

cluster_A::> volume show !vol0,!MDV*
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
SVM1
          SVM1_root
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.50GB    5%
SVM1
          SVM1_data_vol
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_root
                       node_A_2_data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_data_vol
                       node_A_2_data02_unmirrored
                                    online     RW          1GB
972.6MB    5%
```

4. ハードウェア障害をシミュレートするために電源をオフにするノード node_A_1 のプール 1 内のシェルフ

を特定します。

「 storage aggregate show -r -node node_name !!* root

ミラーされたデータアグリゲートを構成するドライブが格納されたシェルフを選択する必要があります。

次の例では、停止する対象としてシェルフ ID 31 を選択します。

```
cluster_A::> storage aggregate show -r -node node_A_2 !*root
Owner Node: node_A_2
 Aggregate: node_A_2_data01_mirrored (online, raid_dp, mirrored) (block
checksums)
  Plex: /node_A_2_data01_mirrored/plex0 (online, normal, active, pool0)
   RAID Group /node_A_2_data01_mirrored/plex0/rg0 (normal, block
checksums)
                                                                   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 (online, normal, active, pool1)
   RAID Group /node_A_2_data01_mirrored/plex4/rg0 (normal, block
checksums)
                                                                   Usable
Physical
     Position Disk                       Pool Type     RPM     Size
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
828.0GB (normal)

 Aggregate: node_A_2_data02_unmirrored (online, raid_dp) (block
checksums)
  Plex: /node_A_2_data02_unmirrored/plex0 (online, normal, active,
pool0)
   RAID Group /node_A_2_data02_unmirrored/plex0/rg0 (normal, block
checksums)
                                                                   Usable
Physical
     Position Disk                       Pool Type     RPM     Size
Size Status
     -------- -------------------------- ---- ----- ------ --------
-------- ----------
     dparity  2.30.12                      0   BSAS    7200  827.7GB
828.0GB (normal)
     parity   2.30.22                      0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.21                      0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.20                      0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.14                      0   BSAS    7200  827.7GB
828.0GB (normal)
15 entries were displayed.
```

5. 選択したシェルフの電源を物理的にオフにします。
6. アグリゲートのステータスを再度確認します。

   「ストレージ・アグリゲート」

   「 storage aggregate show -r -node node_name ！ * root 」

   電源をオフにしたシェルフにドライブがあるアグリゲートの RAID ステータスは「 degraded 」になり、影響を受けたプレックスのドライブのステータスは「 failed 」になります。次に例を示します。

```
cluster_A::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_A_1data01_mirrored
            4.15TB    3.40TB   18% online       3 node_A_1
```

```
raid_dp,

mirrored,

normal
node_A_1root
           707.7GB   34.29GB   95% online       1 node_A_1
raid_dp,

mirrored,

normal
node_A_2_data01_mirrored
            4.15TB    4.12TB    1% online       2 node_A_2
raid_dp,

mirror

degraded
node_A_2_data02_unmirrored
            2.18TB    2.18TB    0% online       1 node_A_2
raid_dp,

normal
node_A_2_root
           707.7GB   34.27GB   95% online       1 node_A_2
raid_dp,

mirror

degraded
cluster_A::> storage aggregate show -r -node node_A_2 !*root
Owner Node: node_A_2
 Aggregate: node_A_2_data01_mirrored (online, raid_dp, mirror degraded)
(block checksums)
  Plex: /node_A_2_data01_mirrored/plex0 (online, normal, active, pool0)
   RAID Group /node_A_2_data01_mirrored/plex0/rg0 (normal, block
checksums)
                                                                   Usable
Physical
     Position Disk                       Pool Type     RPM     Size
Size Status
     -------- -------------------------- ---- ----- ------ --------
-------- ----------
     dparity  2.30.3                      0   BSAS    7200  827.7GB
828.0GB (normal)
```

```
     parity   2.30.4                     0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.6                     0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.8                     0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.5                     0   BSAS    7200  827.7GB
828.0GB (normal)

  Plex: /node_A_2_data01_mirrored/plex4 (offline, failed, inactive,
pool1)
   RAID Group /node_A_2_data01_mirrored/plex4/rg0 (partial, none
checksums)
                                                                  Usable
Physical
     Position Disk                      Pool Type     RPM     Size
Size Status
     -------- ------------------------- ---- ----- ------ --------
-------- ----------
     dparity  FAILED                     -   -          -  827.7GB
-  (failed)
     parity   FAILED                     -   -          -  827.7GB
-  (failed)
     data     FAILED                     -   -          -  827.7GB
-  (failed)
     data     FAILED                     -   -          -  827.7GB
-  (failed)
     data     FAILED                     -   -          -  827.7GB
-  (failed)

 Aggregate: node_A_2_data02_unmirrored (online, raid_dp) (block
checksums)
  Plex: /node_A_2_data02_unmirrored/plex0 (online, normal, active,
pool0)
   RAID Group /node_A_2_data02_unmirrored/plex0/rg0 (normal, block
checksums)
                                                                  Usable
Physical
     Position Disk                      Pool Type     RPM     Size
Size Status
     -------- ------------------------- ---- ----- ------ --------
-------- ----------
     dparity  2.30.12                    0   BSAS    7200  827.7GB
828.0GB (normal)
     parity   2.30.22                    0   BSAS    7200  827.7GB
828.0GB (normal)
```

```
     data     2.30.21                    0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.20                    0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.14                    0   BSAS    7200  827.7GB
828.0GB (normal)
15 entries were displayed.
```

7. データが提供されていること、およびすべてのボリュームがオンラインのままであることを確認します。

   vserver show -type data

   network interface show -fields is-home false

   volume show ！ vol0 、 ！ MDV *

```
cluster_A::> vserver show -type data

cluster_A::> vserver show -type data
                                Admin      Operational Root
Vserver     Type    Subtype    State      State       Volume
Aggregate
----------- ------- ---------- ---------- ----------- ----------
----------
SVM1        data    sync-source           running     SVM1_root
node_A_1_data01_mirrored
SVM2        data    sync-source           running     SVM2_root
node_A_1_data01_mirrored

cluster_A::> network interface show -fields is-home false
There are no entries matching your query.

cluster_A::> volume show !vol0,!MDV*
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
SVM1
          SVM1_root
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.50GB    5%
SVM1
          SVM1_data_vol
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_root
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_data_vol
                       node_A_2_data02_unmirrored
                                    online     RW          1GB
972.6MB    5%
```

8. シェルフの電源を物理的にオンにします。

   再同期が自動的に開始されます

9. 再同期が開始されたことを確認します。

   「 storage aggregate show

   次の例に示すように、影響を受けたアグリゲートの RAID ステータスは「 resyncing 」になります。

```
cluster_A::> storage aggregate show
cluster Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_A_1_data01_mirrored
            4.15TB    3.40TB   18% online       3 node_A_1
raid_dp,

mirrored,

normal
node_A_1_root
           707.7GB   34.29GB   95% online       1 node_A_1
raid_dp,

mirrored,

normal
node_A_2_data01_mirrored
            4.15TB    4.12TB    1% online       2 node_A_2
raid_dp,

resyncing
node_A_2_data02_unmirrored
            2.18TB    2.18TB    0% online       1 node_A_2
raid_dp,

normal
node_A_2_root
           707.7GB   34.27GB   95% online       1 node_A_2
raid_dp,

resyncing
```

10. アグリゲートを監視して、再同期が完了したことを確認します。

    「 storage aggregate show

次の例に示すように、影響を受けるアグリゲートの RAID ステータスは「 normal 」になります。

```
cluster_A::> storage aggregate show
cluster Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_A_1data01_mirrored
            4.15TB    3.40TB   18% online       3 node_A_1
raid_dp,

mirrored,

normal
node_A_1root
           707.7GB   34.29GB   95% online       1 node_A_1
raid_dp,

mirrored,

normal
node_A_2_data01_mirrored
            4.15TB    4.12TB    1% online       2 node_A_2
raid_dp,

normal
node_A_2_data02_unmirrored
            2.18TB    2.18TB    0% online       1 node_A_2
raid_dp,

normal
node_A_2_root
           707.7GB   34.27GB   95% online       1 node_A_2
raid_dp,

resyncing
```

MetroCluster 構成を削除

MetroCluster構成を削除する必要がある場合は、テクニカル サポートにお問い合わせください。

NetAppテクニカルサポートに連絡し、構成に適したガイドを参照してください。 "MetroCluster 構成-解決ガイドからノードを削除する方法"

MetroClusterの構成解除を元に戻すことはできません。このプロセスは、テクニカルサポートの支援を受けてのみ実行してください。MetroCluster構成を削除した後、すべてのMetroCluster接続と相互接続をサポート可能な状態に調整する必要があります。

Active IQ Unified Manager と ONTAP System Manager を使用して設定と監視を強化する方法

Active IQ Unified ManagerおよびONTAPシステムマネージャを使用して詳細な設定と監視を行う

Active IQ Unified Manager と ONTAP の System Manager は、 GUI を使用したクラスタ管理および設定監視に使用できます。

各ノードには ONTAP System Manager が事前にインストールされています。System Manager をロードするには、ノードに接続されている Web ブラウザのアドレスバーにクラスタ管理 LIF アドレスを入力します。

Active IQ Unified Manager を使用して MetroCluster 設定を監視することもできます。

関連情報

"Active IQ Unified Managerのドキュメント"

NTP を使用してシステム時刻を同期します

ノードとそのクライアントの間で時刻を同期するには、クラスタごとに独自の Network Time Protocol （ NTP ；ネットワークタイムプロトコル）サーバが必要です。

このタスクについて

- テイクオーバーの発生後に障害ノードまたはパートナーノードのタイムゾーン設定を変更することはできません。
- ストレッチMetroCluster構成のクラスタごとに、そのMetroClusterサイトのノードで使用する独自のNTPサーバをそれぞれ用意する必要があります。
- MetroCluster Tiebreaker ソフトウェアを使用する場合は、それ専用の NTP サーバも必要です。

ONTAPのバージョンに応じて、System Manager UIの*タブまたは[インサイト]*タブでNTPを設定できます。

クラスタ

System Managerでは、ONTAPのバージョンに応じて*[クラスタ]*タブから次の2つのオプションを使用してNTPを設定できます。

ONTAP 9.8以降：

次の手順に従って、ONTAP 9.8以降の*[クラスタ]*タブからNTPを同期します。

手順

1. [クラスタ]>[概要]*に移動します。
2. 次に、オプションを選択し 

て*[編集]*を選択します。
3. ウィンドウで、**[NTP**サーバ**]**の下の+追加*オプションを選択します。
4. タイムサーバの名前と場所を追加し、IPアドレスを指定します。
5. 次に、*[保存]*を選択します。
6. タイムサーバを追加する場合は、この手順を繰り返します。

ONTAP 9.11.1以降：

次の手順に従って、ONTAP 9.11.1以降の*[クラスタ]タブの*[インサイト]*ウィンドウからNTPを同期します。

手順

1. [クラスタ]>[概要]*に移動します。
2. ページの* Insights ウィンドウまで下にスクロールし、 Too few NTP servers are configured（設定されているNTPサーバが少なすぎる）を探して Fix it（修正）*を選択します。
3. タイムサーバのIPアドレスを指定し、*[保存]*を選択します。
4. タイムサーバを追加する場合は、上記の手順を繰り返します。

分析

ONTAP 9.11.1以降では、System Managerの*[Insights]*タブを使用してNTPを設定することもできます。

手順

1. System Manager UIの*[Insights]*タブに移動します。
2. 下にスクロールして*を選択し、[Fix it]*を選択します。
3. タイムサーバのIPアドレスを指定し、*[保存]*を選択します。
4. タイムサーバを追加する場合は、上記の手順を繰り返します。

MetroCluster 構成で ONTAP を使用する場合の考慮事項

MetroCluster 構成で ONTAP を使用する場合は、ライセンス、 MetroCluster 構成の外部にあるクラスタとのピアリング、ボリューム処理や NVFAIL 処理などの ONTAP 処理の実行について、一定の考慮事項に注意する必要があります。

ライセンスに関する考慮事項

- 両方のサイトに、同じサイトライセンスが設定されている必要があります。
- すべてのノードに同じノードロック式ライセンスが設定されている必要があります。

SnapMirror に関する考慮事項

- SnapMirror SVM ディザスタリカバリは、 ONTAP 9.5 以降のバージョンを実行している MetroCluster 構成でのみサポートされます。

MetroCluster 構成での FlexCache のサポート

ONTAP 9.7 以降では、 MetroCluster 構成で FlexCache ボリュームがサポートされます。スイッチオーバーまたはスイッチバック処理後の手動廃止の要件を理解しておく必要があります。

FlexCache の元のデータとキャッシュが同じ MetroCluster サイト内にある場合のスイッチオーバー後の SVM 削除

ネゴシエートスイッチオーバーまたは計画外スイッチオーバーのあと、クラスタ内の SVM FlexCache ピア関係を手動で設定する必要があります。

たとえば、 SVM vs1 （キャッシュ）と vs2 （元）が site_A にあるとしますこれらの SVM はピア関係にあります。

スイッチオーバー後、 SVM vs1-mc と vs2-mc がパートナーサイト（ site_B ）でアクティブになります。FlexCache が「 vserver peer repeer 」コマンドを使用して機能するには、これらの機能を手動で廃止する必要があります。

FlexCache デスティネーションが第 3 のクラスタにあり、切断モードの場合のスイッチオーバーまたはスイッチバック後の SVM 削除

MetroCluster 構成外のクラスタへの FlexCache 関係では、スイッチオーバー中に関連するクラスタが切断モードになっている場合、スイッチオーバー後に常にピアリングを手動で再設定する必要があります。

例：

- MetroCluster （ vs1 の cache_1 ）の一端が FlexCache site_A にある場合は、 FlexCache の一端になっています
- FlexCache のもう一方の端（ vs2 の origin_1 ）は、 site_A に配置されています（ MetroCluster 構成ではありません）。

スイッチオーバーがトリガーされたときに site_A と site_B が接続されていない場合は、スイッチオーバー後に「 vserver peer repeer 」コマンドを使用して site_B の SVM （スイッチオーバークラスタ）と site_B の SVM を手動で再ピアリングする必要があります。

スイッチバックが実行された場合は、 site_A （元のクラスタ）と site_B の SVM のピア関係を再設定する必要があります

MetroCluster 構成での FabricPool のサポート

ONTAP 9.7 以降では、 MetroCluster 構成で FabricPool ストレージ階層がサポートされます。

FabricPool の使用に関する一般的な情報については、を参照してください "ディスクとアグリゲートの管理"。

FabricPool を使用する際の考慮事項

- クラスタに同じ容量制限の FabricPool ライセンスが必要です。
- 各クラスタに同じ名前の IPspace が必要です。

  これは、デフォルト IPspace または管理者が作成した IP スペースです。この IPspace は、 FabricPool オブジェクトストア設定のセットアップに使用されます。

- 選択したIPspaceについて、外部のオブジェクトストアにアクセスできるクラスタ間LIFが各クラスタで定義されている必要があります。

ミラーリングされた **FabricPool** で使用するアグリゲートを設定する

> アグリゲートを設定する前に、 FabricPool の「 MetroCluster 用のオブジェクトストアのセットアップ」の説明に従ってオブジェクトストアを設定する必要があります "ディスクとアグリゲートの管理"。

FabricPool で使用するアグリゲートを設定するには、次の手順を実行します。

1. アグリゲートを作成するか、既存のアグリゲートを選択します。
2. アグリゲートを MetroCluster 構成内の標準のミラーアグリゲートとしてミラーリングします。
3. の説明に従って、アグリゲートを使用して FabricPool ミラーを作成します "ディスクとアグリゲートの管理"：
   a. プライマリオブジェクトストアを接続します。

      このオブジェクトストアは、クラスタに物理的に近い場所にあります。

   b. ミラーオブジェクトストアを追加します。

      このオブジェクトストアは、プライマリオブジェクトストアよりもクラスタから物理的に離れています。

MetroCluster 構成での FlexGroup のサポート

ONTAP 9.6 以降では、 MetroCluster 構成で FlexGroup ボリュームがサポートされます。

MetroCluster 構成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、どういった整合性が必要とされるかも把握しておく必要があります。

関連情報

"ONTAP の概念"

IPspace オブジェクトのレプリケーションとサブネットの設定の要件

パートナークラスタに IPspace オブジェクトをレプリケートするための要件、および MetroCluster 構成でサブネットと IPv6 を設定するための要件を理解しておく必要があります。

IPspace レプリケーション

IPspace オブジェクトをパートナークラスタにレプリケートするときは、次のガイドラインを考慮する必要があります。

- 2 つのサイトの IPspace 名が一致している必要があります。
- IPspace オブジェクトは手動でパートナークラスタにレプリケートする必要があります。

  IPspace をレプリケートする前に作成されて IPspace に割り当てられた Storage Virtual Machine （ SVM ）は、パートナークラスタにレプリケートされません。

サブネット構成

MetroCluster 構成でサブネットを設定するときは、次のガイドラインを考慮する必要があります。

- MetroCluster 構成の両方のクラスタのサブネットが同じ IPspace にあり、サブネット名、サブネット、ブロードキャストドメイン、ゲートウェイが同じである必要があります。
- 2 つのクラスタの IP 範囲が同じである必要があります。

次の例では、 IP 範囲が異なります。

```
cluster_A::> network subnet show

IPspace: Default
Subnet                       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。

MetroCluster 構成での LIF の作成に関する要件

MetroCluster 構成でネットワークを設定するときは、 LIF の作成に関する要件に注意する必要があります。

LIF を作成する際は、次のガイドラインを考慮する必要があります。

- Fibre Channel ：ストレッチ VSAN またはストレッチファブリックを使用する必要があります。
- IP / iSCSI ：レイヤ 2 拡張ネットワークを使用する必要があります。
- ARP ブロードキャスト： 2 つのクラスタ間で ARP ブロードキャストを有効にする必要があります。
- LIF の重複：同じ IPspace に同じ IP アドレスを持つ複数の LIF （重複する LIF ）を作成することはできません。
- NFS および SAN 構成：ミラーされていないアグリゲートとミラーされたアグリゲートの両方に、異なる Storage Virtual Machine （ SVM ）を使用する必要があります。
- LIFを作成する前にサブネットオブジェクトを作成する必要があります。ONTAPにはブロードキャストドメインが関連付けられているため、サブネットオブジェクトを使用してデスティネーションクラスタのフェイルオーバーターゲットを決定できます。

LIF の作成を確認

MetroCluster 構成内で LIF が正常に作成されたことを確認するには、「 MetroCluster check lif show 」コマン

ドを実行します。LIF の作成中に問題が発生した場合は、「 MetroCluster check lif repair-placement 」コマンドを使用して問題を修正できます。

LIF のレプリケーションおよび配置の要件と問題

MetroCluster 構成での LIF のレプリケーションの要件を理解しておく必要があります。また、レプリケートされた LIF がパートナークラスタにどのように配置されるかを把握し、 LIF のレプリケーションまたは LIF の配置に失敗した場合に発生する問題について確認しておく必要があります。

パートナークラスタへの LIF のレプリケーション

MetroCluster 構成内の 1 つのクラスタに LIF を作成すると、その LIF はパートナークラスタにレプリケートされます。LIF は名前に基づいて 1 対 1 で配置されるわけではありません。スイッチオーバー処理後に LIF を使用できるようにするため、 LIF の配置プロセスは、ポートが LIF をホストできるかどうかを到達可能性とポート属性チェックに基づいて検証します。

LIF をレプリケートしてパートナークラスタに配置するには、システムが次の条件を満たしている必要があります。

条件	LIF タイプ： FC	LIF タイプ： IP / iSCSI
ノードの識別	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 のポートがない場合は LIF を配置できません。 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。 DR サイトに同じファブリックがない場合、 LIF は DR パートナーの任意のポートに配置されます。	上記で特定された DR クラスタの各ポートから配置する LIF のソース IP アドレスに Address Resolution Protocol （ ARP ）ブロードキャストが送信され、その応答に基づいて到達可能性が判別されます。 到達可能性チェックが成功するためには、 2 つのクラスタ間で ARP ブロードキャストが許可されている必要があります。 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 では、アダプタタイプや速度などの属性に基づいてポートが分類され、属性が一致するポートが選択されます。 属性が一致するポートがない場合、 LIF は DR パートナーの任意の接続されたポートに配置されます。	到達可能性チェックで到達可能とマークされたポートのうち、 ONTAP が優先して LIF のサブネットに関連付けられたブロードキャストドメイン内のポートを選択します。 DR クラスタに LIF のサブネットに関連付けられたブロードキャストドメイン内の使用可能なネットワークポートがない場合は、ソース LIF に到達可能なポートが ONTAP によって選択されます。 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は移動されません。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。

ルートアグリゲートでのボリューム作成

MetroCluster 構成内のノードのルートアグリゲート（ HA ポリシーが CFO ）に新しいボリュームを作成することはできません。

この制限があるため、ルートアグリゲートを vserver add-aggregates コマンドで SVM に追加することはできません。

MetroCluster 構成の SVM ディザスタリカバリ

ONTAP 9.5 以降では、 MetroCluster 構成のアクティブな Storage Virtual Machine （ SVM ）を SnapMirror SVM ディザスタリカバリ機能でソースとして使用できます。デスティネーション SVM は、 MetroCluster 構成外の第 3 のクラスタに配置する必要があります。

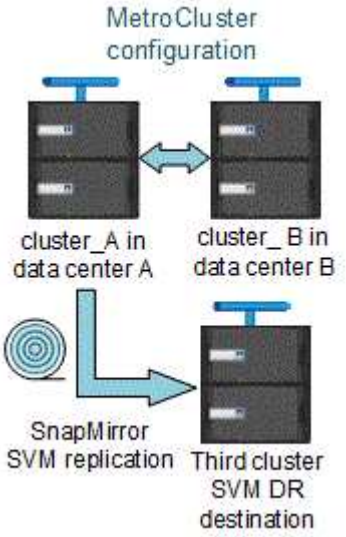
SVM を SnapMirror ディザスタリカバリで使用する場合は、次の要件と制限事項に注意してください。

- SVM ディザスタリカバリ関係のソースとして使用できるのは、 MetroCluster 構成内のアクティブな SVM だけです。

  スイッチオーバー前の同期元の SVM とスイッチオーバー後の同期先の SVM のどちらもソースに使用できます。

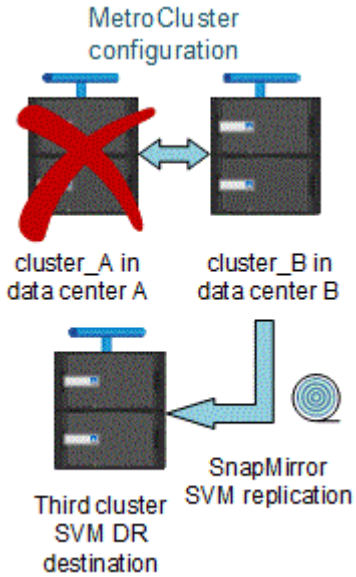
- MetroCluster 構成が安定した状態のときは MetroCluster の同期先の SVM はオンラインでないため、同期先ボリュームを SVM ディザスタリカバリ関係のソースにすることはできません。

  次の図は、安定した状態における SVM ディザスタリカバリの動作を示しています。



- SVM DR 関係のソースが同期元の SVM の場合、ソースの SVM DR 関係情報が MetroCluster パートナーにレプリケートされます。

  これにより、次の図に示すように、スイッチオーバー後も SVM DR の更新を続行できます。



- スイッチオーバーおよびスイッチバックの実行中に、 SVM DR のデスティネーションへのレプリケーションが失敗することがあります。

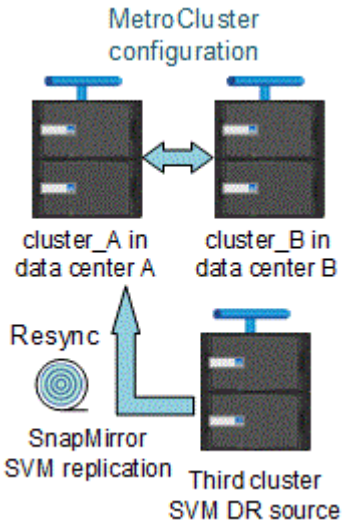
  ただし、スイッチオーバーまたはスイッチバックプロセスの完了後、 SVM DR の次回のスケジュールされている更新は成功します。

の「 SVM の設定のレプリケート」セクションを参照してください "CLI によるデータ保護" SVM DR 関係の設定の詳細については、を参照してください。

ディザスタリカバリサイトでの **SVM** の再同期

再同期では、 MetroCluster 構成の Storage Virtual Machine （ SVM ）ディザスタリカバリ（ DR ）ソースが MetroCluster でないサイトのデスティネーション SVM からリストアされます。

再同期中は、次の図に示すように、ソース SVM （ cluster_A ）が一時的にデスティネーション SVM として機能します。



再同期中に計画外スイッチオーバーが発生した場合

再同期中に計画外スイッチオーバーが発生すると、再同期の転送が停止します。計画外スイッチオーバーが発生した場合は次のようになります。

- MetroCluster サイトのデスティネーション SVM （再同期前のソース SVM ）は、デスティネーション SVM のままです。パートナークラスタの SVM は、同じサブタイプで非アクティブのままです。
- 同期先の SVM をデスティネーションとする SnapMirror 関係を手動で再作成する必要があります。
- スイッチオーバー後、 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。

2 ノードストレッチ **MetroCluster** 構成での **storage disk show** コマンドおよび **storage shelf show** コマンドの出力

2 ノードストレッチ MetroCluster 構成では、「 storage disk show 」コマンドと「 storage shelf show 」コマンドの「 is-local-attach 」フィールドに、ディスクとストレージシェルフがどのノードに接続されているかに関係なく、すべてローカルとして表示されます。

MetroCluster スイッチオーバー後に storage aggregate plex show コマンドの出力が確定しない

MetroCluster のスイッチオーバー後に「 storage aggregate plex show 」コマンドを実行すると、スイッチオーバーされたルートアグリゲートの plex0 のステータスが確定していないため、「 failed 」と表示されます。この間、スイッチオーバーされたルートは更新されません。このプレックスの実際のステータスは、MetroCluster 修復フェーズ後に確定します。

スイッチオーバー発生時に NVFAIL フラグを設定するためのボリュームの変更

MetroCluster スイッチオーバーが発生した場合に NVFAIL フラグが設定されるようにボリュームを変更することができます。NVFAIL フラグが設定されたボリュームは、一切変更されなくなります。コミットされた書き込みがスイッチオーバー後に失われたと想定してボリュームを処理する必要がある場合は、この変更が必要となります。

> 9.0 よりも前のバージョンの ONTAP では、スイッチオーバーのたびに NVFAIL フラグが設定されます。ONTAP 9.0 以降のバージョンでは、計画外スイッチオーバー（ USO ）が使用されます。

手順

1. スイッチオーバー時に MetroCluster 構成が NVFAIL をトリガーできるようにするには、「 vol-dr-force-nvfail 」パラメータを「 on 」に設定します。

   vol modify -vserver_name_-volume_name_-dr-force-nvfail on `

ストレッチからファブリック接続への MetroCluster 構成の移行

ファブリック接続 MetroCluster 構成では、ノードが異なる場所に配置されます。この地理的な違いにより、災害からの保護が強化されます。ストレッチからファブリック接続 MetroCluster 構成に移行するには、 FC スイッチを追加し、必要に応じて FC-to-SAS ブリッジを追加する必要があります。

- MetroCluster modify -auto-switchover failure-domain auto-disabled コマンドを実行して、両方のクラスタで自動スイッチオーバーを無効にする必要があります。
- ノードをシャットダウンしておく必要があります。

  この手順はシステムの停止を伴います。

MetroCluster 構成の移行は両方のサイトで実行する必要があります。MetroCluster 設定をアップグレードしたあと、両方のクラスタで自動スイッチオーバーを有効にする必要があります。また 'MetroCluster check run' コマンドを実行して ' 構成を検証する必要があります

この手順では、必要な手順の概要を示します。詳細な手順については、の特定のセクションを参照する必要があります "ファブリック接続 MetroCluster のインストールと設定"。インストールと設定のすべてを実行する必要はありません。

手順

1. の「 MetroCluster のインストールの準備」セクションをよく確認して、アップグレードの準備をします "ファブリック接続 MetroCluster のインストールと設定"。
2. 必要なスイッチと FC-to-SAS ブリッジの設置、ケーブル接続、設定を行います。

   の「ファブリック接続 MetroCluster 構成のケーブル接続」セクションの手順を使用する必要があります "ファブリック接続 MetroCluster のインストールと設定"。

3. 次の手順に従って、 MetroCluster 構成を更新します。

   『Configuring the MetroCluster software in ONTAP』の手順は使用しないでください。 "ファブリック接続 MetroCluster のインストールと設定"。

   a. advanced 権限モードに切り替えます。 `+*set -privilege advanced *`

   b. MetroCluster 構成を更新します :`+* MetroCluster configure -refresh true *`

      次のコマンドを実行すると、 controller_A_1 を含む DR グループのすべてのノードの MetroCluster 構成が更新されます。

```
controller_A_1::*> metrocluster configure -refresh true
[Job 009] Job succeeded: Configure is successful.
```

   a. admin 特権モードに戻ります :`+**set -privilege admin**`

4. MetroCluster 構成にエラーがないかどうかを確認し、動作していることを確認します。

   の次のセクションの手順を使用する必要があります "ファブリック接続 MetroCluster のインストールと設定" ：

   - Config Advisor での MetroCluster 構成エラーの確認
   - ローカル HA の処理を検証しています
   - スイッチオーバー、修復、スイッチバックを検証しています

追加情報の参照先

MetroCluster の設定と処理の詳細を確認できます。

MetroCluster およびその他の情報

情報	件名
"ONTAP 9 のドキュメント"	• MetroCluster のすべてのガイド
	• MetroCluster FC の構成と運用の技術概要 • MetroCluster FC 構成のベストプラクティス

"ファブリック接続 MetroCluster のインストールと設定"	• ファブリック接続 MetroCluster アーキテクチャ • 構成のケーブル接続 • FC-to-SAS ブリッジの設定 • FC スイッチを設定します • ONTAP で MetroCluster を設定します
"MetroCluster IP のインストールと設定： ONTAP MetroCluster 構成の違い"	• MetroCluster IP アーキテクチャ • 構成のケーブル接続 • ONTAP で MetroCluster を設定します
"MetroCluster の管理とディザスタリカバリ"	• MetroCluster 構成について • スイッチオーバー、修復、スイッチバック • ディザスタリカバリ（ DR ）
"MetroCluster コンポーネントの保守"	• MetroCluster FC 構成のメンテナンスガイドライン • ハードウェアの交換またはアップグレードFC-to-SAS ブリッジおよび FC スイッチのファームウェアアップグレード手順 • ファブリック接続またはストレッチ MetroCluster FC 構成でのディスクシェルフのホットアド • ファブリック接続またはストレッチ MetroCluster FC 構成でのディスクシェルフのホットリムーブ • ファブリック接続またはストレッチ MetroCluster FC 構成のディザスタリカバリサイトでのハードウェア交換 • 2 ノードのファブリック接続またはストレッチ MetroCluster FC 構成の 4 ノード MetroCluster 構成への拡張 • 4 ノードのファブリック接続またはストレッチ MetroCluster FC 構成の 8 ノード MetroCluster FC 構成への拡張
"MetroCluster FC から MetroCluster IP に移行します" "MetroCluster アップグレードおよび拡張ガイド"	• MetroCluster 設定をアップグレードまたは更新する • MetroCluster FC 構成から MetroCluster IP 構成への移行 • ノードの追加による MetroCluster 構成の拡張
"MetroCluster Tiebreaker ソフトウェアのインストールおよび設定"	• MetroCluster Tiebreaker ソフトウェアを使用して MetroCluster 構成を監視する

Active IQ Unified Manager のドキュメント "ネットアップのマニュアル：製品ガイドとリソース"	• MetroCluster の設定とパフォーマンスを監視する
"コピーベースの移行"	• 7-Mode ストレージシステムから clustered Data ONTAP ストレージシステムへデータを移行する
"ONTAP の概念"	• ミラーされたアグリゲートの機能

MetroCluster Tiebreakerのインストールと設定

MetroCluster Tiebreakerのサポートの新機能

MetroCluster Tiebreakerソフトウェアの機能拡張は、リリースごとに提供されます。MetroCluster Tiebreakerの最近のリリースの新機能は次のとおりです。

拡張機能

ONTAP Tiebreakerのバージョン	拡張機能
1.7	• バグ修正 • CLIを使用したスイッチオーバーシミュレーションのサポートを追加
1.6P1	• サポートライブラリの更新 • セキュリティの機能拡張
1.6	• インストールの容易さの向上 • サポートライブラリの更新 • セキュリティの機能拡張
1.5	• サポートライブラリの更新 • セキュリティの機能拡張
1.4	• サポートライブラリの更新

OSサポートマトリックス

次の表に、Tiebreakerの各バージョンでサポートされるオペレーティングシステムを示します。

TiebreakerノOS	1.7	1.6P1	1.6	1.5	1.4
Rocky Linux 9.4	はい。	はい。	いいえ	いいえ	いいえ
Rocky Linux 9.0	いいえ	いいえ	はい。	いいえ	いいえ
Rocky Linux 8.10	はい。	はい。	いいえ	いいえ	いいえ

Red Hat Enterprise Linux (RHEL) 9.6	はい。	はい。	いいえ	いいえ	いいえ
RHEL 9.5	はい。	はい。	いいえ	いいえ	いいえ
RHEL 9.4	はい。	はい。	いいえ	いいえ	いいえ
RHEL 9.3	いいえ	いいえ	いいえ	いいえ	いいえ
RHEL 9.2	はい。	はい。	はい。	いいえ	いいえ
RHEL 9.1	いいえ	いいえ	はい。	いいえ	いいえ
RHEL 9.0	いいえ	いいえ	はい。	いいえ	いいえ
RHEL 8.11～9.0	いいえ	いいえ	はい。	いいえ	いいえ
RHEL 8.10	はい。	はい。	はい。	いいえ	いいえ
RHEL 8.9	いいえ	いいえ	はい。	いいえ	いいえ
RHEL 8.8	はい。	はい。	はい。	いいえ	いいえ
RHEL 8.1～8.7	いいえ	いいえ	はい。	はい。	はい。
RHEL 7～7.9	いいえ	いいえ	いいえ	いいえ	はい。
CentOS 7-7.9	いいえ	いいえ	いいえ	いいえ	はい。

Tiebreaker ソフトウェアの概要

NetApp MetroCluster Tiebreaker ソフトウェアの概要、およびどのように障害のタイプが特定されるかを理解しておくと、 MetroCluster 構成を効率的に監視できます。設定の管理、および MetroCluster 構成のステータスと処理の監視には、 Tiebreaker の CLI を使用します。

NetApp MetroCluster Tiebreaker ソフトウェアによる障害の検出

Tiebreaker ソフトウェアは、 2 つのクラスタおよびクラスタ間の接続ステータスを第 3 のサイトから監視する場合にのみ使用します。Tiebreakerソフトウェアは3番目のサイトのLinuxホストに配置され、クラスタ内の各パートナーでISL障害（サイト間リンクが停止した場合）とサイト障害を区別できます。

Linux ホストに Tiebreaker ソフトウェアをインストールしたら、災害状況を監視するように MetroCluster 構

成内のクラスタを設定できます。

Tiebreakerソフトウェアでは、最大15個のMetroCluster構成を同時に監視できます。MetroCluster IP構成、MetroCluster FC構成、ストレッチMetroCluster構成の組み合わせがサポートされます。

Tiebreaker ソフトウェアでサイト障害を検出する方法

NetApp MetroCluster Tiebreaker ソフトウェアは、 MetroCluster 構成のノードおよびクラスタに到達できるかどうかをチェックして、サイト障害の有無を判断します。また、 Tiebreaker ソフトウェアは、特定の状況でアラートをトリガーします。

Tiebreaker ソフトウェアで監視されるコンポーネント

Tiebreaker ソフトウェアは、 IP ネットワークでホストされるノード管理 LIF およびクラスタ管理 LIF への複数のパスを経由する冗長接続を確立することによって、 MetroCluster 構成内の各コントローラを監視します。

Tiebreaker ソフトウェアで監視される MetroCluster 構成のコンポーネントは次のとおりです。

- ローカルノードインターフェイスを介してノードを追加します
- クラスタ指定インターフェイスを介したクラスタ
- サバイバークラスタ - ディザスタサイトとの接続の有無を評価（ NV インターコネクト、ストレージ、クラスタ間ピアリング）

Tiebreaker ソフトウェアとクラスタ内のすべてのノードおよびクラスタ自体との接続が失われると、クラスタは Tiebreaker ソフトウェアによって「到達不能」と宣言されます。接続障害は 3~5 秒で検出されます。Tiebreaker ソフトウェアからクラスタに到達できない場合、障害が発生していないクラスタ（到達可能なクラスタ）は、 Tiebreaker ソフトウェアがアラートをトリガーする前に、パートナークラスタへのすべてのリンクが切断されていることを示す必要があります。

> サバイバークラスタが FC （ NV インターコネクトとストレージ）とクラスタ間ピアリングを介してディザスタサイトのクラスタと通信できなくなると、すべてのリンクが切断されたとみなされます。

Tiebreaker ソフトウェアがアラートをトリガーする障害シナリオ

Tiebreaker ソフトウェアは、ディザスタサイトのクラスタ（すべてのノード）が停止しているか到達不能であり、サバイバーサイトのクラスタが「 AllLinksSevered 」ステータスを示している場合、アラートをトリガーします。

次のシナリオでは、 Tiebreaker ソフトウェアはアラートをトリガーしません（またはアラートが拒否されます）。

- 8 ノード MetroCluster 構成で、ディザスタサイトの HA ペアの 1 つが停止している場合
- ディザスタサイトのすべてのノードを含むクラスタが停止し、サバイバーサイトの 1 つの HA ペアが停止し、サバイバーサイトのクラスタが「 AllLinksSevered 」ステータスを示している場合

  Tiebreaker ソフトウェアはアラートをトリガーしますが、 ONTAP はアラートを拒否します。この場合、手動によるスイッチオーバーも拒否されます

- Tiebreaker ソフトウェアがディザスタサイトの少なくとも 1 つのノードまたはクラスタインターフェイス

に到達できる、またはサバイバーサイトが FC （ NV インターコネクトとストレージ）またはクラスタ間ピアリングを介してディザスタサイトのいずれかのノードに到達できる場合

関連情報

"MetroCluster Tiebreaker をアクティブモードで使用する場合のリスクと制限事項"

Tiebreaker ソフトウェアでサイト間接続障害を検出する方法

MetroCluster Tiebreaker ソフトウェアは、サイト間のすべての接続が失われると警告します。

ネットワークパスのタイプ

構成によっては、 MetroCluster 構成の 2 つのクラスタ間のネットワークパスに次の 3 つの種類が存在します。

- * FC ネットワーク（ファブリック接続 MetroCluster 構成に存在） *

  この種類のネットワークは、 2 つの冗長 FC スイッチファブリックで構成されます。各スイッチファブリックには 2 つの FC スイッチがあり、各スイッチファブリックの 1 つのスイッチはクラスタと同じ場所に配置されます。各クラスタには、各スイッチファブリックから 1 つずつ、 2 つの FC スイッチがあります。すべてのノードは、同じ場所に配置されている各 FC スイッチに FC （ NV インターコネクトおよび FCP イニシエータ）接続されています。データは、クラスタからクラスタへ、 ISL 経由でレプリケートされます。

- * クラスタ間ピアリングネットワーク *

  この種類のネットワークは、 2 つのクラスタ間の冗長 IP ネットワークパスで構成されます。クラスタピアリングネットワークは、 Storage Virtual Machine （ SVM ）構成をミラーするために必要な接続を提供します。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。

- * IP ネットワーク（ MetroCluster IP 構成に存在） *

  この種類のネットワークは、 2 つの冗長 IP スイッチネットワークで構成されます。各ネットワークには 2 つの IP スイッチがあり、各スイッチファブリックの 1 つのスイッチはクラスタと同じ場所に配置されます。各クラスタには、各スイッチファブリックから 1 つずつ、 2 つの IP スイッチがあります。すべてのノードは、同じ場所に配置されている各 FC スイッチに接続されています。データは、クラスタからクラスタへ、 ISL 経由でレプリケートされます。

サイト間接続を監視する

Tiebreaker ソフトウェアは、サイト間接続のステータスをノードから定期的に取得します。NV インターコネクト接続が失われ、クラスタ間ピアリングが ping に応答しない場合、クラスタはサイトが分離されているとみなし、 Tiebreaker ソフトウェアは「 AllLinksSevered 」というアラートをトリガーします。クラスタが「 AllLinksSevered 」ステータスを識別し、もう一方のクラスタがネットワーク経由で到達できない場合、 Tiebreaker ソフトウェアは「 `d isaster 」としてアラートをトリガーします。

災害のタイプが Tiebreaker ソフトウェアの検出時間に与える影響

ディザスタリカバリへの対応を適切に計画するために、 MetroCluster Tiebreaker ソフトウェアは災害を検出するまでに一定の時間を要します。この時間は「ディザスター検出時間」です。MetroCluster Tiebreaker ソフトウェアは、災害発生から 30 秒以内にサイト障害を検出し、ディザスタリカバリ処理をトリガーして災害に関する通知を送信します。

検出時間は災害の種類によっても異なり、「ローリング災害」と呼ばれるシナリオによっては 30 秒を超えることもあります。ローリングディザスタの主なタイプは次のとおりです。

- 電源喪失
- パニック
- 停止またはリブートします
- ディザスタサイトの FC スイッチが停止する

電源喪失

Tiebreaker ソフトウェアは、ノードが停止するとすぐにアラートをトリガーします。電源に障害が発生すると、クラスタ間ピアリング、 NV インターコネクト、メールボックスディスクなどのすべての接続と更新が停止します。クラスタが到達不能になってから 5 秒のデフォルトのサイレント時間を含めて、災害が検出され、トリガーがトリガーされるまでの時間は 30 秒以内にする必要があります。

パニック

MetroCluster FC構成では、サイト間のNVインターコネクト接続が停止し、サバイバーサイトのステータスが「AllLinksSevered」になると、Tiebreakerソフトウェアによってアラートがトリガーされます。これはコアダンププロセスが完了するまで発生しません。このシナリオでは、クラスタが到達不能になってから災害が検出されるまでの時間は、コアダンププロセスにかかる時間より長いか、ほぼ同じです。多くの場合、検出時間は 30 秒を超えます。

ノードの動作が停止してもコアダンププロセスのファイルが生成されない場合は、検出時間が 30 秒を超えないようにしてください。MetroCluster IP構成では、NVは通信を停止し、サバイバーサイトはコアダンププロセスを認識しません。

停止またはリブートします

Tiebreaker ソフトウェアは、ノードが停止し、サバイバーサイトのステータスが「 AllLinksSevered 」になった場合にのみアラートをトリガーします。クラスタが到達不能になってから災害が検出されるまでの時間は、30 秒を超える可能性があります。このシナリオで災害の検出にかかる時間は、ディザスタサイトのノードがシャットダウンされるまでの時間によって異なります。

ディザスタサイトの **FC** スイッチの喪失（ファブリック接続 **MetroCluster** 構成）

Tiebreaker ソフトウェアは、ノードが停止するとアラートをトリガーします。FC スイッチが失われると、ノードはディスクへのパスのリカバリを約 30 秒間試行します。この間、ノードはピアリングネットワーク上で稼働し、応答しています。両方の FC スイッチが停止してディスクへのパスをリカバリできない場合、ノードは MultiDiskFailure エラーを生成して停止します。FC スイッチの障害からノードが MultiDiskFailure エラーを生成するまでの時間は約 30 秒長くなります。この 30 秒を災害の検出時間に追加する必要があります。

Tiebreaker の CLI とマニュアルページについて

Tiebreaker の CLI では、 Tiebreaker ソフトウェアをリモートで設定したり、 MetroCluster 構成を監視したりするためのコマンドを実行できます。

CLI のコマンドプロンプトは、 NetApp MetroCluster Tiebreaker ：： > で表されます。

マニュアルページは、 CLI のプロンプトで該当するコマンド名を入力すると表示されます。

Tiebreaker ソフトウェアをインストールします

Tiebreakerのインストールワークフロー

Tiebreaker ソフトウェアは、クラスタストレージ環境に監視機能を提供します。また、ノード接続の問題やサイト障害が発生した場合に SNMP 通知を送信します。

このワークフローについて

このワークフローを使用して、Tiebreakerソフトウェアをインストールまたはアップグレードできます。

1. "Tiebreakerソフトウェアをインストールする準備"

Tiebreakerソフトウェアをインストールして設定する前に、システムが一定の要件を満たしていることを確認してください。

2. "インストールのセキュリティを確保する"

MetroCluster Tiebreaker 1.5以降を実行する構成では、ホストOSとデータベースを保護および強化できます。

3. "Tiebreakerソフトウェアパッケージのインストール"

Tiebreakerソフトウェアの新規インストールまたはアップグレードを実行する。実行するインストール手順は、インストールするTiebreakerのバージョンによって異なります。

Tiebreakerソフトウェアをインストールする準備

Tiebreakerソフトウェアをインストールして設定する前に、システムが一定の要件を満たしていることを確認する必要があります。

ソフトウェア要件

インストールするTiebreakerのバージョンに応じて、次のソフトウェア要件を満たしている必要があります。

ONTAP Tiebreaker のバージョン	サポートされるONTAPのバージョン	サポートされている Linux バージョン	Java/MariaDBノヨウケン
1.7	ONTAP 9.12.1以降	を参照してください "OSサポートマトリックス" を参照してください。	なし依存関係はインストールにバンドルされています。
1.6P1	ONTAP 9.12.1以降	を参照してください "OSサポートマトリックス" を参照してください。	なし依存関係はインストールにバンドルされています。

1.6	ONTAP 9.12.1以降	を参照してください "OSサポートマトリックス" を参照してください。	なし依存関係はインストールにバンドルされています。
1.5	ONTAP 9.8からONTAP 9.14.1へ	• Red Hat Enterprise Linux 8.1から8.7	Red Hat Enterprise Linux 8.1から8.7の場合： • MariaDB 10.x（「yum install MariaDB -server. x86_64」を使用してインストールされたデフォルトバージョンを使用） • OpenJDK 17、18、または19
1.4	ONTAP 9.1からONTAP 9.9.1へ	• Red Hat Enterprise Linux 8.1から8.7 • Red Hat Enterprise Linux 7～7.9 • CentOS 7～7.9 64ビット	CentOSの場合： • MariaDB 5.5.52.x / MySQL サーバ 5.6x • 4GB の RAM • JRE 8を開きます Red Hat Enterprise Linux 8.1から8.7の場合： • MariaDB 10.x（「yum install MariaDB -server. x86_64」を使用してインストールされたデフォルトバージョンを使用） • JRE 8

その他の要件

さらに次の要件に注意する必要があります。

- Tiebreaker ソフトウェアは 3 つ目のサイトにインストールします。これにより、スイッチ間リンク（ ISL ）障害（サイト間リンクが停止している）障害とサイト障害をソフトウェアが区別できるようになります。TiebreakerソフトウェアをインストールまたはアップグレードしてMetroCluster構成を監視するには、ホストシステムが一定の要件を満たしている必要があります。
- MetroCluster Tiebreakerソフトウェアとそれに依存するパッケージをインストールするには、「root」権限が必要です。
- 複数のMetroCluster Tiebreakerモニタとの競合を回避するために、MetroCluster 構成ごとに1つのTiebreakerモニタのみを使用できます。
- Tiebreakerソフトウェアのネットワークタイムプロトコル（NTP）ソースを選択する場合は、ローカルのNTPソースを使用する必要があります。Tiebreakerソフトウェアが監視するMetroClusterサイトと同じソースをTiebreakerソフトウェアで使用しないでください。
- ディスク容量： 8GB
- ファイアウォール：

- AutoSupport メッセージをセットアップするための直接アクセス
- SSH （ポート 22 / TCP ）、 HTTPS （ポート 443 / TCP ）、および ping （ ICMP ）

Tiebreakerのホストとデータベースのインストールを保護する

MetroCluster Tiebreaker 1.5以降を実行する構成では、ホストOSとデータベースを保護および強化できます。

ホストを保護します

次のガイドラインは、Tiebreakerソフトウェアがインストールされているホストを保護する方法を示しています。

ユーザ管理の推奨事項

- 「root」ユーザのアクセスを制限します。
  - rootアクセスに昇格できるユーザを使用して、Tiebreakerソフトウェアをインストールおよび管理できます。
  - ルートアクセスに昇格できないユーザを使用してTiebreakerソフトウェアを管理できます。
  - インストール時に、「mcctbgrp」という名前のグループを作成する必要があります。ホストのrootユーザとインストール中に作成されたユーザは、両方ともメンバーである必要があります。Tiebreakerソフトウェアを完全に管理できるのは、このグループのメンバーだけです。

    このグループのメンバーでないユーザはTiebreakerソフトウェアやCLIにアクセスできません。ホスト上に追加のユーザを作成して、それらのユーザをグループのメンバーにすることができます。これらの追加メンバーは、Tiebreakerソフトウェアを完全に管理することはできません。ReadOnlyにアクセスできるため、モニタの追加、変更、削除はできません。

  - Tiebreakerをrootユーザとして実行しないでください。Tiebreakerの実行には、権限のない専用のサービスアカウントを使用します。
- 「/etc/snmp/snmpd.conf」ファイルのデフォルトのコミュニティストリングを変更します。
- 最小限の書き込み権限を許可します。権限のないTiebreakerサービスアカウントには、実行可能バイナリや構成ファイルを上書きするアクセス権がありません。Tiebreakerユーザが書き込みできるのは、ローカルのTiebreakerストレージ（統合バックエンドストレージなど）または監査ログのディレクトリとファイルだけです。
- 匿名ユーザを許可しないでください。
  - AllowTcpForwardingを「no」に設定するか、matchディレクティブを使用して匿名ユーザを制限します。

関連情報

- "Red Hat Enterprise Linux 8の製品ドキュメント"
- "Red Hat Enterprise Linux 9製品ドキュメント"
- "Rocky Linux製品ドキュメント"

- ディスク暗号化を使用する
  - ディスク暗号化を有効にすることができます。FullDiskEncryption（ハードウェア）か、HostOS（ソフトウェア）またはSVMホストが提供する暗号化です。
- 着信接続を許可する未使用のサービスを無効にします。使用していないサービスは無効にすることができます。Tiebreakerソフトウェアでは、Tiebreakerインストールからの接続はすべて発信であるため、受信接続にサービスは必要ありません。デフォルトで有効になっていて無効にできるサービスは次のとおりです。
  - HTTP / HTTPSサーバ
  - FTPサーバ
  - Telnet、RSH、rlogin
  - NFS、CIFS、およびその他のプロトコルアクセス
  - RDP（RemoteDesktopProtocol）、X11サーバ、VNC、またはその他のリモート「デスクトップ」サービスプロバイダー。

> ホストをリモートで管理するには、シリアルコンソールアクセス（サポートされている場合）または少なくとも1つのプロトコルを有効にしておく必要があります。すべてのプロトコルを無効にすると、管理のためにホストに物理的にアクセスする必要があります。

- FIPSを使用してホストを保護します
  - ホストOSをFIPS準拠モードでインストールしてからTiebreakerをインストールできます。

> OpenJDK 19は、ホストがFIPSモードでインストールされているかどうかを起動時にチェックします。手動で変更する必要はありません。

  - ホストを保護する場合は、ユーザの介入なしにホストがブートできることを確認する必要があります。ユーザの操作が必要な場合、ホストが予期せずリブートしたときにTiebreaker機能を使用できないことがあります。この場合、Tiebreaker機能は手動操作後、ホストが完全にブートされた場合にのみ使用できます。
- シェルコマンド履歴を無効にします。
- 頻繁にアップグレードする。Tiebreakerは積極的に開発されており、セキュリティ修正プログラムや、キーの長さや暗号スイートなどのデフォルト設定の変更を組み込むには、頻繁に更新することが重要です。
- HashiCorp Announcementメーリングリストに登録すると、新しいリリースのお知らせを受け取ることができます。Tiebreaker CHANGELOGにアクセスして、新しいリリースの最新のアップデートの詳細を確認してください。
- 正しいファイル権限を使用してください。Tiebreakerソフトウェアを起動する前に、特に機密情報を含むファイルに対して適切な権限が適用されていることを必ず確認してください。
- 多要素認証（MFA）は、管理者がユーザ名とパスワード以外のものを使用して自身を識別するように要求することで、組織のセキュリティを強化します。ユーザー名とパスワードは重要ですが、ブルートフォース攻撃に対して脆弱であり、第三者によって盗まれる可能性があります。
  - Red Hat Enterprise Linux 8にはMFAが用意されており、アカウントまたはLinuxホストに対して正常に認証するために複数の情報を指定する必要があります。追加情報 は、SMSまたはGoogle Authenticator、Twilio Authy、FreeOTPなどのアプリからの認証情報を介して携帯電話に送信されるワ

ンタイムパスワードです。

関連情報

- "Red Hat Enterprise Linux 8の製品ドキュメント"
- "Red Hat Enterprise Linux 9製品ドキュメント"
- "Rocky Linux製品ドキュメント"

データベースのインストールを保護します

次のガイドラインは、MariaDB 10.xデータベースのインストールを保護および強化する方法を示しています。

- 「root」ユーザのアクセスを制限します。
  - Tiebreakerは専用のアカウントを使用します。（設定）データを格納するアカウントとテーブルは、Tiebreakerのインストール時に作成されます。データベースへの昇格アクセスが必要なのは、インストール中だけです。
- インストール中は、次のアクセス権と権限が必要です。
  - データベースとテーブルを作成する機能
  - グローバルオプションを作成する機能
  - データベースユーザを作成し、パスワードを設定する機能
  - データベース・ユーザをデータベースおよびテーブルに関連付け、アクセス権を割り当てる機能

  Tiebreakerのインストール時に指定するユーザアカウントには、これらのすべての権限が必要です。異なるタスクに複数のユーザアカウントを使用することはサポートされていません。
- データベースの暗号化を使用します
  - 保存データの暗号化がサポートされています。"保存データ暗号化の詳細"
  - 転送中のデータは暗号化されません。転送中のデータは、ローカルの「ソックス」ファイル接続を使用します。
  - MariaDBのFIPS準拠—データベースでFIPS準拠を有効にする必要はありません。FIPS準拠モードでホストをインストールすれば十分です。

    "MySQL Enterprise Transparent Data Encryption（TDE）の詳細"

  暗号化設定は、Tiebreakerソフトウェアをインストールする前に有効にする必要があります。

関連情報

- データベースユーザ管理

  "アクセス制御とアカウント管理"

- データベースを保護します

"MySQLを攻撃者から保護する"

"MariaDBの保護"

- Vaultインストールを保護します

"生産性の強化"

Tiebreakerソフトウェアパッケージのインストール

インストール手順の選択

Tiebreakerのインストール手順は、インストールするTiebreakerのバージョンによって異なります。

Tiebreakerバージョン	手順
Tiebreaker 1.7	"Tiebreaker 1.7のインストール"
タイブレーカー 1.6 または 1.6P1	"Tiebreaker 1.6または1.6P1をインストールする"
Tiebreaker 1.5	"Tiebreaker 1.5をインストール"
Tiebreaker 1.4	"Tiebreaker 1.4のインストール"

MetroCluster Tiebreaker 1.7 をインストールする

MetroCluster構成を監視するには、Linux ホストに Tiebreaker 1.7 をインストールするか、アップグレードします。

このタスクについて

- ストレージシステムでONTAP 9.12.1以降が実行されている必要があります。
- Tiebreaker 1.6P1 からのみ Tiebreaker 1.7 にアップグレードできます。参照"Tiebreaker 1.6または1.6P1をインストールする"。
- MetroCluster Tiebreakerは、Tiebreakerのインストール、テーブルとユーザの作成、ユーザパスワードの設定に必要な管理権限を持つroot以外のユーザとしてインストールできます。

手順

1. MetroCluster Tiebreaker 1.7ソフトウェアをダウンロードします。

   "MetroCluster Tiebreaker（ダウンロード）- NetApp Support Site"

2. root ユーザとしてホストにログインします。
3. アップグレードする場合は、実行している Tiebreaker のバージョンを確認してください。

   次の例はタイブレーカー1.6P1を示しています

```
[root@mcctb ~] # netapp-metrocluster-tiebreaker-software-cli
NetApp MetroCluster Tiebreaker :> version show
NetApp MetroCluster Tiebreaker 1.6P1: Sun Mar 13 09:59:02 IST 2022
NetApp MetroCluster Tiebreaker :> exit
```

4. Tiebreakerソフトウェアをインストールまたはアップグレードします。

Tiebreaker 1.7のインストール

Tiebreaker 1.7を新規にインストールする場合は、次の手順を実行します。

手順

a. で次のコマンドを実行します。 `[root@mcctb ~] #` インストールを開始するようにプロンプトを表示します。

```
sh MetroClusterTiebreakerInstall-1.7
```

インストールが完了すると、次の出力が表示されます。

例

```
Extracting the MetroCluster Tiebreaker installation/upgrade
archive
Install digest hash is Ok
Performing the MetroCluster Tiebreaker code signature check
Install code signature is Ok
Enter unix user account to use for the installation:
mcctbadminuser
Unix user account "mcctbadminuser" doesn't exist. Do you wish
to create "mcctbadminuser" user account? [Y/N]: y
useradd: warning: the home directory already exists.
Not copying any file from skel directory into it.
Creating mailbox file: File exists
Unix account "mcctbadminuser" created.
Changing password for user mcctbadminuser.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
MetroCluster Tiebreaker requires unix user account
"mcctbadminuser" to be added to the group "mcctbgrp" for admin
access.
Do you wish to add ? [Y/N]: y
Unix user account "mcctbadminuser" added to "mcctbgrp".
Do you wish to generate your own public-private key pair for
encrypting audit log? [Y/N]: y
Generating public-private key pair...
Configuring Vault...
Starting vault server...
==> Vault server configuration:

             Api Address: <api_address>
                     Cgo: disabled
         Cluster Address: <cluster_address>
   Environment Variables: BASH_FUNC_which%%,
DBUS_SESSION_BUS_ADDRESS, GODEBUG, HISTCONTROL, HISTSIZE,
HOME, HOSTNAME, HOST_ACCOUNT, LANG, LESSOPEN, LOGNAME,
LS_COLORS, MAIL, PATH, PWD, SHELL, SHLVL, SSH_CLIENT,
SSH_CONNECTION, SSH_TTY, STAF_TEMP_DIR, TERM, USER,
VAULT_ADDR, VAULT_TOKEN, XDG_RUNTIME_DIR, XDG_SESSION_ID, _,
vault_Addr, which_declare
              Go Version: go1.20.5
              Listener 1: tcp (addr: "0.0.0.0:8200", cluster
address: "0.0.0.0:8201", max_request_duration: "1m30s",
max_request_size: "33554432", tls: "enabled")
```

```
               Log Level:
                   Mlock: supported: true, enabled: true
           Recovery Mode: false
                 Storage: file
                 Version: Vault v1.14.0, built 2023-06-
19T11:40:23Z
             Version Sha:
13a649f860186dffe3f3a4459814d87191efc321

==> Vault server started! Log data will stream in below:

2023-11-23T15:14:28.532+0530 [INFO]  proxy environment:
http_proxy="" https_proxy="" no_proxy=""
2023-11-23T15:14:28.577+0530 [INFO]  core: Initializing
version history cache for core
2023-11-23T15:14:38.552+0530 [INFO]  core: security barrier
not initialized
2023-11-23T15:14:38.552+0530 [INFO]  core: seal configuration
missing, not initialized
2023-11-23T15:14:38.554+0530 [INFO]  core: security barrier
not initialized
2023-11-23T15:14:38.555+0530 [INFO]  core: security barrier
initialized: stored=1 shares=5 threshold=3
2023-11-23T15:14:38.556+0530 [INFO]  core: post-unseal setup
starting
2023-11-23T15:14:38.577+0530 [INFO]  core: loaded wrapping
token key
2023-11-23T15:14:38.577+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-11-23T15:14:38.577+0530 [INFO]  core: no mounts; adding
default mount table
2023-11-23T15:14:38.578+0530 [INFO]  core: successfully
mounted: type=cubbyhole version="v1.14.0+builtin.vault"
path=cubbyhole/ namespace="ID: root. Path: "
2023-11-23T15:14:38.578+0530 [INFO]  core: successfully
mounted: type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-11-23T15:14:38.578+0530 [INFO]  core: successfully
mounted: type=identity version="v1.14.0+builtin.vault"
path=identity/ namespace="ID: root. Path: "
2023-11-23T15:14:38.581+0530 [INFO]  core: successfully
mounted: type=token version="v1.14.0+builtin.vault"
path=token/ namespace="ID: root. Path: "
2023-11-23T15:14:38.581+0530 [INFO]  rollback: starting
rollback manager
2023-11-23T15:14:38.581+0530 [INFO]  core: restoring leases
```

```
2023-11-23T15:14:38.582+0530 [INFO]  expiration: lease restore
complete
2023-11-23T15:14:38.582+0530 [INFO]  identity: entities
restored
2023-11-23T15:14:38.582+0530 [INFO]  identity: groups restored
2023-11-23T15:14:38.583+0530 [INFO]  core: Recorded vault
version: vault version=1.14.0 upgrade time="2023-11-23
09:44:38.582881162 +0000 UTC" build date=2023-06-19T11:40:23Z
2023-11-23T15:14:38.583+0530 [INFO]  core: usage gauge
collection is disabled
2023-11-23T15:14:38.998+0530 [INFO]  core: post-unseal setup
complete
2023-11-23T15:14:38.999+0530 [INFO]  core: root token
generated
2023-11-23T15:14:38.999+0530 [INFO]  core: pre-seal teardown
starting
2023-11-23T15:14:38.999+0530 [INFO]  rollback: stopping
rollback manager
2023-11-23T15:14:38.999+0530 [INFO]  core: pre-seal teardown
complete
2023-11-23T15:14:39.311+0530 [INFO]  core.cluster-
listener.tcp: starting listener: listener_address=0.0.0.0:8201
2023-11-23T15:14:39.311+0530 [INFO]  core.cluster-listener:
serving cluster requests: cluster_listen_address=[::]:8201
2023-11-23T15:14:39.312+0530 [INFO]  core: post-unseal setup
starting
2023-11-23T15:14:39.312+0530 [INFO]  core: loaded wrapping
token key
2023-11-23T15:14:39.312+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-11-23T15:14:39.313+0530 [INFO]  core: successfully
mounted: type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-11-23T15:14:39.313+0530 [INFO]  core: successfully
mounted: type=identity version="v1.14.0+builtin.vault"
path=identity/ namespace="ID: root. Path: "
2023-11-23T15:14:39.313+0530 [INFO]  core: successfully
mounted: type=cubbyhole version="v1.14.0+builtin.vault"
path=cubbyhole/ namespace="ID: root. Path: "
2023-11-23T15:14:39.314+0530 [INFO]  core: successfully
mounted: type=token version="v1.14.0+builtin.vault"
path=token/ namespace="ID: root. Path: "
2023-11-23T15:14:39.314+0530 [INFO]  rollback: starting
rollback manager
2023-11-23T15:14:39.314+0530 [INFO]  core: restoring leases
2023-11-23T15:14:39.314+0530 [INFO]  identity: entities
```

```
restored
2023-11-23T15:14:39.314+0530 [INFO]  expiration: lease restore
complete
2023-11-23T15:14:39.314+0530 [INFO]  identity: groups restored
2023-11-23T15:14:39.315+0530 [INFO]  core: usage gauge
collection is disabled
2023-11-23T15:14:39.316+0530 [INFO]  core: post-unseal setup
complete
2023-11-23T15:14:39.316+0530 [INFO]  core: vault is unsealed
Success! Uploaded policy: mcctb-policy
2023-11-23T15:14:39.795+0530 [INFO]  core: enabled credential
backend: path=approle/ type=approle version=""
Success! Enabled approle auth method at: approle/
2023-11-23T15:14:39.885+0530 [INFO]  core: successful mount:
namespace="" path=mcctb/ type=kv version=""
Success! Enabled the kv secrets engine at: mcctb/
Success! Data written to: auth/approle/role/mcctb-app
Installing the NetApp-MetroCluster-Tiebreaker-Software-1.7-
1.x86_64.rpm
Preparing...                          #
################################# # [100%]

Updating / installing...

1:NetApp-MetroCluster-Tiebreaker-So#
################################# # [100%]
Performing file integrity check
etc/cron.weekly/metrocluster-tiebreaker-support is Ok
etc/cron.weekly/metrocluster-tiebreaker-support-cov is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software-cov is Ok
etc/logrotate.d/mcctb is Ok
opt/netapp/mcctb/lib/common/activation-1.1.1.jar is Ok
opt/netapp/mcctb/lib/common/aopalliance.jar is Ok
opt/netapp/mcctb/lib/common/args4j.jar is Ok
opt/netapp/mcctb/lib/common/aspectjrt.jar is Ok
opt/netapp/mcctb/lib/common/aspectjweaver.jar is Ok
opt/netapp/mcctb/lib/common/asup.jar is Ok
opt/netapp/mcctb/lib/common/bcpkix-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bctls-fips-1.0.13.jar is Ok
opt/netapp/mcctb/lib/common/bctls-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bcutil-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/cglib.jar is Ok
opt/netapp/mcctb/lib/common/commons-codec.jar is Ok
```

```
opt/netapp/mcctb/lib/common/commons-collections4.jar is Ok
opt/netapp/mcctb/lib/common/commons-compress.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.src.jar is Ok
opt/netapp/mcctb/lib/common/commons-dbcp2.jar is Ok
opt/netapp/mcctb/lib/common/commons-io.jar is Ok
opt/netapp/mcctb/lib/common/commons-lang3.jar is Ok
opt/netapp/mcctb/lib/common/commons-logging.jar is Ok
opt/netapp/mcctb/lib/common/commons-pool2.jar is Ok
opt/netapp/mcctb/lib/common/guava.jar is Ok
opt/netapp/mcctb/lib/common/httpclient.jar is Ok
opt/netapp/mcctb/lib/common/httpcore.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.activation.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.xml.bind-api.jar is Ok
opt/netapp/mcctb/lib/common/java-xmlbuilder.jar is Ok
opt/netapp/mcctb/lib/common/javax.inject.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-api-2.3.1.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-core.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-impl.jar is Ok
opt/netapp/mcctb/lib/common/jline.jar is Ok
opt/netapp/mcctb/lib/common/jna.jar is Ok
opt/netapp/mcctb/lib/common/joda-time.jar is Ok
opt/netapp/mcctb/lib/common/jsch.jar is Ok
opt/netapp/mcctb/lib/common/json.jar is Ok
opt/netapp/mcctb/lib/common/jsvc.zip is Ok
opt/netapp/mcctb/lib/common/junixsocket-common.jar is Ok
opt/netapp/mcctb/lib/common/junixsocket-native-common.jar is
Ok
opt/netapp/mcctb/lib/common/logback-classic.jar is Ok
opt/netapp/mcctb/lib/common/logback-core.jar is Ok
opt/netapp/mcctb/lib/common/mail-1.6.2.jar is Ok
opt/netapp/mcctb/lib/common/mariadb-java-client.jar is Ok
opt/netapp/mcctb/lib/common/mcctb-mib.jar is Ok
opt/netapp/mcctb/lib/common/mcctb.jar is Ok
opt/netapp/mcctb/lib/common/mockito-core.jar is Ok
opt/netapp/mcctb/lib/common/slf4j-api.jar is Ok
opt/netapp/mcctb/lib/common/snmp4j.jar is Ok
opt/netapp/mcctb/lib/common/spring-aop.jar is Ok
opt/netapp/mcctb/lib/common/spring-beans.jar is Ok
opt/netapp/mcctb/lib/common/spring-context-support.jar is Ok
opt/netapp/mcctb/lib/common/spring-context.jar is Ok
opt/netapp/mcctb/lib/common/spring-core.jar is Ok
opt/netapp/mcctb/lib/common/spring-expression.jar is Ok
opt/netapp/mcctb/lib/common/spring-web.jar is Ok
opt/netapp/mcctb/lib/common/vault-java-driver.jar is Ok
opt/netapp/mcctb/lib/common/xz.jar is Ok
```

```
opt/netapp/mcctb/lib/org.jacoco.agent-0.8.8-runtime.jar is Ok
opt/netapp/mcctb/bin/mcctb-asup-invoke is Ok
opt/netapp/mcctb/bin/mcctb_postrotate is Ok
opt/netapp/mcctb/bin/netapp-metrocluster-tiebreaker-software-
cli is Ok
/

Synchronizing state of netapp-metrocluster-tiebreaker-
software.service with SysV service script with
/usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable
netapp-metrocluster-tiebreaker-software
Created symlink /etc/systemd/system/multi-
user.target.wants/netapp-metrocluster-tiebreaker-
software.service → /etc/systemd/system/netapp-metrocluster-
tiebreaker-software.service.

Attempting to start NetApp MetroCluster Tiebreaker software
services
Started NetApp MetroCluster Tiebreaker software services
Successfully installed NetApp MetroCluster Tiebreaker software
version 1.7.
```

1.6P1を1.7にアップグレード

Tiebreaker 1.6P1 ソフトウェア バージョンを Tiebreaker 1.7 にアップグレードするには、次の手順に従います。

手順

a. で次のコマンドを実行します。 `[root@mcctb ~] #` ソフトウェアのアップグレードを求めるプロンプトを表示します。

```
sh MetroClusterTiebreakerInstall-1.7
```

アップグレードが完了すると、次の出力が表示されます。

例

```
Extracting the MetroCluster Tiebreaker installation/upgrade
archive
Install digest hash is Ok
Performing the MetroCluster Tiebreaker code signature check
Install code signature is Ok
NetApp-MetroCluster-Tiebreaker-Software-1.6P1-1.x86_64
Upgrading... to NetApp-MetroCluster-Tiebreaker-Software-1.7-
1.x86_64.rpm
Preparing...
################################## [100%]
Updating / installing...
   1:NetApp-MetroCluster-Tiebreaker-
So################################## [ 50%]
Performing file integrity check
etc/cron.weekly/metrocluster-tiebreaker-support is Ok
etc/cron.weekly/metrocluster-tiebreaker-support-cov is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software-cov is Ok
etc/logrotate.d/mcctb is Ok
opt/netapp/mcctb/lib/common/aopalliance.jar is Ok
opt/netapp/mcctb/lib/common/args4j.jar is Ok
opt/netapp/mcctb/lib/common/aspectjrt.jar is Ok
opt/netapp/mcctb/lib/common/aspectjweaver.jar is Ok
opt/netapp/mcctb/lib/common/asup.jar is Ok
opt/netapp/mcctb/lib/common/bcpkix-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bctls-fips-1.0.19.jar is Ok
opt/netapp/mcctb/lib/common/bctls-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bcutil-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/cglib.jar is Ok
opt/netapp/mcctb/lib/common/commons-codec.jar is Ok
opt/netapp/mcctb/lib/common/commons-collections4.jar is Ok
opt/netapp/mcctb/lib/common/commons-compress.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.src.jar is Ok
opt/netapp/mcctb/lib/common/commons-dbcp2.jar is Ok
opt/netapp/mcctb/lib/common/commons-io.jar is Ok
opt/netapp/mcctb/lib/common/commons-lang3.jar is Ok
opt/netapp/mcctb/lib/common/commons-logging.jar is Ok
opt/netapp/mcctb/lib/common/commons-pool2.jar is Ok
opt/netapp/mcctb/lib/common/guava.jar is Ok
opt/netapp/mcctb/lib/common/httpclient.jar is Ok
opt/netapp/mcctb/lib/common/httpcore.jar is Ok
```

```
opt/netapp/mcctb/lib/common/jakarta.activation.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.mail-2.0.1.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.xml.bind-api.jar is Ok
opt/netapp/mcctb/lib/common/java-xmlbuilder.jar is Ok
opt/netapp/mcctb/lib/common/javax.inject.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-api-2.3.1.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-core.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-impl.jar is Ok
opt/netapp/mcctb/lib/common/jline.jar is Ok
opt/netapp/mcctb/lib/common/jna.jar is Ok
opt/netapp/mcctb/lib/common/joda-time.jar is Ok
opt/netapp/mcctb/lib/common/jsch.jar is Ok
opt/netapp/mcctb/lib/common/json.jar is Ok
opt/netapp/mcctb/lib/common/jsvc.zip is Ok
opt/netapp/mcctb/lib/common/junixsocket-common.jar is Ok
opt/netapp/mcctb/lib/common/junixsocket-native-common.jar is
Ok
opt/netapp/mcctb/lib/common/logback-classic.jar is Ok
opt/netapp/mcctb/lib/common/logback-core.jar is Ok
opt/netapp/mcctb/lib/common/mail-1.6.2.jar is Ok
opt/netapp/mcctb/lib/common/mariadb-java-client.jar is Ok
opt/netapp/mcctb/lib/common/mcctb-mib.jar is Ok
opt/netapp/mcctb/lib/common/mcctb.jar is Ok
opt/netapp/mcctb/lib/common/mockito-core.jar is Ok
opt/netapp/mcctb/lib/common/slf4j-api.jar is Ok
opt/netapp/mcctb/lib/common/snmp4j.jar is Ok
opt/netapp/mcctb/lib/common/spring-aop.jar is Ok
opt/netapp/mcctb/lib/common/spring-beans.jar is Ok
opt/netapp/mcctb/lib/common/spring-context-support.jar is Ok
opt/netapp/mcctb/lib/common/spring-context.jar is Ok
opt/netapp/mcctb/lib/common/spring-core.jar is Ok
opt/netapp/mcctb/lib/common/spring-expression.jar is Ok
opt/netapp/mcctb/lib/common/spring-web.jar is Ok
opt/netapp/mcctb/lib/common/vault-java-driver.jar is Ok
opt/netapp/mcctb/lib/common/xz.jar is Ok
opt/netapp/mcctb/lib/org.jacoco.agent-0.8.8-runtime.jar is Ok
opt/netapp/mcctb/bin/mcctb-asup-invoke is Ok
opt/netapp/mcctb/bin/mcctb_postrotate is Ok
opt/netapp/mcctb/bin/netapp-metrocluster-tiebreaker-software-
cli is Ok
/


Attempting to start NetApp MetroCluster Tiebreaker software
services
Started NetApp MetroCluster Tiebreaker software services
```

```
Successfully upgraded NetApp MetroCluster Tiebreaker software
to version 1.7.
Cleaning up / removing...
   2:NetApp-MetroCluster-Tiebreaker-
So################################## [100%]
```

証明書の不足によりアップグレードがエラーで失敗する場合は、"証明書をインポートする"。証明書をインポートしたら、再度アップグレードを試みることができます。

Tiebreaker 1.6または**1.6P1**をインストールする

ホストLinuxオペレーティングシステムでTiebreaker 1.6またはTiebreaker 1.6P1への新規インストールまたはアップグレードを実行して、MetroCluster構成を監視します。

このタスクについて

- ストレージシステムでONTAP 9.12.1以降が実行されている必要があります。
- MetroCluster Tiebreakerは、Tiebreakerのインストール、テーブルとユーザの作成、ユーザパスワードの設定に必要な管理権限を持つroot以外のユーザとしてインストールできます。

Tiebreaker 1.6P1のインストールまたはアップグレード

Tiebreaker 1.6P1をインストールするか、Tiebreaker 1.6、1.5、または1.4からTiebreaker 1.6P1にアップグレードできます。

手順

1. MetroCluster Tiebreaker 1.6P1ソフトウェアをダウンロードします。

   "MetroCluster Tiebreaker（ダウンロード）- NetApp Support Site"

2. root ユーザとしてホストにログインします。
3. アップグレードを実行する場合は、実行しているTiebreakerのバージョンを確認します。

   次の例はTiebreaker 1.5を示しています。

   ```
   [root@mcctb ~] # netapp-metrocluster-tiebreaker-software-cli
   NetApp MetroCluster Tiebreaker :> version show
   NetApp MetroCluster Tiebreaker 1.5: Sun Mar 13 09:59:02 IST 2022
   NetApp MetroCluster Tiebreaker :> exit
   ```

4. Tiebreakerソフトウェアをインストールまたはアップグレードします。

Tiebreaker 1.6P1をインストール

Tiebreaker 1.6P1を新規にインストールする場合は、次の手順を実行します。

手順

a. で次のコマンドを実行します。 `[root@mcctb ~] #` インストールを開始するようにプロンプトを表示します。

```
sh MetroClusterTiebreakerInstall-1.6P1
```

インストールが完了すると、次の出力が表示されます。

例

```
Extracting the MetroCluster Tiebreaker installation/upgrade
archive
Install digest hash is Ok
Performing the MetroCluster Tiebreaker code signature check
Install code signature is Ok
Enter unix user account to use for the installation:
mcctbadminuser
Unix user account "mcctbadminuser" doesn't exist. Do you wish
to create "mcctbadminuser" user account? [Y/N]: y
useradd: warning: the home directory already exists.
Not copying any file from skel directory into it.
Creating mailbox file: File exists
Unix account "mcctbadminuser" created.
Changing password for user mcctbadminuser.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
MetroCluster Tiebreaker requires unix user account
"mcctbadminuser" to be added to the group "mcctbgrp" for admin
access.
Do you wish to add ? [Y/N]: y
Unix user account "mcctbadminuser" added to "mcctbgrp".
Do you wish to generate your own public-private key pair for
encrypting audit log? [Y/N]: y
Generating public-private key pair...
Configuring Vault...
Starting vault server...
==> Vault server configuration:

             Api Address: <api_address>
                     Cgo: disabled
         Cluster Address: <cluster_address>
   Environment Variables: BASH_FUNC_which%%,
DBUS_SESSION_BUS_ADDRESS, GODEBUG, HISTCONTROL, HISTSIZE,
HOME, HOSTNAME, HOST_ACCOUNT, LANG, LESSOPEN, LOGNAME,
LS_COLORS, MAIL, PATH, PWD, SHELL, SHLVL, SSH_CLIENT,
SSH_CONNECTION, SSH_TTY, STAF_TEMP_DIR, TERM, USER,
VAULT_ADDR, VAULT_TOKEN, XDG_RUNTIME_DIR, XDG_SESSION_ID, _,
vault_Addr, which_declare
              Go Version: go1.20.5
              Listener 1: tcp (addr: "0.0.0.0:8200", cluster
address: "0.0.0.0:8201", max_request_duration: "1m30s",
max_request_size: "33554432", tls: "enabled")
```

```
               Log Level:
                   Mlock: supported: true, enabled: true
           Recovery Mode: false
                 Storage: file
                 Version: Vault v1.14.0, built 2023-06-
19T11:40:23Z
             Version Sha:
13a649f860186dffe3f3a4459814d87191efc321

==> Vault server started! Log data will stream in below:

2023-11-23T15:14:28.532+0530 [INFO]  proxy environment:
http_proxy="" https_proxy="" no_proxy=""
2023-11-23T15:14:28.577+0530 [INFO]  core: Initializing
version history cache for core
2023-11-23T15:14:38.552+0530 [INFO]  core: security barrier
not initialized
2023-11-23T15:14:38.552+0530 [INFO]  core: seal configuration
missing, not initialized
2023-11-23T15:14:38.554+0530 [INFO]  core: security barrier
not initialized
2023-11-23T15:14:38.555+0530 [INFO]  core: security barrier
initialized: stored=1 shares=5 threshold=3
2023-11-23T15:14:38.556+0530 [INFO]  core: post-unseal setup
starting
2023-11-23T15:14:38.577+0530 [INFO]  core: loaded wrapping
token key
2023-11-23T15:14:38.577+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-11-23T15:14:38.577+0530 [INFO]  core: no mounts; adding
default mount table
2023-11-23T15:14:38.578+0530 [INFO]  core: successfully
mounted: type=cubbyhole version="v1.14.0+builtin.vault"
path=cubbyhole/ namespace="ID: root. Path: "
2023-11-23T15:14:38.578+0530 [INFO]  core: successfully
mounted: type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-11-23T15:14:38.578+0530 [INFO]  core: successfully
mounted: type=identity version="v1.14.0+builtin.vault"
path=identity/ namespace="ID: root. Path: "
2023-11-23T15:14:38.581+0530 [INFO]  core: successfully
mounted: type=token version="v1.14.0+builtin.vault"
path=token/ namespace="ID: root. Path: "
2023-11-23T15:14:38.581+0530 [INFO]  rollback: starting
rollback manager
2023-11-23T15:14:38.581+0530 [INFO]  core: restoring leases
```

```
2023-11-23T15:14:38.582+0530 [INFO]  expiration: lease restore
complete
2023-11-23T15:14:38.582+0530 [INFO]  identity: entities
restored
2023-11-23T15:14:38.582+0530 [INFO]  identity: groups restored
2023-11-23T15:14:38.583+0530 [INFO]  core: Recorded vault
version: vault version=1.14.0 upgrade time="2023-11-23
09:44:38.582881162 +0000 UTC" build date=2023-06-19T11:40:23Z
2023-11-23T15:14:38.583+0530 [INFO]  core: usage gauge
collection is disabled
2023-11-23T15:14:38.998+0530 [INFO]  core: post-unseal setup
complete
2023-11-23T15:14:38.999+0530 [INFO]  core: root token
generated
2023-11-23T15:14:38.999+0530 [INFO]  core: pre-seal teardown
starting
2023-11-23T15:14:38.999+0530 [INFO]  rollback: stopping
rollback manager
2023-11-23T15:14:38.999+0530 [INFO]  core: pre-seal teardown
complete
2023-11-23T15:14:39.311+0530 [INFO]  core.cluster-
listener.tcp: starting listener: listener_address=0.0.0.0:8201
2023-11-23T15:14:39.311+0530 [INFO]  core.cluster-listener:
serving cluster requests: cluster_listen_address=[::]:8201
2023-11-23T15:14:39.312+0530 [INFO]  core: post-unseal setup
starting
2023-11-23T15:14:39.312+0530 [INFO]  core: loaded wrapping
token key
2023-11-23T15:14:39.312+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-11-23T15:14:39.313+0530 [INFO]  core: successfully
mounted: type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-11-23T15:14:39.313+0530 [INFO]  core: successfully
mounted: type=identity version="v1.14.0+builtin.vault"
path=identity/ namespace="ID: root. Path: "
2023-11-23T15:14:39.313+0530 [INFO]  core: successfully
mounted: type=cubbyhole version="v1.14.0+builtin.vault"
path=cubbyhole/ namespace="ID: root. Path: "
2023-11-23T15:14:39.314+0530 [INFO]  core: successfully
mounted: type=token version="v1.14.0+builtin.vault"
path=token/ namespace="ID: root. Path: "
2023-11-23T15:14:39.314+0530 [INFO]  rollback: starting
rollback manager
2023-11-23T15:14:39.314+0530 [INFO]  core: restoring leases
2023-11-23T15:14:39.314+0530 [INFO]  identity: entities
```

```
restored
2023-11-23T15:14:39.314+0530 [INFO]  expiration: lease restore
complete
2023-11-23T15:14:39.314+0530 [INFO]  identity: groups restored
2023-11-23T15:14:39.315+0530 [INFO]  core: usage gauge
collection is disabled
2023-11-23T15:14:39.316+0530 [INFO]  core: post-unseal setup
complete
2023-11-23T15:14:39.316+0530 [INFO]  core: vault is unsealed
Success! Uploaded policy: mcctb-policy
2023-11-23T15:14:39.795+0530 [INFO]  core: enabled credential
backend: path=approle/ type=approle version=""
Success! Enabled approle auth method at: approle/
2023-11-23T15:14:39.885+0530 [INFO]  core: successful mount:
namespace="" path=mcctb/ type=kv version=""
Success! Enabled the kv secrets engine at: mcctb/
Success! Data written to: auth/approle/role/mcctb-app
Installing the NetApp-MetroCluster-Tiebreaker-Software-1.6P1-
1.x86_64.rpm
Preparing...                          #
################################# # [100%]

Updating / installing...

1:NetApp-MetroCluster-Tiebreaker-So#
################################# # [100%]
Performing file integrity check
etc/cron.weekly/metrocluster-tiebreaker-support is Ok
etc/cron.weekly/metrocluster-tiebreaker-support-cov is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software-cov is Ok
etc/logrotate.d/mcctb is Ok
opt/netapp/mcctb/lib/common/activation-1.1.1.jar is Ok
opt/netapp/mcctb/lib/common/aopalliance.jar is Ok
opt/netapp/mcctb/lib/common/args4j.jar is Ok
opt/netapp/mcctb/lib/common/aspectjrt.jar is Ok
opt/netapp/mcctb/lib/common/aspectjweaver.jar is Ok
opt/netapp/mcctb/lib/common/asup.jar is Ok
opt/netapp/mcctb/lib/common/bcpkix-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bctls-fips-1.0.13.jar is Ok
opt/netapp/mcctb/lib/common/bctls-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bcutil-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/cglib.jar is Ok
opt/netapp/mcctb/lib/common/commons-codec.jar is Ok
```

```
opt/netapp/mcctb/lib/common/commons-collections4.jar is Ok
opt/netapp/mcctb/lib/common/commons-compress.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.src.jar is Ok
opt/netapp/mcctb/lib/common/commons-dbcp2.jar is Ok
opt/netapp/mcctb/lib/common/commons-io.jar is Ok
opt/netapp/mcctb/lib/common/commons-lang3.jar is Ok
opt/netapp/mcctb/lib/common/commons-logging.jar is Ok
opt/netapp/mcctb/lib/common/commons-pool2.jar is Ok
opt/netapp/mcctb/lib/common/guava.jar is Ok
opt/netapp/mcctb/lib/common/httpclient.jar is Ok
opt/netapp/mcctb/lib/common/httpcore.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.activation.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.xml.bind-api.jar is Ok
opt/netapp/mcctb/lib/common/java-xmlbuilder.jar is Ok
opt/netapp/mcctb/lib/common/javax.inject.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-api-2.3.1.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-core.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-impl.jar is Ok
opt/netapp/mcctb/lib/common/jline.jar is Ok
opt/netapp/mcctb/lib/common/jna.jar is Ok
opt/netapp/mcctb/lib/common/joda-time.jar is Ok
opt/netapp/mcctb/lib/common/jsch.jar is Ok
opt/netapp/mcctb/lib/common/json.jar is Ok
opt/netapp/mcctb/lib/common/jsvc.zip is Ok
opt/netapp/mcctb/lib/common/junixsocket-common.jar is Ok
opt/netapp/mcctb/lib/common/junixsocket-native-common.jar is
Ok
opt/netapp/mcctb/lib/common/logback-classic.jar is Ok
opt/netapp/mcctb/lib/common/logback-core.jar is Ok
opt/netapp/mcctb/lib/common/mail-1.6.2.jar is Ok
opt/netapp/mcctb/lib/common/mariadb-java-client.jar is Ok
opt/netapp/mcctb/lib/common/mcctb-mib.jar is Ok
opt/netapp/mcctb/lib/common/mcctb.jar is Ok
opt/netapp/mcctb/lib/common/mockito-core.jar is Ok
opt/netapp/mcctb/lib/common/slf4j-api.jar is Ok
opt/netapp/mcctb/lib/common/snmp4j.jar is Ok
opt/netapp/mcctb/lib/common/spring-aop.jar is Ok
opt/netapp/mcctb/lib/common/spring-beans.jar is Ok
opt/netapp/mcctb/lib/common/spring-context-support.jar is Ok
opt/netapp/mcctb/lib/common/spring-context.jar is Ok
opt/netapp/mcctb/lib/common/spring-core.jar is Ok
opt/netapp/mcctb/lib/common/spring-expression.jar is Ok
opt/netapp/mcctb/lib/common/spring-web.jar is Ok
opt/netapp/mcctb/lib/common/vault-java-driver.jar is Ok
opt/netapp/mcctb/lib/common/xz.jar is Ok
```

```
opt/netapp/mcctb/lib/org.jacoco.agent-0.8.8-runtime.jar is Ok
opt/netapp/mcctb/bin/mcctb-asup-invoke is Ok
opt/netapp/mcctb/bin/mcctb_postrotate is Ok
opt/netapp/mcctb/bin/netapp-metrocluster-tiebreaker-software-
cli is Ok
/

Synchronizing state of netapp-metrocluster-tiebreaker-
software.service with SysV service script with
/usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable
netapp-metrocluster-tiebreaker-software
Created symlink /etc/systemd/system/multi-
user.target.wants/netapp-metrocluster-tiebreaker-
software.service → /etc/systemd/system/netapp-metrocluster-
tiebreaker-software.service.

Attempting to start NetApp MetroCluster Tiebreaker software
services
Started NetApp MetroCluster Tiebreaker software services
Successfully installed NetApp MetroCluster Tiebreaker software
version 1.6P1.
```

1.6から1.6P1へのアップグレード

Tiebreaker 1.6ソフトウェアのバージョンをTiebreaker 1.6P1にアップグレードするには、次の手順に従います。

> 1.6からTiebreaker 1.6P1にアップグレードしたら、既存のモニタを削除し、MetroCluster設定を監視用に再度追加します。

手順

a. で次のコマンドを実行します。 `[root@mcctb ~] #` ソフトウェアのアップグレードを求めるプロンプトを表示します。

```
sh MetroClusterTiebreakerInstall-1.6P1
```

アップグレードが完了すると、次の出力が表示されます。

例

```
Extracting the MetroCluster Tiebreaker installation/upgrade
archive
Install digest hash is Ok
Performing the MetroCluster Tiebreaker code signature check
Install code signature is Ok
NetApp-MetroCluster-Tiebreaker-Software-1.6P1-1.x86_64
Error making API request.

URL: GET
https://127.0.0.1:8200/v1/sys/internal/ui/mounts/mcctb/data/db
Code: 403. Errors:

* permission denied
Upgrading to NetApp-MetroCluster-Tiebreaker-Software-1.6P1-
1.x86_64.rpm
Preparing...
################################## [100%]
Updating / installing...
   1:NetApp-MetroCluster-Tiebreaker-
So################################## [ 50%]
Performing file integrity check
etc/cron.weekly/metrocluster-tiebreaker-support is Ok
etc/cron.weekly/metrocluster-tiebreaker-support-cov is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software-cov is Ok
etc/logrotate.d/mcctb is Ok
opt/netapp/mcctb/lib/common/aopalliance.jar is Ok
opt/netapp/mcctb/lib/common/args4j.jar is Ok
opt/netapp/mcctb/lib/common/aspectjrt.jar is Ok
opt/netapp/mcctb/lib/common/aspectjweaver.jar is Ok
opt/netapp/mcctb/lib/common/asup.jar is Ok
opt/netapp/mcctb/lib/common/bcpkix-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bctls-fips-1.0.19.jar is Ok
opt/netapp/mcctb/lib/common/bctls-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bcutil-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/cglib.jar is Ok
opt/netapp/mcctb/lib/common/commons-codec.jar is Ok
opt/netapp/mcctb/lib/common/commons-collections4.jar is Ok
opt/netapp/mcctb/lib/common/commons-compress.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.src.jar is Ok
opt/netapp/mcctb/lib/common/commons-dbcp2.jar is Ok
opt/netapp/mcctb/lib/common/commons-io.jar is Ok
```

```
opt/netapp/mcctb/lib/common/commons-lang3.jar is Ok
opt/netapp/mcctb/lib/common/commons-logging.jar is Ok
opt/netapp/mcctb/lib/common/commons-pool2.jar is Ok
opt/netapp/mcctb/lib/common/guava.jar is Ok
opt/netapp/mcctb/lib/common/httpclient.jar is Ok
opt/netapp/mcctb/lib/common/httpcore.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.activation.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.mail-2.0.1.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.xml.bind-api.jar is Ok
opt/netapp/mcctb/lib/common/java-xmlbuilder.jar is Ok
opt/netapp/mcctb/lib/common/javax.inject.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-api-2.3.1.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-core.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-impl.jar is Ok
opt/netapp/mcctb/lib/common/jline.jar is Ok
opt/netapp/mcctb/lib/common/jna.jar is Ok
opt/netapp/mcctb/lib/common/joda-time.jar is Ok
opt/netapp/mcctb/lib/common/jsch.jar is Ok
opt/netapp/mcctb/lib/common/json.jar is Ok
opt/netapp/mcctb/lib/common/jsvc.zip is Ok
opt/netapp/mcctb/lib/common/junixsocket-common.jar is Ok
opt/netapp/mcctb/lib/common/junixsocket-native-common.jar is
Ok
opt/netapp/mcctb/lib/common/logback-classic.jar is Ok
opt/netapp/mcctb/lib/common/logback-core.jar is Ok
opt/netapp/mcctb/lib/common/mail-1.6.2.jar is Ok
opt/netapp/mcctb/lib/common/mariadb-java-client.jar is Ok
opt/netapp/mcctb/lib/common/mcctb-mib.jar is Ok
opt/netapp/mcctb/lib/common/mcctb.jar is Ok
opt/netapp/mcctb/lib/common/mockito-core.jar is Ok
opt/netapp/mcctb/lib/common/slf4j-api.jar is Ok
opt/netapp/mcctb/lib/common/snmp4j.jar is Ok
opt/netapp/mcctb/lib/common/spring-aop.jar is Ok
opt/netapp/mcctb/lib/common/spring-beans.jar is Ok
opt/netapp/mcctb/lib/common/spring-context-support.jar is Ok
opt/netapp/mcctb/lib/common/spring-context.jar is Ok
opt/netapp/mcctb/lib/common/spring-core.jar is Ok
opt/netapp/mcctb/lib/common/spring-expression.jar is Ok
opt/netapp/mcctb/lib/common/spring-web.jar is Ok
opt/netapp/mcctb/lib/common/vault-java-driver.jar is Ok
opt/netapp/mcctb/lib/common/xz.jar is Ok
opt/netapp/mcctb/lib/org.jacoco.agent-0.8.8-runtime.jar is Ok
opt/netapp/mcctb/bin/mcctb-asup-invoke is Ok
opt/netapp/mcctb/bin/mcctb_postrotate is Ok
opt/netapp/mcctb/bin/netapp-metrocluster-tiebreaker-software-
cli is Ok
```

```
/


Attempting to start NetApp MetroCluster Tiebreaker software
services
Started NetApp MetroCluster Tiebreaker software services
Successfully upgraded NetApp MetroCluster Tiebreaker software
to version 1.6P1.
Cleaning up / removing...
   2:NetApp-MetroCluster-Tiebreaker-
So################################## [100%]
```

b. の手順に従って、MetroCluster構成を削除し、再度追加し"Tiebreaker ソフトウェアを設定します"ます。

1.5から**1.6P1**へのアップグレード

Tiebreaker 1.5ソフトウェアのバージョンをTiebreaker 1.6P1にアップグレードするには、次の手順に従います。

手順

a. で次のコマンドを実行します。 `[root@mcctb ~] #` ソフトウェアのアップグレードを求めるプロンプトを表示します。

```
sh MetroClusterTiebreakerInstall-1.6P1
```

アップグレードが完了すると、次の出力が表示されます。

例

```
Extracting the MetroCluster Tiebreaker installation/upgrade
archive
Install digest hash is Ok
Performing the MetroCluster Tiebreaker code signature check
Install code signature is Ok

Enter database user name : root

Please enter database password for root
Enter password:

Password updated successfully in the database.

Do you wish to generate your own public-private key pair for
encrypting audit log? [Y/N]: y
Generating public-private key pair...
Configuring Vault...
==> Vault shutdown triggered
2023-07-21T00:30:22.335+0530 [INFO]  core: marked as sealed
2023-07-21T00:30:22.335+0530 [INFO]  core: pre-seal teardown
starting
2023-07-21T00:30:22.335+0530 [INFO]  rollback: stopping
rollback manager
2023-07-21T00:30:22.335+0530 [INFO]  core: pre-seal teardown
complete
2023-07-21T00:30:22.335+0530 [INFO]  core: stopping cluster
listeners
2023-07-21T00:30:22.335+0530 [INFO]  core.cluster-listener:
forwarding rpc listeners stopped
2023-07-21T00:30:22.375+0530 [INFO]  core.cluster-listener:
rpc listeners successfully shut down
2023-07-21T00:30:22.375+0530 [INFO]  core: cluster listeners
successfully shut down
2023-07-21T00:30:22.376+0530 [INFO]  core: vault is sealed
Starting vault server...
==> Vault server configuration:

             Api Address: <api_address>
                     Cgo: disabled
         Cluster Address: <cluster_address>
   Environment Variables: BASH_FUNC_which%%,
DBUS_SESSION_BUS_ADDRESS, GODEBUG, HISTCONTROL, HISTSIZE,
HOME, HOSTNAME, HOST_ACCOUNT, LANG, LESSOPEN, LOGNAME,
LS_COLORS, MAIL, PATH, PWD, SHELL, SHLVL, SSH_CLIENT,
```

```
SSH_CONNECTION, SSH_TTY, STAF_TEMP_DIR, TERM, USER,
VAULT_ADDR, VAULT_TOKEN, XDG_RUNTIME_DIR, XDG_SESSION_ID, _,
vault_Addr, which_declare
              Go Version: go1.20.5
              Listener 1: tcp (addr: "0.0.0.0:8200", cluster
address: "0.0.0.0:8201", max_request_duration: "1m30s",
max_request_size: "33554432", tls: "enabled")
               Log Level:
                   Mlock: supported: true, enabled: true
           Recovery Mode: false
                 Storage: file
                 Version: Vault v1.14.0, built 2023-06-
19T11:40:23Z
             Version Sha:
13a649f860186dffe3f3a4459814d87191efc321

==> Vault server started! Log data will stream in below:

2023-07-21T00:30:33.065+0530 [INFO]  proxy environment:
http_proxy="" https_proxy="" no_proxy=""
2023-07-21T00:30:33.098+0530 [INFO]  core: Initializing
version history cache for core
2023-07-21T00:30:43.092+0530 [INFO]  core: security barrier
not initialized
2023-07-21T00:30:43.092+0530 [INFO]  core: seal configuration
missing, not initialized
2023-07-21T00:30:43.094+0530 [INFO]  core: security barrier
not initialized
2023-07-21T00:30:43.096+0530 [INFO]  core: security barrier
initialized: stored=1 shares=5 threshold=3
2023-07-21T00:30:43.098+0530 [INFO]  core: post-unseal setup
starting
2023-07-21T00:30:43.124+0530 [INFO]  core: loaded wrapping
token key
2023-07-21T00:30:43.124+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-07-21T00:30:43.124+0530 [INFO]  core: no mounts; adding
default mount table
2023-07-21T00:30:43.125+0530 [INFO]  core: successfully
mounted: type=cubbyhole version="v1.14.0+builtin.vault"
path=cubbyhole/ namespace="ID: root. Path: "
2023-07-21T00:30:43.126+0530 [INFO]  core: successfully
mounted: type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-07-21T00:30:43.126+0530 [INFO]  core: successfully
mounted: type=identity version="v1.14.0+builtin.vault"
```

```
path=identity/ namespace="ID: root. Path: "
2023-07-21T00:30:43.129+0530 [INFO]  core: successfully
mounted: type=token version="v1.14.0+builtin.vault"
path=token/ namespace="ID: root. Path: "
2023-07-21T00:30:43.130+0530 [INFO]  rollback: starting
rollback manager
2023-07-21T00:30:43.130+0530 [INFO]  core: restoring leases
2023-07-21T00:30:43.130+0530 [INFO]  identity: entities
restored
2023-07-21T00:30:43.130+0530 [INFO]  identity: groups restored
2023-07-21T00:30:43.131+0530 [INFO]  core: usage gauge
collection is disabled
2023-07-21T00:30:43.131+0530 [INFO]  expiration: lease restore
complete
2023-07-21T00:30:43.131+0530 [INFO]  core: Recorded vault
version: vault version=1.14.0 upgrade time="2023-07-20
19:00:43.131158543 +0000 UTC" build date=2023-06-19T11:40:23Z
2023-07-21T00:30:43.371+0530 [INFO]  core: post-unseal setup
complete
2023-07-21T00:30:43.371+0530 [INFO]  core: root token
generated
2023-07-21T00:30:43.371+0530 [INFO]  core: pre-seal teardown
starting
2023-07-21T00:30:43.371+0530 [INFO]  rollback: stopping
rollback manager
2023-07-21T00:30:43.372+0530 [INFO]  core: pre-seal teardown
complete
2023-07-21T00:30:43.694+0530 [INFO]  core.cluster-
listener.tcp: starting listener: listener_address=0.0.0.0:8201
2023-07-21T00:30:43.695+0530 [INFO]  core.cluster-listener:
serving cluster requests: cluster_listen_address=[::]:8201
2023-07-21T00:30:43.695+0530 [INFO]  core: post-unseal setup
starting
2023-07-21T00:30:43.696+0530 [INFO]  core: loaded wrapping
token key
2023-07-21T00:30:43.696+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-07-21T00:30:43.697+0530 [INFO]  core: successfully
mounted: type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-07-21T00:30:43.698+0530 [INFO]  core: successfully
mounted: type=identity version="v1.14.0+builtin.vault"
path=identity/ namespace="ID: root. Path: "
2023-07-21T00:30:43.698+0530 [INFO]  core: successfully
mounted: type=cubbyhole version="v1.14.0+builtin.vault"
path=cubbyhole/ namespace="ID: root. Path: "
```

```
2023-07-21T00:30:43.701+0530 [INFO]  core: successfully
mounted: type=token version="v1.14.0+builtin.vault"
path=token/ namespace="ID: root. Path: "
2023-07-21T00:30:43.701+0530 [INFO]  rollback: starting
rollback manager
2023-07-21T00:30:43.702+0530 [INFO]  core: restoring leases
2023-07-21T00:30:43.702+0530 [INFO]  identity: entities
restored
2023-07-21T00:30:43.702+0530 [INFO]  expiration: lease restore
complete
2023-07-21T00:30:43.702+0530 [INFO]  identity: groups restored
2023-07-21T00:30:43.702+0530 [INFO]  core: usage gauge
collection is disabled
2023-07-21T00:30:43.703+0530 [INFO]  core: post-unseal setup
complete
2023-07-21T00:30:43.703+0530 [INFO]  core: vault is unsealed
Success! Uploaded policy: mcctb-policy
2023-07-21T00:30:44.226+0530 [INFO]  core: enabled credential
backend: path=approle/ type=approle version=""
Success! Enabled approle auth method at: approle/
2023-07-21T00:30:44.315+0530 [INFO]  core: successful mount:
namespace="" path=mcctb/ type=kv version=""
Success! Enabled the kv secrets engine at: mcctb/
Success! Data written to: auth/approle/role/mcctb-app
Upgrading to NetApp-MetroCluster-Tiebreaker-Software-1.6P1-
1.x86_64.rpm
Preparing...
################################## [100%]
Updating / installing...
   1:NetApp-MetroCluster-Tiebreaker-
So################################## [ 50%]
Performing file integrity check
etc/cron.weekly/metrocluster-tiebreaker-support is Ok
etc/cron.weekly/metrocluster-tiebreaker-support-cov is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software-cov is Ok
etc/logrotate.d/mcctb is Ok
opt/netapp/mcctb/lib/common/activation-1.1.1.jar is Ok
opt/netapp/mcctb/lib/common/aopalliance.jar is Ok
opt/netapp/mcctb/lib/common/args4j.jar is Ok
opt/netapp/mcctb/lib/common/aspectjrt.jar is Ok
opt/netapp/mcctb/lib/common/aspectjweaver.jar is Ok
opt/netapp/mcctb/lib/common/asup.jar is Ok
opt/netapp/mcctb/lib/common/bcpkix-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk18on.jar is Ok
```

```
opt/netapp/mcctb/lib/common/bctls-fips-1.0.13.jar is Ok
opt/netapp/mcctb/lib/common/bctls-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bcutil-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/cglib.jar is Ok
opt/netapp/mcctb/lib/common/commons-codec.jar is Ok
opt/netapp/mcctb/lib/common/commons-collections4.jar is Ok
opt/netapp/mcctb/lib/common/commons-compress.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.src.jar is Ok
opt/netapp/mcctb/lib/common/commons-dbcp2.jar is Ok
opt/netapp/mcctb/lib/common/commons-io.jar is Ok
opt/netapp/mcctb/lib/common/commons-lang3.jar is Ok
opt/netapp/mcctb/lib/common/commons-logging.jar is Ok
opt/netapp/mcctb/lib/common/commons-pool2.jar is Ok
opt/netapp/mcctb/lib/common/guava.jar is Ok
opt/netapp/mcctb/lib/common/httpclient.jar is Ok
opt/netapp/mcctb/lib/common/httpcore.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.activation.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.xml.bind-api.jar is Ok
opt/netapp/mcctb/lib/common/java-xmlbuilder.jar is Ok
opt/netapp/mcctb/lib/common/javax.inject.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-api-2.3.1.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-core.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-impl.jar is Ok
opt/netapp/mcctb/lib/common/jline.jar is Ok
opt/netapp/mcctb/lib/common/jna.jar is Ok
opt/netapp/mcctb/lib/common/joda-time.jar is Ok
opt/netapp/mcctb/lib/common/jsch.jar is Ok
opt/netapp/mcctb/lib/common/json.jar is Ok
opt/netapp/mcctb/lib/common/jsvc.zip is Ok
opt/netapp/mcctb/lib/common/junixsocket-common.jar is Ok
opt/netapp/mcctb/lib/common/junixsocket-native-common.jar is
Ok
opt/netapp/mcctb/lib/common/logback-classic.jar is Ok
opt/netapp/mcctb/lib/common/logback-core.jar is Ok
opt/netapp/mcctb/lib/common/mail-1.6.2.jar is Ok
opt/netapp/mcctb/lib/common/mariadb-java-client.jar is Ok
opt/netapp/mcctb/lib/common/mcctb-mib.jar is Ok
opt/netapp/mcctb/lib/common/mcctb.jar is Ok
opt/netapp/mcctb/lib/common/mockito-core.jar is Ok
opt/netapp/mcctb/lib/common/slf4j-api.jar is Ok
opt/netapp/mcctb/lib/common/snmp4j.jar is Ok
opt/netapp/mcctb/lib/common/spring-aop.jar is Ok
opt/netapp/mcctb/lib/common/spring-beans.jar is Ok
opt/netapp/mcctb/lib/common/spring-context-support.jar is Ok
opt/netapp/mcctb/lib/common/spring-context.jar is Ok
```

```
opt/netapp/mcctb/lib/common/spring-core.jar is Ok
opt/netapp/mcctb/lib/common/spring-expression.jar is Ok
opt/netapp/mcctb/lib/common/spring-web.jar is Ok
opt/netapp/mcctb/lib/common/vault-java-driver.jar is Ok
opt/netapp/mcctb/lib/common/xz.jar is Ok
opt/netapp/mcctb/bin/mcctb_postrotate is Ok
opt/netapp/mcctb/bin/netapp-metrocluster-tiebreaker-software-
cli is Ok
/

Synchronizing state of netapp-metrocluster-tiebreaker-
software.service with SysV service script with
/usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable
netapp-metrocluster-tiebreaker-software

Attempting to start NetApp MetroCluster Tiebreaker software
services
Started NetApp MetroCluster Tiebreaker software services
Successfully upgraded NetApp MetroCluster Tiebreaker software
to version 1.6P1.
Cleaning up / removing...
   2:NetApp-MetroCluster-Tiebreaker-
So################################## [100%]
```

1.4から1.6P1へのアップグレード

Tiebreaker 1.4ソフトウェアのバージョンをTiebreaker 1.6P1にアップグレードするには、次の手順に従います。

手順

a. で次のコマンドを実行します。 `[root@mcctb ~] #` ソフトウェアのアップグレードを求めるプロンプトを表示します。

```
sh MetroClusterTiebreakerInstall-1.6P1
```

アップグレードが完了すると、次の出力が表示されます。

例

```
Extracting the MetroCluster Tiebreaker installation/upgrade
archive
Install digest hash is Ok
Performing the MetroCluster Tiebreaker code signature check
Install code signature is Ok
Enter unix user account to use for the installation:
mcctbuseradmin1
Unix user account "mcctbuseradmin1" doesn't exist. Do you wish
to create "mcctbuseradmin1" user account? [Y/N]: y
Unix account "mcctbuseradmin1" created.
Changing password for user mcctbuseradmin1.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.

Enter database user name : root

Please enter database password for root
Enter password:

Password updated successfully in the database.

MetroCluster Tiebreaker requires unix user account
"mcctbuseradmin1" to be added to the group "mcctbgrp" for
admin access.
Do you wish to add ? [Y/N]: y
Unix user account "mcctbuseradmin1" added to "mcctbgrp".
Do you wish to generate your own public-private key pair for
encrypting audit log? [Y/N]: y
Generating public-private key pair...
Configuring Vault...
Starting vault server...
==> Vault server configuration:

             Api Address: <api_addess>
                     Cgo: disabled
         Cluster Address: <cluster_address>
   Environment Variables: BASH_FUNC_which%%,
DBUS_SESSION_BUS_ADDRESS, GODEBUG, HISTCONTROL, HISTSIZE,
HOME, HOSTNAME, HOST_ACCOUNT, LANG, LESSOPEN, LOGNAME,
LS_COLORS, MAIL, PATH, PWD, SHELL, SHLVL, SSH_CLIENT,
SSH_CONNECTION, SSH_TTY, STAF_TEMP_DIR, TERM, USER,
VAULT_ADDR, VAULT_TOKEN, XDG_RUNTIME_DIR, XDG_SESSION_ID, _,
vault_Addr, which_declare
```

```
              Go Version: go1.20.5
              Listener 1: tcp (addr: "0.0.0.0:8200", cluster
address: "0.0.0.0:8201", max_request_duration: "1m30s",
max_request_size: "33554432", tls: "enabled")
               Log Level:
                   Mlock: supported: true, enabled: true
           Recovery Mode: false
                 Storage: file
                 Version: Vault v1.14.0, built 2023-06-
19T11:40:23Z
             Version Sha:
13a649f860186dffe3f3a4459814d87191efc321

==> Vault server started! Log data will stream in below:

2023-11-23T15:58:10.400+0530 [INFO]  proxy environment:
http_proxy="" https_proxy="" no_proxy=""
2023-11-23T15:58:10.432+0530 [INFO]  core: Initializing
version history cache for core
2023-11-23T15:58:20.422+0530 [INFO]  core: security barrier
not initialized
2023-11-23T15:58:20.422+0530 [INFO]  core: seal configuration
missing, not initialized
2023-11-23T15:58:20.424+0530 [INFO]  core: security barrier
not initialized
2023-11-23T15:58:20.425+0530 [INFO]  core: security barrier
initialized: stored=1 shares=5 threshold=3
2023-11-23T15:58:20.427+0530 [INFO]  core: post-unseal setup
starting
2023-11-23T15:58:20.448+0530 [INFO]  core: loaded wrapping
token key
2023-11-23T15:58:20.448+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-11-23T15:58:20.448+0530 [INFO]  core: no mounts; adding
default mount table
2023-11-23T15:58:20.449+0530 [INFO]  core: successfully
mounted: type=cubbyhole version="v1.14.0+builtin.vault"
path=cubbyhole/ namespace="ID: root. Path: "
2023-11-23T15:58:20.449+0530 [INFO]  core: successfully
mounted: type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-11-23T15:58:20.449+0530 [INFO]  core: successfully
mounted: type=identity version="v1.14.0+builtin.vault"
path=identity/ namespace="ID: root. Path: "
2023-11-23T15:58:20.451+0530 [INFO]  core: successfully
mounted: type=token version="v1.14.0+builtin.vault"
```

```
path=token/ namespace="ID: root. Path: "
2023-11-23T15:58:20.452+0530 [INFO]  rollback: starting
rollback manager
2023-11-23T15:58:20.452+0530 [INFO]  core: restoring leases
2023-11-23T15:58:20.453+0530 [INFO]  identity: entities
restored
2023-11-23T15:58:20.453+0530 [INFO]  identity: groups restored
2023-11-23T15:58:20.453+0530 [INFO]  expiration: lease restore
complete
2023-11-23T15:58:20.453+0530 [INFO]  core: usage gauge
collection is disabled
2023-11-23T15:58:20.453+0530 [INFO]  core: Recorded vault
version: vault version=1.14.0 upgrade time="2023-11-23
10:28:20.453481904 +0000 UTC" build date=2023-06-19T11:40:23Z
2023-11-23T15:58:20.818+0530 [INFO]  core: post-unseal setup
complete
2023-11-23T15:58:20.819+0530 [INFO]  core: root token
generated
2023-11-23T15:58:20.819+0530 [INFO]  core: pre-seal teardown
starting
2023-11-23T15:58:20.819+0530 [INFO]  rollback: stopping
rollback manager
2023-11-23T15:58:20.819+0530 [INFO]  core: pre-seal teardown
complete
2023-11-23T15:58:21.116+0530 [INFO]  core.cluster-
listener.tcp: starting listener: listener_address=0.0.0.0:8201
2023-11-23T15:58:21.116+0530 [INFO]  core.cluster-listener:
serving cluster requests: cluster_listen_address=[::]:8201
2023-11-23T15:58:21.117+0530 [INFO]  core: post-unseal setup
starting
2023-11-23T15:58:21.117+0530 [INFO]  core: loaded wrapping
token key
2023-11-23T15:58:21.117+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-11-23T15:58:21.119+0530 [INFO]  core: successfully
mounted: type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-11-23T15:58:21.120+0530 [INFO]  core: successfully
mounted: type=identity version="v1.14.0+builtin.vault"
path=identity/ namespace="ID: root. Path: "
2023-11-23T15:58:21.120+0530 [INFO]  core: successfully
mounted: type=cubbyhole version="v1.14.0+builtin.vault"
path=cubbyhole/ namespace="ID: root. Path: "
2023-11-23T15:58:21.123+0530 [INFO]  core: successfully
mounted: type=token version="v1.14.0+builtin.vault"
path=token/ namespace="ID: root. Path: "
```

```
2023-11-23T15:58:21.123+0530 [INFO]  rollback: starting
rollback manager
2023-11-23T15:58:21.124+0530 [INFO]  core: restoring leases
2023-11-23T15:58:21.124+0530 [INFO]  identity: entities
restored
2023-11-23T15:58:21.124+0530 [INFO]  identity: groups restored
2023-11-23T15:58:21.124+0530 [INFO]  expiration: lease restore
complete
2023-11-23T15:58:21.125+0530 [INFO]  core: usage gauge
collection is disabled
2023-11-23T15:58:21.125+0530 [INFO]  core: post-unseal setup
complete
2023-11-23T15:58:21.125+0530 [INFO]  core: vault is unsealed
Success! Uploaded policy: mcctb-policy
2023-11-23T15:58:21.600+0530 [INFO]  core: enabled credential
backend: path=approle/ type=approle version=""
Success! Enabled approle auth method at: approle/
2023-11-23T15:58:21.690+0530 [INFO]  core: successful mount:
namespace="" path=mcctb/ type=kv version=""
Success! Enabled the kv secrets engine at: mcctb/
Success! Data written to: auth/approle/role/mcctb-app
Upgrading to NetApp-MetroCluster-Tiebreaker-Software-1.6P1-
1.x86_64.rpm
Preparing...
################################## [100%]
Updating / installing...
   1:NetApp-MetroCluster-Tiebreaker-
So################################## [ 50%]
Performing file integrity check
etc/cron.weekly/metrocluster-tiebreaker-support is Ok
etc/cron.weekly/metrocluster-tiebreaker-support-cov is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software-cov is Ok
etc/logrotate.d/mcctb is Ok
opt/netapp/mcctb/lib/common/activation-1.1.1.jar is Ok
opt/netapp/mcctb/lib/common/aopalliance.jar is Ok
opt/netapp/mcctb/lib/common/args4j.jar is Ok
opt/netapp/mcctb/lib/common/aspectjrt.jar is Ok
opt/netapp/mcctb/lib/common/aspectjweaver.jar is Ok
opt/netapp/mcctb/lib/common/asup.jar is Ok
opt/netapp/mcctb/lib/common/bcpkix-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bctls-fips-1.0.13.jar is Ok
opt/netapp/mcctb/lib/common/bctls-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bcutil-jdk18on.jar is Ok
```

```
opt/netapp/mcctb/lib/common/cglib.jar is Ok
opt/netapp/mcctb/lib/common/commons-codec.jar is Ok
opt/netapp/mcctb/lib/common/commons-collections4.jar is Ok
opt/netapp/mcctb/lib/common/commons-compress.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.src.jar is Ok
opt/netapp/mcctb/lib/common/commons-dbcp2.jar is Ok
opt/netapp/mcctb/lib/common/commons-io.jar is Ok
opt/netapp/mcctb/lib/common/commons-lang3.jar is Ok
opt/netapp/mcctb/lib/common/commons-logging.jar is Ok
opt/netapp/mcctb/lib/common/commons-pool2.jar is Ok
opt/netapp/mcctb/lib/common/guava.jar is Ok
opt/netapp/mcctb/lib/common/httpclient.jar is Ok
opt/netapp/mcctb/lib/common/httpcore.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.activation.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.xml.bind-api.jar is Ok
opt/netapp/mcctb/lib/common/java-xmlbuilder.jar is Ok
opt/netapp/mcctb/lib/common/javax.inject.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-api-2.3.1.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-core.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-impl.jar is Ok
opt/netapp/mcctb/lib/common/jline.jar is Ok
opt/netapp/mcctb/lib/common/jna.jar is Ok
opt/netapp/mcctb/lib/common/joda-time.jar is Ok
opt/netapp/mcctb/lib/common/jsch.jar is Ok
opt/netapp/mcctb/lib/common/json.jar is Ok
opt/netapp/mcctb/lib/common/jsvc.zip is Ok
opt/netapp/mcctb/lib/common/junixsocket-common.jar is Ok
opt/netapp/mcctb/lib/common/junixsocket-native-common.jar is
Ok
opt/netapp/mcctb/lib/common/logback-classic.jar is Ok
opt/netapp/mcctb/lib/common/logback-core.jar is Ok
opt/netapp/mcctb/lib/common/mail-1.6.2.jar is Ok
opt/netapp/mcctb/lib/common/mariadb-java-client.jar is Ok
opt/netapp/mcctb/lib/common/mcctb-mib.jar is Ok
opt/netapp/mcctb/lib/common/mcctb.jar is Ok
opt/netapp/mcctb/lib/common/mockito-core.jar is Ok
opt/netapp/mcctb/lib/common/slf4j-api.jar is Ok
opt/netapp/mcctb/lib/common/snmp4j.jar is Ok
opt/netapp/mcctb/lib/common/spring-aop.jar is Ok
opt/netapp/mcctb/lib/common/spring-beans.jar is Ok
opt/netapp/mcctb/lib/common/spring-context-support.jar is Ok
opt/netapp/mcctb/lib/common/spring-context.jar is Ok
opt/netapp/mcctb/lib/common/spring-core.jar is Ok
opt/netapp/mcctb/lib/common/spring-expression.jar is Ok
opt/netapp/mcctb/lib/common/spring-web.jar is Ok
```

```
opt/netapp/mcctb/lib/common/vault-java-driver.jar is Ok
opt/netapp/mcctb/lib/common/xz.jar is Ok
opt/netapp/mcctb/lib/org.jacoco.agent-0.8.8-runtime.jar is Ok
opt/netapp/mcctb/bin/mcctb-asup-invoke is Ok
opt/netapp/mcctb/bin/mcctb_postrotate is Ok
opt/netapp/mcctb/bin/netapp-metrocluster-tiebreaker-software-
cli is Ok
/

Synchronizing state of netapp-metrocluster-tiebreaker-
software.service with SysV service script with
/usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable
netapp-metrocluster-tiebreaker-software

Attempting to start NetApp MetroCluster Tiebreaker software
services
Started NetApp MetroCluster Tiebreaker software services
Successfully upgraded NetApp MetroCluster Tiebreaker software
to version 1.6P1.
Cleaning up / removing...
   2:NetApp-MetroCluster-Tiebreaker-
So################################## [100%]
```

Tiebreaker 1.6のインストールまたはアップグレード

Tiebreaker 1.6をインストールするか、Tiebreaker 1.5または1.4からTiebreaker 1.6にアップグレードできます。

手順

1. MetroCluster Tiebreaker 1.6ソフトウェアをダウンロードします。

   "MetroCluster Tiebreaker（ダウンロード）- NetApp Support Site"

2. root ユーザとしてホストにログインします。
3. アップグレードを実行する場合は、実行しているTiebreakerのバージョンを確認します。

   次の例はTiebreaker 1.5を示しています。

```
[root@mcctb ~] # netapp-metrocluster-tiebreaker-software-cli
NetApp MetroCluster Tiebreaker :> version show
NetApp MetroCluster Tiebreaker 1.5: Sun Mar 13 09:59:02 IST 2022
NetApp MetroCluster Tiebreaker :> exit
```

4. Tiebreakerソフトウェアをインストールまたはアップグレードします。

Tiebreaker 1.6のインストール

Tiebreaker 1.6を新規にインストールする場合は、次の手順を実行します。

手順

a. で次のコマンドを実行します。 `[root@mcctb ~] #` インストールを開始するようにプロンプトを表示します。

```
sh MetroClusterTiebreakerInstall-1.6
```

インストールが完了すると、次の出力が表示されます。

例

```
Extracting the MetroCluster Tiebreaker installation/upgrade
archive
Install digest hash is Ok
Performing the MetroCluster Tiebreaker code signature check
Install code signature is Ok
Enter unix user account to use for the installation:
mcctbadminuser
Unix user account "mcctbadminuser" doesn't exist. Do you wish
to create "mcctbadminuser" user account? [Y/N]: y
useradd: warning: the home directory already exists.
Not copying any file from skel directory into it.
Creating mailbox file: File exists
Unix account "mcctbadminuser" created.
Changing password for user mcctbadminuser.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
MetroCluster Tiebreaker requires unix user account
"mcctbadminuser" to be added to the group "mcctbgrp" for admin
access.
Do you wish to add ? [Y/N]: y
Unix user account "mcctbadminuser" added to "mcctbgrp".
Do you wish to generate your own public-private key pair for
encrypting audit log? [Y/N]: y
Generating public-private key pair...
Configuring Vault...
Starting vault server...
==> Vault server configuration:

             Api Address: <api_address>
                     Cgo: disabled
         Cluster Address: <cluster_address>
   Environment Variables: BASH_FUNC_which%%,
DBUS_SESSION_BUS_ADDRESS, GODEBUG, HISTCONTROL, HISTSIZE,
HOME, HOSTNAME, HOST_ACCOUNT, LANG, LESSOPEN, LOGNAME,
LS_COLORS, MAIL, PATH, PWD, SHELL, SHLVL, SSH_CLIENT,
SSH_CONNECTION, SSH_TTY, STAF_TEMP_DIR, TERM, USER,
VAULT_ADDR, VAULT_TOKEN, XDG_RUNTIME_DIR, XDG_SESSION_ID, _,
vault_Addr, which_declare
              Go Version: go1.20.5
              Listener 1: tcp (addr: "0.0.0.0:8200", cluster
address: "0.0.0.0:8201", max_request_duration: "1m30s",
max_request_size: "33554432", tls: "enabled")
```

```
               Log Level:
                   Mlock: supported: true, enabled: true
           Recovery Mode: false
                 Storage: file
                 Version: Vault v1.14.0, built 2023-06-
19T11:40:23Z
             Version Sha:
13a649f860186dffe3f3a4459814d87191efc321

==> Vault server started! Log data will stream in below:

2023-11-23T15:14:28.532+0530 [INFO]  proxy environment:
http_proxy="" https_proxy="" no_proxy=""
2023-11-23T15:14:28.577+0530 [INFO]  core: Initializing
version history cache for core
2023-11-23T15:14:38.552+0530 [INFO]  core: security barrier
not initialized
2023-11-23T15:14:38.552+0530 [INFO]  core: seal configuration
missing, not initialized
2023-11-23T15:14:38.554+0530 [INFO]  core: security barrier
not initialized
2023-11-23T15:14:38.555+0530 [INFO]  core: security barrier
initialized: stored=1 shares=5 threshold=3
2023-11-23T15:14:38.556+0530 [INFO]  core: post-unseal setup
starting
2023-11-23T15:14:38.577+0530 [INFO]  core: loaded wrapping
token key
2023-11-23T15:14:38.577+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-11-23T15:14:38.577+0530 [INFO]  core: no mounts; adding
default mount table
2023-11-23T15:14:38.578+0530 [INFO]  core: successfully
mounted: type=cubbyhole version="v1.14.0+builtin.vault"
path=cubbyhole/ namespace="ID: root. Path: "
2023-11-23T15:14:38.578+0530 [INFO]  core: successfully
mounted: type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-11-23T15:14:38.578+0530 [INFO]  core: successfully
mounted: type=identity version="v1.14.0+builtin.vault"
path=identity/ namespace="ID: root. Path: "
2023-11-23T15:14:38.581+0530 [INFO]  core: successfully
mounted: type=token version="v1.14.0+builtin.vault"
path=token/ namespace="ID: root. Path: "
2023-11-23T15:14:38.581+0530 [INFO]  rollback: starting
rollback manager
2023-11-23T15:14:38.581+0530 [INFO]  core: restoring leases
```

```
2023-11-23T15:14:38.582+0530 [INFO]  expiration: lease restore
complete
2023-11-23T15:14:38.582+0530 [INFO]  identity: entities
restored
2023-11-23T15:14:38.582+0530 [INFO]  identity: groups restored
2023-11-23T15:14:38.583+0530 [INFO]  core: Recorded vault
version: vault version=1.14.0 upgrade time="2023-11-23
09:44:38.582881162 +0000 UTC" build date=2023-06-19T11:40:23Z
2023-11-23T15:14:38.583+0530 [INFO]  core: usage gauge
collection is disabled
2023-11-23T15:14:38.998+0530 [INFO]  core: post-unseal setup
complete
2023-11-23T15:14:38.999+0530 [INFO]  core: root token
generated
2023-11-23T15:14:38.999+0530 [INFO]  core: pre-seal teardown
starting
2023-11-23T15:14:38.999+0530 [INFO]  rollback: stopping
rollback manager
2023-11-23T15:14:38.999+0530 [INFO]  core: pre-seal teardown
complete
2023-11-23T15:14:39.311+0530 [INFO]  core.cluster-
listener.tcp: starting listener: listener_address=0.0.0.0:8201
2023-11-23T15:14:39.311+0530 [INFO]  core.cluster-listener:
serving cluster requests: cluster_listen_address=[::]:8201
2023-11-23T15:14:39.312+0530 [INFO]  core: post-unseal setup
starting
2023-11-23T15:14:39.312+0530 [INFO]  core: loaded wrapping
token key
2023-11-23T15:14:39.312+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-11-23T15:14:39.313+0530 [INFO]  core: successfully
mounted: type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-11-23T15:14:39.313+0530 [INFO]  core: successfully
mounted: type=identity version="v1.14.0+builtin.vault"
path=identity/ namespace="ID: root. Path: "
2023-11-23T15:14:39.313+0530 [INFO]  core: successfully
mounted: type=cubbyhole version="v1.14.0+builtin.vault"
path=cubbyhole/ namespace="ID: root. Path: "
2023-11-23T15:14:39.314+0530 [INFO]  core: successfully
mounted: type=token version="v1.14.0+builtin.vault"
path=token/ namespace="ID: root. Path: "
2023-11-23T15:14:39.314+0530 [INFO]  rollback: starting
rollback manager
2023-11-23T15:14:39.314+0530 [INFO]  core: restoring leases
2023-11-23T15:14:39.314+0530 [INFO]  identity: entities
```

```
restored
2023-11-23T15:14:39.314+0530 [INFO]  expiration: lease restore
complete
2023-11-23T15:14:39.314+0530 [INFO]  identity: groups restored
2023-11-23T15:14:39.315+0530 [INFO]  core: usage gauge
collection is disabled
2023-11-23T15:14:39.316+0530 [INFO]  core: post-unseal setup
complete
2023-11-23T15:14:39.316+0530 [INFO]  core: vault is unsealed
Success! Uploaded policy: mcctb-policy
2023-11-23T15:14:39.795+0530 [INFO]  core: enabled credential
backend: path=approle/ type=approle version=""
Success! Enabled approle auth method at: approle/
2023-11-23T15:14:39.885+0530 [INFO]  core: successful mount:
namespace="" path=mcctb/ type=kv version=""
Success! Enabled the kv secrets engine at: mcctb/
Success! Data written to: auth/approle/role/mcctb-app
Installing the NetApp-MetroCluster-Tiebreaker-Software-1.6-
1.x86_64.rpm
Preparing...                          #
################################# # [100%]

Updating / installing...

1:NetApp-MetroCluster-Tiebreaker-So#
################################# # [100%]
Performing file integrity check
etc/cron.weekly/metrocluster-tiebreaker-support is Ok
etc/cron.weekly/metrocluster-tiebreaker-support-cov is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software-cov is Ok
etc/logrotate.d/mcctb is Ok
opt/netapp/mcctb/lib/common/activation-1.1.1.jar is Ok
opt/netapp/mcctb/lib/common/aopalliance.jar is Ok
opt/netapp/mcctb/lib/common/args4j.jar is Ok
opt/netapp/mcctb/lib/common/aspectjrt.jar is Ok
opt/netapp/mcctb/lib/common/aspectjweaver.jar is Ok
opt/netapp/mcctb/lib/common/asup.jar is Ok
opt/netapp/mcctb/lib/common/bcpkix-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bctls-fips-1.0.13.jar is Ok
opt/netapp/mcctb/lib/common/bctls-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bcutil-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/cglib.jar is Ok
opt/netapp/mcctb/lib/common/commons-codec.jar is Ok
```

```
opt/netapp/mcctb/lib/common/commons-collections4.jar is Ok
opt/netapp/mcctb/lib/common/commons-compress.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.src.jar is Ok
opt/netapp/mcctb/lib/common/commons-dbcp2.jar is Ok
opt/netapp/mcctb/lib/common/commons-io.jar is Ok
opt/netapp/mcctb/lib/common/commons-lang3.jar is Ok
opt/netapp/mcctb/lib/common/commons-logging.jar is Ok
opt/netapp/mcctb/lib/common/commons-pool2.jar is Ok
opt/netapp/mcctb/lib/common/guava.jar is Ok
opt/netapp/mcctb/lib/common/httpclient.jar is Ok
opt/netapp/mcctb/lib/common/httpcore.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.activation.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.xml.bind-api.jar is Ok
opt/netapp/mcctb/lib/common/java-xmlbuilder.jar is Ok
opt/netapp/mcctb/lib/common/javax.inject.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-api-2.3.1.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-core.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-impl.jar is Ok
opt/netapp/mcctb/lib/common/jline.jar is Ok
opt/netapp/mcctb/lib/common/jna.jar is Ok
opt/netapp/mcctb/lib/common/joda-time.jar is Ok
opt/netapp/mcctb/lib/common/jsch.jar is Ok
opt/netapp/mcctb/lib/common/json.jar is Ok
opt/netapp/mcctb/lib/common/jsvc.zip is Ok
opt/netapp/mcctb/lib/common/junixsocket-common.jar is Ok
opt/netapp/mcctb/lib/common/junixsocket-native-common.jar is
Ok
opt/netapp/mcctb/lib/common/logback-classic.jar is Ok
opt/netapp/mcctb/lib/common/logback-core.jar is Ok
opt/netapp/mcctb/lib/common/mail-1.6.2.jar is Ok
opt/netapp/mcctb/lib/common/mariadb-java-client.jar is Ok
opt/netapp/mcctb/lib/common/mcctb-mib.jar is Ok
opt/netapp/mcctb/lib/common/mcctb.jar is Ok
opt/netapp/mcctb/lib/common/mockito-core.jar is Ok
opt/netapp/mcctb/lib/common/slf4j-api.jar is Ok
opt/netapp/mcctb/lib/common/snmp4j.jar is Ok
opt/netapp/mcctb/lib/common/spring-aop.jar is Ok
opt/netapp/mcctb/lib/common/spring-beans.jar is Ok
opt/netapp/mcctb/lib/common/spring-context-support.jar is Ok
opt/netapp/mcctb/lib/common/spring-context.jar is Ok
opt/netapp/mcctb/lib/common/spring-core.jar is Ok
opt/netapp/mcctb/lib/common/spring-expression.jar is Ok
opt/netapp/mcctb/lib/common/spring-web.jar is Ok
opt/netapp/mcctb/lib/common/vault-java-driver.jar is Ok
opt/netapp/mcctb/lib/common/xz.jar is Ok
```

```
opt/netapp/mcctb/lib/org.jacoco.agent-0.8.8-runtime.jar is Ok
opt/netapp/mcctb/bin/mcctb-asup-invoke is Ok
opt/netapp/mcctb/bin/mcctb_postrotate is Ok
opt/netapp/mcctb/bin/netapp-metrocluster-tiebreaker-software-
cli is Ok
/

Synchronizing state of netapp-metrocluster-tiebreaker-
software.service with SysV service script with
/usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable
netapp-metrocluster-tiebreaker-software
Created symlink /etc/systemd/system/multi-
user.target.wants/netapp-metrocluster-tiebreaker-
software.service → /etc/systemd/system/netapp-metrocluster-
tiebreaker-software.service.

Attempting to start NetApp MetroCluster Tiebreaker software
services
Started NetApp MetroCluster Tiebreaker software services
Successfully installed NetApp MetroCluster Tiebreaker software
version 1.6.
```

1.5から1.6へのアップグレード

Tiebreaker 1.5ソフトウェアのバージョンをTiebreaker 1.6にアップグレードするには、次の手順を実行します。

手順

a. で次のコマンドを実行します。 `[root@mcctb ~] #` ソフトウェアのアップグレードを求めるプロンプトを表示します。

```
sh MetroClusterTiebreakerInstall-1.6
```

アップグレードが完了すると、次の出力が表示されます。

例

```
Extracting the MetroCluster Tiebreaker installation/upgrade
archive
Install digest hash is Ok
Performing the MetroCluster Tiebreaker code signature check
Install code signature is Ok

Enter database user name : root

Please enter database password for root
Enter password:

Password updated successfully in the database.

Do you wish to generate your own public-private key pair for
encrypting audit log? [Y/N]: y
Generating public-private key pair...
Configuring Vault...
==> Vault shutdown triggered
2023-07-21T00:30:22.335+0530 [INFO]  core: marked as sealed
2023-07-21T00:30:22.335+0530 [INFO]  core: pre-seal teardown
starting
2023-07-21T00:30:22.335+0530 [INFO]  rollback: stopping
rollback manager
2023-07-21T00:30:22.335+0530 [INFO]  core: pre-seal teardown
complete
2023-07-21T00:30:22.335+0530 [INFO]  core: stopping cluster
listeners
2023-07-21T00:30:22.335+0530 [INFO]  core.cluster-listener:
forwarding rpc listeners stopped
2023-07-21T00:30:22.375+0530 [INFO]  core.cluster-listener:
rpc listeners successfully shut down
2023-07-21T00:30:22.375+0530 [INFO]  core: cluster listeners
successfully shut down
2023-07-21T00:30:22.376+0530 [INFO]  core: vault is sealed
Starting vault server...
==> Vault server configuration:

             Api Address: <api_address>
                     Cgo: disabled
         Cluster Address: <cluster_address>
   Environment Variables: BASH_FUNC_which%%,
DBUS_SESSION_BUS_ADDRESS, GODEBUG, HISTCONTROL, HISTSIZE,
HOME, HOSTNAME, HOST_ACCOUNT, LANG, LESSOPEN, LOGNAME,
LS_COLORS, MAIL, PATH, PWD, SHELL, SHLVL, SSH_CLIENT,
```

```
SSH_CONNECTION, SSH_TTY, STAF_TEMP_DIR, TERM, USER,
VAULT_ADDR, VAULT_TOKEN, XDG_RUNTIME_DIR, XDG_SESSION_ID, _,
vault_Addr, which_declare
              Go Version: go1.20.5
              Listener 1: tcp (addr: "0.0.0.0:8200", cluster
address: "0.0.0.0:8201", max_request_duration: "1m30s",
max_request_size: "33554432", tls: "enabled")
               Log Level:
                   Mlock: supported: true, enabled: true
           Recovery Mode: false
                 Storage: file
                 Version: Vault v1.14.0, built 2023-06-
19T11:40:23Z
             Version Sha:
13a649f860186dffe3f3a4459814d87191efc321

==> Vault server started! Log data will stream in below:

2023-07-21T00:30:33.065+0530 [INFO]  proxy environment:
http_proxy="" https_proxy="" no_proxy=""
2023-07-21T00:30:33.098+0530 [INFO]  core: Initializing
version history cache for core
2023-07-21T00:30:43.092+0530 [INFO]  core: security barrier
not initialized
2023-07-21T00:30:43.092+0530 [INFO]  core: seal configuration
missing, not initialized
2023-07-21T00:30:43.094+0530 [INFO]  core: security barrier
not initialized
2023-07-21T00:30:43.096+0530 [INFO]  core: security barrier
initialized: stored=1 shares=5 threshold=3
2023-07-21T00:30:43.098+0530 [INFO]  core: post-unseal setup
starting
2023-07-21T00:30:43.124+0530 [INFO]  core: loaded wrapping
token key
2023-07-21T00:30:43.124+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-07-21T00:30:43.124+0530 [INFO]  core: no mounts; adding
default mount table
2023-07-21T00:30:43.125+0530 [INFO]  core: successfully
mounted: type=cubbyhole version="v1.14.0+builtin.vault"
path=cubbyhole/ namespace="ID: root. Path: "
2023-07-21T00:30:43.126+0530 [INFO]  core: successfully
mounted: type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-07-21T00:30:43.126+0530 [INFO]  core: successfully
mounted: type=identity version="v1.14.0+builtin.vault"
```

```
path=identity/ namespace="ID: root. Path: "
2023-07-21T00:30:43.129+0530 [INFO]  core: successfully
mounted: type=token version="v1.14.0+builtin.vault"
path=token/ namespace="ID: root. Path: "
2023-07-21T00:30:43.130+0530 [INFO]  rollback: starting
rollback manager
2023-07-21T00:30:43.130+0530 [INFO]  core: restoring leases
2023-07-21T00:30:43.130+0530 [INFO]  identity: entities
restored
2023-07-21T00:30:43.130+0530 [INFO]  identity: groups restored
2023-07-21T00:30:43.131+0530 [INFO]  core: usage gauge
collection is disabled
2023-07-21T00:30:43.131+0530 [INFO]  expiration: lease restore
complete
2023-07-21T00:30:43.131+0530 [INFO]  core: Recorded vault
version: vault version=1.14.0 upgrade time="2023-07-20
19:00:43.131158543 +0000 UTC" build date=2023-06-19T11:40:23Z
2023-07-21T00:30:43.371+0530 [INFO]  core: post-unseal setup
complete
2023-07-21T00:30:43.371+0530 [INFO]  core: root token
generated
2023-07-21T00:30:43.371+0530 [INFO]  core: pre-seal teardown
starting
2023-07-21T00:30:43.371+0530 [INFO]  rollback: stopping
rollback manager
2023-07-21T00:30:43.372+0530 [INFO]  core: pre-seal teardown
complete
2023-07-21T00:30:43.694+0530 [INFO]  core.cluster-
listener.tcp: starting listener: listener_address=0.0.0.0:8201
2023-07-21T00:30:43.695+0530 [INFO]  core.cluster-listener:
serving cluster requests: cluster_listen_address=[::]:8201
2023-07-21T00:30:43.695+0530 [INFO]  core: post-unseal setup
starting
2023-07-21T00:30:43.696+0530 [INFO]  core: loaded wrapping
token key
2023-07-21T00:30:43.696+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-07-21T00:30:43.697+0530 [INFO]  core: successfully
mounted: type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-07-21T00:30:43.698+0530 [INFO]  core: successfully
mounted: type=identity version="v1.14.0+builtin.vault"
path=identity/ namespace="ID: root. Path: "
2023-07-21T00:30:43.698+0530 [INFO]  core: successfully
mounted: type=cubbyhole version="v1.14.0+builtin.vault"
path=cubbyhole/ namespace="ID: root. Path: "
```

```
2023-07-21T00:30:43.701+0530 [INFO]  core: successfully
mounted: type=token version="v1.14.0+builtin.vault"
path=token/ namespace="ID: root. Path: "
2023-07-21T00:30:43.701+0530 [INFO]  rollback: starting
rollback manager
2023-07-21T00:30:43.702+0530 [INFO]  core: restoring leases
2023-07-21T00:30:43.702+0530 [INFO]  identity: entities
restored
2023-07-21T00:30:43.702+0530 [INFO]  expiration: lease restore
complete
2023-07-21T00:30:43.702+0530 [INFO]  identity: groups restored
2023-07-21T00:30:43.702+0530 [INFO]  core: usage gauge
collection is disabled
2023-07-21T00:30:43.703+0530 [INFO]  core: post-unseal setup
complete
2023-07-21T00:30:43.703+0530 [INFO]  core: vault is unsealed
Success! Uploaded policy: mcctb-policy
2023-07-21T00:30:44.226+0530 [INFO]  core: enabled credential
backend: path=approle/ type=approle version=""
Success! Enabled approle auth method at: approle/
2023-07-21T00:30:44.315+0530 [INFO]  core: successful mount:
namespace="" path=mcctb/ type=kv version=""
Success! Enabled the kv secrets engine at: mcctb/
Success! Data written to: auth/approle/role/mcctb-app
Upgrading to NetApp-MetroCluster-Tiebreaker-Software-1.6-
1.x86_64.rpm
Preparing...
################################## [100%]
Updating / installing...
   1:NetApp-MetroCluster-Tiebreaker-
So################################## [ 50%]
Performing file integrity check
etc/cron.weekly/metrocluster-tiebreaker-support is Ok
etc/cron.weekly/metrocluster-tiebreaker-support-cov is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software-cov is Ok
etc/logrotate.d/mcctb is Ok
opt/netapp/mcctb/lib/common/activation-1.1.1.jar is Ok
opt/netapp/mcctb/lib/common/aopalliance.jar is Ok
opt/netapp/mcctb/lib/common/args4j.jar is Ok
opt/netapp/mcctb/lib/common/aspectjrt.jar is Ok
opt/netapp/mcctb/lib/common/aspectjweaver.jar is Ok
opt/netapp/mcctb/lib/common/asup.jar is Ok
opt/netapp/mcctb/lib/common/bcpkix-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk18on.jar is Ok
```

```
opt/netapp/mcctb/lib/common/bctls-fips-1.0.13.jar is Ok
opt/netapp/mcctb/lib/common/bctls-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bcutil-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/cglib.jar is Ok
opt/netapp/mcctb/lib/common/commons-codec.jar is Ok
opt/netapp/mcctb/lib/common/commons-collections4.jar is Ok
opt/netapp/mcctb/lib/common/commons-compress.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.src.jar is Ok
opt/netapp/mcctb/lib/common/commons-dbcp2.jar is Ok
opt/netapp/mcctb/lib/common/commons-io.jar is Ok
opt/netapp/mcctb/lib/common/commons-lang3.jar is Ok
opt/netapp/mcctb/lib/common/commons-logging.jar is Ok
opt/netapp/mcctb/lib/common/commons-pool2.jar is Ok
opt/netapp/mcctb/lib/common/guava.jar is Ok
opt/netapp/mcctb/lib/common/httpclient.jar is Ok
opt/netapp/mcctb/lib/common/httpcore.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.activation.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.xml.bind-api.jar is Ok
opt/netapp/mcctb/lib/common/java-xmlbuilder.jar is Ok
opt/netapp/mcctb/lib/common/javax.inject.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-api-2.3.1.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-core.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-impl.jar is Ok
opt/netapp/mcctb/lib/common/jline.jar is Ok
opt/netapp/mcctb/lib/common/jna.jar is Ok
opt/netapp/mcctb/lib/common/joda-time.jar is Ok
opt/netapp/mcctb/lib/common/jsch.jar is Ok
opt/netapp/mcctb/lib/common/json.jar is Ok
opt/netapp/mcctb/lib/common/jsvc.zip is Ok
opt/netapp/mcctb/lib/common/junixsocket-common.jar is Ok
opt/netapp/mcctb/lib/common/junixsocket-native-common.jar is
Ok
opt/netapp/mcctb/lib/common/logback-classic.jar is Ok
opt/netapp/mcctb/lib/common/logback-core.jar is Ok
opt/netapp/mcctb/lib/common/mail-1.6.2.jar is Ok
opt/netapp/mcctb/lib/common/mariadb-java-client.jar is Ok
opt/netapp/mcctb/lib/common/mcctb-mib.jar is Ok
opt/netapp/mcctb/lib/common/mcctb.jar is Ok
opt/netapp/mcctb/lib/common/mockito-core.jar is Ok
opt/netapp/mcctb/lib/common/slf4j-api.jar is Ok
opt/netapp/mcctb/lib/common/snmp4j.jar is Ok
opt/netapp/mcctb/lib/common/spring-aop.jar is Ok
opt/netapp/mcctb/lib/common/spring-beans.jar is Ok
opt/netapp/mcctb/lib/common/spring-context-support.jar is Ok
opt/netapp/mcctb/lib/common/spring-context.jar is Ok
```

```
opt/netapp/mcctb/lib/common/spring-core.jar is Ok
opt/netapp/mcctb/lib/common/spring-expression.jar is Ok
opt/netapp/mcctb/lib/common/spring-web.jar is Ok
opt/netapp/mcctb/lib/common/vault-java-driver.jar is Ok
opt/netapp/mcctb/lib/common/xz.jar is Ok
opt/netapp/mcctb/bin/mcctb_postrotate is Ok
opt/netapp/mcctb/bin/netapp-metrocluster-tiebreaker-software-
cli is Ok
/

Synchronizing state of netapp-metrocluster-tiebreaker-
software.service with SysV service script with
/usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable
netapp-metrocluster-tiebreaker-software

Attempting to start NetApp MetroCluster Tiebreaker software
services
Started NetApp MetroCluster Tiebreaker software services
Successfully upgraded NetApp MetroCluster Tiebreaker software
to version 1.6.
Cleaning up / removing...
   2:NetApp-MetroCluster-Tiebreaker-
So################################## [100%]
```

1.4から1.6にアップグレード

Tiebreaker 1.4ソフトウェアのバージョンをTiebreaker 1.6にアップグレードするには、次の手順に従います。

手順

a. で次のコマンドを実行します。 `[root@mcctb ~] #` ソフトウェアのアップグレードを求めるプロンプトを表示します。

```
sh MetroClusterTiebreakerInstall-1.6
```

アップグレードが完了すると、次の出力が表示されます。

例

```
Extracting the MetroCluster Tiebreaker installation/upgrade
archive
Install digest hash is Ok
Performing the MetroCluster Tiebreaker code signature check
Install code signature is Ok
Enter unix user account to use for the installation:
mcctbuseradmin1
Unix user account "mcctbuseradmin1" doesn't exist. Do you wish
to create "mcctbuseradmin1" user account? [Y/N]: y
Unix account "mcctbuseradmin1" created.
Changing password for user mcctbuseradmin1.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.

Enter database user name : root

Please enter database password for root
Enter password:

Password updated successfully in the database.

MetroCluster Tiebreaker requires unix user account
"mcctbuseradmin1" to be added to the group "mcctbgrp" for
admin access.
Do you wish to add ? [Y/N]: y
Unix user account "mcctbuseradmin1" added to "mcctbgrp".
Do you wish to generate your own public-private key pair for
encrypting audit log? [Y/N]: y
Generating public-private key pair...
Configuring Vault...
Starting vault server...
==> Vault server configuration:

             Api Address: <api_addess>
                     Cgo: disabled
         Cluster Address: <cluster_address>
   Environment Variables: BASH_FUNC_which%%,
DBUS_SESSION_BUS_ADDRESS, GODEBUG, HISTCONTROL, HISTSIZE,
HOME, HOSTNAME, HOST_ACCOUNT, LANG, LESSOPEN, LOGNAME,
LS_COLORS, MAIL, PATH, PWD, SHELL, SHLVL, SSH_CLIENT,
SSH_CONNECTION, SSH_TTY, STAF_TEMP_DIR, TERM, USER,
VAULT_ADDR, VAULT_TOKEN, XDG_RUNTIME_DIR, XDG_SESSION_ID, _,
vault_Addr, which_declare
```

```
              Go Version: go1.20.5
              Listener 1: tcp (addr: "0.0.0.0:8200", cluster
address: "0.0.0.0:8201", max_request_duration: "1m30s",
max_request_size: "33554432", tls: "enabled")
               Log Level:
                   Mlock: supported: true, enabled: true
           Recovery Mode: false
                 Storage: file
                 Version: Vault v1.14.0, built 2023-06-
19T11:40:23Z
             Version Sha:
13a649f860186dffe3f3a4459814d87191efc321

==> Vault server started! Log data will stream in below:

2023-11-23T15:58:10.400+0530 [INFO]  proxy environment:
http_proxy="" https_proxy="" no_proxy=""
2023-11-23T15:58:10.432+0530 [INFO]  core: Initializing
version history cache for core
2023-11-23T15:58:20.422+0530 [INFO]  core: security barrier
not initialized
2023-11-23T15:58:20.422+0530 [INFO]  core: seal configuration
missing, not initialized
2023-11-23T15:58:20.424+0530 [INFO]  core: security barrier
not initialized
2023-11-23T15:58:20.425+0530 [INFO]  core: security barrier
initialized: stored=1 shares=5 threshold=3
2023-11-23T15:58:20.427+0530 [INFO]  core: post-unseal setup
starting
2023-11-23T15:58:20.448+0530 [INFO]  core: loaded wrapping
token key
2023-11-23T15:58:20.448+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-11-23T15:58:20.448+0530 [INFO]  core: no mounts; adding
default mount table
2023-11-23T15:58:20.449+0530 [INFO]  core: successfully
mounted: type=cubbyhole version="v1.14.0+builtin.vault"
path=cubbyhole/ namespace="ID: root. Path: "
2023-11-23T15:58:20.449+0530 [INFO]  core: successfully
mounted: type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-11-23T15:58:20.449+0530 [INFO]  core: successfully
mounted: type=identity version="v1.14.0+builtin.vault"
path=identity/ namespace="ID: root. Path: "
2023-11-23T15:58:20.451+0530 [INFO]  core: successfully
mounted: type=token version="v1.14.0+builtin.vault"
```

```
path=token/ namespace="ID: root. Path: "
2023-11-23T15:58:20.452+0530 [INFO]  rollback: starting
rollback manager
2023-11-23T15:58:20.452+0530 [INFO]  core: restoring leases
2023-11-23T15:58:20.453+0530 [INFO]  identity: entities
restored
2023-11-23T15:58:20.453+0530 [INFO]  identity: groups restored
2023-11-23T15:58:20.453+0530 [INFO]  expiration: lease restore
complete
2023-11-23T15:58:20.453+0530 [INFO]  core: usage gauge
collection is disabled
2023-11-23T15:58:20.453+0530 [INFO]  core: Recorded vault
version: vault version=1.14.0 upgrade time="2023-11-23
10:28:20.453481904 +0000 UTC" build date=2023-06-19T11:40:23Z
2023-11-23T15:58:20.818+0530 [INFO]  core: post-unseal setup
complete
2023-11-23T15:58:20.819+0530 [INFO]  core: root token
generated
2023-11-23T15:58:20.819+0530 [INFO]  core: pre-seal teardown
starting
2023-11-23T15:58:20.819+0530 [INFO]  rollback: stopping
rollback manager
2023-11-23T15:58:20.819+0530 [INFO]  core: pre-seal teardown
complete
2023-11-23T15:58:21.116+0530 [INFO]  core.cluster-
listener.tcp: starting listener: listener_address=0.0.0.0:8201
2023-11-23T15:58:21.116+0530 [INFO]  core.cluster-listener:
serving cluster requests: cluster_listen_address=[::]:8201
2023-11-23T15:58:21.117+0530 [INFO]  core: post-unseal setup
starting
2023-11-23T15:58:21.117+0530 [INFO]  core: loaded wrapping
token key
2023-11-23T15:58:21.117+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-11-23T15:58:21.119+0530 [INFO]  core: successfully
mounted: type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-11-23T15:58:21.120+0530 [INFO]  core: successfully
mounted: type=identity version="v1.14.0+builtin.vault"
path=identity/ namespace="ID: root. Path: "
2023-11-23T15:58:21.120+0530 [INFO]  core: successfully
mounted: type=cubbyhole version="v1.14.0+builtin.vault"
path=cubbyhole/ namespace="ID: root. Path: "
2023-11-23T15:58:21.123+0530 [INFO]  core: successfully
mounted: type=token version="v1.14.0+builtin.vault"
path=token/ namespace="ID: root. Path: "
```

```
2023-11-23T15:58:21.123+0530 [INFO]  rollback: starting
rollback manager
2023-11-23T15:58:21.124+0530 [INFO]  core: restoring leases
2023-11-23T15:58:21.124+0530 [INFO]  identity: entities
restored
2023-11-23T15:58:21.124+0530 [INFO]  identity: groups restored
2023-11-23T15:58:21.124+0530 [INFO]  expiration: lease restore
complete
2023-11-23T15:58:21.125+0530 [INFO]  core: usage gauge
collection is disabled
2023-11-23T15:58:21.125+0530 [INFO]  core: post-unseal setup
complete
2023-11-23T15:58:21.125+0530 [INFO]  core: vault is unsealed
Success! Uploaded policy: mcctb-policy
2023-11-23T15:58:21.600+0530 [INFO]  core: enabled credential
backend: path=approle/ type=approle version=""
Success! Enabled approle auth method at: approle/
2023-11-23T15:58:21.690+0530 [INFO]  core: successful mount:
namespace="" path=mcctb/ type=kv version=""
Success! Enabled the kv secrets engine at: mcctb/
Success! Data written to: auth/approle/role/mcctb-app
Upgrading to NetApp-MetroCluster-Tiebreaker-Software-1.6-
1.x86_64.rpm
Preparing...
################################## [100%]
Updating / installing...
   1:NetApp-MetroCluster-Tiebreaker-
So################################## [ 50%]
Performing file integrity check
etc/cron.weekly/metrocluster-tiebreaker-support is Ok
etc/cron.weekly/metrocluster-tiebreaker-support-cov is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software-cov is Ok
etc/logrotate.d/mcctb is Ok
opt/netapp/mcctb/lib/common/activation-1.1.1.jar is Ok
opt/netapp/mcctb/lib/common/aopalliance.jar is Ok
opt/netapp/mcctb/lib/common/args4j.jar is Ok
opt/netapp/mcctb/lib/common/aspectjrt.jar is Ok
opt/netapp/mcctb/lib/common/aspectjweaver.jar is Ok
opt/netapp/mcctb/lib/common/asup.jar is Ok
opt/netapp/mcctb/lib/common/bcpkix-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bctls-fips-1.0.13.jar is Ok
opt/netapp/mcctb/lib/common/bctls-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bcutil-jdk18on.jar is Ok
```

```
opt/netapp/mcctb/lib/common/cglib.jar is Ok
opt/netapp/mcctb/lib/common/commons-codec.jar is Ok
opt/netapp/mcctb/lib/common/commons-collections4.jar is Ok
opt/netapp/mcctb/lib/common/commons-compress.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.src.jar is Ok
opt/netapp/mcctb/lib/common/commons-dbcp2.jar is Ok
opt/netapp/mcctb/lib/common/commons-io.jar is Ok
opt/netapp/mcctb/lib/common/commons-lang3.jar is Ok
opt/netapp/mcctb/lib/common/commons-logging.jar is Ok
opt/netapp/mcctb/lib/common/commons-pool2.jar is Ok
opt/netapp/mcctb/lib/common/guava.jar is Ok
opt/netapp/mcctb/lib/common/httpclient.jar is Ok
opt/netapp/mcctb/lib/common/httpcore.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.activation.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.xml.bind-api.jar is Ok
opt/netapp/mcctb/lib/common/java-xmlbuilder.jar is Ok
opt/netapp/mcctb/lib/common/javax.inject.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-api-2.3.1.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-core.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-impl.jar is Ok
opt/netapp/mcctb/lib/common/jline.jar is Ok
opt/netapp/mcctb/lib/common/jna.jar is Ok
opt/netapp/mcctb/lib/common/joda-time.jar is Ok
opt/netapp/mcctb/lib/common/jsch.jar is Ok
opt/netapp/mcctb/lib/common/json.jar is Ok
opt/netapp/mcctb/lib/common/jsvc.zip is Ok
opt/netapp/mcctb/lib/common/junixsocket-common.jar is Ok
opt/netapp/mcctb/lib/common/junixsocket-native-common.jar is
Ok
opt/netapp/mcctb/lib/common/logback-classic.jar is Ok
opt/netapp/mcctb/lib/common/logback-core.jar is Ok
opt/netapp/mcctb/lib/common/mail-1.6.2.jar is Ok
opt/netapp/mcctb/lib/common/mariadb-java-client.jar is Ok
opt/netapp/mcctb/lib/common/mcctb-mib.jar is Ok
opt/netapp/mcctb/lib/common/mcctb.jar is Ok
opt/netapp/mcctb/lib/common/mockito-core.jar is Ok
opt/netapp/mcctb/lib/common/slf4j-api.jar is Ok
opt/netapp/mcctb/lib/common/snmp4j.jar is Ok
opt/netapp/mcctb/lib/common/spring-aop.jar is Ok
opt/netapp/mcctb/lib/common/spring-beans.jar is Ok
opt/netapp/mcctb/lib/common/spring-context-support.jar is Ok
opt/netapp/mcctb/lib/common/spring-context.jar is Ok
opt/netapp/mcctb/lib/common/spring-core.jar is Ok
opt/netapp/mcctb/lib/common/spring-expression.jar is Ok
opt/netapp/mcctb/lib/common/spring-web.jar is Ok
```

```
opt/netapp/mcctb/lib/common/vault-java-driver.jar is Ok
opt/netapp/mcctb/lib/common/xz.jar is Ok
opt/netapp/mcctb/lib/org.jacoco.agent-0.8.8-runtime.jar is Ok
opt/netapp/mcctb/bin/mcctb-asup-invoke is Ok
opt/netapp/mcctb/bin/mcctb_postrotate is Ok
opt/netapp/mcctb/bin/netapp-metrocluster-tiebreaker-software-
cli is Ok
/

Synchronizing state of netapp-metrocluster-tiebreaker-
software.service with SysV service script with
/usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable
netapp-metrocluster-tiebreaker-software

Attempting to start NetApp MetroCluster Tiebreaker software
services
Started NetApp MetroCluster Tiebreaker software services
Successfully upgraded NetApp MetroCluster Tiebreaker software
to version 1.6.
Cleaning up / removing...
   2:NetApp-MetroCluster-Tiebreaker-
So################################## [100%]
```

Tiebreaker 1.5をインストール

ONTAP APIおよび**SSH**への管理アクセスを設定します

ONTAP APIおよびSSHへの管理アクセスを設定できます。

手順

1. ONTAP APIアクセスを持つ管理者ユーザを作成します。 `security login create -user-or-group -name mcctb -application ontapi -authentication-method password`
2. SSHアクセスを持つ管理者ユーザを作成します。 `security login create -user-or-group-name mcctb -application ssh -authentication-method password`
3. 新しい管理者ユーザが作成されたことを確認します。 `security login show`
4. パートナークラスタで同じ手順を繰り返します。

"管理者認証と RBAC" が実装されます。

TiebreakerソフトウェアをインストールまたはアップグレードするLinux前に、ホストのオペレーティングシステムに応じて、MySQLサーバまたはMariaDBサーバをインストールする必要があります。

手順

1. JDKのインストール
2. Vaultをインストールして設定します
3. MySQL サーバまたは MariaDB サーバをインストールします。

Linux ホストの種類は、です	作業
Red Hat Enterprise Linux 7 / CentOS 7.	Red Hat Enterprise Linux 7またはCentOS 7にMySQL Server 5.5.30以降および5.6.xバージョンをインストールする
Red Hat Enterprise Linux 8	Red Hat Enterprise Linux 8へのMariaDBサーバのインストール

JDKのインストール

TiebreakerソフトウェアをインストールまたはアップグレードするLinux前に、ホストシステムにJDKをインストールする必要があります。Tiebreaker 1.5以降では、OpenJDK 17、18、または19がサポートされます。

手順

1. 「root」ユーザまたはadvanced権限モードに変更できるsudoユーザとしてログインします。

```
login as: root
root@mcctb's password:
Last login: Fri Jan  8 21:33:00 2017 from host.domain.com
```

2. 使用可能なJDKバージョンを確認します

```
yum search openjdk
```

3. JDK 17、18、または19をインストールします。

   次のコマンドを実行すると、JDK 17がインストールされます。

```
yum install java-17-openjdk
```

4. インストールを確認します。

```
java -version
```

   インストールが正常に完了すると、次の出力が表示されます。

```
openjdk version "17.0.2" 2022-01-18 LTS
OpenJDK Runtime Environment 21.9 (build 17.0.2+8-LTS)
OpenJDK 64-Bit Server VM 21.9 (build 17.0.2+8-LTS, mixed mode, sharing)
```

Vaultをインストールして設定します

ローカルのボールトサーバーを持っていない場合、または使用する場合は、ボールトをインストールする必要があります。Vaultのインストールについては、この標準の手順 を参照してください。別のガイドラインについては、Hashicorpのインストール手順を参照してください。

> ネットワークにバックアップサーバがある場合は、そのバックアップを使用するようにMetroCluster Tiebreakerホストを設定できます。この場合、ホストにVaultをインストールする必要はありません。

手順

1. に移動します `/bin` ディレクトリ：

```
[root@mcctb] cd /bin
```

2. Vault zipファイルをダウンロードします。

```
[root@mcctb /bin]#  curl -sO
https://releases.hashicorp.com/vault/1.12.2/vault_1.12.2_linux_amd64.zip
```

3. ボールトファイルを解凍します。

```
[root@mcctb /bin]# unzip vault_1.12.2_linux_amd64.zip
Archive:  vault_1.12.2_linux_amd64.zip
  inflating: vault
```

4. インストールを確認します。

```
[root@mcctb /bin]# vault -version
Vault v1.12.2 (415e1fe3118eebd5df6cb60d13defdc01aa17b03), built 2022-11-
23T12:53:46Z
```

5. に移動します `/root` ディレクトリ：

```
[root@mcctb /bin] cd /root
```

6. ボルトコンフィギュレーションファイルを /root ディレクトリ。

   で [root@mcctb ~] プロンプトが表示されたら、次のコマンドをコピーして実行し、 config.hcl ファイル：

```
# cat > config.hcl << EOF
 storage "file" {
  address = "127.0.0.1:8500"
  path    = "/mcctb_vdata/data"
 }
 listener "tcp" {
   address     = "127.0.0.1:8200"
   tls_disable = 1
 }
EOF
```

7. ボールトサーバーを起動します。

```
[root@mcctb ~] vault server -config config.hcl &
```

8. ボールトアドレスをエクスポートします。

```
[root@mcctb ~]# export VAULT_ADDR="http://127.0.0.1:8200"
```

9. Vaultを初期化します。

```
[root@mcctb ~]# vault operator init
2022-12-15T14:57:22.113+0530 [INFO]  core: security barrier not
initialized
2022-12-15T14:57:22.113+0530 [INFO]  core: seal configuration missing,
not initialized
2022-12-15T14:57:22.114+0530 [INFO]  core: security barrier not
initialized
2022-12-15T14:57:22.116+0530 [INFO]  core: security barrier initialized:
stored=1 shares=5 threshold=3
2022-12-15T14:57:22.118+0530 [INFO]  core: post-unseal setup starting
2022-12-15T14:57:22.137+0530 [INFO]  core: loaded wrapping token key
2022-12-15T14:57:22.137+0530 [INFO]  core: Recorded vault version: vault
version=1.12.2 upgrade time="2022-12-15 09:27:22.137200412 +0000 UTC"
build date=2022-11-23T12:53:46Z
2022-12-15T14:57:22.137+0530 [INFO]  core: successfully setup plugin
catalog: plugin-directory=""
2022-12-15T14:57:22.137+0530 [INFO]  core: no mounts; adding default
```

```
mount table
2022-12-15T14:57:22.143+0530 [INFO]  core: successfully mounted backend:
type=cubbyhole version="" path=cubbyhole/
2022-12-15T14:57:22.144+0530 [INFO]  core: successfully mounted backend:
type=system version="" path=sys/
2022-12-15T14:57:22.144+0530 [INFO]  core: successfully mounted backend:
type=identity version="" path=identity/
2022-12-15T14:57:22.148+0530 [INFO]  core: successfully enabled
credential backend: type=token version="" path=token/ namespace="ID:
root. Path: "
2022-12-15T14:57:22.149+0530 [INFO]  rollback: starting rollback manager
2022-12-15T14:57:22.149+0530 [INFO]  core: restoring leases
2022-12-15T14:57:22.150+0530 [INFO]  expiration: lease restore complete
2022-12-15T14:57:22.150+0530 [INFO]  identity: entities restored
2022-12-15T14:57:22.150+0530 [INFO]  identity: groups restored
2022-12-15T14:57:22.151+0530 [INFO]  core: usage gauge collection is
disabled
2022-12-15T14:57:23.385+0530 [INFO]  core: post-unseal setup complete
2022-12-15T14:57:23.387+0530 [INFO]  core: root token generated
2022-12-15T14:57:23.387+0530 [INFO]  core: pre-seal teardown starting
2022-12-15T14:57:23.387+0530 [INFO]  rollback: stopping rollback manager
2022-12-15T14:57:23.387+0530 [INFO]  core: pre-seal teardown complete
Unseal Key 1: <unseal_key_1_id>
Unseal Key 2: <unseal_key_2_id>
Unseal Key 3: <unseal_key_3_id>
Unseal Key 4: <unseal_key_4_id>
Unseal Key 5: <unseal_key_5_id>

Initial Root Token: <initial_root_token_id>


Vault initialized with 5 key shares and a key threshold of 3. Please
securely
distribute the key shares printed above. When the Vault is re-sealed,
restarted, or stopped, you must supply at least 3 of these keys to
unseal it
before it can start servicing requests.

Vault does not store the generated root key. Without at least 3 keys to
reconstruct the root key, Vault will remain permanently sealed!

It is possible to generate new unseal keys, provided you have a quorum
of
existing unseal keys shares. See "vault operator rekey" for more
information.
```

キーIDと初期ルートトークンは、後で手順で使用できるように、記録して安全な場所に保存する必要があります。

10. ボールトルートトークンをエクスポートします。

```
[root@mcctb ~]#  export VAULT_TOKEN="<initial_root_token_id>"
```

11. 作成された5つのキーのうち3つを使用してVaultのシールを解除します。

    を実行する必要があります `vault operator unseal` 3つのキーそれぞれに対して次のコマンドを実行します。

    a. 最初のキーを使用してボールトのシールを解除します。

```
[root@mcctb ~]# vault operator unseal
Unseal Key (will be hidden):
Key                Value
---                -----
Seal Type          shamir
Initialized        true
Sealed             true
Total Shares       5
Threshold          3
Unseal Progress    1/3
Unseal Nonce       <unseal_key_1_id>
Version            1.12.2
Build Date         2022-11-23T12:53:46Z
Storage Type       file
HA Enabled         false
```

    b. 2番目のキーを使用してボールトのシールを解除します。

```
[root@mcctb ~]# vault operator unseal
Unseal Key (will be hidden):
Key                Value
---                -----
Seal Type          shamir
Initialized        true
Sealed             true
Total Shares       5
Threshold          3
Unseal Progress    2/3
Unseal Nonce       <unseal_key_2_id>
Version            1.12.2
Build Date         2022-11-23T12:53:46Z
Storage Type       file
HA Enabled         false
```

c. 3番目のキーを使用してボールトのシールを解除します。

```
[root@mcctb ~]# vault operator unseal
Unseal Key (will be hidden):
2022-12-15T15:15:00.980+0530 [INFO]  core.cluster-listener.tcp:
starting listener: listener_address=127.0.0.1:8201
2022-12-15T15:15:00.980+0530 [INFO]  core.cluster-listener: serving
cluster requests: cluster_listen_address=127.0.0.1:8201
2022-12-15T15:15:00.981+0530 [INFO]  core: post-unseal setup starting
2022-12-15T15:15:00.981+0530 [INFO]  core: loaded wrapping token key
2022-12-15T15:15:00.982+0530 [INFO]  core: successfully setup plugin
catalog: plugin-directory=""
2022-12-15T15:15:00.983+0530 [INFO]  core: successfully mounted
backend: type=system version="" path=sys/
2022-12-15T15:15:00.984+0530 [INFO]  core: successfully mounted
backend: type=identity version="" path=identity/
2022-12-15T15:15:00.984+0530 [INFO]  core: successfully mounted
backend: type=cubbyhole version="" path=cubbyhole/
2022-12-15T15:15:00.986+0530 [INFO]  core: successfully enabled
credential backend: type=token version="" path=token/ namespace="ID:
root. Path: "
2022-12-15T15:15:00.986+0530 [INFO]  rollback: starting rollback
manager
2022-12-15T15:15:00.987+0530 [INFO]  core: restoring leases
2022-12-15T15:15:00.987+0530 [INFO]  expiration: lease restore
complete
2022-12-15T15:15:00.987+0530 [INFO]  identity: entities restored
2022-12-15T15:15:00.987+0530 [INFO]  identity: groups restored
2022-12-15T15:15:00.988+0530 [INFO]  core: usage gauge collection is
disabled
2022-12-15T15:15:00.989+0530 [INFO]  core: post-unseal setup complete
2022-12-15T15:15:00.989+0530 [INFO]  core: vault is unsealed
Key             Value
---             -----
Seal Type       shamir
Initialized     true
Sealed          false
Total Shares    5
Threshold       3
Version         1.12.2
Build Date      2022-11-23T12:53:46Z
Storage Type    file
Cluster Name    vault-cluster
Cluster ID      <cluster_id>
HA Enabled      false
```

12. Vault sealedステータスがfalseであることを確認します。

```
[root@mcctb ~]# vault status
Key             Value
---             -----
Seal Type       shamir
Initialized     true
Sealed          false
Total Shares    5
Threshold       3
Version         1.12.2
Build Date      2022-11-23T12:53:46Z
Storage Type    file
Cluster Name    vault-cluster
Cluster ID      <cluster_id>
HA Enabled      false
```

13. 起動時に起動するようにVaultサービスを設定します。
    a. 次のコマンドを実行します。 `cd /etc/systemd/system`

    ```
    [root@mcctb ~]#  cd /etc/systemd/system
    ```

    b. で `[root@mcctb system]` 次のコマンドをプロンプト表示し、コピーして実行して、ボールトサービスファイルを作成します。

    ```
    # cat > vault.service << EOF
    [Unit]
    Description=Vault Service
    After=mariadb.service

    [Service]
    Type=forking
    ExecStart=/usr/bin/vault server -config /root/config.hcl &
    Restart=on-failure

    [Install]
    WantedBy=multi-user.target
    EOF
    ```

    c. 次のコマンドを実行します。 `systemctl daemon-reload`

    ```
    [root@mcctb system]#  systemctl daemon-reload
    ```

    d. 次のコマンドを実行します。 `systemctl enable vault.service`

```
[root@mcctb system]#  systemctl enable vault.service
Created symlink /etc/systemd/system/multi-
user.target.wants/vault.service → /etc/systemd/system/vault.service.
```

MetroCluster Tiebreakerのインストール時に、この機能を使用するように求められます。Vaultのシールを解除する方法を変更する場合は、MetroCluster Tiebreakerソフトウェアをアンインストールして再インストールする必要があります。

Red Hat Enterprise Linux 7または**CentOS 7**に**MySQL Server 5.5.30**以降および**5.6.x**バージョンをインストールする

Tiebreaker ソフトウェアをインストールまたはアップグレードする前に、ホストシステムに MySQL Server 5.5.30 以降および 5.6.x バージョンをインストールする必要があります。Red Hat Enterprise Linux 8の場合は、 MariaDBサーバのインストール。

手順

1. rootユーザまたはadvanced権限モードに変更できるsudoユーザとしてログインします。

```
login as: root
root@mcctb's password:
Last login: Fri Jan  8 21:33:00 2016 from host.domain.com
```

2. ホストシステムに MySQL リポジトリを追加します。

```
[root@mcctb~]#yum localinstall\https://dev.mysql.com/get/mysql57-community-
release-el6-11.noarch.rpm
```

```
Loaded plugins: product-id, refresh-packagekit, security, subscription-
manager
Setting up Local Package Process
Examining /var/tmp/yum-root-LLUw0r/mysql-community-release-el6-
5.noarch.rpm: mysql-community-release-el6-5.noarch
Marking /var/tmp/yum-root-LLUw0r/mysql-community-release-el6-
5.noarch.rpm to be installed
Resolving Dependencies
--> Running transaction check
---> Package mysql-community-release.noarch 0:el6-5 will be installed
--> Finished Dependency Resolution
Dependencies Resolved
================================================================================
========
Package               Arch   Version
                                      Repository
Size
================================================================================
========
Installing:
mysql-community-release
                       noarch el6-5 /mysql-community-release-el6-
5.noarch 4.3 k
Transaction Summary
================================================================================
========
Install       1 Package(s)
Total size: 4.3 k
Installed size: 4.3 k
Is this ok [y/N]: y
Downloading Packages:
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing : mysql-community-release-el6-5.noarch
1/1
  Verifying  : mysql-community-release-el6-5.noarch
1/1
Installed:
  mysql-community-release.noarch 0:el6-5
Complete!
```

3. MySQL 57リポジトリを無効にします。

```
[root@mcctb~]#yum-config -manager-disable mysql57-community
```

4. MySQL 56リポジトリを有効にします。

```
[root@mcctb~]#yum-config -manager-enable mysql56-community
```

5. リポジトリを有効にします。

```
[root@mcctb~]# yum repolist enabled | grep "mysql.-community."
```

```
mysql-connectors-community           MySQL Connectors Community
21
mysql-tools-community                MySQL Tools Community
35
mysql56-community                    MySQL 5.6 Community Server
231
```

6. MySQL Community Server をインストールします。

`[root@mcctb~]# yum は mysql-community-server をインストールします

```
Loaded plugins: product-id, refresh-packagekit, security, subscription-
manager
This system is not registered to Red Hat Subscription Management. You
can use subscription-manager
to register.
Setting up Install Process
Resolving Dependencies
--> Running transaction check
 .....Output truncated.....
---> Package mysql-community-libs-compat.x86_64 0:5.6.29-2.el6 will be
obsoleting
--> Finished Dependency Resolution
Dependencies Resolved
================================================================================
======
Package                          Arch   Version       Repository
Size
================================================================================
======
Installing:
 mysql-community-client         x86_64  5.6.29-2.el6  mysql56-community
18  M
     replacing  mysql.x86_64 5.1.71-1.el6
 mysql-community-libs           x86_64  5.6.29-2.el6  mysql56-community
1.9 M
```

```
     replacing  mysql-libs.x86_64 5.1.71-1.el6
 mysql-community-libs-compat    x86_64  5.6.29-2.el6  mysql56-community
1.6 M
     replacing  mysql-libs.x86_64 5.1.71-1.el6
 mysql-community-server         x86_64  5.6.29-2.el6  mysql56-community
53  M
     replacing  mysql-server.x86_64 5.1.71-1.el6
Installing for dependencies:
mysql-community-common          x86_64  5.6.29-2.el6  mysql56-community
308 k

Transaction Summary
================================================================================
=======
Install       5 Package(s)
Total download size: 74 M
Is this ok [y/N]: y
Downloading Packages:
(1/5): mysql-community-client-5.6.29-2.el6.x86_64.rpm       |  18 MB
00:28
(2/5): mysql-community-common-5.6.29-2.el6.x86_64.rpm       | 308 kB
00:01
(3/5): mysql-community-libs-5.6.29-2.el6.x86_64.rpm         | 1.9 MB
00:05
(4/5): mysql-community-libs-compat-5.6.29-2.el6.x86_64.rpm  | 1.6 MB
00:05
(5/5): mysql-community-server-5.6.29-2.el6.x86_64.rpm       |  53 MB
03:42
 ------------------------------------------------------------------------
--------
Total                                              289 kB/s |  74 MB
04:24
warning: rpmts_HdrFromFdno: Header V3 DSA/SHA1 Signature, key ID
<key_id> NOKEY
Retrieving key from file:/etc/pki/rpm-gpg/RPM-GPG-KEY-mysql
Importing GPG key 0x5072E1F5:
 Userid : MySQL Release Engineering <mysql-build@oss.oracle.com>
Package: mysql-community-release-el6-5.noarch
         (@/mysql-community-release-el6-5.noarch)
 From   : file:/etc/pki/rpm-gpg/RPM-GPG-KEY-mysql
Is this ok [y/N]: y
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing : mysql-community-common-5.6.29-2.el6.x86_64
```

```
....Output truncated....
1.el6.x86_64
7/8
  Verifying  : mysql-5.1.71-1.el6.x86_64
8/8
Installed:
  mysql-community-client.x86_64 0:5.6.29-2.el6
  mysql-community-libs.x86_64 0:5.6.29-2.el6
  mysql-community-libs-compat.x86_64 0:5.6.29-2.el6
  mysql-community-server.x86_64 0:5.6.29-2.el6

Dependency Installed:
  mysql-community-common.x86_64 0:5.6.29-2.el6

Replaced:
  mysql.x86_64 0:5.1.71-1.el6 mysql-libs.x86_64 0:5.1.71-1.el6
  mysql-server.x86_64 0:5.1.71-1.el6
Complete!
```

7. MySQL サーバを起動します。

   `[root@mcctb~]# サービス mysqld 開始日

```
Initializing MySQL database:  2016-04-05 19:44:38 0 [Warning] TIMESTAMP
with implicit DEFAULT value is deprecated. Please use
--explicit_defaults_for_timestamp server option (see documentation
for more details).
2016-04-05 19:44:38 0 [Note] /usr/sbin/mysqld (mysqld 5.6.29)
        starting as process 2487 ...
2016-04-05 19:44:38 2487 [Note] InnoDB: Using atomics to ref count
        buffer pool pages
2016-04-05 19:44:38 2487 [Note] InnoDB: The InnoDB memory heap is
disabled
....Output truncated....
2016-04-05 19:44:42 2509 [Note] InnoDB: Shutdown completed; log sequence
       number 1625987

PLEASE REMEMBER TO SET A PASSWORD FOR THE MySQL root USER!
To do so, start the server, then issue the following commands:

  /usr/bin/mysqladmin -u root password 'new-password'
  /usr/bin/mysqladmin -u root -h mcctb password 'new-password'

Alternatively, you can run:
  /usr/bin/mysql_secure_installation

which will also give you the option of removing the test
databases and anonymous user created by default.  This is
strongly recommended for production servers.
.....Output truncated.....
WARNING: Default config file /etc/my.cnf exists on the system
This file will be read by default by the MySQL server
If you do not want to use this, either remove it, or use the
--defaults-file argument to mysqld_safe when starting the server

                                                           [  OK  ]
Starting mysqld:                                           [  OK  ]
```

8. MySQL サーバが実行されていることを確認します。

   `[root@mcctb~]# サービス mysqld ステータス

```
mysqld (pid  2739) is running...
```

9. セキュリティとパスワードを設定します。

   `[root@mcctb~]#mysql_secure_install`

```
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MySQL
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!

 In order to log into MySQL to secure it, we'll need the current
 password for the root user.  If you've just installed MySQL, and
 you haven't set the root password yet, the password will be blank,
 so you should just press enter here.

 Enter current password for root (enter for none):   <== on default
install
                                                        hit enter here
 OK, successfully used password, moving on...

 Setting the root password ensures that nobody can log into the MySQL
 root user without the proper authorization.

 Set root password? [Y/n] y
 New password:
 Re-enter new password:
 Password updated successfully!
 Reloading privilege tables..
  ... Success!

 By default, a MySQL installation has an anonymous user, allowing anyone
 to log into MySQL without having to have a user account created for
 them.  This is intended only for testing, and to make the installation
 go a bit smoother.  You should remove them before moving into a
 production environment.

 Remove anonymous users? [Y/n] y
  ... Success!

 Normally, root should only be allowed to connect from 'localhost'.
This
 ensures that someone cannot guess at the root password from the
network.

 Disallow root login remotely? [Y/n] y
  ... Success!

 By default, MySQL comes with a database named 'test' that anyone can
 access.  This is also intended only for testing, and should be removed
 before moving into a production environment.

 Remove test database and access to it? [Y/n] y
  - Dropping test database...
 ERROR 1008 (HY000) at line 1: Can't drop database 'test';
```

```
database doesn't exist
 ... Failed!  Not critical, keep moving...
 - Removing privileges on test database...
 ... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n] y
 ... Success!

All done!  If you've completed all of the above steps, your MySQL
installation should now be secure.

Thanks for using MySQL!

Cleaning up...
```

10. MySQL ログインが機能していることを確認します。

「 [root@mcctb~]#mysql-u root – p`

```
Enter password: <configured_password>
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 17
Server version: 5.6.29 MySQL Community Server (GPL)

Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights
reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input
statement.
mysql>
```

MySQL ログインが動作している場合、出力は「 MySQL>` 」プロンプトで終了します。

MySQLの自動起動設定を有効にする

MySQLデーモンに対して自動起動機能が有効になっていることを確認する必要があります。MySQL デーモンを有効にすると、 MetroCluster Tiebreaker ソフトウェアがインストールされているシステムがリブートした場合に MySQL が自動的に再起動されます。MySQL デーモンが実行されていない場合、 Tiebreaker ソフトウェアは引き続き実行されますが、再起動したり設定を変更したりすることはできません。

ステップ

1. MySQL がブート時に自動で起動することが有効になっていることを確認します

   「 [root@mcctb~]# systemctl list-buny-files mysqld.service` 」と入力します

```
UNIT FILE           State
------------------- ----------
mysqld.service      enabled
```

   ブート時に MySQL を自動で起動することが有効になっていない場合は、 MySQL のドキュメントを参照して、自動起動機能を有効にしてください。

Red Hat Enterprise Linux 8へのMariaDBサーバのインストール

Tiebreaker ソフトウェアをインストールまたはアップグレードする前に、ホストシステムに MariaDB サーバをインストールする必要があります。Red Hat Enterprise Linux 7またはCentOS 7の場合： MySQL Serverのインストール。

作業を開始する前に

ホストシステムが Red Hat Enterprise Linux （ RHEL ） 8 で実行されている必要があります。

手順

1. としてログインします `root` ユーザまたはadvanced権限モードでsudoを実行できるユーザ。

```
login as: root
root@mcctb's password:
Last login: Fri Jan  8 21:33:00 2017 from host.domain.com
```

2. MariaDBサーバをインストールします。

   `[root@mcctb~]#yum は MariaDB -server.x86_64 をインストールします

```
[root@mcctb ~]# yum install mariadb-server.x86_64
Loaded plugins: fastestmirror, langpacks
 ...
 ...

================================================================================
===
 Package                      Arch    Version          Repository
Size
================================================================================
===
Installing:
mariadb-server               x86_64   1:5.5.56-2.el7   base
```

```
11 M
Installing for dependencies:

Transaction Summary
================================================================================
===
Install  1 Package  (+8 Dependent packages)
Upgrade             ( 1 Dependent package)

Total download size: 22 M
Is this ok [y/d/N]: y

Downloading packages:
No Presto metadata available for base warning:
/var/cache/yum/x86_64/7/base/packages/mariadb-libs-5.5.56-
2.el7.x86_64.rpm:
Header V3 RSA/SHA256 Signature,
key ID f4a80eb5: NOKEY] 1.4 MB/s | 3.3 MB  00:00:13 ETA
Public key for mariadb-libs-5.5.56-2.el7.x86_64.rpm is not installed
(1/10): mariadb-libs-5.5.56-2.el7.x86_64.rpm  | 757 kB  00:00:01
..
..
(10/10): perl-Net-Daemon-0.48-5.el7.noarch.rpm|  51 kB  00:00:01
--------------------------------------------------------------------------------
-----------------
Installed:
  mariadb-server.x86_64 1:5.5.56-2.el7

Dependency Installed:
mariadb.x86_64 1:5.5.56-2.el7
perl-Compress-Raw-Bzip2.x86_64 0:2.061-3.el7
perl-Compress-Raw-Zlib.x86_64 1:2.061-4.el7
perl-DBD-MySQL.x86_64 0:4.023-5.el7
perl-DBI.x86_64 0:1.627-4.el7
perl-IO-Compress.noarch 0:2.061-2.el7
perl-Net-Daemon.noarch 0:0.48-5.el7
perl-PlRPC.noarch 0:0.2020-14.el7

Dependency Updated:
  mariadb-libs.x86_64 1:5.5.56-2.el7
Complete!
```

3. MariaDB サーバを起動します。

「[root@mcctb~]# systemctl start MariaDB」

4. MariaDBサーバが起動したことを確認します。

「[root@mcctb~]# systemctl status MariaDB」

```
[root@mcctb ~]# systemctl status mariadb
mariadb.service - MariaDB database server
...
Nov 08 21:28:59 mcctb systemd[1]: Starting MariaDB database server...
...
Nov 08 21:29:01 mcctb systemd[1]: Started MariaDB database server.
```

5. セキュリティとパスワードを設定します。

rootパスワードの入力を求められたら、空のままEnterキーを押してセキュリティとパスワードの設定を続行します。

[root@mcctb~]#mysql_secure_install

```
root@localhost systemd]# mysql_secure_installation

 NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user.  If you've just installed MariaDB, and
you haven't set the root password yet, the password will be blank,
so you should just press enter here.

Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password ensures that nobody can log into the MariaDB
root user without the proper authorisation.

Set root password? [Y/n] y
New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables..
 ... Success!


By default, a MariaDB installation has an anonymous user, allowing
anyone
to log into MariaDB without having to have a user account created for
```

```
them.  This is intended only for testing, and to make the installation
go a bit smoother.  You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] y
 ... Success!

Normally, root should only be allowed to connect from 'localhost'.  This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] y
 ... Success!

By default, MariaDB comes with a database named 'test' that anyone can
access.  This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] y
 - Dropping test database...
  ... Success!
 - Removing privileges on test database...
   ... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n]

 ... Success!

Cleaning up...

All done!  If you've completed all of the above steps, your MariaDB
installation should now be secure.

Thanks for using MariaDB!
```

MariaDBサーバの自動起動設定を有効にする

MariaDBサーバで自動起動機能がオンになっていることを確認する必要があります。自動起動機能を有効にしておらず、 MetroCluster Tiebreaker ソフトウェアがインストールされているシステムをリブートする必要がある場合、 Tiebreaker ソフトウェアは引き続き実行されますが、 MariaDB サービスを再起動できず、設定を変更できません。

手順

1. 自動起動サービスを有効にします。

「 [root@mcctb~]# systemctl enable mariadb.service` 」を参照してください

2. ブート時に MariaDB が自動で起動できることを確認します。

「 [root@mcctb~]# systemctl list-buny-files mariadb.service` 」と入力します

```
UNIT FILE           State
------------------- ----------
mariadb.service     enabled
```

Tiebreaker 1.5のインストールまたはアップグレード

MetroCluster構成を監視するには、ホストLinuxオペレーティングシステムでTiebreaker 1.5の新規インストールまたはアップグレードを実行します。

このタスクについて

- サポートされているバージョンのONTAPがストレージシステムで実行されている必要があります。を参照してください "ソフトウェア要件" 詳細については、表を参照してください。
- を使用してOpenJDKをインストールしておく必要があります `yum install java-x.x.x-openjdk` コマンドを実行しますTiebreaker 1.5以降では、OpenJDK 17、18、または19がサポートされます。
- MetroCluster Tiebreakerは、Tiebreakerのインストール、テーブルとユーザの作成、ユーザパスワードの設定に必要な管理権限を持つroot以外のユーザとしてインストールできます。

手順

1. MetroCluster TiebreakerソフトウェアとMetroCluster_Tiebreaker_RPM_GPGキーをダウンロードします。

MetroCluster_Tiebreaker_RPM_GPGキーは、Tiebreaker 1.5のソフトウェアパッケージをNetApp Support Siteからダウンロードするときと同じページからダウンロードできます。

"MetroCluster Tiebreaker（ダウンロード）- NetApp Support Site"

2. root ユーザとしてホストにログインします。
3. root以外のユーザを作成し、 `mcctbgrp` グループ：

a. root以外のユーザを作成し、パスワードを設定します。

次の例は、という名前のroot以外のユーザを作成します。 `mcctbuser1` ：

```
[root@mcctb ~]# useradd mcctbuser1
[root@mcctb ~]# passwd mcctbuser1
Changing password for user mcctbuser1.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

b. という名前のグループを作成します。 `mcctbgrp`：

```
[root@mcctb ~~]# groupadd mcctbgrp
```

c. 作成したroot以外のユーザをに追加します。 `mcctbgrp` グループ：

次のコマンドでは、 `mcctbuser1` に移動します `mcctbgrp` グループ：

```
[root@mcctb ~]# usermod -a -G mcctbgrp mcctbuser1
```

4. RPMファイルを確認します。

RPMキーが格納されているディレクトリから、次の手順を実行します。

a. RPMキーファイルをダウンロードしてインポートします。

```
[root@mcctb ~]# rpm --import MetroCluster_Tiebreaker_RPM_GPG.key
```

b. フィンガープリントをチェックして、正しいキーがインポートされたことを確認します。

次の例は、正しいキーフィンガープリントを示しています。

```
root@mcctb:~/signing/mcctb-rpms# gpg --show-keys --with-fingerprint
MetroCluster_Tiebreaker_RPM_GPG.key
pub   rsa3072 2022-11-17 [SCEA] [expires: 2025-11-16]
      65AC 1562 E28A 1497 7BBD  7251 2855 EB02 3E77 FAE5
uid                      MCCTB-RPM (mcctb RPM production signing)
<mcctb-rpm@netapp.com>
```

a. 署名を確認します。 `rpm --checksig NetApp-MetroCluster-Tiebreaker-Software-1.5-1.x86_64.rpm`

```
NetApp-MetroCluster-Tiebreaker-Software-1.5-1.x86_64.rpm: digests OK
```

ⓘ 署名を正常に検証してからインストールを続行する必要があります。

5. Tiebreakerソフトウェアをインストールまたはアップグレードします。

ⓘ Tiebreakerバージョン1.4からアップグレードする場合は、Tiebreakerバージョン1.5にのみアップグレードできます。以前のバージョンからTiebreaker 1.5へのアップグレードはサポートされていません。

新規インストールを実行するか、既存のインストールをアップグレードするかに応じて、正しい手順を選択します。

新規インストールを実行します

a. Javaの絶対パスを取得して記録します。

```
[root@mcctb ~]# readlink -f /usr/bin/java
/usr/lib/jvm/java-19-openjdk-19.0.0.0.36-
2.rolling.el8.x86_64/bin/java
```

b. 次のコマンドを実行します。
`rpm -ivh NetApp-MetroCluster-Tiebreaker-Software-1.5-1.x86_64.rpm`

インストールが完了すると、次の出力が表示されます。

インストール中にプロンプトが表示されたら、以前に作成してに割り当てたroot以外のユーザを指定します。 `mcctbgrp` グループ：

例

```
Verifying...
################################# [100%]
Preparing...
################################# [100%]
Updating / installing...
   1:NetApp-MetroCluster-Tiebreaker-
So################################# [100%]
Enter the absolute path for Java : /usr/lib/jvm/java-19-
openjdk-19.0.0.0.36-2.rolling.el8.x86_64/bin/java
Verifying if Java exists...
Found Java. Proceeding with the installation.
Enter host user account to use for the installation:
mcctbuser1
User account mcctbuser1 found. Proceeding with the
installation
Enter database user name:
root
Please enter database password for root
Enter password:
Sealed          false
Do you wish to auto unseal vault(y/n)?y
Enter the key1:
Enter the key2:
Enter the key3:
Success! Uploaded policy: mcctb-policy
Error enabling approle auth: Error making API request.
URL: POST http://127.0.0.1:8200/v1/sys/auth/approle
Code: 400. Errors:
* path is already in use at approle/
Success! Enabled the kv secrets engine at: mcctb/
Success! Data written to: auth/approle/role/mcctb-app
Password updated successfully in the vault.
Synchronizing state of netapp-metrocluster-tiebreaker-
software.service with SysV service script with
/usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable
netapp-metrocluster-tiebreaker-software
Created symlink /etc/systemd/system/multi-
user.target.wants/netapp-metrocluster-tiebreaker-
software.service → /etc/systemd/system/netapp-metrocluster-
tiebreaker-software.service.
Attempting to start NetApp MetroCluster Tiebreaker software
services
```

```
Started NetApp MetroCluster Tiebreaker software services
Successfully installed NetApp MetroCluster Tiebreaker software
version 1.5.
```

既存のインストールをアップグレードする

a. サポートされているバージョンのOpenJDKがインストールされていること、およびホストにある現在のJavaバージョンであることを確認します。

> Tiebreaker 1.5にアップグレードするには、OpenJDKバージョン17、18、または19をインストールする必要があります。

```
[root@mcctb ~]# readlink -f /usr/bin/java
/usr/lib/jvm/java-19-openjdk-19.0.0.0.36-
2.rolling.el8.x86_64/bin/java
```

b. Vaultサービスが封印されておらず、実行されていることを確認します。 `vault status`

```
[root@mcctb ~]# vault status
Key             Value
---             -----
Seal Type       shamir
Initialized     true
Sealed          false
Total Shares    5
Threshold       3
Version         1.12.2
Build Date      2022-11-23T12:53:46Z
Storage Type    file
Cluster Name    vault
Cluster ID      <cluster_id>
HA Enabled      false
```

c. Tiebreakerソフトウェアをアップグレードします。

```
[root@mcctb ~]# rpm -Uvh NetApp-MetroCluster-Tiebreaker-Software-
1.5-1.x86_64.rpm
```

アップグレードが完了すると、次の出力が表示されます。

例

```
Verifying...
################################# [100%]
Preparing...
################################# [100%]
Updating / installing...
   1:NetApp-MetroCluster-Tiebreaker-
So################################# [ 50%]

Enter the absolute path for Java : /usr/lib/jvm/java-19-
openjdk-19.0.0.0.36-2.rolling.el8.x86_64/bin/java
Verifying if Java exists...
Found Java. Proceeding with the installation.
Enter host user account to use for the installation:
mcctbuser1
User account mcctbuser1 found. Proceeding with the
installation
Sealed          false
Do you wish to auto unseal vault(y/n)?y
Enter the key1:
Enter the key2:
Enter the key3:
Success! Uploaded policy: mcctb-policy
Error enabling approle auth: Error making API request.
URL: POST http://127.0.0.1:8200/v1/sys/auth/approle
Code: 400. Errors:
* path is already in use at approle/
Success! Enabled the kv secrets engine at: mcctb/
Success! Data written to: auth/approle/role/mcctb-app
Enter database user name : root
Please enter database password for root
Enter password:
Password updated successfully in the database.
Password updated successfully in the vault.
Synchronizing state of netapp-metrocluster-tiebreaker-
software.service with SysV service script with
/usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable
netapp-metrocluster-tiebreaker-software
Attempting to start NetApp MetroCluster Tiebreaker software
services
Started NetApp MetroCluster Tiebreaker software services
Successfully upgraded NetApp MetroCluster Tiebreaker software
to version 1.5.
```

```
Cleaning up / removing...
   2:NetApp-MetroCluster-Tiebreaker-
So################################## [100%]
```

誤った MySQL ルートパスワードを入力すると、 Tiebreaker ソフトウェアのインストールが完了したことが通知されますが、 Access denied メッセージが表示されます。問題を解決するには 'rpm -e コマンドを使用して Tiebreaker ソフトウェアをアンインストールし ' 正しい MySQL ルート・パスワードを使用してソフトウェアを再インストールする必要があります

6. Tiebreakerホストから各ノード管理LIFおよびクラスタ管理LIFへのSSH接続を開き、MetroCluster ソフトウェアへのTiebreakerの接続を確認します。

関連情報

"ネットアップサポート"

Tiebreaker 1.4のインストール

MetroCluster Tiebreaker 1.4の依存関係のインストール

Tiebreakerソフトウェアをインストールまたはアップグレードする前に、ホストのLinuxオペレーティングシステムに応じて、MySQLサーバまたはMariaDBサーバをインストールします。

手順

1. JDKのインストール。
2. MySQL サーバまたは MariaDB サーバをインストールします。

Linux ホストの種類は、です	作業
Red Hat Enterprise Linux 7 / CentOS 7.	Red Hat Enterprise Linux 7またはCentOS 7にMySQL Server 5.5.30以降および5.6.xバージョンをインストールする
Red Hat Enterprise Linux 8	Red Hat Enterprise Linux 8へのMariaDBサーバのインストール

JDKのインストール

TiebreakerソフトウェアをインストールまたはアップグレードするTiebreakerホストシステムにJDKをインストールする必要があります。Tiebreaker 1.4以前では、JDK 1.8.0がサポートされています。（JRE 8）。

手順

1. 「root」ユーザとしてログインします。

```
login as: root
root@mcctb's password:
Last login: Fri Jan  8 21:33:00 2017 from host.domain.com
```

2. JDK 1.8.0をインストールします。

```
yum install java-1.8.0-openjdk.x86_64
```

```
[root@mcctb ~]# yum install java-1.8.0-openjdk.x86_64
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
... shortened....
Dependencies Resolved

================================================================================
Package               Arch   Version                  Repository    Size
================================================================================
Installing:
 java-1.8.0-openjdk  x86_64  1:1.8.0.144-0.b01.el7_4 updates      238 k
 ..
 ..
Transaction Summary
================================================================================
Install  1 Package  (+ 4 Dependent packages)

Total download size: 34 M
Is this ok [y/d/N]: y

Installed:
java-1.8.0-openjdk.x86_64 1:1.8.0.144-0.b01.el7_4
Complete!
```

Red Hat Enterprise Linux 7またはCentOS 7にMySQL Server 5.5.30以降および5.6.xバージョンをインストールする

Tiebreaker ソフトウェアをインストールまたはアップグレードする前に、ホストシステムに MySQL Server 5.5.30 以降および 5.6.x バージョンをインストールする必要があります。 Red Hat Enterprise Linux 8の場合は、 MariaDBサーバのインストール。

手順

1. root ユーザとしてログインします。

```
login as: root
root@mcctb's password:
Last login: Fri Jan  8 21:33:00 2016 from host.domain.com
```

2. ホストシステムに MySQL リポジトリを追加します。

```
[root@mcctb~]#yum localinstall\https://dev.mysql.com/get/mysql57-community-release-el6-11.noarch.rpm
```

```
Loaded plugins: product-id, refresh-packagekit, security, subscription-
manager
Setting up Local Package Process
Examining /var/tmp/yum-root-LLUw0r/mysql-community-release-el6-
5.noarch.rpm: mysql-community-release-el6-5.noarch
Marking /var/tmp/yum-root-LLUw0r/mysql-community-release-el6-
5.noarch.rpm to be installed
Resolving Dependencies
--> Running transaction check
---> Package mysql-community-release.noarch 0:el6-5 will be installed
--> Finished Dependency Resolution
Dependencies Resolved
================================================================================
========
Package               Arch   Version
                                      Repository
Size
================================================================================
========
Installing:
mysql-community-release
                       noarch el6-5 /mysql-community-release-el6-
5.noarch 4.3 k
Transaction Summary
================================================================================
========
Install       1 Package(s)
Total size: 4.3 k
Installed size: 4.3 k
Is this ok [y/N]: y
Downloading Packages:
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing : mysql-community-release-el6-5.noarch
1/1
  Verifying  : mysql-community-release-el6-5.noarch
1/1
Installed:
  mysql-community-release.noarch 0:el6-5
Complete!
```

3. MySQL 57リポジトリを無効にします。

```
[root@mcctb~]#yum-config -manager-disable mysql57-community
```

4. MySQL 56リポジトリを有効にします。

```
[root@mcctb~]#yum-config -manager-enable mysql56-community
```

5. リポジトリを有効にします。

```
[root@mcctb~]# yum repolist enabled | grep "mysql.-community."
```

```
mysql-connectors-community           MySQL Connectors Community
21
mysql-tools-community                MySQL Tools Community
35
mysql56-community                    MySQL 5.6 Community Server
231
```

6. MySQL Community Server をインストールします。

`[root@mcctb~]# yum は mysql-community-server をインストールします

```
Loaded plugins: product-id, refresh-packagekit, security, subscription-
manager
This system is not registered to Red Hat Subscription Management. You
can use subscription-manager
to register.
Setting up Install Process
Resolving Dependencies
--> Running transaction check
 .....Output truncated.....
---> Package mysql-community-libs-compat.x86_64 0:5.6.29-2.el6 will be
obsoleting
--> Finished Dependency Resolution
Dependencies Resolved
================================================================================
======
Package                          Arch   Version       Repository
Size
================================================================================
======
Installing:
 mysql-community-client         x86_64  5.6.29-2.el6  mysql56-community
18  M
     replacing  mysql.x86_64 5.1.71-1.el6
 mysql-community-libs           x86_64  5.6.29-2.el6  mysql56-community
1.9 M
```

```
     replacing  mysql-libs.x86_64 5.1.71-1.el6
 mysql-community-libs-compat    x86_64  5.6.29-2.el6  mysql56-community
1.6 M
     replacing  mysql-libs.x86_64 5.1.71-1.el6
 mysql-community-server         x86_64  5.6.29-2.el6  mysql56-community
53  M
     replacing  mysql-server.x86_64 5.1.71-1.el6
Installing for dependencies:
mysql-community-common          x86_64  5.6.29-2.el6  mysql56-community
308 k

Transaction Summary
================================================================================
=======
Install       5 Package(s)
Total download size: 74 M
Is this ok [y/N]: y
Downloading Packages:
(1/5): mysql-community-client-5.6.29-2.el6.x86_64.rpm       |  18 MB
00:28
(2/5): mysql-community-common-5.6.29-2.el6.x86_64.rpm       | 308 kB
00:01
(3/5): mysql-community-libs-5.6.29-2.el6.x86_64.rpm         | 1.9 MB
00:05
(4/5): mysql-community-libs-compat-5.6.29-2.el6.x86_64.rpm  | 1.6 MB
00:05
(5/5): mysql-community-server-5.6.29-2.el6.x86_64.rpm       |  53 MB
03:42
 --------------------------------------------------------------------------
--------
Total                                              289 kB/s |  74 MB
04:24
warning: rpmts_HdrFromFdno: Header V3 DSA/SHA1 Signature, key ID
<key_id> NOKEY
Retrieving key from file:/etc/pki/rpm-gpg/RPM-GPG-KEY-mysql
Importing GPG key 0x5072E1F5:
 Userid : MySQL Release Engineering <mysql-build@oss.oracle.com>
Package: mysql-community-release-el6-5.noarch
         (@/mysql-community-release-el6-5.noarch)
 From   : file:/etc/pki/rpm-gpg/RPM-GPG-KEY-mysql
Is this ok [y/N]: y
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing : mysql-community-common-5.6.29-2.el6.x86_64
```

```
....Output truncated....
1.el6.x86_64
7/8
  Verifying  : mysql-5.1.71-1.el6.x86_64
8/8
Installed:
  mysql-community-client.x86_64 0:5.6.29-2.el6
  mysql-community-libs.x86_64 0:5.6.29-2.el6
  mysql-community-libs-compat.x86_64 0:5.6.29-2.el6
  mysql-community-server.x86_64 0:5.6.29-2.el6

Dependency Installed:
  mysql-community-common.x86_64 0:5.6.29-2.el6

Replaced:
  mysql.x86_64 0:5.1.71-1.el6 mysql-libs.x86_64 0:5.1.71-1.el6
  mysql-server.x86_64 0:5.1.71-1.el6
Complete!
```

7. MySQL サーバを起動します。

   `[root@mcctb~]# サービス mysqld 開始日

```
Initializing MySQL database:  2016-04-05 19:44:38 0 [Warning] TIMESTAMP
with implicit DEFAULT value is deprecated. Please use
--explicit_defaults_for_timestamp server option (see documentation
for more details).
2016-04-05 19:44:38 0 [Note] /usr/sbin/mysqld (mysqld 5.6.29)
        starting as process 2487 ...
2016-04-05 19:44:38 2487 [Note] InnoDB: Using atomics to ref count
        buffer pool pages
2016-04-05 19:44:38 2487 [Note] InnoDB: The InnoDB memory heap is
disabled
....Output truncated....
2016-04-05 19:44:42 2509 [Note] InnoDB: Shutdown completed; log sequence
       number 1625987

PLEASE REMEMBER TO SET A PASSWORD FOR THE MySQL root USER!
To do so, start the server, then issue the following commands:

  /usr/bin/mysqladmin -u root password 'new-password'
  /usr/bin/mysqladmin -u root -h mcctb password 'new-password'

Alternatively, you can run:
  /usr/bin/mysql_secure_installation

which will also give you the option of removing the test
databases and anonymous user created by default.  This is
strongly recommended for production servers.
.....Output truncated.....
WARNING: Default config file /etc/my.cnf exists on the system
This file will be read by default by the MySQL server
If you do not want to use this, either remove it, or use the
--defaults-file argument to mysqld_safe when starting the server

                                                           [  OK  ]
Starting mysqld:                                           [  OK  ]
```

8. MySQL サーバが実行されていることを確認します。

   `[root@mcctb~]# サービス mysqld ステータス

```
mysqld (pid  2739) is running...
```

9. セキュリティとパスワードを設定します。

   `[root@mcctb~]#mysql_secure_install`

```
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MySQL
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!

 In order to log into MySQL to secure it, we'll need the current
 password for the root user.  If you've just installed MySQL, and
 you haven't set the root password yet, the password will be blank,
 so you should just press enter here.

 Enter current password for root (enter for none):   <== on default
install
                                                        hit enter here
 OK, successfully used password, moving on...

 Setting the root password ensures that nobody can log into the MySQL
 root user without the proper authorization.

 Set root password? [Y/n] y
 New password:
 Re-enter new password:
 Password updated successfully!
 Reloading privilege tables..
  ... Success!

 By default, a MySQL installation has an anonymous user, allowing anyone
 to log into MySQL without having to have a user account created for
 them.  This is intended only for testing, and to make the installation
 go a bit smoother.  You should remove them before moving into a
 production environment.

 Remove anonymous users? [Y/n] y
  ... Success!

 Normally, root should only be allowed to connect from 'localhost'.
This
 ensures that someone cannot guess at the root password from the
network.

 Disallow root login remotely? [Y/n] y
  ... Success!

 By default, MySQL comes with a database named 'test' that anyone can
 access.  This is also intended only for testing, and should be removed
 before moving into a production environment.

 Remove test database and access to it? [Y/n] y
  - Dropping test database...
 ERROR 1008 (HY000) at line 1: Can't drop database 'test';
```

```
database doesn't exist
 ... Failed!  Not critical, keep moving...
 - Removing privileges on test database...
 ... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n] y
 ... Success!

All done!  If you've completed all of the above steps, your MySQL
installation should now be secure.

Thanks for using MySQL!

Cleaning up...
```

10. MySQL ログインが機能していることを確認します。

「 [root@mcctb~]#mysql-u root – p`

```
Enter password: <configured_password>
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 17
Server version: 5.6.29 MySQL Community Server (GPL)

Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights
reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input
statement.
mysql>
```

MySQLログインが想定どおりに機能している場合、出力は `mysql>` プロンプト。

MySQLの自動起動設定を有効にする

MySQLデーモンに対して自動起動機能が有効になっていることを確認する必要があります。MySQL デーモンを有効にすると、 MetroCluster Tiebreaker ソフトウェアがインストールされているシステムがリブートした場合に MySQL が自動的に再起動されます。MySQL デーモンが実行されていない場合、 Tiebreaker ソフトウェアは引き続き実行されますが、再起動したり設定を変更したりすることはできません。

ステップ

1. MySQL がブート時に自動で起動することが有効になっていることを確認します

   「 [root@mcctb~]# systemctl list-buny-files mysqld.service` 」と入力します

```
UNIT FILE           State
------------------- ----------
mysqld.service      enabled
```

   ブート時に MySQL を自動で起動することが有効になっていない場合は、 MySQL のドキュメントを参照して、自動起動機能を有効にしてください。

Red Hat Enterprise Linux 8へのMariaDBサーバのインストール

Tiebreaker ソフトウェアをインストールまたはアップグレードする前に、ホストシステムに MariaDB サーバをインストールする必要があります。 Red Hat Enterprise Linux 7またはCentOS 7の場合： MySQL Serverのインストール。

作業を開始する前に

ホストシステムが Red Hat Enterprise Linux （ RHEL ） 8 で実行されている必要があります。

手順

1. としてログインします `root` ユーザ：

```
login as: root
root@mcctb's password:
Last login: Fri Jan  8 21:33:00 2017 from host.domain.com
```

2. MariaDBサーバをインストールします。

   `[root@mcctb~]#yum は MariaDB -server.x86_64 をインストールします

```
[root@mcctb ~]# yum install mariadb-server.x86_64
Loaded plugins: fastestmirror, langpacks
 ...
 ...

================================================================================
 Package                    Arch    Version         Repository
Size
================================================================================
Installing:
mariadb-server              x86_64   1:5.5.56-2.el7   base
```

```
11 M
Installing for dependencies:

Transaction Summary
================================================================================
===
Install  1 Package  (+8 Dependent packages)
Upgrade             ( 1 Dependent package)

Total download size: 22 M
Is this ok [y/d/N]: y

Downloading packages:
No Presto metadata available for base warning:
/var/cache/yum/x86_64/7/base/packages/mariadb-libs-5.5.56-
2.el7.x86_64.rpm:
Header V3 RSA/SHA256 Signature,
key ID f4a80eb5: NOKEY] 1.4 MB/s | 3.3 MB  00:00:13 ETA
Public key for mariadb-libs-5.5.56-2.el7.x86_64.rpm is not installed
(1/10): mariadb-libs-5.5.56-2.el7.x86_64.rpm  | 757 kB  00:00:01
..
..
(10/10): perl-Net-Daemon-0.48-5.el7.noarch.rpm|  51 kB  00:00:01
--------------------------------------------------------------------------------
-----------------
Installed:
  mariadb-server.x86_64 1:5.5.56-2.el7

Dependency Installed:
mariadb.x86_64 1:5.5.56-2.el7
perl-Compress-Raw-Bzip2.x86_64 0:2.061-3.el7
perl-Compress-Raw-Zlib.x86_64 1:2.061-4.el7
perl-DBD-MySQL.x86_64 0:4.023-5.el7
perl-DBI.x86_64 0:1.627-4.el7
perl-IO-Compress.noarch 0:2.061-2.el7
perl-Net-Daemon.noarch 0:0.48-5.el7
perl-PlRPC.noarch 0:0.2020-14.el7

Dependency Updated:
  mariadb-libs.x86_64 1:5.5.56-2.el7
Complete!
```

3. MariaDB サーバを起動します。

「[root@mcctb~]# systemctl start MariaDB」

4. MariaDBサーバが起動したことを確認します。

「[root@mcctb~]# systemctl status MariaDB」

```
[root@mcctb ~]# systemctl status mariadb
mariadb.service - MariaDB database server
...
Nov 08 21:28:59 mcctb systemd[1]: Starting MariaDB database server...
...
Nov 08 21:29:01 mcctb systemd[1]: Started MariaDB database server.
```

5. セキュリティとパスワードを設定します。

rootパスワードの入力を求められたら、空のままEnterキーを押してセキュリティとパスワードの設定を続行します。

[root@mcctb~]#mysql_secure_install

```
root@localhost systemd]# mysql_secure_installation

 NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user.  If you've just installed MariaDB, and
you haven't set the root password yet, the password will be blank,
so you should just press enter here.

Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password ensures that nobody can log into the MariaDB
root user without the proper authorisation.

Set root password? [Y/n] y
New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables..
 ... Success!


By default, a MariaDB installation has an anonymous user, allowing
anyone
to log into MariaDB without having to have a user account created for
```

```
them.  This is intended only for testing, and to make the installation
go a bit smoother.  You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] y
 ... Success!

Normally, root should only be allowed to connect from 'localhost'.  This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] y
 ... Success!

By default, MariaDB comes with a database named 'test' that anyone can
access.  This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] y
 - Dropping test database...
  ... Success!
 - Removing privileges on test database...
   ... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n]

  ... Success!

Cleaning up...

All done!  If you've completed all of the above steps, your MariaDB
installation should now be secure.

Thanks for using MariaDB!
```

MariaDBサーバの自動起動設定を有効にする

MariaDBサーバで自動起動機能がオンになっていることを確認する必要があります。自動起動機能を有効にしておらず、 MetroCluster Tiebreaker ソフトウェアがインストールされているシステムをリブートする必要がある場合、 Tiebreaker ソフトウェアは引き続き実行されますが、 MariaDB サービスを再起動できず、設定を変更できません。

手順

1. 自動起動サービスを有効にします。

「 [root@mcctb~]# systemctl enable mariadb.service` 」を参照してください

2. ブート時に MariaDB が自動で起動できることを確認します。

   「 [root@mcctb~]# systemctl list-buny-files mariadb.service` 」と入力します

```
UNIT FILE           State
------------------- ----------
mariadb.service     enabled
```

Tiebreaker 1.4のインストールまたはアップグレード

MetroCluster構成を監視するには、ホストLinuxオペレーティングシステムでTiebreaker 1.4の新規インストールまたはアップグレードを実行します。

このタスクについて

- サポートされているバージョンのONTAPがストレージシステムで実行されている必要があります。を参照してください "ソフトウェア要件" 詳細については、表を参照してください。
- を使用してOpenJDKをインストールしておく必要があります `yum install java-x.x.x-openjdk` コマンドを実行しますTiebreaker 1.4以前では、JDK 1.8.0（JRE 8）がサポートされます。

手順

1. MetroCluster Tiebreakerソフトウェアをダウンロードします。

   "MetroCluster Tiebreaker（ダウンロード）- NetApp Support Site"

2. root ユーザとしてホストにログインします。
3. Tiebreakerソフトウェアをインストールまたはアップグレードします。

   新規インストールを実行するか、既存のインストールをアップグレードするかに応じて、正しい手順を選択します。

新規インストールを実行します

a. を実行してTiebreakerソフトウェアをインストールします。

```
rpm -ivh NetApp-MetroCluster-Tiebreaker-Software-1.4-1.x86_64.rpm
```

インストールが完了すると、次の出力が表示されます。

```
Verifying...
################################# [100%]
Preparing...
################################# [100%]
Updating / installing...
   1:NetApp-MetroCluster-Tiebreaker-
So################################# [100%]
Post installation start Fri Apr  5 02:28:09 EDT 2024
Enter MetroCluster Tiebreaker user password:

Please enter mysql root password when prompted
Enter password:
Synchronizing state of netapp-metrocluster-tiebreaker-
software.service with SysV service script with
/usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable netapp-
metrocluster-tiebreaker-software
Created symlink /etc/systemd/system/multi-
user.target.wants/netapp-metrocluster-tiebreaker-software.service
→ /etc/systemd/system/netapp-metrocluster-tiebreaker-
software.service.
Attempting to start NetApp MetroCluster Tiebreaker software
services
Started NetApp MetroCluster Tiebreaker software services
Enabled autostart of NetApp MetroCluster Tiebreaker software
daemon during boot
Created symbolic link for NetApp MetroCluster Tiebreaker software
CLI
Post installation end Fri Apr  5 02:28:22 EDT 2024
Successfully installed NetApp MetroCluster Tiebreaker software
version 1.4.
```

既存のインストールをアップグレードする

a. Tiebreakerソフトウェアをアップグレードします。

```
[root@mcctb ~]# rpm -Uvh NetApp-MetroCluster-Tiebreaker-Software-
1.4-1.x86_64.rpm
```

アップグレードが完了すると、次の出力が表示されます。

```
Verifying...
################################# [100%]
Preparing...
################################# [100%]
Upgrading NetApp MetroCluster Tiebreaker software....
Stopping NetApp MetroCluster Tiebreaker software services before
upgrade.
Updating / installing...
   1:NetApp-MetroCluster-Tiebreaker-
So################################# [ 50%]
Post installation start Mon Apr  8 06:29:51 EDT 2024
Synchronizing state of netapp-metrocluster-tiebreaker-
software.service with SysV service script with
/usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable netapp-
metrocluster-tiebreaker-software
Attempting to start NetApp MetroCluster Tiebreaker software
services
Started NetApp MetroCluster Tiebreaker software services
Enabled autostart of NetApp MetroCluster Tiebreaker software
daemon during boot
Created symbolic link for NetApp MetroCluster Tiebreaker software
CLI
Post upgrade end Mon Apr  8 06:29:51 EDT 2024
Successfully upgraded NetApp MetroCluster Tiebreaker software to
version 1.4.
Cleaning up / removing...
   2:NetApp-MetroCluster-Tiebreaker-
So################################# [100%]
```

誤った MySQL ルートパスワードを入力すると、 Tiebreaker ソフトウェアのインストールが完了したことが通知されますが、 Access denied メッセージが表示されます。問題を解決するには 'rpm -e コマンドを使用して Tiebreaker ソフトウェアをアンインストールし ' 正しい MySQL ルート・パスワードを使用してソフトウェアを再インストールする必要があります

4. Tiebreakerホストから各ノード管理LIFおよびクラスタ管理LIFへのSSH接続を開き、MetroCluster ソフトウェアへのTiebreakerの接続を確認します。

関連情報

"ネットアップサポート"

Tiebreakerモニタが実行されているホストをアップグレードする

Tiebreakerモニタを実行しているホストのアップグレードが必要になる場合があります。

手順

1. Tiebreakerソフトウェアをアンインストールします。

   ```
   rpm -e NetApp-MetroCluster-Tiebreaker-Software
   ```

2. ホストをアップグレードします。詳細については、ホストOSのドキュメントを参照してください。
3. Tiebreakerソフトウェアを再インストールします。

   の手順に従ってTiebreakerの新規インストールを実行します。 "Tiebreaker ソフトウェアをインストールします"。

MetroCluster Tiebreakerソフトウェアを構成する

Tiebreaker ソフトウェアをインストールしたら、 MetroCluster 構成を追加または変更したり、 Tiebreaker ソフトウェアから削除したりできます。

Tiebreakerソフトウェア**CLI**を起動する

Tiebreakerソフトウェアをインストールしたら、CLIを起動してソフトウェアを設定する必要があります。

1. ソフトウェアをインストールしたホストのプロンプトから CLI を起動します。

   NetApp-metrocluster-Tiebreaker software-cli

2. インストール後および最初の起動時に、データベースにアクセスするためのTiebreakerユーザのパスワードを入力します。これは、インストール時にデータベースユーザに指定したパスワードです。

MetroCluster 構成を追加

NetApp MetroCluster Tiebreaker ソフトウェアをインストールしたら、 MetroCluster 構成を 1 つずつ追加できます。

このタスクについて

- ONTAP 環境に MetroCluster 構成をインストールし、ソフトウェアで設定を有効にしておく必要があります。
- 手順と予想されるコマンド出力は、実行している Tiebreaker のバージョンによって異なります。

タイブレーカー **1.5** 以前

手順

1. Tiebreaker コマンドラインインターフェイス（ CLI ）の monitor add コマンドを使用して、 MetroCluster の設定を追加します。

   ホスト名を使用する場合は、完全修飾ドメイン名（ FQDN ）を指定する必要があります。

   次の例は、 cluster_A の構成を示しています。

   例

   ```
   NetApp MetroCluster Tiebreaker :> monitor add wizard
   Enter monitor Name: <monitor_name>
   Enter Cluster IP Address: <cluster_ip_value>
   Enter Cluster Username: admin
   Enter Cluster Password:
   Enter Cluster IP Address: <peer_cluster_ip_value>
   Enter Peer Cluster Username: admin
   Enter Peer Cluster Password:
   Successfully added monitor to NetApp MetroCluster Tiebreaker
   software.
   ```

2. Tiebreaker CLI の monitor show-status コマンドを使用して、 MetroCluster 構成が正しく追加されたことを確認します。

   ```
   NetApp MetroCluster Tiebreaker :> monitor show -status
   ```

3. Tiebreaker ソフトウェアのオブザーバーモードを無効にして、サイト障害を検出したあとにスイッチオーバーを自動的に開始するようにします。

   `monitor modify -monitor-name <monitor_name> -observer-mode false`

   ```
   NetApp MetroCluster Tiebreaker :> monitor modify -monitor-name 8pack
   -observer-mode false
   Warning: If you are turning observer-mode to false, make sure to
   review the 'risks and limitations'
   as described in the MetroCluster Tiebreaker installation and
   configuration.
   Are you sure you want to enable automatic switchover capability for
   monitor "8pack"? [Y/N]: y
   ```

Tiebreaker 1.6以降

手順

1. Tiebreaker コマンドラインインターフェイス（ CLI ）の monitor add コマンドを使用して、MetroCluster の設定を追加します。

   ホスト名を使用する場合は、完全修飾ドメイン名（ FQDN ）を指定する必要があります。

   次の例は、 cluster_A の構成を示しています。

例

```
NetApp MetroCluster Tiebreaker :> monitor add wizard
Enter Monitor Name: cluster_A
Enter Cluster IP Address: <cluster_ip_value>
Enter Cluster Username: admin
Enter Cluster Password:
Enter Peer Cluster IP Address: <peer_cluster_ip_value>
Enter Peer Cluster Username: admin
Enter Peer Cluster Password:

 NOTE: Before enabling automatic switchover capability, make
sure to review the 'risks and limitations' as described in the
MetroCluster Tiebreaker Installation and Configuration Guide.

Do you want to enable automatic switchover capability for
monitor(Y/N): y
Successfully added monitor to NetApp MetroCluster Tiebreaker
software.
Verifying SSL certificate chain from cluster_A...

================================================
Warning missing SSL certificates
================================================

Cluster: cluster_A

IP Address: <cluster_ip_value>

Result:

The MetroCluster Tiebreaker is unable to verify the SSL
certificate chain.

Recommended Actions:

Run the following command to identify missing certificates:

monitor switchover-simulate

Import any missing certificates as indicated by the command
output.

For detailed instructions, please refer to the MetroCluster
Tiebreaker documentation, or contact NetApp Support for
assistance.
```

```
Note:

Missing certificates will prevent the MetroCluster Tiebreaker
from issuing a switchover request in the event of a site
failure.

================================================================
================================================================
Verifying SSL certificate chain from cluster_B...

SSL certificate chain is valid
```

2. Tiebreaker CLI の monitor show-status コマンドを使用して、 MetroCluster 構成が正しく追加されたことを確認します。

```
NetApp MetroCluster Tiebreaker :> monitor show -status
```

3. 不足している証明書を、Tiebreakerのバージョンに応じた手順でインポートします。証明書をインポートする 。

関連情報

"MetroCluster Tiebreaker をアクティブモードで使用する場合のリスクと制限事項"

証明書をインポートする

Tiebreaker 1.6 以降でシームレスな監視を有効にするには、サーバの Secure Sockets Layer (SSL) 証明書、中間証明書 (存在する場合)、およびルート証明書をONTAPから Java 仮想マシン (JVM) のキー ストアにインポートする必要があります。

このタスクについて

- このタスクは、Tiebreaker 1.6 以降で必須です。
- このタスクは、 MetroCluster構成を Tiebreaker に正常に追加した後、または証明書の有効期限が切れた後に実行します。
- Tiebreaker 1.7 以降では、スイッチオーバー シミュレーションを実行して、証明書をインポートする必要があるかどうかを確認できます。スイッチオーバー シミュレーションが失敗した場合は、 ONTAPから Java 仮想マシン (JVM) のキー ストアに証明書をインポートする必要があります。

タイブレーカー **1.7** 以降

手順

1. 切り替えシミュレーションを実行して、証明書をインポートする必要があるかどうかを確認します。

   a. タイブレーカーの監視ステータスを確認します。
   ```
   monitor show -status
   ```

例

```
NetApp MetroCluster Tiebreaker :> monitor show -status
MetroCluster: A700
    Disaster: false
    Monitor State: Normal
    Observer Mode: false
    Silent Period: 5
    Override Vetoes: false
    Cluster: ClusterA_siteA(UUID:713e5ab2-b4e8-11f0-91aa-
00a098ef36a2)
        Reachable: true
        Intersite Connectivity Available: true
            Node: node_A1(UUID:9f6cecbf-b4e4-11f0-9d0f-
00a098ef36a2)
                Reachable: true
                Intersite Connectivity Available: true
                State: normal
            Node: node_A2(UUID:2719bb56-b4e7-11f0-996c-
00a09897caa3)
                Reachable: true
                Intersite Connectivity Available: true
                State: normal
    Cluster: ClusterB_siteB(UUID:72839591-b4e8-11f0-b688-
00a09897cb73)
        Reachable: true
        Intersite Connectivity Available: true
            Node: node_B1(UUID:abfeab89-b4e4-11f0-a077-
00a09897cb73)
                Reachable: true
                Intersite Connectivity Available: true
                State: normal
            Node: node_B2(UUID:31e395bf-b4e7-11f0-bf99-
00a09897cb2f)
                Reachable: true
                Intersite Connectivity Available: true
                State: normal
```

b. 切り替えシミュレーションをトリガーします。

```
monitor switchover-simulate -monitor-name <monitor_name> -cluster
<cluster_name>
```

JVM に証明書をインポートする必要がある場合、コマンドは次の出力を返します。

```
Failed to trigger Switchover Simulation. Please check Metrocluster
Tiebreaker logs for further information or contact NetApp support.
```

2. インポートする必要がある証明書 (SSL サーバー、中間、またはルート) ごとに次のコマンドを実行します。

   ```
   /opt/netapp/java/bin/keytool -import -trustcacerts -file
   <certificate_file_name> -keystore "/opt/netapp/java/lib/security/cacerts"
   -alias <certificate>
   ```

   - その `<certificate_file_name>` 値には、インポートする証明書のファイル名を指定します。
   - その `-alias <certificate>` 値は、証明書を JVM にインポートした後に証明書を保存する名前を指定します。

     次の例は、ファイル名のルート証明書をインポートする方法を示しています。 `root.crt` ファイル名のSSLサーバー証明書 `ssl_cert.crt`:

     ```
     /opt/netapp/java/bin/keytool -import -trustcacerts -file root.crt
     -keystore "/opt/netapp/java/lib/security/cacerts" -alias root

     /opt/netapp/java/bin/keytool -import -trustcacerts -file
     ssl_cert.crt -keystore "/opt/netapp/java/lib/security/cacerts"
     -alias ssl_cert
     ```

3. Tiebreaker ソフトウェアを再起動します。

   ```
   systemctl restart netapp-metrocluster-tiebreaker-software
   ```

4. 切り替えシミュレーション チェックを再度実行します。

   a. タイブレーカーの監視ステータスを確認します。
      `monitor show -status`

例

```
NetApp MetroCluster Tiebreaker :> monitor show -status
MetroCluster: A700
    Disaster: false
    Monitor State: Normal
    Observer Mode: false
    Silent Period: 5
    Override Vetoes: false
    Cluster: ClusterA_siteA(UUID:713e5ab2-b4e8-11f0-91aa-
00a098ef36a2)
        Reachable: true
        Intersite Connectivity Available: true
            Node: node_A1(UUID:9f6cecbf-b4e4-11f0-9d0f-
00a098ef36a2)
                Reachable: true
                Intersite Connectivity Available: true
                State: normal
            Node: node_A2(UUID:2719bb56-b4e7-11f0-996c-
00a09897caa3)
                Reachable: true
                Intersite Connectivity Available: true
                State: normal
    Cluster: ClusterB_siteB(UUID:72839591-b4e8-11f0-b688-
00a09897cb73)
        Reachable: true
        Intersite Connectivity Available: true
            Node: node_B1(UUID:abfeab89-b4e4-11f0-a077-
00a09897cb73)
                Reachable: true
                Intersite Connectivity Available: true
                State: normal
            Node: node_B2(UUID:31e395bf-b4e7-11f0-bf99-
00a09897cb2f)
                Reachable: true
                Intersite Connectivity Available: true
                State: normal
```

b. 切り替えシミュレーションをトリガーします。

```
monitor switchover-simulate -monitor-name <monitor_name> -cluster
<cluster_name>
```

```
Successfully triggered Switchover Simulation. Please check the
status of the Switchover Simulation on the ONTAP cluster using
command "metrocluster operation history show"
```

タイブレーカー **1.6** または **1.6P1**

手順

1. ONTAPからすべての証明書をインポートします。インポートする必要がある証明書 (SSL サーバー、中間、またはルート) ごとに次のコマンドを実行します。

   ```
   /opt/netapp/java/bin/keytool -import -trustcacerts -file
   <certificate_file_name> -keystore "/opt/netapp/java/lib/security/cacerts"
   -alias <certificate>
   ```

   - その `<certificate_file_name>` 値には、インポートする証明書のファイル名を指定します。
   - その `-alias <certificate>` 値は、証明書を JVM にインポートした後に証明書を保存する名前を指定します。

     次の例は、ファイル名のルート証明書をインポートする方法を示しています。 `root.crt` ファイル名のSSLサーバー証明書 `ssl_cert.crt`:

   ```
   /opt/netapp/java/bin/keytool -import -trustcacerts -file root.crt
   -keystore "/opt/netapp/java/lib/security/cacerts" -alias root

   /opt/netapp/java/bin/keytool -import -trustcacerts -file
   ssl_cert.crt -keystore "/opt/netapp/java/lib/security/cacerts"
   -alias ssl_cert
   ```

2. Tiebreaker ソフトウェアを再起動します。

   ```
   systemctl restart netapp-metrocluster-tiebreaker-software
   ```

MetroCluster Tiebreaker 構成を変更するためのコマンド

MetroCluster 設定は、必要に応じていつでも変更できます。

Tiebreaker CLI の monitor modify コマンドは、次のいずれかのオプションで使用できます。変更を確認するには、 monitor show-status コマンドを使用します。

オプション	説明
-monitor-name を指定します	MetroCluster 設定の名前
-enable-monitor	MetroCluster 設定の監視を有効または無効にします

• サイレント - 期間	MetroCluster Tiebreaker ソフトウェアが検出後にサイト障害の確認を待機する秒数
• オブザーバーモード	オブザーバーモード（ true ）は監視するだけで、サイト障害が発生してもスイッチオーバーをトリガーしません。オンラインモード（ false ）は、サイト障害が発生した場合にスイッチオーバーをトリガーします。 • "Tiebreaker ソフトウェアでサイト障害を検出する方法" • "MetroCluster Tiebreaker をアクティブモードで使用する場合のリスクと制限事項"

次の例は、構成のサイレント期間を変更します。

```
NetApp MetroCluster Tiebreaker :> monitor modify -monitor-name cluster_A
-silent-period 15
Successfully modified monitor in NetApp MetroCluster Tiebreaker
software.
```

Tiebreaker CLI の debug コマンドを使用して、ロギングモードを変更できます。

コマンドを実行します	説明
デバッグステータス	デバッグモードのステータスを表示します
デバッグイネーブル	ロギングのデバッグモードをイネーブルにします
デバッグを無効にします	ロギングのデバッグモードをディセーブルにします

Tiebreaker 1.4以前を実行しているシステムではTiebreaker CLIです `update-mcctb-password` コマンドを使用すると、ユーザパスワードを更新できます。このコマンドはTiebreaker 1.5以降では廃止されています。

コマンドを実行します	説明
update-mccb-password	ユーザパスワードが更新されました

MetroCluster 構成を削除

MetroCluster 構成を監視する必要がなくなった場合は、 Tiebreaker ソフトウェアで監視している MetroCluster 設定を削除できます。

1. MetroCluster 構成を削除するには 'Tiebreaker CLI の monitor remove コマンドを使用します

   次の例では ' "cluster_a" がソフトウェアから削除されています

```
NetApp MetroCluster Tiebreaker :> monitor remove -monitor-name cluster_A
Successfully removed monitor from NetApp MetroCluster Tiebreaker
software.
```

2. Tiebreaker CLI の「 monitor show-status 」コマンドを使用して、 MetroCluster 設定が正しく削除されたことを確認します。

```
NetApp MetroCluster Tiebreaker :> monitor show -status
```

Tiebreaker ソフトウェアの SNMP 設定

TiebreakerソフトウェアでSNMPを使用するには、SNMPを設定する必要があります。

このタスクについて

- Tiebreaker 1.6ではSNMPv3のみがサポートされます。
- Tiebreaker 1.5および1.4ではSNMPv1とSNMPv3がサポートされますが、NetAppではセキュリティを最適化するためにSNMPv3を設定することを強く推奨します。

手順

1. Tiebreaker CLIを使用します `snmp config wizard` コマンドを使用してMetroCluster 構成を追加します。

   現在サポートされている SNMP トラップホストは 1 つだけです。

```
`snmp config wizard`コマンドの応答は、実行している
Tiebreakerのバージョンによって異なります。
```

Tiebreaker 1.6

次に、IPアドレスが192.0.2.255で、トラップメッセージ用のポート番号が162のSNMPv3をサポートするSNMPレシーバの設定例を示します。これで、Tiebreakerソフトウェアは、指定したSNMPレシーバにトラップを送信する準備が整いました。

Tiebreaker 1.6はSNMPv3のみをサポート

```
NetApp MetroCluster Tiebreaker :> snmp config wizard
Enter SNMP Host: 192.0.2.255
Enter SNMP Port: 162
Enter SNMP V3 Security Name: v3sec
Enter SNMP V3 Authentication password:
```

Tiebreaker 1.5および**1.4**

次に、IPアドレスが192.0.2.255で、トラップメッセージ用のポート番号が162のSNMPv3をサポートするSNMPレシーバの設定例を示します。これで、Tiebreakerソフトウェアは、指定したSNMPレシーバにトラップを送信する準備が整いました。

```
NetApp MetroCluster Tiebreaker :> snmp config wizard
Enter SNMP Version[V1/V3]: v3
Enter SNMP Host: 192.0.2.255
Enter SNMP Port: 162
Enter SNMP V3 Security Name: v3sec
Enter SNMP V3 Authentication password:
Enter SNMP V3 Privacy password:
Engine ID : 8000031504932eff571825192a6f1193b265e24593
Successfully added SNMP properties to NetApp MetroCluster Tiebreaker
software.
```

SNMPv1はセキュアではないため、SNMPv3を設定する必要があります。デフォルトのコミュニティストリングが* NOT * PUBLICに設定されていることを確認します。

2. SNMP が設定されたことを確認します。

   「 snmp config test 」

   次の例は、 Tiebreaker ソフトウェアがイベント test_snmp_config の SNMP トラップを送信できることを示しています。

```
NetApp MetroCluster Tiebreaker :> snmp config test
Sending SNMP trap to localhost. Version : V3.
Successfully sent SNMP trap for event TEST_SNMP_CONFIG
NetApp MetroCluster Tiebreaker :>
```

MetroCluster 設定を監視する

MetroCluster Tiebreaker ソフトウェアはリカバリプロセスを自動化します。ユーザは MetroCluster 設定のステータスを監視し、ネットアップカスタマーサポートに送信される SNMP イベントとトラップを評価し、監視処理のステータスを表示できます。

AutoSupport を設定しています

デフォルトでは、 AutoSupport メッセージは Tiebreaker ソフトウェアをインストールしてから 1 週間後にネットアップに送信されます。AutoSupport 通知をトリガーするイベントには、 Tiebreaker ソフトウェアのパニック状態、 MetroCluster 構成での災害状況の検出、 MetroCluster 構成の不明なステータスなどがあります。

作業を開始する前に

AutoSupport メッセージを設定するための直接アクセスが必要です。

手順

1. Tiebreaker CLI の AutoSupport コマンドで、次のオプションを指定します。

オプション	説明
• 呼び出します	AutoSupport メッセージをカスタマーサポートに送信します
• ウィザードを設定します	プロキシサーバのクレデンシャルを設定するウィザード
• 設定を削除します	プロキシサーバのクレデンシャルを削除します
— 有効にします	AutoSupport 通知を有効にします（デフォルト）。
• 無効にします	AutoSupport 通知を無効にします
• 表示	AutoSupport のステータスを表示します

次の例は、 AutoSupport が有効または無効で、 AutoSupport コンテンツの投稿先を示しています。

```
NetApp MetroCluster Tiebreaker :> autosupport enable
AutoSupport already enabled.

NetApp MetroCluster Tiebreaker :> autosupport disable
AutoSupport status            : disabled
Proxy Server IP Address       : 10.234.168.79
Proxy Server Port Number      : 8090
Proxy Server Username         : admin
AutoSupport destination       :
https://support.netapp.com/asupprod/post/1.0/postAsup

NetApp MetroCluster Tiebreaker :> autosupport enable
AutoSupport status            : enabled
Proxy Server IP Address       : 10.234.168.79
Proxy Server Port Number      : 8090
Proxy Server Username         : admin
AutoSupport destination       :
https://support.netapp.com/asupprod/post/1.0/postAsup

NetApp MetroCluster Tiebreaker :> autosupport invoke
AutoSupport transmission      : success
Proxy Server IP Address       : 10.234.168.79
Proxy Server Port Number      : 8090
Proxy Server Username         : admin
AutoSupport destination       :
https://support.netapp.com/asupprod/post/1.0/postAsup
```

次の例は、 IP アドレスとポート番号を使用して、認証されたプロキシサーバを使用して AutoSupport を設定する方法を示しています。

```
NetApp MetroCluster Tiebreaker :> autosupport configure wizard
Enter Proxy Server IP address :  10.234.168.79
Enter Proxy Server port number :  8090
Enter Proxy Server Username :  admin
Enter Proxy Server Password : 123abc
Autosupport configuration updated successfully.
```

次に、 AutoSupport 構成を削除する例を示します。

```
NetApp MetroCluster Tiebreaker :> autosupport delete configuration
Autosupport configuration deleted successfully.
```

SNMP イベントとトラップ

NetApp MetroCluster Tiebreaker ソフトウェアは、 SNMP トラップを使用して重大なイベントをユーザに通知します。これらのトラップは NetApp MIB ファイルに含まれています。各トラップには、トラップ名、重大度、影響レベル、タイムスタンプ、およびメッセージに関する情報が含まれています。

イベント名	イベントの詳細	トラップ番号
MetroCluster Tie-Breaker が MetroCluster 構成に到達できません	ソフトウェアが災害を検出できないことを管理者に警告します。このイベントは、両方のクラスタに到達できない場合に発生します。	25000
MetroCluster Tie-Breaker がクラスタに到達できません	ソフトウェアがいずれかのクラスタに到達できないことを管理者に警告します。	25001
MetroCluster Tie-Breaker がクラスタで災害を検出しました	ソフトウェアがサイト障害を検出したことを管理者に通知します。通知が配信されます。	25002
パートナークラスタ間のすべてのリンクは切断されています。	両方のクラスタに到達可能であることがソフトウェアによって検出されましたが、 2 つのクラスタ間のすべてのネットワークパスが停止しており、クラスタが相互に通信できません。	25005
SNMP テストトラップ	snmp config test コマンドを実行して、 SNMP 設定をテストできるようになりました。	25006

監視処理のステータスを表示する

MetroCluster 構成の監視処理の全体的なステータスを表示できます。

ステップ

1. Tiebreaker CLI の monitor show コマンドを使用して、次のいずれかのオプションを指定して MetroCluster 処理のステータスを表示します。

オプション	説明
-monitor-name を指定します	指定したモニタ名のステータスを表示します
-operation-history のコマンドを実行します	クラスタで最後に実行された監視処理を 10 件まで表示します
• 統計情報	指定したクラスタに関連する統計を表示します
ステータス	指定したクラスタのステータスを表示します。 * MetroCluster Tiebreaker ソフトウェアは、アグリゲートの修復、ルートの修復、スイッチバックなどの処理の完了ステータスが反映されるまでに最大 10 分かかる場合があります。

次の例は、クラスタ cluster_A と cluster_B が接続され、健全な状態であることを示しています。

```
NetApp MetroCluster Tiebreaker:> monitor show -status
MetroCluster: cluster_A
    Disaster: false
    Monitor State: Normal
    Observer Mode: true
    Silent Period: 15
    Override Vetoes: false
    Cluster: cluster_Ba(UUID:4d9ccf24-080f-11e4-9df2-00a098168e7c)
        Reachable: true
        All-Links-Severed: FALSE
            Node: mcc5-a1(UUID:78b44707-0809-11e4-9be1-e50dab9e83e1)
                Reachable: true
                All-Links-Severed: FALSE
                State: normal
            Node: mcc5-a2(UUID:9a8b1059-0809-11e4-9f5e-8d97cdec7102)
                Reachable: true
                All-Links-Severed: FALSE
                State: normal
    Cluster: cluster_B(UUID:70dacd3b-0823-11e4-a7b9-00a0981693c4)
        Reachable: true
        All-Links-Severed: FALSE
            Node: mcc5-b1(UUID:961fce7d-081d-11e4-9ebf-2f295df8fcb3)
                Reachable: true
                All-Links-Severed: FALSE
                State: normal
            Node: mcc5-b2(UUID:9393262d-081d-11e4-80d5-6b30884058dc)
                Reachable: true
                All-Links-Severed: FALSE
                State: normal
```

次の例では、 cluster_B で実行された最後の 7 つの処理が表示されています。

```
NetApp MetroCluster Tiebreaker:> monitor show -operation-history
MetroCluster: cluster_B
 [ 2014-09-15 04:48:32.274 ] MetroCluster Monitor is initialized
 [ 2014-09-15 04:48:32.278 ] Started Discovery and validation of
MetroCluster Setup
 [ 2014-09-15 04:48:35.078 ] Discovery and validation of MetroCluster
Setup succeeded. Started monitoring.
 [ 2014-09-15 04:48:35.246 ] NetApp MetroCluster Tiebreaker software is
able to reach cluster "mcc5a"
 [ 2014-09-15 04:48:35.256 ] NetApp MetroCluster Tiebreaker software is
able to reach cluster "mcc5b"
 [ 2014-09-15 04:48:35.298 ] Link to remote DR cluster is up for cluster
"mcc5a"
 [ 2014-09-15 04:48:35.308 ] Link to remote DR cluster is up for cluster
"mcc5b"
```

MetroCluster の設定情報を表示する

Tiebreaker ソフトウェアでは、 MetroCluster 構成のすべてのインスタンスのモニタ名と IP アドレスを表示できます。

ステップ

1. Tiebreaker CLI の configuration show コマンドを使用して、 MetroCluster の設定情報を表示します。

   次の例は、クラスタ cluster_A と cluster_B の情報を示しています。

```
MetroCluster: North America
    Monitor Enabled: true
    ClusterA name: cluster_A
    ClusterA IpAddress: 10.222.196.130
    ClusterB name: cluster_B
    ClusterB IpAddress: 10.222.196.140
```

ダンプ・ファイルの作成

Tiebreaker ソフトウェアの全体的なステータスを、デバッグのためにダンプファイルに保存します。

ステップ

1. Tiebreaker CLI の monitor dump-status コマンドを使用して、すべての MetroCluster 設定の全体的なステータスのダンプファイルを作成する。

   次の例は、 /var/log/netapp/mcctb/metrocluster-tiebreaker-status.xml ダンプファイルが正常に作成されたことを示しています。

```
NetApp MetroCluster Tiebreaker :> monitor dump -status
MetroCluster Tiebreaker status successfully dumped in file
/var/log/netapp/mcctb/metrocluster-tiebreaker-status.xml
```

タイブレーカーオブザーバーモードを無効にする

Tiebreaker ソフトウェアのオブザーバー モードを無効にすると、サイト障害が検出された後、自動的にスイッチオーバーが開始されます。

Tiebreaker 1.6以降では、 `monitor add wizard`指示。参照"MetroCluster 構成を追加"。

ステップ

1. オブザーバーモードを無効にする:

   monitor modify monitor-name monitor_name -observer -mode false

```
NetApp MetroCluster Tiebreaker :> monitor modify -monitor-name 8pack
-observer-mode false
Warning: If you are turning observer-mode to false, make sure to review
the 'risks and limitations'
as described in the MetroCluster Tiebreaker installation and
configuration.
Are you sure you want to enable automatic switchover capability for
monitor "8pack"? [Y/N]: y
```

MetroCluster Tiebreaker をアクティブモードで使用する場合のリスクと制限事項

アクティブモードの MetroCluster Tiebreaker では、サイト障害検出時のスイッチオーバーは自動的に実行されます。このモードは、 ONTAP / FAS の自動スイッチオーバー機能を補完する目的で使用できます。

MetroCluster Tiebreaker をアクティブモードで実装すると、以下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。

- サイト間リンクで障害が発生した場合、各サイトのコントローラは引き続きクライアントにサービスを提供します。ただし、コントローラはミラーリングされません。一方のサイトのコントローラの障害はサイト障害とみなされ、 MetroCluster Tiebreaker はスイッチオーバーを開始します。リモートサイトとのサイト間リンク障害後にミラーリングされていないデータは失われます。
- リモートサイトのアグリゲートがデグレード状態になるとスイッチオーバーが実行されます。アグリゲートの再同期前にスイッチオーバーが実行された場合、データはレプリケートされません。
- スイッチオーバーの実行中にリモートストレージの障害が発生します。

- ストレージコントローラの不揮発性メモリ（プラットフォームモデルに応じて NVRAM または NVMEM ）は、パートナーサイトのリモートディザスタリカバリ（ DR ）パートナーにミラーリングされません。
- クラスタピアリングネットワークが長時間にわたって停止し、スイッチオーバー後にメタデータボリュームがオンラインにならないと、メタデータが失われます。

ここに記載されていない状況が発生することもあります。ネットアップは、 MetroCluster Tiebreaker をアクティブモードで使用中に発生したいかなる損害についても責任を負いません。リスクおよび制限を許容できない場合は、 MetroCluster Tiebreaker をアクティブモードで使用しないでください。

MetroCluster Tiebreaker のファイアウォール要件

MetroCluster Tiebreaker 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。

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。

ポート / サービス	ソース	宛先	目的
443 / TCP	Tiebreaker	インターネット	ネットアップへの AutoSupport メッセージの送信
22 / TCP	管理ホスト	Tiebreaker	Tiebreaker の管理
443 / TCP	Tiebreaker	クラスタ管理 LIF	HTTP （ SSL ）を使用したクラスタへのセキュアな通信
22 / TCP	Tiebreaker	クラスタ管理 LIF	SSH を使用してクラスタとの通信を保護します
443 / TCP	Tiebreaker	ノード管理 LIFs	HTTP （ SSL ）を使用したノードへのセキュアな通信
22 / TCP	Tiebreaker	ノード管理 LIFs	SSH を使用してノードとの通信を保護します
162/UDP	Tiebreaker	SNMP トラップホスト	アラート通知 SNMP トラップの送信に使用されます
ICMP （ ping ）	Tiebreaker	クラスタ管理 LIF	クラスタ IP に到達できるかどうかを確認します
ICMP （ ping ）	Tiebreaker	ノード管理 LIFs	ノード IP に到達できるかどうかを確認します

MetroCluster Tiebreakerを使用してスイッチオーバーをシミュレートする

MetroCluster Tiebreaker 1.7 以降では、スイッチオーバーをシミュレートして、Tiebreaker のスイッチオーバー機能をテストできます。

このタスクについて

- その `monitor switchover-simulate`コマンドはTiebreaker 1.7以降でのみサポートされます。

手順

1. タイブレーカーの監視ステータスを確認します。
   `monitor show -status`

例

```
NetApp MetroCluster Tiebreaker :> monitor show -status
MetroCluster: A700
    Disaster: false
    Monitor State: Normal
    Observer Mode: false
    Silent Period: 5
    Override Vetoes: false
    Cluster: ClusterA_siteA(UUID:713e5ab2-b4e8-11f0-91aa-
00a098ef36a2)
        Reachable: true
        Intersite Connectivity Available: true
            Node: node_A1(UUID:9f6cecbf-b4e4-11f0-9d0f-00a098ef36a2)
                Reachable: true
                Intersite Connectivity Available: true
                State: normal
            Node: node_A2(UUID:2719bb56-b4e7-11f0-996c-00a09897caa3)
                Reachable: true
                Intersite Connectivity Available: true
                State: normal
    Cluster: ClusterB_siteB(UUID:72839591-b4e8-11f0-b688-
00a09897cb73)
        Reachable: true
        Intersite Connectivity Available: true
            Node: node_B1(UUID:abfeab89-b4e4-11f0-a077-00a09897cb73)
                Reachable: true
                Intersite Connectivity Available: true
                State: normal
            Node: node_B2(UUID:31e395bf-b4e7-11f0-bf99-00a09897cb2f)
                Reachable: true
                Intersite Connectivity Available: true
                State: normal
```

2. 切り替えシミュレーションを実行します。

```
monitor switchover-simulate -monitor-name <monitor_name> -cluster
<cluster_name>
```

このコマンドは、操作が成功すると次の出力を返します。

```
Successfully triggered Switchover Simulation. Please check the status of
the Switchover Simulation on the ONTAP cluster using command
"metrocluster operation history show"
```

MetroCluster Tiebreakerのイベントログファイル

イベントログファイルには、MetroCluster Tiebreakerソフトウェアで実行されたすべての処理のログが含まれています。

Tiebreakerソフトウェアは次の処理を実行します。

- サイト障害を検出
- データベース、他のTiebreakerモニタ、またはMetroCluster Tiebreakerソフトウェアに関連する設定変更を検出します
- SSH接続および切断を検出します
- MetroCluster 構成を検出します

これらのアクションは、次の形式でイベントログファイルに記録されます。

タイムスタンプの重大度/ログレベルのスレッドIDモジュール

```
2022-09-07 06:14:30,797 INFO  [MCCTBCommandServer-16] [SslSupport]
Successfully initiated SSL context. Protocol used is TLSv1.3.
2022-09-07 06:14:34,137 INFO  [MCCTBCommandServer-16] [DataBase]
Successfully read MCCTB database.
2022-09-07 06:14:34,137 INFO  [MCCTBCommandServer-16]
[ConfigurationMonitor] Debug mode disabled.
```

追加情報の参照先

MetroCluster の設定と処理の詳細については、を参照してください。

MetroCluster およびその他の情報

情報	件名
"MetroCluster のドキュメント"	• すべての MetroCluster 情報
"ネットアップテクニカルレポート 4375 ：『 NetApp MetroCluster for ONTAP 9.3 』"	• MetroCluster の設定と運用の技術概要 • MetroCluster 構成のベストプラクティス

"ファブリック接続 MetroCluster のインストールと設定"	• ファブリック接続 MetroCluster アーキテクチャ • 構成のケーブル接続 • FC-to-SAS ブリッジの設定 • FC スイッチを設定します • ONTAP で MetroCluster を設定します
"ストレッチ MetroCluster のインストールと設定"	• ストレッチ MetroCluster アーキテクチャ • 構成のケーブル接続 • FC-to-SAS ブリッジの設定 • ONTAP で MetroCluster を設定します
"MetroCluster IP のインストールと設定"	• MetroCluster IP アーキテクチャ • MetroCluster IP 構成のケーブル接続 • ONTAP で MetroCluster を設定します
"MetroCluster のコンポーネントをメンテナンスします"	• MetroCluster 構成のメンテナンスガイドライン • 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 • ファブリック接続またはストレッチ MetroCluster 構成でのディスクシェルフのホットアド • ファブリック接続またはストレッチ MetroCluster 構成でのディスクシェルフのホットリムーブ • ファブリック接続またはストレッチ MetroCluster 構成のディザスタサイトでのハードウェア交換 • 2 ノードのファブリック接続またはストレッチ MetroCluster 構成の 4 ノード MetroCluster 構成への拡張 • 4 ノードのファブリック接続またはストレッチ MetroCluster 構成の 8 ノード MetroCluster 構成への拡張
Active IQ Unified Manager のドキュメント "ネットアップのマニュアル：製品ガイドとリソース"	• MetroCluster の設定とパフォーマンスを監視する
"コピーベースの移行"	• 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

MetroCluster のデータ保護とディザスタリカバリを理解する

MetroCluster のデータ保護とディザスタリカバリについて理解する

MetroCluster でデータ保護と障害からの透過的なリカバリがどのように行われるかを理解しておくと、スイッチオーバーとスイッチバックの作業を簡単かつ効率的に実施できます。

MetroCluster は、ミラーリングを使用してクラスタ内のデータを保護します。ディザスタリカバリは 1 つの MetroCluster コマンドで実装されます。このコマンドは、サバイバーサイトのセカンダリをアクティブ化して、災害の影響を受けたプライマリサイトが本来所有していた、ミラーリングされたデータを提供できるようにします。

8 ノード / 4 ノード MetroCluster 構成でのローカルフェイルオーバーとスイッチオーバー

8 ノード / 4 ノードの MetroCluster 構成では、ローカルレベルとクラスタレベルの両方でデータが保護されます。MetroCluster 構成をセットアップする場合は、 MetroCluster 構成がどのようにデータを保護するかを理解しておく必要があります。

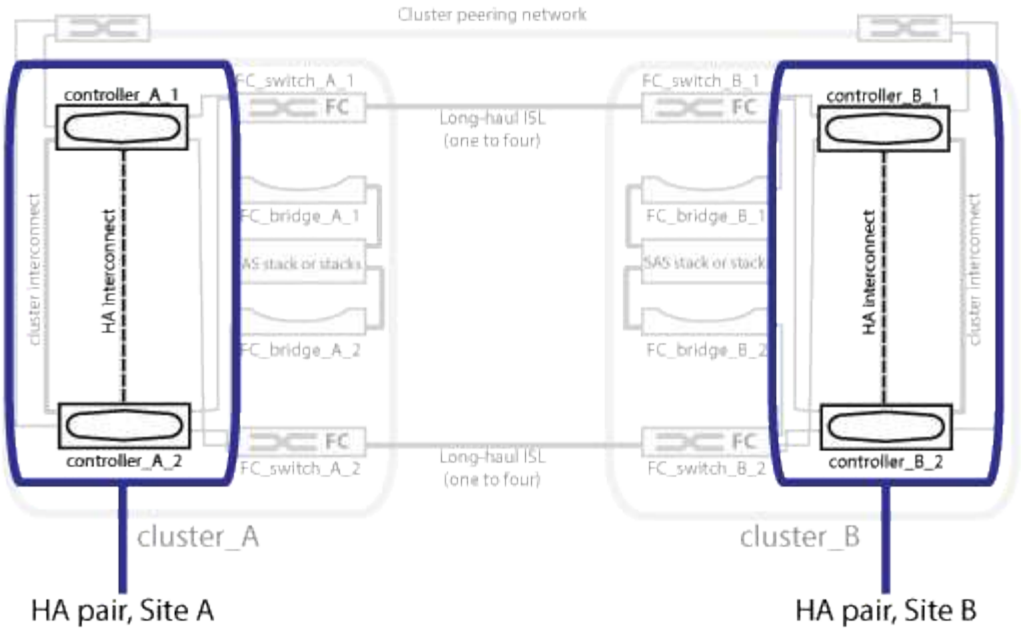
MetroCluster 構成は、物理的に分離され、ミラーされた 2 つのクラスタを使用することでデータを保護各クラスタで、もう一方のクラスタのデータおよび Storage Virtual Machine （ SVM ）の設定が同期的にミラーされます。一方のサイトで災害が発生すると、管理者は、ミラーされた SVM をアクティブ化し、サバイバーサイトからミラーされたデータの提供を開始します。さらに、各クラスタ内のノードは HA ペアとして構成されているため、ローカルフェイルオーバーも可能になります。

MetroCluster 構成でのローカルの HA データ保護の仕組み

MetroCluster 構成での HA ペアの仕組みを理解する必要があります。

ピアネットワークにある 2 つのクラスタは、それぞれがもう一方のクラスタのソースクラスタおよびバックアップクラスタになることで、双方向のディザスタリカバリを実現します。各クラスタは、 HA ペアとして構成された 2 つのノードで構成されます。1 つのノード構成内で障害が発生した場合やメンテナンスが必要な場合、ストレージフェイルオーバーによって、そのノードの処理をローカルの HA パートナーに転送することができます。

次の図は、 MetroCluster FC 構成を示しています。HA 機能は、 HA インターコネクトがクラスタスイッチで確立されている点を除いて、 MetroCluster IP 構成と同じです。



関連情報

"ハイアベイラビリティ構成"

MetroCluster 構成でのデータと設定のレプリケーション

MetroCluster 構成では、各種の ONTAP 機能を使用して、 2 つの MetroCluster サイト間でデータと設定の同期レプリケーションが行われます。

設定レプリケーションサービスによる設定の保護

ONTAP の Configuration Replication Service （ CRS ；設定レプリケーションサービス）は、 DR パートナーに情報を自動的にレプリケートして MetroCluster の設定を保護します。

CRS は、ローカルノードの設定をパートナークラスタの DR パートナーに同期的にレプリケートします。このレプリケーションは、クラスタピアリングネットワーク経由で行われます。

レプリケートされる情報には、クラスタの設定と SVM の設定が含まれます。

MetroCluster 処理中の **SVM** のレプリケーション

ONTAP の Configuration Replication Service （ CRS ；設定レプリケーションサービス）は、冗長なデータサーバ構成と SVM に属するデータボリュームのミラーリングを提供します。スイッチオーバーでは、ソース SVM が停止され、サバイバークラスタ上にあるデスティネーション SVM がアクティブになります。

MetroCluster 構成のデスティネーション SVM の名前には、識別しやすいように「 -mc 」というサフィックスが自動的に付加されます。MetroCluster 構成では、デスティネーション SVM の名前に「 -mc 」というサフィックスが付加されます。 SVM 名にピリオドが含まれている場合は、最初のピリオドの前にサフィックス「 -mc 」が適用されます。たとえば、 SVM 名が SVM.DNS.NAME の場合、サフィックス「 -mc 」は SVM-MC.DNS.NAME のように付加されます。

次の例は、 MetroCluster 構成の SVM を示しています。「 SVM_cluster_A 」はソースサイトの SVM 、「 SVM_cluster_A-mc 」はディザスタリカバリサイトの同期先のアグリゲートです。

- SVM_cluster_A はクラスタ A のデータを提供します

  これは同期元の SVM であり、 SVM の設定（ LIF 、プロトコル、サービス）および SVM に属するボリュームのデータを表します。設定とデータは、クラスタ B にある同期先の SVM 、 SVM_cluster_A-mc にレプリケートされます

- SVM_cluster_B はクラスタ B のデータを提供します

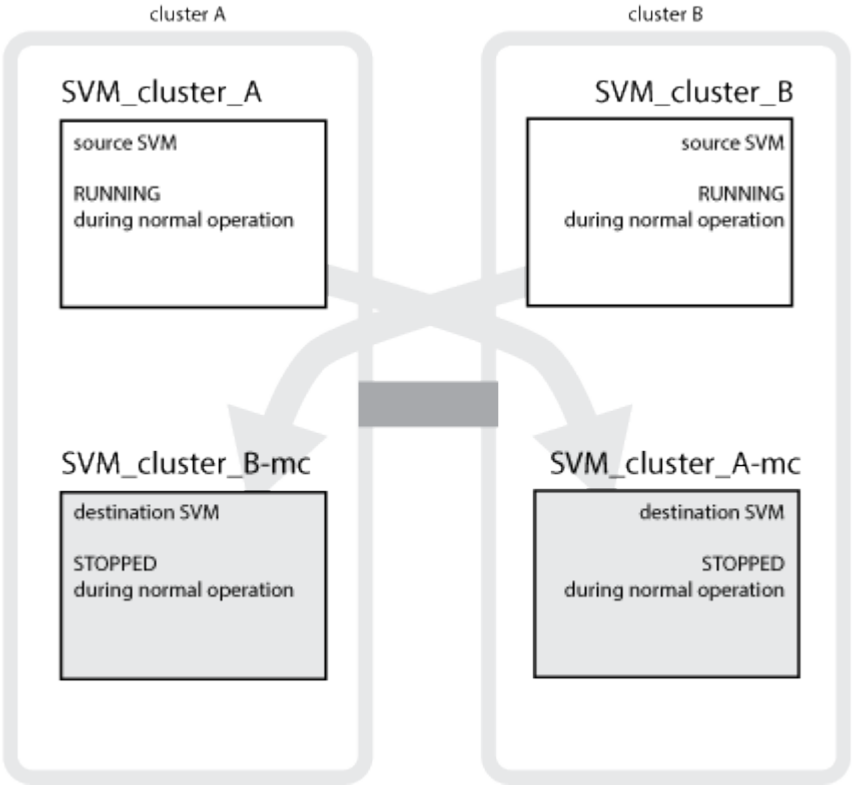
  これは同期元の SVM であり、クラスタ A にある SVM_cluster_B-mc に対する設定とデータを表します

- SVM_cluster_B-mc は同期先の SVM であり、 MetroCluster 構成が通常どおり正常に動作している間は停止しています。

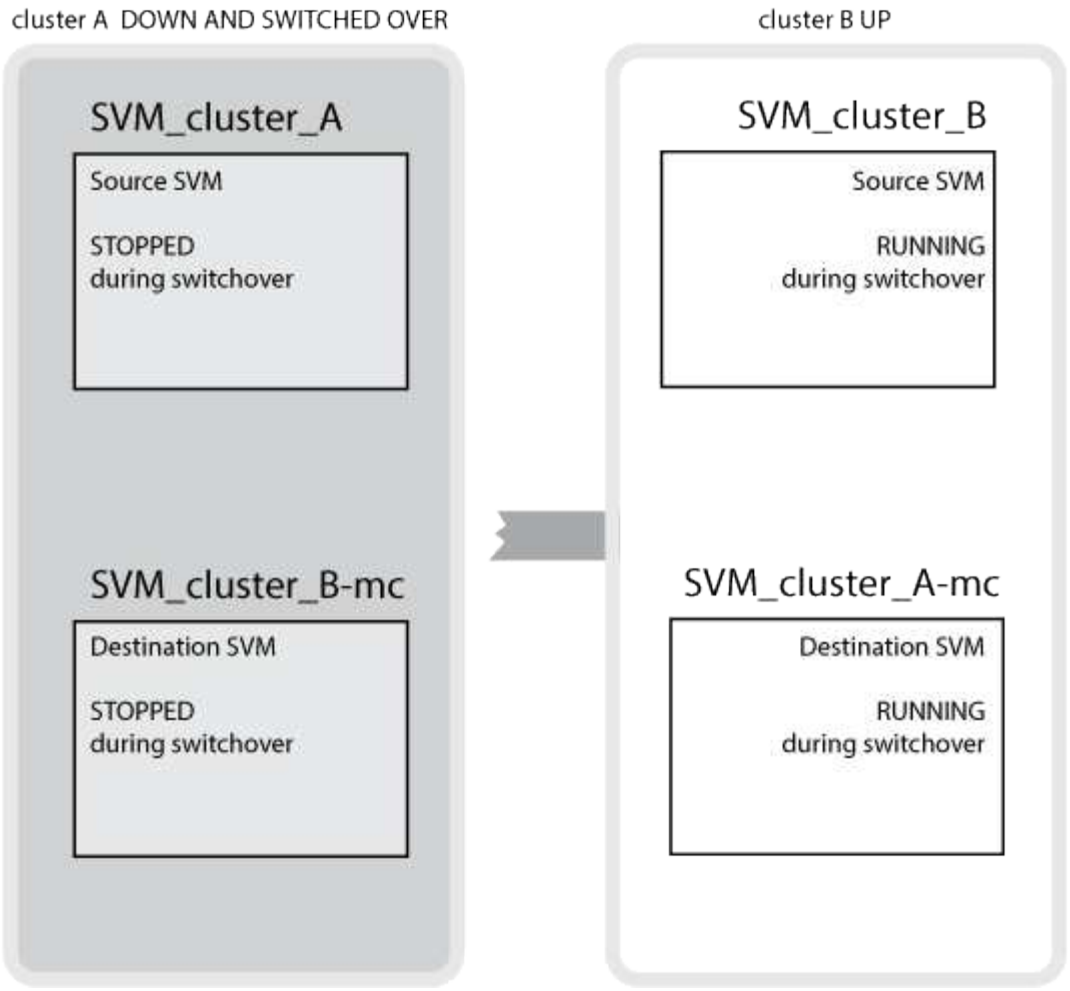
  クラスタ B からクラスタ A へのスイッチオーバーが成功すると SVM_cluster_B は停止し、 SVM_cluster_B-mc がアクティブになって、クラスタ A のデータ提供を開始します

- SVM_cluster_A-mc は同期先の SVM であり、 MetroCluster 構成が通常どおり正常に動作している間は停止しています。

  クラスタ A からクラスタ B へのスイッチオーバーが成功すると SVM_cluster_A は停止し、 SVM_cluster_A-mc がアクティブになって、クラスタ B のデータ提供を開始します



スイッチオーバーでは、サバイバークラスタ上のリモートプレックスがオンラインになり、セカンダリ SVM がデータの提供を開始します。



スイッチオーバー後にリモートプレックスを使用できるかどうかは、 MetroCluster の構成タイプによって異なります。

- MetroCluster FC 構成では、スイッチオーバー後に ISL を使用してディザスタサイトのストレージにアクセスできる場合、ローカルプレックスとリモートプレックスの両方がオンラインのままになります。

  ISL で障害が発生し、ディザスタサイトのストレージを使用できない場合、同期先の SVM がサバイバーサイトからデータの提供を開始します。

- MetroCluster IP 構成でリモートプレックスを使用できるかどうかは、 ONTAP のバージョンによって決まります。
  - ONTAP 9.5 以降では、ディザスタサイトのノードがブートしたままの場合、ローカルプレックスとリモートプレックスの両方がオンラインのままになります。
  - ONTAP 9.5 よりも前のバージョンでは、サバイバーサイトのローカルプレックスからのみストレージを使用できます。

    同期先の SVM がサバイバーサイトからデータの提供を開始します。

関連情報

"システム管理"

MetroCluster 構成で **SyncMirror** を使用してデータの冗長性を実現する方法

SyncMirror 機能を使用するミラーされたアグリゲートにはソースとデスティネーションの Storage Virtual Machine （ SVM ）が所有するボリュームが格納され、データの冗長性が確保されます。データはパートナークラスタのディスクプールにレプリケートされます。ミラーされていないアグリゲートもサポートされます

次の表に、スイッチオーバー後のミラーされていないアグリゲートの状態（オンラインまたはオフライン）を示します。

スイッチオーバーのタイプ	MetroCluster FCの設定状態	MetroCluster IPの設定状態
ネゴシエートスイッチオーバー（ NSO ）	オンライン	オフライン（注1）
自動計画外スイッチオーバー（ AUSO ）	オンライン	オフライン（注1）
計画外スイッチオーバー（ USO ）	• ストレージが使用できない場合は、オフラインになります • ストレージが使用可能な場合：オンライン	オフライン（注1）

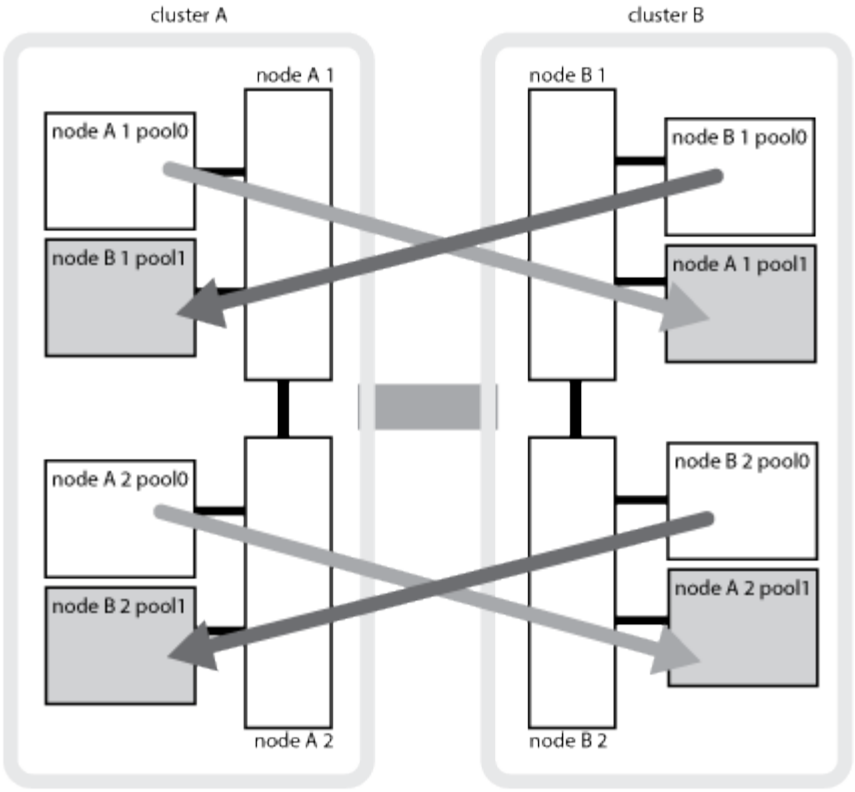
*注1 *：MetroCluster IP構成では、スイッチオーバーの完了後に、ミラーされていないアグリゲートを手動でオンラインにすることができます。

の詳細を確認してください MetroCluster FC 構成と IP 構成のスイッチオーバーの違い。

スイッチオーバー後に、ミラーされていないアグリゲートが DR パートナーノードにある状態でスイッチ間リンク（ ISL ）に障害が発生すると、そのローカルノードで障害が発生することがあります。

次の図は、ディスクプールがパートナークラスタ間でミラーされる仕組みを示しています。ローカルプレックス（プール 0 内）のデータは、リモートプレックス（プール 1 内）にレプリケートされます。

ハイブリッドアグリゲートを使用している場合、ソリッドステートディスク（ SSD ）レイヤがいっぱいになったことが原因で SyncMirror プレックスに障害が発生すると、パフォーマンスが低下する可能性があります。



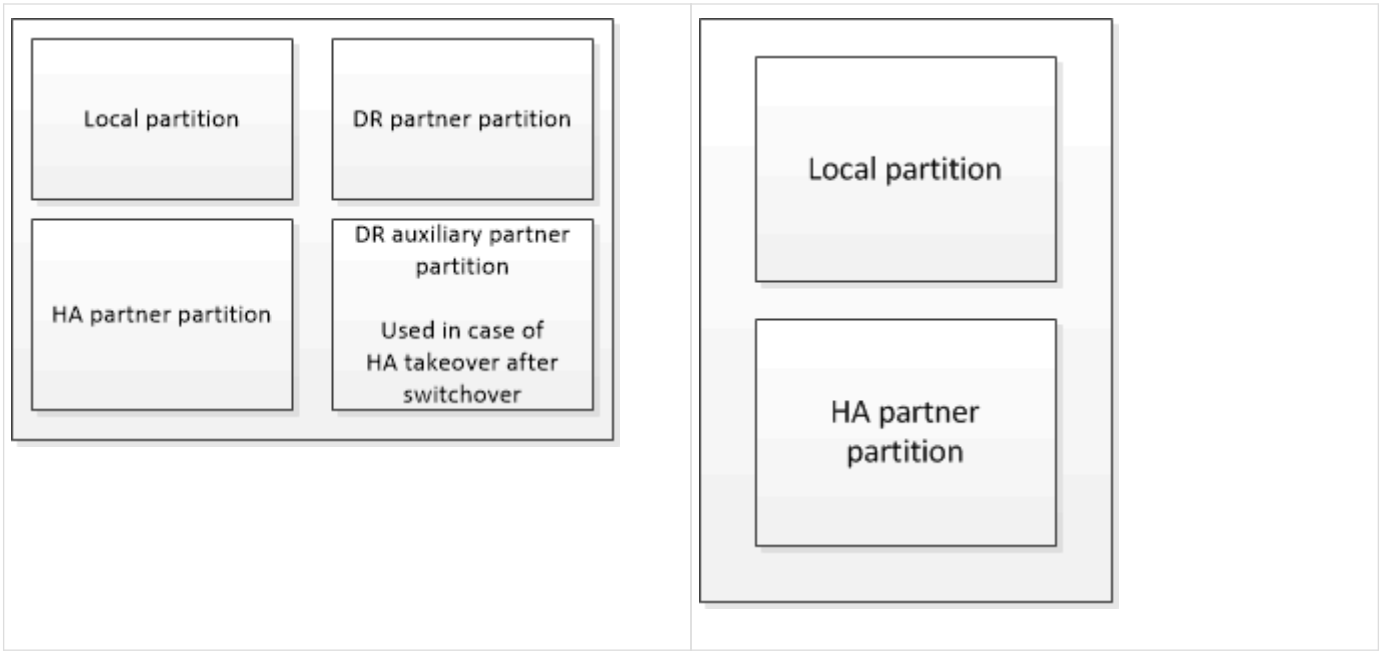
MetroCluster 構成での **NVRAM / NVMEM** キャッシュミラーリングと動的ミラーリング

ストレージコントローラの不揮発性メモリ（プラットフォームモデルに応じて NVRAM または NVMEM ）は、ローカル HA パートナーにローカルでミラーされ、同時にパートナーサイトのリモートディザスタリカバリ（ DR ）パートナーにリモートでミラーされます。この構成により、ローカルでフェイルオーバーまたはスイッチオーバーが発生しても、不揮発性キャッシュ内のデータを保護することができます。

MetroCluster 構成に含まれない HA ペアでは、各ストレージコントローラに、不揮発性キャッシュパーティションが 2 つ保持されます。 1 つは不揮発性キャッシュパーティションで、もう 1 つは HA パートナー用です。

4 ノード MetroCluster 構成では、各ストレージコントローラの不揮発性キャッシュが 4 つのパーティションに分かれています。2 ノード MetroCluster 構成では、ストレージコントローラが HA ペアとして構成されないため、 HA パートナーパーティションと DR 補助パーティションが使用されません。

ストレージコントローラの不揮発性キャッシュ	
MetroCluster 構成の場合	MetroCluster に属さない HA ペア



不揮発性キャッシュには次の情報が格納されます。

- ローカルパーティションは、ストレージコントローラからディスクに書き込まれる前のデータを格納します。
- HA パートナーパーティションは、 HA パートナーのローカルキャッシュのコピーを格納します。

  2 ノード MetroCluster 構成では、ストレージコントローラが HA ペアとして構成されないため、 HA パートナーパーティションは存在しません。

- DR パートナーパーティションは、 DR パートナーのローカルキャッシュのコピーを格納します。

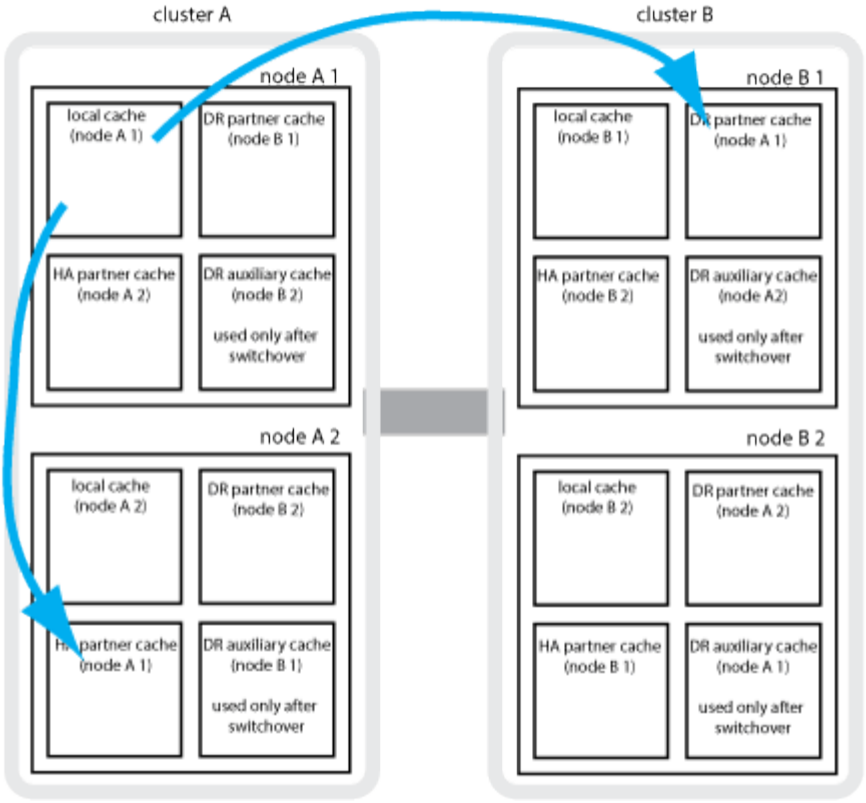
  DR パートナーは、ローカルノードとペアリングされているパートナークラスタ内のノードです。

- DR 補助パートナーパーティションは、 DR 補助パートナーのローカルキャッシュのコピーを格納します。

  DR 補助パートナーは、ローカルノードの DR パートナーの HA パートナーです。このキャッシュは、 HA テイクオーバーが実行された場合（構成の通常動作時または MetroCluster スイッチオーバー後）に必要です。

  2 ノード MetroCluster 構成では、ストレージコントローラが HA ペアとして構成されないため、 DR 補助パートナーパーティションは存在しません。

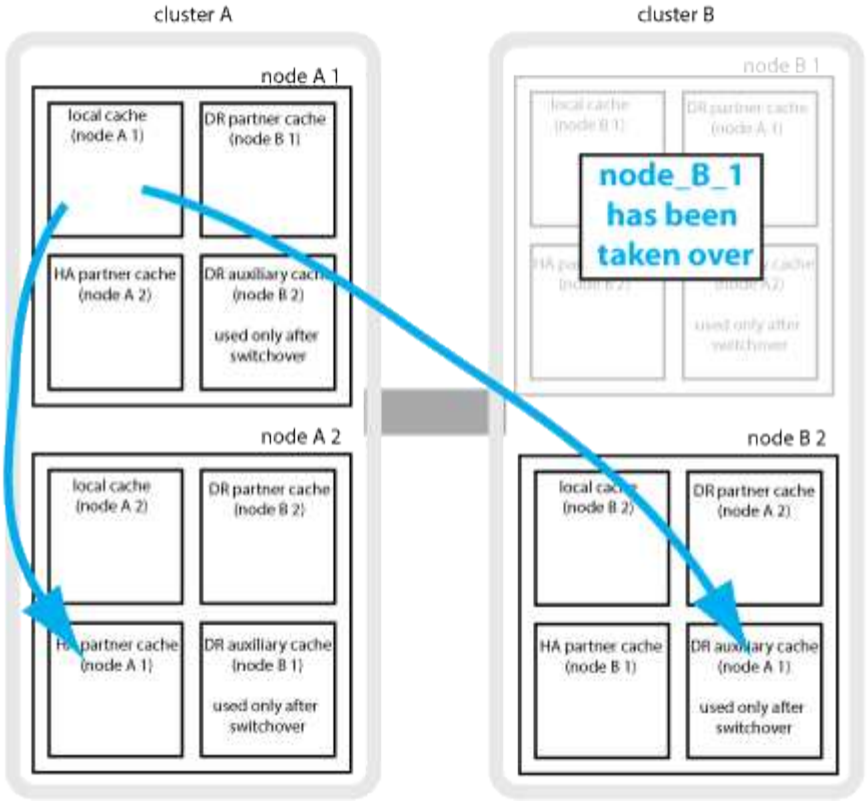
たとえば、ノード（ node_A_1 ）のローカルキャッシュは、 MetroCluster サイトでローカルおよびリモートの両方でミラーされます。次の図では、 node_A_1 のローカルキャッシュが、 HA パートナー（ node_B_2 ）と DR パートナー（ node_B_1 ）にミラーされています。



ローカルの **HA** テイクオーバー時の動的なミラーリング

4 ノード MetroCluster 構成でローカルの HA テイクオーバーが行われると、テイクオーバーされたノードは DR パートナーのミラーとして機能しなくなります。DR ミラーリングを続行するために、ミラーリング先が自動的に DR 補助パートナーに切り替わります。ギブバックが正常に完了すると、ミラーリング先は自動的に DR パートナーに戻ります。

たとえば、 node_B_1 で障害が発生し、 node_B_2 によってテイクオーバーされたとします。node_A_1 のローカルキャッシュを node_B_1 にミラーできなくなります。ミラーリング先が DR 補助パートナー node_B_2 に切り替わります。



災害の種類とリカバリ方法

MetroCluster 構成を使用して適切に対応できるように、さまざまな種類の障害や災害について熟知しておく必要があります。

- 単一ノード障害です

  ローカル HA ペアの 1 つのコンポーネントで障害が発生した場合。

  4 ノード MetroCluster 構成の場合、障害が発生したコンポーネントによっては、障害ノードの自動テイクオーバーまたはネゴシエートテイクオーバーが行われる可能性があります。データ・リカバリについては、を参照してください "ハイアベイラビリティペアの管理" 。

  2 ノード MetroCluster 構成の場合は、 Automatic Unplanned Switchover （ AUSO ；自動計画外スイッチオーバー）が行われます。

- サイト全体のコントローラ障害

  電源の喪失、機器の交換、または災害が原因で、サイトのすべてのコントローラモジュールで発生する障害です。通常、 MetroCluster 構成では障害と災害を区別できません。ただし、 MetroCluster Tiebreaker ソフトウェアなどの監視ソフトウェアはこれらを区別できます。スイッチ間リンク（ ISL ）およびスイッチが稼働しており、ストレージにアクセスできる場合は、サイト全体のコントローラ障害によって自動スイッチオーバーが実行される可能性があります。

  "ハイアベイラビリティペアの管理" サイト全体のコントローラ障害（コントローラ障害を含まない）および1台以上のコントローラを含む障害からのリカバリ方法について詳しく説明します。

- ISL 障害です

サイト間のリンクで障害が発生した場合MetroCluster の設定は何の動作も行いません。各ノードは通常どおりデータを提供しますが、対応するディザスタリカバリサイトにアクセスできないため、ミラーデータの書き込みは行われません。

- 複数の連続的な障害

  複数のコンポーネントで連続して発生する障害です。たとえば、コントローラモジュール、スイッチファブリック、シェルフで連続して障害が発生すると、ダウンタイムやデータ損失から保護するために、ストレージフェイルオーバー、ファブリックの冗長化、および SyncMirror が順次行われる場合があります。

次の表に、障害の種類、および対応するディザスタリカバリ（ DR ）メカニズムとリカバリ方法を示します。

MetroCluster IP構成では、AUSO（自動計画外スイッチオーバー）はサポートされません。

障害のタイプ	DR メカニズム		リカバリ方法の概要	
	4 ノード構成	2 ノード構成	4 ノード構成	2 ノード構成
単一ノード障害です	ローカル HA フェイルオーバー	AUSO	自動フェイルオーバーとギブバックが有効になっている場合は必要なし。	ノードがリストアされた後は ' MetroCluster heal-phase aggregates コマンド 'MetroCluster heal-phase root-aggregates コマンド 'MetroCluster switchback コマンドを使用して ' 手動で修復およびスイッチバックを行う必要があります注 MetroCluster : ONTAP 9.5 以降を実行する MetroCluster IP 構成では 'CLI heal-' コマンドは必要ありません

サイト障害	MetroCluster スイッチオーバー		ノードがリストアされた後には ' MetroCluster healing' および MetroCluster switchback コマンドを使用した手動での修復とスイッチバックが必要ですONTAP 9.5 を実行する MetroCluster IP 構成では 'CLI MetroCluster heal-' コマンドは必要ありません
サイト全体のコントローラ障害	AUSO が行われるのは、ディザスタサイトのストレージにアクセスできる場合のみです。	AUSO （単一ノード障害と同じ）	
複数の連続的な障害	ローカル HA フェイルオーバーのあとに、 MetroCluster switchover -forced -on-disaster コマンドを使用して MetroCluster 強制スイッチオーバーを実行。注：障害が発生したコンポーネントによっては、強制スイッチオーバーは不要な場合があります。	MetroCluster は 'MetroCluster switche-forced-on-disaster コマンドを使用して強制的にスイッチオーバーします	
ISL 障害です	MetroCluster のスイッチオーバーなし。 2 つのクラスタがそれぞれのデータを独立して提供します		このタイプの障害では必要ありません。接続が回復すると、ストレージは自動的に再同期されます。

8 ノード / 4 ノード MetroCluster 構成でのノンストップオペレーションの実現

問題が 1 つのノードに限定されている場合、ローカル HA ペア内でのフェイルオーバーとギブバックにより、中断のないノンストップオペレーションが実現します。この場合、 MetroCluster 構成ではリモートサイトへのスイッチオーバーは必要ありません。

8 ノード / 4 ノードの MetroCluster 構成は各サイトに 1 つ以上の HA ペアで構成されるため、それぞれのサイトでのローカルな障害には、パートナーサイトにスイッチオーバーしなくても対応でき、サービスが中断することはありません。HA ペアの動作は、 MetroCluster 以外の構成の HA ペアと同じです。

4 ノードおよび 8 ノードの MetroCluster 構成では、パニックまたは停電によるノード障害が原因の自動スイッチオーバーによって発生する可能性があります。

"ハイアベイラビリティペアの管理"

ローカルのフェイルオーバー後に 2 回目の障害が発生した場合、 MetroCluster のスイッチオーバーイベントによって、中断のないノンストップオペレーションが実現します。同様に、スイッチオーバー処理後にサバイバーノードの 1 つで次の障害が発生すると、ローカルのフェイルオーバーイベントによってノンストップオペレーションが継続されます。この場合、 1 つのサバイバーノードが、 DR グループ内の他の 3 つのノードにデータを提供します。

MetroCluster 移行中のスイッチオーバーとスイッチバック

MetroCluster FC-to IP の移行では、 MetroCluster IP ノードと IP スイッチを既存の MetroCluster FC 構成に追加し、 MetroCluster FC ノードを撤去します。移行プロセスの各ステージでは、 MetroCluster のスイッチオーバー、修復、スイッチバックの各処理のワークフローが異なります。

を参照してください "移行時のスイッチオーバー、修復、スイッチバックの処理"。

スイッチオーバー後のローカルフェイルオーバーの影響

MetroCluster のスイッチオーバー後にサバイバーサイトで問題が発生した場合は、ローカルフェイルオーバーによって中断のないノンストップオペレーションが実現します。ただし、冗長構成ではなくなるため、システムはリスクにさらされます。

スイッチオーバー後にローカルフェイルオーバーが発生すると、 1 台のコントローラが MetroCluster 構成内のすべてのストレージシステムにデータを提供します。そのため、リソースの問題が発生する可能性があり、さらに障害が発生した場合にはシステムが中断します。

2 ノード MetroCluster 構成でのノンストップオペレーションの実現

パニックが原因で 2 つのサイトのどちらかに問題がある場合は、 MetroCluster スイッチオーバーによって中断のないノンストップオペレーションが実現します。停電がノードとストレージの両方に影響を与える場合 ' スイッチオーバーは自動的には行われず 'MetroCluster switchover' コマンドが発行されるまで停止します

すべてのストレージがミラーリングされるため、ノード障害時の HA ペアでのストレージフェイルオーバーの場合と同様に、サイト障害が発生した場合にスイッチオーバー処理を使用して無停止の耐障害性を実現できます。

2 ノード構成では、 HA ペアで自動ストレージフェイルオーバーをトリガーするイベントと同じイベントによって、自動計画外スイッチオーバー（ AUSO ）がトリガーされます。つまり、 2 ノード MetroCluster 構成では HA ペアと同じ保護レベルが確保されます。

関連情報

"MetroCluster FC 構成での自動計画外スイッチオーバー"

スイッチオーバープロセスの概要

MetroCluster スイッチオーバー処理を実行すると、ストレージおよびクライアントのアクセスがソースクラスタからリモートサイトに移されるため、災害発生後にサービスの迅速な復旧が可能となります。スイッチオーバーが発生した場合に想定される変化と、実行する必要がある操作を把握しておく必要があります。

スイッチオーバー処理では、システムによって次の処理が実行されます。

- ディザスタサイトに属するディスクの所有権がディザスタリカバリ（ DR ）パートナーに変更されます。

  これは、停止中のパートナーに属するディスクの所有権が正常な状態のパートナーに変更されるハイアベイラビリティ（ HA ）ペアでのローカルフェイルオーバーと似ています。

- サバイバーサイトにあるサバイバープレックスがディザスタクラスタ内のノードに属する場合、そのサバイバープレックスは、サバイバーサイトのクラスタでオンラインになります。
- ディザスタサイトに属する同期元の Storage Virtual Machine （ SVM ）が、ネゴシエートスイッチオーバーの実行中のみ停止されます。

  この処理は、ネゴシエートスイッチオーバーにのみ該当します。

- ディザスタサイトに属する同期先の SVM を起動します。

DR パートナーのルートアグリゲートは、スイッチオーバー中にオンラインになりません。

「 MetroCluster switchover 」コマンドは、 MetroCluster 構成のすべての DR グループのノードを切り替えます。たとえば、 8 ノードの MetroCluster 構成では、両方の DR グループでノードがスイッチオーバーされます。

サービスのみをリモートサイトにスイッチオーバーする場合は、サイトをフェンシングせずにネゴシエートスイッチオーバーを実行します。ストレージまたは機器を信頼できない場合は、ディザスタサイトをフェンシングしてから、計画外スイッチオーバーを実行する必要があります。フェンシングにより、ディスクに電源が順次投入されたときの RAID の再構築が回避されます。

この手順は、もう一方のサイトが安定していてオフラインにすることがない場合にのみ使用してください。

スイッチオーバー中にコマンドを使用できるかどうか

次の表に、スイッチオーバー時に使用できるコマンドを示します。

コマンドを実行します	可用性
「 storage aggregate create 」	アグリゲートを作成できます。 • サバイバークラスタの一部であるノードが所有している場合 次の場合はアグリゲートを作成できません。 • ディザスタサイトのノード用 • サバイバークラスタに属するノードの場合
「 storage aggregate delete 」をクリックします	データアグリゲートは削除できます。
「 storage aggregate mirror 」のように表示されます	ミラーされていないアグリゲートのプレックスを作成できます。
「 storage aggregate plex delete 」と入力します	ミラーアグリゲートのプレックスを削除できます。
「 vserver create 」	SVM を作成できます。 • 稼働しているクラスタが所有するデータアグリゲートにルートボリュームがある場合 SVM は作成できません。 • ディザスタサイトのクラスタが所有するデータアグリゲートにルートボリュームがある場合
「 vserver delete 」	sync-source と sync-destination の両方の SVM を削除できます。

「 network interface create -lif 」と入力します	同期元と同期先の両方の SVM に対してデータ SVM LIF を作成できます。
network interface delete -lif	同期元と同期先の両方の SVM のデータ SVM LIF を削除できます。
'volume create'	同期元と同期先の両方の SVM に対してボリュームを作成できます。 • 同期元の SVM の場合、ボリュームはサバイバークラスタが所有するデータアグリゲートに配置されている必要があります • 同期先の SVM の場合、ボリュームはディザスタサイトのクラスタが所有するデータアグリゲートに配置されている必要があります
volume delete	同期元と同期先の両方の SVM のボリュームを削除できます。
ボリューム移動	同期元と同期先の両方の SVM のボリュームを移動できます。 • 同期元の SVM の場合、サバイバークラスタがデスティネーションアグリゲートを所有している必要があります • 同期先の SVM の場合、ディザスタサイトのクラスタがデスティネーションアグリゲートを所有している必要があります
「昼休み」	データ保護ミラーのソースとデスティネーションのエンドポイント間の SnapMirror 関係を解除できます。

MetroCluster FC 構成と **IP** 構成のスイッチオーバーの違い

MetroCluster IP 構成では、 iSCSI ターゲットとして機能するリモート DR パートナーノードを介してリモートディスクがアクセスされるため、スイッチオーバー処理でリモートノードが停止している間はリモートディスクにアクセスできません。そのため、 MetroCluster FC 構成とは次の点が異なります。

- ローカルクラスタが所有するミラーアグリゲートがデグレード状態になります。
- リモートクラスタからスイッチオーバーされたミラーアグリゲートがデグレード状態になります。

ミラーされていないアグリゲートが MetroCluster IP 構成でサポートされている場合、リモートクラスタからスイッチオーバーされていないミラーされていないアグリゲートにはアクセスできません。

4 ノード MetroCluster 構成での HA テイクオーバーおよび MetroCluster スイッチオーバー中のディスク所有権の変更

ハイアベイラビリティ処理および MetroCluster 処理中、ディスク所有権が一時的に変更されます。どのノードがどのディスクを所有するかをシステムが追跡する仕組みを把握しておくと役立ちます。

ONTAP では、コントローラモジュールの一意のシステム ID （ノードの NVRAM カードまたは NVMEM ボードから取得）を使用して、どのノードがどの特定のディスクを所有するかを識別します。システムの HA または DR の状態によっては、ディスク所有権が一時的に変わる場合があります。HA テイクオーバーまたは DR スイッチオーバーによって所有権が変わった場合、どのノードがディスクの元の（「ホーム」）所有者であるかが記録されるため、 HA ギブバックまたは DR スイッチバック後に所有権を戻すことができます。ディスク所有権の追跡には次のフィールドが使用されます。

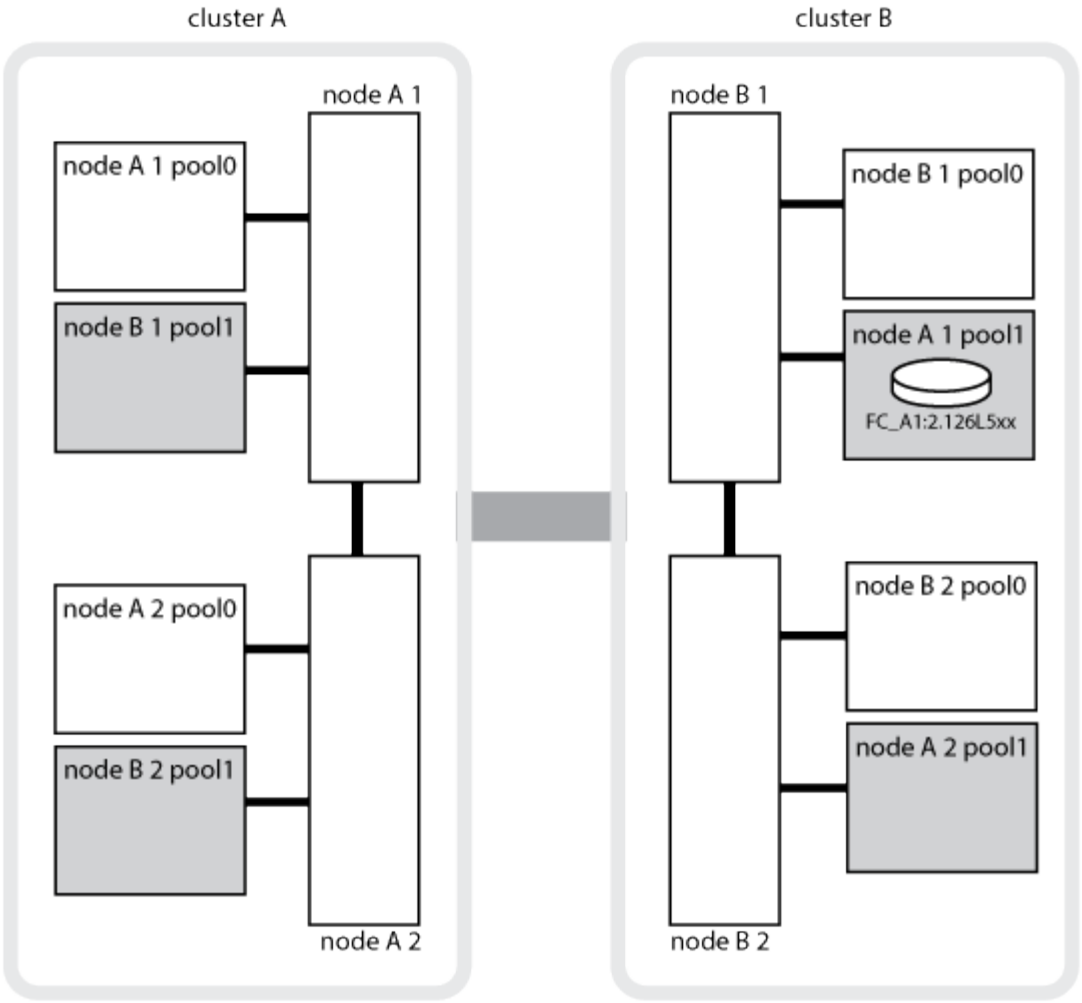
- オーナー
- ホーム所有者
- DR ホーム所有者

MetroCluster 構成でスイッチオーバーが発生した場合、ノードは、パートナークラスタのノードが元々所有していたアグリゲートの所有権を取得できます。このようなアグリゲートは「クラスタ外アグリゲート」と呼ばれます。クラスタ外アグリゲートはその時点でクラスタに認識されていないアグリゲートであるため、 DR ホーム所有者フィールドにはパートナークラスタのノードが所有していることが示されます。HA ペア内の従来の外部アグリゲートは所有者とホーム所有者の値が異なりますが、所有者とホーム所有者の値はクラスタ外アグリゲートで同じであるため、 DR ホーム所有者の値によってクラスタ外アグリゲートを識別できます。

システムの状態が変わると、各フィールドの値も次のように変わります。

フィールド	次の状況における値			
	通常運用時	ローカルの HA テイクオーバー	MetroCluster スイッチオーバー	スイッチオーバー中のテイクオーバー
オーナー	ディスクにアクセスできるノードの ID	一時的にディスクにアクセスできる HA パートナーの ID	一時的にディスクにアクセスできる DR パートナーの ID	一時的にディスクにアクセスできる DR 補助パートナーの ID
ホーム所有者	HA ペア内の元のディスク所有者の ID	HA ペア内の元のディスク所有者の ID	スイッチオーバー中に HA ペアのホーム所有者となる DR パートナーの ID	スイッチオーバー中に HA ペアのホーム所有者となる DR パートナーの ID
DR ホーム所有者	空です	空です	MetroCluster 構成内の元のディスク所有者の ID	MetroCluster 構成内の元のディスク所有者の ID

次の図と表は、物理的には cluster_B に配置されている node_A_1 のディスクプール 1 のディスクについて、所有権が変化する例を示しています



MetroCluster の状態	オーナー	ホーム所有者	DR ホーム所有者	注：
通常の状態：すべてのノードが完全に動作	node_A_1	node_A_1	該当なし	
ローカルの HA テイクオーバー： node_A_1 に属するディスクをテイクオーバーします。	Node_a_2	node_A_1	該当なし	
DR スイッチオーバー： node_B_1 が DR パートナー node_A_1 に属するディスクをテイクオーバー	node_B_1	node_B_1	node_A_1	元のホームノード ID は DR ホーム所有者フィールドに移動します。アグリゲートのスイッチバックまたは修復後、所有権は node_A_1 に戻ります。

DR のスイッチオーバーとローカルの HA テイクオーバー（二重障害）：node_B_2 が HA node_B_1 に属するディスクをテイクオーバー	node_B_2	node_B_1	node_A_1	ギブバック後、所有権は node_B_1 に戻ります。スイッチバックまたは修復後、所有権は node_A_1 に戻ります。
HA ギブバックおよび DR スイッチバック後：すべてのノードが完全に動作	node_A_1	node_A_1	該当なし	

ミラーされていないアグリゲートを使用する場合の

ミラーされていないアグリゲートが構成に含まれている場合、スイッチオーバー処理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。

電源のシャットダウンが必要なメンテナンス実施時のミラーされていないアグリゲートに関する考慮事項

サイト全体の電源のシャットダウンが必要なメンテナンスのためにネゴシエートスイッチオーバーを実行する場合は、最初にディザスタサイトが所有するミラーされていないアグリゲートを手動でオフラインにする必要があります。

そうしないと、複数のディスクがパニック状態になって、サバイバーサイトのノードが停止する可能性があります。この問題は、電源のシャットダウンまたは ISL の喪失によってディザスタサイトのストレージへの接続が失われたことが原因で、スイッチオーバーされたミラーされていないアグリゲートがオフラインになるか、または見つからない場合に発生します。

ミラーされていないアグリゲートと階層状のネームスペースに関する考慮事項

階層状のネームスペースを使用している場合は、パス内のすべてのボリュームがミラーされたアグリゲートのみ、またはミラーされていないアグリゲートのみに配置されるようにジャンクションパスを設定する必要があります。ジャンクションパスにミラーされていないアグリゲートとミラーされたアグリゲートが混在していると、スイッチオーバー処理後にミラーされていないアグリゲートにアクセスできなくなる可能性があります。

ミラーされていないアグリゲート、 **CRS** メタデータボリューム、およびデータ **SVM** ルートボリュームに関する考慮事項

設定レプリケーションサービス（ CRS ）メタデータボリュームとデータ SVM ルートボリュームは、ミラーされたアグリゲートに配置する必要があります。これらのボリュームをミラーされていないアグリゲートに移動することはできませミラーされていないアグリゲートにある場合、ネゴシエートスイッチオーバー処理とスイッチバック処理が拒否されます。MetroCluster check コマンドは ' その場合に警告を表示します

ミラーされていないアグリゲートと **SVM** に関する考慮事項

SVM は、ミラーされたアグリゲートでのみ、またはミラーされていないアグリゲートでのみ設定してください。ミラーされていないアグリゲートとミラーされたアグリゲートが混在しているとスイッチオーバー処理に 2 分以上かかり、ミラーされていないアグリゲートがオンラインにならない場合にデータを利用できなくなることがあります。

LUN がミラーされていないアグリゲート上にないようにしてください。ミラーされていないアグリゲートに LUN を設定すると、スイッチオーバー処理が 120 秒を超え、データを利用できなくなる可能性があります。

MetroCluster FC 構成での自動計画外スイッチオーバー

MetroCluster FC 構成では、サイト全体のコントローラ障害が発生した場合に、特定の状況で自動計画外スイッチオーバー（ AUSO ）がトリガーされ、ノンストップオペレーションが実現します。必要に応じて、 AUSO を無効にすることができます。

MetroCluster IP 構成では、自動計画外スイッチオーバーはサポートされません。

MetroCluster FC 構成では、次の理由でサイトのすべてのノードに障害が発生した場合に AUSO がトリガーされます。

- 電源をオフにします
- 電源喪失
- パニック

8 ノード MetroCluster FC 構成では、 HA ペアの両方のノードで障害が発生した場合に AUSO をトリガーするオプションを設定できます。

2 ノード MetroCluster 構成ではローカル HA フェイルオーバーを使用できないため、システムが AUSO を実行してコントローラ障害発生後も処理が継続されるようにします。この機能は、 HA ペアの HA テイクオーバー機能に相当します。2 ノード MetroCluster 構成では、次のシナリオで AUSO がトリガーされます。

- ノードの電源がオフになりました
- ノードの電源が失われました
- ノードがパニック状態になった
- ノードがリブートしました

AUSO が実行されると、障害ノードの pool0 と pool1 のディスクの所有権が、 disaster recovery （ DR ；ディザスタリカバリ）パートナーに変更されます。この所有権の変更により、スイッチオーバー後にアグリゲートがデグレード状態に陥ることがなくなります。

自動スイッチオーバーが完了したら、修復処理とスイッチバック処理を手動で実行して、コントローラを通常動作に戻す必要があります。

2 ノード **MetroCluster** 構成でのハードウェアアシスト **AUSO**

2 ノード MetroCluster 構成では、コントローラモジュールのサービスプロセッサ（ SP ）が構成を監視します。一部のシナリオでは、 SP は ONTAP ソフトウェアよりも先に障害を検出します。その場合、 SP は AUSO をトリガーします。この機能は自動的に有効になります。

SP は、 DR パートナーとの間で SNMP トラフィックを送受信して健全性を監視します。

MetroCluster FC 構成での AUSO の設定の変更

デフォルトでは、AUSOは「auso-on-cluster-disaster」に設定されています。ステータスはで確認できます `metrocluster show` コマンドを実行します

AUSO の設定は MetroCluster IP 構成には適用されません。

AUSO を無効にするには、「 MetroCluster modify -auto-switchover-failure-domain auto-disabled 」コマンドを使用します。このコマンドは、 DR サイト全体のコントローラ障害時に AUSO がトリガーされないようにします。両方のサイトで AUSO を無効にする場合は、両方のサイトでコマンドを実行する必要があります。

AUSO を再度有効にするには、「 MetroCluster modify -auto-switchover-failure-domain auso-on-cluster-disaster 」コマンドを使用します。

AUSO は「 auso-on-dr-group-disaster 」に設定することもできます。この advanced レベルのコマンドは、 1 つのサイトで HA フェイルオーバーが実行されたときに AUSO をトリガーします。このコマンドは 'dr-group-disaster コマンドを使用して ' 両方のサイトで実行する必要があります MetroCluster modify-auto-switchover-failure-domain auso-on-dr-group-da`command を使用します

スイッチオーバー中の AUSO 設定

スイッチオーバーが発生すると AUSO 設定は無効になります。スイッチオーバー中のサイトを自動的にスイッチオーバーすることはできないためです。

AUSO からのリカバリ

AUSO からリカバリするには、計画されたスイッチオーバーの場合と同じ手順を実行します。

"テストまたはメンテナンスのためのスイッチオーバーの実行"

MetroCluster IP 構成でのメディエーターアシスト自動計画外スイッチオーバー

"MetroCluster IP構成での自動計画外スイッチオーバーのONTAPメディエーターによるサポートの詳細"。

修復時の動作（ MetroCluster FC 構成）

MetroCluster FC 構成での修復では、ミラーされたアグリゲートの再同期が実施され、修復されたディザスタサイトのノードがスイッチバックに向けて準備されます。計画的なイベントであるため、各手順を細かく制御してダウンタイムを最小限にすることができます。修復は、ストレージとコントローラのコンポーネントで発生する、 2 段階のプロセスです。

データアグリゲートの修復

ディザスタサイトでの問題が解決したら、ストレージ修復フェーズを開始します。

1. サバイバーサイトで、すべてのノードが稼働中であることを確認します。
2. ルートアグリゲートを含め、ディザスタサイトのプール 0 のすべてのディスクの所有権を変更します。

このフェーズでは、 RAID サブシステムがミラーされたアグリゲートを再同期し、 WAFL サブシステムが、スイッチオーバー時に pool1 プレックスで障害が発生したミラーされたアグリゲートの nvsave ファイルを再実行します。

一部のソースストレージコンポーネントで障害が発生した場合は、該当するレベル（ストレージ、サンダウン、 RAID ）でエラーが報告されます。

エラーが何も報告されない場合は、アグリゲートの再同期が完了しています。このプロセスは、完了までに数時間かかることがあります。

"構成の修復"

ルートアグリゲートの修復

アグリゲートが同期されたら、 CFO アグリゲートとルートアグリゲートをそれぞれの対応する DR パートナーに戻すことにより、コントローラの修復フェーズを開始します。

"構成の修復"

修復時の動作（ MetroCluster IP 構成）

MetroCluster IP 構成での修復では、ミラーされたアグリゲートの再同期が実施され、修復されたディザスタサイトのノードがスイッチバックに向けて準備されます。計画的なイベントであるため、各手順を細かく制御してダウンタイムを最小限にすることができます。修復は、ストレージとコントローラのコンポーネントで発生する、 2 段階のプロセスです。

MetroCluster FC 構成との違い

MetroCluster IP 構成では、修復処理を実行する前に、ディザスタサイトのクラスタ内のノードをブートする必要があります。

アグリゲートを再同期するときにリモートの iSCSI ディスクにアクセスできるように、ディザスタサイトのクラスタ内のノードが実行されている必要があります。

ディザスタサイトのノードが実行されていない場合、ディザスタノードは必要なディスク所有権の変更を実行できないため、修復処理が失敗します。

データアグリゲートの修復

ディザスタサイトでの問題が解決したら、ストレージ修復フェーズを開始します。

1. サバイバーサイトで、すべてのノードが稼働中であることを確認します。
2. ルートアグリゲートを含め、ディザスタサイトのプール 0 のすべてのディスクの所有権を変更します。

このフェーズでは、 RAID サブシステムがミラーされたアグリゲートを再同期し、 WAFL サブシステムが、スイッチオーバー時に pool1 プレックスで障害が発生したミラーされたアグリゲートの nvsave ファイルを再実行します。

一部のソースストレージコンポーネントで障害が発生した場合は、該当するレベル（ストレージ、サンダウン、 RAID ）でエラーが報告されます。

エラーが何も報告されない場合は、アグリゲートの再同期が完了しています。このプロセスは、完了までに数時間かかることがあります。

"構成の修復"

ルートアグリゲートの修復

アグリゲートが同期されたら、ルートアグリゲートの修復フェーズを実行します。MetroCluster IP 構成では、アグリゲートが修復されたことをこのフェーズで確認します。

"構成の修復"

スイッチオーバー後の **MetroCluster IP** 構成でのアグリゲートの自動修復

ONTAP 9.5 以降の MetroCluster IP 構成では、ネゴシエートスイッチオーバー処理の実行中に自動的に修復が実行されます。ONTAP 9.6 以降では、計画外スイッチオーバー後の自動修復がサポートされます。これにより 'MetroCluster heal-' コマンドを問題する必要がなくなります

ネゴシエートスイッチオーバー後の自動修復（ **ONTAP 9.5** 以降）

ネゴシエートスイッチオーバー（ -forced-on-disaster true オプションを指定せずにスイッチオーバーコマンドを実行）の実施後、システムを通常動作に戻すために必要な手順が自動修復機能によって実行されます。自動修復に対応したシステムでは、スイッチオーバー後に次の状況が発生します。

- ディザスタサイトのノードは稼働したままです。

  これらのノードはスイッチオーバーされているため、ローカルのミラーされたプレックスからはデータを提供していません。

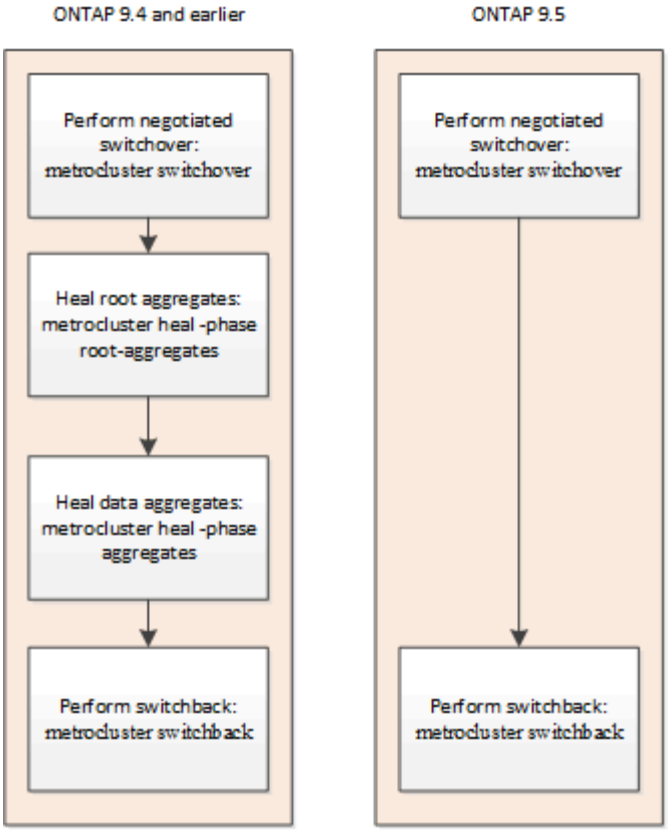
- 災害サイトのノードは「 Waiting for switchback 」状態に移行します。

  ディザスタサイトのノードのステータスは、 MetroCluster operation show コマンドを使用して確認できます。

- 修復コマンドを実行せずにスイッチバック処理を実行できます。

この機能は、 ONTAP 9.5 以降を実行する環境 MetroCluster IP 構成に対応しています。MetroCluster FC 構成には適用されません。

ONTAP 9.4 以前を実行する MetroCluster IP 構成では、引き続き手動で修復コマンドを実行する必要があります。



計画外スイッチオーバー後の自動修復（ **ONTAP 9.6** 以降）

ONTAP 9.6 以降を実行する MetroCluster IP 構成では、計画外スイッチオーバー後の自動修復がサポートされます。計画外のスイッチオーバーでは '-forced-on-disaster true オプションを指定して 'switchover コマンドを問題します

MetroCluster FC 構成では、計画外スイッチオーバー後の自動修復がサポートされません。また、 ONTAP 9.5 以前を実行する MetroCluster IP 構成では、計画外スイッチオーバー後に引き続き手動で修復コマンドを実行する必要があります。

ONTAP 9.6 以降を実行するシステムでは、計画外スイッチオーバー後に次の状況が発生します。

- 災害の規模によっては、ディザスタサイトのノードが停止する可能性があります。

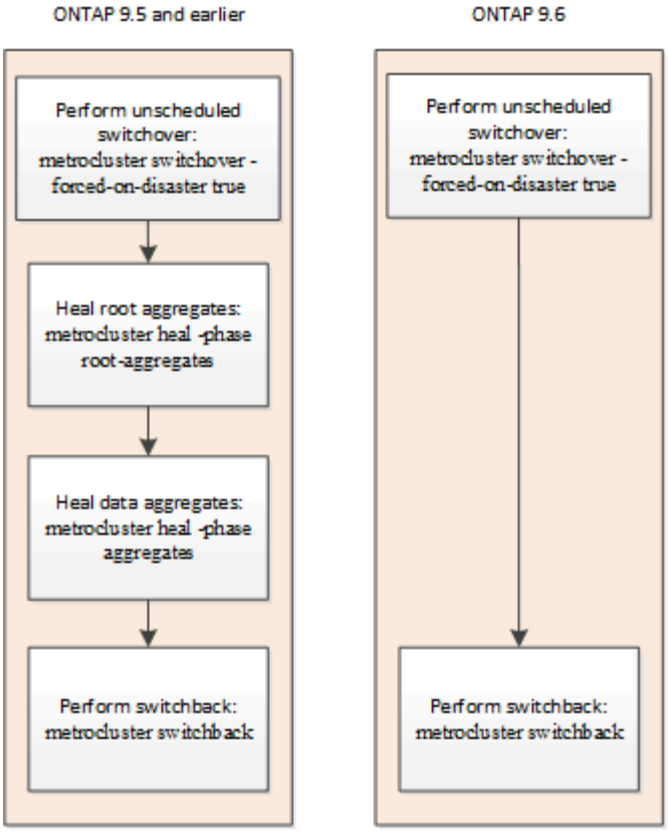
  これらのノードはスイッチオーバーされているため、電源が入っていてもローカルのミラーされたプレックスからはデータを提供していません。

- 災害サイトが停止した場合は、ブート時に災害サイトのノードが「 Waiting for switchback 」状態に移行します。

  災害サイトが稼働していた場合は ' ただちに Waiting for switchback 状態に移行します

- 修復処理が自動的に実行されます。

  MetroCluster operation show コマンドを使用すると ' 災害サイト・ノードのステータスと ' 修復処理が成功したことを確認できます



自動修復が失敗した場合

何らかの理由で自動修復操作が失敗した場合は、 ONTAP 9.6 より前の ONTAP バージョンで行われているように、「 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。

MetroCluster 構成用の SVM の作成

MetroCluster 構成用の SVM を作成して、 MetroCluster 構成用に設定されたクラスタのデータに対して同期ディザスタリカバリおよび高可用性を提供できます。

- 2 つのクラスタが MetroCluster 構成になっている必要があります。
- 両方のクラスタ内でアグリゲートが利用可能でオンラインになっている必要があります。
- 必要に応じて、両方のクラスタに同じ名前の IPspace を作成しておく必要があります。
- MetroCluster 構成を形成する一方のクラスタをスイッチオーバーを使用せずにリブートすると、同期元 SVM が「 started 」ではなく「 stopped 」とオンラインになることがあります。

MetroCluster 構成のどちらかのクラスタに SVM を作成すると、その SVM はソース SVM として作成されます。パートナー SVM は同じ名前で自動的に作成されますが、パートナークラスタには「 -mc 」というサフィックスが付きます。SVM 名にピリオドが含まれている場合、「 -mc 」サフィックスは最初のピリオドの前に適用されます。たとえば、 SVM-MC.DNS.NAME のようになります。

MetroCluster 構成では、 1 つのクラスタに 64 個の SVM を作成できます。MetroCluster 構成は最大 128 個の SVM をサポートします。

1. vserver create コマンドを使用します

   次の例は、ローカルサイトに「 sync-source 」のサブタイプの SVM と、パートナーサイトに「 sync-destination 」サブタイプの SVM を示しています。

   ```
   cluster_A::>vserver create -vserver vs4 -rootvolume vs4_root -aggregate
   aggr1
   -rootvolume-security-style mixed
   [Job 196] Job succeeded:
   Vserver creation completed
   ```

   ローカルサイトに SVM 「 vs4` 」が作成され、パートナーサイトに SVM 「 vs4-mc 」が作成されます。

2. 作成した SVM を表示します。

   ◦ ローカルクラスタで、 SVM の設定状態を確認します。

   MetroCluster vserver show

   次の例は、パートナー SVM とその設定状態を示しています。

   ```
   cluster_A::> metrocluster vserver show

                          Partner    Configuration
   Cluster     Vserver    Vserver    State
   ---------  --------  --------- ------------------
   cluster_A   vs4        vs4-mc     healthy
   cluster_B   vs1        vs1-mc     healthy
   ```

   ◦ ローカルクラスタとパートナークラスタから、新しく設定した SVM の状態を確認します。

   vserver show コマンド

   次の例は、 SVM の管理状態と運用状態を表示します。

```
cluster_A::> vserver show

                              Admin   Operational Root
Vserver Type  Subtype         State   State       Volume     Aggregate
------- ----- -------       ------- --------    -----------
----------
vs4     data  sync-source   running   running    vs4_root   aggr1

cluster_B::> vserver show

                                 Admin   Operational  Root
Vserver Type  Subtype            State   State        Volume
Aggregate
------- ----- -------            ------  ---------    -----------
----------
vs4-mc  data  sync-destination running stopped      vs4_root    aggr1
```

SVM の作成がルートボリュームの作成などの中間処理が原因で失敗した場合、 SVM が「 initializing 」の状態であると、 SVM の作成が失敗することがあります。その場合は、 SVM を削除して再度作成する必要があります。

MetroCluster 構成用の SVM が、 1GB のルートボリュームで作成されます。同期元 SVM の状態は「 running 」、同期先 SVM の状態は「 stopped 」です。

スイッチバック時の動作

ディザスタサイトがリカバリし、アグリゲートが修復されると、 MetroCluster のスイッチバックプロセスによって、ストレージアクセスとクライアントアクセスがディザスタリカバリサイトからホームクラスタに戻ります。

MetroCluster switchback コマンドは ' プライマリ・サイトを通常の完全な MetroCluster 動作に戻します設定に対する変更があった場合、元の SVM に反映されます。次に、データサーバ処理がディザスタサイトの同期元 SVM に返され、サバイバーサイトで動作していた同期先 SVM は非アクティブになります。

MetroCluster 構成がスイッチオーバー状態のときにサバイバーサイトで SVM が削除された場合、スイッチバックプロセスで次の処理が実行されます。

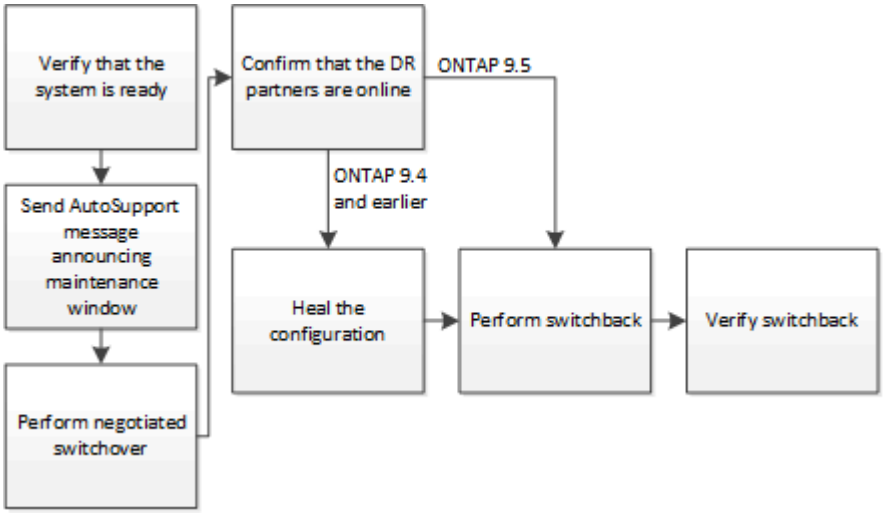
- パートナーサイト（元のディザスタサイト）の対応する SVM を削除する
- 削除された SVM にピアリング関係がある場合は削除する

スイッチオーバー、修復、スイッチバックを実行

テストやメンテナンスのためにスイッチオーバーを実行

テストまたはメンテナンスのためのスイッチオーバーの実行

MetroCluster 機能のテストや計画的メンテナンスを実行する場合は、一方のクラスタをパートナークラスタに完全にスイッチオーバーする、ネゴシエートスイッチオーバーを実行します。その後、構成を修復してスイッチバックします。



ONTAP 9.6 以降では、 ONTAP System Manager を使用して MetroCluster IP 構成でスイッチオーバーとスイッチバックの処理を実行できます。

MetroCluster構成がスイッチオーバー状態の場合の制限事項

システムがスイッチオーバー中のときは、一部の処理を実行しないでください。システムがスイッチオーバー中の場合の制限された処理について説明します。

スイッチオーバー時の制限された処理

システムがスイッチオーバー状態の場合、次の処理はサポートされません。

- アグリゲートおよびボリュームの作成または削除
- SVMの作成または削除
- LIFの作成または削除
- ディスクの追加または削除（リカバリ手順の一環として交換する場合のみ）
- SnapMirror SVM DRに対する設定変更の実行
- 既存のブロードキャストドメインの変更または新しいブロードキャストドメインの作成
- ネットワークサブネットの変更

スイッチオーバー時のハードウェアの交換

システムがスイッチオーバー中の場合は、次の手順に従ってコントローラハードウェアを交換します。

- スイッチオーバー中でないサイトで同じタイプのコントローラを交換する必要がある場合は、の手順に従ってください"マルチコントローラまたはストレージの障害からリカバリする"。
  - サバイバーサイトでノードのスイッチオーバー中にコントローラモジュールとシャーシを交換する必要がある場合は、両方のコントローラをシャットダウンしてから、の手順を実行します"マルチコントローラまたはストレージの障害からリカバリする"。
- コントローラを別のタイプのコントローラに交換する必要がある場合は、の構成に応じた手順に従ってください"コントローラのアップグレード手順 を選択します"。
  - コントローラ障害が原因でシステムのスイッチオーバーが発生した場合やスイッチオーバー中にコントローラ障害が発生した場合は、まずコントローラハードウェアを交換し、スイッチバックを実行してからコントローラのアップグレードを実行する必要があります。
    i. コントローラハードウェアを交換してスイッチバックを実行するには、次の手順に従います。"マルチコントローラまたはストレージの障害からリカバリする"
    ii. ハードウェアを交換したら、の手順に従ってコントローラのアップグレードを実行します"コントローラのアップグレード手順 を選択します"。

スイッチオーバーに向けたシステムの事前チェック

--simulate オプションを使用して ' スイッチオーバー操作の結果をプレビューできますこれにより、処理を開始する前に、処理が成功するために必要なほとんどの前提条件が満たされていることを確認できます。問題：稼働したままになる、サイトからの次のコマンド。

1. 権限レベルを advanced に設定します。「 set -privilege advanced 」
2. 稼働したままになるサイトから ' スイッチオーバー操作をシミュレートします MetroCluster switchover-simulate
3. 返された出力を確認します。

   出力には、スイッチオーバー処理を阻止する拒否の有無が示されます。MetroCluster 処理を実行するたびに、処理が成功するための一連の条件を確認する必要があります。「 "" まで」は、 1 つ以上の条件が満たされない場合に操作を禁止するメカニズムです。拒否には「ソフト」と「ハード」の 2 種類があります。ソフトな拒否は無視できますが、ハードな拒否は無視できません。たとえば、 4 ノード MetroCluster 構成でネゴシエートスイッチオーバーを実行する場合、条件の 1 つとしてすべてのノードが正常に稼働していることがあります。たとえば、 1 つのノードが停止し、 HA パートナーにテイクオーバーされたとします。すべてのノードが正常に稼働している必要があるという条件はハードな条件であるため、スイッチオーバー処理にはハードな拒否が適用されます。ハードな拒否は無視できません。

   拒否は無視しないことを推奨します。

例：検証結果

次の例は、スイッチオーバー処理のシミュレーションで発生したエラーを示しています。

```
cluster4::*> metrocluster switchover -simulate

[Job 126] Preparing the cluster for the switchover operation...
[Job 126] Job failed: Failed to prepare the cluster for the switchover
operation. Use the "metrocluster operation show" command to view detailed
error
information. Resolve the errors, then try the command again.
```

障害が発生したすべてのディスクを交換するまで、ネゴシエートスイッチオーバーとスイッチバックは失敗します。障害が発生したディスクを交換したあとにディザスタリカバリを実行できます。障害が発生したディスクに関する警告を無視するには、ネゴシエートスイッチオーバーとスイッチバックにソフトな拒否を追加します。

カスタム **AutoSupport** メッセージの送信 **-** ネゴシエートスイッチオーバー前

ネゴシエートスイッチオーバーを実行する前に、 AutoSupport メッセージを問題で送信して、メンテナンスが進行中であることをネットアップテクニカルサポートに通知する必要があります。ネゴシエートスイッチオーバーでは、プレックスや MetroCluster の処理が失敗して AutoSupport メッセージがトリガーされることがあります。システム停止が発生したとみなしてテクニカルサポートがケースをオープンしないように、メンテナンスが進行中であることを通知する必要があります。

このタスクは MetroCluster サイトごとに実行する必要があります。

手順

1. Site_A のクラスタにログインします
2. メンテナンスの開始を示す AutoSupport メッセージを起動します。「 system node AutoSupport invoke -node * -type all -message MAINT= maintenance-window-in-hours

   maintenance-window-in-hours にはメンテナンス時間の長さを指定します。最大値は 72 時間です。この時間が経過する前にメンテナンスが完了した場合は、メンテナンス期間が終了したことを示すコマンドを問題に送信できます。「 system node AutoSupport invoke -node * -type all -message MAINT=end 」
3. 同じ手順をパートナーサイトでも実行します。

ネゴシエートスイッチオーバーの実行

ネゴシエートスイッチオーバーは、パートナーサイトのプロセスをクリーンシャットダウンしてから、パートナーサイトの処理をスイッチオーバーします。ネゴシエートスイッチオーバーは、 MetroCluster サイトでのメンテナンスの実施、またはスイッチオーバー機能のテストに使用できます。

- スイッチバック処理を実行する前に、設定の変更がすべて完了している必要があります。

  これにより、ネゴシエートスイッチオーバーまたはスイッチバックの処理との競合が回避されます。

- 停止していたノードがブートし、クラスタクォーラムに参加している必要があります。

  クラスタ・クォーラムの詳細については ' 定足数と Epsilon についての項を参照してください

  "システム管理"

- 両方のサイトからクラスタピアリングネットワークにアクセスできる必要があります。
- MetroCluster 構成のすべてのノードで、同じバージョンの ONTAP ソフトウェアが実行されている必要があります。
- 新しい SnapMirror 関係を作成する前に、 MetroCluster 構成の両方のサイトで replication.create_data_protection_rels.enable オプションを ON に設定しておく必要があります。
- 2 ノード MetroCluster 構成の場合、サイト間で ONTAP のバージョンが一致していないときは、アップグレード時に新しい SnapMirror 関係を作成しないようにする必要があります。
- 4 ノード MetroCluster 構成の場合、サイト間で ONTAP のバージョンが一致している必要があります。

リカバリサイトがスイッチバック処理を実行できるようになるまでに数時間かかることがあります。

MetroCluster switchover コマンドは、 MetroCluster 構成のすべての DR グループで、ノードをスイッチオーバーします。たとえば、 8 ノードの MetroCluster 構成では、両方の DR グループでノードがスイッチオーバーされます。

ネゴシエートスイッチオーバーの準備中および実行中は、クラスタの設定を変更したり、テイクオーバーまたはギブバック処理を実行したりしないでください。

MetroCluster FC 構成の場合：

- 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。
- 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。

MetroCluster IP 構成の場合：

> メンテナンスタスクを実行する前に、 Tiebreaker またはメディエーターユーティリティで MetroCluster 設定を監視している場合は、監視を解除する必要があります。"メンテナンス作業を実行する前に、 ONTAP メディエーターまたは Tiebreaker の監視を削除します"

- 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。

i. MetroCluster check run 、 MetroCluster check show 、および MetroCluster check config-replication show の各コマンドを使用して、進行中または保留中の設定更新がないことを確認します。問題：稼働したままにするサイトからのコマンドです。

ii. 稼働したままにするサイトから ' スイッチオーバーを実行します MetroCluster switchover

この処理が完了するまでに数分かかることがあります。

iii. スイッチオーバーの完了を監視します MetroCluster operation show

```
cluster_A::*> metrocluster operation show
  Operation: Switchover
 Start time: 10/4/2012 19:04:13
      State: in-progress
   End time: -
     Errors:

cluster_A::*> metrocluster operation show
  Operation: Switchover
 Start time: 10/4/2012 19:04:13
      State: successful
   End time: 10/4/2012 19:04:22
     Errors: -
```

iv. SnapMirror 構成または SnapVault 構成があれば、再確立します。

SVMが実行されていて、アグリゲートがオンラインになっていることを確認してください

スイッチオーバーが完了したら、 DR パートナーがディスクの所有権を取得し、パートナー SVM がオンラインになったことを確認する必要があります。

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。

手順

1. storage aggregate show コマンドを使用して、アグリゲートがスイッチオーバーされたことを確認します。

この例では、アグリゲートがスイッチオーバーされています。ルートアグリゲート（ aggr0_b2 ）はデグレード状態、データアグリゲート（ b2_aggr2 ）はミラーされた正常な状態になっています。

```
cluster_A::*> storage aggregate show

.
.
.
mcc1-b Switched Over Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
aggr0_b2    227.1GB   45.1GB    80% online       0 node_A_1
raid_dp,

mirror

degraded
b2_aggr1    227.1GB   200.3GB    20% online       0 node_A_1
raid_dp,

mirrored

normal
```

2. vserver show コマンドを使用して、セカンダリ SVM がオンラインになったことを確認します。

   この例では、これまで休止状態だったセカンダリサイトの同期先 SVM がアクティブで、 Admin State は running になっています。

```
cluster_A::*> vserver show
                                        Admin      Operational  Root
Name    Name
Vserver           Type  Subtype         State      State        Volume
Aggregate  Service Mapping
-----------       ----- ----------      ---------- -----------
--------- ---------- ------- -------
...
cluster_B-vs1b-mc data   sync-destination  running   running
vs1b_vol   aggr_b1   file    file
```

構成を修復

MetroCluster FC 構成の構成を修復します

スイッチオーバーに続いて、特定の順序で修復処理を実行して MetroCluster 機能をリストアする必要があります。

- スイッチオーバーを実行済みで、サバイバーサイトがデータを提供している必要があります。
- ディザスタサイトのノードが停止しているか、電源がオフのままになっている必要があります。

  修復プロセスでは、これらのノードを完全にブートしないでください。

- ディザスタサイトのストレージにアクセスできる（シェルフは電源がオンで稼働しており、アクセス可能である）必要があります。
- ファブリック接続 MetroCluster 構成では、スイッチ間リンク（ ISL ）が稼働している必要があります。
- 4 ノード MetroCluster 構成では、サバイバーサイトのノードが HA フェイルオーバー状態でない（各 HA ペアのすべてのノードが稼働中である）必要があります。

修復処理は、最初にデータアグリゲートで実行し、次にルートアグリゲートで実行する必要があります。

ネゴシエートスイッチオーバー後のデータアグリゲートの修復

メンテナンスまたはテストが完了したら、データアグリゲートを修復する必要があります。この処理では、データアグリゲートを再同期し、ディザスタサイトを通常の動作用に準備します。データアグリゲートの修復は、ルートアグリゲートの修復の前に行う必要があります。

リモートクラスタでの構成の更新はすべてローカルクラスタにレプリケートされます。この手順の一部としてディザスタサイトのストレージに電源を投入しますが、ディザスタサイトにあるコントローラモジュールの電源はオンにしないでください。

手順

1. MetroCluster operation show コマンドを実行して、スイッチオーバーが完了していることを確認します。

```
controller_A_1::> metrocluster operation show
  Operation: switchover
      State: successful
 Start Time: 7/25/2014 20:01:48
   End Time: 7/25/2014 20:02:14
     Errors: -
```

2. サバイバークラスタから MetroCluster heal-phase aggregates コマンドを実行して、データアグリゲートを再同期します。

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

修復が拒否された場合は、 -override-vetoes パラメータを指定して MetroCluster heal コマンドを再実行で

きます。このオプションパラメータを使用すると、修復処理を妨げるソフトな拒否はすべて無視されます。

3. MetroCluster operation show コマンドを実行して、処理が完了したことを確認します。

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2014 18:45:55
   End Time: 7/25/2014 18:45:56
     Errors: -
```

4. storage aggregate show コマンドを実行して、アグリゲートの状態を確認します。

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

5. ディザスタサイトのストレージを交換した場合は、アグリゲートの再ミラーリングが必要になることがあります。

ネゴシエートスイッチオーバー後のルートアグリゲートの修復

データアグリゲートの修復が完了したら、スイッチバック処理に備えてルートアグリゲートを修復する必要があります。

MetroCluster 修復プロセスのデータアグリゲートの修復が完了している必要があります。

手順

1. MetroCluster heal-phase root-aggregates コマンドを実行して、ミラーされたアグリゲートをスイッチバックします。

```
cluster_A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

修復が拒否された場合は、 -override-vetoes パラメータを指定して MetroCluster heal コマンドを再実行できます。このオプションパラメータを使用すると、修復処理を妨げるソフトな拒否はすべて無視されます。

2. 正常なクラスタで MetroCluster operation show コマンドを実行して、修復処理が完了したことを確認します。

```
cluster_A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2014 20:54:41
   End Time: 7/29/2014 20:54:42
     Errors: -
```

3. 正常なサイトで次のコマンドを実行して、ディザスタサイトに障害が発生したディスクがないかどうかを確認し、ある場合は取り外します。「 Disk show -broken 」
4. ディザスタサイトの各コントローラモジュールの電源をオンにするか、ブートします。

   システムに LOADER プロンプトが表示されたら、「 boot_ontap 」コマンドを実行します。

5. ノードがブートしたら、ルートアグリゲートがミラーされていることを確認します。

   両方のプレックスが存在する場合は、プレックスが同期されていないと自動的に再同期が実行されます。1 つのプレックスで障害が発生している場合は、そのプレックスを削除してから、 storage aggregate mirror -aggregate aggregate-name コマンドを使用してミラー関係を再確立し、ミラーを再作成する必要があります。

MetroCluster IP 構成での構成の修復（ **ONTAP 9.4** 以前）

スイッチバック処理の準備として、アグリゲートを修復する必要があります。

ONTAP 9.5 を実行している MetroCluster IP システムでは、自動的に修復が実行されるため、これらのタスクを省略できます。

修復手順を実行するには、次の条件を満たしている必要があります。

- スイッチオーバーを実行済みで、サバイバーサイトがデータを提供している必要があります。
- ディザスタサイトのストレージシェルフの電源がオンで稼働しており、アクセス可能である必要があります。
- ISL が稼働中である必要があります。
- サバイバーサイトのノードが HA フェイルオーバー状態でない（両方のノードが稼働中である）必要があります。

このタスクでは、 ONTAP 9.5 より前のバージョンを実行している環境 MetroCluster IP 構成のみを行います。

この手順は、 MetroCluster FC 構成の修復手順とは異なります。

手順

1. スイッチオーバーされたサイトの各コントローラモジュールの電源をオンにして、完全にブートします。

   システムに LOADER プロンプトが表示されたら、「 boot_ontap 」コマンドを実行します。

2. ルートアグリゲートの修復フェーズ「 MetroCluster heal root-aggregates 」を実行します

```
cluster_A::> metrocluster heal root-aggregates
[Job 137] Job succeeded: Heal Root-Aggregates is successful
```

修復が拒否された場合は、 MetroCluster heal-rootaggregates コマンドを --override-vetoes パラメータで再実行できます。このオプションパラメータを使用すると、修復処理を妨げるソフトな拒否はすべて無視されます。

3. アグリゲートを再同期します。「 MetroCluster heal aggregates 」

```
cluster_A::> metrocluster heal aggregates
[Job 137] Job succeeded: Heal Aggregates is successful
```

修復が拒否された場合は、 -override-vetoes パラメータを指定して MetroCluster heal コマンドを再実行できます。このオプションパラメータを使用すると、修復処理を妨げるソフトな拒否はすべて無視されます。

4. 正常なクラスタで MetroCluster operation show コマンドを実行して、修復処理が完了したことを確認します。

```
cluster_A::> metrocluster operation show
  Operation: heal-aggregates
      State: successful
 Start Time: 7/29/2017 20:54:41
   End Time: 7/29/2017 20:54:42
     Errors: -
```

スイッチバックを実行しています

MetroCluster 構成の修復が完了したら、 MetroCluster のスイッチバック処理を実行できます。MetroCluster のスイッチバック処理を実行すると、構成が通常の動作状態に戻ります。ディザスタサイトにある同期元の Storage Virtual Machine （ SVM ）がアクティブになり、ローカルディスクプールからデータを提供します。

- ディザスタクラスタからサバイバークラスタへのスイッチオーバーが正常に完了している必要があります。
- データアグリゲートとルートアグリゲートに対して修復が実行されている必要があります。
- サバイバークラスタノードが HA フェイルオーバー状態ではない（各 HA ペアのすべてのノードが稼働中である）必要があります。
- ディザスタサイトのコントローラモジュールが完全にブートしていること、および HA テイクオーバーモードでないことが必要です。
- ルートアグリゲートがミラーされている必要があります。
- スイッチ間リンク（ ISL ）がオンラインになっている必要があります。

- 必要なライセンスがシステムにインストールされている必要があります。

a. すべてのノードが enabled 状態であることを確認します MetroCluster node show

次の例は、ノードが有効な状態であることを表示します。

```
cluster_B::>  metrocluster node show

DR                         Configuration  DR
Group Cluster Node         State          Mirroring Mode
----- ------- ----------- -------------- ---------
--------------------
1     cluster_A
              node_A_1    configured     enabled   heal roots
completed
              node_A_2    configured     enabled   heal roots
completed
      cluster_B
              node_B_1    configured     enabled   waiting for
switchback recovery
              node_B_2    configured     enabled   waiting for
switchback recovery
4 entries were displayed.
```

b. すべての SVM で再同期が完了したことを確認します。「 MetroCluster vserver show 」

c. 修復処理によって実行される LIF の自動移行が正常に完了したことを確認します。 MetroCluster check lif show

d. シミュレートされたスイッチバックを実行して、システムが「 MetroCluster switchback -simulate 」状態であることを確認します

e. 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
Last Checked On: 9/13/2018 20:41:37

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         ok
6 entries were displayed.
```

f. サバイバークラスタ内の任意のノードから MetroCluster switchback コマンドを実行して、スイッチバックを実行します。 MetroCluster switchback

g. スイッチバック操作の進行状況を確認します MetroCluster show

出力に waiting-for-switchback と表示された場合は、スイッチバック処理がまだ進行中です。

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                switchover
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                waiting-for-switchback
                          AUSO Failure Domain -
```

出力に normal と表示された場合、スイッチバック処理は完了しています。

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
```

+
スイッチバックが完了するまでに時間がかかる場合は、「 MetroCluster config-replication resync-status

show 」コマンドを使用することで、進行中のベースラインのステータスを確認できます。このコマンドは、 advanced 権限レベルで実行します。

a. SnapMirror 構成または SnapVault 構成があれば、再確立します。

   ONTAP 8.3 では、失われた SnapMirror 構成を MetroCluster スイッチバック処理のあとに手動で再確立する必要があります。ONTAP 9.0 以降では、関係が自動的に再確立されます。

スイッチバックが成功したことを確認する

スイッチバックの実行後に、すべてのアグリゲートと Storage Virtual Machine （ SVM ）がスイッチバックされてオンラインになっていることを確認します。

1. スイッチオーバーされたデータアグリゲートがスイッチバックされたことを確認します。

   「 storage aggregate show

   次の例では、ノード B2 の aggr_b2 がスイッチバックされています。

```
node_B_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 node_B_2   raid_dp,

mirrored,

normal
```

2. サバイバークラスタの同期先のすべてのSVMが休止状態であることを確認します（動作状態が「 stopped」と表示されています）。

   vserver show -subtype sync-destination

```
node_B_1::> vserver show -subtype sync-destination
                                 Admin    Operational  Root
Vserver       Type    Subtype    State    State        Volume
Aggregate
-----------   ------- ---------- -------- ----------   --------
----------
...
cluster_A-vs1a-mc data sync-destination
                               running    stopped    vs1a_vol   aggr_b2
```

MetroCluster 構成の同期先アグリゲートの名前には、識別しやすいように「 -mc 」というサフィックスが自動的に付加されます。

3. ディザスタクラスタの同期元SVMが稼働していることを確認します。

「 vserver show -subtype sync-source 」のようになります

```
node_A_1::> vserver show -subtype sync-source
                                  Admin    Operational  Root
Vserver        Type    Subtype    State    State        Volume
Aggregate
-----------    ------- ---------- -------- ----------   --------
----------
...
vs1a           data    sync-source
                                  running  running    vs1a_vol  aggr_b2
```

4. MetroCluster operation show コマンドを使用して、スイッチバック操作が成功したことを確認します。

出力内容	作業
スイッチバック処理の状態が「 successful 」である	スイッチバックプロセスは完了しており、システムの処理を続行できます。
スイッチバック処理またはスイッチバック継続エージェントの処理が「 partially successful 」である	MetroCluster operation show コマンドの出力に記載されている推奨修正を実行します

上記の手順を繰り返して、逆方向へのスイッチバックを実行する必要があります。site_A が site_B のスイッチオーバーを行った場合は、 site_B で site_A のスイッチオーバーを行います

スイッチオーバー、修復、スイッチバック用のコマンドです

ONTAP には、 MetroCluster のディザスタリカバリプロセスを実行するためのコマンドが用意されています。

状況	使用するコマンド
スイッチオーバーでエラーや拒否が発生しないことを確認します。	MetroCluster switchover -simulate + を advanced 権限レベルで実行します
スイッチバックを実行してもエラーや拒否が発生しないことを確認します。	MetroCluster switchback -simulate + at the advanced privilege level

パートナーノードにスイッチオーバーする（ネゴシエートスイッチオーバー）	MetroCluster スイッチオーバー
パートナーノードにスイッチオーバーする（強制スイッチオーバー）	MetroCluster switchover -forced-on-disaster true
データアグリゲートの修復を実行する	「 MetroCluster heal-phase aggregates 」
ルートアグリゲートの修復を実行する	「 MetroCluster heal-phase root-aggregates 」
ホームノードにスイッチバックする	MetroCluster スイッチバック

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）

メンテナンスを実施したり、問題からリカバリしたりするために、あるMetroCluster IPサイトから別のサイトに制御を切り替えることができます。

スイッチオーバーとスイッチバックの手順は、MetroCluster IP構成でのみサポートされます。

スイッチオーバーとスイッチバックの概要

スイッチオーバーには次の2つのタイプがあります。

- * 計画的スイッチオーバー *

  このスイッチオーバーは、システム管理者がSystem Managerを使用して開始します。計画的スイッチオーバーでは、ローカルクラスタのシステム管理者が制御を切り替えることで、リモートクラスタのデータサービスがローカルクラスタで処理されるようになります。これにより、リモートクラスタの場所にあるシステム管理者がリモートクラスタでメンテナンスを実行できるようになります。

- * 計画外スイッチオーバー *

  MetroClusterクラスタが停止した場合やクラスタ間の接続が停止した場合、ONTAPによってスイッチオーバーが自動的に開始されるため、停止したクラスタのデータ処理が実行中のクラスタで処理されます。

  一方のクラスタのステータスをONTAPが判断できない場合は、稼働しているサイトのシステム管理者がスイッチオーバーを開始して、もう一方のサイトのデータ処理を制御します。

どのタイプのスイッチオーバー手順の場合も、 _switchback プロセスを使用してデータサービス機能がクラスタに返されます。

実行するスイッチオーバーとスイッチバックのプロセスは、ONTAPのバージョンによって異なります。

- ONTAP 9.6または9.7のSystem Managerを使用してスイッチオーバーとスイッチバックを実行
- ONTAP 9.8以降のSystem Managerを使用してスイッチオーバーとスイッチバックを行う

ONTAP 9.6または9.7のSystem Managerを使用してスイッチオーバーとスイッチバックを実行

手順

1. ONTAP 9.6または9.7でSystem Managerにログインします。
2. *（クラシックバージョンに戻る）*をクリックします。
3. [設定]>[MetroCluster]*をクリックします。

   ネゴシエートスイッチオーバーが可能かどうかが検証されます。

4. 検証プロセスが完了したら、次のいずれかの手順を実行します。
   a. 検証に失敗し、サイトBが稼働している場合、エラーが発生しています。たとえば、サブシステムに問題があるか、NVRAMミラーリングが同期されていないことが考えられます。
      i. エラーの原因となっている問題を修正し、*[閉じる]*をクリックして、手順2からやり直します。
      ii. サイトBのノードを停止し、*[閉じる]*をクリックして、の手順を実行します "計画外スイッチオーバーの実行"。
   b. 検証が失敗し、サイトBが停止している場合は、接続に問題がある可能性があります。サイトBが停止していることを確認し、の手順を実行します"計画外スイッチオーバーの実行"。
5. [サイトBからサイトAへのスイッチオーバー]*をクリックしてスイッチオーバープロセスを開始します。
6. [新しいエクスペリエンスに切り替える]*をクリックします。

ONTAP 9.8以降のSystem Managerを使用してスイッチオーバーとスイッチバックを行う

計画的スイッチオーバーの実行（**ONTAP 9.8**以降）

手順

1. ONTAP 9.8以降でSystem Managerにログインします。
2. 「 * ダッシュボード * 」を選択します。「 * MetroCluster * 」セクションには、 2 つのクラスタが接続されています。
3. ローカルクラスタ（左側に表示）で、をクリック ⋮ し、*[リモートデータサービスをローカルサイトにスイッチオーバーする]*を選択します。

   スイッチオーバー要求が検証されると、リモートサイトからローカルサイトに制御が移されます。ローカルサイトが両方のクラスタに対してデータサービス要求を実行します。

   リモートクラスタはリブートしますが、ストレージコンポーネントはアクティブではなく、クラスタはデータ要求を処理しません。計画的なメンテナンスのために利用できるようになりました。

スイッチバックを実行するまでリモートクラスタをデータサービスに使用しないでください。

計画外スイッチオーバーの実行（**ONTAP 9.8**以降）

計画外スイッチオーバーは、ONTAPによって自動的に開始される場合があります。ONTAPでスイッチバックが必要かどうかを判断できない場合は、実行中のMetroClusterサイトのシステム管理者が次の手順でスイッチオーバーを開始します。

手順

1. ONTAP 9.8以降でSystem Managerにログインします。
2. 「 * ダッシュボード * 」を選択します。

   MetroCluster *セクションでは、2つのクラスタ間の接続に「X」が表示されます。これは、接続を検出できず、接続またはクラスタのいずれかが停止していることを意味します。

3. ローカルクラスタ（左側に表示）で、をクリック し、*[リモートデータサービスをローカルサイトにスイッチオーバーする]*を選択します。

   スイッチオーバーがエラーで失敗した場合は、エラーメッセージの[詳細を表示]リンクをクリックして、計画外スイッチオーバーを確認します。

   スイッチオーバー要求が検証されると、リモートサイトからローカルサイトに制御が移されます。ローカルサイトが両方のクラスタに対してデータサービス要求を実行します。

   クラスタを再度オンラインにするには、クラスタを修復する必要があります。

オンラインになったリモートクラスタは、スイッチバックを実行するまでデータサービスに使用しないでください。

スイッチバックの実行（**ONTAP 9.8**以降）

作業を開始する前に

計画的なメンテナンスや災害が原因でリモートクラスタが停止していた場合は、リモートクラスタが稼働中で、スイッチバックを待機している必要があります。

手順

1. ローカルクラスタで、ONTAP 9.8以降のSystem Managerにログインします。
2. 「 * ダッシュボード * 」を選択します。

   「 * MetroCluster * 」セクションには、 2 つのクラスタが表示されます。

3. ローカルクラスタ（左側に表示）でをクリックし 、*[Take back control]*を選択します。

   データは_healed_firstで、両方のクラスタ間でデータが同期およびミラーリングされていることを確認します。

4. データの修復が完了したら、をクリックし 、*[スイッチバックの開始]*を選択します。

   スイッチバックが完了すると、両方のクラスタがアクティブになり、データ要求を処理します。さらに、

データがミラーリングされ、クラスタ間で同期されています。

MetroCluster 設定を監視する

ONTAP MetroCluster コマンドと Active IQ Unified Manager （旧 OnCommand Unified Manager ）を使用して、各種ソフトウェアコンポーネントの健常性および MetroCluster 処理の状態を監視できます。

MetroCluster の設定を確認しています

MetroCluster 構成内のコンポーネントおよび関係が正しく機能していることを確認できます。チェックは、初期設定後と、 MetroCluster 設定に変更を加えたあとに実施する必要があります。また、ネゴシエート（計画的）スイッチオーバーやスイッチバックの処理の前にも実施します。

このタスクについて

いずれかまたは両方のクラスタに対して短時間に MetroCluster check run コマンドを 2 回発行すると ' 競合が発生し ' コマンドがすべてのデータを収集しない場合がありますそれ以降の「 MetroCluster check show 」コマンドでは、期待される出力が表示されません。

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"
   ```

2. 最新の MetroCluster check run コマンドから ' より詳細な結果を表示します

   MetroCluster check aggregate show

   MetroCluster check cluster show

   MetroCluster check config-replication show

   MetroCluster check lif show

   MetroCluster check node show

   「 MetroCluster check show 」コマンドは、最新の「 MetroCluster check run 」コマンドの結果を表示します。MetroCluster check show コマンドを使用する前に ' 必ず MetroCluster check run コマンドを実行し

て ' 表示されている情報が最新であることを確認してください

次に、正常な 4 ノード MetroCluster 構成の MetroCluster check aggregate show コマンドの出力例を示します。

```
cluster_A::> metrocluster check aggregate show

Last Checked On: 8/5/2014 00:42:58

Node                  Aggregate                 Check
Result
---------------       --------------------      ---------------------
---------
controller_A_1        controller_A_1_aggr0
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
ok
                      controller_A_1_aggr1
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
ok
                      controller_A_1_aggr2
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
ok


controller_A_2        controller_A_2_aggr0
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
ok
                      controller_A_2_aggr1
                                                mirroring-status
ok
```

```
                                                    disk-pool-allocation
ok
                                                    ownership-state
ok
                      controller_A_2_aggr2
                                                    mirroring-status
ok
                                                    disk-pool-allocation
ok
                                                    ownership-state
ok

18 entries were displayed.
```

次に、正常な 4 ノード MetroCluster 構成の MetroCluster check cluster show コマンドの出力例を示します。この出力は、必要に応じてネゴシエートスイッチオーバーを実行できる状態であることを示しています。

```
Last Checked On: 9/13/2017 20:47:04

Cluster               Check                          Result
--------------------- ------------------------------ ---------
mccint-fas9000-0102
                      negotiated-switchover-ready    not-applicable
                      switchback-ready               not-applicable
                      job-schedules                  ok
                      licenses                       ok
                      periodic-check-enabled         ok
mccint-fas9000-0304
                      negotiated-switchover-ready    not-applicable
                      switchback-ready               not-applicable
                      job-schedules                  ok
                      licenses                       ok
                      periodic-check-enabled         ok
10 entries were displayed.
```

MetroCluster 設定を確認および監視するためのコマンド

ONTAP には、 MetroCluster 構成を監視し、 MetroCluster 処理を確認するためのコマンドが用意されています。

MetroCluster 処理を確認するためのコマンド

状況	使用するコマンド

MetroCluster 処理のチェックを実行します。 • 注：このコマンドは、 DR 処理実行前のシステムの事前検証に使用できるコマンドとしては使用しないでください。	「 MetroCluster check run 」のようになります
MetroCluster 処理に対する前回のチェック結果を表示する	「 MetroCluster show 」
サイト間の設定レプリケーションに対するチェック結果を表示する	「 MetroCluster check config-replication show MetroCluster check config-replication show-aggregate-eligibility -
ノード設定に対するチェック結果を表示する	MetroCluster check node show
アグリゲート設定に対するチェック結果を表示する	MetroCluster check aggregate show
MetroCluster 構成の LIF 配置エラーを表示する	MetroCluster check lif show

MetroCluster インターコネクトの監視用コマンドです

状況	使用するコマンド
HA および DR のミラーリングステータスと、クラスタ内の MetroCluster ノードに関する情報を表示する	MetroCluster interconnect mirror show

MetroCluster SVM の監視用コマンド

状況	使用するコマンド
MetroCluster 構成の両方のサイトにあるすべての SVM を表示する	MetroCluster vserver show

MetroCluster Tiebreaker または ONTAP メディエーターを使用して設定を監視する

を参照してください "ONTAP メディエーターと MetroCluster Tiebreaker の違い" MetroCluster 構成を監視する方法と自動スイッチオーバーを開始する方法の違いを理解するために、

Tiebreaker またはメディエーターをインストールおよび設定するには、次のリンクを使用します。

- "MetroCluster Tiebreaker ソフトウェアをインストールして設定します。"
- "ONTAPメディエーターのインストール準備"

NetApp MetroCluster Tiebreaker ソフトウェアで障害を検出する方法

Tiebreaker ソフトウェアは Linux ホストにインストールされます。Tiebreaker ソフトウェアは、 2 つのクラス

タおよびクラスタ間の接続ステータスを第 3 のサイトから監視する場合にのみ使用します。これにより、サイト間リンクが停止した場合に、クラスタ内の各パートナーで ISL 障害とサイト障害を区別することができます。

Linux ホストに Tiebreaker ソフトウェアをインストールしたら、災害状況を監視するように MetroCluster 構成内のクラスタを設定できます。

Tiebreaker ソフトウェアでサイト間接続障害を検出する方法

MetroCluster Tiebreaker ソフトウェアは、サイト間のすべての接続が失われると警告します。

ネットワークパスのタイプ

構成によっては、 MetroCluster 構成の 2 つのクラスタ間のネットワークパスに次の 3 つの種類が存在します。

- * FC ネットワーク（ファブリック接続 MetroCluster 構成に存在） *

  この種類のネットワークは、 2 つの冗長 FC スイッチファブリックで構成されます。各スイッチファブリックには 2 つの FC スイッチがあり、各スイッチファブリックの 1 つのスイッチはクラスタと同じ場所に配置されます。各クラスタには、各スイッチファブリックから 1 つずつ、 2 つの FC スイッチがあります。すべてのノードは、同じ場所に配置されている各 IP スイッチに FC （ NV インターコネクトおよび FCP イニシエータ）接続されています。データは、クラスタからクラスタへ、 ISL 経由でレプリケートされます。

- * クラスタ間ピアリングネットワーク *

  この種類のネットワークは、 2 つのクラスタ間の冗長 IP ネットワークパスで構成されます。クラスタピアリングネットワークは、 Storage Virtual Machine （ SVM ）構成をミラーするために必要な接続を提供します。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。

- * IP ネットワーク（ MetroCluster IP 構成に存在） *

  この種類のネットワークは、 2 つの冗長 IP スイッチネットワークで構成されます。各ネットワークには 2 つの IP スイッチがあり、各スイッチファブリックの 1 つのスイッチはクラスタと同じ場所に配置されます。各クラスタには、各スイッチファブリックから 1 つずつ、 2 つの IP スイッチがあります。すべてのノードは、同じ場所に配置されている各 FC スイッチに接続されています。データは、クラスタからクラスタへ、 ISL 経由でレプリケートされます。

サイト間接続を監視する

Tiebreaker ソフトウェアは、サイト間接続のステータスをノードから定期的に取得します。NV インターコネクト接続が失われ、クラスタ間ピアリングが ping に応答しない場合、クラスタはサイトが分離されているとみなし、 Tiebreaker ソフトウェアは「 AllLinksSevered 」としてアラートをトリガーします。クラスタが「 AllLinksSevered 」ステータスを識別し、もう一方のクラスタがネットワーク経由で到達できない場合、 Tiebreaker ソフトウェアは「 disaster 」としてアラートをトリガーします。

Tiebreaker ソフトウェアでサイト障害を検出する方法

NetApp MetroCluster Tiebreaker ソフトウェアは、 MetroCluster 構成のノードおよびクラスタに到達できるかどうかをチェックして、サイト障害の有無を判断します。また、 Tiebreaker ソフトウェアは、特定の状況でアラートをトリガーします。

Tiebreaker ソフトウェアで監視されるコンポーネント

Tiebreaker ソフトウェアは、 IP ネットワークでホストされるノード管理 LIF およびクラスタ管理 LIF への複数のパスを経由する冗長接続を確立することによって、 MetroCluster 構成内の各コントローラを監視します。

Tiebreaker ソフトウェアで監視される MetroCluster 構成のコンポーネントは次のとおりです。

- ローカルノードインターフェイスを介してノードを追加します
- クラスタ指定インターフェイスを介したクラスタ
- サバイバークラスタ - ディザスタサイトとの接続の有無を評価（ NV インターコネクト、ストレージ、クラスタ間ピアリング）

Tiebreaker ソフトウェアとクラスタ内のすべてのノードおよびクラスタ自体との接続が失われると、クラスタは Tiebreaker ソフトウェアによって「到達不能」と宣言されます。接続障害は 3~5 秒で検出されます。Tiebreaker ソフトウェアからクラスタに到達できない場合、障害が発生していないクラスタ（到達可能なクラスタ）は、 Tiebreaker ソフトウェアがアラートをトリガーする前に、パートナークラスタへのすべてのリンクが切断されていることを示す必要があります。

サバイバークラスタが FC （ NV インターコネクトとストレージ）とクラスタ間ピアリングを介してディザスタサイトのクラスタと通信できなくなると、すべてのリンクが切断されたとみなされます。

Tiebreaker ソフトウェアがアラートをトリガーする障害シナリオ

Tiebreaker ソフトウェアは、ディザスタサイトのクラスタ（すべてのノード）が停止しているか到達不能であり、サバイバーサイトのクラスタが「 AllLinksSevered 」ステータスを示している場合、アラートをトリガーします。

次のシナリオでは、 Tiebreaker ソフトウェアはアラートをトリガーしません（またはアラートが拒否されます）。

- 8 ノード MetroCluster 構成で、ディザスタサイトの HA ペアの 1 つが停止している場合
- ディザスタサイトのすべてのノードを含むクラスタが停止し、サバイバーサイトの 1 つの HA ペアが停止し、サバイバーサイトのクラスタが「 AllLinksSevered 」ステータスを示している場合

  Tiebreaker ソフトウェアはアラートをトリガーしますが、 ONTAP はアラートを拒否します。この場合、手動によるスイッチオーバーも拒否されます

- Tiebreaker ソフトウェアがディザスタサイトの少なくとも 1 つのノードまたはクラスタインターフェイスに到達できる、またはサバイバーサイトが FC （ NV インターコネクトとストレージ）またはクラスタ間ピアリングを介してディザスタサイトのいずれかのノードに到達できる場合

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

"MetroCluster IP構成での自動計画外スイッチオーバーのONTAPメディエーターによるサポートの詳細"。

NVFAIL を使用したファイルシステム整合性の監視および保護

volume modify コマンドの -nvfail` パラメータを使用すると、 ONTAP は、システムの起

動時またはスイッチオーバー操作後に NVRAM （不揮発性 RAM ）の不整合を検出できます。また、警告を表示し、ボリュームを手動でリカバリできるようになるまでデータのアクセスと変更ができないようにシステムを保護します。

ONTAP が何らかの問題を検出すると、データベースインスタンスまたはファイルシステムインスタンスは応答を停止するか、シャットダウンされます。ONTAP はコンソールにエラーメッセージを送信して、データベースまたはファイルシステムの状態をチェックするようユーザに警告します。NVFAIL を有効にすると、データベースの有効性を侵害する可能性のある、クラスタ化されたノード間での NVRAM の不整合をデータベース管理者に警告できます。

フェイルオーバーまたはブートリカバリのあとは、 NVFAIL 状態が解消されるまで NFS クライアントはどのノードからもデータにアクセスできません。CIFS クライアントには影響はありません。

NFS ボリュームまたは LUN へのアクセスに対する NVFAIL の影響

NVFAIL 状態は、起動時に ONTAP が NVRAM エラーを検出した場合、 MetroCluster スイッチオーバー処理が実行された場合、または NVFAIL オプションが設定されたボリュームの HA テイクオーバー処理中に発生します。起動時にエラーが検出されなければ、ファイルサービスは正常に開始されます。ただし、 NVRAM エラーが検出された場合、またはディザスタスイッチオーバーで NVFAIL の処理が実行された場合、 ONTAP はデータベースインスタンスの応答を停止します。

NVFAIL オプションを有効にすると、起動時に次の表に示すいずれかのプロセスが開始されます。

状況	作業
ONTAP は NVRAM エラーを検出しませんでした	ファイルサービスが正常に開始されます。
ONTAP が NVRAM エラーを検出した場合	• ONTAP がデータベースにアクセスしようとする NFS クライアントに古いファイルハンドル（ ESTALE ）エラーを返します。これにより、アプリケーションは、応答を中断するか、クラッシュまたは停止します。 ONTAP からシステムコンソールおよびログファイルにエラーメッセージが送信されます。 • アプリケーションが再起動されると、データベースの妥当性が確認されていなくても、 CIFS クライアントからのアクセスが可能になります。 NFS クライアントの場合は、影響を受けたボリューム上の in-nvfailed-state オプションをリセットするまでファイルにアクセスできません。

次のいずれかのパラメータを使用する場合： • 「 dr-force-nvfail 」ボリュームオプションが設定されている • force-nvfail-all 'switchover コマンド・オプションが設定されている	管理者が将来のディザスタスイッチオーバーで NVFAIL 処理を強制的に実行する予定がない場合は、スイッチオーバー後に「 dr-force-nvfail 」オプションを解除できます。NFS クライアントの場合は、影響を受けたボリューム上の in-nvfailed-state オプションをリセットするまでファイルにアクセスできません。 「 force-nvfail-all 」オプションを使用すると、ディザスタスイッチオーバー時に処理されるすべての DR ボリュームで「 dr -force-nvfail 」オプションが設定されます。
ONTAP は、 LUN を含むボリューム上で NVRAM エラーを検出します	そのボリュームの LUN がオフラインになります。ボリュームの in-nvfailed-state オプションをクリアし、さらに影響を受けたボリュームの各 LUN をオンラインにして LUN 上の NVFAIL 属性をクリアする必要があります。LUN の整合性をチェックする手順を実行し、必要に応じて Snapshot コピーまたはバックアップから LUN をリカバリすることができます。ボリューム内のすべての LUN がリカバリされると、影響を受けたボリュームの in-nvfailed-state オプションがクリアされます。

データ損失イベントを監視するコマンド

NVFAIL オプションを有効にすると、 NVRAM の不整合によってシステムクラッシュが発生した場合、または MetroCluster スイッチオーバーが発生した場合に、通知を受け取ることができます。

デフォルトでは、 NVFAIL パラメータは無効になっています。

状況	使用するコマンド
NVFAIL を有効にして新しいボリュームを作成します	'volume create-nvfail on `
既存のボリュームで NVFAIL を有効にする	'volume modify' • 注： * 作成されたボリュームで NVFAIL を有効にするには、 -nvfail オプションを on に設定します。
指定したボリュームで NVFAIL が有効になっているかどうかを表示します	volume show • 注： * 指定したボリュームの NVFAIL 属性を表示するには、「 -fields 」パラメータを「 nvfail 」に設定します。

関連情報

詳細については、各コマンドのマニュアルページを参照してください。

スイッチオーバー後に **NVFAIL** 状態のボリュームにアクセスする場合

スイッチオーバー後に 'volume modify コマンドの -in-nvfailed-state パラメータをリセットし ' クライアントがデータにアクセスする制限を解除することにより 'NVFAIL 状態をクリアする必要があります

作業を開始する前に

データベースまたはファイルシステムが実行されていない、または影響を受けたボリュームにアクセスしようとしていないことが必要です。

このタスクについて

in-nvfailed-state パラメータを設定するには、 advanced 権限が必要です。

ステップ

1. in-nvfailed-state パラメータを false に設定して volume modify コマンドを実行し、ボリュームをリカバリします。

完了後

データベースファイルの有効性を調べる方法については、ご使用のデータベースソフトウェアのマニュアルを参照してください。

データベースで LUN が使用されている場合は、 NVRAM 障害後にホストから LUN にアクセスできるようにする手順を確認してください。

関連情報

"NVFAIL を使用したファイルシステム整合性の監視および保護"

スイッチオーバー後の **NVFAIL** 状態にある **LUN** のリカバリ

スイッチオーバーが発生すると、 NVFAIL 状態にある LUN 上のデータにホストがアクセスできなくなります。データベースが LUN にアクセスできるようにするには、いくつかの作業が必要です。

作業を開始する前に

データベースが実行されていないことを確認します。

手順

1. volume modify コマンドの -in-nvfailed-state パラメータをリセットし、 LUN をホストする、影響を受けたボリュームの NVFAIL 状態をクリアします。
2. 影響を受けた LUN をオンラインにします。
3. LUN でデータの不整合の有無を確認し、これを解決します。

   これには、ホストベースのリカバリか、 SnapRestore を使用してストレージコントローラ上で実行するリカバリが含まれる場合があります。

4. LUN をリカバリしたあと、データベースアプリケーションをオンラインにします。

追加情報の参照先

MetroCluster の設定と処理の詳細については、を参照してください。

MetroCluster およびその他の情報

情報	件名
"MetroCluster のドキュメント"	• すべての MetroCluster 情報
"ネットアップテクニカルレポート 4375 ：『 NetApp MetroCluster for ONTAP 9.3 』"	• MetroCluster の設定と運用の技術概要 • MetroCluster 構成のベストプラクティス
"ファブリック接続 MetroCluster のインストールと設定"	• ファブリック接続 MetroCluster アーキテクチャ • 構成のケーブル接続 • FC-to-SAS ブリッジの設定 • FC スイッチを設定します • ONTAP で MetroCluster を設定します
"ストレッチ MetroCluster のインストールと設定"	• ストレッチ MetroCluster アーキテクチャ • 構成のケーブル接続 • FC-to-SAS ブリッジの設定 • ONTAP で MetroCluster を設定します
"MetroCluster IP のインストールと設定"	• MetroCluster IP アーキテクチャ • 構成のケーブル接続 • ONTAP で MetroCluster を設定します
"MetroCluster Tiebreaker 1.21 ソフトウェアのインストールと設定"	• MetroCluster Tiebreaker ソフトウェアを使用して MetroCluster 構成を監視する
Active IQ Unified Manager のドキュメント "ネットアップのマニュアル：製品ガイドとリソース"	• MetroCluster の設定とパフォーマンスを監視する
"コピーベースの移行"	• 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

MetroCluster のコンポーネントをメンテナンスします

MetroClusterメンテナンスの詳細

MetroClusterのメンテナンスタスクを準備する方法と、構成に適したメンテナンス手順を選択する方法について説明します。

メンテナンスタスクの準備

メンテナンス手順を実行する前に、の情報を確認してください"MetroClusterのメンテナンスの準備"。

メンテナンスタスクを実行する前に、コンソールロギングを有効にし、ONTAPメディエーターまたはTiebreakerの監視を削除する必要があります。

各種のMetroCluster構成のメンテナンス手順

- MetroCluster IP設定を使用している場合は、の手順を確認してください"MetroCluster IP構成のメンテナンス手順"。
- MetroCluster FC構成の場合は、の手順を確認してください"MetroCluster FC構成のメンテナンス手順"。
- 構成に対応するセクションに記載されている手順が見つからない場合は、の手順を確認してください"すべてのMetroCluster構成のメンテナンス手順"。

その他のすべてのメンテナンス手順

次の表に、上記の3つのセクションに記載されていないMetroClusterのメンテナンス手順へのリンクを示します。

コンポーネント	MetroCluster タイプ（ FC または IP ）	タスク	手順
ONTAP ソフトウェア	両方	ONTAP ソフトウェアのアップグレード	"アップグレード、リバート、ダウングレード"

コントローラモジュール	両方	FRU の交換（コントローラモジュール、 PCIe カード、 FC-VI カードなど） MetroCluster ストレージシステム間でのストレージコントローラモジュールまたは NVRAM カードの移動はサポートされていません。	"ONTAPハードウェアシステムのドキュメント"
アップグレードと拡張	"MetroCluster のアップグレードと拡張"	FC から IP への接続に移行します	"MetroCluster FC から MetroCluster IP に移行します"
ドライブシェルフ	FC	その他すべてのシェルフのメンテナンス手順。標準の手順を使用できます。	"DS460C 、 DS224C 、 DS212C ディスクシェルフを保守します"

MetroClusterのメンテナンスの準備

メンテナンスタスクを実行する前にコンソールログを有効にする

メンテナンスタスクを実行する前に、デバイスのコンソールログを有効にしてください。

NetAppでは、メンテナンス手順を実行する前に、使用しているデバイスでコンソールログを有効にし、次の操作を実行することを強く推奨しています。

- メンテナンス中はAutoSupportを有効のままにします。
- メンテナンスの前後にメンテナンスAutoSupportメッセージをトリガーして、メンテナンスアクティビティ中にケースの作成を無効にします。

  ナレッジベースの記事を参照してください "スケジュールされたメンテナンス時間中にケースの自動作成を停止する方法"。

- 任意のCLIセッションのセッションロギングをイネーブルにします。セッションログを有効にする方法については、ナレッジベースの記事の「セッション出力のログ」セクションを参照してください "ONTAPシステムへの接続を最適化するためのPuTTYの設定方法"。

メンテナンス作業を実行する前に、 ONTAP メディエーターまたは Tiebreaker の監視を削除します

メンテナンスタスクを実行する前に、 Tiebreaker またはメディエーターユーティリティで MetroCluster 設定を監視している場合は、監視を解除する必要があります。

メンテナンスタスクには、コントローラプラットフォームのアップグレード、 ONTAP のアップグレード、ネゴシエートスイッチオーバーとスイッチバックの実行が含まれます。

手順

1. 次のコマンドの出力を収集します。

   「 storage iscsi-initiator show 」のように表示されます

2. Tiebreaker 、メディエーター、またはスイッチオーバーを開始できるその他のソフトウェアから既存の MetroCluster 構成を削除します。

使用するポート	使用する手順
Tiebreaker	"MetroCluster 設定の削除" MetroCluster Tiebreaker インストールおよび設定コンテンツで、を参照してください
メディエーター	ONTAP プロンプトで次のコマンドを問題に設定します。 MetroCluster 構成設定のメディエーターが削除されました
サードパーティ製アプリケーション	製品マニュアルを参照してください。

3. MetroCluster 設定のメンテナンスが完了したら、 Tiebreaker またはメディエーターユーティリティを使用して監視を再開できます。

使用するポート	この手順を使用します
Tiebreaker	"MetroCluster 構成を追加しています" *MetroCluster Tiebreaker* のインストールと構成 セクション。
メディエーター	"MetroCluster IP構成からONTAPメディエーターを構成する" *MetroCluster IP* のインストールと構成セクション。
サードパーティ製アプリケーション	製品マニュアルを参照してください。

MetroCluster の障害とリカバリのシナリオ

さまざまな障害の発生時に MetroCluster 構成でどのように対応できるかを把握しておく必要があります。

ノード障害からの追加情報のリカバリについては、の「正しいリカバリ手順の選択」を参照してください "災害からリカバリします"。

イベント	影響	リカバリ
単一ノード障害です	フェイルオーバーがトリガーされます。	ローカルのテイクオーバーによって構成がリカバリされます。RAIDには影響はありません。システムメッセージを確認し、障害が発生した FRU を必要に応じて交換します。 "ONTAPハードウェアシステムのドキュメント"
一方のサイトの 2 つのノードの障害	MetroCluster Tiebreaker ソフトウェアで自動スイッチオーバーが有効になっている場合にのみ、 2 つのノードがスイッチオーバーされます。	MetroCluster Tiebreakerソフトウェアで自動スイッチオーバーが有効になっていない場合は、USOを手動で計画外スイッチオーバーします。 "ONTAPハードウェアシステムのドキュメント"
MetroCluster IP interface — 1 つのポートの障害	システムがデグレード状態になっている。ポート障害がさらに発生すると HA ミラーリングに影響します。	2 番目のポートが使用されます。ポートへの物理リンクが切断されると、ヘルスモニタによってアラートが生成されます。システムメッセージを確認し、障害が発生した FRU を必要に応じて交換します。 "ONTAPハードウェアシステムのドキュメント"
MetroCluster IP interface — 両方のポートの障害	HA 機能に影響します。ノードの RAID SyncMirror の同期が停止します。	HA テイクオーバーは行われないため、すぐに手動でリカバリする必要があります。システムメッセージを確認し、障害が発生した FRU を必要に応じて交換します。 "ONTAPハードウェアシステムのドキュメント"

1 つの MetroCluster IP スイッチの障害	影響はありません。冗長性は、 2 番目のネットワークを通じて提供されます。	障害が発生したスイッチを必要に応じて交換します。 "IP スイッチの交換"
同じネットワーク内にある 2 つの MetroCluster IP スイッチの障害	影響はありません。冗長性は、 2 番目のネットワークを通じて提供されます。	障害が発生したスイッチを必要に応じて交換します。 "IP スイッチの交換"
1 つのサイトにある 2 つの MetroCluster IP スイッチの障害	ノードの RAID SyncMirror の同期が停止します。HA 機能に影響し、クラスタがクォーラムのメンバーでなくなります。	障害が発生したスイッチを必要に応じて交換します。 "IP スイッチの交換"
別々のサイトにありネットワークも異なる（対角の関係にある） 2 つの MetroCluster IP スイッチの障害	ノードの RAID SyncMirror の同期が停止します。	ノードの RAID SyncMirror の同期が停止します。クラスタおよび HA 機能には影響はありません。障害が発生したスイッチを必要に応じて交換します。 "IP スイッチの交換"

Interoperability Matrix Tool を使用した MetroCluster 情報の検索

MetroCluster 構成をセットアップするときは、 Interoperability Tool を使用して、サポートされているソフトウェアとハードウェアのバージョンを使用しているかどうかを確認できます。

"NetApp Interoperability Matrix Tool で確認できます"

Interoperability Matrix を開いたあと、 Storage 解決策フィールドを使用して MetroCluster 解決策を選択できます。

検索を絞り込むには、 * 構成部品エクスプローラ * を使用して構成部品と ONTAP バージョンを選択します。

[結果の表示（ Show Results ）] をクリックすると、条件に一致するサポートされている構成のリストを表示できます。

MetroCluster FC構成のメンテナンス手順

健常性監視用に、スイッチまたはATTOブリッジのIPアドレスを変更します

MetroCluster FCバックエンドスイッチとATTOブリッジのIPアドレスを変更したら、古いヘルスモニタのIPアドレスを新しい値に置き換える必要があります。

- スイッチのIPアドレスを変更します

- ATTOブリッジのIPアドレスを変更します

スイッチのIPアドレスを変更します

MetroCluster FCバックエンドスイッチの古いヘルスモニタIPアドレスを置き換えます。

作業を開始する前に

ヘルスモニタのIPアドレスを変更する前に、使用しているスイッチモデルに対応するスイッチベンダーのドキュメントを参照して、スイッチのIPアドレスを変更してください。

手順

1. を実行します `::> storage switch show` コマンドと出力で、エラーを報告しているスイッチを確認します。
2. 古いIPアドレスを持つスイッチエントリを削除します。

   ```
   ::> storage switch remove -name switch_name
   ```

3. 新しいIPアドレスを使用してスイッチを追加します。

   ```
   ::> storage switch add -name switch_name -address new_IP_address -managed-by
   in-band
   ```

4. 新しいIPアドレスを確認し、エラーがないことを確認します。

   ```
   ::> storage switch show
   ```

5. 必要に応じて、エントリを更新します。

   ```
   ::> set advanced

   ::*> storage switch refresh

   ::*> set admin
   ```

ATTOブリッジのIPアドレスを変更します

ATTOブリッジの古いヘルスモニタIPアドレスを置き換えます。

手順

1. を実行します `::> storage bridge show` コマンドと出力で、エラーを報告しているATTOブリッジを確認します。
2. 古いIPアドレスを使用してATTOブリッジのエントリを削除します。

   ```
   ::> storage bridge remove -name ATTO_bridge_name
   ```

3. 新しいIPアドレスでATTOブリッジを追加します。

   ```
   ::> storage bridge add -name ATTO_bridge_name -address new_IP_address -managed
   -by in-band
   ```

4. 新しいIPアドレスを確認し、エラーがないことを確認します。

```
::> storage bridge show
```

5. 必要に応じて、エントリを更新します。

```
::> set advanced

::*> storage bridge refresh

::*> set admin
```

FC-to-SAS ブリッジのメンテナンス

MetroCluster 構成での FibreBridge 7600N ブリッジのサポート

FibreBridge 7600N ブリッジは、 ONTAP 9.5 以降で、 FibreBridge 7500N / 6500N ブリッジを交換する場合、または MetroCluster 構成に新しいストレージを追加する場合にサポートされます。ゾーニング要件とブリッジの FC ポートの使用に関する制限事項は、 FibreBridge 7500N ブリッジと同じです。

"NetApp Interoperability Matrix Tool で確認できます"

ONTAP 9.8 以降を実行している構成では、 FibreBridge 6500N ブリッジはサポートされません。

ユースケース	ゾーニングの変更が必要か	制限事項	手順
1 つの FibreBridge 7500N ブリッジを 1 つの FibreBridge 7600N ブリッジに交換する	いいえ	FibreBridge 7600N ブリッジの設定は、 FibreBridge 7500N ブリッジとまったく同じにする必要があります。	"FibreBridge 7500N と 7600N ブリッジのホットスワップ"
1 つの FibreBridge 6500N ブリッジを 1 つの FibreBridge 7600N ブリッジに交換する	いいえ	FibreBridge 7600N ブリッジの設定は、 FibreBridge 6500N ブリッジとまったく同じにする必要があります。	"FibreBridge 6500N ブリッジと FibreBridge 7600N / 7500N ブリッジのホットスワップ"

新しい FibreBridge 7600N ブリッジペアを追加して、新しいストレージを追加します	はい。 新しいブリッジの各 FC ポート用のストレージゾーンを追加する必要があります。	FC スイッチファブリック（ファブリック接続 MetroCluster 構成）またはストレージコントローラ（ストレッチ MetroCluster 構成）に使用可能なポートが必要です。 FibreBridge 7500N / 7600N ブリッジペアは、それぞれ最大 4 つのスタックをサポートできます。	"MetroCluster システムへの SAS ディスクシェルフとブリッジのスタックのホットアド"

MetroCluster 構成での **FibreBridge 7500N** ブリッジのサポート

FibreBridge 7500N ブリッジは、 FibreBridge 6500N ブリッジを交換する場合、または MetroCluster 構成に新しいストレージを追加する場合にサポートされます。サポートされる構成には、ゾーニング要件、ブリッジの FC ポートの使用に関する制限事項、およびスタックとストレージシェルフの制限があります。

ONTAP 9.8 以降を実行している構成では、 FibreBridge 6500N ブリッジはサポートされません。

ユースケース	ゾーニングの変更が必要か	制限事項	手順
1 台の FibreBridge 6500N ブリッジを 1 台の FibreBridge 7500N ブリッジに交換する	いいえ	FibreBridge 7500N ブリッジは FibreBridge 6500N ブリッジとまったく同じように設定し、単一の FC ポートを使用して単一のスタックに接続する必要があります。FibreBridge 7500N の 2 つ目の FC ポートは使用できません。	"FibreBridge 6500N ブリッジと FibreBridge 7600N / 7500N ブリッジのホットスワップ"
複数ペアの FibreBridge 6500N ブリッジを単一ペアの FibreBridge 7500N ブリッジと交換することで、複数のスタックを統合する	はい。	この場合、 FibreBridge 6500N ブリッジのサービスを停止して、単一ペアの FibreBridge 7500N ブリッジに交換します。 FibreBridge 7500N / 7600N ブリッジペアは、それぞれ最大 4 個のスタックをサポートできます。 手順の末尾で、上部と下部の両方のスタックを、 FibreBridge 7500N ブリッジの対応するポートに接続する必要があります。	"FibreBridge 6500N ブリッジのペアを 7600N / 7500N ブリッジに交換する"

ユースケース	ゾーニングの変更が必要か	制限事項	手順
新しい FibreBridge 7500N ブリッジペアを追加することで新しいストレージを追加する	はい。 新しいブリッジの各 FC ポート用のストレージゾーンを追加する必要があります。	FC スイッチファブリック（ファブリック接続 MetroCluster 構成）またはストレージコントローラ（ストレッチ MetroCluster 構成）に使用可能なポートが必要です。 FibreBridge 7500N / 7600N ブリッジペアは、それぞれ最大 4 つのスタックをサポートできます。	"MetroCluster システムへの SAS ディスクシェルフとブリッジのスタックのホットアド"

必要に応じて、 **FibreBridge 7600N** ブリッジの **IP** ポートアクセスを有効にする

9.5 より前のバージョンの ONTAP を使用している場合、または Telnet やその他の IP ポートプロトコルおよびサービス（ FTP 、 ExpressNAV 、 ICMP 、 QuickNAV ）を使用して FibreBridge 7600N ブリッジへのアウトオブバンドアクセスを使用する場合は、コンソールポート経由でアクセスサービスを有効にできます。

ATTO FibreBridge 7500Nブリッジとは異なり、FibreBridge 7600Nブリッジは、すべてのIPポートプロトコルおよびサービスが無効になった状態で出荷されます。

ONTAP 9.5 以降では、ブリッジのインバンド管理 _ がサポートされます。これは、 ONTAP CLI からブリッジへの FC 接続を介してブリッジを設定および監視できることを意味します。ブリッジのイーサネットポートを介してブリッジに物理的にアクセスする必要がなく、ブリッジのユーザインターフェイスも必要ありません。

ONTAP 9.8 以降では、ブリッジの _ 帯域内管理 _ がデフォルトでサポートされ、アウトオブバンド SNMP 管理は廃止されています。

このタスクは、ブリッジの管理にインバンド管理を使用していない場合に必要です。この場合は、イーサネット管理ポートを介してブリッジを設定する必要があります。

手順

1. FibreBridge 7600N ブリッジのシリアルポートにシリアルケーブルを接続して、ブリッジのコンソールインターフェイスにアクセスします。
2. コンソールを使用してアクセスサービスを有効にし、設定を保存します。

   set closePort none

   'saveconfigation

   'set closePort none' コマンドを使用すると、ブリッジ上のすべてのアクセスサービスがイネーブルになります。

3. 必要に応じて 'et closePort' を発行し ' 必要に応じてコマンドを繰り返して ' 必要なサービスをすべて無効にします

'set closePort_service_

'set closePort' コマンドは ' 一度に 1 つのサービスを無効にします

「サービス」では、次のいずれかを指定できます。

- エクプレスナヴ
- FTP
- ICMP
- QuickNAV
- SNMP
- Telnet

  特定のプロトコルがイネーブルになっているかディセーブルになっているかを確認するには、 get closePort コマンドを使用します。

4. SNMP を有効にする場合は、 set snmp enabled コマンドも問題で実行する必要があります。

   'set snmp enabled

   SNMP は、別個の enable コマンドを必要とする唯一のプロトコルです。

5. 設定を保存します。

   'saveconfigation

FibreBridge ブリッジのファームウェアを更新しています

ブリッジファームウェアを更新するための手順は、ブリッジモデルと ONTAP のバージョンによって異なります。

このタスクについて

"コンソールログを有効にする" このタスクを実行する前に。

ONTAP 9.4 以降を実行している構成での FibreBridge 7600N / 7500N ブリッジのファームウェアの更新

FibreBridge ブリッジのファームウェアを更新して、最新の機能を実装したり、潜在的な問題を解決したりすることが必要になる場合があります。この手順は、 ONTAP 9.4 以降を実行している構成の FibreBridge 7600N / 7500N ブリッジに使用します。

- MetroCluster 構成が正常に動作している必要があります。
- MetroCluster 構成内のすべての FibreBridge ブリッジが稼働している必要があります。
- すべてのストレージパスが使用可能である必要があります。
- 管理者パスワードと、HTTP、FTP、または TFTP (Trivial File Transfer Protocol) サーバーへのアクセスが必要です。
- サポートされているファームウェアバージョンを使用している必要があります。

  "NetApp Interoperability Matrix Tool で確認できます"

IMT では、 Storage 解決策フィールドを使用して MetroCluster 解決策を選択できます。検索を絞り込むには、 * 構成部品エクスプローラ * を使用して構成部品と ONTAP バージョンを選択します。[結果の表示（ Show Results ）] をクリックすると、条件に一致するサポートされている構成のリストを表示できます。

- このタスクは、 ONTAP 9.4 以降を実行している構成の FibreBridge 7600N / 7500N ブリッジでのみ使用できます。
- このタスクは、 MetroCluster 構成内の各 FibreBridge ブリッジで実行し、すべてのブリッジで同じファームウェアバージョンが実行されるようにする必要があります。

これはシステムの停止を伴わない手順であり、完了までに約 30 分かかります。

ONTAP 9 .8以降では `system bridge`、コマンドがコマンドに置き換えられて `storage bridge`います。次の手順はコマンドを示してい `system bridge`ますが、`ONTAP 9`よりも前のバージョンを実行している場合はコマンドを使用する必要があります。`8 `storage bridge`

手順

1. メンテナンスの開始を通知する AutoSupport メッセージを起動します。

   'system node AutoSupport invoke -node * -type all -message MAINT=*maintenance-window-in-hours*`

   「 maintenance-window-in-hours 」には、メンテナンス・ウィンドウの長さを 72 時間まで指定します。この時間が経過する前にメンテナンスが完了した場合は、メンテナンス期間が終了したことを通知する AutoSupport メッセージを起動できます。

   「 system node AutoSupport invoke -node * -type all -message MAINT= end 」というメッセージが表示されます

2. ATTO FibreBridge のページに移動し、ブリッジに適したファームウェアを選択します。

   "ATTO FibreBridge ファームウェアのダウンロードページ"

3. 「注意 / 必ずお読みください」と「エンドユーザ契約」を確認し、チェックボックスをクリックして同意してください。
4. コントローラモジュールからアクセス可能なネットワーク上の場所にファームウェアファイルを配置します。

   以降の手順のコマンドは、どちらのコントローラモジュールのコンソールでも入力できます。

5. 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（ * > ）。

6. ブリッジ ファームウェアを更新します。

   ONTAP 9 .16.1以降では、ファームウェアパッケージのダウンロードにサーバで必要な場合、クレデンシャルを使用してブリッジファームウェアを更新できます。

クレデンシャルが不要な場合：

a. ブリッジファームウェアを更新します。

```
system bridge firmware update -bridge <name> -uri <URL-of-firmware-
package>
```

例

```
cluster_A> system bridge firmware update -bridge bridge_A_1a -uri
http://192.168.132.97/firmware.ZBD
```

クレデンシャルが必要な場合：

a. ブリッジファームウェアを更新し、必要なユーザ名を指定します。

```
system bridge firmware update -bridge <name> -uri <URL-of-
firmware-package> -username <name>
```

b. 出力にプロンプトが表示されたら、次の例に示すようにパスワードを入力します。

例

```
cluster_A> system bridge firmware update -bridge bridge_A_1a -uri
http://192.168.132.97/firmware.ZBD -username abc

(system bridge)

Enter the password:

[Job 70] Job is queued: System bridge firmware update job.
```

7. admin 権限レベルに戻ります。

「特権管理者」

8. ファームウェアのアップグレードが完了したことを確認します。

```
job show -name "<job_name>"
```

次の例は、「system bridge firmware update」ジョブがまだ実行中であることを示しています。

```
cluster_A> job show -name "system bridge firmware update"
Owning

Job ID Name                  Vserver    Node           State
------ --------------------- ---------- -------------- ----------
2246   job-name
                            cluster_A
                                       node_A_1
                                                      Running
Description: System bridge firmware update job
```

約 10 分後に新しいファームウェアが完全にインストールされ、ジョブの状態は「 Success 」になります。

```
cluster_A> job show -name "system bridge firmware update"

                            Owning
Job ID Name                 Vserver    Node           State
------ --------------------- ---------- -------------- ----------
2246   System bridge firmware update
                            cluster_A
                                       node_A_1
                                                      Success
Description: System bridge firmware update job
```

9. インバンド管理が有効になっているかどうか、およびシステムで実行されている ONTAP のバージョンに応じて、次の手順を実行します。

   ◦ ONTAP 9.4 を実行している場合はインバンド管理がサポートされないため、ブリッジコンソールからコマンドを実行する必要があります。

      i. ブリッジのコンソールで「 flashimages 」コマンドを実行し、正しいファームウェアバージョンが表示されることを確認します。

      次の例では、プライマリフラッシュイメージに新しいファームウェアイメージが表示され、セカンダリフラッシュイメージに古いイメージが表示されています。

      ```
      flashimages

       ;Type Version
      ;=====================================================
      Primary 3.16 001H
      Secondary 3.15 002S
      Ready.
      ```

a. ブリッジから「 firmwareerestart 」コマンドを実行して、ブリッジを再起動します。

- ONTAP 9.5 以降を実行している場合はインバンド管理がサポートされるため、クラスタプロンプトからコマンドを実行できます。

b. コマンドを実行します `system bridge run-cli -name <bridge_name> -command FlashImages`。

次の例では、プライマリフラッシュイメージに新しいファームウェアイメージが表示され、セカンダリフラッシュイメージに古いイメージが表示されています。

```
cluster_A> system bridge run-cli -name ATTO_7500N_IB_1 -command
FlashImages

[Job 2257]

;Type         Version
;=====================================================
Primary 3.16 001H
Secondary 3.15 002S
Ready.


[Job 2257] Job succeeded.
```

a. 必要に応じて、ブリッジを再起動します。

```
system bridge run-cli -name ATTO_7500N_IB_1 -command FirmwareRestart
```

ATTO ファームウェアバージョン 2.95 以降ではブリッジが自動的に再起動するため、この手順は不要です。

10. ブリッジが正常に再起動したことを確認します。

「 sysconfig 」を使用できます

システムは、マルチパスハイアベイラビリティ（両方のコントローラがブリッジ経由で各スタックのディスクシェルフにアクセス可能）用にケーブル接続されている必要があります。

```
cluster_A> node run -node cluster_A-01 -command sysconfig
NetApp Release 9.6P8: Sat May 23 16:20:55 EDT 2020
System ID: 1234567890 (cluster_A-01); partner ID: 0123456789 (cluster_A-
02)
System Serial Number: 200012345678 (cluster_A-01)
System Rev: A4
System Storage Configuration: Quad-Path HA
```

11. FibreBridge ファームウェアが更新されたことを確認します。

    `system bridge show -fields fw-version,symbolic-name`

```
cluster_A> system bridge show -fields fw-version,symbolic-name
name fw-version symbolic-name
---------------- ----------------- -------------
ATTO_20000010affeaffe 3.10 A06X bridge_A_1a
ATTO_20000010affeffae 3.10 A06X bridge_A_1b
ATTO_20000010affeafff 3.10 A06X bridge_A_2a
ATTO_20000010affeaffa 3.10 A06X bridge_A_2b
4 entries were displayed.
```

12. ブリッジのプロンプトからパーティションが更新されたことを確認します。

    「 flashimages 」と入力します

    プライマリフラッシュイメージに新しいファームウェアイメージが表示され、セカンダリフラッシュイメージに古いイメージが表示されます。

```
Ready.
flashimages

;Type          Version
;=====================================================
   Primary    3.16 001H
 Secondary    3.15 002S

 Ready.
```

13. 手順 5 ～ 10 を繰り返して、両方のフラッシュイメージが同じバージョンに更新されることを確認します。
14. 両方のフラッシュイメージが同じバージョンに更新されていることを確認します。

    「 flashimages 」と入力します

    出力には、両方のパーティションで同じバージョンが表示されます。

```
Ready.
flashimages

;Type          Version
;=====================================================
   Primary     3.16 001H
 Secondary     3.16 001H

 Ready.
```

15. 次のブリッジでも手順 5 から 13 を繰り返し、 MetroCluster 構成内のすべてのブリッジを更新します。

単一の **FC-to-SAS** ブリッジの交換

ブリッジを同じモデルのブリッジまたは新しいモデルのブリッジに無停止で交換することができます。

作業を開始する前に

管理パスワードと FTP サーバまたは SCP サーバへのアクセスが必要です。

このタスクについて

これはシステムの停止を伴わない手順であり、完了までに約 60 分かかります。

この手順では、ブリッジ CLI を使用してブリッジを設定および管理し、ブリッジファームウェアと ATTO QuickNAV ユーティリティを更新してブリッジイーサネット管理 1 ポートを設定します。要件を満たしていれば、他のインターフェイスも使用できます。

"他のインターフェイスを使用して FibreBridge ブリッジを設定および管理するための要件"

関連情報

"FibreBridge 6500N ブリッジのペアを 7600N / 7500N ブリッジに交換する"

ストレージ接続を確認しています

ブリッジを交換する前に、ブリッジとストレージの接続を確認する必要があります。設定を変更したあとに接続を確認できるよう、コマンド出力について理解しておいてください。

このタスクについて

これらのコマンドは、メンテナンス中のサイトの MetroCluster 構成にある任意のコントローラモジュールの管理プロンプトから問題できます。

手順

1. いずれかの MetroCluster ノードで次のコマンドを入力して、ディスクへの接続を確認します。

   'run local sysconfig -v

   出力には、コントローラのイニシエータポートに接続されているディスクが表示され、 FC-to-SAS ブリッジに接続されているシェルフが示されます。

```
node_A_1> run local sysconfig -v
NetApp Release 9.3.2X18: Sun Dec 13 01:23:24 PST 2017
System ID: 4068741258 (node_A_1); partner ID: 4068741260 (node_B_1)
System Serial Number: 940001025471 (node_A_1)
System Rev: 70
System Storage Configuration: Multi-Path HA**<=== Configuration should
be multi-path HA**
.
.
.
slot 0: FC Host Adapter 0g (QLogic 8324 rev. 2, N-port, <UP>)**<===
Initiator port**
        Firmware rev:      7.5.0
        Flash rev:         0.0.0
        Host Port Id:      0x60130
        FC Node Name:      5:00a:098201:bae312
        FC Port Name:      5:00a:098201:bae312
        SFP Vendor:        UTILITIES CORP.
        SFP Part Number:   FTLF8529P3BCVAN1
        SFP Serial Number: URQ0Q9R
        SFP Capabilities:  4, 8 or 16 Gbit
        Link Data Rate:    16 Gbit
        Switch Port:       brcd6505-fcs40:1
  **<List of disks visible to port\>**
         ID     Vendor   Model            FW    Size
        brcd6505-fcs29:12.126L1527     : NETAPP   X302_HJUPI01TSSM NA04
847.5GB (1953525168 512B/sect)
        brcd6505-fcs29:12.126L1528     : NETAPP   X302_HJUPI01TSSA NA02
847.5GB (1953525168 512B/sect)
        .
        .
        .
        **<List of FC-to-SAS bridges visible to port\>**
        FC-to-SAS Bridge:
        brcd6505-fcs40:12.126L0        : ATTO     FibreBridge6500N 1.61
FB6500N102980
        brcd6505-fcs42:13.126L0        : ATTO     FibreBridge6500N 1.61
FB6500N102980
        brcd6505-fcs42:6.126L0         : ATTO     FibreBridge6500N 1.61
FB6500N101167
        brcd6505-fcs42:7.126L0         : ATTO     FibreBridge6500N 1.61
FB6500N102974
        .
        .
        .
```

```
  **<List of storage shelves visible to port\>**
        brcd6505-fcs40:12.shelf6: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        brcd6505-fcs40:12.shelf8: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        .
        .
        .
```

同じモデルの交換用ブリッジとのホットスワップ

障害が発生したブリッジを同じモデルの別のブリッジとホットスワップすることができます。

このタスクについて

IP 管理ではなくブリッジのインバンド管理を使用する場合は、該当する手順に記載されているように、イーサネットポートと IP を設定する手順を省略できます。

ONTAP 9.8 以降では 'storage bridge コマンドは 'system bridge コマンドに置き換えられました次の手順は「 storage bridge 」コマンドを示していますが、 ONTAP 9.8 以降を実行している場合は「 system bridge 」コマンドが優先されます。

手順

1. 古いブリッジにアクセスできる場合は、設定情報を取得できます。

状況	作業
• IP 管理 * を使用しています	Telnet 接続を使用して古いブリッジに接続し、ブリッジ設定の出力をコピーします。
• インバンド管理 * を使用しています	次のコマンドを使用して、 ONTAP CLI を使用して設定情報を取得します。 storage bridge run -cli-name_bridge-name_command "info"`  「 storage bridge run -cli-name_bridge-name_command "sasportlist"` 」」

a. 入力するコマンド

   storage bridge run-cli-name bridge_A1 コマンド「 info

```
info

Device Status          = Good
Unsaved Changes        = None
Device                 = "FibreBridge 7500N"
Serial Number          = FB7500N100000
```

```
Device Version        = 3.10
Board Revision        = 7
Build Number          = 007A
Build Type            = Release
Build Date            = "Aug 20 2019" 11:01:24
Flash Revision        = 0.02
Firmware Version      = 3.10
BCE Version (FPGA 1)  = 15
BAU Version (FPGA 2)  = 33
User-defined name     = "bridgeA1"
World Wide Name       = 20 00 00 10 86 A1 C7 00
MB of RAM Installed   = 512
FC1 Node Name         = 20 00 00 10 86 A1 C7 00
FC1 Port Name         = 21 00 00 10 86 A1 C7 00
FC1 Data Rate         = 16Gb
FC1 Connection Mode   = ptp
FC1 FW Revision       = 11.4.337.0
FC2 Node Name         = 20 00 00 10 86 A1 C7 00
FC2 Port Name         = 22 00 00 10 86 A1 C7 00
FC2 Data Rate         = 16Gb
FC2 Connection Mode   = ptp
FC2 FW Revision       = 11.4.337.0
SAS FW Revision       = 3.09.52
MP1 IP Address        = 10.10.10.10
MP1 IP Subnet Mask    = 255.255.255.0
MP1 IP Gateway        = 10.10.10.1
MP1 IP DHCP           = disabled
MP1 MAC Address       = 00-10-86-A1-C7-00
MP2 IP Address        = 0.0.0.0 (disabled)
MP2 IP Subnet Mask    = 0.0.0.0
MP2 IP Gateway        = 0.0.0.0
MP2 IP DHCP           = enabled
MP2 MAC Address       = 00-10-86-A1-C7-01
SNMP                  = enabled
SNMP Community String = public
PS A Status           = Up
PS B Status           = Up
Active Configuration  = NetApp

Ready.
```

b. 入力するコマンド

「 storage bridge run -cli-name bridge_A1 - コマンド「 sasportlist 」

```
SASPortList

;Connector      PHY     Link            Speed   SAS Address
;============================================================
Device  A       1       Up              6Gb     5001086000a1c700
Device  A       2       Up              6Gb     5001086000a1c700
Device  A       3       Up              6Gb     5001086000a1c700
Device  A       4       Up              6Gb     5001086000a1c700
Device  B       1       Disabled        12Gb    5001086000a1c704
Device  B       2       Disabled        12Gb    5001086000a1c704
Device  B       3       Disabled        12Gb    5001086000a1c704
Device  B       4       Disabled        12Gb    5001086000a1c704
Device  C       1       Disabled        12Gb    5001086000a1c708
Device  C       2       Disabled        12Gb    5001086000a1c708
Device  C       3       Disabled        12Gb    5001086000a1c708
Device  C       4       Disabled        12Gb    5001086000a1c708
Device  D       1       Disabled        12Gb    5001086000a1c70c
Device  D       2       Disabled        12Gb    5001086000a1c70c
Device  D       3       Disabled        12Gb    5001086000a1c70c
Device  D       4       Disabled        12Gb    5001086000a1c70c
```

2. ブリッジがファブリック接続 MetroCluster 構成に含まれている場合は、ブリッジの FC ポートに接続しているすべてのスイッチポートを無効にします。
3. ONTAP クラスタのプロンプトで、メンテナンス中のブリッジをヘルスモニタの対象から削除します。
   a. ブリッジ `+storage bridge remove-name_bridge-name_` を削除します
   b. 監視対象のブリッジのリストを表示し、削除したブリッジが含まれていないことを確認します。
      `+storage bridge show`
4. 自身の適切な接地対策を行います
5. ATTOブリッジの電源をオフにし、ブリッジに接続されている電源ケーブルを取り外します。
6. 古いブリッジに接続されているケーブルを外します。

   各ケーブルが接続されていたポートをメモしておいてください。
7. ラックから古いブリッジを取り外します。
8. 新しいブリッジをラックに取り付けます。
9. 電源コードを再接続します。また、ブリッジへの IP アクセスを設定する場合は、シールド付きイーサネットケーブルを再接続します。

   SAS / FC ケーブルはまだ再接続しないでください。
10. ブリッジを電源に接続し、電源をオンにします。

    ブリッジの準備完了を示す LED が点灯し、ブリッジの電源投入時自己診断テストが完了したことを示す

まで、 30 秒ほどかかる場合があります。

11. インバンド管理用に設定する場合は、 FibreBridge RS-232 シリアルポートから PC のシリアル（ COM ）ポートにケーブルを接続します。

    シリアル接続は初期設定と ONTAP によるインバンド管理に使用され、 FC ポートを使用してブリッジの監視と管理を行うことができます。

12. IP 管理用に設定する場合は、使用しているブリッジモデルの ATTO FibreBridge Installation and Operation Manual _ のセクション 2.0 の手順に従って、各ブリッジのイーサネット管理 1 ポートを設定します。

    ONTAP 9.5 以降を実行しているシステムでは、インバンド管理を使用してイーサネットポートではなく FC ポート経由でブリッジにアクセスできます。ONTAP 9.8 以降では、インバンド管理のみがサポートされ、 SNMP 管理は廃止されています。

    QuickNAV を実行してイーサネット管理ポートを設定すると、イーサネットケーブルで接続されているイーサネット管理ポートのみが設定されます。たとえば、イーサネット管理 2 ポートも設定する場合は、イーサネットケーブルをポート 2 に接続して QuickNAV を実行する必要があります。

13. ブリッジを設定します。

    古いブリッジから設定情報を取得した場合は、その情報を使用して新しいブリッジを設定します。

    指定するユーザ名とパスワードは必ずメモしてください。

    使用しているブリッジモデルに対応する _ATTO FibreBridge Installation and Operation Manual _ に、使用可能なコマンドおよびその使用方法に関する最新情報が記載されています。

    > ATTO FibreBridge 7600N または 7500N では時刻同期は設定しないでください。ATTO FibreBridge 7600N または 7500N の時刻は、 ONTAP でブリッジが検出されたあとにクラスタ時間に設定されます。また、 1 日に 1 回定期的に同期されます。使用されるタイムゾーンは GMT で、変更することはできません。

    a. IP 管理用に設定する場合は、ブリッジの IP 設定を行います。

       Quicknav ユーティリティなしで IP アドレスを設定するには、 FibreBridge に対するシリアル接続が必要です。

       CLI を使用する場合は、次のコマンドを実行する必要があります。

       'set ipaddress mp1_ip-address'

       'set ipsubnetmask mp1_subnet-mask_

       'set ipgateway mp1x.x'

       'set ipdhcp mp1 disabled

       「 setethernetspeed mp1 1000」

    b. ブリッジ名を設定します。

       ブリッジ名は、 MetroCluster 構成内でそれぞれ一意である必要があります。

各サイトの 1 つのスタックグループのブリッジ名の例：

- bridge_A_1a
- bridge_A_1b
- bridge_B_1a
- bridge_B_1b

CLI を使用する場合は、次のコマンドを実行する必要があります。

「 set bridgename _bridgename _ 」を入力します

c. ONTAP 9.4 以前を実行している場合は、ブリッジで SNMP を有効にします。

'Set SNMP enabled

ONTAP 9.5 以降を実行しているシステムでは、インバンド管理を使用してイーサネットポートではなく FC ポート経由でブリッジにアクセスできます。ONTAP 9.8 以降では、インバンド管理のみがサポートされ、 SNMP 管理は廃止されています。

14. ブリッジの FC ポートを設定します。

a. ブリッジ FC ポートのデータ速度を設定します。

サポートされる FC データ速度は、モデルブリッジによって異なります。

- FibreBridge 7600Nブリッジは、最大32、16、または8Gbpsをサポートします。
- FibreBridge 7500Nブリッジは、最大16、8、または4Gbpsをサポートします。

選択できる FCDataRate の速度は、ブリッジポートを接続するブリッジとスイッチの両方でサポートされる最大速度以下です。ケーブルでの接続距離が SFP およびその他のハードウェアの制限を超えないようにしてください。

CLI を使用する場合は、次のコマンドを実行する必要があります。

'set FCDataRate_port-number port-speed_

b. FibreBridge 7500Nを設定する場合は、ポートで使用する接続モードを「ptp」に設定します。

FibreBridge 7600N ブリッジを設定する場合、 FCConnMode の設定は不要です。

CLI を使用する場合は、次のコマンドを実行する必要があります。

'et FCConnMode_port-number_ptc'

c. FibreBridge 7600N / 7500N ブリッジを設定する場合は、 FC2 ポートを設定または無効にする必要があります。

- 2 番目のポートを使用する場合は、 FC2 ポートについて同じ手順を繰り返す必要があります。
- 2 番目のポートを使用しない場合は、ポートを無効にする必要があります。

FCPGortDisable_port-number_`

d. FibreBridge 7600N / 7500N ブリッジを設定する場合は、未使用の SAS ポートを無効にします。

'ASPortDisable_SAS-PORT_'

SAS ポート A~D はデフォルトで有効になります。使用していない SAS ポートを無効にする必要があります。SAS ポート A のみを使用している場合は、 SAS ポート B 、 C 、および D を無効にする必要があります。

15. ブリッジへのアクセスを保護し、ブリッジの設定を保存します。

a. コントローラのプロンプトで、ブリッジのステータスを確認します。「 storage bridge show 」

出力には、保護されていないブリッジが表示されます。

b. セキュリティ保護されていないブリッジのポートのステータスを確認します。

「 info 」のようになります

出力には、イーサネットポート MP1 と MP2 のステータスが表示されます。

c. イーサネットポート MP1 がイネーブルの場合は、次のコマンドを実行します。

「 Set EthernetPort mp1 disabled 」です

イーサネットポート MP2 も有効になっている場合は、ポート MP2 について前の手順を繰り返します。

d. ブリッジの設定を保存します。

次のコマンドを実行する必要があります。

'aveConfiguration'

「 FirmwareRestart 」と入力します

ブリッジを再起動するように求められます。

16. FCケーブルを新しいブリッジの同じポートに接続します。

17. 各ブリッジの FibreBridge ファームウェアを更新します。

新しいブリッジのタイプがパートナーブリッジと同じ場合は、パートナーブリッジと同じファームウェアにアップグレードします。新しいブリッジのタイプがパートナーブリッジと異なる場合は、ブリッジおよびONTAPのバージョンでサポートされている最新のファームウェアにアップグレードします。を参照し "FibreBridge ブリッジのファームウェアを更新しています"

18. [step18-reconnect-newbridge]新しいブリッジの同じポートにSASケーブルを再接続します。

ブリッジをシェルフスタックの上部または下部に接続するケーブルを交換する必要があります。FibreBridge 7600N / 7500Nブリッジの接続にはMini-SASケーブルが必要です。

ポートを接続する前に、 10 秒以上待機します。SAS ケーブルのコネクタは、誤挿入を防ぐキーイングが施されているため、正しい向きで SAS ポートに取り付けるとカチッとはまり、ディスクシェルフの SAS ポートの LNK LED が緑色に点灯します。ディスクシェルフの場合は、 SAS ケーブルのコネクタをプルタブ（コネクタの下側）を下にして挿入します。コントローラの場合は、プラットフォームのモデルによって SAS ポートの向きが異なるため、 SAS ケーブルのコネクタの正しい向きもそれに応じて異なります。

19. [[step19-verify-backup -each -bridge]] ブリッジが接続されているすべてのディスクドライブとディスクシェルフを各ブリッジで認識できることを確認します。

使用する手段	作業
ATTO ExpressNAV の GUI	a. サポートされている Web ブラウザで、ブリッジの IP アドレスをブラウザのアドレスバーに入力します。 ATTO FibreBridge のホームページに移動し、リンクが表示されます。 b. リンクをクリックし、ブリッジを設定するときに指定したユーザ名とパスワードを入力します。 ATTO FibreBridge のステータスページが開き、左側にメニューが表示されます。 c. メニューの「 * 詳細設定 * 」をクリックします。 d. 接続されているデバイスを表示します。 「 astargets 」 e. [Submit （送信）] をクリックします。
シリアルポート接続	接続されているデバイスを表示します。 「 astargets 」

出力には、ブリッジが接続されているデバイス（ディスクおよびディスクシェルフ）が表示されます。出力行には行番号が振られているため、デバイスの台数を簡単に把握できます。

出力の先頭に response truncated というテキストが表示される場合は、 Telnet を使用してブリッジに接続し、 'sastargets' コマンドを使用してすべての出力を確認できます。

次の出力は、 10 本のディスクが接続されていることを示します。

```
Tgt VendorID ProductID         Type SerialNumber
  0 NETAPP   X410_S15K6288A15 DISK 3QP1CLE300009940UHJV
  1 NETAPP   X410_S15K6288A15 DISK 3QP1ELF600009940V1BV
  2 NETAPP   X410_S15K6288A15 DISK 3QP1G3EW00009940U2M0
  3 NETAPP   X410_S15K6288A15 DISK 3QP1EWMP00009940U1X5
  4 NETAPP   X410_S15K6288A15 DISK 3QP1FZLE00009940G8YU
  5 NETAPP   X410_S15K6288A15 DISK 3QP1FZLF00009940TZKZ
  6 NETAPP   X410_S15K6288A15 DISK 3QP1CEB400009939MGXL
  7 NETAPP   X410_S15K6288A15 DISK 3QP1G7A900009939FNTT
  8 NETAPP   X410_S15K6288A15 DISK 3QP1FY0T00009940G8PA
  9 NETAPP   X410_S15K6288A15 DISK 3QP1FXW600009940VERQ
```

20. コマンド出力で、スタック内の該当するすべてのディスクおよびディスクシェルフにブリッジが接続されていることを確認します。

出力結果	作業
正解です	ステップ19残りのブリッジについて、この手順を繰り返します。
不正解です	a. SASケーブルに緩みがないかどうかを確認するか、を繰り返してSASケーブル接続を修正します手順 18。 b. 繰り返しますステップ19。

21. ブリッジがファブリック接続 MetroCluster 構成に含まれている場合は、この手順の最初で無効にした FC スイッチポートを再度有効にします。

    このポートはブリッジに接続されている必要があります。

22. 両方のコントローラモジュールのシステムコンソールで、すべてのコントローラモジュールが新しいブリッジを介してディスクシェルフにアクセスできる（つまりシステムがマルチパス HA 用に接続されている）ことを確認します。

    「 run local sysconfig 」を実行します

    システムで検出が完了するまで、 1 分程度かかる場合があります。

    出力がマルチパス HA を示していない場合は、新しいブリッジを介してアクセスできないディスクドライブがあるため、 SAS と FC のケーブル接続を修正する必要があります。

    次の出力は、システムがマルチパス HA 用に接続されていることを示しています。

```
NetApp Release 8.3.2: Tue Jan 26 01:41:49 PDT 2016
System ID: 1231231231 (node_A_1); partner ID: 4564564564 (node_A_2)
System Serial Number: 700000123123 (node_A_1); partner Serial Number:
700000456456 (node_A_2)
System Rev: B0
System Storage Configuration: Multi-Path HA
System ACP Connectivity: NA
```

システムがマルチパス HA 構成で接続されていないと、ブリッジを再起動したときに、ディスクドライブへのアクセスが原因で失われて、複数のディスクがパニック状態になることがあります。

23. ONTAP 9.4 以前を実行している場合は、ブリッジが SNMP 用に設定されていることを確認します。

    ブリッジの CLI を使用している場合は、次のコマンドを実行します。

    ```
    get snmp
    ```

24. ONTAP クラスタのプロンプトで、ブリッジをヘルスモニタの対象に追加します。

    a. 使用している ONTAP のバージョンに対応したコマンドを使用して、ブリッジを追加します。

ONTAP バージョン	コマンドを実行します
9.5 以降	「 storage bridge add -address 0.0.0.0 -managed-by in-band-name_bridge-name_`
9.4 以前	「 storage bridge add -address_bridge-ip-address_-name_bridge-name_` 」

    b. ブリッジが追加され、正しく設定されていることを確認します。

    「 storage bridge show 」

    ポーリング間隔に応じて、すべてのデータが反映されるまで 15 分程度かかる場合があります。ONTAP ヘルスモニタは、「 Status 」列の値が「 ok 」で、ワールドワイド名（ WWN ）などのその他の情報が表示されていれば、ブリッジに接続して監視できます。

    次の例は、 FC-to-SAS ブリッジが設定されていることを示しています。

```
controller_A_1::> storage bridge show

Bridge               Symbolic Name Is Monitored  Monitor Status  Vendor
Model                 Bridge WWN
------------------  ------------ ------------  --------------  ------
-----------------    ----------
ATTO_10.10.20.10  atto01        true          ok              Atto
FibreBridge 7500N      20000010867038c0
ATTO_10.10.20.11  atto02        true          ok              Atto
FibreBridge 7500N      20000010867033c0
ATTO_10.10.20.12  atto03        true          ok              Atto
FibreBridge 7500N      20000010867030c0
ATTO_10.10.20.13  atto04        true          ok              Atto
FibreBridge 7500N      2000001086703b80

4 entries were displayed

 controller_A_1::>
```

25. ONTAP で MetroCluster 構成の動作を確認します。
    a. システムがマルチパスであるかどうかを確認します :+`node run -node -node_name sysconfig -a`
    b. 両方のクラスタにヘルス・アラートがないかどうかを確認します +`system health alert show`
    c. MetroCluster 構成と動作モードが正常であることを確認します。 + MetroCluster show `
    d. MetroCluster チェックを実行します + MetroCluster チェックを実行します
    e. MetroCluster チェックの結果を表示します :+`MetroCluster check show`
    f. スイッチにヘルス・アラートがあるかどうかを確認します（ある場合）： +`storage switch show`
    g. Config Advisor を実行します。

       "ネットアップのダウンロード： Config Advisor"

    h. Config Advisor の実行後、ツールの出力を確認し、推奨される方法で検出された問題に対処します。

関連情報

"FC-to-SAS ブリッジのインバンド管理"

FibreBridge 7500N と 7600N ブリッジのホットスワップ

FibreBridge 7500N ブリッジと 7600N ブリッジをホットスワップできます。

このタスクについて

IP 管理ではなくブリッジのインバンド管理を使用する場合は、該当する手順に記載されているように、イーサネットポートと IP を設定する手順を省略できます。

ONTAP 9.8 以降では 'storage bridge コマンドは 'system bridge コマンドに置き換えられました 次の手順は「 storage bridge 」コマンドを示していますが、 ONTAP 9.8 以降を実行している場合は「 system bridge 」コマンドが優先されます。

手順

1. ブリッジがファブリック接続 MetroCluster 構成に含まれている場合は、ブリッジの FC ポートに接続しているすべてのスイッチポートを無効にします。
2. ONTAP クラスタのプロンプトで、メンテナンス中のブリッジをヘルスモニタの対象から削除します。
   a. ブリッジ `+storage bridge remove-name_bridge-name_` を削除します
   b. 監視対象のブリッジのリストを表示し、削除したブリッジが含まれていないことを確認します。 `+storage bridge show`
3. 自身の適切な接地対策を行います
4. ブリッジに接続されている電源ケーブルを外して、ブリッジの電源をオフにします。
5. 古いブリッジに接続されているケーブルを外します。

   各ケーブルが接続されていたポートをメモしておいてください。
6. ラックから古いブリッジを取り外します。
7. 新しいブリッジをラックに取り付けます。
8. 電源コードとシールド付きイーサネットケーブルを再接続します。

   SAS / FC ケーブルはまだ再接続しないでください。
9. ブリッジを電源に接続し、電源をオンにします。

   ブリッジの準備完了を示す LED が点灯し、ブリッジの電源投入時自己診断テストが完了したことを示すまで、 30 秒ほどかかる場合があります。
10. インバンド管理用に設定する場合は、 FibreBridge RS-232 シリアルポートから PC のシリアル（ COM ）ポートにケーブルを接続します。

    シリアル接続は初期設定と ONTAP によるインバンド管理に使用され、 FC ポートを使用してブリッジの監視と管理を行うことができます。
11. インバンド管理用に設定する場合は、 FibreBridge RS-232 シリアルポートから PC のシリアル（ COM ）ポートにケーブルを接続します。

    シリアル接続は初期設定と ONTAP によるインバンド管理に使用され、 FC ポートを使用してブリッジの監視と管理を行うことができます。
12. IP 管理用に設定する場合は、使用しているブリッジモデルの ATTO FibreBridge Installation and Operation Manual _ のセクション 2.0 の手順に従って、各ブリッジのイーサネット管理 1 ポートを設定します。

    ONTAP 9.5 以降を実行しているシステムでは、インバンド管理を使用してイーサネットポートではなく FC ポート経由でブリッジにアクセスできます。ONTAP 9.8 以降では、インバンド管理のみがサポートされ、 SNMP 管理は廃止されています。

QuickNAV を実行してイーサネット管理ポートを設定すると、イーサネットケーブルで接続されているイーサネット管理ポートのみが設定されます。たとえば、イーサネット管理 2 ポートも設定する場合は、イーサネットケーブルをポート 2 に接続して QuickNAV を実行する必要があります。

13. ブリッジを設定します。

    指定するユーザ名とパスワードは必ずメモしてください。

    使用しているブリッジモデルに対応する _ATTO FibreBridge Installation and Operation Manual _ に、使用可能なコマンドおよびその使用方法に関する最新情報が記載されています。

    FibreBridge 7600N では時刻同期は設定しないでください。FibreBridge 7600N の時刻は、ONTAP でブリッジが検出されたあとにクラスタ時間に設定されます。また、 1 日に 1 回定期的に同期されます。使用されるタイムゾーンは GMT で、変更することはできません。

    a. IP 管理用に設定する場合は、ブリッジの IP 設定を行います。

       Quicknav ユーティリティなしで IP アドレスを設定するには、 FibreBridge に対するシリアル接続が必要です。

       CLI を使用する場合は、次のコマンドを実行する必要があります。

       'set ipaddress mp1_ip-address_'

       'set ipsubnetmask mp1_subnet-mask_

       'set ipgateway mp1x.x'

       'set ipdhcp mp1 disabled

       「 setethernetspeed mp1 1000」

    b. ブリッジ名を設定します。

       ブリッジ名は、 MetroCluster 構成内でそれぞれ一意である必要があります。

       各サイトの 1 つのスタックグループのブリッジ名の例：

       - bridge_A_1a
       - bridge_A_1b
       - bridge_B_1a
       - bridge_B_1b

         CLI を使用する場合は、次のコマンドを実行する必要があります。

    「 set bridgename _bridgename _ 」を入力します

    a. ONTAP 9.4 以前を実行している場合は、ブリッジで SNMP を有効にします。 +'set snmp enabled'

       ONTAP 9.5 以降を実行しているシステムでは、インバンド管理を使用してイーサネットポートではなく FC ポート経由でブリッジにアクセスできます。ONTAP 9.8 以降では、インバンド管理のみがサポートされ、 SNMP 管理は廃止されています。

14. ブリッジの FC ポートを設定します。

    a. ブリッジ FC ポートのデータ速度を設定します。

    サポートされる FC データ速度は、モデルブリッジによって異なります。

    - FibreBridge 7600Nブリッジは、最大32、16、または8Gbpsをサポートします。
    - FibreBridge 7500Nブリッジは、最大16、8、または4Gbpsをサポートします。

    > ⓘ 選択できる FCDataRate の速度は、ブリッジポートを接続するコントローラモジュールまたはスイッチのブリッジ / FC ポートの両方でサポートされる最大速度以下です。ケーブルでの接続距離が SFP およびその他のハードウェアの制限を超えないようにしてください。

    CLI を使用する場合は、次のコマンドを実行する必要があります。

    'set FCDataRate_port-number port-speed_

    b. FC2 ポートを設定または無効にする必要があります。

    - 2 番目のポートを使用する場合は、 FC2 ポートについて同じ手順を繰り返す必要があります。
    - 2 番目のポートを使用しない場合は、未使用のポートを無効にする必要があります。

    FCPGPortDisable ポート番号

    次に、 FC ポート 2 を無効にする例を示します。

    ```
    FCPortDisable 2

    Fibre Channel Port 2 has been disabled.
    ```

    c. 未使用の SAS ポートを無効にします。

    'ASPortDisable_SAS-PORT_'

    > ⓘ SAS ポート A~D はデフォルトで有効になります。使用していない SAS ポートを無効にする必要があります。

    SAS ポート A のみを使用している場合は、 SAS ポート B 、 C 、および D を無効にする必要があります。次の例では、 SAS ポート B を無効にしていますSAS ポート C および D についても、同じように無効にする必要があります。

    ```
    SASPortDisable b

    SAS Port B has been disabled.
    ```

15. ブリッジへのアクセスを保護し、ブリッジの設定を保存します。

a. コントローラのプロンプトで、ブリッジのステータスを確認します。

「 storage bridge show 」

出力には、保護されていないブリッジが表示されます。

b. セキュリティ保護されていないブリッジのポートのステータスを確認します。

「 info 」のようになります

出力には、イーサネットポート MP1 と MP2 のステータスが表示されます。

c. イーサネットポート MP1 がイネーブルの場合は、次のコマンドを実行します。

「 Set EthernetPort mp1 disabled 」です

イーサネットポート MP2 も有効になっている場合は、ポート MP2 について前の手順を繰り返します。

d. ブリッジの設定を保存します。

次のコマンドを実行する必要があります： +

'aveConfiguration'

「 FirmwareRestart 」と入力します

ブリッジを再起動するように求められます。

16. FCケーブルを新しいブリッジの同じポートに接続します。
17. 各ブリッジの FibreBridge ファームウェアを更新します。

"FibreBridge ブリッジのファームウェアを更新します"

18. [step18-reconnect-cables]]新しいブリッジの同じポートにSASケーブルを再接続します。

ポートを接続する前に、 10 秒以上待機します。SAS ケーブルのコネクタは、誤挿入を防ぐキーイングが施されているため、正しい向きで SAS ポートに取り付けるとカチッとはまり、ディスクシェルフの SAS ポートの LNK LED が緑色に点灯します。ディスクシェルフの場合は、 SAS ケーブルのコネクタをプルタブ（コネクタの下側）を下にして挿入します。コントローラの場合は、プラットフォームのモデルによって SAS ポートの向きが異なるため、 SAS ケーブルのコネクタの正しい向きもそれに応じて異なります。

19. 各ブリッジが、ブリッジの接続先のすべてのディスクドライブとディスクシェルフを認識できることを確認します。

「 astargets 」

出力には、ブリッジが接続されているデバイス（ディスクおよびディスクシェルフ）が表示されます。出力行には行番号が振られているため、デバイスの台数を簡単に把握できます。

次の出力は、 10 本のディスクが接続されていることを示します。

```
Tgt VendorID ProductID         Type        SerialNumber
  0 NETAPP   X410_S15K6288A15 DISK        3QP1CLE300009940UHJV
  1 NETAPP   X410_S15K6288A15 DISK        3QP1ELF600009940V1BV
  2 NETAPP   X410_S15K6288A15 DISK        3QP1G3EW00009940U2M0
  3 NETAPP   X410_S15K6288A15 DISK        3QP1EWMP00009940U1X5
  4 NETAPP   X410_S15K6288A15 DISK        3QP1FZLE00009940G8YU
  5 NETAPP   X410_S15K6288A15 DISK        3QP1FZLF00009940TZKZ
  6 NETAPP   X410_S15K6288A15 DISK        3QP1CEB400009939MGXL
  7 NETAPP   X410_S15K6288A15 DISK        3QP1G7A900009939FNTT
  8 NETAPP   X410_S15K6288A15 DISK        3QP1FY0T00009940G8PA
  9 NETAPP   X410_S15K6288A15 DISK        3QP1FXW600009940VERQ
```

20. コマンド出力で、スタック内の該当するすべてのディスクおよびディスクシェルフにブリッジが接続されていることを確認します。

出力結果	作業
正解です	残りの各ブリッジについて、同じ手順を繰り返します。
不正解です	a. SASケーブルに緩みがないかどうかを確認するか、を繰り返してSASケーブル接続を修正します手順 18。 b. 前の手順を繰り返します。

21. ブリッジがファブリック接続 MetroCluster 構成に含まれている場合は、この手順の最初で無効にした FC スイッチポートを再度有効にします。

    このポートはブリッジに接続されている必要があります。

22. 両方のコントローラモジュールのシステムコンソールで、すべてのコントローラモジュールが新しいブリッジを介してディスクシェルフにアクセスできる（つまりシステムがマルチパス HA 用に接続されている）ことを確認します。

    「 run local sysconfig 」を実行します

    システムで検出が完了するまで、 1 分程度かかる場合があります。

    出力がマルチパス HA を示していない場合は、新しいブリッジを介してアクセスできないディスクドライブがあるため、 SAS と FC のケーブル接続を修正する必要があります。

    次の出力は、システムがマルチパス HA 用に接続されていることを示しています。

```
NetApp Release 8.3.2: Tue Jan 26 01:41:49 PDT 2016
System ID: 1231231231 (node_A_1); partner ID: 4564564564 (node_A_2)
System Serial Number: 700000123123 (node_A_1); partner Serial Number:
700000456456 (node_A_2)
System Rev: B0
System Storage Configuration: Multi-Path HA
System ACP Connectivity: NA
```

システムがマルチパス HA 構成で接続されていないと、ブリッジを再起動したときに、ディスクドライブへのアクセスが原因で失われて、複数のディスクがパニック状態になることがあります。

23. ONTAP 9.4 以前を実行している場合は、ブリッジが SNMP 用に設定されていることを確認します。

    ブリッジの CLI を使用している場合は、次のコマンドを実行します。

    'SNMP の取得

24. ONTAP クラスタのプロンプトで、ブリッジをヘルスモニタの対象に追加します。

    a. 使用している ONTAP のバージョンに対応したコマンドを使用して、ブリッジを追加します。

ONTAP バージョン	コマンドを実行します
9.5 以降	「 storage bridge add -address 0.0.0.0 -managed-by in-band-name_bridge-name_`
9.4 以前	「 storage bridge add -address_bridge-ip-address_-name_bridge-name_` 」

    b. ブリッジが追加され、正しく設定されていることを確認します。

    「 storage bridge show 」

    ポーリング間隔に応じて、すべてのデータが反映されるまで 15 分程度かかる場合があります。ONTAP ヘルスモニタは、「 Status 」列の値が「 ok 」で、ワールドワイド名（ WWN ）などのその他の情報が表示されていれば、ブリッジに接続して監視できます。

    次の例は、 FC-to-SAS ブリッジが設定されていることを示しています。

```
controller_A_1::> storage bridge show

Bridge                Symbolic Name Is Monitored  Monitor Status  Vendor
Model                  Bridge WWN
------------------  ------------ ------------  --------------  ------
-----------------    ----------
ATTO_10.10.20.10  atto01        true          ok              Atto
FibreBridge 7500N      20000010867038c0
ATTO_10.10.20.11  atto02        true          ok              Atto
FibreBridge 7500N      20000010867033c0
ATTO_10.10.20.12  atto03        true          ok              Atto
FibreBridge 7500N      20000010867030c0
ATTO_10.10.20.13  atto04        true          ok              Atto
FibreBridge 7500N      2000001086703b80

4 entries were displayed

 controller_A_1::>
```

25. ONTAP で MetroCluster 構成の動作を確認します。
    a. システムがマルチパスであるかどうかを確認します :+`node run -node -node_name sysconfig -a`
    b. 両方のクラスタにヘルス・アラートがないかどうかを確認します +`system health alert show`
    c. MetroCluster 構成と動作モードが正常であることを確認します。 + MetroCluster show `
    d. MetroCluster チェックを実行します + MetroCluster チェックを実行します
    e. MetroCluster チェックの結果を表示します： +

       MetroCluster チェックショー

    f. スイッチにヘルス・アラートがあるかどうかを確認します（ある場合）： +`storage switch show`
    g. Config Advisor を実行します。

       "ネットアップのダウンロード： Config Advisor"

    h. Config Advisor の実行後、ツールの出力を確認し、推奨される方法で検出された問題に対処します。

関連情報

"FC-to-SAS ブリッジのインバンド管理"

FibreBridge 6500N ブリッジと FibreBridge 7600N / 7500N ブリッジのホットスワップ

FibreBridge 6500N ブリッジと FibreBridge 7600N / 7500N ブリッジをホットスワップして、障害が発生したブリッジを交換したり、ファブリック接続またはブリッジ接続 MetroCluster 構成のブリッジをアップグレードしたりできます。

このタスクについて

- この手順は、 1 つの FibreBridge 6500N ブリッジを 1 つの FibreBridge 7600N / 7500N ブリッジとホットスワップするためのものです。
- FibreBridge 6500N ブリッジと FibreBridge 7600N / 7500N ブリッジをホットスワップする場合は、 FibreBridge 7600N / 7500N ブリッジの FC ポートと SAS ポートをそれぞれ 1 つだけ使用する必要があります。
- IP 管理ではなくブリッジのインバンド管理を使用する場合は、該当する手順に記載されているように、イーサネットポートと IP を設定する手順を省略できます。

FibreBridge 6500N ブリッジペアの両方をホットスワップする場合は、を使用する必要があります "複数のストレージスタックを統合" ゾーニング手順については手順を参照してください。両方の FibreBridge 6500N ブリッジを交換することで、 FibreBridge 7600N / 7500N ブリッジの追加ポートを活用できます。

ONTAP 9.8 以降では 'storage bridge コマンドは 'system bridge コマンドに置き換えられました次の手順は「 storage bridge 」コマンドを示していますが、 ONTAP 9.8 以降を実行している場合は「 system bridge 」コマンドが優先されます。

手順

1. 次のいずれかを実行します。
   - 障害が発生したブリッジがファブリック接続 MetroCluster 構成に含まれている場合は、ブリッジ FC ポートに接続するスイッチポートを無効にします。
   - 障害が発生したブリッジがストレッチ MetroCluster 構成である場合は、使用可能ないずれかの FC ポートを使用します。
2. ONTAP クラスタのプロンプトで、メンテナンス中のブリッジをヘルスモニタの対象から削除します。
   a. ブリッジを削除します。

      storage bridge remove-name_bridge-name_`

   b. 監視中のブリッジのリストを表示し、削除したブリッジが含まれていないことを確認します。

      「 storage bridge show 」
3. 自身の適切な接地対策を行います
4. ブリッジの電源スイッチをオフにします。
5. シェルフから FibreBridge 6500N ブリッジのポートに接続されているケーブルおよび電源ケーブルを外します。

   各ケーブルが接続されていたポートをメモしておいてください。
6. 交換が必要な FibreBridge 6500N ブリッジをラックから取り外します。
7. 新しい FibreBridge 7600N / 7500N ブリッジをラックに取り付けます。
8. 電源コードを再接続し、必要に応じてシールド付きイーサネットケーブルを再接続します。

   SAS / FC ケーブルはまだ再接続しないでください。

9. インバンド管理用に設定する場合は、 FibreBridge RS-232 シリアルポートから PC のシリアル（ COM ）ポートにケーブルを接続します。

   シリアル接続は初期設定と ONTAP によるインバンド管理に使用され、 FC ポートを使用してブリッジの監視と管理を行うことができます。

10. IP 管理用に設定する場合は、イーサネットケーブルを使用して、各ブリッジのイーサネット管理 1 ポートをネットワークに接続します。

    ONTAP 9.5 以降を実行しているシステムでは、インバンド管理を使用してイーサネットポートではなく FC ポート経由でブリッジにアクセスできます。ONTAP 9.8 以降では、インバンド管理のみがサポートされ、 SNMP 管理は廃止されています。

    イーサネット管理 1 ポートを使用すると、ブリッジファームウェアを短時間でダウンロードし（ ATTO ExpressNAV または FTP 管理インターフェイスを使用）、コアファイルと抽出ログを取得できます。

11. IP 管理用に設定する場合は、使用しているブリッジモデルの ATTO FibreBridge Installation and Operation Manual _ のセクション 2.0 の手順に従って、各ブリッジのイーサネット管理 1 ポートを設定します。

    ONTAP 9.5 以降を実行しているシステムでは、インバンド管理を使用してイーサネットポートではなく FC ポート経由でブリッジにアクセスできます。ONTAP 9.8 以降では、インバンド管理のみがサポートされ、 SNMP 管理は廃止されています。

    QuickNAV を実行してイーサネット管理ポートを設定すると、イーサネットケーブルで接続されているイーサネット管理ポートのみが設定されます。たとえば、イーサネット管理 2 ポートも設定する場合は、イーサネットケーブルをポート 2 に接続して QuickNAV を実行する必要があります。

12. ブリッジを設定します。

    古いブリッジから設定情報を取得した場合は、その情報を使用して新しいブリッジを設定します。

    指定するユーザ名とパスワードは必ずメモしてください。

    使用しているブリッジモデルに対応する _ATTO FibreBridge Installation and Operation Manual _ に、使用可能なコマンドおよびその使用方法に関する最新情報が記載されています。

    > ATTO FibreBridge 7600N または 7500N では時刻同期は設定しないでください。ATTO FibreBridge 7600N または 7500N の時刻は、 ONTAP でブリッジが検出されたあとにクラスタ時間に設定されます。また、 1 日に 1 回定期的に同期されます。使用されるタイムゾーンは GMT で、変更することはできません。

    a. IP 管理用に設定する場合は、ブリッジの IP 設定を行います。

       Quicknav ユーティリティなしで IP アドレスを設定するには、 FibreBridge に対するシリアル接続が必要です。

       CLI を使用する場合は、次のコマンドを実行する必要があります。

       'set ipaddress mp1_ip-address_'

       'set ipsubnetmask mp1_subnet-mask_

       'set ipgateway mp1x.x'

'set ipdhcp mp1 disabled

「 setethernetspeed mp1 1000」

b. ブリッジ名を設定します。

ブリッジ名は、 MetroCluster 構成内でそれぞれ一意である必要があります。

各サイトの 1 つのスタックグループのブリッジ名の例：

- bridge_A_1a
- bridge_A_1b
- bridge_B_1a
- bridge_B_1b

CLI を使用する場合は、次のコマンドを実行する必要があります。

「 set bridgename _bridgename _ 」を入力します

a. ONTAP 9.4 以前を実行している場合は、ブリッジで SNMP を有効にします。 +'set snmp enabled'

ONTAP 9.5 以降を実行しているシステムでは、インバンド管理を使用してイーサネットポートではなく FC ポート経由でブリッジにアクセスできます。ONTAP 9.8 以降では、インバンド管理のみがサポートされ、 SNMP 管理は廃止されています。

13. ブリッジの FC ポートを設定します。

a. ブリッジ FC ポートのデータ速度を設定します。

サポートされる FC データ速度は、モデルブリッジによって異なります。

- FibreBridge 7600Nブリッジは、最大32、16、または8Gbpsをサポートします。
- FibreBridge 7500Nブリッジは、最大16、8、または4Gbpsをサポートします。
- FibreBridge 6500Nブリッジは、最大8、4、または2Gbpsをサポートします。

選択できる FCDataRate の速度は、ブリッジポートを接続するブリッジとスイッチの両方でサポートされる最大速度以下です。ケーブルでの接続距離が SFP およびその他のハードウェアの制限を超えないようにしてください。

CLI を使用する場合は、次のコマンドを実行する必要があります。

'set FCDataRate_port-number port-speed_

b. FibreBridge 7500N / 6500N ブリッジを設定する場合は、ポートが使用する接続モードを ptp に設定します。

FibreBridge 7600N ブリッジを設定する場合、 FCConnMode の設定は不要です。

CLI を使用する場合は、次のコマンドを実行する必要があります。

'et FCConnMode_port-number_ptc'

c. FibreBridge 7600N / 7500N ブリッジを設定する場合は、 FC2 ポートを設定または無効にする必要があります。

- 2 番目のポートを使用する場合は、 FC2 ポートについて同じ手順を繰り返す必要があります。
- 2 番目のポートを使用しない場合は、ポートを無効にする必要があります。

FCPGortDisable_port-number_`

d. FibreBridge 7600N / 7500N ブリッジを設定する場合は、未使用の SAS ポートを無効にします。

'ASPortDisable_SAS-PORT_'

SAS ポート A~D はデフォルトで有効になります。使用していない SAS ポートを無効にする必要があります。SAS ポート A のみを使用している場合は、 SAS ポート B 、 C 、および D を無効にする必要があります。

14. ブリッジへのアクセスを保護し、ブリッジの設定を保存します。

a. コントローラのプロンプトで、ブリッジのステータスを確認します。

「 storage bridge show 」

出力には、保護されていないブリッジが表示されます。

b. セキュリティ保護されていないブリッジのポートのステータスを確認します。

「 info 」のようになります

出力には、イーサネットポート MP1 と MP2 のステータスが表示されます。

c. イーサネットポート MP1 がイネーブルの場合は、次のコマンドを実行します。

「 Set EthernetPort mp1 disabled 」です

イーサネットポート MP2 も有効になっている場合は、ポート MP2 について前の手順を繰り返します。

d. ブリッジの設定を保存します。

次のコマンドを実行する必要があります。

'aveConfiguration'

「 FirmwareRestart 」と入力します

ブリッジを再起動するように求められます。

15. FibreBridge 7600N / 7500N ブリッジの健全性監視を有効にします。
16. FCケーブルを新しいブリッジのFibre Channel 1ポートに接続します。

FCポートを、FibreBridge 6500Nブリッジが接続されていたスイッチまたはコントローラポートにケーブル接続する必要があります。

17. 各ブリッジの FibreBridge ファームウェアを更新します。

    新しいブリッジのタイプがパートナーブリッジと同じ場合は、パートナーブリッジと同じファームウェアにアップグレードします。新しいブリッジのタイプがパートナーブリッジと異なる場合は、ブリッジでサポートされる最新のファームウェアとバージョンのONTAPにアップグレードします。

    "FibreBridge ブリッジのファームウェアを更新します"

18. 新しいブリッジのSAS AポートにSASケーブルを再接続します。

    SAS ポートは、 FibreBridge 6500N ブリッジが接続されていたシェルフポートにケーブル接続する必要があります。

    > コネクタをポートに無理に押し込まないでください。Mini-SAS ケーブルは、誤挿入を防ぐキーイングが施されているため、正しい向きで SAS ポートに取り付けるとカチッとはまり、ディスクシェルフの SAS ポートの LNK LED が緑色に点灯します。ディスクシェルフの場合は、 SAS ケーブルのコネクタをプルタブ（コネクタの下側）を下にして挿入します。コントローラの場合、 SAS ポートの向きはプラットフォームのモデルによって異なるため、 SAS ケーブルのコネクタの正しい向きは異なります。

19. ブリッジが接続先のすべてのディスクドライブとディスクシェルフを検出できることを確認します。

使用する手段	作業
ATTO ExpressNAV の GUI	a. サポートされている Web ブラウザで、ブリッジの IP アドレスをブラウザのアドレスバーに入力します。 ATTO FibreBridge のホームページに移動し、リンクが表示されます。 b. リンクをクリックし、ブリッジを設定するときに指定したユーザ名とパスワードを入力します。 ATTO FibreBridge のステータスページが開き、左側にメニューが表示されます。 c. メニューの「 * 詳細設定 * 」をクリックします。 d. 次のコマンドを入力し、 * Submit * をクリックして、ブリッジで認識されるディスクのリストを表示します。 「 astargets 」
シリアルポート接続	ブリッジから認識されているディスクのリストを表示します。 「 astargets 」

出力には、ブリッジが接続されているデバイス（ディスクおよびディスクシェルフ）が表示されます。出力行には行番号が振られているため、デバイスの台数を簡単に把握できます。たとえば、次の出力は、

10 本のディスクが接続されていることを示しています。

```
Tgt VendorID ProductID         Type        SerialNumber
  0 NETAPP   X410_S15K6288A15 DISK        3QP1CLE300009940UHJV
  1 NETAPP   X410_S15K6288A15 DISK        3QP1ELF600009940V1BV
  2 NETAPP   X410_S15K6288A15 DISK        3QP1G3EW00009940U2M0
  3 NETAPP   X410_S15K6288A15 DISK        3QP1EWMP00009940U1X5
  4 NETAPP   X410_S15K6288A15 DISK        3QP1FZLE00009940G8YU
  5 NETAPP   X410_S15K6288A15 DISK        3QP1FZLF00009940TZKZ
  6 NETAPP   X410_S15K6288A15 DISK        3QP1CEB400009939MGXL
  7 NETAPP   X410_S15K6288A15 DISK        3QP1G7A900009939FNTT
  8 NETAPP   X410_S15K6288A15 DISK        3QP1FY0T00009940G8PA
  9 NETAPP   X410_S15K6288A15 DISK        3QP1FXW600009940VERQ
```

出力の先頭に「 response truncated 」というテキストが表示される場合は、 Telnet を使用してブリッジにアクセスし、同じコマンドを入力すると、すべての出力を確認できます。

20. コマンド出力で、スタック内の必要なすべてのディスクおよびディスクシェルフにブリッジが接続されていることを確認します。

出力結果	作業
正解です	残りの各ブリッジについて、同じ手順を繰り返します。
不正解です	a. SASケーブルに緩みがないかどうかを確認するか、を繰り返してSASケーブル接続を修正します手順 18。 b. 残りの各ブリッジについて、同じ手順を繰り返します。

21. ブリッジに接続する FC スイッチポートを再度有効にします。
22. 両方のコントローラのシステムコンソールで、すべてのコントローラが新しいブリッジ経由でディスクシェルフにアクセスできること（システムがマルチパス HA 用に適切に接続されていること）を確認します。

「 run local sysconfig 」を実行します

システムで検出が完了するまで、 1 分程度かかる場合があります。

たとえば、次の出力は、システムがマルチパス HA 用に接続されていることを示しています。

```
NetApp Release 8.3.2: Tue Jan 26 01:23:24 PST 2016
System ID: 1231231231 (node_A_1); partner ID: 4564564564 (node_A_2)
System Serial Number: 700000123123 (node_A_1); partner Serial Number:
700000456456 (node_A_2)
System Rev: B0
System Storage Configuration: Multi-Path HA
System ACP Connectivity: NA
```

混在パスまたはシングルパスの HA 構成であることがコマンド出力で示された場合は、新しいブリッジ経由でアクセスできないディスクドライブがあるため、 SAS ケーブルと FC ケーブルの接続を修正する必要があります。

システムがマルチパス HA 構成で接続されていないと、ブリッジを再起動したときに、ディスクドライブへのアクセスが原因で失われて、複数のディスクがパニック状態になることがあります。

23. ONTAP クラスタのプロンプトで、ブリッジをヘルスモニタの対象に追加します。

    a. 使用している ONTAP のバージョンに対応したコマンドを使用して、ブリッジを追加します。

ONTAP バージョン	コマンドを実行します
9.5 以降	「 storage bridge add -address 0.0.0.0 -managed-by in-band-name_bridge-name_`
9.4 以前	「 storage bridge add -address_bridge-ip-address_-name_bridge-name_` 」

    b. ブリッジが追加され、正しく設定されていることを確認します。 `+storage bridge show`

    ポーリング間隔に応じて、すべてのデータが反映されるまで 15 分程度かかる場合があります。ONTAP ヘルスモニタは、「 Status 」列の値が「 ok 」で、ワールドワイド名（ WWN ）などのその他の情報が表示されていれば、ブリッジに接続して監視できます。

    次の例は、 FC-to-SAS ブリッジが設定されていることを示しています。

```
controller_A_1::> storage bridge show

Bridge                Symbolic Name Is Monitored  Monitor Status  Vendor
Model                  Bridge WWN
------------------  ------------ ------------  --------------  ------
-----------------    ----------
ATTO_10.10.20.10  atto01        true          ok              Atto
FibreBridge 7500N      20000010867038c0
ATTO_10.10.20.11  atto02        true          ok              Atto
FibreBridge 7500N      20000010867033c0
ATTO_10.10.20.12  atto03        true          ok              Atto
FibreBridge 7500N      20000010867030c0
ATTO_10.10.20.13  atto04        true          ok              Atto
FibreBridge 7500N      2000001086703b80

4 entries were displayed

 controller_A_1::>
```

24. ONTAP で MetroCluster 構成の動作を確認します。
    a. システムがマルチパスかどうかを確認します。

       'node run -node _node-name_sysconfig -a

    b. 両方のクラスタにヘルス・アラートがないかどうかを確認します +`system health alert show`
    c. MetroCluster 構成と運用モードが正常な状態であることを確認します。

       「 MetroCluster show 」

    d. MetroCluster チェックを実行します。

       「 MetroCluster check run 」のようになります

    e. MetroCluster チェックの結果を表示します。

       MetroCluster チェックショー

    f. スイッチにヘルスアラートがないかどうかを確認します（ある場合）。

       「 storage switch show 」と表示されます

    g. Config Advisor を実行します。

       "ネットアップのダウンロード： Config Advisor"

    h. Config Advisor の実行後、ツールの出力を確認し、推奨される方法で検出された問題に対処します。
25. 部品の交換後、障害のある部品は、キットに付属する RMA 指示書に従ってネットアップに返却してくだ

さい。を参照してください "パーツの返品と交換" 詳細については、を参照してください。

関連情報

"FC-to-SAS ブリッジのインバンド管理"

FibreBridge 6500N ブリッジのペアを **7600N / 7500N** ブリッジに交換する

FibreBridge 7600N / 7500N ブリッジの追加の FC2 ポートを利用してラック数を減らすためには、システムを停止せずに 6500N ブリッジを交換し、 1 組の FibreBridge 7600N / 7500N ブリッジペアに最大 4 つのストレージスタックを統合することができます。

作業を開始する前に

管理パスワードと FTP サーバまたは SCP サーバへのアクセスが必要です。

このタスクについて

この手順は、次の場合に使用します。

- FibreBridge 6500N ブリッジのペアを FibreBridge 7600N / 7500N ブリッジに交換する。

  ペアの両方のブリッジを同じモデルに交換する必要があります。

- 1 台の FibreBridge 6500N ブリッジを 7600N / 7500N ブリッジに交換済みのペアで、 2 台目のブリッジを交換する。
- 使用している FibreBridge 7600N / 7500N ブリッジのペアに使用可能な SAS ポートがあり、現在 FibreBridge 6500N ブリッジで接続されている SAS ストレージスタックを統合する。

これはシステムの停止を伴わない手順であり、完了までに約 2 時間かかります。

関連情報

"単一の FC-to-SAS ブリッジの交換"

ストレージ接続を確認しています

ブリッジを交換する前に、ブリッジとストレージの接続を確認する必要があります。設定を変更したあとに接続を確認できるよう、コマンド出力について理解しておいてください。

これらのコマンドは、メンテナンス中のサイトの MetroCluster 構成にある任意のコントローラモジュールの管理プロンプトから問題できます。

1. いずれかの MetroCluster ノードで次のコマンドを入力して、ディスクへの接続を確認します。

   'run local sysconfig -v

   出力には、コントローラのイニシエータポートに接続されているディスクが表示され、 FC-to-SAS ブリッジに接続されているシェルフが示されます。

```
node_A_1> run local sysconfig -v
NetApp Release 9.3.2X18: Sun Dec 13 01:23:24 PST 2017
System ID: 4068741258 (node_A_1); partner ID: 4068741260 (node_B_1)
```

```
System Serial Number: 940001025471 (node_A_1)
System Rev: 70
System Storage Configuration: Multi-Path HA**<=== Configuration should
be multi-path HA**
.
.
.
slot 0: FC Host Adapter 0g (QLogic 8324 rev. 2, N-port, <UP>)**<===
Initiator port**
        Firmware rev:      7.5.0
        Flash rev:         0.0.0
        Host Port Id:      0x60130
        FC Node Name:      5:00a:098201:bae312
        FC Port Name:      5:00a:098201:bae312
        SFP Vendor:        UTILITIES CORP.
        SFP Part Number:   FTLF8529P3BCVAN1
        SFP Serial Number: URQ0Q9R
        SFP Capabilities:  4, 8 or 16 Gbit
        Link Data Rate:    16 Gbit
        Switch Port:       brcd6505-fcs40:1
  **<List of disks visible to port\>**
         ID     Vendor   Model            FW    Size
        brcd6505-fcs29:12.126L1527     : NETAPP   X302_HJUPI01TSSM NA04
847.5GB (1953525168 512B/sect)
        brcd6505-fcs29:12.126L1528     : NETAPP   X302_HJUPI01TSSA NA02
847.5GB (1953525168 512B/sect)
        .
        .
        .
        **<List of FC-to-SAS bridges visible to port\>**
        FC-to-SAS Bridge:
        brcd6505-fcs40:12.126L0        : ATTO     FibreBridge6500N 1.61
FB6500N102980
        brcd6505-fcs42:13.126L0        : ATTO     FibreBridge6500N 1.61
FB6500N102980
        brcd6505-fcs42:6.126L0         : ATTO     FibreBridge6500N 1.61
FB6500N101167
        brcd6505-fcs42:7.126L0         : ATTO     FibreBridge6500N 1.61
FB6500N102974
        .
        .
        .
  **<List of storage shelves visible to port\>**
        brcd6505-fcs40:12.shelf6: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        brcd6505-fcs40:12.shelf8: DS4243  Firmware rev. IOM3 A: 0200
```

```
IOM3 B: 0200
         .
         .
         .
```

FibreBridge 7600N / 7500N ブリッジのペアを作成するための **FibreBridge 6500N** ブリッジのホットスワップ

1 つまたは 2 つの FibreBridge 6500N ブリッジをホットスワップして、 FibreBridge 7600N / 7500N ブリッジのペアを使用した構成を作成するには、ブリッジを 1 つずつ交換し、正しいケーブル接続手順に従う必要があります。新しいケーブル接続は元のケーブル接続とは異なります。

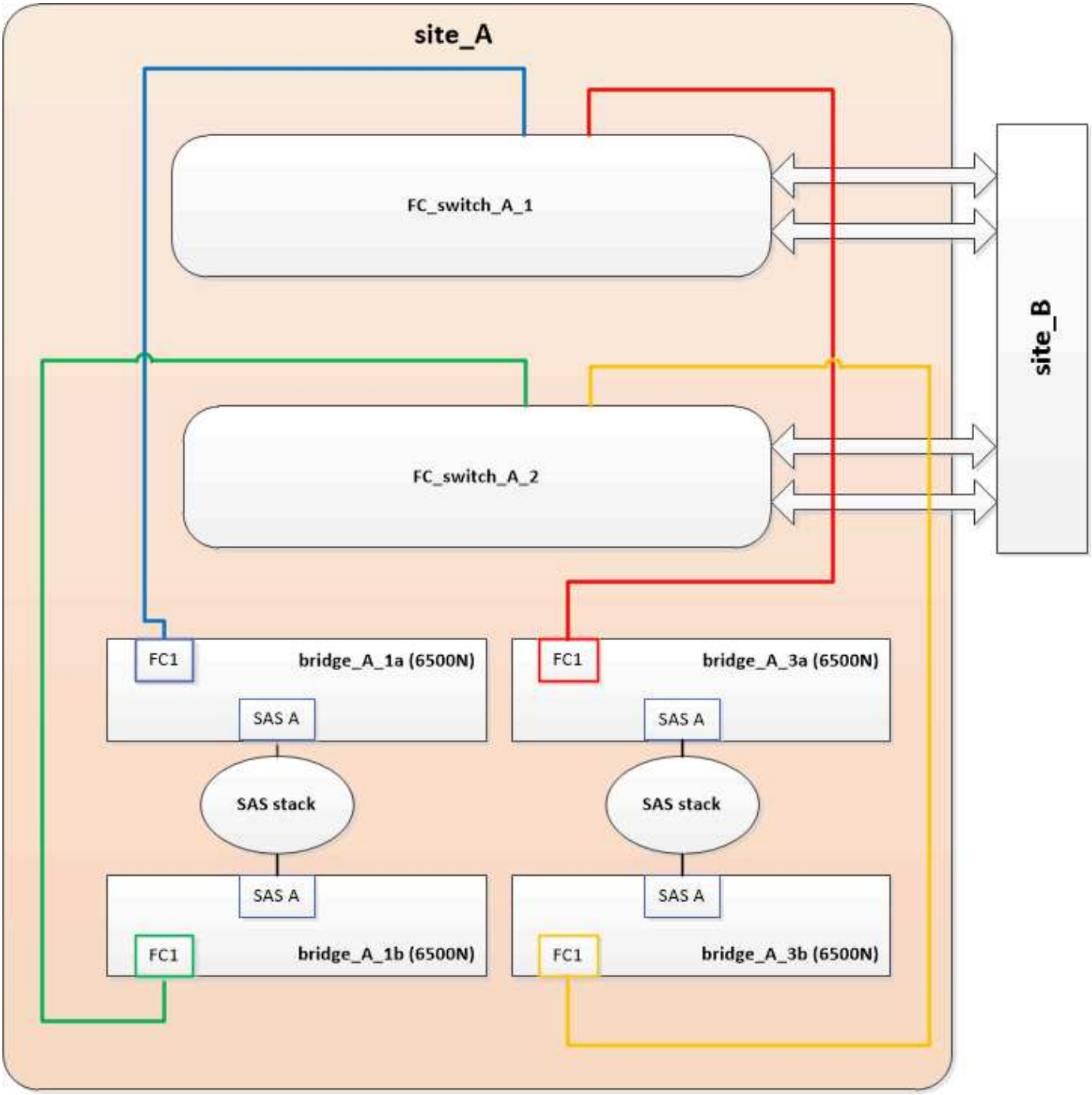
このタスクについて

この手順は、次の条件に該当する場合にも使用できます。

- 同じ SAS ストレージのスタックに接続されている FibreBridge 6500N ブリッジのペアを交換する。
- ペアの一方の FibreBridge 6500N ブリッジを以前に交換済みであり、ストレージスタックに FibreBridge 6500N ブリッジと FibreBridge 7600N / 7500N ブリッジが 1 つずつ設定されている。

  この場合、下記の手順から始めて、下部のFibreBridge 6500NブリッジをFibreBridge 7600N / 7500Nブリッジとホットスワップします。

次の図は、 4 つの FibreBridge 6500N ブリッジで 2 つの SAS ストレージスタックを接続する初期構成の例を示しています。



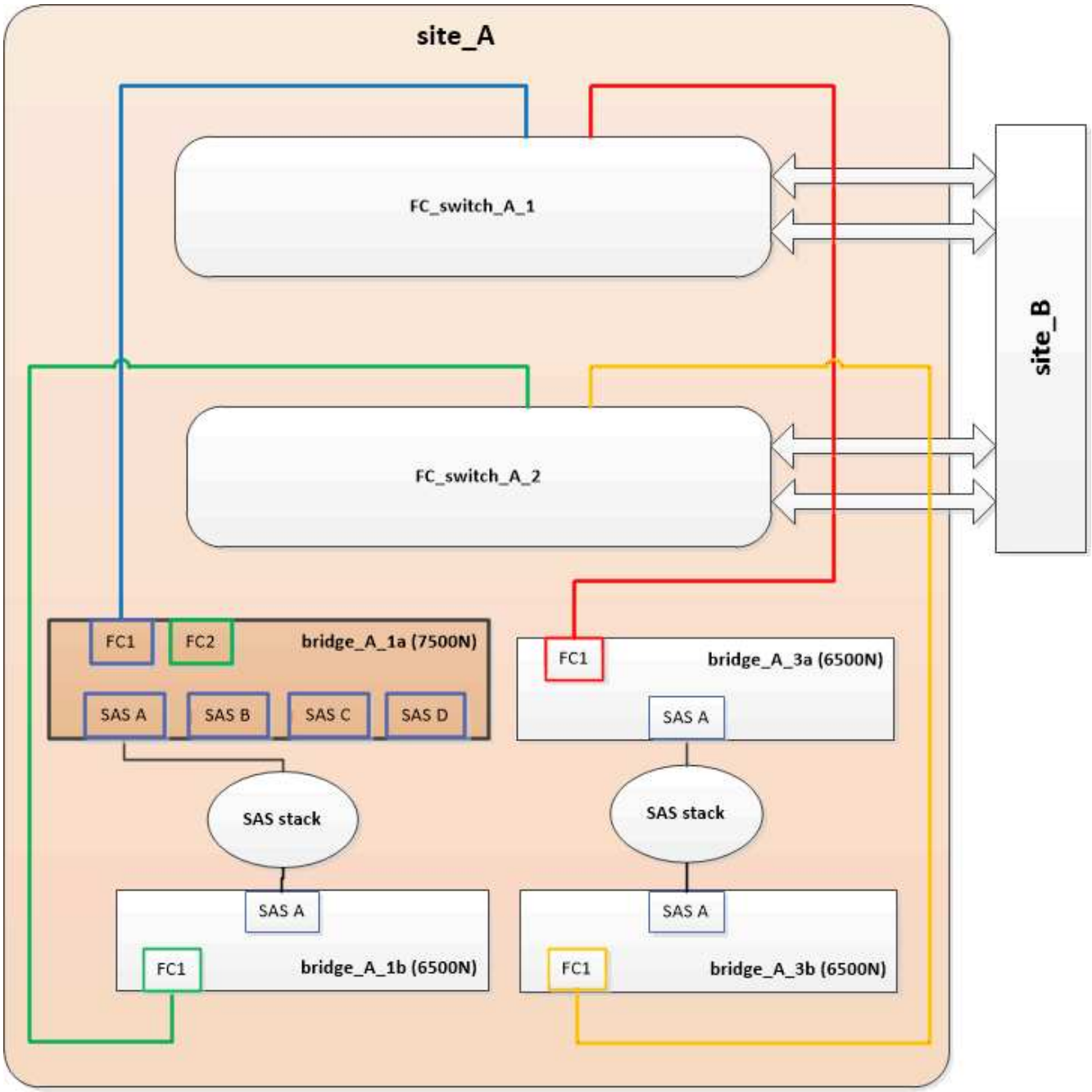
手順

1. 次のガイドラインに従って、の手順を使用して、上部のFibreBridge 6500Nブリッジを FibreBridge 7600N / 7500Nブリッジとホットスワップします。 "FibreBridge 6500N ブリッジと FibreBridge 7600N / 7500N ブリッジのホットスワップ"：

   ◦ FibreBridge 7600N / 7500N ブリッジの FC1 ポートをスイッチまたはコントローラに接続します。

   これは、元の FibreBridge 6500N ブリッジの FC1 ポートへの接続と同じです。

   ◦ ここでは、 FibreBridge 7600N / 7500N ブリッジの FC2 ポートを接続しないでください。次の図は、 bridge_A_1a が FibreBridge 7600N / 7500N ブリッジに交換された状態を示しています。



2. ブリッジに接続されているディスクとの接続と、新しい FibreBridge 7500N が構成に表示されることを確認します。

   'run local sysconfig -v

```
node_A_1> run local sysconfig -v
NetApp Release 9.3.2X18: Sun Dec 13 01:23:24 PST 2015
System ID: 0536872165 (node_A_1); partner ID: 0536872141 (node_B_1)
System Serial Number: 940001025465 (node_A_1)
System Rev: 70
System Storage Configuration: Multi-Path HA**<=== Configuration should
be multi-path HA**
.
```

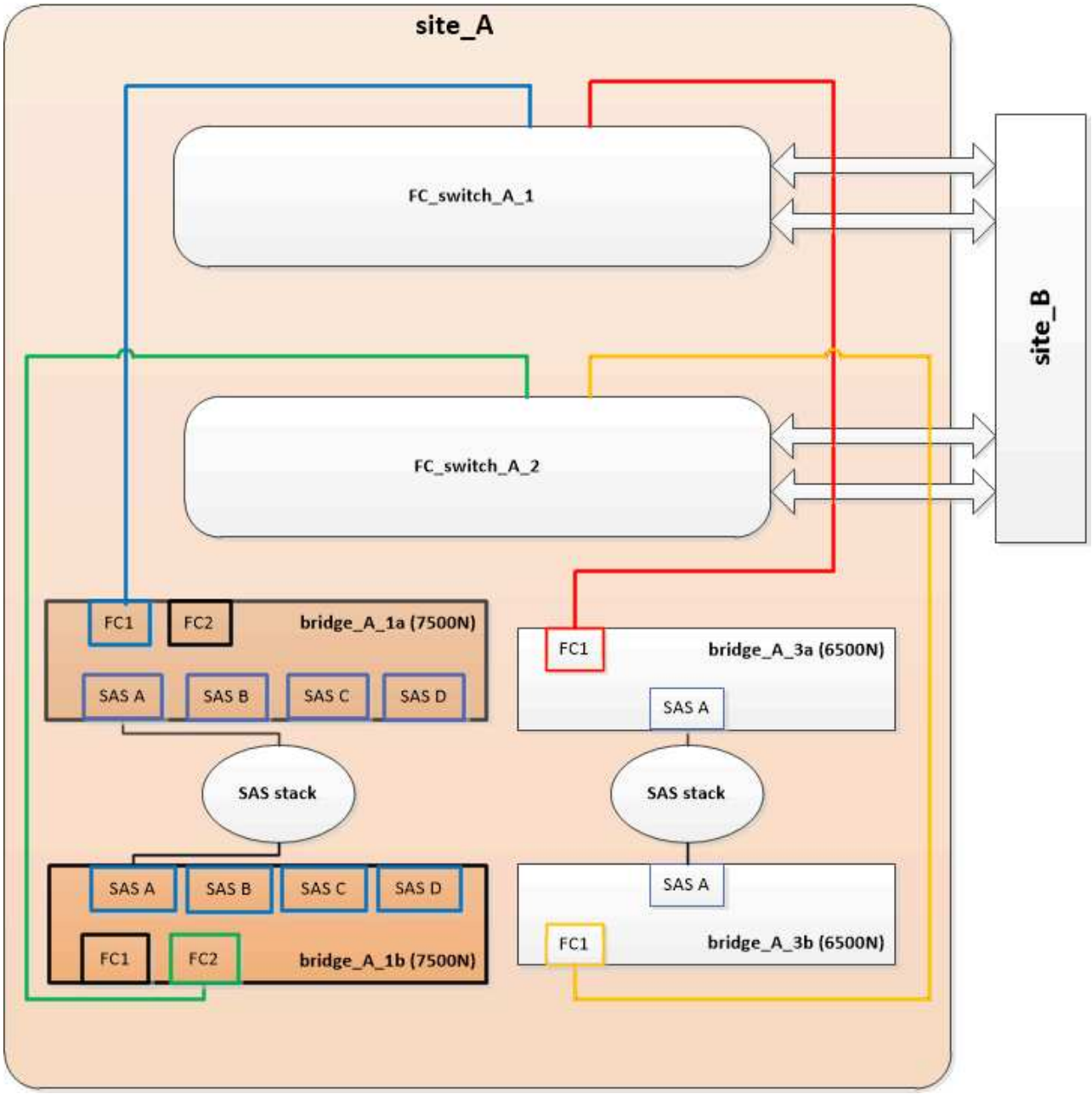
```
.
.
slot 0: FC Host Adapter 0g (QLogic 8324 rev. 2, N-port, <UP>)**<===
Initiator port**
        Firmware rev:      7.5.0
        Flash rev:         0.0.0
        Host Port Id:      0x60100
        FC Node Name:      5:00a:098201:bae312
        FC Port Name:      5:00a:098201:bae312
        SFP Vendor:        FINISAR CORP.
        SFP Part Number:   FTLF8529P3BCVAN1
        SFP Serial Number: URQ0R1R
        SFP Capabilities:  4, 8 or 16 Gbit
        Link Data Rate:    16 Gbit
        Switch Port:       brcd6505-fcs40:1
  **<List of disks visible to port\>**
         ID     Vendor   Model            FW    Size
        brcd6505-fcs40:12.126L1527     : NETAPP   X302_HJUPI01TSSM NA04
847.5GB (1953525168 512B/sect)
        brcd6505-fcs40:12.126L1528     : NETAPP   X302_HJUPI01TSSA NA02
847.5GB (1953525168 512B/sect)
        .
        .
        .
        **<List of FC-to-SAS bridges visible to port\>**
        FC-to-SAS Bridge:
        brcd6505-fcs40:12.126L0        : ATTO     FibreBridge7500N A30H
FB7500N100104**<===**
        brcd6505-fcs42:13.126L0        : ATTO     FibreBridge6500N 1.61
FB6500N102980
        brcd6505-fcs42:6.126L0         : ATTO     FibreBridge6500N 1.61
FB6500N101167
        brcd6505-fcs42:7.126L0         : ATTO     FibreBridge6500N 1.61
FB6500N102974
        .
        .
        .
  **<List of storage shelves visible to port\>**
        brcd6505-fcs40:12.shelf6: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        brcd6505-fcs40:12.shelf8: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        .
        .
        .
```

3. 次のガイドラインに従って、の手順を使用して、下部のFibreBridge 6500Nブリッジを FibreBridge 7600N / 7500Nブリッジとホットスワップします。 "FibreBridge 6500N ブリッジと FibreBridge 7600N / 7500N ブリッジのホットスワップ"：

   ◦ FibreBridge 7600N / 7500N ブリッジの FC2 ポートをスイッチまたはコントローラに接続します。

   これは、元の FibreBridge 6500N ブリッジの FC1 ポートへの接続と同じです。

   ◦ この時点では、FibreBridge 7600N または 7500N ブリッジ FC1 ポートを接続しないでください。



4. ブリッジに接続されているディスクとの接続を確認します。

   'run local sysconfig -v

   出力には、コントローラのイニシエータポートに接続されているディスクが表示され、 FC-to-SAS ブリッジに接続されているシェルフが示されます。

```
node_A_1> run local sysconfig -v
NetApp Release 9.3.2X18: Sun Dec 13 01:23:24 PST 2015
System ID: 0536872165 (node_A_1); partner ID: 0536872141 (node_B_1)
System Serial Number: 940001025465 (node_A_1)
System Rev: 70
System Storage Configuration: Multi-Path HA**<=== Configuration should
be multi-path HA**
.
.
.
slot 0: FC Host Adapter 0g (QLogic 8324 rev. 2, N-port, <UP>)**<===
Initiator port**
        Firmware rev:      7.5.0
        Flash rev:         0.0.0
        Host Port Id:      0x60100
        FC Node Name:      5:00a:098201:bae312
        FC Port Name:      5:00a:098201:bae312
        SFP Vendor:        FINISAR CORP.
        SFP Part Number:   FTLF8529P3BCVAN1
        SFP Serial Number: URQ0R1R
        SFP Capabilities:  4, 8 or 16 Gbit
        Link Data Rate:    16 Gbit
        Switch Port:       brcd6505-fcs40:1
  **<List of disks visible to port\>**
         ID     Vendor   Model            FW    Size
        brcd6505-fcs40:12.126L1527     : NETAPP   X302_HJUPI01TSSM NA04
847.5GB (1953525168 512B/sect)
        brcd6505-fcs40:12.126L1528     : NETAPP   X302_HJUPI01TSSA NA02
847.5GB (1953525168 512B/sect)
        .
        .
        .
        **<List of FC-to-SAS bridges visible to port\>**
        FC-to-SAS Bridge:
        brcd6505-fcs40:12.126L0        : ATTO     FibreBridge7500N A30H
FB7500N100104
        brcd6505-fcs42:13.126L0        : ATTO     FibreBridge7500N A30H
FB7500N100104
        .
        .
        .
  **<List of storage shelves visible to port\>**
        brcd6505-fcs40:12.shelf6: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        brcd6505-fcs40:12.shelf8: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
```

.
.
.

FibreBridge 7600N / 7500N ブリッジによるストレージ統合時のブリッジ **SAS** ポートのケーブル接続

複数の SAS ストレージスタックを、使用可能な SAS ポートがある単一ペアの FibreBridge 7600N / 7500N ブリッジで統合する場合は、上部と下部の SAS ケーブルを新しいブリッジに移動する必要があります。

このタスクについて

FibreBridge 6500N ブリッジの SAS ポートは QSFP コネクタを使用します。FibreBridge 7600N / 7500N ブリッジの SAS ポートは Mini-SAS コネクタを使用します。

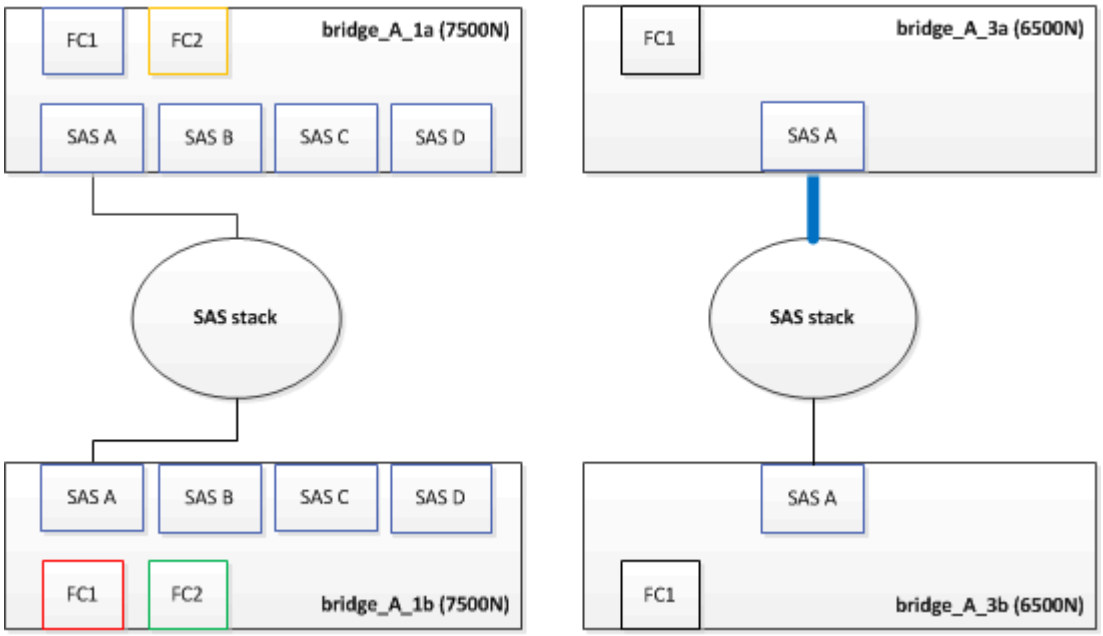
SAS ケーブルを間違ったポートに挿入した場合は、ケーブルを SAS ポートから取り外すときに、 120 秒以上待機してから別の SAS ポートに接続する必要があります。そうしないと、ケーブルが別のポートに移されたことがシステムで認識されません。

ポートを接続する前に、 10 秒以上待機します。SAS ケーブルのコネクタは、誤挿入を防ぐキーイングが施されているため、正しい向きで SAS ポートに取り付けるとカチッとはまり、ディスクシェルフの SAS ポートの LNK LED が緑色に点灯します。ディスクシェルフの場合は、SAS ケーブルのコネクタをプルタブ（コネクタの下側）を下にして挿入します。

手順

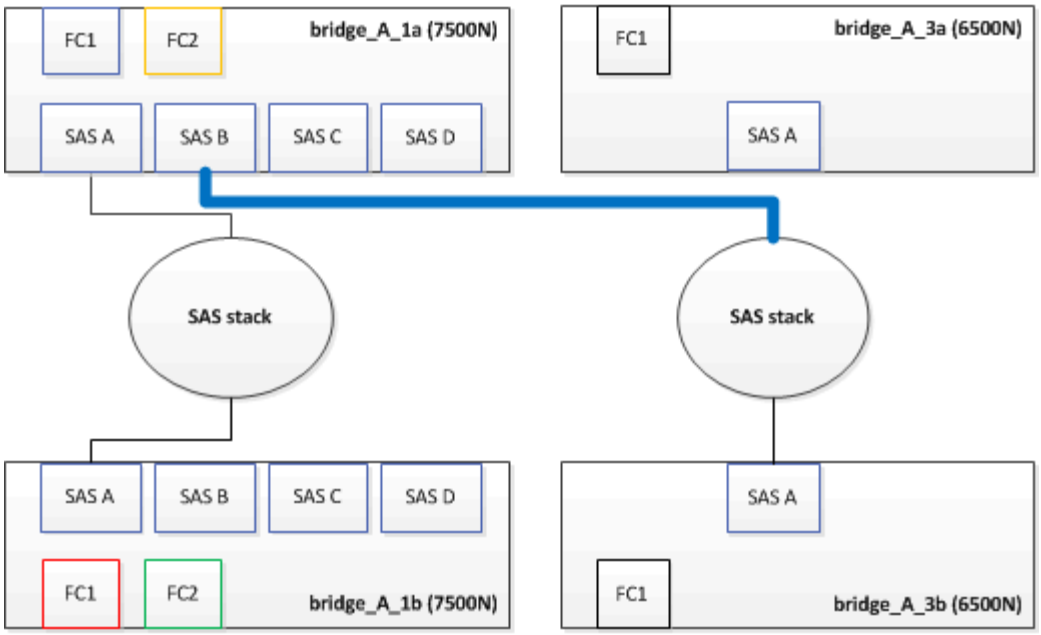
1. 上部の FibreBridge 6500N ブリッジの SAS A ポートを上部の SAS シェルフに接続しているケーブルを外します。その際、接続先ストレージシェルフの SAS ポートをメモします。

   次の例では、ケーブルを青色で示しています。



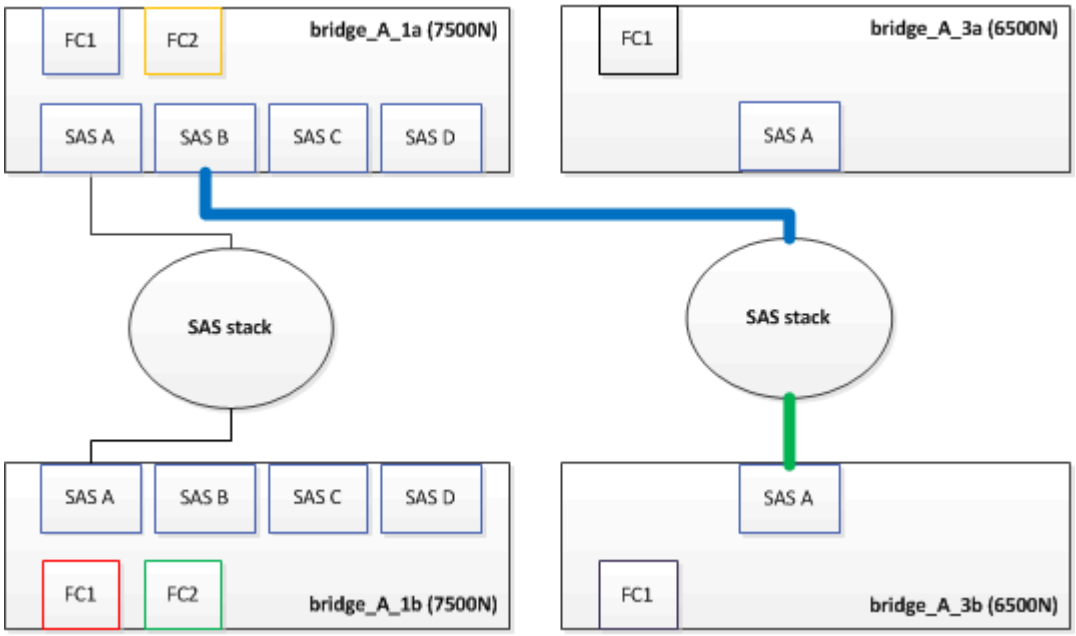
2. Mini-SAS コネクタのケーブルを使用して、ストレージシェルフの同じ SAS ポートを、上部の FibreBridge 7600N / 7500N ブリッジの SAS B ポートに接続します。

次の例では、ケーブルを青色で示しています。



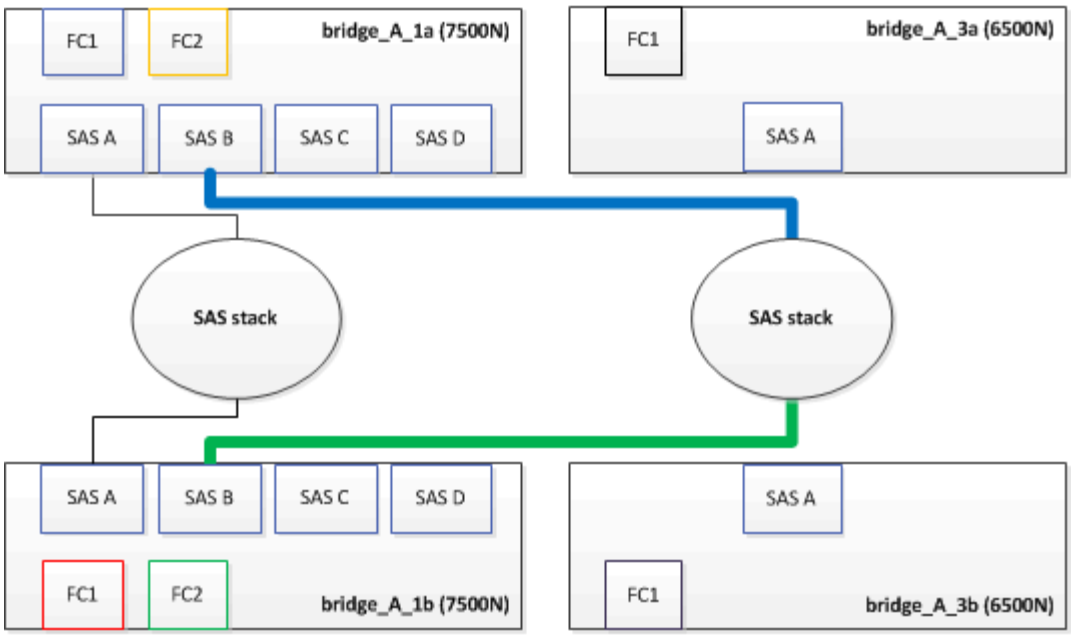
3. 下部の FibreBridge 6500N ブリッジの SAS A ポートを上部の SAS シェルフに接続しているケーブルを外します。その際、接続先ストレージシェルフの SAS ポートをメモします。

   次の例では、このケーブルを緑色で示しています。



4. Mini-SAS コネクタのケーブルを使用して、ストレージシェルフの同じ SAS ポートを、下部の FibreBridge 7600N / 7500N ブリッジの SAS B ポートに接続します。

   次の例では、このケーブルを緑色で示しています。



5. ブリッジに接続されているディスクとの接続を確認します。

   'run local sysconfig -v

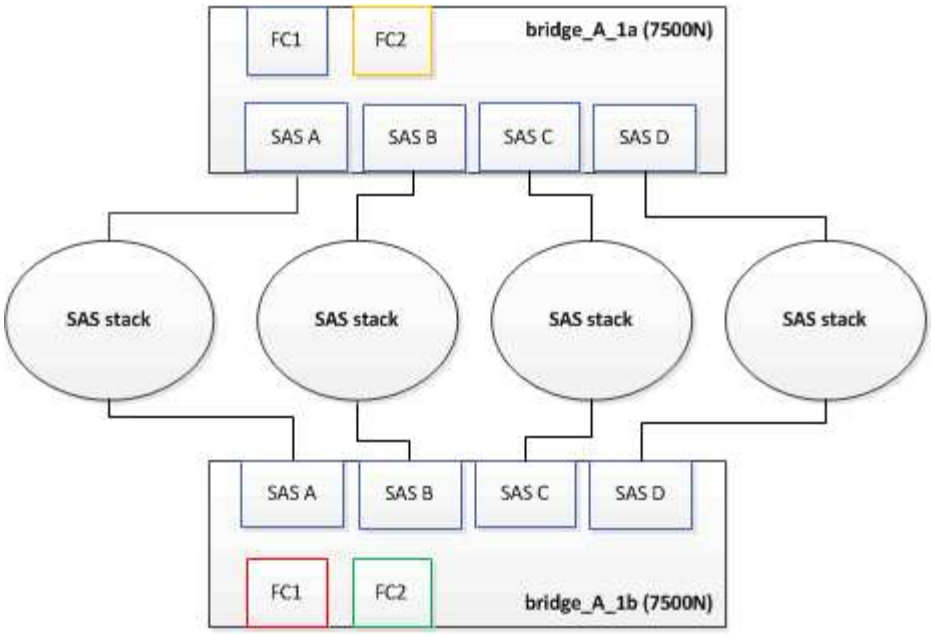
   出力には、コントローラのイニシエータポートに接続されているディスクが表示され、 FC-to-SAS ブリッジに接続されているシェルフが示されます。

```
node_A_1> run local sysconfig -v
NetApp Release 9.3.2X18: Sun Dec 13 01:23:24 PST 2015
System ID: 0536872165 (node_A_1); partner ID: 0536872141 (node_B_1)
System Serial Number: 940001025465 (node_A_1)
System Rev: 70
System Storage Configuration: Multi-Path HA**<=== Configuration should
be multi-path HA**
.
.
.
slot 0: FC Host Adapter 0g (QLogic 8324 rev. 2, N-port, <UP>)**<===
Initiator port**
        Firmware rev:      7.5.0
        Flash rev:         0.0.0
        Host Port Id:      0x60100
        FC Node Name:      5:00a:098201:bae312
        FC Port Name:      5:00a:098201:bae312
        SFP Vendor:        FINISAR CORP.
        SFP Part Number:   FTLF8529P3BCVAN1
        SFP Serial Number: URQ0R1R
        SFP Capabilities:  4, 8 or 16 Gbit
        Link Data Rate:    16 Gbit
        Switch Port:       brcd6505-fcs40:1
```

```
  **<List of disks visible to port\>**
         ID     Vendor   Model            FW    Size
        brcd6505-fcs40:12.126L1527     : NETAPP   X302_HJUPI01TSSM NA04
847.5GB (1953525168 512B/sect)
        brcd6505-fcs40:12.126L1528     : NETAPP   X302_HJUPI01TSSA NA02
847.5GB (1953525168 512B/sect)
        .
        .
        .
        **<List of FC-to-SAS bridges visible to port\>**
        FC-to-SAS Bridge:
        brcd6505-fcs40:12.126L0        : ATTO     FibreBridge7500N A30H
FB7500N100104
        brcd6505-fcs42:13.126L0        : ATTO     FibreBridge7500N A30H
FB7500N100104
        .
        .
        .
  **<List of storage shelves visible to port\>**
        brcd6505-fcs40:12.shelf6: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        brcd6505-fcs40:12.shelf8: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        .
        .
        .
```

6. SAS ストレージから切断した FibreBridge 6500N ブリッジを取り外します。
7. システムが変更を認識するまで 2 分待ちます。
8. システムが正しくケーブル接続されていない場合は、ケーブルを取り外し、ケーブル接続を修正してから、正しいケーブルを再接続します。
9. 必要に応じて上記の手順を繰り返し、 SAS ポート C と D を使用して、最大 2 つの SAS スタックを新しい FibreBridge 7600N / 7500N ブリッジに追加で移動します

   各 SAS スタックは、上部と下部のブリッジの同じ SAS ポートに接続する必要があります。たとえば、スタックの上部を上部のブリッジの SAS B ポートに接続する場合、下部は下部のブリッジの SAS B ポートに接続する必要があります。



FibreBridge 7600N / 7500N ブリッジ追加時のゾーニングの更新

FibreBridge 6500N ブリッジを FibreBridge 7600N / 7500N ブリッジに交換し、 FibreBridge 7600N / 7500N ブリッジの両方の FC ポートを使用する場合は、ゾーニングを変更する必要があります。必要な変更は、実行している ONTAP のバージョンが 9.1 より前か、 9.1 以降かによって異なります。

FibreBridge 7500N ブリッジ追加時のゾーニングの更新（ **ONTAP 9.1** より前）

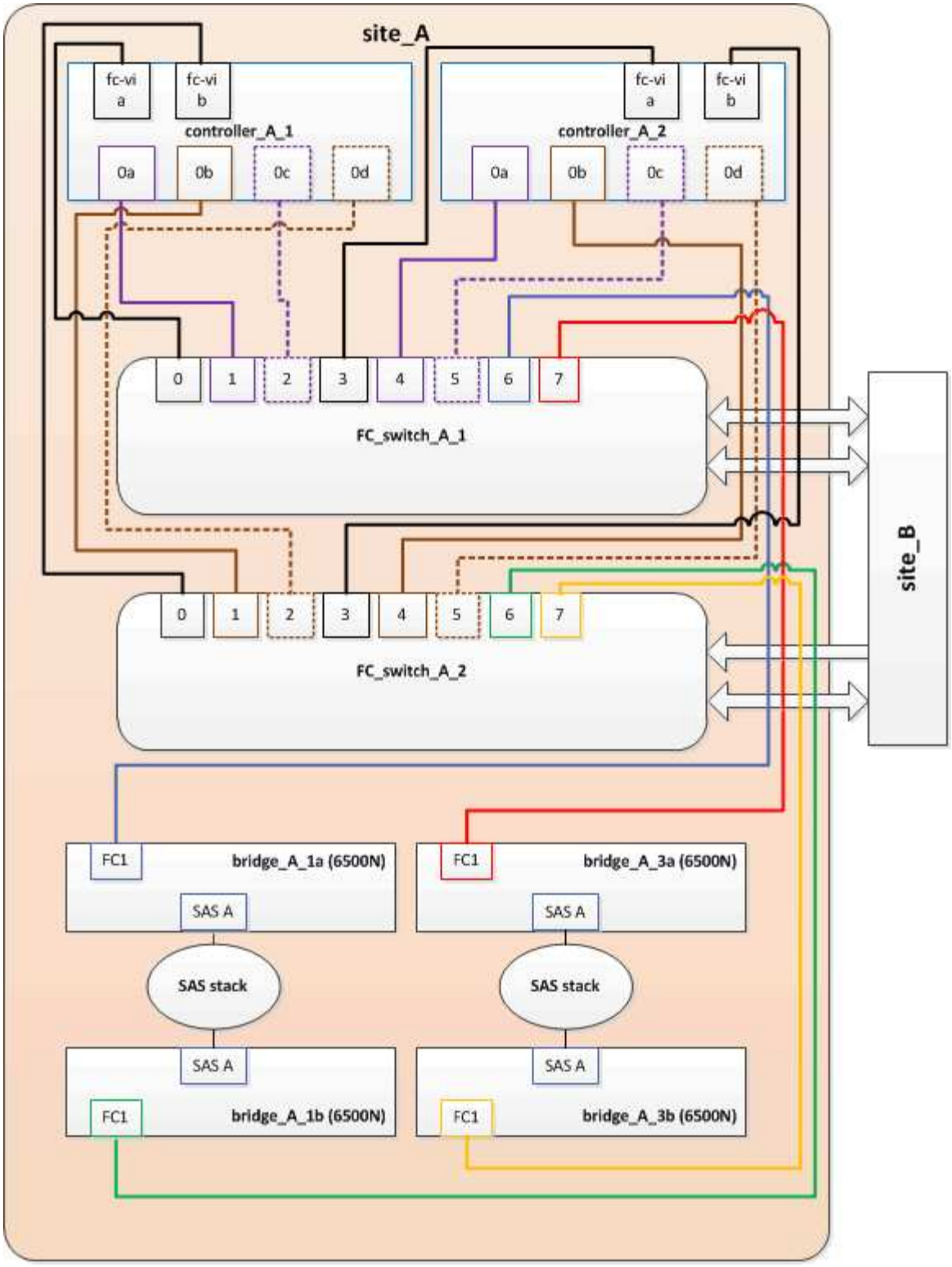
FibreBridge 6500N ブリッジを FibreBridge 7500N ブリッジに交換し、 FibreBridge 7500N ブリッジの両方の FC ポートを使用する場合は、ゾーニングを変更する必要があります。各ゾーンに指定できるイニシエータポートは最大 4 つです。使用するゾーニングは、実行している ONTAP のバージョンが 9.1 より前か、 9.1 以降かによって異なります

このタスクについて

このタスクで使用するゾーニングは、 9.1 より前のバージョンの ONTAP が対象です。

ONTAP では、ディスクへのパスに使用できる FC イニシエータポートは最大 4 つです。そのため、問題を回避するためにゾーニングを変更する必要があります。ケーブル接続を再接続してシェルフを統合すると、各ディスクに 8 つの FC ポートからアクセスできるようにゾーニングが変更されます。ゾーニングを変更して各ゾーンのイニシエータポートを 4 つに減らす必要があります。

次の図は、変更前の site_A のゾーニングを示しています。



手順

1. FC スイッチのストレージゾーンを更新します。具体的には、既存の各ゾーンからイニシエータポートの半分を削除し、 FibreBridge 7500N の FC2 ポート用の新しいゾーンを作成します。

   新しい FC2 ポート用のゾーンには、既存のゾーンから削除したイニシエータポートが含まれます。図では、これらのゾーンが破線で示されています。

   ゾーニングコマンドの詳細については、の FC スイッチに関するセクションを参照してください "ファブ

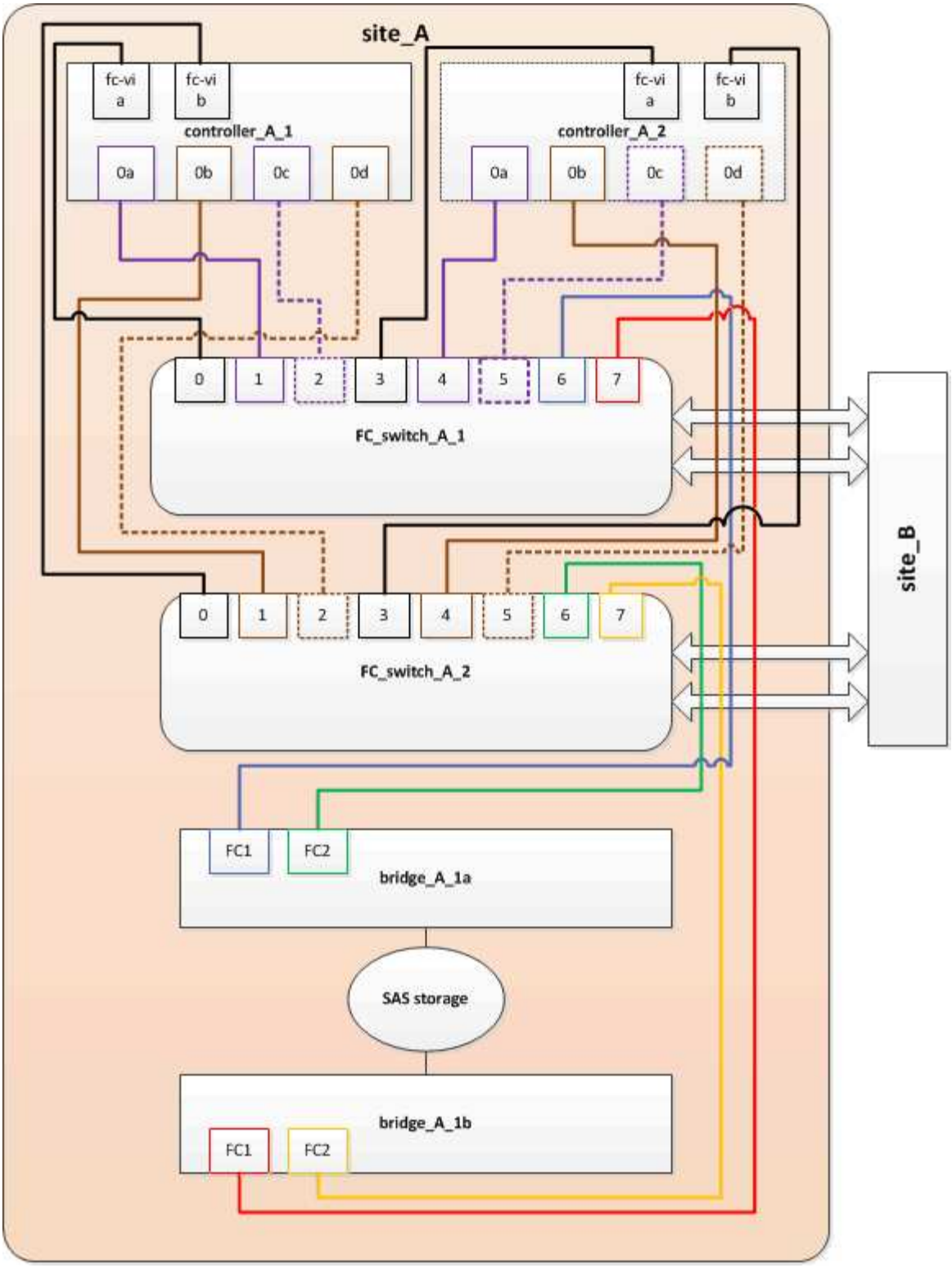
リック接続 MetroCluster のインストールと設定" または "ストレッチ MetroCluster のインストールと設定 "。

次の例は、統合前と統合後のストレージゾーンと各ゾーンのポートを示しています。ポートは、 _domain と port_pairs で識別されます。

- ドメイン 5 は FC_switch_A_1 スイッチを使用します。
- ドメイン 6 は FC_switch_A_2 スイッチで構成されています。
- ドメイン 7 は FC_switch_A_1 スイッチを使用します。
- ドメイン 8 は FC_switch_B_2 で構成されています。

統合前または統合後	ゾーン	ドメインとポート	図の色 (図にはサイト A のみが表示されます)
統合前のゾーン。4 台の FibreBridge 6500N ブリッジの各 FC ポートに 1 つのゾーン。	STOR_A_1a - FC1 の場合	5 、 1 ； 5 、 2 ； 5 、 4 ； 5 、 5 ； 7 、 1 ； 7 、 2 ； 7 、 4 ； 7 、 5 ； 5 、 6	紫 + 紫の破線 + 青
STOR_A_1b-FC1 の場合	6 、 1 ； 6 、 2 ； 6 、 4 ； 6 、 5 ； 8 、 1 ； 8 、 2 、 8 、 4 、 8 、 5 、 6	茶 + 茶の破線 + 緑	STOR_A_2a~FC1 のように設定します
5 、 1 ； 5 、 2 ； 5 、 4 ； 5 、 5 ； 7 、 1 ； 7 、 2 ； 7 、 4 ； 7 、 5 ； 5 、 7	紫 + 紫の破線 + 赤	STOR_A_2b-FC1 の場合	6 、 1 ； 6 、 2 ； 6 、 4 ； 6 、 5 ； 8 、 1 ； 8 、 2 、 8 、 4 、 8 、 5 、 6 、 7
茶 + 茶の破線 + オレンジ	統合後のゾーン。2 台の FibreBridge 7500N ブリッジの各 FC ポートに 1 つのゾーン。	STOR_A_1a - FC1 の場合	7 、 1 ； 7 、 4 ； 5 、 1 ； 5 、 4 ； 5 、 6
紫 + 青	STOR_A_1b-FC1 の場合	7 、 2 ； 7 、 5 ； 5 、 2 ； 5 、 5 ； 5 、 7	紫の破線 + 赤
STOR_A_1a - FC2 を参照します	8 、 1 、 8 、 4 、 6 、 1 、 6 、 4 、 6	茶 + 緑	STOR_A_1b-FC2 を参照します

次の図は、統合後の site_A のゾーニングを示しています。



FibreBridge 7600N / 7500N ブリッジ追加時のゾーニングの更新（ **ONTAP 9.1** 以降）

FibreBridge 6500N ブリッジを FibreBridge 7600N / 7500N ブリッジに交換し、 FibreBridge 7600N / 7500N ブリッジの両方の FC ポートを使用する場合は、ゾーニングを変更する必要があります。各ゾーンに指定できるイニシエータポートは最大 4 つです。

このタスクについて

- このタスクは、環境 ONTAP 9.1 以降で実行します。

- FibreBridge 7600N ブリッジは、 ONTAP 9.6 以降でサポートされます。
- このタスクで使用するゾーニングは、 ONTAP 9.1 以降が対象です。
- ONTAP では、ディスクへのパスに使用できる FC イニシエータポートは最大 4 つです。そのため、問題を回避するためにゾーニングを変更する必要があります。

  ケーブル接続を再接続してシェルフを統合すると、各ディスクに 8 つの FC ポートからアクセスできるようにゾーニングが変更されます。ゾーニングを変更して各ゾーンのイニシエータポートを 4 つに減らす必要があります。

ステップ

1. FC スイッチのストレージゾーンを更新します。具体的には、既存の各ゾーンからイニシエータポートの半分を削除し、 FibreBridge 7600N / 7500N の FC2 ポート用の新しいゾーンを作成します。

   新しい FC2 ポート用のゾーンには、既存のゾーンから削除したイニシエータポートが含まれます。

   の FC スイッチに関するセクションを参照してください "ファブリック接続 MetroCluster のインストールと設定" ゾーニング・コマンドの詳細については、を参照してください。

FibreBridge 7600N / 7500N ブリッジ追加時の **2** つ目のブリッジ **FC** ポートのケーブル接続

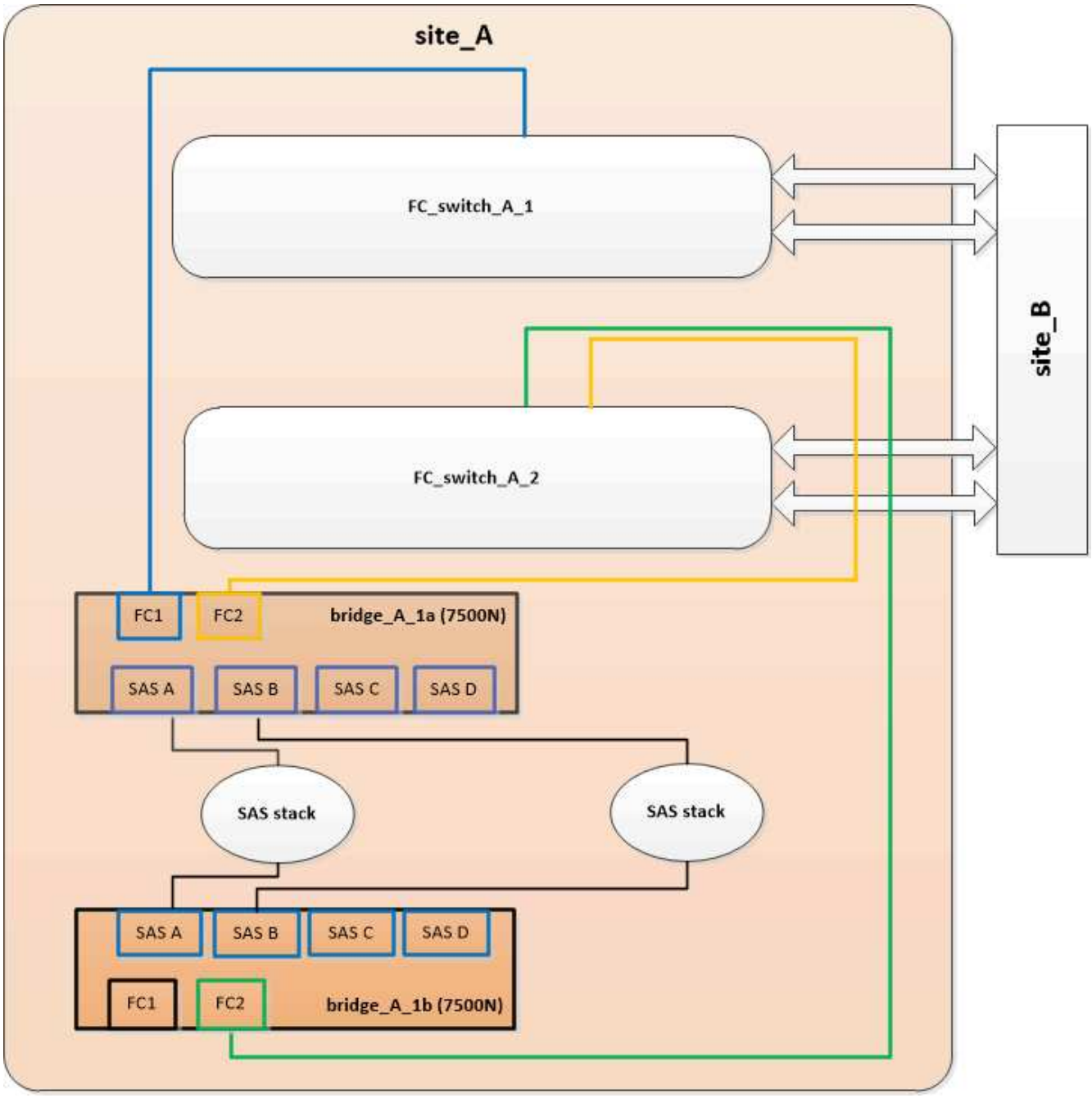
FibreBridge 7600N / 7500N ブリッジを構成に追加した場合、各 FibreBridge 7600N / 7500N ブリッジの 2 つ目の FC ポートをケーブル接続してストレージスタックへの複数のパスを提供することができます。

作業を開始する前に

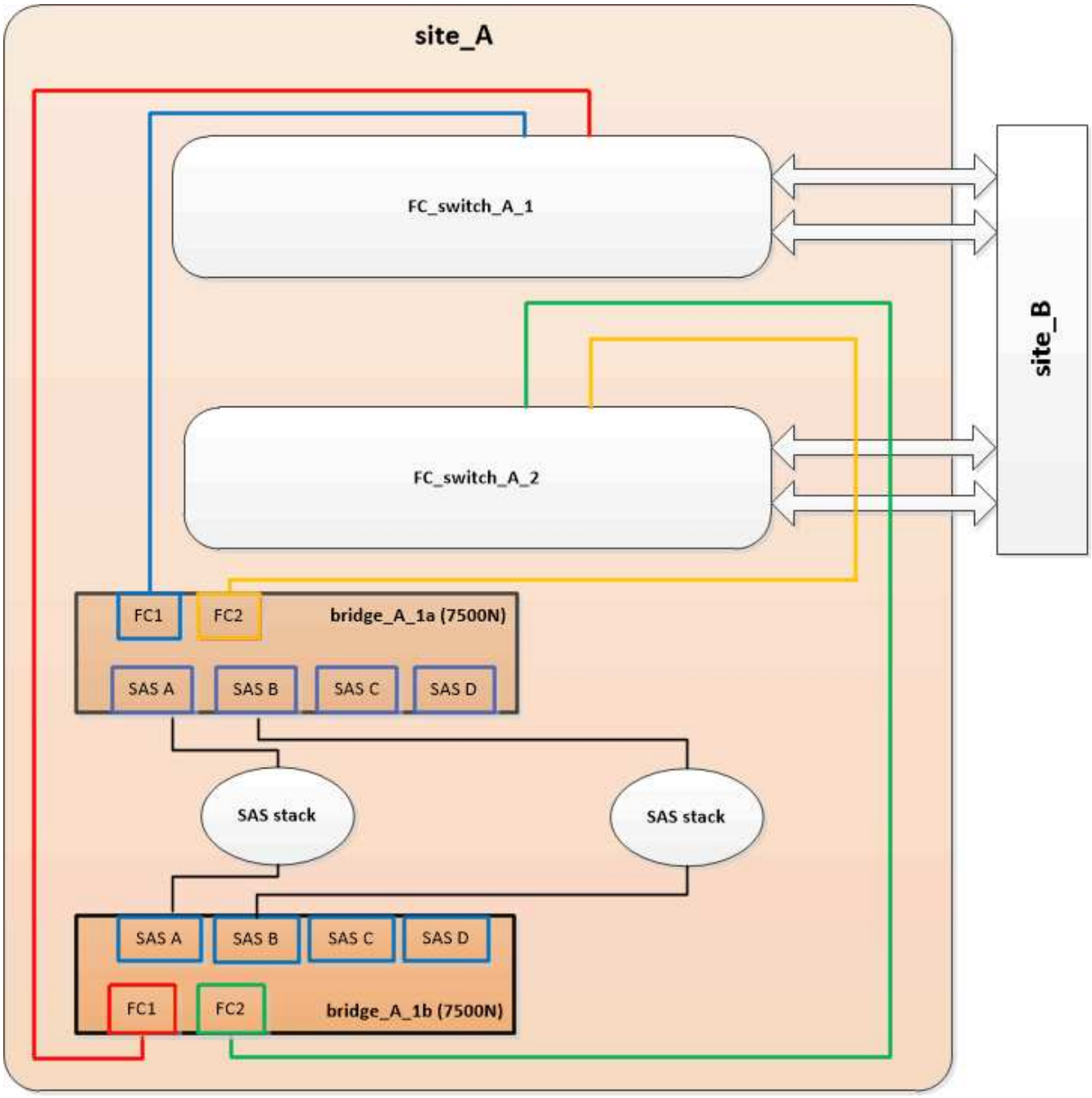
2 つ目の FC ポートにゾーンを提供するようにゾーニングを調整しておく必要があります。

手順

1. 上段のブリッジの FC2 ポートを FC_switch_A_2 の正しいポートにケーブル接続します。



2. 下段のブリッジの FC1 ポートを FC_switch_A_1 の正しいポートにケーブル接続します。



3. ブリッジに接続されているディスクとの接続を確認します。

   'run local sysconfig -v

   出力には、コントローラのイニシエータポートに接続されているディスクが表示され、 FC-to-SAS ブリッジに接続されているシェルフが示されます。

```
node_A_1> run local sysconfig -v
NetApp Release 9.3.2X18: Sun Dec 13 01:23:24 PST 2015
System ID: 0536872165 (node_A_1); partner ID: 0536872141 (node_B_1)
System Serial Number: 940001025465 (node_A_1)
System Rev: 70
System Storage Configuration: Multi-Path HA**<=== Configuration should
```

```
be multi-path HA**
.
.
.
slot 0: FC Host Adapter 0g (QLogic 8324 rev. 2, N-port, <UP>)**<===
Initiator port**
        Firmware rev:      7.5.0
        Flash rev:         0.0.0
        Host Port Id:      0x60100
        FC Node Name:      5:00a:098201:bae312
        FC Port Name:      5:00a:098201:bae312
        SFP Vendor:        FINISAR CORP.
        SFP Part Number:   FTLF8529P3BCVAN1
        SFP Serial Number: URQ0R1R
        SFP Capabilities:  4, 8 or 16 Gbit
        Link Data Rate:    16 Gbit
        Switch Port:       brcd6505-fcs40:1
  **<List of disks visible to port\>**
         ID     Vendor   Model            FW    Size
        brcd6505-fcs40:12.126L1527     : NETAPP   X302_HJUPI01TSSM NA04
847.5GB (1953525168 512B/sect)
        brcd6505-fcs40:12.126L1528     : NETAPP   X302_HJUPI01TSSA NA02
847.5GB (1953525168 512B/sect)
        .
        .
        .
        **<List of FC-to-SAS bridges visible to port\>**
        FC-to-SAS Bridge:
        brcd6505-fcs40:12.126L0        : ATTO     FibreBridge7500N A30H
FB7500N100104
        brcd6505-fcs42:13.126L0        : ATTO     FibreBridge7500N A30H
FB7500N100104
        .
        .
        .
  **<List of storage shelves visible to port\>**
        brcd6505-fcs40:12.shelf6: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        brcd6505-fcs40:12.shelf8: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        .
        .
        .
```

ブリッジのケーブル接続を変更したら、 FC-to-SAS ブリッジの未使用の SAS ポートを無効にして、未使用のポートに関連するヘルスモニタアラートが生成されないようにする必要があります。

手順

1. 上段の FC-to-SAS ブリッジで未使用の SAS ポートを無効にします。

   a. ブリッジの CLI にログインします。

   b. 未使用のポートを無効にします。

      ATTO 7500N ブリッジを設定している場合はすべての SAS ポート（ A~D ）がデフォルトで有効になっているため、使用されていない SAS ポートを無効にする必要があります。

      'SASortDisable_SAS port_

      SAS ポート A と B を使用している場合は、 SAS ポート C と D を無効にする必要があります。次の例は、未使用の SAS ポート C と D を無効にします。

      ```
      Ready. *
      SASPortDisable C

      SAS Port C has been disabled.

      Ready. *
      SASPortDisable D

      SAS Port D has been disabled.

      Ready. *
      ```

   c. ブリッジ設定を保存します :+SaveConfiguration

      次の例は、 SAS ポート C と D が無効になっていることを示しています。設定が保存されたことを示すアスタリスクが表示されなくなります。

```
Ready. *
SaveConfiguration

Ready.
```

2. 下段の FC-to-SAS ブリッジで同じ手順を繰り返します。

シリアルポート、 Telnet 、および FTP を組み合わせて使用すると、推奨される管理インターフェイスの代わりに FibreBridge ブリッジを管理できます。ブリッジをインストールする前に、システムが適切なインターフェイスの要件を満たしている必要があります。

シリアルポートまたは Telnet を使用して、ブリッジとイーサネット管理 1 ポートを設定し、ブリッジを管理できます。FTP を使用して、ブリッジファームウェアを更新できます。

管理インターフェイスの詳細については、使用しているモデルブリッジに対応した ATTO FibreBridge Installation and Operation Manual を参照してください。

ATTO FibreBridge の説明ページにあるリンクを使用して、ATTO Web サイトからこのドキュメントにアクセスできます。

シリアルポート

シリアルポートを使用してブリッジを設定および管理し、イーサネット管理 1 ポートを設定する場合は、システムが次の要件を満たしている必要があります。

- シリアルケーブル（ブリッジのシリアルポートからセットアップに使用するコンピュータのシリアル（ COM ）ポートに接続）

  ブリッジのシリアルポートは RJ-45 で、ピン配列はコントローラと同じです。

- Hyperterminal 、 TeraTerm 、 PuTTY などの端末エミュレーションプログラム。コンソールにアクセスします

  ターミナルプログラムは、画面出力をファイルに記録できる必要があります。

Telnet

Telnet を使用してブリッジを設定および管理する場合は、システムが次の要件を満たしている必要があります。

- シリアルケーブル（ブリッジのシリアルポートからセットアップに使用するコンピュータのシリアル（ COM ）ポートに接続）

  ブリッジのシリアルポートは RJ-45 で、ピン配列はコントローラと同じです。

- （推奨）デフォルト以外のユーザ名とパスワード（ブリッジへのアクセス用）
- Hyperterminal 、 TeraTerm 、 PuTTY などの端末エミュレーションプログラム。コンソールにアクセスします

  ターミナルプログラムは、画面出力をファイルに記録できる必要があります。

- 各ブリッジのイーサネット管理 1 ポートの IP アドレス、サブネットマスク、およびゲートウェイ情報

FTP

FTP を使用してブリッジファームウェアを更新する場合は、システムが次の要件を満たしている必要があります。

- 標準イーサネットケーブル（ブリッジのイーサネット管理 1 ポートからネットワークへの接続用）
- （推奨）デフォルト以外のユーザ名とパスワード（ブリッジへのアクセス用）

障害が発生した電源装置モジュールのホットリプレース

ブリッジの電源装置モジュールのステータスが変わった場合は、電源装置モジュールを取り外して取り付けることができます。

電源装置モジュールのステータスの変化は、ブリッジの LED で確認できます。また、 ExpressNAV GUI とブリッジ CLI 、シリアルポート、または Telnet を使用して、電源装置モジュールのステータスを確認することもできます。

- この手順は NDO （システムの停止を伴わない）機能であり、完了までに約 15 分かかります。
- 管理パスワードと FTP サーバまたは SCP サーバへのアクセスが必要です。

管理インターフェイスの詳細については、使用しているモデルブリッジに対応した ATTO FibreBridge Installation and Operation Manual を参照してください。

ATTO FibreBridge の説明ページに記載されているリンクを使用して、このコンテンツや ATTO Web サイト上のその他のコンテンツにアクセスできます。

FC-to-SAS ブリッジのインバンド管理

ONTAP 9.5 以降では、 FibreBridge 7500N / 7600N ブリッジについて、 IP 管理に代わる方法としてインバンド管理がサポートされます。ONTAP 9.8 以降では、アウトオブバンド管理は廃止されています。

このタスクについて

ONTAP 9.8 以降では 'storage bridge コマンドは 'system bridge コマンドに置き換えられました 次の手順は「 storage bridge 」コマンドを示していますが、 ONTAP 9.8 以降を実行している場合は「 system bridge 」コマンドが優先されます。

インバンド管理を使用すると、 ONTAP CLI からブリッジへの FC 接続を介してブリッジを管理および監視できます。ブリッジのイーサネットポートを介してブリッジに物理的にアクセスする必要がないため、ブリッジのセキュリティの脆弱性が軽減されます。

ブリッジのインバンド管理が可能かどうかは、 ONTAP のバージョンによって異なります。

- ONTAP 9.8 以降では、ブリッジはデフォルトでインバンド接続を介して管理され、 SNMP を介したブリッジのアウトオブバンド管理は廃止されています。
- ONTAP 9.5 から 9.7 ：インバンド管理またはアウトオブバンド管理のどちらかで SNMP 管理がサポートされます。
- ONTAP 9.5 よりも前のバージョンでは、アウトオブバンドの SNMP 管理のみがサポートされます。

ブリッジの CLI コマンドは、 ONTAP インターフェイスの ONTAP インターフェイス「 storage bridge run -cli -name_bridge-name_command_bridge-command-name_` コマンド」から実行できます。

ブリッジの物理接続を制限することでセキュリティを向上させるために、 IP アクセスを無効にしたインバンド管理の使用を推奨します。

関連情報

"同じモデルの交換用ブリッジとのホットスワップ"

"FibreBridge 7500N と 7600N ブリッジのホットスワップ"

"FibreBridge 6500N ブリッジと FibreBridge 7600N / 7500N ブリッジのホットスワップ"

"SAS ディスクシェルフとブリッジのスタックのホットアド"

ONTAP から FibreBridge ブリッジを管理します

ONTAP 9.5 以降では、 ONTAP CLI を使用して FibreBridge コマンドをブリッジに送信し、コマンドの結果を表示することができます。

このタスクについて

ONTAP 9.8 以降では 'storage bridge コマンドは 'system bridge コマンドに置き換えられました 次の手順は「 storage bridge 」コマンドを示していますが、 ONTAP 9.8 以降を実行している場合は「 system bridge 」コマンドが優先されます。

手順

1. 「 storage bridge run -cli 」コマンドで該当する FibreBridge コマンドを実行します。

   storage bridge run -cli-name_bridge-name_command_" コマンドテキスト "_`

   次のコマンドは、 ONTAP プロンプトから FibreBridge 「 S ASPortDisable 」コマンドを実行して、ブリッジの SAS ポート b を無効にします。

```
cluster_A::> storage bridge run-cli -name "SASPortDisable b"

SAS Port B has been disabled.
Ready
cluster_A::>
```

FibreBridge ブリッジをセキュリティ保護または保護解除します

安全性に問題のあるイーサネットプロトコルをブリッジで簡単に無効にできるように、 ONTAP 9.5 以降ではブリッジを保護することができます。これにより、ブリッジのイーサネットポートが無効になります。イーサネットアクセスを再度有効にすることもできます。

- ブリッジをセキュリティ保護すると、ブリッジの Telnet とその他の IP ポートプロトコルおよびサービス

（ FTP 、 ExpressNAV 、 ICMP 、 QuickNAV ）が無効になります。

- この手順では、 ONTAP 9.5 以降で使用可能な ONTAP プロンプトを使用したアウトオブバンド管理を使用します。

  アウトオブバンド管理を使用していない場合は、ブリッジの CLI からコマンドを問題できます。

- イーサネットポートを再度イネーブルにするには '*unsecurebridge *' コマンドを使用します
- ONTAP 9.7 以前では、 ATTO FibreBridge で「 * securebridge * 」コマンドを実行すると、パートナークラスタでブリッジステータスが正しく更新されない可能性がありました。この場合は、パートナークラスタから「 * securebridge * 」コマンドを実行します。

ONTAP 9.8 以降では '*storage bridge *' コマンドは '*system bridge *' に置き換えられています以下の手順は '*storage bridge *' コマンドを示していますが 'ONTAP 9.8 以降を実行している場合は '*system bridge *' コマンドを使用することをお勧めします

手順

1. ブリッジを含むクラスタの ONTAP プロンプトで、ブリッジのセキュリティ保護を設定または解除します。

   次のコマンドは、 bridge_A_1 をセキュリティ保護します。

   ```
   cluster_A> storage bridge run-cli -bridge bridge_A_1 -command
   securebridge
   ```

   次のコマンドは、 bridge_A_1 のセキュリティ保護を解除します。

   ```
   cluster_A> storage bridge run-cli -bridge bridge_A_1 -command
   unsecurebridge
   ```

2. ブリッジを含むクラスタの ONTAP プロンプトで、ブリッジの設定を保存します。

   'storage bridge run-cli-bridge-name_command savecfigation

   次のコマンドは、 bridge_A_1 をセキュリティ保護します。

   ```
   cluster_A> storage bridge run-cli -bridge bridge_A_1 -command
   saveconfiguration
   ```

3. ブリッジを含むクラスタの ONTAP プロンプトから、ブリッジのファームウェアを再起動します。

   *storage bridge run-cli-bridge_name-name_command firmwareestart *

   次のコマンドは、 bridge_A_1 をセキュリティ保護します。

```
cluster_A> storage bridge run-cli -bridge bridge_A_1 -command
firmwarerestart
```

FC スイッチのメンテナンスと交換

Brocade FC スイッチのファームウェアをアップグレードまたはダウングレードします

Brocade FC スイッチのファームウェアをアップグレードまたはダウングレードするには、 Brocade 固有のコマンドを使用してスイッチを無効にし、ファームウェアの変更を実行および確認し、スイッチをリブートして再度有効にする必要があります。

このタスクについて

構成に対して次のタスクを確認し、実行したことを確認します。

- 新しいファームウェアバージョンがソリューションと互換性があることを確認してください。詳細については、"Hardware Universe"をご覧ください。
- ファームウェアファイルを用意しておきます。
- システムが正しくケーブル接続されている。
- ストレージシェルフへのすべてのパスを使用できます。
- ディスクシェルフスタックが安定している。
- FCスイッチファブリックは正常な状態です。
- 障害が発生したコンポーネントがシステムに存在しません。
- システムは正常に動作しています。
- 管理パスワードとFTPサーバまたはSCPサーバへのアクセス権が必要です。
- コンソールロギングが有効になっています。

  "コンソールログを有効にする"

ファームウェアのアップグレードまたはダウングレード中はスイッチファブリックが無効になり、MetroCluster 構成は 2 つ目のファブリックを使用して運用を継続します。

Fabric OS 9.0.1以降では、BrocadeスイッチでSNMPv2はサポートされません。Fabric OS 9.0.1以降にアップグレードする場合は、ヘルスモニタリングにSNMPv3を使用する必要があります。詳細については、を参照してください "MetroCluster 構成での SNMPv3 の設定"。

Fabric OS V 9.2.x以降にアップグレードする場合は、Brocade TruFOS証明書をインストールする必要があります。詳細については、を参照してください。"BrocadeファブリックOSソフトウェアアップグレードガイド（9.2.x）"

各スイッチファブリックでこのタスクを順に実行し、すべてのスイッチで同じファームウェアバージョンが実行されるようにする必要があります。

これはシステムの停止を伴わない手順であり、完了までに約 1 時間かかります。

手順

1. ファブリック内の各スイッチにログインします。

   次の手順の例では 'FC_switch_A_1 スイッチを使用します

2. ファブリック内の各スイッチを無効にします。

   switchCfgPersistentDisable'

   このコマンドが使用できない場合は、「 witchDisable 」コマンドを実行します。

   ```
   FC_switch_A_1:admin> switchCfgPersistentDisable
   ```

3. 必要なファームウェアバージョンをダウンロードします。

   'firmwaredownload

   ファイル名の入力を求められたら、ファームウェアファイルのサブディレクトリまたは相対パスを指定する必要があります。

   ファームウェアダウンロードコマンドは両方のスイッチで同時に実行できますが ' 次の手順に進む前にファームウェアをダウンロードして適切にコミットする必要があります

   ```
   FC_switch_A_1:admin> firmwaredownload
   Server Name or IP Address: 10.64.203.188
   User Name: test
   File Name: v7.3.1b
   Network Protocol(1-auto-select, 2-FTP, 3-SCP, 4-SFTP, 5-HTTP) [1]: 2
   Password:
   Server IP: 10.64.203.188, Protocol IPv4
   Checking system settings for firmwaredownload...
   System settings check passed.
   ```

4. ファームウェアがダウンロードされ、両方のパーティションにコミットされたことを確認します。

   'firmwareShow

   次の例では、両方のイメージが更新されているため、ファームウェアのダウンロードが完了しています。

```
FC_switch_A_1:admin> firmwareShow
Appl     Primary/Secondary Versions

------------------------------------------

FOS      v7.3.1b

         v7.3.1b
```

5. スイッチをリブートします。

   'reboot

   一部のファームウェアバージョンでは、ファームウェアのダウンロードが完了すると自動的に haReboot 処理が実行されます。haReboot が実行された場合でも、この手順のリブートは必要です。

```
FC_switch_A_1:admin> reboot
```

6. 新しいファームウェアが中間ファームウェアレベルであるか、最終版のリリースであるかを確認します。

   ダウンロードが中間ファームウェアレベルの場合は、指定したリリースがインストールされるまで上記の 2 つの手順を実行します。

7. スイッチを有効にします。

   switchCfgPersistentEnable'

   このコマンドを使用できない場合、「 reboot 」コマンドの実行後にスイッチが「 enabled 」状態になっている必要があります。

```
FC_switch_A_1:admin> switchCfgPersistentEnable
```

8. スイッチがオンラインであり、すべてのデバイスがログインされていることを確認します。

   'switchShow

```
FC_switch_A_1:admin> switchShow
```

9. スイッチ内のポートグループまたはすべてのポートグループのバッファ使用状況が正しく表示されることを確認します。

   *portbuffershow *

```
FC_switch_A_1:admin> portbuffershow
```

10. ポートの現在の設定が正しく表示されることを確認します。

    portcfgshow

    ```
    FC_switch_A_1:admin> portcfgshow
    ```

    ポートの設定（速度、モード、トランキング、暗号化など）を確認します。 圧縮機能を使用して、スイッチ間リンク（ ISL ）で出力されるようになりました。ポート設定がファームウェアのダウンロードの影響を受けていないことを確認します。

11. ONTAP で MetroCluster 構成の動作を確認します。
    a. システムがマルチパスかどうかを確認します。 `+* node run -node -name_sysconfig -a *`
    b. 両方のクラスタにヘルス・アラートがないかどうかを確認します `+* system health alert show *`
    c. MetroCluster 構成と動作モードが正常であることを確認します :`+* MetroCluster show*`
    d. MetroCluster チェック :`+* MetroCluster check run*` を実行します
    e. MetroCluster チェックの結果を表示します :`+* MetroCluster check show*`
    f. スイッチにヘルス・アラートがあるかどうかを確認します（ある場合）： `+* storage switch show *`
    g. Config Advisor を実行します。

       "ネットアップのダウンロード： Config Advisor"

    h. Config Advisor の実行後、ツールの出力を確認し、推奨される方法で検出された問題に対処します。
12. 15 分待ってから、 2 つ目のスイッチファブリックについてこの手順を繰り返します。

Cisco FC スイッチのファームウェアをアップグレードまたはダウングレードする

Cisco FC スイッチのファームウェアをアップグレードまたはダウングレードするには、Cisco 固有のコマンドを使用してスイッチを無効にし、アップグレードを実行および確認し、スイッチをリブートして再度有効にする必要があります。

このタスクについて

構成に対して次のタスクを確認し、実行したことを確認します。

- システムが正しくケーブル接続されている。
- ストレージシェルフへのすべてのパスを使用できます。
- ディスクシェルフスタックが安定している。
- FCスイッチファブリックは正常な状態です。
- システムのすべてのコンポーネントが正常である。
- システムは正常に動作しています。
- 管理パスワードとFTPサーバまたはSCPサーバへのアクセス権が必要です。

- コンソールロギングが有効になっています。

  "コンソールログを有効にする"

ファームウェアのアップグレードまたはダウングレード中はスイッチファブリックが無効になり、MetroCluster 構成は 2 つ目のファブリックを使用して運用を継続します。

各スイッチファブリックでこのタスクを順に実行し、すべてのスイッチで同じファームウェアバージョンが実行されていることを確認する必要があります。

ファームウェアファイルが必要です。

これはシステムの停止を伴わない手順であり、完了までに約 1 時間かかります。

手順

1. ファブリック内の各スイッチにログインします。

   この例で使用するスイッチは FC_switch_A_1 および FC_switch_B_1 です。

2. 各スイッチの bootflash ディレクトリに十分なスペースがあるかどうかを確認します。

   「 * dir bootflash*` 」

   それ以外の場合は、「 Delete bootflash: file_name 」コマンドを使用して不要なファームウェアファイルを削除します。

3. Kickstart ファイルとシステムファイルをスイッチにコピーします。

   'copy_source_filetarget_file_

   次の例では、キックスタートファイル (`m 9200-s2ek9-mz.5.2.1.bin'`) とシステムファイル（/firmware/`path の FTP サーバ 10.10.10.55 にあります。

   次の例は、 FC_switch_A_1 で実行するコマンドを示しています。

   ```
   FC_switch_A_1# copy ftp://10.10.10.55/firmware/m9200-s2ek9-kickstart-
   mz.5.2.1.bin bootflash:m9200-s2ek9-kickstart-mz.5.2.1.bin
   FC_switch_A_1# copy ftp://10.10.10.55/firmware/m9200-s2ek9-mz.5.2.1.bin
   bootflash:m9200-s2ek9-mz.5.2.1.bin
   ```

4. このファブリック内の両方のスイッチで、すべてのVSANを無効にします。

   VSANをディセーブルにするには、次の手順 を使用します。

   a. 設定端末を開きます。

      'config t`

   b. 「*VSAN database *'」と入力します

c. VSANの状態を確認します。

show vsan

すべてのVSANがアクティブである必要があります。

d. VSANを一時停止します。

VSAN_vsan-num_suspend

例：'VSAN 10 suspend

e. VSANの状態を再度確認します。

show vsan+all VSANを一時停止する必要があります

f. 設定ターミナルを終了します。

「* end *」と入力します

g. 設定を保存します。

'*copy running-config startup-config *

次の例は、FC_switch_A_1の出力を表示します。

```
FC_switch_A_1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
FC_switch_A_1(config)# vsan database
FC_switch_A_1(config-vsan-db)# show vsan
vsan 1 information
         name:VSAN0001  state:active
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:up

vsan 30 information
         name:MC1_FCVI_2_30  state:active
         interoperability mode:default
         loadbalancing:src-id/dst-id
         operational state:up

vsan 40 information
         name:MC1_STOR_2_40  state:active
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:up

vsan 70 information
```

```
         name:MC2_FCVI_2_70  state:active
         interoperability mode:default
         loadbalancing:src-id/dst-id
         operational state:up

vsan 80 information
         name:MC2_STOR_2_80  state:active
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:up

vsan 4079:evfp_isolated_vsan

vsan 4094:isolated_vsan

FC_switch_A_1(config-vsan-db)# vsan 1 suspend
FC_switch_A_1(config-vsan-db)# vsan 30 suspend
FC_switch_A_1(config-vsan-db)# vsan 40 suspend
FC_switch_A_1(config-vsan-db)# vsan 70 suspend
FC_switch_A_1(config-vsan-db)# vsan 80 suspend
FC_switch_A_1(config-vsan-db)# end
FC_switch_A_1#
FC_switch_A_1# show vsan
vsan 1 information
         name:VSAN0001  state:suspended
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:down

vsan 30 information
         name:MC1_FCVI_2_30  state:suspended
         interoperability mode:default
         loadbalancing:src-id/dst-id
         operational state:down

vsan 40 information
         name:MC1_STOR_2_40  state:suspended
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:down

vsan 70 information
         name:MC2_FCVI_2_70  state:suspended
         interoperability mode:default
         loadbalancing:src-id/dst-id
         operational state:down
```

```
vsan 80 information
         name:MC2_STOR_2_80  state:suspended
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:down

vsan 4079:evfp_isolated_vsan

vsan 4094:isolated_vsan
```

5. 必要なファームウェアをスイッチにインストールします。

   すべてのシステムブートフラッシュをインストールします :__ systemfile_name _kickstart bootflash:_kickstartfile_name _*`

   次の例は、 FC_switch_A_1 で実行するコマンドを示しています。

```
FC_switch_A_1# install all system bootflash:m9200-s2ek9-mz.5.2.1.bin
kickstart bootflash:m9200-s2ek9-kickstart-mz.5.2.1.bin
Enter Yes to confirm the installation.
```

6. 各スイッチのファームウェアのバージョンをチェックして、正しいバージョンがインストールされていることを確認します。

   *show version *`

7. このファブリック内の両方のスイッチで、すべてのVSANを有効にします。

   VSANをイネーブルにするには、次の手順 を使用します。

   a. 設定端末を開きます。

      '**config t**`

   b. 「*VSAN database *'」と入力します

   c. VSANの状態を確認します。

      show vsan

      VSANは一時停止する必要があります。

   d. VSANをアクティブにします。

      '**no vsan_vsan-num_suspend**

      *例：*no vsan 10 suspend`

   e. VSANの状態を再度確認します。

show vsan

すべてのVSANがアクティブである必要があります。

f. 設定ターミナルを終了します。

「* end *」と入力します

g. 設定を保存します。

'*copy running-config startup-config *

次の例は、FC_switch_A_1の出力を表示します。

```
FC_switch_A_1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
FC_switch_A_1(config)# vsan database
FC_switch_A_1(config-vsan-db)# show vsan
vsan 1 information
         name:VSAN0001  state:suspended
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:down

vsan 30 information
         name:MC1_FCVI_2_30  state:suspended
         interoperability mode:default
         loadbalancing:src-id/dst-id
         operational state:down

vsan 40 information
         name:MC1_STOR_2_40  state:suspended
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:down

vsan 70 information
         name:MC2_FCVI_2_70  state:suspended
         interoperability mode:default
         loadbalancing:src-id/dst-id
         operational state:down

vsan 80 information
         name:MC2_STOR_2_80  state:suspended
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:down
```

```
vsan 4079:evfp_isolated_vsan

vsan 4094:isolated_vsan

FC_switch_A_1(config-vsan-db)# no vsan 1 suspend
FC_switch_A_1(config-vsan-db)# no vsan 30 suspend
FC_switch_A_1(config-vsan-db)# no vsan 40 suspend
FC_switch_A_1(config-vsan-db)# no vsan 70 suspend
FC_switch_A_1(config-vsan-db)# no vsan 80 suspend
FC_switch_A_1(config-vsan-db)#
FC_switch_A_1(config-vsan-db)# show vsan
vsan 1 information
         name:VSAN0001  state:active
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:up

vsan 30 information
         name:MC1_FCVI_2_30  state:active
         interoperability mode:default
         loadbalancing:src-id/dst-id
         operational state:up

vsan 40 information
         name:MC1_STOR_2_40  state:active
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:up

vsan 70 information
         name:MC2_FCVI_2_70  state:active
         interoperability mode:default
         loadbalancing:src-id/dst-id
         operational state:up

vsan 80 information
         name:MC2_STOR_2_80  state:active
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:up

vsan 4079:evfp_isolated_vsan

vsan 4094:isolated_vsan

FC_switch_A_1(config-vsan-db)# end
```

```
FC_switch_A_1#
```

8. ONTAP で MetroCluster 構成の動作を確認します。
   a. システムがマルチパスかどうかを確認します。

      '*node run -node node_name sysconfig -a *

   b. ヘルスアラートがないかどうかを両方のクラスタで確認します。

      「 * system health alert show * 」というメッセージが表示されます

   c. MetroCluster 構成と運用モードが正常な状態であることを確認します。

      「 * MetroCluster show * 」と入力します

   d. MetroCluster チェックを実行します。

      「 * MetroCluster check run * 」のようになります

   e. MetroCluster チェックの結果を表示します。

      「 * MetroCluster check show * 」と表示されます

   f. スイッチにヘルスアラートがないかどうかを確認します（ある場合）。

      「 * storage switch show * 」と表示されます

   g. Config Advisor を実行します。

      "ネットアップのダウンロード： Config Advisor"

   h. Config Advisor の実行後、ツールの出力を確認し、推奨される方法で検出された問題に対処します。
9. 2 つ目のスイッチファブリックに対してこの手順を繰り返します。

新しい **Brocade FC** スイッチへのアップグレード

新しい Brocade FC スイッチにアップグレードする場合は、最初のファブリック内のスイッチを交換し、 MetroCluster 構成が完全に動作していることを確認してから、 2 番目のファブリック内のスイッチを交換する必要があります。

- MetroCluster 構成が正常に動作している必要があります。
- MetroCluster スイッチファブリックは 4 つの Brocade スイッチで構成されます。

  以下の手順の図は、現在のスイッチを示しています。

- スイッチがサポート対象の最新のファームウェアを実行している必要があります。

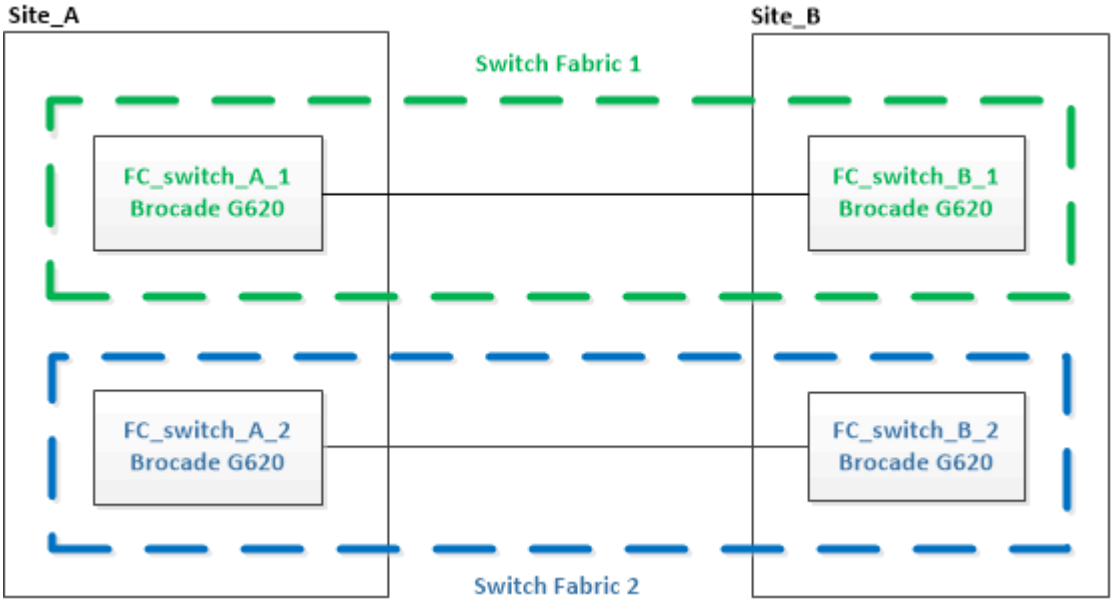
  "NetApp Interoperability Matrix Tool で確認できます"

- これはシステムの停止を伴わない手順であり、完了までに約 2 時間かかります。

- 管理パスワードと FTP サーバまたは SCP サーバへのアクセスが必要です。
- "コンソールログを有効にする" このタスクを実行する前に。

スイッチファブリックは一度に 1 つずつアップグレードされます。

この手順の最後に、 4 つのスイッチすべてを新しいスイッチにアップグレードします。

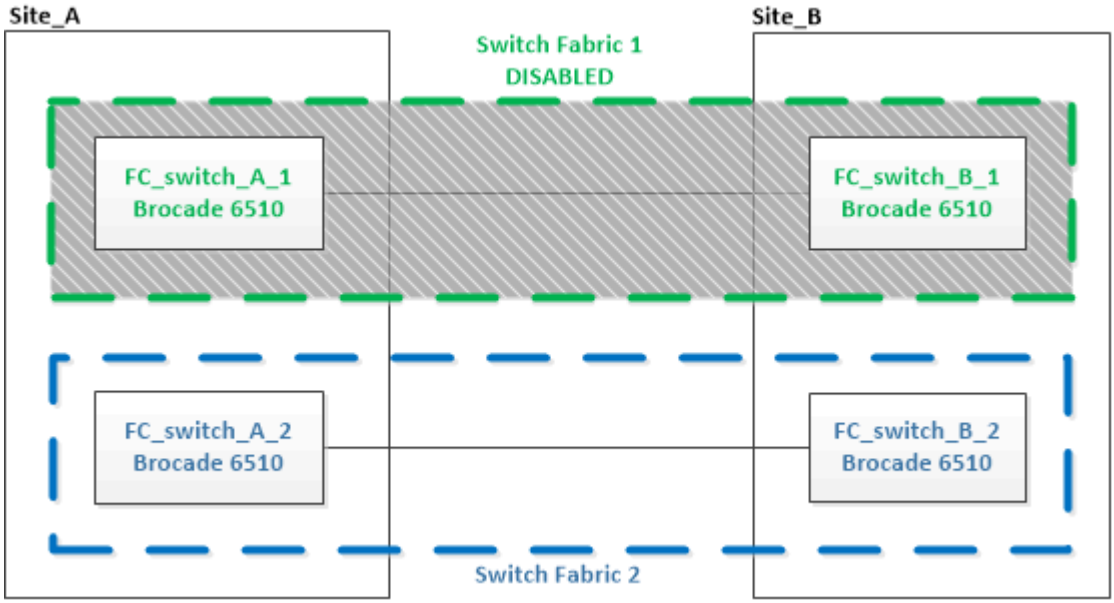


手順

1. 最初のスイッチファブリックを無効にします。

   '*FC_switch_a_1:admin>switchCfgPersistentDisable *

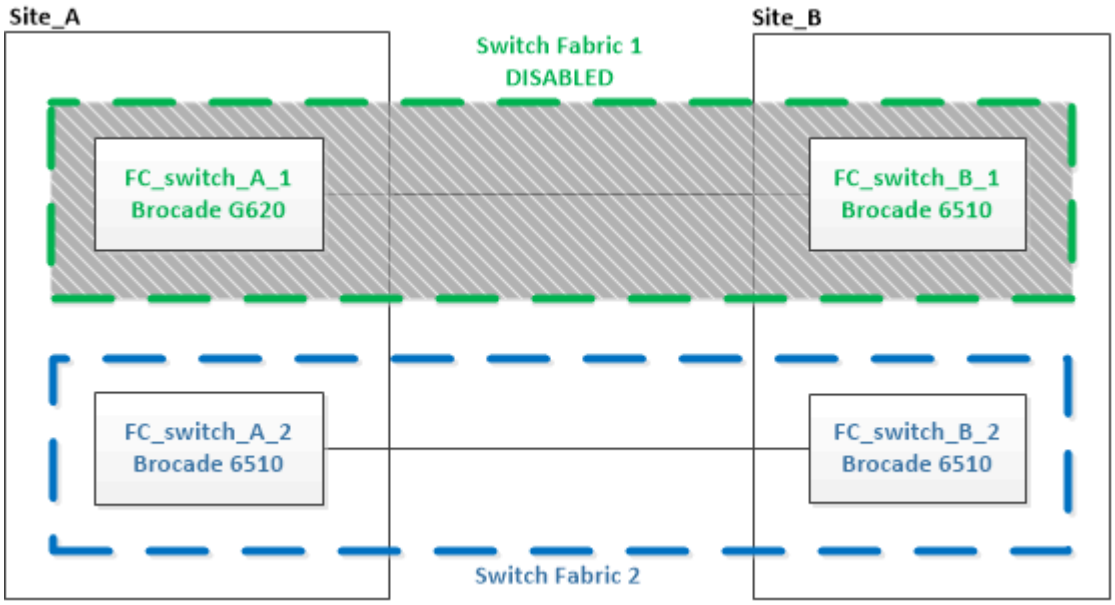
```
FC_switch_A_1:admin> switchCfgPersistentDisable
```



2. 1 つの MetroCluster サイトで古いスイッチを交換します。

   a. 無効なスイッチのケーブルを外してスイッチを取り外します。

   b. 新しいスイッチをラックに設置します。



   c. 両方のスイッチで次のコマンドを実行して、新しいスイッチを無効にします。

      'witchcfgpersistentdisable

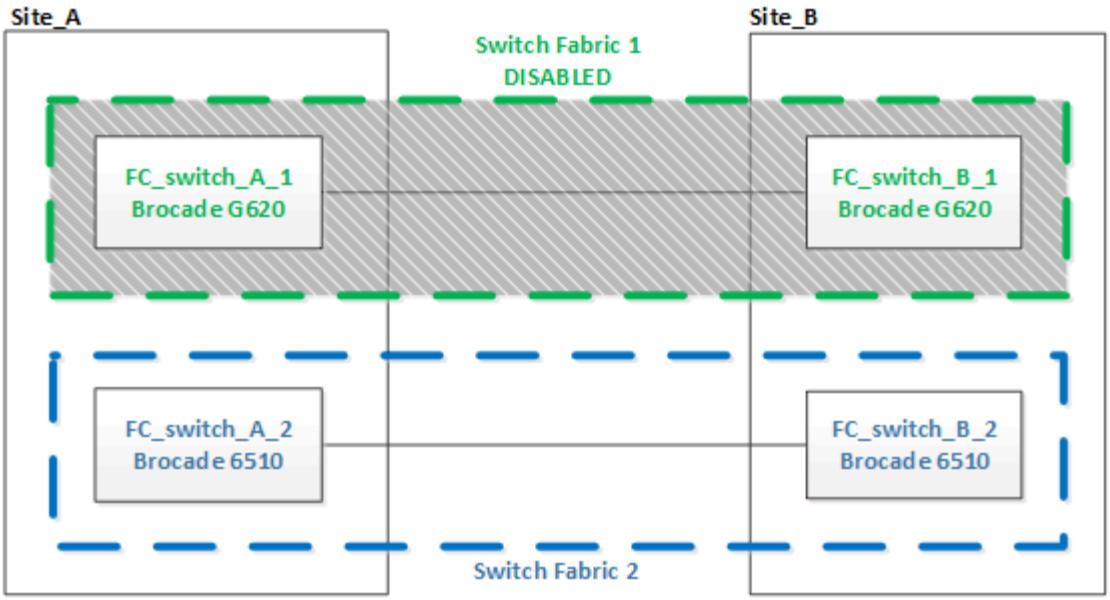
```
FC_switch_A_1:admin> switchCfgPersistentDisable
```

   d. 推奨されるポート割り当てを使用して、新しいスイッチをケーブル接続します。

      "FCスイッチのポート割り当て"

   e. パートナーの MetroCluster サイトで上記の手順を繰り返して、 1 つ目のスイッチファブリック内の 2 つ目のスイッチを交換します。

      ファブリック 1 の両方のスイッチが交換されている。



3. 新しいスイッチに電源を投入し、起動するのを待ちます。
4. 次のいずれかの手順を使用してBrocade FCスイッチを設定します。

   "RCF ファイルを使用して Brocade FC スイッチを設定します"

   "Brocade FC スイッチを手動で設定"

5. スイッチの設定を保存します。

   cfgsave

6. 設定が安定するまで 10 分待ちます。
7. いずれかの MetroCluster ノードで次のコマンドを入力して、ディスクへの接続を確認します。

   'run local sysconfig -v

   出力には、コントローラのイニシエータポートに接続されているディスクが表示され、 FC-to-SAS ブリッジに接続されているシェルフが示されます。

```
node_A_1> run local sysconfig -v
NetApp Release 9.3.2X18: Sun Dec 13 01:23:24 PST 2017
System ID: 4068741258 (node_A_1); partner ID: 4068741260 (node_B_1)
System Serial Number: 940001025471 (node_A_1)
System Rev: 70
System Storage Configuration: Multi-Path HA**<=== Configuration should
be multi-path HA**
.
.
.
slot 0: FC Host Adapter 0g (QLogic 8324 rev. 2, N-port, <UP>)**<===
Initiator port**
```

```
        Firmware rev:      7.5.0
        Flash rev:         0.0.0
        Host Port Id:      0x60130
        FC Node Name:      5:00a:098201:bae312
        FC Port Name:      5:00a:098201:bae312
        SFP Vendor:        UTILITIES CORP.
        SFP Part Number:   FTLF8529P3BCVAN1
        SFP Serial Number: URQ0Q9R
        SFP Capabilities:  4, 8 or 16 Gbit
        Link Data Rate:    16 Gbit
        Switch Port:       brcd6505-fcs40:1
  **<List of disks visible to port\>**
         ID     Vendor   Model            FW    Size
        brcd6505-fcs29:12.126L1527     : NETAPP   X302_HJUPI01TSSM NA04
847.5GB (1953525168 512B/sect)
        brcd6505-fcs29:12.126L1528     : NETAPP   X302_HJUPI01TSSA NA02
847.5GB (1953525168 512B/sect)
        .
        .
        .
        **<List of FC-to-SAS bridges visible to port\>**
        FC-to-SAS Bridge:
        brcd6505-fcs40:12.126L0        : ATTO     FibreBridge6500N 1.61
FB6500N102980
        brcd6505-fcs42:13.126L0        : ATTO     FibreBridge6500N 1.61
FB6500N102980
        brcd6505-fcs42:6.126L0         : ATTO     FibreBridge6500N 1.61
FB6500N101167
        brcd6505-fcs42:7.126L0         : ATTO     FibreBridge6500N 1.61
FB6500N102974
        .
        .
        .
  **<List of storage shelves visible to port\>**
        brcd6505-fcs40:12.shelf6: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        brcd6505-fcs40:12.shelf8: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        .
        .
        .
```

8. スイッチのプロンプトに戻り、スイッチのファームウェアバージョンを確認します。

   「 firmwareShow

スイッチがサポート対象の最新のファームウェアを実行している必要があります。

"NetApp Interoperability Matrix Tool で確認できます"

9. スイッチオーバー処理をシミュレートします。
   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。 + 「 set -privilege advanced 」

      advanced モードで続けるかどうかを尋ねられたら、「 y 」と入力して応答する必要があります。 advanced モードのプロンプトが表示されます（ * > ）。

   b. 「 -simulate 」パラメータを指定して、スイッチオーバー操作を実行します。

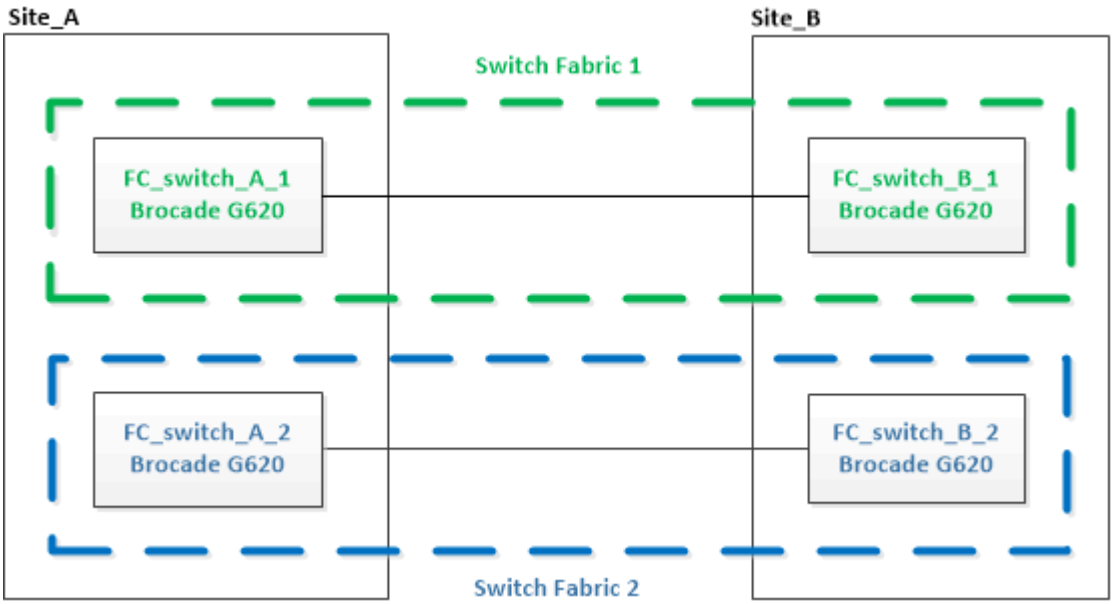
      MetroCluster switchover -simulate

   c. admin 権限レベルに戻ります。

      「特権管理者」

10. 2 つ目のスイッチファブリックで、ここまでの手順を繰り返します。

上記の手順を繰り返して実行すると、 4 つのスイッチすべてがアップグレードされ、 MetroCluster 構成は正常に動作します。



Brocade FC スイッチの交換

この Brocade 固有の手順を使用して、障害が発生したスイッチを交換する必要があります。

このタスクについて

管理パスワードと FTP サーバまたは SCP サーバへのアクセスが必要です。

"コンソールログを有効にする" このタスクを実行する前に。

次の例では、 FC_switch_A_1 が正常に動作しているスイッチ、 FC_switch_B_1 が障害が発生したスイッチです。この例でのスイッチポートの用途を次の表に示します。

ポート接続	ポート
FC-VI 接続	0.3
HBA 接続	1 、 2 、 4 、 5
FC-to-SAS ブリッジの接続	6.7
ISL 接続	10 、 11

例では、 FC-to-SAS ブリッジを 2 つ使用します。FC-to-SAS ブリッジが 3 つ以上ある場合は、追加のポートを無効にしてから有効にする必要があります。

これはシステムの停止を伴わない手順であり、完了までに約 2 時間かかります。

推奨される用途に従ってスイッチポートを割り当ててください。

- "FCスイッチのポート割り当て"

手順

1. 交換中のスイッチをフェンシングします。そのためには、ファブリック内の正常に動作しているスイッチの ISL ポート、および障害が発生したスイッチの FC-VI ポートと HBA ポートを無効にします（障害が発生したスイッチが稼働している場合）。

   a. 各ポートの正常に動作しているスイッチの ISL ポートを無効にします。

      portcfgpersistentdisable_port-number

      ```
      FC_switch_A_1:admin> portcfgpersistentdisable 10
      FC_switch_A_1:admin> portcfgpersistentdisable 11
      ```

   b. 障害が発生したスイッチが稼働している場合は、各ポートの該当するスイッチの FC-VI ポートと HBA ポートを無効にします。

      portcfgpersistentdisable_port-number

```
FC_switch_B_1:admin> portcfgpersistentdisable 0
FC_switch_B_1:admin> portcfgpersistentdisable 1
FC_switch_B_1:admin> portcfgpersistentdisable 2
FC_switch_B_1:admin> portcfgpersistentdisable 3
FC_switch_B_1:admin> portcfgpersistentdisable 4
FC_switch_B_1:admin> portcfgpersistentdisable 5
```

2. 障害が発生したスイッチが動作可能な場合は 'switchshow コマンドの出力を収集します

```
FC_switch_B_1:admin> switchshow
    switchName: FC_switch_B_1
    switchType: 71.2
    switchState:Online
    switchMode: Native
    switchRole: Subordinate
    switchDomain:       2
    switchId:   fffc01
    switchWwn:  10:00:00:05:33:86:89:cb
    zoning:             OFF
    switchBeacon:       OFF
```

3. 新しいスイッチを物理的に設置する前に、スイッチをブートして事前設定します。
   a. 新しいスイッチに電源を投入し、起動するのを待ちます。
   b. スイッチのファームウェアバージョンをチェックして、他の FC スイッチのバージョンと一致していることを確認します。

      「 firmwareShow

   c. のBrocadeの手順に従って、新しいスイッチを設定し"FC スイッチを設定"ます。

      この時点では、新しいスイッチは MetroCluster 構成にケーブル接続されていません。

   d. 新しいスイッチの FC-VI 、 HBA 、ストレージポート、および FC-SAS ブリッジに接続されているポートを無効にします。

```
FC_switch_B_1:admin> portcfgpersistentdisable 0
FC_switch_B_1:admin> portcfgpersistentdisable 1
FC_switch_B_1:admin> portcfgpersistentdisable 2
FC_switch_B_1:admin> portcfgpersistentdisable 3
FC_switch_B_1:admin> portcfgpersistentdisable 4
FC_switch_B_1:admin> portcfgpersistentdisable 5

FC_switch_B_1:admin> portcfgpersistentdisable 6
FC_switch_B_1:admin> portcfgpersistentdisable 7
```

4. スイッチを物理的に交換します。
   a. 障害が発生した FC スイッチの電源をオフにします。
   b. 交換用 FC スイッチの電源をオフにします。
   c. 障害が発生したスイッチのケーブルを外してスイッチを取り外し、どのケーブルがどのポートに接続されているかをメモします。

d. 交換用スイッチをラックに取り付けます。
e. 交換用スイッチを、古いスイッチとまったく同じ配線でケーブル接続します。
f. 新しい FC スイッチの電源をオンにします。

5. ISL暗号化を有効にするには、 "Brocade FC スイッチを手動で設定" 。

   ISL 暗号化を有効にする場合は、次のタスクを実行する必要があります。

   - 仮想ファブリックを無効にします
   - ペイロードを設定します
   - 認証ポリシーを設定します
   - Brocade スイッチで ISL 暗号化を有効にします

6. 新しいスイッチの設定を完了します。

   a. ISL を有効にします。

      portcfgpersistentenable_port-number

      ```
      FC_switch_B_1:admin> portcfgpersistentenable 10
      FC_switch_B_1:admin> portcfgpersistentenable 11
      ```

   b. ゾーニング設定を確認します。

      ```
      cfg show
      ```

   c. 交換用スイッチ（この例では FC_switch_B_1 ）で、 ISL がオンラインであることを確認します。

      'witchshow'

```
FC_switch_B_1:admin> switchshow
switchName: FC_switch_B_1
switchType: 71.2
switchState:Online
switchMode: Native
switchRole: Principal
switchDomain:       4
switchId:   fffc03
switchWwn:  10:00:00:05:33:8c:2e:9a
zoning:             OFF
switchBeacon:       OFF

Index Port Address Media Speed State  Proto
==============================================
...
10   10    030A00 id   16G     Online  FC E-Port
10:00:00:05:33:86:89:cb "FC_switch_A_1"
11   11    030B00 id   16G     Online  FC E-Port
10:00:00:05:33:86:89:cb "FC_switch_A_1" (downstream)
...
```

d. FC ブリッジに接続するストレージポートを有効にします。

```
FC_switch_B_1:admin> portcfgpersistentenable 6
FC_switch_B_1:admin> portcfgpersistentenable 7
```

e. ストレージ、 HBA 、および FC-VI ポートを有効にします。

次の例は、 HBA アダプタに接続されたポートを有効にするコマンドを示しています。

```
FC_switch_B_1:admin> portcfgpersistentenable 1
FC_switch_B_1:admin> portcfgpersistentenable 2
FC_switch_B_1:admin> portcfgpersistentenable 4
FC_switch_B_1:admin> portcfgpersistentenable 5
```

次の例は、 FC-VI アダプタに接続されたポートを有効にするコマンドを示しています。

```
FC_switch_B_1:admin> portcfgpersistentenable 0
FC_switch_B_1:admin> portcfgpersistentenable 3
```

7. ポートがオンラインであることを確認します。

'witchshow'

8. ONTAP で MetroCluster 構成の動作を確認します。
   a. システムがマルチパスかどうかを確認します。

      'node run -node _node-name_sysconfig -a

   b. ヘルスアラートがないかどうかを両方のクラスタで確認します。

      「 system health alert show 」というメッセージが表示されます

   c. MetroCluster 構成と運用モードが正常な状態であることを確認します。

      「 MetroCluster show 」

   d. MetroCluster チェックを実行します。

      「 MetroCluster check run 」のようになります

   e. MetroCluster チェックの結果を表示します。

      MetroCluster チェックショー

   f. スイッチにヘルスアラートがないかどうかを確認します（ある場合）。

      「 storage switch show 」と表示されます

   g. を実行します "Config Advisor"。
   h. Config Advisor の実行後、ツールの出力を確認し、推奨される方法で検出された問題に対処します。

Brocade FC スイッチの名前変更

構成内で一貫性のある名前を使用するために、 Brocade FC スイッチの名前変更が必要になる場合があります。

このタスクについて

"コンソールログを有効にする" このタスクを実行する前に。

手順

1. 1 つのファブリック内のスイッチを永続的に無効にします。

   'switchcfgpersistentdisable

   次の例は '*switchcfgpersistentdisable *' コマンドの出力を示しています

```
7840_FCIP_2:admin> switchcfgpersistentdisable
Switch's persistent state set to 'disabled'
2018/03/09-07:41:06, [ESM-2105], 146080, FID 128, INFO, 7840_FCIP_2, VE
Tunnel 24 is DEGRADED.
2018/03/09-07:41:06, [ESM-2104], 146081, FID 128, INFO, 7840_FCIP_2, VE
Tunnel 24 is OFFLINE.

7840_FCIP_2:admin>
```

2. スイッチの名前を変更します。

   '**switchname_new-switch-name_**

   ファブリック内の両方のスイッチの名前を変更する場合は、各スイッチで同じコマンドを使用します。

   次の例は '**switchname_new-switch-name_**` コマンドの出力を示しています

```
7840_FCIP_2:admin> switchname FC_switch_1_B
Committing configuration...
Done.
Switch name has been changed.Please re-login into the switch for the
change to be applied.
2018/03/09-07:41:20, [IPAD-1002], 146082, FID 128, INFO, FC_switch_1_B,
Switch name has been successfully changed to FC_switch_1_B.
7840_FCIP_2:admin>
```

3. スイッチをリブートします。

   '**reboot**

   ファブリック内の両方のスイッチの名前を変更する場合は、両方のスイッチをリブートします。リブートが完了すると、すべての場所でスイッチの名前が変更されます。

   次に '**reboot**' コマンドの出力例を示します

```
7840_FCIP_2:admin> reboot
Warning: This command would cause the switch to reboot
and result in traffic disruption.
Are you sure you want to reboot the switch [y/n]?y
2018/03/09-07:42:08, [RAS-1007], 146083, CHASSIS, INFO, Brocade7840,
System is about to reload.
Rebooting! Fri Mar  9 07:42:11 CET 2018

Broadcast message from root (ttyS0) Fri Mar  9 07:42:11 2018...

The system is going down for reboot NOW !!
INIT: Switching to runlevel: 6
INIT:
2018/03/09-07:50:48, [ESM-1013], 146104, FID 128, INFO, FC_switch_1_B,
DP0 Configuration replay has completed.
2018/03/09-07:50:48, [ESM-1011], 146105, FID 128, INFO, FC_switch_1_B,
DP0 is ONLINE.

*** CORE FILES WARNING (03/09/18 - 08:00:00 ) ***
10248 KBytes in 1 file(s)
use "supportsave" command to upload


*** FFDC FILES WARNING (03/09/18 - 08:00:00 ) ***
520 KBytes in 1 file(s)
```

4. スイッチを永続的に有効にします :'**switchcfgpersistentenable**

   次の例は '*switchcfgpersistentenable *' コマンドの出力を示しています

```
FC_switch_1_B:admin> switchcfgpersistentenable
Switch's persistent state set to 'enabled'
FC_switch_1_B:admin>
FC_switch_1_B:admin>
FC_switch_1_B:admin> 2018/03/09-08:07:07, [ESM-2105], 146106, FID 128,
INFO, FC_switch_1_B, VE Tunnel 24 is DEGRADED.
2018/03/09-08:07:10, [ESM-2106], 146107, FID 128, INFO, FC_switch_1_B,
VE Tunnel 24 is ONLINE.

FC_switch_1_B:admin>


FC_switch_1_B:admin> switchshow
switchName:     FC_switch_1_B
switchType:     148.0
switchState:    Online
switchMode:     Native
switchRole:     Subordinate
switchDomain:   6
switchId:       fffc06
switchWwn:      10:00:50:eb:1a:9a:a5:79
zoning:         ON (CFG_FAB_2_RCF_9_3)
switchBeacon:   OFF
FC Router:      OFF
FC Router BB Fabric ID: 128
Address Mode:   0
HIF Mode:       OFF

Index Port Address  Media Speed   State       Proto
==================================================
   0   0   060000   id    16G     Online      FC  F-Port
50:0a:09:81:06:a5:5a:08
   1   1   060100   id    16G     Online      FC  F-Port
50:0a:09:83:06:a5:5a:08
```

5. スイッチ名の変更が ONTAP クラスタのプロンプトに表示されることを確認します。

   「 * storage switch show * 」と表示されます

   次に '*storage switch show *' コマンドの出力例を示します

```
cluster_A::*> storage switch show
  (storage switch show)
                      Symbolic                                    Is
Monitor
Switch                Name     Vendor  Model Switch WWN       Monitored
Status
--------------------- -------- ------- ----- ---------------- ---------
-------
Brocade_172.20.7.90
                      RTP-FC01-510Q40
                               Brocade Brocade7840
                                            1000c4f57c904bc8 true
ok
Brocade_172.20.7.91
                      RTP-FC02-510Q40
                               Brocade Brocade7840
                                            100050eb1a9aa579 true
ok
Brocade_172.20.7.92
```

Brocade FC スイッチでの暗号化の無効化

Brocade FC スイッチで暗号化の無効化が必要になる場合があります。

手順

1. メンテナンスの開始を通知する AutoSupport メッセージを両方のサイトから送信します。

```
cluster_A::> autosupport invoke -node * -type all -message MAINT=4h
```

```
cluster_B::> autosupport invoke -node * -type all -message MAINT=4h
```

2. クラスタ A から MetroCluster 構成の動作を確認します
   a. MetroCluster 構成と動作モードが正常であることを確認します :+* MetroCluster show*

```
cluster_A::> metrocluster show
```

   b. MetroCluster チェック :+* MetroCluster check run* を実行します

```
cluster_A::> metrocluster check run
```

c. MetroCluster チェックの結果を表示します :+* `MetroCluster check show*`

```
cluster_A::> metrocluster check show
```

3. 両方のスイッチのステータスを確認します。

「 * fabric show * 」のように表示されます

```
switch_A_1:admin> fabric show
```

```
switch_B_1:admin> fabric show
```

4. 両方のスイッチを無効にします。

*switchdisable *

```
switch_A_1:admin> switchdisable
```

```
switch_B_1:admin> switchdisable
```

5. 各クラスタで使用可能なノードのパスを確認します。

*sysconfig *

```
cluster_A::> system node run -node node-name -command sysconfig -a
```

```
cluster_B::> system node run -node node-name -command sysconfig -a
```

スイッチファブリックが無効になると、システムストレージ構成はシングルパス HA になります。

6. 両方のクラスタのアグリゲートのステータスを確認してください。

```
cluster_A::> aggr status
```

```
cluster_B::> aggr status
```

両方のクラスタについて、アグリゲートがミラーされて正常であることが出力に表示されます。

```
mirrored,normal
```

7. 両方のスイッチで、管理プロンプトから次の手順を繰り返します。

   a. 暗号化されているポートを表示します :+**portenccompshow**

   ```
   switch_A_1:admin> portenccompshow
   ```

   b. 暗号化ポートで暗号化を無効にします。 **+portcfgencrypt – disable_port-number_**

   ```
   switch_A_1:admin> portcfgencrypt --disable 40
   switch_A_1:admin> portcfgencrypt --disable 41
   switch_A_1:admin> portcfgencrypt --disable 42
   switch_A_1:admin> portcfgencrypt --disable 43
   ```

   c. 認証タイプを all に設定します。

   `*authUtil－set -` 全ての `*`

```
switch_A_1:admin> authUtil --set -a all
```

   a. スイッチに認証ポリシーを設定します。オフにするには、 `+*authutil --policy-swoff *` を指定します

   ```
   switch_A_1:admin> authutil --policy -sw off
   ```

   b. 認証 Diffie-Hellman グループを *:+**authutil --set-g *** に設定します

   ```
   switch_A_1:admin> authUtil --set -g *
   ```

   c. 秘密鍵データベース `+*secAuthSecret－remove-all *` を削除します

   ```
   switch_A_1:admin> secAuthSecret --remove -all
   ```

   d. ポートで暗号化が無効になっていることを確認します :+**portenccompshow**

   ```
   switch_A_1:admin> portenccompshow
   ```

e. スイッチ +**switchenable** を有効にします

```
switch_A_1:admin> switchenable
```

f. ISL のステータスを確認します。 +* islshow*

```
switch_A_1:admin> islshow
```

8. 各クラスタで使用可能なノードのパスを確認します。

*sysconfig *

```
cluster_A::> system node run -node * -command sysconfig -a
```

```
cluster_B::> system node run -node * -command sysconfig -a
```

システムの出力は、システムストレージ構成がクアッドパス HA に戻ったことを示しているはずです。

9. 両方のクラスタのアグリゲートのステータスを確認してください。

```
cluster_A::> aggr status
```

```
cluster_B::> aggr status
```

次のシステム出力に示すように、両方のクラスタでアグリゲートがミラーリングされ、正常であることが示されます。

```
mirrored,normal
```

10. クラスタ A から MetroCluster 構成の動作を確認します

a. MetroCluster チェック :+* MetroCluster check run* を実行します

```
cluster_A::> metrocluster check run
```

b. MetroCluster チェックの結果を表示します :+* MetroCluster check show*

```
cluster_A::> metrocluster check show
```

11. メンテナンスが終了したことを示す AutoSupport メッセージを両方のサイトから送信します。

```
cluster_A::> autosupport invoke -node node-name -type all -message
MAINT=END
```

```
cluster_B::> autosupport invoke -node node-name -type all -message
MAINT=END
```

Brocadeスイッチの**ISL**プロパティ、**ISL**ポート、または**IOD / OOD**設定を変更する

追加または高速のコントローラやスイッチなどのハードウェアを追加またはアップグレードする場合は、スイッチへの ISL の追加が必要になることがあります。

作業を開始する前に

システムが正しく設定されていること、すべてのファブリックスイッチが動作していること、およびエラーがないことを確認してください。

"コンソールログを有効にする" このタスクを実行する前に。

ISL リンク上の機器が変更され、新しいリンク設定が現在の設定（トランキングと順序付き配信）をサポートしなくなった場合、ファブリックを正しいルーティングポリシー（配信順序）に再設定する必要があります。In-Order Delivery （ IOD ；インオーダー配信）または Out-of-Order Delivery （ OOD ；アウトオブオーダー配信）のいずれかです。

ONTAPソフトウェアからOODを変更するには、次の手順を実行します。 "ONTAP ソフトウェアでのフレームのインオーダー配信またはアウトオブオーダー配信の設定"

手順

1. FCVI ポートとストレージ HBA ポートを無効にします。

   portcfgpersistentdisable_port number_`

   デフォルトでは、最初の 8 つのポート（ポート 0~7 ）が FCVI とストレージ HBA に使用されます。スイッチのリブート時にポートが無効なままになるように、ポートを永続的に無効にする必要があります。

   次の例では、両方のスイッチで ISL ポート 0~7 を無効にします。

```
Switch_A_1:admin> portcfgpersistentdisable 0-7
Switch_B_1:admin> portcfgpersistentdisable 0-7
```

2. 必要に応じて ISL ポートを変更します。

オプション	ステップ

ISL ポートの速度を変更する	ファブリック上の両方のスイッチで 'portcfgspeed-port number port speed_ コマンドを使用します 次の例では、 ISL ポート速度を 40Gbps から 16Gbps に変更します。 brocade_switch_a_1:admin> portcfgspeed 40 16`  「 witchshow 」コマンドを使用して、速度が変更されたことを確認できます。  'brocade_switch_a_1:admin>switchshow  次の出力が表示されます。  `. . .` ` 40 40 062800 id 16G No_Sync FC Disabled` `. . .`
ISL ポートの距離を変更する	ファブリック内の両方のスイッチで 'portcfglongdistance_port number port distance_ コマンドを使用します
ISL を削除する	リンクを切断します。
ISL を追加する	ISL ポートとして追加するポートに SFP を挿入します。これらのポートがに表示されていることを確認します "ファブリック接続 MetroCluster をインストール" をクリックします。
ISL を再配置する	ISL を再配置する方法は、 ISL を削除してから追加する方法と同じです。まずリンクを切断して ISL を削除し、次に ISL ポートとして追加するポートに SFP を挿入します。

ISLポートを変更する場合は、WDMベンダーが推奨する追加の設定の適用が必要になることがあります。ガイダンスについては、WDMベンダーのドキュメントを参照してください。

3. アウトオブオーダー配信（ OOD ）またはインオーダー配信（ IOD ）を再設定します。

ルーティングポリシーが変更されない場合は再設定は不要で、この手順は無視してかまいません。ONTAP の設定はファブリックの設定と一致する必要があります。ファブリックが OOD に設定されている場合は、 ONTAP も OOD に設定してください。IOD についても同様です。

この手順は、次のシナリオで実行する必要があります。

- 変更前は複数の ISL がトランクを形成していたが、変更後はトランキングがサポートされなくなった。この場合は、ファブリックを OOD に設定する必要があります。

- 変更前は ISL が 1 つで、変更後は複数の ISL を使用する。
- 複数の ISL がトランクを形成する場合は、ファブリックを IOD に設定します。複数の ISL * がトランクを形成できない場合は、ファブリックを OOD に設定します。
- 次の例に示すように 'switchcfgpersistentdisable コマンドを使用して ' スイッチを永続的に無効にします

```
Switch_A_1:admin> switchcfgpersistentdisable
Switch_B_1:admin> switchcfgpersistentdisable
```

i. 次の表に示すように、 ISL ごとにトランキングモードを portcfgtrunkport_port number_` に設定します。

シナリオ（ Scenario ）	手順
ISL をトランキング用に設定する（ IOD ）	'portcfgtrunkport_port number_' を 1 に設定します `FC_switch_A_1:admin> portcfgtrunkport 20 1` `FC_switch_A_1:admin> portcfgtrunkport 21 1` `FC_switch_B_1:admin> portcfgtrunkport 20 1` `FC_switch_B_1:admin> portcfgtrunkport 21 1`
ISL をトランキング用に設定する（ OOD ）	'portcfgtrunkport_port number_' を 0 に設定します `FC_switch_A_1:admin> portcfgtrunkport 20 0` `FC_switch_A_1:admin> portcfgtrunkport 21 0` `FC_switch_B_1:admin> portcfgtrunkport 20 0` `FC_switch_B_1:admin> portcfgtrunkport 21 0`

ii. 必要に応じて、ファブリックを IOD または OOD に設定します。

シナリオ（ Scenario ）	手順

ファブリックを IOD に設定します	次の例に示すように 'iodset’aptpolicypolicy’dlsreset' コマンドを使用して 'IOD ' APT ' および DLS の 3 つの設定を設定します `Switch_A_1:admin> iodset` `Switch_A_1:admin> aptpolicy 1` `Policy updated successfully.` `Switch_A_1:admin> dlsreset` `FC_switch_A_1:admin>portcfgtrunkport 40 1` `FC_switch_A_1:admin>portcfgtrunkport 41 1` `Switch_B_1:admin> iodset` `Switch_B_1:admin> aptpolicy 1` `Policy updated successfully.` `Switch_B_1:admin> dlsreset` `FC_switch_B_1:admin>portcfgtrunkport 20 1` `FC_switch_B_1:admin>portcfgtrunkport 21 1`
ファブリックを OOD に設定します	次の例に示すように 'iodreset’aptpolicy__policy_'dlsset' コマンドを使用して 'IOD ' APT ' および DLS の 3 つの設定を設定します `Switch_A_1:admin> iodreset` `Switch_A_1:admin> aptpolicy 3` `Policy updated successfully.` `Switch_A_1:admin> dlsset` `FC_switch_A_1:admin> portcfgtrunkport 40 0` `FC_switch_A_1:admin> portcfgtrunkport 41 0` `Switch_B_1:admin> iodreset` `Switch_B_1:admin> aptpolicy 3` `Policy updated successfully.` `Switch_B_1:admin> dlsset` `FC_switch_B_1:admin> portcfgtrunkport 40 0` `FC_switch_B_1:admin> portcfgtrunkport 41 0`

iii. スイッチを永続的に有効にします。

'witchcfgpersistentenable

```
switch_A_1:admin>switchcfgpersistentenable
switch_B_1:admin>switchcfgpersistentenable
```

+

このコマンドが存在しない場合は、次の例に示すように、「 witchenable 」コマンドを使用します。

```
brocade_switch_A_1:admin>
switchenable
```

i. 次の例に示すように 'iodshow’aptpolicy’dlsshow' コマンドを使用して OOD 設定を確認します

```
switch_A_1:admin> iodshow
IOD is not set

switch_A_1:admin> aptpolicy

       Current Policy: 3 0(ap)

       3 0(ap) : Default Policy
       1: Port Based Routing Policy
       3: Exchange Based Routing Policy
       0: AP Shared Link Policy
       1: AP Dedicated Link Policy
       command aptpolicy completed

switch_A_1:admin> dlsshow
DLS is set by default with current routing policy
```

これらのコマンドは両方のスイッチで実行する必要があります。

ii. 次の例に示すように 'iodshow' 'aptpolicy' および dlsshow コマンドを使用して IOD 設定を確認します

```
switch_A_1:admin> iodshow
IOD is set

switch_A_1:admin> aptpolicy
       Current Policy: 1 0(ap)

       3 0(ap) : Default Policy
       1: Port Based Routing Policy
       3: Exchange Based Routing Policy
       0: AP Shared Link Policy
       1: AP Dedicated Link Policy
       command aptpolicy completed

switch_A_1:admin> dlsshow
DLS is not set
```

これらのコマンドは両方のスイッチで実行する必要があります。

4. ISL がオンラインであり ' トランキングされていることを確認します（リンク機器がトランキングをサポートしている場合） 'islshow' および trunkshow' コマンドを使用します

FEC が有効になっている場合、ケーブルの長さがすべて同じであるにもかかわらず、トランクグループの最後のオンラインポートの deskew 値に最大 36 の差異が表示されることがあります。

ISL はトランキングされているか	表示されるシステム出力
はい。	ISL がトランキングされている場合 'islshow' コマンドの出力に表示される ISL は 1 つだけですポート 40 または 41 は、トランクマスターに応じて表示されます。trunkshow' の出力は 'ID が 1 つのトランクで ' ポート 40 とポート 41 の両方の物理 ISL を一覧表示します次の例では、ポート 40 および 41 が ISL として使用するように設定されています。 `switch_A_1:admin> islshow 1:` `40-> 40 10:00:00:05:33:88:9c:68 2 switch_B_1 sp: 16.000G bw: 32.000G TRUNK CR_RECOV FEC` `switch_A_1:admin> trunkshow` `1: 40-> 40 10:00:00:05:33:88:9c:68 2 deskew 51 MASTER` `41-> 41 10:00:00:05:33:88:9c:68 2 deskew 15`
いいえ	ISL がトランキングされていない場合 ' 両方の ISL は 'islshow' および trunkshow' の出力に個別に表示されますどちらのコマンドも '1' と 2' の ID を持つ ISL を一覧表示します次の例では、ポート「 40 」と「 41 」が ISL として使用するように設定されています。 `switch_A_1:admin> islshow` `1: 40-> 40 10:00:00:05:33:88:9c:68 2 switch_B_1 sp: 16.000G bw: 16.000G TRUNK CR_RECOV FEC` `2: 41-> 41 10:00:00:05:33:88:9c:68 2 switch_B_1 sp: 16.000G bw: 16.000G TRUNK CR_RECOV FEC` `switch_A_1:admin> trunkshow` `1: 40-> 40 10:00:00:05:33:88:9c:68 2 deskew 51 MASTER` `2: 41-> 41 10:00:00:05:33:88:9c:68 2 deskew 48 MASTER`

5. 両方のスイッチで spinfab' コマンドを実行して 'ISL が正常であることを確認します

```
switch_A_1:admin> spinfab -ports 0/40 - 0/41
```

6. 手順 1 で無効にしたポートを有効にします。

   portEnable_port number_`

   次の例では 'ISL ポート 0 ～ 7 を有効にしています

```
brocade_switch_A_1:admin> portenable 0-7
```

Cisco FC スイッチの交換

障害が発生した Cisco FC スイッチを交換するには、 Cisco 固有の手順を使用する必要があります。

作業を開始する前に

管理パスワードと FTP サーバまたは SCP サーバへのアクセスが必要です。

"コンソールログを有効にする" このタスクを実行する前に。

このタスクについて

これはシステムの停止を伴わない手順であり、完了までに約 2 時間かかります。

この手順の例では、 FC_switch_A_1 が正常に動作しているスイッチ、 FC_switch_B_1 が障害が発生したスイッチです。この例でのスイッチポートの用途を次の表に示します。

ロール	ポート
FC-VI 接続	1/4
HBA 接続	2 、 3 、 5 、 6
FC-to-SAS ブリッジの接続	7 、 8
ISL 接続	36 、 40

例では、 FC-to-SAS ブリッジを 2 つ使用します。FC-to-SAS ブリッジが 3 つ以上ある場合は、追加のポートを無効にしてから有効にする必要があります。

推奨される用途に従ってスイッチポートを割り当ててください。

- "FCスイッチのポート割り当て"

手順

1. 正常に動作しているスイッチの ISL ポートを無効にして、障害が発生したスイッチをフェンシングします。

   次の手順は、正常に動作しているスイッチで実行します。

a. 構成モードに切り替えます :+conf t

b. 「 interface 」コマンドと「 hut 」コマンドを使用して、正常に動作しているスイッチの ISL ポートを無効にします。

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# interface fc1/36
FC_switch_A_1(config)# shut
FC_switch_A_1(config)# interface fc1/40
FC_switch_A_1(config)# shut
```

c. 構成モードを終了し、構成をスタートアップ構成にコピーします。

```
FC_switch_A_1(config)# end
FC_switch_A_1# copy running-config startup-config
FC_switch_A_1#
```

2. 障害が発生したスイッチの FC-VI ポートと HBA ポートをフェンシングします（スイッチが稼働している場合）。

次の手順は、障害が発生したスイッチで実行します。

a. コンフィギュレーションモードを開始します。

「 conf t`

b. 障害が発生したスイッチが稼働している場合は、インターフェイスと shut コマンドを使用して、障害が発生したスイッチの FC-VI ポートと HBA ポートを無効にします。

```
FC_switch_B_1(config)# interface fc1/1
FC_switch_B_1(config)# shut
FC_switch_B_1(config)# interface fc1/4
FC_switch_B_1(config)# shut
FC_switch_B_1(config)# interface fc1/2-3
FC_switch_B_1(config)# shut
FC_switch_B_1(config)# interface fc1/5-6
FC_switch_B_1(config)# shut
```

c. 構成モードを終了し、構成をスタートアップ構成にコピーします。

```
FC_switch_B_1(config)# end
FC_switch_B_1# copy running-config startup-config
FC_switch_B_1#
```

3. 障害が発生したスイッチが稼働している場合は、スイッチの WWN を確認します。

   'How WWN switch`

   ```
   FC_switch_B_1# show wwn switch
   Switch WWN is 20:00:54:7f:ee:e3:86:50
   FC_switch_B_1#
   ```

4. 交換用スイッチを物理的に設置する前に、スイッチをブートして事前設定します。

   この時点では、交換用スイッチは MetroCluster 構成にケーブル接続されていません。パートナースイッチの ISL ポートは無効（シャットモード）かつオフラインになっています。

   a. 交換用スイッチの電源をオンにして、ブートするのを待ちます。
   b. 交換用スイッチのファームウェアバージョンをチェックして、他の FC スイッチのバージョンと一致していることを確認します。

      'how version （バージョンの表示） '

   c. MetroCluster インストールおよび設定ガイドの説明に従って交換用スイッチを設定します（「 Cisco FC スイッチでのゾーニングの設定」セクションは省略します）。

      "ファブリック接続 MetroCluster のインストールと設定"

   ゾーニングはこの手順の後半で設定します。

   a. 交換用スイッチの FC-VI 、 HBA 、およびストレージポートを無効にします。

      ```
      FC_switch_B_1# conf t
      FC_switch_B_1(config)# interface fc1/1
      FC_switch_B_1(config)# shut
      FC_switch_B_1(config)# interface fc1/4
      FC_switch_B_1(config)# shut
      FC_switch_B_1(config)# interface fc1/2-3
      FC_switch_B_1(config)# shut
      FC_switch_B_1(config)# interface fc1/5-6
      FC_switch_B_1(config)# shut
      FC_switch_B_1(config)# interface fc1/7-8
      FC_switch_B_1(config)# shut
      FC_switch_B_1# copy running-config startup-config
      FC_switch_B_1#
      ```

5. 問題のあるスイッチを物理的に交換します。

   a. 障害が発生したスイッチの電源を切ります。
   b. 交換用スイッチの電源をオフにします。

c. 障害が発生したスイッチのケーブルを外してスイッチを取り外し、どのケーブルがどのポートに接続されているかをメモします。

d. 交換用スイッチをラックに取り付けます。

e. 交換用スイッチを、障害が発生したスイッチとまったく同じ配線でケーブル接続します。

f. 交換用スイッチの電源をオンにします。

6. 交換用スイッチの ISL ポートを有効にします。

```
FC_switch_B_1# conf t
FC_switch_B_1(config)# interface fc1/36
FC_switch_B_1(config)# no shut
FC_switch_B_1(config)# end
FC_switch_B_1# copy running-config startup-config
FC_switch_B_1(config)# interface fc1/40
FC_switch_B_1(config)# no shut
FC_switch_B_1(config)# end
FC_switch_B_1#
```

7. 交換用スイッチの ISL ポートが動作していることを確認します。

「インターフェイスの概要」

8. 交換用スイッチのゾーニングを MetroCluster の設定に合わせて調整します。

a. 正常に動作しているファブリックからゾーニング情報を配信します。

この例では、 FC_switch_B_1 が交換され、ゾーニング情報が FC_switch_A_1 から取得されます。

```
FC_switch_A_1(config-zone)# zoneset distribute full vsan 10
FC_switch_A_1(config-zone)# zoneset distribute full vsan 20
FC_switch_A_1(config-zone)# end
```

b. 交換用スイッチで、正常に動作しているスイッチからゾーニング情報が適切に取得されたことを確認します。

「ゾーンの方法」

```
FC_switch_B_1# show zone
zone name FC-VI_Zone_1_10 vsan 10
  interface fc1/1 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/4 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/1 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/4 swwn 20:00:54:7f:ee:b8:24:c0

zone name STOR_Zone_1_20_25A vsan 20
  interface fc1/2 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/3 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/5 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/6 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/2 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/3 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/5 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/6 swwn 20:00:54:7f:ee:b8:24:c0

zone name STOR_Zone_1_20_25B vsan 20
  interface fc1/2 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/3 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/5 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/6 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/2 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/3 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/5 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/6 swwn 20:00:54:7f:ee:b8:24:c0
FC_switch_B_1#
```

c. スイッチの WWN を検索します。

この例では、 2 つのスイッチの WWN は次のとおりです。

- FC_switch_A_1 ： 20 ： 00 ： 54 ： 7F ： ee ： B8 ： 24 ： c0
- FC_switch_B_1 ： 20 ： 00 ： 54 ： 7F ： ee ： C6 ： 80 ： 78

```
FC_switch_B_1# show wwn switch
Switch WWN is 20:00:54:7f:ee:c6:80:78
FC_switch_B_1#

FC_switch_A_1# show wwn switch
Switch WWN is 20:00:54:7f:ee:b8:24:c0
FC_switch_A_1#
```

d. 2 つのスイッチのスイッチ WWN に属していないゾーンメンバーを削除します。

この例では、出力の「 no member interface 」は、ファブリック内のどちらのスイッチのスイッチ WWN にも関連付けられていない次のメンバーを削除する必要があることを示しています。

- ゾーン名 FC-VI_Zone_1_10 VSAN 10
  - インターフェイス fc1/1 sWWN 20:00:54:7F: e:e3:86:50 を参照してください
  - インターフェイス fc1/2 sWWN 20:00:54:7F: e:e3:86:50 を参照してください
- ゾーン名 STOR_Zone_1_20_25A VSAN 20
  - インターフェイス fc1/5 sWWN 20:00:54:7F: e:e3:86:50 を参照してください
  - インターフェイス fc1/8 sWWN 20:00:54:7F: e:e3:86:50 を参照してください
  - インターフェイス fc1/9 sWWN 20:00:54:7F: e:e3:86:50 を参照してください
  - インターフェイス fc1/10 sWWN 20:00:54:7F: e:e3:86:50 を参照してください
  - インターフェイス fc1/11 sWWN 20:00:54:7F: e:e3:86:50 を参照してください
- ゾーン名 STOR_Zone_1_20_25B VSAN 20
  - インターフェイス fc1/8 sWWN 20:00:54:7F: e:e3:86:50 を参照してください
  - インターフェイス fc1/9 sWWN 20:00:54:7F: e:e3:86:50 を参照してください
  - インターフェイス fc1/10 sWWN 20:00:54:7F: e:e3:86:50 を参照してください
  - インターフェイス fc1/11 sWWN 20:00:54:7F:ee:E3-86:50 次の例は、これらのインターフェイスの削除を示しています。

```
 FC_switch_B_1# conf t
 FC_switch_B_1(config)# zone name FC-VI_Zone_1_10 vsan 10
 FC_switch_B_1(config-zone)# no member interface fc1/1 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/2 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# zone name STOR_Zone_1_20_25A vsan
20
 FC_switch_B_1(config-zone)# no member interface fc1/5 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/8 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/9 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/10 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/11 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# zone name STOR_Zone_1_20_25B vsan
20
 FC_switch_B_1(config-zone)# no member interface fc1/8 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/9 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/10 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/11 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# save running-config startup-config
 FC_switch_B_1(config-zone)# zoneset distribute full 10
 FC_switch_B_1(config-zone)# zoneset distribute full 20
 FC_switch_B_1(config-zone)# end
 FC_switch_B_1# copy running-config startup-config
```

e. 交換用スイッチのポートをゾーンに追加します。

   交換用スイッチのケーブル接続は、障害が発生したスイッチとすべて同じにする必要があります。

```
 FC_switch_B_1# conf t
 FC_switch_B_1(config)# zone name FC-VI_Zone_1_10 vsan 10
 FC_switch_B_1(config-zone)# member interface fc1/1 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/2 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# zone name STOR_Zone_1_20_25A vsan 20
 FC_switch_B_1(config-zone)# member interface fc1/5 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/8 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/9 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/10 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/11 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# zone name STOR_Zone_1_20_25B vsan 20
 FC_switch_B_1(config-zone)# member interface fc1/8 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/9 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/10 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/11 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# save running-config startup-config
 FC_switch_B_1(config-zone)# zoneset distribute full 10
 FC_switch_B_1(config-zone)# zoneset distribute full 20
 FC_switch_B_1(config-zone)# end
 FC_switch_B_1# copy running-config startup-config
```

f. ゾーニングが正しく設定されていることを確認します。

「ゾーンの方法」

次の出力例は、 3 つのゾーンを示しています。

```
FC_switch_B_1# show zone
  zone name FC-VI_Zone_1_10 vsan 10
    interface fc1/1 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/2 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/1 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/2 swwn 20:00:54:7f:ee:b8:24:c0

  zone name STOR_Zone_1_20_25A vsan 20
    interface fc1/5 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/8 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/9 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/10 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/11 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/8 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/9 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/10 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/11 swwn 20:00:54:7f:ee:b8:24:c0

  zone name STOR_Zone_1_20_25B vsan 20
    interface fc1/8 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/9 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/10 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/11 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/5 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/8 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/9 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/10 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/11 swwn 20:00:54:7f:ee:b8:24:c0
FC_switch_B_1#
```

g. ストレージとコントローラへの接続を有効にします。

次の例は、ポートの用途を示しています。

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# interface fc1/1
FC_switch_A_1(config)# no shut
FC_switch_A_1(config)# interface fc1/4
FC_switch_A_1(config)# shut
FC_switch_A_1(config)# interface fc1/2-3
FC_switch_A_1(config)# shut
FC_switch_A_1(config)# interface fc1/5-6
FC_switch_A_1(config)# shut
FC_switch_A_1(config)# interface fc1/7-8
FC_switch_A_1(config)# shut
FC_switch_A_1# copy running-config startup-config
FC_switch_A_1#
```

9. ONTAP で MetroCluster 構成の動作を確認します。
   a. システムがマルチパスかどうかを確認します。

      'node run -node _node-name_sysconfig -a

   b. ヘルスアラートがないかどうかを両方のクラスタで確認します。

      「 system health alert show 」というメッセージが表示されます

   c. MetroCluster 構成と運用モードが正常な状態であることを確認します。

      「 MetroCluster show 」

   d. MetroCluster チェックを実行します。

      「 MetroCluster check run 」のようになります

   e. MetroCluster チェックの結果を表示します。

      MetroCluster チェックショー

   f. スイッチにヘルスアラートがないかどうかを確認します（ある場合）。

      「 storage switch show 」と表示されます

   g. Config Advisor を実行します。

      "ネットアップのダウンロード： Config Advisor"

   h. Config Advisor の実行後、ツールの出力を確認し、推奨される方法で検出された問題に対処します。

Cisco FCスイッチの**ISL**プロパティと**IOD / OOD**設定の変更

Cisco FCスイッチでは、スイッチ間リンク（ISL）の追加、ISL速度の変更、In-Order

Delivery（IOD；インオーダー配信）またはOut-of-Order Delivery（OOD；アウトオブオーダー配信）の設定を行うことができます。

Cisco FCスイッチへのISLの追加

ハードウェアを追加またはアップグレードする場合（高速なコントローラや高速なスイッチを追加またはアップグレードする場合など）は、スイッチへのISLの追加が必要になることがあります。

このタスクについて

ファブリック内の両方のスイッチで次の手順を実行して、ISL接続を確認します。

手順

1. ファブリック内の両方のスイッチで、追加する ISL の ISL ポートを無効にします。

   ```
   FC_switch_A_1#config t
   ```

   1行に1つずつ、次のコンフィギュレーションコマンドを入力します。すべてのコンフィギュレーションコマンドを入力したら、Ctrl+Zキーを押します。

   ```
   FC_switch_A_1(config)# interface fc1/36
   FC_switch_A_1(config-if)# shut
   FC_switch_A_1(config)# end
   ```

2. ISLポートとして追加するポートにSFPを挿入し、に従ってケーブル接続し"ファブリック接続 MetroCluster 構成をケーブル接続"ます。

   これらのポートが、追加先のスイッチモデルのケーブル接続ドキュメントに記載されていることを確認します。

3. の手順に従って、ISLポートを設定します"MetroCluster サイト間での ISL のケーブル接続"。
4. ファブリック内の両方のスイッチで、すべての ISL ポートを有効にします（有効になっていない場合）。

   ```
   FC_switch_A_1# config t
   ```

   1行に1つずつ、次のコンフィギュレーションコマンドを入力します。すべてのコンフィギュレーションコマンドを入力したら、Ctrl+Zキーを押して終了します。

   ```
   FC_switch_A_1# interface fc1/36
      FC_switch_A_1(config-if)# no shut
      FC_switch_A_1(config)# end
   ```

5. 両方のスイッチ間に ISL が確立されたことを確認します。

   ```
   show topology isl
   ```

6. 2 つ目のファブリックで手順を繰り返します。

```
--------------------------------------------------------------------------
--------
    ___________Local_________ _________Remote_________ VSAN Cost I/F  PC
I/F  Band
     PC Domain SwName   Port  Port   SwName Domain PC          Stat Stat
Speed width

--------------------------------------------------------------------------
--------
      1   0x11 cisco9 fc1/36  fc1/36 cisco9 0xbc    1    1   15 up   up
16g   64g
      1   0x11 cisco9 fc1/40  fc1/40 cisco9 0xbc    1    1   15 up   up
16g   64g
      1   0x11 cisco9 fc1/44  fc1/44 cisco9 0xbc    1    1   15 up   up
16g   64g
      1   0x11 cisco9 fc1/48  fc1/48 cisco9 0xbc    1    1   15 up   up
16g   64g
```

Cisco FCスイッチでISLポートの速度を変更する

スイッチのISLポートの速度を変更して、ISLの品質を向上させることができます。たとえば、距離が長いISLの速度を下げることができます。

このタスクについて

ファブリック内の両方のスイッチで次の手順を実行して、ISL接続を確認します。

手順

1. ファブリック内の両方のスイッチで、速度を変更するISLのISLポートを無効にします。

   ```
   FC_switch_A_1# config t
   ```

   1行に1つずつ、次のコンフィギュレーションコマンドを入力します。すべてのコンフィギュレーションコマンドを入力したら、Ctrl+Zキーを押して終了します。

   ```
   FC_switch_A_1(config)# interface fc1/36
      FC_switch_A_1(config-if)# shut
      FC_switch_A_1(config)# end
   ```

2. ファブリック内の両方のスイッチで、 ISL ポートの速度を変更します。

   ```
   FC_switch_A_1# config t
   ```

   1行に1つずつ、次のコンフィギュレーションコマンドを入力します。すべてのコンフィギュレーションコマンドを入力したら、Ctrl+Zキーを押して終了します。

```
FC_switch_A_1(config)# interface fc1/36
   FC_switch_A_1(config-if)# switchport speed 16000
```

ポートの速度は16 = 16、000Gbps、8 = 8、000Gbps、4 = 4、000Gbpsです。

スイッチのISLポートがに表示されていることを確認します"ファブリック接続MetroCluster構成をインストールする"。

3. ファブリック内の両方のスイッチで、すべての ISL ポートを有効にします（有効になっていない場合）。

```
FC_switch_A_1# config t
```

1行に1つずつ、次のコンフィギュレーションコマンドを入力します。すべてのコンフィギュレーションコマンドを入力したら、Ctrl+Zキーを押して終了します。

```
FC_switch_A_1(config)# interface fc1/36
   FC_switch_A_1(config-if)# no shut
   FC_switch_A_1(config)# end
```

4. 両方のスイッチ間に ISL が確立されたことを確認します。

```
show topology isl
```

```
------------------------------------------------------------------------
--------
    ___________Local_________ _________Remote_________ VSAN Cost I/F  PC
I/F  Band
     PC Domain SwName   Port  Port   SwName Domain PC          Stat Stat
Speed width

------------------------------------------------------------------------
--------
      1   0x11 cisco9 fc1/36  fc1/36 cisco9 0xbc    1    1   15 up   up
16g   64g
      1   0x11 cisco9 fc1/40  fc1/40 cisco9 0xbc    1    1   15 up   up
16g   64g
      1   0x11 cisco9 fc1/44  fc1/44 cisco9 0xbc    1    1   15 up   up
16g   64g
      1   0x11 cisco9 fc1/48  fc1/48 cisco9 0xbc    1    1   15 up   up
16g   64g
```

5. 2 つ目のスイッチファブリックに対して手順を繰り返します。

標準の IOD 設定を推奨します。OODは、必要な場合にのみ再設定してください。

IODの再設定

フレームのIODを再設定するには、次の手順を実行します。

手順

1. コンフィギュレーションモードを開始します。

   「 conf t`

2. VSAN の交換のインオーダー保証を有効にします。

   ```
   in-order-guarantee vsan <vsan-ID>
   ```

   FC-VI VSAN （ FCVI_1_10 および FCVI_2_30 ）については、フレームと交換のインオーダー保証を VSAN 10 でのみ有効にする必要があります。

   a. VSAN のロードバランシングを有効にします。

      ```
      vsan <vsan-ID> loadbalancing src-dst-id
      ```

   b. 構成モードを終了します。

      「 end 」と入力します

   c. running-config を startup-config にコピーします。

      'copy running-config startup-config

      FC_switch_A_1でフレームのIODを設定するコマンドは次のとおりです。

      ```
      FC_switch_A_1# config t
      FC_switch_A_1(config)# in-order-guarantee vsan 10
      FC_switch_A_1(config)# vsan database
      FC_switch_A_1(config-vsan-db)# vsan 10 loadbalancing src-dst-id
      FC_switch_A_1(config-vsan-db)# end
      FC_switch_A_1# copy running-config startup-config
      ```

      FC_switch_B_1でフレームのIODを設定するコマンドは次のとおりです。

```
FC_switch_B_1# config t
FC_switch_B_1(config)# in-order-guarantee vsan 10
FC_switch_B_1(config)# vsan database
FC_switch_B_1(config-vsan-db)# vsan 10 loadbalancing src-dst-id
FC_switch_B_1(config-vsan-db)# end
FC_switch_B_1# copy running-config startup-config
```

OODの再設定

フレームのOODを再設定するには、次の手順を実行します。

手順

1. コンフィギュレーションモードを開始します。

   「 conf t`

2. VSAN の交換のインオーダー保証を無効にします。

   ```
   no in-order-guarantee vsan <vsan-ID>
   ```

3. VSAN のロードバランシングを有効にします。

   ```
   vsan <vsan-ID> loadbalancing src-dst-id
   ```

4. 構成モードを終了します。

   「 end 」と入力します

5. running-config を startup-config にコピーします。

   'copy running-config startup-config

   FC_switch_A_1でフレームのOODを設定するコマンドは次のとおりです。

   ```
   FC_switch_A_1# config t
   FC_switch_A_1(config)# no in-order-guarantee vsan 10
   FC_switch_A_1(config)# vsan database
   FC_switch_A_1(config-vsan-db)# vsan 10 loadbalancing src-dst-id
   FC_switch_A_1(config-vsan-db)# end
   FC_switch_A_1# copy running-config startup-config
   ```

   FC_switch_B_1でフレームのOODを設定するコマンドは次のとおりです。

```
FC_switch_B_1# config t
FC_switch_B_1(config)# no in-order-guarantee vsan 10
FC_switch_B_1(config)# vsan database
FC_switch_B_1(config-vsan-db)# vsan 10 loadbalancing src-dst-id
FC_switch_B_1(config-vsan-db)# end
FC_switch_B_1# copy running-config startup-config
```

コントローラモジュールに ONTAP を設定する場合は、 MetroCluster 構成の各コントローラモジュールで OOD を明示的に設定する必要があります。

"ONTAPソフトウェアでのフレームのIODまたはOODの設定について"です。

FCスイッチのベンダーまたはモデルを変更する

FCスイッチのベンダーをCiscoからBrocade（またはその逆）に変更するか、スイッチモデルの変更、またはその両方が必要になる場合があります。

このタスクについて

- この手順は、NetApp検証済みスイッチを使用している場合に適用されます。
- "コンソールログを有効にする" このタスクを実行する前に。
- 構成内の両方のファブリックについて、この手順の手順を一度に1つのファブリックで実行する必要があります。

手順

1. [[step_1、手順1]]構成の健全性を確認します。
   a. MetroCluster が構成されていて、各クラスタで通常モードであることを確認します。「 * MetroCluster show * 」

```
cluster_A::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
Remote: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
```

   b. 各ノードでミラーリングが有効になっていることを確認します。「 * 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_1       configured     enabled   normal
2 entries were displayed.
```

c. 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

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
4 entries were displayed.

Command completed. Use the "metrocluster check show -instance"
command or sub-commands in "metrocluster check" directory for
detailed results.
To check if the nodes are ready to do a switchover or switchback
operation, run "metrocluster switchover -simulate" or "metrocluster
switchback -simulate", respectively.
```

d. ヘルス・アラートがないことを確認してください： * system health alert show *

2. 設置前に新しいスイッチを設定します。

   の手順に従います "FC スイッチを設定"。

3. 次の順序で接続を削除して、古いスイッチから接続を切断します。
   a. MetroCluster FCインターフェイスとFCVIインターフェイスを切断します。
   b. ATTO FibreBridgeブリッジを切断します。
   c. MetroCluster ISLを切断します。
4. 古いスイッチの電源をオフにしてケーブルを外し、古いスイッチを新しいスイッチと物理的に交換します。
5. 次の順序でスイッチをケーブル接続します。

の手順に従う必要があります "ファブリック接続 MetroCluster 構成のケーブル接続"。

a. リモートサイトにISLをケーブル接続します。
b. ATTO FibreBridgeブリッジをケーブル接続します。
c. MetroCluster FCインターフェイスとFCVIインターフェイスをケーブル接続します。

6. スイッチの電源をオンにします。
7. を繰り返して、MetroCluster 構成が正常であることを確認します [手順 1.]。
8. 構成内の2つ目のファブリックについて、手順1～7を繰り返します。

ファブリック接続 **MetroCluster** 構成のシェルフを無停止で交換する

ファブリック接続 MetroCluster 構成でシェルフを無停止で交換する方法を確認しておく必要があります。

この手順は、ファブリック接続 MetroCluster 構成でのみ使用します。

シェルフへのアクセスを無効にします

シェルフモジュールを交換する前に、シェルフへのアクセスを無効にする必要があります。

構成の全体的な健全性を確認します。システムが健全でない場合は、問題に対処してから次に進んでください。

手順

1. 両方のクラスタで、関係するシェルフスタック上のディスクを含むすべてのプレックスをオフラインにします。

   「 aggr offline_plex_name_ 」

   次の例は、ONTAPを実行しているコントローラのプレックスをオフラインにするコマンドを示しています。

```
cluster_A_1::> storage aggregate plex offline -aggr aggrA_1_0 -plex
plex0
cluster_A_1::> storage aggregate plex offline -aggr dataA_1_data -plex
plex0
cluster_A_2::> storage aggregate plex offline -aggr aggrA_2_0 -plex
plex0
cluster_A_2::> storage aggregate plex offline -aggr dataA_2_data -plex
plex0
```

2. プレックスがオフラインであることを確認します。

   aggr status --raggr_name_`

   次の例は、 cMode を実行しているコントローラのアグリゲートがオフラインであることを確認するコマ

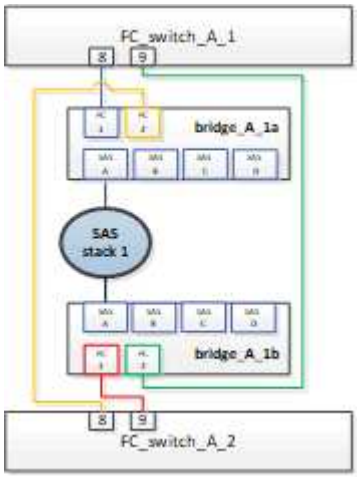
ンドを示しています。

```
Cluster_A_1::> storage aggregate show -aggr aggrA_1_0
Cluster_A_1::> storage aggregate show -aggr dataA_1_data
Cluster_A_2::> storage aggregate show -aggr aggrA_2_0
Cluster_A_2::> storage aggregate show -aggr dataA_2_data
```

3. ターゲットシェルフを接続しているブリッジが SAS スタックを 1 つ接続しているか 2 つ接続しているかに応じて、 SAS ポートまたはスイッチポートを無効にします。

   ◦ ブリッジが SAS スタックを 1 つ接続している場合は、スイッチに対応したコマンドを使用してブリッジの接続先のスイッチポートを無効にします。

   次の例は、ターゲットシェルフを収容する SAS スタックを 1 つ接続するブリッジのペアを示しています。



   各スイッチのスイッチポート 8 と 9 が、ブリッジをネットワークに接続します。

   次の例は、 Brocade スイッチのポート 8 と 9 を無効にします。

```
FC_switch_A_1:admin> portDisable 8
FC_switch_A_1:admin> portDisable 9

FC_switch_A_2:admin> portDisable 8
FC_switch_A_2:admin> portDisable 9
```

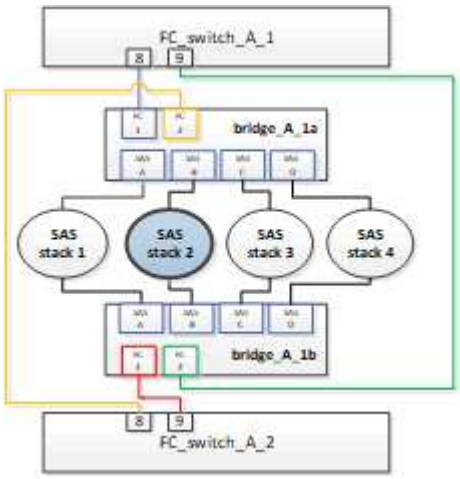
   次の例は、 Cisco スイッチのポート 8 と 9 を無効にします。

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# int fc1/8
FC_switch_A_1(config)# shut
FC_switch_A_1(config)# int fc1/9
FC_switch_A_1(config)# shut
FC_switch_A_1(config)# end

FC_switch_A_2# conf t
FC_switch_A_2(config)# int fc1/8
FC_switch_A_2(config)# shut
FC_switch_A_2(config)# int fc1/9
FC_switch_A_2(config)# shut
FC_switch_A_2(config)# end
```

- ブリッジが 2 つ以上の SAS スタックを接続している場合は、ブリッジをターゲットシェルフに接続している SAS ポートを無効にします。 `+SASportDisable_port number_`

  次の例は、 4 つの SAS スタックを接続するブリッジのペアを示しています。SAS スタック 2 にターゲットシェルフが収容されています。



  SAS ポート B が、ブリッジをターゲットシェルフに接続します。両方のシェルフの SAS ポート B のみを無効にすると、交換用手順の実行中も他の SAS スタックが引き続きデータを提供できます。

  この場合は、ブリッジをターゲットシェルフに接続している SAS ポートを無効にします。

  'SASportDisable_port Number_

  次の例は、ブリッジの SAS ポート B を無効にして、ポート B が無効になっていることを確認します。このコマンドは両方のブリッジで実行する必要があります。

```
Ready. *
SASPortDisable B

SAS Port B has been disabled.
```

4. スイッチポートを無効にしていた場合は、ポートが無効になっていることを確認します。

   'witchshow'

   次の例は、 Brocade スイッチのスイッチポートが無効になっていることを示しています。

```
FC_switch_A_1:admin> switchShow
FC_switch_A_2:admin> switchShow
```

   次の例は、 Cisco スイッチのスイッチポートが無効になっていることを示しています。

```
FC_switch_A_1# show interface fc1/6
FC_switch_A_2# show interface fc1/6
```

5. ディスクが見つからないことが ONTAP に認識されるまで待ちます。
6. 交換するシェルフの電源をオフにします。

シェルフの交換

新しいシェルフとシェルフモジュールを挿入してケーブル接続する前に、すべてのケーブルとシェルフを物理的に取り外す必要があります。

手順

1. すべてのディスクを取り外し、交換するシェルフからすべてのケーブルを外します。
2. シェルフモジュールを取り外します。
3. 新しいシェルフを挿入します。
4. 新しいディスクを新しいシェルフに挿入します。
5. シェルフモジュールを挿入します。
6. シェルフをケーブル接続します（ SAS または電源）。
7. シェルフの電源をオンにします。

アクセスの再有効化と処理の確認

シェルフを交換したら、アクセスを再度有効にして、新しいシェルフが正しく動作していることを確認する必要があります。

手順

1. シェルフの電源が供給され、 IOM モジュールのリンクが存在することを確認します。
2. 次のシナリオに従って、スイッチポートまたは SAS ポートを有効にします。

オプション	ステップ
• 以前にスイッチポートを無効にした場合 *	a. スイッチポートを有効にします。 portEnable_port number_` 次の例は、 Brocade スイッチのスイッチポートを有効にしています。 ``` Switch_A_1:admin> portEnable 6 Switch_A_2:admin> portEnable 6 ``` 次の例は、 Cisco スイッチのスイッチポートを有効にしています。 ``` Switch_A_1# conf t Switch_A_1(config)# int fc1/6 Switch_A_1(config)# no shut Switch_A_1(config)# end Switch_A_2# conf t Switch_A_2(config)# int fc1/6 Switch_A_2(config)# no shut Switch_A_2(config)# end ```
• SAS ポート * を無効にした場合	a. スタックをシェルフの場所に接続している SAS ポートを有効にします。 「 SASportEnable_port number_` 」です 次の例は、ブリッジから SAS ポート A を有効にし、ポートが有効になったことを確認しています。 ``` Ready. * SASPortEnable A SAS Port A has been enabled. ```

3. スイッチポートを無効にしている場合は、ポートが有効でオンラインになっていること、およびすべてのデバイスが正しくログインしていることを確認します。

   'witchshow'

この例は 'switchShow' コマンドを示していますこのコマンドは 'Brocade スイッチがオンラインであることを確認します

```
Switch_A_1:admin> SwitchShow
Switch_A_2:admin> SwitchShow
```

この例は、 Cisco スイッチがオンラインであることを確認するための switchShow コマンドを示しています。

```
Switch_A_1# show interface fc1/6
Switch_A_2# show interface fc1/6
```

数分経過すると、 ONTAP は新しいディスクが挿入されたことを検出し、新しいディスクごとにメッセージを表示します。

4. ONTAP によってディスクが検出されたことを確認します。

「 sysconfig -a 」

5. オフラインになっていたプレックスをオンラインにします。

'aggr online _ *plex_name*'

次の例は、 cMode を実行しているコントローラ上のプレックスをオンラインに戻すコマンドを示しています。

```
Cluster_A_1::> storage aggregate plex online -aggr aggr1 -plex plex2
Cluster_A_1::> storage aggregate plex online -aggr aggr2 -plex plex6
Cluster_A_1::> storage aggregate plex online -aggr aggr3 -plex plex1
```

プレックスが再同期を開始します。

再同期の進行状況は 'aggr status --raggr_name_` コマンドを使用して監視できます

MetroCluster FC 構成へのストレージのホットアド

SAS 光ケーブルを使用した直接接続型 MetroCluster FC 構成での SAS ディスクシェルフのホットアド

SAS 光ケーブルを使用して、直接接続型 MetroCluster FC 構成の SAS ディスクシェルフの既存のスタックに SAS ディスクシェルフをホットアドすることも、 SAS HBA またはコントローラ上のオンボード SAS ポートに新しいスタックとしてホットアドすることもできます。

- これはシステムの停止を伴わない手順であり、完了までに約 2 時間かかります。

- 管理パスワードと FTP サーバまたは SCP サーバへのアクセスが必要です。

このタスクでは、ストレージを SAS ケーブルでストレージコントローラに直接接続する MetroCluster 環境 FC 構成を行います。FC-to-SAS ブリッジまたは FC スイッチファブリックを使用する MetroCluster FC 構成には該当しません。

手順

1. 使用しているディスクシェルフモデルの _ インストールガイド _ に記載されている SAS ディスクシェルフのホットアドの手順に従って、次のタスクを実行してディスクシェルフをホットアドします。
   a. ホットアド用のディスクシェルフを設置します。
   b. 電源装置の電源をオンにして、ホットアド用のシェルフ ID を設定します。
   c. ホットアドしたディスクシェルフをケーブル接続します。
   d. SAS 接続を確認します。

ブリッジ接続型 **MetroCluster FC** 構成への **SAS** ストレージのホットアド

既存の**FibreBridge 7600N / 7500N**ブリッジペアへの**SAS**ディスクシェルフのスタックのホットアド

使用可能なポートがある既存のFibreBridge 7600N / 7500Nブリッジペアに、SASディスクシェルフのスタックをホットアドできます。

作業を開始する前に

- 最新のディスクファームウェアとディスクシェルフファームウェアをダウンロードしておく必要があります。
- MetroCluster 構成内（既存のシェルフ）のすべてのディスクシェルフで同じファームウェアバージョンを実行する必要があります。1 つ以上のディスクまたはシェルフが最新のファームウェアバージョンを実行していない場合は、新しいディスクまたはシェルフを接続する前にファームウェアを更新します。

  "ネットアップのダウンロード：ディスクドライブファームウェア"

  "ネットアップのダウンロード：ディスクシェルフファームウェア"

- FibreBridge 7600N / 7500Nブリッジが接続され、使用可能なSASポートがある必要があります。

このタスクについて

この手順は、推奨されるブリッジ管理インターフェイスである ATTO ExpressNAV GUI と ATTO QuickNAV ユーティリティを使用していることを前提としています。

ATTO ExpressNAV GUI は、ブリッジの設定および管理、ブリッジファームウェアの更新に使用できます。ATTO QuickNAV ユーティリティは、ブリッジのイーサネット管理 1 ポートの設定に使用できます。

必要に応じて、他の管理インターフェイスを使用できます。オプションには、シリアルポートまたは Telnet を使用したブリッジの設定と管理、イーサネット管理 1 ポートの設定、および FTP を使用したブリッジファームウェアの更新があります。これらの管理インターフェイスのいずれかを選択した場合は、に記載された該当する要件を満たす必要があります "その他のブリッジ管理インターフェイス"。

SAS ケーブルを間違ったポートに挿入した場合は、ケーブルを SAS ポートから取り外すときに、 120 秒以上待機してから別の SAS ポートに接続する必要があります。そうしないと、ケーブルが別のポートに移されたことがシステムで認識されません。

手順

1. 自身の適切な接地対策を行います
2. いずれかのコントローラのコンソールで、システム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

   Auto Assign 列には、ディスクの自動割り当てが有効になっているかどうかが示されます。

```
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.
```

3. ペアの各ブリッジで、新しいスタックに接続する SAS ポートを有効にします。

   'SASortEnable_portlet-letter_

   両方のブリッジで同じ SAS ポート（ B 、 C 、または D ）を使用する必要があります。

4. 設定を保存し、各ブリッジをリブートします。

   SaveConfiguration Restart を実行します

5. ディスクシェルフをブリッジにケーブル接続します。

   a. 各スタックのディスクシェルフをデイジーチェーン接続します。

      ディスクシェルフのデイジーチェーン接続の詳細については、使用しているディスクシェルフモデルの Installation and Service Guide を参照してください。

   b. ディスクシェルフの各スタックで、最初のシェルフの IOM A を FibreBridge A の SAS ポート A にケーブル接続し、最後のシェルフの IOM B を FibreBridge B の SAS ポート A にケーブル接続します

      "ファブリック接続 MetroCluster のインストールと設定"

      "ストレッチ MetroCluster のインストールと設定"

      各ブリッジには、ディスクシェルフのスタックへのパスが 1 つあります。ブリッジ A は最初のシェルフ経由でスタックの A 側に接続し、ブリッジ B は最後のシェルフ経由でスタックの B 側に接続します。

      ブリッジの SAS ポート B は無効になっています。

6. 各ブリッジが、ブリッジの接続先のすべてのディスクドライブとディスクシェルフを検出できることを確認します。

使用する手段	作業
ATTO ExpressNAV の GUI	a. サポートされている Web ブラウザで、ブリッジの IP アドレスをブラウザのアドレスバーに入力します。 ATTO FibreBridge のホームページに移動し、リンクが表示されます。 b. リンクをクリックし、ブリッジを設定するときに指定したユーザ名とパスワードを入力します。 ATTO FibreBridge のステータスページが開き、左側にメニューが表示されます。 c. メニューの「 * 詳細設定 * 」をクリックします。 d. 接続されているデバイスを表示します。 「 astargets 」 e. [Submit （送信）] をクリックします。
シリアルポート接続	接続されているデバイスを表示します。 「 astargets 」

出力には、ブリッジが接続されているデバイス（ディスクおよびディスクシェルフ）が表示されます。出力行には行番号が振られているため、デバイスの台数を簡単に把握できます。

出力の先頭に「 response truncated 」というテキストが表示される場合は、 Telnet を使用してブリッジに接続し、「 sastargets 」コマンドを使用してすべての出力を表示できます。

次の出力は、 10 本のディスクが接続されていることを示します。

```
Tgt VendorID ProductID         Type        SerialNumber
  0 NETAPP   X410_S15K6288A15 DISK        3QP1CLE300009940UHJV
  1 NETAPP   X410_S15K6288A15 DISK        3QP1ELF600009940V1BV
  2 NETAPP   X410_S15K6288A15 DISK        3QP1G3EW00009940U2M0
  3 NETAPP   X410_S15K6288A15 DISK        3QP1EWMP00009940U1X5
  4 NETAPP   X410_S15K6288A15 DISK        3QP1FZLE00009940G8YU
  5 NETAPP   X410_S15K6288A15 DISK        3QP1FZLF00009940TZKZ
  6 NETAPP   X410_S15K6288A15 DISK        3QP1CEB400009939MGXL
  7 NETAPP   X410_S15K6288A15 DISK        3QP1G7A900009939FNTT
  8 NETAPP   X410_S15K6288A15 DISK        3QP1FY0T00009940G8PA
  9 NETAPP   X410_S15K6288A15 DISK        3QP1FXW600009940VERQ
```

7. コマンド出力で、スタック内の該当するすべてのディスクおよびディスクシェルフにブリッジが接続されていることを確認します。

出力結果	作業
正解です	残りの各ブリッジについて、同じ手順を繰り返します。
不正解です	a. SAS ケーブルに緩みがないか確認するか、手順を繰り返してディスクシェルフをブリッジに接続し、 SAS ケーブル接続を修正します。 b. 残りの各ブリッジについて、同じ手順を繰り返します。

8. システムコンソールからディスクドライブファームウェアを最新バージョンに更新します。

   「 disk_fw_update 」

   このコマンドは両方のコントローラで実行する必要があります。

   "ネットアップのダウンロード：ディスクドライブファームウェア"

9. ダウンロードしたファームウェアの手順に従って、ディスクシェルフファームウェアを最新バージョンに更新します。

   手順のコマンドは、どちらのコントローラのシステムコンソールでも実行できます。

   "ネットアップのダウンロード：ディスクシェルフファームウェア"

10. システムでディスクの自動割り当てが有効になっていない場合は、ディスクドライブの所有権を割り当てます。

    "ディスクおよびアグリゲートの管理"

    ディスクシェルフの 1 つのスタックの所有権を複数のコントローラに分割する場合は、ディスク所有権を割り当てる前にディスクの自動割り当てを無効にする必要があります（クラスタ内の両方のノードから「 storage disk option modify -autoassign off * 」）。 そうしないと、いずれかのディスクドライブを割り当てたときに、残りのディスクドライブが同じコントローラおよびプールに自動的に割り当てられる可能性があります。

    ディスクドライブファームウェアとディスクシェルフファームウェアが更新され、このタスクの検証手順が完了するまで、アグリゲートまたはボリュームにディスクドライブを追加しないでください。

11. ONTAP で MetroCluster 構成の動作を確認します。

    a. システムがマルチパスかどうかを確認します。

       'node run -node _node-name_sysconfig -a

    b. ヘルスアラートがないかどうかを両方のクラスタで確認します。

       「 system health alert show 」というメッセージが表示されます

c. MetroCluster 構成と運用モードが正常な状態であることを確認します。

「 MetroCluster show 」

d. MetroCluster チェックを実行します。

「 MetroCluster check run 」のようになります

e. MetroCluster チェックの結果を表示します。

MetroCluster チェックショー

f. 新しいスタックを追加したあとに、ブリッジに健全性アラートがないかどうかを確認します。

「 storage bridge show 」

g. Config Advisor を実行します。

"ネットアップのダウンロード： Config Advisor"

h. Config Advisor の実行後、ツールの出力を確認し、推奨される方法で検出された問題に対処します。

12. 必要に応じて、パートナーサイトに対してこの手順を繰り返します。

MetroCluster システムへの **SAS** ディスクシェルフとブリッジのスタックのホットアド

MetroCluster システムにブリッジを含むスタック全体をホットアド（無停止で追加）できます。FC スイッチに使用可能なポートが必要です。変更を反映するには、スイッチゾーニングを更新する必要があります。

このタスクについて

- この手順を使用して、FibreBridge 7600N / 7500Nブリッジを使用してスタックを追加できます。
- この手順は、推奨されるブリッジ管理インターフェイスである ATTO ExpressNAV GUI と ATTO QuickNAV ユーティリティを使用していることを前提としています。
  - ATTO ExpressNAV GUI は、ブリッジの設定および管理、ブリッジファームウェアの更新に使用します。ATTO QuickNAV ユーティリティは、ブリッジのイーサネット管理 1 ポートの設定に使用します。
  - 必要に応じて、他の管理インターフェイスを使用できます。オプションには、シリアルポートまたは Telnet を使用したブリッジの設定と管理、イーサネット管理 1 ポートの設定、および FTP を使用したブリッジファームウェアの更新があります。これらのいずれかの管理インターフェイスを使用する場合は、の該当する要件をシステムが満たしている必要があります "その他のブリッジ管理インターフェイス"

SAS ディスクシェルフとブリッジのスタックのホットアドの準備

SAS ディスクシェルフとブリッジのペアのスタックのホットアドの準備には、ドキュメントおよびディスクドライブとディスクシェルフのファームウェアのダウンロードが含まれます。

作業を開始する前に

- サポートされている構成である必要があり、サポートされているバージョンの ONTAP が実行されている必要があります。

"NetApp Interoperability Matrix Tool で確認できます"

- システム内のすべてのディスクドライブとディスクシェルフで最新のファームウェアバージョンが実行されている必要があります。

  シェルフを追加する前に、 MetroCluster 構成全体でディスクとシェルフのファームウェアを更新しなければならない場合があります。

  "アップグレード、リバート、ダウングレード"

- 各 FC スイッチで、 1 つの FC ポートを 1 つのブリッジに接続できる必要があります。

  FC スイッチの互換性に応じて FC スイッチのアップグレードが必要になる可能性があります。

- ブリッジの設定に使用するコンピュータでは、 ATTO ExpressNAV GUI （ Internet Explorer 8 または 9 、 Mozilla Firefox 3 ）を使用するために、 ATTO でサポートされている Web ブラウザを実行している必要があります。

  ATTO Product Release Notes に、サポートされている Web ブラウザの最新のリストが掲載されています。このドキュメントには、の手順内の情報を使用してアクセスできます。

手順

1. ネットアップサポートサイトから次のドキュメントをダウンロードまたは表示します。
   - "NetApp Interoperability Matrix Tool で確認できます"
   - 使用しているディスクシェルフモデルの Installation and Service Guide を参照してください。
2. ATTO の Web サイトおよびネットアップの Web サイトから必要なデータをダウンロードします。
   a. ATTO FibreBridge 概要のページに移動します。
   b. ATTO FibreBridge 概要のページのリンクを使用して、 ATTO の Web サイトにアクセスし、次の項目をダウンロードします。
      - 使用しているブリッジモデルに対応した ATTO FibreBridge Installation and Operation Manual
      - ATTO QuickNAV ユーティリティ（セットアップに使用するコンピュータへ）
   c. ATTO FibreBridge 概要のページの末尾にある「 * Continue * 」をクリックして、 ATTO FibreBridge ファームウェアのダウンロードページに移動し、次の手順を実行します。
      - ダウンロードページの指示に従って、ブリッジファームウェアファイルをダウンロードします。

        この手順では、リンク先に記載されている手順のダウンロード部分のみを実行します。各ブリッジでのファームウェアの更新は、で指示されたときにあとから実行します "シェルフのスタックのホットアド" セクション。

      - ATTO FibreBridge ファームウェアのダウンロードページとリリースノートのコピーを作成し、あとで参照できます。
3. 最新のディスクファームウェアとディスクシェルフファームウェアをダウンロードし、あとで参照できるよう、手順のインストールに関する部分をコピーします。

   MetroCluster 構成内のすべてのディスクシェルフ（新しいシェルフと既存のシェルフの両方）で同じファ

ームウェアバージョンを実行する必要があります。

> この手順では、リンク先に記載されている手順のダウンロード部分のみを実行し、インストール手順をコピーします。各ディスクおよびディスクシェルフでのファームウェアの更新は、で指示されたときにあとから実行します "シェルフのスタックのホットアド" セクション。

a. ディスクファームウェアをダウンロードし、あとで参照できるよう、ディスクファームウェアの説明書をコピーします。

   "ネットアップのダウンロード：ディスクドライブファームウェア"

b. ディスクシェルフファームウェアをダウンロードし、あとで参照できるよう、ディスクシェルフファームウェアの説明書をコピーします。

   "ネットアップのダウンロード：ディスクシェルフファームウェア"

4. 推奨されるブリッジ管理インターフェイスを使用するために必要なハードウェアおよび情報を収集する - ATTO ExpressNAV GUI および ATTO QuickNAV ユーティリティ

   a. 標準のイーサネットケーブルを用意して、ブリッジのイーサネット管理 1 ポートからネットワークに接続します。

   b. ブリッジへのアクセスに使用するデフォルト以外のユーザ名とパスワードを決定します。

      デフォルトのユーザ名とパスワードを変更することを推奨します。

   c. 各ブリッジのイーサネット管理 1 ポートの IP アドレス、サブネットマスク、およびゲートウェイ情報を取得します。

   d. セットアップに使用するコンピュータで VPN クライアントを無効にします。

      アクティブな VPN クライアント原因がブリッジの QuickNAV スキャンに失敗しました。

5. ブリッジごとに 4 本のネジを用意して、ブリッジの L 字型ブラケットをラックの前面にフラッシュマウントします。

   ブリッジ「 L 」ブラケットの開口部は、 19 インチ（ 482.6 mm ）ラックのラック標準 ETA-310-X に準拠しています。

6. 必要に応じて、構成に追加する新しいブリッジに合わせて FC スイッチゾーニングを更新します。

   ネットアップが提供するリファレンス構成ファイルを使用している場合は、すべてのポート用のゾーンが作成されているため、ゾーニングを更新する必要はありません。ブリッジの FC ポートに接続するスイッチポートごとにストレージゾーンが必要です。

SAS ディスクシェルフとブリッジのスタックのホットアド

SAS ディスクシェルフとブリッジのスタックをホットアドして、ブリッジの容量を増やすことができます。

SAS ディスクシェルフとブリッジのスタックをホットアドするためのすべての要件をシステムが満たしている必要があります。

"SAS ディスクシェルフとブリッジのスタックのホットアドの準備"

- 相互運用性の要件をすべて満たしている場合、 SAS ディスクシェルフとブリッジのスタックのホットアドは無停止の手順となります。

  "NetApp Interoperability Matrix Tool で確認できます"

  "Interoperability Matrix Tool を使用した MetroCluster 情報の検索"

- ブリッジを使用する MetroCluster システムでサポートされている構成はマルチパス HA のみです。

  両方のコントローラモジュールが、各スタックのディスクシェルフにブリッジ経由でアクセスできる必要があります。

- 各サイトで同数のディスクシェルフをホットアドする必要があります。
- IP 管理ではなくブリッジのインバンド管理を使用する場合は、該当する手順に記載されているように、イーサネットポートと IP を設定する手順を省略できます。

ONTAP 9.8 以降では 'storage bridge コマンドは 'system bridge コマンドに置き換えられました次の手順は「 storage bridge 」コマンドを示していますが、 ONTAP 9.8 以降を実行している場合は「 system bridge 」コマンドが優先されます。

SAS ケーブルを間違ったポートに挿入した場合は、ケーブルを SAS ポートから取り外すときに、 120 秒以上待機してから別の SAS ポートに接続する必要があります。そうしないと、ケーブルが別のポートに移されたことがシステムで認識されません。

手順

1. 自身の適切な接地対策を行います
2. いずれかのコントローラモジュールのコンソールで、システムで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確認します。

   「 storage disk option show 」をクリックします

   Auto Assign 列には、ディスクの自動割り当てが有効になっているかどうかが示されます。

```
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.
```

3. 新しいスタックのスイッチポートを無効にします。
4. インバンド管理用に設定する場合は、 FibreBridge RS-232 シリアルポートから PC のシリアル（ COM ）ポートにケーブルを接続します。

   シリアル接続は初期設定と ONTAP によるインバンド管理に使用され、 FC ポートを使用してブリッジの監視と管理を行うことができます。

5. IP 管理用に設定する場合は、使用しているブリッジモデルの ATTO FibreBridge Installation and Operation Manual _ のセクション 2.0 の手順に従って、各ブリッジのイーサネット管理 1 ポートを設定します。

ONTAP 9.5 以降を実行しているシステムでは、インバンド管理を使用してイーサネットポートではなく FC ポート経由でブリッジにアクセスできます。ONTAP 9.8 以降では、インバンド管理のみがサポートされ、 SNMP 管理は廃止されています。

QuickNAV を実行してイーサネット管理ポートを設定すると、イーサネットケーブルで接続されているイーサネット管理ポートのみが設定されます。たとえば、イーサネット管理 2 ポートも設定する場合は、イーサネットケーブルをポート 2 に接続して QuickNAV を実行する必要があります。

6. ブリッジを設定します。

   古いブリッジから設定情報を取得した場合は、その情報を使用して新しいブリッジを設定します。

   指定するユーザ名とパスワードは必ずメモしてください。

   使用しているブリッジモデルに対応する _ATTO FibreBridge Installation and Operation Manual _ に、使用可能なコマンドおよびその使用方法に関する最新情報が記載されています。

   > ATTO FibreBridge 7600N または 7500N では時刻同期は設定しないでください。ATTO FibreBridge 7600N または 7500N の時刻は、 ONTAP でブリッジが検出されたあとにクラスタ時間に設定されます。また、 1 日に 1 回定期的に同期されます。使用されるタイムゾーンは GMT で、変更することはできません。

   a. IP 管理用に設定する場合は、ブリッジの IP 設定を行います。

      Quicknav ユーティリティなしで IP アドレスを設定するには、 FibreBridge に対するシリアル接続が必要です。

      CLI を使用する場合は、次のコマンドを実行する必要があります。

      'set ipaddress mp1_ip-address_'

      'set ipsubnetmask mp1_subnet-mask_

      'set ipgateway mp1x.x'

      'set ipdhcp mp1 disabled

      「 setethernetspeed mp1 1000」

   b. ブリッジ名を設定します。

      ブリッジ名は、 MetroCluster 構成内でそれぞれ一意である必要があります。

      各サイトの 1 つのスタックグループのブリッジ名の例：

      - bridge_A_1a
      - bridge_A_1b
      - bridge_B_1a
      - bridge_B_1b CLI を使用する場合は、次のコマンドを実行する必要があります。

        「 set bridgename _bridgename _ 」を入力します

c. ONTAP 9.4 以前を実行している場合は、ブリッジで SNMP を有効にします。 +'set snmp enabled'

ONTAP 9.5 以降を実行しているシステムでは、インバンド管理を使用してイーサネットポートではなく FC ポート経由でブリッジにアクセスできます。ONTAP 9.8 以降では、インバンド管理のみがサポートされ、 SNMP 管理は廃止されています。

7. ブリッジの FC ポートを設定します。

a. ブリッジ FC ポートのデータ速度を設定します。

サポートされる FC データ速度は、モデルブリッジによって異なります。

- FibreBridge 7600Nブリッジは、最大32、16、または8Gbpsをサポートします。
- FibreBridge 7500Nブリッジは、最大16、8、または4Gbpsをサポートします。



選択できる FCDataRate の速度は、ブリッジポートを接続するブリッジとスイッチの両方でサポートされる最大速度以下です。ケーブルでの接続距離が SFP およびその他のハードウェアの制限を超えないようにしてください。

CLI を使用する場合は、次のコマンドを実行する必要があります。

'set FCDataRate_port-number port-speed_

b. FibreBridge 7500Nブリッジを設定する場合は、ポートで使用する接続モードを「ptp」に設定します。



FibreBridge 7600N ブリッジを設定する場合、 FCConnMode の設定は不要です。

CLI を使用する場合は、次のコマンドを実行する必要があります。

'et FCConnMode_port-number_ptc'

a. FibreBridge 7600N / 7500N ブリッジを設定する場合は、 FC2 ポートを設定または無効にする必要があります。

- 2 番目のポートを使用する場合は、 FC2 ポートについて同じ手順を繰り返す必要があります。
- 2 番目のポートを使用しない場合は、ポート +`FCPortDisable_port-number_` を無効にする必要があります

b. FibreBridge 7600N / 7500N ブリッジを設定する場合は、未使用の SAS ポートを無効にします：
+`SASortDisable_SAS-port_`



SAS ポート A~D はデフォルトで有効になります。使用していない SAS ポートを無効にする必要があります。SAS ポート A のみを使用している場合は、 SAS ポート B 、 C 、および D を無効にする必要があります。

8. ブリッジへのアクセスを保護し、ブリッジの設定を保存します。

a. コントローラのプロンプトで、ブリッジのステータスを確認します。

「 storage bridge show 」

出力には、保護されていないブリッジが表示されます。

b. セキュリティ保護されていないブリッジのポートのステータスを確認します :`+info`

出力には、イーサネットポート MP1 と MP2 のステータスが表示されます。

c. Ethernet ポート MP1 が有効になっている場合は ' 次のコマンドを実行します `+set EthernetPort mp1 disabled`

> イーサネットポート MP2 も有効になっている場合は、ポート MP2 について前の手順を繰り返します。

d. ブリッジの設定を保存します。

次のコマンドを実行する必要があります。

'aveConfiguration'

「 FirmwareRestart 」と入力します

ブリッジを再起動するように求められます。

9. 各ブリッジの FibreBridge ファームウェアを更新します。

新しいブリッジのタイプがパートナーブリッジと同じ場合は、パートナーブリッジと同じファームウェアにアップグレードします。新しいブリッジのタイプがパートナーブリッジと異なる場合は、ブリッジと ONTAP のバージョンでサポートされている最新のファームウェアにアップグレードします。MetroCluster Maintenance _ の「 Updating firmware on a FibreBridge bridge 」セクションを参照してください。

10. [step10-cable-shelves -橋梁] ディスクシェルフをブリッジにケーブル接続します。

a. 各スタックのディスクシェルフをデイジーチェーン接続します。

ディスクシェルフのデイジーチェーン接続の詳細については、使用しているディスクシェルフモデルの Installation Guide を参照してください。

b. ディスクシェルフの各スタックで、最初のシェルフの IOM A を FibreBridge A の SAS ポート A にケーブル接続し、最後のシェルフの IOM B を FibreBridge B の SAS ポート A にケーブル接続します

"ファブリック接続 MetroCluster のインストールと設定"

"ストレッチ MetroCluster のインストールと設定"

各ブリッジには、ディスクシェルフのスタックへのパスが 1 つあります。ブリッジ A は最初のシェルフ経由でスタックの A 側に接続し、ブリッジ B は最後のシェルフ経由でスタックの B 側に接続します。

> ブリッジの SAS ポート B は無効になっています。

11. [[step11-verify-backup -bridge-detect]] ブリッジが接続されているすべてのディスクドライブとディスクシェルフを各ブリッジで検出できることを確認します。

使用する手段	作業
ATTO ExpressNAV の GUI	a. サポートされている Web ブラウザで、ブリッジの IP アドレスをブラウザのアドレスバーに入力します。 ATTO FibreBridge のホームページに移動し、リンクが表示されます。 b. リンクをクリックし、ブリッジを設定するときに指定したユーザ名とパスワードを入力します。 ATTO FibreBridge のステータスページが開き、左側にメニューが表示されます。 c. メニューの「 * 詳細設定 * 」をクリックします。 d. 接続されているデバイスを表示します :+'sastargets' e. [Submit （送信）] をクリックします。
シリアルポート接続	接続されているデバイスを表示します。 「 astargets 」

出力には、ブリッジが接続されているデバイス（ディスクおよびディスクシェルフ）が表示されます。出力行には行番号が振られているため、デバイスの台数を簡単に把握できます。

出力の先頭に response truncated というテキストが表示される場合は、 Telnet を使用してブリッジに接続し、 'sastargets' コマンドを使用してすべての出力を確認できます。

次の出力は、 10 本のディスクが接続されていることを示します。

```
Tgt VendorID ProductID         Type        SerialNumber
  0 NETAPP   X410_S15K6288A15 DISK        3QP1CLE300009940UHJV
  1 NETAPP   X410_S15K6288A15 DISK        3QP1ELF600009940V1BV
  2 NETAPP   X410_S15K6288A15 DISK        3QP1G3EW00009940U2M0
  3 NETAPP   X410_S15K6288A15 DISK        3QP1EWMP00009940U1X5
  4 NETAPP   X410_S15K6288A15 DISK        3QP1FZLE00009940G8YU
  5 NETAPP   X410_S15K6288A15 DISK        3QP1FZLF00009940TZKZ
  6 NETAPP   X410_S15K6288A15 DISK        3QP1CEB400009939MGXL
  7 NETAPP   X410_S15K6288A15 DISK        3QP1G7A900009939FNTT
  8 NETAPP   X410_S15K6288A15 DISK        3QP1FY0T00009940G8PA
  9 NETAPP   X410_S15K6288A15 DISK        3QP1FXW600009940VERQ
```

12. コマンド出力で、スタック内の該当するすべてのディスクおよびディスクシェルフにブリッジが接続されていることを確認します。

出力結果	作業

正解です	繰り返します 手順 11 残りの各ブリッジ。
不正解です	a. SAS ケーブルに緩みがないか確認するか、 SAS ケーブル接続をやり直します 手順 10。 b. 繰り返します 手順 11。

13. ファブリック接続 MetroCluster 構成を設定する場合は、使用している構成、スイッチモデル、および FC-to-SAS ブリッジモデルに対応した表に記載されているケーブルを使用して、各ブリッジをローカルの FC スイッチにケーブル接続します。

次の表に示すように、 Brocade スイッチと Cisco スイッチでは使用するポート番号が異なります。

- Brocade スイッチでは ' 最初のポートに 0 という番号が付けられます
- シスコ製スイッチでは、最初のポートには「 1 」という番号が付けられています。

両方の FC ポート（ FC1 または FC2 ）を使用する FibreBridge 7500N または 7600N を使用する構成												
DR グループ 1												
			Brocade 6505		Brocade 6510 、 Brocade DCX 8510-8		Brocade 6520		Brocade G620 、 Brocade G620 -1 、 Brocade G630 、 Brocade G630-1		Brocade G720	
コンポーネント		ポート	スイッチ 1	スイッチ 2	スイッチ 1	スイッチ 2	スイッチ 1	スイッチ 2	スイッチ 1	スイッチ 2	スイッチ 1	スイッチ 2
スタック 1	bridge_x_1a	fc1	8.		8.		8.		8.		10.	
FC2	-	8.	-	8.	-	8.	-	8.	-	10.	bridge_x_1B	fc1
9.	-	9.	-	9.	-	9.	-	11.	-	FC2	-	9.
-	9.	-	9.	-	9.	-	11.	スタック 2	bridge_x_2a	fc1	10.	-
10.	-	10.	-	10.	-	14	-	FC2	-	10.	-	10.
-	10.	-	10.	-	14	bridge_x_2B	fc1	11.	-	11.	-	11.
-	11.	-	17	-	FC2	-	11.	-	11.	-	11.	-

11.	-	17	スタック 3	bridge_x_3a	fc1	12.	-	12.	-	12.	-	12.
-	18	-	FC2	-	12.	-	12.	-	12.	-	12.	-
18	bridge_x_3B	fc1	13	-	13	-	13	-	13	-	19	-
FC2	-	13	-	13	-	13	-	13	-	19	スタック y	bridge_x_ya
fc1	14	-	14	-	14	-	14	-	20	-	FC2	-
14	-	14	-	14	-	14	-	20	bridge_x_YB	fc1	15	-
15	-	15	-	15	-	21	-	FC2		15		15

両方の FC ポート（ FC1 または FC2 ）を使用する FibreBridge 7500N または 7600N を使用する構成											
DR グループ 2											
			Brocade G620 、 Brocade G620 -1 、 Brocade G630 、 Brocade G630-1		Brocade 6510 、 Brocade DCX 8510-8		Brocade 6520		Brocade G720	
コンポーネント		ポート	スイッチ 1	スイッチ 2	スイッチ 1	スイッチ 2	スイッチ 1	スイッチ 2	スイッチ 1	スイッチ 2
スタック 1	bridge_x_51A	fc1	26	-	32	-	56	-	32	-
FC2	-	26	-	32	-	56	-	32	bridge_x_51b	fc1
27	-	33	-	57	-	33	-	FC2	-	27
-	33	-	57	-	33	スタック 2	bridge_x_52A	fc1	30	-
34	-	58	-	34	-	FC2	-	30	-	34
-	58	-	34	bridge_x_52b	fc1	31.	-	35	-	59

-	35	-	FC2	-	31.	-	35	-	59	-
35	スタック 3	bridge_x_53a	fc1	32	-	36	-	60	-	36
-	FC2	-	32	-	36	-	60	-	36	bridge_x_53B
fc1	33	-	37	-	61	-	37	-	FC2	-
33	-	37	-	61	-	37	スタック y	bridge_x_5ya	fc1	34
-	38	-	62	-	38	-	FC2	-	34	-
38	-	62	-	38	bridge_x_5yb	fc1	35	-	39	-
63	-	39	-	FC2	-	35	-	39	-	63

1つのFCポート（FC1またはFC2）のみを使用するFibreBridge 7500N / 7600Nを使用する構成											
DR グループ 1											
		Brocade 6505		Brocade 6510、Brocade DCX 8510-8		Brocade 6520		Brocade G620、Brocade G620 -1、Brocade G630、Brocade G630-1		Brocade G720	
コンポーネント	ポート	スイッチ 1	スイッチ 2	スイッチ 1	スイッチ 2	スイッチ 1	スイッチ 2	スイッチ 1	スイッチ 2	スイッチ 1	スイッチ 2
スタック 1	bridge_x_1a	8.		8.		8.		8.		10.	
bridge_x_1b	-	8.	-	8.	-	8.	-	8.	-	10.	スタック 2
bridge_x_2a	9.	-	9.	-	9.	-	9.	-	11.	-	bridge_x_2b
-	9.	-	9.	-	9.	-	9.	-	11.	スタック 3	bridge_x_3a

10.	-	10.	-	10.	-	10.	-	14	-	bridge_x_4b	-
10.	-	10.	-	10.	-	10.	-	14	スタック y	bridge_x_ya	11.
-	11.	-	11.	-	11.	-	15	-	bridge_x_YB	-	11.

1つのFCポート（FC1またはFC2）のみを使用するFibreBridge 7500N / 7600Nを使用する構成									
DR グループ 2									
		Brocade G720		Brocade G620 、 Brocade G620 -1 、 Brocade G630 、 Brocade G630-1		Brocade 6510 、 Brocade DCX 8510-8		Brocade 6520	
スタック 1	bridge_x_51A	32	-	26	-	32	-	56	-
bridge_x_51b	-	32	-	26	-	32	-	56	スタック 2
bridge_x_52A	33	-	27	-	33	-	57	-	bridge_x_52b
-	33	-	27	-	33	-	57	スタック 3	bridge_x_53a
34	-	30	-	34	-	58	-	bridge_x_54b	-
34	-	30	-	34	-	58	スタック y	bridge_x_ya	35
-	31.	-	35	-	59	-	bridge_x_YB	-	35

14. ブリッジ接続型 MetroCluster システムを設定する場合は、各ブリッジをコントローラモジュールにケーブル接続します。
    a. ブリッジの FC ポート 1 を、 cluster_A のコントローラモジュールの 16Gb または 8Gb の FC ポートにケーブル接続します
    b. ブリッジの FC ポート 2 を、 cluster_A のコントローラモジュールの同じ速度の FC ポートにケーブル接続します
    c. 他のブリッジでも上記の手順を繰り返し、すべてのブリッジをケーブル接続します。
15. システムコンソールからディスクドライブファームウェアを最新バージョンに更新します。

「 disk_fw_update 」

このコマンドは両方のコントローラモジュールで実行する必要があります。

"ネットアップのダウンロード：ディスクドライブファームウェア"

16. ダウンロードしたファームウェアの手順に従って、ディスクシェルフファームウェアを最新バージョンに更新します。

    手順のコマンドは、どちらのコントローラモジュールのシステムコンソールからも実行できます。

    "ネットアップのダウンロード：ディスクシェルフファームウェア"

17. システムでディスクの自動割り当てが有効になっていない場合は、ディスクドライブの所有権を割り当てます。

    "ディスクおよびアグリゲートの管理"

    ディスクシェルフの 1 つのスタックの所有権を複数のコントローラモジュールに分割する場合は、ディスク所有権を割り当てる前に、クラスタ内の両方のノードでディスクの自動割り当てを無効にする必要があります（「 storage disk option modify -autoassign off * 」）。 そうしないと、 1 本のディスクドライブを割り当てたときに、残りのディスクドライブが同じコントローラモジュールおよびプールに自動的に割り当てられる可能性があります。

    ディスクドライブファームウェアとディスクシェルフファームウェアが更新され、このタスクの検証手順が完了するまで、アグリゲートまたはボリュームにディスクドライブを追加しないでください。

18. 新しいスタックのスイッチポートを有効にします。
19. ONTAP で MetroCluster 構成の動作を確認します。
    a. システムがマルチパスであるかどうかを確認します :+`node run -node -node_name sysconfig -a`
    b. 両方のクラスタにヘルス・アラートがないかどうかを確認します +`system health alert show`
    c. MetroCluster 構成と動作モードが正常であることを確認します。 + MetroCluster show `
    d. MetroCluster チェックを実行します + MetroCluster チェックを実行します
    e. MetroCluster チェックの結果を表示します :+`MetroCluster check show`
    f. スイッチにヘルス・アラートがあるかどうかを確認します（ある場合）： +`storage switch show`
    g. Config Advisor を実行します。

       "ネットアップのダウンロード： Config Advisor"

    h. Config Advisor の実行後、ツールの出力を確認し、推奨される方法で検出された問題に対処します。
20. 必要に応じて、パートナーサイトに対してこの手順を繰り返します。

関連情報

"FC-to-SAS ブリッジのインバンド管理"

SAS ディスクシェルフのスタックに **SAS** ディスクシェルフをホットアドします

パフォーマンスを低下させることなくストレージを拡張するには、ディスクシェルフをホットアドします。

手順**1**：**SAS**ディスクシェルフをホットアドする準備

SASディスクシェルフのホットアドを準備するには、ディスクドライブおよびディスクシェルフファームウェアとともにドキュメントをダウンロードする必要があります。

作業を開始する前に

- システムがサポートされている構成であり、サポートされているバージョンのONTAPを実行していることを確認します。
- システムのすべてのディスクドライブとディスクシェルフが最新のファームウェアバージョンを実行していることを確認します。

  シェルフを追加する前に、MetroCluster構成全体でディスクとシェルフのファームウェアを更新することができます。

  "アップグレード、リバート、ダウングレード"

手順

1. ネットアップサポートサイトから次のドキュメントをダウンロードまたは表示します。
   - "Interoperability Matrix Tool"
   - 使用しているディスクシェルフモデルの Installation Guide
2. ホットアドするディスクシェルフがサポートされていることを確認します。

   "Interoperability Matrix Tool"

3. 最新のディスクファームウェアとディスクシェルフファームウェアをダウンロードします。

   この手順では、手順のダウンロード部分のみを実行します。ディスクシェルフを設置するには、の手順に従う必要がありディスクシェルフのホットアドます。

   a. ディスクファームウェアをダウンロードし、あとで参照できるよう、ディスクファームウェアの説明書をコピーします。

      "ネットアップのダウンロード：ディスクドライブファームウェア"

   b. ディスクシェルフファームウェアをダウンロードし、あとで参照できるよう、ディスクシェルフファームウェアの説明書をコピーします。

      "ネットアップのダウンロード：ディスクシェルフファームウェア"

手順2：ディスクシェルフをホットアドする

スタックにディスクシェルフをホットアドするには、次の手順を実行します。

作業を開始する前に

- システムがのすべての要件を満たしていることを確認しますSASディスクシェルフのホットアドの準備。
- シェルフをホットアドする前に、環境が次のいずれかのシナリオを満たしていることを確認します。
  - SAS ディスクシェルフのスタックに FibreBridge 7500N ブリッジが 2 つ接続されている。
  - SASディスクシェルフのスタックにFibreBridge 7600Nブリッジが2つ接続されている。
  - SASディスクシェルフのスタックにFibreBridge 7500NブリッジとFibreBridge 7600Nブリッジが1つずつ接続されている。

このタスクについて

- この手順は、スタック内の最後のディスクシェルフにディスクシェルフをホットアドするためのものです。

  この手順は、スタック内の最後のディスクシェルフが IOM A からブリッジ A に、 IOM B からブリッジ B に接続されていることを前提としています

- これは無停止の手順です。
- 各サイトで同数のディスクシェルフをホットアドする必要があります。
- 複数のディスクシェルフをホットアドする場合は、ディスクシェルフを 1 つずつホットアドする必要があります。

  FibreBridge 7500N または 7600N ブリッジペアは、それぞれ最大 4 個のスタックをサポートできます。

> ディスクシェルフをホットアドするには、 advanced モードで「 storage disk firmware update 」コマンドを実行して、ホットアドするディスクシェルフのディスクドライブファームウェアを更新する必要があります。システム内の既存のディスクドライブのファームウェアのバージョンが古い場合は、このコマンドを実行するとシステムが停止する可能性があります。
>
> SASケーブルを間違ったポートに挿入した場合は、SASポートからケーブルを取り外したあと、120秒以上待ってから別のSASポートに接続する必要があります。そうしないと、ケーブルを別のポートに移動したことがシステムで認識されません。

手順

1. 自身の適切な接地対策を行います
2. いずれかのコントローラのシステムコンソールからディスクシェルフの接続を確認します。

   「 sysconfig -v 」を使用します

   次のような出力が表示されます。

   - 各 FC ポートの下に、認識されているブリッジがそれぞれ別々の行に表示されます。たとえば、一連の FibreBridge 7500N ブリッジにディスクシェルフをホットアドした場合、出力は次のようになります。

```
FC-to-SAS Bridge:
cisco_A_1-1:9.126L0: ATTO  FibreBridge7500N 2.10  FB7500N100189
cisco_A_1-2:1.126L0: ATTO  FibreBridge7500N 2.10  FB7500N100162
```

- 各 FC ポートの下に、認識されているディスクシェルフがそれぞれ別々の行に表示されます。

```
Shelf   0: IOM6  Firmware rev. IOM6 A: 0173 IOM6 B: 0173
Shelf   1: IOM6  Firmware rev. IOM6 A: 0173 IOM6 B: 0173
```

- 各 FC ポートの下に、認識されているディスクドライブがそれぞれ別々の行に表示されます。

```
cisco_A_1-1:9.126L1   : NETAPP   X421_HCOBD450A10 NA01 418.0GB
(879097968 520B/sect)
cisco_A_1-1:9.126L2   : NETAPP   X421_HCOBD450A10 NA01 418.0GB
(879097968 520B/sect)
```

3. いずれかのコントローラのコンソールで、システムで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確認します。

   「 storage disk option show 」をクリックします

   自動割り当てポリシーが[Auto Assign]列に表示されます。

```
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.
```

4. システムでディスクの自動割り当てが有効になっていない場合や、同じスタック内のディスクドライブを両方のコントローラで所有している場合は、ディスクドライブを適切なプールに割り当てます。

   "ディスクおよびアグリゲートの管理"

- ディスクシェルフの1つのスタックを2台のコントローラに分割する場合は、ディスク所有権を割り当てる前にディスクの自動割り当てを無効にする必要があります。そうしないと、1本のディスクドライブを割り当てたときに、残りのディスクドライブが同じコントローラおよびプールに自動的に割り当てられることがあります。

`storage disk option modify -node <node-name> -autoassign off`コマンドは、ディスクの自動割り当てを無効にします。

- ディスクドライブとディスクシェルフのファームウェアを更新するまで、アグリゲートまたはボリュームにドライブを追加することはできません。

5. ダウンロードしたファームウェアの手順に従って、ディスクシェルフファームウェアを最新バージョンに更新します。

   手順のコマンドは、どちらのコントローラのシステムコンソールでも実行できます。

   "ネットアップのダウンロード：ディスクシェルフファームウェア"

6. ディスクシェルフを設置してケーブル接続します。

   コネクタをポートに無理に押し込まないでください。Mini-SAS ケーブルは、誤挿入を防ぐキーイングが施されているため、正しい向きで SAS ポートに取り付けるとカチッとはまり、ディスクシェルフの SAS ポートの LNK LED が緑色に点灯します。ディスクシェルフの場合、プルタブを上（コネクタの上側）にして SAS ケーブルコネクタを挿入します。

   a. ディスクシェルフを設置して電源をオンにし、シェルフ ID を設定します。

      ディスクシェルフの設置の詳細については、使用しているディスクシェルフモデルの『 Installation Guide 』を参照してください。

      ディスクシェルフの電源を再投入し、各 SAS ディスクシェルフのシェルフ ID をストレージシステム全体で一意にする必要があります。

   b. スタック内の最後のシェルフの IOM B ポートから SAS ケーブルを外し、新しいシェルフの同じポートに再接続します。

      このケーブルのもう一方の端は、ブリッジ B に接続されたままです

   c. 新しいディスクシェルフをデイジーチェーン接続します。そのためには、新しいシェルフの（ IOM A と IOM B の） IOM ポートを最後のシェルフの（ IOM A と IOM B の） IOM ポートにケーブル接続します。

   ディスクシェルフのデイジーチェーン接続の詳細については、使用しているディスクシェルフモデルの Installation Guide を参照してください。

7. システムコンソールからディスクドライブファームウェアを最新バージョンに更新します。

   "ネットアップのダウンロード：ディスクドライブファームウェア"

   a. advanced権限レベルに切り替えます。+

```
set -privilege advanced
```

advanced モードで続けるかどうかを尋ねられたら、「 * y * 」と入力して応答する必要があります。advanced モードのプロンプトが表示されます（ * > ）。

b. システムコンソールからディスクドライブファームウェアを最新バージョンに更新します。+
`storage disk firmware update`

c. admin 権限レベルに戻ります。 +`set -privilege admin`

d. もう一方のコントローラで上記の手順を繰り返します。

8. ONTAP で MetroCluster 構成の動作を確認します。

a. システムがマルチパスかどうかを確認します。

```
node run -node <node-name> sysconfig -a
```

b. 両方のクラスタにヘルス・アラートがないかどうかを確認します +`system health alert show`

c. MetroCluster 構成と動作モードが正常であることを確認します。 + MetroCluster show `

d. MetroCluster チェックを実行します + MetroCluster チェックを実行します

e. MetroCluster チェックの結果を表示します。

MetroCluster チェックショー

f. スイッチにヘルスアラートがないかどうかを確認します（ある場合）。

「 storage switch show 」と表示されます

g. Active IQ Config Advisorを実行します。

"ネットアップのダウンロード： Config Advisor"

h. Config Advisor の実行後、ツールの出力を確認し、推奨される方法で検出された問題に対処します。

9. 複数のディスクシェルフをホットアドする場合は、ホットアドするディスクシェルフごとに上記の手順を繰り返します。

MetroCluster FC 構成からのストレージのホットリムーブ

ドライブシェルフのホットリムーブ（ドライブからアグリゲートを削除済みのシェルフを物理的に取り外す）は、 MetroCluster FC 構成でデータを提供している状態から実行できます。ホットリムーブでは、シェルフのスタックから任意のシェルフを取り外したり、シェルフのスタック全体を取り外したりできます。

- システムは、マルチパス HA 、マルチパス、クアッドパス HA 、またはクアッドパス構成である必要があります。
- 4 ノード MetroCluster FC 構成では、ローカル HA ペアをテイクオーバー状態にすることはできません。
- 取り外すシェルフのドライブからすべてのアグリゲートを削除しておく必要があります。

MetroCluster FC 以外原因の構成では、取り外すシェルフにアグリゲートが含まれたこの手順を使用しようとすると、システムで障害が発生し、複数のドライブがパニック状態になることがあります。

アグリゲートを削除するには、取り外すシェルフ上のミラーされたアグリゲートをスプリットし、別のドライブセットを使用してミラーされたアグリゲートを作成し直す必要があります。

"ディスクおよびアグリゲートの管理"

- 取り外すシェルフのドライブからアグリゲートを削除したあとに、ドライブ所有権を削除しておく必要があります。

  "ディスクおよびアグリゲートの管理"

- スタックからシェルフを取り外す場合は、残ったシェルフ間の距離を考慮する必要があります。

  現在のケーブルでは長さが足りない場合は、もっと長いケーブルを用意する必要があります。

このタスクでは、次の MetroCluster FC 構成を環境に追加します。

- ストレージシェルフが SAS ケーブルでストレージコントローラに直接接続されている直接接続型の MetroCluster FC 構成
- ストレージシェルフが FC-to-SAS ブリッジを使用して接続されているファブリック接続またはブリッジ接続の MetroCluster FC 構成

手順

1. ONTAP で MetroCluster 構成の動作を確認します。
   a. システムがマルチパスかどうかを確認します。 `+* node run -node -name_sysconfig -a *`
   b. ヘルスアラートがないかどうかを両方のクラスタで確認します。

      「 * system health alert show * 」というメッセージが表示されます

   c. MetroCluster 構成と動作モードが正常であることを確認します :`+* MetroCluster show*`
   d. MetroCluster チェックを実行します。

      「 * MetroCluster check run * 」のようになります

   e. MetroCluster チェックの結果を表示します。

      「 * MetroCluster check show * 」と表示されます

   f. スイッチにヘルスアラートがないかどうかを確認します（ある場合）。

      「 * storage switch show * 」と表示されます

   g. Config Advisor を実行します。

      "ネットアップのダウンロード： Config Advisor"

h. Config Advisor の実行後、ツールの出力を確認し、推奨される方法で検出された問題に対処します。

2. 権限レベルを advanced に設定します。

   「 * set -privilege advanced * 」のように指定します

3. シェルフ上にメールボックス・ドライブがないことを確認します。「 * storage failover mailbox-disk show * 」

4. 該当するシナリオの手順に従ってシェルフを取り外します。

シナリオ（ Scenario ）	手順
ミラーされていないアグリゲート、ミラーされたアグリゲート、または両方のタイプのアグリゲートが含まれているシェルフからアグリゲートを削除する	a. アグリゲートを削除するには、「 storage aggregate delete -aggregate name_aggregate name 」コマンドを使用します。 b. 標準の手順を使用してシェルフ内のすべてのドライブの所有権を削除してから、シェルフを物理的に取り外します。 シェルフをホットリムーブするには、使用しているシェルフモデルの SAS Disk Shelves Service Guide に記載されている手順に従ってください。

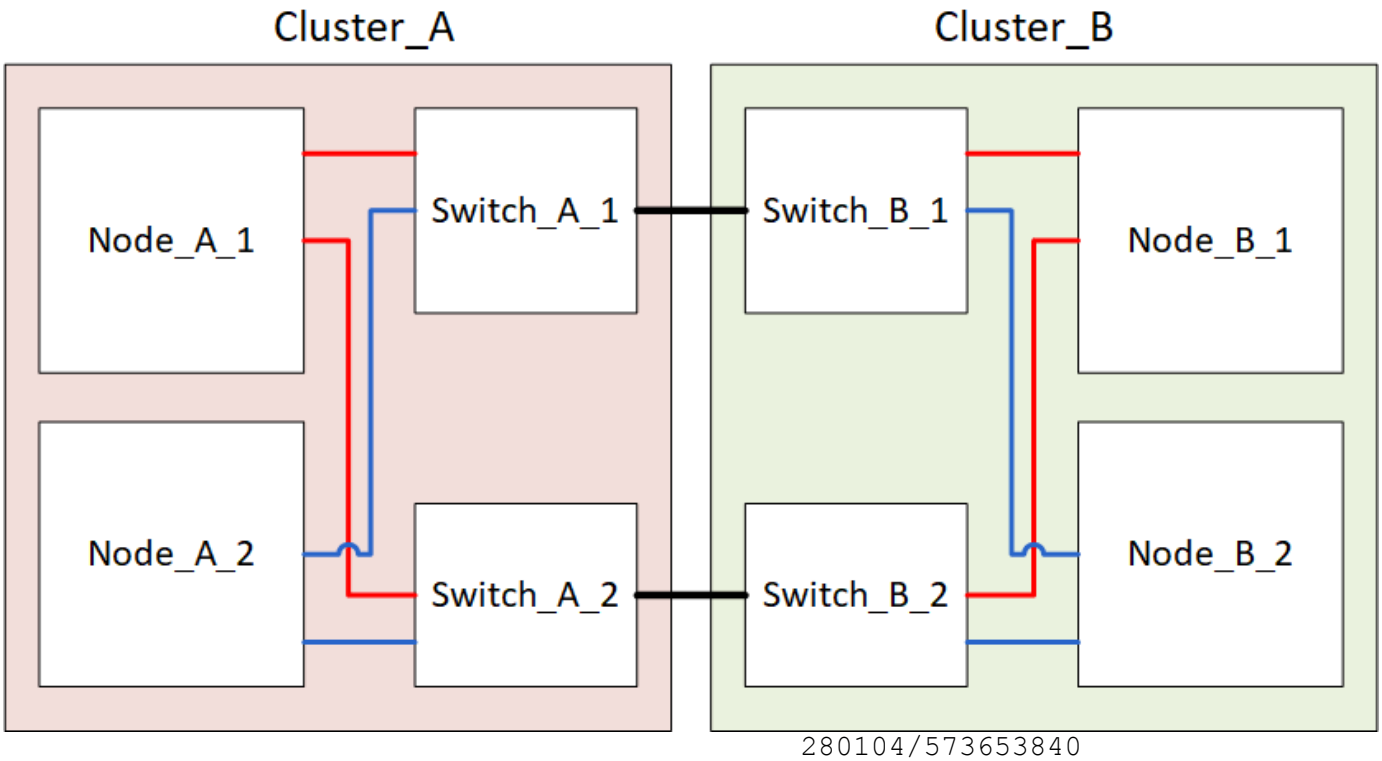
ミラーされたアグリゲートからプレックスを削除するために、アグリゲートのミラーリングを解除する必要がある	a. run -node local sysconfig -r コマンドを使用して ' 削除するプレックスを特定します 次の例では、「 Plex /dpg_mcc_8020_13_a1_aggr1/plex0 」行でプレックスを特定できます。この場合 ' 指定するプレックスは plex0 です `dpgmcc_8020_13_a1a2::storage aggregate> run -node local sysconfig -r` `*** This system has taken over dpg-mcc-8020-13-a1` `Aggregate dpg_mcc_8020_13_a1_aggr1 (online, raid_dp, mirrored) (block checksums)` `  Plex /dpg_mcc_8020_13_a1_aggr1/plex0 (online, normal, active, pool0)` `    RAID group /dpg_mcc_8020_13_a1_aggr1/plex0/rg0 (normal, block checksums)` `      RAID Disk Device HA  SHELF BAY CHAN Pool Type RPM  Used (MB/blks)    Phys (MB/blks)` `      --------- ------ ------------- ---- ---- ---- ----- -------------- --------------` `      dparity   mcc-cisco-8Gb-fab-2:1-1.126L16  0c    32  15 FC:B   0   SAS 15000 272000/557056000 274845/562884296` `      parity    mcc-cisco-8Gb-fab-2:1-1.126L18  0c    32  17 FC:B   0   SAS 15000 272000/557056000 274845/562884296` `      data      mcc-cisco-8Gb-fab-2:1-1.126L19  0c    32  18 FC:B   0   SAS 15000 272000/557056000 274845/562884296` `      data      mcc-cisco-8Gb-fab-2:1-1.126L21  0c    32  20`

MetroCluster FC構成での単一サイトの電源オフと電源オン

MetroCluster FC構成でサイトのメンテナンスを実施したり、単一サイトを再配置したりする必要がある場合は、サイトの電源をオフにして電源をオンにする方法を確認しておく必要があります。

サイトを再配置して再設定する必要がある場合（4ノードクラスタから8ノードクラスタに拡張する必要がある場合など）は、これらのタスクを同時に実行することはできません。この手順では、サイトのメンテナンスを実行するため、またはサイトの構成を変更せずにサイトを再配置するために必要な手順のみを説明します。

次の図は、 MetroCluster 構成を示しています。メンテナンスのためにcluster_Bの電源がオフになっています。



MetroClusterサイトの電源をオフにする

サイトのメンテナンスや再配置を開始する前に、サイトとすべての機器の電源をオフにする必要があります。

このタスクについて

次の手順のすべてのコマンドは、電源をオンにしたままのサイトから実行されます。

手順

1. 開始する前に、ミラーされていないアグリゲートがサイトですべてオフラインになっていることを確認します。
2. ONTAP で MetroCluster 構成の動作を確認します。
   a. システムがマルチパスかどうかを確認します。

      'node run -node _node-name_sysconfig -a

```
FC:B   0   SAS 15000
272000/557056000
2748257562884296
      data      mcc-cisco-8Gb-
fab-2:1-1.126L22  0c    32  21
FC:B   0   SAS 15000
272000/557056000
2748257562884296

      Plex
/dpg_mcc_8020_13_a1_aggr1/plex
1 (online, normal, active,
280104/573653840
      parity    mcc-cisco-8Gb-
fab-3:1-1.126L14  0d    33  13
FC:A   1   SAS 15000
272000/557056000
280104/573653840
      data      mcc-cisco-8Gb-
fab-3:1-1.126L41  0d    34  14
FC:A   1   SAS 15000
272000/557056000
280104/573653840
      data      mcc-cisco-8Gb-
fab-3:1-1.126L15  0d    33  14
FC:A   1   SAS 15000
272000/557056000
280104/573653840
      data      mcc-cisco-8Gb-
fab-3:1-1.126L45  0d    34  18
FC:A   1   SAS 15000
```

b. ヘルスアラートがないかどうかを両方のクラスタで確認します。

「 system health alert show 」というメッセージが表示されます

c. MetroCluster 構成と運用モードが正常な状態であることを確認します。

「 MetroCluster show 」

d. MetroCluster チェックを実行します + MetroCluster チェックを実行します

e. MetroCluster チェックの結果を表示します。

MetroCluster チェックショー

f. スイッチにヘルスアラートがないかどうかを確認します（ある場合）。

「 storage switch show 」と表示されます

g. Config Advisor を実行します。

"ネットアップのダウンロード： Config Advisor"

h. Config Advisor の実行後、ツールの出力を確認し、推奨される方法で検出された問題に対処します。

3. 稼働したままにするサイトから、スイッチオーバーを実施します。

MetroCluster スイッチオーバー

```
cluster_A::*> metrocluster switchover
```

この処理が完了するまでに数分かかることがあります。

ミラーされていないアグリゲートは、アグリゲート内のリモートディスクにアクセスできる場合にのみ、スイッチオーバー後にオンラインになります。ISLで障害が発生すると、ローカルノードはミラーされていないリモートディスクのデータにアクセスできなくなる可能性があります。アグリゲートに障害が発生すると、ローカルノードがリブートされる場合があります。

4. スイッチオーバーの完了を監視して確認します。

「 MetroCluster operation show 」を参照してください

```
cluster_A::*> metrocluster operation show
  Operation: Switchover
 Start time: 10/4/2012 19:04:13
State: in-progress
   End time: -
     Errors:

cluster_A::*> metrocluster operation show
  Operation: Switchover
 Start time: 10/4/2012 19:04:13
      State: successful
   End time: 10/4/2012 19:04:22
     Errors: -
```

5. ミラーされていないアグリゲートに属するボリュームとLUNをすべてオフラインにします。
   a. ボリュームをオフラインにします。

      ```
      cluster_A::* volume offline <volume name>
      ```

   b. LUNをオフラインにします。

      ```
      cluster_A::* lun offline lun_path <lun_path>
      ```

6. ミラーされていないアグリゲートをオフラインにします：「storage aggregate offline

```
cluster_A*::> storage aggregate offline -aggregate <aggregate-name>
```

7. 構成と ONTAP のバージョンに応じて、ディザスタサイト（ cluster_B ）にあるオフラインの影響を受けるプレックスを特定して移動します。

   次のプレックスをオフラインにする必要があります。

   - ディザスタサイトにあるディスクにあるミラーリングされていないプレックス

     ディザスタサイトのミラーされていないプレックスをオフラインにしないと、あとでディザスタサイトの電源をオフにしたときにシステムが停止する可能性があります。

   - ディザスタサイトのディスクにあるミラーされたプレックスを使用してアグリゲートをミラーリングする。オフラインにすると、プレックスにアクセスできなくなります。

   a. 影響を受けるプレックスを特定します。

      サバイバーサイトのノードが所有するプレックスは、プール 1 のディスクで構成されます。ディザスタサイトのノードが所有するプレックスは、プール 0 のディスクで構成されます。

```
Cluster_A::> storage aggregate plex show -fields aggregate,status,is-
online,Plex,pool
aggregate    plex  status        is-online pool
------------ ----- ------------- --------- ----
Node_B_1_aggr0 plex0 normal,active true     0
Node_B_1_aggr0 plex1 normal,active true     1

Node_B_2_aggr0 plex0 normal,active true     0
Node_B_2_aggr0 plex5 normal,active true     1

Node_B_1_aggr1 plex0 normal,active true     0
Node_B_1_aggr1 plex3 normal,active true     1

Node_B_2_aggr1 plex0 normal,active true     0
Node_B_2_aggr1 plex1 normal,active true     1

Node_A_1_aggr0 plex0 normal,active true     0
Node_A_1_aggr0 plex4 normal,active true     1

Node_A_1_aggr1 plex0 normal,active true     0
Node_A_1_aggr1 plex1 normal,active true     1

Node_A_2_aggr0 plex0 normal,active true     0
Node_A_2_aggr0 plex4 normal,active true     1

Node_A_2_aggr1 plex0 normal,active true     0
Node_A_2_aggr1 plex1 normal,active true     1
14 entries were displayed.

Cluster_A::>
```

影響を受けるプレックスは、クラスタ A のリモートにあるプレックスです次の表に、ディスクがクラスタ A に対してローカルかリモートかを示します。

ノード	プール内のディスク	ディスクをオフラインにする必要があるか	オフラインにするプレックスの例を指定します
Node_a_1 および Node_a_2	プール 0 内のディスク	いいえディスクはクラスタ A に対してローカルです	-

プール 1 内のディスク	はい。ディスクはクラスタ A に対してリモートです	node_A_1 の aggr0 / プレックス 4 を使用します node_A_1 の aggr1 / plex1 node_a_2_aggr0/plex4 Node_a_2_aggr1 / plex1 です	Node_B_1 および Node_B_2
プール 0 内のディスク	はい。ディスクはクラスタ A に対してリモートです	node_B_1 の aggr1 / plex0 node_B_1 の aggr0/plex0 node_B_2 の aggr0 / plex0 node_B_2 の aggr1 / plex0	プール 1 内のディスク

b. 影響を受けるプレックスをオフラインにします。

「ストレージアグリゲートのプレックスはオフライン」です

```
storage aggregate plex offline -aggregate Node_B_1_aggr0 -plex plex0
```

+

この手順は、Cluster_Aに対してリモートのディスクを含むすべてのプレックスに対して実行します。

8. スイッチタイプに応じて、ISLスイッチポートを永続的にオフラインにします。

スイッチのタイプ	アクション

Brocade FCスイッチ	a. を使用します `portcfgpersistentdisable <port>` 次の例に示すように、ポートを永続的に無効にするコマンドを実行します。サバイバーサイトにある両方のスイッチで実行する必要があります。 `Switch_A_1:admin> portcfgpersistentdisable 14` `Switch_A_1:admin> portcfgpersistentdisable 15` `Switch_A_1:admin>` b. 次の例に示す 'witchshow' コマンドを使用して ' ポートが無効になっていることを確認します `Switch_A_1:admin> switchshow` `switchName: Switch_A_1` `switchType: 109.1` `switchState: Online` `switchMode: Native` `switchRole: Principal` `switchDomain: 2` `switchId: fffc02` `switchWwn: 10:00:00:05:33:88:9c:68` `zoning: ON (T5_T6)` `switchBeacon: OFF` `FC Router: OFF` `FC Router BB Fabric ID: 128` `Address Mode: 0` `Index Port Address Media Speed State Proto` `==========` `...` `14 14 020e00 id 16G No_Light FC Disabled (Persistent)` `15 15 020f00 id 16G No_Light FC Disabled (Persistent)` `...` `Switch_A_1:admin>`

Cisco FCスイッチ	a. 「 interface 」コマンドを使用して、ポートを永続的に無効にします。次の例は、ポート 14 および 15 を無効にします。 ``` Switch_A_1# conf t Switch_A_1(config)# interface fc1/14-15 Switch_A_1(config)# shut Switch_A_1(config-if)# end Switch_A_1# copy running-config startup-config ``` b. 次の例に示すように、「 show interface brief 」コマンドを使用して、スイッチポートが無効になっていることを確認します。 ``` Switch_A_1# show interface brief Switch_A_1 ```

9. ディザスタサイトの機器の電源をオフにします。

   次の機器の電源を、記載されている順序でオフにする必要があります。

   - ストレージコントローラ-ストレージコントローラは現在、 `LOADER` プロンプトが表示されたら、電源を完全にオフにする必要があります。
   - MetroCluster FC スイッチ
   - ATTO FibreBridge（存在する場合）
   - ストレージシェルフ

電源がオフになっている **MetroCluster** サイトの再配置

サイトの電源をオフにしたら、メンテナンス作業を開始できます。手順は、 MetroCluster コンポーネントを同じデータセンター内で再配置する場合も、別のデータセンターに再配置する場合も同じです。

- ハードウェアは、前のサイトと同じ方法でケーブル接続する必要があります。
- スイッチ間リンク（ ISL ）の速度、長さ、または数が変わった場合は、すべて再設定する必要があります。

手順

1. 新しい場所で正しく再接続できるように、すべてのコンポーネントのケーブル配線が慎重に記録されていることを確認します。
2. すべてのハードウェア、ストレージコントローラ、FCスイッチ、FibreBridge、およびストレージシェルフを物理的に再配置します。
3. ISL ポートを設定し、サイト間接続を確認します。

   a. FCスイッチの電源をオンにします。

他の機器の電源はオンにしないでください。

b. ポートを有効にします。

次の表に示す適切なスイッチタイプに従って、ポートを有効にします。

スイッチのタイプ	コマンドを実行します

Brocade FCスイッチ	i. を使用します `portcfgpersistentenable <port number>` コマンドを実行して、ポートを永続的に有効にします。サバイバーサイトにある両方のスイッチで実行する必要があります。 次の例は、 Switch_A_1 のポート 14 と 15 を有効にします。 ``` switch_A_1:admin> portcfgpersistentenable 14 switch_A_1:admin> portcfgpersistentenable 15 switch_A_1:admin> ``` ii. スイッチポートが有効になっていることを確認します。「 witchshow 」 次の例は、ポート 14 および 15 を有効にします。 ``` switch_A_1:admin> switchshow switchName: Switch_A_1 switchType: 109.1 switchState: Online switchMode: Native switchRole: Principal switchDomain: 2 switchId: fffc02 switchWwn: 10:00:00:05:33:88:9c:68 zoning: ON (T5_T6) switchBeacon: OFF FC Router: OFF FC Router BB Fabric ID: 128 Address Mode: 0 Index Port Address Media Speed State Proto == ==== ... 14 14 020e00 id 16G Online FC E-Port 10:00:00:05:33:86:89:cb "Switch_A_1" 15 15 020f00 id 16G Online FC E-Port 10:00:00:05:33:86:89:cb "Switch_A_1" (downstream) ... switch_A_1:admin> ```

Cisco FCスイッチ	i. 「 interface 」コマンドを入力して、ポートをイネーブルにします。 次の例は、 Switch_A_1 のポート 14 と 15 を有効にします。 ``` switch_A_1# conf t switch_A_1(config)# interface fc1/14-15 switch_A_1(config)# no shut switch_A_1(config-if)# end switch_A_1# copy running-config startup-config ``` ii. スイッチポートが有効になっていることを確認します。「 show interface brief 」 ``` switch_A_1# show interface brief switch_A_1# ```

4. スイッチのツールを使用して（使用可能な場合）、サイト間接続を確認します。

   リンクが正しく設定され、安定している場合にのみ続行してください。

5. リンクが安定していることがわかった場合は、リンクを再度無効にします。

   次の表に示すように、 Brocade スイッチと Cisco スイッチのどちらを使用しているかに基づいてポートを無効にします。

スイッチのタイプ	コマンドを実行します

Brocade FCスイッチ	a. を入力します `portcfgpersistentdisable <port_number>` コマンドを実行して、ポートを永続的に無効にします。 サバイバーサイトにある両方のスイッチで実行する必要があります。次の例は、 Switch_A_1 のポート 14 と 15 を無効にします。 `switch_A_1:admin> portpersistentdisable 14` `switch_A_1:admin> portpersistentdisable 15` `switch_A_1:admin>` b. スイッチポートが無効になっていることを確認します。「 witchshow 」 次の例は、ポート 14 および 15 が無効になっていることを示しています。 `switch_A_1:admin> switchshow` `switchName: Switch_A_1` `switchType: 109.1` `switchState: Online` `switchMode: Native` `switchRole: Principal` `switchDomain: 2` `switchId: fffc02` `switchWwn: 10:00:00:05:33:88:9c:68` `zoning: ON (T5_T6)` `switchBeacon: OFF` `FC Router: OFF` `FC Router BB Fabric ID: 128` `Address Mode: 0` `Index Port Address Media Speed State Proto` `==========` `...` `14 14 020e00 id 16G No_Light FC Disabled (Persistent)` `15 15 020f00 id 16G No_Light FC Disabled (Persistent)` `...` `switch_A_1:admin>`

Cisco FCスイッチ	a. 「 interface 」コマンドを使用して、ポートをディセーブルにします。 次の例は、 Switch_A_1 のポート fc1/14 と fc1/15 を無効にします。 ``` switch_A_1# conf t switch_A_1(config)# interface fc1/14-15 switch_A_1(config)# shut switch_A_1(config-if)# end switch_A_1# copy running-config startup- config ``` b. スイッチポートが無効になっていることを確認するには、「 show interface brief 」コマンドを使用します。 ``` switch_A_1# show interface brief switch_A_1# ```

MetroCluster 構成の電源をオンにして通常動作に戻します

メンテナンスを完了、またはサイトを移動したら、サイトの電源をオンにして MetroCluster 構成を再確立する必要があります。

このタスクについて

次の手順のすべてのコマンドは、電源をオンにしたサイトから実行します。

手順

1. スイッチの電源をオンにします。

   最初にスイッチの電源をオンにする必要があります。サイトを再配置した場合は、前の手順で電源がオンになっている可能性があります。

   a. 必要に応じて、または再配置中に実行されていない場合は、スイッチ間リンク（ ISL ）を再設定します。
   b. フェンシングが完了した場合、 ISL を有効にします。
   c. ISL を確認します。
2. FCスイッチのISLを無効にします。
3. シェルフの電源をオンにし、完全に電源が投入されるまでにはしばらくかかります。
4. FibreBridge ブリッジの電源をオンにします。
   a. FC スイッチで、ブリッジを接続しているポートがオンラインになっていることを確認します。

Brocade スイッチの場合は「 witchshow 」、 Cisco スイッチの場合は「 How interface brief 」などのコマンドを使用できます。

b. ブリッジ上のシェルフとディスクが接続されていることを確認します。

次のコマンドを使用できます。 `sastargets` ATTO CLIで、次の手順を実行します。

5. FC スイッチで ISL を有効にします。

次の表に示すように、 Brocade スイッチと Cisco スイッチのどちらを使用しているかに基づいてポートを有効にします。

スイッチのタイプ	コマンドを実行します

Brocade FCスイッチ	a. を入力します `portcfgpersistentenable <port>` コマンドを使用してポートを永続的に有効にします。サバイバーサイトにある両方のスイッチで実行する必要があります。 次の例は、 Switch_A_1 のポート 14 と 15 を有効にします。 `Switch_A_1:admin> portcfgpersistentenable 14` `Switch_A_1:admin> portcfgpersistentenable 15` `Switch_A_1:admin>` b. + 'witchshow' コマンドを使用して ' スイッチポートが有効になっていることを確認します `switch_A_1:admin> switchshow` `switchName: Switch_A_1` `switchType: 109.1` `switchState: Online` `switchMode: Native` `switchRole: Principal` `switchDomain: 2` `switchId: fffc02` `switchWwn: 10:00:00:05:33:88:9c:68` `zoning: ON (T5_T6)` `switchBeacon: OFF` `FC Router: OFF` `FC Router BB Fabric ID: 128` `Address Mode: 0` `Index Port Address Media Speed State Proto` `==========` `...` `14 14 020e00 id 16G Online FC E-Port 10:00:00:05:33:86:89:cb "Switch_A_1"` `15 15 020f00 id 16G Online FC E-Port 10:00:00:05:33:86:89:cb "Switch_A_1" (downstream)` `...` `switch_A_1:admin>`

Cisco FCスイッチ	a. ポートをイネーブルにするには 'interface コマンドを使用します 次の例は、 Switch_A_1 のポート fc1/14 と fc1/15 を有効にします。 ``` switch_A_1# conf t switch_A_1(config)# interface fc1/14-15 switch_A_1(config)# no shut switch_A_1(config-if)# end switch_A_1# copy running-config startup-config ``` b. スイッチポートが無効になっていることを確認します。 ``` switch_A_1# show interface brief switch_A_1# ```

6. ストレージが認識されていることを確認します。
   a. サバイバーサイトからストレージが認識されていることを確認します。オフラインのプレックスをオンラインに戻して再同期処理を再開し、SyncMirrorを再確立します。
   b. メンテナンスモードのノードからローカルストレージが認識されていることを確認します。

      「ディスクショー V 」

7. MetroCluster 構成を再確立します。

   の手順に従います "スイッチバックに向けたシステムの事前チェック" MetroCluster 構成に応じて修復処理とスイッチバック処理を実行します。

MetroCluster FC 構成全体の電源をオフにします

サイトのメンテナンスや再配置を開始する前に、 MetroCluster FC 構成全体とすべての機器の電源をオフにする必要があります。

このタスクについて

この手順の手順は、両方のサイトで同時に実行する必要があります。

ONTAP 9.8 以降では '**storage switch ***' コマンドは '**system switch**' に置き換えられています以下の手順は '*storage switch *' コマンドを示していますが 'ONTAP 9.8 以降を実行している場合は '*system switch *' コマンドを使用することをお勧めします

手順

1. MetroCluster 構成の両方のサイトから MetroCluster 構成を確認します。
   a. MetroCluster 構成と運用モードが正常な状態であることを確認します。`+* MetroCluster show*`

b. いずれかの MetroCluster ノードで次のコマンドを入力して、ディスクへの接続を確認します。 `+*run local sysconfig -v *`

c. 次のコマンドを実行します :`+* storage bridge show *`

d. 次のコマンドを実行します :`+* storage port show *`

e. 次のコマンドを実行します :`+* storage switch show *`

f. 次のコマンドを実行します :`+* network port show *`

g. MetroCluster チェック :`+* MetroCluster check run*` を実行します

h. MetroCluster チェックの結果を表示します :`+* MetroCluster check show*`

2. AUSO 障害ドメインをに変更して AUSO を無効にします

「 * auso-disabled * 」と表示されます

```
cluster_A_site_A::*>metrocluster modify -auto-switchover-failure-domain
auso-disabled
```

3. コマンドを使用して、変更を確認します

「 * MetroCluster operation show * 」と表示されます

```
    cluster_A_site_A::*> metrocluster operation show
       Operation: modify
           State: successful
      Start Time: 4/25/2020 20:20:36
        End Time: 4/25/2020 20:20:36
          Errors: -
```

4. 次のコマンドを使用してノードを停止します:`* halt *`

◦ 4ノードまたは8ノードのMetroCluster構成の場合は、を使用します **`inhibit-takeover`** および **`skip-lif-migration-before-shutdown`** パラメータ：

```
system node halt -node node1_SiteA -inhibit-takeover true -ignore
-quorum-warnings true -skip-lif-migration-before-shutdown true
```

◦ 2 ノード MetroCluster 構成の場合は、コマンドを使用します。

```
system node halt -node node1_SiteA -ignore-quorum-warnings true
```

5. サイトで次の機器の電源をオフにします。

◦ ストレージコントローラ

- MetroCluster FCスイッチ（2ノードストレッチ構成でない場合に使用）
- ATTO FibreBridge
- ストレージシェルフ

6. 30分待ってから、サイトで次の機器の電源をオンにします。
   - ストレージシェルフ
   - ATTO FibreBridge
   - MetroCluster FC スイッチ
   - ストレージコントローラ
7. コントローラの電源をオンにしたら、両方のサイトで MetroCluster 構成を確認します。

   設定を確認するには、手順 1 を繰り返します。
8. 電源再投入チェックを実行します。
   a. すべての同期元 SVM がオンラインであることを確認します。 `+* vserver show *`
   b. オンラインでない同期元の SVM をすべて起動します。 `+* vserver start *`

MetroCluster IP構成のメンテナンス手順

IP スイッチのメンテナンスと交換

IPスイッチを交換するか、既存の**MetroCluster IP**スイッチの使用方法を変更します

障害が発生したスイッチの交換、スイッチのアップグレードまたはダウングレード、既存のMetroCluster IPスイッチの使用の変更が必要になる場合があります。

このタスクについて

この手順 は、ネットアップ検証済みのスイッチを使用している場合に適用されます。MetroCluster 準拠のスイッチを使用している場合は、スイッチのベンダーを参照してください。

"コンソールログを有効にする" このタスクを実行する前に。

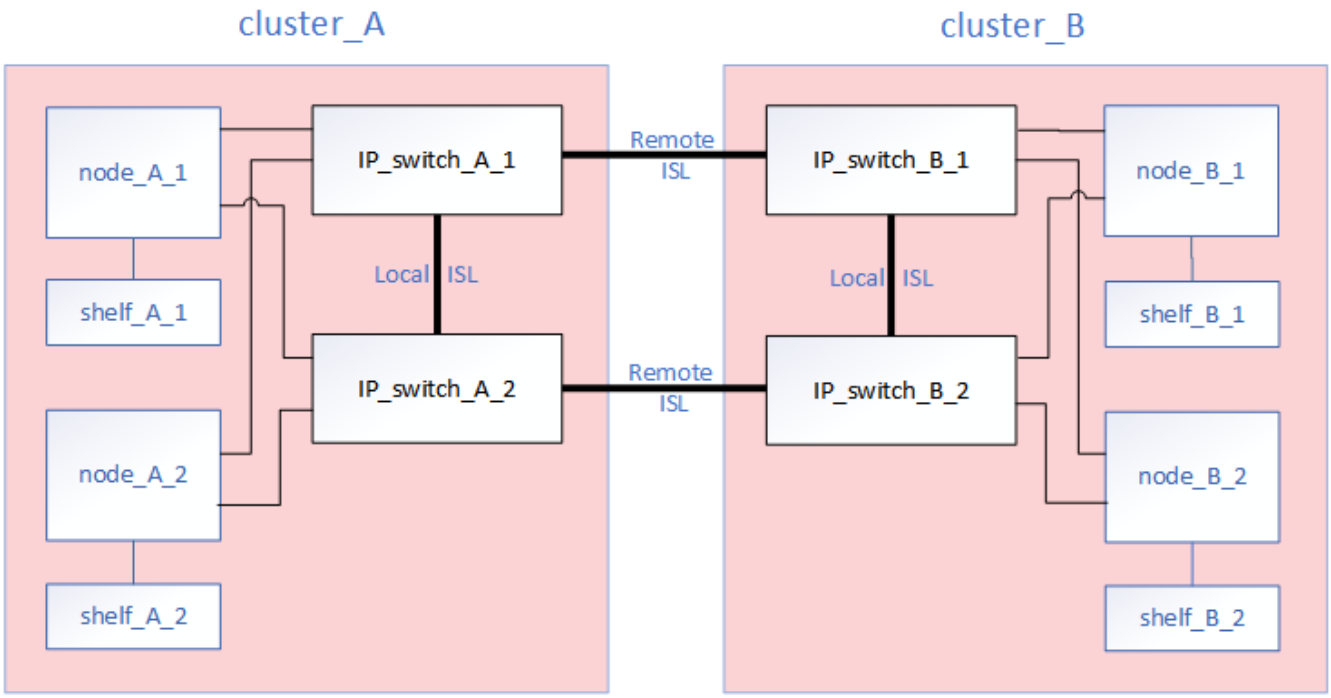
この手順 では、次の変換がサポートされています。

- スイッチのベンダー、タイプ、またはその両方を変更しています。スイッチに障害が発生した場合は、新しいスイッチを古いスイッチと同じにしたり、スイッチのタイプを変更（スイッチをアップグレードまたはダウングレード）したりできます。

  たとえば、AFF A400コントローラとBES-53248スイッチを使用する単一の4ノード構成からAFF A400コントローラを使用する8ノード構成にMetroCluster IP構成を拡張するには、新しい構成ではBES-53248スイッチはサポートされないため、スイッチをサポートされるタイプに変更する必要があります。

  障害が発生したスイッチを同じタイプのスイッチに交換する場合は、障害が発生したスイッチのみを交換します。スイッチをアップグレードまたはダウングレードする場合は、同じネットワークにある2つのスイッチを調整する必要があります。2つのスイッチがスイッチ間リンク（ISL）で接続されており、同じサイトに配置されていない場合、2つのスイッチは同じネットワークにあります。たとえば、次の図に示す

ように、ネットワーク1にはIP_switch_A_1とIP_switch_B_1が含まれ、ネットワーク2にはIP_switch_A_2とIP_switch_B_2が含まれています。



スイッチを交換する場合や別のスイッチにアップグレードする場合は、スイッチのファームウェアとRCFファイルをインストールすることでスイッチを事前に設定できます。

- 共有ストレージのMetroCluster スイッチを使用して、MetroCluster IP構成をMetroCluster IP構成に変換します。

  たとえば、AFF A700コントローラを使用する通常のMetroCluster IP構成で、NS224シェルフを同じスイッチに接続するようにMetroCluster を再設定する場合などです。

  - 共有ストレージMetroCluster IPスイッチを使用してMetroCluster IP構成のシェルフを追加または削除する場合は、の手順を実行します "共有ストレージMetroCluster スイッチを使用したMetroCluster IPへのシェルフの追加"
  - MetroCluster IP構成では、NS224シェルフまたは専用のストレージスイッチにすでに直接接続されている場合があります。

ポート使用ワークシート

次の例は、既存のスイッチを使用して2台のNS224シェルフを接続するMetroCluster IP構成を共有ストレージ構成に変換するワークシートです。

ワークシートの定義：

- Existing configuration：既存のMetroCluster 構成のケーブル接続。
- NS224シェルフを使用する新しい構成：ストレージとMetroCluster 間でスイッチを共有するターゲット構成。

このワークシートで強調表示されているフィールドは、次のとおりです。

- 緑：ケーブルを変更する必要はありません。
- 黄色：同じ構成または異なる構成のポートを移動する必要があります。
- 青：新しい接続のポート。

PORT USAGE OVERVIEW Example of expanding an existing 4Node MetroCluster with 2x NS224 shelves and changing the ISL's from 10G to 40/100G							
Switch port	Existing configuration				New configuration with NS224 shelves		
	Port use	IP_switch_x_1	IP_switch_x_2		Port use	IP_switch_x_1	IP_switch_x_2
1	MetroCluster 1, Local Cluster Interface	Cluster Port 'A'	Cluster Port 'B'		MetroCluster 1, Local Cluster Interface	Cluster Port 'A'	Cluster Port 'B'
2		Cluster Port 'A'	Cluster Port 'B'			Cluster Port 'A'	Cluster Port 'B'
3							
4							
5					Storage shelf 1 (9)	NSM-A, e0a	NSM-A, e0b
6						NSM-B, e0a	NSM-B, e0b
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster			ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	Port 'A'	Port 'B'		MetroCluster 1, MetroCluster interface	Port 'A'	Port 'B'
10		Port 'A'	Port 'B'			Port 'A'	Port 'B'
11							
12							
13					ISL, MetroCluster, native speed 40G / 100G breakout mode 10G	Remote ISL, 2x 40/100G	Remote ISL, 2x 40/100G
14							
15							
16							
17					MetroCluster 1, Storage Interface	Storage Port 'A'	Storage Port 'B'
18						Storage Port 'A'	Storage Port 'B'
19							
20							
21	ISL, MetroCluster breakout mode 10G	Remote ISL, 10G	Remote ISL, 10G		Storage shelf 2 (8)	NSM-A, e0a	NSM-A, e0b
22						NSM-B, e0a	NSM-B, e0b
23							
24							
25							
26							
27							
28							
29							
30							
31							
32							
33							
34							
35							
36							

手順

1. 構成の健全性を確認します。

   a. MetroCluster が構成されていて、各クラスタで通常モードであることを確認します。「 * MetroCluster show * 」

```
cluster_A::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
Remote: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
```

   b. 各ノードでミラーリングが有効になっていることを確認します。「 * 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_1       configured     enabled   normal
2 entries were displayed.
```

   c. 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

Last Checked On: 10/1/2014 16:03:37

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
4 entries were displayed.

Command completed. Use the "metrocluster check show -instance"
command or sub-commands in "metrocluster check" directory for
detailed results.
To check if the nodes are ready to do a switchover or switchback
operation, run "metrocluster switchover -simulate" or "metrocluster
switchback -simulate", respectively.
```

d. ヘルス・アラートがないことを確認してください： * system health alert show *

2. 設置前に新しいスイッチを設定します。

既存のスイッチを再利用する場合は、に進みます 手順 4。

> スイッチをアップグレードまたはダウングレードする場合は、ネットワーク内のすべてのスイッチを設定する必要があります。

の「 IP スイッチの設定」セクションの手順に従います "MetroCluster IP のインストールと設定"

スイッチ _A_1 、 _A_2 、 _B_1 、または _B_2 に、適切な RCF ファイルを適用します。新しいスイッチが古いスイッチと同じ場合は、同じ RCF ファイルを適用する必要があります。

スイッチをアップグレードまたはダウングレードする場合は、サポートされている最新の RCF ファイルを新しいスイッチに適用してください。

3. port show コマンドを実行してネットワークポートに関する情報を表示します。

「 * network port show * 」と表示されます

a. すべてのクラスタLIFを変更して自動リバートを無効にします。

```
network interface modify -vserver <vserver_name> -lif <lif_name>
-auto-revert false
```

4. 古いスイッチから接続を切断します。

古い構成と新しい構成で同じポートを使用していない接続だけを切断します。新しいスイッチを使用する場合は、すべての接続を切断する必要があります。

次の順序で接続を削除します。

a. ローカルクラスタインターフェイスを切断します
b. ローカルクラスタのISLを切断します
c. MetroCluster IPインターフェイスを切断します
d. MetroCluster ISLを切断します

を参照してください [port_usage_worksheet]スイッチは変更されません。MetroCluster ISLは再配置されます。切断する必要があります。ワークシートに緑色でマークされている接続を切断する必要はありません。

5. 新しいスイッチを使用する場合は、古いスイッチの電源をオフにしてケーブルを外し、古いスイッチを物理的に取り外します。

既存のスイッチを再利用する場合は、に進みます 手順 6。

管理インターフェイス（使用している場合）を除き、新しいスイッチをケーブル接続しないでください。

6. 既存のスイッチを設定します。

スイッチがすでに設定されている場合は、この手順を省略できます。

既存のスイッチを設定するには、次の手順に従ってファームウェアとRCFファイルをインストールおよびアップグレードします。

- "MetroCluster IP スイッチでのファームウェアのアップグレード"
- "MetroCluster IP スイッチの RCF ファイルをアップグレードします"

7. スイッチをケーブル接続します。

の「IPスイッチのケーブル接続」セクションの手順に従うことができます "MetroCluster IP のインストールと設定"。

次の順序でスイッチをケーブル接続します（必要な場合）。

a. リモートサイトにISLをケーブル接続します。
b. MetroCluster IPインターフェイスをケーブル接続します。
c. ローカルクラスタインターフェイスをケーブル接続します。

- スイッチタイプが異なる場合は、古いスイッチとは異なるポートが使用されることがあります。スイッチをアップグレードまたはダウングレードする場合は、ローカル ISL を * ケーブル接続しないでください。ローカルISLをケーブル接続するのは、2つ目のネットワークのスイッチをアップグレードまたはダウングレードするときに、一方のサイトの両方のスイッチのタイプとケーブル接続が同じ場合だけにしてください。
- Switch-A1とSwitch-B1をアップグレードする場合は、スイッチSwitch-A2とSwitch-B2について手順1~6を実行する必要があります。

8. ローカルクラスタのケーブル接続を完了します。
   a. ローカルクラスタインターフェイスがスイッチに接続されている場合は、次の手順を実行します。
      i. ローカルクラスタのISLをケーブル接続します。
   b. ローカルクラスタインターフェイスがスイッチに*接続されていない*場合：
      i. を使用します "ネットアップのスイッチクラスタ環境に移行する" 手順 ：スイッチレスクラスタをスイッチクラスタに変換します。に示すポートを使用します "MetroCluster IP のインストールと設定" または、RCFケーブル接続ファイルを使用してローカルクラスタインターフェイスを接続します。
9. スイッチに電源を投入します。

   新しいスイッチが同じ場合は、新しいスイッチの電源をオンにします。スイッチをアップグレードまたはダウングレードする場合は、両方のスイッチに電源を投入します。2 つ目のネットワークが更新されるまで、この構成は各サイトにある 2 つの異なるスイッチで動作します。

10. を繰り返して、MetroCluster 構成が正常であることを確認します 手順 1.。

    1 つ目のネットワークでスイッチをアップグレードまたはダウングレードする場合は、ローカルクラスタリングに関するアラートが表示されることがあります。

    ネットワークをアップグレードまたはダウングレードする場合は、 2 つ目のネットワークに対してすべての手順を繰り返します。

11. すべてのクラスタLIFを変更して自動リバートを再度有効にします。

```
network interface modify -vserver <vserver_name> -lif <lif_name> -auto
-revert true
```

12. 現在ホーム ポートにないすべてのクラスタ LIF をホーム ポートに戻します。

```
network interface revert -vserver * -lif *
```

13. 必要に応じて、NS224シェルフを移動します。

    NS224シェルフをMetroCluster IPスイッチに接続しないMetroCluster IP構成を再構成する場合は、該当する手順 を使用してNS224シェルフを追加または移動します。

    - "共有ストレージMetroCluster スイッチを使用したMetroCluster IPへのシェルフの追加"

- "直接接続型ストレージを使用するスイッチレスクラスタから移行する"
- "ストレージスイッチを再利用して、スイッチ接続ストレージを使用するスイッチレス構成から移行する"

オンラインまたはオフラインの**MetroCluster IP**インターフェイスポート

メンテナンスタスクを実行する際に、MetroCluster IPインターフェイスポートをオフラインまたはオンラインにしなければならない場合があります。

このタスクについて

"コンソールログを有効にする" このタスクを実行する前に。

手順

MetroCluster IPインターフェイスポートをオンラインまたはオフラインにするには、次の手順を実行します。

1. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

出力例

```
Cluster A_1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when
         directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y
```

2. MetroCluster IPインターフェイスポートをオフラインにします。

```
system ha interconnect link off -node <node_name> -link <link_num, 0 or
1>
```

出力例

```
Cluster_A1::*> system ha interconnect link off -node node-a1 -link 0
```

a. MetroCluster IPインターフェイスがオフラインであることを確認します。

```
Cluster_A1::*> system ha interconnect port show
```

出力例

```
Cluster_A1::*> system ha interconnect port show
                                Physical  Link
                 Link           Layer     Layer      Physical   Physical
Active
Node             Monitor  Port  State     State       Link Up  Link Down
Link
--------------  -------  ----  --------  ---------  --------  ---------
------
node-a1        off
                              0  disabled  down              4          3
false
                              1  linkup    active            4          2
true
node-a2        off
                              0  linkup    active            4          2
true
                              1  linkup    active            4          2
true
2 entries were displayed.
```

3. MetroCluster IPインターフェイスポートをオンラインにします。

```
system ha interconnect link on -node <node_name> -link <link_num, 0 or
1>
```

出力例

```
Cluster_A1::*> system ha interconnect link on -node node-a1 -link 0
```

a. MetroCluster IPインターフェイスポートがオンラインであることを確認します。

```
Cluster_A1::*> system ha interconnect port show
```

出力例

```
Cluster_A1::*> system ha interconnect port show
                                Physical  Link
                 Link           Layer     Layer      Physical   Physical
Active
Node             Monitor  Port  State     State       Link Up  Link Down
Link
--------------  -------  ----  --------  ---------  --------  ---------
------
node-a1         off
                              0  linkup    active            5          3
true
                              1  linkup    active            4          2
true
node-a2         off
                              0  linkup    active            4          2
true
                              1  linkup    active            4          2
true
2 entries were displayed.
```

MetroCluster IP スイッチのファームウェアをアップグレードします

MetroCluster IP スイッチのファームウェアのアップグレードが必要になる場合があります。

RCFのサポート状況の確認

ONTAPまたはスイッチファームウェアのバージョンを変更する場合は、そのバージョンでサポートされるリファレンス構成ファイル（RCF）があることを確認する必要があります。このツールを使用する"RcfFileGenerator の順にクリックします"と、構成に応じた正しいRCFが生成されます。

手順

1. スイッチから次のコマンドを使用して、RCFのバージョンを確認します。

スイッチ	問題コマンド
Broadcomスイッチ	`(IP_switch_A_1) # show clibanner`
Cisco スイッチ	ip_switch _A_1# には、 banner motd が表示されます
NVIDIA SN2100スイッチ	`cumulus@mcc1:mgmt:~$ nv config find message`

コマンド出力で、RCFバージョンを示す行を確認します。たとえば、Ciscoスイッチからの次の出力は、RCFバージョンが「v1.80」であることを示しています。

```
Filename : NX3232_v1.80_Switch-A2.txt
```

2. 特定のONTAPバージョン、スイッチ、およびプラットフォームでサポートされているファイルを確認するには、を使用し"MetroCluster IP 用の RcfFileGenerator"ます。既存の構成またはにアップグレードする構成に対してRCFを生成できる場合は、そのRCFがサポートされます。
3. スイッチファームウェアがサポートされていることを確認するには、次のマニュアルを参照してください。
   - "Hardware Universe"
   - "NetApp Interoperability Matrix を参照してください"

スイッチのファームウェアをアップグレードします。

このタスクについて

各スイッチでこのタスクを順に実行する必要があります。

"コンソールログを有効にする" このタスクを実行する前に。

手順

1. 構成の健全性を確認します。
   a. 各クラスタで MetroCluster が設定されており、通常モードであることを確認します。

      「 MetroCluster show 」

      ```
      cluster_A::> metrocluster show
      Cluster                   Entry Name          State
      ------------------------- ------------------- -----------
       Local: cluster_A         Configuration state configured
                                Mode                normal
                                AUSO Failure Domain auso-on-cluster-
      disaster
      Remote: cluster_B         Configuration state configured
                                Mode                normal
                                AUSO Failure Domain auso-on-cluster-
      disaster
      ```

   b. 各ノードでミラーリングが有効であることを確認します。

      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_1       configured     enabled   normal
2 entries were displayed.
```

c. 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 」のようになります

```
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。

d. のあとに入力します `metrocluster check run` 処理が完了しました。run：

MetroCluster チェックショー

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. ヘルスアラートがないことを確認します。

「 system health alert show 」というメッセージが表示されます

2. 最初のスイッチにソフトウェアをインストールします。

スイッチには、 switch_A_1 、 switch_B_1 、 switch_B_2 、 switch_B_2 、 switch_B_2 、スイッチ _B_2 を順番にインストールします。

スイッチタイプがBroadcom、Cisco、NVIDIAのいずれであるかに応じて、該当するトピックのスイッチソフトウェアをインストールする手順に従います。

- "BroadcomスイッチのEFOSソフトウェアをダウンロードしてインストールする"
- "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"
- "NVIDIA SN2100スイッチCumulusソフトウェアのダウンロードとインストール"

3. 各スイッチについて、同じ手順を繰り返します。
4. 繰り返します 手順 1. 構成の健全性を確認します。

MetroCluster IP スイッチの **RCF** ファイルをアップグレードします

MetroCluster IPスイッチのリファレンス構成ファイル（RCF）のアップグレードが必要になる場合があります。たとえば、スイッチで実行しているRCFのバージョンが、ONTAPのバージョン、スイッチのファームウェアのバージョン、またはその両方でサポートされていない場合などです。

作業を開始する前に

- 新しいスイッチファームウェアをインストールする場合は、 RCF ファイルをアップグレードする前にスイッチファームウェアをインストールする必要があります。
- RCFをアップグレードする前に、を"RCFのサポート状況の確認"参照してください。
- "コンソールログを有効にする" このタスクを実行する前に。

このタスクについて

- この手順を実行すると、RCFファイルをアップグレードするスイッチでトラフィックが中断されます。トラフィックは、新しいRCFファイルが適用されると再開されます。
- Switch_A_1、Switch_B_1、Switch_A_2、Switch_B_2の手順を一度に1つずつ実行します。

手順

1. 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 」のようになります

      ```
      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. MetroCluster check run オペレーションが完了したら ' MetroCluster check show を実行して結果を表示します

      約 5 分後に、次の結果が表示されます。

```
-----------
::*> 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 オペレーション履歴 show -job-id 38`

b. ヘルスアラートがないことを確認します。

「 system health alert show 」というメッセージが表示されます

2. 新しい RCF ファイルを適用するための IP スイッチを準備します。

スイッチベンダーの手順に従います。

- "Broadcom IP スイッチを工場出荷時のデフォルトにリセットします"
- "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"
- "NVIDIA IP SN2100スイッチを工場出荷時のデフォルトにリセット"

3. スイッチベンダーに応じて、IP RCFファイルをダウンロードしてインストールします。
   - "Broadcom IPのRCFファイルをダウンロードしてインストールする"
   - "Cisco IP RCFファイルのダウンロードとインストール"
   - "NVIDIA IP RCFファイルのダウンロードとインストール"

> L2共有またはL3ネットワーク構成を使用している場合は、お客様の中間スイッチまたはお客様のスイッチでISLポートの調整が必要になることがあります。スイッチポートモードが「access」モードから「trunk」モードに変わることがあります。スイッチ_A_1とB_1の間のネットワーク接続が完全に機能していて、ネットワークが正常である場合にのみ、2つ目のスイッチペア（A_2、B_2）のアップグレードに進みます。

CleanUpFilesを使用して、**Cisco IP**スイッチの**RCF**ファイルをアップグレードします

Cisco IPスイッチのRCFファイルのアップグレードが必要になる場合があります。たとえば、 ONTAP のアップグレードまたはスイッチファームウェアのアップグレードに

は、どちらも新しい RCF ファイルが必要です。

このタスクについて

- RcfFileGeneratorバージョン1.4a以降では、「write erase」を実行することなく、Cisco IPスイッチのスイッチ設定を変更（アップグレード、ダウングレード、または交換）するための新しいオプションが追加されています。
- "コンソールログを有効にする" このタスクを実行する前に。
- Cisco 9336C-FX2スイッチには2種類のスイッチストレージタイプがあり、RCFではそれぞれ異なる名前が付けられています。次の表を参照して、構成に適したCisco 9336C-FX2ストレージタイプを確認してください。

接続するストレージ	**Cisco 9336C-FX2**ストレージタイプを選択...	**RCF**ファイルのバナー/**MOTD**の例
• 直接接続SASシェルフ • 直接接続型NVMeシェルフ • NVMeシェルフを専用ストレージスイッチに接続	9336C-FX2–ダイレクト・ストレージのみ	`* Switch : NX9336C (direct storage, L2 Networks, direct ISL)`
• 直接接続SASシェルフ • MetroCluster IPスイッチに接続されたNVMeシェルフ ⓘ イーサネット接続NVMeシェルフが少なくとも1つ必要です	9336C-FX2–SASおよびイーサネットストレージ	`* Switch : NX9336C (SAS and Ethernet storage, L2 Networks, direct ISL)`

作業を開始する前に

この方法は、構成が次の要件を満たしている場合に使用できます。

- 標準のRCF設定が適用されます。
- 。 "RcfFileGenerator の順にクリックします" 適用するRCFファイルは、同じバージョンおよび設定（プラットフォーム、VLAN）で作成できる必要があります。
- 適用されるRCFファイルは、特別な設定のためにネットアップから提供されたものではありません。
- RCFファイルは適用前に変更されませんでした。
- 現在のRCFファイルを適用する前に、スイッチを工場出荷時のデフォルトにリセットする手順を実行しました。
- RCFの適用後にスイッチ（ポート）の設定を変更していません。

  これらの要件を満たしていない場合は、RCFファイルの生成時に作成されたCleanUpFilesは使用できません。しかし、この関数を利用して一般的なCleanUpFilesを作成することもできます。このメソッドを使用したクリーンアップは、「show running-config」の出力から得られます。これはベストプラクティスです。

スイッチは、Switch_A_1、Switch_B_1、Switch_A_1、Switch_A_1、Switch_B_2、Switch_B_2の順序で更新します。または、Switch_A_1とSwitch_B_1を同時に更新し、Switch_A_1とSwitch_B_2を更新します。

手順

1. 現在のRCFファイルのバージョン、および使用するポートとVLANを確認します。「ip_switch_A_1# show banner motd」

この情報は4つのスイッチすべてから取得し、次の情報の表を完成させる必要があります。

```
* NetApp Reference Configuration File (RCF)
*
* Switch : NX9336C (SAS storage, L2 Networks, direct ISL)
* Filename : NX9336_v1.81_Switch-A1.txt
* Date : Generator version: v1.3c_2022-02-24_001, file creation time:
2021-05-11, 18:20:50
*
* Platforms : MetroCluster 1 : FAS8300, AFF-A400, FAS8700
*              MetroCluster 2 : AFF-A320, FAS9000, AFF-A700, AFF-A800
* Port Usage:
* Ports 1- 2: Intra-Cluster Node Ports, Cluster: MetroCluster 1, VLAN
111
* Ports 3- 4: Intra-Cluster Node Ports, Cluster: MetroCluster 2, VLAN
151
* Ports 5- 6: Ports not used
* Ports 7- 8: Intra-Cluster ISL Ports, local cluster, VLAN 111, 151
* Ports 9-10: MetroCluster 1, Node Ports, VLAN 119
* Ports 11-12: MetroCluster 2, Node Ports, VLAN 159
* Ports 13-14: Ports not used
* Ports 15-20: MetroCluster-IP ISL Ports, VLAN 119, 159, Port Channel 10
* Ports 21-24: MetroCluster-IP ISL Ports, VLAN 119, 159, Port Channel
11, breakout mode 10gx4
* Ports 25-30: Ports not used
* Ports 31-36: Ports not used
*


#
IP_switch_A_1#
```

この出力から、次の2つの表に示す情報を収集する必要があります。

一般的な情報	MetroCluster	データ
RCF ファイルのバージョン		1.81
スイッチのタイプ		NX9336

ネットワークのタイプロジー		L2ネットワーク、直接ISL
ストレージタイプ		SASストレージ
プラットフォーム	1.	AFF A400
	2.	FAS9000

VLANの情報	ネットワーク	**MetroCluster**の設定	スイッチポート	サイト **A**	サイト **B**
VLANローカルクラスタ	ネットワーク1	1.	1、2	111	222
		2.	3、4	151.	251
	ネットワーク2.	1.	1、2	111	222
		2.	3、4	151.	251
VLAN MetroCluster の略	ネットワーク1	1.	9、10	119 番	119 番
		2.	11、12	159	159
	ネットワーク2.	1.	9、10	219	219
		2.	11、12	259	259

2. [[Create]- RCFファイルおよび-CleanUpFiles-or -create-generic-CleanUpFiles]]現在の設定用にRCFファイルとCleanUpFilesを作成するか、汎用のUpCleanFilesを作成します。

   ご使用の構成が前提条件に記載されている要件を満たしている場合は、*オプション1 *を選択します。お使いの構成が前提条件に記載されている要件を*満たしていない*場合は、*オプション2 *を選択します。

オプション**1**：**RCF**ファイルと**CleanUpFiles**を作成します

この手順 は、構成が要件を満たしている場合に使用します。

手順

a. RcfFileGenerator 1.4a以降を使用して、手順1で取得した情報を使用してRCFファイルを作成します。RcfFileGeneratorの新しいバージョンでは、CleanUpFilesのセットが追加されています。このセットを使用して、いくつかの設定を元に戻し、スイッチで新しいRCF設定を適用する準備をすることができます。

b. banner motdを、現在適用されているRCFファイルと比較します。プラットフォームタイプ、スイッチタイプ、ポート、およびVLANの使用方法は同じである必要があります。

RCFファイルと同じバージョンのCleanUpFilesを使用し、まったく同じ設定を行う必要があります。CleanUpFileを使用しても機能せず、スイッチの完全なリセットが必要になる場合があります。

用に作成したONTAP のバージョンは関係ありません。RCFファイルのバージョンのみが重要です。

RCFファイルには、同じバージョンのものも含まれており、プラットフォームの数が少ない場合もあればそれよりも多い場合もあります。プラットフォームがリストに表示されていることを確認します。

オプション**2**：一般的な**CleanUpFiles**を作成します

この手順 は、構成が*一部の要件を満たしていない場合に使用してください。

手順

a. 各スイッチから「show running-config」の出力を取得します。

b. RcfFileGeneratorツールを開き、ウィンドウの下部にある「Create generic CleanUpFiles」をクリックします

c. 手順1で取得した出力を「1」スイッチから上のウィンドウにコピーします。デフォルトの出力は削除することもそのまま使用することもできます。

d. 'CUFファイルの作成'をクリックします。

e. 下のウィンドウの出力をテキストファイルにコピーします（このファイルはCleanUpFileです）。

f. 構成内のすべてのスイッチについて、手順c、d、eを繰り返します。

この手順 の最後に、スイッチごとに1つずつ、合計4つのテキストファイルが必要です。これらのファイルは、オプション1を使用して作成できるCleanUpFilesと同じ方法で使用できます。

3. [[new-RCF -files-ing-new-configuration]]新しい設定用の「新しい」RCFファイルを作成します。前の手順で作成したファイルと同じ方法でこれらのファイルを作成します。ただし、ONTAP とRCFのそれぞれのファイルバージョンを選択してください。

この手順の完了後、それぞれ12個のファイルで構成される2セットのRCFファイルを用意する必要があり

ます。

4. ブートフラッシュにファイルをダウンロードします。

   a. で作成したCleanUpFilesをダウンロードします RCFファイルとCleanUpFilesを作成するか、現在の設定用の汎用CleanUpFilesを作成します

      このCleanUpFileは、適用されている現在のRCFファイル用であり、アップグレード先の新しいRCF用には*ありません。

      Switch-A1のCleanUpFileの例:'Cleanup_NX9336_v1.81_Switch-A1.txt

   b. で作成した新しいRCFファイルをダウンロードします 新しい構成用に「新しい」RCFファイルを作成します。

      Switch-A1のRCFファイルの例: NX9336_v1.90_Switch-A1.txt

   c. で作成したCleanUpFilesをダウンロードします 新しい構成用に「新しい」RCFファイルを作成します。 この手順はオプションです。あとでこのファイルを使用して、スイッチの設定を更新できます。現在適用されている設定に一致します。

      Switch-A1のCleanUpFileの例:'Cleanup_NX9336_v1.90_Switch-A1.txt

      正しい（一致する）RCFバージョンには、CleanUpFileを使用する必要があります。異なるRCFバージョンまたは別の設定に対してCleanUpFileを使用すると、設定のクリーンアップが正しく機能しない可能性があります。

      次に、3つのファイルをブートフラッシュにコピーする例を示します。

```
IP_switch_A_1# copy sftp://user@50.50.50.50/RcfFiles/NX9336-direct-
SAS_v1.81_MetroCluster-
IP_L2Direct_A400FAS8700_xxx_xxx_xxx_xxx/Cleanup_NX9336_v1.81_Switch-
A1.txt bootflash:
IP_switch_A_1# copy sftp://user@50.50.50.50/RcfFiles/NX9336-direct-
SAS_v1.90_MetroCluster-
IP_L2Direct_A400FAS8700A900FAS9500_xxx_xxx_xxx_xxxNX9336_v1.90//NX9336_v
1.90_Switch-A1.txt bootflash:
IP_switch_A_1# copy sftp://user@50.50.50.50/RcfFiles/NX9336-direct-
SAS_v1.90_MetroCluster-
IP_L2Direct_A400FAS8700A900FAS9500_xxx_xxx_xxx_xxxNX9336_v1.90//Cleanup_
NX9336_v1.90_Switch-A1.txt bootflash:
```

+

   Virtual Routing and Forwarding（VRF；仮想ルーティング転送）を指定するように求められます。

5. CleanUpFileまたはGeneric CleanUpFileを適用します。

一部の設定はリバートされ、スイッチポートは「オフライン」になります。

a. スタートアップコンフィギュレーションに保留中の変更がないことを確認します。「show running-config diff」

```
IP_switch_A_1# show running-config diff
IP_switch_A_1#
```

6. システム出力が表示された場合は、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保存します

> システム出力は、スタートアップコンフィギュレーションと実行コンフィギュレーションが異なること、および保留中の変更であることを示します。保留中の変更を保存しないと、スイッチのリロードを使用してロールバックできません。

a. CleanUpFileを適用します。

```
IP_switch_A_1# copy bootflash:Cleanup_NX9336_v1.81_Switch-A1.txt
running-config

IP_switch_A_1#
```

> スイッチのプロンプトに戻るまでに時間がかかることがあります。出力は想定されません。

7. 実行コンフィギュレーションを表示して、コンフィギュレーションがクリアされたことを確認します。「show running-config」

現在の設定は次のように表示されます。

- クラスマップとIPアクセスリストは設定されていません
- ポリシーマップは設定されません
- サービスポリシーが設定されていません
- ポートプロファイルが設定されていません
- すべてのイーサネットインターフェイス（mgmt0を除くすべての構成を表示しないでください。VLAN 1だけを設定してください）。

  上記のいずれかが設定されている場合は、新しいRCFファイルの設定を適用できない可能性があります。ただし、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保存せずにスイッチ*をリロードすることで、以前のコンフィギュレーションに戻すことができます。スイッチは、以前の設定で起動します。

8. RCFファイルを適用してポートがオンラインであることを確認します。

a. RCFファイルを適用します。

```
IP_switch_A_1# copy bootflash:NX9336_v1.90-X2_Switch-A1.txt running-
config
```

設定の適用中にいくつかの警告メッセージが表示されます。通常、エラーメッセージは予期されません。ただし、SSHを使用してログインすると、次のエラーが表示されることがあります。 `Error: Can't disable/re-enable ssh:Current user is logged in through ssh`

b. 設定を適用したら、「show interface brief」、「show cdp neighbors」、「show lldp neighbors」のいずれかのコマンドを使用して、クラスタポートとMetroCluster ポートがオンラインになっていることを確認します

ローカルクラスタのVLANを変更したあとにサイトの最初のスイッチをアップグレードした場合、古い設定と新しい設定のVLANが一致しないため、クラスタヘルスモニタで状態が「正常」と報告されないことがあります。2番目のスイッチが更新されると、状態はhealthyに戻るはずです。

設定が正しく適用されていない場合、または設定を保持しない場合は、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保存せずにスイッチ*をリロードすることで、以前のコンフィギュレーションに戻すことができます。スイッチは、以前の設定で起動します。

9. 設定を保存し、スイッチをリロードします。

```
IP_switch_A_1# copy running-config startup-config

IP_switch_A_1# reload
```

Cisco IP スイッチの名前変更

構成内で一貫性のある名前を使用するために、 Cisco IP スイッチの名前変更が必要になる場合があります。

このタスクについて

- このタスクの例では、スイッチ名が「 m 」から「 ip_switch_a_1 」に変更されています。
- "コンソールログを有効にする" このタスクを実行する前に。

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 * 」

次の例は、構成モードのプロンプトを示しています。どちらのプロンプトにもスイッチ名「 m yswitch 」が表示されています。

```
myswitch# configure terminal
myswitch(config)#
```

2. スイッチの名前を変更します。

   '*switchname new-switch-name *

   ネットワーク内の両方のスイッチの名前を変更する場合は、各スイッチで同じコマンドを使用します。

   CLI プロンプトの内容が新しい名前に変わります。

```
myswitch(config)# switchname IP_switch_A_1
IP_switch_A_1(config)#
```

3. 構成モードを終了します。

   「 * exit *

   最上位のスイッチプロンプトが表示されます。

```
IP_switch_A_1(config)# exit
IP_switch_A_1#
```

4. 現在の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ファイルにコピーします。

   '*copy running-config startup-config *

5. スイッチ名の変更が ONTAP クラスタのプロンプトに表示されることを確認します。

   新しいスイッチ名が表示され、古いスイッチ名（「 m 」スイッチ）は表示されないことに注意してください。

   a. advanced 権限モードに切り替え、プロンプトが表示されたら「 * y * 」を押します。 +`* set -privilege advanced * `
   b. 接続されているデバイスを表示します :+`* network device-discovery show *`
   c. admin 特権モードに戻ります :+**`set -privilege admin`**

      次の例では ' スイッチが新しい名前で表示されていますつまり 'ip_switch_a_1' です

```
cluster_A::storage show> set advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

cluster_A::storage show*> network device-discovery show
Node/       Local  Discovered
Protocol    Port   Device                    Interface         Platform
----------- ------ ------------------------- ----------------
----------------
node_A_2/cdp
            e0M    LF01-410J53.mycompany.com(SAL18516DZY)
                                             Ethernet125/1/28  N9K-
C9372PX
            e1a    IP_switch_A_1(FOC21211RBU)
                                             Ethernet1/2       N3K-
C3232C
            e1b    IP_switch_A_1(FOC21211RBU)
                                             Ethernet1/10      N3K-
C3232C
.
.
.                                             Ethernet1/18      N9K-
C9372PX
node_A_1/cdp
            e0M    LF01-410J53.mycompany.com(SAL18516DZY)
                                             Ethernet125/1/26  N9K-
C9372PX
            e0a    IP_switch_A_2(FOC21211RB5)
                                             Ethernet1/1       N3K-
C3232C
            e0b    IP_switch_A_2(FOC21211RB5)
                                             Ethernet1/9       N3K-
C3232C
            e1a    IP_switch_A_1(FOC21211RBU)
.
.
.
16 entries were displayed.
```

Cisco IPスイッチの**ISL**ポートを無停止で追加、削除、変更

Cisco IPスイッチでISLポートの追加、削除、または変更が必要になる場合がありま

す。Cisco IPスイッチでは、専用ISLポートを共有ISLポートに変換したり、ISLポートの速度を変更したりできます。

このタスクについて

専用の ISL ポートを共有 ISL ポートに変換する場合は、新しいポートがに対応していることを確認してください "共有 ISL ポートの要件"。

ISL 接続を確保するためには、両方のスイッチですべての手順を実行する必要があります。

次の手順では、スイッチポート Eth1/24/1 に接続されている 10Gb ISL を、スイッチポート 17 と 18 に接続されている 2 つの 100Gb ISL に交換します。

> NS224シェルフを接続する共有構成でCisco 9336C-FX2スイッチを使用している場合は、ISLを変更するときに新しいRCFファイルが必要になることがあります。現在のISL速度が40Gbpsおよび100Gbpsの場合は、新しいRCFファイルは必要ありません。ISLの速度に対するその他の変更には、新しいRCFファイルが必要です。たとえば、ISLの速度を40Gbpsから100Gbpsに変更しても新しいRCFファイルは必要ありませんが、ISLの速度を10Gbpsから40Gbpsに変更するには新しいRCFファイルが必要です。

作業を開始する前に

の*スイッチ*セクションを参照してください。 "NetApp Hardware Universe の略" をクリックして、サポートされているトランシーバを確認します。

"コンソールログを有効にする" このタスクを実行する前に。

手順

1. 変更するファブリック内の両方のスイッチで、 ISL の ISL ポートを無効にします。

> 現在の ISL ポートを無効にするのは、ポートを別のポートに移動している場合や ISL の速度が変更されている場合だけです。既存の ISL と同じ速度の ISL ポートを追加する場合は、手順 3 に進みます。

次の例に示すように、設定コマンドを 1 行に 1 つ入力し、すべてのコマンドを入力したら Ctrl+Z キーを押す必要があります。

```
switch_A_1# conf t
switch_A_1(config)# int eth1/24/1
switch_A_1(config-if)# shut
switch_A_1(config-if)#
switch_A_1#

switch_B_1# conf t
switch_B_1(config)# int eth1/24/1
switch_B_1(config-if)# shut
switch_B_1(config-if)#
switch_B_1#
```

2. 既存のケーブルとトランシーバを取り外します。
3. 必要に応じて ISL ポートを変更します。

> NS224シェルフを接続する共有構成でCisco 9336C-FX2スイッチを使用していて、RCFファイルをアップグレードして新しいISLポートに新しい構成を適用する必要がある場合は、次の手順を実行します。 "MetroCluster IPスイッチでRCFファイルをアップグレードします。"

オプション	ステップ
ISL ポートの速度を変更する	速度に応じて、新しい ISL を指定のポートにケーブル接続します。使用しているスイッチの ISL ポートが MetroCluster IP インストールおよび設定に表示されていることを確認する必要があります。
ISL を追加する	ISL ポートとして追加するポートに QFSP を挿入します。MetroCluster IP のインストールと設定に表示されていることを確認し、それに応じてケーブルを接続します。

4. ファブリック内の両方のスイッチですべての ISL ポートを有効にします（有効になっていない場合）。最初に次のコマンドを入力します。

   'switch_A_1# conf t`

   設定コマンドを 1 行に 1 つ入力し、すべてのコマンドを入力したら Ctrl+Z キーを押す必要があります。

```
switch_A_1# conf t
switch_A_1(config)# int eth1/17
switch_A_1(config-if)# no shut
switch_A_1(config-if)# int eth1/18
switch_A_1(config-if)# no shut
switch_A_1(config-if)#
switch_A_1#
switch_A_1# copy running-config startup-config

switch_B_1# conf t
switch_B_1(config)# int eth1/17
switch_B_1(config-if)# no shut
switch_B_1(config-if)# int eth1/18
switch_B_1(config-if)# no shut
switch_B_1(config-if)#
switch_B_1#
switch_B_1# copy running-config startup-config
```

5. 両方のスイッチ間にISLとポートチャネルが確立されていることを確認します。

```
switch_A_1# show int brief
```

次の例に示すように、 ISL インターフェイスがコマンド出力に表示されます。

```
Switch_A_1# show interface brief
--------------------------------------------------------------------------------
--------
Ethernet        VLAN    Type Mode   Status  Reason                   Speed
Port
Interface
Ch #
--------------------------------------------------------------------------------
--------
Eth1/17         1       eth  access down    XCVR not inserted
auto(D) --
Eth1/18         1       eth  access down    XCVR not inserted
auto(D) --

--------------------------------------------------------------------------------
------------------
Port-channel VLAN    Type Mode   Status  Reason
Speed   Protocol
Interface
--------------------------------------------------------------------------------
------------------
Po10         1       eth  trunk  up      none
a-100G(D)  lacp
Po11         1       eth  trunk  up      none
a-100G(D)  lacp
```

6. ファブリック 2 についても手順を繰り返します。

MetroCluster IP 構成でのストレージの特定

ドライブまたはシェルフモジュールを交換する必要がある場合、まずその場所を特定する必要があります。

ローカルシェルフとリモートシェルフの ID

MetroCluster サイトのシェルフ情報を表示する場合、すべてのリモートドライブは 0m 、仮想 iSCSI ホストアダプタです。つまり、ドライブは MetroCluster IP インターフェイス経由でアクセスされます。それ以外のドライブはすべてローカルです。

シェルフがリモート（ 0m 上）かどうかを特定したら、シリアル番号、または構成でのシェルフ ID の割り当てによってはシェルフ ID で、ドライブまたはシェルフを詳細に特定できます。

ONTAP 9.4 を実行する MetroCluster IP 構成では、 MetroCluster サイト間でシェルフ ID を一意にする必要はありません。これには内蔵シェルフ（ 0 ）と外付けシェルフの両方が含まれます。シリアル番号は、どちらの MetroCluster サイトのどのノードから見ても変わりません。

シェルフ ID は、内蔵シェルフを除き、ディザスタリカバリ（ DR ）グループ内で一意である必要があります。

ドライブまたはシェルフモジュールを特定したら、該当する手順を使用してコンポーネントを交換できます。

"DS460C 、 DS224C 、 DS212C ディスクシェルフを保守します"

sysconfig -a の出力例

次に、「 sysconfig -a 」コマンドを使用して、 MetroCluster IP 構成のノード上のデバイスを表示する例を示します。このノードには次のシェルフとデバイスが接続されています。

- スロット 0 ：内蔵ドライブ（ローカルドライブ）
- スロット 3 ：外部シェルフ ID 75 および 76 （ローカルドライブ）
- スロット 0 ：仮想 iSCSI ホストアダプタ 0m （リモートドライブ）

```
node_A_1> run local sysconfig -a

NetApp Release R9.4:  Sun Mar 18 04:14:58 PDT 2018
System ID: 1111111111 (node_A_1); partner ID: 2222222222 (node_A_2)
System Serial Number: serial-number (node_A_1)
.
.
.
slot 0: NVMe Disks
                0    : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500528)
                1    : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500735)
                2    : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J501165)
.
.
.
slot 3: SAS Host Adapter 3a (PMC-Sierra PM8072 rev. C, SAS, <UP>)
MFG Part Number:    Microsemi Corp. 110-03801 rev. A0
Part number:        111-03801+A0
Serial number:      7A1063AF14B
Date Code:          20170320
Firmware rev:       03.08.09.00
Base WWN:           5:0000d1:702e69e:80
Phy State:          [12] Enabled, 12.0 Gb/s
                    [13] Enabled, 12.0 Gb/s
```

```
                    [14] Enabled, 12.0 Gb/s
                    [15] Enabled, 12.0 Gb/s
Mini-SAS HD Vendor:        Molex Inc.
Mini-SAS HD Part Number:   112-00436+A0
Mini-SAS HD Type:          Passive Copper (unequalized) 0.5m ID:00
Mini-SAS HD Serial Number: 614130640
                75.0 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG501805)
                75.1 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG502050)
                75.2 : NETAPP   X438_PHM2400MCTO NA04 381.3GB 520B/sect
(25M0A03WT2KA)
                75.3 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG501793)
                75.4 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG502158)
.
.
.

Shelf 75: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220
Shelf 76: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220

slot 3: SAS Host Adapter 3c (PMC-Sierra PM8072 rev. C, SAS, <UP>)
MFG Part Number:    Microsemi Corp. 110-03801 rev. A0
Part number:        111-03801+A0
Serial number:      7A1063AF14B
Date Code:          20170320
Firmware rev:       03.08.09.00
Base WWN:           5:0000d1:702e69e:88
Phy State:          [0] Enabled, 12.0 Gb/s
                    [1] Enabled, 12.0 Gb/s
                    [2] Enabled, 12.0 Gb/s
                    [3] Enabled, 12.0 Gb/s
Mini-SAS HD Vendor:        Molex Inc.
Mini-SAS HD Part Number:   112-00436+A0
Mini-SAS HD Type:          Passive Copper (unequalized) 0.5m ID:00
Mini-SAS HD Serial Number: 614130691
                75.0 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG501805)
                75.1 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG502050)
                75.2 : NETAPP   X438_PHM2400MCTO NA04 381.3GB 520B/sect
(25M0A03WT2KA)
                75.3 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG501793)
```

```
.
.
.
Shelf 75: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220
Shelf 76: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220

slot 3: SAS Host Adapter 3d (PMC-Sierra PM8072 rev. C, SAS, <UP>)
MFG Part Number:    Microsemi Corp. 110-03801 rev. A0
Part number:        111-03801+A0
Serial number:      7A1063AF14B
Date Code:          20170320
Firmware rev:       03.08.09.00
Base WWN:           5:0000d1:702e69e:8c
Phy State:          [4] Enabled, 12.0 Gb/s
                    [5] Enabled, 12.0 Gb/s
                    [6] Enabled, 12.0 Gb/s
                    [7] Enabled, 12.0 Gb/s
Mini-SAS HD Vendor:        Molex Inc.
Mini-SAS HD Part Number:   112-00436+A0
Mini-SAS HD Type:          Passive Copper (unequalized) 0.5m ID:01
Mini-SAS HD Serial Number: 614130690
                75.0 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG501805)
                75.1 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG502050)
                75.2 : NETAPP   X438_PHM2400MCTO NA04 381.3GB 520B/sect
(25M0A03WT2KA)
.
.
.
Shelf 75: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220
Shelf 76: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220

slot 4: Quad 10 Gigabit Ethernet Controller X710 SFP+
.
.
.
slot 0: Virtual iSCSI Host Adapter 0m
                0.0  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500690)
                0.1  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500571)
                0.2  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500323)
                0.3  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500724)
```

```
                0.4  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500734)
                0.5  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500598)
                0.12 : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J501094)
                0.13 : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500519)
.
.
.
Shelf 0: FS4483PSM3E  Firmware rev. PSM3E A: 0103  PSM3E B: 0103
Shelf 35: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220
Shelf 36: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220

node_A_1::>
```

共有ストレージ **MetroCluster** スイッチを使用した **MetroCluster IP** へのシェルフの追加

共有ストレージ MetroCluster スイッチを使用して、 NS224 シェルフを MetroCluster に追加する必要がある場合があります。

ONTAP 9.10.1 以降では、共有のストレージ / MetroCluster スイッチを使用して、 MetroCluster から NS224 シェルフを追加できます。シェルフは一度に複数追加できます。

作業を開始する前に

- ノードで ONTAP 9.9.1 以降が実行されている必要があります。
- 現在接続されているすべての NS224 シェルフは、 MetroCluster と同じスイッチに接続する必要があります（共有ストレージ / MetroCluster スイッチ構成）。
- この手順を使用して、専用のイーサネットスイッチに接続された NS224 シェルフまたは NS224 シェルフを使用する構成を、共有ストレージ / MetroCluster スイッチを使用して構成に変換することはできません。
- "コンソールログを有効にする" このタスクを実行する前に。

カスタム **AutoSupport** メッセージをメンテナンス前に送信する

メンテナンスを実行する前に、 AutoSupport an 問題 message to notify NetApp technical support that maintenance is maintenancing （メンテナンスが進行中であることをネットアップテクニカルサポートに通知する）を実行システム停止が発生したとみなしてテクニカルサポートがケースをオープンしないように、メンテナンスが進行中であることを通知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 サイトごとに実行する必要があります。

手順

1. サポートケースが自動で生成されないようにするには、アップグレードが進行中であることを示す AutoSupport メッセージを送信します。

   a. 次のコマンドを問題に設定します。

      「 system node AutoSupport invoke -node * -type all -message 」 MAINT=10h NS224 シェルフの追加または削除中」に進みます

      この例では、 10 時間のメンテナンス時間を指定しています。プランによっては、さらに時間をかけたい場合もあります。

      この時間が経過する前にメンテナンスが完了した場合は、メンテナンス期間が終了したことを通知する AutoSupport メッセージを起動できます。

   「 system node AutoSupport invoke -node * -type all -message MAINT= end 」というメッセージが表示されます

   a. パートナークラスタに対してこのコマンドを繰り返します。

MetroCluster 構成の健全性の確認

移行を実行する前に、 MetroCluster 構成の健全性と接続を確認する必要があります。

手順

1. ONTAP で MetroCluster 構成の動作を確認します。

   a. システムがマルチパスかどうかを確認します。

      'node run -node _node-name_sysconfig -a

   b. ヘルスアラートがないかどうかを両方のクラスタで確認します。

      「 system health alert show 」というメッセージが表示されます

   c. MetroCluster 構成と運用モードが正常な状態であることを確認します。

      「 MetroCluster show 」

   d. MetroCluster チェックを実行します。

      「 MetroCluster check run 」のようになります

   e. MetroCluster チェックの結果を表示します。

      MetroCluster チェックショー

   f. Config Advisor を実行します。

      "ネットアップのダウンロード： Config Advisor"

   g. Config Advisor の実行後、ツールの出力を確認し、推奨される方法で検出された問題に対処します。

2. クラスタが正常であることを確認します。

cluster show -vserver Cluster

```
cluster_A::> cluster show -vserver Cluster
Node            Health  Eligibility   Epsilon
--------------- ------  -----------   -------
node_A_1    true    true          false
node_A_2    true    true          false

cluster_A::>
```

3. すべてのクラスタポートが動作していることを確認します。

「 network port show -ipspace cluster 」のように表示されます

```
cluster_A::> network port show -ipspace cluster

Node: node_A_1-old

                                                  Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

Node: node_A_2-old

                                                  Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

4 entries were displayed.

cluster_A::>
```

4. すべてのクラスタ LIF が動作していることを確認します。

「 network interface show -vserver Cluster 」のように表示されます

各クラスタ LIF で、 Is Home には true 、 Status Admin/Oper には up/up と表示されるはずです

```
cluster_A::> network interface show -vserver cluster

            Logical      Status     Network          Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- -----
Cluster
            node_A_1-old_clus1
                       up/up      169.254.209.69/16  node_A_1   e0a
true
            node_A_1-old_clus2
                       up/up      169.254.49.125/16  node_A_1   e0b
true
            node_A_2-old_clus1
                       up/up      169.254.47.194/16  node_A_2   e0a
true
            node_A_2-old_clus2
                       up/up      169.254.19.183/16  node_A_2   e0b
true

4 entries were displayed.

cluster_A::>
```

5. すべてのクラスタ LIF で自動リバートが有効になっていることを確認します。

   network interface show -vserver Cluster -fields auto-revert を実行します

```
cluster_A::> network interface show -vserver Cluster -fields auto-revert

          Logical
Vserver   Interface     Auto-revert
--------- ------------- ------------
Cluster
           node_A_1-old_clus1
                        true
           node_A_1-old_clus2
                        true
           node_A_2-old_clus1
                        true
           node_A_2-old_clus2
                        true

    4 entries were displayed.

cluster_A::>
```

新しい **RCF** ファイルをスイッチに適用しています

> スイッチがすでに正しく設定されている場合は、以降のセクションを省略して、に直接進むことができます Cisco 9336C スイッチでの MACsec 暗号化の設定（該当する場合）またはに移動します 新しい NS224 シェルフを接続します。

- シェルフを追加するには、スイッチの構成を変更する必要があります。
- ケーブル接続の詳細については、を参照してください "プラットフォームポートの割り当て"。
- 構成に合わせて RCF ファイルを作成するには、 **RcfFileGenerator** ツールを使用する必要があります。。 "RcfFileGenerator の順にクリックします" また、各スイッチのポートごとのケーブル接続の概要についても説明します。正しいシェルフ数を選択していることを確認してください。RCF ファイルと一緒に追加ファイルが作成され、特定のオプションに一致する詳細なケーブルレイアウトが提供されます。新しいシェルフをケーブル接続する際には、この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 IP スイッチでの **RCF** ファイルのアップグレード

新しいスイッチファームウェアをインストールする場合は、 RCF ファイルをアップグレードする前にスイッチファームウェアをインストールする必要があります。

この手順では、 RCF ファイルをアップグレードするスイッチ上のトラフィックが中断されます。新しい RCF ファイルが適用されると、トラフィックは再開されます。

手順

1. 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 * 」のようになります

```
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. MetroCluster check run オペレーションが完了したら ' MetroCluster check show を実行して結果を表示します

約 5 分後に、次の結果が表示されます。

```
-----------
::*> metrocluster check show

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         not-applicable
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するには、次のコマンドを使用します。 +* `MetroCluster operation history show -job-id 38*`

b. ヘルス・アラートがないことを確認します +* `system health alert show *`

2. 新しい RCF ファイルを適用するための IP スイッチを準備します。

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

新しいバージョンのソフトウェアと RCF をインストールする前に、 Cisco スイッチの設定を消去し、基本的な設定を完了する必要があります。

この手順は、 MetroCluster IP 構成の各 IP スイッチで実行する必要があります。

1. スイッチを工場出荷時のデフォルトにリセットします。

a. 既存の設定を消去します。「 write erase 」

b. スイッチソフトウェアをリロードします

システムがリブートし、設定ウィザードが表示されます。起動中に、 Abort Auto Provisioning （自動プロビジョニングの中止）というプロンプトが表示され、通常のセットアップを続行する場合（ yes/no ） [n] 、「 yes 」と入力して続行します。

c. 設定ウィザードで、スイッチの基本設定を入力します。

- 管理パスワード
- スイッチ名
- アウトオブバンド管理設定
- デフォルトゲートウェイ
- SSH サービス（ 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。

```
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。

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"

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.I4.6.bin ファイルを 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しています。

```
IP_switch_A_1# copy sftp://root@10.10.99.99/tftpboot/nxos.7.0.3.I4.6.bin
bootflash: vrf management
root@10.10.99.99's password: password
sftp> progress
Progress meter enabled
sftp> get   /tftpboot/nxos.7.0.3.I4.6.bin
/bootflash/nxos.7.0.3.I4.6.bin
Fetching /tftpboot/nxos.7.0.3.I4.6.bin to /bootflash/nxos.7.0.3.I4.6.bin
/tftpboot/nxos.7.0.3.I4.6.bin                 100%  666MB   7.2MB/s
01:32
sftp> exit
Copy complete, now saving to disk (please wait)...
```

3. 各スイッチの bootflash: `d IR bootflash: ` に、スイッチの NX-OS ファイルが存在することを各スイッチで確認します

   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。“ install all nxos bootflash:nxos.version-number.bin “

   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 : 'how 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. 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 9336C スイッチでの **MACsec** 暗号化の設定

必要に応じて、サイト間で実行される WAN ISL ポートに MACsec 暗号化を設定できます。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 暗号化は、 WAN ISL ポートにのみ適用できます。

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 構成での Cisco MACsec 暗号化 WAN ISL のイネーブル化

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。

1. グローバルコンフィギュレーションモード「 configure terminal 」を入力します

```
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

```
IP_switch_A_1(config)# copy running-config startup-config
```

Cisco MACsec Encryption 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。

暗号化を無効にする場合は、キーも削除する必要があります。

1. グローバルコンフィギュレーションモード「 configure terminal 」を入力します

```
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 」

```
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、ポリシー、およびフォールバックキーチェーンを削除して、 MACsec 設定を削除します。「 no MACsec keychain -name policy -name fallback-keychain keychain -name 」

   ```
   IP_switch_A_1(config-if)# no macsec keychain kc2 policy abc fallback-
   keychain fb_kc2
   ```

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

   ```
   IP_switch_A_1(config)# copy running-config startup-config
   ```

MACsec キーチェーンおよびキーの設定

MACsec キーチェーンの設定の詳細については、ご使用のスイッチのシスコのマニュアルを参照してください。

新しい NS224 シェルフを接続します

手順

1. キットに付属のパンフレットに従って、シェルフに付属のレールマウントキットを取り付けます。
2. パンフレットに従って、サポートブラケットとラックまたはキャビネットにシェルフを設置して固定します。
3. 電源コードをシェルフに接続し、電源コード固定クリップで固定してから、耐障害性を確保するために別々の電源に接続します。

   電源に接続するとシェルフの電源がオンになり、電源スイッチはありません。電源装置が正常に動作している場合は、 LED が緑色に点灯します。

4. シェルフ ID は、 HA ペア内および構成全体で一意の番号に設定します。
5. シェルフポートは次の順序で接続します。
   a. SMA-A 、 e0a をスイッチ（ Switch-A1 または Switch-B1 ）に接続します。
   b. NSM-B 、 e0a をスイッチ（ Switch-A2 または Switch-B2 ）に接続します。
   c. NSM-A’e0b をスイッチ（ Switch-A1 または Switch-B1 ）に接続します

d. NSM-B 、 e0b をスイッチ（ Switch-A2 または Switch-B2 ）に接続します。

6. **RcfFileGenerator** ツールで生成されたケーブルレイアウトを使用して、シェルフを適切なポートにケーブル接続します。

   新しいシェルフが正しくケーブル接続されると、 ONTAP はそのシェルフをネットワーク上で自動的に検出します。

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	• AFF A800、AFF C800 • AFF A20、 AFF A30、 AFF C30、 AFF A50、 AFF C60 • AFF A70、 AFF A90、 AFF A1K、 AFF C80 • FAS50、FAS70、FAS90
ONTAP 9.15.1	• AFF A400 • AFF C400用 • FAS8300 • FAS8700 の場合

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

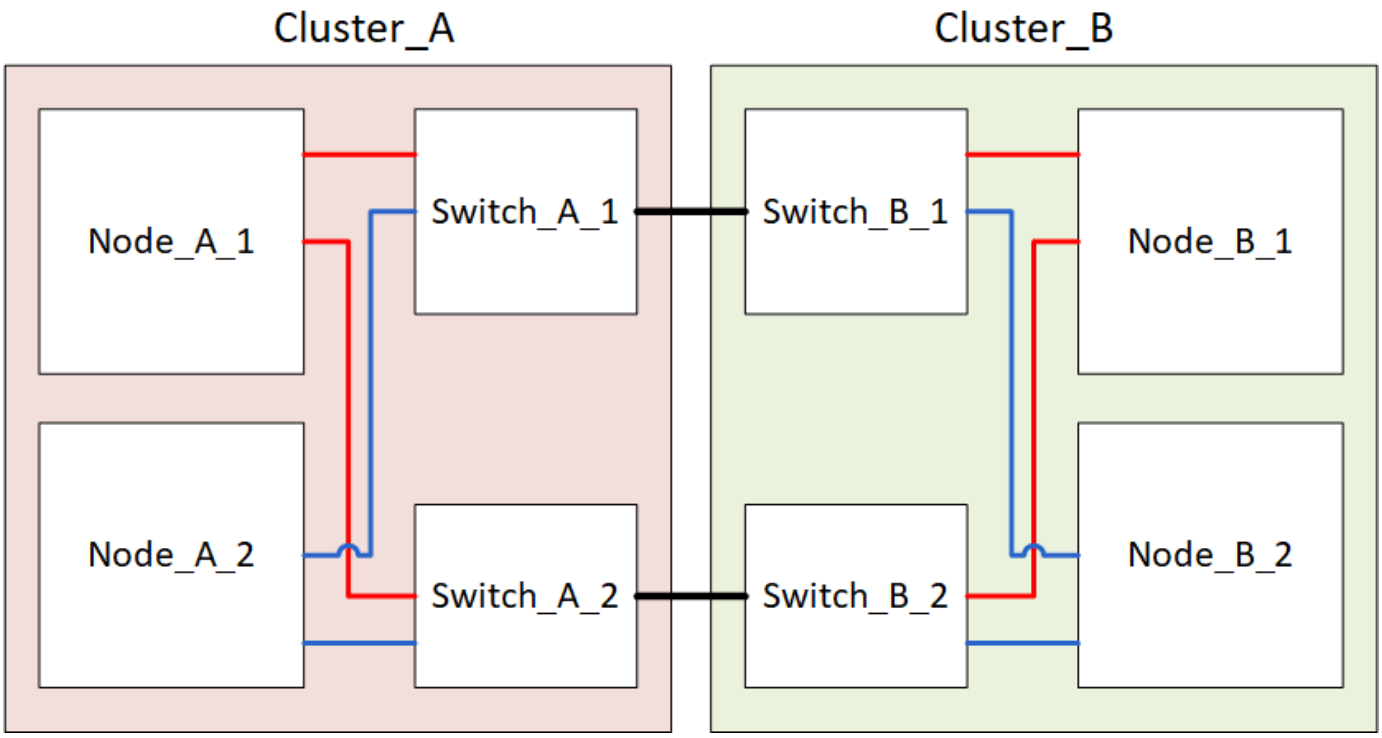
dr-group-id cluster    node      configuration-state is-encryption-
enabled
----------- ---------- --------  ------------------- -----------------
1           cluster_A  node_A_1  configured          false
1           cluster_A  node_A_2  configured          false
1           cluster_B  node_B_1  configured          false
1           cluster_B  node_B_2  configured          false
4 entries were displayed.
```

MetroCluster IP構成での単一サイトの電源オフと電源オン

MetroCluster IP構成でサイトのメンテナンスを実施したり、単一サイトを再配置したりする必要がある場合は、サイトの電源をオフにしてオンにする方法を把握しておく必要があります。

サイトを再配置して再設定する必要がある場合（4ノードクラスタから8ノードクラスタに拡張する必要がある場合など）は、これらのタスクを同時に実行することはできません。この手順では、サイトのメンテナンスを実行するため、またはサイトの構成を変更せずにサイトを再配置するために必要な手順のみを説明します。

次の図は、 MetroCluster 構成を示しています。メンテナンスのためにcluster_Bの電源がオフになっています。



MetroClusterサイトの電源をオフにする

サイトのメンテナンスや再配置を開始する前に、サイトとすべての機器の電源をオフにする必要があります。

このタスクについて

次の手順のすべてのコマンドは、電源をオンにしたままのサイトから実行されます。

手順

1. 開始する前に、ミラーされていないアグリゲートがサイトですべてオフラインになっていることを確認します。
2. ONTAP で MetroCluster 構成の動作を確認します。
   a. システムがマルチパスかどうかを確認します。

      'node run -node _node-name_sysconfig -a

   b. ヘルスアラートがないかどうかを両方のクラスタで確認します。

      「 system health alert show 」というメッセージが表示されます

   c. MetroCluster 構成と運用モードが正常な状態であることを確認します。

      「 MetroCluster show 」

   d. MetroCluster チェックを実行します + MetroCluster チェックを実行します
   e. MetroCluster チェックの結果を表示します。

      MetroCluster チェックショー

f. スイッチにヘルスアラートがないかどうかを確認します（ある場合）。

「 storage switch show 」と表示されます

g. Config Advisor を実行します。

"ネットアップのダウンロード： Config Advisor"

h. Config Advisor の実行後、ツールの出力を確認し、推奨される方法で検出された問題に対処します。

3. 稼働したままにするサイトから、スイッチオーバーを実施します。

MetroCluster スイッチオーバー

```
cluster_A::*> metrocluster switchover
```

この処理が完了するまでに数分かかることがあります。

4. スイッチオーバーの完了を監視して確認します。

「 MetroCluster operation show 」を参照してください

```
cluster_A::*> metrocluster operation show
  Operation: Switchover
 Start time: 10/4/2012 19:04:13
State: in-progress
   End time: -
     Errors:

cluster_A::*> metrocluster operation show
  Operation: Switchover
 Start time: 10/4/2012 19:04:13
      State: successful
   End time: 10/4/2012 19:04:22
     Errors: -
```

5. ONTAP 9.6 以降を実行している MetroCluster IP 構成がある場合は、ディザスタサイトのプレックスがオンラインになり、修復処理が自動的に完了するまで待ちます。

ONTAP 9.5以前を実行しているMetroCluster IP構成では、ディザスタサイトのノードはONTAPで自動的にブートせず、プレックスはオフラインのままです。

6. ミラーされていないアグリゲートに属するボリュームとLUNをすべてオフラインにします。

a. ボリュームをオフラインにします。

```
cluster_A::* volume offline <volume name>
```

b. LUNをオフラインにします。

```
cluster_A::* lun offline lun_path <lun_path>
```

7. ミラーされていないアグリゲートをオフラインにします：「storage aggregate offline

```
cluster_A*::> storage aggregate offline -aggregate <aggregate-name>
```

8. 構成と ONTAP のバージョンに応じて、ディザスタサイト（ cluster_B ）にあるオフラインの影響を受けるプレックスを特定して移動します。

   次のプレックスをオフラインにする必要があります。

   ◦ ディザスタサイトにあるディスクにあるミラーリングされていないプレックス

     ディザスタサイトのミラーされていないプレックスをオフラインにしないと、あとでディザスタサイトの電源をオフにしたときにシステムが停止する可能性があります。

   ◦ ディザスタサイトのディスクにあるミラーされたプレックスを使用してアグリゲートをミラーリングする。オフラインにすると、プレックスにアクセスできなくなります。

   a. 影響を受けるプレックスを特定します。

      サバイバーサイトのノードが所有するプレックスは、プール 1 のディスクで構成されます。ディザスタサイトのノードが所有するプレックスは、プール 0 のディスクで構成されます。

```
Cluster_A::> storage aggregate plex show -fields aggregate,status,is-
online,Plex,pool
aggregate    plex  status        is-online pool
------------ ----- ------------- --------- ----
Node_B_1_aggr0 plex0 normal,active true     0
Node_B_1_aggr0 plex1 normal,active true     1

Node_B_2_aggr0 plex0 normal,active true     0
Node_B_2_aggr0 plex5 normal,active true     1

Node_B_1_aggr1 plex0 normal,active true     0
Node_B_1_aggr1 plex3 normal,active true     1

Node_B_2_aggr1 plex0 normal,active true     0
Node_B_2_aggr1 plex1 normal,active true     1

Node_A_1_aggr0 plex0 normal,active true     0
Node_A_1_aggr0 plex4 normal,active true     1

Node_A_1_aggr1 plex0 normal,active true     0
Node_A_1_aggr1 plex1 normal,active true     1

Node_A_2_aggr0 plex0 normal,active true     0
Node_A_2_aggr0 plex4 normal,active true     1

Node_A_2_aggr1 plex0 normal,active true     0
Node_A_2_aggr1 plex1 normal,active true     1
14 entries were displayed.

Cluster_A::>
```

影響を受けるプレックスは、クラスタ A のリモートにあるプレックスです次の表に、ディスクがクラスタ A に対してローカルかリモートかを示します。

ノード	プール内のディスク	ディスクをオフラインにする必要があるか	オフラインにするプレックスの例を指定します
Node_a_1 および Node_a_2	プール 0 内のディスク	いいえディスクはクラスタ A に対してローカルです	-

プール 1 内のディスク	はい。ディスクはクラスタ A に対してリモートです	node_A_1 の aggr0 / プレックス 4 を使用します node_A_1 の aggr1 / plex1 node_a_2_aggr0/plex4 Node_a_2_aggr1 / plex1 です	Node_B_1 および Node_B_2
プール 0 内のディスク	はい。ディスクはクラスタ A に対してリモートです	node_B_1 の aggr1 / plex0 node_B_1 の aggr0/plex0 node_B_2 の aggr0 / plex0 node_B_2 の aggr1 / plex0	プール 1 内のディスク

b. 影響を受けるプレックスをオフラインにします。

「ストレージアグリゲートのプレックスはオフライン」です

```
storage aggregate plex offline -aggregate Node_B_1_aggr0 -plex plex0
```

+

> この手順は、Cluster_Aに対してリモートのディスクを含むすべてのプレックスに対して実行します。

9. スイッチタイプに応じて、ISLスイッチポートを永続的にオフラインにします。
10. 各ノードで次のコマンドを実行して、ノードを停止します。

```
node halt -inhibit-takeover true -skip-lif-migration true -node <node-name>
```

11. ディザスタサイトの機器の電源をオフにします。

次の機器の電源を、記載されている順序でオフにする必要があります。

- ストレージコントローラ-ストレージコントローラは現在、 `LOADER` プロンプトが表示されたら、電源を完全にオフにする必要があります。
- MetroCluster IP スイッチ
- ストレージシェルフ

電源がオフになっている **MetroCluster** サイトの再配置

サイトの電源をオフにしたら、メンテナンス作業を開始できます。手順は、 MetroCluster コンポーネントを同じデータセンター内で再配置する場合も、別のデータセンターに再配置する場合も同じです。

- ハードウェアは、前のサイトと同じ方法でケーブル接続する必要があります。
- スイッチ間リンク（ ISL ）の速度、長さ、または数が変わった場合は、すべて再設定する必要があります。

手順

1. 新しい場所で正しく再接続できるように、すべてのコンポーネントのケーブル配線が慎重に記録されていることを確認します。
2. すべてのハードウェア、ストレージ コントローラ、IP スイッチ、およびストレージ シェルフを物理的に再配置します。
3. ISL ポートを設定し、サイト間接続を確認します。
   a. IPスイッチの電源をオンにします。

      他の機器の電源はオンにしないでください。

4. スイッチのツールを使用して（使用可能な場合）、サイト間接続を確認します。

   リンクが正しく設定され、安定している場合にのみ続行してください。

5. リンクが安定していることがわかった場合は、リンクを再度無効にします。

MetroCluster 構成の電源をオンにして通常動作に戻します

メンテナンスを完了、またはサイトを移動したら、サイトの電源をオンにして MetroCluster 構成を再確立する必要があります。

このタスクについて

次の手順のすべてのコマンドは、電源をオンにしたサイトから実行します。

手順

1. スイッチの電源をオンにします。

   最初にスイッチの電源をオンにする必要があります。サイトを再配置した場合は、前の手順で電源がオンになっている可能性があります。

   a. 必要に応じて、または再配置中に実行されていない場合は、スイッチ間リンク（ ISL ）を再設定します。
   b. フェンシングが完了した場合、 ISL を有効にします。
   c. ISL を確認します。
2. ストレージコントローラの電源をオンにし、 `LOADER` プロンプト。コントローラが完全にブートしないようにする必要があります。

   自動起動が有効になっている場合は、 `Ctrl+C` コントローラの自動ブートを停止します。

   コントローラの電源を入れる前にシェルフの電源を入れないでください。これにより、コントローラが意図しないONTAPでブートされるのを防ぐことができます。

3. シェルフの電源をオンにし、電源が完全にオンになるまで十分な時間を確保します。
4. メンテナンス モードからストレージが表示可能であることを確認します。
   a. メンテナンス モードで起動します。

      「 boot_ontap maint 」を使用してください

   b. 残存サイトからストレージが見えることを確認します。
   c. メンテナンス モードのノードからローカル ストレージとリモート ストレージが表示されていることを確認します：

      「ディスクショー V 」

5. ノードを停止します。

   「 halt 」

6. MetroCluster 構成を再確立します。

   の手順に従います "スイッチバックに向けたシステムの事前チェック" MetroCluster 構成に応じて修復処理とスイッチバック処理を実行します。

MetroCluster IP 構成全体の電源をオフにします

メンテナンスや再配置を開始する前に、 MetroCluster IP 構成全体とすべての機器の電源をオフにする必要があります。

ONTAP 9.8 以降では '**storage switch ***' コマンドは '***system switch**' に置き換えられています以下の手順は '*storage switch *' コマンドを示していますが 'ONTAP 9.8 以降を実行している場合は '*system switch *' コマンドを使用することをお勧めします

1. MetroCluster 構成の両方のサイトから MetroCluster 構成を確認します。
   a. MetroCluster の構成と運用モードが正常な状態であることを確認します。`+* MetroCluster show*`
   b. 次のコマンドを実行します :+**`MetroCluster interconnect show`**
   c. いずれかの MetroCluster ノードで次のコマンドを入力して、ディスクへの接続を確認します。 `+*run local sysconfig -v *`
   d. 次のコマンドを実行します :`+* storage port show *`
   e. 次のコマンドを実行します :`+* storage switch show *`
   f. 次のコマンドを実行します :`+* network interface show *`
   g. 次のコマンドを実行します :`+* network port show *`
   h. 次のコマンドを実行します :`+* network device-discovery show *`
   i. MetroCluster チェック :`+* MetroCluster check run*` を実行します
   j. MetroCluster チェックの結果を表示します :`+* MetroCluster check show*`
   k. 次のコマンドを実行します。 `+* MetroCluster configurion-settings interface show *`

2. 必要に応じて、 AUSO 障害ドメインをに変更して AUSO を無効にします

   「 * auso-disabled * 」と表示されます

```
cluster_A_site_A::*>metrocluster modify -auto-switchover-failure-domain
auso-disabled
```

   MetroCluster IP 構成では、 ONTAP メディエーターが設定されていないかぎり、 AUSO 障害ドメインはすでに「 auso-disabled 」に設定されています。

3. コマンドを使用して、変更を確認します

   「 * MetroCluster operation show * 」と表示されます

```
    cluster_A_site_A::*> metrocluster operation show
       Operation: modify
           State: successful
      Start Time: 4/25/2020 20:20:36
        End Time: 4/25/2020 20:20:36
          Errors: -
```

4. ノードを停止します。

   *halt *`

```
system node halt -node node1_SiteA -inhibit-takeover true -ignore-quorum
-warnings true
```

5. サイトで次の機器の電源をオフにします。
   - ストレージコントローラ
   - MetroCluster IP スイッチ
   - ストレージシェルフ
6. 30分待ってから、すべてのストレージシェルフ、MetroCluster IPスイッチ、およびストレージコントローラの電源をオンにします。
7. コントローラの電源をオンにしたら、両方のサイトで MetroCluster 構成を確認します。

   設定を確認するには、手順 1 を繰り返します。

8. 電源再投入チェックを実行します。
   a. すべての同期元 SVM がオンラインであることを確認します。 `+* vserver show *`
   b. オンラインでない同期元の SVM をすべて起動します。 `+* vserver start *`

すべてのMetroCluster構成のメンテナンス手順

ストレッチ MetroCluster 構成のシェルフの無停止での交換

ディスクシェルフまたはディスクシェルフシャーシがフル装備されたストレッチ MetroCluster 構成では、システムを停止することなくディスクシェルフを交換し、取り外すシェルフからコンポーネントを移すことができます。

設置するディスクシェルフモデルが、に記載されているストレージシステムの要件を満たしている必要があります "Hardware Universe"サポートされるシェルフモデル、サポートされるディスクドライブタイプ、スタック内のディスクシェルフの最大数、サポートされる ONTAP バージョンなどがあります。

手順

1. 自身の適切な接地対策を行います
2. 交換するシェルフが含まれているループのディスクがあるアグリゲートとボリュームをすべて特定し、関係するプレックス名をメモします。

   いずれかのノードに、関係するシェルフとホストアグリゲートまたはホストボリュームのループのディスクが含まれている場合があります。

3. 計画している交換のシナリオに基づいて、次の 2 つのオプションのいずれかを選択します。
   - シェルフシャーシ、ディスク、および I/O モジュール（ IOM ）を含むディスクシェルフ全体を交換する場合は、次の表の対応する操作を実行します。

シナリオ（ Scenario ）	アクション
関係するプレックスに含まれるディスク数が関係するシェルフよりも少ない。	関係するシェルフのディスクを別のシェルフのスペアと 1 本ずつ交換します。 ディスク交換の完了後にプレックスをオフラインにすることができます。
関係するプレックスに含まれるディスク数が関係するシェルフよりも多い。	プレックスをオフラインにして削除します。
関係するプレックスに関係するシェルフのいずれかのディスクが含まれる。	プレックスをオフラインにしますが削除はしません。

   - ディスクシェルフシャーシのみを交換し、他のコンポーネントは交換しない場合は、次の手順を実行します。
     i. 関係するプレックスをホストしているコントローラで、それらのプレックスをオフラインにします。

        「アグリゲートはオフライン」です

     ii. プレックスがオフラインであることを確認します。

アグリゲート・ステータス -r

4. 関係するシェルフループが接続されているコントローラ SAS ポートを特定し、両方のサイトコントローラでその SAS ポートを無効にします。

   storage port disable -node node_name -port_sas_port_

   関係するシェルフループが両方のサイトに接続されます。

5. ディスクが見つからないことが ONTAP で認識されるまで待ちます。
   a. ディスクがないことを確認します。

      「 sysconfig -a 」または「 sysconfig -r 」です

6. ディスクシェルフの電源スイッチをオフにします。
7. ディスクシェルフからすべての電源コードを取り外します。
8. 新しいディスクシェルフを同じようにケーブル接続できるように、ケーブルを取り外したポートをメモしておいてください。
9. ディスクシェルフを他のディスクシェルフまたはストレージシステムに接続しているケーブルを取り外します。
10. ラックからディスクシェルフを取り外します。

    ディスクシェルフを軽くして扱いやすくするために、電源装置と IOM を取り外します。ディスクシェルフシャーシを設置する場合は、ディスクドライブやキャリアも取り外します。そうでない場合は、過度に動かすと原因の内蔵ドライブが破損する可能性があるため、ディスクドライブやキャリアはできるだけ取り外さないようにしてください。

11. 交換用ディスクシェルフをサポートブラケットとラックに設置して固定します。
12. ディスクシェルフシャーシを設置した場合は、電源装置と IOM を再度取り付けます。
13. 取り外したディスクシェルフとまったく同じように、交換用ディスクシェルフのポートにすべてのケーブルを接続してディスクシェルフのスタックを再構成します。
14. 交換用ディスクシェルフの電源をオンにし、ディスクドライブがスピンアップするまで待ちます。
15. ディスクシェルフ ID を 0~98 の一意の ID に変更します。
16. 無効にした SAS ポートを有効にします。
    a. ディスクが挿入されたことが ONTAP で認識されるまで待ちます。
    b. ディスクが挿入されたことを確認します。

       「 sysconfig -a 」または「 sysconfig -r 」です

17. ディスクシェルフ全体（ディスクシェルフシャーシ、ディスク、 IOM ）を交換する場合は、次の手順を実行します。

    ディスクシェルフシャーシのみを交換し、他のコンポーネントは交換しない場合は、手順 19 に進みます。

    a. 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確認します（ on ）。

storage disk option modify -autoassign

ディスクの割り当ては自動的に実行されます。

a. ディスクの自動割り当てが有効になっていない場合は、ディスク所有権を手動で割り当てます。

18. プレックスをオンラインに戻します。

'aggregate online_plex name_`

19. アグリゲートをミラーリングして、削除されたプレックスを再作成します。
20. プレックスで再同期が開始されるのを監視します。

'aggregate status -r < アグリゲート名 >`

21. ストレージシステムが想定どおりに機能していることを確認します。

「 system health alert show 」というメッセージが表示されます

ルートボリュームを新しいデスティネーションに移行するタイミング

2 ノードまたは 4 ノードの MetroCluster 構成内で、ルートボリュームを別のルートアグリゲートに移動しなければならない場合があります。

2 ノード **MetroCluster** 構成でルートボリュームを移行

2 ノード MetroCluster 構成内で新しいルートアグリゲートにルートボリュームをマイグレートする場合は、を参照してください "2 ノードの clustered MetroCluster スイッチオーバーを使用した新しいルートアグリゲートへの mroot の移動方法"。この手順では、 MetroCluster スイッチオーバー処理の実行中にルートボリュームを無停止で移行する方法を示します。この手順は、 4 ノード構成で使用する手順とは少し異なります。

4 ノード **MetroCluster** 構成でのルートボリュームの移行

4 ノード MetroCluster 構成内で新しいルートアグリゲートにルートボリュームを移行する場合は、を使用します "system node migrate-root" コマンドを実行しながら、次の要件を満たしていること。

- system node migrate-root は、 4 ノード MetroCluster 構成内でルートアグリゲートを移動する場合に使用できます。
- ルートアグリゲートがすべてミラーされている必要があります。
- ルートアグリゲートをホストするための小容量のドライブを搭載した新しいシェルフを両方のサイトに追加することができます。
- 新しいドライブを接続する前に、プラットフォームでサポートされているドライブの最大数を確認する必要があります。

  "NetApp Hardware Universe の略"

- ルートアグリゲートを小容量のドライブに移動する場合は、プラットフォームの最小ルートボリュームサイズを調整して、すべてのコアファイルが保存されるようにする必要があります。

4 ノード手順は 8 ノード構成にも適用できます。

MetroCluster 構成でのメタデータボリュームの移動

MetroCluster 構成では、アグリゲート間でメタデータボリュームを移動できます。メタデータボリュームの移動が必要となるのは、ソースアグリゲートが運用停止になるかミラーリングを解除されたとき、または何らかの理由でアグリゲートが条件を満たさなくなったときです。

- このタスクを実行するには、クラスタ管理者の権限が必要です。
- ターゲットアグリゲートがミラーされており、かつデグレード状態でないことが必要です。
- ターゲットアグリゲートに、移動するメタデータボリュームよりも大きな使用可能スペースがあることが必要です。

手順

1. 権限レベルを advanced に設定します。

   「 * set -privilege advanced * 」のように指定します

2. 移動するメタデータボリュームを特定します。

   ```
   * volume show MDV_CRS **
   ```

```
Cluster_A::*> volume show MDV_CRS*
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
Cluster_A
          MDV_CRS_14c00d4ac9f311e7922800a0984395f1_A
                       Node_A_1_aggr1
                                    online     RW         10GB
9.50GB    5%
Cluster_A
          MDV_CRS_14c00d4ac9f311e7922800a0984395f1_B
                       Node_A_2_aggr1
                                    online     RW         10GB
9.50GB    5%
Cluster_A
          MDV_CRS_15035e66c9f311e7902700a098439625_A
                       Node_B_1_aggr1
                                    -          RW             -
-     -
Cluster_A
          MDV_CRS_15035e66c9f311e7902700a098439625_B
                       Node_B_2_aggr1
                                    -          RW             -
-     -
4 entries were displayed.

Cluster_A::>
```

3. 対象となるターゲットアグリゲートを特定します。

   '*MetroCluster check config-replication show-aggregate-eligibility *

   次のコマンドは、メタデータボリュームをホストできる cluster_A 内のアグリゲートを特定します。

```
Cluster_A::*> metrocluster check config-replication show-aggregate-
eligibility

Aggregate Hosted Config Replication Vols Host Addl Vols Comments
------------ ------------------------------------------ --------------
--------
Node_A_1_aggr0 - false Root Aggregate
Node_A_2_aggr0 - false Root Aggregate
Node_A_1_aggr1 MDV_CRS_1bc7134a5ddf11e3b63f123478563412_A true -
Node_A_2_aggr1 MDV_CRS_1bc7134a5ddf11e3b63f123478563412_B true -
Node_A_1_aggr2 - true
Node_A_2_aggr2 - true
Node_A_1_Aggr3 - false Unable to determine available space of aggregate
Node_A_1_aggr5 - false Unable to determine mirror configuration
Node_A_2_aggr6 - false Mirror configuration does not match requirement
Node_B_1_aggr4 - false NonLocal Aggregate
```

この例では、 Node_A_1_aggr2 と Node_A_2_aggr2 が該当します。

4. ボリューム移動処理を開始します。

   ` * volume move start -vserver_svm_name_-volume_volume_name_-destination-aggregate -destination_aggregate_name_*`

   次のコマンドは、メタデータボリューム「 M DV_CRS_14c00d4ac9f311e7922800a0984395f1 」を「 aggregate Node_A_1_aggr1 」から「 aggregate Node_A_1_aggr2 」に移動します。

```
Cluster_A::*> volume move start -vserver svm_cluster_A -volume
MDV_CRS_14c00d4ac9f311e7922800a0984395f1
-destination-aggregate aggr_cluster_A_02_01

Warning: You are about to modify the system volume
         "MDV_CRS_9da04864ca6011e7b82e0050568be9fe_A".  This may cause
severe
         performance or stability problems.  Do not proceed unless
directed to
         do so by support.  Do you want to proceed? {y|n}: y
[Job 109] Job is queued: Move
"MDV_CRS_9da04864ca6011e7b82e0050568be9fe_A" in Vserver
"svm_cluster_A" to aggregate "aggr_cluster_A_02_01".
Use the "volume move show -vserver svm_cluster_A -volume
MDV_CRS_9da04864ca6011e7b82e0050568be9fe_A" command to view the status
of this operation.
```

5. ボリューム移動処理の状態を確認します。

'**volume move show -volume vol_constituent_name**

6. admin 権限レベルに戻ります。

   '**set -privilege admin**

MetroCluster 構成のクラスタの名前変更

MetroCluster 構成のクラスタの名前を変更する場合は、名前を変更してから、ローカルクラスタとリモートクラスタの両方で変更が正しく反映されたことを確認します。

手順

1. を使用してクラスタ名を表示する

   '**MetroCluster node show**

   コマンドを実行します

```
cluster_1::*> metrocluster node show
DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_1
              node_A_1           configured     enabled   normal
              node_A_2           configured     enabled   normal
      cluster_2
              node_B_1           configured     enabled   normal
              node_B_2           configured     enabled   normal
4 entries were displayed.
```

2. クラスタの名前を変更します。

   '**cluster identity modify -name_new_name_**

   次の例では 'cluster_1' クラスタの名前は 'cluster_a ' に変更されています

```
cluster_1::*> cluster identity modify -name cluster_A
```

3. 名前を変更したクラスタが正常に稼働していることをローカルクラスタで確認します。

   '**MetroCluster node show**

   次の例では ' 新しく名前が変更された 'cluster_a が正常に稼働しています

```
cluster_A::*> metrocluster node show
DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
              node_A_1           configured     enabled   normal
              node_A_2           configured     enabled   normal
      cluster_2
              node_B_1           configured     enabled   normal
              node_B_2           configured     enabled   normal
4 entries were displayed.
```

4. リモートクラスタの名前を変更します。

   'cluster peer modify -local-name -name_cluster_2_-new-name_cluster_B_

   次の例では 'cluster_2' は 'cluster_B' という名前に変更されています

```
cluster_A::> cluster peer modify-local-name -name cluster_2 -new-name
cluster_B
```

5. ローカルクラスタの名前が変更されて正常に実行されていることをリモートクラスタで確認します。

   「 _ MetroCluster node show_` 」

   次の例では ' 新しく名前を変更した 'cluster_B' は正常に動作しています

```
cluster_B::*> metrocluster node show
DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_B
              node_B_1           configured     enabled   normal
              node_B_2           configured     enabled   normal
      cluster_A
              node_A_1           configured     enabled   normal
              node_A_2           configured     enabled   normal
4 entries were displayed.
```

6. 名前を変更するクラスタごとに、上記の手順を繰り返します。

MetroCluster構成の健全性の確認

MetroClusterコンポーネントが正常であることを確認する方法について説明します。

このタスクについて

- MetroCluster IP構成およびFC構成では、CLIを使用して健全性チェックコマンドを実行し、MetroClusterコンポーネントの状態を確認できます。
- ONTAP 9 .8以降を実行するMetroCluster IP構成では、ONTAP System Managerを使用して健全性チェックアラートの監視とトラブルシューティングを行うこともできます。

手順

CLIとSystem Managerのどちらを使用しているかに応じて、MetroCluster構成の健全性を確認します。

CLI

CLIを使用してMetroCluster構成の健全性を確認するには、次の手順を実行します。

手順

1. 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。

2. 処理が完了したら、 `metrocluster check run`結果を表示します。

```
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.
```

3. 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>
```

4. ヘルスアラートがないことを確認します。

```
system health alert show
```

ONTAPシステムマネージャ（**MetroCluster IP**のみ）

ONTAP 9 .8以降では、System ManagerによってMetroCluster IP構成の健常性が監視され、発生する可能性のある問題を特定して修正できます。

System Managerは、MetroCluster IP構成の健全性を定期的にチェックします。ダッシュボードのMetroClusterセクションを表示すると、通常は「MetroCluster systems are healthy」というメッセージが表示されます。

ただし、問題が発生すると、イベントの数がメッセージに表示されます。このメッセージをクリックすると、次のコンポーネントの健全性チェックの結果を確認できます。

- ノード
- ネットワークインターフェイス
- ティア（ストレージ）
- クラスタ
- 接続
- ボリューム
- 設定のレプリケーション

[ステータス *] 列は問題のあるコンポーネントを示し、 [詳細 *] 列は問題の解決方法を示します。

手順

1. System Manager で、 * Dashboard * を選択します。
2. 「* MetroCluster *」セクションのメッセージを表示します。
   a. メッセージにMetroCluster構成が正常であり、クラスタとONTAPメディエーターの間の接続（チェックマークが表示されている）が正常であることが示されていれば、問題は解決しません。
   b. メッセージにイベント数が表示されている場合、または接続がダウンしている場合（「X」が表示されている場合）は、次の手順に進みます。
3. イベント数を示すメッセージをクリックします。

   MetroCluster健全性レポートが表示されます。
4. レポートに表示される問題のトラブルシューティングを、 **Details** 列の推奨事項を使用して行います。
5. すべての問題を修正したら、 * MetroCluster の正常性を確認 * をクリックします。

   MetroClusterヘルスチェックは大量のリソースを使用するため、チェックを実行する前にすべてのトラブルシューティングタスクを実行する必要があります。

   MetroCluster健全性チェックはバックグラウンドで実行されます。タスクが完了するまで待つ間に、他のタスクを処理することができます。

追加情報の参照先

MetroCluster 構成の設定、運用、監視の詳細については、ネットアップのドキュメントを参照してください。

情報	件名
"MetroCluster のドキュメント"	• すべての MetroCluster 情報
"NetApp MetroCluster 解決策のアーキテクチャと設計"	• MetroCluster の設定と運用の技術概要 • MetroCluster 構成のベストプラクティス
"ファブリック接続 MetroCluster のインストールと設定"	• ファブリック接続 MetroCluster アーキテクチャ • 構成のケーブル接続 • FC-to-SAS ブリッジの設定 • FC スイッチを設定します • ONTAP で MetroCluster を設定します
"ストレッチ MetroCluster のインストールと設定"	• ストレッチ MetroCluster アーキテクチャ • 構成のケーブル接続 • FC-to-SAS ブリッジの設定 • ONTAP で MetroCluster を設定します
"MetroCluster IP のインストールと設定"	• MetroCluster IP アーキテクチャ • MetroCluster IP 構成のケーブル接続 • ONTAP で MetroCluster を設定します
"ネットアップのマニュアル：製品ガイドとリソース"	• MetroCluster の設定とパフォーマンスを監視する
"MetroCluster Tiebreaker ソフトウェアのインストールおよび設定"	• MetroCluster Tiebreaker ソフトウェアを使用して MetroCluster 構成を監視する
"コピーベースの移行"	• 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

MetroCluster FC から MetroCluster IP に移行します

移行する手順を選択

MetroCluster IP 構成に移行する場合は、サポートされているプラットフォームモデルを組み合わせて使用する必要があります。

また、MetroCluster IPプラットフォームが、MetroCluster FC構成からMetroCluster IP構成に移行する負荷に適したサイズであることを確認する必要があります。

サポートされるプラットフォームの組み合わせ

- 移行手順を実行するには、特に記載がないかぎり、または個 々 のプラットフォームで必要とされる場合を除き、ONTAP 9.8以降が必要です。
- MetroCluster構成内のすべてのノードで同じバージョンのONTAPが実行されている必要があります。たとえば、8ノード構成の場合は、8つのすべてのノードで同じバージョンのONTAPを実行する必要があります。ご使用の組み合わせでサポートされるONTAPの最小バージョンについては、を参照して"Hardware Universe"ください。

- 組み合わせて使用するプラットフォームの「下位」のオブジェクト制限を超えないようにしてください。2つのプラットフォームのオブジェクトの下限を適用します。
- ターゲットプラットフォームの制限がMetroCluster の制限よりも低い場合は、新しいノードを追加する前に、ターゲットプラットフォームの制限以下になるようにMetroCluster を再設定する必要があります。
- を参照してください "Hardware Universe" プラットフォームの制限：

サポートされる**AFF**と**FAS**の移行の組み合わせ

次の表に、サポートされるプラットフォームの組み合わせを示します。色分けされた表のセルで示されているように、最初の列のプラットフォームから、右側の列でサポートされているプラットフォームに移行できます。

たとえば、 AFF8060 コントローラモジュールで構成される MetroCluster FC 構成から、 AFF A400 コントローラモジュールで構成される IP 構成への移行がサポートされます。

テーブルは次の2つのグループに分割されます。

- *グループ1 *は、AFF A150 FAS8700、AFF AFF C400 A20、FAS2750 AFF A400、AFF A220、FAS500f、AFF C250、AFF A250、FAS50、AFF A300 C30、AFF A320 A30、FAS8200、AFF、AFF 、FAS8300システムへの移行の組み合わせを示しています。
- *グループ2 *は、AFF C60、AFF A50、FAS70、FAS9000、AFF A700、AFF A90、AFF A900、AFF 、FAS9500、AFF C800、AFF A800 C80、FAS90、AFF A70、およびAFF A1Kシステムへの移行の組み合わせを示しています。

次の注意事項は両方のグループに適用されます。

- 注1：このプラットフォームの組み合わせには、ONTAP 9.11.1以降が必要です。
- 注2：FCノードのローカルクラスタインターフェイスには40GbEインターフェイスが必要です。
- 注3：FCノードのローカルクラスタインターフェイスには100GbEインターフェイスが必要です。

AFFと**FAS**の組み合わせグループ**1**

AFF A150 FAS8700、AFF AFF C400 A20、FAS2750 AFF A400、AFF A220、FAS500f、AFF C250、AFF A250、FAS50、AFF A300 C30、AFF A320 A30、FAS8200、AFF、AFF、FAS8300の各システムへの移行でサポートされる組み合わせを確認します。

AFF and FAS		Target MetroCluster IP platform									
		AFF A150	AFF A20	FAS2750 AFF A220	FAS500f AFF C250 AFF A250	FAS50	AFF C30 AFF A30	FAS8200 AFF A300	AFF A320	FAS8300 AFF C400 AFF A400	FAS8700
Source MetroCluster FC platform	FAS8020 AFF8020 FAS8040 AFF8040										
	FAS8060 AFF8060 FAS8080 AFF8080										
	FAS8200 AFF A300				Note 1						
	FAS8300 AFF A400										
	FAS9000 AFF A700										
	FAS9500 AFF A900										

AFFと**FAS**の組み合わせグループ**2**

C60、AFF A50、FAS70、、AFF A700、AFF A70、AFF C800、AFF、AFF A90、FAS9000、AFF、AFF A900、AFF A800 C80、FAS90、FAS9500、およびAFF A1Kシステムへの移行でサポートされる組み合わせを確認します。

AFF and FAS		Target MetroCluster IP platform									
		AFF C60	AFF A50	FAS70	FAS9000 AFF A700	AFF A70	AFF C800 AFF A800	FAS9500 AFF A900	AFF C80	FAS90 AFF A90	AFF A1K
Source MetroCluster FC platform	FAS8020 AFF8020 FAS8040 AFF8040										
	FAS8060 AFF8060 FAS8080 AFF8080										
	FAS8200 AFF A300										
	FAS8300 AFF A400										
	FAS9000 AFF A700			Note 2	Note 2	Note 2	Note 2	Note 2	Note 2	Note 2	Note 2
	FAS9500 AFF A900							Note 3	Note 3	Note 3	Note 3

サポートされる**ASA**移行プラットフォームの組み合わせ

次の表に、ASAシステムでサポートされるプラットフォームの組み合わせを示します。

ソース**MetroCluster FC**プラットフォーム	ターゲット**MetroCluster IP**プラットフォーム	サポートの有無
ASA A400	ASA A400	はい。
	ASA A900	いいえ
ASA A900	ASA A400	いいえ
	ASA A900	はい。

移行する手順を選択

既存の MetroCluster FC 構成に応じて、移行手順を選択する必要があります。

移行手順は、バックエンドの FC スイッチファブリックまたは FC-VI 接続を IP スイッチネットワークに置き換えます。正確な手順は、使用する開始構成によって異なります。

元のプラットフォームと FC スイッチがある場合、そのスイッチは移行手順の最後で廃止されます。

変更前の構成	システムを停止するか、システムを停止	要件	手順
4ノードまたは8ノード	無停止	新しいプラットフォームには新しいストレージ シェルフが必要です。移行が完了すると、古いコントローラー、シェルフ、ディスクはクラスターから削除されます。	"手順 へのリンク" 注: この手順では、次の FC から IP への移行がサポートされます。 • 4ノードMetroCluster FC構成から4ノードMetroCluster IP構成へ • 8ノードのMetroCluster FC構成から8ノードのMetroCluster IP構成へ
2 ノード	システムの停止を伴う	新しいストレージシェルフは、元のプラットフォームと新しいプラットフォームの両方でサポートされます。	"手順 へのリンク"

2 ノード	システムの停止を伴う	新しいストレージシェルフは、元のプラットフォームと新しいプラットフォームの両方でサポートされます。古いストレージシェルフは撤去する必要があります。	"手順 へのリンク"
2 ノード	システムの停止を伴う	古いストレージシェルフは、新しいプラットフォームではサポートされません。古いストレージシェルフは撤去する必要があります。	"手順 へのリンク"

MetroCluster FC から MetroCluster IP 構成への無停止での移行（ ONTAP 9.8 以降）

MetroCluster FC から MetroCluster IP 構成への無停止での移行（ ONTAP 9.8 以降）

既存のMetroCluster FC構成から新しいMetroCluster IP構成へ、ワークロードやデータを無停止で移行できます。

ONTAP 9.13.1以降では、MetroClusterとドライブシェルフが同じIPスイッチに接続されたMetroCluster IP構成（共有ストレージスイッチ構成）でこの手順がサポートされます。

ONTAP 9.13.1 以降では、既存の 8 ノードMetroCluster FC 構成から新しい 8 ノードMetroCluster IP 構成へのワークロードとデータの無停止移行を実行できます。この手順を使用して、1 つの 4 ノード FC DR グループを移行し、空の FC DR グループを削除してから、2 番目の FC DR グループに対して手順を繰り返します。

ONTAP 9.8 以降では、既存の 4 ノードMetroCluster FC 構成から新しい 4 ノードMetroCluster IP 構成へのワークロードとデータの無停止移行を実行できます。移行が完了したら、必要に応じて 8 ノードのMetroCluster IP 構成に拡張できます。見る"MetroCluster IP設定を展開します"。

- この手順は無停止で実行されます。

  MetroCluster 構成では、処理中もデータの提供を継続できます。

- この手順 は、4ノードおよび8ノードのMetroCluster FC構成にのみ適用されます。

  2 ノード MetroCluster FC 構成の場合は、を参照してください "移行する手順を選択します"。

- この手順 では、1つの4ノードFC DRグループを移行するために必要な手順について説明します。8ノード構成（2つのFC DRグループ）の場合は、FC DRグループごとに手順 全体を繰り返す必要があります。

この手順の一環として DR グループを追加または削除する場合は、別の DR グループを追加または削除する前に、DR グループの削除または追加が成功したことを確認する必要があります。

- すべての要件を満たし、手順のすべての手順に従う必要があります。

古いプラットフォームモデルを追加する場合の重要な情報

次のガイダンスは、新しいプラットフォーム モデル (ONTAP 9.15.1 以降でリリースされたプラットフォーム) を含む既存のMetroCluster構成に古いプラットフォーム モデル (ONTAP 9.15.1 より前にリリースされたプラットフォーム) を追加する必要がある、まれなシナリオを対象としています。 8 ノードの FC から IP への移行では、最初の FC DR グループをONONTAP 9.15.1 以降で導入されたプラットフォーム モデルに移行し、2 番目の DR グループをONONTAP 9.15.1 より前に導入されたプラットフォームに移行する予定の場合、このガイダンスが適用されます。

既存のMetroCluster構成に、共有クラスタ**/HA** ポート を使用するプラットフォーム (ONTAP 9.15.1 以降でリリースされたプラットフォーム) が含まれている場合、構成内のすべてのノードをONTAP 9.15.1P11 またはONTAP 9.16.1P4 以降にアップグレードせずに、共有**MetroCluster/HA** ポート を使用するプラットフォーム (ONTAP 9.15.1 より前にリリースされたプラットフォーム) を追加することはできません。

共有**/ MetroCluster HA** ポート を使用する古いプラットフォーム モデルを、共有クラスタ**/HA** ポート を使用する新しいプラットフォーム モデルを含むMetroClusterに追加することはまれなシナリオであり、ほとんどの組み合わせは影響を受けません。

次の表を使用して、組み合わせが影響を受けるかどうかを確認してください。既存のプラットフォームが最初の列にリストされ、構成に追加するプラットフォームが 2 番目の列にリストされている場合、新しい DR グループを追加するには、構成内のすべてのノードでONTAP 9.15.1P11 またはONTAP 9.16.1P4 以降が実行されている必要があります。

既存の **MetroCluster** に以下が含まれている場合...		追加するプラットフォームは...		作業
共有クラスター/**HA** ポート を使用する AFF システム: • AFF A20用 • AFF A30用 • AFF C30 • AFF A50用 • AFF C60 • AFF C80用 • AFF A70用 • AFF A90用 • AFF A1K用	共有クラスター/**HA** ポート を使用する FAS システム: • FAS50 • FAS70 • FAS90	共有 **MetroCluster/HA** ポート を使用する AFF システム: • AFF A150、ASA A150向け • AFF A220 • AFF C250 、ASA C250向け • AFF A250、ASA A250向け • AFF A300 • AFF A320 • AFF C400 、ASA C400向け • AFF A400、ASA A400向け • AFF A700 • AFF C800 、ASA C800向け • AFF A800、ASA A800向け • AFF A900、ASA A900向け	共有 **MetroCluster/HA** ポート を使用する FAS システム: • FAS2750 • FAS500f • FAS8200 • FAS8300 • FAS8700 の場合 • FAS9000 • FAS9500	既存の MetroCluster 構成に新しいプラットフォームを追加する前に、既存および新しい構成内のすべてのノードを ONTAP 9.15.1P11 または ONTAP 9.16.1P4 以降にアップグレードします。

MetroCluster FC 構成から **MetroCluster IP** 構成への移行を準備

コンソールログを有効にする

このタスクを実行する前に、デバイスでコンソールログを有効にしてください。

NetAppでは、使用しているデバイスでコンソールロギングをイネーブルにし、この手順を実行する際に次のアクションを実行することを強く推奨します。

- メンテナンス中はAutoSupportを有効のままにします。
- メンテナンスの前後にメンテナンスAutoSupportメッセージをトリガーして、メンテナンスアクティビティ中にケースの作成を無効にします。

  ナレッジベースの記事を参照してください "スケジュールされたメンテナンス時間中にケースの自動作成

を停止する方法"。

- 任意のCLIセッションのセッションロギングをイネーブルにします。セッションログを有効にする方法については、ナレッジベースの記事の「セッション出力のログ」セクションを参照してください "ONTAPシステムへの接続を最適化するためのPuTTYの設定方法"。

FC から **IP** への無停止での移行に関する要件

移行プロセスを開始する前に、構成が要件を満たしていることを確認します。

FCからIPへの移行は、次の要件を満たしている構成であれば、無停止で実行できます。

- 8ノード構成の場合は、すべてのノードでONTAP 9.13.1以降が実行されています。
- 4ノード構成の場合は、すべてのノードでONTAP 9.8以降が実行されています。
- 既存のプラットフォームと新しいプラットフォームの組み合わせが移行対象としてサポートされます。

  "無停止移行でサポートされるプラットフォーム"

- ご使用の構成では、スイッチクラスタ構成がサポートされます。

  "Hardware Universe"

> 共有ストレージMetroClusterスイッチを使用している場合は、4ノードのMetroCluster IP構成にのみ移行できます。共有ストレージMetroClusterスイッチを使用した8ノードMetroCluster IP構成への移行はサポートされていません。4ノードMetroCluster IP構成への移行が完了したら、移行"8ノードMetroCluster IP構成に拡張"を実行できます。

- ご使用の構成はすべての要件を満たしており、次の_ MetroClusterインストールおよび構成手順の説明に従ってケーブル接続されています。

  "ファブリック接続 MetroCluster のインストールと設定"

  "ストレッチ MetroCluster のインストールと設定"

移行が **MetroCluster** のハードウェアコンポーネントに及ぼす影響

移行手順が完了したあと、既存の MetroCluster 構成の主要コンポーネントが交換または再設定されている。

- * コントローラモジュール *

  既存のコントローラモジュールが新しいコントローラモジュールに交換されます。既存のコントローラモジュールは、移行手順の終了時に運用停止されます。

- * ストレージシェルフ *

  データは古いシェルフから新しいシェルフに移動されます。古いシェルフは、移行手順の終了時に運用停止されます。

- * MetroCluster （バックエンド）およびクラスタスイッチ *

バックエンドスイッチ機能は、 IP スイッチファブリックに置き換えられます。MetroCluster FC 構成に FC スイッチおよび FC-to-SAS ブリッジが含まれていた場合、それらのブリッジはこの手順の最後で運用停止されます。

MetroCluster FC 構成でクラスタインターコネクトにクラスタスイッチを使用していた場合は、場合によってはそのスイッチを再利用してバックエンド IP スイッチファブリックを提供できます。再利用するクラスタスイッチには、プラットフォームおよびスイッチ固有の RCF を再設定する必要があります。の手順。

MetroCluster FC 構成でクラスタスイッチを使用していなかった場合は、バックエンドスイッチファブリックを提供する新しい IP スイッチが追加されます。

"IP スイッチに関する考慮事項"

- * クラスタピアリングネットワーク *

お客様提供の既存のクラスタピアリングネットワークを、新しい MetroCluster IP 構成に使用できます。クラスタピアリングは、移行手順の一部として MetroCluster IP ノードで設定します。

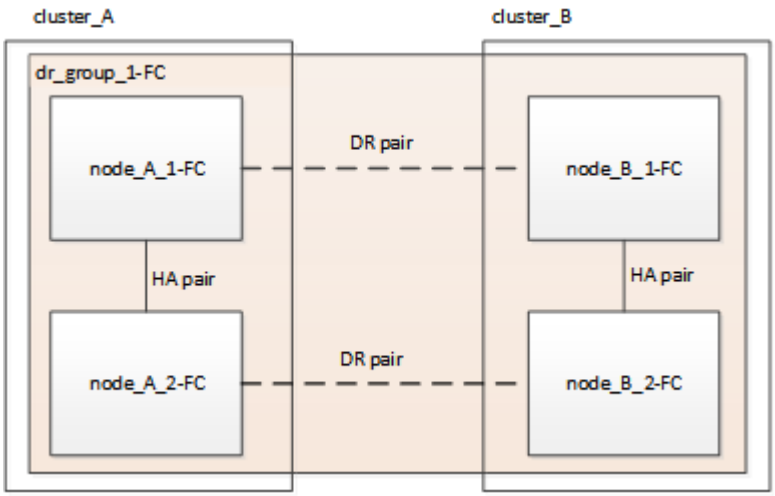
無停止での **MetroCluster** の移行のワークフロー

無停止移行を成功させるには、特定のワークフローに従う必要があります。構成に応じたワークフローを選択します。

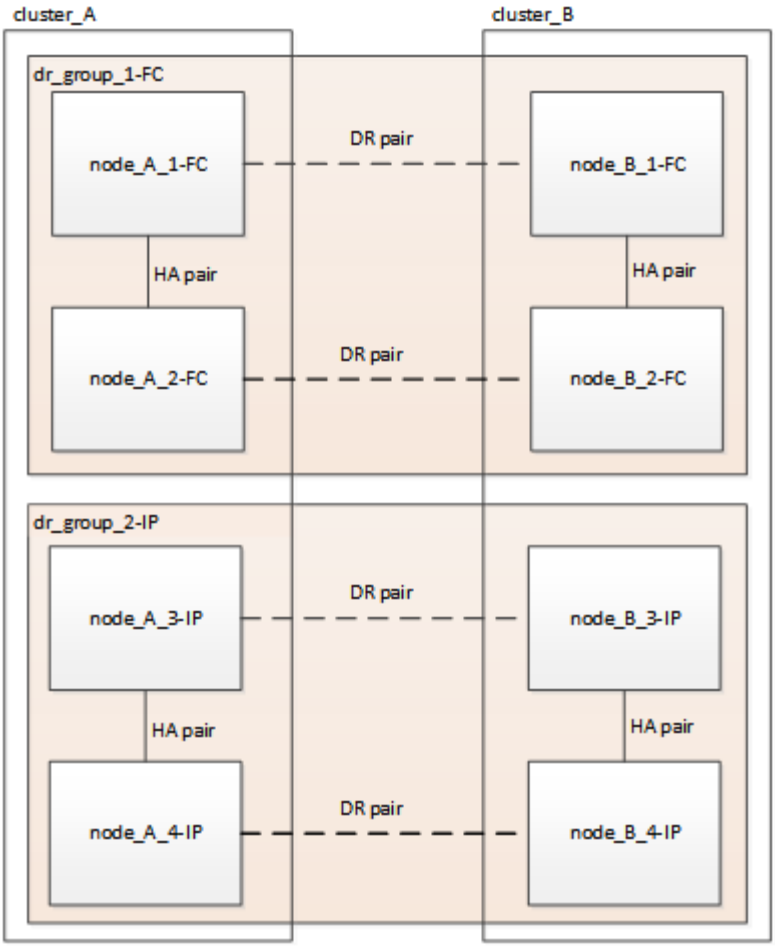
- 4ノードFC構成の移行ワークフロー
- 8ノードFC構成の移行ワークフロー

4ノード**FC**構成の移行ワークフロー

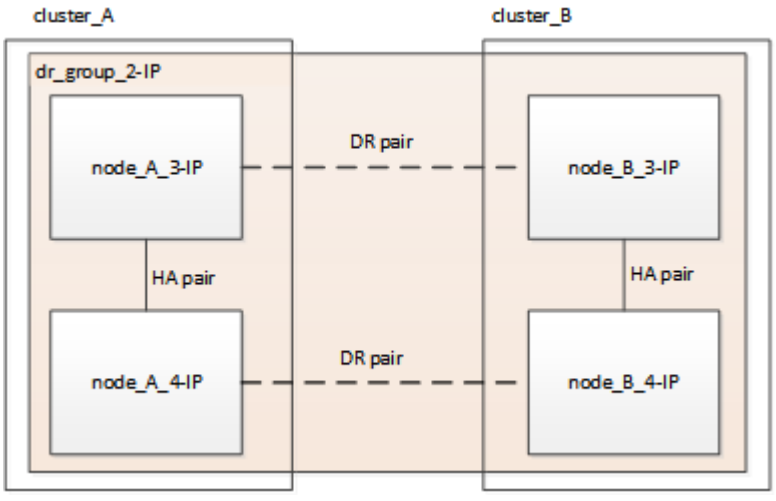
移行プロセスは、正常な 4 ノード MetroCluster FC 構成から始まります。



新しい MetroCluster IP ノードは 2 つ目の DR グループとして追加されます。

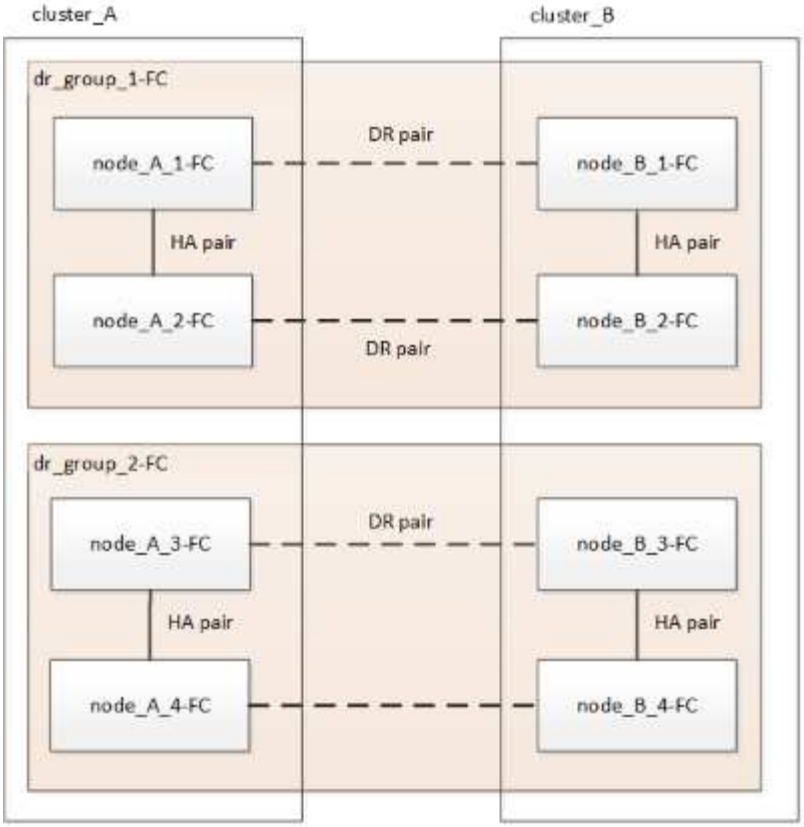


データが古い DR グループから新しい DR グループに転送され、古いノードとそのストレージが構成から削除されて運用が停止されます。プロセスは、 4 ノード MetroCluster の IP 構成で終了します。

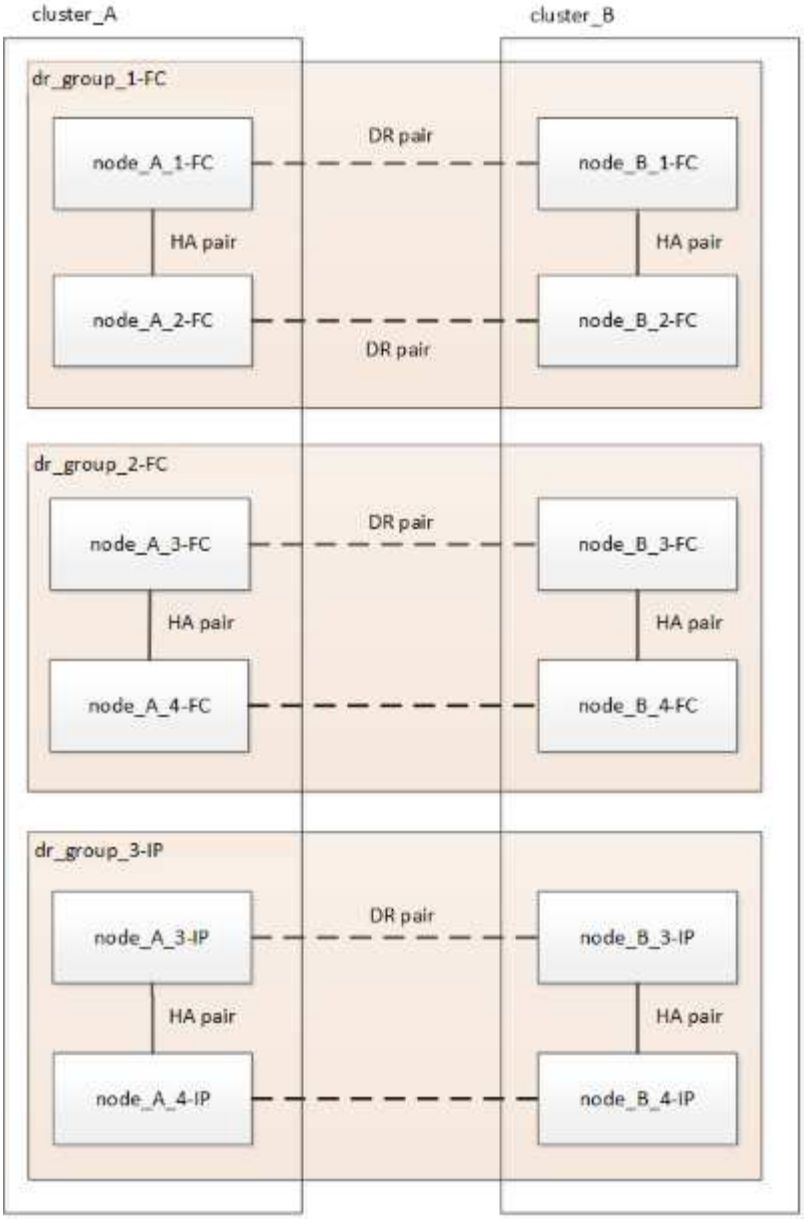


8ノード**FC**構成の移行ワークフロー

移行プロセスは、正常な8ノードMetroCluster FC構成から始まります。

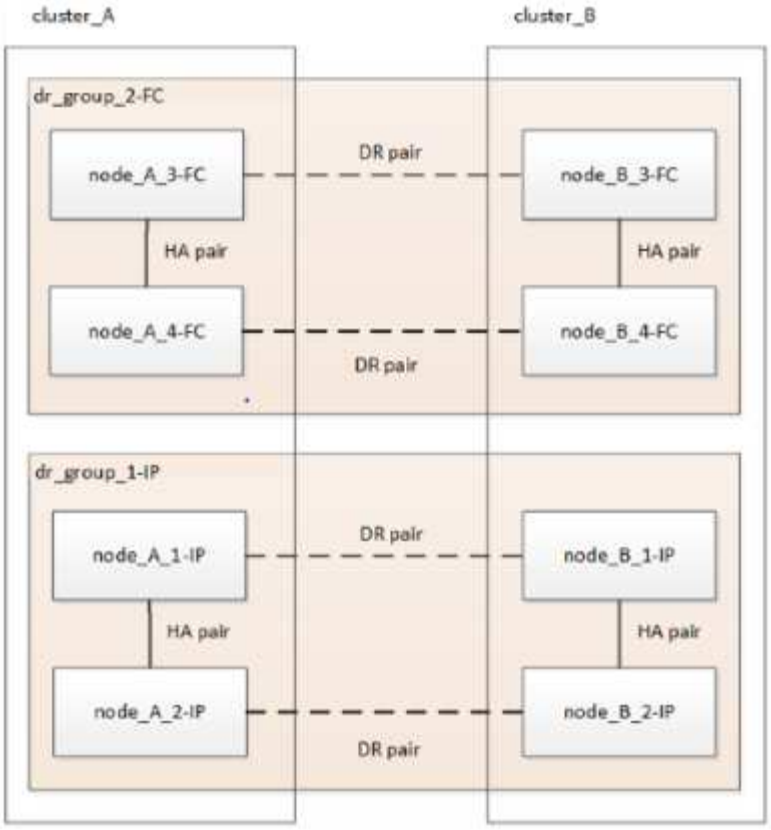


新しいMetroCluster IPノードが3つ目のDRグループとして追加されます。

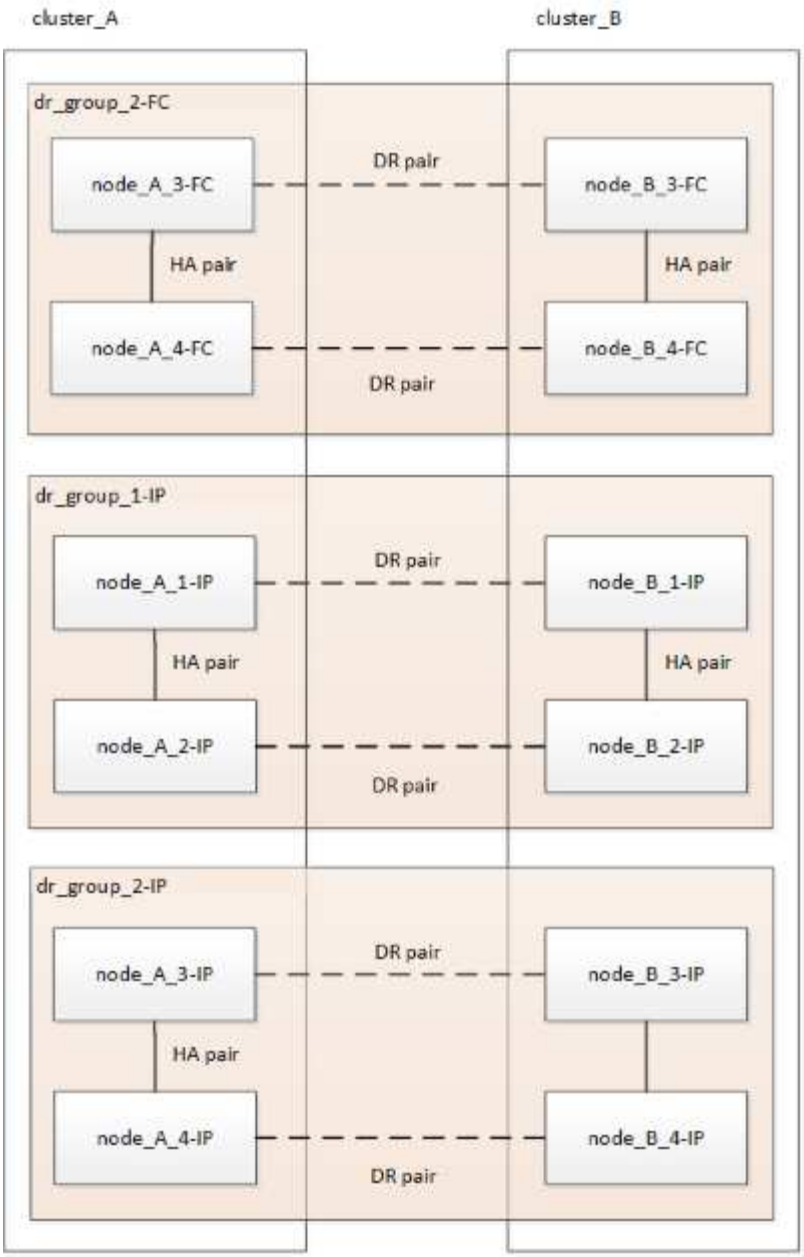


データがDR_GROUP_1-FCからDR_GROUP_1-IPに転送され、古いノードとそのストレージが構成から削除されて運用が停止されます。

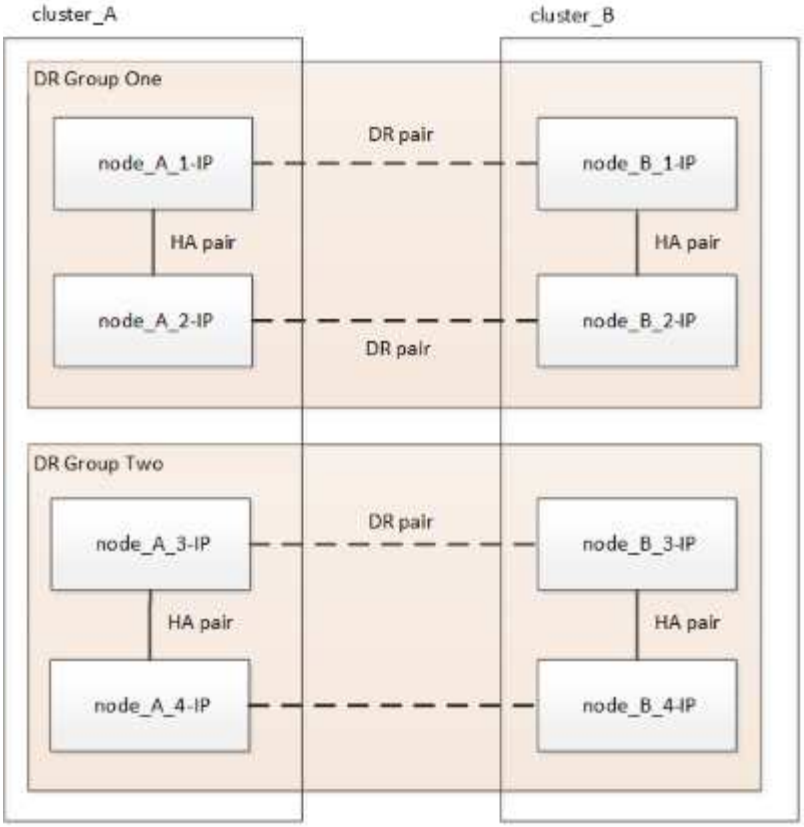
8ノードFC構成から4ノードIP構成に移行する場合は、dr_group_1-FCおよびdr_group_2-FCのすべてのデータを新しいIP DRグループ（dr_group_1-IP）に移行する必要があります。その後、両方のFC DRグループの運用を停止できます。FC DRグループを削除すると、4ノードのMetroCluster IP構成でプロセスが終了します。



残りのMetroCluster IPノードを既存のMetroCluster 構成に追加します。同じ手順を繰り返して、dr_group_2-FCノードからdr_group_2-IPノードにデータを転送します。

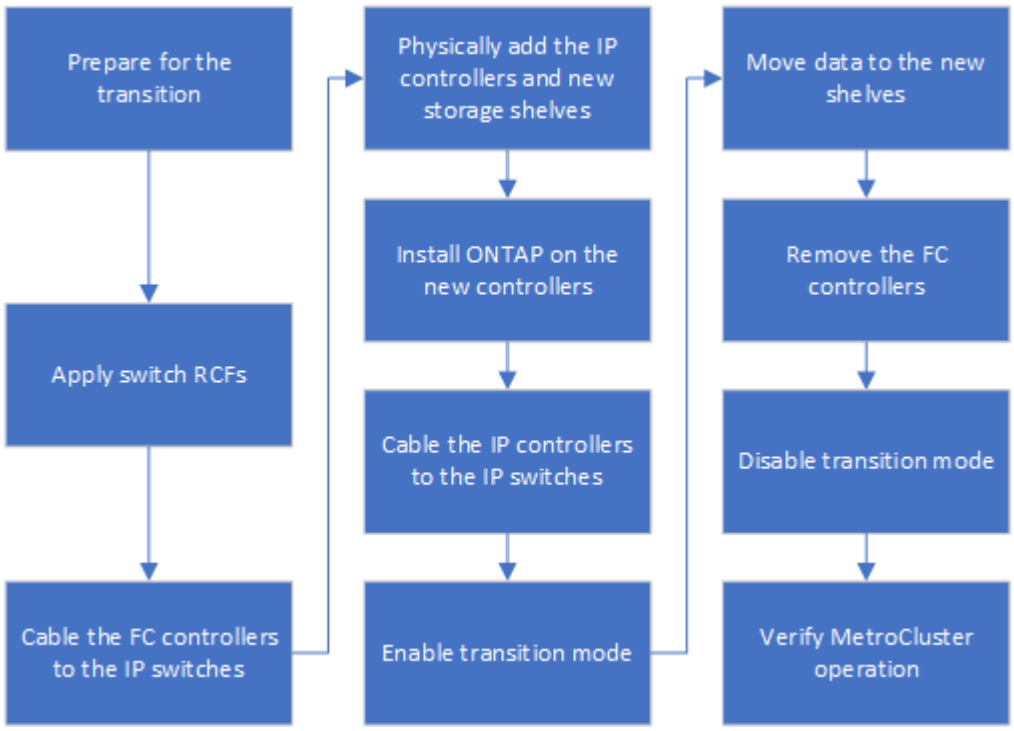


dr_group_2-FCを削除すると、8ノードのMetroCluster IP構成でプロセスが終了します。



移行プロセスのワークフロー

MetroCluster 構成を移行するには、次のワークフローを使用します。



IP スイッチに関する考慮事項

IP スイッチがサポートされていることを確認する必要があります。既存のスイッチモデ

ルが元の MetroCluster FC 構成と新しい MetroCluster IP 構成の両方でサポートされている場合は、既存のスイッチを再利用できます。

サポートされるスイッチ

ネットアップ製のスイッチを使用する必要があります。

- MetroCluster 準拠のスイッチ（ネットアップが提供する検証済みではないスイッチ）の使用は、移行ではサポートされていません。
- MetroCluster FC 構成と MetroCluster IP 構成の両方で、 IP スイッチがクラスタスイッチとしてサポートされている必要があります。
- MetroCluster FC がスイッチクラスタで、 IP クラスタスイッチが MetroCluster IP 構成でサポートされている場合は、 IP スイッチを新しい MetroCluster IP 構成で再利用できます。
- 新しい IP スイッチは、通常次の場合に使用されます。
  - MetroCluster FC はスイッチレスクラスタであるため、新しいスイッチが必要です。
  - MetroCluster FC はスイッチクラスタですが、 MetroCluster IP 構成では既存の IP スイッチはサポートされません。
  - MetroCluster IP 設定に別のスイッチを使用する。

> 共有ストレージMetroClusterスイッチを使用している場合は、4ノードのMetroCluster IP構成にのみ移行できます。共有ストレージMetroClusterスイッチを使用した8ノードMetroCluster IP構成への移行はサポートされていません。4ノードMetroCluster IP構成への移行が完了したら、移行"8ノードMetroCluster IP構成に拡張"を実行できます。

プラットフォームモデルおよびスイッチのサポートについては、を参照してください "Hardware Universe"。

無停止移行時のスイッチオーバー、修復、スイッチバックの処理

移行プロセスの各ステージに応じて、 MetroCluster のスイッチオーバー、修復、スイッチバックの各処理で MetroCluster FC または MetroCluster IP のいずれかのワークフローが使用されます。

次の表に、移行プロセスの各段階で使用されるワークフローを示します。段階によっては、スイッチオーバーとスイッチバックがサポートされない場合があります。

- MetroCluster FC ワークフローでは、スイッチオーバー、修復、スイッチバックの手順は MetroCluster FC 構成で使用されます。
- MetroCluster IP ワークフローでは、スイッチオーバー、修復、スイッチバックの手順は MetroCluster IP 構成で使用されます。
- ユニファイドワークフローでは、 FC ノードと IP ノードの両方を設定する場合、手順は NSO と USO のどちらが実行されるかによって異なります。詳細が表に表示されます。

スイッチオーバー、修復、スイッチバックに関する MetroCluster FC および IP のワークフローについては、を参照してください "MetroCluster のデータ保護とディザスタリカバリについて理解する"。

> 自動計画外スイッチオーバーは、移行プロセスでは使用できません。

移行のステージ	ネゴシエートスイッチオーバーで使用するワークフロー	計画外スイッチオーバーで使用するワークフロー
MetroCluster IP ノードがクラスタに参加する前	MetroCluster FC の略	MetroCluster FC の略
MetroCluster IP ノードがクラスタに参加した後で 'MetroCluster configure' コマンドが実行されます	サポート対象外	MetroCluster FC の略
MetroCluster configure コマンドが発行された後。ボリューム移動を実行中の可能性があります。	unified ：リモートサイトのすべてのノードが稼働したままであり、自動的に修復されます	統合： • MetroCluster FC ノードが所有するミラーアグリゲートがミラーリングされるのは、ストレージにアクセスできる場合だけで、それ以外のアグリゲートはスイッチオーバー後にデグレード状態になります。 • すべてのリモートサイトノードがブート可能である。 • 「アグリゲートの修復」コマンドと「ルートの修復」コマンドは、手動で実行する必要があります。
MetroCluster FC ノードが設定解除されました。	サポート対象外	MetroCluster IP の略
MetroCluster FC ノードで cluster unjoin コマンドが実行されました	MetroCluster IP の略	MetroCluster IP の略

移行時のアラートメッセージとツールのサポート

移行中にアラートメッセージが表示されることがあります。これらのアラートは無視してかまいません。また、一部のツールは移行時に使用できません。

- ARS は移行中に警告を発する場合があります。

  これらのアラートは無視してかまいません。移行が完了すると表示されなくなります。

- OnCommand Unified Manager で移行時にアラートが生成されることがあります。

  これらのアラートは無視してかまいません。移行が完了すると表示されなくなります。

- Config Advisor は移行中にサポートされません。
- System Manager は移行時にサポートされません。

この手順での命名例

この手順では、全体的な名前の例を使用して、 DR グループ、ノード、および関連するスイッチを特定します。

DR グループ	site_A で cluster_A	site_B （ site_B
dr_group_1 - FC	• node_A_1 - FC • Node_a_2-FC	• node_B_1 - FC • node_B_2 - FC
dr_group_2 - IP	• node_A_1 の IP • node_A_1 の 4 - IP	• node_B_2 - IP • node_B_2 - IP
スイッチ	初期スイッチ（ファブリック接続構成の場合：） • switch_A_1 - FC • switch_A_1 - FC MetroCluster IP スイッチ： • switch_A_1 - IP • switch_a_2-ip	初期スイッチ（ファブリック接続構成の場合）： • switch_B_1 - FC • switch_B_2 - FC MetroCluster IP スイッチ： • switch_B_1 - IP • switch_B_2 - IP

MetroCluster FC から MetroCluster IP 構成への移行

MetroCluster 構成の健全性の確認

移行を実行する前に、 MetroCluster 構成の健全性と接続を確認する必要があります

1. ONTAP で MetroCluster 構成の動作を確認します。
   a. システムがマルチパスであるかどうかを確認します。「 node run -node node-name sysconfig -a ` 」
   b. 両方のクラスタにヘルスアラートがないかどうかを確認します。 'system health alert show'
   c. MetroCluster 構成と動作モードが正常であることを確認します。 MetroCluster show
   d. MetroCluster チェック「 MetroCluster check run 」を実行します
   e. MetroCluster チェックの結果を表示します。「 MetroCluster check show 」
   f. スイッチにヘルスアラートがないかどうかを確認します（ある場合）：「 storage switch show 」
   g. Config Advisor を実行します。

      "ネットアップのダウンロード： Config Advisor"

   h. Config Advisor の実行後、ツールの出力を確認し、推奨される方法で検出された問題に対処します。
2. クラスタが正常であることを確認します :cluster show

```
cluster_A::> cluster show
Node            Health  Eligibility   Epsilon
--------------- ------  -----------   -------
node_A_1_FC     true    true          false
node_A_2_FC     true    true          false

cluster_A::>
```

3. すべてのクラスタポートが up であることを確認します。「 network port show -ipspace cluster 」

```
cluster_A::> network port show -ipspace cluster

Node: node_A_1_FC

                                                  Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

Node: node_A_2_FC

                                                  Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

4 entries were displayed.

cluster_A::>
```

4. すべてのクラスタ LIF が up で動作していることを確認します。「 network interface show -vserver cluster 」

   各クラスタ LIF で、「 Is Home 」には「 true 」、「 Status Admin/Oper 」には「 up/up 」と表示される必要があります。

```
cluster_A::> network interface show -vserver cluster

            Logical      Status     Network          Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- -----
Cluster
            node_A-1_FC_clus1
                       up/up      169.254.209.69/16  node_A-1_FC   e0a
true
            node_A_1_FC_clus2
                       up/up      169.254.49.125/16  node_A_1_FC   e0b
true
            node_A_2_FC_clus1
                       up/up      169.254.47.194/16  node_A_2_FC   e0a
true
            node_A_2_FC_clus2
                       up/up      169.254.19.183/16  node_A_2_FC   e0b
true

4 entries were displayed.

cluster_A::>
```

5. すべてのクラスタ LIF で自動リバートが有効になっていることを確認します。「 network interface show -vserver Cluster -fields auto-revert

```
cluster_A::> network interface show -vserver Cluster -fields auto-revert

          Logical
Vserver   Interface     Auto-revert
--------- ------------- ------------
Cluster
           node_A_1_FC_clus1
                        true
           node_A_1_FC_clus2
                        true
           node_A_2_FC_clus1
                        true
           node_A_2_FC_clus2
                        true

    4 entries were displayed.

cluster_A::>
```

Tiebreaker またはその他の監視ソフトウェアから既存の設定を削除します

スイッチオーバーを開始できる MetroCluster Tiebreaker 構成や他社製アプリケーション（ ClusterLion など）で既存の構成を監視している場合は、移行の前に Tiebreaker またはその他のソフトウェアから MetroCluster 構成を削除する必要があります。

1. Tiebreaker ソフトウェアから既存の MetroCluster 設定を削除します。

   "MetroCluster 構成を削除しています"

2. スイッチオーバーを開始できるサードパーティ製アプリケーションから既存の MetroCluster 構成を削除します。

   アプリケーションのマニュアルを参照してください。

新しい **IP** スイッチへの **RCF** の生成と適用

MetroCluster IP 設定に新しい IP スイッチを使用する場合は、カスタム RCF ファイルでスイッチを設定する必要があります。

このタスクは、新しいスイッチを使用する場合に必要です。

既存のスイッチを使用している場合は、に進みます "ローカルクラスタ接続を移動しています"。

1. 新しい IP スイッチを設置してラックに設置します。
2. 新しい RCF ファイルを適用するための IP スイッチを準備します。

スイッチベンダーに対応するセクションを参照してください。

- "Broadcom IP スイッチを工場出荷時のデフォルトにリセットします"
- "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"
- "NVIDIA IP SN2100スイッチを工場出荷時のデフォルトにリセット"

3. 必要に応じて、スイッチのファームウェアをサポートされているバージョンにアップデートします。
4. RCF ジェネレータツールを使用してスイッチベンダーとプラットフォームモデルに応じた RCF ファイルを作成し、その後ファイルでスイッチを更新します。

   スイッチベンダーに対応するセクションを参照してください。

   - "Broadcom IPのRCFファイルをダウンロードしてインストールする"
   - "Cisco IP RCFファイルのダウンロードとインストール"
   - "NVIDIA RCFファイルをダウンロードしてインストールする"

ローカルクラスタ接続を移動します

MetroCluster FC 構成のクラスタ インターフェイスを IP スイッチに移動します。

ステップ**1: MetroCluster FC**ノード上のクラスタ接続を移動する

MetroCluster FCノード上のクラスタ接続をIPスイッチに移動します。手順は、既存のIPスイッチを使用するか、新しいIPスイッチを使用するかによって異なります。

このタスクについて

- このタスクは両方の MetroCluster サイトで実行します。

移動する接続

以下のタスクでは、コントローラモジュールがクラスタ接続に2つのポートを使用していることを前提としています。一部のコントローラモジュールモデルでは、クラスタ接続に4つ以上のポートを使用します。この例では、ポートは2つのグループに分割され、2つのグループ間でポートが交互に使用されます。

次の表に、このタスクで使用するポートの例を示します。

コントローラモジュール上のクラスタ接続の数	ポートをグループ化します	グループ B のポート
2 つ	e0a	e0b
4.	e0a 、 e0c	e0b 、 e0d

- ポートをグループ A でローカルスイッチ switch_x_1-ip に接続します。
- グループ B のポートはローカルスイッチ switch_x_2-IP に接続します。

次の表に、 FC ノードの接続先のスイッチポートを示します。Broadcom BES-53248 スイッチの場合、ポートの用途は MetroCluster IP ノードのモデルによって異なります。

スイッチモデル	MetroCluster IP ノードモデル	スイッチポート	に接続します
Cisco 3132Q-V の設定	任意	5、6	FCノード上のローカルクラスタインターフェイス
Cisco 9336C-FX2（12ポート）	任意	3、4、または11、12 注: スイッチ ポート 11 および 12 を使用するには、2 つの速度モードを選択する必要があります。	FCノード上のローカルクラスタインターフェイス
Cisco 3232C、または9336C-FX2（36ポート）	任意	5、6、または13、14 注: スイッチ ポート 13 および 14 を使用するには、2 つの速度モードを選択する必要があります。	FCノード上のローカルクラスタインターフェイス
Cisco 9336C-FX2 共有（36ポート）	任意	3、4、または11、12 注: スイッチ ポート 11 および 12 を使用するには、2 つの速度モードを選択する必要があります。	FCノード上のローカルクラスタインターフェイス
Broadcom BES-53248 の場合	FAS500f/A250	1 ~ 6	FCノード上のローカルクラスタインターフェイス
	FAS8200 / A300	3、4、9、10、11、 12.	FCノード上のローカルクラスタインターフェイス
	FAS8300 / A400 / FAS8700	1 ~ 6	FCノード上のローカルクラスタインターフェイス
NVIDIA SN2100	任意	5、6、または11、12 注: スイッチ ポート 11 および 12 を使用するには、2 つの速度モードを選択する必要があります。	FCノード上のローカルクラスタインターフェイス

新しいIPスイッチを使用するときにローカルクラスタ接続を移動する

新しい IP スイッチを使用している場合は、既存の MetroCluster FC ノードのクラスタ接続を新しいスイッチに物理的に移動します。

手順

1. MetroCluster FC ノードグループ A のクラスタ接続を新しい IP スイッチに移動します。

   で説明したポートを使用します [移動する接続]。

   a. スイッチからすべてのグループ A ポートを切断します。 MetroCluster FC 構成がスイッチレスクラスタの場合は、パートナーノードからポートを切断します。
   b. グループ A のポートを node_A_1 の FC と FC_switch_A_2 の FC から切断します。
   c. node_A_1 のグループ A のポートを、 switch_A_1 -IP の FC ノードのスイッチポートに接続します
   d. FC_switch_A_2 のグループ A のポートを switch_A_1 の FC ノードのスイッチポートに接続します
2. すべてのクラスタポートが動作していることを確認します。

   「 network port show -ipspace cluster 」のように表示されます

```
cluster_A::*> network port show -ipspace Cluster

Node: node_A_1-FC

                                                  Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

Node: node_A_2-FC

                                                  Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

4 entries were displayed.

cluster_A::*>
```

3. サイト間スイッチリンク（ISL）が稼働し、ポートチャネルが動作していることを確認します。

   「インターフェイスの概要」

   次の例では、ISLポート「Eth1/15」から「eth1/20」がリモートサイトリンクの「Po10」として設定さ

れ、「eth1/7」から「eth1/8」がローカルクラスタISLの「Po1」として設定されています。「Eth1/15」から「Eth1/20」、「Eth1/7」から「Eth1/8」、「Po10」、および「Po1」の状態は「up」にする必要があります。

```
IP_switch_A_1# show interface brief

--------------------------------------------------------------------
Port   VRF          Status   IP Address        Speed      MTU
--------------------------------------------------------------------
mgmt0  --            up        100.10.200.20    1000      1500
--------------------------------------------------------------------------------
--------
Ethernet     VLAN   Type Mode    Status     Reason               Speed
Port
Interface                                    Ch #
--------------------------------------------------------------------------------
--------

...

Eth1/7        1     eth  trunk    up        none                 100G(D)
1
Eth1/8        1     eth  trunk    up        none                 100G(D)
1

...

Eth1/15       1     eth  trunk    up        none                 100G(D)
10
Eth1/16       1     eth  trunk    up        none                 100G(D)
10
Eth1/17       1     eth  trunk    up        none                 100G(D)
10
Eth1/18       1     eth  trunk    up        none                 100G(D)
10
Eth1/19       1     eth  trunk    up        none                 100G(D)
10
Eth1/20       1     eth  trunk    up        none                 100G(D)
10

--------------------------------------------------------------------------------
--------
Port-channel VLAN  Type Mode   Status   Reason         Speed    Protocol
Interface
--------------------------------------------------------------------------------
--------
```

```
Po1          1     eth  trunk   up      none            a-100G(D) lacp
Po10         1     eth  trunk   up      none            a-100G(D) lacp
Po11         1     eth  trunk   down    No operational  auto(D)   lacp
                                        members
IP_switch_A_1#
```

4. すべてのインターフェイスが Is Home カラムに true と表示されていることを確認します。

   「 network interface show -vserver cluster 」のように表示されます

   この処理が完了するまでに数分かかることがあります。

```
cluster_A::*> network interface show -vserver cluster

            Logical      Status     Network          Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- -----
Cluster
            node_A_1_FC_clus1
                       up/up      169.254.209.69/16  node_A_1_FC   e0a
true
            node_A_1-FC_clus2
                       up/up      169.254.49.125/16  node_A_1-FC   e0b
true
            node_A_2-FC_clus1
                       up/up      169.254.47.194/16  node_A_2-FC   e0a
true
            node_A_2-FC_clus2
                       up/up      169.254.19.183/16  node_A_2-FC   e0b
true

4 entries were displayed.

cluster_A::*>
```

5. 両方のノード（ node_A_1 -FC および node_B_2 ）で上記の手順を実行して、クラスタインターフェイスのグループ B ポートを移動します。
6. パートナー・クラスタ「 cluster_B 」で上記の手順を繰り返します。

既存の**IP**スイッチを再利用するときにローカルクラスタ接続を移動する

既存の IP スイッチを再利用する場合は、ファームウェアを更新し、正しい参照構成ファイル (RCF) を使用してスイッチを再構成し、接続をスイッチごとに正しいポートに移動します。

このタスクについて

このタスクを実行する必要があるのは、 FC ノードが既存の IP スイッチに接続されており、スイッチを再利用する場合のみです。

手順

1. switch_A_1 IP に接続されているローカルクラスタ接続を切断します

   a. グループ A のポートを既存の IP スイッチから切断します。

   b. switch_A_1 の ISL ポートを切断します。

      クラスタポートの使用状況を確認するには、プラットフォームのインストールとセットアップの手順を参照してください。

      "AFF A320 システム：設置とセットアップ"

      "AFF A220 / FAS2700 システムの設置とセットアップの手順"

      "AFF A800 システムの設置とセットアップの手順"

      "AFF A300 システム『 Installation and Setup Instructions 』"

   "FAS8200 システム設置とセットアップの手順"

2. プラットフォームの組み合わせと移行用に生成された RCF ファイルを使用して switch_A_1 IP を再設定します。

   使用しているスイッチベンダーの手順の手順に従い、 MetroCluster IP Installation and Configuration_ から実行します。

   "MetroCluster IP のインストールと設定"

   a. 必要に応じて、新しいスイッチファームウェアをダウンロードしてインストールします。

      MetroCluster IP ノードでサポートされる最新のファームウェアを使用する必要があります。

      - "BroadcomスイッチのEFOSソフトウェアをダウンロードしてインストールする"
      - "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"
      - "NVIDIA Cumulusソフトウェアをダウンロードしてインストールする"

   b. 新しい RCF ファイルを適用するための IP スイッチを準備します。

      - "Broadcom IP スイッチを工場出荷時のデフォルトにリセットします"
      - "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"
      - "NVIDIA IP SN2100スイッチを工場出荷時のデフォルトにリセット"

   c. 使用しているスイッチベンダーに応じて、 IP RCF ファイルをダウンロードしてインストールします。

      - "Broadcom IP RCF ファイルのダウンロードとインストール"
      - "Cisco IP RCF ファイルのダウンロードとインストール"

- "NVIDIA RCFファイルをダウンロードしてインストールする"

3. グループ A のポートを switch_A_1 の IP に再接続します。

   で説明したポートを使用します [移動する接続]。

4. すべてのクラスタポートが動作していることを確認します。

   「 network port show -ipspace cluster 」のように表示されます

```
Cluster-A::*> network port show -ipspace cluster

Node: node_A_1_FC

                                                  Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

Node: node_A_2_FC

                                                  Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

4 entries were displayed.

Cluster-A::*>
```

5. すべてのインターフェイスがそれぞれのホームポートにあることを確認します。

   「 network interface show -vserver Cluster 」のように表示されます

```
Cluster-A::*> network interface show -vserver Cluster

            Logical      Status     Network          Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- -----
Cluster
            node_A_1_FC_clus1
                       up/up      169.254.209.69/16  node_A_1_FC   e0a
true
            node_A_1_FC_clus2
                       up/up      169.254.49.125/16  node_A_1_FC   e0b
true
            node_A_2_FC_clus1
                       up/up      169.254.47.194/16  node_A_2_FC   e0a
true
            node_A_2_FC_clus2
                       up/up      169.254.19.183/16  node_A_2_FC   e0b
true

4 entries were displayed.

Cluster-A::*>
```

6. switch_A_1 で、上記の手順をすべて繰り返します。
7. ローカルクラスタの ISL ポートを再接続します。
8. スイッチ B_1_IP およびスイッチ B_2_IP について、 site_B で上記の手順を繰り返します。
9. サイト間でリモート ISL を接続します。

ステップ**2:** クラスター接続が移動され、クラスターが正常であることを確認する

適切な接続が確保され、構成が移行プロセスを続行する準備ができていることを確認するには、クラスター接続が正しく移動され、クラスター スイッチが認識され、クラスターが正常であることを確認します。

手順

1. すべてのクラスタポートが動作していることを確認します。

   「 network port show -ipspace cluster 」のように表示されます

```
Cluster-A::*> network port show -ipspace Cluster

Node: Node-A-1-FC

                                                  Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

Node: Node-A-2-FC

                                                  Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

4 entries were displayed.

Cluster-A::*>
```

2. すべてのインターフェイスがそれぞれのホームポートにあることを確認します。

   「 network interface show -vserver Cluster 」のように表示されます

   この処理が完了するまでに数分かかることがあります。

   次に、すべてのインターフェイスの「 Is Home 」列に true が表示される例を示します。

```
Cluster-A::*> network interface show -vserver Cluster

            Logical      Status     Network          Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- -----
Cluster
            Node-A-1_FC_clus1
                       up/up      169.254.209.69/16  Node-A-1_FC   e0a
true
            Node-A-1-FC_clus2
                       up/up      169.254.49.125/16  Node-A-1-FC   e0b
true
            Node-A-2-FC_clus1
                       up/up      169.254.47.194/16  Node-A-2-FC   e0a
true
            Node-A-2-FC_clus2
                       up/up      169.254.19.183/16  Node-A-2-FC   e0b
true

4 entries were displayed.

Cluster-A::*>
```

3. 両方のローカル IP スイッチがノードで検出されたことを確認します。

   「 network device-discovery show -protocol cdp 」と入力します

```
Cluster-A::*> network device-discovery show -protocol cdp

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface         Platform
----------- ------ ------------------------- ----------------
----------------
Node-A-1-FC
           /cdp
            e0a    Switch-A-3-IP             1/5/1             N3K-
C3232C
            e0b    Switch-A-4-IP             0/5/1             N3K-
C3232C
Node-A-2-FC
           /cdp
            e0a    Switch-A-3-IP             1/6/1             N3K-
C3232C
            e0b    Switch-A-4-IP             0/6/1             N3K-
C3232C

4 entries were displayed.

Cluster-A::*>
```

4. IP スイッチで、両方のローカル IP スイッチで MetroCluster IP ノードが検出されたことを確認します。

   'How CDP Neighbors' を参照してください

   この手順は各スイッチで実行する必要があります。

   この例は、 Switch-A-3-IP でノードが検出されていることを確認する方法を示しています。

```
(Switch-A-3-IP)# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform      Port
ID
Node-A-1-FC         Eth1/5/1       133    H         FAS8200       e0a
Node-A-2-FC         Eth1/6/1       133    H         FAS8200       e0a
Switch-A-4-IP(FDO220329A4)
                    Eth1/7         175    R S I s   N3K-C3232C    Eth1/7
Switch-A-4-IP(FDO220329A4)
                    Eth1/8         175    R S I s   N3K-C3232C    Eth1/8
Switch-B-3-IP(FDO220329B3)
                    Eth1/20        173    R S I s   N3K-C3232C
Eth1/20
Switch-B-3-IP(FDO220329B3)
                    Eth1/21        173    R S I s   N3K-C3232C
Eth1/21

Total entries displayed: 4

(Switch-A-3-IP)#
```

この例は、 Switch-A-4-IP でノードが検出されていることを確認する方法を示しています。

```
(Switch-A-4-IP)# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform      Port
ID
Node-A-1-FC         Eth1/5/1       133    H         FAS8200       e0b
Node-A-2-FC         Eth1/6/1       133    H         FAS8200       e0b
Switch-A-3-IP(FDO220329A3)
                    Eth1/7         175    R S I s   N3K-C3232C    Eth1/7
Switch-A-3-IP(FDO220329A3)
                    Eth1/8         175    R S I s   N3K-C3232C    Eth1/8
Switch-B-4-IP(FDO220329B4)
                    Eth1/20        169    R S I s   N3K-C3232C
Eth1/20
Switch-B-4-IP(FDO220329B4)
                    Eth1/21        169    R S I s   N3K-C3232C
Eth1/21

Total entries displayed: 4

(Switch-A-4-IP)#
```

MetroCluster IP コントローラの準備

4 つの新しい MetroCluster IP ノードを準備し、正しいバージョンの ONTAP をインストールする必要があります。

このタスクは新しい各ノードで実行する必要があります。

- node_A_1 の IP
- Node_a_2-IP
- node_B_1 - IP
- node_B_2 - IP

この手順では、ノードの設定をクリアし、新しいドライブのメールボックスのリージョンをクリアします。

1. MetroCluster IP 構成用に新しいコントローラをラックに設置します。

   この時点では、 MetroCluster FC ノード（ node_A_1 と node_B_1 ）のケーブル接続が維持されます。

2. に示すように、 MetroCluster IP ノードを IP スイッチにケーブル接続します "IP スイッチのケーブル接続

"。

3. 次のセクションを使用して、 MetroCluster IP ノードを設定します。
   a. "必要な情報を収集"
   b. "コントローラモジュールのシステムデフォルトの復元"
   c. "コンポーネントの ha-config 状態を確認"
   d. "プール0のドライブを手動で割り当てる（ONTAP 9.4以降）"
4. 保守モードから問題 the halt コマンドを実行して保守モードを終了し、 boot_ontap コマンドを問題してシステムをブートしてクラスタセットアップを開始します。

   このとき、クラスタウィザードやノードウィザードを実行しないでください。
5. 他の MetroCluster IP ノードに対して上記の手順を繰り返します。

MetroCluster を移行対象として設定する

移行に向けた構成を準備するには、既存の MetroCluster 構成に新しいノードを追加してから、新しいノードにデータを移動します。

カスタム **AutoSupport** メッセージをメンテナンス前に送信する

メンテナンスを実行する前に、 AutoSupport an 問題 message to notify NetApp technical support that maintenance is maintenancing （メンテナンスが進行中であることをネットアップテクニカルサポートに通知する）を実行システム停止が発生したとみなしてテクニカルサポートがケースをオープンしないように、メンテナンスが進行中であることを通知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 サイトごとに実行する必要があります。

手順

1. サポートケースが自動で生成されないようにするには、メンテナンスが進行中であることを示す AutoSupport メッセージを送信します。

   「 system node AutoSupport invoke -node * -type all -message MAINT= maintenance-window-in-hours 」というメッセージが表示されます

   「 maintenance-window-in-hours 」には、メンテナンス・ウィンドウの長さを 72 時間まで指定します。この時間が経過する前にメンテナンスが完了した場合は、メンテナンス期間が終了したことを通知する AutoSupport メッセージを起動できます。

   「 system node AutoSupport invoke -node * -type all -message MAINT= end 」というメッセージが表示されます
2. パートナークラスタに対してこのコマンドを繰り返します。

移行モードを有効にしてクラスタ **HA** を無効にします

古いノードと新しいノードを MetroCluster 構成で一緒に動作できるようにし、クラスタ HA を無効にするには、 MetroCluster 移行モードを有効にする必要があります。

1. 移行を有効にします。

   a. advanced 権限レベルに切り替えます。

      「 advanced 」の権限が必要です

   b. 移行モードを有効にします。

      MetroCluster transition enable-transition-mode non-disruptive

      このコマンドは 1 つのクラスタでのみ実行してください。

```
cluster_A::*> metrocluster transition enable -transition-mode non-
disruptive

Warning: This command enables the start of a "non-disruptive"
MetroCluster
         FC-to-IP transition. It allows the addition of hardware for
another DR
         group that uses IP fabrics, and the removal of a DR group that
uses FC
         fabrics. Clients will continue to access their data during a
         non-disruptive transition.

         Automatic unplanned switchover will also be disabled by this
command.
Do you want to continue? {y|n}: y

cluster_A::*>
```

   a. admin 権限レベルに戻ります。

      「特権管理者」

2. 両方のクラスタで移行が有効になっていることを確認します。

```
cluster_A::> metrocluster transition show-mode
Transition Mode

non-disruptive

cluster_A::*>


cluster_B::*> metrocluster transition show-mode
Transition Mode

non-disruptive

Cluster_B::>
```

3. クラスタ HA を無効にします。

   このコマンドは両方のクラスタで実行する必要があります。

```
cluster_A::*> cluster ha modify -configured false

Warning: This operation will unconfigure cluster HA. Cluster HA must be
configured on a two-node cluster to ensure data access availability in
the event of storage failover.
Do you want to continue? {y|n}: y
Notice: HA is disabled.

cluster_A::*>


cluster_B::*> cluster ha modify -configured false

Warning: This operation will unconfigure cluster HA. Cluster HA must be
configured on a two-node cluster to ensure data access availability in
the event of storage failover.
Do you want to continue? {y|n}: y
Notice: HA is disabled.

cluster_B::*>
```

4. クラスタ HA が無効になっていることを確認する。

   このコマンドは両方のクラスタで実行する必要があります。

```
cluster_A::> cluster ha show

High Availability Configured: false
Warning: Cluster HA has not been configured. Cluster HA must be
configured
on a two-node cluster to ensure data access availability in the
event of storage failover. Use the "cluster ha modify -configured
true" command to configure cluster HA.

cluster_A::>

cluster_B::> cluster ha show

High Availability Configured: false
Warning: Cluster HA has not been configured. Cluster HA must be
configured
on a two-node cluster to ensure data access availability in the
event of storage failover. Use the "cluster ha modify -configured
true" command to configure cluster HA.

cluster_B::>
```

MetroCluster IP ノードのクラスタへの追加

4 つの新しい MetroCluster IP ノードを既存の MetroCluster 構成に追加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クラスタで実行する必要があります。

手順

1. 既存の MetroCluster 構成に MetroCluster IP ノードを追加
   a. 最初のMetroCluster IPノード（node_A_1のIP）を既存のMetroCluster FC構成に追加します。

```
Welcome to the cluster setup wizard.

You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the cluster setup wizard.
     Any changes you made before quitting will be saved.

You can return to cluster setup at any time by typing "cluster
setup".
To accept a default or omit a question, do not enter a value.
```

```
This system will send event messages and periodic reports to NetApp
Technical
Support. To disable this feature, enter autosupport modify -support
disable
within 24 hours.

Enabling AutoSupport can significantly speed problem determination
and
resolution, should a problem occur on your system.
For further information on AutoSupport, see:
http://support.netapp.com/autosupport/

Type yes to confirm and continue {yes}: yes

Enter the node management interface port [e0M]:
Enter the node management interface IP address: 172.17.8.93
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 172.17.8.93
has been created.

Use your web browser to complete cluster setup by accessing
https://172.17.8.93

Otherwise, press Enter to complete cluster setup using the command
line
interface:

Do you want to create a new cluster or join an existing cluster?
{create, join}:
join


Existing cluster interface configuration found:

Port    MTU     IP              Netmask
e0c     9000    169.254.148.217 255.255.0.0
e0d     9000    169.254.144.238 255.255.0.0

Do you want to use this configuration? {yes, no} [yes]: yes
.
.
.
```

b. 2つ目のMetroCluster IPノード（node_A_1の4つのIP）を既存のMetroCluster FC構成に追加します。

2. 同じ手順を繰り返して、node_B_1のIPとnode_B_2のIPをcluster_Bに追加します
3. オンボード キー マネージャーを使用している場合は、新しいノードを追加したクラスターから次の手順を実行します。
   a. キー マネージャーの構成を同期します。

      「セキュリティキーマネージャオンボード同期」

   b. プロンプトが表示されたら、オンボード キー マネージャーのパスフレーズを入力します。

クラスタ間 **LIF** の設定、 **MetroCluster** インターフェイスの作成、およびルートアグリゲートのミラーリングを行います

クラスタピア LIF を作成し、新しい MetroCluster IP ノードに MetroCluster インターフェイスを作成する必要があります。

このタスクについて

例で使用しているホームポートはプラットフォーム固有です。MetroCluster IP ノードプラットフォームに固有の適切なホームポートを使用する必要があります。

手順

1. 新しい MetroCluster IP ノードで、 "クラスタ間 LIF を設定"。
2. 各サイトで、クラスタピアリングが設定されていることを確認します。

   cluster peer show

   次の例は、 cluster_A のクラスタピアリング設定を示しています。

```
cluster_A:> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability
Authentication
------------------------- --------------------- --------------
--------------
cluster_B                 1-80-000011           Available      ok
```

   次の例は、 cluster_B でのクラスタピアリング設定を示しています。

```
cluster_B:> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability
Authentication
------------------------- --------------------- --------------
--------------
cluster_A 1-80-000011 Available ok
```

3. MetroCluster IP ノードの DR グループを設定します。

   MetroCluster 構成設定 dr-group create -partner-cluster

```
cluster_A::> metrocluster configuration-settings dr-group create
-partner-cluster
cluster_B -local-node node_A_3-IP -remote-node node_B_3-IP
[Job 259] Job succeeded: DR Group Create is successful.
cluster_A::>
```

4. DR グループが作成されたことを確認します。

「 MetroCluster configurion-settings dr-group show 」を参照してください

```
cluster_A::> metrocluster configuration-settings dr-group show

DR Group ID Cluster                    Node               DR Partner
Node
----------- -------------------------- -----------------
-----------------
2           cluster_A
                                       node_A_3-IP        node_B_3-IP
                                       node_A_4-IP        node_B_4-IP
            cluster_B
                                       node_B_3-IP        node_A_3-IP
                                       node_B_4-IP        node_A_4-IP

4 entries were displayed.

cluster_A::>
```

「 MetroCluster configurion-settings dr-group show 」コマンドを実行した場合、古い MetroCluster FC ノード（ DR グループ 1 ）の DR グループは表示されません。

両方のサイトで「 MetroCluster node show 」コマンドを使用すると、すべてのノードを一覧表示できます。

```
cluster_A::> metrocluster node show

DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
              node_A_1-FC         configured     enabled   normal
              node_A_2-FC         configured     enabled   normal
      cluster_B
              node_B_1-FC         configured     enabled   normal
              node_B_2-FC         configured     enabled   normal
2     cluster_A
              node_A_3-IP      ready to configure
                                                 -         -
              node_A_4-IP      ready to configure
                                                 -         -

cluster_B::> metrocluster node show

DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_B
              node_B_1-FC         configured     enabled   normal
              node_B_2-FC         configured     enabled   normal
      cluster_A
              node_A_1-FC         configured     enabled   normal
              node_A_2-FC         configured     enabled   normal
2     cluster_B
              node_B_3-IP      ready to configure
                                                 -         -
              node_B_4-IP      ready to configure
                                                 -         -
```

5. 新しく参加した MetroCluster IP ノードの MetroCluster IP 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 構成設定インターフェイス create-cluster-name

を参照してください "MetroCluster IP インターフェイスの設定と接続" IP インターフェイスを設定する際の考慮事項については、を参照して

どちらのクラスタからも MetroCluster IP インターフェイスを設定できます。

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_3-IP -home-port e1a -address
172.17.26.10 -netmask 255.255.255.0
[Job 260] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_3-IP -home-port e1b -address
172.17.27.10 -netmask 255.255.255.0
[Job 261] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_4-IP -home-port e1a -address
172.17.26.11 -netmask 255.255.255.0
[Job 262] Job succeeded: Interface Create is successful.

cluster_A::> :metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_4-IP -home-port e1b -address
172.17.27.11 -netmask 255.255.255.0
[Job 263] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_3-IP -home-port e1a -address
172.17.26.12 -netmask 255.255.255.0
[Job 264] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_3-IP -home-port e1b -address
172.17.27.12 -netmask 255.255.255.0
[Job 265] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_4-IP -home-port e1a -address
172.17.26.13 -netmask 255.255.255.0
[Job 266] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_4-IP -home-port e1b -address
172.17.27.13 -netmask 255.255.255.0
[Job 267] Job succeeded: Interface Create is successful.
```

6. MetroCluster IP インターフェイスが作成されたことを確認します。

「 MetroCluster configurion-settings interface show 」を参照してください

```
cluster_A::>metrocluster configuration-settings interface show

DR
Config
Group Cluster Node    Network Address Netmask         Gateway
State
----- ------- ------- --------------- --------------- ---------------
---------
2     cluster_A
             node_A_3-IP
                 Home Port: e1a
                      172.17.26.10    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.10    255.255.255.0   -
completed
              node_A_4-IP
                 Home Port: e1a
                      172.17.26.11    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.11    255.255.255.0   -
completed
      cluster_B
             node_B_3-IP
                 Home Port: e1a
                      172.17.26.13    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.13    255.255.255.0   -
completed
              node_B_3-IP
                 Home Port: e1a
                      172.17.26.12    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.12    255.255.255.0   -
completed
8 entries were displayed.

cluster_A>
```

7. MetroCluster IP インターフェイスを接続します。

   MetroCluster 構成設定接続接続

このコマンドの実行には数分かかることがあります。

```
cluster_A::> metrocluster configuration-settings connection connect

cluster_A::>
```

8. 接続が正しく確立されたことを確認します。

「 MetroCluster configurion-settings connection show 」を参照してください

```
cluster_A::> metrocluster configuration-settings connection show

DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
2     cluster_A
              node_A_3-IP**
                 Home Port: e1a
                      172.17.26.10    172.17.26.11    HA Partner
completed
                 Home Port: e1a
                      172.17.26.10    172.17.26.12    DR Partner
completed
                 Home Port: e1a
                      172.17.26.10    172.17.26.13    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.27.10    172.17.27.11    HA Partner
completed
                 Home Port: e1b
                      172.17.27.10    172.17.27.12    DR Partner
completed
                 Home Port: e1b
                      172.17.27.10    172.17.27.13    DR Auxiliary
completed
              node_A_4-IP
                 Home Port: e1a
                      172.17.26.11    172.17.26.10    HA Partner
completed
                 Home Port: e1a
                      172.17.26.11    172.17.26.13    DR Partner
completed
```

```
                 Home Port: e1a
                      172.17.26.11    172.17.26.12    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.27.11    172.17.27.10    HA Partner
completed
                 Home Port: e1b
                      172.17.27.11    172.17.27.13    DR Partner
completed
                 Home Port: e1b
                      172.17.27.11    172.17.27.12    DR Auxiliary
completed

DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
2     cluster_B
              node_B_4-IP
                 Home Port: e1a
                      172.17.26.13    172.17.26.12    HA Partner
completed
                 Home Port: e1a
                      172.17.26.13    172.17.26.11    DR Partner
completed
                 Home Port: e1a
                      172.17.26.13    172.17.26.10    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.27.13    172.17.27.12    HA Partner
completed
                 Home Port: e1b
                      172.17.27.13    172.17.27.11    DR Partner
completed
                 Home Port: e1b
                      172.17.27.13    172.17.27.10    DR Auxiliary
completed
              node_B_3-IP
                 Home Port: e1a
                      172.17.26.12    172.17.26.13    HA Partner
completed
                 Home Port: e1a
                      172.17.26.12    172.17.26.10    DR Partner
completed
                 Home Port: e1a
```

```
                      172.17.26.12    172.17.26.11    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.27.12    172.17.27.13    HA Partner
completed
                 Home Port: e1b
                      172.17.27.12    172.17.27.10    DR Partner
completed
                 Home Port: e1b
                      172.17.27.12    172.17.27.11    DR Auxiliary
completed
24 entries were displayed.

cluster_A::>
```

9. ディスクの自動割り当てとパーティショニングを確認します。

   「 Disk show -pool Pool1 」

```
cluster_A::> disk show -pool Pool1
                     Usable           Disk    Container   Container
Disk                   Size Shelf Bay Type    Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
1.10.4                    -    10   4 SAS     remote      -
node_B_2
1.10.13                   -    10  13 SAS     remote      -
node_B_2
1.10.14                   -    10  14 SAS     remote      -
node_B_1
1.10.15                   -    10  15 SAS     remote      -
node_B_1
1.10.16                   -    10  16 SAS     remote      -
node_B_1
1.10.18                   -    10  18 SAS     remote      -
node_B_2
...
2.20.0                546.9GB    20   0 SAS     aggregate   aggr0_rha1_a1
node_a_1
2.20.3                546.9GB    20   3 SAS     aggregate   aggr0_rha1_a2
node_a_2
2.20.5                546.9GB    20   5 SAS     aggregate   rha1_a1_aggr1
node_a_1
2.20.6                546.9GB    20   6 SAS     aggregate   rha1_a1_aggr1
node_a_1
2.20.7                546.9GB    20   7 SAS     aggregate   rha1_a2_aggr1
node_a_2
2.20.10               546.9GB    20  10 SAS     aggregate   rha1_a1_aggr1
node_a_1
...
43 entries were displayed.
cluster_A::>
```

アドバンストドライブパーティショニング（ADP）用に構成されたシステムでは、次の出力例のようにコンテナタイプが「remote」ではなく「shared」になっています。

10. ルートアグリゲートをミラーします。

```
storage aggregate mirror -aggregate aggr0_node_A_3_IP
```

この手順は MetroCluster IP ノードごとに実行する必要があります。

```
cluster_A::> aggr mirror -aggregate aggr0_node_A_3_IP

Info: Disks would be added to aggregate "aggr0_node_A_3_IP"on node
"node_A_3-IP"
      in the following manner:

      Second Plex

        RAID Group rg0, 3 disks (block checksum, raid_dp)
                                                                  Usable
Physical
          Position   Disk                      Type           Size
Size
          ---------- ------------------------- ---------- --------
--------
          dparity    4.20.0                    SAS               -
-
          parity     4.20.3                    SAS               -
-
          data       4.20.1                    SAS         546.9GB
558.9GB

      Aggregate capacity available for volume use would be 467.6GB.

Do you want to continue? {y|n}: y

cluster_A::>
```

11. ルートアグリゲートがミラーされたことを確認します。

「 storage aggregate show

```
cluster_A::> aggr show

Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
aggr0_node_A_1_FC
           349.0GB   16.84GB   95% online       1 node_A_1-FC
raid_dp,

mirrored,

normal
```

```
aggr0_node_A_2_FC
           349.0GB   16.84GB   95% online       1 node_A_2-FC
raid_dp,

mirrored,

normal
aggr0_node_A_3_IP
           467.6GB   22.63GB   95% online       1 node_A_3-IP
raid_dp,

mirrored,

normal
aggr0_node_A_4_IP
           467.6GB   22.62GB   95% online       1 node_A_4-IP
raid_dp,

mirrored,

normal
aggr_data_a1
            1.02TB    1.01TB    1% online       1 node_A_1-FC
raid_dp,

mirrored,

normal
aggr_data_a2
            1.02TB    1.01TB    1% online       1 node_A_2-FC
raid_dp,

mirrored,
```

MetroCluster IP ノードの追加を完了しています

新しい DR グループを MetroCluster 構成に組み込み、新しいノードにミラーされたデータアグリゲートを作成する必要があります。

手順

1. 両方のクラスタに単一のデータ アグリゲートがあるか複数のデータ アグリゲートがあるかに応じて MetroCluster を構成します。

MetroCluster 構成の内容	操作

両方のクラスター上の複数のデータ集約	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>` 「 MetroCluster configure 」と「 MetroCluster configure -refresh true 」ではなく「 * 」を実行する必要があります
両方のクラスタにミラーリングされた単一のデータ集約	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 と応答する必要があります `y` advancedモードで続けるかどうかを尋ねられたら、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 <node-name>` c. admin 権限レベルに戻ります。 「特権管理者」

ミラーされたデータアグリゲートを複数使用することを推奨します。ミラーされたアグリゲートが1つしかない場合、メタデータボリュームは別 々 のアグリゲートではなく同じアグリゲートに配置されるため、保護レベルは低くなります。

2. 新しい各ノードをリブートします。

```
node reboot -node <node_name> -inhibit-takeover true
```

ノードを特定の順序でリブートする必要はありませんが、1つのノードが完全にブートしてすべての接続が確立されるまで待ってから、次のノードをリブートしてください。

3. ノードが対応する DR グループに追加されたことを確認します。

MetroCluster node show

```
cluster_A::> metrocluster node show

DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
              node-A-1-FC        configured     enabled   normal
              node-A-2-FC        configured     enabled   normal
      Cluster-B
              node-B-1-FC        configured     enabled   normal
              node-B-2-FC        configured     enabled   normal
2     cluster_A
              node-A-3-IP        configured     enabled   normal
              node-A-4-IP        configured     enabled   normal
      Cluster-B
              node-B-3-IP        configured     enabled   normal
              node-B-4-IP        configured     enabled   normal
8 entries were displayed.

cluster_A::>
```

4. 新しい MetroCluster ノードのそれぞれで、ミラーされたデータアグリゲートを作成します。

「 storage aggregate create -aggregate aggregate-name -node node-name -diskcount no-disks-mirror true 」のように指定します

> ミラーされたデータアグリゲートをサイトごとに少なくとも1つ作成する必要があります。MDVボリュームをホストするために、サイトごとに2つのミラーされたデータアグリゲートをMetroCluster IPノード上に配置することを推奨しますが、サイトごとに1つのアグリゲートがサポートされます（ただし推奨されません）。MetroClusterの一方のサイトにミラーされたデータアグリゲートが1つあり、もう一方のサイトに複数のミラーされたデータアグリゲートがあります。

次の例は、node_A_1のIP上にアグリゲートを作成します。

```
cluster_A::> storage aggregate create -aggregate data_a3 -node node_A_3-
IP -diskcount 10 -mirror t

Info: The layout for aggregate "data_a3" on node "node_A_3-IP" would be:

      First Plex

        RAID Group rg0, 5 disks (block checksum, raid_dp)
                                                              Usable
Physical
```

```
          Position   Disk                      Type           Size
Size
          ---------- ------------------------- ---------- --------
--------
          dparity    5.10.15                   SAS               -
-
          parity     5.10.16                   SAS               -
-
          data       5.10.17                   SAS         546.9GB
547.1GB
          data       5.10.18                   SAS         546.9GB
558.9GB
          data       5.10.19                   SAS         546.9GB
558.9GB

      Second Plex

        RAID Group rg0, 5 disks (block checksum, raid_dp)
                                                            Usable
Physical
          Position   Disk                      Type           Size
Size
          ---------- ------------------------- ---------- --------
--------
          dparity    4.20.17                   SAS               -
-
          parity     4.20.14                   SAS               -
-
          data       4.20.18                   SAS         546.9GB
547.1GB
          data       4.20.19                   SAS         546.9GB
547.1GB
          data       4.20.16                   SAS         546.9GB
547.1GB

      Aggregate capacity available for volume use would be 1.37TB.

Do you want to continue? {y|n}: y
[Job 440] Job succeeded: DONE

cluster_A::>
```

5. クラスタ内のすべてのノードが正常であることを確認します。

   「 cluster show 」を参照してください

出力に `true` をクリックします `health` すべてのノードのフィールド。

6. 両方のクラスタで次のコマンドを実行して、テイクオーバーが可能で、ノードが接続されていることを確認します。

   「 storage failover show 」をクリックします

```
cluster_A::> storage failover show
                                    Takeover
Node           Partner              Possible    State Description
-------------- -------------------- ---------   ------------------
Node_FC_1      Node_FC_2              true      Connected to Node_FC_2
Node_FC_2      Node_FC_1              true      Connected to Node_FC_1
Node_IP_1      Node_IP_2              true      Connected to Node_IP_2
Node_IP_2      Node_IP_1              true      Connected to Node_IP_1
```

7. 新しく追加したMetroCluster IPノードに接続されているすべてのディスクがあることを確認します。

   「ディスクショー」

8. 次のコマンドを実行して、MetroCluster構成の健全性を確認します。
   a. 「 MetroCluster check run 」のようになります
   b. MetroCluster チェックショー
   c. MetroCluster interconnect mirror show
   d. MetroCluster インターコネクト・アダプタ・ショー
9. advanced 権限で、 MDV_CRS ボリュームを古いノードから新しいノードに移動します。
   a. ボリュームを表示して MDV ボリュームを特定します。

      各サイトにミラーされたデータアグリゲートが 1 つある場合、両方の MDV ボリュームをこの 1 つのアグリゲートに移動します。ミラーされたデータアグリゲートが 2 つ以上ある場合、各 MDV ボリュームを別々のアグリゲートに移動します。

      次の例は、 volume show の出力にある MDV ボリュームを示しています。

```
cluster_A::> volume show
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
...

cluster_A   MDV_CRS_2c78e009ff5611e9b0f300a0985ef8c4_A
                       aggr_b1      -          RW            -
-     -
cluster_A   MDV_CRS_2c78e009ff5611e9b0f300a0985ef8c4_B
                       aggr_b2      -          RW            -
-     -
cluster_A   MDV_CRS_d6b0b313ff5611e9837100a098544e51_A
                       aggr_a1      online     RW         10GB
9.50GB    0%
cluster_A   MDV_CRS_d6b0b313ff5611e9837100a098544e51_B
                       aggr_a2      online     RW         10GB
9.50GB    0%
...
11 entries were displayed.mple
```

b. advanced 権限レベルを設定します。

「 advanced 」の権限が必要です

c. MDV ボリュームを 1 つずつ移動します。

'volume move start -volume MDV_volume-destination-aggregate aggr-on -new-node-vserver -name

次の例は、 MDV_CRS_d6b0b313ff5611e9837100a098544e51_a を node_A_1 のアグリゲートに移動するコマンドと出力を示しています。

```
cluster_A::*> vol move start -volume
MDV_CRS_d6b0b313ff5611e9837100a098544e51_A -destination-aggregate
data_a3 -vserver cluster_A

Warning: You are about to modify the system volume
         "MDV_CRS_d6b0b313ff5611e9837100a098544e51_A". This might
cause severe
         performance or stability problems. Do not proceed unless
directed to
         do so by support. Do you want to proceed? {y|n}: y
[Job 494] Job is queued: Move
"MDV_CRS_d6b0b313ff5611e9837100a098544e51_A" in Vserver "cluster_A"
to aggregate "data_a3". Use the "volume move show -vserver cluster_A
-volume MDV_CRS_d6b0b313ff5611e9837100a098544e51_A" command to view
the status of this operation.
```

d. volume show コマンドを使用して、 MDV ボリュームが正常に移動されたことを確認します。

volume show MDV_name

次の出力は、 MDV ボリュームが移動されたことを示しています。

```
cluster_A::*> vol show MDV_CRS_d6b0b313ff5611e9837100a098544e51_B
Vserver     Volume       Aggregate    State      Type       Size
Available Used%
---------   ------------ ------------ ---------- ---- ----------
---------- -----
cluster_A   MDV_CRS_d6b0b313ff5611e9837100a098544e51_B
                      aggr_a2      online     RW         10GB
9.50GB    0%
```

a. admin モードに戻ります。

「特権管理者」

新しいドライブシェルフへのデータの移動

移行時に、 MetroCluster FC 構成のドライブシェルフから新しい MetroCluster IP 構成へデータを移動します。

作業を開始する前に

新しいアグリゲートにボリュームを移動する前に、デスティネーションノードまたはIPノードに新しいSAN LIFを作成し、ホストを接続する必要があります。

1. サポートケースの自動生成を再開するには、メンテナンスが完了したことを示す AutoSupport メッセージ

を送信します。

a. 問題次のコマンドを実行します。「 system node AutoSupport invoke -node * -type all -message MAINT=end 」

b. パートナークラスタに対してこのコマンドを繰り返します。

2. 新しいコントローラ上のアグリゲートに、一度に 1 つのボリュームずつデータボリュームを移動します。

   の手順を使用します "アグリゲートの作成と新しいノードへのボリュームの移動"。

3. 追加したノードに SAN LIF を作成します。

   の次の手順を使用します "新しいノードの LUN パスを更新しています"。

4. FC ノードにノードロックライセンスがあるかどうかを確認します。ある場合は、新しく追加したノードに追加する必要があります。

   の次の手順を使用します "ノードロックライセンスを追加しています"。

5. データ LIF を移行

   の手順を使用します "SAN 以外のデータ LIF とクラスタ管理 LIF を新しいノードに移動する" クラスタ管理 LIF を移行する手順は、 do * not * ：最後の 2 つの手順で行ってください。

- VMware vStorage APIs for Array Integration （ VAAI ）でコピーオフロード処理に使用されている LIF を移行することはできません。
- MetroCluster ノードのFCからIPへの移行が完了したあと、iSCSIホスト接続を新しいノードに移動しなければならない場合があります。を参照してください "Linux iSCSIホストをMetroCluster FCノードからMetroCluster IPノードに移動しています。"

MetroCluster FC コントローラの取り外し

クリーンアップタスクを実行し、古いコントローラモジュールを MetroCluster 構成から取り外す必要があります。

1. サポートケースが自動で生成されないようにするには、メンテナンスが進行中であることを示す AutoSupport メッセージを送信します。

   a. 問題次のコマンドを実行します。「 system node AutoSupport invoke -node * -type all -message MAINT= maintenance-window-in-hours 」

      maintenance-window-in-hours にはメンテナンス時間の長さを指定します。最大値は 72 時間です。この時間が経過する前にメンテナンスが完了した場合は、メンテナンス期間の終了を通知する AutoSupport メッセージ「 'System node AutoSupport invoke -node * -type all -message MAINT=end` 」を起動できます

   b. パートナークラスタに対してこのコマンドを繰り返します。

2. 削除が必要な MetroCluster FC 構成でホストされているアグリゲートを特定します。

   この例では、 MetroCluster FC cluster_B によってホストされている次のデータアグリゲートを削除する必要があります。 aggr_data_A1 と aggr_data_A2 。

両方のクラスタでデータアグリゲートを特定、オフライン、および削除するには、次の手順を実行する必要があります。この例は、 1 つのクラスタだけを対象としています。

```
cluster_B::> aggr show

Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
aggr0_node_A_1-FC
           349.0GB   16.83GB   95% online       1 node_A_1-FC
raid_dp,

mirrored,

normal
aggr0_node_A_2-FC
           349.0GB   16.83GB   95% online       1 node_A_2-FC
raid_dp,

mirrored,

normal
aggr0_node_A_3-IP
           467.6GB   22.63GB   95% online       1 node_A_3-IP
raid_dp,

mirrored,

normal
aggr0_node_A_3-IP
           467.6GB   22.62GB   95% online       1 node_A_4-IP
raid_dp,

mirrored,

normal
aggr_data_a1
            1.02TB    1.02TB    0% online       0 node_A_1-FC
raid_dp,

mirrored,

normal
aggr_data_a2
```

```
            1.02TB    1.02TB    0% online       0 node_A_2-FC
raid_dp,

mirrored,

normal
aggr_data_a3
            1.37TB    1.35TB    1% online       3 node_A_3-IP
raid_dp,

mirrored,

normal
aggr_data_a4
            1.25TB    1.24TB    1% online       2 node_A_4-IP
raid_dp,

mirrored,

normal
8 entries were displayed.

cluster_B::>
```

3. FC ノード上のデータアグリゲートに MDV_AUD ボリュームがあるかどうかを確認し、アグリゲートを削除する前にそれらを削除してください。

   MDV_AUD ボリュームは移動できないため、削除する必要があります。

4. 各データアグリゲートをオフラインにしてから削除します。

   a. アグリゲートをオフラインにします。「 storage aggregate offline -aggregate aggregate-name 」

      次の例は、aggr_data_A1アグリゲートをオフラインにします。

      ```
      cluster_B::> storage aggregate offline -aggregate aggr_data_a1

      Aggregate offline successful on aggregate: aggr_data_a1
      ```

   b. アグリゲート「 storage aggregate delete -aggregate aggregate-name 」を削除します

      プロンプトが表示されたら、プレックスを破棄できます。

      次の例は、aggr_data_A1アグリゲートを削除する方法を示しています。

```
cluster_B::> storage aggregate delete -aggregate aggr_data_a1
Warning: Are you sure you want to destroy aggregate "aggr_data_a1"?
{y|n}: y
[Job 123] Job succeeded: DONE

cluster_B::>
```

5. 削除が必要な MetroCluster FC DR グループを特定します。

   次の例では、 MetroCluster FC ノードが DR グループ「 1 」に含まれており、これは削除する必要がある DR グループです。

```
cluster_B::> metrocluster node show

DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
              node_A_1-FC        configured     enabled   normal
              node_A_2-FC        configured     enabled   normal
      cluster_B
              node_B_1-FC        configured     enabled   normal
              node_B_2-FC        configured     enabled   normal
2     cluster_A
              node_A_3-IP        configured     enabled   normal
              node_A_4-IP        configured     enabled   normal
      cluster_B
              node_B_3-IP        configured     enabled   normal
              node_B_3-IP        configured     enabled   normal
8 entries were displayed.

cluster_B::>
```

6. クラスタ管理 LIF を MetroCluster FC ノードから MetroCluster IP ノードに移動します。「 cluster_B ：： > network interface migrate -vserver SVM_name -lif cluster_mgmt -destination -node node -in-MetroCluster -IP-DR-group-destination -port available -port
7. クラスタ管理 LIF のホームノードとホームポートを変更します。「 cluster_B ：： > network interface modify -vserver SVM_name -lif cluster_mgmt -service -policy default -management-home-node node-inMetroCluster-IP-DR-group-home-port lif-port
8. MetroCluster FC ノードから MetroCluster IP ノードにイプシロンを移動します。
   a. 現在イプシロンが設定されているノードを特定します。 cluster show -fields epsilon

```
cluster_B::> cluster show -fields epsilon
node             epsilon
---------------- -------
node_A_1-FC      true
node_A_2-FC      false
node_A_1-IP      false
node_A_2-IP      false
4 entries were displayed.
```

b. MetroCluster FC ノード（ node_A_1 の FC ）でイプシロンを false に設定します。 cluster modify -node fc -node-epsilon false

c. MetroCluster IP ノード（ node_A_1 の IP ）でイプシロンを true に設定します。 cluster modify -node IP-node-epsilon true

d. イプシロンが正しいノードに移動したことを確認します。 cluster show -fields epsilon

```
cluster_B::> cluster show -fields epsilon
node             epsilon
---------------- -------
node_A_1-FC      false
node_A_2-FC      false
node_A_1-IP      true
node_A_2-IP      false
4 entries were displayed.
```

9. 各クラスタの移行したIPノードのクラスタピアのIPアドレスを変更します。

a. を使用して、cluster_Aピアを特定します `cluster peer show` コマンドを実行します

```
cluster_A::> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability
Authentication
------------------------- --------------------- --------------
--------------
cluster_B         1-80-000011           Unavailable    absent
```

i. cluster_AピアのIPアドレスを変更します。

```
cluster peer modify -cluster cluster_A -peer-addrs node_A_3_IP -address
-family ipv4
```

b. を使用して、cluster_Bピアを特定します `cluster peer show` コマンドを実行します

```
cluster_B::> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability
Authentication
------------------------- --------------------- --------------
--------------
cluster_A         1-80-000011           Unavailable    absent
```

i. cluster_BピアのIPアドレスを変更します。

```
cluster peer modify -cluster cluster_B -peer-addrs node_B_3_IP -address
-family ipv4
```

c. 各クラスタのクラスタピアIPアドレスが更新されていることを確認します。

i. を使用して、各クラスタのIPアドレスが更新されていることを確認します `cluster peer show -instance` コマンドを実行します

。 `Remote Intercluster Addresses` 次の例のフィールドには、更新されたIPアドレスが表示されます。

cluster_Aの例：

```
cluster_A::> cluster peer show -instance

Peer Cluster Name: cluster_B
           Remote Intercluster Addresses: 172.21.178.204,
172.21.178.212
      Availability of the Remote Cluster: Available
                     Remote Cluster Name: cluster_B
                     Active IP Addresses: 172.21.178.212,
172.21.178.204
                   Cluster Serial Number: 1-80-000011
                    Remote Cluster Nodes: node_B_3-IP,
                                          node_B_4-IP
                   Remote Cluster Health: true
                 Unreachable Local Nodes: -
          Address Family of Relationship: ipv4
    Authentication Status Administrative: use-authentication
       Authentication Status Operational: ok
                         Last Update Time: 4/20/2023 18:23:53
            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

cluster_A::>
```

+
たとえば、cluster_Bです

```
cluster_B::> cluster peer show -instance

                          Peer Cluster Name: cluster_A
              Remote Intercluster Addresses: 172.21.178.188, 172.21.178.196
<<<<<<<< Should reflect the modified address
      Availability of the Remote Cluster: Available
                     Remote Cluster Name: cluster_A
                     Active IP Addresses: 172.21.178.196, 172.21.178.188
                   Cluster Serial Number: 1-80-000011
                    Remote Cluster Nodes: node_A_3-IP,
                                          node_A_4-IP
                   Remote Cluster Health: true
                 Unreachable Local Nodes: -
          Address Family of Relationship: ipv4
    Authentication Status Administrative: use-authentication
       Authentication Status Operational: ok
                         Last Update Time: 4/20/2023 18:23:53
            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

cluster_B::>
```

10. 各クラスタで、古いノードを含む DR グループを MetroCluster FC 構成から削除します。

    この手順は、両方のクラスタで一度に 1 つずつ実行する必要があります。

```
cluster_B::> metrocluster remove-dr-group -dr-group-id 1

Warning: Nodes in the DR group that are removed from the MetroCluster
         configuration will lose their disaster recovery protection.

         Local nodes "node_A_1-FC, node_A_2-FC" will be removed from the
         MetroCluster configuration. You must repeat the operation on
the
         partner cluster "cluster_B" to remove the remote nodes in the
DR group.
Do you want to continue? {y|n}: y

Info: The following preparation steps must be completed on the local and
partner
      clusters before removing a DR group.

      1. Move all data volumes to another DR group.
      2. Move all MDV_CRS metadata volumes to another DR group.
      3. Delete all MDV_aud metadata volumes that may exist in the DR
group to
      be removed.
      4. Delete all data aggregates in the DR group to be removed. Root
      aggregates are not deleted.
      5. Migrate all data LIFs to home nodes in another DR group.
      6. Migrate the cluster management LIF to a home node in another DR
group.
      Node management and inter-cluster LIFs are not migrated.
      7. Transfer epsilon to a node in another DR group.

      The command is vetoed ifthe preparation steps are not completed on
the
      local and partner clusters.
Do you want to continue? {y|n}: y
[Job 513] Job succeeded: Remove DR Group is successful.

cluster_B::>
```

11. ノードをクラスタから削除する準備が完了していることを確認します。

    この手順は両方のクラスタで実行する必要があります。

    この時点で、 MetroCluster node show コマンドはローカル MetroCluster FC ノードのみを表示し、パートナークラスタの一部であるノードは表示しなくなります。

```
cluster_B::> metrocluster node show

DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
              node_A_1-FC        ready to configure
                                                -         -
              node_A_2-FC        ready to configure
                                                -         -
2     cluster_A
              node_A_3-IP        configured     enabled   normal
              node_A_4-IP        configured     enabled   normal
      cluster_B
              node_B_3-IP        configured     enabled   normal
              node_B_4-IP        configured     enabled   normal
6 entries were displayed.

cluster_B::>
```

12. MetroCluster FC ノードのストレージフェイルオーバーを無効にします。

    この手順は各ノードで実行する必要があります。

```
cluster_A::> storage failover modify -node node_A_1-FC -enabled false
cluster_A::> storage failover modify -node node_A_2-FC -enabled false
cluster_A::>
```

13. クラスタから MetroCluster FC ノードを分離します cluster unjoin -node node-name

    この手順は各ノードで実行する必要があります。

```
cluster_A::> cluster unjoin -node node_A_1-FC

Warning: This command will remove node "node_A_1-FC"from the cluster.
You must
         remove the failover partner as well. After the node is removed,
erase
         its configuration and initialize all disks by usingthe "Clean
         configuration and initialize all disks (4)" option from the
boot menu.
Do you want to continue? {y|n}: y
[Job 553] Job is queued: Cluster remove-node of Node:node_A_1-FC with
UUID:6c87de7e-ff54-11e9-8371
[Job 553] Checking prerequisites
[Job 553] Cleaning cluster database
[Job 553] Job succeeded: Node remove succeeded
If applicable, also remove the node's HA partner, and then clean its
configuration and initialize all disks with the boot menu.
Run "debug vreport show" to address remaining aggregate or volume
issues.

cluster_B::>
```

14. FC-to-SAS ブリッジまたは FC バックエンドスイッチを使用する構成の場合は、接続を解除して取り外します。

FC-to-SASブリッジの削除

a. ブリッジを特定します。

```
system bridge show
```

b. ブリッジを削除します。

```
system bridge remove -name <bridge_name>
```

c. ブリッジが削除されたことを確認します。

```
system bridge show
```

次の例は、ブリッジを削除したことを示しています。

例

```
cluster1::> system bridge remove -name ATTO_10.226.197.16
cluster1::> system bridge show

Is        Monitor
    Bridge     Symbolic Name Vendor  Model     Bridge WWN
Monitored Status
    ---------- ------------- ------- --------- ----------------
--------- -------
    ATTO_FibreBridge6500N_1
               Bridge Number 16
                             Atto    FibreBridge 6500N
                                                2000001086603824
false     -
    ATTO_FibreBridge6500N_2
               Not Set       Atto    FibreBridge 6500N
                                                20000010866037e8
false     -
    ATTO_FibreBridge6500N_3
               Not Set       Atto    FibreBridge 6500N
                                                2000001086609e0e
false     -
    ATTO_FibreBridge6500N_4
               Not Set       Atto    FibreBridge 6500N
                                                2000001086609c06
false     -
    4 entries were displayed.
```

FCスイッチを削除する

a. スイッチを特定します。

```
system switch fibre-channel show
```

b. スイッチを取り外します。

```
system switch fibre-channel remove -switch-name <switch_name>
```

c. スイッチが取り外されたことを確認します。

```
system switch fibre-channel show
```

例

```
cluster1::> system switch fibre-channel show
                Symbolic                                        Is
Monitor
    Switch      Name     Vendor  Model      Switch WWN
Monitored Status
    ----------- -------- ------- ---------- ----------------
--------- -------
    Cisco_10.226.197.34
                mcc-cisco-8Gb-fab-4
                         Cisco   DS-C9148-16P-K9
                                             2000547fee78f088
true      ok
    mcc-cisco-8Gb-fab-1
                mcc-cisco-8Gb-fab-1
                         Cisco   -          -
false     -
    mcc-cisco-8Gb-fab-2
                mcc-cisco-8Gb-fab-2
                         Cisco   -          -
false     -
    mcc-cisco-8Gb-fab-3
                mcc-cisco-8Gb-fab-3
                         Cisco   -          -
false     -
    4 entries were displayed.
cluster1::> system switch fibre-channel remove -switch-name
Cisco_10.226.197.34
cluster1::> system switch fibre-channel show
                Symbolic                                        Is
Monitor
    Switch      Name     Vendor  Model      Switch WWN
Monitored Status
    ----------- -------- ------- ---------- ----------------
--------- -------
    mcc-cisco-8Gb-fab-4
                mcc-cisco-8Gb-fab-4
                         Cisco
                                 -          -
false     -
    mcc-cisco-8Gb-fab-1
                mcc-cisco-8Gb-fab-1
                         Cisco   -          -
false     -
```

```
    mcc-cisco-8Gb-fab-2
                mcc-cisco-8Gb-fab-2
                         Cisco   -           -
false     -
    mcc-cisco-8Gb-fab-3
                mcc-cisco-8Gb-fab-3
                         Cisco   -           -
false     -
    4 entries were displayed
cluster1::>
```

15. MetroCluster FC コントローラモジュールとストレージシェルフの電源をオフにします。
16. MetroCluster FC コントローラモジュールとストレージシェルフを取り外します。

移行を完了します

移行を完了するには、新しい MetroCluster IP 構成の処理を検証する必要があります。

1. MetroCluster の IP 設定を確認します。

   この手順は、各クラスターで高度な権限モードで実行する必要があります。

   次の例は、 cluster_A の出力を示しています

```
cluster_A::> cluster show
Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  ------------
node_A_1-IP          true    true          false
node_A_2-IP          true    true          false
2 entries were displayed.

cluster_A::>
```

   次の例は、 cluster_B についての出力を示しています

```
cluster_B::> cluster show
Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  ------------
node_B_1-IP          true    true          false
node_B_2-IP          true    true          false
2 entries were displayed.

cluster_B::>
```

2. クラスタ HA とストレージフェイルオーバーを有効にします。

   この手順は各クラスタで実行する必要があります。

3. クラスタ HA 機能が有効になっていることを確認する。

```
cluster_A::> cluster ha show
High Availability Configured: true

cluster_A::>


cluster_A::> storage  failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- --------
-------------------------------------
node_A_1-IP    node_A_2-IP    true     Connected to node_A_2-IP
node_A_2-IP    node_A_1-IP    true     Connected to node_A_1-IP
2 entries were displayed.

cluster_A::>
```

4. MetroCluster 移行モードを無効にします。

   a. advanced 権限レベルに切り替えます。「 set -privilege advanced 」
   b. 移行モードを無効にします：「クラスタ移行を無効にする
   c. admin 権限レベルに戻ります。「 set -privilege admin 」

```
cluster_A::*> metrocluster transition disable

cluster_A::*>
```

5. 移行が無効になっていることを確認します

これらの手順を両方のクラスタで実行する必要があります。

```
cluster_A::> metrocluster transition show-mode
Transition Mode
--------------------------
not-enabled

cluster_A::>
```

```
cluster_B::> metrocluster transition show-mode
Transition Mode
--------------------------
not-enabled

cluster_B::>
```

6. 8ノード構成の場合は、から始まる手順 全体を繰り返す必要があります "MetroCluster FC 構成から MetroCluster IP 構成への移行を準備" （FC DRグループごとに）をクリックします。

メンテナンス後にカスタム **AutoSupport** メッセージを送信する

移行が完了したら、メンテナンスの終了を通知する AutoSupport メッセージを送信してケースの自動作成を再開します。

1. サポートケースの自動生成を再開するには、メンテナンスが完了したことを示す AutoSupport メッセージを送信します。
   a. 問題次のコマンドを実行します。「 system node AutoSupport invoke -node * -type all -message MAINT=end 」
   b. パートナークラスタに対してこのコマンドを繰り返します。

Tiebreaker またはメディエーターの監視をリストアしています

MetroCluster 構成の移行が完了したら、 Tiebreaker またはメディエーターユーティリティを使用して監視を再開できます。

1. 構成に適した手順を使用します。

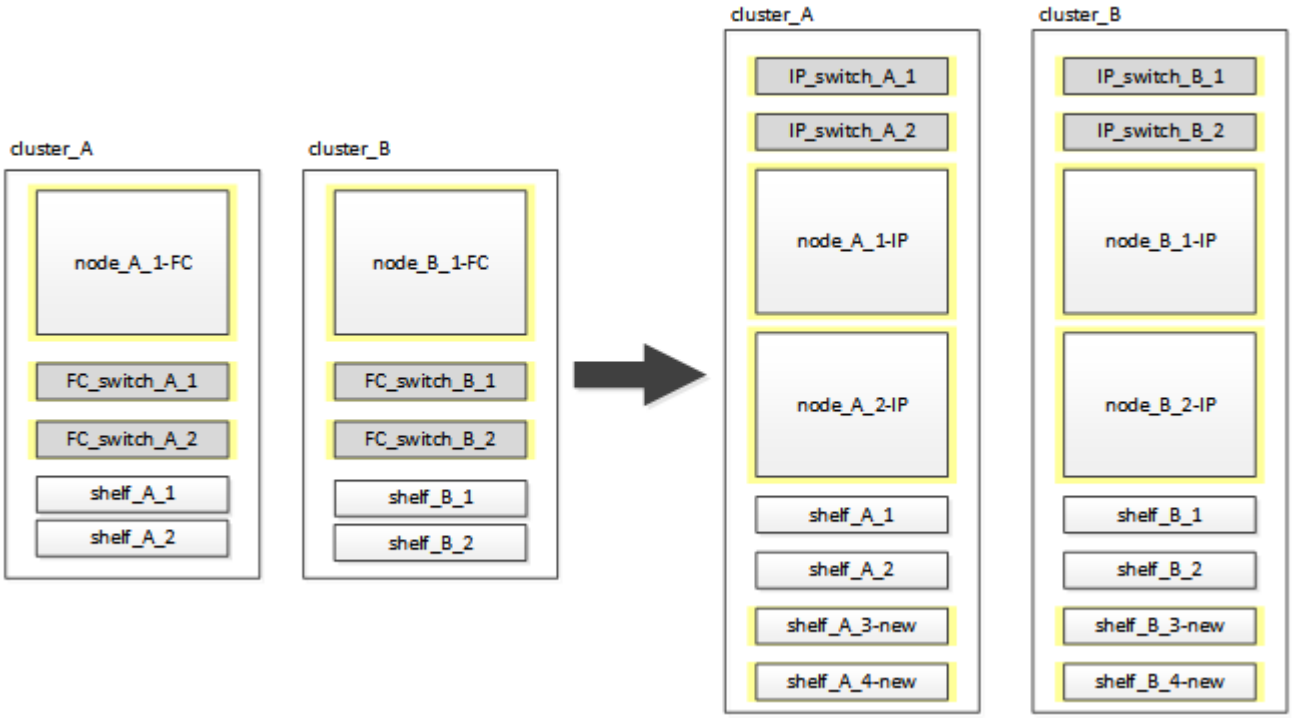
使用するポート	この手順を使用します
Tiebreaker	"MetroCluster 構成を追加しています"
メディエーター	"MetroCluster IP構成からONTAPメディエーターを構成する"

2 ノード MetroCluster FC から 4 ノード MetroCluster IP 構成への無停止での移行（ ONTAP 9.8 以降）

2 ノード MetroCluster FC から 4 ノード MetroCluster IP 構成への無停止での移行（ ONTAP 9.8 以降）

ONTAP 9.8 以降では、既存の 2 ノード MetroCluster FC 構成から新しい 4 ノード MetroCluster IP 構成にワークロードとデータを移行できます。MetroCluster FC ノードから IP ノードにディスクシェルフが移動されます。

次の図は、この移行手順の実行前と実行後の構成を簡単に示したものです。



- この手順は、 ONTAP 9.8 以降を実行しているシステムでサポートされています。
- この手順はシステムの停止を伴います。
- この手順は、 2 ノード MetroCluster FC 構成にのみ適用されます。

  4 ノード MetroCluster FC 構成の場合は、を参照してください "移行する手順を選択します"。

- ADP は、この手順で作成された 4 ノード MetroCluster IP 構成ではサポートされません。
- すべての要件を満たし、手順のすべての手順に従う必要があります。
- 既存のストレージシェルフは新しい MetroCluster IP ノードに移動されます。
- 必要に応じて、ストレージシェルフを構成に追加できます。

  を参照してください "FC から IP への移行を停止させるために、ドライブシェルフを再利用し、ドライブ要件を満たしておく必要があります"。

この手順での命名例

この手順では、全体的な名前の例を使用して、 DR グループ、ノード、および関連するスイッチを特定します。

元の構成のノードにはサフィックス -FC が付加され、ファブリック接続またはストレッチの MetroCluster 構成に含まれていることが示されます。

コンポーネント	site_A で cluster_A	site_B （ site_B
dr_group_1 - FC	• node_A_1 - FC • shelf_A_1. • shelf_A_2.	• node_B_1 - FC • shelf_B_1. • shelf_B_2.
dr_group_2 - IP	• node_A_1 の IP • Node_a_2-IP • shelf_A_1. • shelf_A_2. • shelf_A_3 - 新規 • shelf_A_4 - 新規	• node_B_1 - IP • node_B_2 - IP • shelf_B_1. • shelf_B_2. • shelf_B_3 - 新規 • shelf_B_4- 新規
スイッチ	• switch_A_1 - FC • switch_A_1 - FC • switch_A_1 - IP • switch_a_2-ip	• switch_B_1 - FC • switch_B_2 - FC • switch_B_1 - IP • switch_B_2 - IP

FC から IP への移行を停止させる準備をしています

移行プロセスを開始する前に、構成が要件を満たしていることを確認する必要があります。

コンソールログを有効にする

NetAppでは、使用しているデバイスでコンソールロギングをイネーブルにし、この手順を実行する際に次のアクションを実行することを強く推奨します。

- メンテナンス中はAutoSupportを有効のままにします。
- メンテナンスの前後にメンテナンスAutoSupportメッセージをトリガーして、メンテナンスアクティビティ中にケースの作成を無効にします。

  ナレッジベースの記事を参照してください "スケジュールされたメンテナンス時間中にケースの自動作成を停止する方法"。

- 任意のCLIセッションのセッションロギングをイネーブルにします。セッションログを有効にする方法については、ナレッジベースの記事の「セッション出力のログ」セクションを参照してください "ONTAPシ

ステムへの接続を最適化するためのPuTTYの設定方法"。

FC から **IP** への移行を停止するための一般的な要件

既存の MetroCluster FC 構成が次の要件を満たしている必要があります。

- 2 ノード構成であり、すべてのノードで ONTAP 9.8 以降が実行されている必要があります。

  2 ノードのファブリック接続または拡張 MetroCluster です。

- MetroCluster のインストールと設定の手順に記載されているすべての要件とケーブル接続を満たしている必要があります。

  "ファブリック接続 MetroCluster のインストールと設定"

  "ストレッチ MetroCluster のインストールと設定"

- NetApp Storage Encryption （ NSE ）では設定できません。
- MDV ボリュームは暗号化できません。

MetroCluster サイトから 6 つのすべてのノードのリモートコンソールアクセスが必要です。または、手順で必要に応じてサイト間の移動を計画しておく必要があります。

FC から **IP** への移行を停止させるために、ドライブシェルフを再利用し、ドライブ要件を満たしておく必要があります

ストレージシェルフに利用可能な十分なスペアドライブとルートアグリゲートスペースがあることを確認する必要があります。

既存のストレージシェルフを再利用する

この手順を使用する場合、既存のストレージシェルフは新しい構成で使用できるように保持されます。node_A_1 - FC と node_B_1 - FC を削除した場合、既存のドライブシェルフは cluster_B の node_A_1 - IP と node_B_2 - IP に接続され、 node_B_1 - IP と node_B_2 の node_B_2 - IP に接続されます

- 既存のストレージシェルフ（ node_A_1 の FC および node_B_1 に接続されたシェルフ）が新しいプラットフォームモデルでサポートされている必要があります。

  既存のシェルフが新しいプラットフォームモデルでサポートされていない場合は、を参照してください " 新しいコントローラで既存シェルフを使用できない場合の停止を伴う移行（ ONTAP 9.8 以降）"。

- プラットフォームについて、ドライブなどの制限を超えないようにする必要があります

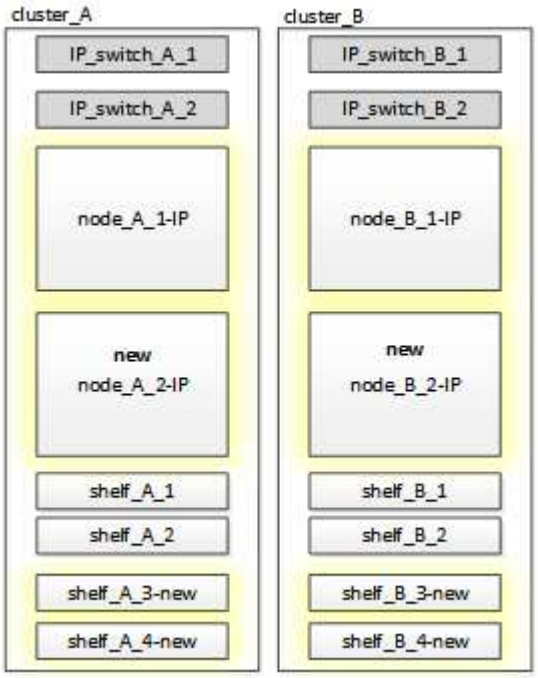
  "NetApp Hardware Universe の略"

追加のコントローラのストレージ要件

2 つのコントローラ（ node_B_2 - IP と node_B_2 - IP ）の構成が 2 ノードから 4 ノードに変更されるため、必要に応じてストレージを追加する必要があります。

- 既存のシェルフで使用可能なスペアドライブに応じて、追加のコントローラに対応するドライブを追加する必要があります。

この場合、次の図に示すように、追加のストレージシェルフが必要になることがあります。



3 台目と 4 台目のコントローラ（ node_B_2 - IP および node_B_2 - IP ）のそれぞれに 14 ~ 18 本のドライブを追加する必要があります。

- 3 本のプール 0 ドライブ
- プール 1 ドライブ × 3
- 2 本のスペアドライブ
- システムボリューム用に 6 ～ 10 台のドライブ

- 新しいノードを含む構成が、ドライブ数、ルートアグリゲートのサイズ容量など、構成のプラットフォーム制限を超えないようにする必要があります

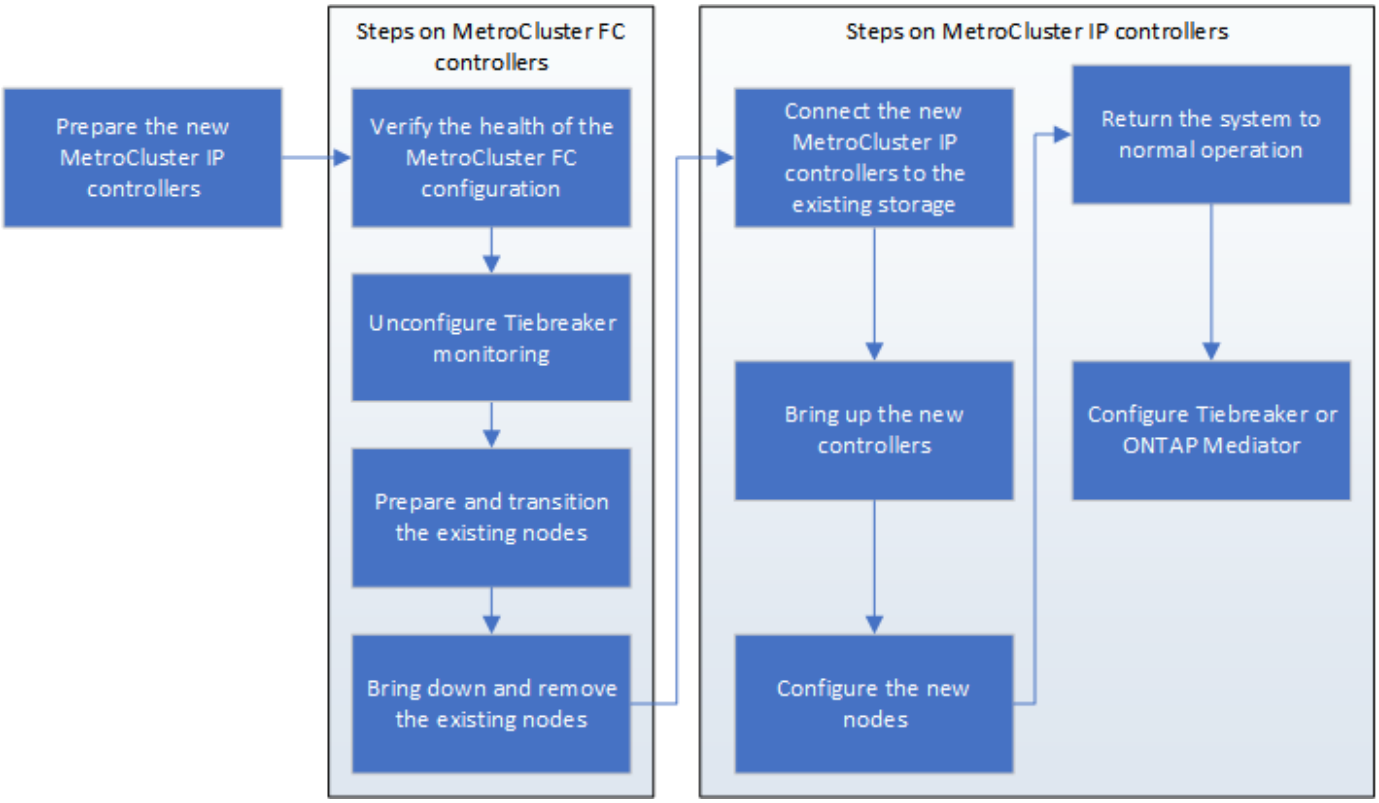
  この情報は、各プラットフォームモデルの NetApp Hardware Universe _ で確認できます。

  "NetApp Hardware Universe の略"

停止を伴う移行のワークフロー

移行を成功させるには、特定のワークフローに従う必要があります。

移行を準備する際は、サイト間の移動を計画します。リモートノードがラックに設置されてケーブル接続されたら、ノードへのシリアルターミナルアクセスが必要です。ノードが設定されるまでサービスプロセッサへのアクセスは許可されません。



MetroCluster FC ノードから **MetroCluster IP** ノードへのポートのマッピング

MetroCluster FC ノードのポートと LIF の設定を、交換する MetroCluster IP ノードと互換性があるように調整する必要があります。

このタスクについて

アップグレードプロセスで最初に新しいノードがブートされると、各ノードは交換するノードの最新の設定を使用します。node_A_1 の IP をブートする際、 ONTAP は、 node_A_1 の FC で使用されていたポート上で LIF をホストしようとします。

移行手順では、クラスタ LIF 、管理 LIF 、およびデータ LIF の構成が正しくなるように、古いノードと新しいノードの両方で手順を実行します。

手順

1. 既存の MetroCluster FC ポートの用途と新しいノードでの MetroCluster IP インターフェイスのポートの用途が競合していないかを特定します。

   次の表を使用して、新しい MetroCluster IP コントローラの MetroCluster IP ポートを特定する必要があります。次に、 MetroCluster FC ノードのそれらのポートにデータ LIF またはクラスタ LIF が存在するかどうかを確認して記録します。

   これらの競合するデータ LIF または MetroCluster FC ノード上のクラスタ LIF は、移行手順の該当するステップで移動されます。

   次の表に、 MetroCluster IP ポートをプラットフォームモデル別に示します。VLAN ID 列は無視してかまいません。

プラットフォームモデル	MetroCluster の IP ポート	VLAN ID	

AFF A800	e0b	使用されません	
	e1b		
AFF A700 および FAS9000	e5		
	e5b		
AFF A320	e0g		
	E0h		
AFF A300 および FAS8200	E1A		
	e1b		
FAS8300 / A400 / FAS8700	E1A	10.	
	e1b	20	
AFF A250 および FAS500f	e0c	10.	
	e0b	20	

次の表に記入して、移行手順で後ほど参照できます。

ポート	対応する MetroCluster IP インターフェイスポート（上の表を参照）	MetroCluster FC ノードのこれらのポートで LIF が競合しています
node_A_1 の FC 上の最初の MetroCluster IP ポート		
node_A_1 の FC 上の 2 番目の MetroCluster IP ポート		
node_B_1 の最初の MetroCluster IP ポート： FC		
node_B_1 の 2 つ目の MetroCluster IP ポート： FC		

2. 新しいコントローラで使用できる物理ポートとポートでホストできる LIF を確認します。

   コントローラのポートの用途は、 MetroCluster IP 構成で使用するプラットフォームモデルと IP スイッチモデルによって異なります。新しいプラットフォームのポート使用量を NetApp Hardware Universe から

収集できます。

"NetApp Hardware Universe の略"

3. 必要に応じて、 node_A_1 の FC と node_A_1 の IP のポート情報を記録します。

この表は、移行手順を実行するときに参照します。

node_A_1 の列で、新しいコントローラモジュールの物理ポートを追加し、新しいノードの IPspace とブロードキャストドメインを計画します。

	node_A_1 - FC			node_A_1 の IP		
LIF	ポート	IPspace	ブロードキャストドメイン	ポート	IPspace	ブロードキャストドメイン
クラスタ 1						
クラスタ 2						
クラスタ 3						
クラスタ 4						
ノード管理						
クラスタ管理						
データ 1						
データ 2.						
データ 3						
データ 4.						
SAN						
クラスタ間ポート						

4. 必要に応じて、 node_B_1 FC のすべてのポート情報を記録します。

この表は、アップグレード手順を実行するときに参照します。

node_B_1 の IP の列で、新しいコントローラモジュールの物理ポートを追加し、新しいノードの LIF ポートの使用、 IPspace 、およびブロードキャストドメインを計画します。

	node_B_1 - FC			node_B_1 - IP		
LIF	物理ポート	IPspace	ブロードキャストドメイン	物理ポート	IPspace	ブロードキャストドメイン
クラスタ 1						
クラスタ 2						
クラスタ 3						
クラスタ 4						
ノード管理						
クラスタ管理						
データ 1						
データ 2.						
データ 3						
データ 4.						
SAN						
クラスタ間ポート						

MetroCluster IP コントローラの準備

4 つの新しい MetroCluster IP ノードを準備し、正しいバージョンの ONTAP をインストールする必要があります。

このタスクについて

このタスクは新しい各ノードで実行する必要があります。

- node_A_1 の IP
- Node_a_2-IP
- node_B_1 - IP
- node_B_2 - IP

ノードは新しい * ストレージシェルフに接続する必要があります。既存のストレージシェルフにデータを格納している状態は * 接続しないでください。

ここ手順で説明する手順は、コントローラとシェルフがラックに設置されたときに実行することも、あとで実行することもできます。いずれの場合も、構成をクリアし、ノードを既存のストレージシェルフに接続する前 * および MetroCluster FC ノードの構成を変更する前 * に、ノードを準備する必要があります。

MetroCluster FC コントローラに接続された既存のストレージシェルフに MetroCluster IP コントローラを接続した状態では、この手順を実行しないでください。

この手順では、ノードの設定をクリアし、新しいドライブのメールボックスのリージョンをクリアします。

手順

1. コントローラモジュールを新しいストレージシェルフに接続します。
2. 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 」

   すべてのコンポーネントの HA 状態は「 mccip 」である必要があります。

3. 表示されたコントローラまたはシャーシのシステム状態が正しくない場合は、 HA 状態を設定します。

   「 ha-config modify controller mccip 」「 ha-config modify chassis mccip 」

4. メンテナンスモードを終了します。

   「 halt 」

   コマンドの実行後、ノードが LOADER プロンプトで停止するまで待ちます。

5. 4 つのすべてのノードで次の手順を繰り返して、設定をクリアします。

   a. 環境変数をデフォルト値に設定します。

      「デフォルト設定」

   b. 環境を保存します。

      'aveenv

   さようなら

6. ブートメニューの 9a オプションを使用して、次の手順を繰り返して 4 つのノードをすべてブートします。

   a. LOADER プロンプトで、ブートメニューを起動します。

      「 boot_ontap menu

   b. 起動メニューでオプション [9a`] を選択して、コントローラを再起動します。

7. ブートメニューのオプション「 5 」を使用して、 4 つのノードのそれぞれをメンテナンスモードでブートします。
8. システム ID と 4 つの各ノードの ID を記録します。

「 sysconfig 」を使用できます

9. node_A_1 の IP と node_B_1 の IP について、次の手順を繰り返します。
   a. 各サイトのローカルなすべてのディスクの所有権を割り当てます。

      「 disk assign adapter.xx.*` 」のように指定します

   b. node_A_1 の IP と node_B_1 の IP でドライブシェルフが接続されている HBA ごとに、上記の手順を繰り返します。
10. node_A_1 の IP と node_B_1 の IP で次の手順を繰り返し、各ローカルディスクのメールボックス領域をクリアします。
    a. 各ディスクのメールボックス領域を破棄します。

       「 mailbox destroy local 」「 mailbox destroy partner 」を実行します

11. 4 台のコントローラをすべて停止します。

    「 halt 」

12. 各コントローラで、ブートメニューを表示します。

    「 boot_ontap menu

13. 4 台のコントローラのそれぞれで、設定をクリアします。

    wipeconfig

    wipeconfig 処理が完了すると、ノードは自動的にブートメニューに戻ります。

14. ブートメニューの 9a オプションを使用して、次の手順を繰り返して 4 つのノードをすべてブートします。
    a. LOADER プロンプトで、ブートメニューを起動します。

       「 boot_ontap menu

    b. 起動メニューでオプション [9a`] を選択して、コントローラを再起動します。
    c. コントローラモジュールのブートが完了してから次のコントローラモジュールに移動します。

    "9a`" が完了すると、ノードは自動的にブートメニューに戻ります。

15. コントローラの電源をオフにします。

MetroCluster FC 構成の健全性の確認

移行を実行する前に、 MetroCluster FC 構成の健全性と接続を確認する必要があります

このタスクは、 MetroCluster FC 構成上で実行します。

1. ONTAP で MetroCluster 構成の動作を確認します。
   a. システムがマルチパスかどうかを確認します。

node run -node node-name sysconfig -a `

b. ヘルスアラートがないかどうかを両方のクラスタで確認します。

「 system health alert show 」というメッセージが表示されます

c. MetroCluster 構成と運用モードが正常な状態であることを確認します。

「 MetroCluster show 」

d. MetroCluster チェックを実行します。

「 MetroCluster check run 」のようになります

e. MetroCluster チェックの結果を表示します。

MetroCluster チェックショー

f. スイッチにヘルスアラートがないかどうかを確認します（ある場合）。

「 storage switch show 」と表示されます

g. Config Advisor を実行します。

"ネットアップのダウンロード： Config Advisor"

h. Config Advisor の実行後、ツールの出力を確認し、推奨される方法で検出された問題に対処します。

2. ノードが非 HA モードになっていることを確認します。

「 storage failover show 」をクリックします

Tiebreaker またはその他の監視ソフトウェアから既存の設定を削除します

スイッチオーバーを開始できる MetroCluster Tiebreaker 構成や他社製アプリケーション（ ClusterLion など）で既存の構成を監視している場合は、移行の前に Tiebreaker またはその他のソフトウェアから MetroCluster 構成を削除する必要があります。

手順

1. Tiebreaker ソフトウェアから既存の MetroCluster 設定を削除します。

"MetroCluster 構成を削除しています"

2. スイッチオーバーを開始できるサードパーティ製アプリケーションから既存の MetroCluster 構成を削除します。

アプリケーションのマニュアルを参照してください。

MetroCluster FC ノードを移行します

既存の MetroCluster FC ノードから情報を収集し、メンテナンスの開始を通知する

AutoSupport メッセージを送信し、ノードを移行する必要があります。

移行前に既存のコントローラモジュールから情報を収集

移行の前に、各ノードの情報を収集する必要があります。

このタスクは既存のノードで実行します。

- node_A_1 - FC
- node_B_1 - FC

a. 次の表に示すコマンドの出力を収集します。

カテゴリ	コマンド	注：
使用許諾	system license show コマンドを実行します	
各シェルフおよびフラッシュストレージのディスクシェルフとディスク数、およびメモリと NVRAM とネットワークカード	system node run -node node_name sysconfig	
クラスタネットワーク LIF とノード管理 LIF	system node run -node node_name sysconfig network interface show -role 「 cluster 、 node-mgmt 、 data 」	
SVM 情報	vserver show のコマンドです	
プロトコル情報	nfs show iscsi show cifs show のように表示されます	
物理ポート	network port show -node node_name -type 物理ネットワークポート show	
フェイルオーバーグループ	network interface failover-groups show -vserver vserver_name	clusterwide 以外のフェイルオーバーグループの名前とポートを記録します。
VLAN の設定	network port vlan show -node node_name	各ネットワークポートと VLAN ID のペアを記録します。
インターフェイスグループの設定	ネットワークポート ifgrp show -node node_name -instance	インターフェイスグループの名前と割り当てられているポートを記録します。
ブロードキャストドメイン	network port broadcast-domain show	
表示されます	network ipspace show のコマンド	
ボリューム情報	volume show フィールドと volume show フィールドの暗号化	

カテゴリ	コマンド	注：
アグリゲート情報	storage aggregate show および storage aggr encryption show と storage aggregate object-store show の 2 つのコマンドを実行します	
ディスク所有権情報	storage aggregate show および storage aggr encryption show と storage aggregate object-store show の 2 つのコマンドを実行します	
暗号化	storage failover mailbox-disk show および security key-manager backup show の 2 つのコマンドがあります	key-manager を有効にするときに使用したパスフレーズはそのままにしておきます。外部キー管理ツールの場合は、クライアントとサーバの認証情報が必要です。
暗号化	security key-manager show のコマンド	
暗号化	security key-manager external show のコマンド	
暗号化	システムシェルローカルの kenv kmip.init.ipaddr ip-address	
暗号化	システムシェルローカルの kenv kmip.init.netmask ネットマスク	
暗号化	システムシェルローカルの kenv kmip.init.gateway ゲートウェイ	
暗号化	システムシェルのローカル kenv kmip.init.interface インターフェイス	

カスタム **AutoSupport** メッセージをメンテナンス前に送信する

メンテナンスを実行する前に、 AutoSupport an 問題 message to notify NetApp technical support that maintenance is maintenancing （メンテナンスが進行中であることをネットアップテクニカルサポートに通知する）を実行これにより、システム停止が発生したとみなしてユーザがケースをオープンすることを防止できます。

このタスクは MetroCluster サイトごとに実行する必要があります。

1. サポートケースが自動で生成されないようにするには、メンテナンスが進行中であることを示す AutoSupport メッセージを送信します。
   a. 問題次のコマンドを実行します。「 system node AutoSupport invoke -node * -type all -message MAINT= maintenance-window-in-hours 」

      maintenance-window-in-hours にはメンテナンス時間の長さを指定します。最大値は 72 時間です。この時間が経過する前にメンテナンスが完了した場合は、メンテナンス期間の終了を通知する AutoSupport メッセージ「 'System node AutoSupport invoke -node * -type all -message MAINT=end` 」を起動できます

b. パートナークラスタに対してこのコマンドを繰り返します。

MetroCluster FC ノードの移行、シャットダウン、削除

MetroCluster FC ノードに対してコマンドを実行するだけでなく、このタスクには、各サイトでのコントローラモジュールの物理的なケーブル接続の解除と削除が含まれます。

このタスクは、古いノードごとに実行する必要があります。

- node_A_1 - FC
- node_B_1 - FC

手順

1. すべてのクライアントトラフィックを停止します。
2. いずれかの MetroCluster FC ノード（例： node_A_1 ）で、移行を有効にします。
   a. advanced 権限レベル「 set -priv advanced 」を設定します
   b. イネーブル移行 : MetroCluster transition enable-transition-mode disruptive
   c. admin モードに戻ります。 'set-priv admin'
3. ルートアグリゲートのリモートプレックスを削除して、ルートアグリゲートのミラーを解除します。
   a. ルートアグリゲートを特定します。「 storage aggregate show -root true 」
   b. プール 1 のアグリゲート「 storage aggregate plex show -pool 1 」を表示します
   c. ルートアグリゲートのリモートプレックスをオフラインにして削除します。+
   `aggr plex offline <root-aggregate> -plex <remote-plex-for-root-aggregate>`

   `aggr plex delete <root-aggregate> -plex <remote-plex-for-root-aggregate>`

   例：

```
# aggr plex offline aggr0_node_A_1-FC_01 -plex remoteplex4
```

+

```
# aggr plex delete aggr0_node_A_1-FC_01 -plex remoteplex4
```

4. 各コントローラで次のコマンドを使用して処理を進める前に、メールボックス数、ディスクの自動割り当て、および移行モードを確認します。
   a. advanced 権限レベル「 set -priv advanced 」を設定します
   b. 各コントローラモジュールに表示されるメールボックスドライブが「 storage failover mailbox-disk show 」の 3 つだけであることを確認します
   c. admin モードに戻ります。 'set-priv admin'
   d. 移行モードが停止を伴うことを確認します。 MetroCluster transition show

5. 破損ディスクがないかどうかを確認します
6. 破損ディスクを取り外すか交換します。
7. node_A_1-FCとnode_B_1-FCで次のコマンドを使用して、アグリゲートが正常であることを確認します。

   「 storage aggregate show

   「 storage aggregate plex show 」と表示されます

   storage aggregate show コマンドは、ルートアグリゲートがミラーされていないことを示します。

8. VLANまたはインターフェイスグループがないかどうかを確認します。

   ```
   network port ifgrp show
   ```

   ```
   network port vlan show
   ```

   何も表示されない場合は、次の 2 つの手順をスキップします。

9. VLANまたはifgrpを使用しているLIFのリストを表示します。

   network interface show -fields home-port 、 curr -port

   ```
   network port show -type if-group | vlan
   ```

10. VLAN とインターフェイスグループを削除します。

    この手順は、サフィックスが -mc の SVM を含むすべての SVM のすべての LIF で実行する必要があります。

    a. VLAN またはインターフェイスグループを使用している LIF を使用可能なポートに移動します。「 network interface modify -vserver vserver-name -lif lif_name -home-port port
    b. ホームポートにない LIF を表示します。「 network interface show -is-home false 」
    c. すべての LIF をそれぞれのホームポートにリバートします。「 network interface revert -vserver vserver_name -lif lif_name
    d. すべての LIF がそれぞれのホームポートにあることを確認します。「 network interface show -is-home false 」

       出力に LIF が表示されません。

    e. VLANポートとifgrpポートをブロードキャストドメインから削除します。 `network port broadcast-domain remove-ports -ipspace ipspace -broadcast-domain broadcast-domain-name -ports nodename:portname,nodename:portname,..`
    f. すべての VLAN ポートと ifgrp ポートがブロードキャストドメインに割り当てられていないことを確認します。「 network port show -type if-group | vlan
    g. すべての VLAN を削除します。「 network port vlan delete -node nodename -vlan-name vlan-name 」
    h. インターフェイスグループを削除します。「 network port ifgrp delete -node nodename -ifgrp ifgrp_name 」

11. MetroCluster の IP インターフェイスポートとの競合を解決するために、必要に応じて LIF をすべて移動します。

    特定された LIF は、の手順 1 に移動する必要があります "MetroCluster FC ノードから MetroCluster IP ノードへのポートのマッピング"。

    a. 目的のポートでホストされている LIF を別のポートに移動します。「 network interface modify -lif lifname -vserver vserver-name -home-port new -homeport ` network interface revert -lif lifname -vserver vservername 」

    b. 必要に応じて、デスティネーションポートを適切な IPspace とブロードキャストドメインに移動します。network port broadcast-domain remove-ports -ipspace current-ipspace current-broadcast-domain current-broadcast-domain -ports controller-name ： current-port `network port broadcast-domain add-ports -ipspace new-ipspace-broadcast-domain new-broadcast-domain new-broadcast-domain-ports controller-name ： new-port ’

12. MetroCluster FC コントローラ（ node_A_1 -FC および node_B_1 - FC ）を停止します。「 system node halt

13. LOADER プロンプトで、 FC コントローラモジュールと IP コントローラモジュールのハードウェアクロックを同期します。

    a. 古い MetroCluster FC ノード（ node_A_1 -FC ）で ' 日付を表示します 'how date

    b. 新しい MetroCluster IP コントローラ（ node_A_1 の IP および node_B_1 の IP ）で、元のコントローラに表示される日付を設定します。 'et date mm/dd/yy

    c. 新しい MetroCluster IP コントローラ（ node_A_1 の IP および node_B_1 の IP ）で、日付を「日付」で確認します

14. MetroCluster FC コントローラモジュール（ node_A_1 の FC と node_B_1 の FC ）、 FC-to-SAS ブリッジ（存在する場合）、 FC スイッチ（存在する場合）、およびそれらのノードに接続されている各ストレージシェルフを停止し、電源をオフにします。

15. MetroCluster FC コントローラからシェルフを切断し、各クラスタにローカルストレージとして使用するシェルフを文書化します。

16. FC-to-SAS ブリッジまたは FC バックエンドスイッチを使用する構成の場合は、接続を解除して取り外します。

FC-to-SASブリッジの削除

a. ブリッジを特定します。

```
system bridge show
```

b. ブリッジを削除します。

```
system bridge remove -name <bridge_name>
```

c. ブリッジが削除されたことを確認します。

```
system bridge show
```

次の例は、ブリッジを削除したことを示しています。

例

```
cluster1::> system bridge remove -name ATTO_10.226.197.16
cluster1::> system bridge show

Is        Monitor
    Bridge     Symbolic Name Vendor  Model     Bridge WWN
Monitored Status
    ---------- ------------- ------- --------- ----------------
--------- -------
    ATTO_FibreBridge6500N_1
               Bridge Number 16
                             Atto    FibreBridge 6500N
                                                2000001086603824
false     -
    ATTO_FibreBridge6500N_2
               Not Set       Atto    FibreBridge 6500N
                                                20000010866037e8
false     -
    ATTO_FibreBridge6500N_3
               Not Set       Atto    FibreBridge 6500N
                                                2000001086609e0e
false     -
    ATTO_FibreBridge6500N_4
               Not Set       Atto    FibreBridge 6500N
                                                2000001086609c06
false     -
    4 entries were displayed.
```

FCスイッチを削除する

a. スイッチを特定します。

```
system switch fibre-channel show
```

b. スイッチを取り外します。

```
system switch fibre-channel remove -switch-name <switch_name>
```

c. スイッチが取り外されたことを確認します。

```
system switch fibre-channel show
```

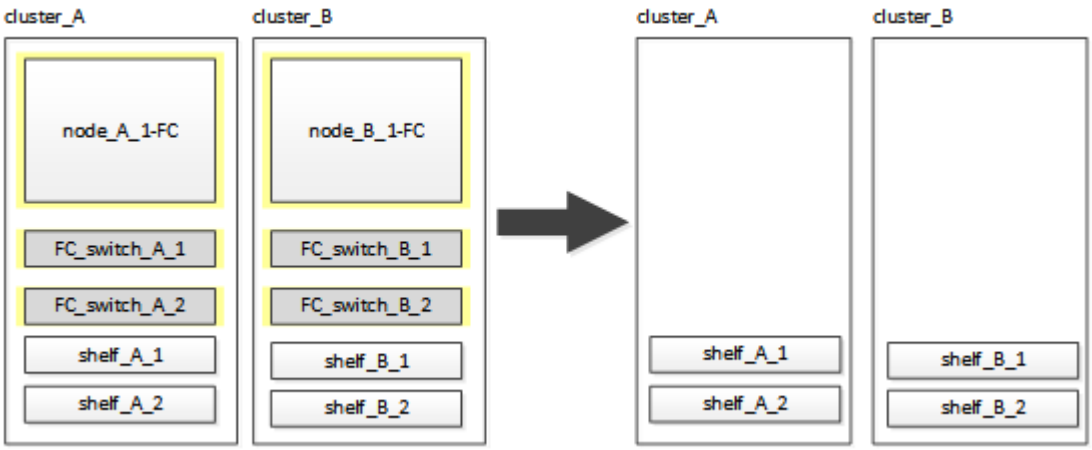
例

```
cluster1::> system switch fibre-channel show
                Symbolic                                        Is
Monitor
    Switch      Name     Vendor  Model      Switch WWN
Monitored Status
    ----------- -------- ------- ---------- ----------------
--------- -------
    Cisco_10.226.197.34
                mcc-cisco-8Gb-fab-4
                         Cisco   DS-C9148-16P-K9
                                             2000547fee78f088
true      ok
    mcc-cisco-8Gb-fab-1
                mcc-cisco-8Gb-fab-1
                         Cisco   -          -
false     -
    mcc-cisco-8Gb-fab-2
                mcc-cisco-8Gb-fab-2
                         Cisco   -          -
false     -
    mcc-cisco-8Gb-fab-3
                mcc-cisco-8Gb-fab-3
                         Cisco   -          -
false     -
    4 entries were displayed.
cluster1::> system switch fibre-channel remove -switch-name
Cisco_10.226.197.34
cluster1::> system switch fibre-channel show
                Symbolic                                        Is
Monitor
    Switch      Name     Vendor  Model      Switch WWN
Monitored Status
    ----------- -------- ------- ---------- ----------------
--------- -------
    mcc-cisco-8Gb-fab-4
                mcc-cisco-8Gb-fab-4
                         Cisco
                                 -          -
false     -
    mcc-cisco-8Gb-fab-1
                mcc-cisco-8Gb-fab-1
                         Cisco   -          -
false     -
```

```
    mcc-cisco-8Gb-fab-2
                mcc-cisco-8Gb-fab-2
                         Cisco    -           -
false      -
    mcc-cisco-8Gb-fab-3
                mcc-cisco-8Gb-fab-3
                         Cisco    -           -
false      -
    4 entries were displayed
cluster1::>
```

17. MetroCluster FC ノード（ node_A_1 の FC と node_B_1 の FC ）のメンテナンスモードで、ディスクが接続されていないことを確認します。「ディスク show -v 」
18. MetroCluster FC ノードの電源をオフにして取り外します。

この時点で、 MetroCluster FC コントローラが取り外され、シェルフがすべてのコントローラから切断されています。



MetroCluster IP コントローラモジュールを接続します

4 つの新しいコントローラモジュールとストレージシェルフを構成に追加する必要があります。新しいコントローラモジュールは一度に 2 つずつ追加されます。

新しいコントローラをセットアップする

新しい MetroCluster IP コントローラを、以前に MetroCluster FC コントローラに接続したストレージシェルフにラックに設置してケーブル接続する必要があります。

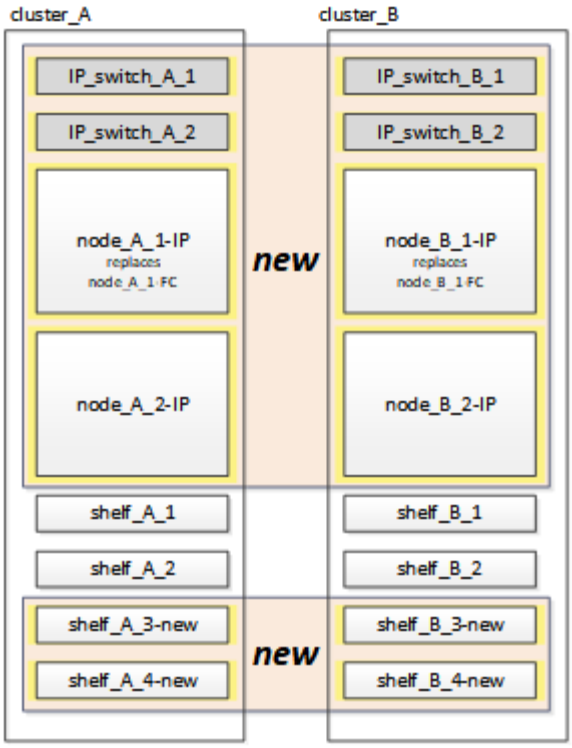
このタスクについて

この手順は、各 MetroCluster IP ノードで実行する必要があります。

- node_A_1 の IP
- Node_a_2-IP

- node_B_1 - IP
- node_B_2 - IP

次の例では、新しいコントローラモジュールに対応するストレージを提供するために、各サイトにストレージシェルフが 2 台追加されています。



手順

1. 必要に応じて、新しいコントローラモジュールとストレージシェルフ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、構成内のストレージシェルフ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. 新しい機器をラックに設置します。コントローラ、ストレージシェルフ、 IP スイッチが設置されている必要があります。

   この時点では、ストレージシェルフまたは IP スイッチをケーブル接続しないでください。

4. 電源ケーブルと管理コンソールをコントローラに接続します。
5. すべてのストレージシェルフの電源がオフになっていることを確認する。
6. 4 つのノードすべてで次の手順を実行して、ドライブが接続されていないことを確認します。

   a. LOADER プロンプトで、ブートメニューを起動します。

      「 boot_ontap maint 」を使用してください

   b. ドライブが接続されていないことを確認します。

「ディスクショー V 」

出力にドライブが表示されないことを確認します。

a. ノードを停止します。

「 halt 」

7. ブートメニューの 9a オプションを使用して、 4 つのノードすべてをブートします。

a. LOADER プロンプトで、ブートメニューを起動します。

「 boot_ontap menu

b. 起動メニューでオプション [9a`] を選択して、コントローラを再起動します。

c. コントローラモジュールのブートが完了してから次のコントローラモジュールに移動します。

"9a`" が完了すると、ノードは自動的にブートメニューに戻ります。

8. ストレージシェルフをケーブル接続します。

ケーブル接続の情報については、使用しているモデルに対応したコントローラの設置とセットアップの手順を参照してください。

"ONTAPハードウェアシステムのドキュメント"

9. の説明に従って、コントローラを IP スイッチにケーブル接続します "IP スイッチのケーブル接続"。

10. 新しい RCF ファイルを適用するための IP スイッチを準備します。

スイッチベンダーの手順に従います。

- "Broadcom IP スイッチを工場出荷時のデフォルトにリセットします"
- "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"
- "NVIDIA IP SN2100スイッチを工場出荷時のデフォルトにリセット"

11. RCF ファイルをダウンロードしてインストールします。

スイッチベンダーの手順に従います。

- "Broadcom IPのRCFファイルをダウンロードしてインストールする"
- "Cisco IP RCFファイルのダウンロードとインストール"
- "NVIDIA RCFファイルをダウンロードしてインストールする"]

12. 最初の新しいコントローラ（ node_A_1 の IP ）の電源をオンにし、 Ctrl+C キーを押してブートプロセスを中断し、 LOADER プロンプトを表示します。

13. コントローラをメンテナンスモードでブートします。

「 boot_ontap maint 」を使用します

14. コントローラのシステム ID を表示します。

「 sysconfig -v 」を使用します

15. 既存の構成のシェルフが新しい MetroCluster IP ノードから認識されていることを確認します。

    storage show shelf 'disk show -v' のように表示されます

16. ノードを停止します。

    「 halt 」

17. パートナーサイト（ site_B ）のもう一方のノードで、上記の手順を繰り返します。

node_A_1 の **IP** と **node_B_1** の **IP** を接続し、ブートします

MetroCluster IP コントローラと IP スイッチを接続したら、 node_A_1 の IP と node_B_1 の IP を移行してブートします。

node_A_1 の **IP** を起動しています

正しい移行オプションを使用してノードをブートする必要があります。

手順

1. node_A_1 の IP をブートメニューでブートします。

   「 boot_ontap menu

2. 問題ブートメニュープロンプトで次のコマンドを実行して移行を開始します。

   「 boot_after_MCC_transition 」を参照してください

   - このコマンドは、 node_A_1 の FC が所有するすべてのディスクを node_A_1 の IP に再割り当てします。
     - node_A_1 - FC ディスクが node_A_1 の IP に割り当てられます
     - node_B_1 - FC ディスクが node_B_1 の IP に割り当てられます
   - また、 MetroCluster IP ノードが ONTAP プロンプトからブートできるように、このコマンドを使用すると、必要な他のシステム ID の再割り当ても自動的に行われます。
   - boot_after_MCC_transition コマンドが何らかの理由で失敗した場合は、ブートメニューから再実行する必要があります。

   - 次のプロンプトが表示されたら、 Ctrl+C キーを押して続行します。MCC DR の状態を確認しています … [Ctrl + C （履歴書）、 S （ステータス）、 L （リンク）] _ を入力します
   - ルートボリュームが暗号化されている場合、ノードは次のメッセージで停止します。ルートボリュームが暗号化されており（ NetApp Volume Encryption ）、キーのインポートに失敗したため、システムを停止します。このクラスタに外部（ KMIP ）キー管理ツールが設定されている場合は、キーサーバの健常性を確認します。

```
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)?
`boot_after_mcc_transition`
This will replace all flash-based configuration with the last backup
to disks. Are you sure you want to continue?: yes

MetroCluster Transition: Name of the MetroCluster FC node: `node_A_1-
FC`
MetroCluster Transition: Please confirm if this is the correct value
[yes|no]:? y
MetroCluster Transition: Disaster Recovery partner sysid of
MetroCluster FC node node_A_1-FC: `systemID-of-node_B_1-FC`
MetroCluster Transition: Please confirm if this is the correct value
[yes|no]:? y
MetroCluster Transition: Disaster Recovery partner sysid of local
MetroCluster IP node: `systemID-of-node_B_1-IP`
MetroCluster Transition: Please confirm if this is the correct value
[yes|no]:? y
```

3. データボリュームが暗号化されている場合は、キー管理設定に対応したコマンドを使用してキーをリストアします。

使用するポート	使用するコマンド
• オンボードキー管理 *	「セキュリティキーマネージャオンボード同期」 詳細については、を参照してください "オンボードキー管理の暗号化キーのリストア"。
• 外部キー管理 *	'security key-manager key query -node node-name 詳細については、を参照してください "外部キー管理の暗号化キーのリストア"。

4. ルートボリュームが暗号化されている場合は、の手順を使用します "ルートボリュームが暗号化されている場合のキー管理のリカバリ"。

ルートボリュームが暗号化されている場合は、特別なブートコマンドを使用してキー管理をリストアする必要があります。

作業を開始する前に

パスフレーズを事前に収集しておく必要があります。

手順

1. オンボードキー管理を使用している場合は、次の手順を実行して構成をリストアします。

   a. LOADER プロンプトで、ブートメニューを表示します。

      「 boot_ontap menu

   b. ブート・メニューからオプション（ 10 ） Set onboard key management recovery secrets （オンボード・キー管理リカバリシークレットの設定）を選択します

      プロンプトに従って応答します。

      ```
      This option must be used only in disaster recovery procedures. Are
      you sure? (y or n): y
      Enter the passphrase for onboard key management: passphrase
      Enter the passphrase again to confirm: passphrase

      Enter the backup data: backup-key
      ```

      システムがブートしてブートメニューが表示されます。

   c. ブート・メニューでオプション「 6` 」を入力します。

      プロンプトに従って応答します。

      ```
      This will replace all flash-based configuration with the last backup
      to
      disks. Are you sure you want to continue?: y

      Following this, the system will reboot a few times and the following
      prompt will be available continue by saying y

      WARNING: System ID mismatch. This usually occurs when replacing a
      boot device or NVRAM cards!
      Override system ID? {y|n} y
      ```

      リブートが完了すると、システムに LOADER プロンプトが表示されます。

   d. LOADER プロンプトで、ブートメニューを表示します。

「 boot_ontap menu

e. もう一度 ' ブート・メニューからオプション（ 10 ） Set onboard key management recovery secrets （オンボード・キー管理リカバリシークレットの設定）を選択します

プロンプトに従って応答します。

```
This option must be used only in disaster recovery procedures. Are
you sure? (y or n): `y`
Enter the passphrase for onboard key management: `passphrase`
Enter the passphrase again to confirm:`passphrase`

Enter the backup data:`backup-key`
```

システムがブートしてブートメニューが表示されます。

f. ブート・メニューでオプション「 1 」を入力します。

次のプロンプトが表示された場合は、 Ctrl+C キーを押してプロセスを再開できます。

```
 Checking MCC DR state... [enter Ctrl-C(resume), S(status), L(link)]
```

システムが ONTAP プロンプトでブートします。

g. オンボードキー管理をリストアします。

「セキュリティキーマネージャオンボード同期」

前の手順で収集したパスフレーズを使用して、必要に応じてプロンプトに応答します。

```
cluster_A::> security key-manager onboard sync
Enter the cluster-wide passphrase for onboard key management in Vserver
"cluster_A":: passphrase
```

2. 外部キー管理を使用している場合は、次の手順を実行して設定をリストアします。

a. 必要な bootargs を設定します。

setsetenv bootarg.kmip.init.ipaddr ip-address

setsetenv bootarg.kmip.init.netmask netmask

setsetenv bootarg.kmip.init.gateway gateway-address

setsetenv bootarg.kmip.init.interface interface-id`

b. LOADER プロンプトで、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（ 11 ） Configure node for external key management （外部キー管理用のノードの設定）を選択します

システムがブートしてブートメニューが表示されます。

d. ブート・メニューでオプション「 6` 」を入力します。

システムが何度もブートします。起動プロセスを続行するかどうかを確認するメッセージが表示されたら、肯定応答を返すことができます。

リブートが完了すると、システムに LOADER プロンプトが表示されます。

e. 必要な bootargs を設定します。

setsetenv bootarg.kmip.init.ipaddr ip-address

setsetenv bootarg.kmip.init.netmask netmask

setsetenv bootarg.kmip.init.gateway gateway-address

setsetenv bootarg.kmip.init.interface interface-id`

a. LOADER プロンプトで、ブートメニューを表示します。

「 boot_ontap menu

b. ブート・メニューからオプション（ 11 ） Configure node for external key management を再度選択し ' 必要に応じてプロンプトに応答します

システムがブートしてブートメニューが表示されます。

c. 外部キー管理をリストアします。

「セキュリティキーマネージャの外部リストア」

ネットワーク設定を作成しています

FC ノードの設定に一致するネットワーク設定を作成する必要があります。これは、 MetroCluster の IP ノードがブート時に同じ設定を再生するためです。つまり、 node_A_1 の IP ブートと node_B_1 の IP ブート時に、 ONTAP は node_A_1 の FC と node_B_1 の FC で使用されていたポートで LIF をホストしようとします。

このタスクについて

ネットワーク設定を作成するときは、で作成したプランを使用してください "MetroCluster FC ノードから MetroCluster IP ノードへのポートのマッピング" を参照してください。

MetroCluster IP ノードの設定が完了したら、データ LIF を稼働するために追加の設定が必要になる場合があります。

手順

1. すべてのクラスタポートが適切なブロードキャストドメインに属していることを確認します。

   クラスタ LIF を作成するには、クラスタ IPspace とクラスタブロードキャストドメインが必要です

   a. IP スペースを表示します。

      network ipspace show

   b. IP スペースを作成し、必要に応じてクラスタポートを割り当てます。

      "IPspace の設定（クラスタ管理者のみ）"

   c. ブロードキャストドメインを表示します。

      「 network port broadcast-domain show 」

   d. 必要に応じて、ブロードキャストドメインにクラスタポートを追加します。

      "ブロードキャストドメインのポートの追加と削除"

   e. 必要に応じて、 VLAN とインターフェイスグループを再作成します。

      VLAN およびインターフェイスグループのメンバーシップは、古いノードと異なる場合があります。

      "VLAN を作成する"

   "物理ポートを組み合わせたインターフェイスグループの作成"

2. ポートおよびブロードキャストドメインに対して MTU 設定が正しく設定されていることを確認し、次のコマンドを使用して変更を加えます。

   「 network port broadcast-domain show 」

   「 network port broadcast-domain modify -broadcast-domain *bcastdomainname _ -mtu_mtu_value*`

クラスタポートとクラスタ **LIF** をセットアップする

クラスタポートと LIF をセットアップする必要があります。ルートアグリゲートでブートされたサイト A のノードで、次の手順を実行する必要があります。

手順

1. 目的のクラスタポートを使用して LIF のリストを特定します。

   network interface show -curr-node portname

   network interface show -home-node portname

2. 各クラスタポートについて、そのポートのいずれかの LIF のホームポートを別のポートに変更します。

   a. advanced 権限モードに切り替え、続行するかどうかを尋ねられたら「 y 」と入力します。

      'set priv advanced'

b. 変更する LIF がデータ LIF である場合は、次の手順を実行します。

「 vserver config override command 」 network interface modify -lif lif_name _ -vserver *vservername* -home-node *new-datahomeport* 」という形式で指定します

c. LIF がデータ LIF でない場合は、次の手順を実行します。

'network interface modify -lif lif_lifname_-vservername_-home-node home_port_datahome_port_`

d. 変更した LIF をホームポートにリバートします。

「 network interface revert * -vserver_vserver_name _ 」のように指定します

e. クラスタポートに LIF がないことを確認します。

network interface show -curr-node Curr -port_portname _

'network interface show -home-node port_portname _`

a. 現在のブロードキャストドメインからポートを削除します。

「 network port broadcast-domain remove-ports 」 -ipspacename --broadcast -domain_bcastdomainname — ports_node_name : port_name_`

b. クラスタの IPspace とブロードキャストドメインにポートを追加します。

「 network port broadcast-domain add-ports -ipspace Cluster -broadcast-domain Cluster -ports_node_name ： port_name_`

c. ポートのロールが変更されたことを確認します。「 network port show 」

d. クラスタポートごとに上記の手順を繰り返します。

e. admin モードに戻ります。

'set priv admin' のように設定します

3. 新しいクラスタポートにクラスタ LIF を作成します。

a. クラスタ LIF のリンクローカルアドレスを使用して自動設定を行うには、次のコマンドを使用します。

「 network interface create -vserver Cluster -lif cluster_lifname 」 -service-policy_default_cluster_ -home-node *a1name* _ -home-port cluster port -auto true 」のように指定します

b. クラスタ LIF に静的 IP アドレスを割り当てるには、次のコマンドを使用します。

「 network interface create -vserver Cluster -lif cluster_lifname _ *service-policy default -cluster-home -node-a1name*-home-node *clusterport*-address *ip-address_netmask*-status-admin up

LIF の構成を確認しています

古いコントローラからのストレージの移動後も、ノード管理 LIF 、クラスタ管理 LIF 、およびクラスタ間 LIF が残ったままです。必要に応じて、 LIF を適切なポートに移動する必要があります。

手順

1. 管理 LIF とクラスタ管理 LIF がすでに目的のポートにあるかどうかを確認します。

   「 network interface show -service -policy default -management 」を参照してください

   「 network interface show -service -policy default -intercluster 」のように表示されます

   LIF が目的のポートに接続されている場合は、このタスクの残りの手順を省略して次の手順に進むことができます。

2. 目的のポートにないノード、クラスタ管理、またはクラスタ間 LIF のそれぞれについて、そのポートのいずれかの LIF のホームポートを別のポートに変更します。

   a. 目的のポートでホストされている LIF を別のポートに移動することにより、目的のポートを転用します。

      「 vserver config override command 」 network interface modify -lif lif_name _ -vserver *vservername* -home-node *new-datahomeport* 」という形式で指定します

   b. 変更した LIF を新しいホームポートにリバートします。

      vserver config override -command 「 network interface revert -lif lifname _ -vservername 」のように入力します

   c. 適切な IPspace とブロードキャストドメインにないポートがある場合は、現在の IPspace とブロードキャストドメインからそのポートを削除します。

      「 network port broadcast-domain remove-ports - ipspace_current - broadcast-domain_current - broadcast-domain_Ports_controller-name ： current-port_`

   d. 目的のポートを適切な IPspace とブロードキャストドメインに移動します。

      「 network port broadcast-domain add -ports -ipspace_new-ipspace 」 -broadcast-domain _new-broadcast-domain _ports_port_name ： new-port _`

   e. ポートのロールが変更されたことを確認します。

      「 network port show 」のように表示されます

   f. ポートごとに上記の手順を繰り返します。

3. ノード、クラスタ管理 LIF 、およびクラスタ間 LIF を目的のポートに移動します。

   a. LIF のホームポートを変更します。

      「 network interface modify -vserver _ -lif *node-mgmt*-home-node _homenode _ 」を入力します

   b. LIF を新しいホームポートにリバートします。

      'network interface revert -lif LIF_name -vserver_mgmt_' ： vserver_vservername_`

   c. クラスタ管理 LIF のホームポートを変更します。

      「 network interface modify -vserver _ -lif クラスター -mgmt -lif-lif-name _ -home-port_port_-home

-node _homenode _ 」と入力します

d. クラスタ管理 LIF を新しいホームポートにリバートします。

「 network interface revert -lif cluster_mgmt -lif-name _ -vservername_` 」のようになります

e. クラスタ間 LIF のホームポートを変更します。

「 network interface modify -vserver _ -lif _ intercluster -lif-name _ -home-nodename_home -port_nodename _ *home_port_port*`

f. クラスタ間 LIF を新しいホームポートにリバートします。

「 network interface revert -lif lif_intercluster-lif-name _ -vservername_` 」のように入力します

node_B_2 と **node_B_2** の **IP** を起動しています

各サイトで新しい MetroCluster IP ノードを起動して設定し、各サイトに HA ペアを作成する必要があります。

node_B_2 と **node_B_2** の **IP** を起動しています

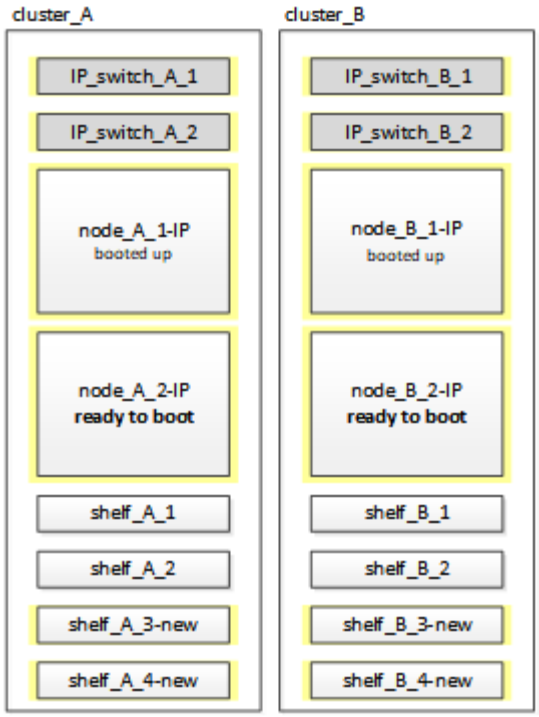
新しいコントローラモジュールは、ブートメニューの適切なオプションを使用して、一度に 1 つずつブートする必要があります。

このタスクについて

この手順では、 2 つの新しいノードをブートして、 2 ノード構成を 4 ノード構成に拡張します。

これらの手順は、次のノードで実行します。

- Node_a_2-IP
- node_B_2 - IP



手順

1. ブート・オプション「 9C 」を使用して、新しいノードをブートします。

```
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)? 9c
```

ノードの初期化とブートは、次のようなノードセットアップウィザードで実行されます。

```
Welcome to node setup
You can enter the following commands at any time:
"help" or "?" - if you want to have a question clarified,
"back" - if you want to change previously answered questions, and
"exit" or "quit" - if you want to quit the setup wizard.
Any changes you made before quitting will be saved.
To accept a default or omit a question, do not enter a value. .
.
.
```

オプション "9C`" が正常に実行されない場合は ' データ損失の可能性を避けるため ' 次の手順に従います

- オプション 9a は実行しないでください。
- 元の MetroCluster FC 構成（ shelf_A_1 、 shelf_A_2 、 shelf_B_1 、 shelf_B_2 ）のデータが格納されている既存のシェルフを物理的に取り外します。
- 技術情報アーティクルを参照して、テクニカルサポートに連絡してください "MetroCluster FC から IP への移行 - オプション 9C が失敗しました"。

  "ネットアップサポート"

2. ウィザードの指示に従って、 AutoSupport ツールを有効にします。
3. プロンプトに従ってノード管理インターフェイスを設定します。

```
Enter the node management interface port: [e0M]:
Enter the node management interface IP address: 10.228.160.229
Enter the node management interface netmask: 225.225.252.0
Enter the node management interface default gateway: 10.228.160.1
```

4. ストレージフェイルオーバーモードが HA に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

   モードが HA でない場合は、設定します。

   「 storage failover modify -mode ha -node *localhost*` 」です

   変更を有効にするには、ノードをリブートする必要があります。

5. 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
```

6. ノードのセットアップウィザードを終了します。

   「exit

7. admin ユーザ名を使用して admin アカウントにログインします。
8. クラスタセットアップウィザードを使用して既存のクラスタに参加する。

```
:> cluster setup
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.
Do you want to create a new cluster or join an existing cluster?
{create, join}:
join
```

9. クラスタセットアップウィザードが完了したら、次のコマンドを入力して、クラスタがアクティブで、ノードが正常であることを確認します。

「 cluster show 」を参照してください

10. ディスクの自動割り当てを無効にする：

    storage disk option modify -autoassign off -node node_name IP

11. 暗号化を使用する場合は、キー管理設定に対応したコマンドを使用してキーをリストアします。

使用するポート	使用するコマンド
• オンボードキー管理 *	「セキュリティキーマネージャオンボード同期」 詳細については、を参照してください "オンボードキー管理の暗号化キーのリストア"。
• 外部キー管理 *	'security key-manager key query -node-node-name-' 詳細については、を参照してください "外部キー管理の暗号化キーのリストア"。

12. 2 つ目の新しいコントローラモジュール（ node_B_2 - IP ）について、上記の手順を繰り返します。

MTU 設定を確認しています

ポートとブロードキャストドメインに対して MTU 設定が正しく設定されていることを確認し、変更を加えます。

手順

1. クラスタブロードキャストドメインで使用されている MTU サイズを確認します。

    「 network port broadcast-domain show 」

2. 必要に応じて MTU サイズを更新します。

    「 network port broadcast-domain modify -broadcast-domain *bcast-domain-name-name*-mtu_mtu-size_` 」

クラスタ間 LIF を設定しています

クラスタピアリングに必要なクラスタ間 LIF を設定

このタスクは、新しい両方のノード、 node_B_2 - IP と node_B_2 - IP の両方で実行する必要があります。

ステップ

1. クラスタ間 LIF を設定を参照してください "クラスタ間 LIF を設定しています"

クラスタピアリングを検証しています

cluster_A と cluster_B にピア関係が確立されており、各クラスタのノードが相互に通信できることを確認します。

手順

1. クラスタピア関係を確認します。

   cluster peer health show

```
cluster01::> cluster peer health show
Node       cluster-Name                Node-Name
             Ping-Status               RDB-Health Cluster-Health  Avail…
---------- --------------------------- ---------  ---------------
--------
node_A_1-IP
           cluster_B                   node_B_1-IP
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
                                       node_B_2-IP
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
node_A_2-IP

image::../media/transition_2n_booting_a_2_and_b_2.png["Booting new IP
nodes during transition"]
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
                                       node_B_2-IP
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
```

2. ping を実行して、ピアアドレスに到達できることを確認します。

   cluster peer ping -originating -node *local-node-destination-cluster_remote-cluster-name*`

新しいノードの設定と移行の完了

新しいノードを追加したら、移行手順を完了して、 MetroCluster IP ノードを設定する必要があります。

MetroCluster IP ノードを設定し、移行を無効にします

MetroCluster IP 接続を実装し、 MetroCluster 構成を更新し、移行モードを無効にする必要があります。

手順

1. コントローラ node_A_1 の IP から次のコマンドを実行して、新しいノードを DR グループに形成します。

```
metrocluster configuration-settings dr-group create -partner-cluster
<peer_cluster_name> -local-node <local_controller_name> -remote-node
<remote_controller_name>
```

「 MetroCluster configurion-settings dr-group show 」を参照してください

2. MetroCluster IP インターフェイスを作成します（ node_A_1 の IP 、 node_B_2 の IP 、 node_B_1 の IP 、 node_B_2 の IP 、 node_B_2 の IP ） - コントローラごとに 2 つのインターフェイスを作成します。合計 8 つのインターフェイスが必要です。



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 <controller_name> -home-port <port_name> -address
<ip_address> -netmask <netmask_address> -vlan-id <vlan_id>
```

「 MetroCluster configurion-settings interface show 」を参照してください

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。

3. コントローラ node_A_1 の IP から MetroCluster 接続処理を実行して MetroCluster サイトを接続 - この処理には数分かかることがあります。

   MetroCluster 構成設定接続接続

4. リモートクラスタのディスクが、 iSCSI 接続を介して各コントローラから認識されていることを確認します。

   「ディスクショー」

   構成内の他のノードに属するリモートディスクが表示されます。

5. node_A_1 の IP と node_B_1 の IP のルートアグリゲートをミラーします。

   「 aggregate mirror -aggregate root-aggr 」のように指定します

6. node_B_2 の IP と node_B_2 の IP のディスクを割り当て

   ブートメニューで boot_after_MCC_transtion コマンドを実行した場合に、 node_A_1 と node_B_1 に対してすでに作成されているプール 1 のディスク割り当て

   a. 問題： node_A_1 の IP に対して次のコマンドを実行します。

      disk assign disk1disk2disk3… diskn-sysid node_B_2-ip-control-sysid-pool 1-force

   b. 問題 node_B_2 IP で次のコマンドを実行します。

disk assign disk1disk2disk3… diskn -sysid node-a _2 -ip-controller-sysid -pool 1 -force

7. リモートディスクの所有権が更新されたことを確認します。

   「ディスクショー」

8. 必要に応じて、次のコマンドを使用して所有権情報を更新します。
   a. advanced 権限モードに切り替えて、続行するかどうかを尋ねられたら「 y 」と入力します。

      'set priv advanced'

   b. ディスク所有権を更新します。

      「 disk refresh-ownership controller-name 」と入力します

   c. admin モードに戻ります。

      'set priv admin' のように設定します

9. node_B_2 の IP と node_B_2 の IP のルートアグリゲートをミラーリングします。

   「 aggregate mirror -aggregate root-aggr 」のように指定します

10. ルートアグリゲートとデータアグリゲートの再同期が完了したことを確認します。

    aggr show `aggr plex show`

    再同期には時間がかかることがありますが、完了してから次の手順に進んでください。

11. MetroCluster 構成を更新して新しいノードを組み込みます。
    a. advanced 権限モードに切り替えて、続行するかどうかを尋ねられたら「 y 」と入力します。

       'set priv advanced'

    b. 構成を更新します。

設定内容	問題コマンド
各クラスタにアグリゲートが 1 つあります。	「 MetroCluster configure -refresh true -allow-with -one-aggregate true 」
各クラスタに複数のアグリゲートがあります	MetroCluster configure -refresh true

    c. admin モードに戻ります。

       'set priv admin' のように設定します

12. MetroCluster 移行モードを無効にします。
    a. advanced 権限モードに切り替え、続行するかどうかを尋ねられたら「 y 」と入力します。

       'set priv advanced'

b. 移行モードを無効にします。

MetroCluster transition disable`

c. admin モードに戻ります。

'set priv admin' のように設定します

新しいノードにデータ **LIF** をセットアップ

新しいノード、 node_B_2 の IP および node_B_2 の IP にデータ LIF を設定する必要があります。

新しいコントローラで使用可能な新しいポートがブロードキャストドメインに割り当てられていない場合は、そのドメインに追加する必要があります。必要に応じて、新しいポートに VLAN またはインターフェイスグループを作成します。を参照してください "Network Management の略"

1. 現在のポートの使用状況とブロードキャストドメインを特定します。

network port show ` network port broadcast-domain show 」

2. 必要に応じて、ブロードキャストドメインと VLAN にポートを追加します。

a. IP スペースを表示します。

network ipspace show

b. IP スペースを作成し、必要に応じてデータポートを割り当てます。

"IPspace の設定（クラスタ管理者のみ）"

c. ブロードキャストドメインを表示します。

「 network port broadcast-domain show 」

d. 必要に応じて、ブロードキャストドメインにデータポートを追加します。

"ブロードキャストドメインのポートの追加と削除"

e. 必要に応じて、 VLAN とインターフェイスグループを再作成します。

VLAN およびインターフェイスグループのメンバーシップは、古いノードと異なる場合があります。

"VLAN を作成する"

"物理ポートを組み合わせたインターフェイスグループの作成"

3. 必要に応じて、 MetroCluster IP ノード（ -mc を備えた SVM を含む）の適切なノードとポートで LIF がホストされていることを確認します。

で収集した情報を参照してください "ネットワーク設定を作成しています"。

a. LIF のホームポートを確認します。

「 network interface show - field home-port 」のように表示されます

b. 必要に応じて、 LIF の設定を変更します。

```
vserver config override -command "network interface modify -vserver
<svm_name> -home-port <active_port_after_upgrade> -lif <lif_name> -home-node
<new_node_name>
```

c. LIF をそれぞれのホームポートにリバートします。

```
network interface revert * -vserver <svm_name>
```

SVM を起動する

LIF の設定が変更されたため、新しいノードで SVM を再起動する必要があります。

手順

1. SVM の状態を確認します。

   MetroCluster vserver show

2. サフィックスが「 -mc 」のない cluster_A 上の SVM を再起動します。

   ```
   vserver start -vserver <svm_name> -force true
   ```

3. パートナークラスタで上記の手順を繰り返します。
4. すべての SVM が健全な状態であることを確認します。

   MetroCluster vserver show

5. すべてのデータ LIF がオンラインであることを確認します。

   「 network interface show 」を参照してください

新しいノードへのシステムボリュームの移動

耐障害性を高めるには、システムボリュームを controller_A_1 から IP コントローラ node_A_1 に、さらに node_B_1 から node_B_2 の IP に移動する必要があります。システムボリュームのデスティネーションノードにミラーされたアグリゲートを作成する必要があります。

このタスクについて

システムボリュームの名前の形式は「 MDV _crs_*_a' 」または「 MDV_CRS_*_b` 」です。 このセクションで使用されている site_A および site_B の参照とは関係がありません。たとえば、 MDV_CRS_*_A は site_A と関連付けられていません

手順

1. 必要に応じて、コントローラ node_A_1 の IP および node_B_2 の IP に少なくとも 3 本のプール 0 と 3 本のプール 1 ディスクを割り当てます。
2. ディスクの自動割り当てを有効にします。

3. site_A から次の手順を実行して、 _B システムボリュームを node_A_1 の IP から node_B_2 の IP に移動します

   a. システムボリュームを格納するために、コントローラ node_A_1 にミラーアグリゲートを作成します。

      ```
      aggr create -aggregate new_node_A_2-IP_aggr -diskcount 10 -mirror true -node
      node_A_2-IP
      ```

      「 aggr show 」と入力します

      ミラーされたアグリゲートには、 5 つのプール 0 と 5 つのプール 1 スペアディスクが必要です。これらのディスクはコントローラ node_A_1 のコントローラ node_A_1 の IP で所有されます。

      ディスクが不足している場合は ' アドバンス・オプションの -force-small-aggregate true を使用すると ' ディスクの使用を 3 プール 0 および 3 プール 1 のディスクに制限できます

   b. 管理 SVM に関連付けられているシステムボリュームの一覧を表示します。

      「 vserver show 」

      ```
      volume show -vserver <admin_svm_name>
      ```

   site_A が所有するアグリゲートに含まれているボリュームを特定しますsite_B のシステムボリュームも表示されます。

4. site_A 用の MDV_CRS_*_B システムボリュームを、コントローラ node_A_1 で作成されたミラーアグリゲートに移動します

   a. 可能なデスティネーションアグリゲートがないかどうかを確認します

      ```
      volume move target-aggr show -vserver <admin_svm_name> -volume MDV_CRS_*_B
      ```

      node_A_1 に作成されたアグリゲートが表示されます。

   b. node_A_1 に作成した新しいアグリゲートにボリュームを移動します。

      「高度」

      ```
      volume move start -vserver <admin_svm_name> -volume MDV_CRS_*_B -destination
      -aggregate new_node_A_2-IP_aggr -cutover-window 40
      ```

   c. 移動処理のステータスを確認します。

      ```
      volume move show -vserver <admin_svm_name> -volume MDV_CRS_*_B
      ```

   d. 移動処理が完了したら、 MDV_CRS_*_B システムが node_A_1 の新しいアグリゲートに含まれていることを確認します。

      「管理者」

   ```
   volume show -vserver <admin_svm_name>
   ```

5. site_B （ node_B_1 - IP と node_B_2 - IP ）で上記の手順を繰り返します。

システムを通常動作に戻します

最後の設定手順を実行し、 MetroCluster の設定を通常動作に戻す必要があります。

移行後の **MetroCluster** 処理の検証とドライブの割り当て

MetroCluster が正しく動作していることを確認し、新しいノードの 2 つ目のペア（ node_B_2 - IP と node_B_2 - IP ）にドライブを割り当てる必要があります。

1. MetroCluster の構成タイプが ip-fabric ： MetroCluster show であることを確認します
2. MetroCluster チェックを実行します。
   a. 問題次のコマンドを実行します MetroCluster check run
   b. MetroCluster チェックの結果を表示します。「 MetroCluster check show 」
3. MetroCluster IP ノードを持つ DR グループが構成されていることを確認します MetroCluster node show
4. 必要に応じて、各サイトでコントローラの node_B_2 IP および node_B_2 の IP 用に追加のデータアグリゲートを作成してミラーリング

新しいコントローラモジュール用のライセンスをインストールしています

標準（ノードロック）ライセンスが必要な ONTAP サービスがある場合は、新しいコントローラモジュールにライセンスを追加する必要があります。標準ライセンスを使用する機能では、クラスタ内の各ノードにその機能用のキーが必要です。

ライセンスの詳細については、ネットアップサポートサイトの技術情報アーティクル 3013749 ：「 Data ONTAP 8.2 Licensing Overview and References 」と「 *System Administration Reference*」 を参照してください。

1. 必要に応じて、ネットアップサポートサイトの「ソフトウェアライセンス」の下の「 My Support 」セクションで新しいノードのライセンスキーを取得します。

   ライセンスの置換の詳細については、Knowledge Baseの記事を参照してください "マザーボードの交換後プロセスを実行して、AFF / FASシステムのライセンスを更新"

2. 問題各ライセンスキーをインストールするには、次のコマンドを実行します。 'system license add license-code license_key'

   license_key は 28 桁の数字です。

   必要な標準（ノードロック）ライセンスごとにこの手順を繰り返します。

ノードの設定を完了します

手順を完了する前に実行できるその他の設定手順があります。これらの手順の一部はオプションです。

1. サービスプロセッサを設定します。「 system service-processor network modify 」
2. 新しいノードで AutoSupport を設定します。「 system node AutoSupport modify 」

3. 必要に応じて、コントローラの名前を移行時に変更できます。コントローラの名前を変更するには、「 system node rename -node <old-name> -newname <new-name> 」コマンドを使用します

   名前変更処理が完了するまでに数分かかることがあります。system show -fields node コマンドを使用して他の手順を続行する前に、名前の変更が各ノードに伝播されていることを確認します。

4. 必要に応じて監視サービスを設定します。

   "メディエーターに関する考慮事項"

   "計画外の自動スイッチオーバー用に ONTAP Mediator を構成する"

   "Tiebreaker ソフトウェアのインストールと設定"

メンテナンス後にカスタム **AutoSupport** メッセージを送信する

移行が完了したら、メンテナンスの終了を通知する AutoSupport メッセージを送信してケースの自動作成を再開します。

1. サポートケースの自動生成を再開するには、メンテナンスが完了したことを示す AutoSupport メッセージを送信します。
   a. 問題次のコマンドを実行します。「 system node AutoSupport invoke -node * -type all -message MAINT=end 」
   b. パートナークラスタに対してこのコマンドを繰り返します。

ストレージシェルフを撤去する際の、 MetroCluster FC から MetroCluster IP への停止を伴う移行（ ONTAP 9.8 以降）

ONTAP 9.8 以降では、 2 ノードの MetroCluster FC 構成を 4 ノードの MetroCluster IP 構成に無停止で移行し、既存のストレージシェルフを撤去できます。手順には、既存のドライブシェルフから新しい構成にデータを移動し、古いシェルフを撤去する手順が含まれています。

- この手順は、既存のストレージシェルフを撤去し、 MetroCluster IP 構成内の新しいシェルフにすべてのデータを移動する場合に使用します。
- 既存のストレージシェルフモデルが新しい MetroCluster IP ノードでサポートされている必要があります。
- この手順は、 ONTAP 9.8 以降を実行しているシステムでサポートされています。
- この手順はシステムの停止を伴います。
- この手順は、 2 ノード MetroCluster FC 構成にのみ適用されます。

  4 ノード MetroCluster FC 構成の場合は、を参照してください "移行する手順を選択します"。

- すべての要件を満たし、手順のすべての手順に従う必要があります。

コンソールログを有効にする

NetAppでは、使用しているデバイスでコンソールロギングをイネーブルにし、この手順を実行する際に次のアクションを実行することを強く推奨します。

- メンテナンス中はAutoSupportを有効のままにします。
- メンテナンスの前後にメンテナンスAutoSupportメッセージをトリガーして、メンテナンスアクティビティ中にケースの作成を無効にします。

  ナレッジベースの記事を参照してください "スケジュールされたメンテナンス時間中にケースの自動作成を停止する方法"。

- 任意のCLIセッションのセッションロギングをイネーブルにします。セッションログを有効にする方法については、ナレッジベースの記事の「セッション出力のログ」セクションを参照してください "ONTAPシステムへの接続を最適化するためのPuTTYの設定方法"。

古いシェルフを撤去する場合の移行要件

移行プロセスを開始する前に、既存の MetroCluster FC 構成が要件を満たしていることを確認する必要があります。

- 2 ノードのファブリック接続またはストレッチ MetroCluster 構成で、すべてのノードで ONTAP 9.8 以降が実行されている必要があります。

  新しい MetroCluster IP コントローラモジュールは、同じバージョンの ONTAP 9.8 を実行している必要があります。

- 既存のプラットフォームと新しいプラットフォームの組み合わせは、移行対象としてサポートされている必要があります。

  "無停止移行でサポートされるプラットフォーム"

- MetroCluster インストールおよび設定ガイド _ に記載されているすべての要件とケーブル接続を満たしている必要があります。

  "ファブリック接続 MetroCluster のインストールと設定"

新しい構成は、次の要件も満たす必要があります。

- 新しい MetroCluster IP プラットフォームモデルで古いストレージシェルフモデルがサポートされている必要があります。

  "NetApp Hardware Universe の略"

- 既存のシェルフで使用可能なスペアディスクに応じて、ドライブを追加する必要があります。

  必要なドライブシェルフがほかにもあります。

  各コントローラに 14~18 本のドライブを追加する必要があります。

  - プール 0 ドライブ × 3

- プール 1 ドライブ × 3
- 2 本のスペアドライブ
- システムボリューム用に 6 ～ 10 台のドライブ

- 新しいノードを含む構成が、ドライブ数、ルートアグリゲートのサイズ容量など、構成のプラットフォーム制限を超えないようにする必要があります

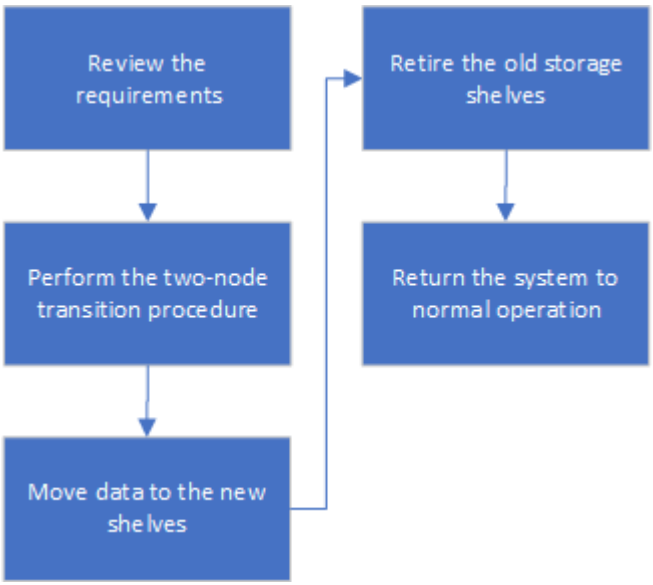
  この情報は、各プラットフォームモデルので確認できます "NetApp Hardware Universe の略"

MetroCluster サイトから 6 つのすべてのノードのリモートコンソールアクセスが必要です。または、手順で必要に応じてサイト間の移動を計画しておく必要があります。

データを移動する場合や古いストレージシェルフを撤去する場合の、停止を伴う移行ワークフロー

移行を成功させるには、特定のワークフローに従う必要があります。

移行を準備する際は、サイト間の移動を計画します。リモートノードがラックに設置されてケーブル接続されたら、ノードへのシリアルターミナルアクセスが必要です。ノードが設定されるまでサービスプロセッサへのアクセスは許可されません。



構成を移行しています

詳細な移行手順に従う必要があります。

このタスクについて

次の手順では、他の手順に進みます。参照されている各手順で、指定された順序で手順を実行する必要があります。

手順

1. の手順に従って、ポートマッピングを計画します "MetroCluster FC ノードから MetroCluster IP ノードへのポートのマッピング"。

2. の手順に従って、 MetroCluster IP コントローラを準備します "MetroCluster IP コントローラの準備"。
3. MetroCluster FC 構成の健常性を確認

   の手順を実行します "MetroCluster FC 構成の健全性の確認"。

4. MetroCluster FC 構成から情報を収集

   の手順を実行します "移行前に既存のコントローラモジュールから情報を収集"。

5. 必要に応じて Tiebreaker による監視を削除

   の手順を実行します "Tiebreaker またはその他の監視ソフトウェアから既存の設定を削除します"。

6. 既存の MetroCluster FC ノードを準備して削除

   の手順を実行します "MetroCluster FC ノードを移行します"。

7. 新しい MetroCluster IP ノードを接続します。

   の手順を実行します "MetroCluster IP コントローラモジュールを接続します"。

8. 新しい MetroCluster IP ノードを設定し、移行を完了します。

   の手順を実行します "新しいノードの設定と移行の完了"。

ルートアグリゲートを移行します

移行が完了したら、残りの既存のルートアグリゲートを MetroCluster FC 構成から MetroCluster IP 構成の新しいシェルフに移行します。

このタスクについて

このタスクでは、 node_A_1 の FC および node_B_1 のルートアグリゲートを、新しい MetroCluster IP コントローラが所有するディスクシェルフに移動します。

手順

1. 新しいローカルストレージシェルフのプール 0 のディスクを、移動するルートのあるコントローラに割り当てます（例： node_A_1 のルートを移行する場合は、新しいシェルフのプール 0 のディスクを node_A_1 の IP に割り当てます）。

   migrate_Removes はルート・ミラー _ を再作成しないため 'migrate コマンドを実行する前にプール 1 のディスクを割り当てる必要はありません

2. 権限モードを advanced に設定します。

   'set priv advanced'

3. ルートアグリゲートを移行します。

   system node migrate-root -node node_name -disklist disk-id1 、 disk-id2 、 diskn -raid-type raid-type `

   ◦ node-name は、ルートアグリゲートの移行先のノードです。

- disk-id は、新しいシェルフのプール 0 ディスクを識別します。
- 通常、 RAID タイプは既存のルートアグリゲートの RAID タイプと同じです。
- 移行ステータスを確認するには、コマンド「 job show -idjob-id-instance 」を使用します。ここで、 job-id は、 migrate-root コマンドの実行時に指定された値です。

  たとえば、 node_A_1 の FC のルートアグリゲートの構成が、 RAID-DP を使用して 3 本のディスクで構成されていた場合は、次のコマンドを使用して、ルートを新しいシェルフ 11 に移行します。

```
system node migrate-root -node node_A_1-IP -disklist
3.11.0,3.11.1,3.11.2 -raid-type raid_dp
```

4. 移行処理が完了してノードが自動的にリブートするまで待ちます。
5. リモートクラスタに直接接続した新しいシェルフのルートアグリゲートのプール 1 のディスクを割り当てます。
6. 移行されたルートアグリゲートをミラーリングします。
7. ルートアグリゲートの再同期が完了するまで待ちます。

   storage aggregate show コマンドを使用して、アグリゲートの同期ステータスを確認できます。

8. もう一方のルートアグリゲートに対して同じ手順を繰り返します。

データアグリゲートを移行する

新しいシェルフにデータアグリゲートを作成し、ボリューム移動を使用して、古いシェルフから新しいシェルフ上のアグリゲートにデータボリュームを転送します。

1. 新しいコントローラ上のアグリゲートに、一度に 1 つのボリュームずつデータボリュームを移動します。

   "アグリゲートの作成と新しいノードへのボリュームの移動"

撤去するシェルフは **node_A_1** から **FC** 、 **node_A_1** から **FC** を移行

元の MetroCluster FC 構成から古いストレージシェルフを撤去します。これらのシェルフの所有者は、もともと node_A_1 の FC と node_A_1 の FC です。

1. 削除が必要な cluster_B の古いシェルフ上のアグリゲートを特定します。

   この例では、 MetroCluster FC cluster_B によってホストされている次のデータアグリゲートを削除する必要があります。 aggr_data_A1 と aggr_data_A2 。

   シェルフ上のデータアグリゲートを特定、オフライン、および削除するには、次の手順を実行する必要があります。この例は、 1 つのクラスタだけを対象としています。

```
cluster_B::> aggr show

Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
aggr0_node_A_1-FC
           349.0GB   16.83GB   95% online       1 node_A_1-IP
raid_dp,

mirrored,

normal
aggr0_node_A_2-IP
           349.0GB   16.83GB   95% online       1 node_A_2-IP
raid_dp,

mirrored,

normal
...
8 entries were displayed.

cluster_B::>
```

2. データアグリゲートに MDV_AUD ボリュームが含まれているかどうかを確認し、アグリゲートを削除する前にそれらを削除してください。

   MDV_AUD ボリュームは移動できないため、削除する必要があります。

3. 各アグリゲートをオフラインにしてから削除します。

   a. アグリゲートをオフラインにします。

      「 storage aggregate offline-aggregate aggregate-name 」の形式で指定します

      次の例は、アグリゲート node_B_1 をオフラインにします。

      ```
      cluster_B::> storage aggregate offline -aggregate node_B_1_aggr0

      Aggregate offline successful on aggregate: node_B_1_aggr0
      ```

   b. アグリゲートを削除します。

      「 storage aggregate delete -aggregate aggregate-name 」の形式で指定します

プロンプトが表示されたら、プレックスを破棄できます。

次の例は、削除するアグリゲート node_B_1 の aggr0 を示しています。

```
cluster_B::> storage aggregate delete -aggregate node_B_1_aggr0
Warning: Are you sure you want to destroy aggregate "node_B_1_aggr0"?
{y|n}: y
[Job 123] Job succeeded: DONE

cluster_B::>
```

4. すべてのアグリゲートを削除したら、電源をオフにし、シェルフを切断して取り外します。
5. 上記の手順を繰り返して、 cluster_A シェルフを撤去します。

移行を完了しています

古いコントローラモジュールを取り外した状態で、移行プロセスを完了できます。

ステップ

1. 移行プロセスを完了します。

   の手順を実行します "システムを通常動作に戻します"。

新しいコントローラで既存シェルフを使用できない場合の停止を伴う移行（ ONTAP 9.8 以降）

ONTAP 9.8 以降では、 2 ノードの MetroCluster FC 構成を無停止で移行し、既存のストレージシェルフが新しい MetroCluster IP ノードでサポートされていない場合でも、既存のドライブシェルフからデータを移動できます。

- この手順は、既存のストレージシェルフモデルが新しい MetroCluster IP プラットフォームモデルでサポートされていない場合にのみ使用してください。
- この手順は、 ONTAP 9.8 以降を実行しているシステムでサポートされています。
- この手順はシステムの停止を伴います。
- この手順は、 2 ノード MetroCluster FC 構成にのみ適用されます。

  4 ノード MetroCluster FC 構成の場合は、を参照してください "移行する手順を選択します"。

- すべての要件を満たし、手順のすべての手順に従う必要があります。

コンソールログを有効にする

NetAppでは、使用しているデバイスでコンソールロギングをイネーブルにし、この手順を実行する際に次のアクションを実行することを強く推奨します。

- メンテナンス中はAutoSupportを有効のままにします。
- メンテナンスの前後にメンテナンスAutoSupportメッセージをトリガーして、メンテナンスアクティビティ中にケースの作成を無効にします。

  ナレッジベースの記事を参照してください "スケジュールされたメンテナンス時間中にケースの自動作成を停止する方法"。

- 任意のCLIセッションのセッションロギングをイネーブルにします。セッションログを有効にする方法については、ナレッジベースの記事の「セッション出力のログ」セクションを参照してください "ONTAPシステムへの接続を最適化するためのPuTTYの設定方法"。

新しいノードでシェルフがサポートされていない場合の移行の要件

移行プロセスを開始する前に、構成が要件を満たし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

- 既存の構成は 2 ノードのファブリック接続またはストレッチ MetroCluster 構成である必要があり、すべてのノードで ONTAP 9.8 以降が実行されている必要があります。

  新しい MetroCluster IP コントローラモジュールは、同じバージョンの ONTAP 9.8 を実行している必要があります。

- 既存のプラットフォームと新しいプラットフォームの組み合わせは、移行対象としてサポートされている必要があります。

  "無停止移行でサポートされるプラットフォーム"

- の説明に従って、すべての要件とケーブル配線を満たしている必要があります "ファブリック接続 MetroCluster のインストールと設定"。
- 新しいコントローラに付属する新しいストレージシェルフ（ node_A_1 の IP 、 node_B_2 の IP 、 node_B_1 の IP 、および node_B_2 の IP ）が古いコントローラ（ node_A_1 の FC と node_B_1 の FC ）でサポートされている必要があります。

  "NetApp Hardware Universe の略"

- 古いストレージシェルフは、新しい MetroCluster IP プラットフォームモデルでは * サポートされていません。

  "NetApp Hardware Universe の略"

- 既存のシェルフで使用可能なスペアディスクに応じて、ドライブを追加する必要があります。

  必要なドライブシェルフがほかにもあります。

  各コントローラに 14~18 本のドライブを追加する必要があります。

  - 3 本のプール 0 ドライブ
  - プール 1 ドライブ × 3
  - 2 本のスペアドライブ
  - システムボリューム用に 6 ～ 10 台のドライブ

- 新しいノードを含む構成が、ドライブ数、ルートアグリゲートのサイズ容量など、構成のプラットフォーム制限を超えないようにする必要があります

  この情報は、各プラットフォームモデルの NetApp Hardware Universe _ で確認できます。

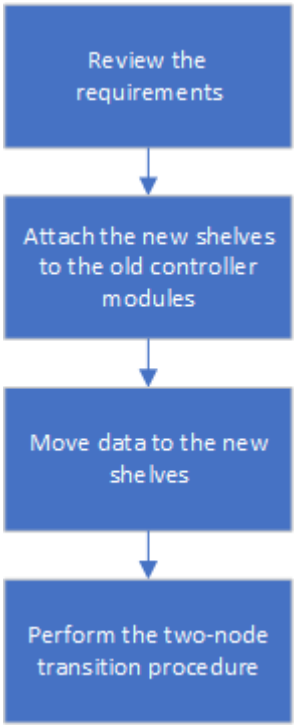
  "NetApp Hardware Universe の略"

- MetroCluster サイトから 6 つのすべてのノードのリモートコンソールアクセスが必要です。または、手順で必要に応じてサイト間の移動を計画しておく必要があります。

新しいコントローラでシェルフがサポートされない場合の停止を伴う移行のワークフロー

既存のシェルフモデルが新しいプラットフォームモデルでサポートされない場合は、新しいシェルフを古い構成に接続し、新しいシェルフにデータを移動して、新しい構成に移行する必要があります。

移行を準備する際は、サイト間の移動を計画します。リモートノードがラックに設置されてケーブル接続されたら、ノードへのシリアルターミナルアクセスが必要です。ノードが設定されるまでサービスプロセッサへのアクセスは許可されません。



新しいコントローラモジュールの準備を行います

新しいコントローラモジュールと新しいストレージシェルフの構成とディスク所有権をクリアする必要があります。

手順

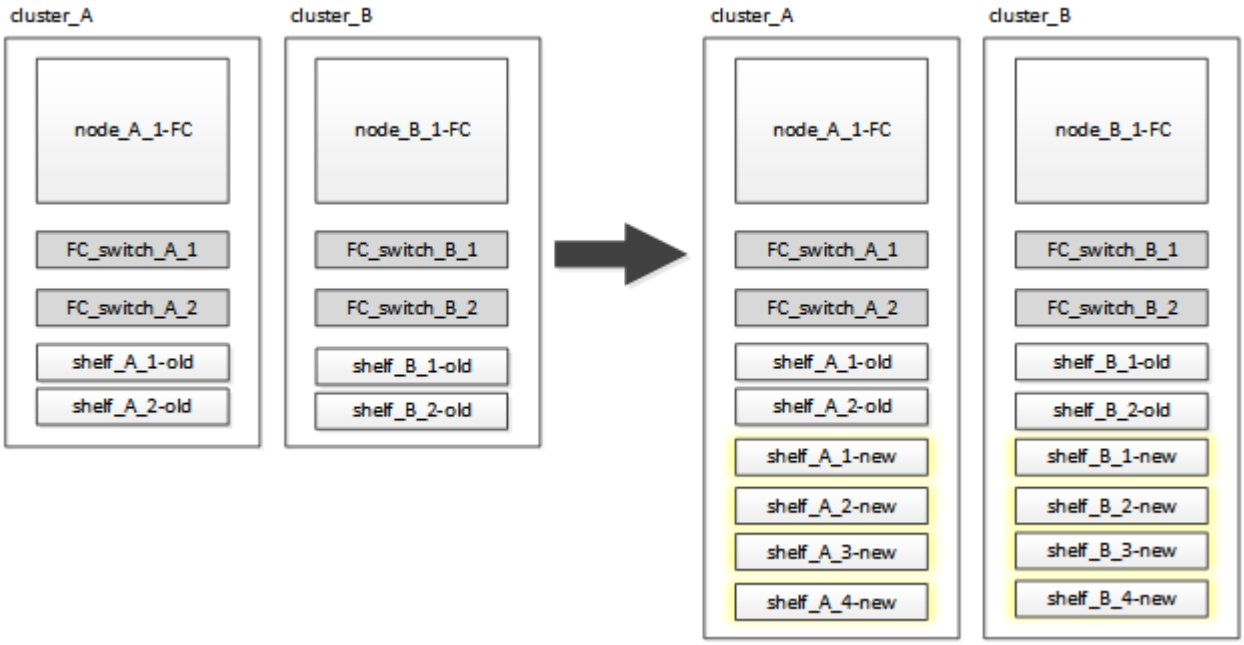
1. 新しいストレージシェルフを新しい MetroCluster IP コントローラモジュールに接続して、のすべての手順を実行します "MetroCluster IP コントローラの準備"。
2. 新しい MetroCluster IP コントローラモジュールから新しいストレージシェルフを切断します。

新しいディスクシェルフを既存の MetroCluster FC コントローラに接続

MetroCluster IP 構成に移行する前に、新しいドライブシェルフを既存のコントローラモジュールに接続する必要があります。

このタスクについて

次の図は、 MetroCluster FC 構成に新しいシェルフが接続された状態を示しています。



手順

1. node_A_1 の FC と node_A_2 のディスク自動割り当てを無効にします。

   disk option modify -node node_name autoassign off

   このコマンドはノードごとに実行する必要があります。

   ディスクの自動割り当ては、 node_A_1 に FC および node_B_1 に追加するシェルフの割り当てを回避するために無効になります。移行の一環として、ノード node_A_1 の IP と node_B_1 の IP にディスクを使用し、自動割り当てを許可した場合は、あとでディスク所有権を削除してから、 node_A_1 の IP と node_B_2 の IP にディスクを割り当てる必要があります。

2. 必要に応じて FC-to-SAS ブリッジを使用し、新しいシェルフを既存の MetroCluster FC ノードに接続します。

   の要件と手順を参照してください "MetroCluster FC 構成へのストレージのホットアド"

ルートアグリゲートを移行して、新しいディスクシェルフにデータを移動します

古いドライブシェルフから、 MetroCluster IP ノードで使用する新しいドライブシェルフにルートアグリゲートを移動する必要があります。

このタスクについて

このタスクは、既存のノード（ node_A_1 の FC と node_B_1 の FC ）に移行する前に実行します。

手順

1. コントローラ node_B_1 から FC からネゴシエートスイッチオーバーを実行します。

   MetroCluster スイッチオーバー

2. node_B_1 から FC へのリカバリのアグリゲートの修復とルートの修復の手順を実行します。

   「 MetroCluster heal-phase aggregates 」

   「 MetroCluster heal-phase root-aggregates 」

3. ブートコントローラ node_A_1 - FC ：

   「 boot_ontap 」

4. 新しいシェルフの未割り当てディスクをコントローラ node_A_1 の FC の適切なプールに割り当てます。

   a. シェルフのディスクを特定します。

      disk show -shelf pool_0_shelf-fields container-type 、 diskpathnames

      disk show -shelf pool_1_shelf-fields container-type 、 diskpathnames

   b. ローカルモードに切り替えて、ローカルノードでコマンドを実行します。

      'run local' のように指定します

   c. ディスクを割り当てます。

      「 disk assign disk1disk2disk3disk… 」 -p 0`

   「 disk assign disk4disk5disk6disk …」 -p 1`

   a. ローカルモードを終了します。

      「 exit

5. 新しいミラーされたアグリゲートを作成してコントローラ node_A_1 の新しいルートアグリゲートにします。

   a. 権限モードを advanced に設定します。

      'set priv advanced'

   b. アグリゲートを作成します。

      アグリゲート create -aggregate new_aggr-disklist disk1 、 disk2 、 disk3 、… -mirror-disklist disk4disk5 、 disk6 、… -raidtypese-as -exist-root-force-small-aggregate true aggr show -aggregate new_aggr-fields percent-snapshot-space を使用できます

      percent-snapshot-space 値が 5% 未満の場合は、 5% を超える値にする必要があります。

   aggr modify new_aggr-percent-snapshotSpace 5`

a. 権限モードを admin に戻します。

'set priv admin' のように設定します

6. 新しいアグリゲートが適切に作成されたことを確認します。

'node run -node local sysconfig -r を実行します

7. ノードレベルとクラスタレベルの構成バックアップを作成します。

> スイッチオーバー中にバックアップが作成されると、クラスタはスイッチオーバーされたリカバリの状態を認識します。システム構成のバックアップとアップロードは、このバックアップがなければクラスタ間で MetroCluster 構成を再確立できないために成功する必要があります。

a. クラスタバックアップを作成します。

' system configuration backup create -node local-backup-type cluster -backup-name_cluster-backup -name_`

b. クラスタバックアップの作成を確認します

「 job show -id job-IDStatus 」のように入力します

c. ノードバックアップを作成します。

system configuration backup create -node local-backup-type node-backup-name_node-backup-name-name_`

d. クラスタとノードの両方のバックアップを確認します。

「 system configuration backup show 」を参照してください

出力に両方のバックアップが表示されるまで、コマンドを繰り返し実行できます。

8. バックアップのコピーを作成します。

バックアップは、新しいルート・ボリュームのブート時にローカルで失われるため、別の場所に保存する必要があります。

FTP または HTTP サーバにバックアップをアップロードしたり、「 scp 」コマンドを使用してバックアップをコピーしたりできます。

プロセス	手順

• バックアップを FTP または HTTP サーバ * にアップロードします	a. クラスタバックアップをアップロードします。 'system configuration backup upload -node local-backup_cluster-backup-name_-destination url b. ノードバックアップをアップロードします。 'system configuration backup upload -node local-backup_node-backup-name_-destination url
• セキュアコピー * を使用して、バックアップをリモート・サーバにコピーします	リモートサーバから次の scp コマンドを使用します。 a. クラスタバックアップをコピーします。 `scp diagnode-mgmt -FC) :/mroot/etc/backup/config/cluster-backup-name.7z b. ノードのバックアップをコピーします。 「 scp diag@node-mgmt -fc ： /mroot/etc/backup/config/node-backup-name.7z 」を参照してください

9. node_A_1 の停止 - FC ：

   halt -node local-ignore-quorum -warnings true

10. node_A_1 のブート - FC をメンテナンスモードにします。

    「 boot_ontap maint 」を使用してください

11. メンテナンスモードで、必要な変更を行ってアグリゲートを root として設定します。

    a. HA ポリシーを CFO に設定します。

       「 aggr options new_aggr ha_policy cfo 」を参照してください

       続行するかどうかを確認するメッセージが表示されたら、「 yes 」と入力します。

```
Are you sure you want to proceed (y/n)?
```

    a. 新しいアグリゲートを root として設定します。

       「 aggr options new_aggr root 」のように指定します

    b. LOADER プロンプトに移動します。

       「 halt 」

12. コントローラをブートして、システム構成をバックアップします。

新しいルートボリュームが検出されると、ノードはリカバリモードでブートします

a. コントローラをブートします。

「 boot_ontap 」

b. ログインし、設定をバックアップします。

ログインすると、次の警告が表示されます。

```
Warning: The correct cluster system configuration backup must be
restored. If a backup
from another cluster or another system state is used then the root
volume will need to be
recreated and NGS engaged for recovery assistance.
```

a. advanced 権限モードに切り替えます。

「 advanced 」の権限が必要です

b. クラスタ構成をサーバにバックアップします。

「 system configuration backup download -node local-source url of server/cluster-backup-name.7z

c. ノード構成をサーバにバックアップします。

「 system configuration backup download -node local-source url of server/node-backup-name.7z

d. admin モードに戻ります。

「特権管理者」

13. クラスタの健常性を確認します。

a. 次のコマンドを問題に設定します。

「 cluster show 」を参照してください

b. 権限モードを advanced に設定します。

「 advanced 」の権限が必要です

c. クラスタ構成の詳細を確認します。

「 cluster ring show 」を参照してください

d. admin 権限レベルに戻ります。

「特権管理者」

14. MetroCluster 構成の運用モードを確認し、 MetroCluster チェックを実行

a. MetroCluster 構成と運用モードが正常な状態であることを確認します。

「 MetroCluster show 」

b. 想定されるすべてのノードが表示されることを確認します。

MetroCluster node show

c. 次のコマンドを問題に設定します。

「 MetroCluster check run 」のようになります

d. MetroCluster チェックの結果を表示します。

MetroCluster チェックショー

15. コントローラ node_B_1 から FC にスイッチバックを実行します。

MetroCluster スイッチバック

16. MetroCluster 構成の動作を確認します。

a. MetroCluster 構成と運用モードが正常な状態であることを確認します。

「 MetroCluster show 」

b. MetroCluster チェックを実行します。

「 MetroCluster check run 」のようになります

c. MetroCluster チェックの結果を表示します。

MetroCluster チェックショー

17. 新しいルートボリュームを Volume Location Database に追加します。

a. 権限モードを advanced に設定します。

「 advanced 」の権限が必要です

b. ノードにボリュームを追加します。

volume add-other-volumes – node node_A_1 -FC

c. admin 権限レベルに戻ります。

「特権管理者」

18. ボリュームが認識され、 mroot であることを確認します。

a. アグリゲートを表示します。

「 storage aggregate show

b. ルートボリュームの mroot が使用されていることを確認します。

storage aggregate show -fields には -mroot があります

c. ボリュームを表示します。

volume show

19. 新しいセキュリティ証明書を作成して System Manager へのアクセスを再度有効にします。

'security certificate create -common-name_-type server-size 2048

20. 同じ手順を繰り返して、 node_A_1 の FC が所有するシェルフのアグリゲートを移行します。
21. クリーンアップを実行します。

古いルートボリュームとルートアグリゲートを削除するには、 node_A_1 の FC と node_B_1 の両方で次の手順を実行する必要があります。

a. 古いルートボリュームを削除します。

'run local' のように指定します

vol offline old_vol0

「 vol destroy old_vol0 」のようになります

「 exit

volume remove-other-volume -vserver node_name -volume old_vol0

b. 元のルートアグリゲートを削除します。

「 aggr offline -aggregate old_aggr0_cluster1_01 」のように表示されます

「 aggr delete -aggregate old_aggr0_cluster1_01 」のように表示されます

22. 新しいコントローラ上のアグリゲートに、一度に 1 つのボリュームずつデータボリュームを移行します。

を参照してください "アグリゲートの作成と新しいノードへのボリュームの移動"

23. の手順をすべて実行して古いシェルフを撤去します "撤去するシェルフは node_A_1 から FC 、 node_A_1 から FC を移行"。

構成を移行しています

詳細な移行手順に従う必要があります。

このタスクについて

以降の手順では、他のトピックに進んでいます。各トピックの手順は記載された順序で実行する必要があります。

手順

1. ポートマッピングを計画

   のすべての手順を実行します "MetroCluster FC ノードから MetroCluster IP ノードへのポートのマッピング"。

2. MetroCluster IP コントローラを準備

   のすべての手順を実行します "MetroCluster IP コントローラの準備"。

3. MetroCluster 構成の健全性を確認

   のすべての手順を実行します "MetroCluster FC 構成の健全性の確認"。

4. 既存の MetroCluster FC ノードを準備して削除

   のすべての手順を実行します "MetroCluster FC ノードを移行します"。

5. 新しい MetroCluster IP ノードを追加します。

   のすべての手順を実行します "MetroCluster IP コントローラモジュールを接続します"。

6. 新しい MetroCluster IP ノードの移行と初期設定を完了します。

   のすべての手順を実行します "新しいノードの設定と移行の完了"。

FC SAN ワークロードを MetroCluster FC ノードから MetroCluster IP ノードに移動する

MetroCluster FC ノードから IP ノードへの無停止移行時は、 FC SAN ホストオブジェクトを MetroCluster FC ノードから IP ノードに無停止で移動する必要があります。

FC SAN ワークロードを MetroCluster FC ノードから MetroCluster IP ノードに移動する

手順

1. MetroCluster IP ノードで新しい FC インターフェイス（ LIF ）をセットアップします。

   a. 必要に応じて、 MetroCluster IP ノードで、 FC ターゲットパーソナリティへのクライアント接続に使用する FC ポートを変更します。

      そのためには、ノードのリブートが必要になる場合があります。

   b. すべてのSAN SVMについて、IPノードにFC LIF /インターフェイスを作成します。必要に応じて、新しく作成したFC LIFのWWPNがFC SANスイッチにログインしていることを確認します。

2. MetroCluster IP ノードに新しく追加した FC LIF の SAN ゾーニング設定を更新します。

   FC SAN クライアントにデータをアクティブに提供している LUN を含むボリュームを移動しやすいように、既存の FC スイッチゾーンを更新して、 FC SAN クライアントが MetroCluster IP ノード上の LUN にアクセスできるようにします。

a. FC SAN スイッチ（ Cisco または Brocade ）で、新しく追加した FC SAN LIF の WWPN をゾーンに追加します。

b. ゾーニングの変更を更新、保存、コミットします。

c. クライアントから、 MetroCluster IP ノード上の新しい SAN LIF への FC イニシエータログインを確認します。「 svmluns lun show -p

この時点で、クライアントは MetroCluster FC ノードと MetroCluster IP ノードの両方の FC インターフェイスを認識し、ログインしている必要があります。LUN とボリュームは引き続き MetroCluster FC ノードで物理的にホストされます。

MetroCluster は FC ノードインターフェイスでのみ報告されるため、クライアントには FC ノード経由のパスのみが表示されます。これは、の出力で確認できます。 `sanlun lun show -p` および `multipath -ll -d` コマンド

```
[root@stemgr]# sanlun lun show -p
ONTAP Path: vsa_1:/vol/vsa_1_vol6/lun_linux_12
 LUN: 4
 LUN Size: 2g
 Product: cDOT
 Host Device: 3600a098038304646513f4f674e52774b
 Multipath Policy: service-time 0
 Multipath Provider: Native
--------- ---------- ------- ------------
----------------------------------------------
host vserver
path path /dev/ host vserver
state type node adapter LIF
--------- ---------- ------- ------------
----------------------------------------------
up primary sdk host3 iscsi_lf__n2_p1_
up secondary sdh host2 iscsi_lf__n1_p1_

[root@stemgr]# multipath -ll -d
3600a098038304646513f4f674e52774b dm-5 NETAPP ,LUN C-Mode
size=2.0G features='4 queue_if_no_path pg_init_retries 50
retain_attached_hw_handle' hwhandler='1 alua' wp=rw
|-+- policy='service-time 0' prio=50 status=active
| `- 3:0:0:4 sdk 8:160 active ready running
`-+- policy='service-time 0' prio=10 status=enabled
 `- 2:0:0:4 sdh 8:112 active ready running
```

3. レポートノードを変更して MetroCluster IP ノードを追加します

a. SVM 上の LUN のレポートノードを一覧表示します。 lun mapping show -vserver vserver-name -fields reporting-nodes -ostype linux

表示されるレポートノードはローカルノードで、 LUN は FC ノード A_1 および a_2 に物理的に配置されています。

```
cluster_A::> lun mapping show -vserver vsa_1 -fields reporting-nodes
-ostype linux

vserver  path                          igroup         reporting-nodes
-------  ----------------------------- ------------
-------------------------------------
vsa_1    /vol/vsa_1_vol1/lun_linux_2 igroup_linux   A_1,A_2
vsa_1    /vol/vsa_1_vol1/lun_linux_3 igroup_linux   A_1,A_2
vsa_1    /vol/vsa_1_vol2/lun_linux_4 igroup_linux   A_1,A_2
vsa_1    /vol/vsa_1_vol3/lun_linux_7 igroup_linux   A_1,A_2
vsa_1    /vol/vsa_1_vol4/lun_linux_8 igroup_linux   A_1,A_2
vsa_1    /vol/vsa_1_vol4/lun_linux_9 igroup_linux   A_1,A_2
vsa_1    /vol/vsa_1_vol6/lun_linux_12 igroup_linux  A_1,A_2
vsa_1    /vol/vsa_1_vol6/lun_linux_13 igroup_linux  A_1,A_2
vsa_1    /vol/vsa_1_vol7/lun_linux_14 igroup_linux  A_1,A_2
vsa_1    /vol/vsa_1_vol8/lun_linux_17 igroup_linux  A_1,A_2
vsa_1    /vol/vsa_1_vol9/lun_linux_18 igroup_linux  A_1,A_2
vsa_1    /vol/vsa_1_vol9/lun_linux_19 igroup_linux  A_1,A_2
12 entries were displayed.
```

b. MetroCluster IP ノードを追加してレポートノードを追加します。

```
cluster_A::> lun mapping add-reporting-nodes -vserver vsa_1 -path
/vol/vsa_1_vol*/lun_linux_* -nodes B_1,B_2 -igroup igroup_linux

12 entries were acted on.
```

c. レポートノードをリストし、新しいノードが存在することを確認します。

```
cluster_A::> lun mapping show -vserver vsa_1 -fields reporting-nodes
-ostype linux

vserver path                            igroup          reporting-nodes
------- ------------------------------  ------------
-------------------------------------------------------------------------
----------

vsa_1   /vol/vsa_1_vol1/lun_linux_2   igroup_linux    A_1,A_2,B_1,B_2
vsa_1   /vol/vsa_1_vol1/lun_linux_3   igroup_linux    A_1,A_2,B_1,B_2
vsa_1   /vol/vsa_1_vol2/lun_linux_4   igroup_linux    A_1,A_2,B_1,B_2
vsa_1   /vol/vsa_1_vol3/lun_linux_7   igroup_linux    A_1,A_2,B_1,B_2
...

12 entries were displayed.
```

d. を確認します `sg3-utils` パッケージがLinuxホストにインストールされている。これにより、 `rescan-scsi-bus.sh utility not found` 新しくマッピングされたLUNのLinuxホストをを使用して再スキャンするとエラーが発生する `rescan-scsi-bus` コマンドを実行します

e. ホストのSCSIバスを再スキャンして、新しく追加したパスを検出します。 `/usr/bin/rescan-scsi-bus.sh -a`

```
[root@stemgr]# /usr/bin/rescan-scsi-bus.sh -a
Scanning SCSI subsystem for new devices
Scanning host 0 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 1 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 2 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
 Scanning for device 2 0 0 0 ...
.
.
.
OLD: Host: scsi5 Channel: 00 Id: 00 Lun: 09
 Vendor: NETAPP Model: LUN C-Mode Rev: 9800
 Type: Direct-Access ANSI SCSI revision: 05
0 new or changed device(s) found.
0 remapped or resized device(s) found.
0 device(s) removed.
```

f. 新しく追加されたパス「 'lun lun lun lun show -p 」を表示します

各 LUN には 4 つのパスがあります。

```
[root@stemgr]# sanlun lun show -p
ONTAP Path: vsa_1:/vol/vsa_1_vol6/lun_linux_12
 LUN: 4
 LUN Size: 2g
 Product: cDOT
 Host Device: 3600a0980383046465l3f4f674e52774b
 Multipath Policy: service-time 0
 Multipath Provider: Native
--------- ---------- ------- ------------
----------------------------------------------
host vserver
path path /dev/ host vserver
state type node adapter LIF
--------- ---------- ------- ------------
----------------------------------------------
up primary sdk host3 iscsi_lf__n2_p1_
up secondary sdh host2 iscsi_lf__n1_p1_
up secondary sdag host4 iscsi_lf__n4_p1_
up secondary sdah host5 iscsi_lf__n3_p1_
```

g. コントローラで、 LUN が含まれているボリュームを MetroCluster FC から MetroCluster IP ノードに移動します。

```
cluster_A::> vol move start -vserver vsa_1 -volume vsa_1_vol1
-destination-aggregate A_1_htp_005_aggr1
[Job 1877] Job is queued: Move "vsa_1_vol1" in Vserver "vsa_1" to
aggregate "A_1_htp_005_aggr1". Use the "volume move show -vserver
vsa_1 -volume vsa_1_vol1"
command to view the status of this operation.
cluster_A::> volume move show
Vserver    Volume    State    Move Phase   Percent-Complete Time-To-
Complete
--------- ---------- -------- ----------   ---------------
----------------
vsa_1     vsa_1_vol1 healthy  initializing
 - -
```

h. FC SAN クライアントで、 LUN 情報「 lun lun show -p 」を表示します

LUN が配置された MetroCluster IP ノードの FC インターフェイスは、プライマリパスとして更新されます。ボリューム移動後にプライマリパスが更新されない場合は、 /usr/bin/rescan-scsi-bus.sh -a を実行するか、マルチパスの再スキャンが実行されるのを待ちます。

次の例のプライマリパスは、 MetroCluster IP ノード上の LIF です。

```
[root@localhost ~]# sanlun lun show -p

                    ONTAP Path: vsa_1:/vol/vsa_1_vol1/lun_linux_2
                           LUN: 22
                      LUN Size: 2g
                       Product: cDOT
                   Host Device: 3600a098038302d324e5d50305063546e
              Multipath Policy: service-time 0
            Multipath Provider: Native
--------- ---------- ------- ------------
----------------------------------------------
host      vserver
path      path       /dev/   host         vserver
state     type       node    adapter      LIF
--------- ---------- ------- ------------
----------------------------------------------
up        primary    sddv    host6        fc_5
up        primary    sdjx    host7        fc_6
up        secondary  sdgv    host6        fc_8
up        secondary  sdkr    host7        fc_8
```

a. FC SAN ホストに属するすべてのボリューム、 LUN 、および FC インターフェイスについて、上記の手順を繰り返します。

   完了したら、特定の SVM および FC SAN ホストのすべての LUN を MetroCluster IP ノードに配置する必要があります。

4. レポートノードを削除し、クライアントからパスを再スキャンします。

   a. Linux LUN のリモートレポートノード（ MetroCluster FC ノード）を削除します。「 lun mapping remove-reporting-nodes -vserver vsA_1-path * -igroup igroup_linux-remote-nodes true

      ```
      cluster_A::> lun mapping remove-reporting-nodes -vserver vsa_1 -path
      * -igroup igroup_linux -remote-nodes true
      12 entries were acted on.
      ```

   b. LUN のレポートノードを確認します。「 lun mapping show -vserver vsA_1 -fields reporting-nodes -ostype linux

```
cluster_A::> lun mapping show -vserver vsa_1 -fields reporting-nodes
-ostype linux

vserver path igroup reporting-nodes
------- --------------------------- ------------
----------------------------------------
vsa_1 /vol/vsa_1_vol1/lun_linux_2 igroup_linux B_1,B_2
vsa_1 /vol/vsa_1_vol1/lun_linux_3 igroup_linux B_1,B_2
vsa_1 /vol/vsa_1_vol2/lun_linux_4 igroup_linux B_1,B_2
...

12 entries were displayed.
```

c. クライアントのSCSIバスを再スキャンします。 `/usr/bin/rescan-scsi-bus.sh -r`

MetroCluster FC ノードからパスが削除されます。

```
[root@stemgr]# /usr/bin/rescan-scsi-bus.sh -r
Syncing file systems
Scanning SCSI subsystem for new devices and remove devices that have
disappeared
Scanning host 0 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 1 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 2 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
sg0 changed: LU not available (PQual 1)
REM: Host: scsi2 Channel: 00 Id: 00 Lun: 00
DEL: Vendor: NETAPP Model: LUN C-Mode Rev: 9800
 Type: Direct-Access ANSI SCSI revision: 05
sg2 changed: LU not available (PQual 1)
.
.
.
OLD: Host: scsi5 Channel: 00 Id: 00 Lun: 09
 Vendor: NETAPP Model: LUN C-Mode Rev: 9800
 Type: Direct-Access ANSI SCSI revision: 05
0 new or changed device(s) found.
0 remapped or resized device(s) found.
24 device(s) removed.
 [2:0:0:0]
 [2:0:0:1]
...
```

a. MetroCluster IP ノードからのパスだけがホストから認識されていることを確認します。 'lun lun lun show -p

b. 必要に応じて、 MetroCluster FC ノードから iSCSI LIF を削除します。

他のクライアントにマッピングされたノード上に他の LUN がない場合に実施する必要があります。

Linux iSCSI ホストを MetroCluster FC ノードから MetroCluster IP ノードに移動

MetroCluster ノードを FC から IP に移行したあと、 iSCSI ホスト接続を新しいノードに移動しなければならない場合があります。

このタスクについて

- IPv4インターフェイスは、新しいiSCSI接続のセットアップ時に作成されます。
- ホストのコマンドと例は、Linuxオペレーティングシステムに固有のものです。
- MetroCluster FCノードは「古いノード」、MetroCluster IPノードは「新しいノード」と呼ばれます。

手順1：新しいiSCSI接続をセットアップする

iSCSI接続を移行するには、新しいノードへの新しいiSCSI接続をセットアップします。

手順

1. 新しいノードにiSCSIインターフェイスを作成し、iSCSIホストから新しいノードの新しいインターフェイスへのping接続を確認します。

   "ネットワークインターフェイスを作成"

   SVMのすべてのiSCSIインターフェイスにiSCSIホストから到達できる必要があります。

2. iSCSIホストで、ホストから古いノードへの既存のiSCSI接続を特定します。

   ```
   iscsiadm -m session
   ```

   ```
   [root@scspr1789621001 ~]# iscsiadm -m session
   tcp: [1] 10.230.68.236:3260,1156 iqn.1992-
   08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6 (non-flash)
   tcp: [2] 10.230.68.237:3260,1158 iqn.1992-
   08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6 (non-flash)
   ```

3. 新しいノードで、新しいノードからの接続を確認します。

   ```
   iscsi session show -vserver <svm-name>
   ```

```
node_A_1-new::*> iscsi session show -vserver vsa_1
 Tpgroup Initiator Initiator
Vserver Name TSIH Name ISID Alias
--------- ------- ---- ----------------------- ---------
--------------------
vsa_1 iscsi_lf__n1_p1_ 4 iqn.2020-
01.com.netapp.englab.gdl:scspr1789621001 00:02:3d:00:00:01
scspr1789621001.gdl.englab.netapp.com
vsa_1 iscsi_lf__n2_p1_ 4 iqn.2020-
01.com.netapp.englab.gdl:scspr1789621001 00:02:3d:00:00:02
scspr1789621001.gdl.englab.netapp.com
2 entries were displayed.
```

4. 新しいノードで、インターフェイスが含まれているSVMのONTAPのiSCSIインターフェイスを一覧表示します。

```
iscsi interface show -vserver <svm-name>
```

```
sti8200mcchtp001htp_siteA::*> iscsi interface show -vserver vsa_1
 Logical Status Curr Curr
Vserver Interface  TPGT Admin/Oper IP Address Node Port Enabled
------- ---------- ---- ---------- --------------- ----------- ----
-------
vsa_1 iscsi_lf__n1_p1_ 1156 up/up 10.230.68.236 sti8200mcc-htp-001 e0g
true
vsa_1 iscsi_lf__n1_p2_ 1157 up/up fd20:8b1e:b255:805e::78c9 sti8200mcc-
htp-001 e0h true
vsa_1 iscsi_lf__n2_p1_ 1158 up/up 10.230.68.237 sti8200mcc-htp-002 e0g
true
vsa_1 iscsi_lf__n2_p2_ 1159 up/up fd20:8b1e:b255:805e::78ca sti8200mcc-
htp-002 e0h true
vsa_1 iscsi_lf__n3_p1_ 1183 up/up 10.226.43.134 sti8200mccip-htp-005 e0c
true
vsa_1 iscsi_lf__n4_p1_ 1188 up/up 10.226.43.142 sti8200mccip-htp-006 e0c
true
6 entries were displayed.
```

5. iSCSIホストで、SVMのいずれかのiSCSI IPアドレスで検出を実行して、新しいターゲットを検出します。

```
iscsiadm -m discovery -t sendtargets -p iscsi-ip-address
```

検出は、 iSCSI 以外のインターフェイスを含め、 SVM の任意の IP アドレスで実行できます。

```
[root@scspr1789621001 ~]# iscsiadm -m discovery -t sendtargets -p
10.230.68.236:3260
10.230.68.236:3260,1156 iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6
10.226.43.142:3260,1188 iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6
10.226.43.134:3260,1183 iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6
10.230.68.237:3260,1158 iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6
```

6. iSCSIホストで、検出されたすべてのアドレスにログインします。

```
iscsiadm -m node -L all -T node-address -p portal-address -l
```

```
[root@scspr1789621001 ~]# iscsiadm -m node -L all -T iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6 -p
10.230.68.236:3260 -l
Logging in to [iface: default, target: iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6, portal:
10.226.43.142,3260] (multiple)
Logging in to [iface: default, target: iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6, portal:
10.226.43.134,3260] (multiple)
Login to [iface: default, target: iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6, portal:
10.226.43.142,3260] successful.
Login to [iface: default, target: iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6, portal:
10.226.43.134,3260] successful.
```

7. iSCSIホストで、ログインと接続を確認します。

```
iscsiadm -m session
```

```
[root@scspr1789621001 ~]# iscsiadm -m session
tcp: [1] 10.230.68.236:3260,1156 iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6 (non-flash)
tcp: [2] 10.230.68.237:3260,1158 iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6 (non-flash)
tcp: [3] 10.226.43.142:3260,1188 iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6 (non-flash)
```

8. 新しいノードで、ログインとホストとの接続を確認します。

```
iscsi initiator show -vserver <svm-name>
```

```
sti8200mcchtp001htp_siteA::*> iscsi initiator show -vserver vsa_1
 Tpgroup Initiator
Vserver Name              TSIH Name                   ISID
Igroup Name
------- --------          ---- -------------------- -----------------
-----------------
vsa_1 iscsi_lf__n1_p1_ 4 iqn.2020-
01.com.netapp.englab.gdl:scspr1789621001 00:02:3d:00:00:01 igroup_linux
vsa_1 iscsi_lf__n2_p1_ 4 iqn.2020-
01.com.netapp.englab.gdl:scspr1789621001 00:02:3d:00:00:02 igroup_linux
vsa_1 iscsi_lf__n3_p1_ 1 iqn.2020-
01.com.netapp.englab.gdl:scspr1789621001 00:02:3d:00:00:04 igroup_linux
vsa_1 iscsi_lf__n4_p1_ 1 iqn.2020-
01.com.netapp.englab.gdl:scspr1789621001 00:02:3d:00:00:03 igroup_linux
4 entries were displayed.
```

結果

このタスクが完了すると、（古いノードと新しいノードの）すべてのiSCSIインターフェイスが認識され、それらのすべてのインターフェイスにログインします。

LUNとボリュームは、古いノードで物理的にホストされたままです。LUNは古いノードインターフェイスでのみ報告されるため、ホストには古いノード経由のパスのみが表示されます。これを確認するには、 `sanlun lun show -p` および `multipath -ll -d` ホスト上のコマンドとコマンド出力を確認します。

```
[root@scspr1789621001 ~]# sanlun lun show -p
ONTAP Path: vsa_1:/vol/vsa_1_vol6/lun_linux_12
 LUN: 4
 LUN Size: 2g
 Product: cDOT
 Host Device: 3600a098038304646513f4f674e52774b
 Multipath Policy: service-time 0
 Multipath Provider: Native
--------- ---------- ------- ------------ ------------------
host vserver
path path /dev/ host vserver
state     type       node    adapter      LIF
--------- ---------- ------- ------------ ------------------
up        primary    sdk     host3        iscsi_lf__n2_p1_
up        secondary  sdh     host2        iscsi_lf__n1_p1_
[root@scspr1789621001 ~]# multipath -ll -d
3600a098038304646513f4f674e52774b dm-5 NETAPP ,LUN C-Mode
size=2.0G features='4 queue_if_no_path pg_init_retries 50
retain_attached_hw_handle' hwhandler='1 alua' wp=rw
|-+- policy='service-time 0' prio=50 status=active
| `- 3:0:0:4 sdk 8:160 active ready running
`-+- policy='service-time 0' prio=10 status=enabled
 `- 2:0:0:4 sdh 8:112 active ready running
```

手順2：新しいノードをレポートノードとして追加する

新しいノードへの接続をセットアップしたら、新しいノードをレポートノードとして追加します。

手順

1. 新しいノードで、SVM上のLUNのレポートノードのリストを表示します。

   ```
   lun mapping show -vserver <svm-name> -fields reporting-nodes -ostype
   linux
   ```

   次のレポートノードは、LUNが物理的に古いノードnode_A_1-oldとnode_A_2-oldにあるため、ローカルノードです。

```
node_A_1-new::*> lun mapping show -vserver vsa_1 -fields reporting-nodes
-ostype linux
vserver path                          igroup       reporting-nodes
------- ----------------------------- ------------
---------------------------
vsa_1   /vol/vsa_1_vol1/lun_linux_2  igroup_linux node_A_1-old,node_A_2-
old
.
.
.
vsa_1   /vol/vsa_1_vol9/lun_linux_19 igroup_linux node_A_1-old,node_A_2-
old
12 entries were displayed.
```

2. 新しいノードで、レポートノードを追加します。

```
lun mapping add-reporting-nodes -vserver <svm-name> -path
/vol/vsa_1_vol*/lun_linux_* -nodes node1,node2 -igroup <igroup_name>
```

```
node_A_1-new::*> lun mapping add-reporting-nodes -vserver vsa_1 -path
/vol/vsa_1_vol*/lun_linux_* -nodes node_A_1-new,node_A_2-new
-igroup igroup_linux
12 entries were acted on.
```

3. 新しいノードで、新しく追加したノードが存在することを確認します。

```
lun mapping show -vserver <svm-name> -fields reporting-nodes -ostype
linux vserver path igroup reporting-nodes
```

```
node_A_1-new::*> lun mapping show -vserver vsa_1 -fields reporting-nodes
-ostype linux vserver path igroup reporting-nodes
------- -------------------------- ------------
------------------------------------------------------------------------
-------
vsa_1 /vol/vsa_1_vol1/lun_linux_2 igroup_linux node_A_1-old,node_A_2-
old,node_A_1-new,node_A_2-new
vsa_1 /vol/vsa_1_vol1/lun_linux_3 igroup_linux node_A_1-old,node_A_2-
old,node_A_1-new,node_A_2-new
.
.
.
12 entries were displayed.
```

4. 。 `sg3-utils` パッケージがLinuxホストにインストールされている必要があります。これにより、 `rescan-scsi-bus.sh utility not found` 新しくマッピングされたLUNのLinuxホストをを使用して再スキャンするとエラーが発生する `rescan-scsi-bus` コマンドを実行します

   ホストで、 `sg3-utils` パッケージがインストールされています：

   - Debianベースのディストリビューションの場合:

     ```
     dpkg -l | grep sg3-utils
     ```

   - Red Hatベースのディストリビューションの場合：

     ```
     rpm -qa | grep sg3-utils
     ```

   必要に応じて、 `sg3-utils` Linuxホストのパッケージ：

   ```
   sudo apt-get install sg3-utils
   ```

5. ホストで、ホストのSCSIバスを再スキャンし、新しく追加したパスを検出します。

   ```
   /usr/bin/rescan-scsi-bus.sh -a
   ```

```
[root@stemgr]# /usr/bin/rescan-scsi-bus.sh -a
Scanning SCSI subsystem for new devices
Scanning host 0 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 1 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 2 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
 Scanning for device 2 0 0 0 ...
.
.
.
OLD: Host: scsi5 Channel: 00 Id: 00 Lun: 09
 Vendor: NETAPP Model: LUN C-Mode Rev: 9800
 Type: Direct-Access ANSI SCSI revision: 05
0 new or changed device(s) found.
0 remapped or resized device(s) found.
0 device(s) removed.
```

6. iSCSIホストで、新しく追加したパスの一覧を表示します。

```
sanlun lun show -p
```

LUN ごとに 4 つのパスが表示されます。

```
[root@stemgr]# sanlun lun show -p
ONTAP Path: vsa_1:/vol/vsa_1_vol6/lun_linux_12
 LUN: 4
 LUN Size: 2g
 Product: cDOT
 Host Device: 3600a098038304646513f4f674e52774b
 Multipath Policy: service-time 0
 Multipath Provider: Native
------- ---------- ------- ----------- ---------------------
host vserver
path path /dev/ host vserver
state   type       node    adapter     LIF
------  ---------- ------- ----------- ---------------------
up      primary    sdk      host3      iscsi_lf__n2_p1_
up      secondary  sdh     host2       iscsi_lf__n1_p1_
up      secondary  sdag    host4       iscsi_lf__n4_p1_
up      secondary  sdah    host5       iscsi_lf__n3_p1_
```

7. 新しいノードで、LUNを含むボリュームを古いノードから新しいノードに移動します。

```
node_A_1-new::*> vol move start -vserver vsa_1 -volume vsa_1_vol1
-destination-aggregate sti8200mccip_htp_005_aggr1
[Job 1877] Job is queued: Move "vsa_1_vol1" in Vserver "vsa_1" to
aggregate "sti8200mccip_htp_005_aggr1". Use the "volume move show
-vserver
vsa_1 -volume vsa_1_vol1" command to view the status of this operation.
node_A_1-new::*> vol move show
Vserver  Volume      State       Move       Phase            Percent-
Complete  Time-To-Complete
-------- ----------  --------    ---------- ----------------
---------------  ----------------
vsa_1    vsa_1_vol1  healthy                initializing     -
-
```

8. 新しいノードへのボリュームの移動が完了したら、ボリュームがオンラインになっていることを確認します。

```
volume show -state
```

9. LUNを配置した新しいノードのiSCSIインターフェイスがプライマリパスとして更新されます。ボリューム移動後にプライマリパスが更新されない場合は、次のコマンドを実行します。 `/usr/bin/rescan-scsi-bus.sh -a` および `multipath -v3` またはマルチパスの再スキャンが実行されるまで待ちます。

   次の例では、新しいノードのLIFがプライマリパスになっています。

```
[root@stemgr]# sanlun lun show -p
ONTAP Path: vsa_1:/vol/vsa_1_vol6/lun_linux_12
 LUN: 4
 LUN Size: 2g
 Product: cDOT
 Host Device: 3600a098038304646513f4f674e52774b
 Multipath Policy: service-time 0
 Multipath Provider: Native
--------- ---------- ------- ------------ ----------------------
host vserver
path path /dev/ host vserver
state     type       node    adapter      LIF
--------- ---------- ------- ------------ ------------------------
up        primary    sdag    host4        iscsi_lf__n4_p1_
up        secondary  sdk     host3        iscsi_lf__n2_p1_
up        secondary  sdh     host2        iscsi_lf__n1_p1_
up        secondary  sdah    host5        iscsi_lf__n3_p1_
```

手順3：レポートノードを削除してパスを再スキャンする

レポートノードを削除し、パスを再スキャンする必要があります。

手順

1. 新しいノードで、Linux LUNのリモートのレポートノード（新しいノード）を削除します。

```
lun mapping remove-reporting-nodes -vserver <svm-name> -path * -igroup
<igroup_name> -remote-nodes true
```

この場合、リモートノードは古いノードです。

```
node_A_1-new::*> lun mapping remove-reporting-nodes -vserver vsa_1 -path
* -igroup igroup_linux -remote-nodes true
12 entries were acted on.
```

2. 新しいノードで、LUNのレポートノードを確認します。

```
lun mapping show -vserver <svm-name> -fields reporting-nodes -ostype
linux
```

```
node_A_1-new::*> lun mapping show -vserver vsa_1 -fields reporting-nodes
-ostype linux
vserver  path                           igroup        reporting-nodes
-------  -----------------------------  ------------
-------------------------
vsa_1    /vol/vsa_1_vol1/lun_linux_2  igroup_linux  node_A_1-
new,node_A_2-new
vsa_1    /vol/vsa_1_vol1/lun_linux_3  igroup_linux  node_A_1-
new,node_A_2-new
vsa_1    /vol/vsa_1_vol2/lun_linux_4  group_linux   node_A_1-
new,node_A_2-new
.
.
.
12 entries were displayed.
```

3. 。 `sg3-utils` パッケージがLinuxホストにインストールされている必要があります。これにより、 `rescan-scsi-bus.sh utility not found` 新しくマッピングされたLUNのLinuxホストをを使用して再スキャンするとエラーが発生する `rescan-scsi-bus` コマンドを実行します

ホストで、 `sg3-utils` パッケージがインストールされています：

- Debianベースのディストリビューションの場合:

```
dpkg -l | grep sg3-utils
```

- Red Hatベースのディストリビューションの場合：

```
rpm -qa | grep sg3-utils
```

必要に応じて、 `sg3-utils` Linuxホストのパッケージ：

```
sudo apt-get install sg3-utils
```

4. iSCSIホストで、SCSIバスを再スキャンします。

```
/usr/bin/rescan-scsi-bus.sh -r
```

削除されるパスは古いノードからのパスです。

```
[root@scspr1789621001 ~]# /usr/bin/rescan-scsi-bus.sh -r
Syncing file systems
Scanning SCSI subsystem for new devices and remove devices that have
disappeared
Scanning host 0 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 1 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 2 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
sg0 changed: LU not available (PQual 1)
REM: Host: scsi2 Channel: 00 Id: 00 Lun: 00
DEL: Vendor: NETAPP Model: LUN C-Mode Rev: 9800
 Type: Direct-Access ANSI SCSI revision: 05
sg2 changed: LU not available (PQual 1)
.
.
.
OLD: Host: scsi5 Channel: 00 Id: 00 Lun: 09
 Vendor: NETAPP Model: LUN C-Mode Rev: 9800
 Type: Direct-Access ANSI SCSI revision: 05
0 new or changed device(s) found.
0 remapped or resized device(s) found.
24 device(s) removed.
 [2:0:0:0]
 [2:0:0:1]
.
.
.
```

5. iSCSIホストで、新しいノードからのパスだけが認識されることを確認します。

```
sanlun lun show -p
```

```
multipath -ll -d
```

追加情報の参照先

MetroCluster 設定の詳細については、を参照してください。

MetroCluster およびその他の情報

情報	件名

"MetroCluster IP 解決策のアーキテクチャおよび設計、 TR-4689"	• MetroCluster IP の構成と運用の技術概要 • MetroCluster IP 構成のベスト プラクティス。
"ファブリック接続 MetroCluster のインストールと設定"	• ファブリック接続 MetroCluster アーキテクチャ • 構成のケーブル接続 • FC-to-SAS ブリッジの設定 • FC スイッチを設定します • ONTAP で MetroCluster を設定します
"ストレッチ MetroCluster のインストールと設定"	• ストレッチ MetroCluster アーキテクチャ • 構成のケーブル接続 • FC-to-SAS ブリッジの設定 • ONTAP で MetroCluster を設定します
"MetroCluster の管理"	• MetroCluster 構成について • スイッチオーバー、修復、スイッチバック
"ディザスタリカバリ"	• ディザスタリカバリ • 強制スイッチオーバー • 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
"MetroCluster メンテナンス"	• MetroCluster FC 構成のメンテナンスガイドライン • 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 • ファブリック接続またはストレッチ MetroCluster FC 構成でのディスクシェルフのホットアド • ファブリック接続またはストレッチ MetroCluster FC 構成でのディスクシェルフのホットリムーブ • ファブリック接続またはストレッチ MetroCluster FC 構成のディザスタサイトでのハードウェア交換 • 2 ノードのファブリック接続またはストレッチ MetroCluster FC 構成の 4 ノード MetroCluster 構成への拡張 • 4 ノードのファブリック接続またはストレッチ MetroCluster FC 構成の 8 ノード MetroCluster FC 構成への拡張

"MetroCluster のアップグレードと拡張"	• MetroCluster 設定をアップグレードまたは更新する • ノードの追加による MetroCluster 構成の拡張
"MetroCluster の移行"	• MetroCluster FC 構成から MetroCluster IP 構成への移行
"MetroCluster のアップグレード、移行、拡張"	• MetroCluster Tiebreaker ソフトウェアを使用して MetroCluster 構成を監視する
"ONTAPハードウェアシステムのドキュメント" • 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。	• ディスクシェルフのホットアド • ディスクシェルフのホットリムーブ
"コピーベースの移行"	• 7-Mode ストレージシステムから clustered Data ONTAP ストレージシステムへデータを移行する
"ONTAP の概念"	• ミラーされたアグリゲートの機能

MetroCluster 構成をアップグレード、更新、または拡張します

まずはこちらから-手順 を選択してください

はじめに：コントローラのアップグレード、システムの更新、拡張のいずれかを選択してください

機器のアップグレードの範囲に応じて、コントローラのアップグレード手順 、システムの更新手順 、または拡張手順 を選択します。

- コントローラのアップグレード手順は、コントローラモジュールにのみ適用されます。コントローラが新しいコントローラモデルに置き換えられます。

  ストレージシェルフモデルはアップグレードされません。

  - スイッチオーバーとスイッチバックの手順では、パートナークラスタのコントローラモジュールをアップグレードしている間、 MetroCluster スイッチオーバー処理を使用してクライアントに無停止のサービスが提供されます。
  - ARL ベースコントローラのアップグレード手順では、アグリゲートの再配置処理を使用して、古い構成からアップグレード後の新しい構成へ、データを無停止で移動します。
- 更新手順は、コントローラとストレージシェルフに適用されます。

  更新手順では、新しいコントローラとシェルフを MetroCluster 構成に追加して 2 つ目の DR グループを作成すると、データが新しいノードに無停止で移行されます。

  その後、元のコントローラが撤去されます。
- 拡張手順によって、MetroCluster 構成にコントローラとシェルフが追加されるだけで、取り外しは不要になります。

  使用する手順 は、MetroCluster のタイプと既存のコントローラの数によって異なります。

SVMの移行が実行中の場合は、すべての移行プロセスが完了するまで待ってから、コントローラのアップグレード手順またはシステムの更新手順を開始します。アップグレードまたは更新のプロセス中は、新しいSVM移行処理を開始しないでください。

アップグレードの種類	手順
コントローラのアップグレード	"コントローラのアップグレード手順 を選択します"
システムの更新	"システム更新手順 を選択します"

拡張	• "2ノードMetroCluster から4ノード" • "4ノードMetroCluster FCから8ノード" • "4ノードMetroCluster のIPアドレスを8に設定します"

コントローラのアップグレード手順 を選択します

使用するコントローラアップグレード手順 は、プラットフォームモデルとMetroCluster 構成のタイプによって異なります。

アップグレード手順 では、コントローラが新しいコントローラモデルに置き換えられます。ストレージシェルフモデルはアップグレードされません。

- スイッチオーバーとスイッチバックの手順では、パートナークラスタのコントローラモジュールをアップグレードしている間、 MetroCluster スイッチオーバー処理を使用してクライアントに無停止のサービスが提供されます。
- ARL ベースコントローラのアップグレード手順では、アグリゲートの再配置処理を使用して、古い構成からアップグレード後の新しい構成へ、データを無停止で移動します。

サポートされるコントローラのアップグレード

サポートされるMetroCluster IPコントローラとFCコントローラのアップグレードの組み合わせについて説明します。

system controller replaceコマンドを使用したサポートされる**MetroCluster IP**コントローラのアップグレード

サポートされるプラットフォームについては、の表を参照して "「system controller replace」コマンドを使用したスイッチオーバーとスイッチバックを使用した4ノードMetroCluster IP構成のコントローラのアップグレード（ONTAP 9.13.1以降）" ください。

サポートされているその他すべての**MetroCluster IP**コントローラのアップグレード

このセクションのMetroClusterコントローラーのアップグレード表から、お使いの*ソース*プラットフォームを検索してください。*ソース*プラットフォーム行と*ターゲット*プラットフォーム列が空白の場合、アップグレードはサポートされていません。

- お使いのプラットフォームがリストに表示されない場合は、サポートされているコントローラのアップグレードの組み合わせはありません。
- コントローラのアップグレードを実行するときは、古いプラットフォームタイプと新しいプラットフォームタイプ*が一致している必要があります*。
  - FASシステムをFASシステムにアップグレードしたり、AFF AシリーズをAFF Aシリーズにアップグレードしたりすることができます。
  - FASシステムをAFF Aシリーズにアップグレードしたり、AFF AシリーズをAFF Cシリーズにアップグレードしたりすることはできません。

    たとえば、アップグレードするプラットフォームがFAS8200の場合は、FAS9000にアップグレードできます。FAS8200システムをAFF A700システムにアップグレードすることはできません。

- MetroCluster構成内のすべてのノード（新旧のノード）で同じバージョンのONTAPが実行されている必要があります。ご使用の組み合わせでサポートされるONTAPの最小バージョンについては、を参照して"Hardware Universe"ください。

サポートされる**AFF**および**FAS MetroCluster IP**コントローラのアップグレード

次の表に、MetroCluster IP構成でAFFまたはFASシステムを手動でアップグレードする場合にサポートされるプラットフォームの組み合わせを2つのグループに分けて示します。

- *グループ1 *は、AFF A150 FAS8700、AFF AFF C400 A20、FAS2750 AFF A400、AFF A220、FAS500f、AFF C250、AFF A250、FAS50、AFF A300 C30、AFF A320 A30、FAS8200、AFF、AFF、FAS8300システムへのアップグレードの組み合わせを示しています。
- *グループ2 *は、AFF C60、AFF A50、FAS70、FAS9000、AFF A700、AFF A90、AFF A900、AFF、FAS9500、AFF C800、AFF A800 C80、FAS90、AFF A70、およびAFF A1Kシステムへのアップグレードの組み合わせを示しています。

次の注意事項は両方のグループに適用されます。

- 注1：このアップグレードでは、次の手順を使用してください。"スイッチオーバーとスイッチバックを使用して、MetroCluster IP構成のAFF A700 / FAS9000からAFF A900 / FAS9500にコントローラをアップグレードする（ONTAP 9.10.1以降）"
- 注2：コントローラのアップグレードは、ONTAP 9.13.1以降を実行しているシステムでサポートされます。
- 注3：コントローラのアップグレードが完了するまで、ターゲットプラットフォームに内蔵ドライブを搭載することはできません。内蔵ドライブはアップグレード後に追加できます。
- 注 4：統合システム（ディスクとコントローラが同じシャーシ内にある）をアップグレードする場合は、既存のシャーシとディスクを保持しながらコントローラ モジュールを交換する必要があります。
- 注5：古いコントローラを外付けSASシェルフに変換するには、IOMモジュールが必要です。サポートされているIOMモジュールについては、を参照してください"Hardware Universe"。

AFFと**FAS**の組み合わせグループ**1**

AFF A150 FAS8700、AFF AFF C400 A20、FAS2750 AFF A400、AFF A220、AFF、AFF C250、AFF A250、FAS50、FAS500f C30、AFF A320 A30、FAS8200、AFF A300、AFF、FAS8300システムへのアップグレードでサポートされる組み合わせを確認します。

AFF and FAS		Target MetroCluster IP platform									
		AFF A150	AFF A20	FAS2750 AFF A220	FAS500f AFF C250 AFF A250	FAS50	AFF C30 AFF A30	FAS8200 AFF A300	AFF A320	FAS8300 AFF C400 AFF A400	FAS8700
Source MetroCluster IP platform	AFF A150		Note 5								
	AFF A20										
	FAS2750 AFF A220		Note 5								
	FAS500f AFF C250 AFF A250						Note 4				
	FAS50										
	AFF C30 AFF A30										
	FAS8200 AFF A300										
	AFF A320										
	FAS8300 AFF C400 AFF A400										
	FAS8700										
	AFF C60										
	AFF A50										
	FAS70										
	FAS9000 AFF A700										
	AFF A70										
	AFF C800 AFF A800										
	FAS9500 AFF A900										
	AFF C80										
	FAS90										
	AFF A90										
	AFF A1K										

AFFと**FAS**の組み合わせグループ**2**

C60、AFF A50、FAS70、、AFF A700、AFF A70、AFF C800、AFF、AFF A90、FAS9000、AFF、AFF A900、AFF A800 C80、FAS90、FAS9500、およびAFF A1Kシステムへのアップグレードでサポートされる組み合わせを確認します。

AFF and FAS		Target MetroCluster IP platform										
		AFF C60	AFF A50	FAS70	FAS9000 AFF A700	AFF A70	AFF C800 AFF A800	FAS9500 AFF A900	AFF C80	FAS90	AFF A90	AFF A1K
Source MetroCluster IP platform	AFF A150											
	AFF A20											
	FAS2750 AFF A220											
	FAS500f AFF C250 AFF A250											
	FAS50											
	AFF C30 AFF A30											
	FAS8200 AFF A300					Note 3		Note 2			Note 3	
	AFF A320											
	FAS8300 AFF C400 AFF A400					Note 3		Note 2	Note 3		Note 3	
	FAS8700							Note 2				
	AFF C60											
	AFF A50											
	FAS70											
	FAS9000 AFF A700					Note 3		Note 1			Note 3	
	AFF A70										Note 4	
	AFF C800 AFF A800								Note 4		Note 4	
	FAS9500 AFF A900										Note 3	
	AFF C80											
	FAS90											
	AFF A90											
	AFF A1K											

サポートされる**ASA MetroCluster IP**コントローラのアップグレード

次の表に、MetroCluster IP構成でASAシステムを手動でアップグレードする場合にサポートされるプラットフォームの組み合わせを示します。

ASA		Target MetroCluster IP platform							
		ASA A150	ASA C250	ASA A250	ASA C400	ASA A400	ASA C800	ASA A800	ASA A900
Source MetroCluster IP platform	ASA A150								
	ASA C250								
	ASA A250								
	ASA C400								
	ASA A400								Note 1
	ASA C800								
	ASA A800								
	ASA A900								

- 注1：コントローラのアップグレードは、ONTAP 9.13.1以降を実行しているシステムでサポートされます。

サポートされる**MetroCluster FC**コントローラのアップグレード

このセクションのMetroClusterコントローラーのアップグレード表から、お使いの*ソース*プラットフォームを検索してください。*ソース*プラットフォーム行と*ターゲット*プラットフォーム列が空白の場合、アップグレードはサポートされていません。

- お使いのプラットフォームがリストに表示されない場合は、サポートされているコントローラのアップグレードの組み合わせはありません。
- コントローラのアップグレードを実行するときは、古いプラットフォームタイプと新しいプラットフォームタイプ*が一致している必要があります*。
  - FASシステムをFASシステムにアップグレードしたり、AFF AシリーズをAFF Aシリーズにアップグレ

ードしたりすることができます。

- FASシステムをAFF Aシリーズにアップグレードしたり、AFF AシリーズをAFF Cシリーズにアップグレードしたりすることはできません。

  たとえば、アップグレードするプラットフォームがFAS8200の場合は、FAS9000にアップグレードできます。FAS8200システムをAFF A700システムにアップグレードすることはできません。

- MetroCluster構成内のすべてのノード（新旧のノード）で同じバージョンのONTAPが実行されている必要があります。ご使用の組み合わせでサポートされるONTAPの最小バージョンについては、を参照して"Hardware Universe"ください。

サポートされる**AFF**および**FAS MetroCluster FC**コントローラのアップグレード

次の表に、MetroCluster FC構成のAFFシステムまたはFASシステムのアップグレードでサポートされるプラットフォームの組み合わせを示します。

FAS and AFF		Target MetroCluster FC platform									
		FAS80x0	AFF80x0	FAS8200	AFF A300	FAS8300	AFF A400	FAS9000	AFF A700	FAS9500	AFF A900
Source MetroCluster FC platform	FAS8020	Note 1		Note 1		Note 1		Note 1			
	AFF8020		Note 1		Note 1		Note 1		Note 1		
	FAS8040 FAS8060 FAS8080										
	AFF8040 AFF8060 AFF8080										
	FAS8200					Note 2		Note 2		Note 4	
	AFF A300						Note 2		Note 2		Note 4
	FAS8300									Note 4	
	AFF A400										Note 4
	FAS9000									Note 3	
	AFF A700										Note 3
	FAS9500										
	AFF A900										

- 注1：既存のFAS8020またはAFF8020ノードでFCVI接続にポート1cと1dを使用する場合は、次のコントローラをアップグレードしますhttps://kb.netapp.com/Advice_and_Troubleshooting/Data_Protection_and_Security/MetroCluster/Upgrading_controllers_when_FCVI_connections_on_existing_FAS8020_or_AFF8020_nodes_use_ports_1c_and_1d["ナレッジベースの記事"^]。
- 注2：オンボードポート0eおよび0fをFC-VI接続として使用するAFF A300またはFAS8200プラットフォームからのコントローラのアップグレードは、次のシステムでのみサポートされます。
  - ONTAP 9.9.1以前
  - ONTAP 9.10.1P9
  - ONTAP 9.11.1P5
  - ONTAP 9.12.1GA
  - ONTAP 9.13.1以降

  詳細については、を参照してください"パブリックレポート"。
- 注3：このアップグレードについては、を参照してください"スイッチオーバーとスイッチバックを使用して、MetroCluster FC構成のAFF A700 / FAS9000からAFF A900/ FAS9500にコントローラをアップグレード（ONTAP 9.10.1以降）"
- 注4：コントローラのアップグレードは、ONTAP 9.13.1以降を実行しているシステムでサポートされます。

サポートされる**ASA MetroCluster FC**コントローラのアップグレード

次の表に、MetroCluster FC構成のASAシステムのアップグレードでサポートされるプラットフォームの組み合わせを示します。

ソース**MetroCluster FC**プラットフォーム	デスティネーション**MetroCluster FC**プラットフォーム	サポートの有無
ASA A400	ASA A400	はい。
	ASA A900	いいえ
ASA A900	ASA A400	いいえ
	ASA A900	○（注1を参照）

- 注1：コントローラのアップグレードは、ONTAP 9.14.1以降を実行しているシステムでサポートされます。

スイッチオーバーとスイッチバックのプロセスを使用する手順を選択

サポートされるアップグレードの組み合わせを確認したら、構成に適したコントローラのアップグレード手順を選択します。

MetroCluster タイプ	アップグレード方法	ONTAP バージョン	手順
IP	「system controller replace」コマンドを使用してアップグレードします	9.13.1以降	"手順 へのリンク"
FC	「system controller replace」コマンドを使用してアップグレードします	9.10.1 以降	"手順 へのリンク"
FC	CLIコマンドによる手動アップグレード（AFF A700 / FAS9000からAFF A900 / FAS9500へのアップグレードのみ）	9.10.1 以降	"手順 へのリンク"

IP	CLIコマンドによる手動アップグレード（AFF A700 / FAS9000からAFF A900 / FAS9500へのアップグレードのみ）	9.10.1 以降	"手順 へのリンク"
FC	CLIコマンドを使用した手動アップグレード	9.8 以降	"手順 へのリンク"
IP	CLIコマンドを使用した手動アップグレード	9.8 以降	"手順 へのリンク"

アグリゲートの再配置を使用した手順の選択

ARL ベースコントローラのアップグレード手順では、アグリゲートの再配置処理を使用して、古い構成からアップグレード後の新しい構成へ、データを無停止で移動します。

MetroCluster タイプ	アグリゲートの再配置	**ONTAP** バージョン	手順
FC	「system controller replace」コマンドを使用して、同じシャーシ内のコントローラモデルをアップグレードします	9.10.1 以降	"手順 へのリンク"
FC	「 system controller replace 」コマンドを使用します	9.8 以降	"手順 へのリンク"
FC	「 system controller replace 」コマンドを使用します	9.5 ～ 9.7	"手順 へのリンク"
FC	手動 ARL コマンドを使用	9.8	"手順 へのリンク"
FC	手動 ARL コマンドを使用	9.7 以前	"手順 へのリンク"

システムの更新方法を選択する

使用するシステム更新手順 は、プラットフォームモデルおよびMetroCluster 構成のタイプによって異なります。更新手順は、コントローラとストレージシェルフに適用されます。更新手順では、新しいコントローラとシェルフを MetroCluster 構成に追加して 2 つ

目の DR グループを作成すると、データが新しいノードに無停止で移行されます。その後、元のコントローラが撤去されます。

サポートされている**MetroCluster IP Tech Refresh**の組み合わせ

- 新しい負荷を追加する前に、機器更改（Tech Refresh）の手順 を完了する必要があります。
- MetroCluster構成内のすべてのノードで同じバージョンのONTAPが実行されている必要があります。たとえば、8ノード構成の場合は、8つのすべてのノードで同じバージョンのONTAPを実行する必要があります。ご使用の組み合わせでサポートされるONTAPの最小バージョンについては、を参照して"Hardware Universe"ください。
- 組み合わせて使用するプラットフォームの「下位」のオブジェクト制限を超えないようにしてください。2つのプラットフォームのオブジェクトの下限を適用します。
- ターゲットプラットフォームの制限がMetroCluster の制限よりも低い場合は、新しいノードを追加する前に、ターゲットプラットフォームの制限以下になるようにMetroCluster を再設定する必要があります。
- を参照してください "Hardware Universe" プラットフォームの制限：

サポートされる**AFF**と**FAS MetroCluster IP**の機器更改の組み合わせ

次の表に、MetroCluster IP構成のAFFシステムまたはFASシステムの更新でサポートされるプラットフォームの組み合わせを示します。テーブルは次の2つのグループに分割されます。

- *グループ1 *は、、AFF A20、FAS2750、AFF A220、AFF A150、FAS500f、AFF C250、FAS8200、FAS50、AFF C400 C30、AFF A30、AFF A250、AFF A300、AFF A400、FAS8700、AFF、AFF A320、FAS8300システムの組み合わせを示しています。
- *グループ2 *は、AFF C60、AFF A50、FAS70、FAS9000、AFF A700、AFF A70、AFF C800、AFF、FAS9500、AFF A900、AFF A800 C80、FAS90、AFF A90、およびAFF A1Kシステムの組み合わせを示しています。

次の注意事項は両方のグループに適用されます。

- 注1：この組み合わせを使用するには、ONTAP 9.13.1以降が必要です。

AFFとFASの組み合わせグループ1

AFF A150 FAS8700、AFF AFF C400 A20、FAS2750 AFF A400、AFF A220、AFF、AFF C250、AFF A250、FAS50、FAS500f C30、AFF A320 A30、FAS8200、AFF A300、AFF、FAS8300システムのシステム更新の組み合わせを確認します。

AFF and FAS		Target MetroCluster IP platform									
		AFF A150	AFF A20	FAS2750 AFF A220	FAS500f AFF C250 AFF A250	FAS50	AFF C30 AFF A30	FAS8200 AFF A300	AFF A320	FAS8300 AFF C400 AFF A400	FAS8700
Source MetroCluster IP platform	AFF A150	Note 1		Note 1	Note 1					Note 1	Note 1
	AFF A20										
	FAS2750 AFF A220	Note 1		Note 1	Note 1					Note 1	Note 1
	FAS500f AFF C250 AFF A250				Note 1					Note 1	Note 1
	FAS50										
	AFF C30 AFF A30										
	FAS8200 AFF A300										
	AFF A320										
	FAS8300 AFF C400 AFF A400										
	FAS8700										
	AFF C60										
	AFF A50										
	FAS70										
	FAS9000 AFF A700										
	AFF A70										
	AFF C800 AFF A800										
	FAS9500 AFF A900										
	AFF C80										
	FAS90 AFF A90										
	AFF A1K										

AFFとFASの組み合わせグループ2

C60、AFF A50、FAS70、、AFF A700、AFF A70、AFF C800、AFF、AFF A90、FAS9000、AFF、AFF A1K、AFF A800 C80、FAS90、FAS9500、AFF A900システムのシステム更新の組み合わせを確認します。

AFF and FAS		Target MetroCluster IP platform									
		AFF C60	AFF A50	FAS70	FAS9000 AFF A700	AFF A70	AFF C800 AFF A800	FAS9500 AFF A900	AFF C80	FAS90 AFF A90	AFF A1K
Source MetroCluster IP platform	AFF A150				Note 1		Note 1	Note 1			
	AFF A20										
	FAS2750 AFF A220				Note 1		Note 1	Note 1			
	FAS500f AFF C250 AFF A250				Note 1		Note 1	Note 1			
	FAS50										
	AFF C30 Aff A30										
	FAS8200 AFF A300										
	AFF A320										
	FAS8300 AFF C400 AFF A400										
	FAS8700										
	AFF C60										
	AFF A50										
	FAS70										
	FAS9000 AFF A700										
	AFF A70										
	AFF C800 AFF A800										
	FAS9500 AFF A900										
	AFF C80										
	FAS90 AFF A90										
	AFF A1K										

サポートされる**ASA MetroCluster IP**の機器更改の組み合わせ

次の表に、MetroCluster IP構成でASAシステムを更新する際にサポートされるプラットフォームの組み合わせを示します。

ASA		Target MetroCluster IP platform							
		ASA A150	ASA C250	ASA A250	ASA C400	ASA A400	ASA C800	ASA A800	ASA A900
Source MetroCluster IP platform	ASA A150								
	ASA C250								
	ASA A250								
	ASA C400								
	ASA A400								
	ASA C800								
	ASA A800								
	ASA A900								

サポートされる**MetroCluster FC**機器更改の組み合わせ

- 新しい負荷を追加する前に、機器更改（Tech Refresh）の手順 を完了する必要があります。
- MetroCluster構成内のすべてのノードで同じバージョンのONTAPが実行されている必要があります。たとえば、8ノード構成の場合は、8つのすべてのノードで同じバージョンのONTAPを実行する必要があります。ご使用の組み合わせでサポートされるONTAPの最小バージョンについては、を参照して"Hardware Universe"ください。
- 組み合わせて使用するプラットフォームの「下位」のオブジェクト制限を超えないようにしてください。2つのプラットフォームのオブジェクトの下限を適用します。
- ターゲットプラットフォームの制限がMetroCluster の制限よりも低い場合は、新しいノードを追加する前

に、ターゲットプラットフォームの制限以下になるようにMetroCluster を再設定する必要があります。

- を参照してください "Hardware Universe" プラットフォームの制限：

サポートされる**AFF**と**FAS MetroCluster FC**の機器更改の組み合わせ

次の表に、MetroCluster FC構成のAFFシステムまたはFASシステムの更新でサポートされるプラットフォームの組み合わせを示します。

FAS and AFF		Destination MetroCluster FC platform							
		FAS8200	AFF A300	FAS8300	AFF A400	FAS9000	AFF A700	FAS9500	AFF A900
Source MetroCluster FC platform	FAS8200	■	■	■	■	■	■	■	■
	AFF A300	■	■	■	■	■	■	■	■
	FAS8300			■	■	■	■	■	■
	AFF A400			■	■	■	■	■	■
	FAS9000					■	■	■	■
	AFF A700					■	■	■	■
	FAS9500							■	■
	AFF A900							■	■

サポートされる**ASA MetroCluster FC**機器更改の組み合わせ

次の表に、MetroCluster FC構成のASAシステムの更新でサポートされるプラットフォームの組み合わせを示します。

ソース**MetroCluster FC**プラットフォーム	デスティネーション**MetroCluster FC**プラットフォーム	サポートの有無
ASA A400	ASA A400	はい。
	ASA A900	いいえ
ASA A900	ASA A400	いいえ
	ASA A900	はい。

更新手順の選択

次の表から、構成に応じた更新手順を選択します。

リフレッシュ方法	構成タイプ	**ONTAP** バージョン	手順
• 方法： MetroCluster 設定を展開して古いノードを削除します	4ノードFC	9.6 以降	"手順 へのリンク"
• 方法： MetroCluster 設定を展開して古いノードを削除します	4ノードIP	9.8 以降	"手順 へのリンク"

拡張手順 を選択します

使用する拡張手順 は、MetroCluster 構成のタイプとONTAP のバージョンによって異な

ります。

拡張手順 では、新しいコントローラとストレージをMetroCluster 構成に追加します。各サイトには偶数台のコントローラを配置し、元のMetroCluster 構成のノード数に応じて手順 を使用する必要があります。

拡張方法	構成タイプ	**ONTAP** バージョン	手順
方法：2ノードのMetroCluster FCを4に拡張します	2ノードFC	ONTAP 9以降（ONTAP 9.2以降ではプラットフォームがサポートされている必要があります）	"手順 へのリンク"
方法：4ノードMetroCluster FCを8に拡張	4ノードFC	ONTAP 9以降	"手順 へのリンク"
方法：4ノードMetroCluster IPを8に拡張する	4ノードIP	ONTAP 9.9.1以降	"手順 へのリンク"

「**system controller replace**」コマンドを使用したスイッチオーバーとスイッチバックを使用して、**4**ノード**MetroCluster IP**のコントローラをアップグレードする（**ONTAP 9.13.1**以降）

system controller replaceコマンドを使用した**MetroCluster IP**コントローラのアップグレードワークフロー（**ONTAP 9.13.1**以降）

このガイド付きの自動MetroClusterスイッチオーバー処理を使用すると、ONTAP 9.13.1以降を実行している4ノードMetroCluster IP構成でコントローラの無停止アップグレードを実行できます。この手順で他のコンポーネント（ストレージシェルフやスイッチなど）をアップグレードすることはできません。

このワークフローについて

このワークフローを使用して、コマンドでスイッチオーバーとスイッチバックを使用して、ONTAP 9.13.1以降を実行するMetroCluster IPコントローラをアップグレードできます `system controller replace`。

1. "アップグレードを準備"

サポートされているアップグレードの組み合わせと要件を確認し、必要な手順を実行してシステムをコントローラのアップグレードに備えます。コントローラの自動アップグレードプロセスでは、まず一連の事前確認が行われてから、設定情報を収集して既存の監視ソフトウェアを削除します。

2. "コントローラのアップグレード"

自動化処理によってスイッチオーバー処理が開始されます。これらの処理が完了すると処理が一時停止し、古いコントローラのネットワーク設定を準備し、新しいコントローラをラックに設置し、ルートアグリゲートディスクを再割り当てし、新しいコントローラをブートできるようになります。

3 "アップグレードを完了します"

ネットワークに到達できるかどうかを確認し、2つ目のサイトでアップグレードタスクを繰り返して、監視設定をリストアすることで、コントローラの自動アップグレードを完了します。

アップグレードを準備

system controller replaceコマンドを使用したサポートされる**MetroCluster IP**コントローラのアップグレード

MetroCluster IPコントローラのアップグレードを開始する前に、アップグレードの組み合わせがサポートされていることを確認する必要があります。

このセクションのMetroClusterコントローラーのアップグレード表から、お使いの*ソース*プラットフォームを検索してください。*ソース*プラットフォーム行と*ターゲット*プラットフォーム列が空白の場合、アップグレードはサポートされていません。

アップグレードを開始する前に、次の考慮事項を確認して、構成がサポートされていることを確認してください。

- お使いのプラットフォームがリストに表示されない場合は、サポートされているコントローラのアップグレードの組み合わせはありません。
- コントローラのアップグレードを実行するときは、古いプラットフォームタイプと新しいプラットフォームタイプ*が一致している必要があります*。
  - FASシステムをFASシステムにアップグレードしたり、AFF AシリーズをAFF Aシリーズにアップグレードしたりすることができます。
  - FASシステムをAFF Aシリーズにアップグレードしたり、AFF AシリーズをAFF Cシリーズにアップグレードしたりすることはできません。

    たとえば、アップグレードするプラットフォームがFAS8200の場合は、FAS9000にアップグレードできます。FAS8200システムをAFF A700システムにアップグレードすることはできません。
- MetroCluster構成内のすべてのノード（新旧のノード）で同じバージョンのONTAPが実行されている必要があります。ご使用の組み合わせでサポートされるONTAPの最小バージョンについては、を参照して"Hardware Universe"ください。

サポートされる**AFF**および**FAS MetroCluster IP**コントローラのアップグレード

次の表に、「system controller replace」コマンドを使用してMetroCluster IP構成のAFFまたはFASシステムをアップグレードする場合にサポートされるプラットフォームの組み合わせを2つのグループに分けて示します。

- *グループ1 *は、AFF A150 FAS8700、AFF AFF C400 A20、FAS2750 AFF A400、AFF A220、FAS500f、AFF C250、AFF A250、FAS50、AFF A300 C30、AFF A320 A30、FAS8200、AFF、AFF 、FAS8300システムへのアップグレードの組み合わせを示しています。
- *グループ2 *は、AFF C60、AFF A50、FAS70、FAS9000、AFF A700、AFF A90、AFF A900、AFF

、FAS9500、AFF C800、AFF A800 C80、FAS90、AFF A70、およびAFF A1Kシステムへのアップグレードの組み合わせを示しています。

次の注意事項は両方のグループに適用されます。

- 注1：コントローラのアップグレードは、ONTAP 9.13.1以降を実行しているシステムでサポートされます。
- 注2：コントローラのアップグレードが完了するまで、ターゲットプラットフォームに内蔵ドライブを搭載することはできません。内蔵ドライブはアップグレード後に追加できます。
- 注 3：統合システム（ディスクとコントローラが同じシャーシ内にある）のアップグレードでは、既存のシャーシとディスクを保持しながらコントローラモジュールを交換する必要があります。
- 注4：古いコントローラを外付けSASシェルフに変換するには、IOMモジュールが必要です。サポートされているIOMモジュールについては、"Hardware Universe"を参照してください。
- 注 5：ONTAP 9.18.1GA 以降が必要です。

AFFと**FAS**の組み合わせグループ**1**

AFF A150 FAS8700、AFF AFF C400 A20、FAS2750 AFF A400、AFF A220、AFF、AFF C250、AFF A250、FAS50、FAS500f C30、AFF A320 A30、FAS8200、AFF A300、AFF、FAS8300システムへのアップグレードでサポートされる組み合わせを確認します。

FAS and AFF		Target MetroCluster IP platform									
		AFF A150	AFF A20	FAS2750 AFF A220	FAS500f AFF C250 AFF A250	FAS50	AFF C30 AFF A30	FAS8200 AFF A300	AFF A320	FAS8300 AFF C400 AFF A400	FAS8700
Source MetroCluster IP platform	AFF A150		Note 4								
	AFF A20										
	FAS2750 AFF A220		Note 4								
	FAS500f AFF C250 AFF A250						Note 3				
	FAS50										
	AFF C30 AFF A20										
	FAS8200 AFF A300										
	AFF A320										
	FAS8300 AFF C400 AFF A400										
	FAS8700										
	AFF C60										
	AFF A50										
	FAS70										
	FAS9000 AFF A700										
	AFF A70										
	AFF C800 AFF A800										
	FAS9500 AFF A900										
	AFF C80										
	FAS90										
	AFF A90										
	AFF A1K										

AFFと**FAS**の組み合わせグループ**2**

C60、AFF A50、FAS70、、AFF A700、AFF A70、AFF C800、AFF、AFF A90、FAS9000、AFF、AFF A900、AFF A800 C80、FAS90、FAS9500、およびAFF A1Kシステムへのアップグレードでサポートされる組み合わせを確認します。

FAS and AFF		Target MetroCluster IP platform										
		AFF C60	AFF A50	FAS70	FAS9000 AFF A700	AFF A70	AFF C800 AFF A800	FAS9500 AFF A900	AFF C80	FAS90	AFF A90	AFF A1K
Source MetroCluster IP platform	AFF A150											
	AFF A20											
	FAS2750 AFF A220											
	FAS500f AFF C250 AFF A250											
	FAS50											
	AFF C30 AFF A20											
	FAS8200 AFF A300					Note 2		Note 1			Note 2	
	AFF A320											
	FAS8300 AFF C400 AFF A400					Note 2			Note 2		Note 2	
	FAS8700											
	AFF C60											
	AFF A50											
	FAS70									Note 5		
	FAS9000 AFF A700					Note 2					Note 2	
	AFF A70										Note 3 and Note 5	
	AFF C800 AFF A800								Note 3		Note 3	
	FAS9500 AFF A900										Note 2	
	AFF C80											
	FAS90											
	AFF A90											
	AFF A1K											

サポートされる**ASA MetroCluster IP**コントローラのアップグレード

ASAシステムでコマンドを使用したコントローラのアップグレード `system controller replace` はサポートされていません。

その他の手順については、を参照してください"アップグレードまたは更新の方法を選択"。

次の手順

を確認します "このアップグレード手順を使用するための要件"。

このMetroCluster IPアップグレード手順を使用するための要件

コントローラのアップグレードを実行する前に、システムがすべての要件を満たしていることを確認してください。

*コントローラーをアップグレードするたびに、この手順を記載どおりに実行する必要があります。*新しいプラットフォームがリリースされると、従う必要のある新しい手順や変更された手順が発生する可能性があります。たとえば、 ONTAP 9.15.1以降で導入されたプラットフォームにアップグレードする場合は、 "必要なブート引数を設定する" アップグレードを成功させるには、その他の追加手順を実行します。

- この手順は、コントローラのアップグレードにのみ使用できます。

  ストレージシェルフやスイッチなど、構成内の他のコンポーネントは同時にアップグレードできません。

- MetroCluster IPスイッチ（スイッチタイプ、ベンダー、モデル）とファームウェアバージョンがアップグレード構成の既存および新しいコントローラでサポートされている必要があります。

サポートされているスイッチとファームウェアのバージョンについては、またはを参照してください "Hardware Universe" "IMT" 。

- MetroCluster IPシステムが両方のサイトで同じバージョンのONTAPを実行している必要があります。
- 新しいシステムよりも多くのスロットまたはポートがあるシステムからアップグレードする場合は、新しいシステムに十分なスロットとポートがあることを確認する必要があります。

  アップグレードを開始する前に、を参照し"Hardware Universe"て、新しいシステムのスロットとポートの数を確認してください。

- この手順 を使用して、NSOベースの自動スイッチオーバーとスイッチバックを使用して4ノードMetroCluster IP構成のコントローラをアップグレードできます。

  4ノードMetroCluster IP構成では、「systems controller replace」コマンドを使用したアグリゲートの再配置（ARL）を使用したアップグレードはサポートされていません。

- システムで有効になっている場合は "エンドツーエンドの暗号化を無効にする" 、アップグレードを実行する前に実行します。
- NSOコントローラの自動アップグレード手順 を使用して、両方のサイトのコントローラを順番にアップグレードする必要があります。
- この NSO ベースのコントローラの自動アップグレード手順を使用すると、 MetroCluster ディザスタリカバリ（ DR ）サイトでコントローラの交換を開始できます。コントローラの交換は一度に 1 つのサイトでしか開始できません。
- サイト A でコントローラの交換を開始するには、サイト B からコントローラの交換開始コマンドを実行する必要があります交換処理ガイドは、サイト A の両方のノードのコントローラのみを交換する場合に使用します。サイト B のコントローラを交換するには、サイト A からコントローラ交換の開始コマンドを実行する必要がありますコントローラを交換するサイトを示すメッセージが表示されます。

この手順では、次の名前が使用されています。

- site_A で cluster_A
  - アップグレード前：
    - node_A_1 - 古い
    - Node_a_2-old
  - アップグレード後：
    - node_A_1 - 新規
    - Node_a_2 - 新規
- site_B （ site_B
  - アップグレード前：
    - node_B_1 - 古い
    - node_B_2 - 古い
  - アップグレード後：
    - node_B_1 - 新規

- node_B_2 - 新規

次の手順

"コンソールログを有効にする"です。

MetroCluster IPのアップグレード前にコンソールログを有効にする

コントローラのアップグレードを実行する前に、デバイスのコンソールログを有効にしてください。

NetAppでは、使用しているデバイスでコンソールロギングをイネーブルにし、この手順を実行する際に次のアクションを実行することを強く推奨します。

- メンテナンス中はAutoSupportを有効のままにします。
- メンテナンスの前後にメンテナンスAutoSupportメッセージをトリガーして、メンテナンスアクティビティ中にケースの作成を無効にします。

  ナレッジベースの記事を参照してください "スケジュールされたメンテナンス時間中にケースの自動作成を停止する方法"。

- 任意のCLIセッションのセッションロギングをイネーブルにします。セッションログを有効にする方法については、ナレッジベースの記事の「セッション出力のログ」セクションを参照してください "ONTAPシステムへの接続を最適化するためのPuTTYの設定方法"。

次の手順

の情報を参照し"必要なbootargを設定する（9.15.1以降で導入されたシステムにアップグレードする場合）"て、既存のシステムに必要なbootargを設定する必要があるかどうかを確認します。

必要な**bootarg**の設定（**ONTAP 9.15.1**以降で導入されたシステムへの**MetroCluster IP**のアップグレードの場合）

ONTAP 9.15.1 以降で導入されたシステムにアップグレードする場合は、通常、アップグレードを開始する前に、古いコントローラで bootarg を設定する必要があります。

> アップグレードの組み合わせが影響を受ける場合、アップグレードを成功させるには、すべての古いコントローラーで bootarg を設定する必要があります。このセクションの情報を注意深く確認して、アップグレードの組み合わせで bootarg を設定する必要があるかどうか、また組み合わせに対して正しい bootarg を設定する方法を確認してください。

ステップ**1:** 古いコントローラに**bootarg**を設定する必要があるかどうかを確認します

アップグレードを開始する前に、次の情報を使用して、古いコントローラに bootarg を設定する必要があるかどうかを確認します：

- 特に明記されていない限り、以下のシステムへのサポートされているアップグレードでは、古いコントローラに bootarg を設定する必要があります。
  - AFF A70、AFF A90、AFF A1K
  - FAS70、FAS90

- AFF C80用
- AFF A50、AFF A20、AFF A30
- AFF C30、AFF C60
- FAS50

- アップグレードが次のいずれかの組み合わせである場合、古いコントローラーで bootarg を設定する必要はありません。
  - AFF A70システムからAFF A90システムへ
  - FAS70システムからFAS90システムへ

アップグレードで bootarg を設定する必要がない場合は、このタスクをスキップして直接"システムのアップグレードを準備"に進むことができます。

ステップ**2:** 古いコントローラに設定する**bootarg**を決定する

影響を受けるアップグレードのほとんどは、 `hw.cxgbe.toe_keepalive_disable`古いコントローラ上の bootarg。ただし、特定のアップグレードパスでは、 `bootarg.siw.interop_enabled`代わりに bootarg を使用してください。

次の表を参照して、それぞれのアップグレードの組み合わせに設定する必要があるbootargを特定してください。

アップグレード対象	**bootarg**の設定
AFF A250からAFF A30へ	`bootarg.siw.interop_enabled`
AFF C250からAFF C30へ	`bootarg.siw.interop_enabled`
AFF A150からAFF A20へ	`bootarg.siw.interop_enabled`
AFF A220からAFF A20へ	`bootarg.siw.interop_enabled`
AFF A70、 AFF A90、 AFF A1K、FAS70、FAS90、AFF C80、 AFF A50、 AFF A30、 AFF C30、 AFF C60、またはFAS50システムへのその他のすべてのアップグレード 注**:** AFF A70システムからAFF A90システム、またはFAS70 システムから FAS90 システムへのアップグレードの場合は、bootarg を設定する必要はありません。	`hw.cxgbe.toe_keepalive_disable`

ステップ**3:** 古いコントローラに必要な**bootarg**を設定する

アップグレードの組み合わせに必要な bootarg を決定したら、手順に従って古いコントローラで bootarg を設定します。

アップグレードを開始する前に、両方のサイトのすべての古いノードで bootarg を設定する必要があります。

手順

1. 両方のサイトで一方のノードを停止し、そのHAパートナーでノードのストレージテイクオーバーを実行できるようにします。

   ```
   halt -node <node_name>
   ```

2. アップグレードの組み合わせに必要なbootargを設定します。の表を使用して、設定する必要があるbootargを決めておき設定が必要なbootargを特定するます。

   hw.cxgbe.toe_keepalive_disable

   a. `LOADER`停止したノードのプロンプトで、次のように入力します。

      ```
      setenv hw.cxgbe.toe_keepalive_disable 1
      ```

      'aveenv

      ```
      printenv hw.cxgbe.toe_keepalive_disable
      ```

   bootarg.siw.interop_enabled

   a. `LOADER`停止したノードのプロンプトで、次のように入力します。

      ```
      setenv bootarg.siw.interop_enabled 1
      ```

      'aveenv

      ```
      printenv bootarg.siw.interop_enabled
      ```

3. ノードをブートします。

   「 boot_ontap 」

4. ノードがブートしたら、プロンプトでノードのギブバックを実行します。

   ```
   storage failover giveback -ofnode <node_name>
   ```

5. アップグレードするDRグループ内の4つのノードすべてに対して、この手順を繰り返します。

次のステップ
"システムのアップグレードを準備"です。

MetroCluster IPシステムのアップグレードを準備

コントローラのアップグレードの準備として、新旧のプラットフォームモデルによっては、スイッチリファレンス構成ファイル（RCF）のアップグレードが必要になる場合があります。その後、システムの事前確認を実行し、設定情報を収集し、既存の監視ソフトウェアを削除します。

プラットフォームの新旧モデルによっては、コントローラをアップグレードする前にMetroCluster Switch Reference Configuration File（RCF；スイッチリファレンス構成ファイル）の更新が必要になる場合があります。

このタスクについて

この作業は、次の状況で実行します。

- スイッチのRCF設定が最小バージョンになっていません。
- バックエンドMetroCluster接続で使用するVLAN IDを変更する必要があります。

作業を開始する前に

コントローラをアップグレードする前にRCFの更新が必要かどうかを確認します。

- スイッチにサポートされる最小バージョンのRCFが設定されていない場合は、コントローラをアップグレードする前にRCFを更新する必要があります。

スイッチモデル	必要なRCFバージョン
Cisco 3132Q-V の設定	1.7 以降
Cisco 3232C	1.7 以降
Broadcom BES-53248 の場合	1.3 以降
NVIDIA SN2100	2.0以降

- 使用している古いプラットフォームモデルと新しいプラットフォームモデルの両方が次のリストにある場合は、コントローラをアップグレードする前にVLAN IDを更新する必要は*ありません*。
  - FAS8200またはAFF A300
  - AFF A320
  - FAS9000またはAFF A700
  - AFF A800、AFF C800、ASA A800、またはASA C800

    使用している古いプラットフォームモデルと新しいプラットフォームモデルのいずれかが上記に記載されていない場合は、MetroClusterインターフェイスでサポートされているVLAN IDが使用されていることを確認する必要があります。MetroClusterインターフェイスでサポートされるVLAN IDは、10、20、または101～4096の範囲です。

- VLAN IDが10、20、101~4096の範囲にない場合は、コントローラをアップグレードする前にスイッチのRCFをアップグレードする必要があります。
- ローカルクラスタ接続には任意のVLANを使用できます。指定した範囲内にある必要はありません。
- アップグレード先の新しいRCFでVLAN 10、20、または101~4096の範囲のVLANを使用する必要があります。ローカルクラスタのVLANは、必要な場合以外は変更しないでください。

手順

1. IPスイッチで新しいRCFを適用できるように準備します。

   スイッチベンダーに対応するセクションを参照してください。

   スイッチはswitch_A_1、switch_B_1、switch_A_2、switch_B_2の順に更新する必要があります。

   - "Broadcom IP スイッチを工場出荷時のデフォルトにリセットします"
   - "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"
   - "NVIDIA IP SN2100スイッチを工場出荷時のデフォルトにリセット"

2. RCFをダウンロードしてインストールします。

   スイッチベンダーに対応するセクションを参照してください。

   - "Broadcom RCFのダウンロードとインストール"
   - "Cisco IP RCFのダウンロードとインストール"
   - "NVIDIA IP RCFのダウンロードとインストール"

コントローラー交換操作を開始する

自動コントローラー交換操作を開始すると、一連の事前チェックが実行され、その後一時停止して、構成関連情報を手動で収集できるようになります。

このタスクについて

MetroClusterのチェックを開始する前に、ONTAPメディエーターがインストールされている場合は自動的に検出され、削除されます。削除を確認するには、ユーザ名とパスワードの入力を求められます。アップグレード完了時に事前チェックが失敗した場合、またはアップグレードを続行しないことを選択した場合は、手動で削除する必要があります。 "ONTAPメディエーターサービスを再設定する" 。

アップグレードのどの段階でも、サイト A から「 system controller replace show 」または「 system controller replace show -details 」コマンドを実行してステータスを確認できます。コマンドから何も出力されない場合は、数分待ってからコマンドを再実行してください。

手順

1. サイト B のコントローラーを交換するには、サイト A から次のコマンドを実行します。

```
system controller replace start -nso true
```

- 使用しない場合は `-nso true`コマンドにパラメータを指定すると、コントローラのアップグレード手順では、MetroCluster IP システムのデフォルトの手順として NSO ベースの自動スイッチオーバーとスイッチバックが選択されます。
- 一方のサイトでコントローラーを交換した後に、もう一方のサイトで同じ手順を繰り返すと、各サイトのノード間の不一致によりエラーが発生します。これは、両サイトで異なるプラットフォームモデルが存在する場合に想定される動作です。

  不一致エラーのみが返された場合は、 `-skip-metrocluster-check true`オプション `system controller replace start` MetroCluster チェックをスキップするコマンド。

自動操作によりチェックが実行されます。問題が見つからなかった場合は処理が一時停止するため、構成に関連する情報を手動で収集できます。

現在のソースシステムと互換性のあるすべてのターゲットシステムが表示されます。ソースコントローラを異なるONTAPバージョンまたは互換性のないプラットフォームのコントローラに交換した場合、新しいノードの起動後に自動化処理が停止し、エラーが報告されます。クラスタを正常な状態に戻すには、手動リカバリ手順に従ってください。

「 system controller replace start 」コマンドで、次の事前確認エラーが報告されることがあります。

```
Cluster-A::*>system controller replace show
Node         Status          Error-Action
------------ --------------- -------------------------------------
Node-A-1     Failed          MetroCluster check failed. Reason : MCC check
showed errors in component aggregates
```

アグリゲートのミラーされていないか、別のアグリゲート問題が原因で、このエラーが発生していないかどうかを確認してくださいすべてのミラーアグリゲートが正常で、デグレードまたはミラーデグレードでないことを確認します。このエラーの原因がミラーされていないアグリゲートのみである場合は、「 system controller replace start 」コマンドで「 -skip-metrocluster-check true 」オプションを選択することで、このエラーを無視できます。リモートストレージにアクセスできる場合、ミラーされていないアグリゲートはスイッチオーバー後にオンラインになります。リモートストレージリンクに障害が発生すると、ミラーされていないアグリゲートがオンラインになりません。

2. サイト B にログインし、「 system controller replace show 」または「 system controller replace show -details 」コマンドのコンソールメッセージに表示されるコマンドに従って、設定情報を手動で収集します。

アップグレード前に情報を収集

アップグレードの実行前にルートボリュームが暗号化されている場合は、暗号化された古いルートボリュームを含む新しいコントローラをブートするために、バックアップキーとその他の情報を収集する必要があります。

このタスクについて

このタスクは、既存のMetroCluster IP設定で実行します。

手順

1. 既存のコントローラのケーブルにラベルを付けておくと、新しいコントローラをセットアップするときに識別しやすくなります。
2. バックアップキーやその他の情報を取得するコマンドを表示します。

   「 system controller replace show 」と表示されます

   パートナークラスタから 'how コマンドの下に一覧表示されているコマンドを実行します

   。 `show` コマンド出力には、MetroCluster インターフェイスIP、システムID、およびシステムUUIDを含む3つのテーブルが表示されます。この情報は、手順 の後半の工程で新しいノードのブート時にbootargを設定する際に必要になります。

3. MetroCluster 構成内のノードのシステム ID を収集します。

   MetroCluster node show -fields node-systemid 、 dr-partner-systemid'

   手順のアップグレード時に、これらの古いシステムIDを新しいコントローラモジュールのシステムIDに置き換えます。

   この4ノードMetroCluster IP構成の例では、次の古いシステムIDが取得されます。

   - node_A_1 - 古い： 4068741258
   - node_A_2 - 古い： 4068741260
   - node_B_1 - 古い： 4068741254
   - node_B_2 - 古い： 4068741256

```
metrocluster-siteA::> metrocluster node show -fields node-systemid,ha-
partner-systemid,dr-partner-systemid,dr-auxiliary-systemid
dr-group-id        cluster           node            node-systemid
ha-partner-systemid     dr-partner-systemid    dr-auxiliary-systemid
-----------        ---------------   ----------      -------------
-------------------     -------------------    ---------------------
1                    Cluster_A       Node_A_1-old    4068741258
4068741260              4068741256             4068741256
1                    Cluster_A       Node_A_2-old    4068741260
4068741258              4068741254             4068741254
1                    Cluster_B       Node_B_1-old    4068741254
4068741256              4068741258             4068741260
1                    Cluster_B       Node_B_2-old    4068741256
4068741254              4068741260             4068741258
4 entries were displayed.
```

   この2ノードMetroCluster IP構成の例では、次の古いシステムIDが取得されます。

   - node_A_1 ： 4068741258
   - node_B_1 ： 4068741254

```
metrocluster node show -fields node-systemid,dr-partner-systemid

dr-group-id cluster    node          node-systemid dr-partner-systemid
----------- ---------- --------      ------------- ------------
1           Cluster_A  Node_A_1-old  4068741258    4068741254
1           Cluster_B  node_B_1-old  -             -
2 entries were displayed.
```

4. 古い各ノードのポートとLIFの情報を収集します。

   ノードごとに次のコマンドの出力を収集する必要があります。

   - 'network interface show -role cluster, node-mgmt
   - `network port show -node <node-name> -type physical`
   - `network port vlan show -node <node-name>`
   - `network port ifgrp show -node <node-name> -instance`
   - 「 network port broadcast-domain show 」
   - 「 network port reachability show-detail` 」と表示されます
   - network ipspace show
   - volume show
   - 「 storage aggregate show
   - `system node run -node <node-name> sysconfig -a`
   - `aggr show -r`
   - 「ディスクショー」
   - `system node run <node-name> disk show`
   - `vol show -fields type`
   - `vol show -fields type , space-guarantee`
   - 「 vserver fcp initiator show 」のように表示されます
   - 「 storage disk show 」を参照してください
   - 「 MetroCluster configurion-settings interface show 」を参照してください
5. MetroCluster ノードが SAN 構成になっている場合は、関連情報を収集します。

   次のコマンドの出力を収集する必要があります。

   - 「 fcp adapter show -instance 」のように表示されます
   - 「 fcp interface show -instance 」の略
   - 「 iscsi interface show 」と表示されます
   - ucadmin show

6. ルートボリュームが暗号化されている場合は、 key-manager に使用するパスフレーズを収集して保存します。

   「 securitykey-manager backup show 」を参照してください

7. MetroCluster ノードがボリュームまたはアグリゲートに暗号化を使用している場合は、キーとパスフレーズに関する情報をコピーします。

   詳細については、を参照してください "オンボードキー管理情報の手動でのバックアップ"。

   a. オンボードキーマネージャが設定されている場合：

      「 securitykey manager onboard show-backup 」を参照してください

      パスフレーズは、あとでアップグレード手順で必要になります。

   b. Enterprise Key Management （ KMIP ）が設定されている場合は、次のコマンドを問題で実行します。

      「 securitykey-manager external show -instance 」

   「セキュリティキーマネージャのキークエリ」

8. 設定情報の収集が完了したら、処理を再開します。

   「システムコントローラの交換が再開」

Tiebreakerまたはその他の監視ソフトウェアから既存の構成を削除する

アップグレードを開始する前に、Tiebreakerまたはその他の監視ソフトウェアから既存の設定を削除してください。

スイッチオーバーを開始できる MetroCluster Tiebreaker 構成またはその他のサードパーティアプリケーション（たとえば、 ClusterLion ）で既存の構成を監視している場合は、古いコントローラを交換する前に、 Tiebreaker またはその他のソフトウェアから MetroCluster 構成を削除する必要があります。

手順

1. "既存の MetroCluster 設定を削除します" Tiebreaker ソフトウェアから。
2. スイッチオーバーを開始できるサードパーティ製アプリケーションから既存の MetroCluster 構成を削除します。

   アプリケーションのマニュアルを参照してください。

次の手順

"古いコントローラのネットワーク構成を準備"です。

コントローラのアップグレード

情報を収集して処理を再開すると、自動化処理がスイッチオーバーに進みます。

作業を開始する前に

スイッチオーバーを開始する前に自動化処理が一時停止するため、サイト B のすべての LIF が「稼働」していることを手動で確認できます必要に応じて 'down' の LIF を up にし 'system controller replace resume' コマンドを使用して自動化処理を再開します

自動化処理によってスイッチオーバー処理が開始されます。これらの処理が完了すると、処理は* paused for user intervention *で一時停止します。これにより、コントローラをラックに設置し、パートナーコントローラをブートし、先ほど収集したを使用してフラッシュバックアップからルートアグリゲートディスクを新しいコントローラモジュールに再割り当てできます `sysids`。

このタスクについて

- このタスクは、古いノードごとに実行する必要があります。
- で収集した情報を使用します"アップグレード前に情報を収集"。

手順

1. 古いノードをブートし、ノードにログインします。

   「 boot_ontap 」

2. アップグレードするシステムで*共有クラスタ/ HAポート*を使用している場合は、MetroCluster IPインターフェイスでサポートされているIPアドレスが使用されていることを確認します。

   次の情報を使用して、新しいシステムで共有クラスタ/ HAポートが使用されているかどうかを確認します。

共有クラスタ/ **HA**ポート

次の表に示すシステムは、共有クラスタ/ HAポートを使用します。

AFFおよび**ASA**システム	**FAS**システム
• AFF A20用 • AFF A30用 • AFF C30 • AFF A50用 • AFF C60 • AFF C80用 • AFF A70用 • AFF A90用 • AFF A1K用	• FAS50 • FAS70 • FAS90

共有**MetroCluster / HA**ポート

次の表に示すシステムは、共有MetroCluster / HAポートを使用します。

AFFおよび**ASA**システム	**FAS**システム
• AFF A150、ASA A150向け • AFF A220 • AFF C250、ASA C250向け • AFF A250、ASA A250向け • AFF A300 • AFF A320 • AFF C400、ASA C400向け • AFF A400、ASA A400向け • AFF A700 • AFF C800、ASA C800向け • AFF A800、ASA A800向け • AFF A900、ASA A900向け	• FAS2750 • FAS500f • FAS8200 • FAS8300 • FAS8700 の場合 • FAS9000 • FAS9500

a. 古いコントローラのMetroClusterインターフェイスのIPアドレスを確認します。

「 MetroCluster configurion-settings interface show 」を参照してください

b. MetroClusterインターフェイスで169.254.17.xまたは169.254.18.xのIPアドレスが使用されている場合は、アップグレードを開始する前に、を参照し"記事「MetroCluster IPインターフェイスのプロパティ

を変更する方法」"てインターフェイスのIPアドレスを変更してください。

> MetroClusterインターフェイスに169.254.17.xまたは169.254.18.xのIPアドレスが設定されている場合、*共有クラスタ/ HAポート*を使用するシステムへのアップグレードはサポートされません。

3. 古いコントローラのクラスタ間LIFを変更して、HAインターコネクトまたはMetroCluster IP DRインターコネクトに使用するポートとは別のホームポートを新しいコントローラで使用するようにします。

> この手順は、アップグレードを成功させるために必要です。

古いコントローラのクラスタ間LIFでは、新しいコントローラのHAインターコネクトまたはMetroCluster IP DRインターコネクトに使用されるポートとは別のホームポートを使用する必要があります。たとえば、AFF A90コントローラにアップグレードすると、HAインターコネクトポートはe1aとe7aになり、MetroCluster IP DRインターコネクトポートはe2bとe3bになります。古いコントローラのインタークラスタLIFがポートe1a、e7a、e2b、またはe3bでホストされている場合は、クラスタ間LIFを移動する必要があります。

新しいノードでのポートの分散と割り当てについては、を参照して "Hardware Universe"ください。

a. 古いコントローラで、クラスタ間LIFを表示します。

```
network interface show -role intercluster
```

古いコントローラのクラスタ間LIFが、HAインターコネクトに使用するポートと同じポートを使用するか、新しいコントローラのMetroCluster IP DRインターコネクトに使用するポートと同じポートを使用するかに応じて、次のいずれかの処理を実行します。

クラスタ間**LIF**の状況	手順
同じホームポートを使用する	サブステップb
別のホームポートを使用する	手順 4

b. 別のホームポートを使用するようにクラスタ間LIFを変更します。

```
network interface modify -vserver <vserver> -lif <intercluster_lif> -home
-port <port-not-used-for-ha-interconnect-or-mcc-ip-dr-interconnect-on-new-
nodes>
```

c. すべてのインタークラスタLIFが新しいホームポートにあることを確認します。

```
network interface show -role intercluster -is-home false
```

すべてのクラスタ間LIFがそれぞれのホームポートにある場合は、コマンド出力が空になります。

d. ホームポートにないLIFをリバートします。

```
network interface revert -lif <intercluster_lif>
```

ホームポートにないインタークラスタLIFごとにコマンドを繰り返します。

4. 古いコントローラのすべてのデータLIFのホームポートを、新旧両方のコントローラモジュールで同じ共通のポートに割り当てます。

> 新旧のコントローラに共通のポートがない場合は、データLIFを変更する必要はありません。この手順を省略して、に直接進みます手順 5。

a. LIF を表示します。

「 network interface show 」を参照してください

SANとNASを含むすべてのデータLIFはスイッチオーバーサイト（cluster_A）で稼働しているため、管理者は「up」、運用上は「down」になります。

b. の出力を確認して、クラスタポートとして使用されていない新旧両方のコントローラで同じ共通の物理ネットワークポートを特定します。

たとえば、「 e0d 」は古いコントローラ上の物理ポートであり、新しいコントローラ上にも存在します。「 e0d 」は、クラスタポートとしても、新しいコントローラ上でも使用されません。

各プラットフォームモデルのポートの用途については、を参照してください"Hardware Universe"。

c. すべてのデータ LIF で共通ポートをホームポートとして使用するように変更します。

```
network interface modify -vserver <svm-name> -lif <data-lif> -home-port
<port-id>
```

次の例では、これは「 e0d 」です。

例：

```
network interface modify -vserver vs0 -lif datalif1 -home-port e0d
```

5. ブロードキャストドメインを変更して、削除が必要なVLANと物理ポートを削除します。

```
broadcast-domain remove-ports -broadcast-domain <broadcast-domain-name>-ports
<node-name:port-id>
```

すべての VLAN ポートと物理ポートについて、この手順を繰り返します。

6. クラスタポートをメンバーポートとして使用し、インターフェイスグループをメンバーポートとして使用している VLAN ポートをすべて削除します。

a. VLAN ポートを削除します。

```
network port vlan delete -node <node-name> -vlan-name <portid-vlandid>
```

例：

```
network port vlan delete -node node1 -vlan-name e1c-80
```

b. インターフェイスグループから物理ポートを削除します。

```
network port ifgrp remove-port -node <node-name> -ifgrp <interface-group-name> -port <portid>
```

例：

```
network port ifgrp remove-port -node node1 -ifgrp a1a -port e0d
```

a. ブロードキャストドメインからVLANポートとインターフェイスグループポートを削除します。

```
network port broadcast-domain remove-ports -ipspace <ipspace> -broadcast-domain <broadcast-domain-name>-ports <nodename:portname,nodename:portname>,..
```

b. 必要に応じて、インターフェイスグループポートを変更して他の物理ポートをメンバーとして使用します。

```
ifgrp add-port -node <node-name> -ifgrp <interface-group-name> -port <port-id>
```

7. ノードを停止します。

```
halt -inhibit-takeover true -node <node-name>
```

この手順は両方のノードで実行する必要があります。

8. ノードがプロンプトに表示されていることを確認し `LOADER`、現在の環境変数を収集して保持します。
9. bootarg の値を収集します。

printenv

10. コントローラをアップグレードするサイトでノードとシェルフの電源をオフにします。

次の手順

"新しいコントローラをセットアップしてネットブートする"です。

新しい**MetroCluster IP**コントローラのセットアップとネットブート

コントローラをネットブートする前に新しいコントローラをセットアップして、新しいノードで元のノードと同じバージョンのONTAPが実行されていることを確認します。

新しいコントローラをセットアップ

新しいコントローラをラックに設置してケーブルを接続する必要があります。

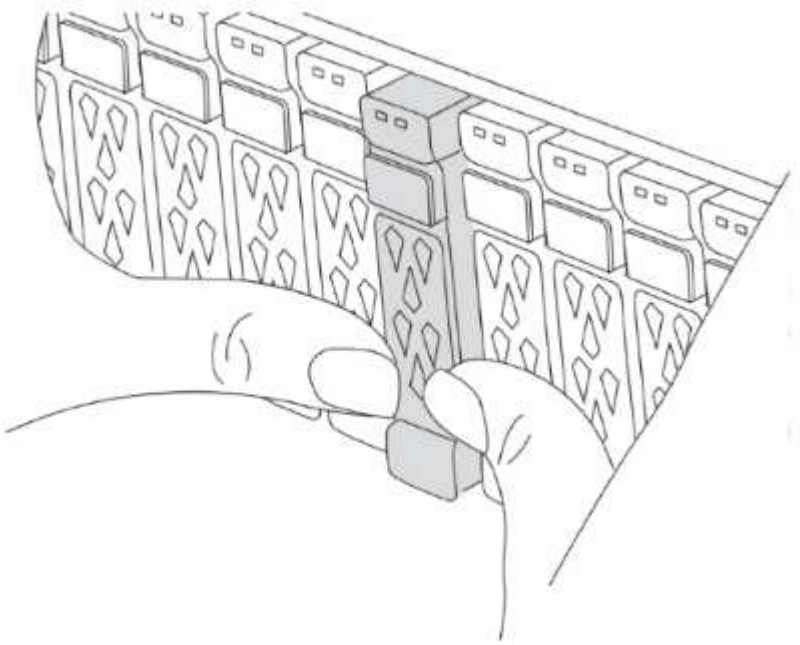
手順

1. 必要に応じて、新しいコントローラモジュールとストレージシェルフ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、構成内のストレージシェルフ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. AFF A800からAFF A90システムへのアップグレードやAFF C800からAFF C80システムへのアップグレードなど、コントローラモジュールの交換が必要なアップグレードの場合は、コントローラモジュールを交換するときにコントローラモジュールをシャーシから取り外す必要があります。その他のすべてのアップグレードの場合は、に進みます 手順 4。

   シャーシの前面で、プラスのストッパーになるまで、親指で各ドライブをしっかりと押し込みます。ドライブがシャーシのミッドプレーンにしっかりと装着されていることを確認します。



4. コントローラモジュールを設置します。

   インストール手順は、アップグレードでコントローラモジュールの交換が必要かどうか、または古いコントローラを外付けシェルフに変換するためにIOMモジュールが必要かどうかによって異なります。

アップグレード対象	実行する手順
• AFF A150からAFF A20システムへ • AFF A220からAFF A20システムへ	コントローラから外付けシェルフへの変換
• AFF A800からAFF A90システムへ • AFF C800からAFF C80システムへ • AFF A250からAFF A30システムへ • AFF C250からAFF C30システムへ • AFF A70からAFF A90システムへ	コントローラ モジュールの交換
その他のコントローラのアップグレードの組み合わせ	その他すべてのアップグレード

コントローラから外付けシェルフへの変換

元のMetroCluster IPコントローラがAFF A150モデルまたはAFF A220モデルの場合は、AFF A150またはAFF A220のHAペアをDS224Cドライブシェルフに変換して、新しいノードに接続できます。

たとえば、AFF A150またはAFF A220システムからAFF A20システムにアップグレードする場合、AFF A150またはAFF A220のコントローラモジュールをIOM12モジュールと交換することで、AFF A150またはAFF A220のHAペアをDS224Cシェルフに変換できます。

手順

a. IOM12シェルフモジュールで変換するノードのコントローラモジュールを交換します。

   "Hardware Universe"

b. ドライブシェルフ ID を設定します。

   シャーシを含む各ドライブシェルフには、一意の ID が必要です。

c. 必要に応じて、他のドライブシェルフ ID をリセットします。

d. シェルフの電源をオフにします。

e. 変換したドライブシェルフを新しいシステムの SAS ポートに接続し、アウトオブバンド ACP ケーブルを使用している場合は新しいノードの ACP ポートに接続します。

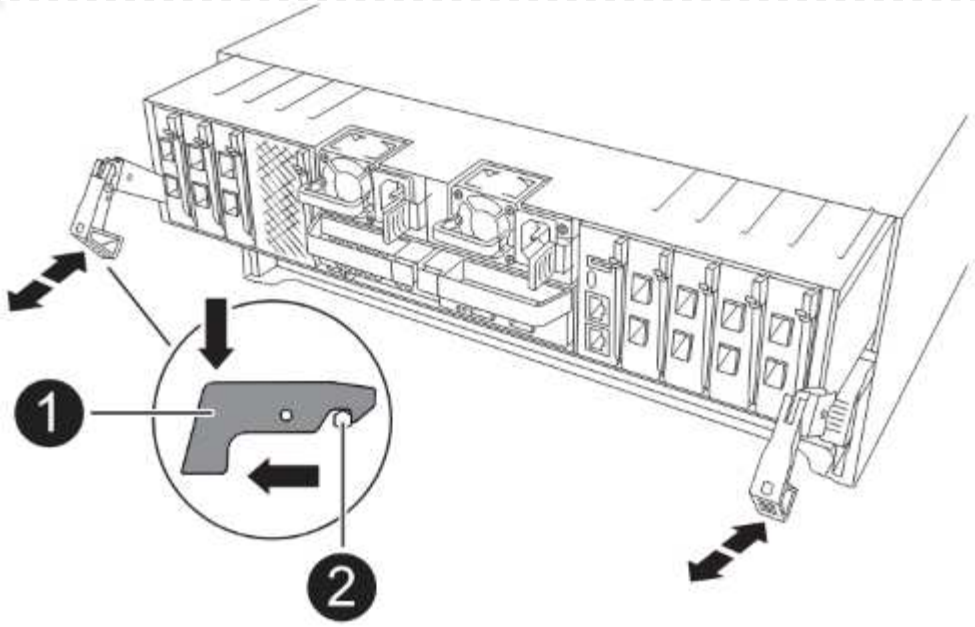
f. 変換したドライブシェルフおよび新しいノードに接続されているその他のドライブシェルフの電源をオンにします。

g. 新しいノードの電源をオンにしてから、各ノードで Ctrl+C キーを押してブートプロセスを中断し、ブート環境プロンプトにアクセスします。

コントローラ モジュールの交換

ディスクとコントローラを同じシャーシに搭載した統合システム（AFF A800システムからAFF A90システムなど）をアップグレードする場合、新しいコントローラを別 々 に設置することはできません。古いコントローラの電源をオフにしたあと、次の図に示すように、新しいコントローラモジュールとI/Oカードを交換する必要があります。

次の図の例は表示用です。コントローラモジュールとI/Oカードはシステムによって異なります。



その他すべてのアップグレード

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。

5. の説明に従って、コントローラの電源、シリアルコンソール、および管理接続をケーブル接続します。 "MetroCluster IP スイッチをケーブル接続します"

   この時点で古いコントローラから切断されていた他のケーブルは接続しないでください。

   "ONTAPハードウェアシステムのドキュメント"

6. 新しいノードの電源をオンにし、プロンプトが表示されたらCtrl+Cキーを押してプロンプトを表示し `LOADER` ます。

新しいコントローラをネットブート

新しいノードを設置したら、ネットブートを実行して、新しいノードが元のノードと同じバージョンの ONTAP を実行するようにする必要があります。ネットブートという用語は、リモート・サーバに保存された ONTAP イメージからブートすることを意味します。ネットブートの準備を行うときは、システムがアクセスできる Web サーバに、 ONTAP 9 ブート・イメージのコピーを配置する必要があります。

このタスクは、新しい各コントローラモジュールで実行します。

手順

1. にアクセスします "ネットアップサポートサイト" システムのネットブートの実行に使用するファイルをダウンロードするには、次の手順を実行します。
2. ネットアップサポートサイトのソフトウェアダウンロードセクションから適切な ONTAP ソフトウェアをダウンロードし、「 ONTAP-version _image.tgz 」ファイルを Web にアクセスできるディレクトリに保存します。
3. Web にアクセスできるディレクトリに移動し、必要なファイルが利用可能であることを確認します。

   ディレクトリの一覧にカーネルファイルを含むネットブートフォルダが表示されます。 `ontap-`

version_image.tgz

ファイルを展開する必要はありません ontap-version_image.tgz。

4. `LOADER`プロンプトで、管理LIFのネットブート接続を設定します。
   - IP アドレスが DHCP の場合は、自動接続を設定します。

     ifconfig e0M -auto

   - IP アドレスが静的な場合は、手動接続を設定します。

     ifconfig e0M -addr= ip_addr-mask= netmask `-gw= gateway `

5. ネットブートを実行します。

   netboot\http://web_server_ip/path_to_web-accessible_directory/ontap-version_image.tgz`

6. ブートメニューからオプション * （７） Install new software first * を選択し、新しいソフトウェアイメージをダウンロードしてブートデバイスにインストールします。

```
 Disregard the following message: "This procedure is not supported for
Non-Disruptive Upgrade on an HA pair". It applies to nondisruptive
upgrades of software, not to upgrades of controllers.
```

. 手順を続行するかどうかを確認するメッセージが表示されたら、「 y 」と入力し、パッケージの入力を求められたらイメージファイルの URL 「 ¥ http://web_server_ip/path_to_web-accessible_directory/ontap-version_image.tgz` 」を入力します

```
Enter username/password if applicable, or press Enter to continue.
```

7. 入力 n 次のようなプロンプトが表示されたら、バックアップの回復をスキップします。

```
Do you want to restore the backup configuration now? {y|n} n
```

8. 次のようなプロンプトが表示されたら 'y' と入力して再起動します

```
The node must be rebooted to start using the newly installed software.
Do you want to reboot now? {y|n} y
```

新しくインストールされたソフトウェアを使用するには、ノードを再起動する必要があります。

コントローラモジュールの設定をクリアします

MetroCluster 構成で新しいコントローラモジュールを使用する前に、既存の構成をクリアする必要があります。

手順

1. 必要に応じて、ノードを停止してプロンプトを表示し `LOADER`ます。

   「 halt 」

2. `LOADER`プロンプトで、環境変数をデフォルト値に設定します。

   「デフォルト設定」

3. 環境を保存します。

   'aveenv

4. `LOADER`プロンプトでブートメニューを起動します。

   「 boot_ontap menu

5. ブートメニューのプロンプトで、設定を消去します。

   wipeconfig

   確認プロンプトに「 yes 」と応答します。

   ノードがリブートし、もう一度ブートメニューが表示されます。

6. ブートメニューでオプション * 5 * を選択し、システムをメンテナンスモードでブートします。

   確認プロンプトに「 yes 」と応答します。

次の手順

"HBA構成をリストアしてHAの状態を設定"です。

HBA構成をリストアし、**MetroCluster IP**コントローラとシャーシの**HA**状態を設定

コントローラモジュールでHBAカードを設定し、コントローラとシャーシのHAの状態を確認および設定します。

HBA 構成をリストア

コントローラモジュールでのHBAカードの有無と設定に応じて、サイトに合わせてHBAカードを正しく設定する必要があります。

手順

1. メンテナンスモードで、システムのHBAを設定します。

   a. ucadmin show と入力し、各ポートの現在の設定を確認します

b. 必要に応じてポートの設定を更新します。

HBA のタイプと目的のモード	使用するコマンド
CNA FC	`ucadmin modify -m fc -t initiator <adapter-name>`
CNA イーサネット	`ucadmin modify -mode cna <adapter-name>`
FC ターゲット	`fcadmin config -t target <adapter-name>`
FC イニシエータ	`fcadmin config -t initiator <adapter-name>`

2. メンテナンスモードを終了します。

「 halt 」

コマンドの実行後、ノードがプロンプトで停止するまで待ちます `LOADER` 。

3. ノードをブートしてメンテナンスモードに戻り、設定の変更を適用します。

「 boot_ontap maint 」を使用してください

4. 変更を確認します。

HBA のタイプ	使用するコマンド
CNA	ucadmin show
FC	fcadmin show`

新しいコントローラとシャーシで **HA** 状態を設定

コントローラとシャーシの HA 状態を確認し、必要に応じてシステム構成に合わせて更新する必要があります。

手順

1. メンテナンスモードで、コントローラモジュールとシャーシの HA 状態を表示します。

「 ha-config show 」

すべてのコンポーネントの HA 状態は「 mccip 」である必要があります。

2. 表示されたコントローラまたはシャーシのシステム状態が正しくない場合は、 HA 状態を設定します。

「 ha-config modify controller mccip 」を参照してください

「 ha-config modify chassis mccip 」を参照してください

3. NS224シェルフまたはストレージスイッチに接続されているイーサネットポートを確認および変更します。

   a. NS224シェルフまたはストレージスイッチに接続されているイーサネットポートを確認します。

      ```
      storage port show
      ```

   b. イーサネットシェルフまたはストレージスイッチに接続されているすべてのイーサネットポート（ストレージとクラスタの共有スイッチを含む）をモードに設定し `storage` ます。

      ```
      storage port modify -p <port> -m storage
      ```

      例：

      ```
      *> storage port modify -p e5b -m storage
      Changing NVMe-oF port e5b to storage mode
      ```

      アップグレードを成功させるには、影響を受けるすべてのポートでこの値を設定する必要があります。

      イーサネットポートに接続されているシェルフのディスクが出力に報告され `sysconfig -v` ます。

   アップグレード先のシステムのストレージポートについては、を参照して "Hardware Universe" ください。

   a. モードが設定されていることを確認し `storage` 、ポートがonline状態であることを確認します。

      ```
      storage port show
      ```

4. ノードを停止します

   ノードは 'loader>` プロンプトで停止する必要があります

5. 各ノードで、システムの日付、時刻、およびタイムゾーンを確認します。「 show date 」
6. 必要に応じて 'UTC または GMT:'set date <mm/dd/yyyy>' で日付を設定します
7. ブート環境プロンプトで次のコマンドを使用して ' 時刻を確認します
8. 必要に応じて、時刻を UTC または GMT:' 設定時刻 <:hh:mm:ss>` で設定します
9. 設定を保存します： saveenv
10. 環境変数 :printenv' を収集します

新しいコントローラのシャーシから内部ドライブを取り外します

外部ドライブのみを備えたシステムから外部ドライブと内部ドライブ (同じシャーシ内のディスクとコントローラ) を備えたシステムにアップグレードする場合は、アップグレードが完了するまで、新しいシステムからすべての内部ドライブを取り外すか、取り外す必要があります。

このタスクは、影響を受けるシステムでコントローラーを正常にアップグレードするために必須です。

、新しいシステムから内部ドライブを取り外す必要があります。

このタスクを完了すると、内部ドライブにアクセスできなくなります。手順の後半で、新しいコントローラにドライブを追加します。

次の手順

"スイッチのRCFファイルを更新し、MetroCluster IPのbootarg値を設定する"です。

スイッチの**RCF**を更新し、**MetroCluster IP**の**bootarg**値を設定

新しいプラットフォーム用のスイッチリファレンス構成ファイル（RCF）を更新し、コントローラモジュールでMetroCluster IP bootargの値を設定します。

新しいプラットフォームに合わせてスイッチの**RCF**を更新

スイッチは、新しいプラットフォームモデルをサポートする構成に更新する必要があります。

このタスクについて

このタスクは、現在アップグレード中のコントローラを含むサイトで実行します。この手順の例では、まず site_B をアップグレードします。

site_A のコントローラをアップグレードすると、 site_A のスイッチがアップグレードされます。

手順

1. IPスイッチで新しいRCFを適用できるように準備します。

   スイッチベンダーに対応するセクションを参照してください。

   - "Broadcom IP スイッチを工場出荷時のデフォルトにリセットします"
   - "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"
   - "NVIDIA IP SN2100スイッチを工場出荷時のデフォルトにリセット"

2. RCFをダウンロードしてインストールします。

   スイッチベンダーに対応するセクションを参照してください。

   - "Broadcom RCFのダウンロードとインストール"
   - "Cisco IP RCFのダウンロードとインストール"
   - "NVIDIA IP RCFのダウンロードとインストール"

MetroCluster の **bootarg IP** 変数を設定します

新しいコントローラモジュールには特定の MetroCluster IP bootarg 値を設定する必要があります。これらの値は、古いコントローラモジュールに設定されている値と一致する必要があります。

このタスクについて

- のアップグレード手順で前述したUUIDとシステムIDが必要です"アップグレード前に情報を収集"。
- プラットフォームモデルに応じて、パラメータを使用してVLAN IDを指定できます `-vlan-id`。次のプラットフォームでは、パラメータはサポートされません `-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、パラメータがサポートされ `-vlan-id` ます。
- 設定するMetroClusterのbootargの値は、新しいシステムで共有のクラスタ/ HAポートを使用するか、共有のMetroCluster / HAポートを使用するかによって異なります。

共有クラスタ/ **HA**ポート

次の表に示すシステムは、共有クラスタ/ HAポートを使用します。

AFFおよび**ASA**システム	**FAS**システム
• AFF A20用 • AFF A30用 • AFF C30 • AFF A50用 • AFF C60 • AFF C80用 • AFF A70用 • AFF A90用 • AFF A1K用	• FAS50 • FAS70 • FAS90

共有**MetroCluster / HA**ポート

次の表に示すシステムは、共有MetroCluster / HAポートを使用します。

AFFおよび**ASA**システム	**FAS**システム
• AFF A150、ASA A150向け • AFF A220 • AFF C250、ASA C250向け • AFF A250、ASA A250向け • AFF A300 • AFF A320 • AFF C400、ASA C400向け • AFF A400、ASA A400向け • AFF A700 • AFF C800、ASA C800向け • AFF A800、ASA A800向け • AFF A900、ASA A900向け	• FAS2750 • FAS500f • FAS8200 • FAS8300 • FAS8700 の場合 • FAS9000 • FAS9500

手順

1. 「 LOADER> 」プロンプトで、 site_B の新しいノードで次のブート引数を設定します。

   実行する手順は、新しいプラットフォームモデルで使用するポートによって異なります。

共有クラスタ/ **HA**ポートを使用するシステム

a. 次のbootargを設定します。

```
setenv bootarg.mcc.port_a_ip_config <local-IP-address/local-IP-
mask,0,0,DR-partner-IP-address,DR-aux-partnerIP-address,vlan-id>

setenv bootarg.mcc.port_b_ip_config <local-IP-address/local-IP-
mask,0,0,DR-partner-IP-address,DR-aux-partnerIP-address,vlan-id>
```

インターフェイスがデフォルトのVLAN IDを使用している場合、 `vlan-id`パラメータは必要ありません。

次の例は、1つ目のネットワークにVLAN 120、2つ目のネットワークにVLAN 130を使用して、node_B_1-newの値を設定します。

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,0,172.17.26.13,172.17.26.12,120
setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,0,172.17.27.13,172.17.27.12,130
```

次の例は、1つ目のネットワークにVLAN 120、2つ目のネットワークにVLAN 130を使用して、node_B_2-newの値を設定します。

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.11/23,0,0,172.17.26.12,172.17.26.13,120
setenv bootarg.mcc.port_b_ip_config
172.17.27.11/23,0,0,172.17.27.12,172.17.27.13,130
```

次の例は、すべてのMetroCluster IP DR接続にデフォルトのVLANを使用してnode_B_1-newの値を設定します。

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,0,172.17.26.13,172.17.26.12
setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,0,172.17.27.13,172.17.27.12
```

次の例は、すべてのMetroCluster IP DR接続にデフォルトのVLANを使用してnode_B_2-newの値を設定します。

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.11/23,0,0,172.17.26.12,172.17.26.13
setenv bootarg.mcc.port_b_ip_config
172.17.27.11/23,0,0,172.17.27.12,172.17.27.13
```

共有**MetroCluster / HA**ポートを使用するシステム

a. 次のbootargを設定します。

```
setenv bootarg.mcc.port_a_ip_config <local-IP-address/local-IP-
mask,0,HA-partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-
address,vlan-id>

setenv bootarg.mcc.port_b_ip_config <local-IP-address/local-IP-
mask,0,HA-partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-
address,vlan-id>
```



インターフェイスがデフォルトのVLAN IDを使用している場合、 `vlan-id`パラメータは必要ありません。

次の例は、1つ目のネットワークにVLAN 120、2つ目のネットワークにVLAN 130を使用して、node_B_1-newの値を設定します。

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12,120
setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12,130
```

次の例は、1つ目のネットワークにVLAN 120、2つ目のネットワークにVLAN 130を使用して、node_B_2-newの値を設定します。

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.11/23,0,172.17.26.10,172.17.26.12,172.17.26.13,120
setenv bootarg.mcc.port_b_ip_config
172.17.27.11/23,0,172.17.27.10,172.17.27.12,172.17.27.13,130
```

次の例は、すべてのMetroCluster IP DR接続にデフォルトのVLANを使用してnode_B_1-newの値を設定します。

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12
setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12
```

次の例は、すべてのMetroCluster IP DR接続にデフォルトのVLANを使用してnode_B_2-newの値を設定します。

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.11/23,0,172.17.26.10,172.17.26.12,172.17.26.13
setenv bootarg.mcc.port_b_ip_config
172.17.27.11/23,0,172.17.27.10,172.17.27.12,172.17.27.13
```

2. 新しいノードの LOADER プロンプトで、 UUID を設定します。

```
setenv bootarg.mgwd.partner_cluster_uuid <partner-cluster-UUID>

setenv bootarg.mgwd.cluster_uuid <local-cluster-UUID>

setenv bootarg.mcc.pri_partner_uuid <DR-partner-node-UUID>

setenv bootarg.mcc.aux_partner_uuid <DR-aux-partner-node-UUID>

setenv bootarg.mcc_iscsi.node_uuid <local-node-UUID>
```

a. node_B_1 で UUID を設定します。

次の例は、 node_B_1 で新規の UUID を設定するコマンドを示しています。

```
setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039
setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.pri_partner_uuid f37b240b-9ac1-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.aux_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-
00a098ca379f
setenv bootarg.mcc_iscsi.node_uuid f03cb63c-9a7e-11e7-b68b-
00a098908039
```

b. node_B_2 の UUID を設定します。 new ：

次の例は、 node_B_2 の UUID を設定するコマンドを示しています。

```
setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039
setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.pri_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
setenv bootarg.mcc.aux_partner_uuid f37b240b-9ac1-11e7-9b42-00a098c9e55d
setenv bootarg.mcc_iscsi.node_uuid aa9a7a7a-9a81-11e7-a4e9-00a098908c35
```

3. 稼働しているサイトで次のコマンドを実行して、元のシステムがアドバンストドライブパーティショニング（ADP）用に設定されているかどうかを確認します。

   「ディスクショー」

   ADPが設定されている場合、出力に「container type」列に「shared」と表示されます `disk show` 。「container type」にそれ以外の値が指定されている場合、ADPはシステムで設定されていません。次の出力例は、ADPが設定されたシステムを示しています。

```
::> 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".
----------------    ---------- ----- --- ------- ----------- ---------
--------
1.11.0              894.0GB    11    0   SSD      shared     testaggr
node_A_1
1.11.1              894.0GB    11    1   SSD      shared     testaggr
node_A_1
1.11.2              894.0GB    11    2   SSD      shared     testaggr
node_A_1
```

4. 元のシステムでADP用にパーティショニングされたディスクが設定されていた場合は、各交換用ノードのプロンプトで有効にし `LOADER` ます。

   'etenv bootarg.me.adp_enabled true

5. 次の変数を設定します。

```
setenv bootarg.mcc.local_config_id <original-sys-id>

setenv bootarg.mcc.dr_partner <dr-partner-sys-id>
```

   「 bootarg env.MCC.local_config_id` 」変数は、 * 元の * コントローラモジュール node_B_1 の sys-id に設定する必要があります。

   a. node_B_1 で変数を設定します。

      次の例は、 node_B_1 で新規の値を設定するコマンドを示しています。

```
setenv bootarg.mcc.local_config_id 537403322
setenv bootarg.mcc.dr_partner 537403324
```

b. node_B_2 の変数を設定します。

次の例は、 node_B_2 の値を設定するコマンドを示しています。

```
setenv bootarg.mcc.local_config_id 537403321
setenv bootarg.mcc.dr_partner 537403323
```

6. 外部キー管理ツールで暗号化を使用する場合は、必要な bootargs を設定します。

「 etenv bootarg.kmip.init.ipaddr` 」を参照してください

「 etenv bootarg.kmip.kmip.init.netmask` 」を参照してください

「 etenv bootarg.kmip.kmip.init.gateway` 」を参照してください

「 etenv bootarg.kmip.kmip.init.interface` 」を参照してください

次の手順

"ルートアグリゲートディスクを再割り当て"です。

ルートアグリゲートディスクを新しい**MetroCluster IP**コントローラモジュールに再割り当て

前の手順で確認したシステムIDを使用して、ルートアグリゲートディスクを新しいコントローラモジュールに再割り当てします。

このタスクについて

このタスクはメンテナンスモードで実行します。

古いシステムIDはで特定しました "アップグレード前に情報を収集"。

この手順の例では、次のシステム ID を持つコントローラを使用します。

ノード	古いシステム ID	新しいシステム ID
node_B_1	4068741254	1574774970

手順

1. 他のすべての接続（FC-VI、ストレージ、クラスタインターコネクトなど）を新しいコントローラモジュールにケーブル接続します。
2. システムを停止して 'LOADER' プロンプトからメンテナンス・モードで起動します

「 boot_ontap maint 」を使用してください

3. node_B_1 古いが所有するディスクを表示します。

「ディスクショー - A` 」

コマンド出力には、新しいコントローラモジュールのシステムID（1574774970）が表示されます。ただ

し、ルートアグリゲートディスクの所有者は古いシステムID（4068741254）のままです。この例には、MetroCluster構成の他のノードが所有するドライブは表示されていません。

ディスクの再割り当てを続行する前に、ノードのルートアグリゲートに属するpool0とpool1のディスクが出力に表示されていることを確認し `disk show`ます。次の例では、node_B_1-oldが所有するpool0とpool1のディスクが出力に表示されています。

```
*> disk show -a
Local System ID: 1574774970

  DISK         OWNER                     POOL   SERIAL NUMBER    HOME
DR HOME
------------   -------------             -----  -------------
-------------             -------------
...
rr18:9.126L44 node_B_1-old(4068741254)   Pool1  PZHYN0MD
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:9.126L49 node_B_1-old(4068741254)   Pool1  PPG3J5HA
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L21 node_B_1-old(4068741254)   Pool1  PZHTDSZD
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L2  node_B_1-old(4068741254)   Pool0  S0M1J2CF
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L3  node_B_1-old(4068741254)   Pool0  S0M0CQM5
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:9.126L27 node_B_1-old(4068741254)   Pool0  S0M1PSDW
node_B_1-old(4068741254)  node_B_1-old(4068741254)
...
```

4. ドライブシェルフのルートアグリゲートディスクを新しいコントローラに再割り当てします。

```
disk reassign -s <old-sysid> -d <new-sysid>
```

MetroCluster IPシステムにアドバンストディスクパーティショニングが設定されている場合は、コマンドを実行してDRパートナーシステムIDを含める必要があります `disk reassign -s old-sysid -d new-sysid -r dr-partner-sysid`。

次の例は、ドライブの再割り当てを示しています。

```
*> disk reassign -s 4068741254 -d 1574774970
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)? n

After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)? Jul 14 19:23:49
[localhost:config.bridge.extra.port:error]: Both FC ports of FC-to-SAS
bridge rtp-fc02-41-rr18:9.126L0 S/N [FB7500N107692] are attached to this
controller.
y
Disk ownership will be updated on all disks previously belonging to
Filer with sysid 4068741254.
Do you want to continue (y/n)? y
```

5. すべてのディスクが想定どおりに再割り当てされていることを確認します。

   「ディスクショー」

```
*> disk show
Local System ID: 1574774970

  DISK         OWNER                      POOL   SERIAL NUMBER   HOME
DR HOME
------------  -------------              -----  -------------
-------------              -------------
rr18:8.126L18 node_B_1-new(1574774970)   Pool1  PZHYN0MD
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:9.126L49 node_B_1-new(1574774970)   Pool1  PPG3J5HA
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L21 node_B_1-new(1574774970)   Pool1  PZHTDSZD
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L2  node_B_1-new(1574774970)   Pool0  S0M1J2CF
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:9.126L29 node_B_1-new(1574774970)   Pool0  S0M0CQM5
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L1  node_B_1-new(1574774970)   Pool0  S0M1PSDW
node_B_1-new(1574774970)  node_B_1-new(1574774970)
*>
```

6. アグリゲートのステータスを表示します。

   「 aggr status 」を入力します

```
*> aggr status
           Aggr             State       Status            Options
aggr0_node_b_1-root         online      raid_dp, aggr     root, nosnap=on,
                            mirrored
mirror_resync_priority=high(fixed)
                            fast zeroed
                            64-bit
```

7. パートナーノードで上記の手順を繰り返します（ node_B_2 - 新規）。

次の手順

"新しいコントローラをブートしてLIF設定をリストア"です。

新しい**MetroCluster IP**コントローラのブートと**LIF**設定のリストア

コマンドを使用して新しいコントローラをブートし、LIFが適切なノードとポートでホストされていることを確認してから、処理を再開し `system controller replace resume`ます。

新しいコントローラのブート

新しいコントローラをブートし、bootarg変数が正しいことを確認し、必要に応じて暗号化のリカバリ手順を実行します。

このタスクについて

このタスクはすべての新しいコントローラで実行する必要があります。

手順

1. ノードを停止します。

   「 halt 」

2. 外部キー管理ツールが設定されている場合は、関連する bootargs を設定します。

```
setenv bootarg.kmip.init.ipaddr <ip-address>

setenv bootarg.kmip.init.netmask <netmask>

setenv bootarg.kmip.init.gateway <gateway-address>

setenv bootarg.kmip.init.interface <interface-id>
```

3. partner-sysid が正しいかどうかを確認します。

   printenv partner-sysid

partner-sysid が正しくない場合は、次のように設定します。

```
setenv partner-sysid <partner-sysID>
```

4. ブートメニューを表示します。

「 boot_ontap menu

5. ルート暗号化を使用する場合は、キー管理設定のブートメニューオプションを選択します。

使用するポート	選択するブートメニューオプション
オンボードキー管理	オプション "10 `" プロンプトに従って、キー管理ツールの構成をリカバリおよびリストアするために必要な入力を指定します。
外部キー管理	オプション "11`" プロンプトに従って、キー管理ツールの構成をリカバリおよびリストアするために必要な入力を指定します。

6. ブートメニューからオプション "6`" を実行します

オプション「6」は、プロセスが完了する前にノードを2回リブートします。

システムIDの変更プロンプトに「y」と入力します。2回目のリブートメッセージが表示されるまで待ちます。

```
Successfully restored env file from boot media...

Rebooting to load the restored env file...
```

オプション"`6`"の後のいずれかの再起動中に、確認プロンプトが表示されます `Override system ID? {y|n}` 表示されます。入力するコマンド `y`。

7. `LOADER`プロンプトで、bootargの値を確認し、必要に応じて値を更新します。

"MetroCluster の bootarg IP 変数を設定します"の手順を使用します。

8. partner-sysid が正しいことを確認します：

printenv partner-sysid

partner-sysid が正しくない場合は、次のように設定します。

```
setenv partner-sysid <partner-sysID>
```

9. ルート暗号化を使用する場合は、キー管理設定のブートメニューオプションを再度選択します。

使用するポート	選択するブートメニューオプション
オンボードキー管理	オプション "10 `" プロンプトに従って、キー管理ツールの構成をリカバリおよびリストアするために必要な入力を指定します。
外部キー管理	オプション "11`" プロンプトに従って、キー管理ツールの構成をリカバリおよびリストアするために必要な入力を指定します。

キー・マネージャの設定に応じて '10 またはオプション 11 を選択し ' 最初のブート・メニュー・プロンプトでオプション 6 を選択して 'recovery 手順を実行しますノードを完全にブートするには ' オプション "1" によって続行されるリカバリ手順 (通常のブート) を繰り返す必要がある場合があります

10. ノードをブートします。

「 boot_ontap 」

11. 交換したノードがブートするまで待ちます。

いずれかのノードがテイクオーバーモードの場合は、「 storage failover giveback 」コマンドを使用してギブバックを実行します。

12. すべてのポートがブロードキャストドメインに属していることを確認します。

a. ブロードキャストドメインを表示します。

「 network port broadcast-domain show 」

b. 新しくアップグレードしたコントローラのデータポート用に新しいブロードキャストドメインを作成する場合は、そのブロードキャストドメインを削除します。

> ⓘ 新しいブロードキャストドメインだけを削除します。アップグレードを開始する前に存在していたブロードキャストドメインは削除しないでください。

```
broadcast-domain delete -broadcast-domain <broadcast_domain_name>
```

c. 必要に応じて、ブロードキャストドメインにポートを追加します。

"ブロードキャストドメインのポートを追加または削除します"

d. インタークラスタLIFをホストする物理ポートを対応するブロードキャストドメインに追加します。

e. 新しい物理ポートをホームポートとして使用するようにクラスタ間 LIF を変更します。

f. クラスタ間 LIF が起動したら、クラスタピアのステータスを確認し、必要に応じてクラスタピアリン

グを再確立します。

クラスタピアリングの再設定が必要になる場合があります。

"クラスタピア関係を作成します。"

g. 必要に応じて、 VLAN とインターフェイスグループを再作成します。

VLAN およびインターフェイスグループのメンバーシップは、古いノードと異なる場合があります。

"VLANを作成します。"

"物理ポートを組み合わせてインターフェイスグループを作成"

a. パートナークラスタが到達可能であり、パートナークラスタで設定が再同期されたことを確認します。

```
metrocluster switchback -simulate true
```

13. 暗号化を使用する場合は、キー管理設定に対応したコマンドを使用してキーをリストアします。

使用するポート	使用するコマンド
オンボードキー管理	「セキュリティキーマネージャオンボード同期」 詳細については、を参照してください "オンボードキー管理暗号化キーのリストア"。
外部キー管理	`security key-manager external restore -vserver <svm-name> -node <node-name> -key-server <host_name

14. MetroClusterが正しく設定されていることを確認します。ノードのステータスを確認します。

MetroCluster node show

新しいノード（ site_B ）の状態が「 Waiting for switchback state * from site_A 」であることを確認します

LIF の設定を確認してリストア

自動スイッチバック処理を開始する前に、LIFが適切なノードでホストされていることを確認してください。

このタスクについて

- このタスクは site_B で実行します

> スイッチバックを実行する前に、新しいノードでデータLIFの場所が正しいことを確認する必要があります。構成をスイッチバックすると、ONTAPはLIFで使用されているホームポートでトラフィックの再開を試みます。スイッチポートおよびVLANへのホームポート接続が正しくないと、I/O障害が発生する可能性があります。

手順

1. スイッチバックの前に、LIFが適切なノードとポートでホストされていることを確認します。

   a. advanced 権限レベルに切り替えます。

      「 advanced 」の権限が必要です

   b. LIFを表示し、各データLIFが正しいホームポートを使用していることを確認します。

      「 network interface show 」を参照してください

   c. 正しいホームポートを使用していないLIFを変更します。

      ```
      network interface modify -vserver <svm-name> -lif <data-lif> -home-port
      <port-id>
      ```

      コマンドからエラーが返された場合は、ポート設定を上書きできます。

      ```
      vserver config override -command "network interface modify -vserver <svm-
      name> -home-port <active_port_after_upgrade> -lif <lif_name> -home-node
      <new_node_name>"
      ```

   vserver config override コマンドで network interface modify コマンドを入力した場合は、 tab autoccomplete 機能を使用することはできません。autoccomplete を使用してネットワーク 'interface modify' を作成してから 'vserver config override' コマンドで囲むことができます

   a. すべてのデータLIFが正しいホームポートにあることを確認します。

      「 network interface show 」を参照してください

   b. admin 権限レベルに戻ります。

      「特権管理者」

2. インターフェイスをホームノードにリバートします。

   ```
   network interface revert * -vserver <svm-name>
   ```

   必要に応じて、すべての SVM でこの手順を実行します。

3. 処理を再開します。

   「システムコントローラの交換が再開」

次の手順

"コントローラのアップグレードの完了"です。

MetroCluster IPコントローラのアップグレードの完了

ネットワークに到達できるかどうかを確認し、監視設定をリストアすることで、コントローラの自動アップグレードプロセスを完了します。

ネットワークの到達可能性の確認

自動処理では、検証システムのチェックが実行されたあと一時停止するため、ネットワークの到達可能性を確認できます。検証が完了すると、リソースの再取得フェーズが開始され、自動化処理によってサイト A でスイッチバックが実行され、アップグレード後のチェックで一時停止されます。自動処理を再開すると、アップグレード後のチェックが実行され、エラーが検出されない場合はアップグレードが完了としてマークされます。

手順

1. コンソールメッセージに従って、ネットワークの到達可能性を確認します。
2. 検証が完了したら、処理を再開します。

   「システムコントローラの交換が再開」

3. 自動化処理が実行されます `heal-aggregate`、 `heal-root-aggregate`、サイトAでのスイッチバック処理、およびアップグレード後のチェックが実行されます。処理が一時停止した場合は、コンソールメッセージに従って SAN LIF のステータスを手動で確認し、ネットワーク設定を確認します。
4. 検証が完了したら、処理を再開します。

   「システムコントローラの交換が再開」

5. アップグレード後チェックのステータスを確認します。

   「 system controller replace show 」と表示されます

   アップグレード後のチェックでエラーが報告されなかった場合、アップグレードは完了しています。

6. コントローラのアップグレードが完了したら、サイト B でログインし、交換したコントローラが正しく設定されていることを確認します。

cluster_Aのノードをアップグレードします。

アップグレード手順を繰り返して、サイトAのcluster_Aのノードをアップグレードする必要があります。

手順

1. cluster_Aのノードをアップグレードするために、上記の手順を繰り返し"アップグレードを準備"ます。

   手順を繰り返すと、クラスターとノードへのすべての例の参照が逆になります。

新しいコントローラに内部ドライブを再度追加します

外付けドライブのみを搭載したシステムから、外付けドライブと内蔵ドライブ（ディスクとコントローラが同一シャーシ内）を搭載したシステムにアップグレードした場合、新しいシステムの内部スロットから取り外したディスクを追加または再装着できます。これは、両サイトでアップグレードが完了し、クラスタが正常な状態になった後であればいつでも実行できます。

ドライブを再度追加または再装着すると、必要に応じてONTAPで使用できるようになります。

このタスクは、特定のアップグレードの組み合わせにのみ適用されます。詳細については、を参照してください "新しいコントローラのシャーシから内部ドライブを取り外す" 。

ONTAP メディエーターを再設定します

アップグレードを開始する前に自動的に削除されたONTAP メディエーターを手動で設定します。

1. の手順を使用します"MetroCluster IP構成からONTAPメディエーターを構成する"。

Tiebreaker による監視をリストアします

MetroCluster 構成が Tiebreaker ソフトウェアで監視するように設定されている場合は、 Tiebreaker 接続をリストアできます。

1. の手順を使用します "MetroCluster 構成を追加"。

エンドツーエンドの暗号化を設定する

ご使用のシステムでサポートされている場合は、MetroCluster IP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。を参照してください "エンドツーエンドの暗号化を設定する" を参照してください。

スイッチオーバーとスイッチバックを使用したMetroCluster IPのコントローラのアップグレード（ONTAP 9.8以降）

スイッチオーバーとスイッチバックを使用したMetroCluster IPコントローラのアップグレードのワークフロー（ONTAP 9.8以降）

ONTAP 9.8 以降では、 MetroCluster スイッチオーバー処理を使用して、パートナークラスタのコントローラモジュールをアップグレードする際にクライアントに無停止でサービスを提供できます。この手順の一部として他のコンポーネント（ストレージシェルフやスイッチなど）をアップグレードすることはできません。

このワークフローについて

このワークフローを使用して、ONTAP 9.8以降を実行しているシステムでスイッチオーバーとスイッチバックを使用してMetroCluster IPコントローラをアップグレードできます。

1 "アップグレードを準備"

サポートされているアップグレードの組み合わせと要件を確認し、必要な手順を実行してシステムをコントローラのアップグレードに備えます。

2 "コントローラのアップグレード"

スイッチバックを実行する前に、MetroCluster構成をスイッチオーバーして、古いコントローラから構成を削除し、新しいコントローラをラックに設置し、ルートアグリゲートディスクを再割り当てし、新しいコントローラをブートします。

3 "アップグレードを完了します"

2番目のサイトでアップグレードタスクを繰り返し、監視設定をリストアすることで、コントローラのアップグレードを完了します。

アップグレードを準備

このMetroCluster IPアップグレード手順を使用するための要件

コントローラのアップグレードを実行する前に、システムがすべての要件を満たしていることを確認してください。

*コントローラーをアップグレードするたびに、この手順を記載どおりに実行する必要があります。*新しいプラットフォームがリリースされると、従う必要のある新しい手順や変更された手順が発生する可能性があります。たとえば、 ONTAP 9.15.1以降で導入されたプラットフォームにアップグレードする場合は、 "必要なブート引数を設定する" アップグレードを成功させるには、その他の追加手順を実行します。

この手順 でサポートされているプラットフォーム

- プラットフォームで ONTAP 9.8 以降が実行されている必要があります。
- ターゲット（新規）プラットフォームは、元のプラットフォームとは異なるモデルである必要があります。
- MetroCluster IP構成では、この手順 を使用してアップグレードできるプラットフォームモデルは限られています。
  - サポートされるプラットフォームのアップグレードの組み合わせについては、のMetroCluster IPアップグレードの表を参照してください"コントローラのアップグレード手順 を選択します"。

    を参照してください "アップグレードまたは更新方法を選択します" を参照してください。

要件

- この手順環境コントローラモジュールは MetroCluster IP 構成です。
- 構成内のすべてのコントローラは、同じメンテナンス期間にアップグレードする必要があります。

  このメンテナンス作業以外では、コントローラタイプが異なる MetroCluster 構成を運用することはできません。

- MetroCluster IPシステムが両方のサイトで同じバージョンのONTAPを実行している必要があります。
- MetroCluster IPスイッチ（スイッチタイプ、ベンダー、モデル）とファームウェアのバージョンが、アップグレード構成の既存および新しいコントローラでサポートされている必要があります。

  サポートされているスイッチとファームウェアのバージョンについては、またはを参照してください "Hardware Universe" "IMT" 。

- 新しいシステムよりも多くのスロットまたはポートがあるシステムからアップグレードする場合は、新しいシステムに十分なスロットとポートがあることを確認する必要があります。

  アップグレードを開始する前に、を参照し"Hardware Universe"て、新しいシステムのスロットとポートの数を確認してください。

- システムで有効になっている場合は"エンドツーエンドの暗号化を無効にする"、アップグレードを実行する前に実行します。
- 新しいプラットフォームのスロット数が元のシステムのスロット数より少ない場合、またはポートのタイプが異なる場合は、新しいシステムにアダプタを追加しなければならないことがあります。
- 元のプラットフォームのIPアドレス、ネットマスク、ゲートウェイは新しいプラットフォームで再利用します。

この手順では、次の名前が使用されています。

- site_A で cluster_A
  - アップグレード前：
    - node_A_1 - 古い
    - Node_a_2-old
  - アップグレード後：
    - node_A_1 - 新規
    - Node_a_2 - 新規
- site_B （ site_B
  - アップグレード前：
    - node_B_1 - 古い
    - node_B_2 - 古い
  - アップグレード後：
    - node_B_1 - 新規
    - node_B_2 - 新規

次の手順

"コンソールログを有効にする"です。

MetroCluster IPコントローラのアップグレード前にコンソールログを有効にする

コントローラのアップグレードを実行する前に、デバイスのコンソールログを有効にしてください。

NetAppでは、使用しているデバイスでコンソールロギングをイネーブルにし、この手順を実行する際に次のアクションを実行することを強く推奨します。

- メンテナンス中はAutoSupportを有効のままにします。
- メンテナンスの前後にメンテナンスAutoSupportメッセージをトリガーして、メンテナンスアクティビティ中にケースの作成を無効にします。

  ナレッジベースの記事を参照してください "スケジュールされたメンテナンス時間中にケースの自動作成を停止する方法"。

- 任意のCLIセッションのセッションロギングをイネーブルにします。セッションログを有効にする方法に

ついては、ナレッジベースの記事の「セッション出力のログ」セクションを参照してください "ONTAP システムへの接続を最適化するためのPuTTYの設定方法"。

次の手順

の情報を参照し"必要なbootargを設定する（9.15.1以降で導入されたシステムにアップグレードする場合）"て、既存のシステムに必要なbootargを設定する必要があるかどうかを確認します。

必要な**bootarg**の設定（**ONTAP 9.15.1**以降で導入されたシステムへの**MetroCluster IP**のアップグレードの場合）

ONTAP 9.15.1 以降で導入されたシステムにアップグレードする場合は、通常、アップグレードを開始する前に、古いコントローラで bootarg を設定する必要があります。

アップグレードの組み合わせが影響を受ける場合、アップグレードを成功させるには、すべての古いコントローラーで bootarg を設定する必要があります。このセクションの情報を注意深く確認して、アップグレードの組み合わせで bootarg を設定する必要があるかどうか、また組み合わせに対して正しい bootarg を設定する方法を確認してください。

ステップ**1:** 古いコントローラに**bootarg**を設定する必要があるかどうかを確認します

アップグレードを開始する前に、次の情報を使用して、古いコントローラに bootarg を設定する必要があるかどうかを確認します：

- 特に明記されていない限り、以下のシステムへのサポートされているアップグレードでは、古いコントローラに bootarg を設定する必要があります。
  - AFF A70、AFF A90、AFF A1K
  - FAS70、FAS90
  - AFF C80用
  - AFF A50、AFF A20、AFF A30
  - AFF C30、AFF C60
  - FAS50
- アップグレードが次のいずれかの組み合わせである場合、古いコントローラーで bootarg を設定する必要はありません。
  - AFF A70システムからAFF A90システムへ
  - FAS70システムからFAS90システムへ

アップグレードでbootargを設定する必要がない場合は、このタスクをスキップして直接"システムのアップグレードを準備"。

ステップ**2:** 古いコントローラに設定する**bootarg**を決定する

影響を受けるアップグレードのほとんどは、 `hw.cxgbe.toe_keepalive_disable`古いコントローラ上の bootarg。ただし、特定のアップグレードパスでは、 `bootarg.siw.interop_enabled`代わりに bootarg を使用してください。

次の表を参照して、それぞれのアップグレードの組み合わせに設定する必要があるbootargを特定してください。

アップグレード対象	**bootarg**の設定
AFF A250からAFF A30へ	`bootarg.siw.interop_enabled`
AFF C250からAFF C30へ	`bootarg.siw.interop_enabled`
AFF A150からAFF A20へ	`bootarg.siw.interop_enabled`
AFF A220からAFF A20へ	`bootarg.siw.interop_enabled`
AFF A70、 AFF A90、 AFF A1K、FAS70、FAS90、AFF C80、 AFF A50、 AFF A30、 AFF C30、 AFF C60、またはFAS50システムへのその他のすべてのアップグレード 注: AFF A70システムからAFF A90システム、またはFAS70 システムから FAS90 システムへのアップグレードの場合は、bootarg を設定する必要はありません。	`hw.cxgbe.toe_keepalive_disable`

ステップ**3:** 古いコントローラに必要な**bootarg**を設定する

アップグレードの組み合わせに必要な bootarg を決定したら、手順に従って古いコントローラで bootarg を設定します。

アップグレードを開始する前に、両方のサイトのすべての古いノードで bootarg を設定する必要があります。

手順

1. 両方のサイトで一方のノードを停止し、そのHAパートナーでノードのストレージテイクオーバーを実行できるようにします。

   ```
   halt -node <node_name>
   ```

2. アップグレードの組み合わせに必要なbootargを設定します。の表を使用して、設定する必要があるbootargを決めておき設定が必要なbootargを特定するます。

hw.cxgbe.toe_keepalive_disable

a. `LOADER`停止したノードのプロンプトで、次のように入力します。

```
setenv hw.cxgbe.toe_keepalive_disable 1
```

'aveenv

```
printenv hw.cxgbe.toe_keepalive_disable
```

bootarg.siw.interop_enabled

a. `LOADER`停止したノードのプロンプトで、次のように入力します。

```
setenv bootarg.siw.interop_enabled 1
```

'aveenv

```
printenv bootarg.siw.interop_enabled
```

3. ノードをブートします。

「 boot_ontap 」

4. ノードがブートしたら、プロンプトでノードのギブバックを実行します。

```
storage failover giveback -ofnode <node_name>
```

5. アップグレードするDRグループまたはDRグループ内のすべてのノードで、この手順を繰り返します。

次の手順

"システムのアップグレードを準備"です。

MetroCluster IPシステムのアップグレードを準備

既存のMetroCluster構成に変更を加える前に、構成の健全性を確認し、新しいプラットフォームを準備し、その他のタスクを実行します。

コントローラをアップグレードする前に**MetroCluster**スイッチ**RCF**を更新する

プラットフォームの新旧モデルによっては、コントローラをアップグレードする前にMetroCluster Switch Reference Configuration File（RCF；スイッチリファレンス構成ファイル）の更新が必要になる場合があります。

このタスクについて

この作業は、次の状況で実行します。

- スイッチのRCF設定が最小バージョンになっていません。
- バックエンドMetroCluster接続で使用するVLAN IDを変更する必要があります。

作業を開始する前に

コントローラをアップグレードする前にRCFの更新が必要かどうかを確認します。

- スイッチにサポートされる最小バージョンのRCFが設定されていない場合は、コントローラをアップグレードする前にRCFを更新する必要があります。

スイッチモデル	必要なRCFバージョン
Cisco 3132Q-V の設定	1.7 以降
Cisco 3232C	1.7 以降
Broadcom BES-53248 の場合	1.3 以降
NVIDIA SN2100	2.0以降

- 使用している古いプラットフォームモデルと新しいプラットフォームモデルの両方が次のリストにある場合は、コントローラをアップグレードする前にVLAN IDを更新する必要は*ありません*。
  - FAS8200またはAFF A300
  - AFF A320
  - FAS9000またはAFF A700
  - AFF A800、AFF C800、ASA A800、またはASA C800

  使用している古いプラットフォームモデルと新しいプラットフォームモデルのいずれかが上記に記載されていない場合は、MetroClusterインターフェイスでサポートされているVLAN IDが使用されていることを確認する必要があります。MetroClusterインターフェイスでサポートされるVLAN IDは、10、20、または101～4096の範囲です。

  - VLAN IDが10、20、101~4096の範囲にない場合は、コントローラをアップグレードする前にスイッチのRCFをアップグレードする必要があります。
  - ローカルクラスタ接続には任意のVLANを使用できます。指定した範囲内にある必要はありません。
  - アップグレード先の新しいRCFでVLAN 10、20、または101~4096の範囲のVLANを使用する必要があります。ローカルクラスタのVLANは、必要な場合以外は変更しないでください。

手順

1. IPスイッチで新しいRCFを適用できるように準備します。

   スイッチベンダーに対応するセクションを参照してください。

   スイッチはswitch_A_1、switch_B_1、switch_A_2、switch_B_2の順に更新する必要があります。

   - "Broadcom IP スイッチを工場出荷時のデフォルトにリセットします"

- "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"
- "NVIDIA IP SN2100スイッチを工場出荷時のデフォルトにリセット"

2. RCFをダウンロードしてインストールします。

   スイッチベンダーに対応するセクションを参照してください。

   - "Broadcom RCFのダウンロードとインストール"
   - "Cisco IP RCFのダウンロードとインストール"
   - "NVIDIA IP RCFのダウンロードとインストール"

古いノードから新しいノードへのポートのマッピング

node_A_1-oldの物理ポートがnode_A_1-newの物理ポートに正しくマッピングされていることを確認する必要があります。これにより、アップグレード後にnode_A_1-newがクラスタ内の他のノードおよびネットワークと通信できるようになります。

このタスクについて

アップグレードプロセス中に新しいノードが最初にブートすると、交換する古いノードの最新の設定が再生されます。node_A_1-newをブートすると、ONTAPはnode_A_1-oldと同じポートでLIFをホストしようとします。そのため、ポートとLIFの設定は、アップグレード時に古いノードの設定と互換性があるように調整する必要があります。アップグレードの手順では、クラスタLIF、管理LIF、およびデータLIFの設定が正しいことを確認するために、古いノードと新しいノードの両方で手順を実行します。

次の表に、新しいノードのポート要件に関連する設定変更の例を示します。

クラスタインターコネクトの物理ポート		
古いコントローラ	新しいコントローラ	必要なアクション
e0a 、 e0b	e3a 、 e3b	一致するポートがありません。アップグレード後に、クラスタポートを再作成する必要があります。
e0c 、 e0d	e0a 、 e0b 、 e0c 、 e0d	e0cとe0dは同じポートです。設定を変更する必要はありませんが、アップグレード後に使用可能なクラスタポートにクラスタLIFを分散させることができます。

手順

1. 新しいコントローラで使用できる物理ポートとポートでホストできる LIF を確認します。

   コントローラのポートの用途は、プラットフォームモジュール、およびMetroCluster IP構成で使用するスイッチによって異なります。新しいプラットフォームで使用するポートをから収集できます"Hardware Universe"。

2. ポートの使用状況を計画し、次の表に新しいノードごとに参考情報を記入します。

   この表は、アップグレード手順を実行するときに参照します。

	node_A_1 - 古い			node_A_1 - 新規		
LIF	ポート	IPspace	ブロードキャストドメイン	ポート	IPspace	ブロードキャストドメイン
クラスタ 1						
クラスタ 2						
クラスタ 3						
クラスタ 4						
ノード管理						
クラスタ管理						
データ 1						
データ 2.						
データ 3						
データ 4.						
SAN						
クラスタ間ポート						

新しいコントローラをネットブート

新しいノードを設置したら、ネットブートを実行して、新しいノードが元のノードと同じバージョンの ONTAP を実行するようにする必要があります。ネットブートという用語は、リモート・サーバに保存された ONTAP イメージからブートすることを意味します。ネットブートの準備を行うときは、システムがアクセスできる Web サーバに、 ONTAP 9 ブート・イメージのコピーを配置する必要があります。

手順

1. 新しいコントローラをネットブートします。

   a. にアクセスします "ネットアップサポートサイト" システムのネットブートの実行に使用するファイルをダウンロードするには、次の手順を実行します。

   b. ネットアップサポートサイトのソフトウェアダウンロードセクションから適切な ONTAP ソフトウェアをダウンロードし、「 ONTAP-version _image.tgz 」ファイルを Web にアクセスできるディレクトリに保存します。

   c. Web にアクセスできるディレクトリに移動し、必要なファイルが利用可能であることを確認します。

ディレクトリの一覧に、カーネルファイルを含むネットブートフォルダが含まれるようにします。

`_ontap - version_image.tgz

ファイルを抽出する必要はありません `_ontap-version_image.tgz`。

d. `LOADER`プロンプトで、管理LIFのネットブート接続を設定します。

IP アドレス	作業
DHCP	自動接続を設定します。 ifconfig e0M -auto
静的	手動接続を設定します。 ifconfig e0M -addr= *ip_addr*-mask= *netmask* _ *-gw= _gateway*`

e. ネットブートを実行します。

netboot\http://_web_server_ip/path_to_web-accessible_directory/ontap-version_image.tgz`

f. ブートメニューからオプション **(7) Install new software first** を選択して、新しいソフトウェアイメージをダウンロードし、ブートデバイスにインストールします。

次のメッセージは無視してください。

「この手順は、 HA ペアでの無停止アップグレードではサポートされていません」というメッセージが表示されます。IT 環境：ソフトウェアの無停止アップグレード。コントローラのアップグレードは対象外。

a. 手順を続行するかどうかを確認するメッセージが表示されたら 'y' と入力し ' パッケージの入力を求められたら ' イメージ・ファイルの URL を入力します

http://*web_server_ip/path_to_web-accessible_directory/ontap-version*_image.tgz`

b. 必要に応じてユーザ名とパスワードを入力するか、 Enter キーを押して続行します。

c. 入力 `n` 次のようなプロンプトが表示されたら、バックアップの回復をスキップします。

```
Do you want to restore the backup configuration now? {y|n} n
```

d. 次のようなプロンプトが表示されたら '**y**' を入力して再起動します

```
The node must be rebooted to start using the newly installed
software. Do you want to reboot now? {y|n} y
```

新しくインストールされたソフトウェアを使用するには、ノードを再起動する必要があります。

コントローラモジュールの設定をクリアします

MetroCluster 構成で新しいコントローラモジュールを使用する前に、既存の構成をクリアする必要があります。

手順

1. 必要に応じて、ノードを停止してプロンプトを表示し `LOADER`ます。

   「 halt 」

2. `LOADER`プロンプトで、環境変数をデフォルト値に設定します。

   「デフォルト設定」

3. 環境を保存します。

   'aveenv

4. `LOADER`プロンプトでブートメニューを起動します。

   「 boot_ontap menu

5. ブートメニューのプロンプトで、設定を消去します。

   wipeconfig

   確認プロンプトに「 yes 」と応答します。

   ノードがリブートし、もう一度ブートメニューが表示されます。

6. ブートメニューでオプション * 5 * を選択し、システムをメンテナンスモードでブートします。

   確認プロンプトに「 yes 」と応答します。

サイトをアップグレードする前に **MetroCluster** の健全性を確認

アップグレードを実行する前に、MetroCluster 構成の健全性と接続性を確認します。

最初のサイトでコントローラをアップグレードした後、2番目のサイトをアップグレードする前に、 `metrocluster check run`に続く `metrocluster check show`エラーを返します `config-replication`フィールド。このエラーは、各サイトのノード間でNVRAMのサイズが一致していないことを示しています。これは、両サイトで異なるプラットフォームモデルが存在する場合に想定される動作です。DRグループ内のすべてのノードでコントローラーのアップグレードが完了するまで、このエラーは無視できます。

手順

1. ONTAP で MetroCluster 構成の動作を確認します。

a. ノードがマルチパス構成になっているかどうかを確認します。+
`node run -node <node_name> sysconfig -a`

MetroCluster構成の各ノードに対してこのコマンドを実行します。

b. 「 storage disk show -broken 」の構成に破損ディスクがないことを確認してください

MetroCluster構成の各ノードでこのコマンドを実行します。

c. ヘルスアラートがないかどうかを確認します。

「 system health alert show 」というメッセージが表示されます

このコマンドは各クラスタで実行します。

d. クラスタのライセンスを確認します。

「 system license show 」を参照してください

このコマンドは各クラスタで実行します。

e. ノードに接続されているデバイスを確認します。

「 network device-discovery show 」のように表示されます

このコマンドは各クラスタで実行します。

f. 両方のサイトでタイムゾーンと時間が正しく設定されていることを確認します。

cluster date show

このコマンドは各クラスタで実行します。時間とタイムゾーンを設定するには、コマンドを使用し `cluster date`ます。

2. MetroCluster 構成の運用モードを確認し、 MetroCluster チェックを実行
   a. MetroCluster の構成と動作モードが「 normal 」であることを確認します。 + MetroCluster show
   b. 想定されるすべてのノードが表示されることを確認します。 + MetroCluster node show `
   c. 次のコマンドを問題に設定します。

「 MetroCluster check run 」のようになります

   d. MetroCluster チェックの結果を表示します。

MetroCluster チェックショー

3. Config Advisor ツールを使用して MetroCluster のケーブル接続を確認します。
   a. Config Advisor をダウンロードして実行します。

"ネットアップのダウンロード： Config Advisor"

   b. Config Advisor の実行後、ツールの出力を確認し、推奨される方法で検出された問題に対処します。

アップグレードの開始前に各ノードについて情報を収集し、必要に応じてネットワークブロードキャストドメインを調整し、 VLAN やインターフェイスグループを削除して、暗号化情報を収集する必要があります。

手順

1. 各ノードの物理的なケーブル接続をメモし、必要に応じてケーブルにラベルを付けて新しいノードを正しくケーブル接続できるようにします。
2. 各ノードのインターコネクト、ポート、LIFの情報を収集します。

   ノードごとに次のコマンドの出力を収集します。

   - MetroCluster interconnect show
   - 「 MetroCluster configurion-settings connection show 」を参照してください
   - 'network interface show -role cluster, node-mgmt
   - `network port show -node <node_name> -type physical`
   - `network port vlan show -node <node_name>`
   - `network port ifgrp show -node <node_name> -instance`
   - 「 network port broadcast-domain show 」
   - 「 network port reachability show-detail` 」と表示されます
   - network ipspace show
   - volume show
   - 「 storage aggregate show
   - `system node run -node <node_name> sysconfig -a`
   - `aggr show -r`
   - 「ディスクショー」
   - `system node run <node-name> disk show`
   - `vol show -fields type`
   - `vol show -fields type , space-guarantee`
   - 「 vserver fcp initiator show 」のように表示されます
   - 「 storage disk show 」を参照してください
   - 「 MetroCluster configurion-settings interface show 」を参照してください
3. site_B （プラットフォームを現在アップグレード中のサイト）の UUID を収集します。

   MetroCluster node show -fields node-cluster.uuid 、 node-uuid

   アップグレードが成功するためには、これらの値がsite_Bの新しいコントローラモジュールで正しく設定されている必要があります。アップグレードプロセスの後半でコマンドにコピーできるように、値をファイルにコピーします。

   次の例は、 UUID を指定したコマンドの出力を示しています。

```
cluster_B::> metrocluster node show -fields node-cluster-uuid, node-uuid
  (metrocluster node show)
dr-group-id cluster     node   node-uuid
node-cluster-uuid
----------- --------- -------- ------------------------------------
------------------------------
1           cluster_A node_A_1 f03cb63c-9a7e-11e7-b68b-00a098908039
ee7db9d5-9a82-11e7-b68b-00a098908039
1           cluster_A node_A_2 aa9a7a7a-9a81-11e7-a4e9-00a098908c35
ee7db9d5-9a82-11e7-b68b-00a098908039
1           cluster_B node_B_1 f37b240b-9ac1-11e7-9b42-00a098c9e55d
07958819-9ac6-11e7-9b42-00a098c9e55d
1           cluster_B node_B_2 bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
07958819-9ac6-11e7-9b42-00a098c9e55d
4 entries were displayed.
cluster_B::*
```

NetAppでは、次のような表にUUIDを記録することを推奨しています。

クラスタまたはノード	UUID
cluster_B	07958819 - 9ac6-11e7-9b42 - 00a098c9e55d
node_B_1	f37b240b-9ac1-11e7-9b42 -00a098c9e55d
node_B_2	bf8e3f8f-9ac4-117-bd4e-00a098c379f です
cluster_A	ee7db9d5-9a82-11e7-b68b-00a098908039
node_A_1	f03cb63c-9a7e-11e7-b68b-00a098908039
Node_a_2	aa9a7a7a1-9a81-11e7-a4e9-00a098908c35

4. MetroCluster ノードが SAN 構成になっている場合は、関連情報を収集します。

   次のコマンドの出力を収集します。

   - 「 fcp adapter show -instance 」のように表示されます
   - 「 fcp interface show -instance 」の略
   - 「 iscsi interface show 」と表示されます
   - ucadmin show

5. ルートボリュームが暗号化されている場合は、キー管理ツールに使用するパスフレーズを収集して保存します。

「 securitykey-manager backup show 」を参照してください

6. MetroCluster ノードがボリュームまたはアグリゲートに暗号化を使用している場合は、キーとパスフレーズに関する情報をコピーします。

   詳細については、を参照してください "オンボードキー管理情報の手動でのバックアップ"。

   a. オンボード・キー・マネージャが構成されている場合： +'securitykey-manager onboard show-backup

      パスフレーズは、アップグレード手順の後半で必要になります。

   b. Enterprise Key Management （ KMIP ）が設定されている場合は、次のコマンドを問題で実行します。

      「 securitykey manager external show -instance 」 'ecurity key manager key query 」を参照してください

7. 既存のノードのシステム ID を収集します。

   「 MetroCluster node show -fields node-systemid 、 ha-partner-systemid 、 dr-partner-systemid 、 dr-auxiliary-systemid 」を指定します

   次の出力は、再割り当てされたドライブを示しています。

```
::> metrocluster node show -fields node-systemid,ha-partner-systemid,dr-
partner-systemid,dr-auxiliary-systemid

dr-group-id cluster     node     node-systemid ha-partner-systemid dr-
partner-systemid dr-auxiliary-systemid
----------- ----------- -------- ------------- ------------------
------------------ ---------------------
1           cluster_A node_A_1   537403324     537403323
537403321           537403322
1           cluster_A node_A_2   537403323     537403324
537403322           537403321
1           cluster_B node_B_1   537403322     537403321
537403323           537403324
1           cluster_B node_B_2   537403321     537403322
537403324           537403323
4 entries were displayed.
```

メディエーターまたは **Tiebreaker** の監視を削除します

プラットフォームをアップグレードする前に、 MetroCluster 設定を Tiebreaker またはメディエーターユーティリティで監視している場合は、監視を解除する必要があります。

手順

1. 次のコマンドの出力を収集します。

「 storage iscsi-initiator show 」のように表示されます

2. Tiebreaker 、メディエーター、またはスイッチオーバーを開始できるその他のソフトウェアから既存の MetroCluster 構成を削除します。

使用するポート	使用する手順
Tiebreaker	"MetroCluster 設定の削除"
メディエーター	ONTAP プロンプトで次のコマンドを問題に設定します。 MetroCluster 構成設定のメディエーターが削除されました
サードパーティ製アプリケーション	製品マニュアルを参照してください。

カスタム **AutoSupport** メッセージをメンテナンス前に送信する

メンテナンスを実行する前に、 AutoSupport an 問題 message to notify NetApp technical support that maintenance is maintenancing （メンテナンスが進行中であることをネットアップテクニカルサポートに通知する）を実行システム停止が発生したとみなしてテクニカルサポートがケースをオープンしないように、メンテナンスが進行中であることを通知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 サイトごとに実行する必要があります。

手順

1. クラスタにログインします。
2. メンテナンスの開始を通知する AutoSupport メッセージを起動します。

   「 system node AutoSupport invoke -node * -type all -message MAINT= *maintenance-window-in-hours* 」というメッセージが表示されます

   「 maintenance-window-in-hours 」パラメータには、メンテナンス時間の長さを最大 72 時間指定します。この時間が経過する前にメンテナンスが完了した場合は、メンテナンス期間が終了したことを通知する AutoSupport メッセージを起動できます。

   「 system node AutoSupport invoke -node * -type all -message MAINT= end 」というメッセージが表示されます

3. 同じ手順をパートナーサイトでも実行します。

次の手順

"MetroCluster 構成をスイッチオーバーします"です。

コントローラのアップグレード

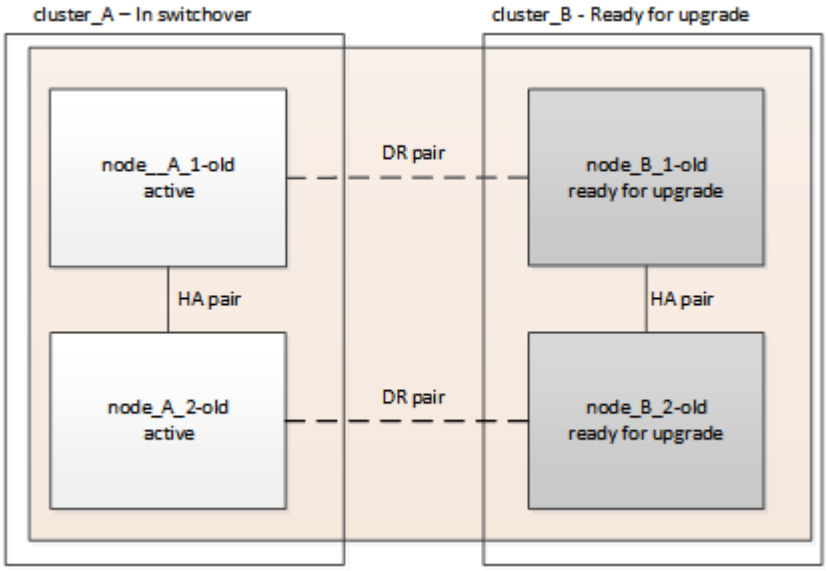
site_Bのプラットフォームをアップグレードできるように、site_Aに構成をスイッチオーバーします。

このタスクについて

このタスクは site_A で実行する必要があります

このタスクの完了後、次の作業を行います。

- cluster_Aはアクティブで、両方のサイトにデータを提供しています。
- cluster_Bは非アクティブになり、アップグレードプロセスを開始できる状態になります。



手順

1. site_B のノードをアップグレードできるように、 MetroCluster 構成を site_A にスイッチオーバーします。

   a. cluster_A で次のコマンドを問題します。

      MetroCluster switche-controller-replacement true

      この処理が完了するまでに数分かかることがあります。

   b. スイッチオーバー処理を監視します。

      「 MetroCluster operation show 」を参照してください

   c. 処理が完了したら、ノードがスイッチオーバー状態であることを確認します。

      「 MetroCluster show 」

   d. MetroCluster ノードのステータスを確認します。

      MetroCluster node show

コントローラのアップグレード中は、ネゴシエートスイッチオーバー後のアグリゲートの自動修復が無効になります。

次の手順

"インターフェイス設定を削除し、古いコントローラをアンインストールする"です。

インターフェイス設定を削除し、古い**MetroCluster IP**コントローラをアンインストールする

LIFの配置が正しいことを確認その後、古いコントローラのVLANとインターフェイスグループを削除し、コントローラを物理的に取り外します。

このタスクについて

- これらの手順は古いコントローラ（node_B_1-old、node_B_2-old）で実行します。
- この手順で使用するには、で収集した情報が必要"古いノードから新しいノードへのポートのマッピング"です。

手順

1. 古いノードをブートして、ノードにログインします。

   「 boot_ontap 」

2. アップグレードするシステムで*共有クラスタ/ HAポート*を使用している場合は、MetroCluster IPインターフェイスでサポートされているIPアドレスが使用されていることを確認します。

   次の情報を使用して、新しいシステムで共有クラスタ/ HAポートが使用されているかどうかを確認します。

共有クラスタ/ **HA**ポート

次の表に示すシステムは、共有クラスタ/ HAポートを使用します。

AFFおよび**ASA**システム	**FAS**システム
• AFF A20用 • AFF A30用 • AFF C30 • AFF A50用 • AFF C60 • AFF C80用 • AFF A70用 • AFF A90用 • AFF A1K用	• FAS50 • FAS70 • FAS90

共有**MetroCluster / HA**ポート

次の表に示すシステムは、共有MetroCluster / HAポートを使用します。

AFFおよび**ASA**システム	**FAS**システム
• AFF A150、ASA A150向け • AFF A220 • AFF C250、ASA C250向け • AFF A250、ASA A250向け • AFF A300 • AFF A320 • AFF C400、ASA C400向け • AFF A400、ASA A400向け • AFF A700 • AFF C800、ASA C800向け • AFF A800、ASA A800向け • AFF A900、ASA A900向け	• FAS2750 • FAS500f • FAS8200 • FAS8300 • FAS8700 の場合 • FAS9000 • FAS9500

a. 古いコントローラのMetroClusterインターフェイスのIPアドレスを確認します。

「 MetroCluster configurion-settings interface show 」を参照してください

b. MetroClusterインターフェイスで169.254.17.xまたは169.254.18.xのIPアドレスが使用されている場合は、アップグレードを開始する前に、を参照し"記事「MetroCluster IPインターフェイスのプロパティ

を変更する方法」"てインターフェイスのIPアドレスを変更してください。

> MetroClusterインターフェイスに169.254.17.xまたは169.254.18.xのIPアドレスが設定されている場合、*共有クラスタ/ HAポート*を使用するシステムへのアップグレードはサポートされません。

3. 古いコントローラのクラスタ間LIFを変更して、HAインターコネクトまたはMetroCluster IP DRインターコネクトに使用するポートとは別のホームポートを新しいコントローラで使用するようにします。

> この手順は、アップグレードを成功させるために必要です。

古いコントローラのクラスタ間LIFでは、新しいコントローラのHAインターコネクトまたはMetroCluster IP DRインターコネクトに使用されるポートとは別のホームポートを使用する必要があります。たとえば、AFF A90コントローラにアップグレードすると、HAインターコネクトポートはe1aとe7aになり、MetroCluster IP DRインターコネクトポートはe2bとe3bになります。古いコントローラのインタークラスタLIFがポートe1a、e7a、e2b、またはe3bでホストされている場合は、クラスタ間LIFを移動する必要があります。

新しいノードでのポートの分散と割り当てについては、を参照して "Hardware Universe"ください。

a. 古いコントローラで、クラスタ間LIFを表示します。

```
network interface show -role intercluster
```

古いコントローラのクラスタ間LIFが、HAインターコネクトに使用するポートと同じポートを使用するか、新しいコントローラのMetroCluster IP DRインターコネクトに使用するポートと同じポートを使用するかに応じて、次のいずれかの処理を実行します。

クラスタ間**LIF**の状況	手順
同じホームポートを使用する	サブステップb
別のホームポートを使用する	手順 4

b. 別のホームポートを使用するようにクラスタ間LIFを変更します。

```
network interface modify -vserver <vserver> -lif <intercluster_lif> -home
-port <port-not-used-for-ha-interconnect-or-mcc-ip-dr-interconnect-on-new-
nodes>
```

c. すべてのインタークラスタLIFが新しいホームポートにあることを確認します。

```
network interface show -role intercluster -is-home false
```

すべてのクラスタ間LIFがそれぞれのホームポートにある場合は、コマンド出力が空になります。

d. ホームポートにないLIFをリバートします。

```
network interface revert -lif <intercluster_lif>
```

ホームポートにないクラスタ間LIFごとにコマンドを繰り返します。

4. 古いコントローラのすべてのデータLIFのホームポートを、新旧両方のコントローラモジュールで同じ共通のポートに割り当てます。

> 新旧のコントローラに共通のポートがない場合は、データLIFを変更する必要はありません。この手順を省略して、に直接進みます手順 5。

a. LIF を表示します。

「 network interface show 」を参照してください

SANとNASを含むすべてのデータLIFはスイッチオーバーサイト（cluster_A）で稼働しているため、管理状態はupで動作状態はdownです。

b. の出力を確認して、クラスタポートとして使用されていない新旧両方のコントローラで同じ共通の物理ネットワークポートを特定します。

たとえば、 e0d は古いコントローラの物理ポートで、新しいコントローラにも存在します。e0d は、クラスタポート、または新しいコントローラ上で使用されません。

プラットフォームモデルのポートの用途については、を参照してください。 "Hardware Universe"

c. すべてのデータLIFで共通のポートをホームポートとして使用するように変更します。+
`network interface modify -vserver <svm-name> -lif <data-lif> -home-port <port-id>`

次の例では、これは「 e0d 」です。

例：

```
network interface modify -vserver vs0 -lif datalif1 -home-port e0d
```

5. ブロードキャストドメインを変更して、削除が必要なVLANと物理ポートを削除します。

`broadcast-domain remove-ports -broadcast-domain <broadcast-domain-name> -ports <node-name:port-id>`

すべての VLAN ポートと物理ポートについて、この手順を繰り返します。

6. クラスタポートをメンバーポートとして使用し、インターフェイスグループをメンバーポートとして使用している VLAN ポートをすべて削除します。

a. VLANポートの削除：+
`network port vlan delete -node <node_name> -vlan-name <portid-vlandid>`

例：

```
network port vlan delete -node node1 -vlan-name e1c-80
```

b. インターフェイスグループから物理ポートを削除します。

```
network port ifgrp remove-port -node <node_name> -ifgrp <interface-group-
name> -port <portid>
```

例：

```
network port ifgrp remove-port -node node1 -ifgrp a1a -port e0d
```

a. ブロードキャストドメインからVLANポートとインターフェイスグループポートを削除します。

```
network port broadcast-domain remove-ports -ipspace <ipspace> -broadcast
-domain <broadcast-domain-name> -ports
<nodename:portname,nodename:portnamee>,..
```

b. 必要に応じて、インターフェイスグループポートを変更して他の物理ポートをメンバーとして使用します。

```
ifgrp add-port -node <node_name> -ifgrp <interface-group-name> -port <port-
id>
```

7. ノードを停止してプロンプトを表示し `LOADER`ます。

「 halt -inhibit-takeover true 」と入力します

8. site_Bの古いコントローラ（node_B_1-oldとnode_B_2-old）のシリアルコンソールに接続し、プロンプトが表示されていることを確認します `LOADER`。
9. bootarg の値を収集します。

printenv

10. node_B_1-oldとnode_B_2-oldのストレージ接続とネットワーク接続を切断します。新しいノードに再接続できるように、ケーブルにラベルを付けます。
11. node_B_1 から古いおよび node_B_2 から電源ケーブルを外します。
12. node_B_1 古いコントローラと node_B_2 の古いコントローラをラックから取り外します。

次の手順

"新しいコントローラをセットアップ"です。

新しい**MetroCluster IP**コントローラのセットアップ

新しいMetroCluster IPコントローラをラックに設置してケーブル接続します。

手順

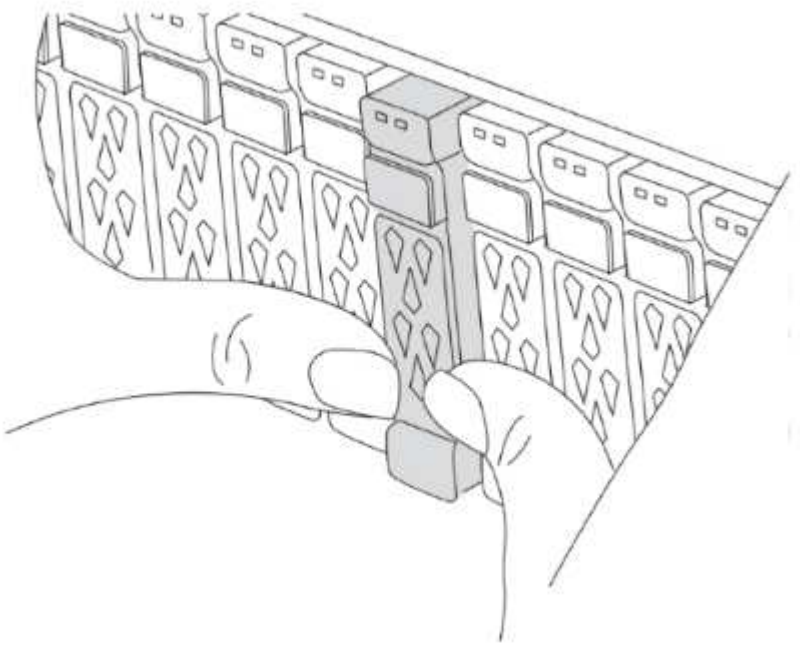
1. 必要に応じて、新しいコントローラモジュールとストレージシェルフの配置を計画します。

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、構成内のストレージシェルフ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. AFF A800からAFF A90システムへのアップグレードやAFF C800からAFF C80システムへのアップグレードなど、コントローラモジュールの交換が必要なアップグレードの場合は、コントローラモジュールを交換するときにコントローラモジュールをシャーシから取り外す必要があります。その他のすべてのアップグレードの場合は、に進みます 手順 4。

   シャーシの前面で、プラスのストッパーになるまで、親指で各ドライブをしっかりと押し込みます。ドライブがシャーシのミッドプレーンにしっかりと装着されていることを確認します。



4. コントローラモジュールを設置します。

   インストール手順は、アップグレードでコントローラモジュールの交換が必要かどうか、または古いコントローラを外付けシェルフに変換するためにIOMモジュールが必要かどうかによって異なります。

アップグレード対象	実行する手順
• AFF A150からAFF A20システムへ • AFF A220からAFF A20システムへ	コントローラから外付けシェルフへの変換
• AFF A800からAFF A90システムへ • AFF C800からAFF C80システムへ • AFF A250からAFF A30システムへ • AFF C250からAFF C30システムへ • AFF A70からAFF A90システムへ	コントローラ モジュールの交換
その他のコントローラのアップグレードの組み合わせ	その他すべてのアップグレード

コントローラから外付けシェルフへの変換

元のMetroCluster IPコントローラがAFF A150モデルまたはAFF A220モデルの場合は、AFF A150またはAFF A220のHAペアをDS224Cドライブシェルフに変換して、新しいノードに接続できます。

たとえば、AFF A150またはAFF A220システムからAFF A20システムにアップグレードする場合、AFF A150またはAFF A220のコントローラモジュールをIOM12モジュールと交換することで、AFF A150またはAFF A220のHAペアをDS224Cシェルフに変換できます。

手順

a. IOM12シェルフモジュールで変換するノードのコントローラモジュールを交換します。

   "Hardware Universe"

b. ドライブシェルフ ID を設定します。

   シャーシを含む各ドライブシェルフには、一意の ID が必要です。

c. 必要に応じて、他のドライブシェルフ ID をリセットします。

d. シェルフの電源をオフにします。

e. 変換したドライブシェルフを新しいシステムの SAS ポートに接続し、アウトオブバンド ACP ケーブルを使用している場合は新しいノードの ACP ポートに接続します。

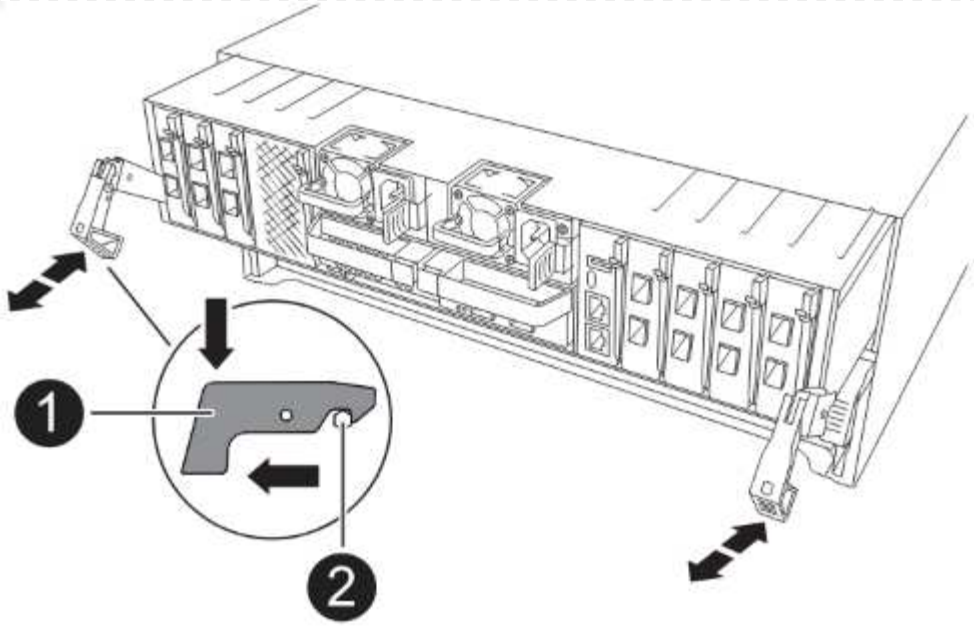
f. 変換したドライブシェルフおよび新しいノードに接続されているその他のドライブシェルフの電源をオンにします。

g. 新しいノードの電源をオンにしてから、各ノードで Ctrl+C キーを押してブートプロセスを中断し、ブート環境プロンプトにアクセスします。

コントローラ モジュールの交換

ディスクとコントローラを同じシャーシに搭載した統合システム（AFF A800システムからAFF A90システムなど）をアップグレードする場合、新しいコントローラを別 々 に設置することはできません。古いコントローラの電源をオフにしたあと、次の図に示すように、新しいコントローラモジュールとI/Oカードを交換する必要があります。

次の図の例は表示用です。コントローラモジュールとI/Oカードはシステムによって異なります。



その他すべてのアップグレード

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。

5. の説明に従って、コントローラの電源、シリアルコンソール、および管理接続をケーブル接続しますMetroCluster IP スイッチをケーブル接続します。

   この時点では、古いコントローラから取り外した他のケーブルは接続しないでください。

   ONTAPハードウェアシステムのドキュメント

6. 新しいノードの電源をオンにして、メンテナンスモードでブートします。

次の手順

HBA構成をリストアしてHAの状態を設定です。

HBA構成をリストアし、**MetroCluster IP**コントローラとシャーシの**HA**状態を設定

コントローラモジュールでHBAカードを設定し、コントローラとシャーシのHAの状態を確認および設定します。

HBA 構成をリストア

コントローラモジュールでのHBAカードの有無と設定に応じて、サイトに合わせてHBAカードを正しく設定する必要があります。

手順

1. メンテナンスモードで、システムのHBAを設定します。

   a. ucadmin show と入力し、各ポートの現在の設定を確認します

   b. 必要に応じてポートの設定を更新します。

HBA のタイプと目的のモード	使用するコマンド
CNA FC	`ucadmin modify -m fc -t initiator <adapter-name>`
CNA イーサネット	`ucadmin modify -mode cna <adapter-name>`
FC ターゲット	`fcadmin config -t target <adapter-name>`
FC イニシエータ	`fcadmin config -t initiator <adapter-name>`

2. メンテナンスモードを終了します。

   「 halt 」

   コマンドの実行後、ノードがプロンプトで停止するまで待ちます `LOADER` 。

3. ノードをブートしてメンテナンスモードに戻り、設定の変更を適用します。

   「 boot_ontap maint 」を使用してください

4. 変更を確認します。

HBA のタイプ	使用するコマンド
CNA	ucadmin show
FC	fcadmin show`

新しいコントローラとシャーシで **HA** 状態を設定

コントローラとシャーシの HA 状態を確認し、必要に応じてシステム構成に合わせて更新する必要があります。

手順

1. メンテナンスモードで、コントローラモジュールとシャーシの HA 状態を表示します。

   「 ha-config show 」

   すべてのコンポーネントの HA 状態は「 mccip 」である必要があります。

2. 表示されたコントローラまたはシャーシのシステム状態が正しくない場合は、HAの状態を設定します。

   「 ha-config modify controller mccip 」を参照してください

   「 ha-config modify chassis mccip 」を参照してください

3. NS224シェルフまたはストレージスイッチに接続されているイーサネットポートを確認および変更します。

   a. NS224シェルフまたはストレージスイッチに接続されているイーサネットポートを確認します。

      ```
      storage port show
      ```

   b. イーサネットシェルフまたはストレージスイッチに接続されているすべてのイーサネットポート（ストレージとクラスタの共有スイッチを含む）をモードに設定し `storage` ます。

      ```
      storage port modify -p <port> -m storage
      ```

      例：

      ```
      *> storage port modify -p e5b -m storage
      Changing NVMe-oF port e5b to storage mode
      ```

      アップグレードを成功させるには、影響を受けるすべてのポートでこの値を設定する必要があります。

      イーサネットポートに接続されているシェルフのディスクが出力に報告され `sysconfig -v` ます。

   アップグレード先のシステムのストレージポートについては、を参照して "Hardware Universe" ください。

   a. モードが設定されていることを確認し `storage` 、ポートがonline状態であることを確認します。

      ```
      storage port show
      ```

4. ノードを停止します

   ノードは 'loader>` プロンプトで停止する必要があります

5. 各ノードで、システムの日付、時刻、およびタイムゾーンを確認します。「 show date 」
6. 必要に応じて 'UTC または GMT:'set date <mm/dd/yyyy>' で日付を設定します
7. ブート環境プロンプトで次のコマンドを使用して ' 時刻を確認します
8. 必要に応じて、時刻を UTC または GMT:' 設定時刻 <:hh:mm:ss>` で設定します
9. 設定を保存します： saveenv
10. 環境変数 :printenv' を収集します

新しいコントローラのシャーシから内部ドライブを取り外します

外部ドライブのみを備えたシステムから外部ドライブと内部ドライブ (同じシャーシ内のディスクとコントローラ) を備えたシステムにアップグレードする場合は、アップグレードが完了するまで、新しいシステムからすべての内部ドライブを取り外すか、取り外す必要があります。

このタスクは、影響を受けるシステムでコントローラーを正常にアップグレードするために必須です。

、新しいシステムから内部ドライブを取り外す必要があります。

このタスクを完了すると、内部ドライブにアクセスできなくなります。手順の後半で、新しいコントローラにドライブを追加します。

次の手順

"スイッチのRCFを更新し、MetroCluster IPのbootarg値を設定"です。

スイッチの**RCF**を更新し、**MetroCluster IP**の**bootarg**値を設定

新しいプラットフォーム用のスイッチリファレンス構成ファイル（RCF）を更新し、コントローラモジュールでMetroCluster IP bootargの値を設定します。

新しいプラットフォームに合わせてスイッチの**RCF**を更新

スイッチは、新しいプラットフォームモデルをサポートする構成に更新する必要があります。

このタスクについて

このタスクは、現在アップグレード中のコントローラを含むサイトで実行します。この手順の例では、まず site_B をアップグレードします。

site_A のコントローラをアップグレードすると、 site_A のスイッチがアップグレードされます。

手順

1. IPスイッチで新しいRCFを適用できるように準備します。

   スイッチベンダーに対応するセクションを参照してください。

   - "Broadcom IP スイッチを工場出荷時のデフォルトにリセットします"
   - "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"
   - "NVIDIA IP SN2100スイッチを工場出荷時のデフォルトにリセット"
2. RCFをダウンロードしてインストールします。

   スイッチベンダーに対応するセクションを参照してください。

   - "Broadcom RCFのダウンロードとインストール"
   - "Cisco IP RCFのダウンロードとインストール"
   - "NVIDIA IP RCFのダウンロードとインストール"

MetroCluster の **bootarg IP** 変数を設定します

新しいコントローラモジュールでは、特定のMetroCluster IP bootarg値を設定する必要があります。bootargの値は、古いコントローラモジュールで設定されている値と同じである必要があります。

このタスクについて

- のアップグレード手順で特定したUUIDとシステムIDを使用します"アップグレード前に情報を収集"。
- プラットフォームモデルに応じて、パラメータを使用してVLAN IDを指定できます `-vlan-id`。次のプラットフォームでは、パラメータはサポートされません `-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、パラメータがサポートされ `-vlan-id` ます。
- 設定するMetroClusterのbootargの値は、新しいシステムで共有のクラスタ/ HAポートを使用するか、共有のMetroCluster / HAポートを使用するかによって異なります。

共有クラスタ/ **HA**ポート

次の表に示すシステムは、共有クラスタ/ HAポートを使用します。

AFFおよび**ASA**システム	**FAS**システム
• AFF A20用 • AFF A30用 • AFF C30 • AFF A50用 • AFF C60 • AFF C80用 • AFF A70用 • AFF A90用 • AFF A1K用	• FAS50 • FAS70 • FAS90

共有**MetroCluster / HA**ポート

次の表に示すシステムは、共有MetroCluster / HAポートを使用します。

AFFおよび**ASA**システム	**FAS**システム
• AFF A150、ASA A150向け • AFF A220 • AFF C250、ASA C250向け • AFF A250、ASA A250向け • AFF A300 • AFF A320 • AFF C400、ASA C400向け • AFF A400、ASA A400向け • AFF A700 • AFF C800、ASA C800向け • AFF A800、ASA A800向け • AFF A900、ASA A900向け	• FAS2750 • FAS500f • FAS8200 • FAS8300 • FAS8700 の場合 • FAS9000 • FAS9500

手順

1. 「 LOADER> 」プロンプトで、 site_B の新しいノードで次のブート引数を設定します。

   実行する手順は、新しいプラットフォームモデルで使用するポートによって異なります。

共有クラスタ/ **HA**ポートを使用するシステム

a. 次のbootargを設定します。

```
setenv bootarg.mcc.port_a_ip_config <local-IP-address/local-IP-
mask,0,0,DR-partner-IP-address,DR-aux-partnerIP-address,vlan-id>

setenv bootarg.mcc.port_b_ip_config <local-IP-address/local-IP-
mask,0,0,DR-partner-IP-address,DR-aux-partnerIP-address,vlan-id>
```

インターフェイスがデフォルトのVLAN IDを使用している場合、 `vlan-id`パラメータは必要ありません。

次の例は、1つ目のネットワークにVLAN 120、2つ目のネットワークにVLAN 130を使用して、node_B_1-newの値を設定します。

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,0,172.17.26.13,172.17.26.12,120
setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,0,172.17.27.13,172.17.27.12,130
```

次の例は、1つ目のネットワークにVLAN 120、2つ目のネットワークにVLAN 130を使用して、node_B_2-newの値を設定します。

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.11/23,0,0,172.17.26.12,172.17.26.13,120
setenv bootarg.mcc.port_b_ip_config
172.17.27.11/23,0,0,172.17.27.12,172.17.27.13,130
```

次の例は、すべてのMetroCluster IP DR接続にデフォルトのVLANを使用してnode_B_1-newの値を設定します。

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,0,172.17.26.13,172.17.26.12
setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,0,172.17.27.13,172.17.27.12
```

次の例は、すべてのMetroCluster IP DR接続にデフォルトのVLANを使用してnode_B_2-newの値を設定します。

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.11/23,0,0,172.17.26.12,172.17.26.13
setenv bootarg.mcc.port_b_ip_config
172.17.27.11/23,0,0,172.17.27.12,172.17.27.13
```

共有**MetroCluster / HA**ポートを使用するシステム

a. 次のbootargを設定します。

```
setenv bootarg.mcc.port_a_ip_config <local-IP-address/local-IP-
mask,0,HA-partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-
address,vlan-id>

setenv bootarg.mcc.port_b_ip_config <local-IP-address/local-IP-
mask,0,HA-partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-
address,vlan-id>
```



インターフェイスがデフォルトのVLAN IDを使用している場合、 `vlan-id`パラメータは必要ありません。

次の例は、1つ目のネットワークにVLAN 120、2つ目のネットワークにVLAN 130を使用して、node_B_1-newの値を設定します。

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12,120
setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12,130
```

次の例は、1つ目のネットワークにVLAN 120、2つ目のネットワークにVLAN 130を使用して、node_B_2-newの値を設定します。

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.11/23,0,172.17.26.10,172.17.26.12,172.17.26.13,120
setenv bootarg.mcc.port_b_ip_config
172.17.27.11/23,0,172.17.27.10,172.17.27.12,172.17.27.13,130
```

次の例は、すべてのMetroCluster IP DR接続にデフォルトのVLANを使用してnode_B_1-newの値を設定します。

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12
setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12
```

次の例は、すべてのMetroCluster IP DR接続にデフォルトのVLANを使用してnode_B_2-newの値を設定します。

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.11/23,0,172.17.26.10,172.17.26.12,172.17.26.13
setenv bootarg.mcc.port_b_ip_config
172.17.27.11/23,0,172.17.27.10,172.17.27.12,172.17.27.13
```

2. 新しいノードの LOADER プロンプトで、 UUID を設定します。

```
setenv bootarg.mgwd.partner_cluster_uuid <partner-cluster-UUID>

setenv bootarg.mgwd.cluster_uuid <local-cluster-UUID>

setenv bootarg.mcc.pri_partner_uuid <DR-partner-node-UUID>

setenv bootarg.mcc.aux_partner_uuid <DR-aux-partner-node-UUID>

setenv bootarg.mcc_iscsi.node_uuid <local-node-UUID>
```

   a. node_B_1-newのUUIDを設定します。

      次の例は、 node_B_1 で新規の UUID を設定するコマンドを示しています。

```
setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039
setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.pri_partner_uuid f37b240b-9ac1-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.aux_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-
00a098ca379f
setenv bootarg.mcc_iscsi.node_uuid f03cb63c-9a7e-11e7-b68b-
00a098908039
```

   b. node_B_2 の UUID を設定します。 new ：

      次の例は、 node_B_2 の UUID を設定するコマンドを示しています。

```
setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039
setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.pri_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
setenv bootarg.mcc.aux_partner_uuid f37b240b-9ac1-11e7-9b42-00a098c9e55d
setenv bootarg.mcc_iscsi.node_uuid aa9a7a7a-9a81-11e7-a4e9-00a098908c35
```

3. 稼働しているサイトで次のコマンドを実行して、元のシステムがアドバンストドライブパーティショニング（ADP）用に設定されているかどうかを確認します。

   「ディスクショー」

   ADPが設定されている場合、出力に「container type」列に「shared」と表示されます `disk show` 。「container type」にそれ以外の値が指定されている場合、ADPはシステムで設定されていません。次の出力例は、ADPが設定されたシステムを示しています。

```
::> 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".
---------------    ---------- ----- --- ------- ----------- ---------
--------
1.11.0              894.0GB    11    0   SSD      shared     testaggr
node_A_1
1.11.1              894.0GB    11    1   SSD      shared     testaggr
node_A_1
1.11.2              894.0GB    11    2   SSD      shared     testaggr
node_A_1
```

4. 元のシステムでADP用にパーティショニングされたディスクが設定されていた場合は、各交換用ノードのプロンプトで有効にし `LOADER` ます。

   'etenv bootarg.me.adp_enabled true

5. 次の変数を設定します。

```
setenv bootarg.mcc.local_config_id <original-sys-id>

setenv bootarg.mcc.dr_partner <dr-partner-sys-id>
```

   ⓘ 「 bootarg env.MCC.local_config_id` 」変数は、 * 元の * コントローラモジュール node_B_1 の sys-id に設定する必要があります。

   a. node_B_1 で変数を設定します。

      次の例は、 node_B_1 で新規の値を設定するコマンドを示しています。

```
setenv bootarg.mcc.local_config_id 537403322
setenv bootarg.mcc.dr_partner 537403324
```

b. node_B_2 の変数を設定します。

次の例は、 node_B_2 の値を設定するコマンドを示しています。

```
setenv bootarg.mcc.local_config_id 537403321
setenv bootarg.mcc.dr_partner 537403323
```

6. 外部キー管理ツールで暗号化を使用する場合は、必要な bootargs を設定します。

「 etenv bootarg.kmip.init.ipaddr` 」を参照してください

「 etenv bootarg.kmip.kmip.init.netmask` 」を参照してください

「 etenv bootarg.kmip.kmip.init.gateway` 」を参照してください

「 etenv bootarg.kmip.kmip.init.interface` 」を参照してください

次の手順

"ルートアグリゲートディスクを再割り当て"です。

ルートアグリゲートディスクを新しい**MetroCluster IP**コントローラモジュールに再割り当て

前の手順で確認したシステムIDを使用して、ルートアグリゲートディスクを新しいコントローラモジュールに再割り当てします。

このタスクについて

古いシステムIDはで特定しました "アップグレード前に情報を収集"。

この手順はメンテナンスモードで実行します。

コントローラのアップグレードプロセスで再割り当てが必要なディスクは、ルートアグリゲートディスクだけです。データアグリゲートのディスク所有権は、スイッチオーバー/スイッチバック処理の一環として処理されます。

手順

1. システムをメンテナンスモードでブートします。

「 boot_ontap maint 」を使用してください

2. メンテナンスモードのプロンプトから node_B_1 で新しいディスクを表示します。

「ディスクショー - A` 」

ディスクの再割り当てを続行する前に、ノードのルートアグリゲートに属するpool0とpool1のディスクが出力に表示されていることを確認し `disk show`ます。次の例では、node_B_1-oldが所有するpool0とpool1のディスクが出力に表示されています。

コマンド出力には、新しいコントローラモジュールのシステムID（1574774970）が表示されます。ただ

し、古いシステムID（537403322）はルートアグリゲートディスクをまだ所有しています。この例には、MetroCluster構成の他のノードが所有するドライブは表示されていません。

```
*> disk show -a
Local System ID: 1574774970
DISK                  OWNER                  POOL   SERIAL NUMBER   HOME
DR HOME
------------          ---------              -----  -------------
-------------         -------------
prod3-rk18:9.126L44   node_B_1-old(537403322)  Pool1  PZHYN0MD
node_B_1-old(537403322)  node_B_1-old(537403322)
prod4-rk18:9.126L49   node_B_1-old(537403322)  Pool1  PPG3J5HA
node_B_1-old(537403322)  node_B_1-old(537403322)
prod4-rk18:8.126L21   node_B_1-old(537403322)  Pool1  PZHTDSZD
node_B_1-old(537403322)  node_B_1-old(537403322)
prod2-rk18:8.126L2    node_B_1-old(537403322)  Pool0  S0M1J2CF
node_B_1-old(537403322)  node_B_1-old(537403322)
prod2-rk18:8.126L3    node_B_1-old(537403322)  Pool0  S0M0CQM5
node_B_1-old(537403322)  node_B_1-old(537403322)
prod1-rk18:9.126L27   node_B_1-old(537403322)  Pool0  S0M1PSDW
node_B_1-old(537403322)  node_B_1-old(537403322)
.
.
.
```

3. ドライブシェルフのルートアグリゲートディスクを新しいコントローラに再割り当てします。

ADP を使用する環境	使用するコマンド
はい。	`disk reassign -s <old-sysid> -d <new-sysid> -r <dr-partner-sysid>`
いいえ	`disk reassign -s <old-sysid> -d <new-sysid>`

4. ドライブシェルフのルートアグリゲートディスクを新しいコントローラに再割り当てします。

   `disk reassign -s <old-sysid> -d <new-sysid>`

   次の例は、 ADP 以外の構成でのドライブの再割り当てを示しています。

```
*> disk reassign -s 537403322 -d 1574774970
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)? n

After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)? y
Disk ownership will be updated on all disks previously belonging to
Filer with sysid 537403322.
Do you want to continue (y/n)? y
```

5. ルートアグリゲートのディスクが正しく再割り当てされたことを確認します。

   「ディスクショー」

   「ストレージ・アグリゲートのステータス」

```
*> disk show
Local System ID: 537097247

  DISK                    OWNER                    POOL   SERIAL NUMBER
HOME                    DR HOME
------------             -------------            -----  -------------
-------------           -------------
prod03-rk18:8.126L18 node_B_1-new(537097247)  Pool1  PZHYN0MD
node_B_1-new(537097247)   node_B_1-new(537097247)
prod04-rk18:9.126L49 node_B_1-new(537097247)  Pool1  PPG3J5HA
node_B_1-new(537097247)   node_B_1-new(537097247)
prod04-rk18:8.126L21 node_B_1-new(537097247)  Pool1  PZHTDSZD
node_B_1-new(537097247)   node_B_1-new(537097247)
prod02-rk18:8.126L2  node_B_1-new(537097247)  Pool0  S0M1J2CF
node_B_1-new(537097247)   node_B_1-new(537097247)
prod02-rk18:9.126L29 node_B_1-new(537097247)  Pool0  S0M0CQM5
node_B_1-new(537097247)   node_B_1-new(537097247)
prod01-rk18:8.126L1  node_B_1-new(537097247)  Pool0  S0M1PSDW
node_B_1-new(537097247)   node_B_1-new(537097247)
::>
::> aggr status
           Aggr          State           Status                Options
aggr0_node_B_1           online          raid_dp, aggr         root,
nosnap=on,
                                         mirrored
mirror_resync_priority=high(fixed)
                                         fast zeroed
                                         64-bit
```

次の手順

"新しいコントローラをブートしてLIF設定をリストア"です。

新しい**MetroCluster IP**コントローラのブートと**LIF**設定のリストア

新しいコントローラをブートし、LIFが適切なノードとポートでホストされていることを確認します。

新しいコントローラのブート

新しいコントローラをブートする必要があります。 bootarg 変数が正しいことを確認し、必要に応じて暗号化のリカバリ手順を実行するように注意してください。

手順

1. 新しいノードを停止します。

「 halt 」

2. 外部キー管理ツールが設定されている場合は、関連する bootargs を設定します。

```
setenv bootarg.kmip.init.ipaddr <ip-address>

setenv bootarg.kmip.init.netmask <netmask>

setenv bootarg.kmip.init.gateway <gateway-addres>

setenv bootarg.kmip.init.interface <interface-id>
```

3. partner-sysid が現在のものかどうかを確認します。

   printenv partner-sysid

   partner-sysid が正しくない場合は、次のように設定します。

```
setenv partner-sysid <partner-sysID>
```

4. ONTAP ブートメニューを表示します。

   「 boot_ontap menu

5. ルート暗号化を使用する場合は、キー管理設定のブートメニューオプションを選択します。

使用するポート	選択するブートメニューオプション
オンボードキー管理	オプション 10 プロンプトに従って、キー管理ツールの構成をリカバリおよびリストアするために必要な入力を指定します。
外部キー管理	オプションは 11 です プロンプトに従って、キー管理ツールの構成をリカバリおよびリストアするために必要な入力を指定します。

6. 起動メニューから「 (6) Update flash from backup config 」を選択します。

   オプション6では、プロセスが完了する前にノードが2回リブートされます。

   システムIDの変更プロンプトに「y」と入力します。2回目のリブートメッセージが表示されるまで待ちます。

```
Successfully restored env file from boot media...

Rebooting to load the restored env file...
```

7. `LOADER`プロンプトで、bootargの値を確認し、必要に応じて値を更新します。

   の手順を使用します"MetroCluster の bootarg IP 変数を設定します"。

8. パートナーシステムIDが正しいことを確認します。

   printenv partner-sysid

   partner-sysid が正しくない場合は、次のように設定します。

   `setenv partner-sysid <partner-sysID>`

9. ルート暗号化を使用する場合は、キー管理設定のブートメニューオプションを再度選択します。

使用するポート	選択するブートメニューオプション
オンボードキー管理	オプション 10 プロンプトに従って、キー管理ツールの構成をリカバリおよびリストアするために必要な入力を指定します。
外部キー管理	オプション "11`" プロンプトに従って、キー管理ツールの構成をリカバリおよびリストアするために必要な入力を指定します。

   キー・マネージャの設定に応じて '10 またはオプション 11 を選択し ' 最初のブート・メニュー・プロンプトでオプション 6 を選択して 'Recovery 手順を実行しますノードを完全にブートするには ' オプション "1" によって続行されるリカバリ手順 (通常のブート) を繰り返す必要がある場合があります

10. 交換したノードがブートするまで待ちます。

    いずれかのノードがテイクオーバーモードの場合は、「 storage failover giveback 」コマンドを使用してギブバックを実行します。

11. 暗号化を使用する場合は、キー管理設定に対応したコマンドを使用してキーをリストアします。

使用するポート	使用するコマンド
オンボードキー管理	「セキュリティキーマネージャオンボード同期」 詳細については、を参照してください "オンボードキー管理暗号化キーのリストア"。

外部キー管理	`security key-manager external restore -vserver <SVM> -node <node> -key-server <host_name

12. すべてのポートがブロードキャストドメインに属していることを確認します。

    a. ブロードキャストドメインを表示します。

       「 network port broadcast-domain show 」

    b. 新しくアップグレードしたコントローラのデータポート用に新しいブロードキャストドメインを作成する場合は、そのブロードキャストドメインを削除します。

       新しいブロードキャストドメインだけを削除します。アップグレードの開始前に存在していたブロードキャストドメインは削除しないでください。

       ```
       broadcast-domain delete -broadcast-domain <broadcast_domain_name>
       ```

    c. 必要に応じてブロードキャストドメインにポートを追加します。

       "ブロードキャストドメインのポートを追加または削除します"

    d. 必要に応じて、 VLAN とインターフェイスグループを再作成します。

       VLANおよびインターフェイスグループのメンバーシップは、古いノードと異なる場合があります。

       "VLANを作成します。"

"物理ポートを組み合わせてインターフェイスグループを作成"

LIF の設定を確認してリストア

アップグレード手順の開始時にマッピングされた適切なノードとポートで LIF がホストされていることを確認します。

このタスクについて

- このタスクは site_B で実行します
- で作成したポートマッピング計画を確認します"古いノードから新しいノードへのポートのマッピング"。

スイッチバックを実行する前に、新しいノードでデータLIFの場所が正しいことを確認する必要があります。構成をスイッチバックすると、ONTAPはLIFで使用されているホームポートでトラフィックの再開を試みます。スイッチポートおよびVLANへのホームポート接続が正しくないと、I/O障害が発生する可能性があります。

手順

1. スイッチバックの前に、LIFが適切なノードとポートでホストされていることを確認します。

    a. advanced 権限レベルに切り替えます。

       「 advanced 」の権限が必要です

b. LIFを表示し、各データLIFが正しいホームポートを使用していることを確認します。

「 network interface show 」を参照してください

c. 正しいホームポートを使用していないLIFを変更します。

```
network interface modify -vserver <svm-name> -lif <data-lif> -home-port
<port-id>
```

コマンドからエラーが返された場合は、ポート設定を上書きできます。

```
vserver config override -command "network interface modify -vserver <svm-
name> -home-port <active_port_after_upgrade> -lif <lif_name> -home-node
<new_node_name>"
```

vserver config override コマンドで network interface modify コマンドを入力した場合は、 tab autoccomplete 機能を使用することはできません。autoccomplete を使用してネットワーク 'interface modify' を作成してから 'vserver config override' コマンドで囲むことができます

a. すべてのデータLIFが正しいホームポートにあることを確認します。

「 network interface show 」を参照してください

b. admin 権限レベルに戻ります。

「特権管理者」

2. インターフェイスをホームノードにリバートします。

```
network interface revert * -vserver <svm-name>
```

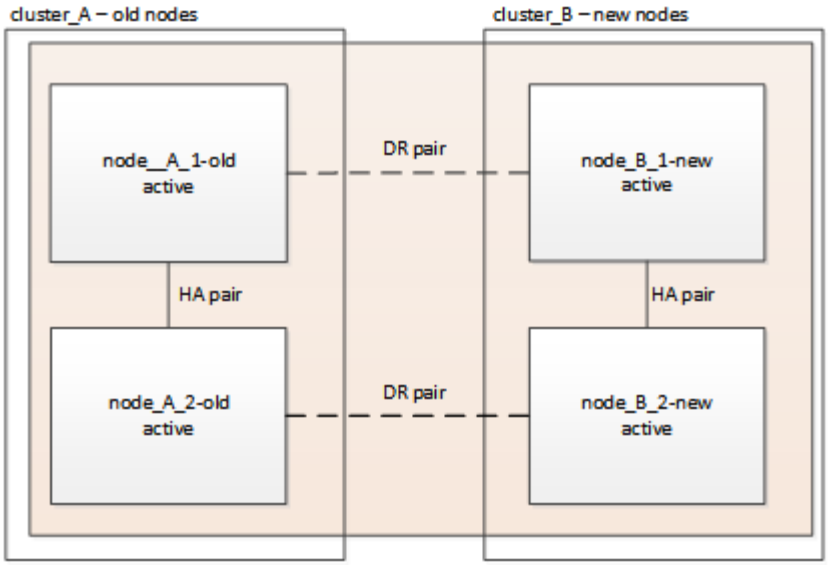
必要に応じて、すべての SVM でこの手順を実行します。

次の手順

"MetroCluster構成のスイッチバック"です。

MetroCluster IP構成をスイッチバックします。

スイッチバック処理を実行してMetroCluster構成を通常動作に戻します。site_Aのノードはまだアップグレード待ちです。



手順

1. site_B の MetroCluster node show コマンドを問題し ' 出力を確認します
   a. 新しいノードが正しく表示されることを確認します。
   b. 新しいノードの状態が「 Waiting for switchback 」であることを確認します。
2. アクティブなクラスタ（アップグレードを実行していないクラスタ）の任意のノードから必要なコマンドを実行して、修復とスイッチバックを実行します。
   a. データアグリゲートを修復します。 + MetroCluster heal aggregates `
   b. ルートアグリゲートを修復します。

      MetroCluster はルートを修復します

   c. クラスタをスイッチバックします。

      MetroCluster スイッチバック

3. スイッチバック処理の進捗を確認します。

   「 MetroCluster show 」

   出力に「 waiting-for-switchback 」と表示されたら、スイッチバック処理はまだ進行中です。

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                switchover
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                waiting-for-switchback
                          AUSO Failure Domain -
```

出力に normal と表示された場合、スイッチバック処理は完了しています。

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
```

スイッチバックが完了するまでに時間がかかる場合は、「 MetroCluster config-replication resync-status show 」コマンドを使用することで、進行中のベースラインのステータスを確認できます。このコマンドは、 advanced 権限レベルで実行します。

次の手順

"アップグレードを完了します"です。

MetroCluster IPコントローラのアップグレードの完了

コントローラモジュールをアップグレードしたら、必要なタスクを実行してコントローラのアップグレードを完了します。

MetroCluster 構成の健全性を確認します

コントローラモジュールをアップグレードしたら、 MetroCluster 構成の健全性を確認する必要があります。

このタスクについて

このタスクは、MetroCluster構成の任意のノードで実行できます。

手順

1. MetroCluster 構成の動作を確認します。
   a. MetroCluster 構成と動作モードが正常であることを確認します。 + MetroCluster show `
   b. MetroCluster チェックを実行します + MetroCluster チェックを実行します
   c. MetroCluster チェックの結果を表示します。

      MetroCluster チェックショー
2. MetroCluster の接続およびステータスを確認します。
   a. MetroCluster IP 接続を確認します。

      「 storage iscsi-initiator show 」のように表示されます
   b. ノードが動作していることを確認します。

MetroCluster node show

c. MetroCluster IP インターフェイスが動作していることを確認します。

「 MetroCluster configurion-settings interface show 」を参照してください

d. ローカルフェイルオーバーが有効になっていることを確認します。

「 storage failover show 」をクリックします

cluster_Aのノードをアップグレードします。

アップグレード手順を繰り返して、サイトAのcluster_Aのノードをアップグレードする必要があります。

手順

1. cluster_Aのノードをアップグレードするために、上記の手順を繰り返し"アップグレードを準備"ます。

   手順を繰り返すと、クラスターとノードへの参照がすべて逆になります。例えば、cluster_Aからのスイッチオーバーの例は、cluster_Bからのスイッチオーバーになります。

新しいコントローラに内部ドライブを再度追加します

外付けドライブのみを搭載したシステムから、外付けドライブと内蔵ドライブ（ディスクとコントローラが同一シャーシ内）を搭載したシステムにアップグレードした場合、新しいシステムの内部スロットから取り外したディスクを追加または再装着できます。これは、両サイトでアップグレードが完了し、クラスタが正常な状態になった後であればいつでも実行できます。

ドライブを再度追加または再装着すると、必要に応じてONTAPで使用できるようになります。

このタスクは、特定のアップグレードの組み合わせにのみ適用されます。詳細については、を参照してください "新しいコントローラのシャーシから内部ドライブを取り外す" 。

Tiebreaker またはメディエーターの監視をリストアします

MetroCluster 構成のアップグレードが完了したら、 Tiebreaker またはメディエーターユーティリティを使用して監視を再開できます。

手順

1. 必要に応じて、構成に応じて手順を使用してリストアを監視します。

使用するポート	この手順を使用します
Tiebreaker	"MetroCluster 構成を追加"。
メディエーター	"MetroCluster IP構成からONTAPメディエーターを構成する"です。
サードパーティ製アプリケーション	製品マニュアルを参照してください。

カスタム **AutoSupport** メッセージをメンテナンス後に送信します

アップグレードの完了後、ケースの自動作成を再開できるように、メンテナンスの終了を通知するAutoSupport メッセージを送信する必要があります。

手順

1. サポートケースの自動生成を再開するには、メンテナンスが完了したことを示す AutoSupport メッセージを送信します。
   a. 次のコマンドを問題で実行します。 + 「 system node AutoSupport invoke -node * -type all -message MAINT= end 」
   b. パートナークラスタに対してこのコマンドを繰り返します。

エンドツーエンドの暗号化を設定する

ご使用のシステムでサポートされている場合は、MetroCluster IP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。を参照してください "エンドツーエンドの暗号化を設定する" を参照してください。

スイッチオーバーとスイッチバックを使用して、MetroCluster IP構成のAFF A700 / FAS9000からAFF A900 / FAS9500にコントローラをアップグレードする（ONTAP 9.10.1以降）

MetroCluster スイッチオーバー処理を使用すると、パートナークラスタのコントローラモジュールのアップグレード中もクライアントに無停止でサービスを提供できます。この手順の一部として他のコンポーネント（ストレージシェルフやスイッチなど）をアップグレードすることはできません。

このタスクについて

- AFF A700コントローラモジュールをAFF A900にアップグレードするには、コントローラでONTAP 9.10.1以降が実行されている必要があります。
- FAS9000コントローラモジュールをFAS9500にアップグレードするには、コントローラでONTAP 9.10.1P3以降が実行されている必要があります。
- 構成内のすべてのコントローラは、同じメンテナンス期間にアップグレードする必要があります。

  AFF A700とAFF A900、またはFAS9000とFAS9500コントローラを使用したMetroCluster 構成の運用は、この保守作業の外部ではサポートされません。
- サポートされているファームウェアバージョンが IP スイッチで実行されている必要があります。
- 元のプラットフォームの IP アドレス、ネットマスク、ゲートウェイを新しいプラットフォームで再利用します。
- この手順 では、例と図の両方で次の名前が使用されています。
  - site_A
    - アップグレード前：
      - node_A_1 - A700

        - Node_a_2-A700
    - アップグレード後：
        - node_A_1 - A900
        - Node_a_2-A900
- site_B
    - アップグレード前：
        - node_B_1 - A700
        - node_B_2 - A700
    - アップグレード後：
        - Node_B_1-A900
        - node_B_2 - A900

コンソールログを有効にする

NetAppでは、使用しているデバイスでコンソールロギングをイネーブルにし、この手順を実行する際に次のアクションを実行することを強く推奨します。

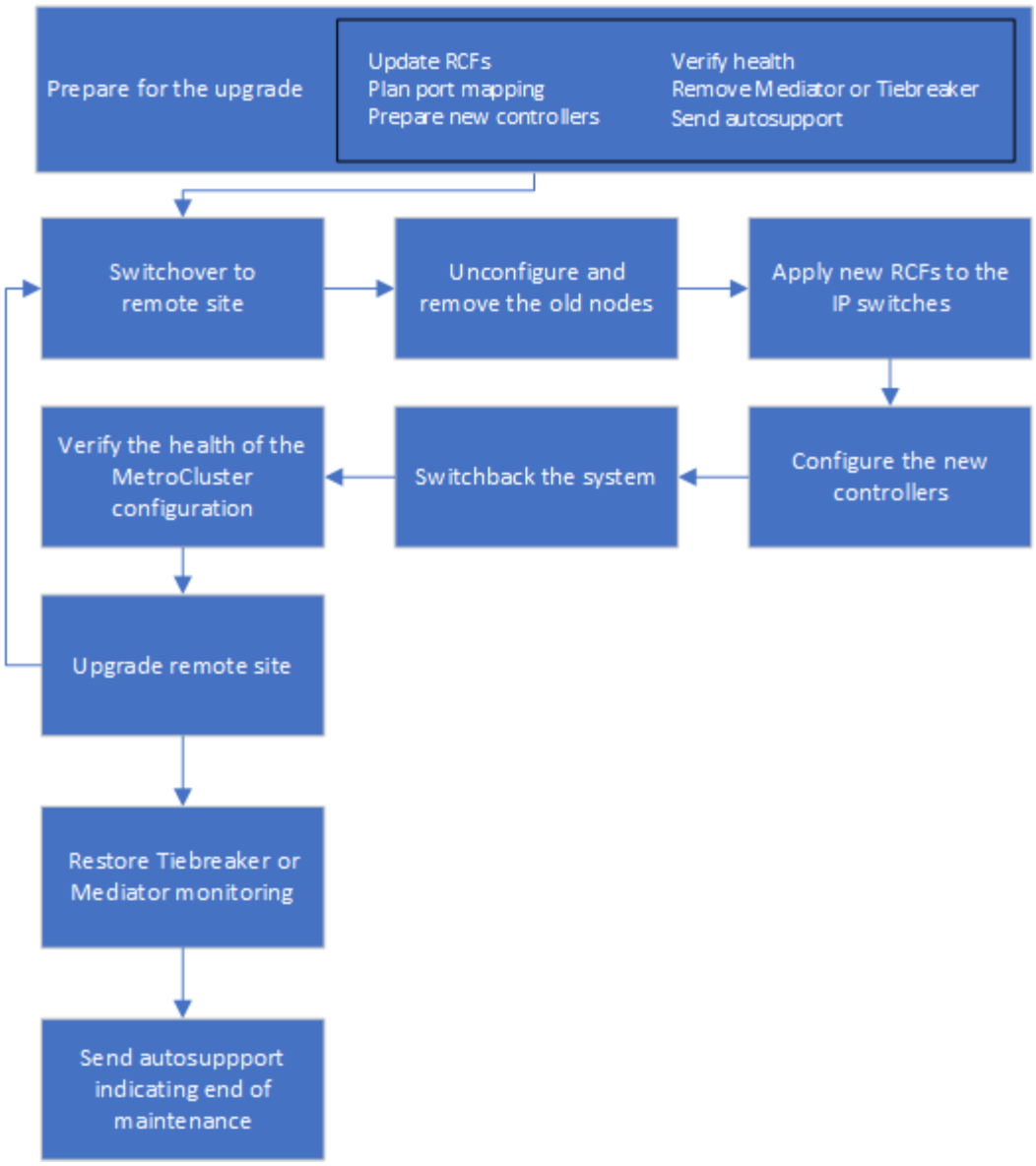
- メンテナンス中はAutoSupportを有効のままにします。
- メンテナンスの前後にメンテナンスAutoSupportメッセージをトリガーして、メンテナンスアクティビティ中にケースの作成を無効にします。

  ナレッジベースの記事を参照してください "スケジュールされたメンテナンス時間中にケースの自動作成を停止する方法"。

- 任意のCLIセッションのセッションロギングをイネーブルにします。セッションログを有効にする方法については、ナレッジベースの記事の「セッション出力のログ」セクションを参照してください "ONTAPシステムへの接続を最適化するためのPuTTYの設定方法"。

MetroCluster IP 構成のコントローラをアップグレードするためのワークフロー

ワークフロー図は、アップグレードタスクを計画する際に役立ちます。



アップグレードを準備

既存の MetroCluster 構成に変更を加える前に、構成の健全性を確認し、新しいプラットフォームを準備し、その他のタスクを実行する必要があります。

AFF A700または**FAS9000**コントローラのスロット**7**をクリアします

AFF A900またはFAS9500のMetroCluster 構成では、スロット5と7にあるDRカードの各ポートのいずれかが使用されます。アップグレードを開始する前に、AFF A700またはFAS9000のスロット7にカードがある場合は、それらをクラスタのすべてのノード用の他のスロットに移動する必要があります。

コントローラをアップグレードする前に、 **MetroCluster** スイッチの **RCF** ファイルを更新してください

このアップグレードを実行するときは、MetroCluster スイッチでRCFファイルを更新する必要があります。次の表に、AFF A900/FAS9500 MetroCluster IP構成でサポートされるVLAN範囲を示します。

プラットフォームモデル	サポートされる VLAN ID

• AFF A900またはFAS9500	• 10. • 20 • 101 ~ 4096 の範囲の任意の値。

- サポートされている最小バージョンの RCF ファイルがスイッチに設定されていない場合は、 RCF ファイルを更新する必要があります。使用しているスイッチモデルに対応した正しい RCF ファイルバージョンについては、を参照してください "RcfFileGenerator ツール"。次に、 RCF ファイルアプリケーションの手順を示します。

手順

1. 新しい RCF ファイルを適用するための IP スイッチを準備します。

   スイッチベンダーに対応するセクションを参照してください。

   - "Broadcom IP スイッチを工場出荷時のデフォルトにリセットします"
   - "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"
   - "NVIDIA IPスイッチを工場出荷時のデフォルトにリセット"

2. RCF ファイルをダウンロードしてインストールします。

   スイッチベンダーに対応するセクションを参照してください。

   - "BroadcomのRCFファイルをダウンロードしてインストールする"
   - "Cisco IP RCFファイルのダウンロードとインストール"
   - "NVIDIA IP RCFファイルのダウンロードとインストール"

古いノードから新しいノードへのポートのマッピング

AFF A700からAFF A900またはFAS9000からFAS9500にアップグレードした場合、データネットワークポート、FCP SANアダプタポート、SASストレージポートとNVMeストレージポートは変更されません。データ LIF は、アップグレード中もアップグレード後もそのままの状態になります。そのため、古いノードのネットワークポートを新しいノードにマッピングする必要はありません。

サイトをアップグレードする前に **MetroCluster** の健全性を確認

アップグレードを実行する前に、MetroCluster 構成の健全性と接続性を確認します。

> 最初のサイトでコントローラをアップグレードした後、2番目のサイトをアップグレードする前に、 `metrocluster check run`に続く `metrocluster check show`エラーを返します `config-replication`フィールド。このエラーは、各サイトのノード間でNVRAMのサイズが一致していないことを示しています。これは、両サイトで異なるプラットフォームモデルが存在する場合に想定される動作です。DRグループ内のすべてのノードでコントローラーのアップグレードが完了するまで、このエラーは無視できます。

手順

1. ONTAP で MetroCluster 構成の動作を確認します。

a. ノードがマルチパスであるかどうかを確認します。 +node run -node node_name sysconfig -a

このコマンドは、 MetroCluster 構成のノードごとに問題で実行する必要があります。

b. 「 storage disk show -broken 」の構成に破損ディスクがないことを確認してください

このコマンドは、 MetroCluster 構成の各ノードで問題を実行する必要があります。

c. ヘルスアラートがないかどうかを確認します。

「 system health alert show 」というメッセージが表示されます

このコマンドは、各クラスタで問題を実行する必要があります。

d. クラスタのライセンスを確認します。

「 system license show 」を参照してください

このコマンドは、各クラスタで問題を実行する必要があります。

e. ノードに接続されているデバイスを確認します。

「 network device-discovery show 」のように表示されます

このコマンドは、各クラスタで問題を実行する必要があります。

f. 両方のサイトでタイムゾーンと時間が正しく設定されていることを確認します。

cluster date show

このコマンドは、各クラスタで問題を実行する必要があります。時刻とタイムゾーンを設定するには 'cluster date コマンドを使用します

2. MetroCluster 構成の運用モードを確認し、 MetroCluster チェックを実行
   a. MetroCluster の構成と動作モードが「 normal 」であることを確認します。 + MetroCluster show
   b. 想定されるすべてのノードが表示されることを確認します。 + MetroCluster node show `
   c. 次のコマンドを問題に設定します。

「 MetroCluster check run 」のようになります

   d. MetroCluster チェックの結果を表示します。

MetroCluster チェックショー

3. Config Advisor ツールを使用して MetroCluster のケーブル接続を確認します。
   a. Config Advisor をダウンロードして実行します。

"ネットアップのダウンロード： Config Advisor"

   b. Config Advisor の実行後、ツールの出力を確認し、推奨される方法で検出された問題に対処します。

アップグレード前に情報を収集

アップグレードの開始前に各ノードについて情報を収集し、必要に応じてネットワークブロードキャストドメインを調整し、 VLAN やインターフェイスグループを削除して、暗号化情報を収集する必要があります。

手順

1. 各ノードの物理的なケーブル接続をメモし、必要に応じてケーブルにラベルを付けて新しいノードを正しくケーブル接続できるようにします。
2. ノードごとに次のコマンドの出力を収集します。
   - MetroCluster interconnect show
   - 「 MetroCluster configurion-settings connection show 」を参照してください
   - 'network interface show -role cluster, node-mgmt
   - network port show -node node_name -type physical
   - 'network port vlan show -node -node-name _`
   - 「 network port ifgrp show -node node_name 」 - instance 」を指定します
   - 「 network port broadcast-domain show 」
   - 「 network port reachability show-detail` 」と表示されます
   - network ipspace show
   - volume show
   - 「 storage aggregate show
   - 「 system node run -node _node-name_sysconfig -a 」のように入力します
   - 「 vserver fcp initiator show 」のように表示されます
   - 「 storage disk show 」を参照してください
   - 「 MetroCluster configurion-settings interface show 」を参照してください
3. site_B （プラットフォームが現在アップグレード中のサイト）の UUID を収集します。 MetroCluster node show -fields node-cluster.uuid 、 node-uuid

   アップグレードを正常に実行するには、新しい site_B のコントローラモジュールでこれらの値を正確に設定する必要があります。あとでアップグレードプロセスの適切なコマンドに値をコピーできるように、ファイルに値をコピーします。+ 次の例は、 UUID を指定したコマンドの出力を示しています。

```
cluster_B::> metrocluster node show -fields node-cluster-uuid, node-uuid
   (metrocluster node show)
dr-group-id cluster     node   node-uuid
node-cluster-uuid
----------- --------- -------- ------------------------------------
------------------------------
1           cluster_A node_A_1-A700 f03cb63c-9a7e-11e7-b68b-00a098908039
ee7db9d5-9a82-11e7-b68b-00a098908039
1           cluster_A node_A_2-A700 aa9a7a7a-9a81-11e7-a4e9-00a098908c35
ee7db9d5-9a82-11e7-b68b-00a098908039
1           cluster_B node_B_1-A700 f37b240b-9ac1-11e7-9b42-00a098c9e55d
07958819-9ac6-11e7-9b42-00a098c9e55d
1           cluster_B node_B_2-A700 bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
07958819-9ac6-11e7-9b42-00a098c9e55d
4 entries were displayed.
cluster_B::*
```

UUID を次のようなテーブルに記録することを推奨します。

クラスタまたはノード	UUID
cluster_B	07958819 - 9ac6-11e7-9b42 - 00a098c9e55d
node_B_1 - A700	f37b240b-9ac1-11e7-9b42 -00a098c9e55d
node_B_2 - A700	bf8e3f8f-9ac4-117-bd4e-00a098c379f です
cluster_A	ee7db9d5-9a82-11e7-b68b-00a098908039
node_A_1 - A700	f03cb63c-9a7e-11e7-b68b-00a098908039
Node_a_2-A700	aa9a7a7a1-9a81-11e7-a4e9-00a098908c35

4. MetroCluster ノードが SAN 構成になっている場合は、関連情報を収集します。

   次のコマンドの出力を収集する必要があります。

   - 「 fcp adapter show -instance 」のように表示されます
   - 「 fcp interface show -instance 」の略
   - 「 iscsi interface show 」と表示されます
   - ucadmin show
5. ルート・ボリュームが暗号化されている場合は 'key-manager に使用するパスフレーズを収集して保存しますつまり 'security key-manager backup show
6. MetroCluster ノードがボリュームまたはアグリゲートに暗号化を使用している場合は、キーとパスフレー

ズに関する情報をコピーします。追加情報の場合は、を参照してください "オンボードキー管理情報の手動でのバックアップ"。

a. Onboard Key Manager が設定されている場合： security key-manager onboard show-backup + アップグレード手順であとでパスフレーズが必要になります。

b. Enterprise Key Management （ KMIP ）が設定されている場合は、次のコマンドを問題で実行します。

```
security key-manager external show -instance
security key-manager key query
```

7. 既存のノードのシステム ID を収集します。 MetroCluster node show -fields node-systemid 、 ha-partner-systemid 、 dr-partner-systemid 、 dr-auxiliary-systemid

次の出力は、再割り当てされたドライブを示しています。

```
::> metrocluster node show -fields node-systemid,ha-partner-systemid,dr-
partner-systemid,dr-auxiliary-systemid

dr-group-id cluster     node     node-systemid ha-partner-systemid dr-
partner-systemid dr-auxiliary-systemid
----------- ----------- -------- ------------- ------------------
------------------ ---------------------
1           cluster_A node_A_1-A700   537403324     537403323
537403321           537403322
1           cluster_A node_A_2-A700   537403323     537403324
537403322           537403321
1           cluster_B node_B_1-A700   537403322     537403321
537403323           537403324
1           cluster_B node_B_2-A700   537403321     537403322
537403324           537403323
4 entries were displayed.
```

メディエーターまたは **Tiebreaker** の監視を削除します

プラットフォームをアップグレードする前に、 MetroCluster 設定を Tiebreaker またはメディエーターユーティリティで監視している場合は、監視を解除する必要があります。

手順

1. 次のコマンドの出力を収集します。

「 storage iscsi-initiator show 」のように表示されます

2. Tiebreaker 、メディエーター、またはスイッチオーバーを開始できるその他のソフトウェアから既存の MetroCluster 構成を削除します。

使用するポート	使用する手順
Tiebreaker	"MetroCluster 設定の削除" *MetroCluster Tiebreaker* のインストールと構成コンテンツ
メディエーター	ONTAP プロンプトで次のコマンドを問題に設定します。 MetroCluster 構成設定のメディエーターが削除されました
サードパーティ製アプリケーション	製品マニュアルを参照してください。

カスタム **AutoSupport** メッセージをメンテナンス前に送信する

メンテナンスを実行する前に、 AutoSupport an 問題 message to notify technical support that maintenance is maintenance.システム停止が発生したとみなしてテクニカルサポートがケースをオープンしないように、メンテナンスが進行中であることを通知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 サイトごとに実行する必要があります。

手順

1. クラスタにログインします。
2. メンテナンスの開始を通知する AutoSupport メッセージを起動します。

   「 system node AutoSupport invoke -node * -type all -message MAINT= *maintenance-window-in-hours* 」というメッセージが表示されます

   「 maintenance-window-in-hours 」パラメータには、メンテナンス時間の長さを最大 72 時間指定します。この時間が経過する前にメンテナンスが完了した場合は、メンテナンス期間が終了したことを通知する AutoSupport メッセージを起動できます。

   「 system node AutoSupport invoke -node * -type all -message MAINT= end 」というメッセージが表示されます

3. 同じ手順をパートナーサイトでも実行します。

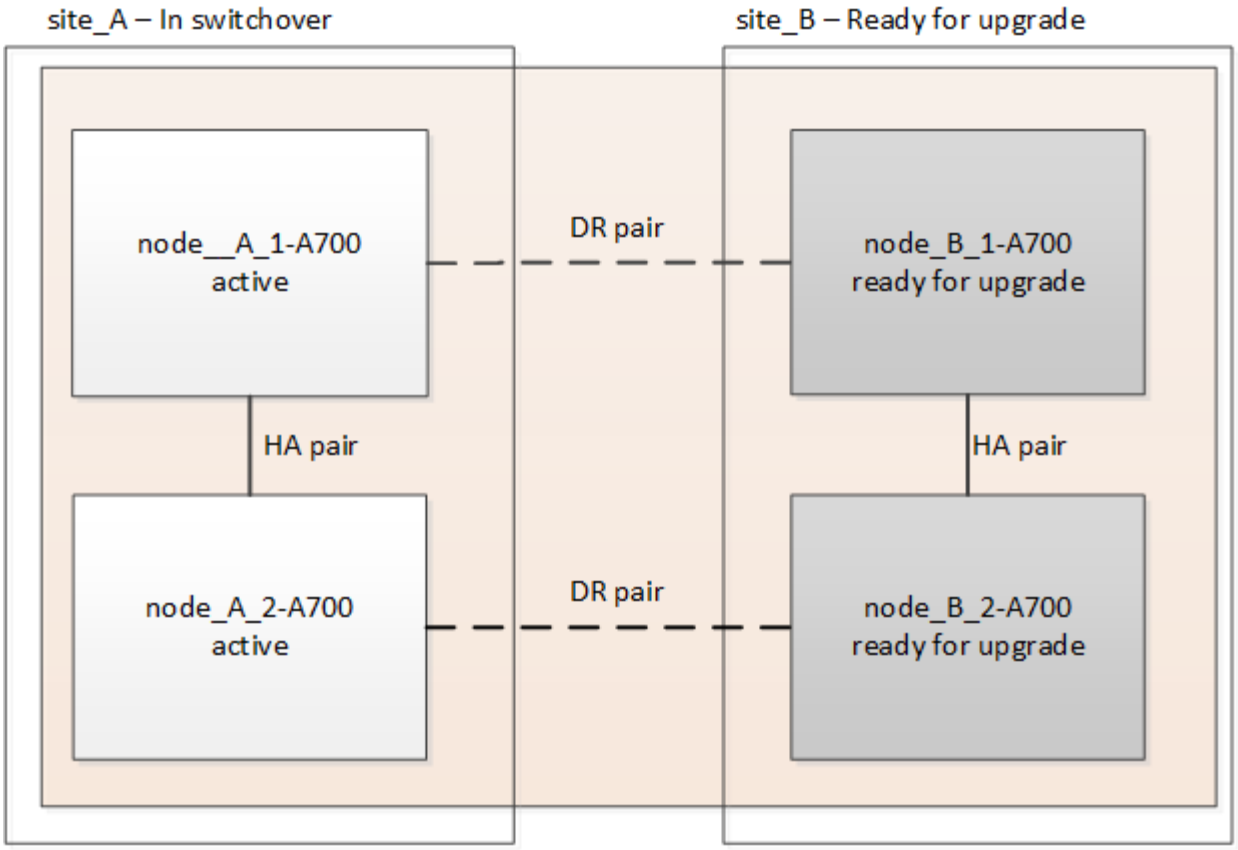
MetroCluster 構成をスイッチオーバーします

site_B のプラットフォームをアップグレードできるように、設定を site_A にスイッチオーバーする必要があります。

このタスクについて

このタスクは site_A で実行する必要があります

このタスクを完了すると、 site_A がアクティブになり、両方のサイトにデータが提供されます。site_B は非アクティブで、アップグレードプロセスを開始する準備ができています。



手順

1. site_B のノードをアップグレードできるように、 MetroCluster 構成を site_A にスイッチオーバーします。

   a. site_A で次のコマンドを問題に設定します。

      MetroCluster switche-controller-replacement true

      この処理が完了するまでに数分かかることがあります。

   b. スイッチオーバー処理を監視します。

      「 MetroCluster operation show 」を参照してください

   c. 処理が完了したら、ノードがスイッチオーバー状態であることを確認します。

      「 MetroCluster show 」

   d. MetroCluster ノードのステータスを確認します。

      MetroCluster node show

   コントローラのアップグレード中は、ネゴシエートスイッチオーバー後のアグリゲートの自動修復が無効になります。site_B のノードは、 LOADER プロンプトで停止および停止します。

AFF A700またはFAS9000プラットフォームのコントローラモジュールとNVSを取り外します

このタスクについて

接地対策がまだの場合は、自身で適切に実施します。

手順

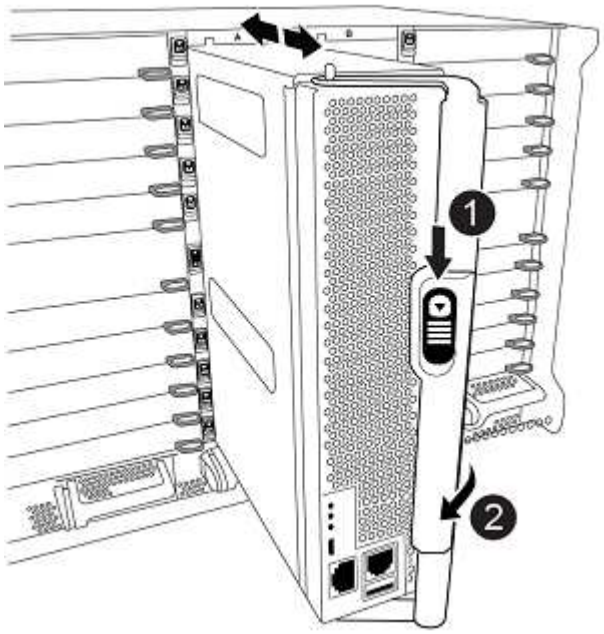
1. site_B の両方のノードから bootarg の値を収集します printenv
2. site_B のシャーシの電源をオフにします

AFF A700またはFAS9000コントローラモジュールを取り外します

次の手順 を使用して、AFF A700またはFAS9000コントローラモジュールを取り外します

手順

1. コントローラモジュールを取り外す前に、コントローラモジュールからコンソールケーブル（ある場合）と管理ケーブルを外します。
2. コントローラモジュールのロックを解除してシャーシから取り外します。
   a. カムハンドルのオレンジ色のボタンを下にスライドさせてロックを解除します。



	カムハンドルのリリースボタン
	カムハンドル

   a. カムハンドルを回転させて、コントローラモジュールをシャーシから完全に外し、コントローラモジュールをシャーシから引き出します。このとき、空いている手でコントローラモジュールの底面を支えてください。

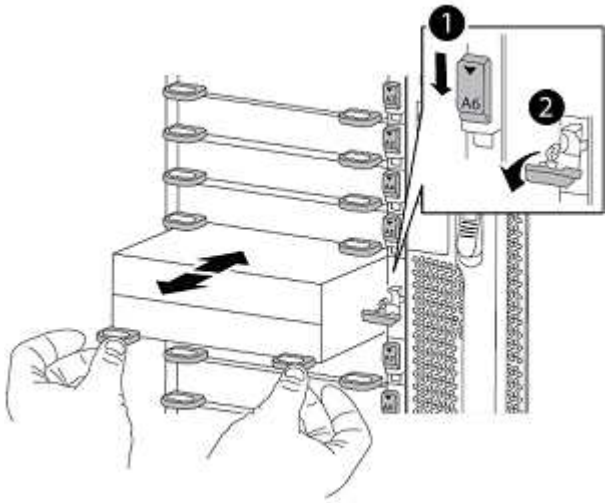
AFF A700またはFAS9000 NVSモジュールを取り外します

次の手順 を使用して、AFF A700またはFAS9000 NVSモジュールを取り外します。

メモ：NVSモジュールはスロット6にあり、システム内の他のモジュールと比較して高さが2倍になっています。

手順

1. NVS のロックを解除し、スロット 6 から取り外します。
   a. 文字と数字が記載された「カム」ボタンを押し下げます。カムボタンがシャーシから離れます。
   b. カムラッチを下に回転させて水平にします。NVS がシャーシから外れ、数インチ移動します。
   c. NVS をシャーシから取り外すには、モジュール前面の両側にあるプルタブを引いてください。



	文字と数字が記載された I/O カムラッチ
	ロックが完全に解除された I/O ラッチ

2. AFF A700またはFAS9000 NVSでコアダンプデバイスとして使用されるアドオンモジュールを使用している場合、それらのモジュールをAFF A900またはFAS9500 NVSに転送しないでください。AFF A700またはFAS9000コントローラモジュールとNVSからAFF A900またはFAS9500モジュールにパーツを転送しないでください。

AFF A900またはFAS9500 NVSとコントローラモジュールを取り付けます

アップグレードキットに含まれていたAFF A900またはFAS9500 NVSとコントローラモジュールをsite_Bの両方のノードにインストールする必要がありますコアダンプデバイスをAFF A700またはFAS9000 NVSモジュールからAFF A900またはFAS9500 NVSモジュールに移動しないでください。

このタスクについて

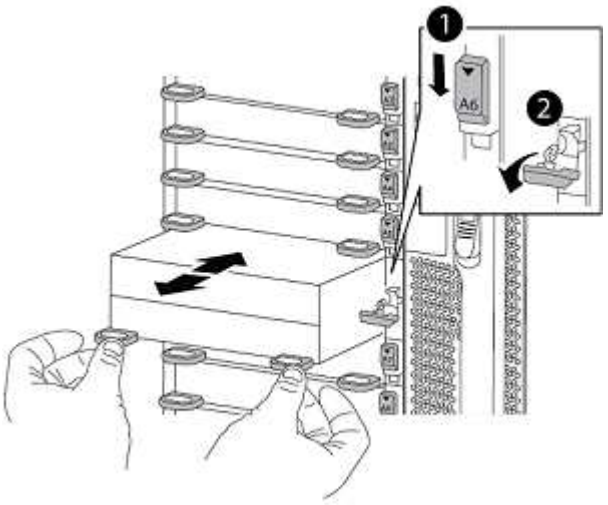
接地対策がまだの場合は、自身で適切に実施します。

AFF A900またはFAS9500 NVSをインストールします

次の手順 を使用して、site_Bの両方のノードのスロット6にAFF A900またはFAS9500 NVSをインストールします

手順

1. NVS をスロット 6 のシャーシ開口部の端に合わせます。
2. NVS をスロットにそっと挿入し、文字と数字が記載された I/O カムラッチを上に押して NVS を所定の位置にロックします。



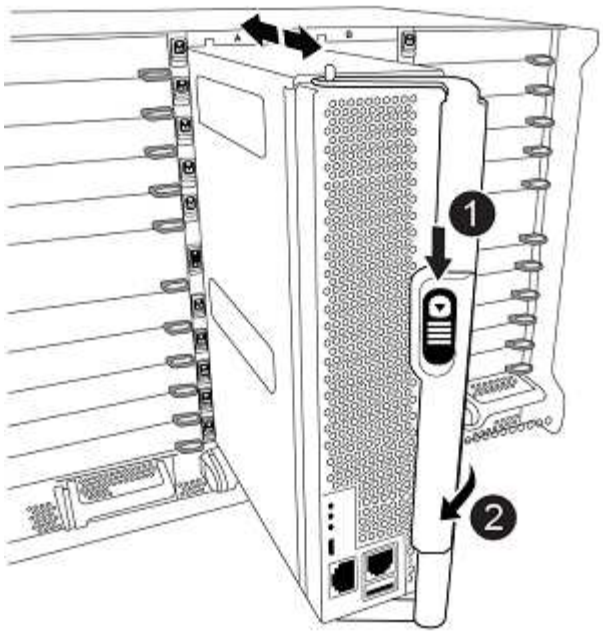
	文字と数字が記載された I/O カムラッチ
	ロックが完全に解除された I/O ラッチ

AFF A900またはFAS9500コントローラモジュールを取り付けます。

次の手順 を使用して、AFF A900またはFAS9500コントローラモジュールをインストールします。

手順

1. コントローラモジュールの端をシャーシの開口部に合わせ、コントローラモジュールをシステムに半分までそっと押し込みます。
2. コントローラモジュールをシャーシに挿入し、ミッドプレーンまでしっかりと押し込んで完全に装着します。コントローラモジュールが完全に装着されると、ロックラッチが上がります。注意：コネクタの破損を防ぐため、コントローラモジュールをシャーシに挿入する際に力を入れすぎないように注意してください。
3. 管理ポートとコンソールポートをコントローラモジュールにケーブル接続します。



	カムハンドルのリリースボタン
	カムハンドル

4. 各ノードのスロット 7 に 2 枚目の X91146A カードを取り付けます
   a. e5b 接続を e7b に移動します。
   b. e5a の接続を e5b に移動します。

> の項で説明したように、クラスタのすべてのノードのスロット7を空にする必要があります 古いノードから新しいノードへのポートのマッピング 。

5. シャーシの電源を入れ、シリアルコンソールに接続します。
6. BIOS の初期化後にノードで自動ブートが開始された場合は、 Ctrl-C を押して自動ブートを中断します
7. 自動ブートが中断されると、ノードは LOADER プロンプトで停止します。ブートを中断せずに node1 でブートが開始された場合は、プロンプトで Ctrl+C キーを押してブートメニューに移動します。ブートメニューでノードが停止したら、オプション 8 を使用してノードをリブートし、リブート時に自動ブートを中断します。
8. LOADER プロンプトで、デフォルトの環境変数を設定します。 set-defaults
9. デフォルトの環境変数設定である saveenv を保存します

site_B のネットブートノード

AFF A900またはFAS9500コントローラモジュールとNVSを交換したら、AFF A900またはFAS9500ノードをネットブートして、クラスタで実行されているものと同じバージョンのONTAP とパッチレベルをインストールする必要があります。ネットブートという用語は、リモート・サーバに保存された ONTAP イメージからブートすることを意味します。ネットブートの準備を行うときは、システムがアクセスできる Web サーバに、ONTAP 9 ブート・イメージのコピーを追加する必要があります。AFF A900またはFAS9500コントローラモジュールのブートメディアにインストールされているONTAP のバージョンは、シャーシに取り付けて電源がオ

ンになっていないかぎり確認できません。AFF A900またはFAS9500ブートメディア上のONTAP バージョンは、アップグレード対象のAFF A700またはFAS9000システムで実行されているONTAP バージョンと同じで、プライマリブートイメージとバックアップブートイメージの両方が一致している必要があります。イメージを設定するには、ネットブートを実行してからブートメニューの「 wipeconfig 」コマンドを実行します。コントローラモジュールが以前に別のクラスタで使用されていた場合は、「 wipeconfig 」コマンドはブートメディア上の残留設定をクリアします。

を開始する前に

- システムから HTTP サーバにアクセスできることを確認します。
- ご使用のシステムに必要なシステムファイルと、適切なバージョンの ONTAP をネットアップサポートサイトからダウンロードする必要があります。

このタスクについて

インストールされている ONTAP のバージョンが元のコントローラにインストールされているバージョンと異なる場合は、新しいコントローラをネットブートする必要があります。新しいコントローラをそれぞれ取り付けたら、 Web サーバに保存されている ONTAP 9 イメージからシステムをブートします。その後、以降のシステムブートで使用するブートメディアデバイスに正しいファイルをダウンロードできます。

手順

1. にアクセスします "ネットアップサポートサイト" システムのネットブートの実行に使用するファイルをダウンロードするには、次の手順を実行します。
2. [step2-download-software]] ネットアップサポートサイトのソフトウェアダウンロードセクションから適切な ONTAP ソフトウェアをダウンロードし、「 ONTAP-version image.tgz 」ファイルを Web にアクセスできるディレクトリに保存します。
3. Web にアクセスできるディレクトリに移動し、必要なファイルが利用可能であることを確認します。
4. ディレクトリの一覧に <ONTAP_version>_image.tgz が表示されている必要があります。
5. 次のいずれかを実行してネットブート接続を設定します。

ネットブート接続として管理ポートおよび IP を使用する必要があります。アップグレードの実行中にデータ LIF IP を使用しないでください。データ LIF が停止する可能性があります。

Dynamic Host Configuration Protocol （ DCHP ）の設定	作業
実行中です	ブート環境プロンプトで次のコマンドを使用して、自動的に接続を設定します。 ifconfig e0M -auto

実行されていません	ブート環境プロンプトで次のコマンドを使用して、接続を手動で設定します。 ifconfig e0M -addr= <filer_addr> -mask= <netmask> -gw= <gateway> -dns= <dns_addr> domain= <dns_domain> 「 <filer_addr> 」は、ストレージ・システムの IP アドレスです。<netmask> はストレージシステムのネットワークマスクです。「 <gateway>` 」は、ストレージシステムのゲートウェイです。「 <dns_addr> 」は、ネットワーク上のネームサーバの IP アドレスです。このパラメータはオプションです。「 <dns_domain> 」は、 Domain Name Service （ DNS ；ドメインネームサービス）ドメイン名です。このパラメータはオプションです。注：使用しているインターフェイスによっては、他のパラメータが必要になる場合もあります。ファームウェア・プロンプトで「 help ifconfig 」と入力すると、詳細が表示されます。

6. node_B_1でネットブートを実行します。
`netboot http://<web_server_ip/path_to_web_accessible_directory>/netboot/kernel`

「 <path_the_web-accessible_directory> 」は、「 <ONTAP_version>_image.tgz 」をダウンロードした場所に配置する必要があります 手順 2。

トランクを中断しないでください。

7. AFF A900またはFAS9500コントローラモジュールで実行されているnode_B_1がブートするまで待ち、次のようにブートメニューオプションを表示します。

```
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)?
```

8. 起動メニューから ' オプション (7) Install new software first.`` を選択します このメニューオプションを選択すると、新しい ONTAP イメージがブートデバイスにダウンロードおよびインストールされます。注意 : 次のメッセージは無視してください : この手順は 'HA ペアでの無停止アップグレードではサポートされ

ていません 環境の無停止の ONTAP ソフトウェアアップグレード。コントローラのアップグレードは含まれません。

新しいノードを希望するイメージに更新する場合は、必ずネットブートを使用してください。別の方法で新しいコントローラにイメージをインストールした場合、正しいイメージがインストールされないことがあります。この問題環境 All ONTAP リリース

9. 手順を続行するかどうかを確認するメッセージが表示されたら、と入力します。 `y`パッケージの入力を求められたら、次のURLを入力します。
`\http://<web_server_ip/path_to_web-accessible_directory>/<ontap_version>\_image.tgz`
10. 次の手順を実行してコントローラモジュールをリブートします。
    a. 入力 `n` 次のプロンプトが表示されたら、バックアップの回復をスキップします。

    ```
    Do you want to restore the backup configuration now? {y|n} n
    ```

    b. 入力 `y` 次のプロンプトが表示されたら再起動してください。

    ```
    The node must be rebooted to start using the newly installed
    software. Do you want to reboot now? {y|n} y
    ```

    コントローラモジュールはリブートしますが、ブートメニューで停止します。これは、ブートデバイスが再フォーマットされたことにより、構成データのリストアが必要なためです。

    新しくインストールされたソフトウェアを使用するには、ノードを再起動する必要があります。

11. プロンプトで「 wipeconfig 」コマンドを実行して、ブートメディアの以前の設定をクリアします。
    a. 次のメッセージが表示されたら、回答は「 yes 」を選択します。これにより、クラスタメンバーシップを含む重要なシステム構成が削除されます。警告：テイクオーバーされた HA ノードでは実行しないでください。続行してもよろしいですか ?:`
    b. ノードがリブートして「 wipeconfig 」を終了し、ブートメニューで停止します。
12. ブート・メニューからオプション「 5 」を選択して、保守モードに切り替えます。ノードが保守モードで停止して ' コマンド・プロンプト *> が表示されるまで ' プロンプトを表示します回答
13. 上記の手順を繰り返して、 node_B_2 をネットブートします。

HBA 構成をリストア

コントローラモジュールに HBA カードが搭載されているかどうかや設定によっては、サイトで使用するために正しく設定する必要があります。

手順

1. メンテナンスモードで、システム内の HBA の設定を行います。

a. ポートの現在の設定を確認します。

ucadmin show

b. 必要に応じてポートの設定を更新します。

HBA のタイプと目的のモード	使用するコマンド
CNA FC	ucadmin modify -m fc -t initiator_adapter-name _ `
CNA イーサネット	ucadmin modify -mode cna_adapter-name_ `
FC ターゲット	fcadmin config -t target_adapter-name_ `
FC イニシエータ	fcadmin config -t initiator_adapter-name_ `

2. メンテナンスモードを終了します。

「 halt 」

コマンドの実行後、ノードが LOADER プロンプトで停止するまで待ちます。

3. ノードをブートしてメンテナンスモードに戻り、設定の変更が反映されるようにします。

「 boot_ontap maint 」を使用してください

4. 変更内容を確認します。

HBA のタイプ	使用するコマンド
CNA	ucadmin show
FC	fcadmin show`

新しいコントローラとシャーシで **HA** 状態を設定

コントローラとシャーシの HA 状態を確認し、必要に応じてシステム構成に合わせて更新する必要があります。

手順

1. メンテナンスモードで、コントローラモジュールとシャーシの HA 状態を表示します。

「 ha-config show 」

すべてのコンポーネントの HA 状態は「 mccip 」である必要があります。

2. 表示されたコントローラまたはシャーシのシステム状態が正しくない場合は、 HA 状態を設定します。

「 ha-config modify controller mccip 」を参照してください

「 ha-config modify chassis mccip 」を参照してください

3. ノードを停止します

   ノードは 'loader>` プロンプトで停止する必要があります

4. 各ノードで、システムの日付、時刻、およびタイムゾーンを確認します。「 show date 」
5. 必要に応じて 'UTC または GMT:'set date <mm/dd/yyyy>' で日付を設定します
6. ブート環境プロンプトで次のコマンドを使用して ' 時刻を確認します
7. 必要に応じて、時刻を UTC または GMT:' 設定時刻 <:hh:mm:ss>` で設定します
8. 設定を保存します： saveenv
9. 環境変数 :printenv' を収集します

新しいプラットフォームに対応できるようにスイッチの **RCF** ファイルを更新します

スイッチは、新しいプラットフォームモデルをサポートする構成に更新する必要があります。

このタスクについて

このタスクは、現在アップグレード中のコントローラを含むサイトで実行します。この手順の例では、まず site_B をアップグレードします。

site_A のコントローラをアップグレードすると、 site_A のスイッチがアップグレードされます。

手順

1. IPスイッチで新しいRCFを適用できるように準備します。

   スイッチベンダーに対応するセクションを参照してください。

   - "Broadcom IP スイッチを工場出荷時のデフォルトにリセットします"
   - "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"
   - "NVIDIA IP SN2100スイッチを工場出荷時のデフォルトにリセット"

2. RCFをダウンロードしてインストールします。

   スイッチベンダーに対応するセクションを参照してください。

   - "Broadcom RCFのダウンロードとインストール"
   - "Cisco IP RCFのダウンロードとインストール"
   - "NVIDIA IP RCFのダウンロードとインストール"

新しいコントローラを設定します

この時点で、新しいコントローラの準備が整い、ケーブル接続が完了している必要があります。

MetroCluster の bootarg IP 変数を設定します

新しいコントローラモジュールには特定の MetroCluster IP bootarg 値を設定する必要があります。これらの値は、古いコントローラモジュールに設定されている値と一致する必要があります。

このタスクについて

このタスクでは、のアップグレード手順で特定したUUIDとシステムIDを使用し [アップグレード前に情報を収集]ます。

手順

1. 「 LOADER> 」プロンプトで、 site_B の新しいノードで次のブート引数を設定します。

   'etenvarge.MCC.port_a_ip_config_local-ip-address/local-ip-mask'0 、 ha-partner-ip-address 、 dr-partner-ip-address 、 dr-aux-partnerip-address 、 vlan-id_`

   「 etenvarge.MCC.port_b_ip_config_local-ip-address/local-ip-mask, 0,ha-partner-ip-address 、 dr-partner-ip-address 、 dr-aux-partnerip-address 、 vlan-id_` 」を指定します

   次の例は、最初のネットワークに VLAN 120 を、 2 番目のネットワークに VLAN 130 を使用して、 node_B_1 から A900 の値を設定します。

   ```
   setenv bootarg.mcc.port_a_ip_config
   172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12,120
   setenv bootarg.mcc.port_b_ip_config
   172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12,130
   ```

   次の例は、最初のネットワークに VLAN 120 を、 2 番目のネットワークに VLAN 130 を使用して、 node_B_2 から A900 に値を設定します。

   ```
   setenv bootarg.mcc.port_a_ip_config
   172.17.26.11/23,0,172.17.26.10,172.17.26.12,172.17.26.13,120
   setenv bootarg.mcc.port_b_ip_config
   172.17.27.11/23,0,172.17.27.10,172.17.27.12,172.17.27.13,130
   ```

2. 新しいノードの LOADER プロンプトで ' UUID を設定します

   「 etenv bootarg.mgwd.partner_uuid_partner -cluster-UUID_` 」と入力します

   「 etenv bootarg.mgwd.cluster_ue_local-cluster-UUID_` 」と入力します

   「 etenv bootarge.MCC.pri_partner_uuid_dr-partner -node-UUID_` 」と入力します

   'etenv bootarg.mcc.aux_partner_uuid *dr-au-partner -UUID*`

   「 etenv bootarg.mcc_iscsi.node_uuid *local-node-UUID*` 」と入力します

   a. node_B_1 から A900 の UUID を設定します。

次の例は、 node_B_1 から A900 の UUID を設定するコマンドを示しています。

```
setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039
setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.pri_partner_uuid f37b240b-9ac1-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.aux_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-
00a098ca379f
setenv bootarg.mcc_iscsi.node_uuid f03cb63c-9a7e-11e7-b68b-
00a098908039
```

b. node_B_2 - A900 の UUID を設定します。

次の例は、 node_B_2 - A900 の UUID を設定するコマンドを示しています。

```
setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039
setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.pri_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
setenv bootarg.mcc.aux_partner_uuid f37b240b-9ac1-11e7-9b42-00a098c9e55d
setenv bootarg.mcc_iscsi.node_uuid aa9a7a7a-9a81-11e7-a4e9-00a098908c35
```

3. 元のシステムが ADP 用に設定されていた場合は、交換用ノードの LOADER プロンプトで ADP を有効にします。

'etenv bootarg.me.adp_enabled true

4. 次の変数を設定します。

「 etenv bootarg.me.local_config_id_original-sys-sys-id_` 」を返します

「 etenv bootarge.MCC.DR_PARTNER_DR-partner -sys-id_` 」を選択します

> setenbootarg.mb.local_config_id' 変数は ' 元の * コントローラ・モジュールである node_B_1 A700 の sys-id に設定する必要があります

a. node_B_1 から A900 の変数を設定します。

次の例は、 node_B_1 から A900 の値を設定するコマンドを示しています。

```
setenv bootarg.mcc.local_config_id 537403322
setenv bootarg.mcc.dr_partner 537403324
```

b. node_B_2 - A900 の変数を設定します。

次の例は、 node_B_2 から A900 の値を設定するコマンドを示しています。

```
setenv bootarg.mcc.local_config_id 537403321
setenv bootarg.mcc.dr_partner 537403323
```

5. 外部キー管理ツールで暗号化を使用する場合は、必要な bootargs を設定します。

   「 etenv bootarg.kmip.init.ipaddr` 」を参照してください

   「 etenv bootarg.kmip.kmip.init.netmask` 」を参照してください

   「 etenv bootarg.kmip.kmip.init.gateway` 」を参照してください

   「 etenv bootarg.kmip.kmip.init.interface` 」を参照してください

ルートアグリゲートディスクを再割り当てします

前の手順で確認したシステム ID を使用して、ルートアグリゲートディスクを新しいコントローラモジュールに再割り当てします。

このタスクについて

以下の手順はメンテナンスモードで実行します。

手順

1. システムをメンテナンスモードでブートします。

   「 boot_ontap maint 」を使用してください

2. メンテナンスモードのプロンプトから node_B_1 - A900 のディスクを表示します。

   「ディスクショー - A` 」

   コマンド出力に、新しいコントローラモジュール（ 1574774970 ）のシステム ID が表示されます。ただし、ルートアグリゲートディスクの所有者は古いシステム ID （ 537403322 ）になります。この例で表示されているのは、 MetroCluster 構成の他のノードが所有するドライブではありません。

```
*> disk show -a
Local System ID: 1574774970
DISK                  OWNER                  POOL   SERIAL NUMBER   HOME
DR HOME
------------          ---------              -----  -------------
-------------         -------------
prod3-rk18:9.126L44   node_B_1-A700(537403322)  Pool1  PZHYN0MD
node_B_1-A700(537403322)  node_B_1-A700(537403322)
prod4-rk18:9.126L49  node_B_1-A700(537403322)  Pool1  PPG3J5HA
node_B_1-A700(537403322)  node_B_1-700(537403322)
prod4-rk18:8.126L21   node_B_1-A700(537403322)  Pool1  PZHTDSZD
node_B_1-A700(537403322)  node_B_1-A700(537403322)
prod2-rk18:8.126L2    node_B_1-A700(537403322)  Pool0  S0M1J2CF
node_B_1-(537403322)  node_B_1-A700(537403322)
prod2-rk18:8.126L3    node_B_1-A700(537403322)  Pool0  S0M0CQM5
node_B_1-A700(537403322)  node_B_1-A700(537403322)
prod1-rk18:9.126L27   node_B_1-A700(537403322)  Pool0  S0M1PSDW
node_B_1-A700(537403322)  node_B_1-A700(537403322)
.
.
.
```

3. ドライブシェルフのルートアグリゲートディスクを新しいコントローラに再割り当てします。

ADP を使用する環境	使用するコマンド
はい。	「ディスクの再割り当て -s *old-sysid*-d_new-sysid_ -r_dr -partner sysid_`
いいえ	「ディスクの再割り当て -s *old-sysid*-d_new-sysid_`

4. ドライブシェルフのルートアグリゲートディスクを新しいコントローラに再割り当てします。

   「ディスク再割り当て -s old-sysid -d new-sysid 」

   次の例は、 ADP 以外の構成でのドライブの再割り当てを示しています。

```
*> disk reassign -s 537403322 -d 1574774970
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)? n

After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)? y
Disk ownership will be updated on all disks previously belonging to
Filer with sysid 537403322.
Do you want to continue (y/n)? y
```

5. ルートアグリゲートのディスクが正しく再割り当てされていることを確認します。 old-remove

   「ディスクショー」

   「ストレージ・アグリゲートのステータス」

```
*> disk show
Local System ID: 537097247

  DISK                    OWNER                    POOL   SERIAL NUMBER
HOME                    DR HOME
------------             -------------            -----  -------------
-------------           -------------
prod03-rk18:8.126L18 node_B_1-A900(537097247)  Pool1  PZHYN0MD
node_B_1-A900(537097247)   node_B_1-A900(537097247)
prod04-rk18:9.126L49 node_B_1-A900(537097247)  Pool1  PPG3J5HA
node_B_1-A900(537097247)   node_B_1-A900(537097247)
prod04-rk18:8.126L21 node_B_1-A900(537097247)  Pool1  PZHTDSZD
node_B_1-A900(537097247)   node_B_1-A900(537097247)
prod02-rk18:8.126L2  node_B_1-A900(537097247)  Pool0  S0M1J2CF
node_B_1-A900(537097247)   node_B_1-A900(537097247)
prod02-rk18:9.126L29 node_B_1-A900(537097247)  Pool0  S0M0CQM5
node_B_1-A900(537097247)   node_B_1-A900(537097247)
prod01-rk18:8.126L1  node_B_1-A900(537097247)  Pool0  S0M1PSDW
node_B_1-A900(537097247)   node_B_1-A900(537097247)
::>
::> aggr status
           Aggr          State           Status                Options
aggr0_node_B_1           online          raid_dp, aggr         root,
nosnap=on,
                                         mirrored
mirror_resync_priority=high(fixed)
                                         fast zeroed
                                         64-bit
```

新しいコントローラをブートします

新しいコントローラをブートする必要があります。 bootarg 変数が正しいことを確認し、必要に応じて暗号化のリカバリ手順を実行するように注意してください。

手順

1. 新しいノードを停止します。

   「 halt 」

2. 外部キー管理ツールが設定されている場合は、関連する bootargs を設定します。

   'setenv bootarg.kmip.init.ipaddr *ip-address*'

   'setenv bootarg.kmip.init.netmask *netmask*`

   'setenv bootarg.kmip.init.gateway *gateway-address*

'setenv bootarg.kmip.init.interface *interface-id*

3. partner-sysid が現在のものかどうかを確認します。

   printenv partner-sysid

   partner-sysid が正しくない場合は、次のように設定します。

   'setenv partner-sysid_partner-SysID_`

4. ONTAP ブートメニューを表示します。

   「 boot_ontap menu

5. ルート暗号化を使用する場合は、キー管理設定のブートメニューオプションを選択します。

使用するポート	選択するブートメニューオプション
オンボードキー管理	オプション 10 を選択し、画面の指示に従って、キー管理ツールの構成をリカバリまたはリストアするために必要な入力を指定します
外部キー管理	オプション 11 を選択し、画面の指示に従って、キー管理ツールの設定をリカバリまたはリストアするために必要な入力を指定します

6. ブート・メニューから '(6) Update flash from backup config' を選択します

   オプション 6 を指定すると、完了前にノードが 2 回リブートされます

   システム ID 変更プロンプトに「 y 」と入力します。2 回目のリブートメッセージが表示されるまで待ちます。

```
Successfully restored env file from boot media...

Rebooting to load the restored env file...
```

7. 自動ブートを中断して、コントローラを LOADER で停止します。

   各ノードで、に設定された bootargs を確認します "MetroCluster の bootarg IP 変数の設定" 正しくない値があれば修正します。bootarg の値を確認したあとに次の手順にのみ移動してください。

8. partner-sysid が正しいことを確認します。

   printenv partner-sysid

   partner-sysid が正しくない場合は、次のように設定します。

'setenv partner-sysid_partner-SysID_`

9. ルート暗号化を使用する場合は、キー管理設定のブートメニューオプションを選択します。

使用するポート	選択するブートメニューオプション
オンボードキー管理	オプション 10 を選択し、画面の指示に従って、キー管理ツールの構成をリカバリまたはリストアするために必要な入力を指定します
外部キー管理	オプション 11 を選択し、画面の指示に従って、キー管理ツールの設定をリカバリまたはリストアするために必要な入力を指定します

キー管理ツールの設定に応じてオプション 10 またはオプション 11 を選択し、ブートメニューのプロンプトでオプション 6 を選択して、リカバリ手順を実行する必要があります。ノードを完全にブートするには、オプション 1 （通常ブート）のリカバリ手順の実行が必要になる場合があります。

10. 新しいノード node_B_1 と node_B_2 がブートするまで待ちます。

いずれかのノードがテイクオーバーモードの場合は、「 storage failover giveback 」コマンドを使用してギブバックを実行します。

11. 暗号化を使用する場合は、キー管理設定に対応したコマンドを使用してキーをリストアします。

使用するポート	使用するコマンド
オンボードキー管理	「セキュリティキーマネージャオンボード同期」 詳細については、を参照してください "オンボードキー管理の暗号化キーのリストア"。
外部キー管理	「 securitykey manager external restore -vserver *svm*-node __ key -server_host_name

12. すべてのポートがブロードキャストドメインに属していることを確認します。

a. ブロードキャストドメインを表示します。

「 network port broadcast-domain show 」

b. 必要に応じて、ブロードキャストドメインにポートを追加します。

"ブロードキャストドメインのポートの追加と削除"

c. 必要に応じて、 VLAN とインターフェイスグループを再作成します。

VLAN およびインターフェイスグループのメンバーシップは、古いノードと異なる場合があります。

"VLAN を作成する"

"物理ポートを組み合わせたインターフェイスグループの作成"

LIF の設定を確認してリストア

アップグレード手順の開始時にマッピングされた適切なノードとポートで LIF がホストされていることを確認します。

このタスクについて

- このタスクは site_B で実行します
- で作成したポートマッピングプランを表示します。 古いノードから新しいノードへのポートのマッピング

手順

1. スイッチバックの前に、 LIF が適切なノードとポートにホストされていることを確認します。

   a. advanced 権限レベルに切り替えます。

      「 advanced 」の権限が必要です

   b. ポート設定を無視して LIF が適切に配置されるようにします。

      「 vserver config override command 」 network interface modify -vserver vserver_name __ -home -node _active_port_after_upgrade _ -lif LIF_name -home-node _new_node_name _

   vserver config override コマンドで network interface modify コマンドを入力した場合は、 tab autoccomplete 機能を使用することはできません。autoccomplete を使用してネットワーク 'interface modify' を作成してから 'vserver config override' コマンドで囲むことができます

   a. admin 権限レベルに戻ります。

      「特権管理者」

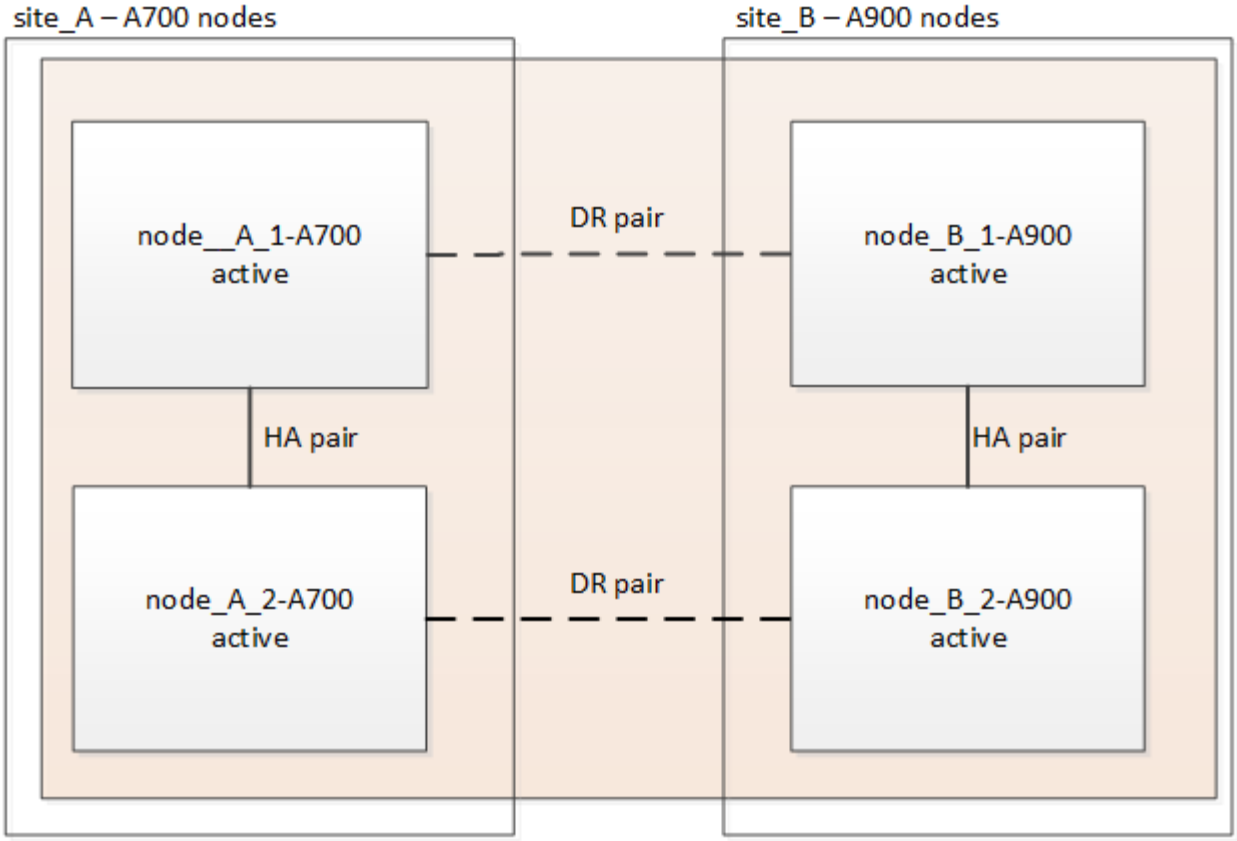
2. インターフェイスをホームノードにリバートします。

   「 network interface revert * -vserver_vserver-name に指定します

   必要に応じて、すべての SVM でこの手順を実行します。

MetroCluster 構成をスイッチバックします

このタスクでは、スイッチバック処理を実行し、 MetroCluster 構成が通常運用時の状態に戻ります。site_A のノードはまだアップグレード待ちです。



手順

1. site_B の MetroCluster node show コマンドを問題し ' 出力を確認します
   a. 新しいノードが正しく表示されることを確認します。
   b. 新しいノードの状態が「 Waiting for switchback 」であることを確認します。
2. アクティブなクラスタ（アップグレードを実行していないクラスタ）の任意のノードから必要なコマンドを実行して、修復とスイッチバックを実行します。
   a. データアグリゲートを修復します。 + MetroCluster heal aggregates `
   b. ルートアグリゲートを修復します。

      MetroCluster はルートを修復します

   c. クラスタをスイッチバックします。

      MetroCluster スイッチバック

3. スイッチバック処理の進捗を確認します。

   「 MetroCluster show 」

   出力に「 waiting-for-switchback 」と表示されたら、スイッチバック処理はまだ進行中です。

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                switchover
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                waiting-for-switchback
                          AUSO Failure Domain -
```

出力に normal と表示された場合、スイッチバック処理は完了しています。

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
```

スイッチバックが完了するまでに時間がかかる場合は、「 MetroCluster config-replication resync-status show 」コマンドを使用することで、進行中のベースラインのステータスを確認できます。このコマンドは、 advanced 権限レベルで実行します。

MetroCluster 構成の健全性を確認します

コントローラモジュールをアップグレードしたら、 MetroCluster 構成の健全性を確認する必要があります。

このタスクについて

このタスクは、 MetroCluster 構成の任意のノードで実行できます。

手順

1. MetroCluster 構成の動作を確認します。
   a. MetroCluster 構成と動作モードが正常であることを確認します。 + MetroCluster show `
   b. MetroCluster チェックを実行します + MetroCluster チェックを実行します
   c. MetroCluster チェックの結果を表示します。

      MetroCluster チェックショー
2. MetroCluster の接続およびステータスを確認します。
   a. MetroCluster IP 接続を確認します。

「 storage iscsi-initiator show 」のように表示されます

b. ノードが動作していることを確認します。

MetroCluster node show

c. MetroCluster IP インターフェイスが動作していることを確認します。

「 MetroCluster configurion-settings interface show 」を参照してください

d. ローカルフェイルオーバーが有効になっていることを確認します。

「 storage failover show 」をクリックします

site_A でノードをアップグレードします

site_A でアップグレードタスクを繰り返します

手順

1. この手順を繰り返して、site_Aのノードをアップグレードします。 アップグレードを準備

タスクを実行すると、サイトおよびノードへのすべてのサンプル参照が反転されます。たとえば、この例で site_A からスイッチオーバーする場合は site_B からスイッチオーバーします

Tiebreaker またはメディエーターの監視をリストアします

MetroCluster 構成のアップグレードが完了したら、 Tiebreaker またはメディエーターユーティリティを使用して監視を再開できます。

手順

1. 必要に応じて、構成に応じて手順を使用してリストアを監視します。

使用するポート	この手順を使用します
Tiebreaker	"MetroCluster 構成を追加しています" *MetroCluster Tiebreaker* のインストールと構成 セクション。
メディエーター	"MetroCluster IP構成からONTAPメディエーターを構成する" *MetroCluster IP* のインストールと構成 セクション。
サードパーティ製アプリケーション	製品マニュアルを参照してください。

カスタム AutoSupport メッセージをメンテナンス後に送信します

アップグレードの完了後、ケースの自動作成を再開できるように、メンテナンスの終了を通知する AutoSupport メッセージを送信する必要があります。

手順

1. サポートケースの自動生成を再開するには、メンテナンスが完了したことを示す AutoSupport メッセージを送信します。

   a. 次のコマンドを問題で実行します。 + 「 system node AutoSupport invoke -node * -type all -message MAINT= end 」

   b. パートナークラスタに対してこのコマンドを繰り返します。

スイッチオーバーとスイッチバックを使用して、 MetroCluster FC 構成のコントローラをアップグレードします

MetroCluster スイッチオーバー処理を使用すると、パートナークラスタのコントローラモジュールのアップグレード中もクライアントに無停止でサービスを提供できます。この手順の一部として他のコンポーネント（ストレージシェルフやスイッチなど）をアップグレードすることはできません。

サポートされるプラットフォームの組み合わせ

MetroCluster FC構成では、スイッチオーバーとスイッチバックの処理を使用して特定のプラットフォームをアップグレードできます。

サポートされるプラットフォームのアップグレードの組み合わせについては、のMetroCluster FCアップグレードの表を参照してください "コントローラのアップグレード手順 を選択します"。

を参照してください "アップグレードまたは更新方法を選択します" を参照してください。

このタスクについて

- この手順は、コントローラのアップグレードにのみ使用できます。

  ストレージシェルフやスイッチなど、構成内の他のコンポーネントは同時にアップグレードできません。

- この手順 は、特定のバージョンのONTAP で使用できます。
  - ONTAP 9.3 以降では 2 ノード構成がサポートされます。
  - ONTAP 9.8以降では、4ノード構成と8ノード構成がサポートされます。

    ONTAP 9.8 より前のバージョンを実行している 4 ノードまたは 8 ノード構成では、この手順を使用しないでください。

- 元のプラットフォームと新しいプラットフォームに互換性があり、サポートされている必要があります。

  "NetApp Hardware Universe の略"

> 元のプラットフォームまたは新しいプラットフォームがFAS8020またはAFF8020システムでは、FC-VIモードのポート1cと1dを使用する場合は、ナレッジベースの記事を参照してください "既存のFAS8020またはAFF8020ノードでFCVI接続にポート1cと1dを使用する場合は、コントローラをアップグレードします。"

- 両方のサイトでライセンスが一致している必要があります。から新しいライセンスを取得できます "ネットアップサポート"。
- この 手順 環境 コントローラモジュールは、MetroCluster FC構成（2ノードのストレッチMetroCluster 構成または2ノード、4ノード、または8ノードのファブリック接続MetroCluster 構成）で使用します。
- 同じDRグループ内のすべてのコントローラは、同じメンテナンス期間にアップグレードする必要があります。

  同じDRグループに種類の異なるコントローラを含むMetroCluster 構成の運用は、このメンテナンス作業以外ではサポートされません。8ノードMetroCluster 構成では、DRグループ内のコントローラは同じである必要がありますが、両方のDRグループで異なる種類のコントローラを使用できます。

- 元のノードと新しいノードの間のストレージ、 FC 、イーサネット接続をあらかじめマッピングしておくことを推奨します。
- 新しいプラットフォームのスロット数が元のシステムのスロット数より少ない場合、またはポートのタイプが異なる場合は、新しいシステムにアダプタを追加しなければならないことがあります。

  詳細については、を参照してください "NetApp Hardware Universe の略"

この手順では、次の名前が使用されています。

- site_A
  - アップグレード前：
    - node_A_1 - 古い
    - Node_a_2-old
  - アップグレード後：
    - node_A_1 - 新規
    - Node_a_2 - 新規
- site_B
  - アップグレード前：
    - node_B_1 - 古い
    - node_B_2 - 古い
  - アップグレード後：
    - node_B_1 - 新規
    - node_B_2 - 新規

コンソールログを有効にする

NetAppでは、使用しているデバイスでコンソールロギングをイネーブルにし、この手順を実行する際に次のアクションを実行することを強く推奨します。

- メンテナンス中はAutoSupportを有効のままにします。
- メンテナンスの前後にメンテナンスAutoSupportメッセージをトリガーして、メンテナンスアクティビティ中にケースの作成を無効にします。

ナレッジベースの記事を参照してください "スケジュールされたメンテナンス時間中にケースの自動作成を停止する方法"。

- 任意のCLIセッションのセッションロギングをイネーブルにします。セッションログを有効にする方法については、ナレッジベースの記事の「セッション出力のログ」セクションを参照してください "ONTAPシステムへの接続を最適化するためのPuTTYの設定方法"。

アップグレードを準備

既存の MetroCluster 構成に変更を加える前に、構成の健全性を確認し、新しいプラットフォームを準備し、その他のタスクを実行する必要があります。

MetroCluster 構成の健全性を確認

アップグレードを実行する前に、MetroCluster 構成の健全性と接続性を確認します。

> 最初のサイトでコントローラをアップグレードした後、2番目のサイトをアップグレードする前に、 `metrocluster check run`に続く `metrocluster check show`エラーを返します `config-replication`フィールド。このエラーは、各サイトのノード間でNVRAMのサイズが一致していないことを示しています。これは、両サイトで異なるプラットフォームモデルが存在する場合に想定される動作です。DRグループ内のすべてのノードでコントローラーのアップグレードが完了するまで、このエラーは無視できます。

手順

1. ONTAP で MetroCluster 構成の動作を確認します。

   a. ノードがマルチパスであるかどうかを確認します。 `+node run -node node_name sysconfig -a`

      このコマンドは、 MetroCluster 構成のノードごとに問題で実行する必要があります。

   b. 構成に破損ディスクがないことを確認します。

      「 storage disk show -broken 」

      このコマンドは、 MetroCluster 構成の各ノードで問題を実行する必要があります。

   c. ヘルスアラートがないかどうかを確認します。

      「 system health alert show 」というメッセージが表示されます

      このコマンドは、各クラスタで問題を実行する必要があります。

   d. クラスタのライセンスを確認します。

      「 system license show 」を参照してください

      このコマンドは、各クラスタで問題を実行する必要があります。

   e. ノードに接続されているデバイスを確認します。

      「 network device-discovery show 」のように表示されます

このコマンドは、各クラスタで問題を実行する必要があります。

f. 両方のサイトでタイムゾーンと時間が正しく設定されていることを確認します。

cluster date show

このコマンドは、各クラスタで問題を実行する必要があります。時刻とタイムゾーンを設定するには 'cluster date コマンドを使用します

2. スイッチにヘルスアラートがないかどうかを確認します（ある場合）。

「 storage switch show 」と表示されます

このコマンドは、各クラスタで問題を実行する必要があります。

3. MetroCluster 構成の運用モードを確認し、 MetroCluster チェックを実行

a. MetroCluster 構成と運用モードが正常な状態であることを確認します。

「 MetroCluster show 」

b. 想定されるすべてのノードが表示されることを確認します。

MetroCluster node show

c. 次のコマンドを問題に設定します。

「 MetroCluster check run 」のようになります

d. MetroCluster チェックの結果を表示します。

MetroCluster チェックショー

4. Config Advisor ツールを使用して MetroCluster のケーブル接続を確認します。

a. Config Advisor をダウンロードして実行します。

"ネットアップのダウンロード： Config Advisor"

b. Config Advisor の実行後、ツールの出力を確認し、推奨される方法で検出された問題に対処します。

古いノードから新しいノードへのポートのマッピング

古いノードの物理ポートと新しいノードの物理ポートのマッピングを計画する必要があります。

このタスクについて

アップグレードプロセスで最初に新しいノードがブートされると、交換前の古いノードの最新の設定が再生されます。node_A_1 を新規にブートすると、 ONTAP は node_A_1 の古いポートで使用されていた LIF をホストしようとします。そのため、アップグレードの一環として、ポートと LIF の設定を古いノードと互換性があるように調整する必要があります。アップグレード手順では、クラスタ LIF 、管理 LIF 、およびデータ LIF の構成が正しくなるように、古いノードと新しいノードの両方で手順を実行します。

次の表に、新しいノードのポート要件に関連する設定変更の例を示します。

クラスタインターコネクトの物理ポート		
古いコントローラ	新しいコントローラ	必要なアクション
e0a 、 e0b	e3a 、 e3b	一致するポートがありません。アップグレード後に、クラスタポートを再作成します。"既存のコントローラモジュールのクラスタポートを準備"
e0c 、 e0d	e0a 、 e0b 、 e0c 、 e0d	e0c と e0d は同じポートです。構成を変更する必要はありませんが、アップグレード後は、使用可能なクラスタポートにクラスタ LIF を分散させることができます。

手順

1. 新しいコントローラで使用できる物理ポートとポートでホストできる LIF を確認します。

   コントローラのポートの用途は、プラットフォームモジュールおよび MetroCluster IP 構成で使用するスイッチによって異なります。新しいプラットフォームのポート使用量をから収集できます "NetApp Hardware Universe の略"。

   また、 FC-VI カードスロットの用途も示します。

2. ポートの使用状況を計画し、必要に応じて次の表に新しいノードそれぞれを記載します。

   この表は、アップグレード手順を実行するときに参照します。

	node_A_1 - 古い			node_A_1 - 新規		
LIF	ポート	IPspace	ブロードキャストドメイン	ポート	IPspace	ブロードキャストドメイン
クラスタ 1						
クラスタ 2						
クラスタ 3						
クラスタ 4						
ノード管理						
クラスタ管理						
データ 1						
データ 2.						
データ 3						

データ 4.						
SAN						
クラスタ間ポート						

アップグレード前に情報を収集

アップグレードの前に、古い各ノードの情報を収集し、必要に応じてネットワークブロードキャストドメインを調整し、VLANとインターフェイスグループを削除し、暗号化情報を収集する必要があります。

このタスクについて

このタスクは、既存の MetroCluster FC 構成で実行します。

手順

1. 新しいコントローラをセットアップするときにケーブルを簡単に識別できるように、既存のコントローラのケーブルにラベルを付けます。
2. MetroCluster 構成内のノードのシステム ID を収集します。

   MetroCluster node show -fields node-systemid 、 dr-partner-systemid'

   手順のアップグレード時に、これらの古いシステムIDを新しいコントローラモジュールのシステムIDに置き換えます。

   この 4 ノード MetroCluster FC 構成の例では、次の古いシステム ID が取得されます。

   - node_A_1 - 古い： 4068741258
   - node_A_2 - 古い： 4068741260
   - node_B_1 - 古い： 4068741254
   - node_B_2 - 古い： 4068741256

```
metrocluster-siteA::> metrocluster node show -fields node-
systemid,ha-partner-systemid,dr-partner-systemid,dr-auxiliary-
systemid
dr-group-id   cluster                        node
node-systemid          ha-partner-systemid     dr-partner-systemid
dr-auxiliary-systemid
-----------        ------------------------- ------------------
-------------                   --------------------
-------------------              ----------------------
1                    Cluster_A                  Node_A_1-old
4068741258              4068741260                         4068741256
4068741256
1                    Cluster_A                    Node_A_2-old
4068741260              4068741258                         4068741254
4068741254
1                    Cluster_B                    Node_B_1-old
4068741254              4068741256                          4068741258
4068741260
1                    Cluster_B                    Node_B_2-old
4068741256              4068741254                         4068741260
4068741258
4 entries were displayed.
```

この 2 ノード MetroCluster FC 構成の例では、次の古いシステム ID が取得されます。

- node_A_1 ： 4068741258
- node_B_1 ： 4068741254

```
metrocluster node show -fields node-systemid,dr-partner-systemid

dr-group-id cluster    node      node-systemid dr-partner-systemid
----------- ---------- --------  ------------- ------------
1           Cluster_A  Node_A_1-old  4068741258    4068741254
1           Cluster_B  node_B_1-old  -             -
2 entries were displayed.
```

3. 古い各ノードのポートとLIFの情報を収集します。

   ノードごとに次のコマンドの出力を収集する必要があります。

   - 'network interface show -role cluster, node-mgmt
   - 'network port show -node node_name -type physical ’
   - 'network port vlan show -node -node-name _`
   - 「 network port ifgrp show -node node_name 」 - instance 」を指定します

- 「 network port broadcast-domain show 」
- 「 network port reachability show-detail` 」と表示されます
- network ipspace show
- volume show
- 「 storage aggregate show
- 「 system node run -node _node-name_sysconfig -a 」のように入力します

4. MetroCluster ノードが SAN 構成になっている場合は、関連情報を収集します。

   次のコマンドの出力を収集する必要があります。

   - 「 fcp adapter show -instance 」のように表示されます
   - 「 fcp interface show -instance 」の略
   - 「 iscsi interface show 」と表示されます
   - ucadmin show

5. ルートボリュームが暗号化されている場合は、 key-manager に使用するパスフレーズを収集して保存します。

   「 securitykey-manager backup show 」を参照してください

6. MetroCluster ノードがボリュームまたはアグリゲートに暗号化を使用している場合は、キーとパスフレーズに関する情報をコピーします。

   追加情報の場合は、を参照してください "オンボードキー管理情報の手動でのバックアップ"。

   a. オンボードキーマネージャが設定されている場合：

      「 securitykey manager onboard show-backup 」を参照してください

      パスフレーズは、あとでアップグレード手順で必要になります。

   b. Enterprise Key Management （ KMIP ）が設定されている場合は、次のコマンドを問題で実行します。

      「 securitykey-manager external show -instance 」

   「セキュリティキーマネージャのキークエリ」

Tiebreaker またはその他の監視ソフトウェアから既存の設定を削除します

スイッチオーバーを開始できる MetroCluster Tiebreaker 構成や他社製アプリケーション（ ClusterLion など）で既存の構成を監視している場合は、移行の前に Tiebreaker またはその他のソフトウェアから MetroCluster 構成を削除する必要があります。

手順

1. Tiebreaker ソフトウェアから既存の MetroCluster 設定を削除します。

   "MetroCluster 構成を削除"

2. スイッチオーバーを開始できるサードパーティ製アプリケーションから既存の MetroCluster 構成を削除します。

   アプリケーションのマニュアルを参照してください。

カスタム **AutoSupport** メッセージをメンテナンス前に送信する

メンテナンスを実行する前に、 AutoSupport an 問題 message to notify NetApp technical support that maintenance is maintenancing （メンテナンスが進行中であることをネットアップテクニカルサポートに通知する）を実行システム停止が発生したとみなしてテクニカルサポートがケースをオープンしないように、メンテナンスが進行中であることを通知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 サイトごとに実行する必要があります。

手順

1. サポートケースが自動で生成されないようにするには、メンテナンスが進行中であることを示す AutoSupport メッセージを送信します。

   a. 次のコマンドを問題に設定します。

      「 system node AutoSupport invoke -node * -type all -message MAINT= *maintenance-window-in-hours* 」というメッセージが表示されます

      「メンテナンス時間」では、メンテナンス時間の長さを最大 72 時間指定します。この時間が経過する前にメンテナンスが完了した場合は、メンテナンス期間が終了したことを通知する AutoSupport メッセージを起動できます。

   「 system node AutoSupport invoke -node * -type all -message MAINT= end 」というメッセージが表示されます

   a. パートナークラスタに対してこのコマンドを繰り返します。

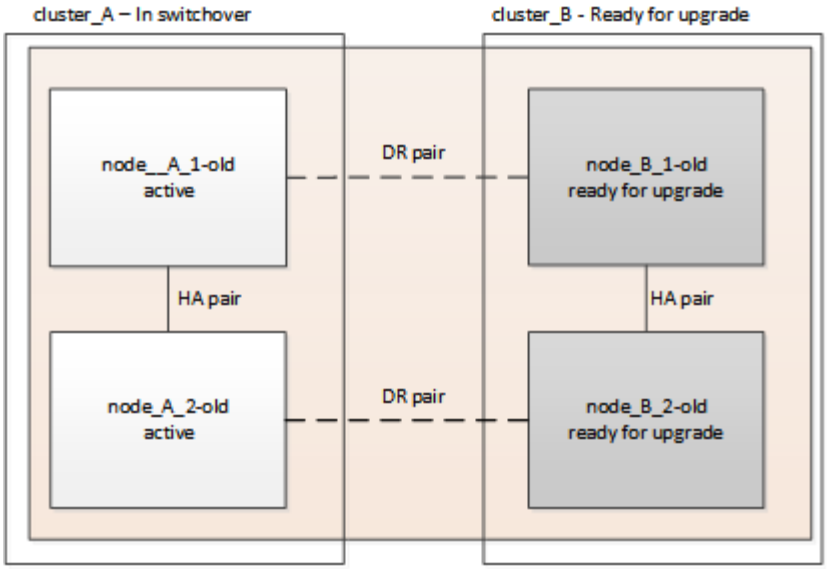
MetroCluster 構成をスイッチオーバーします

site_B のプラットフォームをアップグレードできるように、設定を site_A にスイッチオーバーする必要があります。

このタスクについて

このタスクは site_A で実行する必要があります

このタスクを完了すると、 cluster_A はアクティブになり、両方のサイトでデータを提供します。cluster_B は非アクティブで、次の図に示すようにアップグレードプロセスを開始できます。



手順

1. site_B のノードをアップグレードできるように、 MetroCluster 構成を site_A にスイッチオーバーします。

   a. 構成に一致するオプションを選択し、cluster_Aの正しいコマンドを問題 します。

      オプション**1**：**ONTAP 9.8**以降を実行する**4**ノードまたは**8**ノードの**FC**構成

      次のコマンドを実行します。 `metrocluster switchover -controller-replacement true`

      オプション**2**：**ONTAP 9.3**以降を実行する**2**ノード**FC**構成

      次のコマンドを実行します。 `metrocluster switchover`

      この処理が完了するまでに数分かかることがあります。

   b. スイッチオーバー処理を監視します。

      「 MetroCluster operation show 」を参照してください

   c. 処理が完了したら、ノードがスイッチオーバー状態であることを確認します。

      「 MetroCluster show 」

   d. MetroCluster ノードのステータスを確認します。

      MetroCluster node show

2. データアグリゲートを修復します。

   a. データアグリゲートを修復します。

      MetroCluster は ' データ・アグリゲートを修復します

   b. 正常なクラスタで MetroCluster operation show コマンドを実行して、修復操作が完了したことを確認

します。

```
cluster_A::> metrocluster operation show
  Operation: heal-aggregates
      State: successful
 Start Time: 7/29/2020 20:54:41
   End Time: 7/29/2020 20:54:42
     Errors: -
```

3. ルートアグリゲートを修復します。
   a. データ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

   b. 正常なクラスタで MetroCluster operation show コマンドを実行して、修復操作が完了したことを確認します。

```
cluster_A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2020 20:58:41
   End Time: 7/29/2020 20:59:42
     Errors: -
```

古いコントローラのネットワーク構成を準備

新しいコントローラでネットワークが正常に再開されるようにするには、 LIF を共通ポートに移動して、古いコントローラのネットワーク設定を削除する必要があります。

このタスクについて

- このタスクは、古いノードごとに実行する必要があります。
- で収集した情報を使用します "古いノードから新しいノードへのポートのマッピング"。

手順

1. 古いノードをブートし、ノードにログインします。

   「 boot_ontap 」

2. 古いコントローラのすべてのデータ LIF のホームポートを、新旧両方のコントローラモジュールで同じ共通ポートに割り当てます。
   a. LIF を表示します。

      「 network interface show 」を参照してください

      SAN と NAS を含むすべてのデータ LIF は、スイッチオーバーサイト（ cluster_A ）で稼働しているた

め、管理上および運用上のダウン状態になります。

b. の出力を確認して、クラスタポートとして使用されていない新旧両方のコントローラで同じ共通の物理ネットワークポートを特定します。

たとえば、 e0d は古いコントローラの物理ポートで、新しいコントローラにも存在します。e0d は、クラスタポート、または新しいコントローラ上で使用されません。

プラットフォームモデルのポートの用途については、を参照してください "NetApp Hardware Universe の略"

c. すべてのデータ LIF で共通ポートをホームポートとして使用するように変更します。

「 network interface modify -vserver *svm -name _ -lif data -lif lif _ -home-port_port -id* 」と入力します

次の例では、これは「 e0d 」です。

例：

```
network interface modify -vserver vs0 -lif datalif1 -home-port e0d
```

3. ブロードキャストドメインを変更して、削除する必要がある VLAN と物理ポートを削除します。

「 broadcast-domain remove-ports -broadcast-domain_domain-name-name_ports_node-name ： port-id_` 」

すべての VLAN ポートと物理ポートについて、この手順を繰り返します。

4. クラスタポートをメンバーポートとして使用し、 ifgrp をメンバーポートとして使用している VLAN ポートを削除します。

a. VLAN ポートを削除します。

「 network port vlan delete -node-node-name-vlan-name_portid -vlandid_ 」のように指定します

例：

```
network port vlan delete -node node1 -vlan-name e1c-80
```

b. インターフェイスグループから物理ポートを削除します。

「 network port ifgrp remove-port -node-node_name -ifgrp_interface-group-name _ *port_portid* 」の形式で指定します

例：

```
network port ifgrp remove-port -node node1 -ifgrp a1a -port e0d
```

a. ブロードキャストドメインから VLAN ポートとインターフェイスグループポートを削除します。

'network port broadcast-domain remove-ports -ipspace_ipspace -broadcast-domain_domain -name_ports_nodename ： portname 、 nodename ： portname _ 、

b. 必要に応じて、他の物理ポートをメンバーとして使用するようにインターフェイスグループポートを変更します。

ifgrp add-port -node node_name -ifgrp *interface -group-name_port_port-id*`

5. ノードを停止します。

halt -inhibit-takeover true -node node_name `

この手順は両方のノードで実行する必要があります。

古いプラットフォームを削除する

古いコントローラを構成から削除しておく必要があります。

このタスクについて

このタスクは site_B で実行します

手順

1. site_B の古いコントローラのシリアルコンソール（ node_B_1 古いコントローラと node_B_2 古いコントローラ）に接続し、 LOADER プロンプトが表示されていることを確認します。
2. node_B_1 古いと node_B_2 のストレージ接続とネットワーク接続を切断し、新しいノードに再接続できるようにケーブルにラベルを付けます。
3. node_B_1 から古いおよび node_B_2 から電源ケーブルを外します。
4. node_B_1 古いコントローラと node_B_2 の古いコントローラをラックから取り外します。

新しいコントローラを設定します

コントローラをラックに設置して設置し、メンテナンスモードで必要なセットアップを実行してから、コントローラをブートし、コントローラの LIF の設定を確認する必要があります。

新しいコントローラをセットアップ

新しいコントローラをラックに設置してケーブルを接続する必要があります。

手順

1. 必要に応じて、新しいコントローラモジュールとストレージシェルフ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、構成内のストレージシェルフ数によって異なります。

2. 自身の適切な接地対策を行います
3. コントローラモジュールをラックまたはキャビネットに設置します。

"ONTAPハードウェアシステムのドキュメント"

4. 新しいコントローラモジュールに固有の FC-VI カードがない場合、および古いコントローラの FC-VI カードに新しいコントローラの互換性がある場合は、 FC-VI カードを交換し、正しいスロットに取り付けます。

   を参照してください "NetApp Hardware Universe の略" を参照してください。

5. コントローラの電源、シリアルコンソール、および管理接続を、 MetroCluster インストールおよび設定ガイド _ の説明に従ってケーブル接続します。

   この時点で古いコントローラから切断されていた他のケーブルは接続しないでください。

   "ONTAPハードウェアシステムのドキュメント"

6. 新しいノードに電源を投入し、 LOADER プロンプトを表示するよう求められたら Ctrl+C キーを押します。

新しいコントローラをネットブート

新しいノードを設置したら、ネットブートを実行して、新しいノードが元のノードと同じバージョンの ONTAP を実行するようにする必要があります。ネットブートという用語は、リモート・サーバに保存された ONTAP イメージからブートすることを意味します。ネットブートの準備を行うときは、システムがアクセスできる Web サーバに、 ONTAP 9 ブート・イメージのコピーを配置する必要があります。

このタスクは、新しい各コントローラモジュールで実行します。

手順

1. にアクセスします "ネットアップサポートサイト" システムのネットブートの実行に使用するファイルをダウンロードするには、次の手順を実行します。
2. ネットアップサポートサイトのソフトウェアダウンロードセクションから該当する ONTAP ソフトウェアをダウンロードし、 Web にアクセスできるディレクトリに image.tgz ファイルを保存します。
3. Web にアクセスできるディレクトリに移動し、必要なファイルが利用可能であることを確認します。

プラットフォームモデル	作業
FAS/AFF8000 シリーズシステム	ターゲットディレクトリに version_image.tgzfile の内容を展開します。 tar -zxvf ONTAP-version _image.tgz 注： Windows で内容を展開する場合は、 7-Zip または WinRAR を使用してネットブートイメージを展開します。ディレクトリの一覧に、カーネルファイル netboot/ kernel を含むネットブートフォルダが表示される必要があります
その他すべてのシステム	ディレクトリの一覧に、カーネルファイルがあるネットブートフォルダを含める必要があります。 ONTAP-version _image.tgz ファイルを展開する必要はありません。

4. LOADER プロンプトで、管理 LIF のネットブート接続を設定します。
   - IP アドレスが DHCP の場合は、自動接続を設定します。

ifconfig e0M -auto

- IP アドレスが静的な場合は、手動接続を設定します。

  ifconfig e0M -addr= ip_addr-mask= netmask `-gw= gateway `

5. ネットブートを実行します。
   - プラットフォームが 80xx シリーズシステムの場合は、次のコマンドを使用します。

     netboot\http://web_server_ip/path_to_web-accessible_directory/netboot/kernel`

   - プラットフォームが他のシステムの場合は、次のコマンドを使用します。

     netboot\http://web_server_ip/path_to_web-accessible_directory/ontap-version_image.tgz`

6. ブートメニューからオプション * （７） Install new software first * を選択し、新しいソフトウェアイメージをダウンロードしてブートデバイスにインストールします。

```
 Disregard the following message: "This procedure is not supported for
Non-Disruptive Upgrade on an HA pair". It applies to nondisruptive
upgrades of software, not to upgrades of controllers.
```

．手順を続行するかどうかを確認するメッセージが表示されたら、「 `y` 」と入力し、パッケージの入力を求められたらイメージファイルの `URL` 「 `¥ http://web_server_ip/path_to_web-accessible_directory/ontap-version_image.tgz` 」を入力します

```
Enter username/password if applicable, or press Enter to continue.
```

7. 入力 `n` 次のようなプロンプトが表示されたら、バックアップの回復をスキップします。

```
Do you want to restore the backup configuration now? {y|n} n
```

8. 次のようなプロンプトが表示されたら 'y' と入力して再起動します

```
The node must be rebooted to start using the newly installed software.
Do you want to reboot now? {y|n} y
```

新しくインストールされたソフトウェアを使用するには、ノードを再起動する必要があります。

コントローラモジュールの設定をクリアします

MetroCluster 構成で新しいコントローラモジュールを使用する前に、既存の構成をクリアする必要があります。

手順

1. 必要に応じて、ノードを停止してプロンプトを表示し `LOADER`ます。

   「 halt 」

2. `LOADER`プロンプトで、環境変数をデフォルト値に設定します。

   「デフォルト設定」

3. 環境を保存します。

   'aveenv

4. `LOADER`プロンプトでブートメニューを起動します。

   「 boot_ontap menu

5. ブートメニューのプロンプトで、設定を消去します。

   wipeconfig

   確認プロンプトに「 yes 」と応答します。

   ノードがリブートし、もう一度ブートメニューが表示されます。

6. ブートメニューでオプション * 5 * を選択し、システムをメンテナンスモードでブートします。

   確認プロンプトに「 yes 」と応答します。

HBA 構成をリストア

コントローラモジュールに HBA カードが搭載されているかどうかや設定によっては、サイトで使用するために正しく設定する必要があります。

手順

1. メンテナンスモードで、システム内の HBA の設定を行います。

   a. ucadmin show と入力し、各ポートの現在の設定を確認します

   b. 必要に応じてポートの設定を更新します。

HBA のタイプと目的のモード	使用するコマンド
CNA FC	ucadmin modify -m fc -t initiator_adapter-name _ `
CNA イーサネット	ucadmin modify -mode cna_adapter-name_`
FC ターゲット	fcadmin config -t target_adapter-name_`
FC イニシエータ	fcadmin config -t initiator_adapter-name_`

2. メンテナンスモードを終了します。

   「 halt 」

   コマンドの実行後、ノードが LOADER プロンプトで停止するまで待ちます。

3. ノードをブートしてメンテナンスモードに戻り、設定の変更が反映されるようにします。

   「 boot_ontap maint 」を使用してください

4. 変更内容を確認します。

HBA のタイプ	使用するコマンド
CNA	ucadmin show
FC	fcadmin show`

新しいコントローラとシャーシで **HA** 状態を設定

コントローラとシャーシの HA 状態を確認し、必要に応じてシステム構成に合わせて更新する必要があります。

手順

1. メンテナンスモードで、コントローラモジュールとシャーシの HA 状態を表示します。

   「 ha-config show 」

   すべてのコンポーネントの HA の状態が mcc である必要があります。

MetroCluster 構成の内容	HA の状態
2 ノード	mcc-2n
4 ノードまたは 8 ノード	MCC

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とシャーシの HA 状態を設定します。

MetroCluster 構成の内容	問題コマンド
• 2 ノード *	「 ha-config modify controller mcc-2n 」という形式で指定します 「 ha-config modify chassis mcc-2n 」というようになりました

• 4 ノードまたは 8 ノード *	「 ha-config modify controller mcc 」 「 ha-config modify chassis mcc 」

ルートアグリゲートディスクを再割り当てします

前の手順で確認したシステム ID を使用して、ルートアグリゲートディスクを新しいコントローラモジュールに再割り当てします

このタスクについて

このタスクはメンテナンスモードで実行します。

古いシステムIDはで特定しました "アップグレード前に情報を収集"。

この手順の例では、次のシステム ID を持つコントローラを使用します。

ノード	古いシステム ID	新しいシステム ID
node_B_1	4068741254	1574774970

手順

1. 他のすべての接続を新しいコントローラモジュール（ FC-VI 、ストレージ、クラスタインターコネクトなど）にケーブル接続します。
2. システムを停止し、 LOADER プロンプトからメンテナンスモードでブートします。

   「 boot_ontap maint 」を使用してください

3. node_B_1 古いが所有するディスクを表示します。

   「ディスクショー - A` 」

   コマンド出力に、新しいコントローラモジュール（ 1574774970 ）のシステム ID が表示されます。ただし、ルートアグリゲートディスクは古いシステム ID （ 4068741254 ）で所有されます。この例で表示されているのは、 MetroCluster 構成の他のノードが所有するドライブではありません。

```
*> disk show -a
Local System ID: 1574774970

  DISK         OWNER                      POOL   SERIAL NUMBER    HOME
DR HOME
------------   -------------              -----  -------------
-------------             -------------
...
rr18:9.126L44 node_B_1-old(4068741254)   Pool1  PZHYN0MD
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:9.126L49 node_B_1-old(4068741254)   Pool1  PPG3J5HA
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L21 node_B_1-old(4068741254)   Pool1  PZHTDSZD
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L2  node_B_1-old(4068741254)   Pool0  S0M1J2CF
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L3  node_B_1-old(4068741254)   Pool0  S0M0CQM5
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:9.126L27 node_B_1-old(4068741254)   Pool0  S0M1PSDW
node_B_1-old(4068741254)  node_B_1-old(4068741254)
...
```

4. ドライブシェルフのルートアグリゲートディスクを新しいコントローラに再割り当てします。

   「ディスクの再割り当て -s *old-sysid*-d_new-sysid_`

   次の例は、ドライブの再割り当てを示しています。

```
*> disk reassign -s 4068741254 -d 1574774970
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)? n

After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)? Jul 14 19:23:49
[localhost:config.bridge.extra.port:error]: Both FC ports of FC-to-SAS
bridge rtp-fc02-41-rr18:9.126L0 S/N [FB7500N107692] are attached to this
controller.
y
Disk ownership will be updated on all disks previously belonging to
Filer with sysid 4068741254.
Do you want to continue (y/n)? y
```

5. すべてのディスクが想定どおりに再割り当てされていることを確認します。

   「ディスクショー」

```
*> disk show
Local System ID: 1574774970

  DISK         OWNER                      POOL   SERIAL NUMBER   HOME
DR HOME
------------  -------------              -----  -------------
-------------              -------------
rr18:8.126L18 node_B_1-new(1574774970)   Pool1  PZHYN0MD
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:9.126L49 node_B_1-new(1574774970)   Pool1  PPG3J5HA
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L21 node_B_1-new(1574774970)   Pool1  PZHTDSZD
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L2  node_B_1-new(1574774970)   Pool0  S0M1J2CF
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:9.126L29 node_B_1-new(1574774970)   Pool0  S0M0CQM5
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L1  node_B_1-new(1574774970)   Pool0  S0M1PSDW
node_B_1-new(1574774970)  node_B_1-new(1574774970)
*>
```

6. アグリゲートのステータスを表示します。

   「 aggr status 」を入力します

```
*> aggr status
           Aggr             State       Status            Options
aggr0_node_b_1-root    online      raid_dp, aggr    root, nosnap=on,
                           mirrored
mirror_resync_priority=high(fixed)
                           fast zeroed
                           64-bit
```

7. パートナーノードで上記の手順を繰り返します（ node_B_2 - 新規）。

新しいコントローラをブートします

コントローラのフラッシュイメージを更新するには、ブートメニューからコントローラをリブートする必要があります。暗号化が設定されている場合は、追加の手順が必要です。

このタスクについて

このタスクはすべての新しいコントローラで実行する必要があります。

手順

1. ノードを停止します。

   「 halt 」

2. 外部キー管理ツールが設定されている場合は、関連する bootargs を設定します。

   'setenv bootarg.kmip.init.ipaddr *ip-address*'

   'setenv bootarg.kmip.init.netmask *netmask*`

   'setenv bootarg.kmip.init.gateway *gateway-address*

   'setenv bootarg.kmip.init.interface *interface-id*

3. ブートメニューを表示します。

   「 boot_ontap menu

4. ルート暗号化を使用する場合は、使用している ONTAP のバージョンに応じて、キー管理設定のブートメニューオプションまたは問題 the boot menu コマンドを選択します。

ONTAP 9.8以降

ONTAP 9.8 以降では、ブート・メニュー・オプションを選択します。

使用するポート	選択するブートメニューオプション
オンボードキー管理	オプション "10 `" プロンプトに従って、キー管理ツールの構成をリカバリおよびリストアするために必要な入力を指定します。
外部キー管理	オプション "11`" プロンプトに従って、キー管理ツールの構成をリカバリおよびリストアするために必要な入力を指定します。

ONTAP 9.7以前

ONTAP 9.7以前の場合は、ブートメニューコマンドを問題します。

使用するポート	問題ブートメニュープロンプトでのコマンド
オンボードキー管理	「 recover _onboard keymanager 」を参照してください
外部キー管理	「 RE_EXTERNAL_KEYmanager 」と入力します

5. AUTOBOOT が有効になっている場合は、 CTRL-C を押して AUTOBOOT を中断します
6. ブートメニューからオプション "6`" を実行します

   オプション "6`" を選択すると ' 完了前にノードが 2 回再起動されます

   システム ID 変更プロンプトに「 y 」と入力します。2 回目のリブートメッセージが表示されるまで待ちます。

```
Successfully restored env file from boot media...

Rebooting to load the restored env file...
```

7. partner-sysid が正しいことを確認します。

   printenv partner-sysid

   partner-sysid が正しくない場合は、次のように設定します。

'setenv partner-sysid_partner-SysID_`

8. ルート暗号問題化を使用する場合は、使用している ONTAP のバージョンに応じて、キー管理設定に対してブートメニューオプションを選択するか、ブートメニューコマンドを再度実行します。

ONTAP 9.8以降

ONTAP 9.8 以降では、ブート・メニュー・オプションを選択します。

使用するポート	選択するブートメニューオプション
オンボードキー管理	オプション "10 `" プロンプトに従って、キー管理ツールの構成をリカバリおよびリストアするために必要な入力を指定します。
外部キー管理	オプション "11`" プロンプトに従って、キー管理ツールの構成をリカバリおよびリストアするために必要な入力を指定します。

キー・マネージャの設定に応じて '10 またはオプション 11 を選択し ' 最初のブート・メニュー・プロンプトでオプション 6 を選択して 'recovery 手順を実行しますノードを完全にブートするには ' オプション "1" によって続行されるリカバリ手順 (通常のブート) を繰り返す必要がある場合があります

ONTAP 9.7以前

ONTAP 9.7以前の場合は、ブートメニューコマンドを問題します。

使用するポート	問題ブートメニュープロンプトでのコマンド
オンボードキー管理	「 recover _onboard keymanager 」を参照してください
外部キー管理	「 RE_EXTERNAL_KEYmanager 」と入力します

ノードが完全にブートするまで、ブートメニュープロンプトで「 recover_xxxxxxxx_keymanager 」コマンドを何度も問題に接続する必要がある場合があります。

9. ノードをブートします。

「 boot_ontap 」

10. 交換したノードがブートするまで待ちます。

いずれかのノードがテイクオーバーモードの場合は、ギブバックを実行します。

「 storage failover giveback 」を参照してください

11. すべてのポートがブロードキャストドメインに属していることを確認します。

    a. ブロードキャストドメインを表示します。

       「 network port broadcast-domain show 」

    b. 必要に応じて、ブロードキャストドメインにポートを追加します。

       "ブロードキャストドメインのポートを追加または削除します"

    c. インタークラスタ LIF をホストする物理ポートを対応するブロードキャストドメインに追加します。

    d. 新しい物理ポートをホームポートとして使用するようにクラスタ間 LIF を変更します。

    e. クラスタ間 LIF が起動したら、クラスタピアのステータスを確認し、必要に応じてクラスタピアリングを再確立します。

       クラスタピアリングの再設定が必要になる場合があります。

       "クラスタピア関係を作成します。"

    f. 必要に応じて、 VLAN とインターフェイスグループを再作成します。

       VLAN およびインターフェイスグループのメンバーシップは、古いノードと異なる場合があります。

       "VLANを作成します。"

    "物理ポートを組み合わせてインターフェイスグループを作成"

12. 暗号化を使用する場合は、キー管理設定に対応したコマンドを使用してキーをリストアします。

使用するポート	使用するコマンド
オンボードキー管理	「セキュリティキーマネージャオンボード同期」 詳細については、を参照してください "オンボードキー管理の暗号化キーのリストア"。
外部キー管理	「 securitykey manager external restore -vserver *svm*-node __ key -server_host_name

LIF の設定を確認

スイッチバックの前に、 LIF が適切なノード / ポートにホストされていることを確認します。次の手順を実行する必要があります

このタスクについて

このタスクは site_B で実行します。ノードはルートアグリゲートでブートされています。

手順

1. スイッチバックの前に、 LIF が適切なノードとポートにホストされていることを確認します。

   a. advanced 権限レベルに切り替えます。

      「 advanced 」の権限が必要です

   b. ポート設定を無視して LIF が適切に配置されるようにします。

      「 vserver config override command 」 network interface modify -vserver vserver_name __ -home -node _active_port_after_upgrade _ -lif LIF_name -home-node _new_node_name _

   「 vserver config override 」コマンド内で「 network interface modify 」コマンドを入力する場合、 Tab autoccomplete 機能は使用できません。autoccomplete を使用して「 network interface modify 」を作成し、「 vserver config override 」コマンドで囲むことができます。

   a. admin 権限レベルに戻ります。 `+set -privilege admin`

2. インターフェイスをホームノードにリバートします。

   「 network interface revert * -vserver_vserver-name に指定します

   必要に応じて、すべての SVM でこの手順を実行します。

新しいライセンスをインストールします

スイッチバック処理の前に、新しいコントローラのライセンスをインストールする必要があります。

手順

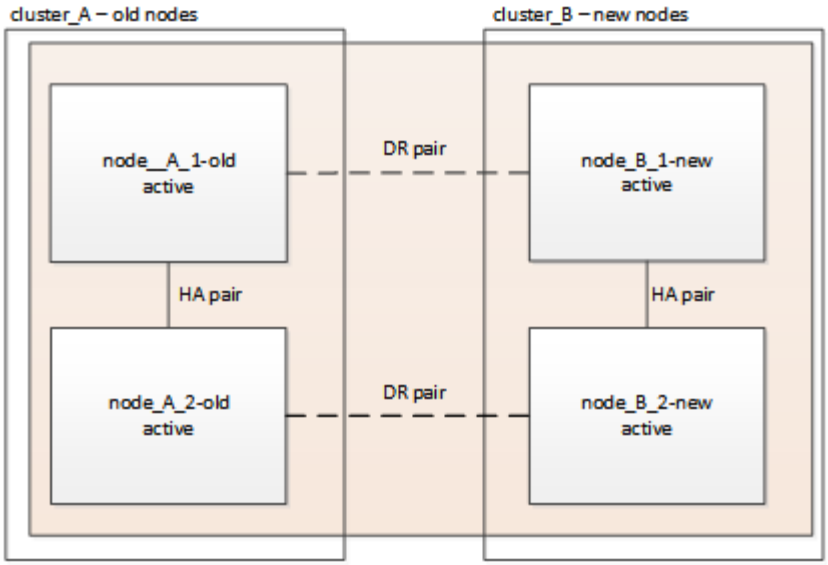
1. "新しいコントローラモジュール用のライセンスをインストールしています"

MetroCluster 構成をスイッチバックします

新しいコントローラを設定したら、 MetroCluster 構成をスイッチバックして構成を通常動作に戻します。

このタスクについて

このタスクでは、スイッチバック処理を実行して MetroCluster 構成を通常動作に戻します。site_A のノードはまだアップグレード待ちです。



手順

1. site_B の MetroCluster node show コマンドを問題し ' 出力を確認します
   a. 新しいノードが正しく表示されることを確認します。
   b. 新しいノードの状態が「 Waiting for switchback 」であることを確認します。
2. クラスタをスイッチバックします。

   MetroCluster スイッチバック

3. スイッチバック処理の進捗を確認します。

   「 MetroCluster show 」

   出力に「 waiting-for-switchback 」と表示されたら、スイッチバック処理はまだ進行中です。

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                switchover
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                waiting-for-switchback
                          AUSO Failure Domain -
```

   出力に「 normal 」と表示された場合、スイッチバック処理は完了しています。

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
```

スイッチバックが完了するまでに時間がかかる場合は、「 MetroCluster config-replication resync-status show 」コマンドを使用することで、進行中のベースラインのステータスを確認できます。このコマンドは、 advanced 権限レベルで実行します。

MetroCluster 構成の健全性を確認します

コントローラモジュールをアップグレードしたら、 MetroCluster 構成の健全性を確認する必要があります。

このタスクについて

このタスクは、 MetroCluster 構成の任意のノードで実行できます。

手順

1. MetroCluster 構成の動作を確認します。

   a. MetroCluster 構成と運用モードが正常な状態であることを確認します。

      「 MetroCluster show 」

   b. MetroCluster チェックを実行します。

      「 MetroCluster check run 」のようになります

   c. MetroCluster チェックの結果を表示します。

      MetroCluster チェックショー

      MetroCluster check runとMetroCluster check showを実行すると'次のようなエラーメッセージが表示されます

例

```
Failed to validate the node and cluster components before the switchover
operation.
                  Cluster_A:: node_A_1 (non-overridable veto): DR
partner NVLog mirroring is not online. Make sure that the links between
the two sites are healthy and properly configured.
```

+
これは、アップグレードプロセス時にコントローラが一致しないことが原因で想定される動作であり、エラーメッセージが無視しても問題ありません。

cluster_Aのノードをアップグレードします。

cluster_A についてもアップグレード手順を繰り返す必要があります

ステップ

1. cluster_Aのノードをアップグレードするために、上記の手順を繰り返し"アップグレードを準備"ます。

   手順を繰り返すと、クラスターとノードへの参照がすべて逆になります。例えば、cluster_Aからのスイッチオーバーの例は、cluster_Bからのスイッチオーバーになります。

カスタム AutoSupport メッセージをメンテナンス後に送信します

アップグレードの完了後、ケースの自動作成を再開できるように、メンテナンスの終了を通知する AutoSupport メッセージを送信する必要があります。

ステップ

1. サポートケースの自動生成を再開するには、メンテナンスが完了したことを示す AutoSupport メッセージを送信します。

   a. 次のコマンドを問題に設定します。

      「 system node AutoSupport invoke -node * -type all -message MAINT= end 」というメッセージが表示されます

   b. パートナークラスタに対してこのコマンドを繰り返します。

Tiebreaker による監視をリストアします

MetroCluster 構成が Tiebreaker ソフトウェアで監視するように設定されている場合は、 Tiebreaker 接続をリストアできます。

1. 以下の手順で "MetroCluster 構成を追加" *MetroCluster Tiebreaker* のインストールと構成 を参照してください。

スイッチオーバーとスイッチバックを使用して、MetroCluster FC構成のAFF A700 / FAS9000からAFF A900/ FAS9500にコントローラをアップグレード（ONTAP 9.10.1以降）

MetroCluster スイッチオーバー処理を使用すると、パートナークラスタのコントローラモジュールのアップグレード中もクライアントに無停止でサービスを提供できます。この手順の一部として他のコンポーネント（ストレージシェルフやスイッチなど）をアップグレードすることはできません。

このタスクについて

- この手順は、コントローラのアップグレードにのみ使用できます。

  ストレージシェルフやスイッチなど、構成内の他のコンポーネントも同時にアップグレードすることはできません。

- この手順 ONTAP を使用して、AFF A700からAFF 9.10.1以降を搭載したA900にアップグレードできます。
- この手順 を使用して、ONTAP 9.10.1P3以降を搭載したFAS9000をFAS9500にアップグレードできます。
  - ONTAP 9.10.1 以降では、 4 ノードと 8 ノードの構成がサポートされます。

    AFF A900 システムは、 ONTAP 9.10.1 以降でのみサポートされます。

  "NetApp Hardware Universe の略"

- 構成内のすべてのコントローラは、同じメンテナンス期間にアップグレードする必要があります。

  次の表に、コントローラのアップグレードでサポートされるモデルマトリックスを示します。

旧プラットフォームモデル	新しいプラットフォームモデル
• AFF A700	• AFF A900 の略
• FAS9000	• FAS9500

- アップグレード用の手順では、 RCF やケーブル接続の物理的な変更を含めて、 MetroCluster ファブリックを変更する必要があります。RCF およびケーブル接続の変更は、コントローラのアップグレード前に実行できます。
- このアップグレード手順では、元のノードと新しいノードの間のストレージ接続、 FC 接続、イーサネット接続を変更する必要はありません。
- 手順 のアップグレード中は、AFF A700またはFAS9000システムに他のカードを追加したり取り外したりしないでください。詳細については、を参照してください "NetApp Hardware Universe の略"

この手順 の例と図では、次の名前が使用されています。

- site_A
  - アップグレード前：
    - node_A_1 - A700
    - Node_a_2-A700
  - アップグレード後：
    - node_A_1 - A900
    - Node_a_2-A900
- site_B
  - アップグレード前：
    - node_B_1 - A700

        - node_B_2 - A700
    - アップグレード後：
        - Node_B_1-A900
        - node_B_2 - A900

コンソールログを有効にする

NetAppでは、使用しているデバイスでコンソールロギングをイネーブルにし、この手順を実行する際に次のアクションを実行することを強く推奨します。

- メンテナンス中はAutoSupportを有効のままにします。
- メンテナンスの前後にメンテナンスAutoSupportメッセージをトリガーして、メンテナンスアクティビティ中にケースの作成を無効にします。

  ナレッジベースの記事を参照してください "スケジュールされたメンテナンス時間中にケースの自動作成を停止する方法"。

- 任意のCLIセッションのセッションロギングをイネーブルにします。セッションログを有効にする方法については、ナレッジベースの記事の「セッション出力のログ」セクションを参照してください "ONTAPシステムへの接続を最適化するためのPuTTYの設定方法"。

アップグレードを準備

既存のMetroCluster 構成に変更を加える前に、構成の健全性を確認し、RCFファイルとケーブル接続をAFF A900またはFAS9000ファブリックのMetroCluster 構成に必要な新しいポート接続トポロジに変更し、その他のタスクを実行する必要があります。

AFF A700 コントローラのスロット 7 をクリアします

AFF A900またはFAS9500のMetroCluster 構成では、スロット5と7のFC-VIカードに8つのFC-VIポートが必要です。アップグレードを開始する前に、AFF A700またはFAS9000のスロット7にカードがある場合は、それらをクラスタのすべてのノード用の他のスロットに移動する必要があります。

MetroCluster 構成の健全性を確認

AFF A900またはFAS9500ファブリックのMetroCluster 構成用にRCFファイルを更新してケーブル接続する前に、構成の健全性と接続を確認する必要があります。

> 最初のサイトでコントローラをアップグレードした後、2番目のサイトをアップグレードする前に、 `metrocluster check run`に続く `metrocluster check show`エラーを返します `config-replication`フィールド。このエラーは、各サイトのノード間でNVRAMのサイズが一致していないことを示しています。これは、両サイトで異なるプラットフォームモデルが存在する場合に想定される動作です。DRグループ内のすべてのノードでコントローラーのアップグレードが完了するまで、このエラーは無視できます。

手順

1. ONTAP で MetroCluster 構成の動作を確認します。

    a. ノードがマルチパスであるかどうかを確認します。 `+node run -node node_name sysconfig`

-a

このコマンドは、 MetroCluster 構成のノードごとに問題で実行する必要があります。

b. 構成に破損ディスクがないことを確認します。

「 storage disk show -broken 」

このコマンドは、 MetroCluster 構成の各ノードで問題を実行する必要があります。

c. ヘルスアラートがないかどうかを確認します。

「 system health alert show 」というメッセージが表示されます

このコマンドは、各クラスタで問題を実行する必要があります。

d. クラスタのライセンスを確認します。

「 system license show 」を参照してください

このコマンドは、各クラスタで問題を実行する必要があります。

e. ノードに接続されているデバイスを確認します。

「 network device-discovery show 」のように表示されます

このコマンドは、各クラスタで問題を実行する必要があります。

f. 両方のサイトでタイムゾーンと時間が正しく設定されていることを確認します。

cluster date show

このコマンドは、各クラスタで問題を実行する必要があります。時刻とタイムゾーンを設定するには 'cluster date コマンドを使用します

2. スイッチにヘルスアラートがないかどうかを確認します（ある場合）。

「 storage switch show 」と表示されます

このコマンドは、各クラスタで問題を実行する必要があります。

3. MetroCluster 構成の運用モードを確認し、 MetroCluster チェックを実行

a. MetroCluster 構成と運用モードが正常な状態であることを確認します。

「 MetroCluster show 」

b. 想定されるすべてのノードが表示されることを確認します。

MetroCluster node show

c. 次のコマンドを問題に設定します。

「 MetroCluster check run 」のようになります

d. MetroCluster チェックの結果を表示します。

MetroCluster チェックショー

4. Config Advisor ツールを使用して MetroCluster のケーブル接続を確認します。

a. Config Advisor をダウンロードして実行します。

"ネットアップのダウンロード： Config Advisor"

b. Config Advisor の実行後、ツールの出力を確認し、推奨される方法で検出された問題に対処します。

ファブリックスイッチの **RCF** ファイルを更新します

AFF A900またはFAS9500ファブリックのMetroCluster では、ノードごとに2つの4ポートFC-VIアダプタが必要です。AFF A700で必要な4ポートFC-VIアダプタは1つだけです。AFF A900またはFAS9500コントローラへのコントローラのアップグレードを開始する前に、ファブリックスイッチのRCFファイルを変更して、AFF A900またはFAS9500接続トポロジをサポートする必要があります。

1. から "MetroCluster の RCF ファイルのダウンロードページ"で、AFF A900またはFAS9500ファブリックのMetroCluster と、AFF A700またはFAS9000構成で使用されているスイッチモデルに対応した正しいRCFファイルをダウンロードします。
2. の手順に従って、ファブリック A のスイッチ、スイッチ A1 、およびスイッチ B1 の RCF ファイルを更新します "FC スイッチを設定します"。

> AFF A900またはFAS9500ファブリックのMetroCluster 構成をサポートするためのRCFファイルの更新では、AFF A700またはFAS9000ファブリックのMetroCluster 構成に使用されるポートと接続には影響しません。

3. ファブリック A のスイッチで RCF ファイルを更新したら、ストレージと FC-VI のすべての接続をオンラインにする必要があります。FC-VI 接続を確認します。

MetroCluster interconnect mirror show

a. ローカル・サイト・ディスクとリモート・サイト・ディスクが sysconfig 出力結果に表示されていることを確認します

4. ファブリック A スイッチの MetroCluster ファイル更新後に、 が正常な状態であることを確認する必要があります。

a. メトロ・クラスタ接続を確認します MetroCluster interconnect mirror show

b. MetroCluster check: MetroCluster check run' を実行します

c. 実行が完了したら、 MetroCluster の実行結果を確認します。「 MetroCluster check show 」

5. を繰り返してファブリック B のスイッチ（スイッチ 2 と 4 ）を更新します 手順 2 終了： 手順 5。

RCF ファイルの更新後に **MetroCluster** 設定の健全性を確認します

アップグレードを実行する前に、 MetroCluster 構成の健全性と接続を確認する必要があります。

手順

1. ONTAP で MetroCluster 構成の動作を確認します。

a. ノードがマルチパスであるかどうかを確認します。 +node run -node node_name sysconfig -a

このコマンドは、 MetroCluster 構成のノードごとに問題で実行する必要があります。

b. 構成に破損ディスクがないことを確認します。

「 storage disk show -broken 」

このコマンドは、 MetroCluster 構成の各ノードで問題を実行する必要があります。

c. ヘルスアラートがないかどうかを確認します。

「 system health alert show 」というメッセージが表示されます

このコマンドは、各クラスタで問題を実行する必要があります。

d. クラスタのライセンスを確認します。

「 system license show 」を参照してください

このコマンドは、各クラスタで問題を実行する必要があります。

e. ノードに接続されているデバイスを確認します。

「 network device-discovery show 」のように表示されます

このコマンドは、各クラスタで問題を実行する必要があります。

f. 両方のサイトでタイムゾーンと時間が正しく設定されていることを確認します。

cluster date show

このコマンドは、各クラスタで問題を実行する必要があります。時刻とタイムゾーンを設定するには 'cluster date コマンドを使用します

2. スイッチにヘルスアラートがないかどうかを確認します（ある場合）。

「 storage switch show 」と表示されます

このコマンドは、各クラスタで問題を実行する必要があります。

3. MetroCluster 構成の運用モードを確認し、 MetroCluster チェックを実行

a. MetroCluster 構成と運用モードが正常な状態であることを確認します。

「 MetroCluster show 」

b. 想定されるすべてのノードが表示されることを確認します。

MetroCluster node show

c. 次のコマンドを問題に設定します。

「 MetroCluster check run 」のようになります

d. MetroCluster チェックの結果を表示します。

MetroCluster チェックショー

4. Config Advisor ツールを使用して MetroCluster のケーブル接続を確認します。

a. Config Advisor をダウンロードして実行します。

"ネットアップのダウンロード： Config Advisor"

b. Config Advisor の実行後、ツールの出力を確認し、推奨される方法で検出された問題に対処します。

AFF A700ノードまたは**FAS9000**ノードから**AFF A900**ノードまたは**FAS9500**ノードへのポートのマッピング

コントローラのアップグレードプロセスで変更する必要があるのは、この手順に記載されている接続だけです。

AFF A700またはFAS9000コントローラのスロット7手順 にカードが取り付けられている場合は、コントローラのアップグレードを開始する前に、カードを別のスロットに移動する必要があります。AFF A900またはFAS9500コントローラでファブリックMetroCluster を機能させるために必要な2つ目のFC-VIアダプタを追加するために、スロット7を用意しておく必要があります。

アップグレード前に情報を収集

アップグレードの前に、古い各ノードの情報を収集し、必要に応じてネットワークブロードキャストドメインを調整し、VLANとインターフェイスグループを削除し、暗号化情報を収集する必要があります。

このタスクについて

このタスクは、既存の MetroCluster FC 構成で実行します。

手順

1. MetroCluster 構成ノードのシステム ID を収集します。

MetroCluster node show -fields node-systemid 、 dr-partner-systemid'

手順のアップグレード時に、これらの古いシステムIDをコントローラモジュールのシステムIDに置き換えます。

この 4 ノード MetroCluster FC 構成の例では、次の古いシステム ID が取得されます。

- node_A_1 - A700 ： 537037649
- Node_a_2-A700 ： 537407030
- Node_B_1-A700 ： 0537407114
- node_B_2 - A700 ： 537035354

```
Cluster_A::*> metrocluster node show -fields node-systemid,ha-partner-
systemid,dr-partner-systemid,dr-auxiliary-systemid
dr-group-id cluster    node           node-systemid ha-partner-systemid
dr-partner-systemid dr-auxiliary-systemid
----------- ---------- ------------- ------------------
------------------- ---------------------
1           Cluster_A  nodeA_1-A700   537407114     537035354
537411005           537410611
1           Cluster_A  nodeA_2-A700   537035354     537407114
537410611           537411005
1           Cluster_B  nodeB_1-A700   537410611     537411005
537035354           537407114
1           Cluster_B  nodeB_2-A700   537411005

4 entries were displayed.
```

2. 古い各ノードのポートとLIFの情報を収集します。

   ノードごとに次のコマンドの出力を収集する必要があります。

   - 'network interface show -role cluster, node-mgmt
   - 'network port show -node node_name -type physical ’
   - 'network port vlan show -node -node-name _`
   - 「 network port ifgrp show -node node_name 」 - instance 」を指定します
   - 「 network port broadcast-domain show 」
   - 「 network port reachability show-detail` 」と表示されます
   - network ipspace show
   - volume show
   - 「 storage aggregate show
   - 「 system node run -node _node-name_sysconfig -a 」のように入力します

3. MetroCluster ノードが SAN 構成になっている場合は、関連情報を収集します。

   次のコマンドの出力を収集する必要があります。

   - 「 fcp adapter show -instance 」のように表示されます
   - 「 fcp interface show -instance 」の略
   - 「 iscsi interface show 」と表示されます
   - ucadmin show

4. ルートボリュームが暗号化されている場合は、 key-manager に使用するパスフレーズを収集して保存します。

   「 securitykey-manager backup show 」を参照してください

5. MetroCluster ノードがボリュームまたはアグリゲートに暗号化を使用している場合は、キーとパスフレーズに関する情報をコピーします。

   追加情報の場合は、を参照してください "オンボードキー管理情報の手動でのバックアップ"。

   a. オンボードキーマネージャが設定されている場合：

      「 securitykey manager onboard show-backup 」を参照してください

      パスフレーズは、あとでアップグレード手順で必要になります。

   b. Enterprise Key Management （ KMIP ）が設定されている場合は、次のコマンドを問題で実行します。

      「 securitykey-manager external show -instance 」

   「セキュリティキーマネージャのキークエリ」

Tiebreaker またはその他の監視ソフトウェアから既存の設定を削除します

スイッチオーバーを開始できる MetroCluster Tiebreaker 構成や他社製アプリケーション（ ClusterLion など）で既存の構成を監視している場合は、移行の前に Tiebreaker またはその他のソフトウェアから MetroCluster 構成を削除する必要があります。

手順

1. Tiebreaker ソフトウェアから既存の MetroCluster 設定を削除します。

   "MetroCluster 設定の削除"

2. スイッチオーバーを開始できるサードパーティ製アプリケーションから既存の MetroCluster 構成を削除します。

   アプリケーションのマニュアルを参照してください。

カスタム **AutoSupport** メッセージをメンテナンス前に送信する

メンテナンスを実行する前に、 AutoSupport an 問題 message to notify NetApp technical support that maintenance is maintenancing （メンテナンスが進行中であることをネットアップテクニカルサポートに通知する）を実行システム停止が発生したとみなしてテクニカルサポートがケースをオープンしないように、メンテナンスが進行中であることを通知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 サイトごとに実行する必要があります。

手順

1. サポートケースが自動で生成されないようにするには、メンテナンスが進行中であることを示す AutoSupport メッセージを送信します。

   a. 次のコマンドを問題に設定します。

      「 system node AutoSupport invoke -node * -type all -message MAINT= *maintenance-window-in-hours*

」というメッセージが表示されます

「メンテナンス時間」では、メンテナンス時間の長さを最大 72 時間指定します。この時間が経過する前にメンテナンスが完了した場合は、メンテナンス期間が終了したことを通知する AutoSupport メッセージを起動できます。

「 system node AutoSupport invoke -node * -type all -message MAINT= end 」というメッセージが表示されます

a. パートナークラスタに対してこのコマンドを繰り返します。

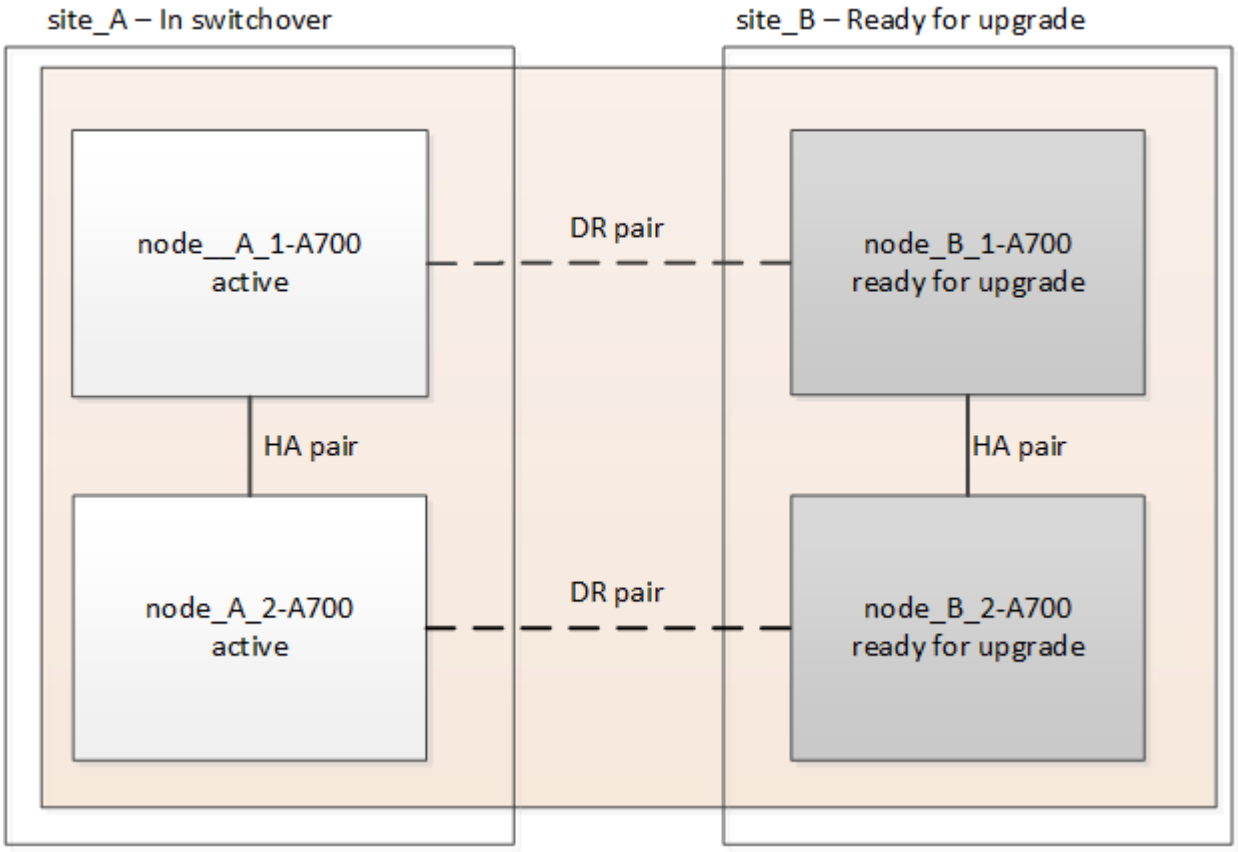
MetroCluster 構成をスイッチオーバーします

site_B のプラットフォームをアップグレードできるように、設定を site_A にスイッチオーバーする必要があります。

このタスクについて

このタスクは site_A で実行する必要があります

このタスクを完了すると、 site_A がアクティブになり、両方のサイトにデータが提供されます。site_B は非アクティブで、次の図のようにアップグレードプロセスを開始する準備ができています。（この図は環境 でもFAS9000をFAS9500コントローラにアップグレードした場合を示しています）。



手順

1. site_B のノードをアップグレードできるように、 MetroCluster 構成を site_A にスイッチオーバーします。

a. site_A で次のコマンドを問題に設定します。

MetroCluster switche-controller-replacement true

この処理が完了するまでに数分かかることがあります。

a. スイッチオーバー処理を監視します。

「 MetroCluster operation show 」を参照してください

b. 処理が完了したら、ノードがスイッチオーバー状態であることを確認します。

「 MetroCluster show 」

c. MetroCluster ノードのステータスを確認します。

MetroCluster node show

2. データアグリゲートを修復します。

a. データアグリゲートを修復します。

MetroCluster は ' データ・アグリゲートを修復します

b. 正常なクラスタで MetroCluster operation show コマンドを実行して、修復操作が完了したことを確認します。

```
cluster_A::> metrocluster operation show
  Operation: heal-aggregates
      State: successful
 Start Time: 7/29/2020 20:54:41
   End Time: 7/29/2020 20:54:42
     Errors: -
```

3. ルートアグリゲートを修復します。

a. データ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

b. 正常なクラスタで MetroCluster operation show コマンドを実行して、修復操作が完了したことを確認します。

```
cluster_A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2020 20:58:41
   End Time: 7/29/2020 20:59:42
     Errors: -
```

site_BまたはAFF A700コントローラモジュールとNVSをsite_Bで取り外します

構成から古いコントローラを削除する必要があります。

このタスクは site_B で実行します

作業を開始する前に

接地対策がまだの場合は、自身で適切に実施します。

手順

1. site_B の古いコントローラのシリアルコンソール（ node_B_1 700 および node_B_2 700 ）に接続し、「 LOADER」 プロンプトが表示されていることを確認します。
2. site_B の両方のノードから bootarg の値を収集します printenv
3. site_B のシャーシの電源をオフにします

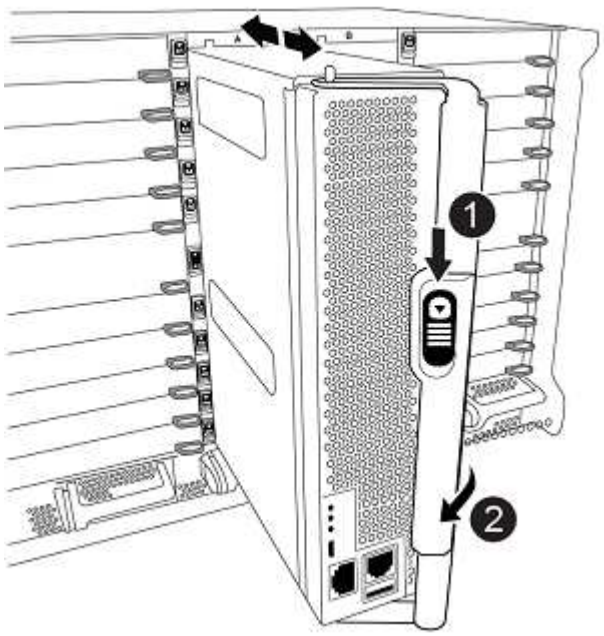
site_B の両方のノードからコントローラモジュールと NVS を取り外します

AFF A700またはFAS9000コントローラモジュールを取り外します

次の手順 を使用して、AFF A700またはFAS9000コントローラモジュールを取り外します。

手順

1. コントローラモジュールを取り外す前に、コントローラモジュールからコンソールケーブル（ある場合）と管理ケーブルを外します。
2. コントローラモジュールのロックを解除してシャーシから取り外します。
   a. カムハンドルのオレンジ色のボタンを下にスライドさせてロックを解除します。



	カムハンドルのリリースボタン
	カムハンドル

a. カムハンドルを回転させて、コントローラモジュールをシャーシから完全に外し、コントローラモジュールをシャーシから引き出します。このとき、空いている手でコントローラモジュールの底面を支えてください。

AFF A700または**FAS9000 NVS**モジュールを取り外します

次の手順 を使用して、AFF A700またはFAS9000 NVSモジュールを取り外します。

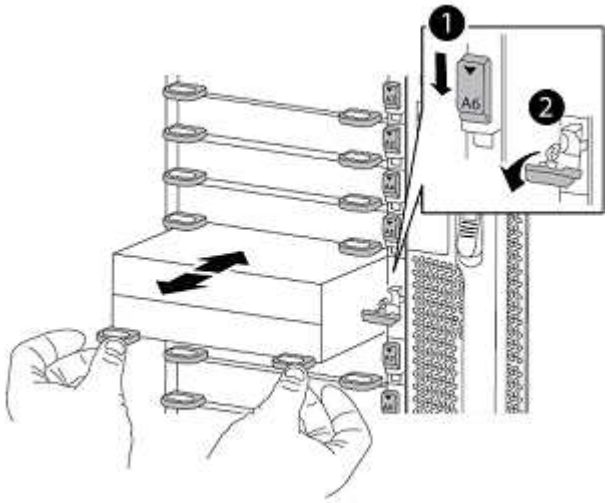
AFF A700またはFAS9000 NVSモジュールはスロット6に搭載されており、システム内の他のモジュールと比較して高さが2倍になっています。

1. NVS のロックを解除し、スロット 6 から取り外します。

a. 文字と数字が記載されたカムボタンを押し下げます。カムボタンがシャーシから離れます。

b. カムラッチを下に回転させて水平にします。NVS がシャーシから外れ、数インチ移動します。

c. NVS をシャーシから取り外すには、モジュール前面の両側にあるプルタブを引いてください。



	文字と数字が記載された I/O カムラッチ
	ロックが完全に解除された I/O ラッチ

- スロット6のAFF A700不揮発性ストレージモジュールでコアダンプデバイスとして使用されているアドオンモジュールをAFF A900 NVSモジュールに転送しないでください。AFF A700コントローラおよびNVSモジュールからAFF A900コントローラモジュールにパーツを移さないでください。
- FAS9000からFAS9500へのアップグレードでは、FAS9000 NVSモジュールのFlash Cacheモジュールのみを FAS9500 NVSモジュールに転送してください。FAS9000コントローラモジュールおよびNVSモジュールからFAS9500コントローラモジュールに他のパーツを移さないでください。

AFF A900またはFAS9500 NVSとコントローラモジュールを取り付けます

Site_Bの両方のノードに、アップグレードキットからAFF A900またはFAS9500 NVSとコントローラモジュールをインストールする必要がありますコアダンプデバイスをAFF A700またはFAS9000 NVSモジュールからAFF A900またはFAS9500 NVSモジュールに移動しないでください。

を開始する前に

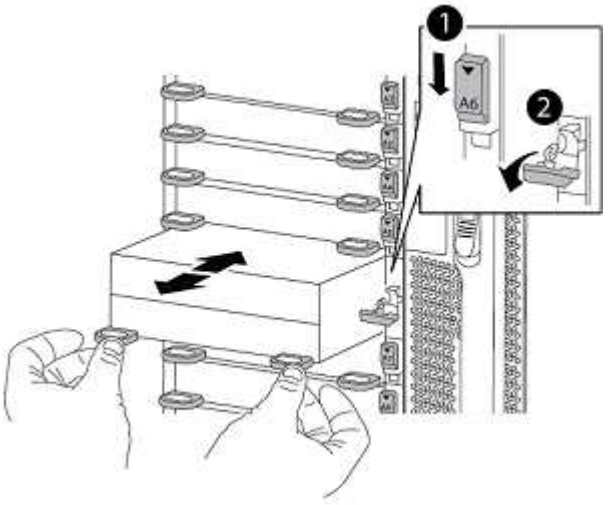
接地対策がまだの場合は、自身で適切に実施します。

AFF A900またはFAS9500 NVSをインストールします

次の手順 を使用して、site_Bの両方のノードのスロット6にAFF A900またはFAS9500 NVSをインストールします

手順

1. NVS をスロット 6 のシャーシ開口部の端に合わせます。
2. NVS をスロットにそっと挿入し、文字と数字が記載された I/O カムラッチを上に押して NVS を所定の位置にロックします。



	文字と数字が記載された I/O カムラッチ
	ロックが完全に解除された I/O ラッチ

AFF A900または**FAS9500**コントローラモジュールを取り付けます

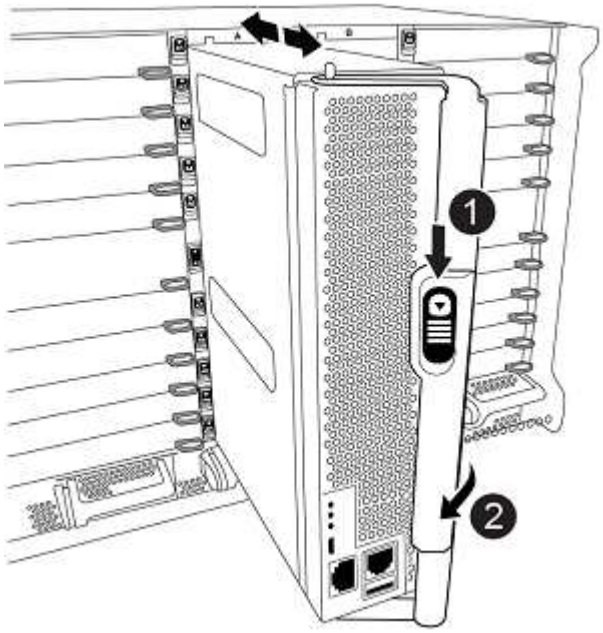
次の手順 を使用して、AFF A900またはFAS9500コントローラモジュールをインストールします。

手順

1. コントローラモジュールの端をシャーシの開口部に合わせ、コントローラモジュールをシステムに半分までそっと押し込みます。
2. コントローラモジュールをシャーシに挿入し、ミッドプレーンまでしっかりと押し込んで完全に装着します。コントローラモジュールが完全に装着されると、ロックラッチが上がります。

> コネクタの破損を防ぐため、コントローラモジュールをスライドしてシャーシに挿入する際に力を入れすぎないでください。

3. 管理ポートとコンソールポートをコントローラモジュールにケーブル接続します。



	カムハンドルのリリースボタン
	カムハンドル

4. 各ノードのスロット 7 に 2 枚目の X91129A カードを取り付けます。
   a. スロット 7 の FC-VI ポートをスイッチに接続します。を参照してください "ファブリック接続型のインストールと設定" ドキュメントを参照し、環境内のスイッチタイプに応じたAFF A900またはFAS9500ファブリックのMetroCluster 接続要件を確認します。
5. シャーシの電源を入れ、シリアルコンソールに接続します。
6. BIOS の初期化後にノードで自動ブートが開始された場合は、 Ctrl-C を押して自動ブートを中断します
7. AUTOBOOT を中断すると、ノードで LOADER プロンプトが停止します。ブートを中断せずに node1 でブートが開始された場合は、 Ctrl+C キーを押してブートメニューに入るまで待ちます。ブートメニューでノードが停止したら、オプション 8 を使用してノードをリブートし、リブート時に自動ブートを中断し

ます。

8. 「 loader 」プロンプトで、デフォルトの環境変数「 set-defaults 」を設定します
9. デフォルトの環境変数設定である saveenv を保存します

site_B のノードをネットブートします

AFF A900またはFAS9500コントローラモジュールとNVSを交換したら、AFF A900またはFAS9500ノードをネットブートして、クラスタで実行されているものと同じバージョンのONTAP とパッチレベルをインストールする必要があります。「 netboot 」という用語は、リモート・サーバに保存されている ONTAP イメージからブートすることを意味します。ネットブートを準備するときは ' システムがアクセスできる Web サーバに ONTAP 9 ブート・イメージのコピーを追加する必要があります

AFF A900またはFAS9500コントローラモジュールのブートメディアにインストールされているONTAP のバージョンは、シャーシに取り付けて電源がオンになっていないかぎり確認できません。AFF A900またはFAS9500ブートメディア上のONTAP バージョンは、アップグレード対象のAFF A700またはFAS9000システムで実行されているONTAP バージョンと同じで、プライマリブートイメージとバックアップブートイメージの両方が一致している必要があります。イメージを設定するには、「 netboot 」に続けて「 wipeconfig 」コマンドを実行します。コントローラモジュールが以前に別のクラスタで使用されていた場合は、「 wipeconfig 」コマンドはブートメディア上の残留設定をクリアします。

を開始する前に

- システムから HTTP サーバにアクセスできることを確認します。
- ご使用のシステムに必要なシステムファイルと、適切なバージョンの ONTAP をからダウンロードする必要があります "ネットアップサポート" サイトこのタスクについて、インストールされている ONTAP のバージョンが元のコントローラにインストールされているバージョンと異なる場合は、新しいコントローラを「ネットブート」する必要があります。新しいコントローラをそれぞれ取り付けたら、 Web サーバに保存されている ONTAP 9 イメージからシステムをブートします。その後、以降のシステムブートで使用するブートメディアデバイスに正しいファイルをダウンロードできます。

手順

1. にアクセスします "ネットアップサポート" システムのネットブートの実行に使用するシステム・ネットブートの実行に必要なファイルをダウンロードするには、次の手順を実行します。
2. [step2-download-software]] ネットアップサポートサイトのソフトウェアダウンロードセクションから適切な ONTAP ソフトウェアをダウンロードし、「 <ONTAP_version>_image.tgz 」ファイルを Web にアクセスできるディレクトリに保存します。
3. Web にアクセスできるディレクトリに移動し、必要なファイルが利用可能であることを確認します。ディレクトリの一覧には「 <ONTAP_version>_image.tgz 」が含まれている必要があります。
4. 次のいずれかの操作を選択して 'netboot' 接続を構成しますメモ：管理ポートと IP を「 netboot 」接続として使用してください。アップグレードの実行中にデータ LIF IP を使用しないでください。データ LIF が停止する可能性があります。

動的ホスト構成プロトコル（ DHCP ）の状態	作業
実行中です	ブート環境プロンプトで次のコマンドを使用して、自動的に接続を設定します。 ifconfig e0M -auto

実行されていません	ブート環境プロンプトで次のコマンドを使用して、接続を手動で設定します。 ifconfig e0M -addr= <filer_addr> -mask= <netmask> -gw= <gateway> -dns= <dns_addr> domain= <dns_domain> `<filer_addr><netmask>` はストレージシステムのネットワークマスクです。「 <gateway>` 」は、ストレージシステムのゲートウェイです。「 <dns_addr> 」は、ネットワーク上のネームサーバの IP アドレスです。このパラメータはオプションです。「 <dns_domain> 」は、 Domain Name Service （ DNS ；ドメインネームサービス）ドメイン名です。このパラメータはオプションです。注：使用しているインターフェイスによっては、他のパラメータが必要になる場合もあります。詳細については、ファームウェアのプロンプトで「 help ifconfig 」と入力してください。

5. ノード 1 でネットブートを実行します http://<web_server_ip/path_to_web_accessible_directory>/netboot/kernel`「 <path_the_web-accessible_directory> 」は、「 <ONTAP_version>_image.tgz 」をダウンロードした場所を指します 手順 2。

   トランクを中断しないでください。

6. AFF A900またはFAS9500コントローラモジュールで実行されているノード1がブートするまで待ち、次のようにブートメニューオプションを表示します。

```
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)?
```

7. 起動メニューからオプション（ 7 ） Install new software first （新しいソフトウェアを最初にインストール）を選択します。このメニューオプションを選択すると、新しい ONTAP イメージがブートデバイスにダウンロードおよびインストールされます。

次のメッセージは無視してください： This 手順 is not supported for Non-Disruptive Upgrade on an HA pair. 環境の無停止の ONTAP ソフトウェアアップグレード。コントローラのアップグレードは含まれません。新しいノードを希望するイメージに更新する場合は、必ずネットブートを使用してください。別の方法で新しいコントローラにイメージをインストールした場合、間違ったイメージがインストールされることがあります。この問題環境 All ONTAP リリース

8. 手順を続行するかどうかを確認するメッセージが表示されたら、と入力します。 `y`パッケージの入力を求められたら、次のURLを入力します。

   ```
   http://<web_server_ip/path_to_web-
   accessible_directory>/<ontap_version>_image.tgz
   ```

9. 次の手順を実行してコントローラモジュールをリブートします。

   a. 入力 `n` 次のプロンプトが表示されたら、バックアップの回復をスキップします。

      ```
      Do you want to restore the backup configuration now? {y|n} n
      ```

   b. 入力 `y` 次のプロンプトが表示されたら再起動してください。

      ```
      The node must be rebooted to start using the newly installed software. Do
      you want to reboot now? {y|n} y
      ```

      コントローラモジュールはリブートしますが、ブートメニューで停止します。これは、ブートデバイスが再フォーマットされたことにより、構成データのリストアが必要なためです。

      新しくインストールされたソフトウェアを使用するには、ノードを再起動する必要があります。

10. プロンプトで「 wipeconfig 」コマンドを実行して、ブートメディアの以前の設定をクリアします。

    a. 次のメッセージが表示されたら、回答は「 yes 」を選択します。これにより、クラスタメンバーシップを含む重要なシステム構成が削除されます。警告：テイクオーバーされた HA ノードでは実行しないでください。続行してもよろしいですか ?:`

    b. ノードがリブートして「 wipeconfig 」を終了し、ブートメニューで停止します。

11. ブート・メニューからオプション「 5 」を選択して、保守モードに切り替えます。ノードがメンテナンス・モードで停止し ' コマンド・プロンプト *>` が表示されるまで ' プロンプトを表示します回答

HBA 構成をリストア

コントローラモジュールに HBA カードが搭載されているかどうかや設定によっては、サイトで使用するために正しく設定する必要があります。

手順

1. メンテナンスモードで、システム内の HBA の設定を行います。

   a. ucadmin show と入力し、各ポートの現在の設定を確認します

b. 必要に応じてポートの設定を更新します。

HBA のタイプと目的のモード	使用するコマンド
CNA FC	ucadmin modify -m fc -t initiator_adapter-name _ `
CNA イーサネット	ucadmin modify -mode cna_adapter-name_`
FC ターゲット	fcadmin config -t target_adapter-name_`
FC イニシエータ	fcadmin config -t initiator_adapter-name_`

新しいコントローラとシャーシで **HA** 状態を設定

コントローラとシャーシの HA 状態を確認し、必要に応じてシステム構成に合わせて更新する必要があります。

手順

1. メンテナンスモードで、コントローラモジュールとシャーシの HA 状態を表示します。

   「 ha-config show 」

   すべてのコンポーネントの HA の状態が mcc である必要があります。

2. 表示されたコントローラまたはシャーシのシステム状態が正しくない場合は、 HA 状態を設定します。

   「 ha-config modify controller mcc 」

   「 ha-config modify chassis mcc 」

3. ノードを停止しますノードは 'LOADER>` プロンプトで停止します
4. 各ノードで ' システムの日付 ' 時刻 ' タイムゾーンを確認しますつまり ' 日付を表示します
5. 必要に応じて、日付を UTC またはグリニッジ標準時（ GMT ）に設定します。「 set date <mm/dd/yyyy>` 」
6. ブート環境プロンプトで次のコマンドを使用して ' 時刻を確認します
7. 必要に応じて、時刻を UTC または GMT:' 設定時刻 <:hh:mm:ss>` で設定します
8. 設定を保存します： saveenv
9. 環境変数 :printenv' を収集します
10. ノードをブートして保守モードに戻り、設定の変更が反映されるようにします。「 boot_ontap maint 」
11. 行った変更が有効であることを確認し、 ucadmin に FC イニシエータポートがオンラインで表示されるようにします。

HBA のタイプ	使用するコマンド
CNA	ucadmin show

FC	fcadmin show`

12. ha-config モードを確認します。「 ha-config show
    a. 次の出力があることを確認します。

```
*> ha-config show
Chassis HA configuration: mcc
Controller HA configuration: mcc
```

新しいコントローラとシャーシで **HA** 状態を設定

コントローラとシャーシの HA 状態を確認し、必要に応じてシステム構成に合わせて更新する必要があります。

手順

1. メンテナンスモードで、コントローラモジュールとシャーシの HA 状態を表示します。

   「 ha-config show 」

   すべてのコンポーネントの HA の状態が mcc である必要があります。

MetroCluster 構成の内容	HA の状態
2 ノード	mcc-2n
4 ノードまたは 8 ノード	MCC

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とシャーシの HA 状態を設定します。

MetroCluster 構成の内容	問題コマンド
• 2 ノード *	「 ha-config modify controller mcc-2n 」という形式で指定します 「 ha-config modify chassis mcc-2n 」というようになりました
• 4 ノードまたは 8 ノード *	「 ha-config modify controller mcc 」 「 ha-config modify chassis mcc 」

ルートアグリゲートディスクを再割り当てします

前の手順で確認したシステム ID を使用して、ルートアグリゲートディスクを新しいコントローラモジュール

に再割り当てします

このタスクについて

このタスクはメンテナンスモードで実行します。

古いシステム ID は、で識別されています "アップグレード前に情報を収集"。

この手順の例では、次のシステム ID を持つコントローラを使用します。

ノード	古いシステム ID	新しいシステム ID
node_B_1	4068741254	1574774970

手順

1. 他のすべての接続を新しいコントローラモジュール（ FC-VI 、ストレージ、クラスタインターコネクトなど）にケーブル接続します。
2. システムを停止して 'LOADER' プロンプトからメンテナンス・モードで起動します

   「 boot_ontap maint 」を使用してください
3. node_B_1 A700 が所有するディスクを表示します。

   「ディスクショー - A` 」

   次の出力例は、新しいコントローラモジュールのシステム ID （ 1574774970 ）を示しています。ただし、ルートアグリゲートディスクは古いシステム ID （ 4068741254 ）で所有されます。この例で表示されているのは、 MetroCluster 構成の他のノードが所有するドライブではありません。

```
*> disk show -a
Local System ID: 1574774970

  DISK         OWNER                      POOL   SERIAL NUMBER    HOME
DR HOME
------------   -------------              -----  -------------
-------------             -------------
...
rr18:9.126L44 node_B_1-A700(4068741254)   Pool1  PZHYN0MD
node_B_1-A700(4068741254)  node_B_1-A700(4068741254)
rr18:9.126L49 node_B_1-A700(4068741254)   Pool1  PPG3J5HA
node_B_1-A700(4068741254)  node_B_1-A700(4068741254)
rr18:8.126L21 node_B_1-A700(4068741254)   Pool1  PZHTDSZD
node_B_1-A700(4068741254)  node_B_1-A700(4068741254)
rr18:8.126L2  node_B_1-A700(4068741254)   Pool0  S0M1J2CF
node_B_1-A700(4068741254)  node_B_1-A700(4068741254)
rr18:8.126L3  node_B_1-A700(4068741254)   Pool0  S0M0CQM5
node_B_1-A700(4068741254)  node_B_1-A700(4068741254)
rr18:9.126L27 node_B_1-A700(4068741254)   Pool0  S0M1PSDW
node_B_1-A700(4068741254)  node_B_1-A700(4068741254)
...
```

4. ドライブシェルフのルートアグリゲートディスクを新しいコントローラに再割り当てします。

   「ディスクの再割り当て -s *old-sysid*-d_new-sysid_`

   次の例は、ドライブの再割り当てを示しています。

```
*> disk reassign -s 4068741254 -d 1574774970
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)? n

After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)? Jul 14 19:23:49
[localhost:config.bridge.extra.port:error]: Both FC ports of FC-to-SAS
bridge rtp-fc02-41-rr18:9.126L0 S/N [FB7500N107692] are attached to this
controller.
y
Disk ownership will be updated on all disks previously belonging to
Filer with sysid 4068741254.
Do you want to continue (y/n)? y
```

5. すべてのディスクが期待どおりに再割り当てされていることを確認します

```
*> disk show
Local System ID: 1574774970

  DISK         OWNER                      POOL   SERIAL NUMBER   HOME
DR HOME
------------  -------------              -----  -------------
-------------             -------------
rr18:8.126L18 node_B_1-A900(1574774970)   Pool1  PZHYN0MD
node_B_1-A900(1574774970)  node_B_1-A900(1574774970)
rr18:9.126L49 node_B_1-A900(1574774970)   Pool1  PPG3J5HA
node_B_1-A900(1574774970)  node_B_1-A900(1574774970)
rr18:8.126L21 node_B_1-A900(1574774970)   Pool1  PZHTDSZD
node_B_1-A900(1574774970)  node_B_1-A900(1574774970)
rr18:8.126L2  node_B_1-A900(1574774970)   Pool0  S0M1J2CF
node_B_1-A900(1574774970)  node_B_1-A900(1574774970)
rr18:9.126L29 node_B_1-A900(1574774970)   Pool0  S0M0CQM5
node_B_1-A900(1574774970)  node_B_1-A900(1574774970)
rr18:8.126L1  node_B_1-A900(1574774970)   Pool0  S0M1PSDW
node_B_1-A900(1574774970)  node_B_1-A900(1574774970)
*>
```

6. アグリゲートのステータスを表示します。「 aggr status 」を選択します

```
*> aggr status
           Aggr             State       Status            Options
aggr0_node_b_1-root    online      raid_dp, aggr    root, nosnap=on,
                                   mirrored
mirror_resync_priority=high(fixed)
                                   fast zeroed
                                   64-bit
```

7. パートナーノード（ node_B_2 - A900 ）に対して上記の手順を繰り返します。

新しいコントローラをブートします

コントローラのフラッシュイメージを更新するには、ブートメニューからコントローラをリブートする必要があります。暗号化が設定されている場合は、追加の手順が必要です。

このタスクについて

このタスクはすべての新しいコントローラで実行する必要があります。

手順

1. ノードを停止します
2. 外部キー管理ツールが設定されている場合は、関連する bootargs を設定します。

   'setenv bootarg.kmip.init.ipaddr *ip-address*'

   'setenv bootarg.kmip.init.netmask *netmask*`

   'setenv bootarg.kmip.init.gateway *gateway-address*

   'setenv bootarg.kmip.init.interface *interface-id*

3. ブートメニューを表示します：「 boot_ontap menu
4. ルート暗号化を使用問題する場合は、キー管理設定の boot menu コマンドを使用します。

使用するポート	選択するブートメニューオプション
オンボードキー管理	オプション 10 を選択し、画面の指示に従って、キー管理ツールの構成をリカバリまたはリストアするために必要な入力を指定します
外部キー管理	オプション 11 を選択し、画面の指示に従って、キー管理ツールの設定をリカバリまたはリストアするために必要な入力を指定します

5. 自動ブートが有効になっている場合は、 control-C を押して自動ブートを中断します
6. ブートメニューからオプション（ 6 ）を実行します。

オプション 6 を指定すると、完了前にノードが 2 回リブートされます

システム ID 変更プロンプトに「 y 」と入力します。2 回目のリブートメッセージが表示されるまで待ちます。

```
Successfully restored env file from boot media...

Rebooting to load the restored env file...
```

7. partner-sysid が正しいことをダブルチェックします :printenv partner-sysid

   partner-sysid が正しくない場合は、「 setenv partner-sysid_partner-SysID_` 」と設定します

8. ルート暗号化を使用問題する場合は、キー管理設定に対して boot menu コマンドを再度実行します。

使用するポート	選択するブートメニューオプション
オンボードキー管理	オプション 10 を選択し、画面の指示に従って、キー管理ツールの構成をリカバリまたはリストアするために必要な入力を指定します
外部キー管理	オプション 11 を選択し、画面の指示に従って、キー管理ツールの設定をリカバリまたはリストアするために必要な入力を指定します

   ノードが完全にブートするまで、ブートメニュープロンプトで「 recover_xxxxxxxx_keymanager 」コマンドを何度も問題に接続する必要がある場合があります。

9. ノード「 boot_ontap 」をブートします
10. 交換したノードがブートするまで待ちます。

    いずれかのノードがテイクオーバーモードの場合は、「 storage failover giveback 」コマンドを使用してギブバックを実行します。

11. すべてのポートがブロードキャストドメインに属していることを確認します。

    a. ブロードキャストドメインを表示します。

       「 network port broadcast-domain show 」

    b. 必要に応じて、ブロードキャストドメインにポートを追加します。

       "ブロードキャストドメインのポートを追加または削除します"

    c. インタークラスタ LIF をホストする物理ポートを対応するブロードキャストドメインに追加します。
    d. 新しい物理ポートをホームポートとして使用するようにクラスタ間 LIF を変更します。
    e. クラスタ間 LIF が起動したら、クラスタピアのステータスを確認し、必要に応じてクラスタピアリン

グを再確立します。

クラスタピアリングの再設定が必要になる場合があります。

"クラスタピア関係を作成"

f. 必要に応じて、 VLAN とインターフェイスグループを再作成します。

VLAN およびインターフェイスグループのメンバーシップは、古いノードと異なる場合があります。

"VLAN を作成する"

"物理ポートを組み合わせたインターフェイスグループの作成"

12. 暗号化を使用する場合は、キー管理設定に対応したコマンドを使用してキーをリストアします。

使用するポート	使用するコマンド
オンボードキー管理	「セキュリティキーマネージャオンボード同期」 詳細については、を参照してください "オンボードキー管理の暗号化キーのリストア"。
外部キー管理	「 securitykey manager external restore -vserver *svm*-node __ key -server_host_name

LIF の設定を確認

スイッチバックの前に、 LIF が適切なノード / ポートにホストされていることを確認します。次の手順を実行する必要があります

このタスクについて

このタスクは site_B で実行します。ノードはルートアグリゲートでブートされています。

手順

1. スイッチバックの前に、 LIF が適切なノードとポートにホストされていることを確認します。

a. advanced 権限レベルに切り替えます。

「 advanced 」の権限が必要です

b. ポート設定を無視して LIF が適切に配置されるようにします。

「 vserver config override command 」 network interface modify -vserver vserver_name __ -home -node _active_port_after_upgrade _ -lif LIF_name -home-node _new_node_name _

「 vserver config override 」コマンド内で「 network interface modify 」コマンドを入力する場合、 Tab autoccomplete 機能は使用できません。autoccomplete を使用して「 network interface modify 」を作成し、「 vserver config override 」コマンドで囲むことができます。

a. admin 権限レベルに戻ります。 `+set -privilege admin`

2. インターフェイスをホームノードにリバートします。

「 network interface revert * -vserver_vserver-name に指定します

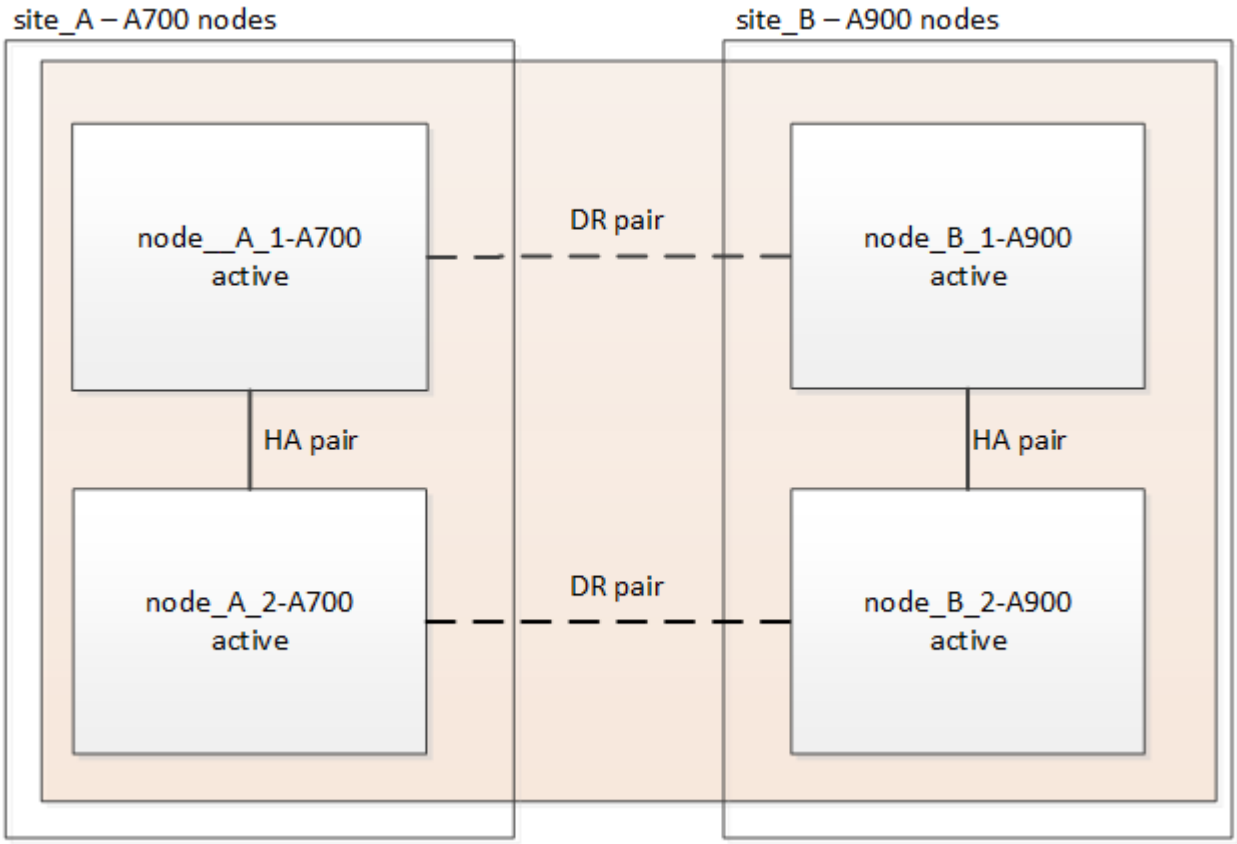
必要に応じて、すべての SVM でこの手順を実行します。

MetroCluster 構成をスイッチバックします

新しいコントローラを設定したら、 MetroCluster 構成をスイッチバックして構成を通常動作に戻します。

このタスクについて

このタスクでは、スイッチバック処理を実行して MetroCluster 構成を通常動作に戻します。次の図に示すように、site_Aのノードはまだアップグレードを待っています。（この図は環境 でもFAS9000をFAS9500コントローラにアップグレードした場合を示しています）。



手順

1. site_B の MetroCluster node show コマンドを問題し ' 出力を確認します

a. 新しいノードが正しく表示されることを確認します。

b. 新しいノードの状態が「 Waiting for switchback 」であることを確認します。

2. クラスタをスイッチバックします。

MetroCluster スイッチバック

3. スイッチバック処理の進捗を確認します。

「 MetroCluster show 」

出力に「 waiting-for-switchback 」と表示されたら、スイッチバック処理はまだ進行中です。

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                switchover
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                waiting-for-switchback
                          AUSO Failure Domain -
```

出力に「 normal 」と表示された場合、スイッチバック処理は完了しています。

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
```

スイッチバックが完了するまでに時間がかかる場合は、「 MetroCluster config-replication resync-status show 」コマンドを使用することで、進行中のベースラインのステータスを確認できます。このコマンドは、 advanced 権限レベルで実行します。

MetroCluster 構成の健全性を確認します

コントローラモジュールをアップグレードしたら、 MetroCluster 構成の健全性を確認する必要があります。

このタスクについて

このタスクは、 MetroCluster 構成の任意のノードで実行できます。

手順

1. MetroCluster 構成の動作を確認します。

   a. MetroCluster 構成と運用モードが正常な状態であることを確認します。

      「 MetroCluster show 」

b. MetroCluster チェックを実行します。

「 MetroCluster check run 」のようになります

c. MetroCluster チェックの結果を表示します。

MetroCluster チェックショー

を実行したあと `metrocluster check run` および `metrocluster check show` 次の例のようなエラーが表示されることがあります。

```
Cluster_A:: node_A_1 (non-overridable veto): DR partner NVLog mirroring
is not online. Make sure that the links between the two sites are
healthy and properly configured.
```

+
このエラーは、アップグレードプロセス中のコントローラの不一致が原因で発生します。このエラーは無視してsite_Aのノードのアップグレードに進みます

site_A でノードをアップグレードします

site_A でアップグレードタスクを繰り返します

ステップ

1. 同じ手順を繰り返して、 site_A のノードをアップグレードします "アップグレードを準備"。

タスクを実行すると、サイトおよびノードへのすべてのサンプル参照が反転されます。たとえば、この例で site_A からスイッチオーバーする場合は、 site_B からスイッチオーバーします

カスタム AutoSupport メッセージをメンテナンス後に送信します

アップグレードの完了後、ケースの自動作成を再開できるように、メンテナンスの終了を通知する AutoSupport メッセージを送信する必要があります。

ステップ

1. サポートケースの自動生成を再開するには、メンテナンスが完了したことを示す AutoSupport メッセージを送信します。

a. 次のコマンドを問題に設定します。

「 system node AutoSupport invoke -node * -type all -message MAINT= end 」というメッセージが表示されます

b. パートナークラスタに対してこのコマンドを繰り返します。

Tiebreaker による監視をリストアします

MetroCluster 構成が Tiebreaker ソフトウェアで監視するように設定されている場合は、 Tiebreaker 接続をリストアできます。

1. 次の手順を使用します。 "MetroCluster 構成を追加しています" *MetroCluster Tiebreaker* のインストールと構成 セクション。

「system controller replace」コマンドを使用したスイッチオーバーとスイッチバックを使用した4ノードMetroCluster FC構成のコントローラのアップグレード（ONTAP 9.10.1以降）

このガイドに記載された自動 MetroCluster スイッチオーバー処理を使用して、 4 ノード MetroCluster FC 構成のコントローラを無停止でアップグレードできます。この手順の一部として他のコンポーネント（ストレージシェルフやスイッチなど）をアップグレードすることはできません。

サポートされるプラットフォームの組み合わせ

- サポートされるプラットフォームアップグレードの組み合わせについては、のMetroCluster FCアップグレードの表を参照してください "コントローラのアップグレード手順 を選択します"。

その他の手順については、を参照してください"アップグレードまたは更新の方法を選択"。

このタスクについて

- この手順は、コントローラのアップグレードにのみ使用できます。

  ストレージシェルフやスイッチなど、構成内の他のコンポーネントは同時にアップグレードできません。

- この手順環境コントローラモジュールは、 4 ノード MetroCluster FC 構成です。
- プラットフォームで ONTAP 9.10.1 以降が実行されている必要があります。

  "NetApp Hardware Universe の略"

- この手順を使用して、 NSO ベースの自動スイッチオーバーとスイッチバックを使用して、 4 ノード MetroCluster FC 構成のコントローラをアップグレードできます。アグリゲートの再配置（ ARL ）を使用してコントローラをアップグレードする場合は、を参照してください "ONTAP 9.8 以降を実行しているコントローラハードウェアをアップグレードするには、「 system controller replace 」コマンドを使用します"。NSO ベースの自動化された手順を使用することを推奨します。
- MetroCluster サイトが物理的に 2 つの異なる場所にある場合は、 NSO コントローラの自動アップグレード手順を使用して、両方のサイトのコントローラを順番にアップグレードする必要があります。
- この NSO ベースのコントローラの自動アップグレード手順を使用すると、 MetroCluster ディザスタリカバリ（ DR ）サイトでコントローラの交換を開始できます。コントローラの交換は一度に 1 つのサイトでしか開始できません。
- サイト A でコントローラの交換を開始するには、サイト B からコントローラの交換開始コマンドを実行する必要があります交換処理ガイドは、サイト A の両方のノードのコントローラのみを交換する場合に使用します。サイト B のコントローラを交換するには、サイト A からコントローラ交換の開始コマンドを実行する必要がありますコントローラを交換するサイトを示すメッセージが表示されます。

この手順では、次の名前が使用されています。

- site_A
  - アップグレード前：
    - node_A_1 - 古い
    - Node_a_2-old
  - アップグレード後：
    - node_A_1 - 新規
    - Node_a_2 - 新規
- site_B
  - アップグレード前：
    - node_B_1 - 古い
    - node_B_2 - 古い
  - アップグレード後：
    - node_B_1 - 新規
    - node_B_2 - 新規

コンソールログを有効にする

NetAppでは、使用しているデバイスでコンソールロギングをイネーブルにし、この手順を実行する際に次のアクションを実行することを強く推奨します。

- メンテナンス中はAutoSupportを有効のままにします。
- メンテナンスの前後にメンテナンスAutoSupportメッセージをトリガーして、メンテナンスアクティビティ中にケースの作成を無効にします。

  ナレッジベースの記事を参照してください "スケジュールされたメンテナンス時間中にケースの自動作成を停止する方法"。

- 任意のCLIセッションのセッションロギングをイネーブルにします。セッションログを有効にする方法については、ナレッジベースの記事の「セッション出力のログ」セクションを参照してください "ONTAPシステムへの接続を最適化するためのPuTTYの設定方法"。

アップグレードを準備

コントローラのアップグレードを準備するには、システムの事前確認を実行し、構成情報を収集する必要があります。

アップグレードのどの段階でも、サイト A から「 system controller replace show 」または「 system controller replace show -details 」コマンドを実行してステータスを確認できます。コマンドから何も出力されない場合は、数分待ってからコマンドを再実行してください。

手順

1. サイト B のコントローラーを交換するには、サイト A から次のコマンドを実行します。

   'System controller replace start' （システムコントローラの交換開始

◦ 一方のサイトでコントローラーを交換した後に、もう一方のサイトで同じ手順を繰り返すと、各サイトのノード間の不一致によりエラーが発生します。これは、両サイトで異なるプラットフォームモデルが存在する場合に想定される動作です。

不一致エラーのみが返された場合は、 `-skip-metrocluster-check true`オプション `system controller replace start` MetroCluster チェックをスキップするコマンド。

自動操作によりチェックが実行されます。問題が見つからなかった場合は処理が一時停止するため、構成に関連する情報を手動で収集できます。

現在のソースシステムと互換性のあるすべてのターゲットシステムが表示されます。ソースコントローラを異なるONTAPバージョンまたは互換性のないプラットフォームのコントローラに交換した場合、新しいノードの起動後に自動化処理が停止し、エラーが報告されます。クラスタを正常な状態に戻すには、手動リカバリ手順に従ってください。

「 system controller replace start 」コマンドで、次の事前確認エラーが報告されることがあります。

```
Cluster-A::*>system controller replace show
Node         Status          Error-Action
------------ --------------- -------------------------------------
Node-A-1     Failed          MetroCluster check failed. Reason : MCC check
showed errors in component aggregates
```

アグリゲートのミラーされていないか、別のアグリゲート問題が原因で、このエラーが発生していないかどうかを確認してくださいすべてのミラーアグリゲートが正常で、デグレードまたはミラーデグレードでないことを確認します。このエラーの原因がミラーされていないアグリゲートのみである場合は、「 system controller replace start 」コマンドで「 -skip-metrocluster-check true 」オプションを選択することで、このエラーを無視できます。リモートストレージにアクセスできる場合、ミラーされていないアグリゲートはスイッチオーバー後にオンラインになります。リモートストレージリンクに障害が発生すると、ミラーされていないアグリゲートがオンラインになりません。

2. サイト B にログインし、「 system controller replace show 」または「 system controller replace show -details 」コマンドのコンソールメッセージに表示されるコマンドに従って、設定情報を手動で収集します。

アップグレード前に情報を収集

アップグレードの実行前にルートボリュームが暗号化されている場合は、暗号化された古いルートボリュームを含む新しいコントローラをブートするために、バックアップキーとその他の情報を収集する必要があります。

このタスクについて

このタスクは、既存の MetroCluster FC 構成で実行します。

手順

1. 既存のコントローラのケーブルにラベルを付けておくと、新しいコントローラをセットアップするときに識別しやすくなります。
2. バックアップキーやその他の情報を取得するコマンドを表示します。

「 system controller replace show 」と表示されます

パートナークラスタから 'how コマンドの下に一覧表示されているコマンドを実行します

3. MetroCluster 構成内のノードのシステム ID を収集します。

   MetroCluster node show -fields node-systemid 、 dr-partner-systemid'

   手順のアップグレード時に、これらの古いシステムIDを新しいコントローラモジュールのシステムIDに置き換えます。

   この 4 ノード MetroCluster FC 構成の例では、次の古いシステム ID が取得されます。

   - node_A_1 - 古い： 4068741258
   - node_A_2 - 古い： 4068741260
   - node_B_1 - 古い： 4068741254
   - node_B_2 - 古い： 4068741256

```
metrocluster-siteA::> metrocluster node show -fields node-systemid,ha-
partner-systemid,dr-partner-systemid,dr-auxiliary-systemid
dr-group-id        cluster           node            node-systemid
ha-partner-systemid     dr-partner-systemid    dr-auxiliary-systemid
-----------        ---------------   ----------      -------------
-------------------     -------------------    ---------------------
1                    Cluster_A       Node_A_1-old    4068741258
4068741260              4068741256             4068741256
1                    Cluster_A       Node_A_2-old    4068741260
4068741258              4068741254             4068741254
1                    Cluster_B       Node_B_1-old    4068741254
4068741256              4068741258             4068741260
1                    Cluster_B       Node_B_2-old    4068741256
4068741254              4068741260             4068741258
4 entries were displayed.
```

   この 2 ノード MetroCluster FC 構成の例では、次の古いシステム ID が取得されます。

   - node_A_1 ： 4068741258
   - node_B_1 ： 4068741254

```
metrocluster node show -fields node-systemid,dr-partner-systemid

dr-group-id cluster    node          node-systemid dr-partner-systemid
----------- ---------- --------      ------------- ------------
1           Cluster_A  Node_A_1-old  4068741258    4068741254
1           Cluster_B  node_B_1-old  -             -
2 entries were displayed.
```

4. 古い各ノードのポートとLIFの情報を収集します。

   ノードごとに次のコマンドの出力を収集する必要があります。

   - 'network interface show -role cluster, node-mgmt
   - 'network port show -node node_name -type physical ’
   - 'network port vlan show -node -node-name _`
   - 「 network port ifgrp show -node node_name 」 - instance 」を指定します
   - 「 network port broadcast-domain show 」
   - 「 network port reachability show-detail` 」と表示されます
   - network ipspace show
   - volume show
   - 「 storage aggregate show
   - 「 system node run -node _node-name_sysconfig -a 」のように入力します

5. MetroCluster ノードが SAN 構成になっている場合は、関連情報を収集します。

   次のコマンドの出力を収集する必要があります。

   - 「 fcp adapter show -instance 」のように表示されます
   - 「 fcp interface show -instance 」の略
   - 「 iscsi interface show 」と表示されます
   - ucadmin show

6. ルートボリュームが暗号化されている場合は、 key-manager に使用するパスフレーズを収集して保存します。

   「 securitykey-manager backup show 」を参照してください

7. MetroCluster ノードがボリュームまたはアグリゲートに暗号化を使用している場合は、キーとパスフレーズに関する情報をコピーします。

   追加情報の場合は、を参照してください "オンボードキー管理情報の手動でのバックアップ"。

   a. オンボードキーマネージャが設定されている場合：

      「 securitykey manager onboard show-backup 」を参照してください

パスフレーズは、あとでアップグレード手順で必要になります。

b. Enterprise Key Management （ KMIP ）が設定されている場合は、次のコマンドを問題で実行します。

「 securitykey-manager external show -instance 」

「セキュリティキーマネージャのキークエリ」

8. 設定情報の収集が完了したら、処理を再開します。

「システムコントローラの交換が再開」

Tiebreaker またはその他の監視ソフトウェアから既存の設定を削除します

スイッチオーバーを開始できる MetroCluster Tiebreaker 構成またはその他のサードパーティアプリケーション（たとえば、 ClusterLion ）で既存の構成を監視している場合は、古いコントローラを交換する前に、 Tiebreaker またはその他のソフトウェアから MetroCluster 構成を削除する必要があります。

手順

1. "既存の MetroCluster 設定を削除します" Tiebreaker ソフトウェアから。
2. スイッチオーバーを開始できるサードパーティ製アプリケーションから既存の MetroCluster 構成を削除します。

アプリケーションのマニュアルを参照してください。

古いコントローラを交換して新しいコントローラをブート

情報を収集して処理を再開すると、スイッチオーバー処理が自動化されます。

このタスクについて

自動化処理によってスイッチオーバーが開始され、 `heal-aggregates`および `heal root-aggregates` 操作：これらの処理が完了すると、処理は* paused for user intervention *で一時停止します。これにより、を使用して、コントローラをラックに設置し、パートナーコントローラをブートし、ルートアグリゲートディスクをフラッシュバックアップから新しいコントローラモジュールに再割り当てできます `sysids` さっき集まった。

作業を開始する前に

スイッチオーバーを開始する前に自動化処理が一時停止するため、サイト B のすべての LIF が「稼働」していることを手動で確認できます必要に応じて 'down' の LIF を up にし 'system controller replace resume' コマンドを使用して自動化処理を再開します

古いコントローラのネットワーク構成を準備

新しいコントローラでネットワークが正常に再開されるようにするには、 LIF を共通ポートに移動して、古いコントローラのネットワーク設定を削除する必要があります。

このタスクについて

- このタスクは、古いノードごとに実行する必要があります。

- で収集した情報を使用します [アップグレードを準備]。

手順

1. 古いノードをブートし、ノードにログインします。

   「 boot_ontap 」

2. 古いコントローラのすべてのデータ LIF のホームポートを、新旧両方のコントローラモジュールで同じ共通ポートに割り当てます。

   a. LIF を表示します。

      「 network interface show 」を参照してください

      SAN と NAS を含むすべてのデータ LIF は ' スイッチオーバーサイト（ cluster_A ）で稼働しているため ' 管理上の "" および運用上の "" ダウン "" になります

   b. の出力を確認して、クラスタポートとして使用されていない新旧両方のコントローラで同じ共通の物理ネットワークポートを特定します。

      たとえば、「 e0d 」は古いコントローラ上の物理ポートであり、新しいコントローラ上にも存在します。「 e0d 」は、クラスタポートとしても、新しいコントローラ上でも使用されません。

      プラットフォームモデルのポートの用途については、を参照してください "NetApp Hardware Universe の略"

   c. すべてのデータ LIF で共通ポートをホームポートとして使用するように変更します。

      「 network interface modify -vserver *svm -name _ -lif data -lif lif _ -home-port_port -id* 」と入力します

      次の例では、これは「 e0d 」です。

      例：

```
network interface modify -vserver vs0 -lif datalif1 -home-port e0d
```

3. ブロードキャストドメインを変更して、削除する必要がある VLAN と物理ポートを削除します。

   「 broadcast-domain remove-ports -broadcast-domain_domain-name-name_ports_node-name ： port-id_` 」

   すべての VLAN ポートと物理ポートについて、この手順を繰り返します。

4. クラスタポートをメンバーポートとして使用し、インターフェイスグループをメンバーポートとして使用している VLAN ポートをすべて削除します。

   a. VLAN ポートを削除します。

      「 network port vlan delete -node-node-name-vlan-name_portid -vlandid_ 」のように指定します

      例：

```
network port vlan delete -node node1 -vlan-name e1c-80
```

b. インターフェイスグループから物理ポートを削除します。

「 network port ifgrp remove-port -node-node_name -ifgrp_interface-group-name _ *port_portid* 」の形式で指定します

例：

```
network port ifgrp remove-port -node node1 -ifgrp a1a -port e0d
```

a. ブロードキャストドメインから VLAN ポートとインターフェイスグループポートを削除します。

'network port broadcast-domain remove-ports -ipspace_ipspace -broadcast-domain_domain -name_ports_nodename ： portname 、 nodename ： portname _ 、

b. 必要に応じて、他の物理ポートをメンバーとして使用するようにインターフェイスグループポートを変更します。

ifgrp add-port -node node_name -ifgrp *interface -group-name_port_port-id*`

5. ノードを停止します。

halt -inhibit-takeover true -node node_name `

この手順は両方のノードで実行する必要があります。

新しいコントローラをセットアップ

新しいコントローラをラックに設置してケーブルを接続する必要があります。

手順

1. 必要に応じて、新しいコントローラモジュールとストレージシェルフ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、構成内のストレージシェルフ数によって異なります。

2. 自身の適切な接地対策を行います
3. コントローラモジュールをラックまたはキャビネットに設置します。

"ONTAPハードウェアシステムのドキュメント"

4. 新しいコントローラモジュールに固有の FC-VI カードがない場合、および古いコントローラの FC-VI カードに新しいコントローラの互換性がある場合は、 FC-VI カードを交換し、正しいスロットに取り付けます。

を参照してください "NetApp Hardware Universe の略" を参照してください。

5. コントローラの電源、シリアルコンソール、および管理接続を、 MetroCluster インストールおよび設定ガイド _ の説明に従ってケーブル接続します。

   この時点で古いコントローラから切断されていた他のケーブルは接続しないでください。

   "ONTAPハードウェアシステムのドキュメント"

6. 新しいノードに電源を投入し、 LOADER プロンプトを表示するよう求められたら Ctrl+C キーを押します。

新しいコントローラをネットブート

新しいノードを設置したら、ネットブートを実行して、新しいノードが元のノードと同じバージョンの ONTAP を実行するようにする必要があります。ネットブートという用語は、リモート・サーバに保存された ONTAP イメージからブートすることを意味します。ネットブートの準備を行うときは、システムがアクセスできる Web サーバに、 ONTAP 9 ブート・イメージのコピーを配置する必要があります。

このタスクは、新しい各コントローラモジュールで実行します。

手順

1. にアクセスします "ネットアップサポートサイト" システムのネットブートの実行に使用するファイルをダウンロードするには、次の手順を実行します。
2. ネットアップサポートサイトのソフトウェアダウンロードセクションから該当する ONTAP ソフトウェアをダウンロードし、 Web にアクセスできるディレクトリに image.tgz ファイルを保存します。
3. Web にアクセスできるディレクトリに移動し、必要なファイルが利用可能であることを確認します。

プラットフォームモデル	作業
FAS/AFF8000 シリーズシステム	ターゲットディレクトリに version_image.tgzfile の内容を展開します。 tar -zxvf ONTAP-version _image.tgz 注： Windows で内容を展開する場合は、 7-Zip または WinRAR を使用してネットブートイメージを展開します。ディレクトリの一覧に、カーネルファイル netboot/ kernel を含むネットブートフォルダが表示される必要があります
その他すべてのシステム	ディレクトリの一覧に、カーネルファイルがあるネットブートフォルダを含める必要があります。 ONTAP-version _image.tgz ファイルを展開する必要はありません。

4. LOADER プロンプトで、管理 LIF のネットブート接続を設定します。
   - IP アドレスが DHCP の場合は、自動接続を設定します。

     ifconfig e0M -auto

   - IP アドレスが静的な場合は、手動接続を設定します。

     ifconfig e0M -addr= ip_addr-mask= netmask `-gw= gateway `

5. ネットブートを実行します。

- プラットフォームが 80xx シリーズシステムの場合は、次のコマンドを使用します。

  netboot\http://web_server_ip/path_to_web-accessible_directory/netboot/kernel`

- プラットフォームが他のシステムの場合は、次のコマンドを使用します。

  netboot\http://web_server_ip/path_to_web-accessible_directory/ontap-version_image.tgz`

6. ブートメニューからオプション * （７） Install new software first * を選択し、新しいソフトウェアイメージをダウンロードしてブートデバイスにインストールします。

```
 Disregard the following message: "This procedure is not supported for
Non-Disruptive Upgrade on an HA pair". It applies to nondisruptive
upgrades of software, not to upgrades of controllers.
```

．手順を続行するかどうかを確認するメッセージが表示されたら、「 `y` 」と入力し、パッケージの入力を求められたらイメージファイルの `URL` 「 `¥ http://web_server_ip/path_to_web-accessible_directory/ontap-version_image.tgz` 」を入力します

```
Enter username/password if applicable, or press Enter to continue.
```

7. 入力 `n` 次のようなプロンプトが表示されたら、バックアップの回復をスキップします。

```
Do you want to restore the backup configuration now? {y|n} n
```

8. 次のようなプロンプトが表示されたら 'y' と入力して再起動します

```
The node must be rebooted to start using the newly installed software.
Do you want to reboot now? {y|n} y
```

新しくインストールされたソフトウェアを使用するには、ノードを再起動する必要があります。

コントローラモジュールの設定をクリアします

MetroCluster 構成で新しいコントローラモジュールを使用する前に、既存の構成をクリアする必要があります。

手順

1. 必要に応じて、ノードを停止してプロンプトを表示し `LOADER`ます。

   「 halt 」

2. `LOADER`プロンプトで、環境変数をデフォルト値に設定します。

「デフォルト設定」

3. 環境を保存します。

   'aveenv

4. `LOADER`プロンプトでブートメニューを起動します。

   「 boot_ontap menu

5. ブートメニューのプロンプトで、設定を消去します。

   wipeconfig

   確認プロンプトに「 yes 」と応答します。

   ノードがリブートし、もう一度ブートメニューが表示されます。

6. ブートメニューでオプション * 5 * を選択し、システムをメンテナンスモードでブートします。

   確認プロンプトに「 yes 」と応答します。

HBA 構成をリストア

コントローラモジュールに HBA カードが搭載されているかどうかや設定によっては、サイトで使用するために正しく設定する必要があります。

手順

1. メンテナンスモードで、システム内の HBA の設定を行います。

   a. ucadmin show と入力し、各ポートの現在の設定を確認します

   b. 必要に応じてポートの設定を更新します。

HBA のタイプと目的のモード	使用するコマンド
CNA FC	ucadmin modify -m fc -t initiator_adapter-name _ `
CNA イーサネット	ucadmin modify -mode cna_adapter-name_`
FC ターゲット	fcadmin config -t target_adapter-name_`
FC イニシエータ	fcadmin config -t initiator_adapter-name_`

2. メンテナンスモードを終了します。

   「 halt 」

   コマンドの実行後、ノードが LOADER プロンプトで停止するまで待ちます。

3. ノードをブートしてメンテナンスモードに戻り、設定の変更が反映されるようにします。

「 boot_ontap maint 」を使用してください

4. 変更内容を確認します。

HBA のタイプ	使用するコマンド
CNA	ucadmin show
FC	fcadmin show`

ルートアグリゲートディスクを再割り当てします

前の手順で確認した「 sysconfig 」を使用して、ルートアグリゲートディスクを新しいコントローラモジュールに再割り当てします

このタスクについて

このタスクはメンテナンスモードで実行します。

古いシステムIDはで特定しました "アップグレード前に情報を収集"。

この手順の例では、次のシステム ID を持つコントローラを使用します。

ノード	古いシステム ID	新しいシステム ID
node_B_1	4068741254	1574774970

手順

1. 他のすべての接続を新しいコントローラモジュール（ FC-VI 、ストレージ、クラスタインターコネクトなど）にケーブル接続します。
2. システムを停止し、 LOADER プロンプトからメンテナンスモードでブートします。

   「 boot_ontap maint 」を使用してください

3. node_B_1 古いが所有するディスクを表示します。

   「ディスクショー - A` 」

   コマンド出力に、新しいコントローラモジュール（ 1574774970 ）のシステム ID が表示されます。ただし、ルートアグリゲートディスクは古いシステム ID （ 4068741254 ）で所有されます。この例で表示されているのは、 MetroCluster 構成の他のノードが所有するドライブではありません。

```
*> disk show -a
Local System ID: 1574774970

  DISK         OWNER                      POOL   SERIAL NUMBER    HOME
DR HOME
------------   -------------              -----  -------------
-------------             -------------
...
rr18:9.126L44 node_B_1-old(4068741254)   Pool1  PZHYN0MD
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:9.126L49 node_B_1-old(4068741254)   Pool1  PPG3J5HA
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L21 node_B_1-old(4068741254)   Pool1  PZHTDSZD
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L2  node_B_1-old(4068741254)   Pool0  S0M1J2CF
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L3  node_B_1-old(4068741254)   Pool0  S0M0CQM5
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:9.126L27 node_B_1-old(4068741254)   Pool0  S0M1PSDW
node_B_1-old(4068741254)  node_B_1-old(4068741254)
...
```

4. ドライブシェルフのルートアグリゲートディスクを新しいコントローラに再割り当てします。

   「ディスクの再割り当て -s *old-sysid*-d_new-sysid_`

   次の例は、ドライブの再割り当てを示しています。

```
*> disk reassign -s 4068741254 -d 1574774970
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)? n

After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)? Jul 14 19:23:49
[localhost:config.bridge.extra.port:error]: Both FC ports of FC-to-SAS
bridge rtp-fc02-41-rr18:9.126L0 S/N [FB7500N107692] are attached to this
controller.
y
Disk ownership will be updated on all disks previously belonging to
Filer with sysid 4068741254.
Do you want to continue (y/n)? y
```

5. すべてのディスクが想定どおりに再割り当てされていることを確認します。

   「ディスクショー」

```
*> disk show
Local System ID: 1574774970

  DISK         OWNER                      POOL   SERIAL NUMBER   HOME
DR HOME
------------  -------------              -----  -------------
-------------              -------------
rr18:8.126L18 node_B_1-new(1574774970)   Pool1  PZHYN0MD
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:9.126L49 node_B_1-new(1574774970)   Pool1  PPG3J5HA
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L21 node_B_1-new(1574774970)   Pool1  PZHTDSZD
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L2  node_B_1-new(1574774970)   Pool0  S0M1J2CF
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:9.126L29 node_B_1-new(1574774970)   Pool0  S0M0CQM5
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L1  node_B_1-new(1574774970)   Pool0  S0M1PSDW
node_B_1-new(1574774970)  node_B_1-new(1574774970)
*>
```

6. アグリゲートのステータスを表示します。

   「 aggr status 」を入力します

```
*> aggr status
           Aggr             State       Status            Options
aggr0_node_b_1-root         online      raid_dp, aggr     root, nosnap=on,
                            mirrored
mirror_resync_priority=high(fixed)
                            fast zeroed
                            64-bit
```

7. パートナーノードで上記の手順を繰り返します（ node_B_2 - 新規）。

新しいコントローラをブートします

コントローラのフラッシュイメージを更新するには、ブートメニューからコントローラをリブートする必要があります。暗号化が設定されている場合は、追加の手順が必要です。

VLAN とインターフェイスグループを再設定できます。必要に応じて、「 system controller replace resume 」コマンドを使用して処理を再開する前に、クラスタ LIF とブロードキャストドメインのポートを手動で変更します。

このタスクについて

このタスクはすべての新しいコントローラで実行する必要があります。

手順

1. ノードを停止します。

   「 halt 」

2. 外部キー管理ツールが設定されている場合は、関連する bootargs を設定します。

   'setenv bootarg.kmip.init.ipaddr *ip-address*'

   'setenv bootarg.kmip.init.netmask *netmask*`

   'setenv bootarg.kmip.init.gateway *gateway-address*

   'setenv bootarg.kmip.init.interface *interface-id*

3. ブートメニューを表示します。

   「 boot_ontap menu

4. ルート暗号化を使用する場合は、キー管理設定のブートメニューオプションを選択します。

使用するポート	選択するブートメニューオプション

オンボードキー管理	オプション "10 `" プロンプトに従って、キー管理ツールの構成をリカバリおよびリストアするために必要な入力を指定します。
外部キー管理	オプション "11`" プロンプトに従って、キー管理ツールの構成をリカバリおよびリストアするために必要な入力を指定します。

5. 自動ブートが有効になっている場合は、 Ctrl+C を押して自動ブートを中断します
6. ブートメニューからオプション "6`" を実行します

   オプション "6`" を選択すると ' 完了前にノードが 2 回再起動されます

   システム ID 変更プロンプトに「 y 」と入力します。2 回目のリブートメッセージが表示されるまで待ちます。

```
Successfully restored env file from boot media...

Rebooting to load the restored env file...
```

7. partner-sysid が正しいことを確認します。

   printenv partner-sysid

   partner-sysid が正しくない場合は、次のように設定します。

   'setenv partner-sysid_partner-SysID_`

8. ルート暗号化を使用する場合は、キー管理設定のブートメニューオプションを再度選択します。

使用するポート	選択するブートメニューオプション
オンボードキー管理	オプション "10 `" プロンプトに従って、キー管理ツールの構成をリカバリおよびリストアするために必要な入力を指定します。
外部キー管理	オプション "11`" プロンプトに従って、キー管理ツールの構成をリカバリおよびリストアするために必要な入力を指定します。

キー・マネージャの設定に応じて '10 またはオプション 11 を選択し ' 最初のブート・メニュー・プロンプトでオプション 6 を選択して 'recovery 手順を実行しますノードを完全にブートするには ' オプション "1" によって続行されるリカバリ手順 (通常のブート) を繰り返す必要がある場合があります

9. ノードをブートします。

   「 boot_ontap 」

10. 交換したノードがブートするまで待ちます。

    いずれかのノードがテイクオーバーモードの場合は、「 storage failover giveback 」コマンドを使用してギブバックを実行します。

11. すべてのポートがブロードキャストドメインに属していることを確認します。

    a. ブロードキャストドメインを表示します。

       「 network port broadcast-domain show 」

    b. 必要に応じて、ブロードキャストドメインにポートを追加します。

       "ブロードキャストドメインのポートを追加または削除します"

    c. インタークラスタLIFをホストする物理ポートを対応するブロードキャストドメインに追加します。

    d. 新しい物理ポートをホームポートとして使用するようにクラスタ間 LIF を変更します。

    e. クラスタ間 LIF が起動したら、クラスタピアのステータスを確認し、必要に応じてクラスタピアリングを再確立します。

       クラスタピアリングの再設定が必要になる場合があります。

       "クラスタピア関係を作成します。"

    f. 必要に応じて、 VLAN とインターフェイスグループを再作成します。

       VLAN およびインターフェイスグループのメンバーシップは、古いノードと異なる場合があります。

       "VLANを作成します。"

    "物理ポートを組み合わせてインターフェイスグループを作成"

    a. パートナークラスタが到達可能であり、パートナークラスタで設定が再同期されたことを確認します。

       ```
       metrocluster switchback -simulate true
       ```

12. 暗号化を使用する場合は、キー管理設定に対応したコマンドを使用してキーをリストアします。

使用するポート	使用するコマンド

オンボードキー管理	「セキュリティキーマネージャオンボード同期」 詳細については、を参照してください "オンボードキー管理暗号化キーのリストア"。
外部キー管理	「 securitykey manager external restore -vserver *svm*-node __ key -server_host_name

13. 処理を再開する前に、 MetroCluster が正しく設定されていることを確認してください。ノードのステータスを確認します。

    MetroCluster node show

    新しいノード（ site_B ）の状態が「 Waiting for switchback state * from site_A 」であることを確認します

14. 処理を再開します。

    「システムコントローラの交換が再開」

アップグレードを完了します

自動処理では、検証システムのチェックが実行されたあと一時停止するため、ネットワークの到達可能性を確認できます。検証が完了すると、リソースの再取得フェーズが開始され、自動化処理によってサイト A でスイッチバックが実行され、アップグレード後のチェックで一時停止されます。自動処理を再開すると、アップグレード後のチェックが実行され、エラーが検出されない場合はアップグレードが完了としてマークされます。

手順

1. コンソールメッセージに従って、ネットワークの到達可能性を確認します。
2. 検証が完了したら、処理を再開します。

    「システムコントローラの交換が再開」

3. 自動化処理では、サイト A でスイッチバックが実行され、アップグレード後のチェックが実行されます。処理が一時停止した場合は、コンソールメッセージに従って SAN LIF のステータスを手動で確認し、ネットワーク設定を確認します。
4. 検証が完了したら、処理を再開します。

    「システムコントローラの交換が再開」

5. アップグレード後チェックのステータスを確認します。

    「 system controller replace show 」と表示されます

    アップグレード後のチェックでエラーが報告されなかった場合、アップグレードは完了です。

6. コントローラのアップグレードが完了したら、サイト B でログインし、交換したコントローラが正しく設定されていることを確認します。

cluster_Aのノードをアップグレードします。

アップグレード手順を繰り返して、サイトAのcluster_Aのノードをアップグレードする必要があります。

手順

1. cluster_Aのノードをアップグレードするために、上記の手順を繰り返しアップグレードを準備ます。

   手順を繰り返すと、クラスターとノードへのすべての例の参照が逆になります。

Tiebreaker 監視をリストアしています

MetroCluster 構成が Tiebreaker ソフトウェアで監視するように設定されている場合は、 Tiebreaker 接続をリストアできます。

1. の手順を使用します "MetroCluster 構成を追加"。

4 ノード MetroCluster FC 構成を更新しています

4 ノード MetroCluster 構成のコントローラとストレージをアップグレードするには、構成を拡張して 8 ノード構成にし、古いディザスタリカバリ（ DR ）グループを削除します。

このタスクについて

「古いノード」とは、置き換えるノードを意味します。

- この手順 を使用できるのは、MetroCluster FC構成の特定のプラットフォームモデルのみです。
  - サポートされるプラットフォームアップグレードの組み合わせについては、のMetroCluster FC更新の表を参照してください "システムの更新方法を選択する"。

コンソールログを有効にする

NetAppでは、使用しているデバイスでコンソールロギングをイネーブルにし、この手順を実行する際に次のアクションを実行することを強く推奨します。

- メンテナンス中はAutoSupportを有効のままにします。
- メンテナンスの前後にメンテナンスAutoSupportメッセージをトリガーして、メンテナンスアクティビティ中にケースの作成を無効にします。

  ナレッジベースの記事を参照してください "スケジュールされたメンテナンス時間中にケースの自動作成を停止する方法"。

- 任意のCLIセッションのセッションロギングをイネーブルにします。セッションログを有効にする方法については、ナレッジベースの記事の「セッション出力のログ」セクションを参照してください "ONTAPシステムへの接続を最適化するためのPuTTYの設定方法"。

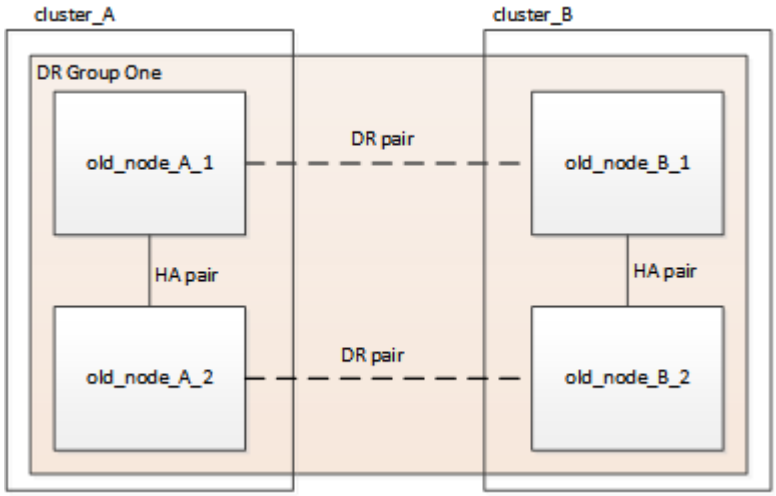
更新手順の実行

MetroCluster FC構成を更新するには、次の手順を実行します。

手順

1. 古いノードから情報を収集します。

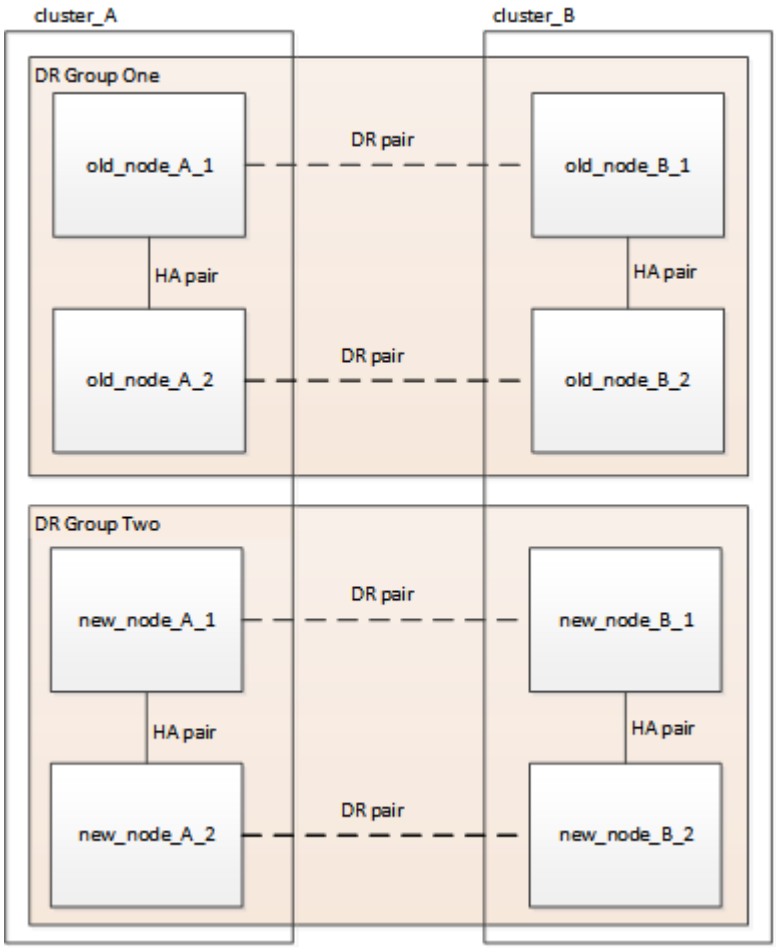
   この段階では、次の図に示すように 4 ノード構成が表示されます。



2. MetroCluster タイプに対応した 4 ノード拡張手順のすべての手順を実行します。

   "4 ノード MetroCluster FC 構成から 8 ノード構成への拡張"

   拡張手順が完了すると、次の図のような構成が表示されます。



3. CRS ボリュームを移動します。

   の手順を実行します "MetroCluster 構成でメタデータボリュームを移動する"。

4. 次の手順に従って、古いノードから新しいノードにデータを移動します。

   a. のすべての手順を実行します "アグリゲートの作成と新しいノードへのボリュームの移動"。

      アグリゲートのミラーリングは、作成時または作成後に実行できます。

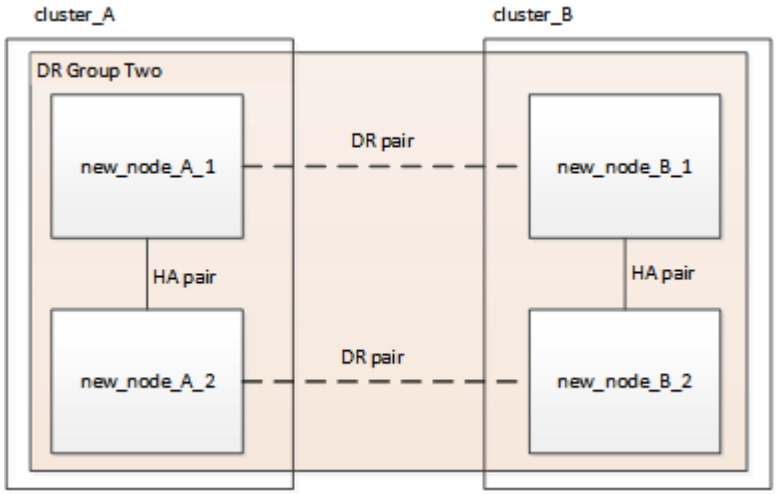
   b. のすべての手順を実行します "SAN 以外のデータ LIF とクラスタ管理 LIF を新しいノードに移動します"。

   c. のすべての手順を実行します "SAN LIF が元のノードから不要になりました"。

5. 手順の手順に従って、古い DR グループを削除します。

   "ディザスタリカバリグループを削除しています"

   古い DR グループ（ DR グループ 1 ）を削除すると、次の図のような構成が表示されます。



4ノードまたは8ノードのMetroCluster IP構成を更新（ONTAP 9.8以降）

この手順 を使用して、4ノードまたは8ノード構成のコントローラとストレージをアップグレードできます。

ONTAP 9.13.1以降では、8ノードMetroCluster IP構成のコントローラとストレージをアップグレードできます。そのためには、構成を拡張して一時的に12ノード構成にし、古いディザスタリカバリ（DR）グループを削除します。

ONTAP 9.8以降では、4ノードMetroCluster IP構成のコントローラとストレージをアップグレードできます。そのためには、構成を拡張して一時的な8ノード構成にしてから、古いDRグループを削除します。

古いプラットフォームモデルを追加する場合の重要な情報

次のガイダンスは、新しいプラットフォーム モデル (ONTAP 9.15.1 以降でリリースされたプラットフォー

ム) を含む既存のMetroCluster構成に古いプラットフォーム モデル (ONTAP 9.15.1 より前にリリースされたプラットフォーム) を追加する必要がある、まれなシナリオを対象としています。

既存のMetroCluster構成に、共有クラスタ/**HA** ポート を使用するプラットフォーム (ONTAP 9.15.1 以降でリリースされたプラットフォーム) が含まれている場合、構成内のすべてのノードをONTAP 9.15.1P11 またはONTAP 9.16.1P4 以降にアップグレードせずに、共有**MetroCluster/HA** ポート を使用するプラットフォーム (ONTAP 9.15.1 より前にリリースされたプラットフォーム) を追加することはできません。



共有/ **MetroCluster HA** ポート を使用する古いプラットフォーム モデルを、共有クラスタ/**HA** ポート を使用する新しいプラットフォーム モデルを含むMetroClusterに追加することはまれなシナリオであり、ほとんどの組み合わせは影響を受けません。

次の表を使用して、組み合わせが影響を受けるかどうかを確認してください。既存のプラットフォームが最初の列にリストされ、構成に追加するプラットフォームが 2 番目の列にリストされている場合、新しい DR グループを追加するには、構成内のすべてのノードでONTAP 9.15.1P11 またはONTAP 9.16.1P4 以降が実行されている必要があります。

既存の **MetroCluster** に以下が含まれている場合...		追加するプラットフォームは...		作業
共有クラスター/**HA** ポート を使用する AFF システム: • AFF A20用 • AFF A30用 • AFF C30 • AFF A50用 • AFF C60 • AFF C80用 • AFF A70用 • AFF A90用 • AFF A1K用	共有クラスター/**HA** ポート を使用する FAS システム: • FAS50 • FAS70 • FAS90	共有 **MetroCluster/HA** ポート を使用する AFF システム: • AFF A150、ASA A150向け • AFF A220 • AFF C250 、ASA C250向け • AFF A250、ASA A250向け • AFF A300 • AFF A320 • AFF C400 、ASA C400向け • AFF A400、ASA A400向け • AFF A700 • AFF C800 、ASA C800向け • AFF A800、ASA A800向け • AFF A900、ASA A900向け	共有 **MetroCluster/HA** ポート を使用する FAS システム: • FAS2750 • FAS500f • FAS8200 • FAS8300 • FAS8700 の場合 • FAS9000 • FAS9500	既存の MetroCluster 構成に新しいプラットフォームを追加する前に、既存および新しい構成内のすべてのノードを ONTAP 9.15.1P11 または ONTAP 9.16.1P4 以降にアップグレードします。

このタスクについて

- 8ノード構成の場合は、システムでONTAP 9.13.1以降が実行されている必要があります。
- 4ノード構成の場合は、システムでONTAP 9.8以降が実行されている必要があります。
- IPスイッチもアップグレードする場合は、このリフレッシュ手順 を実行する前にスイッチをアップグレードする必要があります。
- この手順 では、1つの4ノードDRグループを更新するために必要な手順について説明します。8ノード構成（DRグループが2つ）の場合は、一方または両方のDRグループを更新できます。

```
 Refresh DR groups one at a time.
* References to "old nodes" mean the nodes that you intend to replace.
* For eight-node configurations, the source and target eight-node
MetroCluster platform combination must be supported.
```

両方のDRグループを更新する場合、最初のDRグループを更新したあとにプラットフォームの組み合わせがサポートされないことがあります。サポートされる8ノード構成にするには、両方のDRグループを更新する必要があります。

- MetroCluster IP構成では、この手順 を使用して特定のプラットフォームモデルのみを更新できます。
  - サポートされるプラットフォームのアップグレードの組み合わせについては、のMetroCluster IP更新テーブルを参照してください "システムの更新方法を選択する"。
- ソースプラットフォームとターゲットプラットフォームの下限が適用されます。上位のプラットフォームに移行する場合は、すべてのDRグループの機器更改が完了するまで新しいプラットフォームの制限が適用されません。
- ソースプラットフォームよりも制限が低いプラットフォームに対して機器更改を実行する場合は、この手順 を実行する前に、ターゲットプラットフォームの制限に合わせて制限を調整し、制限をターゲットプラットフォームの制限以下にする必要があります。

コンソールログを有効にする

NetAppでは、使用しているデバイスでコンソールロギングをイネーブルにし、この手順を実行する際に次のアクションを実行することを強く推奨します。

- メンテナンス中はAutoSupportを有効のままにします。
- メンテナンスの前後にメンテナンスAutoSupportメッセージをトリガーして、メンテナンスアクティビティ中にケースの作成を無効にします。

  ナレッジベースの記事を参照してください "スケジュールされたメンテナンス時間中にケースの自動作成を停止する方法"。

- 任意のCLIセッションのセッションロギングをイネーブルにします。セッションログを有効にする方法については、ナレッジベースの記事の「セッション出力のログ」セクションを参照してください "ONTAPシステムへの接続を最適化するためのPuTTYの設定方法"。

更新手順の実行

MetroCluster IP設定を更新するには、次の手順を実行します。

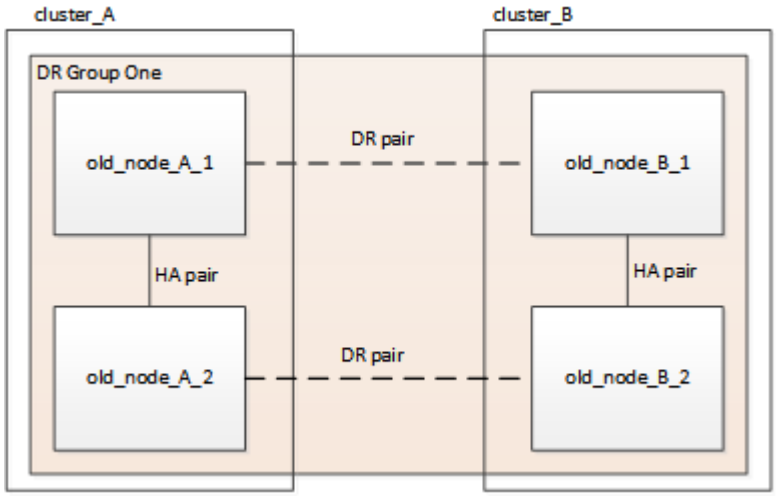
手順

1. 古いノードにデフォルトのブロードキャストドメインが作成されていることを確認します。

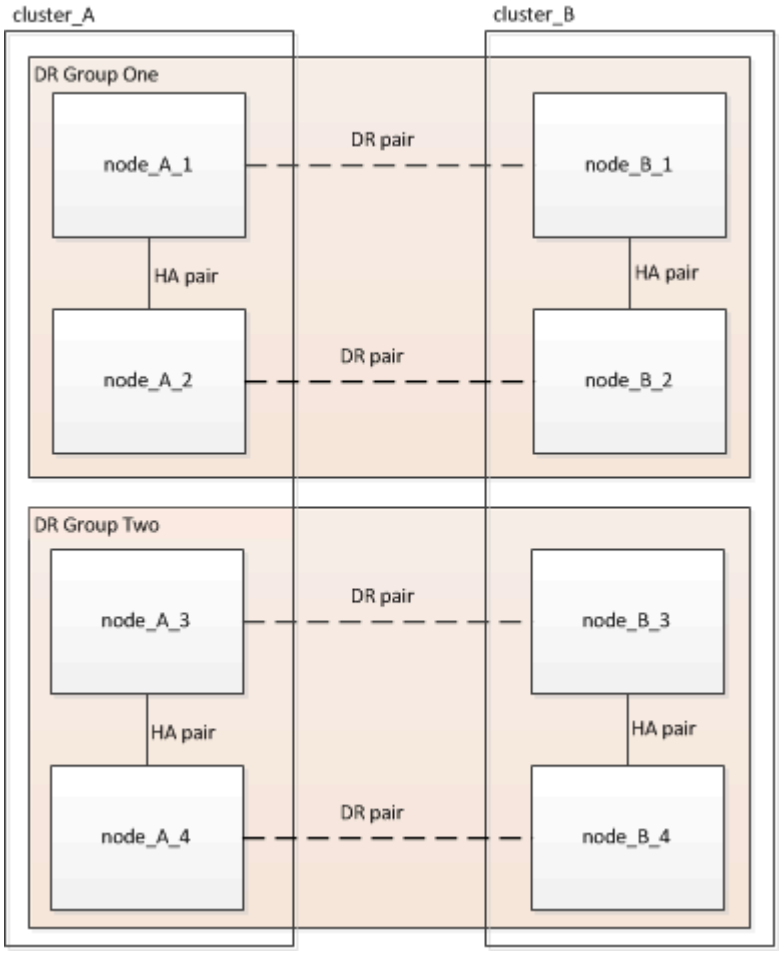
   デフォルトのブロードキャストドメインがない既存のクラスタに新しいノードを追加すると、想定される名前ではなくUniversal Unique Identifier（UUID）を使用して新しいノード用のノード管理LIFが作成されます。詳細については、技術情報アーティクルを参照してください "UUID名で生成された新しく追加されたノードのノード管理LIF"。

2. 古いノードから情報を収集します。

   この段階では、次の図に示すように 4 ノード構成が表示されます。



   次の図のような8ノード構成が表示されます。



3. サポートケースが自動で生成されないようにするには、アップグレードが進行中であることを示す AutoSupport メッセージを送信します。

   a. 次のコマンドを問題で実行します。 + 「 system node AutoSupport invoke -node * -type all -message

」 MAINT=10h Upgrading _old-model_To _new-model 」 _`

次の例では、メンテナンス時間を10時間にしています。計画に応じて追加の時間を確保してください。

この時間が経過する前にメンテナンスが完了した場合は、メンテナンス期間が終了したことを通知する AutoSupport メッセージを起動できます。

「 system node AutoSupport invoke -node * -type all -message MAINT= end 」というメッセージが表示されます

a. パートナークラスタに対してこのコマンドを繰り返します。

4. エンドツーエンドの暗号化が有効になっている場合は、次の手順を実行します。 "エンドツーエンドの暗号化を無効にする"。

5. Tiebreaker 、メディエーター、またはスイッチオーバーを開始できるその他のソフトウェアから既存の MetroCluster 構成を削除します。

使用するポート	使用する手順
Tiebreaker	a. MetroCluster 構成を削除するには 'Tiebreaker CLI の monitor remove コマンドを使用します 次の例では ' "cluster_a" がソフトウェアから削除されています `NetApp MetroCluster Tiebreaker :> monitor remove -monitor -name cluster_A Successfully removed monitor from NetApp MetroCluster Tiebreaker software.` b. Tiebreaker CLIを使用して、MetroCluster の設定が正しく削除されたことを確認します `monitor show -status` コマンドを実行します `NetApp MetroCluster Tiebreaker :> monitor show -status`
メディエーター	ONTAP プロンプトで次のコマンドを問題に設定します。 MetroCluster 構成設定のメディエーターが削除されました

サードパーティ製アプリケーション	製品マニュアルを参照してください。

6. のすべての手順を実行します "MetroCluster IP構成の拡張" をクリックして新しいノードとストレージを構成に追加してください。

   拡張手順 が完了すると、一時的な設定が次の図のように表示されます。

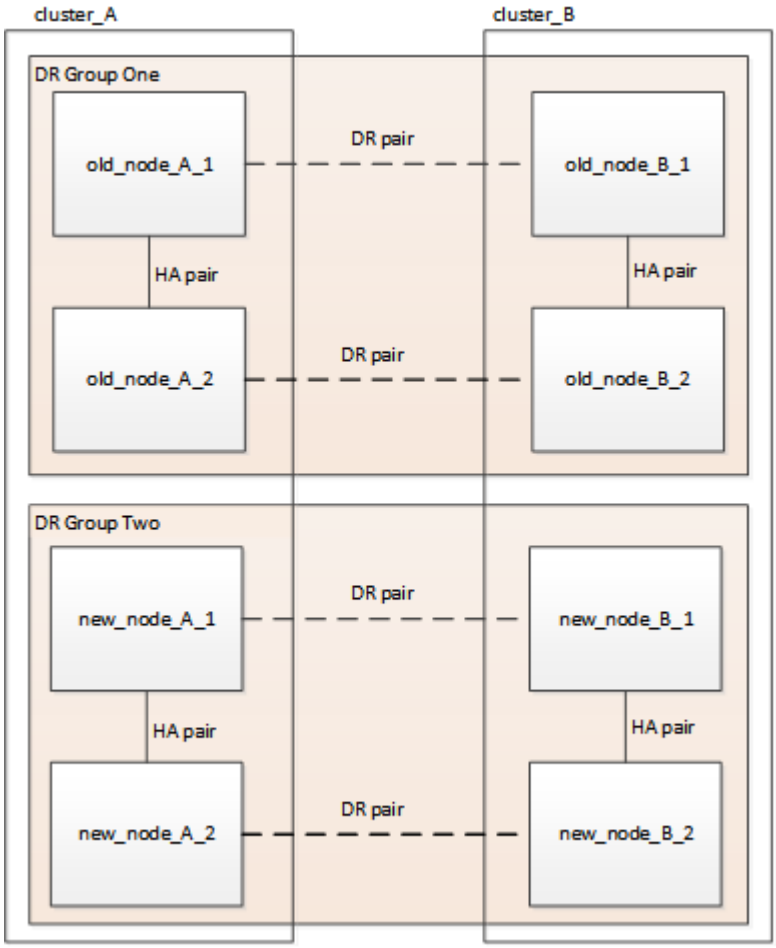


図 **1. 8**ノードの一時的な構成

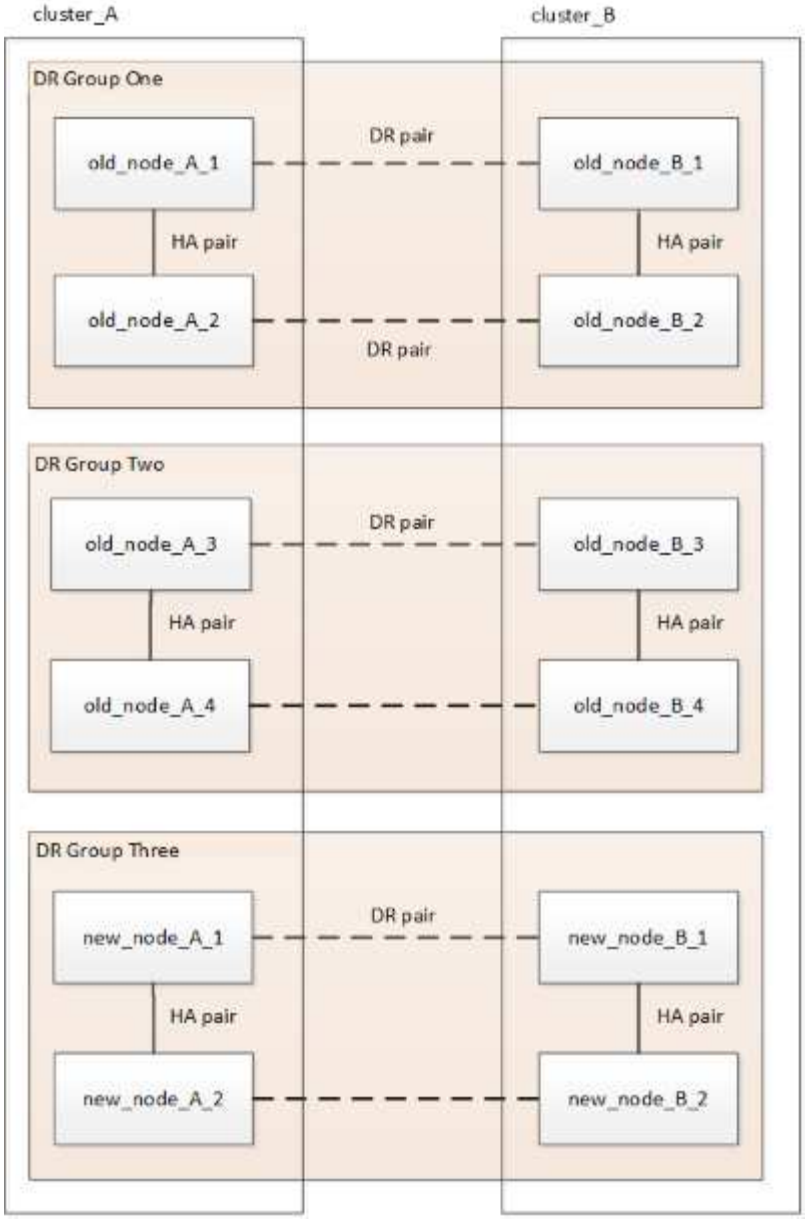


図 **2.** 一時的な**12**ノード構成

7. 両方のクラスタで次のコマンドを実行して、テイクオーバーが可能で、ノードが接続されていることを確認します。

「 storage failover show 」をクリックします

```
cluster_A::> storage failover show
                                    Takeover
Node           Partner              Possible    State Description
-------------- -------------------- ---------   ------------------
Node_FC_1      Node_FC_2              true      Connected to Node_FC_2
Node_FC_2      Node_FC_1              true      Connected to Node_FC_1
Node_IP_1      Node_IP_2              true      Connected to Node_IP_2
Node_IP_2      Node_IP_1              true      Connected to Node_IP_1
```

8. CRS ボリュームを移動します。

   の手順を実行します "MetroCluster 構成でのメタデータボリュームの移動"。

9. 次の手順を使用して、古いノードから新しいノードにデータを移動します。
   a. のすべての手順を実行します "アグリゲートを作成してボリュームを新しいノードに移動"。

      アグリゲートのミラーリングは、作成時または作成後に実行できます。

   b. のすべての手順を実行します "SAN以外のデータLIFとクラスタ管理LIFを新しいノードに移動する"。
10. 各クラスタについて、移行したノードのクラスタピアのIPアドレスを変更します。
    a. を使用して、cluster_Aピアを特定します `cluster peer show` コマンドを実行します

```
cluster_A::> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability
Authentication
------------------------- --------------------- --------------
--------------
cluster_B         1-80-000011           Unavailable    absent
```

       i. cluster_Aピアの IPアドレスを変更します。

```
cluster peer modify -cluster cluster_A -peer-addrs node_A_3_IP -address
-family ipv4
```

    b. を使用して、cluster_Bピアを特定します `cluster peer show` コマンドを実行します

```
cluster_B::> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability
Authentication
------------------------- --------------------- --------------
--------------
cluster_A         1-80-000011           Unavailable    absent
```

       i. cluster_Bピアの IPアドレスを変更します。

```
cluster peer modify -cluster cluster_B -peer-addrs node_B_3_IP -address
-family ipv4
```

    c. 各クラスタのクラスタピアIPアドレスが更新されていることを確認します。

       i. を使用して、各クラスタのIPアドレスが更新されていることを確認します `cluster peer show -instance` コマンドを実行します

          。 `Remote Intercluster Addresses` 次の例のフィールドには、更新されたIPアドレスが表示

されます。

cluster_Aの例：

```
cluster_A::> cluster peer show -instance

Peer Cluster Name: cluster_B
           Remote Intercluster Addresses: 172.21.178.204,
172.21.178.212
      Availability of the Remote Cluster: Available
                     Remote Cluster Name: cluster_B
                     Active IP Addresses: 172.21.178.212,
172.21.178.204
                   Cluster Serial Number: 1-80-000011
                    Remote Cluster Nodes: node_B_3-IP,
                                          node_B_4-IP
                   Remote Cluster Health: true
                 Unreachable Local Nodes: -
          Address Family of Relationship: ipv4
    Authentication Status Administrative: use-authentication
       Authentication Status Operational: ok
                         Last Update Time: 4/20/2023 18:23:53
            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

cluster_A::>
```

+
たとえば、cluster_Bです

```
cluster_B::> cluster peer show -instance

                          Peer Cluster Name: cluster_A
              Remote Intercluster Addresses: 172.21.178.188, 172.21.178.196
<<<<<<<< Should reflect the modified address
      Availability of the Remote Cluster: Available
                     Remote Cluster Name: cluster_A
                     Active IP Addresses: 172.21.178.196, 172.21.178.188
                   Cluster Serial Number: 1-80-000011
                    Remote Cluster Nodes: node_A_3-IP,
                                          node_A_4-IP
                   Remote Cluster Health: true
                 Unreachable Local Nodes: -
           Address Family of Relationship: ipv4
    Authentication Status Administrative: use-authentication
       Authentication Status Operational: ok
                         Last Update Time: 4/20/2023 18:23:53
             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

cluster_B::>
```

11. の手順に従います "ディザスタリカバリグループを削除しています" をクリックして、古いDRグループを削除します。
12. 8 ノード構成で両方の DR グループを更新する必要がある場合は、各 DR グループに対して手順全体を繰り返します。

古いDRグループを削除すると、次の図のような設定が表示されます。

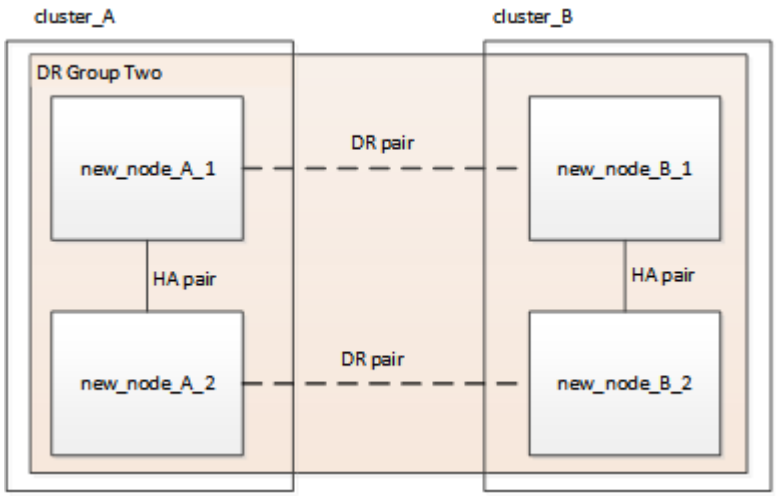


図 **3. 4** ノード構成

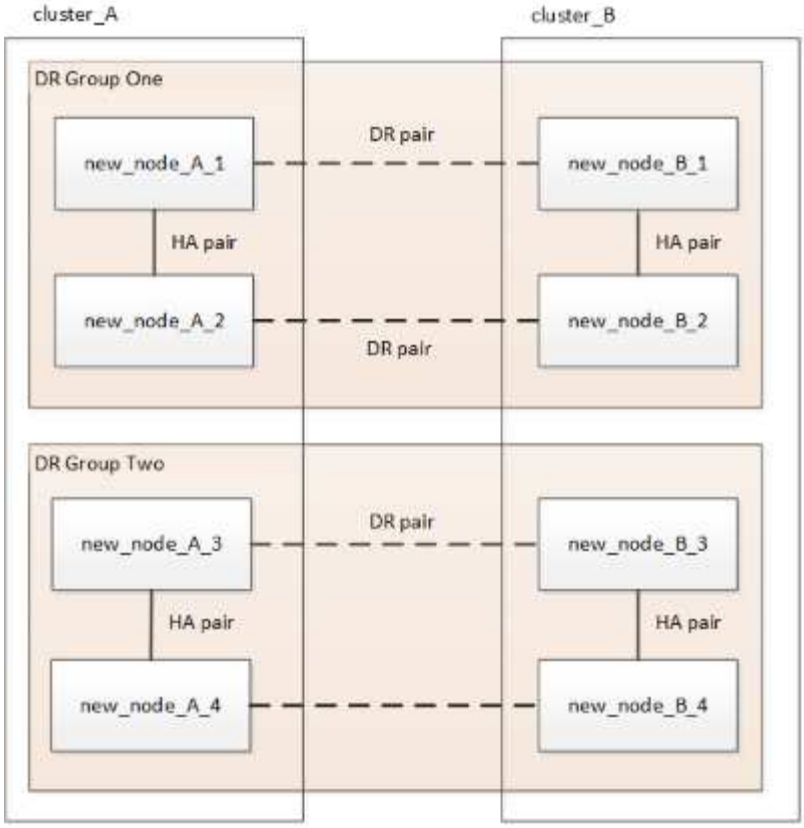


図 **4. 8**ノード構成

13. MetroCluster 構成の運用モードを確認し、 MetroCluster チェックを実行
    a. MetroCluster 構成と運用モードが正常な状態であることを確認します。

       「 MetroCluster show 」

    b. 想定されるすべてのノードが表示されることを確認します。

       MetroCluster node show

    c. 次のコマンドを問題に設定します。

       「 MetroCluster check run 」のようになります

    d. MetroCluster チェックの結果を表示します。

       MetroCluster チェックショー

14. 新しいノードを追加する前にエンドツーエンドの暗号化を無効にした場合は、の手順に従って再度有効にできます。 "エンドツーエンドの暗号化を実現"。
15. 必要に応じて、構成に応じて手順を使用してリストアを監視します。

使用するポート	この手順を使用します

Tiebreaker	"MetroCluster 構成を追加しています" *MetroCluster Tiebreaker* のインストールと構成 を参照してください。
メディエーター	"MetroCluster IP構成からONTAPメディエーターを構成する" *MetroCluster IP* のインストールと構成を参照してください。
サードパーティ製アプリケーション	製品マニュアルを参照してください。

16. サポートケースの自動生成を再開するには、メンテナンスが完了したことを示す AutoSupport メッセージを送信します。

    a. 次のコマンドを問題に設定します。

       「 system node AutoSupport invoke -node * -type all -message MAINT= end 」というメッセージが表示されます

    b. パートナークラスタに対してこのコマンドを繰り返します。

2 ノード MetroCluster FC 構成を 4 ノード構成に拡張

2 ノード MetroCluster FC 構成から 4 ノード構成への拡張

2 ノード MetroCluster FC 構成を 4 ノード MetroCluster FC 構成に拡張するには、各クラスタにコントローラを追加して各 MetroCluster サイトに HA ペアを形成してから、MetroCluster FC 構成をリフレッシュします。

作業を開始する前に

- ノードが MetroCluster FC 構成で ONTAP 9 以降を実行している必要があります。

  この手順は、以前のバージョンの ONTAP または MetroCluster IP 構成ではサポートされていません。

- 2 ノード構成のプラットフォームが ONTAP 9.2 でサポートされない場合に、 ONTAP 9.2_or_expand でサポートされるプラットフォームにアップグレードするには、 MetroCluster FC 構成を拡張する前に 2 ノード構成のプラットフォームをアップグレードする必要があります。
- 既存の MetroCluster FC 構成が健全な状態である必要があります。
- 追加する機器がサポートされており、次の手順で説明するすべての要件を満たしている必要があります。

  "ファブリック接続 MetroCluster のインストールと設定"

  "ストレッチ MetroCluster のインストールと設定"

- 新しいコントローラとブリッジに対応する FC スイッチポートが必要です。
- 古いノードにデフォルトのブロードキャストドメインが作成されていることを確認します。

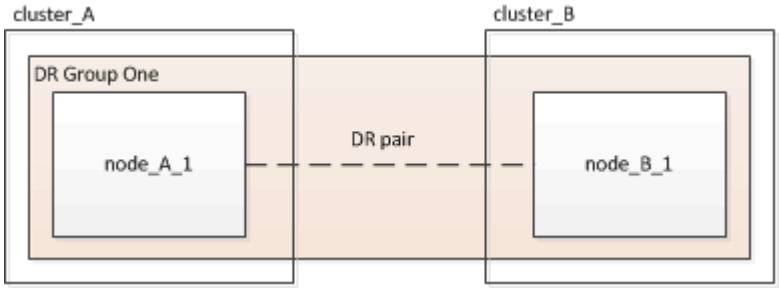
  デフォルトのブロードキャストドメインがない既存のクラスタに新しいノードを追加すると、想定される

名前ではなくUniversal Unique Identifier（UUID）を使用して新しいノード用のノード管理LIFが作成されます。詳細については、技術情報アーティクルを参照してください "UUID名で生成された新しく追加されたノードのノード管理LIF"。

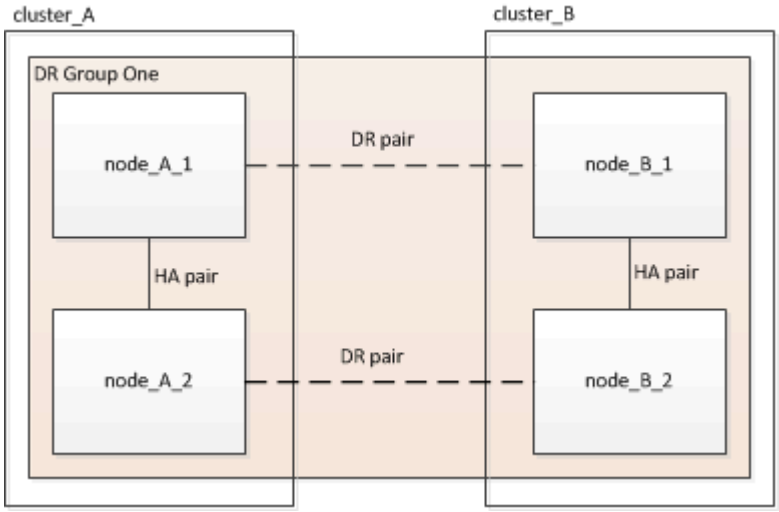
- 管理パスワードと FTP サーバまたは SCP サーバへのアクセスが必要です。

このタスクについて

- この手順は、 MetroCluster FC 構成にのみ適用されます。
- この手順はシステムの停止を伴うため、完了までに約 4 時間かかります。
- この手順を実行する前は、 2 つのシングルノードクラスタで MetroCluster FC 構成が構成されています。



この手順の完了後、各サイトに 1 つずつ、 2 つの HA ペアで MetroCluster FC 構成が構成されます。



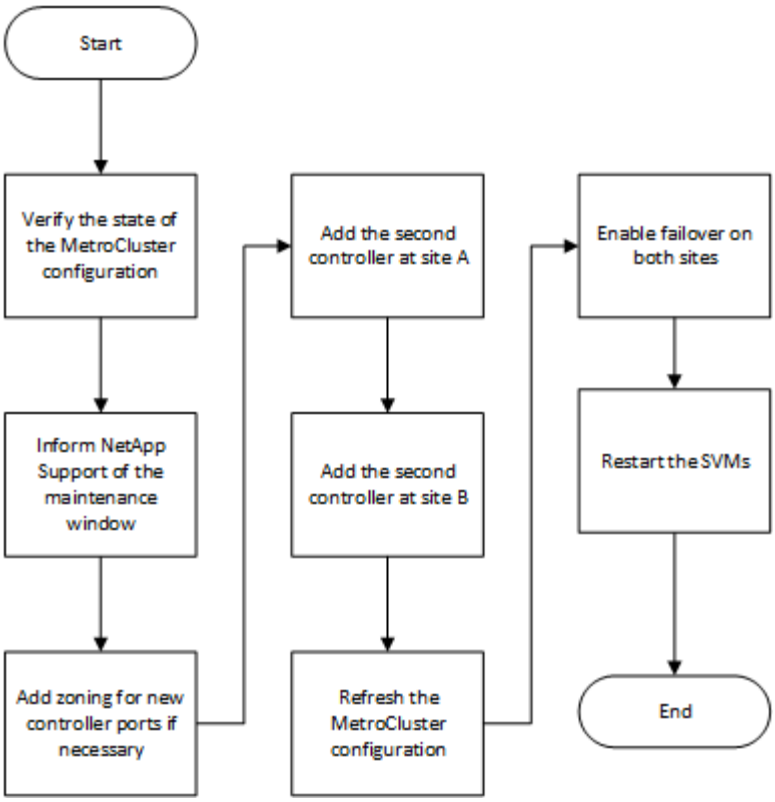
- 両方のサイトを同じように拡張する必要があります。

  MetroCluster 構成では、ノードの数を奇数にすることはできません。

- この手順にはサイトごとに 1 時間以上かかることがあり、ディスクの初期化や新しいノードのネットブートなどのタスクに時間がかかります。

  ディスクの初期化にかかる時間は、ディスクのサイズによって異なります。

- この手順では次のワークフローを使用します。



コンソールログを有効にする

このタスクを実行する前に、デバイスでコンソールログを有効にしてください。

NetAppでは、使用しているデバイスでコンソールロギングをイネーブルにし、この手順を実行する際に次のアクションを実行することを強く推奨します。

- メンテナンス中はAutoSupportを有効のままにします。
- メンテナンスの前後にメンテナンスAutoSupportメッセージをトリガーして、メンテナンスアクティビティ中にケースの作成を無効にします。

  ナレッジベースの記事を参照してください "スケジュールされたメンテナンス時間中にケースの自動作成を停止する方法"。

- 任意のCLIセッションのセッションロギングをイネーブルにします。セッションログを有効にする方法については、ナレッジベースの記事の「セッション出力のログ」セクションを参照してください "ONTAPシステムへの接続を最適化するためのPuTTYの設定方法"。

MetroCluster 構成の状態の確認

既存のコントローラを特定し、コントローラ間のディザスタリカバリ（ DR ）関係、コントローラが通常モードであること、およびアグリゲートがミラーされていることを確認する必要があります。

手順

1. 構成内の任意のノードから、 MetroCluster 構成内のノードの詳細を表示します。

MetroCluster node show -fields node 、 dr-partner 、 dr-partner-systemid`

次の出力は、この MetroCluster 構成に DR グループが 1 つ、各クラスタにノードが 1 つあることを示しています。

```
cluster_A::> metrocluster node show -fields node,dr-partner,dr-partner-
systemid

dr-group-id  cluster         node            dr-partner      dr-partner-
systemid
-----------  -------------   -------         ----------
-------------------
1            cluster_A       controller_A_1  controller_B_1  536946192
1            cluster_B       controller_B_1  controller_A_1  536946165
2 entries were displayed.
```

2. MetroCluster 設定の状態を表示します。

「 MetroCluster show 」

次の出力は、 MetroCluster 構成内の既存のノードが通常モードであることを示しています。

```
cluster_A::> metrocluster show

Configuration: two-node-fabric

Cluster                           Entry Name              State
----------------------------- ----------------------
---------------------
Local: cluster_A                  Configuration State     configured
                                  Mode                    normal
                                  AUSO Failure Domain     auso-on-cluster-
disaster
Remote: controller_B_1_siteB
                                  Configuration State     configured
                                  Mode                    normal
                                  AUSO Failure Domain     auso-on-cluster-
disaster
```

3. MetroCluster 構成の各ノードのアグリゲートの状態を確認します。

「 storage aggregate show

次の出力は、 cluster_A のアグリゲートがオンラインであり、ミラーされていることを示しています。

```
cluster_A::> storage aggregate show


Aggregate                 Size     Available Used%  State   #Vols  Nodes
RAID Status
---------                 -------- --------- -----  ------- ------
---------------- ------------
aggr0_controller_A_1_0   1.38TB   68.63GB   95%    online    1
controller_A_1   raid_dp,mirrored
controller_A_1_aggr1     4.15TB   4.14TB    0%     online    2
controller_A_1   raid_dp,mirrored
controller_A_1_aggr2     4.15TB   4.14TB    0%     online    1
controller_A_1   raid_dp,mirrored
3 entries were displayed.

cluster_A::>
```

AutoSupport 構成にノードを追加する前にカスタム MetroCluster メッセージを送信する

メンテナンスが進行中であることをネットアップテクニカルサポートに通知するには、AutoSupport に問題メッセージを送信する必要があります。システム停止が発生したとみなしてテクニカルサポートがケースをオープンしないように、メンテナンスが進行中であることを通知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 サイトごとに実行する必要があります。

手順

1. Site_A のクラスタにログインします
2. メンテナンスの開始を通知する AutoSupport メッセージを起動します。

   「 system node AutoSupport invoke -node * -type all -message MAINT= *maintenance-window-in-hours* 」というメッセージが表示されます

   「 maintenance-window-in-hours 」パラメータは、メンテナンス時間の長さを指定します。最大値は 72 時間です。この時間が経過する前にメンテナンスが完了問題した場合は、次のコマンドを使用して、メンテナンス期間が終了したことを通知できます。

   「 system node AutoSupport invoke -node * -type all -message MAINT= end 」というメッセージが表示されます

3. 同じ手順をパートナーサイトでも実行します。

ファブリック接続 **MetroCluster** 構成でコントローラモジュールを追加する際の新しいコントローラポートのゾーニング

FC スイッチゾーニングが新しいコントローラ接続に対応している必要があります。ネットアップが提供する Reference Configuration File （ RCF ；リファレンス構成ファイル）を使用してスイッチを設定した場合、ゾーニングは事前に設定されているため、変更は必要ありません。

FC スイッチを手動で設定した場合は、ゾーニングが新しいコントローラモジュールからのイニシエータ接続に対応していることを確認する必要があります。のゾーニングに関するセクションを参照してください "ファブリック接続 MetroCluster のインストールと設定"。

各クラスタに新しいコントローラモジュールを追加します

各クラスタに新しいコントローラモジュールを追加しています

各サイトに新しいコントローラモジュールを追加して、各サイトに HA ペアを作成する必要があります。これは、ハードウェアとソフトウェアの両方の変更を伴う複数の手順からなるプロセスであり、それぞれのサイトで正しい順序で実行する必要があります。

このタスクについて

- 新しいコントローラモジュールを、アップグレードキットの一部としてネットアップから入手しておく必要があります。

  新しいコントローラモジュールの PCIe カードに互換性があり、 PCIe カードが新しいコントローラモジュールでサポートされていることを確認する必要があります。

  "NetApp Hardware Universe の略"

- シングルシャーシの HA ペア（両方のコントローラモジュールを同じシャーシに配置 HA ペア）にアップグレードする場合は、新しいコントローラモジュール用の空きスロットが必要です。

  この構成はすべてのシステムでサポートされているわけではありません。ONTAP 9 でサポートされるシングルシャーシ構成のプラットフォームは、 AFF A300 、 FAS8200 、 FAS8300 、 AFF A400 、 AFF80xx です。 FAS8020 、 FAS8060 、 FAS8080 、 FAS9000 ：

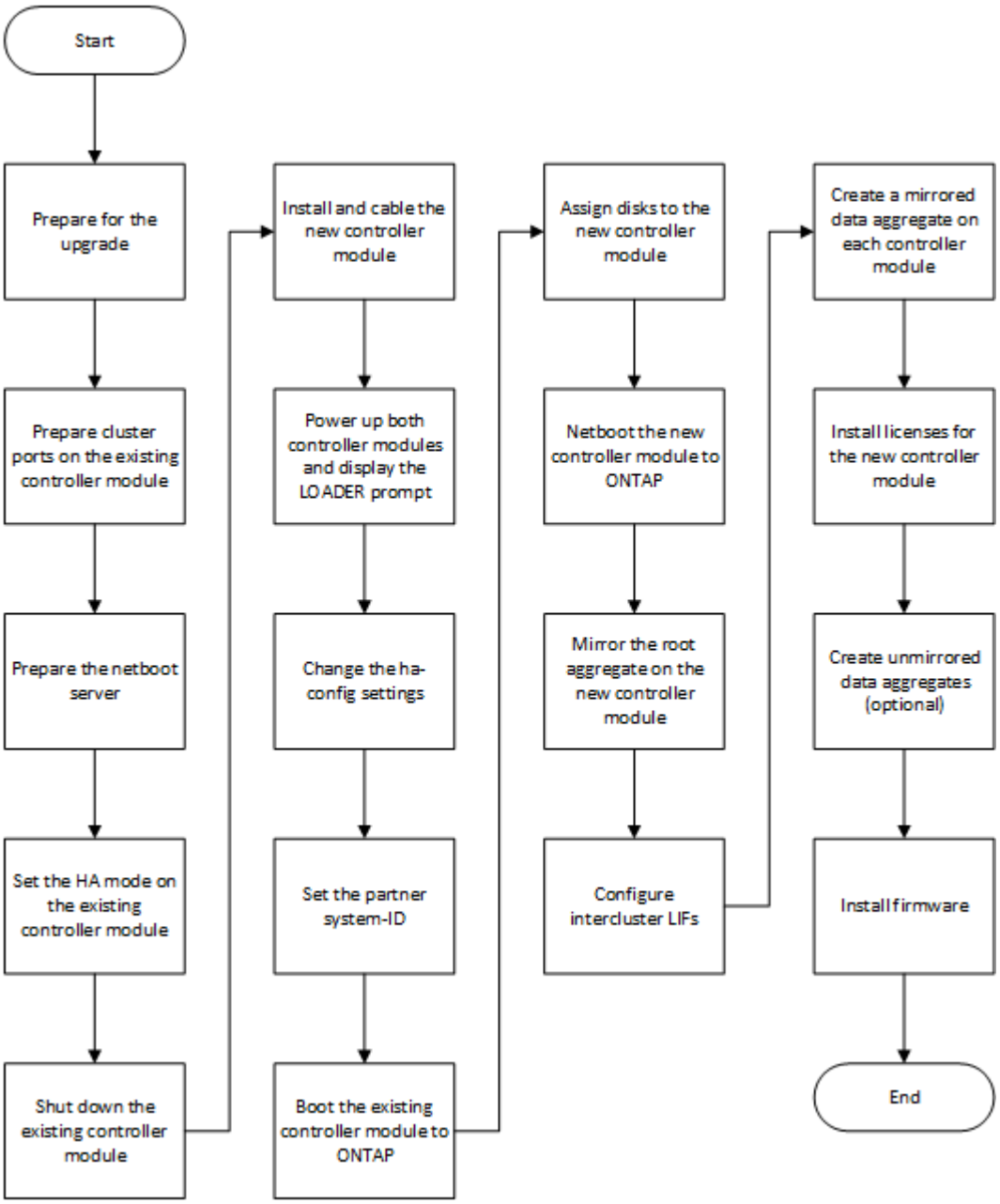
- デュアルシャーシの HA ペア（コントローラモジュールを別々のシャーシに配置 HA ペア）にアップグレードする場合は、新しいコントローラモジュール用のラックスペースとケーブルが必要です。

  この構成はすべてのシステムでサポートされているわけではありません。

- 各コントローラモジュールを、 e0a ポートを介して管理ネットワークに接続する必要があります。システムに e0a ポートがある場合は、管理ポートとして e0M ポートに接続できます。
- これらのタスクは各サイトで実行する必要があります。
- 既存のコントローラモジュールは、 _EXISTN_controller モジュールと呼ばれます。

  この手順の例では、コンソール・プロンプトは「 existing_ctlr>` です。

- 追加するコントローラモジュールは、 _new_controller モジュールと呼ばれます。この手順の例では、コンソールプロンプトは「 new_ctlr>` です。
- このタスクのワークフローは次のとおりです。



アップグレードの準備を行います

HA ペアにアップグレードする前に、システムがすべての要件を満たしていること、および必要な情報がすべて揃っていることを確認する必要があります。

手順

1. 次のコマンドを使用して、新しいコントローラモジュールに割り当て可能な未割り当てのディスクまたはスペアディスクを特定します。
    - storage disk show -container-type spare

- 'storage disk show -container-type unassigned （ storage disk show -container-type unassigned

2. 次の手順を実行します。
   a. 既存のノードのアグリゲートが配置されている場所を特定します。

      「 storage aggregate show

   b. ディスク所有権の自動割り当てを有効にしている場合は無効にします。

      「 storage disk option modify -node node_name -autoassign off

   c. アグリゲートのないディスクの所有権を削除します。

      「 storage disk removeowner _disk_name _ 」を選択します

   d. 新しいノードに必要な数のディスクについて、前の手順を繰り返します。
3. 次の接続用のケーブルがあることを確認します。
   - クラスタ接続

     2 ノードスイッチレスクラスタを作成する場合は、コントローラモジュールを接続するために 2 本のケーブルが必要です。それ以外の場合は、クラスタネットワークスイッチへのコントローラモジュール接続ごとに 2 本、合計 4 本以上のケーブルが必要です。その他のシステム（ 80xx シリーズなど）では、デフォルトで 4 つまたは 6 つのクラスタ接続が設定されています。

   - デュアルシャーシの HA ペアのシステムの場合、 HA インターコネクト接続を確立します
4. コントローラモジュールに使用できるシリアルポートコンソールがあることを確認します。
5. 環境がサイトとシステムの要件を満たしていることを確認します。

   "NetApp Hardware Universe の略"

6. 新しいコントローラモジュールの IP アドレスとその他のネットワークパラメータをすべて収集します。

コントローラモジュールでの設定の消去

MetroCluster 構成で新しいコントローラモジュールを使用する前に、既存の構成をクリアする必要があります。

手順

1. 必要に応じて、ノードを停止してプロンプトを表示し `LOADER`ます。

   「 halt 」

2. `LOADER`プロンプトで、環境変数をデフォルト値に設定します。

   「デフォルト設定」

3. 環境を保存します。

   'aveenv

4. `LOADER`プロンプトでブートメニューを起動します。

   「 boot_ontap menu

5. ブートメニューのプロンプトで、設定を消去します。

   wipeconfig

   確認プロンプトに「 yes 」と応答します。

   ノードがリブートし、もう一度ブートメニューが表示されます。

6. ブートメニューでオプション * 5 * を選択し、システムをメンテナンスモードでブートします。

   確認プロンプトに「 yes 」と応答します。

既存のコントローラモジュールのクラスタポートを準備しています

新しいコントローラモジュールを設置する前に、既存のコントローラモジュールにクラスタポートを設定して、クラスタポートが新しいコントローラモジュールとクラスタ通信できるようにする必要があります。

このタスクについて

（クラスタネットワークスイッチを使用しない） 2 ノードスイッチレスクラスタを作成する場合は、スイッチレスクラスタネットワークモードを有効にする必要があります。

ONTAP のポート、 LIF 、およびネットワーク設定の詳細については、を参照してください "Network Management の略"。

手順

1. ノードのクラスタポートとして使用するポートを決定します。

   プラットフォームのデフォルトのポートロールのリストについては、を参照してください "Hardware Universe"

   クラスタネットワーク接続用のポートに関する情報については、ネットアップサポートサイトでご使用のプラットフォームの _ インストールおよびセットアップ手順 _ を参照してください。

2. 各クラスタポートのロールを特定します。

   「 network port show 」のように表示されます

   次の例では、ポート「 e0a 」、「 e0b 」、「 e0c 」、および「 e0d 」をクラスタポートに変更する必要があります。

```
cluster_A::> network port show

Node: controller_A_1
Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link  MTU    Admin/Oper  Status
--------- ------------ ---------------- ----  ----   ----------
--------
e0M       Default      mgmt_bd_1500     up    1500   auto/1000   healthy
e0a       Default      Default          up    1500   auto/10000  healthy
e0b       Default      Default          up    1500   auto/10000  healthy
e0c       Default      Default          up    1500   auto/10000  healthy
e0d       Default      Default          up    1500   auto/10000  healthy
e0i       Default      Default          down  1500   auto/10     -
e0j       Default      Default          down  1500   auto/10     -
e0k       Default      Default          down  1500   auto/10     -
e0l       Default      Default          down  1500   auto/10     -
e2a       Default      Default          up    1500   auto/10000  healthy
e2b       Default      Default          up    1500   auto/10000  healthy
e4a       Default      Default          up    1500   auto/10000  healthy
e4b       Default      Default          up    1500   auto/10000  healthy
13 entries were displayed.
```

3. ホームポートまたは現在のポートとしてクラスタポートを使用しているデータ LIF について、データポートをホームポートとして使用するように LIF を変更します。

   「 network interface modify 」を参照してください

   次の例は、データ LIF のホームポートをデータポートに変更します。

```
cluster1::> network interface modify -lif datalif1 -vserver vs1 -home
-port e1b
```

4. 変更した各 LIF について、 LIF を新しいホームポートにリバートします。

   「 network interface revert 」の略

   次の例では、 LIF 「 datalif1 」を新しいホームポート「 e1b 」にリバートします。

```
cluster1::> network interface revert -lif datalif1 -vserver vs1
```

5. クラスタポートをメンバーポートとして使用し、 ifgrp をメンバーポートとして使用している VLAN ポートを削除します。

   a. VLAN ポートを削除します。 `+network port vlan delete -node_node-name _ vlan-name_portid -vlandid`

例：

```
network port vlan delete -node node1 -vlan-name e1c-80
```

b. インターフェイスグループから物理ポートを削除します。

「 network port ifgrp remove-port -node-node_name -ifgrp_interface-group-name _ *port_portid* 」の形式で指定します

例：

```
network port ifgrp remove-port -node node1 -ifgrp a1a -port e0d
```

a. ブロードキャストドメインから VLAN ポートとインターフェイスグループポートを削除します。

'network port broadcast-domain remove-ports -ipspace_ipspace -broadcast-domain_domain -name_ports_nodename ： portname 、 nodename ： portname _ 、

b. 必要に応じて、他の物理ポートをメンバーとして使用するようにインターフェイスグループポートを変更します。 `+ifgrp add-port -node -node_name -ifgrp` *`interface -group -name_port_id`*

6. ポートロールが変更されたことを確認します。

「 network port show 」のように表示されます

次の例は、ポート「 e0a 」、「 e0b 」、「 e0c 」、および「 e0d 」がクラスタポートになったことを示しています。

```
Node: controller_A_1
Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link  MTU    Admin/Oper  Status
--------- ------------ ---------------- ----  ----   -----------
--------
e0M       Default      mgmt_bd_1500     up    1500   auto/1000   healthy
e0a       Cluster      Cluster          up    9000   auto/10000  healthy
e0b       Cluster      Cluster          up    9000   auto/10000  healthy
e0c       Cluster      Cluster          up    9000   auto/10000  healthy
e0d       Cluster      Cluster          up    9000   auto/10000  healthy
e0i       Default      Default          down  1500   auto/10 -
e0j       Default      Default          down  1500   auto/10 -
e0k       Default      Default          down  1500   auto/10 -
e0l       Default      Default          down  1500   auto/10 -
e2a       Default      Default          up    1500   auto/10000  healthy
e2b       Default      Default          up    1500   auto/10000  healthy
e4a       Default      Default          up    1500   auto/10000  healthy
e4b       Default      Default          up    1500   auto/10000  healthy
13 entries were displayed.
```

7. クラスタのブロードキャストドメインにポートを追加します。

   'broadcast-domain add-ports -ipspace Cluster-broadcast-domain Cluster-ports_port-id'*port-id*'_*port-id*'_*port-id*'*port-id*'…

   例：

```
broadcast-domain add-ports -ipspace Cluster -broadcast-domain Cluster
-ports cluster1-01:e0a
```

8. システムがスイッチクラスタの一部である場合は、クラスタポートにクラスタ LIF を作成します。「 network interface create 」

   次の例は、ノードのクラスタポートの 1 つにクラスタ LIF を作成します。auto-パラメータ は、リンクローカル IP アドレスを使用するように LIF を設定します。

```
cluster1::> network interface create -vserver Cluster -lif clus1 -role
cluster -home-node node0 -home-port e1a -auto true
```

9. 2 ノードスイッチレスクラスタを作成する場合は、スイッチレスクラスタネットワークモードを有効にします。

   a. いずれかのノードから 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・モードを続行するかどうかを確認するメッセージが表示されたら 'y' と入力しますadvanced モードのプロンプトが表示されます（「 * > 」）。

a. スイッチレスクラスタネットワークモードを有効にします。

   network options switchless-cluster modify -enabled true

b. admin 権限レベルに戻ります。

   「特権管理者」

2 ノードスイッチレスクラスタシステム内の既存ノードのクラスタインターフェイスの作成は、新しいコントローラモジュールでネットブートを使用したクラスタのセットアップが完了したあとに実行されます。

イメージをダウンロードするためのネットブートサーバの準備

ネットブートサーバの準備ができたら、適切な ONTAP のネットブートイメージをネットアップサポートサイトからネットブートサーバにダウンロードして、 IP アドレスをメモする必要があります。

このタスクについて

- 新しいコントローラモジュールを追加する前とあとに、システムから HTTP サーバにアクセスできる必要があります。
- 使用しているプラットフォームと ONTAP のバージョンに必要なシステムファイルをダウンロードするために、ネットアップサポートサイトへのアクセス権が必要です。

  "ネットアップサポートサイト"

- HA ペアの両方のコントローラモジュールで同じバージョンの ONTAP を実行する必要があります。

手順

1. ネットアップサポートサイトのソフトウェアダウンロードセクションから適切な ONTAP ソフトウェアをダウンロードし、「 <ONTAP_version>_image.tgz 」ファイルを Web にアクセスできるディレクトリに保存します。

   「 <ONTAP_version>_image.tgz 」ファイルは、システムのネットブートを実行するために使用します。

2. Web にアクセスできるディレクトリに移動し、必要なファイルが利用可能であることを確認します。

用途	作業

FAS2200 、 FAS2500 、 FAS3200 、 FAS6200 、 FAS/AFF8000 シリーズシステム	ターゲットディレクトリに <ONTAP_version>_image.tgz ファイルの内容を展開します。 tar -zxvf <ONTAP_version>_image.tgz Windows で内容を展開する場合は、 7-Zip または WinRAR を使用してネットブートイメージを展開します。 ディレクトリの一覧に、カーネルファイルを含むネットブートフォルダが含まれるようにします。 netboot/ カーネル
その他すべてのシステム	ディレクトリの一覧に次のファイルが表示されます。 「 <ONTAP_version>_image.tgz 」 ファイルの内容を抽出する必要はありません。

3. 既存のコントローラモジュールの IP アドレスを確認します。

   このアドレスは、この手順の後半では「既存のコントローラの IP アドレス」と呼ばれます。

4. IP アドレスが到達可能であることを確認するために 'ping *ip-address-of -existing controller* を実行します

既存のコントローラモジュールで **HA** モードを設定

既存のコントローラモジュールのモードを設定するには、 storage failover modify コマンドを使用する必要があります。モード設定はコントローラモジュールのリブート後に有効になります。

手順

1. モードを HA に設定します。

   「 storage failover modify -mode ha -node _existing_node_name _ 」を選択します

既存のコントローラモジュールをシャットダウンしています

既存のコントローラモジュールのクリーンシャットダウンを実行して、すべてのデータがディスクに書き込まれたことを確認する必要があります。また、電源装置の接続を解除する必要があります。

このタスクについて

システムコンポーネントを交換する前にシステムのクリーンシャットダウンを実行し、NVRAM または NVMEM 内の書き込み前のデータが失われないようにする必要があります。

手順

1. 既存のコントローラモジュールのプロンプトからノードを停止します。

   halt local-inhibit-takeover true

   手順の停止を続行するかどうかを確認するメッセージが表示されたら、「 y 」と入力し、システムが LOADER プロンプトで停止するまで待ちます。

   80xx システムでは NVMEM の LED はコントローラモジュールのネットワークポートの右側にあり、電池のマークが付いています。

   NVRAM 内に書き込み前のデータがある場合、この LED が点滅します。この LED が halt コマンドの実行後も黄色く点滅する場合は、システムをリブートし、もう一度 halt を実行する必要があります。

2. 接地対策がまだの場合は、自身で適切に実施します。
3. システムと電源装置タイプに適した方法で、電源装置の電源を切り、電源を切断します。

システムの用途	作業
AC 電源装置	電源から電源コードを抜き、電源コードを取り外します。
DC 電源装置	DC 電源の電源を切り、必要に応じて DC ケーブルを取り外します。

新しいコントローラモジュールを設置してケーブル接続します

新しいコントローラモジュールを設置してケーブル接続

新しいコントローラモジュールをシャーシに物理的に設置し、ケーブルを接続する必要があります。

手順

1. I/O 拡張モジュール（ IOXM ）が搭載されているシステムでシングルシャーシの HA ペアを作成する場合は、 IOXM をケーブルを外して取り出す必要があります。

   空になったベイを新しいコントローラモジュールに使用できます。ただし、新しい構成では IOXM によって追加の I/O は提供されません。

2. 新しいコントローラモジュールを物理的に設置し、必要に応じて追加のファンを取り付けます。

コントローラモジュールの追加先	実行する手順

空のベイに追加してシングルシャーシの HA ペアを作成する。システムのプラットフォームは次のいずれか：	a. 新しいコントローラモジュールを取り付ける空のベイに対応するシャーシ背面のブランクプレートを取り外します。 b. コントローラモジュールをシャーシの途中までそっと押し込みます。 コントローラモジュールが自動的にブートしないようにするために、この手順の後半までシャーシに完全に挿入しないでください。
既存の構成がコントローラ IOX モジュール構成である場合、 HA パートナーとは別のシャーシにデュアルシャーシの HA ペアを作成します。 • FAS8200 • 80XX	新しいシステムをラックまたはシステムキャビネットに設置します。

3. 必要に応じて、クラスタネットワーク接続をケーブル接続します。

   a. コントローラモジュールでクラスタ接続用のポートを特定します。

      "AFF A320 システム：設置とセットアップ"

      "AFF A220 / FAS2700 システムの設置とセットアップの手順"

      "AFF A800 システムの設置とセットアップの手順"

      "AFF A300 システム『 Installation and Setup Instructions 』"

      "FAS8200 システム設置とセットアップの手順"

   b. スイッチクラスタを設定する場合は、クラスタネットワークスイッチで使用するポートを特定します。

      を参照してください "『Clustered Data ONTAP Switch Setup Guide for Cisco Switches』"、 "^『NetApp 10G Cluster-Mode Switch Installation Guide』" または "『 NetApp 1G Cluster-Mode Switch Installation Guide 』"（使用しているスイッチによって異なります）。

   c. クラスタポートにケーブルを接続します。

クラスタの種類	作業
2 ノードスイッチレスクラスタ	既存のコントローラモジュールのクラスタポートを、新しいコントローラモジュールの対応するクラスタポートに直接接続します。
スイッチクラスタ	各コントローラのクラスタポートを、手順 b で特定したクラスタネットワークスイッチのポートに接続します

新しいコントローラモジュールの **FC-VI** ポートおよび **HBA** ポートを **FC** スイッチにケーブル接続します

新しいコントローラモジュールの FC-VI ポートと HBA （ホストバスアダプタ）をサイトの FC スイッチにケーブル接続する必要があります。

手順

1. 構成とスイッチモデルの表を使用して、 FC-VI ポートと HBA ポートをケーブル接続します。
   - "FCスイッチのポート割り当て"
   - "2 つのイニシエータポートを使用するシステムのポート割り当て"

新しいコントローラモジュールのクラスタピアリングのケーブル接続

パートナーサイトのクラスタと接続できるように、新しいコントローラモジュールをクラスタピアリングネットワークにケーブル接続する必要があります。

このタスクについて

クラスタピアリングには、各コントローラモジュールの少なくとも 2 つのポートを使用します。

ポートおよびネットワーク接続の推奨される最小帯域幅は 1GbE です。

手順

1. クラスタピアリングに使用する少なくとも 2 つのポートを特定してケーブル接続し、そのポートがパートナークラスタとネットワーク接続されていることを確認します。

両方のコントローラモジュールの電源投入と **LOADER** プロンプトの表示

既存のコントローラモジュールと新しいコントローラモジュールの電源をオンにして LOADER プロンプトを表示します。

手順

構成に対応した手順で、コントローラモジュールの電源をオンにしてブートプロセスを中断します。

コントローラモジュールの場所	作業

同じシャーシ内	1. 新しいコントローラモジュールがベイに * 完全に挿入されていない * ことを確認します。 既存のコントローラモジュールはシャーシから取り外されていないため、ベイに完全に挿入する必要がありますが、新しいコントローラモジュールは完全に挿入しないでください。 2. 電源を接続し、電源装置をオンにして、既存のコントローラモジュールに電力を供給します。 3. Ctrl+C を押して、既存のコントローラモジュールのブートプロセスを中断します 4. 新しいコントローラモジュールをベイにしっかりと押し込みます。 新しいコントローラモジュールが完全に収まると、電力が供給されて自動的にブートします。 5. Ctrl+C を押してブートプロセスを中断します 6. カムハンドルの取り付けネジがある場合は、締めます。 7. ケーブルマネジメントデバイスがある場合は、取り付けます。 8. ケーブルマネジメントデバイスに接続されているケーブルをフックとループストラップでまとめます。
別のシャーシに搭載	1. 既存のコントローラモジュールの電源装置をオンにします。 2. Ctrl+C を押してブートプロセスを中断します 3. 新しいコントローラモジュールについて、上記の手順を繰り返します

各コントローラモジュールには、 LOADER プロンプト（「 LOADER>` 」、「 LOADER-A> 」、または「 LOADER-B>` ）が表示されます。

LOADERプロンプトが表示されない場合は、エラーメッセージを記録してください。システムにブートメニューが表示された場合は、リブートし、もう一度ブートプロセスを中断します。

既存および新規のコントローラモジュールの **ha-config** 設定を変更します

MetroCluster 構成を拡張する場合は、既存のコントローラモジュールと新しいコントローラモジュールの ha-config 設定を更新する必要があります。また、新しいコントローラモジュールのシステム ID も確認する必要があります。

このタスクについて

このタスクは、既存および新規の両方のコントローラモジュールでメンテナンスモードで実行します。

手順

1. 既存のコントローラモジュールの ha-config 設定を変更します。

    a. 既存のコントローラモジュールとシャーシの ha-config 設定を表示します。

「 ha-config show 」

コントローラモジュールが 2 ノード MetroCluster 構成であったため、すべてのコンポーネントの ha-config 設定は「 m cc-2n 」です。

b. 既存のコントローラモジュールの ha-config 設定を「 `m cc:+ha-config modify controller mcc` 」に変更します

c. 既存のシャーシの ha-config 設定を「 mcc 」に変更します。

「 ha-config modify chassis mcc 」

d. 既存のコントローラモジュールのシステム ID を取得します。

「 sysconfig 」を使用できます

システム ID をメモします。新しいコントローラモジュールでパートナー ID を設定するときに必要になります。

a. メンテナンスモードを終了して LOADER プロンプトに戻ります。

「 halt 」

2. ha-config 設定を変更し、新しいコントローラモジュールのシステム ID を取得します。

a. 新しいコントローラモジュールがまだメンテナンスモードになっていない場合は、メンテナンスモードでブートします。

「 boot_ontap maint 」を使用してください

b. 新しいコントローラモジュールの ha-config 設定を「 `m cc` 」に変更します。

「 ha-config modify controller mcc 」

c. 新しいシャーシの ha-config 設定を mcc に変更します。

「 ha-config modify chassis mcc 」

d. 新しいコントローラモジュールのシステム ID を取得します。

「 sysconfig 」を使用できます

システム ID をメモします。パートナー ID を設定し、新しいコントローラモジュールにディスクを割り当てる際に必要になります。

a. メンテナンスモードを終了して LOADER プロンプトに戻ります。

「 halt 」

両方のコントローラモジュールのパートナーシステム **ID** の設定

両方のコントローラモジュールにパートナーシステム ID を設定し、 HA ペアを形成でき

るようにする必要があります。

このタスクについて

このタスクは、両方のコントローラモジュールの LOADER プロンプトで実行します。

手順

1. 既存のコントローラモジュールで、パートナーシステム ID を新しいコントローラモジュールの ID に設定します。

   'setenv partner-sysid_SysID_OF_new_controller_

2. 新しいコントローラモジュールで、パートナーシステム ID を既存のコントローラモジュールの ID に設定します。

   'setenv partner-sysid_SysID_OF_existing_controller_

既存のコントローラモジュールのブート

既存のコントローラモジュールを ONTAP でブートする必要があります。

手順

1. LOADER プロンプトで、既存のコントローラモジュールを ONTAP でブートします。

   「 boot_ontap 」

新しいコントローラモジュールにディスクを割り当てています

ネットブートを使用して新しいコントローラモジュールの設定を完了する前に、モジュールにディスクを割り当てる必要があります。

このタスクについて

既存のアグリゲートに含まれていない十分な数のスペア、未割り当てディスク、または割り当て済みディスクがあることを確認しておく必要があります。

"アップグレードの準備を行います"

以下の手順は、既存のコントローラモジュールで実行します。

手順

1. 新しいコントローラモジュールにルートディスクを割り当てます。

   「 storage disk assign -disk disk_name --sysid_new_controller_SysID__ -force true 」を参照してください

   プラットフォームのモデルがアドバンストドライブパーティショニング（ ADP ）機能を使用している場合は、 -root true パラメータを指定する必要があります。

   「 storage disk assign -disk disk_name -root true -sysid_new_controller_SysID__ -force true 」を参照してください

2. ディスクごとに次のコマンドを入力して、必要なディスクをすべて新しいコントローラモジュールに割り当てます。

   「 storage disk assign -disk disk_name --sysid_new_controller_SysID__ -force true 」を参照してください

3. ディスクの割り当てが正しいことを確認します。

   「 storage disk show -partitionownership * 」のように表示されます

   新しいノードに割り当てるディスクをすべて割り当てておきます。

新しいコントローラモジュールでの **ONTAP** のネットブートとセットアップ

既存の MetroCluster 構成にコントローラモジュールを追加する場合、一連の手順を実行して、新しいコントローラモジュールで ONTAP オペレーティングシステムをネットブート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

- このタスクは、新しいコントローラモジュールの LOADER プロンプトから開始します。
- このタスクにはディスクの初期化も含まれます。

  ディスクの初期化に必要な時間は、ディスクのサイズによって異なります。

- 新しいコントローラモジュールには、 2 本のディスクが自動的に割り当てられます。

  "ディスクおよびアグリゲートの管理"

手順

1. LOADER プロンプトで、 DHCP を使用可能かどうかに基づいて新しいコントローラモジュールの IP アドレスを設定します。

DHCP の状況	入力するコマンド
利用可能	「 * ifconfig e0M -auto * 」と入力します

使用できません	ifconfig e0M -addr= *filer_addr* -mask= *netmask* -gw= *gateway_-dns*= dns_addr_-domain=*dns_domain__ds*`  *`filer_addr`* は、ストレージシステムのIPアドレスです。  *`netmask`* は、ストレージシステムのネットワークマスクです。  *`gateway`* は、ストレージシステムのゲートウェイです。  *`dns_addr`* は、ネットワーク上のネームサーバのIPアドレスです。  *`dns_domain`* は、Domain Name System（DNS；ドメインネームシステム）ドメイン名です。このオプションパラメータを使用する場合は、ネットブートサーバの URL に完全修飾ドメイン名を指定する必要はなく、サーバのホスト名だけを指定します。 インターフェイスによっては、その他のパラメータが必要になる場合もあります。詳細については、 LOADER プロンプトで「 help ifconfig 」コマンドを使用してください。

2. LOADER プロンプトで、新しいノードをネットブートします。

用途	問題コマンド
FAS2200 、 FAS2500 、 FAS3200 、 FAS6200 、 FAS/AFF8000 シリーズシステム	ネットブート <a href="http://web_server_ip/path_to_web-accessible_directory/netboot/kernel`" class="bare">http://<em>web_server_ip/path_to_web-accessible_directory</em>/netboot/kernel`
その他すべてのシステム	`netboot \http://web_server_ip/path_to_web-accessible_directory/<ontap_version>_image.tgz`

「 _path_to_the_web-accessible_directory _ 」は、ダウンロードした「 <ONTAP_version>_image.tgz 」ファイルの場所です。

3. 表示されたメニューから、「 * Install new software first * 」オプションを選択します。

   このメニューオプションを選択すると、新しい ONTAP イメージがブートデバイスにダウンロードおよびインストールされます。

   - HA ペアでの無停止アップグレードではこの手順はサポートされていないというメッセージが表示されたら、「 y 」と入力する必要があります。
   - このプロセスで既存の ONTAP ソフトウェアが新しいソフトウェアに置き換えられることを警告するメッセージが表示されたら、「 y 」と入力する必要があります。
   - image.tgz ファイルの URL を求めるプロンプトが表示されたら、次のパスを入力する必要があります。

     http://*path_to_the_web-accessible_directory*/image.tgz`

4. ソフトウェアの無停止アップグレードまたは交換に関するプロンプトが表示されたら 'y`" と入力します
5. パッケージの URL を指定するように求められたら、 image.tgz ファイルへのパスを入力します。

```
What is the URL for the package? `http://path_to_web-
accessible_directory/image.tgz`
```

6. バックアップ構成のリストアを要求されたら ' バックアップ・リカバリをスキップするには 'n` を入力します

```
*****************************************************************
*             Restore Backup Configuration                      *
*  This procedure only applies to storage controllers that      *
*  are configured as an HA pair.                                *
*                                                               *
*  Choose Yes to restore the "varfs" backup configuration       *
*  from the SSH server.  Refer to the Boot Device Replacement   *
*  guide for more details.                                      *
*  Choose No to skip the backup recovery and return to the      *
*  boot menu.                                                   *
*****************************************************************

Do you want to restore the backup configuration
now? {y|n} `n`
```

7. 今すぐ再起動するように求められたら 'y`" と入力します

```
The node must be rebooted to start using the newly installed software.
Do you want to
reboot now? {y|n} `y`
```

8. 必要に応じて、「 Clean configuration and initialize all disks 」オプションを選択し、ノードのブート後にすべてのディスクを初期化します。

   新しいコントローラモジュールを設定していて、新しいコントローラモジュールのディスクは空であるため、すべてのディスクが消去されるという警告が表示されたら「 y 」と入力します。

   ディスクの初期化に要する時間は、ディスクのサイズと構成によって異なります。

9. ディスクが初期化され、クラスタセットアップウィザードが起動したら、ノードをセットアップします。

   コンソールでノード管理 LIF の情報を入力します。

10. ノードにログインし 'cluster setup を入力し ' クラスタへの参加を求めるプロンプトが表示されたら 'join を入力します

```
Do you want to create a new cluster or join an existing cluster?
{create, join}: `join`
```

11. サイトに応じて、残りのプロンプトに応答します。

    。 "ONTAP をセットアップします" 詳細については、お使いのバージョンの ONTAP のを参照してください。

12. システムが 2 ノードスイッチレスクラスタ構成の場合は、 network interface create コマンドを使用して既存のノードにクラスタインターフェイスを作成し、クラスタポートにクラスタ LIF を作成します。

    次の例は、ノードのクラスタポートの 1 つにクラスタ LIF を作成するコマンドを示しています。auto パラメータは、 LIF でリンクローカル IP アドレスを使用するように設定します。

    ```
    cluster_A::> network interface create -vserver Cluster -lif clus1 -role
    cluster -home-node node_A_1 -home-port e1a -auto true
    ```

13. セットアップが完了したら、ノードが正常に機能しており、クラスタへの参加条件を満たしていることを確認します。

    「 cluster show 」を参照してください

    次の例は、 2 つ目のノード（ cluster1-02 ）をクラスタに追加したあとのクラスタを示しています。

    ```
    cluster_A::> cluster show
    Node                  Health  Eligibility
    --------------------- ------- ------------
    node_A_1              true    true
    node_A_2              true    true
    ```

    cluster setup コマンドを使用すると、クラスタセットアップウィザードにアクセスして、管理 Storage Virtual Machine （ SVM ）またはノード SVM に対して入力した値を変更できます。

14. クラスタインターコネクトとして 4 つのポートが構成されていることを確認します。

    「 network port show 」のように表示されます

    次の例は、 cluster_A の 2 台のコントローラモジュールについての出力です。

```
cluster_A::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
node_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
node_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.
```

新しいコントローラでルートアグリゲートをミラーリング

MetroCluster 構成にコントローラを追加する場合は、ルートアグリゲートをミラーしてデータを保護する必要があります。

このタスクは新しいコントローラモジュールで実行する必要があります。

1. ルートアグリゲートをミラーします。

   「 storage aggregate mirror _aggr_name _ 」のようになります

   次のコマンドでは、 controller_A_1 のルートアグリゲートがミラーされます。

```
controller_A_1::> storage aggregate mirror aggr0_controller_A_1
```

   これによりアグリゲートがミラーされるため、ローカルのプレックスとリモートのプレックスがリモートの MetroCluster サイトに配置されたアグリゲートが作成されます。

専用ポートと共有ポートにクラスタ間LIFを設定する方法について説明します。

専用ポートにクラスタ間 **LIF** を設定します

専用ポートにクラスタ間LIFを設定して、レプリケーショントラフィックに使用できる帯域幅を増やすことができます。

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
       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に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 SVM 「 cluster01 」上のフェイルオーバーグループ「 intercluster01 」に割り当てます。

   ```
   cluster01::> network interface failover-groups create -vserver
   cluster01 -failover-group
   intercluster01 -targets
   cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
   ```

4. フェイルオーバーグループが作成されたことを確認します。

   「 network interface failover-groups show 」と表示されます

   コマンド構文全体については、マニュアルページを参照してください。

```
cluster01::> network interface failover-groups show
                                  Failover
Vserver          Group            Targets
---------------- ----------------
--------------------------------------------
Cluster
                 Cluster
                                  cluster01-01:e0a, cluster01-
01:e0b,
                                  cluster01-02:e0a, cluster01-02:e0b
cluster01
                 Default
                                  cluster01-01:e0c, cluster01-
01:e0d,
                                  cluster01-02:e0c, cluster01-
02:e0d,
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
                 intercluster01
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
```

5. システム SVM にクラスタ間 LIF を作成して、フェイルオーバーグループに割り当てます。

ONTAP バージョン	コマンドを実行します
9.6 以降	`network interface create -vserver <system_SVM> -lif <LIF_name> -service-policy default-intercluster -home -node <node> -home-port <port> -address <port_IP> -netmask <netmask> -failover-group <failover_group>`
9.5 以前	`network interface create -vserver system_SVM -lif <LIF_name> -role intercluster -home-node <node> -home -port <port> -address <port_IP> -netmask <netmask> -failover-group <failover_group>`

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： *
「 network interface show -service -policy default -intercluster 」のように表示されます
* ONTAP 9.5 以前： *
「 network interface show -role intercluster 」の略

コマンド構文全体については、マニュアルページを参照してください。

```
cluster01::> network interface show -service-policy default-
intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01
e0e     true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02
e0f     true
```

7. クラスタ間 LIF が冗長構成になっていることを確認します。

* ONTAP 9.6 以降： *

「 network interface show -service -policy default -intercluster-failover 」のように入力します
* ONTAP 9.5 以前： *
「 network interface show -role intercluster-failover 」の略

コマンド構文全体については、マニュアルページを参照してください。

次の例は、 SVM 「 e0e 」ポート上のクラスタ間 LIF 「 cluster01_icl01 」と「 cluster01_icl02 」が「 e0f 」ポートにフェイルオーバーされることを示しています。

```
cluster01::> network interface show -service-policy default-
intercluster –failover
         Logical         Home                  Failover
Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- ---------------
--------
cluster01
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

共有データポートにクラスタ間 **LIF** を設定します

データネットワークと共有するポートにクラスタ間LIFを設定することで、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： *
`network interface create -vserver <system_SVM> -lif <LIF_name> -service -policy default-intercluster -home-node <node> -home-port <port> -address <port_IP> -netmask <netmask>`
* ONTAP 9.5 以前： *
`network interface create -vserver <system_SVM> -lif <LIF_name> -role intercluster -home-node <node> -home-port <port> -address <port_IP> -netmask <netmask>`

コマンド構文全体については、マニュアルページを参照してください。

次の例は、クラスタ間 LIF 「 cluster01_icl01 」と「 cluster01_icl02 」を作成します。

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. クラスタ間 LIF が作成されたことを確認します。

* ONTAP 9.6 以降： *
「 network interface show -service -policy default -intercluster 」のように表示されます
* ONTAP 9.5 以前： *
「 network interface show -role intercluster 」の略

コマンド構文全体については、マニュアルページを参照してください。

```
cluster01::> network interface show -service-policy default-
intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01
e0c     true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02
e0c     true
```

4. クラスタ間 LIF が冗長構成になっていることを確認します。

* ONTAP 9.6 以降： *

「 network interface show – service-policy default-intercluster-failover 」と表示されます
* ONTAP 9.5 以前： *
「 network interface show -role intercluster-failover 」の略

コマンド構文全体については、マニュアルページを参照してください。

次の例は、「 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
```

各**MetroCluster FC**ノードでミラーリングされたデータ 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。
- システムに複数のドライブ タイプがある場合（異機種混在ストレージ）、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。
- 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。

> 最適なストレージ パフォーマンスと可用性を確保するには、ミラー化されたアグリゲートに少なくとも 20% の空き領域を確保することをお勧めします。ミラーリングされていないアグリゲートの場合、推奨値は 10% ですが、追加の 10% のスペースは、増分変更を吸収するためにファイル システムによって使用できます。増分変更により、ONTAPのcopy-on-write Snapshotベースのアーキテクチャにより、ミラー化されたアグリゲートのスペース使用率が増加します。これらのベスト プラクティスに従わないと、パフォーマンスに悪影響が出る可能性があります。

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ている場合は、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ていることを確認するには、 `-node` パラメータを使用するか、そのノードが所有するドライブを指定します。

   次のオプションを指定できます。

   - アグリゲートのホームノード（通常運用時にアグリゲートを所有するノード）
   - アグリゲートに追加するドライブのリスト
   - 追加するドライブ数

     > 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
   - RPM の異なるドライブが許可されるかどうか

     これらのオプションの詳細については 'storage aggregate create のマニュアルページを参照してくだ

さい

次のコマンドでは、 10 本のディスクを含むミラーアグリゲートが作成されます。

```
cluster_A::> storage aggregate create aggr1_node_A_1 -diskcount 10 -node
node_A_1 -mirror true
[Job 15] Job is queued: Create aggr1_node_A_1.
[Job 15] The job is starting.
[Job 15] Job succeeded: DONE
```

3. 新しいアグリゲートの RAID グループとドライブを確認します。

   ```
   storage aggregate show-status -aggregate <aggregate-name>
   ```

新しいコントローラモジュール用のライセンスをインストールしています

標準（ノードロック）ライセンスが必要な ONTAP サービスがある場合は、新しいコントローラモジュールにライセンスを追加する必要があります。標準ライセンスを使用する機能では、クラスタ内の各ノードにその機能用のキーが必要です。

ライセンスの詳細については、ネットアップサポートサイトの技術情報アーティクル 3013749 ：「 Data ONTAP 8.2 Licensing Overview and References 」と「 *System Administration Reference*」 を参照してください。

手順

1. 必要に応じて、ネットアップサポートサイトの「ソフトウェアライセンス」の下の「 My Support 」セクションで新しいノードのライセンスキーを取得します。

   ライセンスの置換の詳細については、Knowledge Baseの記事を参照してください "マザーボードの交換後プロセスを実行して、AFF / FASシステムのライセンスを更新"

2. 問題各ライセンスキーをインストールするには、次のコマンドを使用します。

   'system license add -license-code_license_key_`

   `license_key` は 28 桁の長さである。

3. 必要な標準（ノードロック）ライセンスごとにこの手順を繰り返します。

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 _Installation と Setup_documentation の手順を使用してください。

   "ONTAPハードウェアシステムのドキュメント"

2. 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>
   ```

3. アグリゲートを作成します。

   「 storage aggregate create 」

   クラスタ管理インターフェイスでクラスタにログインした場合、クラスタ内の任意のノードにアグリゲートを作成できます。アグリゲートが特定のノード上に作成されていることを確認するには、「 -node 」パラメータを使用するか、そのノードが所有するドライブを指定します。

   ミラーされていないシェルフのドライブだけがアグリゲートに追加されていることを確認します。

   次のオプションを指定できます。

   - アグリゲートのホームノード（通常運用時にアグリゲートを所有するノード）
   - アグリゲートに追加するドライブのリスト
   - 追加するドライブ数
   - アグリゲートに使用するチェックサム形式
   - 使用するドライブのタイプ
   - 使用するドライブのサイズ
   - 使用するドライブの速度
   - アグリゲート上の RAID グループの RAID タイプ
   - RAID グループに含めることができるドライブの最大数

◦ RPM の異なるドライブが許可されるかどうか

これらのオプションの詳細については 'storage aggregate create のマニュアルページを参照してください

次のコマンドでは、 10 本のディスクを含むミラーされていないアグリゲートが作成さ

```
controller_A_1::> storage aggregate create aggr1_controller_A_1
-diskcount 10 -node controller_A_1
[Job 15] Job is queued: Create aggr1_controller_A_1.
[Job 15] The job is starting.
[Job 15] Job succeeded: DONE
```

+

コマンドのパラメータを使用して、アグリゲートに使用するディスクを指定することもできます `-disklist`。

4. 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>
```

関連情報

"ディスクおよびアグリゲートの管理"

コントローラモジュール追加後のファームウェアのインストール

コントローラモジュールを追加したら、コントローラモジュールが ONTAP で正しく機能するように、新しいコントローラモジュールに最新のファームウェアをインストールする必要があります。

手順

1. ご使用のシステムの最新バージョンのファームウェアをダウンロードし、手順に従って新しいファームウェアをダウンロードしてインストールします。

"ネットアップのダウンロード：システムファームウェアおよび診断"

新しいコントローラで **MetroCluster** 設定を更新しています

MetroCluster 構成を 2 ノード構成から 4 ノード構成に拡張する場合は、 構成を更新する必要があります。

手順

1. MetroCluster 構成を更新します。

a. advanced 権限モードに切り替えます。 + 「 set -privilege advanced 」

b. MetroCluster 構成を更新します。 + MetroCluster configure -refresh true -allow-with-one-aggregate true

次のコマンドを実行すると、 controller_A_1 を含む DR グループのすべてのノードの MetroCluster 構成が更新されます。

```
controller_A_1::*> metrocluster configure -refresh true -allow-with-one
-aggregate true

[Job 726] Job succeeded: Configure is successful.
```

a. admin 権限モードに戻ります。

「特権管理者」

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
                                                          Speed (Mbps)
Node   Port      IPspace   Broadcast Domain Link   MTU    Admin/Oper
------ --------- --------- ---------------- ----- ------- ------------
controller_A_1
       e0a       Cluster   Cluster          up     9000  auto/1000
       e0b       Cluster   Cluster          up     9000  auto/1000
       e0c       Default   Default          up     1500  auto/1000
       e0d       Default   Default          up     1500  auto/1000
       e0e       Default   Default          up     1500  auto/1000
       e0f       Default   Default          up     1500  auto/1000
       e0g       Default   Default          up     1500  auto/1000
controller_A_2
       e0a       Cluster   Cluster          up     9000  auto/1000
       e0b       Cluster   Cluster          up     9000  auto/1000
       e0c       Default   Default          up     1500  auto/1000
       e0d       Default   Default          up     1500  auto/1000
       e0e       Default   Default          up     1500  auto/1000
       e0f       Default   Default          up     1500  auto/1000
       e0g       Default   Default          up     1500  auto/1000
14 entries were displayed.
```

3. MetroCluster 構成の両方のサイトから MetroCluster 構成を確認します。

a. サイト A から構成を確認します。

「 MetroCluster show 」

```
cluster_A::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
Remote: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
```

b. サイト B から構成を確認します。

「 MetroCluster show 」

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
Remote: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
```

c. DR 関係が正しく作成されたことを確認します。

MetroCluster node show -fields dr-cluster 、 dr-auxiliary 、 node-object-limit 、 automatic-suso 、 ha-partner 、 dr-partner

```
metrocluster node show -fields dr-cluster,dr-auxiliary,node-object-
limit,automatic-uso,ha-partner,dr-partner
dr-group-id cluster     node    ha-partner dr-cluster  dr-partner   dr-
auxiliary  node-object-limit automatic-uso
----------- ---------   ----    ---------- ----------  ----------
------------  ----------------- -------------
2           cluster_A   node_A_1 node_A_2    cluster_B  node_B_1
node_B_2      on                true
2           cluster_A   node_A_2 node_A_1    cluster_B  node_B_2
node_B_1      on                true
2           cluster_B   node_B_1 node_B_2    cluster_A  node_A_1
node_A_2      on                true
2           cluster_B   node_B_2 node_B_1    cluster_A  node_A_2
node_A_1      on                true
4 entries were displayed.
```

両方のコントローラモジュールでのストレージフェイルオーバーの有効化およびクラスタ **HA** の有効化

MetroCluster 構成に新しいコントローラモジュールを追加したら、両方のコントローラモジュールでストレージフェイルオーバーを有効にし、各モジュールでクラスタ HA を有効にする必要があります。

作業を開始する前に

MetroCluster の設定は ' MetroCluster configure -refresh true コマンドを使用して事前に更新されている必要があります

このタスクについて

このタスクは MetroCluster サイトごとに実行する必要があります。

手順

1. ストレージフェイルオーバーを有効にします。

   「 storage failover modify -enabled true -node _existing-node-name _ 」を選択します

   1 つのコマンドで両方のコントローラモジュールのストレージフェイルオーバーが有効になります。

2. ストレージフェイルオーバーが有効になっていることを確認します。

   「 storage failover show 」をクリックします

   次のような出力が表示されます。

```
Node            Partner         Possible State Description
--------------- --------------- -------- ----------------------
old-ctlr         new-ctlr       true      Connected to new-ctlr
new-ctlr         old-ctlr       true      Connected to old-ctlr
2 entries were displayed.
```

3. クラスタ HA を有効にします。

   cluster ha modify -configured true

   クラスタに含まれるノードが 2 つだけで、クラスタのハイアベイラビリティ（ HA ）がストレージフェイルオーバーによって提供される HA と異なる場合は、クラスタの HA を構成する必要があります。

SVM を再起動しています

MetroCluster 構成を拡張したら、 SVM を再起動する必要があります。

手順

1. 再起動が必要な SVM を特定します。

   MetroCluster vserver show

   このコマンドは、両方の MetroCluster クラスタの SVM を表示します。

2. 最初のクラスタで SVM を再起動します。
   a. advanced 権限モードに切り替えて、プロンプトが表示されたら「 * y * 」を押します。

      「 advanced 」の権限が必要です

   b. SVM を再起動します。

      「 vserver start -vserver *svm_name*-force true 」を指定します

   c. admin 権限モードに戻ります。

      「特権管理者」

3. パートナークラスタで同じ手順を繰り返します。
4. SVM が健全な状態であることを確認します。

   MetroCluster vserver show

4 ノード MetroCluster FC 構成を 8 ノード構成に拡張

4 ノード MetroCluster FC 構成から 8 ノード構成への拡張

4 ノード MetroCluster FC 構成を 8 ノード MetroCluster FC 構成に拡張するには、各クラスタに 2 台のコントローラを追加して各 MetroCluster サイトに 2 つ目の HA ペアを形成してから、 MetroCluster FC の構成処理を実行します。

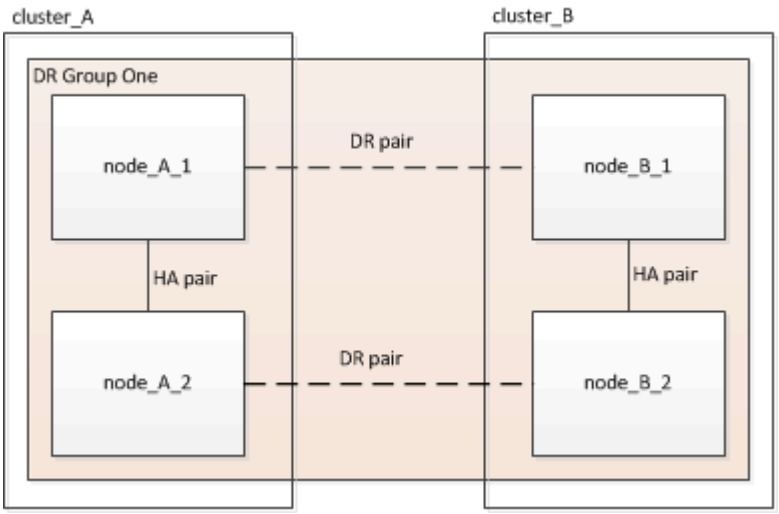
このタスクについて

- ノードが MetroCluster FC 構成で ONTAP 9 を実行している必要があります。

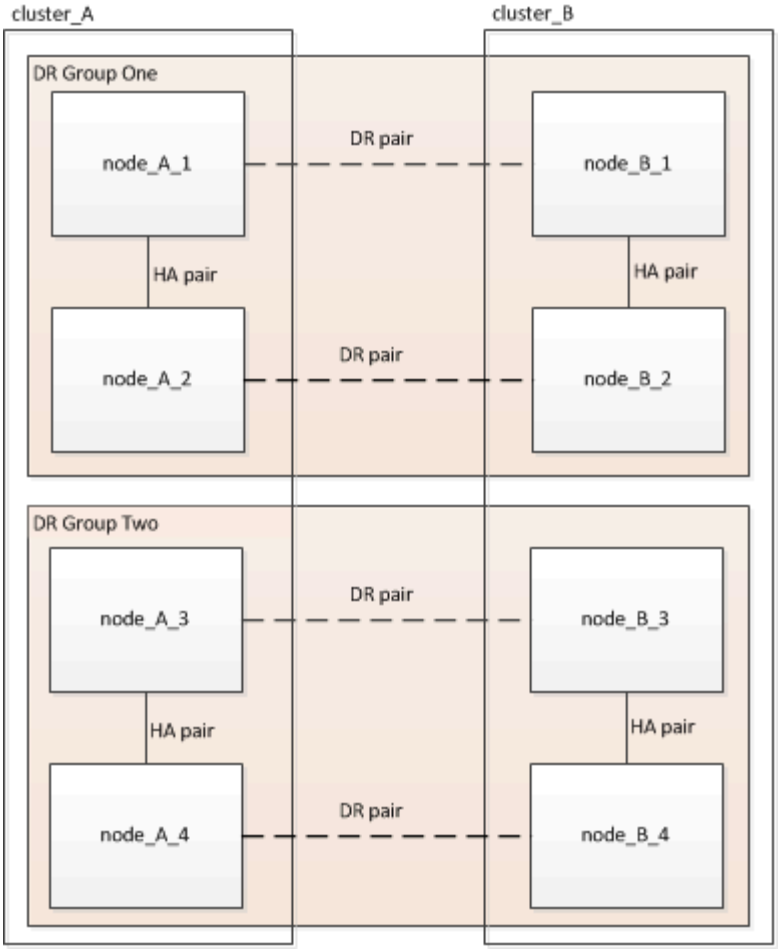
  この手順は、以前のバージョンの ONTAP または MetroCluster IP 構成ではサポートされていません。

- 既存の MetroCluster FC 構成が健全な状態である必要があります。
- 追加する機器がサポートされており、に記載されたすべての要件を満たしている必要があります "ファブリック接続 MetroCluster のインストールと設定"
- 新しいコントローラとブリッジに対応する FC スイッチポートが必要です。
- 管理パスワードと FTP サーバまたは SCP サーバへのアクセスが必要です。
- この手順は、 MetroCluster FC 構成にのみ適用されます。
- この手順はシステムを停止せずに実行でき、ディスクが初期化されている場合は約 1 日で完了します（ラックとスタックは除く）。

この手順を実行する前の MetroCluster FC 構成は 4 つのノードで構成されており、各サイトに HA ペアが 1 つあります。



この手順の完了後、 MetroCluster FC 構成の各サイトには 2 つの HA ペアが含まれます。



両方のサイトを同じように拡張する必要があります。MetroCluster FC 構成では、ノードの数を奇数にすることはできません。

2つ目の**DR**グループを追加する際にサポートされるプラットフォームの組み合わせ

次の表に、8ノードMetroCluster FC構成でサポートされるプラットフォームの組み合わせを示します。

- MetroCluster構成内のすべてのノードで同じバージョンのONTAPが実行されている必要があります。たとえば、8ノード構成の場合は、8つのすべてのノードで同じバージョンのONTAPを実行する必要があります。
- この表の組み合わせは、通常または永続的な8ノード構成にのみ該当します。
- 移行手順または更新手順を使用している場合、この表のプラットフォームの組み合わせは適用*されません*。
- 1つのDRグループ内のすべてのノードのタイプと構成が同じである必要があります。

サポートされる**AFF**と**FAS MetroCluster FC**の拡張の組み合わせ

次の表に、MetroCluster FC構成でAFFシステムまたはFASシステムを拡張する場合にサポートされるプラットフォームの組み合わせを示します。

FAS and AFF		Eight-node DR group 2							
		FAS8200	AFF A300	FAS8300	AFF A400	FAS9000	AFF A700	FAS9500	AFF A900
Eight-node DR group 1	FAS8200								
	AFF A300								
	FAS8300								
	AFF A400								
	FAS9000								
	AFF A700								
	FAS9500								
	AFF A900								

サポートされる**ASA MetroCluster FC**拡張の組み合わせ

次の表に、MetroCluster FC構成でASAシステムを拡張する場合にサポートされるプラットフォームの組み合わせを示します。

8ノードの**DR**グループ**1**	**8**ノードの**DR**グループ**2**	サポートの有無
ASA A400	ASA A400	はい。
	ASA A900	いいえ
ASA A900	ASA A400	いいえ
	ASA A900	はい。

コンソールログを有効にする

このタスクを実行する前に、デバイスでコンソールログを有効にしてください。

NetAppでは、使用しているデバイスでコンソールロギングをイネーブルにし、この手順を実行する際に次のアクションを実行することを強く推奨します。

- メンテナンス中はAutoSupportを有効のままにします。
- メンテナンスの前後にメンテナンスAutoSupportメッセージをトリガーして、メンテナンスアクティビティ中にケースの作成を無効にします。

  ナレッジベースの記事を参照してください "スケジュールされたメンテナンス時間中にケースの自動作成を停止する方法"。

- 任意のCLIセッションのセッションロギングをイネーブルにします。セッションログを有効にする方法については、ナレッジベースの記事の「セッション出力のログ」セクションを参照してください "ONTAPシステムへの接続を最適化するためのPuTTYの設定方法"。

新しいケーブルレイアウトの決定

新しいコントローラモジュールおよび新しいディスクシェルフと既存の FC スイッチとのケーブル接続を決定する必要があります。

このタスクについて

このタスクは MetroCluster サイトごとに実行する必要があります。

手順

1. の手順を使用します "ファブリック接続 MetroCluster のインストールと設定" 8 ノード MetroCluster 構成のポート用途を使用して、スイッチタイプに対応したケーブルレイアウトを作成します。

   リファレンス構成ファイル（ RCF ）を使用できるようにするためには、 FC スイッチポートの用途が手順に記載されている用途と同じである必要があります。

   RCF ファイルを使用できるようにケーブル接続できない場合は、の手順に従ってシステムを手動で設定する必要があります "ファブリック接続 MetroCluster のインストールと設定"。RCF ファイルを使用できないケーブル接続の場合は、この手順を使用しないでください。

新しい機器をラックに設置

新しいノードの機器をラックに設置する必要があります。

手順

1. の手順を使用します "ファブリック接続 MetroCluster のインストールと設定" 新しいストレージシステム、ディスクシェルフ、および FC-to-SAS ブリッジをラックに設置するため。

MetroCluster 構成の健全性の確認

MetroCluster 構成の健全性をチェックして、正常に動作することを確認する必要があります。

手順

1. 各クラスタで MetroCluster が設定されており、通常モードであることを確認します。

   「 MetroCluster show 」

```
cluster_A::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-disaster
Remote: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-disaster
```

2. 各ノードでミラーリングが有効であることを確認します。

   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_1       configured     enabled   normal
2 entries were displayed.
```

3. 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 」のようになります

```
cluster_A::> metrocluster check run

Last Checked On: 10/1/2014 16:03:37

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
4 entries were displayed.

Command completed. Use the "metrocluster check show -instance" command
or sub-commands in "metrocluster check" directory for detailed results.
To check if the nodes are ready to do a switchover or switchback
operation, run "metrocluster switchover -simulate" or "metrocluster
switchback -simulate", respectively.
```

4. ヘルスアラートがないことを確認します。

「 system health alert show 」というメッセージが表示されます

5. スイッチオーバー処理をシミュレートします。

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。 + 「 set -privilege advanced 」

advanced モードで続けるかどうかを尋ねられたら、「 * y * 」と入力して応答する必要があります。 advanced モードのプロンプトが表示されます（ * > ）。

b. simulate パラメータを指定して、スイッチオーバー処理を実行します。 + MetroCluster switchover

-simulate `

c. admin 権限レベルに戻ります。 `+set -privilege admin`

Config Advisor での MetroCluster 構成エラーの確認

一般的な構成エラーの有無を確認する Config Advisor ツールをネットアップサポートサイトからダウンロードできます。

このタスクについて

Config Advisor は、構成の検証や健常性のチェックに使用できるツールです。データ収集とシステム分析のために、セキュアなサイトにもセキュアでないサイトにも導入できます。

Config Advisor のサポートには制限があり、オンラインでしか使用できません。

手順

1. Config Advisor のダウンロードページにアクセスし、ツールをダウンロードします。

   "ネットアップのダウンロード： Config Advisor"

2. Config Advisor を実行し、ツールの出力を確認して、問題が検出された場合は出力に表示される推奨事項に従って対処します。

カスタム AutoSupport メッセージの送信 - MetroCluster 構成へのノードの追加前

メンテナンスが進行中であることをネットアップテクニカルサポートに通知するには、AutoSupport に問題メッセージを送信する必要があります。システム停止が発生したとみなしてテクニカルサポートがケースをオープンしないように、メンテナンスが進行中であることを通知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 サイトごとに実行する必要があります。

手順

1. Site_A のクラスタにログインします
2. メンテナンスの開始を通知する AutoSupport メッセージを起動します。

   「 system node AutoSupport invoke -node * -type all -message MAINT= *maintenance-window-in-hours* 」というメッセージが表示されます

   「 maintenance-window-in-hours 」パラメータは、メンテナンス時間の長さを指定します。最大値は 72 時間です。この時間が経過問題する前にメンテナンスが完了した場合は、次のコマンドを使用して、メンテナンス期間が終了したことを通知できます。

   「 system node AutoSupport invoke -node * -type all -message MAINT= end 」というメッセージが表示されます

3. 同じ手順をパートナーサイトでも実行します。

新しいノードのスイッチファブリックにケーブルを再接続してゾーニングします

ファブリックから既存の **DR** グループを切断します

ファブリック内の FC スイッチから既存のコントローラモジュールを切断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 サイトごとに実行する必要があります。

手順

1. 既存のコントローラモジュールをメンテナンス中のスイッチファブリックに接続している HBA ポートを無効にします。

   「 storage port disable -node -node-name 」 - ポート番号 _

2. ローカルの FC スイッチで、既存のコントローラモジュールの HBA 、 FC-VI 、および ATTO ブリッジ用ポートからケーブルを外します。

   ケーブルを再接続するときに簡単に識別できるように、ケーブルにラベルを付けておく必要があります。ISL ポートのケーブルだけを接続したままにしておきます。

スイッチにケーブルを再接続して再設定します

RCF ファイルを適用して、新しいノードに対応するようにゾーニングを再設定する必要があります。

RCFファイルを使用してスイッチを設定できない場合は、スイッチを手動で設定する必要があります。を参照してください

- "Brocade FC スイッチを手動で設定"
- "Cisco FC スイッチを手動で設定"

手順

1. 使用している構成用の RCF ファイルを探します。

   使用しているスイッチモデルに対応した 8 ノード構成用の RCF ファイルを使用する必要があります。

2. ダウンロードページの指示に従って RCF ファイルを適用し、必要に応じて ISL 設定を調整します。
3. スイッチの設定が保存されていることを確認します。
4. FC スイッチをリブートします。
5. 作成したケーブルレイアウトを使用して、既存の FC-to-SAS ブリッジと新しい FC-to-SAS ブリッジの両方を FC スイッチにケーブル接続します。

   FC スイッチポートの用途が、に記載されている 8 ノード MetroCluster の用途と同じである必要があります "ファブリック接続 MetroCluster のインストールと設定" リファレンス構成ファイル（ RCF ）を使用できるようにするためです。

6. スイッチに対応したコマンドを使用して、ポートがオンラインであることを確認します。

スイッチベンダー	コマンドを実行します
Brocade	SwitchShow
シスコ	インターフェイスの概要を表示します

7. の手順を使用します "ファブリック接続 MetroCluster のインストールと設定" 作成したケーブルレイアウトを使用して、既存のコントローラの FC-VI ポートと新しいコントローラのケーブルを接続します。

   FC スイッチポートの用途が、に記載されている 8 ノード MetroCluster の用途と同じである必要があります "ファブリック接続 MetroCluster のインストールと設定" リファレンス構成ファイル（ RCF ）を使用できるようにするためです。

8. 既存のノードから、 FC-VI ポートがオンラインであることを確認します。

   MetroCluster インターコネクト・アダプタ・ショー

   MetroCluster interconnect mirror show

9. 現在のコントローラの HBA ポートを新しいコントローラにケーブル接続します。
10. 既存のコントローラモジュールで、メンテナンス中のスイッチファブリックに接続されているポートを有効にします。

    「 storage port enable -NODE-NODE-NAME_-PORT_PORT_ID_` 」

11. 新しいコントローラを起動し、メンテナンスモードでブートします。

    「 boot_ontap maint 」を使用してください

12. 新しい DR グループが使用するストレージのみが新しいコントローラモジュールに認識されることを確認します。

    他の DR グループが使用するストレージが認識されないようにしてください。

13. このプロセスの最初に戻り、 2 つ目のスイッチファブリックを再ケーブル接続します。

新しいコントローラで **ONTAP** を設定します

コントローラモジュールでの設定の消去

MetroCluster 構成で新しいコントローラモジュールを使用する前に、既存の構成をクリアする必要があります。

手順

1. 必要に応じて、ノードを停止してプロンプトを表示し `LOADER`ます。

   「 halt 」

2. `LOADER`プロンプトで、環境変数をデフォルト値に設定します。

   「デフォルト設定」

3. 環境を保存します。

   'aveenv

4. `LOADER`プロンプトでブートメニューを起動します。

   「 boot_ontap menu

5. ブートメニューのプロンプトで、設定を消去します。

   wipeconfig

   確認プロンプトに「 yes 」と応答します。

   ノードがリブートし、もう一度ブートメニューが表示されます。

6. ブートメニューでオプション * 5 * を選択し、システムをメンテナンスモードでブートします。

   確認プロンプトに「 yes 」と応答します。

AFF システムでディスク所有権を割り当てます

アグリゲートがミラーされた AFF システムを使用する構成で、ノードにディスク（ SSD ）が正しく割り当てられていない場合は、各シェルフの半分のディスクを 1 つのローカルノードに割り当て、残りの半分を対応する HA パートナーノードに割り当てる必要があります。構成内の各ノードのローカルディスクプールとリモートディスクプールでディスク数が同じになるように設定する必要があります。

このタスクについて

ストレージコントローラがメンテナンスモードになっている必要があります。

これは、アグリゲートがミラーされていない構成、アクティブ / パッシブ構成、ローカルプールとリモートプールのディスク数が異なる構成には該当しません。

このタスクは、工場出荷時にディスクが正しく割り当てられている場合は必要ありません。

> プール 0 にはディスクを所有するストレージシステムと同じサイトにあるディスクを割り当て、プール 1 にはディスクを所有するストレージシステムに対してリモートなディスクを割り当てます。

手順

1. システムをブートしていない場合は、メンテナンスモードでブートします。
2. 最初のサイト（サイト A ）にあるノードにディスクを割り当てます。

   各プールに同じ数のディスクを割り当てる必要があります。

a. 最初のノードで、各シェルフの半分のディスクをプール 0 に、残りの半分を HA パートナーのプール 0 に割り当てます。 +Disk assign-disk_disk-name -*p_pool*-n_number-of-disks_

ストレージコントローラ Controller_A_1 にシェルフが 4 台あり、各シェルフに SSD が 8 本ある場合は、次のコマンドを問題に設定します。

```
*> disk assign -shelf FC_switch_A_1:1-4.shelf1 -p 0 -n 4
*> disk assign -shelf FC_switch_A_1:1-4.shelf2 -p 0 -n 4

*> disk assign -shelf FC_switch_B_1:1-4.shelf1 -p 1 -n 4
*> disk assign -shelf FC_switch_B_1:1-4.shelf2 -p 1 -n 4
```

b. ローカルサイトの 2 番目のノードに対して処理を繰り返し、各シェルフの半分のディスクをプール 1 に、残りの半分を HA パートナーのプール 1 に割り当てます。 +Disk assign-disk_disk_name *p_pool*

ストレージコントローラ Controller_A_1 にシェルフが 4 台あり、各シェルフに SSD が 8 本ある場合は、次のコマンドを問題に設定します。

```
*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1 -n 4

*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1 -n 4
```

3. 2 番目のサイト（サイト B ）にあるノードにディスクを割り当てます。

各プールに同じ数のディスクを割り当てる必要があります。

a. リモートサイトの最初のノードで、各シェルフの半分のディスクをプール 0 に、残りの半分を HA パートナーのプール 0 に割り当てます。 +Disk assign -disk disk_name *p_pool*

ストレージコントローラ Controller_B_1 にシェルフが 4 台あり、各シェルフに SSD が 8 本ある場合は、次のコマンドを問題で実行します。

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf1 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-5.shelf2 -p 0 -n 4

*> disk assign -shelf FC_switch_A_1:1-5.shelf1 -p 1 -n 4
*> disk assign -shelf FC_switch_A_1:1-5.shelf2 -p 1 -n 4
```

b. リモートサイトの 2 番目のノードに対して処理を繰り返し、各シェルフの半分のディスクをプール 1 に、残りの半分を HA パートナーのプール 1 に割り当てます。

「 disk assign -disk disk-name-p_pool_` 」

ストレージコントローラ Controller_B_2 にシェルフが 4 台あり、各シェルフに SSD が 8 本ある場合は、次のコマンドを問題に設定します。

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf3 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-5.shelf4 -p 0 -n 4

*> disk assign -shelf FC_switch_A_1:1-5.shelf3 -p 1 -n 4
*> disk assign -shelf FC_switch_A_1:1-5.shelf4 -p 1 -n 4
```

4. ディスクの割り当てを確認します。

   「 storage show disk 」を参照してください

5. メンテナンスモードを終了します。

   「 halt 」

6. ブートメニューを表示します。

   「 boot_ontap menu

7. 各ノードで、オプション * 4 * を選択してすべてのディスクを初期化します。

AFF 以外のシステムでディスク所有権を割り当てています

MetroCluster ノードにディスクが正しく割り当てられていない場合、または構成で DS460C ディスクシェルフを使用している場合は、 MetroCluster 構成内の各ノードにシェルフ単位でディスクを割り当てる必要があります。構成内の各ノードのローカルディスクプールとリモートディスクプールでディスク数が同じになるように設定します。

このタスクについて

ストレージコントローラがメンテナンスモードになっている必要があります。

構成に DS460C ディスクシェルフが含まれている場合を除き、工場出荷時の状態でディスクが正しく割り当てられていればこのタスクは必要ありません。

プール 0 には、ディスクを所有するストレージシステムと同じサイトにあるディスクを割り当てます。

プール 1 には、ディスクを所有するストレージシステムに対してリモートなディスクを割り当てます。

構成に DS460C ディスクシェルフが含まれている場合は、それぞれの 12 ディスクドロワーについて、次のガイドラインに従ってディスクを手動で割り当てる必要があります。

ドロワーのディスク	ノードとプール
0 ～ 2	ローカルノードのプール 0

3-5	HA パートナーノードのプール 0
6 ~ 8	ローカルノードのプール 1 の DR パートナー
9 ~ 11	HA パートナーのプール 1 の DR パートナー

このディスク割り当てパターンに従うことで、ドロワーがオフラインになった場合のアグリゲートへの影響を最小限に抑えることができます。

手順

1. システムをブートしていない場合は、メンテナンスモードでブートします。
2. 最初のサイト（サイト A ）にあるノードにディスクシェルフを割り当てます。

   ノードと同じサイトにあるディスクシェルフはプール 0 に割り当て、パートナーサイトにあるディスクシェルフはプール 1 に割り当てます。

   各プールに同じ数のシェルフを割り当てる必要があります。

   a. 最初のノードで、ローカルディスクシェルフをプール 0 に、リモートディスクシェルフをプール 1 に割り当てます。

      「 Disk assign-shelf_local-switch-name ： shelf-name .port_-p_pool_`

      ストレージコントローラ Controller_A_1 にシェルフが 4 台ある場合は、次のコマンドを問題に設定します。

      ```
      *> disk assign -shelf FC_switch_A_1:1-4.shelf1 -p 0
      *> disk assign -shelf FC_switch_A_1:1-4.shelf2 -p 0

      *> disk assign -shelf FC_switch_B_1:1-4.shelf1 -p 1
      *> disk assign -shelf FC_switch_B_1:1-4.shelf2 -p 1
      ```

   b. ローカルサイトの 2 番目のノードに対して処理を繰り返し、ローカルディスクシェルフをプール 0 に、リモートディスクシェルフをプール 1 に割り当てます。

      「 Disk assign-shelf_local-switch-name ： shelf-name .port_-p_pool_`

      ストレージコントローラ Controller_A_2 にシェルフが 4 台ある場合は、次のコマンドを問題に設定します。

```
*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0
*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1

*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0
*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1
```

3. 2 番目のサイト（サイト B ）にあるノードにディスクシェルフを割り当てます。

   ノードと同じサイトにあるディスクシェルフはプール 0 に割り当て、パートナーサイトにあるディスクシェルフはプール 1 に割り当てます。

   各プールに同じ数のシェルフを割り当てる必要があります。

   a. リモートサイトの最初のノードで、ローカルディスクシェルフをプール 0 に、リモートディスクシェルフをプール 1 に割り当てます。

      「ディスク assign -shelf_local-switch-namesshelf-name -*p_pool*` 」

      ストレージコントローラ Controller_B_1 にシェルフが 4 台ある場合は、次のコマンドを問題します。

      ```
      *> disk assign -shelf FC_switch_B_1:1-5.shelf1 -p 0
      *> disk assign -shelf FC_switch_B_1:1-5.shelf2 -p 0

      *> disk assign -shelf FC_switch_A_1:1-5.shelf1 -p 1
      *> disk assign -shelf FC_switch_A_1:1-5.shelf2 -p 1
      ```

   b. リモートサイトの 2 番目のノードに対して処理を繰り返し、ローカルディスクシェルフをプール 0 に、リモートディスクシェルフをプール 1 に割り当てます。

      「ディスク assign -shelf_shelf-name-p_pool_` 」

      ストレージコントローラ Controller_B_2 にシェルフが 4 台ある場合は、次のコマンドを問題に実行します。

   ```
   *> disk assign -shelf FC_switch_B_1:1-5.shelf3 -p 0
   *> disk assign -shelf FC_switch_B_1:1-5.shelf4 -p 0

   *> disk assign -shelf FC_switch_A_1:1-5.shelf3 -p 1
   *> disk assign -shelf FC_switch_A_1:1-5.shelf4 -p 1
   ```

4. シェルフの割り当てを確認します。

   「 storage show shelf

5. メンテナンスモードを終了します。

   「 halt 」

6. ブートメニューを表示します。

   「 boot_ontap menu

7. 各ノードで、オプション * 4 * を選択してすべてのディスクを初期化します。

コンポーネントの **ha-config** 状態の確認

MetroCluster 構成では、コントローラモジュールとシャーシコンポーネントの ha-config 状態を * mcc * に設定して、適切にブートするようにする必要があります。

このタスクについて

- システムをメンテナンスモードにする必要があります。
- このタスクは、新しいコントローラモジュールごとに実行する必要があります。

手順

1. メンテナンスモードで、コントローラモジュールとシャーシの HA 状態を表示します。

   「 ha-config show 」

   すべてのコンポーネントの HA の状態が「 mcc 」である必要があります。

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の HA 状態を設定します。

   「 ha-config modify controller mcc 」

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 HA 状態を設定します。

   「 ha-config modify chassis mcc 」

4. 交換した他のノードで同じ手順を繰り返します。

新しいコントローラのブートおよびクラスタへの追加

新しいコントローラをクラスタに追加するには、新しい各コントローラモジュールをブートし、 ONTAP クラスタセットアップウィザードを使用して、参加するクラスタを特定する必要があります。

作業を開始する前に

MetroCluster 構成のケーブル接続を完了しておく必要があります。

このタスクを実行する前に、サービスプロセッサの設定を済ませておく必要があります。

このタスクについて

このタスクは、 MetroCluster 構成の両方のクラスタにある新しい各コントローラで実行する必要があります。

手順

1. 各ノードに電源が入っていない場合は、電源を投入してブートします。

   システムが保守モードになっている場合は、問題 the 'halt コマンドを使用して保守モードを終了し、 LOADER プロンプトから次のコマンドを問題します。

   「 boot_ontap 」

コントローラモジュールがノードセットアップウィザードを開始します。

次のような出力が表示されます。

```
Welcome to node setup

You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the setup wizard.
                Any changes you made before quitting will be saved.

To accept a default or omit a question, do not enter a value.
.
.
.
```

2. システムの指示に従って AutoSupport ツールを有効にします。
3. プロンプトに従ってノード管理インターフェイスを設定します。

次のようなプロンプトが表示されます。

```
Enter the node management interface port: [e0M]:
Enter the node management interface IP address: 10.228.160.229
Enter the node management interface netmask: 225.225.252.0
Enter the node management interface default gateway: 10.228.160.1
```

4. ノードがハイアベイラビリティモードで設定されていることを確認します。

「 storage failover show -fields mode 」を選択します

そうでない場合は、各ノードで次のコマンドを問題処理してからノードをリブートする必要があります。

「 storage failover modify -mode ha -node localhost 」を参照してください

このコマンドを実行するとハイアベイラビリティモードが設定されますが、ストレージフェイルオーバーは有効になりません。ストレージ・フェイルオーバーは ' 構成プロセスの後半で MetroCluster configure コマンドを問題すると ' 自動的に有効になります

5. クラスタインターコネクトとして 4 つのポートが構成されていることを確認します。

「 network port show 」のように表示されます

次の例は、 cluster_A の 2 台のコントローラについての出力です2 ノード MetroCluster 構成の場合、出力に表示されるノードは 1 つだけです。

```
cluster_A::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
node_A_1
       **e0a       Cluster      Cluster          up       1500
auto/1000
       e0b       Cluster      Cluster          up       1500
auto/1000**
       e0c       Default      Default          up       1500  auto/1000
       e0d       Default      Default          up       1500  auto/1000
       e0e       Default      Default          up       1500  auto/1000
       e0f       Default      Default          up       1500  auto/1000
       e0g       Default      Default          up       1500  auto/1000
node_A_2
       **e0a       Cluster      Cluster          up       1500
auto/1000
       e0b       Cluster      Cluster          up       1500
auto/1000**
       e0c       Default      Default          up       1500  auto/1000
       e0d       Default      Default          up       1500  auto/1000
       e0e       Default      Default          up       1500  auto/1000
       e0f       Default      Default          up       1500  auto/1000
       e0g       Default      Default          up       1500  auto/1000
14 entries were displayed.
```

6. CLI を使用してクラスタをセットアップするため、ノードのセットアップウィザードを終了します。

   「 exit

7. admin ユーザ名を使用して admin アカウントにログインします
8. クラスタセットアップウィザードを開始し、既存のクラスタに参加します。

   クラスタ・セットアップ

```
::> cluster setup

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.


Do you want to create a new cluster or join an existing cluster?
{create, join}:`join`
```

9. クラスタセットアップ * ウィザードが完了したら、次のコマンドを入力して、クラスタがアクティブで、ノードが正常であることを確認します。

   「 cluster show 」を参照してください

   次の例は、第 1 ノードが含まれるクラスタ（ cluster1-01 ）が正常に機能しており、クラスタへの参加条件を満たしていることを示しています。

```
cluster_A::> cluster show
Node                 Health  Eligibility
-------------------- ------- ------------
node_A_1             true    true
node_A_2             true    true
node_A_3             true    true
```

   管理 SVM またはノード SVM に対して入力した設定のいずれかを変更する必要がある場合は、「 cluster setup command 」を使用して「 * Cluster Setup * 」ウィザードにアクセスできます。

クラスタを **MetroCluster** 構成に設定

クラスタ間 **LIF** を設定する

専用ポートと共有ポートにクラスタ間LIFを設定する方法について説明します。

専用ポートにクラスタ間 **LIF** を設定します

専用ポートにクラスタ間LIFを設定して、レプリケーショントラフィックに使用できる帯域幅を増やすことができます。

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
       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に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 SVM 「 cluster01 」上のフェイルオーバーグループ「 intercluster01 」に割り当てます。

   ```
   cluster01::> network interface failover-groups create -vserver
   cluster01 -failover-group
   intercluster01 -targets
   cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
   ```

4. フェイルオーバーグループが作成されたことを確認します。

   「 network interface failover-groups show 」と表示されます

   コマンド構文全体については、マニュアルページを参照してください。

```
cluster01::> network interface failover-groups show
                                  Failover
Vserver          Group            Targets
---------------- ----------------
--------------------------------------------
Cluster
                 Cluster
                                  cluster01-01:e0a, cluster01-
01:e0b,
                                  cluster01-02:e0a, cluster01-02:e0b
cluster01
                 Default
                                  cluster01-01:e0c, cluster01-
01:e0d,
                                  cluster01-02:e0c, cluster01-
02:e0d,
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
                 intercluster01
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
```

5. システム SVM にクラスタ間 LIF を作成して、フェイルオーバーグループに割り当てます。

ONTAP バージョン	コマンドを実行します
9.6 以降	`network interface create -vserver <system_SVM> -lif <LIF_name> -service-policy default-intercluster -home -node <node> -home-port <port> -address <port_IP> -netmask <netmask> -failover-group <failover_group>`
9.5 以前	`network interface create -vserver system_SVM -lif <LIF_name> -role intercluster -home-node <node> -home -port <port> -address <port_IP> -netmask <netmask> -failover-group <failover_group>`

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： *
「 network interface show -service -policy default -intercluster 」のように表示されます
* ONTAP 9.5 以前： *
「 network interface show -role intercluster 」の略

コマンド構文全体については、マニュアルページを参照してください。

```
cluster01::> network interface show -service-policy default-
intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01
e0e     true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02
e0f     true
```

7. クラスタ間 LIF が冗長構成になっていることを確認します。

* ONTAP 9.6 以降： *

「 network interface show -service -policy default -intercluster-failover 」のように入力します
* ONTAP 9.5 以前： *
「 network interface show -role intercluster-failover 」の略

コマンド構文全体については、マニュアルページを参照してください。

次の例は、 SVM 「 e0e 」ポート上のクラスタ間 LIF 「 cluster01_icl01 」と「 cluster01_icl02 」が「 e0f 」ポートにフェイルオーバーされることを示しています。

```
cluster01::> network interface show -service-policy default-
intercluster –failover
         Logical         Home                  Failover
Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- ---------------
--------
cluster01
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

共有データポートにクラスタ間 **LIF** を設定します

データネットワークと共有するポートにクラスタ間LIFを設定することで、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： *
`network interface create -vserver <system_SVM> -lif <LIF_name> -service -policy default-intercluster -home-node <node> -home-port <port> -address <port_IP> -netmask <netmask>`
* ONTAP 9.5 以前： *
`network interface create -vserver <system_SVM> -lif <LIF_name> -role intercluster -home-node <node> -home-port <port> -address <port_IP> -netmask <netmask>`

コマンド構文全体については、マニュアルページを参照してください。

次の例は、クラスタ間 LIF 「 cluster01_icl01 」と「 cluster01_icl02 」を作成します。

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. クラスタ間 LIF が作成されたことを確認します。

* ONTAP 9.6 以降： *
「 network interface show -service -policy default -intercluster 」のように表示されます
* ONTAP 9.5 以前： *
「 network interface show -role intercluster 」の略

コマンド構文全体については、マニュアルページを参照してください。

```
cluster01::> network interface show -service-policy default-
intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01
e0c     true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02
e0c     true
```

4. クラスタ間 LIF が冗長構成になっていることを確認します。

* ONTAP 9.6 以降： *

「 network interface show – service-policy default-intercluster-failover 」と表示されます
* ONTAP 9.5 以前： *
「 network interface show -role intercluster-failover 」の略

コマンド構文全体については、マニュアルページを参照してください。

次の例は、「 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
```

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。

デフォルトでは、ルートアグリゲートは RAID-DP タイプのアグリゲートとして作成されます。ルートアグリゲートのタイプは RAID-DP から RAID4 に変更することができます。次のコマンドは、ルートアグリゲートを RAID4 タイプのアグリゲートに変更します。

```
storage aggregate modify –aggregate aggr_name -raidtype raid4
```

ADP 以外のシステムでは、ミラーリングの実行前後に、アグリゲートの RAID タイプをデフォルトの RAID-DP から RAID4 に変更できます。

手順

1. ルートアグリゲートをミラーします。

「 storage aggregate mirror _aggr_name _ 」のようになります

次のコマンドでは、 controller_A_1 のルートアグリゲートがミラーされます。

```
controller_A_1::> storage aggregate mirror aggr0_controller_A_1
```

これによりアグリゲートがミラーされるため、ローカルのプレックスとリモートのプレックスがリモートの MetroCluster サイトに配置されたアグリゲートが作成されます。

2. MetroCluster 構成の各ノードについて、同じ手順を繰り返します。

MetroCluster 構成の実装

MetroCluster 構成に追加したノードでデータ保護を開始するには 'MetroCluster configure -refresh true 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

MetroCluster 構成を更新するには ' 新しく追加されたノードの 1 つで ' MetroCluster configure -refresh true コマンドを 1 回実行します問題各サイトまたは各ノードでコマンドを問題処理する必要はありません。

MetroCluster configure -refresh true コマンドは '2 つのクラスタそれぞれのシステム ID が最も小さい 2 つのノードを 'DR （災害復旧）パートナーとして自動的にペア設定します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。

手順

1. MetroCluster 構成を更新します。

   a. advanced 権限モードに切り替えます。

      「 advanced 」の権限が必要です

   b. 新しいノードの 1 つで MetroCluster 設定を更新します。 + MetroCluster configure -refresh true

      次の例では、両方の DR グループで MetroCluster 構成を更新しています。

```
controller_A_2::*> metrocluster configure -refresh true

[Job 726] Job succeeded: Configure is successful.
```

+

```
controller_A_4::*> metrocluster configure -refresh true

[Job 740] Job succeeded: Configure is successful.
```

a. admin 権限モードに戻ります。

「特権管理者」

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
                                                            Speed (Mbps)
Node   Port      IPspace   Broadcast Domain Link   MTU    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
```

a. 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
```

各**MetroCluster FC**ノードでミラーリングされたデータ 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。
- システムに複数のドライブ タイプがある場合（異機種混在ストレージ）、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。
- 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。

> 最適なストレージ パフォーマンスと可用性を確保するには、ミラー化されたアグリゲートに少なくとも 20% の空き領域を確保することをお勧めします。ミラーリングされていないアグリゲートの場合、推奨値は 10% ですが、追加の 10% のスペースは、増分変更を吸収するためにファイル システムによって使用できます。増分変更により、ONTAPのcopy-on-write Snapshotベースのアーキテクチャにより、ミラー化されたアグリゲートのスペース使用率が増加します。これらのベスト プラクティスに従わないと、パフォーマンスに悪影響が出る可能性があります。

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ている場合は、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ていることを確認するには、 `-node` パラメータを使用するか、そのノードが所有するドライブを指定します。

   次のオプションを指定できます。

   - アグリゲートのホームノード（通常運用時にアグリゲートを所有するノード）
   - アグリゲートに追加するドライブのリスト
   - 追加するドライブ数

     > 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
   - RPM の異なるドライブが許可されるかどうか

     これらのオプションの詳細については 'storage aggregate create のマニュアルページを参照してください

     次のコマンドでは、 10 本のディスクを含むミラーアグリゲートが作成されます。

```
cluster_A::> storage aggregate create aggr1_node_A_1 -diskcount 10 -node
node_A_1 -mirror true
[Job 15] Job is queued: Create aggr1_node_A_1.
[Job 15] The job is starting.
[Job 15] Job succeeded: DONE
```

3. 新しいアグリゲートの RAID グループとドライブを確認します。

```
storage aggregate show-status -aggregate <aggregate-name>
```

健常性監視用の **FC-to-SAS** ブリッジの設定

健全性監視用にFC-to-SASブリッジを設定する方法について説明します。

このタスクについて

- FibreBridge ブリッジでは、サードパーティ製の SNMP 監視ツールはサポートされません。
- ONTAP 9.8 以降では、デフォルトで FC-to-SAS ブリッジがインバンド接続で監視されるため、追加の設定は必要ありません。

ONTAP 9.8 以降では 'storage bridge コマンドは 'system bridge コマンドに置き換えられました 次の手順は「 storage bridge 」コマンドを示していますが、 ONTAP 9.8 以降を実行している場合は「 system bridge 」コマンドが優先されます。

ステップ

1. ONTAP クラスタのプロンプトで、ブリッジをヘルスモニタの対象に追加します。

   a. 使用している ONTAP のバージョンに対応したコマンドを使用して、ブリッジを追加します。

ONTAP バージョン	コマンドを実行します
9.5 以降	「 storage bridge add -address 0.0.0.0 -managed -by in-band-name_bridge-name_`
9.4 以前	「 storage bridge add -address_bridge-ip -address_-name_bridge-name_` 」

   b. ブリッジが追加され、正しく設定されていることを確認します。

      「 storage bridge show 」

      ポーリング間隔に応じて、すべてのデータが反映されるまで 15 分程度かかる場合があります。「 Status 」列の値が「 ok 」で、 World Wide Name （ WWN ；ワールドワイド名）などのその他の情報が表示されていれば、 ONTAP ヘルスモニタでブリッジに接続して監視できます。

      次の例は、 FC-to-SAS ブリッジが設定されていることを示しています。

```
controller_A_1::> storage bridge show

Bridge               Symbolic Name Is Monitored  Monitor Status  Vendor
Model                 Bridge WWN
------------------  ------------ ------------  --------------  ------
-----------------    ----------
ATTO_10.10.20.10  atto01        true          ok              Atto
FibreBridge 7500N      20000010867038c0
ATTO_10.10.20.11  atto02        true          ok              Atto
FibreBridge 7500N      20000010867033c0
ATTO_10.10.20.12  atto03        true          ok              Atto
FibreBridge 7500N      20000010867030c0
ATTO_10.10.20.13  atto04        true          ok              Atto
FibreBridge 7500N      2000001086703b80

4 entries were displayed

 controller_A_1::>
```

MetroCluster 構成でのメタデータボリュームの移動

MetroCluster 構成では、アグリゲート間でメタデータボリュームを移動できます。メタデータボリュームの移動が必要となるのは、ソースアグリゲートが運用停止になるかミラーリングを解除されたとき、または何らかの理由でアグリゲートが条件を満たさなくなったときです。

このタスクについて

- このタスクを実行するには、クラスタ管理者の権限が必要です。
- ターゲットアグリゲートがミラーされており、かつデグレード状態でないことが必要です。
- ターゲットアグリゲートに、移動するメタデータボリュームよりも大きな使用可能スペースがあることが必要です。

手順

1. 権限レベルを advanced に設定します。

   「 advanced 」の権限が必要です

2. 移動するメタデータボリュームを特定します。

   volume show MDV_CRS *

```
Cluster_A::*> volume show MDV_CRS*
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
Cluster_A
          MDV_CRS_14c00d4ac9f311e7922800a0984395f1_A
                       Node_A_1_aggr1
                                    online     RW         10GB
9.50GB    5%
Cluster_A
          MDV_CRS_14c00d4ac9f311e7922800a0984395f1_B
                       Node_A_2_aggr1
                                    online     RW         10GB
9.50GB    5%
Cluster_A
          MDV_CRS_15035e66c9f311e7902700a098439625_A
                       Node_B_1_aggr1
                                    -          RW             -
-     -
Cluster_A
          MDV_CRS_15035e66c9f311e7902700a098439625_B
                       Node_B_2_aggr1
                                    -          RW             -
-     -
4 entries were displayed.

Cluster_A::>
```

3. 対象となるターゲットアグリゲートを特定します。

   MetroCluster check config-replication show-aggregate-eligibility

   次のコマンドは、メタデータボリュームをホストできる cluster_A 内のアグリゲートを特定します。

```
Cluster_A::*> metrocluster check config-replication show-aggregate-
eligibility

Aggregate Hosted Config Replication Vols Host Addl Vols Comments
------------ ------------------------------------------ --------------
--------
Node_A_1_aggr0 - false Root Aggregate
Node_A_2_aggr0 - false Root Aggregate
Node_A_1_aggr1 MDV_CRS_1bc7134a5ddf11e3b63f123478563412_A true -
Node_A_2_aggr1 MDV_CRS_1bc7134a5ddf11e3b63f123478563412_B true -
Node_A_1_aggr2 - true
Node_A_2_aggr2 - true
Node_A_1_Aggr3 - false Unable to determine available space of aggregate
Node_A_1_aggr5 - false Unable to determine mirror configuration
Node_A_2_aggr6 - false Mirror configuration does not match requirement
Node_B_1_aggr4 - false NonLocal Aggregate
```

この例では、 Node_A_1_aggr2 と Node_A_2_aggr2 が該当します。

4. ボリューム移動処理を開始します。

   'volume move start -vserver_svm_name_-volume_volume_name_-destination aggregate-destination_destination_aggregate-name_*'

   次のコマンドは、メタデータボリューム「 MDV_CRS_14c00d4ac9f311e7922800a0984395f1 」を「アグリゲート Node_A_1_aggr1 」から「アグリゲート Node_A_1_aggr2 」に移動します。

```
Cluster_A::*> volume move start -vserver svm_cluster_A -volume
MDV_CRS_14c00d4ac9f311e7922800a0984395f1
-destination-aggregate aggr_cluster_A_02_01

Warning: You are about to modify the system volume
         "MDV_CRS_9da04864ca6011e7b82e0050568be9fe_A".  This may cause
severe
         performance or stability problems.  Do not proceed unless
directed to
         do so by support.  Do you want to proceed? {y|n}: y
[Job 109] Job is queued: Move
"MDV_CRS_9da04864ca6011e7b82e0050568be9fe_A" in Vserver
"svm_cluster_A" to aggregate "aggr_cluster_A_02_01".
Use the "volume move show -vserver svm_cluster_A -volume
MDV_CRS_9da04864ca6011e7b82e0050568be9fe_A" command to view the status
of this operation.
```

5. ボリューム移動処理の状態を確認します。

volume move show -volume vol_constituent_name 」と表示されます

6. admin 権限レベルに戻ります。

「特権管理者」

MetroCluster の設定を確認しています

MetroCluster 構成内のコンポーネントおよび関係が正しく機能していることを確認できます。チェックは、初期設定後と、 MetroCluster 設定に変更を加えたあとに実施する必要があります。また、ネゴシエート（計画的）スイッチオーバーやスイッチバックの処理の前にも実施します。

このタスクについて

いずれかまたは両方のクラスタに対して短時間に MetroCluster check run コマンドを 2 回発行すると ' 競合が発生し ' コマンドがすべてのデータを収集しない場合がありますそれ以降の「 MetroCluster check show 」コマンドでは、期待される出力が表示されません。

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

Last Checked On: 8/5/2014 00:42:58

Node                  Aggregate                 Check
Result
---------------       --------------------      ---------------------
---------
controller_A_1        controller_A_1_aggr0
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
ok
                      controller_A_1_aggr1
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
ok
                      controller_A_1_aggr2
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
ok
```

```
controller_A_2        controller_A_2_aggr0
                                                  mirroring-status
ok
                                                  disk-pool-allocation
ok
                                                  ownership-state
ok
                      controller_A_2_aggr1
                                                  mirroring-status
ok
                                                  disk-pool-allocation
ok
                                                  ownership-state
ok
                      controller_A_2_aggr2
                                                  mirroring-status
ok
                                                  disk-pool-allocation
ok
                                                  ownership-state
ok

18 entries were displayed.
```

次に、正常な 4 ノード MetroCluster 構成の MetroCluster check cluster show コマンドの出力例を示します。この出力は、必要に応じてネゴシエートスイッチオーバーを実行できる状態であることを示しています。

```
Last Checked On: 9/13/2017 20:47:04

Cluster                 Check                           Result
---------------------- ------------------------------- ---------
mccint-fas9000-0102
                        negotiated-switchover-ready     not-applicable
                        switchback-ready                not-applicable
                        job-schedules                   ok
                        licenses                        ok
                        periodic-check-enabled          ok
mccint-fas9000-0304
                        negotiated-switchover-ready     not-applicable
                        switchback-ready                not-applicable
                        job-schedules                   ok
                        licenses                        ok
                        periodic-check-enabled          ok
10 entries were displayed.
```

Config Advisor での MetroCluster 構成エラーの確認

一般的な構成エラーの有無を確認する Config Advisor ツールをネットアップサポートサイトからダウンロードできます。

このタスクについて

Config Advisor は、構成の検証や健常性のチェックに使用できるツールです。データ収集とシステム分析のために、セキュアなサイトにもセキュアでないサイトにも導入できます。

Config Advisor のサポートには制限があり、オンラインでしか使用できません。

手順

1. Config Advisor のダウンロードページにアクセスし、ツールをダウンロードします。

   "ネットアップのダウンロード： Config Advisor"

2. Config Advisor を実行し、ツールの出力を確認して、問題が検出された場合は出力に表示される推奨事項に従って対処します。

カスタム AutoSupport メッセージは、 MetroCluster 構成へのノードの追加後に送信します

保守が完了したことをネットアップテクニカルサポートに通知するには、 AutoSupport メッセージを問題で送信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 サイトごとに実行する必要があります。

手順

1. Site_A のクラスタにログインします
2. メンテナンスの終了を通知する AutoSupport メッセージを起動します。

   「 system node AutoSupport invoke -node * -type all -message MAINT= end 」というメッセージが表示されます

3. 同じ手順をパートナーサイトでも実行します。

スイッチオーバー、修復、スイッチバックを検証しています

MetroCluster 構成のスイッチオーバー、修復、スイッチバックの処理を検証する必要があります。

手順

1. のネゴシエートスイッチオーバー、修復、スイッチバックの手順を使用します "MetroCluster の管理とディザスタリカバリ"。

MetroCluster IP設定を展開します

ONTAP のバージョンに応じて、4つの新しいノードを新しいDRグループとして追加することでMetroCluster IP構成を拡張できます。

ONTAP 9.13.1以降では、8ノードMetroCluster構成を一時的に拡張してコントローラとストレージを更新できます。を参照してください "4ノードまたは8ノードのMetroCluster IP構成の更新（ONTAP 9.8以降）" を参照してください。

ONTAP 9.9.9..1 以降では、 4 つの新しいノードを 2 つ目の DR グループとして MetroCluster IP 構成に追加できます。これにより、 8 ノード MetroCluster 構成が作成されます。

古いプラットフォームモデルを追加する場合の重要な情報

次のガイダンスは、新しいプラットフォーム モデル (ONTAP 9.15.1 以降でリリースされたプラットフォーム) を含む既存のMetroCluster構成に古いプラットフォーム モデル (ONTAP 9.15.1 より前にリリースされたプラットフォーム) を追加する必要がある、まれなシナリオを対象としています。

既存のMetroCluster構成に、共有クラスタ**/HA** ポート を使用するプラットフォーム (ONTAP 9.15.1 以降でリリースされたプラットフォーム) が含まれている場合、構成内のすべてのノードをONTAP 9.15.1P11 またはONTAP 9.16.1P4 以降にアップグレードせずに、共有**MetroCluster/HA** ポート を使用するプラットフォーム (ONTAP 9.15.1 より前にリリースされたプラットフォーム) を追加することはできません。

> 共有**/ MetroCluster HA** ポート を使用する古いプラットフォーム モデルを、共有クラスタ**/HA** ポート を使用する新しいプラットフォーム モデルを含むMetroClusterに追加することはまれなシナリオであり、ほとんどの組み合わせは影響を受けません。

次の表を使用して、組み合わせが影響を受けるかどうかを確認してください。既存のプラットフォームが最初の列にリストされ、構成に追加するプラットフォームが 2 番目の列にリストされている場合、新しい DR グループを追加するには、構成内のすべてのノードでONTAP 9.15.1P11 またはONTAP 9.16.1P4 以降が実行されている必要があります。

既存の **MetroCluster** に以下が含まれている場合...		追加するプラットフォームは...		作業
共有クラスター/**HA** ポート を使用する AFF システム: • AFF A20用 • AFF A30用 • AFF C30 • AFF A50用 • AFF C60 • AFF C80用 • AFF A70用 • AFF A90用 • AFF A1K用	共有クラスター/**HA** ポート を使用する FAS システム: • FAS50 • FAS70 • FAS90	共有 **MetroCluster/HA** ポート を使用する AFF システム: • AFF A150、ASA A150向け • AFF A220 • AFF C250 、ASA C250向け • AFF A250、ASA A250向け • AFF A300 • AFF A320 • AFF C400 、ASA C400向け • AFF A400、ASA A400向け • AFF A700 • AFF C800 、ASA C800向け • AFF A800、ASA A800向け • AFF A900、ASA A900向け	共有 **MetroCluster/HA** ポート を使用する FAS システム: • FAS2750 • FAS500f • FAS8200 • FAS8300 • FAS8700 の場合 • FAS9000 • FAS9500	既存の MetroCluster 構成に新しいプラットフォームを追加する前に、既存および新しい構成内のすべてのノードを ONTAP 9.15.1P11 または ONTAP 9.16.1P4 以降にアップグレードします。

作業を開始する前に

- 古いノードと新しいノードで同じバージョンの ONTAP を実行する必要があります。
- この手順では、既存のMetroCluster IP構成に4ノードDRグループを1つ追加する手順について説明します。8ノード構成を更新する場合は、手順全体をDRグループごとに1つずつ追加して繰り返す必要があります。
- 新旧のプラットフォームモデルでプラットフォームの混在がサポートされていることを確認します。

  "NetApp Hardware Universe の略"

- 古いプラットフォームモデルと新しいプラットフォームモデルの両方がIPスイッチでサポートされていることを確認します。

  "NetApp Hardware Universe の略"

- 実行中の場合 "4ノードまたは8ノードのMetroCluster IP構成の更新"新しいノードには、古いノードのデータを収容するための十分なストレージに加え、ルートアグリゲート用の十分なディスクとスペアディスクが必要です。
- 古いノードにデフォルトのブロードキャストドメインが作成されていることを確認します。

  デフォルトのブロードキャストドメインがない既存のクラスタに新しいノードを追加すると、想定される名前ではなくUniversal Unique Identifier（UUID）を使用して新しいノード用のノード管理LIFが作成されます。詳細については、技術情報アーティクルを参照してください "UUID名で生成された新しく追加されたノードのノード管理LIF"。

コンソールログを有効にする

NetAppでは、使用しているデバイスでコンソールロギングをイネーブルにし、この手順を実行する際に次のアクションを実行することを強く推奨します。

- メンテナンス中はAutoSupportを有効のままにします。
- メンテナンスの前後にメンテナンスAutoSupportメッセージをトリガーして、メンテナンスアクティビティ中にケースの作成を無効にします。

  ナレッジベースの記事を参照してください "スケジュールされたメンテナンス時間中にケースの自動作成を停止する方法"。

- 任意のCLIセッションのセッションロギングをイネーブルにします。セッションログを有効にする方法については、ナレッジベースの記事の「セッション出力のログ」セクションを参照してください "ONTAPシステムへの接続を最適化するためのPuTTYの設定方法"。

この手順での命名例

この手順では、全体的な名前の例を使用して、 DR グループ、ノード、および関連するスイッチを特定します。

DR グループ	site_A で cluster_A	site_B （ site_B
dr_group_1 - 古い	• node_A_1 - 古い • Node_a_2-old	• node_B_1 - 古い • node_B_2 - 古い
dr_group_2 - 新規	• Node_a_3 - 新規 • Node_a_4 - 新規	• node_B_2 - 新規 • node_B_2 - 新規

2つ目のDRグループを追加する際にサポートされるプラットフォームの組み合わせ

次の表に、8ノードMetroCluster IP構成でサポートされるプラットフォームの組み合わせを示します。

- MetroCluster構成内のすべてのノードで同じバージョンのONTAPが実行されている必要があります。たとえば、8ノード構成の場合は、8つのすべてのノードで同じバージョンのONTAPを実行する必要があります。ご使用の組み合わせでサポートされるONTAPの最小バージョンについては、を参照して"Hardware Universe"ください。
- この表の組み合わせは、通常または永続的な8ノード構成にのみ該当します。
- この表に示されているプラットフォームの組み合わせは、移行手順または更新手順を使用する場合は適用されません*。
- 1つのDRグループ内のすべてのノードのタイプと構成が同じである必要があります。

サポートされる**AFF**と**FAS MetroCluster IP**の拡張の組み合わせ

次の表に、MetroCluster IP構成でAFFシステムまたはFASシステムを拡張する場合にサポートされるプラットフォームの組み合わせを示します。テーブルは次の2つのグループに分割されます。

- *グループ1 *は、、AFF A20、FAS2750、AFF A220、AFF A150、FAS500f、AFF C250、FAS8200、FAS50、AFF C400 C30、AFF A30、AFF A250、AFF A300、AFF A400、FAS8700、AFF、AFF A320、FAS8300システムの組み合わせを示しています。
- *グループ2 *は、AFF C60、AFF A50、FAS70、FAS9000、AFF A700、AFF A70、AFF C800、AFF、FAS9500、AFF A900、AFF A800 C80、FAS90、AFF A90、およびAFF A1Kシステムの組み合わせを示しています。

次の注意事項は両方のグループに適用されます。

- 注1：これらの組み合わせには、ONTAP 9.9.1以降（またはプラットフォームでサポートされるONTAPの最小バージョン）が必要です。
- 注2：これらの組み合わせには、ONTAP 9.13.1以降（またはプラットフォームでサポートされるONTAPの最小バージョン）が必要です。

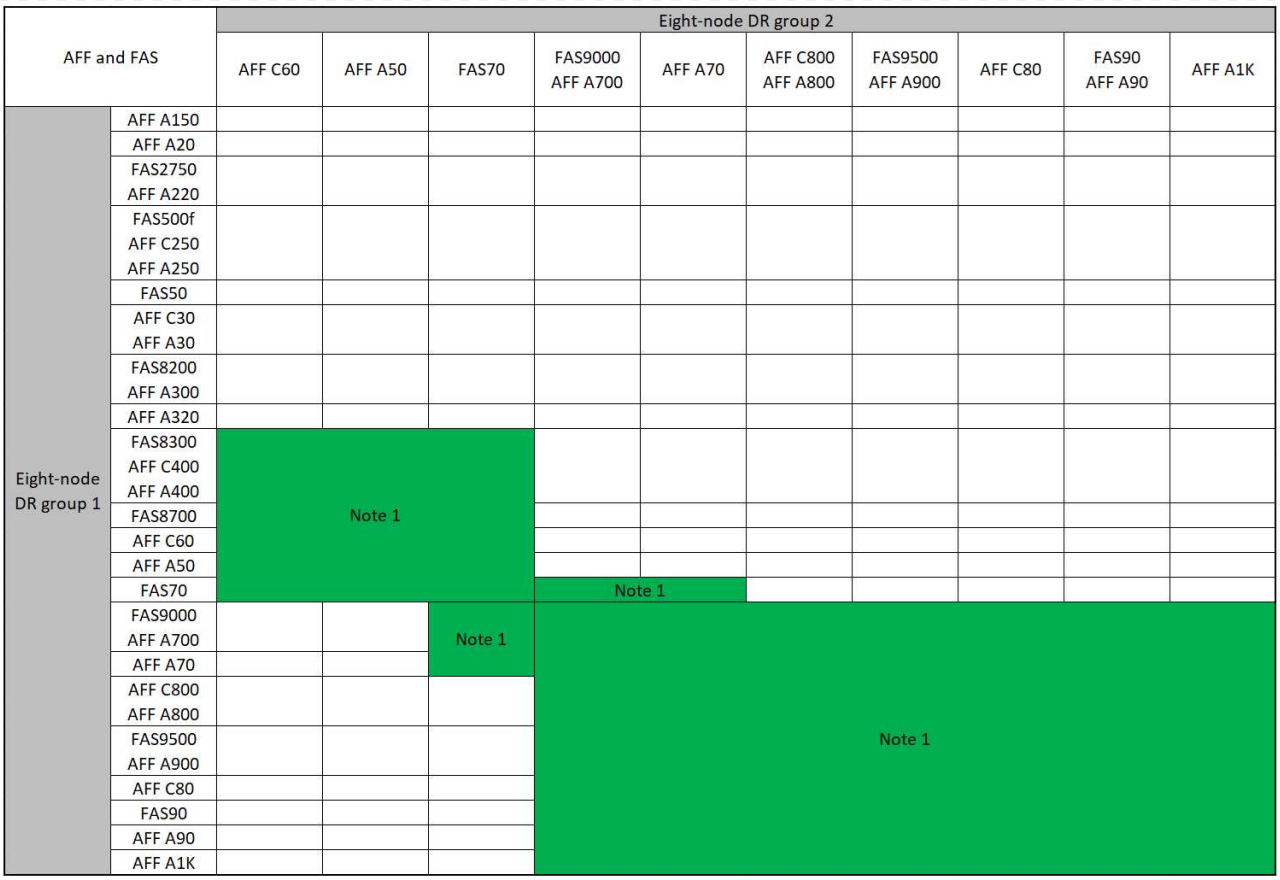
AFFと**FAS**の組み合わせグループ**1**

AFF A150、AFF A20、FAS2750 AFF A400、AFF A220、FAS500f、AFF A320、FAS8200、FAS50、AFF C30、AFF A30、AFF A250、AFF C400、AFF C250、FAS8300、AFF A300、FAS8700システムの拡張の組み合わせを確認します。

<table>
<tr><th colspan="2" rowspan="2">AFF and FAS</th><th colspan="10">Eight-node DR group 2</th></tr>
<tr><th>AFF A150</th><th>AFF A20</th><th>FAS2750
AFF A220</th><th>FAS500f
AFF C250
AFF A250</th><th>FAS50</th><th>AFF C30
AFF A30</th><th>FAS8200
AFF A300</th><th>AFF A320</th><th>FAS8300
AFF C400
AFF A400</th><th>FAS8700</th></tr>
<tr><td rowspan="24">Eight-node
DR group 1</td><td>AFF A150</td><td colspan="6" rowspan="8">Note 2</td><td></td><td></td><td></td><td></td></tr>
<tr><td>AFF A20</td><td></td><td></td><td></td><td></td></tr>
<tr><td>FAS2750
AFF A220</td><td></td><td></td><td></td><td></td></tr>
<tr><td>FAS500f
AFF C250
AFF A250</td><td></td><td></td><td></td><td></td></tr>
<tr><td>FAS50</td><td></td><td></td><td></td><td></td></tr>
<tr><td>AFF C30
AFF A30</td><td></td><td></td><td></td><td></td></tr>
<tr><td>FAS8200
AFF A300</td><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="2" rowspan="2">Note 1</td><td></td><td></td></tr>
<tr><td>AFF A320</td><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="4">Note 1</td></tr>
<tr><td>FAS8300
AFF C400
AFF A400</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td rowspan="2">Note 1</td><td colspan="2" rowspan="5">Note 1</td></tr>
<tr><td>FAS8700</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>AFF C60</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>AFF A50</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>FAS70</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>FAS9000
AFF A700</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>AFF A70</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>AFF C800
AFF A800</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>FAS9500
AFF A900</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>AFF C80</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>FAS90</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>AFF A90</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>AFF A1K</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

AFFと**FAS**の組み合わせグループ**2**

C60、AFF A50、FAS70、FAS9000、AFF A700、AFF A70、AFF C800、AFF、AFF A90、AFF、AFF A1K、AFF A800 C80、FAS90、FAS9500、AFF A900システムの拡張の組み合わせを確認します。



サポートされる**ASA MetroCluster IP**拡張の組み合わせ

次の表に、MetroCluster IP構成でASAシステムを拡張する場合にサポートされるプラットフォームの組み合わせを示します。

ASA		Eight-node DR group 2							
		ASA A150	ASA C250	ASA A250	ASA C400	ASA A400	ASA C800	ASA A800	ASA A900
Eight-node DR group 1	ASA A150	■							
	ASA C250		■						
	ASA A250			■					
	ASA C400				■				
	ASA A400					■			
	ASA C800						■		
	ASA A800							■	
	ASA A900								■

カスタム **AutoSupport** メッセージをメンテナンス前に送信する

メンテナンスを実行する前に、 AutoSupport an 問題 message to notify NetApp technical support that maintenance is maintenancing （メンテナンスが進行中であることをネットアップテクニカルサポートに通知する）を実行システム停止が発生したとみなしてテクニカルサポートがケースをオープンしないように、メンテナンスが進行中であることを通知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 サイトごとに実行する必要があります。

手順

1. サポートケースが自動で生成されないようにするには、アップグレードが進行中であることを示すAutoSupport メッセージを送信します。

   a. 次のコマンドを問題に設定します。

      ```
      system node autosupport invoke -node * -type all -message "MAINT=10h
      Upgrading <old-model> to <new-model>
      ```

      この例では、 10 時間のメンテナンス時間を指定しています。プランによっては、さらに時間をかけたい場合もあります。

      この時間が経過する前にメンテナンスが完了した場合は、メンテナンス期間が終了したことを通知する AutoSupport メッセージを起動できます。

「 system node AutoSupport invoke -node * -type all -message MAINT= end 」というメッセージが表示されます

   a. パートナークラスタに対してこのコマンドを繰り返します。

新しいDRグループを追加する際のVLANに関する考慮事項

- MetroCluster IP構成を拡張する場合は、次のVLANに関する考慮事項が適用されます。

  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。

- 4ノードから8ノードのMetroCluster構成に拡張する場合は、両方のDRグループで同じVLANが使用されます。
- 同じVLANを使用して両方のDRグループを設定できない場合は、パラメータをサポートしていないDRグループをアップグレードして、他のDRグループでサポートされているVLANを使用する必要があり `vlan-id` ます。

MetroCluster 構成の健全性の確認

拡張を実行する前に、MetroCluster構成の健全性と接続を確認する必要があります。

手順

1. ONTAP で MetroCluster 構成の動作を確認します。
   a. システムがマルチパスかどうかを確認します。

      ```
      node run -node <node-name> sysconfig -a
      ```

   b. ヘルスアラートがないかどうかを両方のクラスタで確認します。

      「 system health alert show 」というメッセージが表示されます

   c. MetroCluster 構成と運用モードが正常な状態であることを確認します。

      「 MetroCluster show 」

d. MetroCluster チェックを実行します。

「 MetroCluster check run 」のようになります

e. MetroCluster チェックの結果を表示します。

MetroCluster チェックショー

f. Config Advisor を実行します。

"ネットアップのダウンロード： Config Advisor"

g. Config Advisor の実行後、ツールの出力を確認し、推奨される方法で検出された問題に対処します。

2. クラスタが正常であることを確認します。

「 cluster show 」を参照してください

```
cluster_A::> cluster show
Node            Health  Eligibility
--------------- ------  -----------
node_A_1        true    true
node_A_2        true    true

cluster_A::>
```

3. すべてのクラスタポートが動作していることを確認します。

「 network port show -ipspace cluster 」のように表示されます

```
cluster_A::> network port show -ipspace Cluster

Node: node_A_1-old

                                                  Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

Node: node_A_2-old

                                                  Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

4 entries were displayed.

cluster_A::>
```

4. すべてのクラスタ LIF が動作していることを確認します。

   「 network interface show -vserver Cluster 」のように表示されます

   各クラスタ LIF で、 Is Home には true 、 Status Admin/Oper には up/up と表示されるはずです

```
cluster_A::> network interface show -vserver cluster

            Logical      Status     Network          Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- -----
Cluster
            node_A_1-old_clus1
                       up/up      169.254.209.69/16  node_A_1   e0a
true
            node_A_1-old_clus2
                       up/up      169.254.49.125/16  node_A_1   e0b
true
            node_A_2-old_clus1
                       up/up      169.254.47.194/16  node_A_2   e0a
true
            node_A_2-old_clus2
                       up/up      169.254.19.183/16  node_A_2   e0b
true

4 entries were displayed.

cluster_A::>
```

5. すべてのクラスタ LIF で自動リバートが有効になっていることを確認します。

   network interface show -vserver Cluster -fields auto-revert を実行します

```
cluster_A::> network interface show -vserver Cluster -fields auto-revert

          Logical
Vserver   Interface     Auto-revert
--------- ------------- ------------
Cluster
           node_A_1-old_clus1
                        true
           node_A_1-old_clus2
                        true
           node_A_2-old_clus1
                        true
           node_A_2-old_clus2
                        true

    4 entries were displayed.

cluster_A::>
```

監視アプリケーションから構成を削除します

ONTAP Tiebreaker ソフトウェア、 MetroCluster メディエーター、またはスイッチオーバーを開始できるその他の他社製アプリケーション（ ClusterLion など）で既存の構成を監視している場合は、アップグレードの前に、監視ソフトウェアから MetroCluster 構成を削除する必要があります。

手順

1. Tiebreaker 、メディエーター、またはスイッチオーバーを開始できるその他のソフトウェアから既存の MetroCluster 構成を削除します。

使用するポート	使用する手順
Tiebreaker	"MetroCluster 設定の削除"。
メディエーター	ONTAP プロンプトで次のコマンドを問題に設定します。 MetroCluster 構成設定のメディエーターが削除されました
サードパーティ製アプリケーション	製品マニュアルを参照してください。

2. スイッチオーバーを開始できるサードパーティ製アプリケーションから既存の MetroCluster 構成を削除します。

   アプリケーションのマニュアルを参照してください。

新しいコントローラモジュールの準備を行います

4 つの新しい MetroCluster ノードを準備し、正しいバージョンの ONTAP をインストールする必要があります。

このタスクについて

このタスクは新しい各ノードで実行する必要があります。

- Node_a_3 - 新規
- Node_a_4 - 新規
- node_B_2 - 新規
- node_B_2 - 新規

この手順では、ノードの設定をクリアし、新しいドライブのメールボックスのリージョンをクリアします。

手順

1. 新しいコントローラをラックに設置します。
2. に示すように、新しいMetroCluster IPノードをIPスイッチにケーブル接続し "IPスイッチのケーブル接続" ます。
3. 次の手順に従ってMetroCluster IPノードを設定します。
   a. "必要な情報を収集"
   b. "コントローラモジュールのシステムデフォルトの復元"
   c. "コンポーネントの ha-config 状態を確認"
   d. "プール0のドライブを手動で割り当てる（ONTAP 9.4以降）"
4. 保守モードから問題 the halt コマンドを実行して保守モードを終了し、 boot_ontap コマンドを問題してシステムをブートしてクラスタセットアップを開始します。

   このとき、クラスタウィザードやノードウィザードを実行しないでください。

RCF ファイルをアップグレードします

新しいスイッチファームウェアをインストールする場合は、 RCF ファイルをアップグレードする前にスイッチファームウェアをインストールする必要があります。

このタスクについて

この手順では、 RCF ファイルをアップグレードするスイッチ上のトラフィックが中断されます。新しい RCF ファイルが適用されると、トラフィックは再開されます。

手順

1. 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 」のようになります

```
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. MetroCluster check run オペレーションが完了したら ' MetroCluster check show を実行して結果を表示します

約 5 分後に、次の結果が表示されます。

```
-----------
::*> 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 オペレーション履歴 show -job-id 38`

b. ヘルスアラートがないことを確認します。

「 system health alert show 」というメッセージが表示されます

2. 新しい RCF ファイルを適用するための IP スイッチを準備します。

スイッチベンダーの手順に従います。

- "Broadcom IP スイッチを工場出荷時のデフォルトにリセットします"
- "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"
- "NVIDIA IP SN2100スイッチを工場出荷時のデフォルトにリセット"

3. スイッチベンダーに応じて、IP RCFファイルをダウンロードしてインストールします。

スイッチを次の順序で更新します。Switch_A_1、Switch_B_1、Switch_A_1、Switch_B_2

- "Broadcom IPのRCFファイルをダウンロードしてインストールする"
- "Cisco IP RCFファイルのダウンロードとインストール"

- "NVIDIA IP RCFファイルのダウンロードとインストール"

> L2共有またはL3ネットワーク構成の場合は、中間スイッチまたはお客様のスイッチのISLポートの調整が必要になることがあります。スイッチポートモードが「access」から「trunk」モードに変わる可能性があります。2つ目のスイッチペア（A_2、B_2）のアップグレードに進むのは、スイッチA_1とB_1間のネットワーク接続が完全に動作していて、ネットワークが正常な場合だけにしてください。

新しいノードをクラスタに追加

4 つの新しい MetroCluster IP ノードを既存の MetroCluster 構成に追加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クラスタで実行する必要があります。

手順

1. 新しい MetroCluster IP ノードを既存の MetroCluster 構成に追加
   a. 最初の新しい MetroCluster IP ノード（ node_A_1 の新しいノード）を既存の MetroCluster IP 構成に追加します。

```
Welcome to the cluster setup wizard.

You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the cluster setup wizard.
     Any changes you made before quitting will be saved.

You can return to cluster setup at any time by typing "cluster
setup".
To accept a default or omit a question, do not enter a value.

This system will send event messages and periodic reports to NetApp
Technical
Support. To disable this feature, enter
autosupport modify -support disable
within 24 hours.

Enabling AutoSupport can significantly speed problem determination
and
resolution, should a problem occur on your system.
For further information on AutoSupport, see:
http://support.netapp.com/autosupport/

Type yes to confirm and continue {yes}: yes
```

```
Enter the node management interface port [e0M]: 172.17.8.93

172.17.8.93 is not a valid port.

The physical port that is connected to the node management network.
Examples of
node management ports are "e4a" or "e0M".

You can type "back", "exit", or "help" at any question.


Enter the node management interface port [e0M]:
Enter the node management interface IP address: 172.17.8.93
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 172.17.8.93
has been created.

Use your web browser to complete cluster setup by accessing
https://172.17.8.93

Otherwise, press Enter to complete cluster setup using the command
line
interface:


Do you want to create a new cluster or join an existing cluster?
{create, join}:
join


Existing cluster interface configuration found:

Port    MTU     IP              Netmask
e0c     9000    169.254.148.217 255.255.0.0
e0d     9000    169.254.144.238 255.255.0.0

Do you want to use this configuration? {yes, no} [yes]: yes
.
.
.
```

b. 2 つ目の新しい MetroCluster IP ノード（ node_A_1 の新しいノード）を既存の MetroCluster IP 構成に追加します。

2. 同じ手順を繰り返して、 node_B_1 の新規クラスタ B に node_B_2 を追加します

クラスタ間 LIF の設定、 MetroCluster インターフェイスの作成、およびルートアグリゲートのミラーリングを行います

クラスタピア LIF を作成し、新しい MetroCluster IP ノードに MetroCluster インターフェイスを作成する必要があります。

このタスクについて

- この例で使用しているホームポートはプラットフォーム固有です。MetroCluster IPノードプラットフォームに固有のホームポートを使用する必要があります。
- このタスクを実行する前に、の情報を確認してください 新しいDRグループを追加する際のVLANに関する考慮事項 。

手順

1. 新しい MetroCluster IP ノードで、次の手順に従ってクラスタ間 LIF を設定します。

   "専用ポートでのクラスタ間 LIF の設定"

   "共有データポートでのクラスタ間 LIF の設定"

2. 各サイトで、クラスタピアリングが設定されていることを確認します。

   cluster peer show

   次の例は、 cluster_A のクラスタピアリング設定を示しています。

   ```
   cluster_A:> cluster peer show
   Peer Cluster Name         Cluster Serial Number Availability
   Authentication
   ------------------------- --------------------- --------------
   --------------
   cluster_B                 1-80-000011           Available      ok
   ```

   次の例は、 cluster_B でのクラスタピアリング設定を示しています。

   ```
   cluster_B:> cluster peer show
   Peer Cluster Name         Cluster Serial Number Availability
   Authentication
   ------------------------- --------------------- --------------
   --------------
   cluster_A                 1-80-000011           Available      ok
   cluster_B::>
   ```

3. MetroCluster IP ノードの DR グループを作成します。

   MetroCluster 構成設定 dr-group create -partner-cluster

   MetroCluster の設定と接続の詳細については、次のトピックを参照してください。

"MetroCluster IP 構成に関する考慮事項"

"DR グループを作成します"

```
cluster_A::> metrocluster configuration-settings dr-group create
-partner-cluster
cluster_B -local-node node_A_1-new -remote-node node_B_1-new
[Job 259] Job succeeded: DR Group Create is successful.
cluster_A::>
```

4. DR グループが作成されたことを確認します。

「 MetroCluster configurion-settings dr-group show 」を参照してください

```
cluster_A::> metrocluster configuration-settings dr-group show

DR Group ID Cluster                    Node               DR Partner
Node
----------- -------------------------- ------------------
------------------
1           cluster_A
                                       node_A_1-old        node_B_1-old
                                       node_A_2-old        node_B_2-old
            cluster_B
                                       node_B_1-old        node_A_1-old
                                       node_B_2-old        node_A_2-old
2           cluster_A
                                       node_A_1-new        node_B_1-new
                                       node_A_2-new        node_B_2-new
            cluster_B
                                       node_B_1-new        node_A_1-new
                                       node_B_2-new        node_A_2-new
8 entries were displayed.

cluster_A::>
```

5. 新しく参加した MetroCluster IP ノードの MetroCluster IP 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。
- 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）を指定できます `-vlan-id metrocluster configuration-settings interface create` 。サポートされるプラットフォームの情報については、を参照してください 新しいDRグループを追加する際のVLANに関する考慮事項 。
- どちらのクラスタからも MetroCluster IP インターフェイスを設定できます。

MetroCluster 構成設定インターフェイス create-cluster-name

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_1-new -home-port e1a -address
172.17.26.10 -netmask 255.255.255.0
[Job 260] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_1-new -home-port e1b -address
172.17.27.10 -netmask 255.255.255.0
[Job 261] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_2-new -home-port e1a -address
172.17.26.11 -netmask 255.255.255.0
[Job 262] Job succeeded: Interface Create is successful.

cluster_A::> :metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_2-new -home-port e1b -address
172.17.27.11 -netmask 255.255.255.0
[Job 263] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_1-new -home-port e1a -address
172.17.26.12 -netmask 255.255.255.0
[Job 264] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_1-new -home-port e1b -address
172.17.27.12 -netmask 255.255.255.0
[Job 265] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_2-new -home-port e1a -address
172.17.26.13 -netmask 255.255.255.0
[Job 266] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_2-new -home-port e1b -address
172.17.27.13 -netmask 255.255.255.0
[Job 267] Job succeeded: Interface Create is successful.
```

6. MetroCluster IP インターフェイスが作成されたことを確認します。

「 MetroCluster configurion-settings interface show 」を参照してください

```
cluster_A::>metrocluster configuration-settings interface show
```

```
DR
Config
Group Cluster Node    Network Address Netmask         Gateway
State
----- ------- ------- --------------- --------------- ---------------
---------
1     cluster_A
             node_A_1-old
                 Home Port: e1a
                      172.17.26.10    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.10    255.255.255.0   -
completed
              node_A_2-old
                 Home Port: e1a
                      172.17.26.11    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.11    255.255.255.0   -
completed
      cluster_B
             node_B_1-old
                 Home Port: e1a
                      172.17.26.13    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.13    255.255.255.0   -
completed
              node_B_1-old
                 Home Port: e1a
                      172.17.26.12    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.12    255.255.255.0   -
completed
2     cluster_A
             node_A_3-new
                 Home Port: e1a
                      172.17.28.10    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.29.10    255.255.255.0   -
completed
              node_A_3-new
```

```
                  Home Port: e1a
                       172.17.28.11    255.255.255.0   -
completed
                  Home Port: e1b
                       172.17.29.11    255.255.255.0   -
completed
      cluster_B
             node_B_3-new
                  Home Port: e1a
                       172.17.28.13    255.255.255.0   -
completed
                  Home Port: e1b
                       172.17.29.13    255.255.255.0   -
completed
              node_B_3-new
                  Home Port: e1a
                       172.17.28.12    255.255.255.0   -
completed
                  Home Port: e1b
                       172.17.29.12    255.255.255.0   -
completed
8 entries were displayed.

cluster_A>
```

7. MetroCluster IP インターフェイスを接続します。

   MetroCluster 構成設定接続接続

   このコマンドの実行には数分かかることがあります。

```
cluster_A::> metrocluster configuration-settings connection connect

cluster_A::>
```

8. 接続が正しく確立されていることを確認します MetroCluster configurion-settings connection show

```
cluster_A::> metrocluster configuration-settings connection show

DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
```

```
1     cluster_A
              node_A_1-old
                 Home Port: e1a
                      172.17.28.10    172.17.28.11    HA Partner
completed
                 Home Port: e1a
                      172.17.28.10    172.17.28.12    DR Partner
completed
                 Home Port: e1a
                      172.17.28.10    172.17.28.13    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.29.10    172.17.29.11    HA Partner
completed
                 Home Port: e1b
                      172.17.29.10    172.17.29.12    DR Partner
completed
                 Home Port: e1b
                      172.17.29.10    172.17.29.13    DR Auxiliary
completed
              node_A_2-old
                 Home Port: e1a
                      172.17.28.11    172.17.28.10    HA Partner
completed
                 Home Port: e1a
                      172.17.28.11    172.17.28.13    DR Partner
completed
                 Home Port: e1a
                      172.17.28.11    172.17.28.12    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.29.11    172.17.29.10    HA Partner
completed
                 Home Port: e1b
                      172.17.29.11    172.17.29.13    DR Partner
completed
                 Home Port: e1b
                      172.17.29.11    172.17.29.12    DR Auxiliary
completed

DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
1     cluster_B
```

```
              node_B_2-old
                 Home Port: e1a
                      172.17.28.13    172.17.28.12    HA Partner
completed
                 Home Port: e1a
                      172.17.28.13    172.17.28.11    DR Partner
completed
                 Home Port: e1a
                      172.17.28.13    172.17.28.10    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.29.13    172.17.29.12    HA Partner
completed
                 Home Port: e1b
                      172.17.29.13    172.17.29.11    DR Partner
completed
                 Home Port: e1b
                      172.17.29.13    172.17.29.10    DR Auxiliary
completed
              node_B_1-old
                 Home Port: e1a
                      172.17.28.12    172.17.28.13    HA Partner
completed
                 Home Port: e1a
                      172.17.28.12    172.17.28.10    DR Partner
completed
                 Home Port: e1a
                      172.17.28.12    172.17.28.11    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.29.12    172.17.29.13    HA Partner
completed
                 Home Port: e1b
                      172.17.29.12    172.17.29.10    DR Partner
completed
                 Home Port: e1b
                      172.17.29.12    172.17.29.11    DR Auxiliary
completed

DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
2     cluster_A
              node_A_1-new**
```

```
                 Home Port: e1a
                      172.17.26.10    172.17.26.11    HA Partner
completed
                 Home Port: e1a
                      172.17.26.10    172.17.26.12    DR Partner
completed
                 Home Port: e1a
                      172.17.26.10    172.17.26.13    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.27.10    172.17.27.11    HA Partner
completed
                 Home Port: e1b
                      172.17.27.10    172.17.27.12    DR Partner
completed
                 Home Port: e1b
                      172.17.27.10    172.17.27.13    DR Auxiliary
completed
              node_A_2-new
                 Home Port: e1a
                      172.17.26.11    172.17.26.10    HA Partner
completed
                 Home Port: e1a
                      172.17.26.11    172.17.26.13    DR Partner
completed
                 Home Port: e1a
                      172.17.26.11    172.17.26.12    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.27.11    172.17.27.10    HA Partner
completed
                 Home Port: e1b
                      172.17.27.11    172.17.27.13    DR Partner
completed
                 Home Port: e1b
                      172.17.27.11    172.17.27.12    DR Auxiliary
completed

DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
2     cluster_B
              node_B_2-new
                 Home Port: e1a
```

```
                    172.17.26.13    172.17.26.12    HA Partner
completed
                Home Port: e1a
                    172.17.26.13    172.17.26.11    DR Partner
completed
                Home Port: e1a
                    172.17.26.13    172.17.26.10    DR Auxiliary
completed
                Home Port: e1b
                    172.17.27.13    172.17.27.12    HA Partner
completed
                Home Port: e1b
                    172.17.27.13    172.17.27.11    DR Partner
completed
                Home Port: e1b
                    172.17.27.13    172.17.27.10    DR Auxiliary
completed
            node_B_1-new
                Home Port: e1a
                    172.17.26.12    172.17.26.13    HA Partner
completed
                Home Port: e1a
                    172.17.26.12    172.17.26.10    DR Partner
completed
                Home Port: e1a
                    172.17.26.12    172.17.26.11    DR Auxiliary
completed
                Home Port: e1b
                    172.17.27.12    172.17.27.13    HA Partner
completed
                Home Port: e1b
                    172.17.27.12    172.17.27.10    DR Partner
completed
                Home Port: e1b
                    172.17.27.12    172.17.27.11    DR Auxiliary
completed
48 entries were displayed.

cluster_A::>
```

9. ディスクの自動割り当てとパーティショニングを確認します。

   「 Disk show -pool Pool1 」

```
cluster_A::> disk show -pool Pool1
                     Usable           Disk    Container   Container
Disk                   Size Shelf Bay Type    Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
1.10.4                    -    10   4 SAS     remote      -
node_B_2
1.10.13                   -    10  13 SAS     remote      -
node_B_2
1.10.14                   -    10  14 SAS     remote      -
node_B_1
1.10.15                   -    10  15 SAS     remote      -
node_B_1
1.10.16                   -    10  16 SAS     remote      -
node_B_1
1.10.18                   -    10  18 SAS     remote      -
node_B_2
...
2.20.0                546.9GB    20   0 SAS     aggregate   aggr0_rha1_a1
node_a_1
2.20.3                546.9GB    20   3 SAS     aggregate   aggr0_rha1_a2
node_a_2
2.20.5                546.9GB    20   5 SAS     aggregate   rha1_a1_aggr1
node_a_1
2.20.6                546.9GB    20   6 SAS     aggregate   rha1_a1_aggr1
node_a_1
2.20.7                546.9GB    20   7 SAS     aggregate   rha1_a2_aggr1
node_a_2
2.20.10               546.9GB    20  10 SAS     aggregate   rha1_a1_aggr1
node_a_1
...
43 entries were displayed.

cluster_A::>
```

10. ルートアグリゲートをミラーします。

「 storage aggregate mirror -aggregate aggr0_cluster1_01 -new 」という名前のアグリゲートが作成されます

この手順は MetroCluster IP ノードごとに実行する必要があります。

```
cluster_A::> aggr mirror -aggregate aggr0_node_A_1-new

Info: Disks would be added to aggregate "aggr0_node_A_1-new"on node
"node_A_1-new"
      in the following manner:

      Second Plex

        RAID Group rg0, 3 disks (block checksum, raid_dp)
                                                                  Usable
Physical
          Position   Disk                      Type           Size
Size
          ---------- ------------------------- ---------- --------
--------
          dparity    4.20.0                    SAS               -
-
          parity     4.20.3                    SAS               -
-
          data       4.20.1                    SAS         546.9GB
558.9GB

      Aggregate capacity available forvolume use would be 467.6GB.

Do you want to continue? {y|n}: y

cluster_A::>
```

11. ルートアグリゲートがミラーされたことを確認します。

「 storage aggregate show

```
cluster_A::> aggr show

Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
aggr0_node_A_1-old
           349.0GB   16.84GB   95% online       1 node_A_1-old
raid_dp,

mirrored,

normal
```

```
aggr0_node_A_2-old
           349.0GB   16.84GB   95% online       1 node_A_2-old
raid_dp,

mirrored,

normal
aggr0_node_A_1-new
           467.6GB   22.63GB   95% online       1 node_A_1-new
raid_dp,

mirrored,

normal
aggr0_node_A_2-new
           467.6GB   22.62GB   95% online       1 node_A_2-new
raid_dp,

mirrored,

normal
aggr_data_a1
            1.02TB    1.01TB    1% online       1 node_A_1-old
raid_dp,

mirrored,

normal
aggr_data_a2
            1.02TB    1.01TB    1% online       1 node_A_2-old
raid_dp,

mirrored,
```

新しいノードの追加を完了しています

新しい DR グループを MetroCluster 構成に組み込み、新しいノードにミラーされたデータアグリゲートを作成する必要があります。

手順

1. MetroCluster 構成を更新します。

   a. advanced 権限モードに切り替えます。

      「 advanced 」の権限が必要です

b. 新しく追加されたノードのいずれかでMetroCluster構成を更新します。

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、次のコマンドを実行します。 `metrocluster configure <node-name>`
ミラーされた1つのデータアグリゲートを一方または両方のサイトに配置	いずれかのノードのプロンプトで、 `-allow-with-one-aggregate true` パラメータを使用してMetroClusterを設定します。 `metrocluster configure -allow-with-one-aggregate true <node-name>`

c. 新しい各ノードをリブートします。

```
node reboot -node <node_name> -inhibit-takeover true
```

ノードを特定の順序でリブートする必要はありませんが、1つのノードが完全にブートしてすべての接続が確立されるまで待ってから、次のノードをリブートしてください。

a. admin 権限モードに戻ります。

「特権管理者」

2. 新しい MetroCluster ノードのそれぞれで、ミラーされたデータアグリゲートを作成します。

```
storage aggregate create -aggregate <aggregate-name> -node <node-name>
-diskcount <no-of-disks> -mirror true
```

- ミラーされたデータアグリゲートをサイトごとに少なくとも1つ作成する必要があります。MDVボリュームをホストするために、サイトごとに2つのミラーされたデータアグリゲートをMetroCluster IPノード上に配置することを推奨しますが、サイトごとに1つのアグリゲートがサポートされます（ただし推奨されません）。MetroClusterの一方のサイトにミラーされたデータアグリゲートが1つあり、もう一方のサイトに複数のミラーされたデータアグリゲートがあります。
- 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。

次の例は、 node_A_1 で新しいアグリゲートを作成します。

```
cluster_A::> storage aggregate create -aggregate data_a3 -node node_A_1-
new -diskcount 10 -mirror t

Info: The layout for aggregate "data_a3" on node "node_A_1-new" would
be:
```

```
      First Plex

        RAID Group rg0, 5 disks (block checksum, raid_dp)
                                                                  Usable
Physical
          Position   Disk                      Type           Size
Size
          ---------- ------------------------- ---------- --------
--------
          dparity    5.10.15                   SAS               -
-
          parity     5.10.16                   SAS               -
-
          data       5.10.17                   SAS         546.9GB
547.1GB
          data       5.10.18                   SAS         546.9GB
558.9GB
          data       5.10.19                   SAS         546.9GB
558.9GB

      Second Plex

        RAID Group rg0, 5 disks (block checksum, raid_dp)
                                                                  Usable
Physical
          Position   Disk                      Type           Size
Size
          ---------- ------------------------- ---------- --------
--------
          dparity    4.20.17                   SAS               -
-
          parity     4.20.14                   SAS               -
-
          data       4.20.18                   SAS         546.9GB
547.1GB
          data       4.20.19                   SAS         546.9GB
547.1GB
          data       4.20.16                   SAS         546.9GB
547.1GB

      Aggregate capacity available for volume use would be 1.37TB.

Do you want to continue? {y|n}: y
[Job 440] Job succeeded: DONE

cluster_A::>
```

3. ノードが DR グループに追加されたことを確認します。

```
cluster_A::*> metrocluster node show

DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
              node_A_1-old        configured     enabled   normal
              node_A_2-old        configured     enabled   normal
      cluster_B
              node_B_1-old        configured     enabled   normal
              node_B_2-old        configured     enabled   normal
2     cluster_A
              node_A_3-new        configured     enabled   normal
              node_A_4-new        configured     enabled   normal
      cluster_B
              node_B_3-new        configured     enabled   normal
              node_B_4-new        configured     enabled   normal
8 entries were displayed.

cluster_A::*>
```

4. MDV_CRSボリュームをadvanced権限モードで移動します。

   a. ボリュームを表示して MDV ボリュームを特定します。

      各サイトにミラーされたデータアグリゲートが 1 つある場合、両方の MDV ボリュームをこの 1 つのアグリゲートに移動します。ミラーされたデータアグリゲートが 2 つ以上ある場合、各 MDV ボリュームを別々のアグリゲートに移動します。

      4ノードMetroCluster構成を永続的な8ノード構成に拡張する場合は、MDVボリュームの1つを新しいDRグループに移動する必要があります。

      次に 'volume show 出力の MDV ボリュームの例を示します

```
cluster_A::> volume show
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
...

cluster_A   MDV_CRS_2c78e009ff5611e9b0f300a0985ef8c4_A
                       aggr_b1      -          RW            -
-     -
cluster_A   MDV_CRS_2c78e009ff5611e9b0f300a0985ef8c4_B
                       aggr_b2      -          RW            -
-     -
cluster_A   MDV_CRS_d6b0b313ff5611e9837100a098544e51_A
                       aggr_a1      online     RW         10GB
9.50GB    0%
cluster_A   MDV_CRS_d6b0b313ff5611e9837100a098544e51_B
                       aggr_a2      online     RW         10GB
9.50GB    0%
...
11 entries were displayed.mple
```

b. advanced 権限レベルを設定します。

「 advanced 」の権限が必要です

c. MDV ボリュームを 1 つずつ移動します。

```
volume move start -volume <mdv-volume> -destination-aggregate <aggr-on-new-
node> -vserver <svm-name>
```

次の例は、「 MDV_CRS_d6b0b313ff5611e9837100a098544e51_a 」を「 node_A_1 」のアグリゲート「 node_A_1 」に移動するコマンドと出力を示しています。

```
cluster_A::*> vol move start -volume
MDV_CRS_d6b0b313ff5611e9837100a098544e51_A -destination-aggregate
data_a3 -vserver cluster_A

Warning: You are about to modify the system volume
         "MDV_CRS_d6b0b313ff5611e9837100a098544e51_A". This might
cause severe
         performance or stability problems. Do not proceed unless
directed to
         do so by support. Do you want to proceed? {y|n}: y
[Job 494] Job is queued: Move
"MDV_CRS_d6b0b313ff5611e9837100a098544e51_A" in Vserver "cluster_A"
to aggregate "data_a3". Use the "volume move show -vserver cluster_A
-volume MDV_CRS_d6b0b313ff5611e9837100a098544e51_A" command to view
the status of this operation.
```

d. volume show コマンドを使用して、 MDV ボリュームが正常に移動されたことを確認します。

```
volume show <mdv-name>
```

次の出力は、 MDV ボリュームが移動されたことを示しています。

```
cluster_A::*> vol show MDV_CRS_d6b0b313ff5611e9837100a098544e51_B
Vserver     Volume       Aggregate    State      Type       Size
Available Used%
---------   ------------ ------------ ---------- ---- ----------
---------- -----
cluster_A   MDV_CRS_d6b0b313ff5611e9837100a098544e51_B
                       aggr_a2      online     RW         10GB
9.50GB    0%
```

5. 古いノードから新しいノードにイプシロンを移動します。

a. 現在イプシロンが設定されているノードを特定します。

cluster show -fields epsilon

```
cluster_B::*> cluster show -fields epsilon
node              epsilon
----------------- -------
node_A_1-old       true
node_A_2-old       false
node_A_3-new       false
node_A_4-new       false
4 entries were displayed.
```

b. 古いノード（ node_A_1 古い）でイプシロンを false に設定します。

```
cluster modify -node <old-node> -epsilon false*
```

c. 新しいノード（ node_A_1 ）でイプシロンを true に設定します。

```
cluster modify -node <new-node> -epsilon true
```

d. イプシロンが正しいノードに移動されたことを確認します。

cluster show -fields epsilon

```
cluster_A::*> cluster show -fields epsilon
node              epsilon
----------------- -------
node_A_1-old       false
node_A_2-old       false
node_A_3-new       true
node_A_4-new       false
4 entries were displayed.
```

6. システムでエンドツーエンドの暗号化がサポートされている場合は、次の操作を実行できます。 "エンドツーエンドの暗号化を実現" 新しいDRグループ。

MetroCluster構成からDRグループを削除する

ONTAP 9.8 以降では、8 ノードMetroCluster構成からディザスタ リカバリ (DR) グループを削除して、4 ノードMetroCluster構成を作成できます。

これらの手順は、移行およびシステム更新のワークフロー中に使用します。

コンソールログを有効にする

NetAppでは、使用しているデバイスでコンソールロギングをイネーブルにし、この手順を実行する際に次のアクションを実行することを強く推奨します。

- メンテナンス中はAutoSupportを有効のままにします。
- メンテナンスの前後にメンテナンスAutoSupportメッセージをトリガーして、メンテナンスアクティビティ中にケースの作成を無効にします。

  ナレッジベースの記事を参照してください "スケジュールされたメンテナンス時間中にケースの自動作成を停止する方法"。

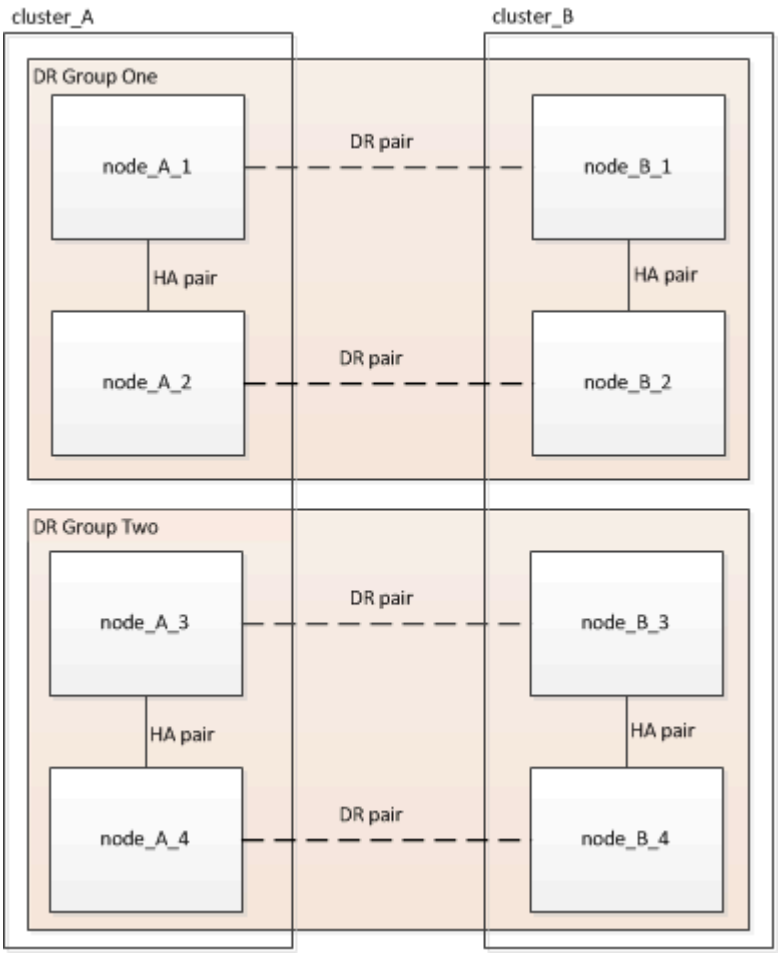
- 任意のCLIセッションのセッションロギングをイネーブルにします。セッションログを有効にする方法については、ナレッジベースの記事の「セッション出力のログ」セクションを参照してください "ONTAPシステムへの接続を最適化するためのPuTTYの設定方法"。

各クラスタからDRグループノードを削除します

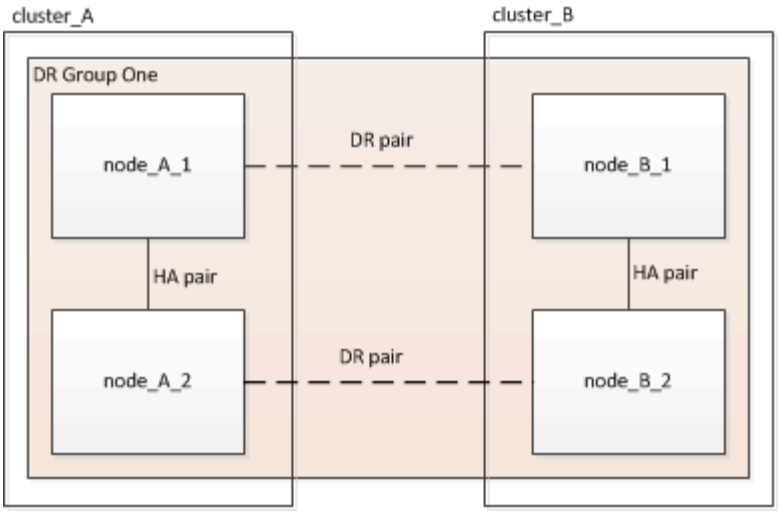
この手順は、 ONTAP 9.8 以降でサポートされています。 ONTAP 9.7 以前を実行しているシステムの場合は、次のナレッジベースの記事を参照してください。"MetroCluster 構成からDRグループを削除する方法" 。

このタスクについて

8 ノード構成では、 8 つのノードが 2 つの 4 ノード DR グループとして編成されています。



DR グループを削除すると、構成内に 4 つのノードが残ります。



作業を開始する前に

- この手順は両方のクラスタで実行する必要があります。
- 「 MetroCluster remove-dr-group 」コマンドは、 ONTAP 9.8 以降でのみサポートされます。

手順

1. まだ DR グループを削除していない場合は、削除する準備をします。

   a. すべてのデータボリュームを別の DR グループに移動します。

   b. 削除する DR グループに負荷共有ミラー ボリュームがある場合は、別の DR グループにすべての負荷共有ミラー ボリュームを再作成し、削除する DR グループからそれらを削除します。

   c. の手順に従って、すべてのMDV_CRSメタデータボリュームを別のDRグループに移動します "MetroCluster 構成でのメタデータボリュームの移動" 手順

   d. 削除する DR グループにある MDV_AUD メタデータボリュームをすべて削除してください。

   e. 削除する DR グループ内のすべてのデータ集約を削除します。

```
ClusterA::> storage aggregate show -node ClusterA-01, ClusterA-02
-fields aggregate ,node
ClusterA::> aggr delete -aggregate aggregate_name
ClusterB::> storage aggregate show -node ClusterB-01, ClusterB-02
-fields aggregate ,node
ClusterB::> aggr delete -aggregate aggregate_name
```

   ルートアグリゲートは削除されません。

   f. NFS および CIFS (SMB) に使用するすべての NAS データ LIF を別の DR グループ内のホーム ノードに移行します。+

```
network interface show -home-node <old_node>

network interface migrate -vserver <svm_name> -lif <data_lif> -destination
-node <new_node> -destination-port <port>
```

g. データ LIF を別の DR グループ内の新しいホーム ノードに移動します。
`network interface modify -vserver <svm-name> -lif <data-lif> -home-node <new_node> -home-port <port>`

h. クラスタ管理 LIF を別の DR グループのホームノードに移行する。

network interface show -role cluster-mgmt-`

`network interface modify -vserver <svm-name> -lif <cluster_mgmt> -home-node <new_node> -home-port <port-id>`

> ◦ ノード管理LIFとクラスタ間LIFは移行されません。必要に応じて、DR グループのノードに新しいノード管理 LIF とクラスタ間 LIF を作成します。
> ◦ ブロック アクセス (SAN) に使用される FCP インターフェイスをノード間で移行または移動することはできません。必要に応じて新しい FCP インターフェイスを作成します。
> ◦ ホーム ノードとホーム ポートを更新する前に、iSCSI SAN LIF を停止する必要があります。

a. 必要に応じて、別の DR グループ内のノードにイプシロンを移動します。

```
ClusterA::> set advanced
ClusterA::*> cluster show
Move epsilon if needed
ClusterA::*> cluster modify -node nodename -epsilon false
ClusterA::*> cluster modify -node nodename -epsilon true

ClusterB::> set advanced
ClusterB::*> cluster show
ClusterB::*> cluster modify -node nodename -epsilon false
ClusterB::*> cluster modify -node nodename -epsilon true
ClusterB::*> set admin
```

2. DR グループを特定して削除します。

a. 削除する適切な DR グループを特定します。

MetroCluster node show

b. DR グループノードを削除します。 +dr-dr MetroCluster -group-dr -group-id 1'

次の例は、 cluster_A の DR グループ構成を削除します

例

```
cluster_A::*>

Warning: Nodes in the DR group that are removed from the
MetroCluster
         configuration will lose their disaster recovery protection.

         Local nodes "node_A_1-FC, node_A_2-FC"will be removed from
the
         MetroCluster configuration. You must repeat the operation
on the
         partner cluster "cluster_B"to remove the remote nodes in
the DR group.
Do you want to continue? {y|n}: y

Info: The following preparation steps must be completed on the local
and partner
      clusters before removing a DR group.

      1. Move all data volumes to another DR group.
      2. Move all MDV_CRS metadata volumes to another DR group.
      3. Delete all MDV_aud metadata volumes that may exist in the
DR group to
      be removed.
      4. Delete all data aggregates in the DR group to be removed.
Root
      aggregates are not deleted.
      5. Migrate all data LIFs to home nodes in another DR group.
      6. Migrate the cluster management LIF to a home node in
another DR group.
      Node management and inter-cluster LIFs are not migrated.
      7. Transfer epsilon to a node in another DR group.

      The command is vetoed if the preparation steps are not
completed on the
      local and partner clusters.
Do you want to continue? {y|n}: y
[Job 513] Job succeeded: Remove DR Group is successful.

cluster_A::*>
```

3. パートナークラスタで同じ手順を繰り返します。
4. 古い DR グループのノードでストレージ フェイルオーバーを無効にします。

```
storage failover modify -node <node-name> -enable false
```

5. MetroCluster IP 構成の場合は、次の手順を実行して、ルート アグリゲートのリモート プレックスを削除し、古い DR グループのノード上のディスク所有権を削除します。

   これらの手順は、各サイトの HA ペアの両方のノードに対して実行する必要があります。

   a. 削除する DR グループ内のノード上のルート アグリゲートのリモート プレックスを表示します。

      ```
      storage aggregate plex show -aggregate <root_aggr_name> -pool 1
      ```

   b. リモート プレックスを削除します。

      ```
      storage aggregate plex delete -aggregate <root_aggr_name> -plex
      <plex_from_previous_step>
      ```

   c. DR グループ内のノードが所有するリモート ディスクを識別します。

      使用するコマンドは、パーティション/共有ディスクを使用しているか、ディスク全体を使用しているかによって異なります。

      > カンマ区切りのリストを使用してください `-owner <node_names>`削除する DR グループ内のノード名を指定するフィールド。

      パーティション/共有ディスク:

      i. 権限レベルを advanced に設定します。

         「高度」

      ii. リモート ディスクを表示します。

         ```
         storage disk show -pool Pool1 -owner <node_names> -partition
         -ownership
         ```

      ディスク全体:

      i. 権限レベルを advanced に設定します。

         「高度」

      ii. リモート ディスクを表示します。

         ```
         storage disk show -pool Pool1 -owner <node_names>
         ```

   d. ディスクの自動割り当てを無効にする:

      ```
      disk option modify -node <node_names_in_the_DR_group_to_be_deleted>
      -autoassign off
      ```

   e. 削除する各 DR グループ ノード上の pool1 ディスクの所有権を削除します。削除する各ノードに対し

てこれらの手順を実行します。

i. ノードシェルに移動します。

```
run -node <node_name>
```

ii. pool1 ディスクを識別します。

```
aggr status -s
```

ノードが所有するプール 0 およびプール 1 スペア ディスクを含むすべてのスペア ディスクが表示されます。

i. 各プール1スペアディスクのディスク所有権を削除します。

```
disk remove_ownership <disk_name>
```

パーティション化されたディスクの場合は、パーティションの所有権を削除してから、コンテナ ディスクの所有権を削除します。

6. MetroCluster IP 構成の場合は、古い DR グループのノード上のMetroCluster接続を削除します。

これらのコマンドはどちらのクラスターからも発行でき、両方のクラスターにまたがる DR グループ全体に適用されます。

a. 接続を切断します。

```
metrocluster configuration-settings connection disconnect -dr-group-id
<dr_group_id>
```

例

```
cluster_A::*> metrocluster configuration-settings connection
disconnect -dr-group-id 1

Warning: For the nodes in the DR group 1, this command will
remove the existing connections that are used to mirror NV logs
and access remote storage.
Do you want to continue? {y|n}: y

Warning: Before proceeding with disconnect, you must verify the
following:
      1. Unmirrored aggregates do not have disks in remote
plexes.
      2. Aggregates are not mirrored.
      3. No disks are assigned in Pool1.
      4. Storage failover is not enabled.
      Follow the "MetroCluster Installation and Configuration
guide" for detailed instructions to verify this.
Do you want to continue? {y|n}: y
```

b. 古い DR グループのノード上の MetroCluster インターフェイスを削除します。



この手順は、DR グループの各ノードで繰り返す必要があります。

MetroCluster 構成設定インタフェースは削除されます

a. 古い DR グループの構成を削除します。+ MetroCluster 構成設定 DR-group delete

7. 古い DR グループからノードを分離

各クラスターでこの手順を実行します。

a. advanced 権限レベルを設定します。

「 advanced 」の権限が必要です

b. ノードを切断:
`cluster unjoin -node <node-name>`

古い DR グループ内のもう一方のローカルノードに対して、この手順を繰り返します。

c. 権限レベルをadminに設定します。

「特権管理者」

8. 新しい DR グループでクラスター HA が有効になっていることを確認します。必要に応じて、クラスター

HA を再度有効にします。

cluster ha modify -configured true

各クラスターでこの手順を実行します。

9. 古いコントローラモジュールとストレージシェルフを停止、電源オフ、および取り外します。

追加情報の参照先

MetroCluster の設定と処理の詳細については、を参照してください。

MetroCluster およびその他の情報

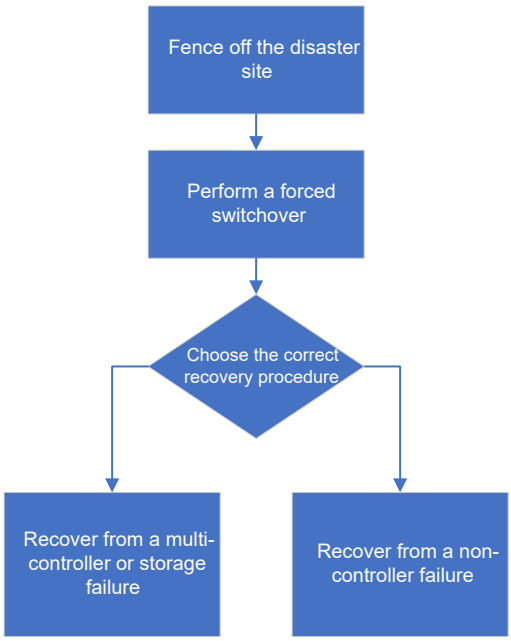
情報	件名
"MetroCluster のドキュメント"	• すべての MetroCluster 情報
"ファブリック接続 MetroCluster のインストールと設定"	• ファブリック接続 MetroCluster アーキテクチャ • 構成のケーブル接続 • FC-to-SAS ブリッジの設定 • FC スイッチを設定します • ONTAP で MetroCluster を設定します
"ストレッチ MetroCluster のインストールと設定"	• ストレッチ MetroCluster アーキテクチャ • 構成のケーブル接続 • FC-to-SAS ブリッジの設定 • ONTAP で MetroCluster を設定します
"MetroCluster の管理とディザスタリカバリ"	• MetroCluster 構成について • スイッチオーバー、修復、スイッチバック • ディザスタリカバリ

"MetroCluster コンポーネントの保守"	• MetroCluster FC 構成のメンテナンスガイドライン • 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 • ファブリック接続またはストレッチ MetroCluster FC 構成でのディスクシェルフのホットアド • ファブリック接続またはストレッチ MetroCluster FC 構成でのディスクシェルフのホットリムーブ • ファブリック接続またはストレッチ MetroCluster FC 構成のディザスタサイトでのハードウェア交換 • 2 ノードのファブリック接続またはストレッチ MetroCluster FC 構成の 4 ノード MetroCluster 構成への拡張 • 4 ノードのファブリック接続またはストレッチ MetroCluster FC 構成の 8 ノード MetroCluster FC 構成への拡張
"MetroCluster のアップグレード、移行、拡張"	• MetroCluster 設定をアップグレードまたは更新する • MetroCluster FC 構成から MetroCluster IP 構成への移行 • ノードの追加による MetroCluster 構成の拡張
"MetroCluster Tiebreaker ソフトウェアのインストールおよび設定"	• MetroCluster Tiebreaker ソフトウェアを使用して MetroCluster 構成を監視する
"ONTAPハードウェアシステムのドキュメント" ストレージシェルフの標準的なメンテナンス手順を MetroCluster IP 構成で使用できます。	• ディスクシェルフのホットアド • ディスクシェルフのホットリムーブ
"コピーベースの移行"	• 7-Mode ストレージシステムから clustered Data ONTAP ストレージシステムへデータを移行する
"ONTAP の概念"	• ミラーされたアグリゲートの機能

災害からリカバリします

ディザスタリカバリのワークフロー

ワークフローを使用してディザスタリカバリを実行します。



災害後の強制スイッチオーバーの実行

災害が発生した場合にデータサービスを安全に継続できるようにするには、スイッチオーバー後にディザスタクラスタとサバイバークラスタの両方でいくつかの手順を実行する必要があります。

災害が発生したかどうかを次の方法で確認します。

- 管理者
- MetroCluster Tiebreaker ソフトウェア（設定されている場合）
- ONTAP メディエーターソフトウェアが設定されている場合は

ディザスタサイトのフェンシング

災害後にディザスタサイトノードの交換が必要となった場合は、サイトがサービスを再開しないようにノードを停止する必要があります。そうしないと、交換用手順が完了する前にクライアントがノードへのアクセスを開始した場合に、データが破損するおそれがあります。

ステップ

1. ディザスタサイトでノードを停止して電源をオフのままにするか、 ONTAP をブートするように指示されるまで LOADER プロンプトで待機します。

「 system node halt -node disaster -site -node-name 」のように入力します

ディザスタサイトノードが破損したか停止できない場合は、ノードへの電源をオフにし、リカバリ用手順で指示が出るまで交換用ノードをブートしないでください。

強制スイッチオーバーの実行

スイッチオーバープロセスによって、テスト時とメンテナンス時のノンストップオペレーションが実現するだけでなく、コマンド 1 つでサイト障害からリカバリできます。

作業を開始する前に

- スイッチオーバーを実行する前に、サバイバーサイトの少なくとも1つのノードが稼働している必要があります。
- スイッチバック処理を実行する前に、設定の変更がすべて完了している必要があります。

  これにより、ネゴシエートスイッチオーバーまたはスイッチバックの処理との競合が回避されます。

SnapMirror と SnapVault の設定は自動的に削除されます。

このタスクについて

「 MetroCluster switchover 」コマンドは、 MetroCluster 構成のすべての DR グループのノードを切り替えます。たとえば、 8 ノードの MetroCluster 構成では、両方の DR グループでノードがスイッチオーバーされます。

手順

1. サバイバーサイトで次のコマンドを実行して、スイッチオーバーを実行します。

   MetroCluster switchover -forced-on-disaster true

   処理が完了するまでに数分かかることがあります。進捗状況はを使用して確認できます `metrocluster operation show` コマンドを実行します

2. スイッチオーバーを続行するかどうかを確認するメッセージが表示されたら、回答は y を押します。
3. を実行して、スイッチオーバーが正常に完了したことを確認します `metrocluster operation show` コマンドを実行します

```
mcc1A::> metrocluster operation show
  Operation: switchover
 Start time: 10/4/2012 19:04:13
      State: in-progress
   End time: -
     Errors:

mcc1A::> metrocluster operation show
  Operation: switchover
 Start time: 10/4/2012 19:04:13
      State: successful
   End time: 10/4/2012 19:04:22
     Errors: -
```

スイッチオーバーが拒否された場合は '--override-override-vetoes オプションを指定して MetroCluster switchover -forced-on-disaster true コマンドを再実行できますこのオプションパラメータを使用すると、スイッチオーバーを妨げるソフトな拒否はすべて無視されます。

完了後

スイッチオーバー後に、 SnapMirror 関係を再確立する必要があります。

MetroCluster スイッチオーバー後に storage aggregate plex show コマンドの出力が確定しない

MetroCluster のスイッチオーバー後に「 storage aggregate plex show 」コマンドを実行すると、スイッチオーバーされたルートアグリゲートの plex0 のステータスが確定していないため、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。

スイッチオーバー後に NVFAIL 状態のボリュームにアクセスする場合

スイッチオーバー後に 'volume modify コマンドの -in-nvfailed-state パラメータをリセットし ' クライアントがデータにアクセスする制限を解除することにより 'NVFAIL 状態をクリアする必要があります

作業を開始する前に

データベースまたはファイルシステムが実行されていない、または影響を受けたボリュームにアクセスしようとしていないことが必要です。

このタスクについて

in-nvfailed-state パラメータを設定するには、 advanced 権限が必要です。

ステップ

1. -in-nvfailed-state パラメータを false に設定して volume modify コマンドを実行し ' ボリュームをリカバリします

完了後

データベースファイルの有効性を調べる方法については、ご使用のデータベースソフトウェアのマニュアルを

参照してください。

データベースで LUN が使用されている場合は、 NVRAM 障害後にホストから LUN にアクセスできるようにする手順を確認してください。

関連情報

"NVFAIL を使用したデータベースの有効性監視および保護"

正しいリカバリ手順の選択

MetroCluster 構成で障害が発生した場合は、正しいリカバリ手順を選択する必要があります。次の表と例を使用して、適切なリカバリ手順を選択してください。

次の表に示す情報は、インストールまたは移行が完了していること、つまりが完了していることを前提としています `metrocluster configure` コマンドが実行されました。

ディザスタサイトでの障害の範囲	手順
• ハードウェア障害（停電など）がない	"コントローラ以外の障害からのリカバリ"
• コントローラモジュールの障害はなし • 他のハードウェアで障害が発生した	"コントローラ以外の障害からのリカバリ"
• 1 台のコントローラモジュールの障害またはコントローラモジュール内の FRU コンポーネントの障害 • ドライブは障害状態ではありません	障害が 1 台のコントローラモジュールに限定されている場合は、プラットフォームモデルに対応したコントローラモジュール FRU 交換用手順を使用する必要があります。4 ノードまたは 8 ノードの MetroCluster 構成では、このような障害がローカル HA ペアに分離されます。 • 注： * ドライブやその他のハードウェアに障害が発生していない場合は、コントローラモジュールの FRU 交換用手順を 2 ノード MetroCluster 構成で使用できます。 "ONTAPハードウェアシステムのドキュメント"
• 1 台のコントローラモジュールの障害またはコントローラモジュール内の FRU コンポーネントの障害 • ドライブで障害が発生している	"マルチコントローラまたはストレージの障害からのリカバリ"

• 1 台のコントローラモジュールの障害またはコントローラモジュール内の FRU コンポーネントの障害 • ドライブは障害状態ではありません • コントローラモジュールの外部にあるハードウェアでも障害が発生した	"マルチコントローラまたはストレージの障害からのリカバリ" ドライブ割り当てのすべての手順を省略する必要があります。
• DR グループ内の複数のコントローラモジュールの障害（その他の障害あり、またはなし）	"マルチコントローラまたはストレージの障害からのリカバリ"

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

MetroCluster 構成手順 でのコントローラモジュール障害への対応は、が搭載されているかどうかによって異なります `metrocluster configure` コマンドが完了しました。

- 状況に応じて `metrocluster configure` コマンドがまだ実行されていないか失敗しました。交換用コントローラモジュールを使用して、MetroCluster ソフトウェア設定手順 を最初から再起動する必要があります。

> の手順を必ず実行してください "コントローラモジュールでのシステムデフォルトのリストア" 各コントローラ（交換用コントローラを含む）で、以前の設定が削除されたことを確認します。

- 状況に応じて `metrocluster configure` コマンドが正常に完了し、コントローラモジュールが故障しました。前の表を使用して、正しいリカバリ手順 を特定してください。

MetroCluster FC-to-IP移行時のコントローラモジュールの障害のシナリオ

リカバリ手順は、移行中にサイト障害が発生した場合に使用できます。ただし、この方法を使用できるのは、FC DR グループと IP DR グループの両方が完全に設定された安定した混在構成の場合のみです。「 MetroCluster node show 」コマンドの出力には、 8 つのノードすべてを含む両方の DR グループが表示されます。

> ノードの追加または削除を実行中に移行中に障害が発生した場合は、テクニカルサポートに連絡する必要があります。

8 ノード MetroCluster 構成でのコントローラモジュールの障害のシナリオ

障害シナリオ：

- 1 つの DR グループでの 1 台のコントローラモジュールの障害
- 1 つの DR グループでの 2 台のコントローラモジュールの障害
- 別々の DR グループでの 1 台のコントローラモジュールの障害
- 複数の DR グループにまたがる 3 台のコントローラモジュールの障害

1 つの **DR** グループでの **1** 台のコントローラモジュールの障害

この場合、障害は HA ペアに限定されます。

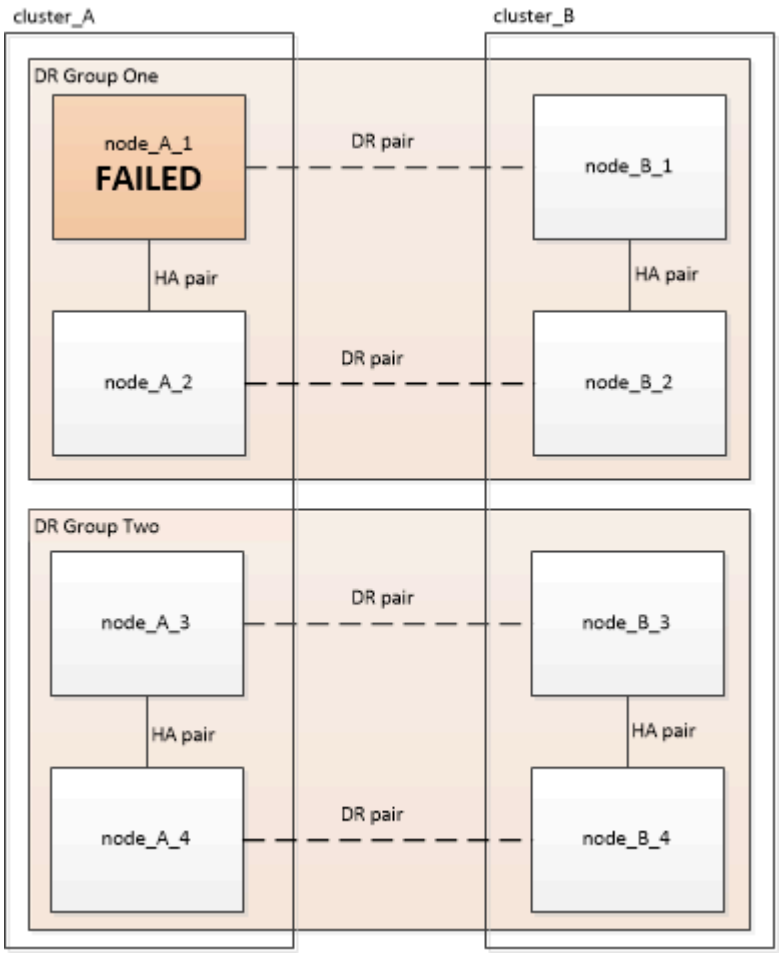
- ストレージを交換する必要がない場合は、プラットフォームモデルに対応したコントローラモジュールの FRU 交換用手順を使用できます。

  "ONTAPハードウェアシステムのドキュメント"

- ストレージの交換が必要な場合は、マルチコントローラモジュールのリカバリ手順を使用できます。

  "マルチコントローラまたはストレージの障害からのリカバリ"

  このシナリオでは、環境の 4 ノード MetroCluster 構成も使用します。

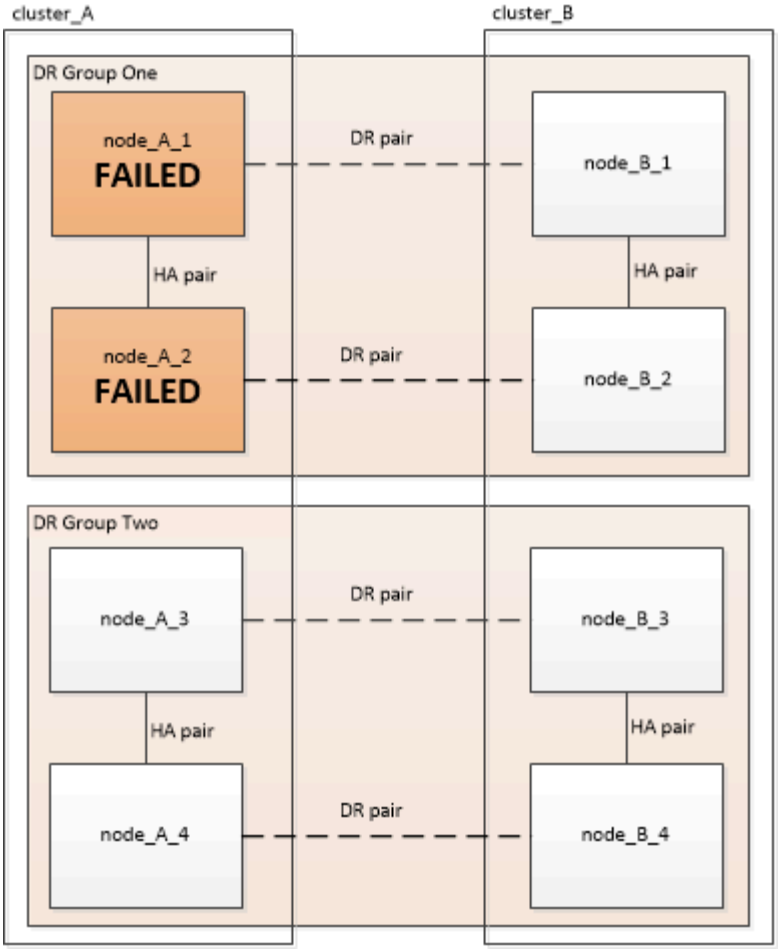


1 つの **DR** グループでの **2** 台のコントローラモジュールの障害

この障害の場合は、スイッチオーバーが必要です。マルチコントローラモジュールの障害からのリカバリ用手順を使用できます。

"マルチコントローラまたはストレージの障害からのリカバリ"

このシナリオでは、環境の 4 ノード MetroCluster 構成も使用します。



別々の **DR** グループでの **1** 台のコントローラモジュールの障害

この場合、障害は個別の HA ペアに限定されます。

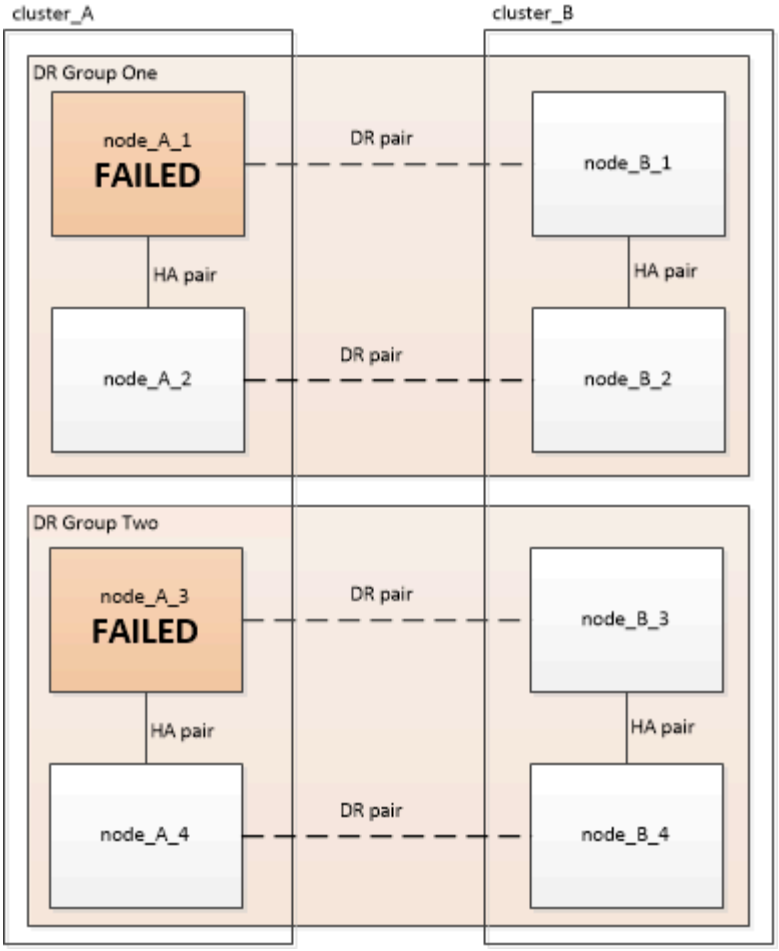
- ストレージを交換する必要がない場合は、プラットフォームモデルに対応したコントローラモジュールの FRU 交換用手順を使用できます。

  FRU 交換手順は、障害が発生したコントローラモジュールごとに 1 回、 2 回実行されます。

  "ONTAPハードウェアシステムのドキュメント"

- ストレージの交換が必要な場合は、マルチコントローラモジュールのリカバリ手順を使用できます。

  "マルチコントローラまたはストレージの障害からのリカバリ"



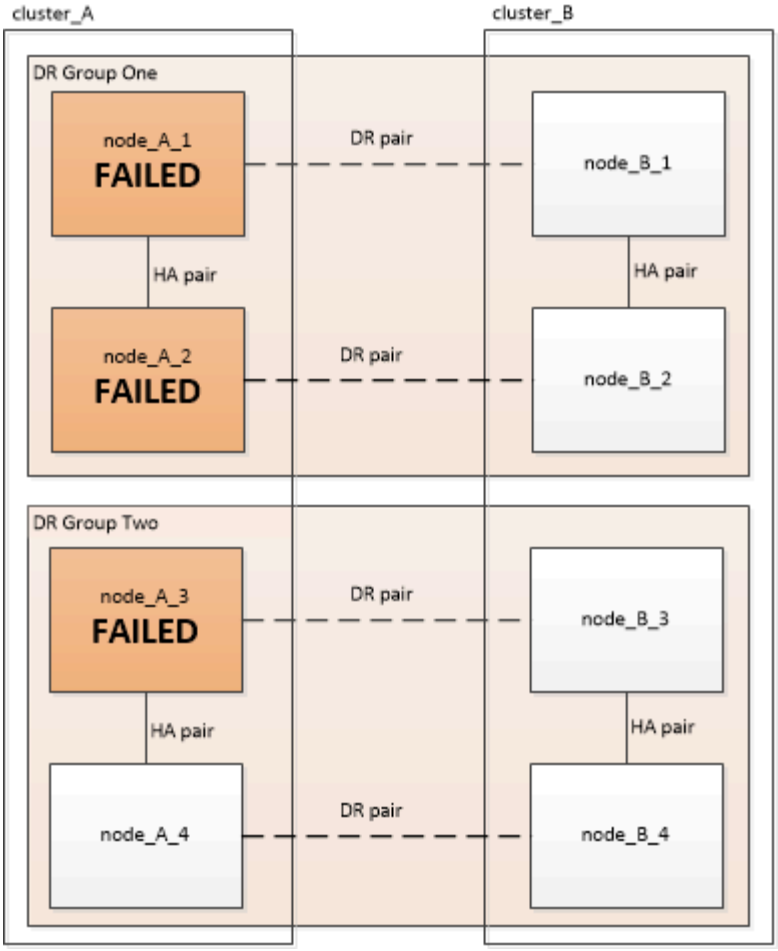
複数の **DR** グループにまたがる **3** 台のコントローラモジュールの障害

この障害の場合は、スイッチオーバーが必要です。マルチコントローラモジュールの障害からのリカバリ用手順を DR グループ 1 に使用できます。

"マルチコントローラまたはストレージの障害からのリカバリ"

プラットフォーム固有のコントローラモジュールの FRU 交換用手順を DR グループ 2 に使用できます。

"ONTAPハードウェアシステムのドキュメント"



2 ノード MetroCluster 構成でのコントローラモジュールの障害のシナリオ

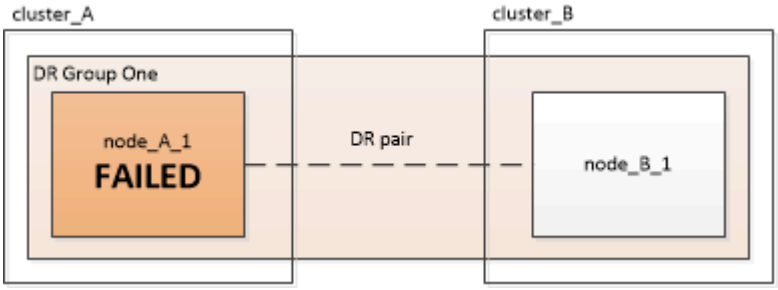
使用する手順は、障害の範囲によって異なります。

- ストレージを交換する必要がない場合は、プラットフォームモデルに対応したコントローラモジュールの FRU 交換用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"

- ストレージの交換が必要な場合は、マルチコントローラモジュールのリカバリ手順を使用できます。

  "マルチコントローラまたはストレージの障害からのリカバリ"



マルチコントローラまたはストレージの障害からリカバリする

マルチコントローラまたはストレージの障害からのリカバリ

MetroCluster 構成内の DR グループの一方の側のすべてのコントローラモジュール（ 2 ノード MetroCluster 構成の 1 台のコントローラを含む）でコントローラの障害が発生した場合、またはストレージが交換された場合は、機器を交換し、ドライブの所有権を再割り当てして、災害からリカバリする必要があります。

この手順を実行する前に、次のタスクを確認して実行したことを確認します。

- この手順の使用を決定する前に、使用可能なリカバリ手順を確認してください。

  "正しいリカバリ手順の選択"

- デバイスでコンソールログが有効になっていることを確認します。

  "コンソールログを有効にする"

- ディザスタサイトがフェンシングされていることを確認します。

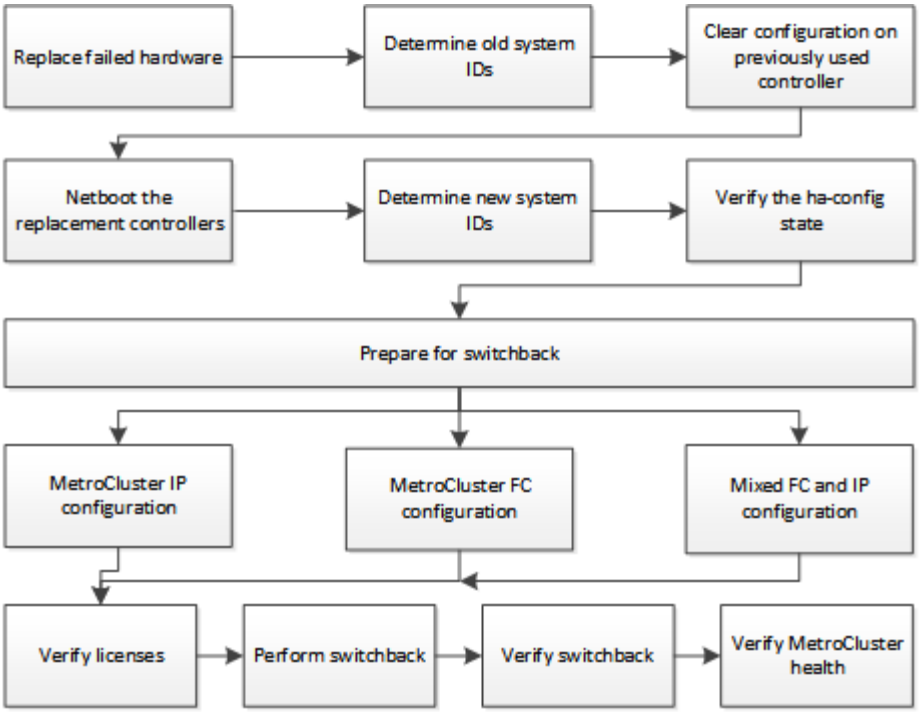
  "ディザスタサイトのフェンシング"。

- スイッチオーバーが実行されたことを確認します。

  "強制スイッチオーバーの実行"。

- 交換用ドライブとコントローラモジュールが新しく、以前に所有権が割り当てられていないことを確認します。
- この手順の例では、 2 ノードまたは 4 ノードの構成を示しています。8 ノード構成（ 2 つの DR グループ）の場合は、追加のコントローラモジュールの障害をすべて考慮し、必要なリカバリタスクを実行する必要があります。

この手順では次のワークフローを使用します。



この手順は、障害発生時に移行中だったシステムに対してリカバリを実行する場合に使用できます。その場合は、手順に示されているように、スイッチバックの準備の際に適切な手順を実行する必要があります。

コンソールログを有効にする

ハードウェアの交換と新しいコントローラのブートに進む前に、デバイスのコンソールログを有効にしてください。

NetAppでは、使用しているデバイスでコンソールロギングをイネーブルにし、この手順を実行する際に次のアクションを実行することを強く推奨します。

- メンテナンス中はAutoSupportを有効のままにします。
- メンテナンスの前後にメンテナンスAutoSupportメッセージをトリガーして、メンテナンスアクティビティ中にケースの作成を無効にします。

  ナレッジベースの記事を参照してください "スケジュールされたメンテナンス時間中にケースの自動作成を停止する方法"。

- 任意のCLIセッションのセッションロギングをイネーブルにします。セッションログを有効にする方法については、ナレッジベースの記事の「セッション出力のログ」セクションを参照してください "ONTAPシステムへの接続を最適化するためのPuTTYの設定方法"。

ハードウェアを交換し、新しいコントローラをブート

ハードウェアコンポーネントの交換が必要な場合は、該当するハードウェア交換 / 設置ガイドに従って交換する必要があります。

ディザスタサイトでのハードウェアの交換

作業を開始する前に

ストレージコントローラの電源がオフになっているか、停止したままになっている必要があります（ LOADER プロンプトが表示されている）。

手順

1. 必要に応じてコンポーネントを交換します。

この手順では、コンポーネントを交換し、災害発生前とまったく同じようにケーブル接続します。コンポーネントの電源は入れないでください。

交換対象	実行する手順	使用するガイド
MetroCluster FC 構成の FC スイッチ	a. 新しいスイッチを設置します。 b. ISL リンクをケーブル接続します。このとき、 FC スイッチの電源は入れないでください。	"MetroCluster コンポーネントの保守"
MetroCluster IP 構成の IP スイッチ	a. 新しいスイッチを設置します。 b. ISL リンクをケーブル接続します。このとき、 IP スイッチの電源は入れないでください。	"MetroCluster IP のインストールと設定： ONTAP MetroCluster 構成の違い"
ディスクシェルフ	a. ディスクシェルフとディスクを設置します。 ◦ ディスクシェルフのスタックは、サバイバーサイトと同じ構成であることが必要です。 ◦ ディスクは元のディスクと同じかまたはそれ以上のサイズのディスクを使用できますが、タイプ（ SAS または SATA ）は同じである必要があります。 b. ディスクシェルフを、スタック内の隣接するシェルフおよび FC-to-SAS ブリッジにケーブル接続します。このとき、ディスクシェルフの電源は入れないでください。	"ONTAPハードウェアシステムのドキュメント"

SAS ケーブル	a. 新しいケーブルを取り付けます。このとき、ディスクシェルフの電源は入れないでください。	"ONTAPハードウェアシステムのドキュメント"
MetroCluster FC 構成の FC-to-SAS ブリッジ	a. FC-to-SAS ブリッジを設置します。 b. FC-to-SAS ブリッジをケーブル接続します。 接続先は、 MetroCluster の構成タイプに応じて、 FC スイッチまたはコントローラモジュールとなります。 このとき、 FC-to-SAS ブリッジの電源は入れないでください。	"ファブリック接続 MetroCluster のインストールと設定" "ストレッチ MetroCluster のインストールと設定"

コントローラモジュール	a. 新しいコントローラモジュールを設置します。 ◦ コントローラモジュールは、交換するコントローラモジュールと同じモデルである必要があります。 たとえば、 8080 コントローラモジュールは 8080 コントローラモジュールと交換する必要があります。 ◦ MetroCluster 構成または既存のクラスタ構成内のクラスタに含まれていたことのあるコントローラモジュールは使用できません。 その場合は、デフォルト値を設定して「 wipeconfig 」プロセスを実行する必要があります。 ◦ すべてのネットワークインターフェイスカード（イーサネットや FC など）を、古いコントローラモジュールと同じスロットに装着します。 b. 新しいコントローラモジュールを元のコントローラモジュールとまったく同じようにケーブル接続します。 コントローラモジュールをストレージに接続するポート（ IP スイッチまたは FC スイッチへの接続、 FC-to-SAS ブリッジへの接続、または直接接続を使用）は、災害発生前と同じでなければなりません。 このとき、コントローラモジュールの電源は入れないでください。	"ONTAPハードウェアシステムのドキュメント"

2. 構成に応じてすべてのコンポーネントが正しくケーブル接続されていることを確認します。

- "MetroCluster の IP 設定"
- "MetroCluster ファブリック接続構成"

古いコントローラモジュールのシステム**ID**と**VLAN ID**の確認

ディザスタサイトですべてのハードウェアを交換したら、交換したコントローラモジュールのシステム ID を確認する必要があります。古いシステム ID は、新しいコントローラモジュールへのディスクの再割り当てを行うときに必要になります。システムが AFF A220 、 AFF A250 、 AFF A400 、 AFF A800 、 FAS2750 、 FAS500f 、 FAS8300 、 FAS8700 の各モデルでは、 MetroCluster IP インターフェイスで使用される VLAN ID も確認する必要があります。

作業を開始する前に

ディザスタサイトにあるすべての機器の電源をオフにする必要があります。

このタスクについて

ここでは、 2 ノードと 4 ノードの構成の例を示します。8 ノード構成の場合は、 2 つ目の DR グループのノードでの障害を考慮する必要があります。

2 ノード MetroCluster 構成の場合、各サイトの 2 つ目のコントローラモジュールに関する説明は無視してください。

この手順の例は、次の前提に基づいています。

- サイト A はディザスタサイト
- node_A_1 は障害発生後に完全に交換済み
- Node_a_2 で障害が発生し、完全に交換中です。

  Node_a_2 は 4 ノード MetroCluster 構成にのみ存在します。

- サイト B はサバイバーサイトです。
- node_B_1 は健全
- node_B_2 は正常

  node_B_2 が存在するのは 4 ノード MetroCluster 構成のみ

各コントローラモジュールの元々のシステム ID は次のとおりです。

MetroCluster 構成のノード数	ノード	元のシステム ID
4.	node_A_1	4068741258
Node_a_2	4068741260	node_B_1
4068741254	node_B_2	4068741256
2 つ	node_A_1	4068741258

手順

1. サバイバーサイトから、 MetroCluster 構成内のノードのシステム ID を表示します。

MetroCluster 構成のノード数	使用するコマンド
4 台または 8 台	「 MetroCluster node show -fields node-systemid 、 ha-partner-systemid 、 dr-partner-systemid 、 dr-auxiliary-systemid 」を指定します
2 つ	MetroCluster node show -fields node-systemid 、 dr-partner-systemid'

この 4 ノード MetroCluster 構成の例では、次の古いシステム ID が取得されます。

- node_A_1 ： 4068741258
- node_A_2 ： 4068741260

古いコントローラモジュールによって所有されていたディスクは、引き続きこれらのシステム ID に所有されています。

```
metrocluster node show -fields node-systemid,ha-partner-systemid,dr-
partner-systemid,dr-auxiliary-systemid

dr-group-id cluster    node      node-systemid ha-partner-systemid
dr-partner-systemid dr-auxiliary-systemid
----------- ---------- --------  ------------- ------ ------------
------ ------------ ------ --------------
1           Cluster_A  Node_A_1  4068741258    4068741260
4068741254          4068741256
1           Cluster_A  Node_A_2  4068741260    4068741258
4068741256          4068741254
1           Cluster_B  Node_B_1  -             -                    -
-
1           Cluster_B  Node_B_2  -             -                    -
-
4 entries were displayed.
```

この 2 ノード MetroCluster 構成の例では、次の古いシステム ID が取得されます。

- node_A_1 ： 4068741258

古いコントローラモジュールによって所有されていたディスクは、引き続きこのシステム ID に所有されています。

```
metrocluster node show -fields node-systemid,dr-partner-systemid

dr-group-id cluster    node      node-systemid dr-partner-systemid
----------- ---------- --------  ------------- ------------
1           Cluster_A  Node_A_1  4068741258    4068741254
1           Cluster_B  Node_B_1  -             -
2 entries were displayed.
```

2. ONTAP Mediator を使用した MetroCluster IP 構成の場合は、ONTAP Mediator の IP アドレスを取得します。

   「 storage iscsi-initiator show -node * -label mediator 」という名前のストレージがあります

3. システムが AFF A220 、 AFF A400 、 FAS2750 、 FAS8300 、または FAS8700 の場合、 VLAN ID を確認します。

   MetroCluster interconnect show

   VLAN ID は、出力の Adapter 列に表示されるアダプタ名に含まれています。

   この例では、 VLAN ID は 120 および 130 です。

```
metrocluster interconnect show
                          Mirror   Mirror
                  Partner Admin    Oper
Node Partner Name Type    Status   Status  Adapter Type   Status
---- ------------ ------- -------- ------- ------- ------ ------
Node_A_1 Node_A_2 HA      enabled  online
                                           e0a-120 iWARP  Up
                                           e0b-130 iWARP  Up
         Node_B_1 DR      enabled  online
                                           e0a-120 iWARP  Up
                                           e0b-130 iWARP  Up
         Node_B_2 AUX     enabled  offline
                                           e0a-120 iWARP  Up
                                           e0b-130 iWARP  Up
Node_A_2 Node_A_1 HA      enabled  online
                                           e0a-120 iWARP  Up
                                           e0b-130 iWARP  Up
         Node_B_2 DR      enabled  online
                                           e0a-120 iWARP  Up
                                           e0b-130 iWARP  Up
         Node_B_1 AUX     enabled  offline
                                           e0a-120 iWARP  Up
                                           e0b-130 iWARP  Up
12 entries were displayed.
```

サバイバーサイトから交換用ドライブを分離（**MetroCluster IP**構成）

MetroCluster iSCSI イニシエータ接続を停止して、サバイバーノードから交換用ドライブをすべて分離する必要があります。

このタスクについて

この手順は、 MetroCluster IP 構成でのみ必要です。

手順

1. どちらかのサバイバー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 モードで続けるかどうかを尋ねられたら、「 y 」と入力して応答する必要があります。
   advanced モードのプロンプトが表示されます（ * > ）。

2. DR グループ内の両方のサバイバーノードで、 iSCSI イニシエータを切断します。

   「 storage iscsi-initiator disconnect -node Survived-node-label * 」のように表示されます

   このコマンドはサバイバーノードごとに 1 回、計 2 回実行する必要があります。

次の例は、サイト B でイニシエータを切断するコマンドを示しています。

```
site_B::*> storage iscsi-initiator disconnect -node node_B_1 -label *
site_B::*> storage iscsi-initiator disconnect -node node_B_2 -label *
```

3. admin 権限レベルに戻ります。

   「特権管理者」

コントローラモジュールの設定をクリアします

MetroCluster 構成で新しいコントローラモジュールを使用する前に、既存の構成をクリアする必要があります。

手順

1. 必要に応じて、ノードを停止してプロンプトを表示し `LOADER`ます。

   「 halt 」

2. `LOADER`プロンプトで、環境変数をデフォルト値に設定します。

   「デフォルト設定」

3. 環境を保存します。

   'aveenv

4. `LOADER`プロンプトでブートメニューを起動します。

   「 boot_ontap menu

5. ブートメニューのプロンプトで、設定を消去します。

   wipeconfig

   確認プロンプトに「 yes 」と応答します。

   ノードがリブートし、もう一度ブートメニューが表示されます。

6. ブートメニューでオプション * 5 * を選択し、システムをメンテナンスモードでブートします。

   確認プロンプトに「 yes 」と応答します。

新しいコントローラモジュールをネットブート

新しいコントローラモジュールの ONTAP のバージョンが、稼働しているコントローラモジュールのバージョンと異なる場合は、新しいコントローラモジュールをネットブートする必要があります。

作業を開始する前に

- HTTP サーバにアクセスできる必要があります。

- 使用するプラットフォームおよび実行している ONTAP のバージョンに必要なシステムファイルをダウンロードするために、ネットアップサポートサイトにアクセスできる必要があります。

  "ネットアップサポート"

手順

1. にアクセスします "ネットアップサポートサイト" システムのネットブートの実行に使用するファイルをダウンロードするには、次の手順を実行します。
2. ネットアップサポートサイトのソフトウェアダウンロードセクションから該当する ONTAP ソフトウェアをダウンロードし、 Web にアクセスできるディレクトリに image.tgz ファイルを保存します。
3. Web にアクセスできるディレクトリに移動し、必要なファイルが利用可能であることを確認します。

プラットフォームモデル	作業
FAS/AFF8000 シリーズシステム	ターゲットディレクトリに version_image.tgzfile の内容を展開します。 tar -zxvf ONTAP-version _image.tgz 注： Windows で内容を展開する場合は、 7-Zip または WinRAR を使用してネットブートイメージを展開します。ディレクトリの一覧に、カーネルファイル netboot/ kernel を含むネットブートフォルダが表示される必要があります
その他すべてのシステム	ディレクトリの一覧に、カーネルファイルがあるネットブートフォルダを含める必要があります。 ONTAP-version _image.tgz ファイルを展開する必要はありません。

4. LOADER プロンプトで、管理 LIF のネットブート接続を設定します。
   - IP アドレスが DHCP の場合は、自動接続を設定します。

     ifconfig e0M -auto

   - IP アドレスが静的な場合は、手動接続を設定します。

     ifconfig e0M -addr= ip_addr-mask= netmask `-gw= gateway `
5. ネットブートを実行します。
   - プラットフォームが 80xx シリーズシステムの場合は、次のコマンドを使用します。

     netboot\http://web_server_ip/path_to_web-accessible_directory/netboot/kernel`

   - プラットフォームが他のシステムの場合は、次のコマンドを使用します。

     netboot\http://web_server_ip/path_to_web-accessible_directory/ontap-version_image.tgz`
6. ブートメニューからオプション * （ 7 ） Install new software first * を選択し、新しいソフトウェアイメージをダウンロードしてブートデバイスにインストールします。

```
 Disregard the following message: "This procedure is not supported for
Non-Disruptive Upgrade on an HA pair". It applies to nondisruptive
upgrades of software, not to upgrades of controllers.
```
. 手順を続行するかどうかを確認するメッセージが表示されたら、「 `y` 」と入力し、パッケージの入力を求められたらイメージファイルの `URL` 「 `¥ http://web_server_ip/path_to_web-accessible_directory/ontap-version_image.tgz` 」を入力します

```
Enter username/password if applicable, or press Enter to continue.
```

7. 入力 `n` 次のようなプロンプトが表示されたら、バックアップの回復をスキップします。

```
Do you want to restore the backup configuration now? {y|n} n
```

8. 次のようなプロンプトが表示されたら 'y' と入力して再起動します

```
The node must be rebooted to start using the newly installed software.
Do you want to reboot now? {y|n} y
```

新しくインストールされたソフトウェアを使用するには、ノードを再起動する必要があります。

9. ブートメニューから * オプション 5 * を選択し、メンテナンスモードに切り替えます。
10. 4 ノード MetroCluster 構成の場合は、もう一方の新しいコントローラモジュールでこの手順を繰り返します。

交換用コントローラモジュールのシステム**ID**の確認

ディザスタサイトですべてのハードウェアを交換したら、新たに設置したストレージコントローラモジュールのシステム ID を確認する必要があります。

このタスクについて

この手順は、交換用コントローラモジュールを使用してメンテナンスモードで実行する必要があります。

ここでは、 2 ノードと 4 ノードの構成の例を示します。2 ノード構成の場合、各サイトの 2 つ目のノードに関する説明は無視してください。8 ノード構成の場合は、 2 つ目の DR グループの追加のノードを考慮する必要があります。この例で想定している状況は次のとおりです。

- サイト A はディザスタサイト
- node_A_1 は交換済み
- Node_a_2 は交換済み

4 ノード MetroCluster 構成にのみ存在します。

- サイト B はサバイバーサイトです。
- node_B_1 は健全
- node_B_2 は正常

4 ノード MetroCluster 構成にのみ存在します。

この手順の例では、次のシステム ID を持つコントローラを使用します。

MetroCluster 構成のノード数	ノード	元のシステム ID	新しいシステム ID	DR パートナーとしてペアにします
4.	node_A_1	4068741258	1574774970	node_B_1
Node_a_2	4068741260	157477991	node_B_2	node_B_1
4068741254	変更なし	node_A_1	node_B_2	4068741256
変更なし	Node_a_2	2 つ	node_A_1	4068741258
1574774970	node_B_1	node_B_1	4068741254	変更なし

4 ノード MetroCluster 構成では、 site_A で最もシステム ID が小さいノードと site_B で最もシステム ID が小さいノードが自動的にペアになって DR パートナーシップが設定されますシステム ID は変化するため、コントローラ交換後の DR ペアが災害発生前と異なる場合があります。

上記の例では、次のようになり

- node_A_1 （ 1574774970 ）が node_B_1 （ 4068741254 ）とペアになります。
- node_A_2 （ 1574774991 ）が node_B_2 （ 4068741256 ）とペアになります。

手順

1. ノードを保守モードにして、各ノードからのノードのローカルシステム ID を表示します

   次の例では、新しいローカルシステム ID は 1574774970 です。

   ```
   *> disk show
    Local System ID: 1574774970
    ...
   ```

2. 2 つ目のノードで、同じ手順を繰り返します。

   2 ノード MetroCluster 構成ではこの手順は必要ありません。

次の例では、新しいローカルシステム ID は 1574774991 です。

```
*> disk show
 Local System ID: 1574774991
 ...
```

コンポーネントの **ha-config** 状態を確認

MetroCluster 構成では、コントローラモジュールおよびシャーシコンポーネントの ha-config 状態を「 mcc 」または「 mcc-2n 」に設定して、適切にブートするようにする必要があります。

作業を開始する前に

システムをメンテナンスモードにする必要があります。

このタスクについて

このタスクは、新しいコントローラモジュールごとに実行する必要があります。

手順

1. メンテナンスモードで、コントローラモジュールとシャーシの HA 状態を表示します。

   「 ha-config show 」

   HA の正しい状態は、 MetroCluster 構成によって異なります。

MetroCluster 構成のコントローラの数	すべてのコンポーネントの HA の状態
8 ノードまたは 4 ノード MetroCluster FC 構成	MCC
2 ノード MetroCluster FC 構成	mcc-2n
MetroCluster の IP 設定	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の HA 状態を設定します。

MetroCluster 構成のコントローラの数	コマンドを実行します
8 ノードまたは 4 ノード 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
MetroCluster の IP 設定	「 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 HA 状態を設定します。

MetroCluster 構成のコントローラの数	コマンドを実行します
8 ノードまたは 4 ノード 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た
MetroCluster の IP 設定	「 ha-config modify chassis mccip 」を参照してください

4. 交換した他のノードで同じ手順を繰り返します。

元のシステムでエンドツーエンドの暗号化が有効になっているかどうかを確認する

元のシステムでエンドツーエンドの暗号化が設定されているかどうかを確認する必要があります。

ステップ

1. サバイバーサイトで次のコマンドを実行します。

   ```
   metrocluster node show -fields is-encryption-enabled
   ```

   暗号化が有効になっている場合は、次の出力が表示されます。

   ```
   1 cluster_A node_A_1 true
   1 cluster_A node_A_2 true
   1 cluster_B node_B_1 true
   1 cluster_B node_B_2 true
   4 entries were displayed.
   ```

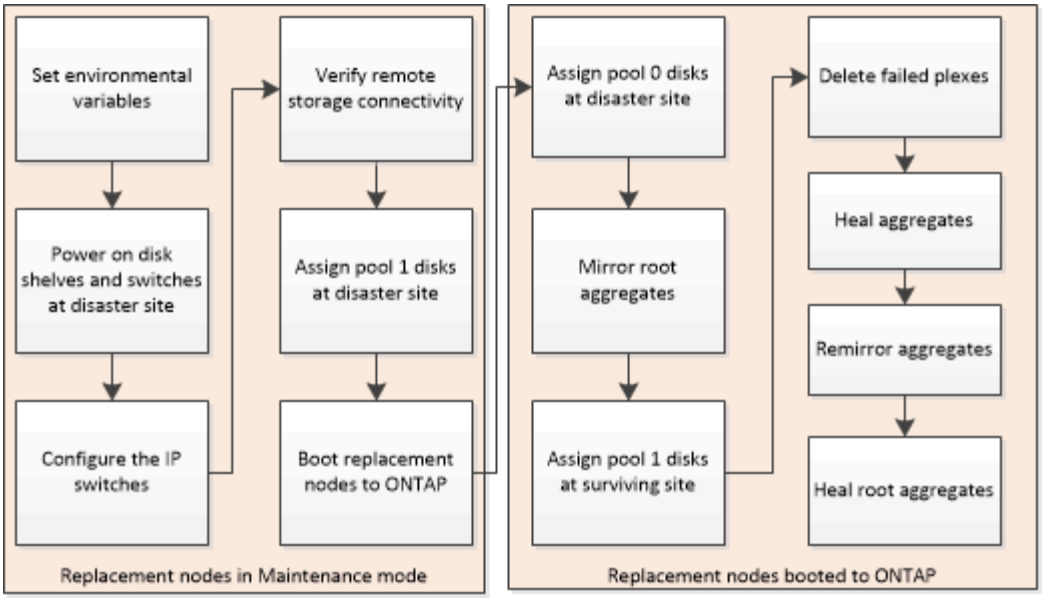
   を参照してください "エンドツーエンドの暗号化を設定する" サポートされているシステムの場合。

MetroCluster IP 構成でスイッチバックを準備

MetroCluster IP 構成でスイッチバックを準備

スイッチバック処理用に MetroCluster IP 構成を準備するには、特定のタスクを実行する必要があります。

このタスクについて



MetroCluster IP 構成に必要な環境変数を設定します

MetroCluster IP 構成では、イーサネットポートの MetroCluster インターフェイスの IP アドレスを取得し、そのアドレスを使用して交換用コントローラモジュールのインターフェイスを設定する必要があります。

このタスクについて

- このタスクを実行する必要があるのは、 MetroCluster IP 構成の場合だけです。
- このタスクのコマンドは、サバイバーサイトのクラスタプロンプトおよびディザスタサイトのノードの LOADER プロンプトから実行します。
- 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、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` 。

  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、パラメータがサポートされ `vlan-id` ます。
- これらの例のノードの MetroCluster IP 接続には、次の IP アドレスが使用されます。

> 以下は AFF A700 システムまたは FAS9000 システムの例です。インターフェイスはプラットフォームモデルによって異なります。

ノード	ポート	IP アドレス
node_A_1	e5	172.17.26.10
e5b	172.17.27.10	Node_a_2
e5	172.17.26.11	e5b
172.17.27.11	node_B_1	e5
172.17.26.13	e5b	172.17.27.13
node_B_2	e5	172.17.26.12

次の表は、ノードと各ノードの MetroCluster IP アドレスの関係をまとめたものです。

ノード	HA パートナー	DR パートナー	DR 補助パートナー
node_A_1 • e5a ： 172.17.26.10 • e5b ： 172.17.27.10	Node_a_2 • e51:172.17.26.11 • e5b ： 172.17.27.11	node_B_1 • e51:172.17.26.13 • e5b ： 172.17.27.13	node_B_2 • e5a ： 172.17.26.12 • e5b ： 172.17.27.12
Node_a_2 • e51:172.17.26.11 • e5b ： 172.17.27.11	node_A_1 • e5a ： 172.17.26.10 • e5b ： 172.17.27.10	node_B_2 • e5a ： 172.17.26.12 • e5b ： 172.17.27.12	node_B_1 • e51:172.17.26.13 • e5b ： 172.17.27.13
node_B_1 • e51:172.17.26.13 • e5b ： 172.17.27.13	node_B_2 • e5a ： 172.17.26.12 • e5b ： 172.17.27.12	node_A_1 • e5a ： 172.17.26.10 • e5b ： 172.17.27.10	Node_a_2 • e51:172.17.26.11 • e5b ： 172.17.27.11
node_B_2 • e5a ： 172.17.26.12 • e5b ： 172.17.27.12	node_B_1 • e51:172.17.26.13 • e5b ： 172.17.27.13	Node_a_2 • e51:172.17.26.11 • e5b ： 172.17.27.11	node_A_1 • e5a ： 172.17.26.10 • e5b ： 172.17.27.10

- 設定するMetroClusterのbootargの値は、新しいシステムで共有のクラスタ/ HAポートを使用するか、共有のMetroCluster / HAポートを使用するかによって異なります。次の情報を使用して、システムのポートを確認します。

共有クラスタ/ **HA**ポート

次の表に示すシステムは、共有クラスタ/ HAポートを使用します。

AFFおよび**ASA**システム	**FAS**システム
• AFF A20用 • AFF A30用 • AFF C30 • AFF A50用 • AFF C60 • AFF C80用 • AFF A70用 • AFF A90用 • AFF A1K用	• FAS50 • FAS70 • FAS90

共有**MetroCluster / HA**ポート

次の表に示すシステムは、共有MetroCluster / HAポートを使用します。

AFFおよび**ASA**システム	**FAS**システム
• AFF A150、ASA A150向け • AFF A220 • AFF C250、ASA C250向け • AFF A250、ASA A250向け • AFF A300 • AFF A320 • AFF C400、ASA C400向け • AFF A400、ASA A400向け • AFF A700 • AFF C800、ASA C800向け • AFF A800、ASA A800向け • AFF A900、ASA A900向け	• FAS2750 • FAS500f • FAS8200 • FAS8300 • FAS8700 の場合 • FAS9000 • FAS9500

手順

1. サバイバーサイトから、ディザスタサイトの MetroCluster インターフェイスの IP アドレスを収集します。

   「 MetroCluster configurion-settings connection show 」を参照してください

必要なアドレスは、「 * Destination Network Address * 」列に表示されている DR パートナーのアドレスです。

コマンド出力は、プラットフォームモデルで共有クラスタ/ HAポートを使用するか共有MetroCluster / HAポートを使用するかによって異なります。

共有クラスタ/ **HA**ポートを使用するシステム

```
cluster_B::*> metrocluster configuration-settings connection show
DR                    Source          Destination
DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
1     cluster_B
              node_B_1
                 Home Port: e5a
                      172.17.26.13    172.17.26.10    DR Partner
completed
                 Home Port: e5a
                      172.17.26.13    172.17.26.11    DR Auxiliary
completed
                 Home Port: e5b
                      172.17.27.13    172.17.27.10    DR Partner
completed
                 Home Port: e5b
                      172.17.27.13    172.17.27.11    DR Auxiliary
completed
              node_B_2
                 Home Port: e5a
                      172.17.26.12    172.17.26.11    DR Partner
completed
                 Home Port: e5a
                      172.17.26.12    172.17.26.10    DR Auxiliary
completed
                 Home Port: e5b
                      172.17.27.12    172.17.27.11    DR Partner
completed
                 Home Port: e5b
                      172.17.27.12    172.17.27.10    DR Auxiliary
completed
12 entries were displayed.
```

共有**MetroCluster / HA**ポートを使用するシステム

次の出力は、 AFF A700 システムと FAS9000 システムを使用した構成で MetroCluster IP インターフェイスがポート e5a および e5b にある場合の IP アドレスを示しています。インターフェイスはプラットフォームタイプによって異なります。

```
cluster_B::*> metrocluster configuration-settings connection show
DR                    Source          Destination
```

```
DR                       Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
1     cluster_B
              node_B_1
                 Home Port: e5a
                      172.17.26.13    172.17.26.12    HA Partner
completed
                 Home Port: e5a
                      172.17.26.13    172.17.26.10    DR Partner
completed
                 Home Port: e5a
                      172.17.26.13    172.17.26.11    DR Auxiliary
completed
                 Home Port: e5b
                      172.17.27.13    172.17.27.12    HA Partner
completed
                 Home Port: e5b
                      172.17.27.13    172.17.27.10    DR Partner
completed
                 Home Port: e5b
                      172.17.27.13    172.17.27.11    DR Auxiliary
completed
              node_B_2
                 Home Port: e5a
                      172.17.26.12    172.17.26.13    HA Partner
completed
                 Home Port: e5a
                      172.17.26.12    172.17.26.11    DR Partner
completed
                 Home Port: e5a
                      172.17.26.12    172.17.26.10    DR Auxiliary
completed
                 Home Port: e5b
                      172.17.27.12    172.17.27.13    HA Partner
completed
                 Home Port: e5b
                      172.17.27.12    172.17.27.11    DR Partner
completed
                 Home Port: e5b
                      172.17.27.12    172.17.27.10    DR Auxiliary
completed
12 entries were displayed.
```

2. インターフェイスの VLAN ID またはゲートウェイアドレスを確認する必要がある場合は、サバイバーサイトから VLAN ID を確認します。

   「 MetroCluster configurion-settings interface show 」を参照してください

   - プラットフォームモデルでVLAN IDがサポートされている場合（を参照）、およびデフォルトのVLAN IDを使用していない場合は、VLAN IDを確認する必要があり 上のリストます。
   - を使用する場合は、ゲートウェイアドレスが必要です "レイヤ 3 ワイドエリアネットワーク"。

     VLAN ID は、出力の * Network Address * 列に含まれています。[**Gateway**] 列には、ゲートウェイ IP アドレスが表示されます。

     次の例では、 VLAN ID が 120 の e0a と、 VLAN ID が 130 の e0b がインターフェイスです。

```
Cluster-A::*> metrocluster configuration-settings interface show
DR
Config
Group Cluster Node     Network Address Netmask         Gateway
State
----- ------- ------- --------------- --------------- ---------------
---------
1
      cluster_A
              node_A_1
                  Home Port: e0a-120
                          172.17.26.10  255.255.255.0  -
completed
                  Home Port: e0b-130
                          172.17.27.10  255.255.255.0  -
completed
```

3. `LOADER`プラットフォームモデルで共有のクラスタ/ HAポートを使用するか共有のMetroCluster / HAポートを使用するかに応じて、ディザスタサイトの各ノードのプロンプトでbootargの値を設定します。

   - インターフェイスがデフォルトのVLANを使用している場合、またはプラットフォームモデルがVLAN IDを使用していない場合（を参照 上のリスト）、_vlan-id_は必要ありません。
   - 構成が使用していない場合 "レイヤ 3 広域ネットワーク"、 _gateway-ip-address_is * 0 *（ゼロ）の値。

共有クラスタ/ **HA**ポートを使用するシステム

次のbootargを設定します。

```
setenv bootarg.mcc.port_a_ip_config local-IP-address/local-IP-
mask,0,0,DR-partner-IP-address,DR-aux-partnerIP-address,vlan-id

setenv bootarg.mcc.port_b_ip_config local-IP-address/local-IP-
mask,0,0,DR-partner-IP-address,DR-aux-partnerIP-address,vlan-id
```

次のコマンドは、最初のネットワークに VLAN 120 、 2 番目のネットワークに VLAN 130 を使用して node_A_1 の値を設定します。

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,0,172.17.26.13,172.17.26.12,120

setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,0,172.17.27.13,172.17.27.12,130
```

次の例は、 VLAN ID のない node_A_1 のコマンドを示しています。

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,0,172.17.26.13,172.17.26.12

setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,0,172.17.27.13,172.17.27.12
```

共有**MetroCluster / HA**ポートを使用するシステム

次のbootargを設定します。

```
setenv bootarg.mcc.port_a_ip_config local-IP-address/local-IP-
mask,0,HA-partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-
address,vlan-id

setenv bootarg.mcc.port_b_ip_config local-IP-address/local-IP-
mask,0,HA-partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-
address,vlan-id
```

次のコマンドは、最初のネットワークに VLAN 120 、 2 番目のネットワークに VLAN 130 を使用して node_A_1 の値を設定します。

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12,120

setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12,130
```

次の例は、 VLAN ID のない node_A_1 のコマンドを示しています。

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12

setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12
```

4. サバイバーサイトから、ディザスタサイトの UUID を収集します。

   MetroCluster node show -fields node-cluster.uuid 、 node-uuid

```
cluster_B::> metrocluster node show -fields node-cluster-uuid, node-uuid

  (metrocluster node show)
dr-group-id cluster     node     node-uuid
node-cluster-uuid
----------- ----------- -------- -------------------------------------
------------------------------
1           cluster_A   node_A_1 f03cb63c-9a7e-11e7-b68b-00a098908039
ee7db9d5-9a82-11e7-b68b-00a098

908039
1           cluster_A   node_A_2 aa9a7a7a-9a81-11e7-a4e9-00a098908c35
ee7db9d5-9a82-11e7-b68b-00a098

908039
1           cluster_B   node_B_1 f37b240b-9ac1-11e7-9b42-00a098c9e55d
07958819-9ac6-11e7-9b42-00a098

c9e55d
1           cluster_B   node_B_2 bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
07958819-9ac6-11e7-9b42-00a098

c9e55d
4 entries were displayed.
cluster_A::*>
```

ノード	UUID
cluster_B	07958819 - 9ac6-11e7-9b42 - 00a098c9e55d
node_B_1	f37b240b-9ac1-11e7-9b42 -00a098c9e55d
node_B_2	bf8e3f8f-9ac4-117-bd4e-00a098c379f です
cluster_A	ee7db9d5-9a82-11e7-b68b-00a098908039
node_A_1	f03cb63c-9a7e-11e7-b68b-00a098908039
Node_a_2	aa9a7a7a1-9a81-11e7-a4e9-00a098908c35

5. 交換用ノードの LOADER プロンプトで、 UUID を設定します。

```
setenv bootarg.mgwd.partner_cluster_uuid partner-cluster-UUID

setenv bootarg.mgwd.cluster_uuid local-cluster-UUID

setenv bootarg.mcc.pri_partner_uuid DR-partner-node-UUID

setenv bootarg.mcc.aux_partner_uuid DR-aux-partner-node-UUID

setenv bootarg.mcc_iscsi.node_uuid local-node-UUID`
```

a. node_A_1 の UUID を設定します。

次の例は、 node_A_1 の UUID を設定するコマンドを示しています。

```
setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039

setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
00a098c9e55d

setenv bootarg.mcc.pri_partner_uuid f37b240b-9ac1-11e7-9b42-
00a098c9e55d

setenv bootarg.mcc.aux_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-
00a098ca379f

setenv bootarg.mcc_iscsi.node_uuid f03cb63c-9a7e-11e7-b68b-
00a098908039
```

b. node_A_2 の UUID を設定します。

次の例は、 node_A_2 の UUID を設定するコマンドを示しています。

```
setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039

setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
00a098c9e55d

setenv bootarg.mcc.pri_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f

setenv bootarg.mcc.aux_partner_uuid f37b240b-9ac1-11e7-9b42-00a098c9e55d

setenv bootarg.mcc_iscsi.node_uuid aa9a7a7a-9a81-11e7-a4e9-00a098908c35
```

6. 元のシステムが ADP 用に設定されていた場合は、交換用ノードの LOADER プロンプトで ADP を有効に

します。

'etenv bootarg.me.adp_enabled true

7. 交換用ノードの LOADER プロンプトで ONTAP 9.5 、 9.6 、または 9.7 を実行している場合は、次の変数を有効にします。

   'etenv bootarg.mf.lun_part true

   a. node_A_1 の変数を設定します。

      次の例は、 ONTAP 9.6 を実行している場合に node_A_1 の値を設定するコマンドを示しています。

      ```
      setenv bootarg.mcc.lun_part true
      ```

   b. node_A_1 の変数を設定します。

      次の例は、 ONTAP 9.6 を実行している場合に node_A_1 の値を設定するコマンドを示しています。

```
setenv bootarg.mcc.lun_part true
```

8. 元のシステムがエンドツーエンドの暗号化用に設定されていた場合は、交換用ノードのLOADERプロンプトで次のbootargを設定します。

   ```
   setenv bootarg.mccip.encryption_enabled 1
   ```

9. 元のシステムが ADP 用に設定されていた場合は、交換用ノードの LOADER プロンプトで、元のシステム ID （交換用コントローラモジュールのシステム ID ではなく * ）とノードの DR パートナーのシステム ID を設定します。

   'setenv bootarg.me.local_config_id original-SysID

   'etenv bootarg.MCC.DR_partner DR_PARTNER -SysID

   "古いコントローラモジュールのシステムIDの確認"

   a. node_A_1 の変数を設定します。

      次の例は、 node_A_1 のシステム ID を設定するコマンドを示しています。

      - node_A_1 の古いシステム ID は 4068741258 です。
      - node_B_1 のシステム ID は 4068741254 です。

        ```
        setenv bootarg.mcc.local_config_id 4068741258
        setenv bootarg.mcc.dr_partner 4068741254
        ```

   b. node_A_1 の変数を設定します。

次の例は、 node_A_1 のシステム ID を設定するコマンドを示しています。

- node_A_1 の古いシステム ID は 4068741260 です。
- node_B_1 のシステム ID は 4068741256 です。

```
setenv bootarg.mcc.local_config_id 4068741260
setenv bootarg.mcc.dr_partner 4068741256
```

ディザスタサイトの機器の電源投入（ **MetroCluster IP** 構成）

ディザスタサイトのディスクシェルフおよび MetroCluster IP スイッチコンポーネントの電源をオンにする必要があります。ディザスタサイトのコントローラモジュールでは、 LOADER プロンプトが表示されたままになります。

このタスクについて

この手順の例では、次のことを想定しています。

- サイト A はディザスタサイト
- サイト B はサバイバーサイトです。

手順

1. ディザスタサイトのディスクシェルフの電源をオンにし、すべてのディスクが実行されていることを確認します。
2. MetroCluster IP スイッチがまだオンになっていない場合は、オンにします。

IP スイッチの設定（ **MetroCluster IP** 構成）

交換した 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

このタスクは、環境 MetroCluster IP 構成のみで実行します。

両方のスイッチで実行する必要があります。最初のスイッチの設定後に、サバイバーサイトでのストレージアクセスに影響がないことを確認します。

サバイバーサイトでのストレージアクセスに影響がある場合は、 2 つ目のスイッチの設定に進まないでください。

手順

1. を参照してください "MetroCluster IP のインストールと設定： ONTAP MetroCluster 構成の違い" 交換用スイッチのケーブル接続と設定の手順については、を参照してください。

   次のセクションの手順を使用できます。

   - IP スイッチのケーブル接続

◦ IP スイッチを設定しています

2. サバイバーサイトで ISL が無効になっている場合は、 ISL を有効にして、 ISL がオンラインであることを確認します。

   a. 1 つ目のスイッチで ISL インターフェイスを有効にします。

      「シャットダウンなし」

      次の例は、 Broadcom IP スイッチまたは Cisco IP スイッチ用のコマンドを示しています。

スイッチベンダー	コマンド
Broadcom	(IP_Switch_A_1)> enable (IP_switch_A_1)# configure (IP_switch_A_1)(Config)# interface 0/13-0/16 (IP_switch_A_1)(Interface 0/13- 0/16)# no shutdown (IP_switch_A_1)(Interface 0/13- 0/16)# exit (IP_switch_A_1)(Config)# exit
シスコ	IP_switch_A_1# conf t IP_switch_A_1(config)# int eth1/15-eth1/20 IP_switch_A_1(config)# no shutdown IP_switch_A_1(config)# copy running startup IP_switch_A_1(config)# show interface brief

   b. パートナースイッチで ISL インターフェイスを有効にします。

      「シャットダウンなし」

      次の例は、 Broadcom IP スイッチまたは Cisco IP スイッチ用のコマンドを示しています。

スイッチベンダー	コマンド

Broadcom	(IP_Switch_A_2)> enable (IP_switch_A_2)# configure (IP_switch_A_2)(Config)# interface 0/13-0/16 (IP_switch_A_2)(Interface 0/13- 0/16)# no shutdown (IP_switch_A_2)(Interface 0/13- 0/16)# exit (IP_switch_A_2)(Config)# exit
シスコ	IP_switch_A_2# conf t IP_switch_A_2(config)# int eth1/15-eth1/20 IP_switch_A_2(config)# no shutdown IP_switch_A_2(config)# copy running startup IP_switch_A_2(config)# show interface brief

c. インターフェイスが有効になっていることを確認します。

「インターフェイスの概要」

次の例は、 Cisco スイッチの出力例を示しています。

```
IP_switch_A_2(config)# show interface brief

--------------------------------------------------------------
Port VRF Status IP Address Speed MTU
--------------------------------------------------------------
mt0 -- up 10.10.99.10 100 1500
--------------------------------------------------------------
Ethernet    VLAN Type Mode    Status Reason Speed   Port
Interface                                         Ch
#
--------------------------------------------------------------
.
.
.
Eth1/15    10   eth   access  up     none   40G(D)  --
Eth1/16    10   eth   access  up     none   40G(D)  --
Eth1/17    10   eth   access  down   none   auto(D) --
Eth1/18    10   eth   access  down   none   auto(D) --
Eth1/19    10   eth   access  down   none   auto(D) --
Eth1/20    10   eth   access  down   none   auto(D) --
.
.
.
IP_switch_A_2#
```

リモートサイトへのストレージ接続の確認（ **MetroCluster IP** 構成）

交換したノードがサバイバーサイトのディスクシェルフに接続さ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

このタスクはディザスタサイトの交換用ノードで実行します。

このタスクはメンテナンスモードで実行します。

手順

1. 元のシステム ID が所有するディスクを表示します。

   「ディスク・ショー -s old-system-ID 」

   リモートディスクは 0m デバイスで認識されます。0m は、 MetroCluster iSCSI 接続を使用してディスクが接続されていることを示します。リカバリ手順にこれらのディスクを再割り当てする必要があります。

```
*> disk show -s 4068741256
Local System ID: 1574774970

  DISK     OWNER                  POOL   SERIAL NUMBER   HOME
DR HOME
---------- --------------------- ----- -------------
--------------------- ----------------------
0m.i0.0L11 node_A_2 (4068741256) Pool1 S396NA0HA02128  node_A_2
(4068741256) node_A_2  (4068741256)
0m.i0.1L38 node_A_2 (4068741256) Pool1 S396NA0J148778  node_A_2
(4068741256) node_A_2  (4068741256)
0m.i0.0L52 node_A_2 (4068741256) Pool1 S396NA0J148777  node_A_2
(4068741256) node_A_2  (4068741256)
...
...
NOTE: Currently 49 disks are unowned. Use 'disk show -n' for additional
information.
*>
```

2. 交換した他のノードについてもこの手順を繰り返します

ディザスタサイトのプール **1** ディスクのディスク所有権の再割り当て（ **MetroCluster IP** 構成）

ディザスタサイトのどちらかまたは両方のコントローラモジュールか NVRAM カードを交換した場合、システム ID が変わっているため、ルートアグリゲートに属するディスクを交換用コントローラモジュールに再割り当てする必要があります。

このタスクについて

ノードがスイッチオーバーモードであるため、このタスクでは、ディザスタサイトのプール 1 のルートアグリゲートを含むディスクのみを再割り当てします。この時点で古いシステム ID に所有されているのはこれらのディスクだけです。

このタスクはディザスタサイトの交換用ノードで実行します。

このタスクはメンテナンスモードで実行します。

この例で想定している状況は次のとおりです。

- サイト A はディザスタサイト
- node_A_1 は交換済み
- Node_a_2 は交換済み
- サイト B はサバイバーサイトです。
- node_B_1 は健全
- node_B_2 は正常

古いシステムIDと新しいシステムIDについては、を参照して "ハードウェアを交換し、新しいコントローラをブート"ください。

この手順の例では、次のシステム ID を持つコントローラを使用します。

ノード	元のシステム ID	新しいシステム ID
node_A_1	4068741258	1574774970
Node_a_2	4068741260	157477991
node_B_1	4068741254	変更なし
node_B_2	4068741256	変更なし

手順

1. メンテナンスモードの交換用ノードで、システムに ADP と ONTAP のバージョンが設定されているかどうかに応じて、適切なコマンドを使用してルートアグリゲートディスクを再割り当てします。

   プロンプトが表示されたら、再割り当てを続行できます。

システムでの ADP の使用の有無	ディスクの再割り当てに使用するコマンド
○（ ONTAP 9.8 ）	「ディスクの再割り当て」 - 「 old-system-ID -d new-system-ID -r dr-partner -system-ID 」
○（ ONTAP 9.7.x 以前）	「ディスクの再割り当て」 - 「 old-system-ID -d new-system-ID -p old-partner -system-ID 」
いいえ	「ディスクの再割り当て - s old-system-ID -d new-system-ID 」

   次の例は、 ADP 以外のシステムでのドライブの再割り当てを示しています。

```
*> disk reassign -s 4068741256 -d 1574774970
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)? n

After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)? y
Disk ownership will be updated on all disks previously belonging to
Filer with sysid 537037643.
Do you want to continue (y/n)? y
disk reassign parameters: new_home_owner_id 537070473 ,
new_home_owner_name
Disk 0m.i0.3L14 will be reassigned.
Disk 0m.i0.1L6 will be reassigned.
Disk 0m.i0.1L8 will be reassigned.
Number of disks to be reassigned: 3
```

2. メールボックスディスクの内容を破棄します。

   「マイボックス破壊ローカル」

   プロンプトが表示されたら、破棄処理を続行できます。

   次の例は、 mailbox destroy local コマンドの出力を示しています。

```
*> mailbox destroy local
Destroying mailboxes forces a node to create new empty mailboxes,
which clears any takeover state, removes all knowledge
of out-of-date plexes of mirrored volumes, and will prevent
management services from going online in 2-node cluster
HA configurations.
Are you sure you want to destroy the local mailboxes? y
..............Mailboxes destroyed.
*>
```

3. ディスクを交換した場合は、障害が発生したローカルプレックスを削除する必要があります。

   a. アグリゲートのステータスを表示します。

      「 aggr status 」を入力します

次の例では、プレックス node_A_1_aggr0/plex0 で障害が発生しています。

```
*> aggr status
Aug 18 15:00:07 [node_B_1:raid.vol.mirror.degraded:ALERT]: Aggregate
node_A_1_aggr0 is
   mirrored and one plex has failed. It is no longer protected by
mirroring.
Aug 18 15:00:07 [node_B_1:raid.debug:info]: Mirrored aggregate
node_A_1_aggr0 has plex0
   clean(-1), online(0)
Aug 18 15:00:07 [node_B_1:raid.debug:info]: Mirrored aggregate
node_A_1_aggr0 has plex2
   clean(0), online(1)
Aug 18 15:00:07 [node_B_1:raid.mirror.vote.noRecord1Plex:error]:
WARNING: Only one plex
   in aggregate node_A_1_aggr0 is available. Aggregate might contain
stale data.
Aug 18 15:00:07 [node_B_1:raid.debug:info]:
volobj_mark_sb_recovery_aggrs: tree:
   node_A_1_aggr0 vol_state:1 mcc_dr_opstate: unknown
Aug 18 15:00:07 [node_B_1:raid.fsm.commitStateTransit:debug]:
/node_A_1_aggr0 (VOL):
   raid state change UNINITD -> NORMAL
Aug 18 15:00:07 [node_B_1:raid.fsm.commitStateTransit:debug]:
/node_A_1_aggr0 (MIRROR):
   raid state change UNINITD -> DEGRADED
Aug 18 15:00:07 [node_B_1:raid.fsm.commitStateTransit:debug]:
/node_A_1_aggr0/plex0
   (PLEX): raid state change UNINITD -> FAILED
Aug 18 15:00:07 [node_B_1:raid.fsm.commitStateTransit:debug]:
/node_A_1_aggr0/plex2
   (PLEX): raid state change UNINITD -> NORMAL
Aug 18 15:00:07 [node_B_1:raid.fsm.commitStateTransit:debug]:
/node_A_1_aggr0/plex2/rg0
   (GROUP): raid state change UNINITD -> NORMAL
Aug 18 15:00:07 [node_B_1:raid.debug:info]: Topology updated for
aggregate node_A_1_aggr0
   to plex plex2
*>
```

b. 障害が発生したプレックスを削除します。

「 aggr destroy plex-id 」

```
*> aggr destroy node_A_1_aggr0/plex0
```

4. ノードを停止して LOADER プロンプトを表示します。

   「 halt 」

5. ディザスタサイトのもう一方のノードで、上記の手順を繰り返します。

MetroCluster IP 構成の交換用コントローラモジュールでの **ONTAP** のブート

ディザスタサイトの交換用ノードで ONTAP オペレーティングシステムをブートする必要があります。

このタスクについて

このタスクは、メンテナンスモードのディザスタサイトのノードから開始します。

手順

1. 交換用ノードの 1 つで、 LOADER プロンプト「 halt 」を終了します
2. ブートメニューを表示します：「 boot_ontap menu
3. ブートメニューからオプション 6 、 * アップデートフラッシュをバックアップ構成から * 選択します。

   システムが 2 回ブートします。続行するかどうかを確認するメッセージが表示されたら 'yes' と入力します2 回目の起動後、システム ID の不一致に関するプロンプトが表示されたら、「 y 」と応答する必要があります。

   > 使用した交換用コントローラモジュールの NVRAM の内容を消去しなかった場合は、「 PANIC ： NVRAM contents are invalid… 」というパニックメッセージが表示されることがあります この場合は、システムをもう一度 ONTAP プロンプト（「 boot_ontap menu 」）でブートしてください。次に、が必要です boot_recoveryおよびr確保 するr確保 するノードをrdbにリセットします

   - 続行の確認のプロンプト：

     ```
     Selection (1-9)? 6

     This will replace all flash-based configuration with the last backup
     to
     disks. Are you sure you want to continue?: yes
     ```

   - システム ID の不一致のプロンプト：

     ```
     WARNING: System ID mismatch. This usually occurs when replacing a
     boot device or NVRAM cards!
     Override system ID? {y|n} y
     ```

4. サバイバーサイトで、正しいパートナーシステム ID がノードに適用されていることを確認します。

   「 MetroCluster node show -fields node-systemid 、 ha-partner-systemid 、 dr-partner-systemid 、 dr-auxiliary-systemid 」を指定します

   この例では、次の新しいシステム ID が出力に表示されます。

   - node_A_1 ： 1574774970
   - node_A_2 ： 1574774991

   「 ha-partner-systemid 」列に新しいシステム ID が表示されます。

```
metrocluster node show -fields node-systemid,ha-partner-systemid,dr-
partner-systemid,dr-auxiliary-systemid

dr-group-id cluster    node      node-systemid ha-partner-systemid dr-
partner-systemid dr-auxiliary-systemid
----------- ---------- --------  ------------- ------ ------------
------ ------------ ------ --------------
1           Cluster_A  Node_A_1  1574774970    1574774991
4068741254          4068741256
1           Cluster_A  Node_A_2  1574774991    1574774970
4068741256          4068741254
1           Cluster_B  Node_B_1  -             -                    -
-
1           Cluster_B  Node_B_2  -             -                    -
-
4 entries were displayed.
```

5. パートナーシステム ID が正しく設定されていない場合は、正しい値を手動で設定する必要があります。
   a. ノードを停止して、 LOADER プロンプトを表示します。
   b. パートナーの bootarg ID の現在の値を確認します。

      printenv

   c. 値を正しいパートナーシステム ID に設定します。

      'setenv partner-sysid partner-SysID

   d. ノードをブートします。

      「 boot_ontap 」

   e. 必要に応じて、もう一方のノードで上記の手順を繰り返します。
6. ディザスタサイトの交換用ノードでスイッチバックの準備が完了していることを確認します。

   MetroCluster node show

交換用ノードは、スイッチバックリカバリモードを待機している必要があります。通常モードの場合は、交換用ノードをリブートします。ブート後、ノードはスイッチバックリカバリモードを待機する必要があります。

次の例は、交換用ノードでスイッチバックの準備が完了していることを示しています。

```
cluster_B::> metrocluster node show
DR                              Configuration  DR
Group Cluster Node              State          Mirroring Mode
----- ------- ----------------- -------------- ---------
--------------------
1     cluster_B
              node_B_1          configured     enabled   switchover
completed
              node_B_2          configured     enabled   switchover
completed
      cluster_A
              node_A_1          configured     enabled   waiting for
switchback recovery
              node_A_2          configured     enabled   waiting for
switchback recovery
4 entries were displayed.

cluster_B::>
```

7. MetroCluster 接続の設定を確認します。

「 MetroCluster configurion-settings connection show 」を参照してください

設定状態が「 Completed 」になっている必要があります。

```
cluster_B::*> metrocluster configuration-settings connection show
DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
1     cluster_B
              node_B_2
                 Home Port: e5a
                      172.17.26.13    172.17.26.12    HA Partner
completed
                 Home Port: e5a
                      172.17.26.13    172.17.26.10    DR Partner
completed
                 Home Port: e5a
```

```
                    172.17.26.13    172.17.26.11    DR Auxiliary
completed
                Home Port: e5b
                    172.17.27.13    172.17.27.12    HA Partner
completed
                Home Port: e5b
                    172.17.27.13    172.17.27.10    DR Partner
completed
                Home Port: e5b
                    172.17.27.13    172.17.27.11    DR Auxiliary
completed
            node_B_1
                Home Port: e5a
                    172.17.26.12    172.17.26.13    HA Partner
completed
                Home Port: e5a
                    172.17.26.12    172.17.26.11    DR Partner
completed
                Home Port: e5a
                    172.17.26.12    172.17.26.10    DR Auxiliary
completed
                Home Port: e5b
                    172.17.27.12    172.17.27.13    HA Partner
completed
                Home Port: e5b
                    172.17.27.12    172.17.27.11    DR Partner
completed
                Home Port: e5b
                    172.17.27.12    172.17.27.10    DR Auxiliary
completed
      cluster_A
            node_A_2
                Home Port: e5a
                    172.17.26.11    172.17.26.10    HA Partner
completed
                Home Port: e5a
                    172.17.26.11    172.17.26.12    DR Partner
completed
                Home Port: e5a
                    172.17.26.11    172.17.26.13    DR Auxiliary
completed
                Home Port: e5b
                    172.17.27.11    172.17.27.10    HA Partner
completed
                Home Port: e5b
                    172.17.27.11    172.17.27.12    DR Partner
```

```
completed
                 Home Port: e5b
                      172.17.27.11    172.17.27.13    DR Auxiliary
completed
              node_A_1
                 Home Port: e5a
                      172.17.26.10    172.17.26.11    HA Partner
completed
                 Home Port: e5a
                      172.17.26.10    172.17.26.13    DR Partner
completed
                 Home Port: e5a
                      172.17.26.10    172.17.26.12    DR Auxiliary
completed
                 Home Port: e5b
                      172.17.27.10    172.17.27.11    HA Partner
completed
                 Home Port: e5b
                      172.17.27.10    172.17.27.13    DR Partner
completed
                 Home Port: e5b
                      172.17.27.10    172.17.27.12    DR Auxiliary
completed
24 entries were displayed.

cluster_B::*>
```

8. ディザスタサイトのもう一方のノードで、上記の手順を繰り返します。

[[Reset-The -boot-recovery]] boot_recoveryとrdata_Corrupt bootargsをリセットします

必要に応じて、boot_recovery引数とrd_corrupt_bootargsをリセットできます

手順

1. ノードを停止してLOADERプロンプトに戻ります。

```
siteA::*> halt -node <node-name>
```

2. 次のbootargsが設定されているかどうかを確認します

```
LOADER> printenv bootarg.init.boot_recovery
LOADER> printenv bootarg.rdb_corrupt
```

3. どちらかのbootargが値に設定されている場合は、設定を解除してONTAP をブートします。

```
LOADER> unsetenv bootarg.init.boot_recovery
LOADER> unsetenv bootarg.rdb_corrupt
LOADER> saveenv
LOADER> bye
```

サバイバーノードからディザスタサイトへの接続のリストア（ **MetroCluster IP** 構成）

サバイバーノードから MetroCluster iSCSI イニシエータ接続をリストア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 構成でのみ必要です。

手順

1. どちらかのサバイバー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 モードで続けるかどうかを尋ねられたら、「 y 」と入力して応答する必要があります。
   advanced モードのプロンプトが表示されます（ * > ）。

2. DR グループ内の両方のサバイバーノードに iSCSI イニシエータを接続します。

   「 storage iscsi-initiator connect-node Survived-node-label * 」のようになります

   次の例は、サイト B のイニシエータを接続するコマンドを示しています。

   ```
   site_B::*> storage iscsi-initiator connect -node node_B_1 -label *
   site_B::*> storage iscsi-initiator connect -node node_B_2 -label *
   ```

3. admin 権限レベルに戻ります。

   「特権管理者」

自動割り当ての検証またはプール **0** ドライブの手動割り当て

ADP 用に設定されたシステムでは、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する必要があります。ADP 用に設定され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。

ディザスタサイトの **ADP** システム（ **MetroCluster IP** システム）でのプール **0** ドライブの割り当て確認

ディザスタサイトでドライブを交換し、システムが ADP 用に設定されている場合は、リモートドライブがノードから認識され、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。

ステップ

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のない AFF A800 システムで、 4 分の 1 （ 8 本のドライブ）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。残りのドライブが、 node_B_1 と node_B_2 のリモート（プール 1 ）ドライブになります。

```
cluster_A::*> disk show
                  Usable      Disk      Container           Container
Disk              Size        Shelf Bay Type    Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
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.
```

ディザスタサイトの **ADP** 以外のシステムでのプール **0** ドライブの割り当て（ **MetroCluster IP** 構成）

ドライブを交換したディザスタサイトでシステムが ADP 用に設定されていない場合は、新しいドライブをプール 0 に手動で割り当てる必要があります。

このタスクについて

ADP システムのドライブは自動的に割り当てられます。

手順

1. ディザスタサイトの一方の交換用ノードで、プール 0 のドライブを再割り当てします。

   'storage disk assign -n Number of -of -replacement disks -p 0

   このコマンドは、ディザスタサイトに新しく追加された所有権が未設定のドライブを割り当てます。災害発生前にノードに割り当てられていたドライブと同じ数および同じ（またはそれ以上の）サイズのドライブを割り当てる必要があります。「 storage disk assign 」のマニュアルページには、より詳細なドライブ割り当ての実行方法が記載されています。

2. ディザスタサイトのもう一方の交換用ノードで、手順を繰り返します。

サバイバーサイトでのプール **1** ドライブの割り当て（ **MetroCluster IP** 構成）

ドライブを交換したディザスタサイトでシステムが ADP 用に設定されていない場合は、サバイバーサイトで、ディザスタサイトにあるリモートドライブをサバイバーノードのプール 1 に手動で割り当てる必要があります。割り当てるドライブの数を確認しておく必要があります。

このタスクについて

ADP システムのドライブは自動的に割り当てられます。

ステップ

1. サバイバーサイトで、最初のノードのプール 1 （リモート）ドライブを割り当てます。「 storage disk assign -n number-to-replacement disks -p 1 0m * 」

   このコマンドは、ディザスタサイトに新しく追加された所有権が未設定のドライブを割り当てます。

   次のコマンドでは、 22 本のドライブを割り当てます。

```
cluster_B::> storage disk assign -n 22 -p 1 0m*
```

サバイバーサイトが所有する障害プレックスの削除（ **MetroCluster IP** 構成）

ハードウェアを交換してディスクを割り当てたら、障害が発生したリモートプレックスを削除する必要があります。このリモートプレックスはサバイバーサイトのノードが所有していますが、ディザスタサイトにあります。

このタスクについて

以下の手順はサバイバークラスタで実行します。

手順

1. ローカルアグリゲートを特定します。「 storage aggregate show -is-home true 」

```
cluster_B::> storage aggregate show -is-home true

cluster_B Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_B_1_aggr0 1.49TB  74.12GB 95% online       1 node_B_1
raid4,

mirror

degraded
node_B_2_aggr0 1.49TB  74.12GB 95% online       1 node_B_2
raid4,

mirror

degraded
node_B_1_aggr1 2.99TB  2.88TB   3% online      15 node_B_1
raid_dp,

mirror
```

```
degraded
node_B_1_aggr2 2.99TB  2.91TB   3% online      14 node_B_1
raid_tec,

mirror

degraded
node_B_2_aggr1 2.95TB  2.80TB   5% online      37 node_B_2
raid_dp,

mirror

degraded
node_B_2_aggr2 2.99TB  2.87TB   4% online      35 node_B_2
raid_tec,

mirror

degraded
6 entries were displayed.

cluster_B::>
```

2. 障害が発生したリモートプレックスを特定します。

   「 storage aggregate plex show 」と表示されます

   次の例では、リモートの（ plex0 ではない）プレックス（ステータスが「 failed 」）を呼び出します。

```
cluster_B::> storage aggregate plex show -fields aggregate,status,is-
online,Plex,pool
aggregate    plex  status        is-online pool
------------ ----- ------------- --------- ----
node_B_1_aggr0 plex0 normal,active true     0
node_B_1_aggr0 plex4 failed,inactive false  - <<<<---Plex at remote site
node_B_2_aggr0 plex0 normal,active true     0
node_B_2_aggr0 plex4 failed,inactive false  - <<<<---Plex at remote site
node_B_1_aggr1 plex0 normal,active true     0
node_B_1_aggr1 plex4 failed,inactive false  - <<<<---Plex at remote site
node_B_1_aggr2 plex0 normal,active true     0
node_B_1_aggr2 plex1 failed,inactive false  - <<<<---Plex at remote site
node_B_2_aggr1 plex0 normal,active true     0
node_B_2_aggr1 plex4 failed,inactive false  - <<<<---Plex at remote site
node_B_2_aggr2 plex0 normal,active true     0
node_B_2_aggr2 plex1 failed,inactive false  - <<<<---Plex at remote site
node_A_1_aggr1 plex0 failed,inactive false  -
node_A_1_aggr1 plex4 normal,active true     1
node_A_1_aggr2 plex0 failed,inactive false  -
node_A_1_aggr2 plex1 normal,active true     1
node_A_2_aggr1 plex0 failed,inactive false  -
node_A_2_aggr1 plex4 normal,active true     1
node_A_2_aggr2 plex0 failed,inactive false  -
node_A_2_aggr2 plex1 normal,active true     1
20 entries were displayed.

cluster_B::>
```

3. 各障害プレックスをオフラインにしてから削除します。

   a. 障害プレックスをオフラインにします。

      「 storage aggregate plex offline-aggregate aggregate-name -plex plex-id

      次の例は、アグリゲート「 node_B_2 の aggr1 / plex1 」をオフラインにします。

      ```
      cluster_B::> storage aggregate plex offline -aggregate node_B_1_aggr0
      -plex plex4

      Plex offline successful on plex: node_B_1_aggr0/plex4
      ```

   b. 障害が発生したプレックスを削除します。

      「 storage aggregate plex delete -aggregate aggregate-name -plex plex-id

プロンプトが表示されたら、プレックスを破棄できます。

次の例は、削除するプレックス node_B_2 の aggr1 / plex1 を示しています。

```
cluster_B::> storage aggregate plex delete -aggregate  node_B_1_aggr0
-plex plex4

Warning: Aggregate "node_B_1_aggr0" is being used for the local
management root
         volume or HA partner management root volume, or has been
marked as
         the aggregate to be used for the management root volume
after a
         reboot operation. Deleting plex "plex4" for this aggregate
could lead
         to unavailability of the root volume after a disaster
recovery
         procedure. Use the "storage aggregate show -fields
         has-mroot,has-partner-mroot,root" command to view such
aggregates.

Warning: Deleting plex "plex4" of mirrored aggregate "node_B_1_aggr0"
on node
         "node_B_1" in a MetroCluster configuration will disable its
         synchronous disaster recovery protection. Are you sure you
want to
         destroy this plex? {y|n}: y
[Job 633] Job succeeded: DONE

cluster_B::>
```

障害プレックスごとに上記の手順を繰り返す必要があります。

4. プレックスが削除されたことを確認します。

「 storage aggregate plex show -fields aggregate 、 status 、 is-online 、 plex 、 pool 」などのコマンドを実行します

```
cluster_B::> storage aggregate plex show -fields aggregate,status,is-
online,Plex,pool
aggregate    plex  status        is-online pool
------------ ----- ------------- --------- ----
node_B_1_aggr0 plex0 normal,active true     0
node_B_2_aggr0 plex0 normal,active true     0
node_B_1_aggr1 plex0 normal,active true     0
node_B_1_aggr2 plex0 normal,active true     0
node_B_2_aggr1 plex0 normal,active true     0
node_B_2_aggr2 plex0 normal,active true     0
node_A_1_aggr1 plex0 failed,inactive false  -
node_A_1_aggr1 plex4 normal,active true     1
node_A_1_aggr2 plex0 failed,inactive false  -
node_A_1_aggr2 plex1 normal,active true     1
node_A_2_aggr1 plex0 failed,inactive false  -
node_A_2_aggr1 plex4 normal,active true     1
node_A_2_aggr2 plex0 failed,inactive false  -
node_A_2_aggr2 plex1 normal,active true     1
14 entries were displayed.

cluster_B::>
```

5. スイッチオーバーされたアグリゲートを特定します。

   「 storage aggregate show -is-home false

   「 storage aggregate plex show -fields aggregate 、 status 、 is-online 、 plex 、 pool 」コマンドを使用して、プレックス 0 のスイッチオーバーされたアグリゲートを識別することもできます。ステータスが「 failed 、 inactive 」になります。

   次のコマンドは、 4 つのスイッチオーバーされたアグリゲートを表示します。

   - node_A_1 の aggr1
   - node_A_1 の aggr2
   - Node_a_2_aggr1
   - Node_A_2_aggr2

```
cluster_B::> storage aggregate show -is-home false

cluster_A Switched Over Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_A_1_aggr1 2.12TB  1.88TB   11% online      91 node_B_1
raid_dp,

mirror

degraded
node_A_1_aggr2 2.89TB  2.64TB    9% online      90 node_B_1
raid_tec,

mirror

degraded
node_A_2_aggr1 2.12TB  1.86TB   12% online      91 node_B_2
raid_dp,

mirror

degraded
node_A_2_aggr2 2.89TB  2.64TB    9% online      90 node_B_2
raid_tec,

mirror

degraded
4 entries were displayed.

cluster_B::>
```

6. スイッチオーバーされたプレックスを特定します。

   「 storage aggregate plex show -fields aggregate 、 status 、 is-online 、 Plex 、 pool 」などのコマンドを実行します

   ステータスが「 failed 、 inactive 」のプレックスを特定する必要があります。

   次のコマンドは、 4 つのスイッチオーバーされたアグリゲートを表示します。

```
cluster_B::> storage aggregate plex show -fields aggregate,status,is-
online,Plex,pool
aggregate    plex  status        is-online pool
------------ ----- ------------- --------- ----
node_B_1_aggr0 plex0 normal,active true     0
node_B_2_aggr0 plex0 normal,active true     0
node_B_1_aggr1 plex0 normal,active true     0
node_B_1_aggr2 plex0 normal,active true     0
node_B_2_aggr1 plex0 normal,active true     0
node_B_2_aggr2 plex0 normal,active true     0
node_A_1_aggr1 plex0 failed,inactive false  -  <<<<-- Switched over
aggr/Plex0
node_A_1_aggr1 plex4 normal,active true     1
node_A_1_aggr2 plex0 failed,inactive false  -  <<<<-- Switched over
aggr/Plex0
node_A_1_aggr2 plex1 normal,active true     1
node_A_2_aggr1 plex0 failed,inactive false  -  <<<<-- Switched over
aggr/Plex0
node_A_2_aggr1 plex4 normal,active true     1
node_A_2_aggr2 plex0 failed,inactive false  -  <<<<-- Switched over
aggr/Plex0
node_A_2_aggr2 plex1 normal,active true     1
14 entries were displayed.

cluster_B::>
```

7. 障害が発生したプレックスを削除します。

   「 storage aggregate plex delete -aggregate node_A_1 _aggr1 -plex plex0

   プロンプトが表示されたら、プレックスを破棄できます。

   次の例は、プレックス node_A_1 の aggr1 / plex0 を削除しています。

```
cluster_B::> storage aggregate plex delete -aggregate node_A_1_aggr1
-plex plex0

Warning: Aggregate "node_A_1_aggr1" hosts MetroCluster metadata volume
         "MDV_CRS_e8457659b8a711e78b3b00a0988fe74b_A". Deleting plex
"plex0"
         for this aggregate can lead to the failure of configuration
         replication across the two DR sites. Use the "volume show
-vserver
         <admin-vserver> -volume MDV_CRS*" command to verify the
location of
         such volumes.

Warning: Deleting plex "plex0" of mirrored aggregate "node_A_1_aggr1" on
node
         "node_A_1" in a MetroCluster configuration will disable its
         synchronous disaster recovery protection. Are you sure you want
to
         destroy this plex? {y|n}: y
[Job 639] Job succeeded: DONE

cluster_B::>
```

障害アグリゲートごとに上記の手順を繰り返す必要があります。

8. サバイバーサイトに障害プレックスが残っていないことを確認します。

   次の出力は、すべてのプレックスがオンラインであり、正常、アクティブ、およびオンラインであることを示しています。

```
cluster_B::> storage aggregate plex show -fields aggregate,status,is-
online,Plex,pool
aggregate    plex  status        is-online pool
------------ ----- ------------ --------- ----
node_B_1_aggr0 plex0 normal,active true     0
node_B_2_aggr0 plex0 normal,active true     0
node_B_1_aggr1 plex0 normal,active true     0
node_B_2_aggr2 plex0 normal,active true     0
node_B_1_aggr1 plex0 normal,active true     0
node_B_2_aggr2 plex0 normal,active true     0
node_A_1_aggr1 plex4 normal,active true     1
node_A_1_aggr2 plex1 normal,active true     1
node_A_2_aggr1 plex4 normal,active true     1
node_A_2_aggr2 plex1 normal,active true     1
10 entries were displayed.

cluster_B::>
```

アグリゲートの修復とミラーのリストア（ **MetroCluster IP** 構成）

ONTAP 9.5 以前を実行するシステムでは、ハードウェアを交換してディスクを割り当てたあとに、 MetroCluster 修復処理を実行できます。すべてのバージョンの ONTAP で、アグリゲートがミラーされたことを確認し、必要に応じてミラーリングを再開します。

このタスクについて

ONTAP 9.6 以降では、修復処理はディザスタサイトのノードがブートするときに自動的に実行されます。修復コマンドは必要ありません。

以下の手順はサバイバークラスタで実行します。

手順

1. ONTAP 9.6 以降を使用している場合は、自動修復が正常に完了したことを確認する必要があります。

   a. heal-aggr-auto と heal-root-aggr-auto の処理が完了したことを確認します。

      「 MetroCluster operation history show 」と表示されます

      次の出力は、これらの処理が cluster_A で正常に完了したことを示しています

```
cluster_B::*> metrocluster operation history show
Operation                      State          Start Time       End
Time
------------------------------ -------------- ----------------
----------------
heal-root-aggr-auto            successful      2/25/2019 06:45:58

2/25/2019 06:46:02
heal-aggr-auto                 successful     2/25/2019 06:45:48

2/25/2019 06:45:52
.
.
.
```

b. ディザスタサイトでスイッチバックの準備が完了していることを確認します。

MetroCluster node show

次の出力は、これらの処理が cluster_A で正常に完了したことを示しています

```
cluster_B::*> metrocluster node show
DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              node_A_1       configured     enabled   heal roots
completed
              node_A_2       configured     enabled   heal roots
completed
      cluster_B
              node_B_1       configured     enabled   waiting for
switchback recovery
              node_B_2       configured     enabled   waiting for
switchback recovery
4 entries were displayed.
```

2. ONTAP 9.5 以前を使用している場合は、アグリゲートの修復を実行する必要があります。

a. ノードの状態を確認します。

MetroCluster node show

次の出力は、スイッチオーバーが完了して修復を実行できる状態であることを示しています。

```
cluster_B::> metrocluster node show
DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_B
              node_B_1           configured     enabled   switchover
completed
              node_B_2           configured     enabled   switchover
completed
      cluster_A
              node_A_1           configured     enabled   waiting for
switchback recovery
              node_A_2           configured     enabled   waiting for
switchback recovery
4 entries were displayed.

cluster_B::>
```

b. アグリゲートの修復フェーズを実行します。

「 MetroCluster heal-phase aggregates 」

次の出力は、一般的なアグリゲート修復処理を示しています。

```
cluster_B::*> metrocluster heal -phase aggregates
[Job 647] Job succeeded: Heal Aggregates is successful.

cluster_B::*> metrocluster operation show
  Operation: heal-aggregates
      State: successful
 Start Time: 10/26/2017 12:01:15
   End Time: 10/26/2017 12:01:17
     Errors: -

cluster_B::*>
```

c. アグリゲートの修復が完了し、ディザスタサイトでスイッチバックの準備が完了していることを確認します。

MetroCluster node show

次の出力は、 cluster_A で「アグリゲートの修復」フェーズが完了したことを示しています

```
cluster_B::> metrocluster node show
DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
              node_A_1           configured     enabled   heal
aggregates completed
              node_A_2           configured     enabled   heal
aggregates completed
      cluster_B
              node_B_1           configured     enabled   waiting for
switchback recovery
              node_B_2           configured     enabled   waiting for
switchback recovery
4 entries were displayed.

cluster_B::>
```

3. ディスクを交換した場合は、ローカルおよびスイッチオーバーされたアグリゲートをミラーする必要があります。

   a. アグリゲートを表示します。

      「 storage aggregate show

```
cluster_B::> storage aggregate show
cluster_B Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes
RAID Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_B_1_aggr0 1.49TB  74.12GB   95% online     1 node_B_1
raid4,

normal
node_B_2_aggr0 1.49TB  74.12GB   95% online     1 node_B_2
raid4,

normal
node_B_1_aggr1 3.14TB  3.04TB    3% online     15 node_B_1
raid_dp,

normal
node_B_1_aggr2 3.14TB  3.06TB    3% online     14 node_B_1
```

```
raid_tec,

normal
node_B_1_aggr1 3.14TB  2.99TB    5% online     37 node_B_2
raid_dp,

normal
node_B_1_aggr2 3.14TB  3.02TB    4% online     35 node_B_2
raid_tec,

normal

cluster_A Switched Over Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes
RAID Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_A_1_aggr1 2.36TB  2.12TB   10% online     91 node_B_1
raid_dp,

normal
node_A_1_aggr2 3.14TB  2.90TB    8% online     90 node_B_1
raid_tec,

normal
node_A_2_aggr1 2.36TB  2.10TB   11% online     91 node_B_2
raid_dp,

normal
node_A_2_aggr2 3.14TB  2.89TB    8% online     90 node_B_2
raid_tec,

normal
12 entries were displayed.

cluster_B::>
```

b. アグリゲートをミラーします。

「 storage aggregate mirror -aggregate aggregate-name 」のように指定します

次の出力は、一般的なミラーリング処理を示しています。

```
cluster_B::> storage aggregate mirror -aggregate node_B_1_aggr1

Info: Disks would be added to aggregate "node_B_1_aggr1" on node
"node_B_1" in
      the following manner:

      Second Plex

        RAID Group rg0, 6 disks (block checksum, raid_dp)
          Position   Disk                      Type
Size
          ---------- ------------------------- ----------
---------------
          dparity    5.20.6                    SSD
-
          parity     5.20.14                   SSD
-
          data       5.21.1                    SSD
894.0GB
          data       5.21.3                    SSD
894.0GB
          data       5.22.3                    SSD
894.0GB
          data       5.21.13                   SSD
894.0GB

      Aggregate capacity available for volume use would be 2.99TB.

Do you want to continue? {y|n}: y
```

c. サバイバーサイトの各アグリゲートについて同じ手順を繰り返します。

d. アグリゲートが再同期されるまで待ちます。ステータスは「 storage aggregate show 」コマンドで確認できます。

次の出力は、複数のアグリゲートが再同期中であることを示しています。

```
cluster_B::> storage aggregate show

cluster_B Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes
RAID Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_B_1_aggr0 1.49TB  74.12GB   95% online     1 node_B_1
raid4,
```

```
mirrored,

normal
node_B_2_aggr0 1.49TB  74.12GB   95% online     1 node_B_2
raid4,

mirrored,

normal
node_B_1_aggr1 2.86TB  2.76TB    4% online     15 node_B_1
raid_dp,

resyncing
node_B_1_aggr2 2.89TB  2.81TB    3% online     14 node_B_1
raid_tec,

resyncing
node_B_2_aggr1 2.73TB  2.58TB    6% online     37 node_B_2
raid_dp,

resyncing
node_B-2_aggr2 2.83TB  2.71TB    4% online     35 node_B_2
raid_tec,

resyncing

cluster_A Switched Over Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes
RAID Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_A_1_aggr1 1.86TB  1.62TB   13% online     91 node_B_1
raid_dp,

resyncing
node_A_1_aggr2 2.58TB  2.33TB   10% online     90 node_B_1
raid_tec,

resyncing
node_A_2_aggr1 1.79TB  1.53TB   14% online     91 node_B_2
raid_dp,

resyncing
node_A_2_aggr2 2.64TB  2.39TB    9% online     90 node_B_2
raid_tec,
```

```
resyncing
12 entries were displayed.
```

e. すべてのアグリゲートが再同期されてオンラインになっていることを確認します。

「 storage aggregate plex show 」と表示されます

次に、すべてのアグリゲートが再同期されたことを示す出力を示します。

```
cluster_A::> storage aggregate plex show
  ()
                    Is      Is         Resyncing
Aggregate Plex      Online  Resyncing    Percent Status
--------- --------- ------- ---------- --------- ---------------
node_B_1_aggr0 plex0 true    false              - normal,active
node_B_1_aggr0 plex8 true    false              - normal,active
node_B_2_aggr0 plex0 true    false              - normal,active
node_B_2_aggr0 plex8 true    false              - normal,active
node_B_1_aggr1 plex0 true    false              - normal,active
node_B_1_aggr1 plex9 true    false              - normal,active
node_B_1_aggr2 plex0 true    false              - normal,active
node_B_1_aggr2 plex5 true    false              - normal,active
node_B_2_aggr1 plex0 true    false              - normal,active
node_B_2_aggr1 plex9 true    false              - normal,active
node_B_2_aggr2 plex0 true    false              - normal,active
node_B_2_aggr2 plex5 true    false              - normal,active
node_A_1_aggr1 plex4 true    false              - normal,active
node_A_1_aggr1 plex8 true    false              - normal,active
node_A_1_aggr2 plex1 true    false              - normal,active
node_A_1_aggr2 plex5 true    false              - normal,active
node_A_2_aggr1 plex4 true    false              - normal,active
node_A_2_aggr1 plex8 true    false              - normal,active
node_A_2_aggr2 plex1 true    false              - normal,active
node_A_2_aggr2 plex5 true    false              - normal,active
20 entries were displayed.
```

4. ONTAP 9.5 以前を実行するシステムで、ルートアグリゲートの修復フェーズを実行します。

「 MetroCluster heal-phase root-aggregates 」

```
cluster_B::> metrocluster heal -phase root-aggregates
[Job 651] Job is queued: MetroCluster Heal Root Aggregates Job.Oct 26
13:05:00
[Job 651] Job succeeded: Heal Root Aggregates is successful.
```

5. 「ルートの修復」フェーズが完了し、ディザスタサイトでスイッチバックの準備が完了していることを確認します。

   次の出力は、 cluster_A で「ルートの修復」フェーズが完了したことを示しています

```
cluster_B::> metrocluster node show
DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
              node_A_1           configured     enabled   heal roots
completed
              node_A_2           configured     enabled   heal roots
completed
      cluster_B
              node_B_1           configured     enabled   waiting for
switchback recovery
              node_B_2           configured     enabled   waiting for
switchback recovery
4 entries were displayed.

cluster_B::>
```

交換したノードのライセンスの確認に進みます。

"交換したノードのライセンスを確認しています"

MetroCluster FC 構成でスイッチバックを準備

ポート設定の確認（ **MetroCluster FC** 構成のみ）

MetroCluster 構成に備えて、ノードの環境変数を設定し、電源をオフにする必要があります。

このタスクについて

この手順は、交換用コントローラモジュールを使用してメンテナンスモードで実行します。

ポートの設定を確認する手順は、 FC ポートまたは CNA ポートがイニシエータモードで使用されているシステムでのみ必要です。

手順

1. メンテナンスモードで、 FC ポートの設定をリストアします。

   ucadmin modify -m fc -t initiatoradapter_name `

   イニシエータ設定でポートペアのうちどちらか 1 つだけを使用する場合は、アダプタ名には正確な値を入力してください。

2. 構成に応じて、次のいずれかの操作を実行します。

FC ポート設定	作業
両方のポートで同じです	ポートペアの 1 つのポートを変更すると、もう 1 つのポートも変更されるため、システムからプロンプトが表示されたら回答 “y” と入力します。
違う	a. システムからのプロンプトが表示されたら回答 “n” b. FC ポート設定をリストアします。 ucadmin modify -m fc -t initiator

3. メンテナンスモードを終了します。

   「 halt 」

   コマンドを問題したら、システムが LOADER プロンプトで停止するまで待ちます。

4. ノードをブートしてメンテナンスモードに戻り、設定の変更が反映されるようにします。

   「 boot_ontap maint 」を使用してください

5. 変数の値を確認します。

   ucadmin show

6. メンテナンスモードを終了して LOADER プロンプトを表示します。

   「 halt 」

FC-to-SAS ブリッジの設定（ **MetroCluster FC** 構成のみ）

FC-to-SAS ブリッジを交換した場合は、交換したブリッジを MetroCluster 構成のリストア時に設定する必要があります。手順は、 FC-to-SAS ブリッジの初期設定と同じです。

手順

1. FC-to-SAS ブリッジの電源をオンにします。
2. 「 set IPAddress port ipaddress 」コマンドを使用して、イーサネットポートの IP アドレスを設定します。

- 「 port 」には「 MP1 」または「 MP2 」を指定できます。
- ipipaddress には 'xxx.xxx.xxx.xxx という形式の IP アドレスを指定できます

  次の例は、イーサネットポート 1 の IP アドレス 10.10.10.55 を示しています。

```
Ready.
set IPAddress MP1 10.10.10.55

Ready. *
```

3. 「 set IPSubnetMask port mask 」コマンドを使用して、イーサネットポートに IP サブネットマスクを設定します。
   - 「 port 」には「 MP1 」または「 MP2 」を指定できます。
   - 「マスク」には、 xxx.xxx.xxx.xxx という形式のサブネットマスクを指定できます。

     次の例では、 IP サブネットマスクはイーサネットポート 1 の 255.255.255.0 です。

```
Ready.
set IPSubnetMask MP1 255.255.255.0

Ready. *
```

4. 「 set EthernetSpeed port speed 」コマンドを使用して、イーサネットポートに速度を設定します。
   - 「 port 」には「 MP1 」または「 MP2 」を指定できます。
   - 「speed」には「100」または「1000」を指定できます。

     次の例では、イーサネットポート 1 のイーサネット速度が 1000 に設定されています。

```
Ready.
set EthernetSpeed MP1 1000

Ready. *
```

5. 'aveConfiguration' コマンドを使用して設定を保存し ' プロンプトが表示されたらブリッジを再起動します

   イーサネットポートの設定後に設定を保存すると、 Telnet を使用してブリッジの設定を続行でき、 FTP を使用してブリッジにアクセスしてファームウェアの更新を実行できます。

   次の例は 'aveConfiguration' コマンドと ' ブリッジを再起動するためのプロンプトを示しています

```
Ready.
SaveConfiguration
  Restart is necessary....
  Do you wish to restart (y/n) ?
Confirm with 'y'. The bridge will save and restart with the new
settings.
```

6. FC-to-SAS ブリッジがリブートしたら、再度ログインします。
7. 「 set fcdatarate port speed 」コマンドを使用して、 FC ポートの速度を設定します。
   - 「 port 」には「 1 」または「 2 」を指定できます。
   - 「速度」には、モデルブリッジに応じて「 2 Gb 」、「 4 Gb 」、「 8 Gb 」、または「 16 Gb 」を指定できます。

   次の例では、ポートの FC1 速度が「 8Gb 」に設定されています。

```
Ready.
set fcdatarate 1 8Gb

Ready. *
```

8. 「 set FCConnMode port mode 」コマンドを使用して、 FC ポートのトポロジを設定します。
   - 「 port 」には「 1 」または「 2 」を指定できます。
   - 「 m ode 」には、「 ptp 」、「 loop 」、「 ptp-loop 」、または「 auto 」を指定できます。

   次の例では、ポート FC1 のトポロジが「 ptp 」に設定されています。

```
Ready.
set FCConnMode 1 ptp

Ready. *
```

9. 'aveConfiguration' コマンドを使用して設定を保存し ' プロンプトが表示されたらブリッジを再起動します

   次の例は 'aveConfiguration' コマンドと ' ブリッジを再起動するためのプロンプトを示しています

```
 Ready.
 SaveConfiguration
    Restart is necessary....
    Do you wish to restart (y/n) ?
 Confirm with 'y'. The bridge will save and restart with the new
settings.
```

10. FC-to-SAS ブリッジがリブートしたら、再度ログインします。
11. FC-to-SAS ブリッジがファームウェア 1.60 以降を実行している場合は、 SNMP を有効にします。

```
Ready.
set snmp enabled

Ready. *
saveconfiguration

Restart is necessary....
Do you wish to restart (y/n) ?

Verify with 'y' to restart the FibreBridge.
```

12. FC-to-SAS ブリッジの電源を切ります。

FC スイッチの設定（ MetroCluster FC 構成のみ）

ディザスタサイトで FC スイッチを交換した場合は、ベンダー固有の手順を使用してスイッチを設定する必要があります。スイッチを 1 つ設定し、サバイバーサイトでのストレージアクセスに影響がないことを確認してから、 2 つ目のスイッチを設定します。

関連タスク

"FCスイッチのポート割り当て"

サイト災害発生後の Brocade FC スイッチの設定

この Brocade 固有の手順を使用して交換用スイッチを設定し、 ISL ポートを有効化する必要があります。

このタスクについて

この手順の例は、次の前提に基づいています。

- サイト A はディザスタサイト
- FC_switch_A_1 は交換済み
- FC_switch_A_2 は交換済み
- サイト B はサバイバーサイトです。

- FC_switch_B_1 は正常
- FC_switch_B_2 は正常

FC スイッチをケーブル接続するときは、指定のポート割り当てを使用していることを確認する必要があります。

- "FCスイッチのポート割り当て"

例では、 FC-to-SAS ブリッジを 2 つ使用します。ブリッジが 3 つ以上ある場合は、追加のポートを無効にしてから有効にする必要があります。

手順

1. 新しいスイッチをブートし、事前設定します。

   a. 新しいスイッチに電源を投入し、起動するのを待ちます。

   b. スイッチのファームウェアバージョンをチェックして、他の FC スイッチのバージョンと一致していることを確認します。

      「 firmwareShow

   c. 次のトピックの説明に従って新しいスイッチを設定します。スイッチのゾーニング設定に関する手順は省略します。

      "ファブリック接続 MetroCluster のインストールと設定"

      "ストレッチ MetroCluster のインストールと設定"

   d. スイッチを永続的に無効にします。

      'witchcfgpersistentdisable

      リブート後や高速ブート後もスイッチは無効なままです。このコマンドが使用できない場合は 'witchdisable コマンドを使用します

      次の例は、 BrocadeSwitchA に対するコマンドを示しています。

      ```
      BrocadeSwitchA:admin> switchcfgpersistentdisable
      ```

      次の例は、 BrocadeSwitchB に対するコマンドを示しています。

```
BrocadeSwitchA:admin> switchcfgpersistentdisable
```

2. 新しいスイッチの設定を完了します。

   a. サバイバーサイトで ISL を有効にします。

      portcfgpersistentenable port-number

```
FC_switch_B_1:admin> portcfgpersistentenable 10
FC_switch_B_1:admin> portcfgpersistentenable 11
```

b. 交換用スイッチで ISL を有効にします。

portcfgpersistentenable port-number

```
FC_switch_A_1:admin> portcfgpersistentenable 10
FC_switch_A_1:admin> portcfgpersistentenable 11
```

c. 交換用スイッチ（この例では FC_switch_A_1 ）で、 ISL がオンラインであることを確認します。

'witchshow'

```
FC_switch_A_1:admin> switchshow
switchName: FC_switch_A_1
switchType: 71.2
switchState:Online
switchMode: Native
switchRole: Principal
switchDomain:       4
switchId:   fffc03
switchWwn:  10:00:00:05:33:8c:2e:9a
zoning:             OFF
switchBeacon:       OFF

Index Port Address Media Speed State  Proto
==============================================
...
10   10    030A00 id   16G     Online  FC E-Port 10:00:00:05:33:86:89:cb
"FC_switch_A_1"
11   11    030B00 id   16G     Online  FC E-Port 10:00:00:05:33:86:89:cb
"FC_switch_A_1" (downstream)
...
```

3. スイッチを永続的に有効にします。

'witchcfgpersistentenable

4. ポートがオンラインであることを確認します。

'witchshow'

Cisco 固有の手順を使用して交換用スイッチを設定し、 ISL ポートを有効化する必要があります。

このタスクについて

この手順の例は、次の前提に基づいています。

- サイト A はディザスタサイト
- FC_switch_A_1 は交換済み
- FC_switch_A_2 は交換済み
- サイト B はサバイバーサイトです。
- FC_switch_B_1 は正常
- FC_switch_B_2 は正常

手順

1. スイッチを設定します。
   a. を参照してください "ファブリック接続 MetroCluster のインストールと設定"
   b. のスイッチの設定手順に従います "Cisco FC スイッチの設定" セクション、 _except _ 「 Configuring zoning on a Cisco FC switch 」を参照してください。

      ゾーニングはこの手順の後半で設定します。

2. 正常に動作しているスイッチ（この例では FC_switch_B_1 ）で、 ISL ポートを有効にします。

   次の例は、ポートを有効にするコマンドを示しています。

   ```
   FC_switch_B_1# conf t
   FC_switch_B_1(config)# int fc1/14-15
   FC_switch_B_1(config)# no shut
   FC_switch_B_1(config)# end
   FC_switch_B_1# copy running-config startup-config
   FC_switch_B_1#
   ```

3. show interface brief コマンドを使用して、 ISL ポートが動作していることを確認します。
4. ファブリックからゾーニング情報を取得します。

   次の例は、ゾーニング設定を分散するコマンドを示しています。

   ```
   FC_switch_B_1(config-zone)# zoneset distribute full vsan 10
   FC_switch_B_1(config-zone)# zoneset distribute full vsan 20
   FC_switch_B_1(config-zone)# end
   ```

   FC_switch_B_1 が「 vsan 10 」と「 vsan 20 」のファブリック内の他のすべてのスイッチに分散され、ゾーニング情報が FC_switch_A_1 から取得されます。

5. 正常に動作しているスイッチで、ゾーニング情報がパートナースイッチから適切に取得されたことを確認します。

   「ゾーンの方法」

```
FC_switch_B_1# show zone
zone name FC-VI_Zone_1_10 vsan 10
  interface fc1/1 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/2 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/1 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/2 swwn 20:00:54:7f:ee:b8:24:c0

zone name STOR_Zone_1_20_25A vsan 20
  interface fc1/5 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/8 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/9 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/10 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/11 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/8 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/9 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/10 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/11 swwn 20:00:54:7f:ee:b8:24:c0

zone name STOR_Zone_1_20_25B vsan 20
  interface fc1/8 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/9 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/10 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/11 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/5 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/8 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/9 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/10 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/11 swwn 20:00:54:7f:ee:b8:24:c0
FC_switch_B_1#
```

6. スイッチファブリック内のスイッチの Worldwide Name （ WWN ；ワールドワイドネーム）を確認します。

   この例では、 2 つのスイッチの WWN は次のとおりです。

   - FC_switch_A_1 ： 20 ： 00 ： 54 ： 7F ： ee ： B8 ： 24 ： c0
   - FC_switch_B_1 ： 20 ： 00 ： 54 ： 7F ： ee ： C6 ： 80 ： 78

```
FC_switch_B_1# show wwn switch
Switch WWN is 20:00:54:7f:ee:c6:80:78
FC_switch_B_1#

FC_switch_A_1# show wwn switch
Switch WWN is 20:00:54:7f:ee:b8:24:c0
FC_switch_A_1#
```

7. ゾーンの構成モードに切り替えて、 2 つのスイッチのスイッチ WWN に属していないゾーンメンバーを削除します。

   no member interface interface-ide swwn

   この例では、ファブリック内のどちらのスイッチの WWN にも関連付けられていない次のメンバーを削除する必要があります。

   - ゾーン名 FC-VI_Zone_1_10 VSAN 10
     - インターフェイス fc1/1 sWWN 20:00:54:7F: e:e3:86:50 を参照してください
     - インターフェイス fc1/2 sWWN 20:00:54:7F: e:e3:86:50 を参照してください

     AFF A700 システムと FAS9000 システムは 4 つの FC-VI ポートをサポートします。FC-VI ゾーンから 4 つのポートをすべて削除する必要があります。

   - ゾーン名 STOR_Zone_1_20_25A VSAN 20
     - インターフェイス fc1/5 sWWN 20:00:54:7F: e:e3:86:50 を参照してください
     - インターフェイス fc1/8 sWWN 20:00:54:7F: e:e3:86:50 を参照してください
     - インターフェイス fc1/9 sWWN 20:00:54:7F: e:e3:86:50 を参照してください
     - インターフェイス fc1/10 sWWN 20:00:54:7F: e:e3:86:50 を参照してください
     - インターフェイス fc1/11 sWWN 20:00:54:7F: e:e3:86:50 を参照してください
   - ゾーン名 STOR_Zone_1_20_25B VSAN 20
     - インターフェイス fc1/8 sWWN 20:00:54:7F: e:e3:86:50 を参照してください
     - インターフェイス fc1/9 sWWN 20:00:54:7F: e:e3:86:50 を参照してください
     - インターフェイス fc1/10 sWWN 20:00:54:7F: e:e3:86:50 を参照してください
     - インターフェイス fc1/11 sWWN 20:00:54:7F: e:e3:86:50 を参照してください

   次の例は、これらのインターフェイスの削除を示しています。

```
 FC_switch_B_1# conf t
 FC_switch_B_1(config)# zone name FC-VI_Zone_1_10 vsan 10
 FC_switch_B_1(config-zone)# no member interface fc1/1 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/2 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# zone name STOR_Zone_1_20_25A vsan 20
 FC_switch_B_1(config-zone)# no member interface fc1/5 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/8 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/9 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/10 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/11 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# zone name STOR_Zone_1_20_25B vsan 20
 FC_switch_B_1(config-zone)# no member interface fc1/8 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/9 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/10 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/11 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# save running-config startup-config
 FC_switch_B_1(config-zone)# zoneset distribute full 10
 FC_switch_B_1(config-zone)# zoneset distribute full 20
 FC_switch_B_1(config-zone)# end
 FC_switch_B_1# copy running-config startup-config
```

8. [[step8] 新しいスイッチのポートをゾーンに追加します。

   次の例では、交換用スイッチのケーブル接続が古いスイッチのケーブル接続と同じであることを前提としています。

```
 FC_switch_B_1# conf t
 FC_switch_B_1(config)# zone name FC-VI_Zone_1_10 vsan 10
 FC_switch_B_1(config-zone)# member interface fc1/1 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/2 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# zone name STOR_Zone_1_20_25A vsan 20
 FC_switch_B_1(config-zone)# member interface fc1/5 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/8 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/9 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/10 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/11 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# zone name STOR_Zone_1_20_25B vsan 20
 FC_switch_B_1(config-zone)# member interface fc1/8 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/9 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/10 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/11 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# save running-config startup-config
 FC_switch_B_1(config-zone)# zoneset distribute full 10
 FC_switch_B_1(config-zone)# zoneset distribute full 20
 FC_switch_B_1(config-zone)# end
 FC_switch_B_1# copy running-config startup-config
```

9. ゾーニングが適切に構成されていることを確認します : 'how zone

   次の出力例は、 3 つのゾーンを示しています。

```
FC_switch_B_1# show zone
  zone name FC-VI_Zone_1_10 vsan 10
    interface fc1/1 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/2 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/1 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/2 swwn 20:00:54:7f:ee:b8:24:c0

  zone name STOR_Zone_1_20_25A vsan 20
    interface fc1/5 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/8 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/9 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/10 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/11 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/8 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/9 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/10 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/11 swwn 20:00:54:7f:ee:b8:24:c0

  zone name STOR_Zone_1_20_25B vsan 20
    interface fc1/8 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/9 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/10 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/11 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/5 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/8 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/9 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/10 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/11 swwn 20:00:54:7f:ee:b8:24:c0
FC_switch_B_1#
```

ストレージ構成の確認

すべてのストレージをサバイバーノードから認識できることを確認する必要があります。

手順

1. ディザスタサイトにあるすべてのストレージコンポーネントが、サバイバーサイトでも容量、タイプともに同じであることを確認します。

   ディスクシェルフスタック、ディスクシェルフ、およびディスクの数が、サバイバーサイトとディザスタサイトで同じであることが必要です。ブリッジ接続型またはファブリック接続型の MetroCluster 構成では、サイトの FC-to-SAS ブリッジの数が同じであることが必要です。

2. ディザスタサイトで交換したすべてのディスクに所有権が設定されていないことを確認します。

   run local disk show -n

所有権のないディスクは unowned と表示されます。

3. ディスクを 1 本も交換しなかった場合は、すべてのディスクが存在することを確認します。

   「ディスクショー」

ディザスタサイトの機器の電源投入

スイッチバックの準備が整ったら、ディザスタサイトで MetroCluster コンポーネントの電源をオンにする必要があります。また、直接接続型の MetroCluster 構成で SAS ストレージ接続のケーブル接続をやり直し、ファブリック接続型の MetroCluster 構成でスイッチ間以外のリンクポートを有効にする必要があります。

作業を開始する前に

MetroCluster コンポーネントを交換し、交換前とまったく同じ状態にケーブル接続しておく必要があります。

"ファブリック接続 MetroCluster のインストールと設定"

"ストレッチ MetroCluster のインストールと設定"

このタスクについて

この手順の例では、次のことを想定しています。

- サイト A はディザスタサイト
  - FC_switch_A_1 は交換済み
  - FC_switch_A_2 は交換済み
- サイト B はサバイバーサイトです。
  - FC_switch_B_1 は正常
  - FC_switch_B_2 は正常

FC スイッチは、ファブリック接続 MetroCluster 構成にのみ存在します。

手順

1. SAS ケーブルを使用する（ FC スイッチファブリックや FC-to-SAS ブリッジは使用しない）ストレッチ MetroCluster 構成で、両方のサイトのすべてのストレージ（リモートストレージを含む）を接続します。

   ディザスタサイトのコントローラで、電源をオフのままにするか、 LOADER プロンプトを表示する必要があります。

2. サバイバーサイトで、ディスクの自動割り当てを無効にします。

   「 storage disk option modify -autoassign off * 」を参照してください

```
cluster_B::> storage disk option modify -autoassign off *
2 entries were modified.
```

3. サバイバーサイトで、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。

   「 storage disk option show 」をクリックします

```
cluster_B::> storage disk option show
Node     BKg. FW. Upd.  Auto Copy   Auto Assign  Auto Assign Policy
--------  -------------  -----------  -----------  ------------------
node_B_1       on            on          off             default
node_B_2       on            on          off             default
2 entries were displayed.

 cluster_B::>
```

4. ディザスタサイトのディスクシェルフの電源をオンにし、すべてのディスクが実行されていることを確認します。
5. ブリッジ接続型またはファブリック接続型の MetroCluster 構成で、ディザスタサイトのすべての FC-to-SAS ブリッジの電源をオンにします。
6. 交換したディスクがある場合は、コントローラの電源をオフのままにするか、 LOADER プロンプトを表示します。
7. ファブリック接続 MetroCluster 構成で、 FC スイッチの非 ISL ポートを有効にします。

スイッチベンダー	ポートを有効化する手順

Brocade	a. FC-to-SAS ブリッジに接続されているポートを永続的に有効にします :portpersistentenable port-number 次の例では、ポート 6 とポート 7 を有効にします。 ``` FC_switch_A_1:admin> portpersistentenable 6 FC_switch_A_1:admin> portpersistentenable 7 FC_switch_A_1:admin> ``` b. HBA および FC-VI アダプタに接続されているポート portpersistentenable port-number を永続的に有効にします 次の例では、ポート 6 とポート 7 を有効にします。 ``` FC_switch_A_1:admin> portpersistentenable 1 FC_switch_A_1:admin> portpersistentenable 2 FC_switch_A_1:admin> portpersistentenable 4 FC_switch_A_1:admin> portpersistentenable 5 FC_switch_A_1:admin> ``` AFF A700 システムと FAS9000 システムでは、switchcfgpersistentenable コマンドを使用して、 4 つの FC-VI ポートをすべて永続的に有効にする必要があります。 c. サバイバーサイトの 2 つ目の FC スイッチに対して手順 a と b を繰り返します。

シスコ	a. インターフェイスの構成モードを開始し、 no shut コマンドを使用してポートを有効化します。 次の例では、ポート fc1/36 が無効化されます。 ``` FC_switch_A_1# conf t FC_switch_A_1(config)# interface fc1/36 FC_switch_A_1(config)# no shut FC_switch_A_1(config-if)# end FC_switch_A_1# copy running- config startup-config ``` b. スイッチポートが有効になっていることを確認します。「 show interface brief 」 c. FC-to-SAS ブリッジ、 HBA 、および FC-VI アダプタに接続されている他のポートに対して手順 a と b を繰り返します。 d. サバイバーサイトの 2 つ目の FC スイッチに対して手順 a 、 b 、 c を繰り返します。

交換したドライブの所有権を割り当てます

ディザスタサイトでハードウェアをリストアするときにドライブを交換した場合、またはドライブの初期化や所有権の削除が必要になった場合は、該当するドライブに所有権を割り当てる必要があります。

作業を開始する前に

ディザスタサイトに、災害発生前に使用可能だったドライブと同数以上のドライブが必要です。

ドライブシェルフとドライブの配置がの要件を満たしている必要があります "MetroCluster IP の必須のコンポーネントと命名規則" のセクション "MetroCluster IP のインストールと設定"。

このタスクについて

以下の手順は、ディザスタサイトのクラスタで実行します。

この手順には、ディザスタサイトでの全ドライブの再割り当ておよび新しいプレックスの作成が表示されます。新しいプレックスとは、サバイバーサイトのリモートプレックスとディザスタサイトのローカルプレックスです。

ここでは、 2 ノードと 4 ノードの構成の例を示します。2 ノード構成の場合、各サイトの 2 つ目のノードに関する説明は無視してください。8 ノード構成の場合は、 2 つ目の DR グループの追加のノードを考慮する必要があります。この例で想定している状況は次のとおりです。

- サイト A はディザスタサイト

- node_A_1 は交換済み
- Node_a_2 は交換済み

  4 ノード MetroCluster 構成にのみ存在します。

- サイト B はサバイバーサイトです。
  - node_B_1 は健全
  - node_B_2 は正常

  4 ノード MetroCluster 構成にのみ存在します。

各コントローラモジュールの元々のシステム ID は次のとおりです。

MetroCluster 構成のノード数	ノード	元のシステム ID
4.	node_A_1	4068741258
Node_a_2	4068741260	node_B_1
4068741254	node_B_2	4068741256
2 つ	node_A_1	4068741258

ドライブを割り当てる際には、次の点に注意してください。

- old-count-of-disks には、災害前に各ノードに割り当てられていたディスク数と同じ数、またはそれ以上の数を指定する必要があります。

  元のディスク数より少ない数を指定するか、または少ない数のディスク数しかない場合、スペース不足により修復処理を完了できない場合があります。

- 新たに作成するプレックスは、サバイバーサイト（ node_B_x の pool1 ）に属するリモートプレックスとディザスタサイト（ node_B_x の pool0 ）に属するローカルプレックスです。
- 必要なドライブの総数にルートアグリゲートディスクを含めないでください。

  サバイバーサイトの pool1 に n 本のディスクを割り当てる場合、ルートアグリゲートが 3 本のディスクを使用するという想定では、ディザスタサイトに n -3 本のディスクを割り当てる必要があります。

- 同じスタック上の他のすべてのディスクが割り当てられているプールとは異なるディスクをプールに割り当てることはできません。
- サバイバーサイトに属するディスクはプール 1 に割り当てられ、ディザスタサイトに属するディスクはプール 0 に割り当てられます。

手順

1. MetroCluster の構成が 4 ノード構成と 2 ノード構成のどちらであるかに基づいて、所有権が未設定の新しいドライブを割り当てます。

◦ 4 ノード MetroCluster 構成の場合は、交換用ノードで次の一連のコマンドを使用して、新しい未割り当てのディスクを適切なディスクプールに割り当てます。

i. 各ノードの交換したディスクをそれぞれのディスクプールに体系的に割り当てます。

「ディスク割り当て -s sysid -n old-count-of-disks -p pool 」

サバイバーサイト問題から、各ノードの disk assign コマンドを実行します。

```
cluster_B::> disk assign -s node_B_1-sysid -n old-count-of-disks
-p 1 **\(remote pool of surviving site\)**
cluster_B::> disk assign -s node_B_2-sysid -n old-count-of-disks
-p 1 **\(remote pool of surviving site\)**
cluster_B::> disk assign -s node_A_1-old-sysid -n old-count-of-
disks -p 0 **\(local pool of disaster site\)**
cluster_B::> disk assign -s node_A_2-old-sysid -n old-count-of-
disks -p 0 **\(local pool of disaster site\)**
```

次の例は、システム ID を指定したコマンドを示しています。

```
cluster_B::> disk assign -s 4068741254 -n 21 -p 1
cluster_B::> disk assign -s 4068741256 -n 21 -p 1
cluster_B::> disk assign -s 4068741258 -n 21 -p 0
cluster_B::> disk assign -s 4068741260 -n 21 -p 0
```

i. ディスクの所有権を確認します。

「 storage disk show -fields owner 、 pool 」という 2 つのフィールドがあります

```
storage disk show -fields owner, pool
cluster_A::> storage disk show -fields owner, pool
disk     owner          pool
-------- ------------- -----
0c.00.1  node_A_1      Pool0
0c.00.2  node_A_1      Pool0
.
.
.
0c.00.8  node_A_1      Pool1
0c.00.9  node_A_1      Pool1
.
.
.
0c.00.15 node_A_2      Pool0
0c.00.16 node_A_2      Pool0
.
.
.
0c.00.22 node_A_2      Pool1
0c.00.23 node_A_2      Pool1
.
.
.
```

- 2 ノード MetroCluster 構成の場合は、交換用ノードで次の一連のコマンドを使用して、新しい未割り当てのディスクを適切なディスクプールに割り当てます。
  i. ローカルシェルフ ID を表示します。

     run local storage show shelf

  ii. 正常なノードの交換したディスクをプール 1 に割り当てます。

     「 run local disk assign -shelf shelf-id -n old-count-of-disks -p 1 -s node_B_1-sysid -f 」を実行します

  iii. 交換用ノードの交換したディスクをプール 0 に割り当てます。

     「 run local disk assign -shelf shelf-id -n old-count-of-disks -p 0 -s node_A_1-sysid -f 」を実行します

2. サバイバーサイトで、ディスクの自動割り当てを再度有効にします。

「 storage disk option modify -autoassign on * 」のように表示されます

```
cluster_B::> storage disk option modify -autoassign on *
2 entries were modified.
```

3. サバイバーサイトで、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

```
 cluster_B::> storage disk option show
 Node     BKg. FW. Upd.  Auto Copy   Auto Assign  Auto Assign Policy
--------  -------------  -----------  -----------  ------------------
node_B_1       on             on          on              default
node_B_2       on             on          on              default
2 entries were displayed.

 cluster_B::>
```

関連情報

"ディスクおよびアグリゲートの管理"

"MetroCluster 構成で SyncMirror を使用してデータの冗長性を実現する方法"

アグリゲートの修復とミラーのリストア（ **MetroCluster FC** 構成）

ハードウェアを交換してディスクを割り当てたら、 MetroCluster 修復処理を実行できます。その後、アグリゲートがミラーされたことを確認し、必要に応じてミラーリングを再開します。

手順

1. ディザスタサイトで 2 つの修復フェーズ（アグリゲートの修復とルートの修復）を実行します。

```
cluster_B::> metrocluster heal -phase aggregates

cluster_B::> metrocluster heal -phase root-aggregates
```

2. 修復を監視し、アグリゲートが resyncing または mirrored のいずれかの状態であることを確認します。

「 storage aggregate show -node local 」と入力します

アグリゲートの状態	作業
再同期中です	対処は不要です。アグリゲートの再同期が完了するのを待ちます。

ミラーデグレード	に進みます オフラインのままのプレックスがある場合は、追加の手順を実行してミラーを再構築する必要があります。
ミラー、正常	対処は不要です。
不明、オフラインです	ディザスタサイトのすべてのディスクを交換した場合は、ルートアグリゲートがこの状態になります。

```
cluster_B::> storage aggregate show -node local

 Aggregate     Size Available Used% State   #Vols  Nodes       RAID
Status
 --------- -------- --------- ----- ------- ------ ----------
------------
 node_B_1_aggr1
            227.1GB   11.00GB   95% online       1 node_B_1    raid_dp,
                                                               resyncing
 NodeA_1_aggr2
            430.3GB   28.02GB   93% online       2 node_B_1    raid_dp,
                                                               mirror
                                                               degraded
 node_B_1_aggr3
            812.8GB   85.37GB   89% online       5 node_B_1    raid_dp,
                                                               mirrored,
                                                               normal
 3 entries were displayed.

cluster_B::>
```

次の例では、 3 つのアグリゲートがそれぞれ異なる状態にあります。

ノード	状態
node_B_1 アグリゲート	再同期中です
node_B_1 の aggr2	ミラーデグレード
node_B_1 の aggr3 になります	ミラー、正常

3. 1 つ以上のプレックスがオフラインのままの場合は、ミラーを再構築するための追加の手順が必要です。

   上の表の node_B_1_aggr2 は、ミラーを再構築する必要があります。

a. アグリゲートの詳細を表示して障害プレックスを特定します。

「 storage aggregate show -r -aggregate node_B_1_aggr2 」という名前のアグリゲートがあります

次の例では、プレックス /node_B_1_aggr2/plex0 で障害が発生しています。

```
cluster_B::> storage aggregate show -r -aggregate node_B_1_aggr2

 Owner Node: node_B_1
  Aggregate: node_B_1_aggr2 (online, raid_dp, mirror degraded) (block
checksums)
   Plex: /node_B_1_aggr2/plex0 (offline, failed, inactive, pool0)
    RAID Group /node_B_1_aggr2/plex0/rg0 (partial)
                                                                    Usable
Physical
      Position Disk                     Pool Type     RPM     Size
Size Status
      -------- ------------------------ ---- ----- ------ --------
-------- ----------

   Plex: /node_B_1_aggr2/plex1 (online, normal, active, pool1)
    RAID Group /node_B_1_aggr2/plex1/rg0 (normal, block checksums)
                                                                    Usable
Physical
      Position Disk                     Pool Type     RPM     Size
Size Status
      -------- ------------------------ ---- ----- ------ --------
-------- ----------
      dparity  1.44.8                    1   SAS    15000  265.6GB
273.5GB (normal)
      parity   1.41.11                   1   SAS    15000  265.6GB
273.5GB (normal)
      data     1.42.8                    1   SAS    15000  265.6GB
273.5GB (normal)
      data     1.43.11                   1   SAS    15000  265.6GB
273.5GB (normal)
      data     1.44.9                    1   SAS    15000  265.6GB
273.5GB (normal)
      data     1.43.18                   1   SAS    15000  265.6GB
273.5GB (normal)
 6 entries were displayed.

 cluster_B::>
```

a. 障害が発生したプレックスを削除します。

「 storage aggregate plex delete -aggregate aggregate-name -plex plex 」と入力します

b. ミラーを再確立します。

「 storage aggregate mirror -aggregate aggregate-name 」のように指定します

c. すべてのミラーが再確立され、すべてのアグリゲートが mirrored 、 normal ステータスになるまで、プレックスの再同期とミラーリングのステータスを監視します。

「 storage aggregate show

交換用コントローラモジュールへのルートアグリゲートのディスク所有権の再割り当て（ **MetroCluster FC** 構成）

ディザスタサイトのどちらかまたは両方のコントローラモジュールか NVRAM カードを交換した場合、システム ID が変わっているため、ルートアグリゲートに属するディスクを交換用コントローラモジュールに再割り当てする必要があります。

このタスクについて

ノードがスイッチオーバーモードで、修復が完了しているため、このセクションでは、ディザスタサイトのプール 1 のルートアグリゲートを含むディスクのみを再割り当てします。この時点で古いシステム ID に所有されているのはこれらのディスクだけです。

ここでは、 2 ノードと 4 ノードの構成の例を示します。2 ノード構成の場合、各サイトの 2 つ目のノードに関する説明は無視してください。8 ノード構成の場合は、 2 つ目の DR グループの追加のノードを考慮する必要があります。この例で想定している状況は次のとおりです。

- サイト A はディザスタサイト
  - node_A_1 は交換済み
  - Node_a_2 は交換済み

    4 ノード MetroCluster 構成にのみ存在します。
- サイト B はサバイバーサイトです。
  - node_B_1 は健全
  - node_B_2 は正常

    4 ノード MetroCluster 構成にのみ存在します。

古いシステムIDと新しいシステムIDについては、を参照して "ハードウェアを交換し、新しいコントローラをブート"ください。

この手順の例では、次のシステム ID を持つコントローラを使用します。

ノードの数	ノード	元のシステム ID	新しいシステム ID

4.	node_A_1	4068741258	1574774970
	Node_a_2	4068741260	157477991
	node_B_1	4068741254	変更なし
	node_B_2	4068741256	変更なし
2 つ	node_A_1	4068741258	1574774970

手順

1. メンテナンスモードの交換用ノードで、ルートアグリゲートディスクを再割り当てします。

   「ディスクの再割り当て - s old-system-ID -d new-system-ID 」

   ```
   *> disk reassign -s 4068741258 -d 1574774970
   ```

2. ディスクを表示して、ディザスタサイトの pool1 のルートアグリゲートディスクの所有権が、交換用ノードに変わったことを確認します。

   「ディスクショー」

   出力に表示されるディスク数は、ルートアグリゲート内のディスク数と、そのうち障害が発生して交換したディスクが何本あるかによって変わってきます。ディスクが交換された場合、プール 0 のディスクは出力に表示されません。

   ディザスタサイトのプール 1 のルートアグリゲートディスクが交換用ノードに割り当てられます。

```
*> disk show
Local System ID: 1574774970

  DISK             OWNER                 POOL   SERIAL NUMBER   HOME
DR HOME
------------       -------------         -----  -------------
-------------       -------------
sw_A_1:6.126L19    node_A_1(1574774970) Pool0  serial-number
node_A_1(1574774970)
sw_A_1:6.126L3     node_A_1(1574774970) Pool0  serial-number
node_A_1(1574774970)
sw_A_1:6.126L7     node_A_1(1574774970) Pool0  serial-number
node_A_1(1574774970)
sw_B_1:6.126L8     node_A_1(1574774970) Pool1  serial-number
node_A_1(1574774970)
sw_B_1:6.126L24    node_A_1(1574774970) Pool1  serial-number
node_A_1(1574774970)
sw_B_1:6.126L2     node_A_1(1574774970) Pool1  serial-number
node_A_1(1574774970)

*> aggr status
         Aggr State           Status
 node_A_1_root online          raid_dp, aggr
                               mirror degraded
                               64-bit
*>
```

3. アグリゲートのステータスを表示します。

   「 aggr status 」を入力します

   出力に表示されるディスク数は、ルートアグリゲート内のディスク数と、そのうち障害が発生して交換したディスクが何本あるかによって変わってきます。ディスクが交換された場合、プール 0 のディスクは出力に表示されません。

```
*> aggr status
          Aggr State           Status
  node_A_1_root online          raid_dp, aggr
                                mirror degraded
                                64-bit
*>
```

4. メールボックスディスクの内容を削除します。

   「マイボックス破壊ローカル」

5. アグリゲートがオンラインになっていない場合は、オンラインにします。

   「 aggr online aggr_name 」のようになります

6. ノードを停止して LOADER プロンプトを表示します。

   「 halt 」

新しいコントローラモジュールのブート（ **MetroCluster FC** 構成）

データアグリゲートとルートアグリゲート両方の修復が完了したら、ディザスタサイトのノードをブートする必要があります。

このタスクについて

このタスクは、 LOADER プロンプトが表示されたノードから開始します。

手順

1. ブートメニューを表示します。

   「 boot_ontap menu

2. [step2 、 Step 2] ブートメニューからオプション 6 、 * バックアップ設定からフラッシュを更新 * を選択します。
3. 次のプロンプトに「 y 」と入力します。

   これは ' オール・フラッシュ・ベースの構成をディスクへの最後のバックアップに置き換えます続行してもよろしいですか ?:y`

   システムが 2 回ブートし、 2 回目に新しい設定がロードされます。

   > 使用した交換用コントローラの NVRAM の内容を消去しなかった場合は、パニック状態が発生して「 PANIC ： NVRAM contents are invalid… 」というメッセージが表示されることがあります この場合は、を繰り返します ブートメニューからオプション 6 、 * アップデートフラッシュをバックアップ構成から * 選択します。 システムをブートして ONTAP プロンプトを表示します。次に、が必要です ブートリカバリとr確保 されていないbootargsRDBの破損をリセットします

4. プレックス 0 でルートアグリゲートをミラーします。
   a. 3 本の pool0 ディスクを新しいコントローラモジュールに割り当てます。
   b. ルートアグリゲートの pool1 プレックスをミラーします。

      「 aggr mirror root-aggr-name 」のようになります

   c. 未割り当てディスクをローカルノードのプール 0 に割り当てます
5. 4 ノード構成の場合は、ディザスタサイトのもう一方のノードで上記の手順を繰り返します。
6. MetroCluster 構成を更新します。
   a. advanced 権限モードに切り替えます。

「 advanced 」の権限が必要です

b. 構成を更新します。

MetroCluster configure -refresh true

c. admin 権限モードに戻ります。

「特権管理者」

7. ディザスタサイトの交換用ノードでスイッチバックの準備が完了していることを確認します。

MetroCluster node show

交換用ノードは「 waiting for switchback recovery 」モードになっている必要があります。これらのノードが「通常」モードの場合は、交換用ノードを再起動できます。ブート後、ノードは「 waiting for switchback recovery 」モードになります。

次の例は、交換用ノードでスイッチバックの準備が完了していることを示しています。

```
cluster_B::> metrocluster node show
DR                    Configuration  DR
Grp Cluster Node      State          Mirroring Mode
--- ------- --------- -------------- --------- --------------------
1   cluster_B
            node_B_1  configured     enabled   switchover completed
            node_B_2  configured     enabled   switchover completed
    cluster_A
            node_A_1  configured     enabled   waiting for switchback
recovery
            node_A_2  configured     enabled   waiting for switchback
recovery
4 entries were displayed.

cluster_B::>
```

次に何をするか

に進みます "ディザスタリカバリプロセスを完了する"。

[[Reset-The -boot-recovery]] boot_recoveryとrdata_Corrupt bootargsをリセットします

必要に応じて、boot_recovery引数とrd_corrupt_bootargsをリセットできます

手順

1. ノードを停止してLOADERプロンプトに戻ります。

```
siteA::*> halt -node <node-name>
```

2. 次のbootargsが設定されているかどうかを確認します

```
LOADER> printenv bootarg.init.boot_recovery
LOADER> printenv bootarg.rdb_corrupt
```

3. どちらかのbootargが値に設定されている場合は、設定を解除してONTAP をブートします。

```
LOADER> unsetenv bootarg.init.boot_recovery
LOADER> unsetenv bootarg.rdb_corrupt
LOADER> saveenv
LOADER> bye
```

混在構成でのスイッチバックの準備（移行中のリカバリ）

スイッチバック処理用に MetroCluster IP と FC を混在させる構成を準備するには、特定のタスクを実行する必要があります。この手順のみの環境構成で、 MetroCluster から IP への移行プロセスで障害が発生しました。

このタスクについて

この手順は、障害発生時に移行中だったシステムに対してリカバリを実行する場合にのみ使用してください。

このシナリオでは、 MetroCluster が混在構成です。

- 1 つの DR グループは、ファブリック接続の MetroCluster FC ノードで構成されます。

  作成したノードで MetroCluster FC のリカバリ手順を実行する必要があります。

- 1 つの DR グループは MetroCluster IP ノードで構成されます。

  これらのノードで MetroCluster IP リカバリ手順を実行する必要があります。

手順

次の手順を順序どおりに実行します。

1. 次のタスクを順序どおりに実行して、 FC ノードのスイッチバックを準備します。
   a. "ポート設定の確認（ MetroCluster FC 構成のみ）"
   b. "FC-to-SAS ブリッジの設定（ MetroCluster FC 構成のみ）"
   c. "FC スイッチの設定（ MetroCluster FC 構成のみ）"
   d. "ストレージ構成の確認"（交換した MetroCluster FC ノードのドライブでのみ以下の手順を実行します）

e. "ディザスタサイトの機器の電源投入"（交換した MetroCluster FC ノードのドライブでのみ以下の手順を実行します）

f. "交換したドライブの所有権を割り当てます"（交換した MetroCluster FC ノードのドライブでのみ以下の手順を実行します）

g. の手順を実行します "交換用コントローラモジュールへのルートアグリゲートのディスク所有権の再割り当て（ MetroCluster FC 構成）"メールボックスの破棄コマンドの問題へのステップまで。

h. ルートアグリゲートのローカルプレックス（プレックス 0 ）を破棄します。

「 aggr destroy plex-id 」

i. ルートアグリゲートがオンラインになっていない場合は、オンラインにします。

2. MetroCluster FC ノードをブートします。

これらの手順を両方の MetroCluster FC ノードで実行する必要があります。

a. ブートメニューを表示します。

「 boot_ontap menu

b. ブートメニューからオプション 6 、 * アップデートフラッシュをバックアップ構成から * 選択します。

c. 次のプロンプトに「 y 」と入力します。

これは ' オール・フラッシュ・ベースの構成をディスクへの最後のバックアップに置き換えます続行してもよろしいですか ?:y`

システムが 2 回ブートし、 2 回目に新しい設定がロードされます。

使用した交換用コントローラの NVRAM の内容を消去しなかった場合は、パニック状態が発生して「 PANIC ： NVRAM contents are invalid… 」というメッセージが表示されることがあります この場合は、上記の手順を繰り返して、システムを ONTAP プロンプトにブートします。次に、が必要です ブートリカバリとr確保 されていないbootargsRDBの破損をリセットします

3. プレックス 0 でルートアグリゲートをミラーします。

これらの手順を両方の MetroCluster FC ノードで実行する必要があります。

a. 3 本の pool0 ディスクを新しいコントローラモジュールに割り当てます。

b. ルートアグリゲートの pool1 プレックスをミラーします。

「 aggr mirror root-aggr-name 」のようになります

c. 未割り当てディスクをローカルノードのプール 0 に割り当てます

4. メンテナンスモードに戻ります。

これらの手順を両方の MetroCluster FC ノードで実行する必要があります。

a. ノードを停止します。

「 halt 」

b. ノードをメンテナンス モードで起動します。

「 boot_ontap maint 」を使用してください

5. メールボックスディスクの内容を削除します。

「マイボックス破壊ローカル」

これらの手順を両方の MetroCluster FC ノードで実行する必要があります。

6. ノードを停止します :+`halt

7. ノードがブートしたら、ノードのステータスを確認します。

MetroCluster node show

```
siteA::*> metrocluster node show
DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     siteA
              wmc66-a1           configured     enabled   waiting for
switchback recovery
              wmc66-a2           configured     enabled   waiting for
switchback recovery
      siteB
              wmc66-b1           configured     enabled   switchover
completed
              wmc66-b2           configured     enabled   switchover
completed
2     siteA
              wmc55-a1           -              -         -
              wmc55-a2           unreachable    -         -
      siteB
              wmc55-b1           configured     enabled   switchover
completed
              wmc55-b2           configured
```

8. のタスクを実行して、 MetroCluster IP ノードのスイッチバックを準備します "MetroCluster IP 構成でのスイッチバックの準備" を含むことができます "サバイバーサイトが所有する障害プレックスの削除（ MetroCluster IP 構成）"。

9. MetroCluster FC ノードで、の手順を実行します "アグリゲートの修復とミラーのリストア（ MetroCluster FC 構成）"。

10. MetroCluster IP ノードで、の手順を実行します "アグリゲートの修復とミラーのリストア（ MetroCluster IP 構成）"。

11. 以降のリカバリプロセスの残りのタスクを実行します "FabricPool 構成のオブジェクトストアの再確立"。

[[Reset-The -boot-recovery]] boot_recoveryとrdata_Corrupt bootargsをリセットします

必要に応じて、boot_recovery引数とrd_corrupt_bootargsをリセットできます

手順

1. ノードを停止してLOADERプロンプトに戻ります。

```
siteA::*> halt -node <node-name>
```

2. 次のbootargsが設定されているかどうかを確認します

```
LOADER> printenv bootarg.init.boot_recovery
LOADER> printenv bootarg.rdb_corrupt
```

3. どちらかのbootargが値に設定されている場合は、設定を解除してONTAP をブートします。

```
LOADER> unsetenv bootarg.init.boot_recovery
LOADER> unsetenv bootarg.rdb_corrupt
LOADER> saveenv
LOADER> bye
```

リカバリを完了しています

必要なタスクを実行して、マルチコントローラまたはストレージの障害からのリカバリを完了します。

FabricPool 構成のオブジェクトストアの再確立

FabricPool ミラーのオブジェクトストアの 1 つが MetroCluster ディザスタサイトと同じ場所にあり破損した場合は、そのオブジェクトストアと FabricPool ミラーを再確立する必要があります。

このタスクについて

- オブジェクトストアがリモートにある場合に MetroCluster サイトが破損しても、オブジェクトストアを再構築する必要はなく、オブジェクトストアの元の設定とコールドデータの内容は保持されます。
- FabricPool 構成の詳細については、を参照してください "ディスクとアグリゲートの管理"。

ステップ

1. の手順「 Replacing a FabricPool mirror on a MetroCluster configuration 」に従います "ディスクとアグリゲートの管理"。

交換したノードのライセンスを確認しています

障害ノードが標準（ノードロック）ライセンスを必要とする ONTAP 機能を使用していた場合は、交換ノード用の新しいライセンスをインストールする必要があります。標準ライセンスを使用する機能では、クラスタ内の各ノードにその機能用のキーが必要です。

このタスクについて

ライセンスキーをインストールするまでの間も、標準ライセンスを必要とする機能を交換用ノードで引き続き使用できます。ただし、該当する機能のライセンスがクラスタ内でその障害ノードにしかなかった場合、機能の設定を変更することはできません。また、ライセンスされていない機能をノードで使用するとライセンス契約に違反する可能性があるため、できるだけ早く交換用ノードにライセンスキーをインストールする必要があります。

ライセンスキーは 28 文字の形式です。

ライセンスキーは 90 日間の猶予期間中にインストールする必要があります。この猶予期間を過ぎると、古いライセンスはすべて無効になります。有効なライセンスキーをインストールしたら、 24 時間以内にすべてのキーをインストールする必要があります。



サイトのすべてのノード（ 2 ノード MetroCluster 構成の場合は 1 つのノード）を交換した場合は、スイッチバックの前にライセンスキーを交換用ノードにインストールする必要があります。

手順

1. ノードのライセンスを特定します。

   「 license show 」を参照してください

   次の例は、システム内のライセンスに関する情報を表示します。

```
cluster_B::>  license show
          (system license show)

Serial Number: 1-80-00050
Owner: site1-01
Package           Type       Description             Expiration
-------           -------    -------------           -----------
Base              license    Cluster Base License        -
NFS               site       NFS License                 -
CIFS              site       CIFS License                -
iSCSI             site       iSCSI License               -
FCP               site       FCP License                 -
FlexClone         site       FlexClone License           -

6 entries were displayed.
```

2. スイッチバック後のノードのライセンスに問題がないことを確認します。

「 MetroCluster check license show 」を参照してください

次の例は、ノードのライセンスに問題がないことを表示します。

```
cluster_B::> metrocluster check license show

Cluster           Check                              Result
-------           -------                            -------------
Cluster_B         negotiated-switchover-ready        not-applicable
NFS               switchback-ready                   not-applicable
CIFS              job-schedules                      ok
iSCSI             licenses                           ok
FCP               periodic-check-enabled             ok
```

3. 新しいライセンスキーが必要な場合は、ネットアップサポートサイトの「ソフトウェアライセンス」の下の「サポート」セクションで交換用ライセンスキーを入手します。

> 必要な新しいライセンスキーが自動的に生成され、 E メールで送信されます。30日以内にライセンスキーが記載された電子メールを受信できない場合は、Knowledge Baseの記事の_「ライセンスに問題がある場合は、誰に連絡すればよいですか？」_セクションを参照してください "マザーボードの交換後プロセスを実行して、AFF / FASシステムのライセンスを更新"

4. 各ライセンスキーをインストールします。

'system license add - license-code license-key’license-key…+' を選択します

5. 必要に応じて、古いライセンスを削除します。
   a. 使用されていないライセンスがないかどうか

「 license clean-up-unused - simulate 」を入力します

   b. リストに間違いがなければ、未使用のライセンスを削除します。

「 license clean-up -unused 」のようになります

キー管理をリストアしています

データボリュームが暗号化されている場合は、キー管理をリストアする必要があります。ルートボリュームが暗号化されている場合は、キー管理をリカバリする必要があります。

手順

1. データボリュームが暗号化されている場合は、キー管理設定に対応したコマンドを使用してキーをリストアします。

使用するポート	使用するコマンド

• オンボードキー管理 *	「セキュリティキーマネージャオンボード同期」 詳細については、を参照してください "オンボードキー管理の暗号化キーのリストア"。
• 外部キー管理 *	'security key-manager key query -node node-name 詳細については、を参照してください "外部キー管理の暗号化キーのリストア"。

2. ルートボリュームが暗号化されている場合は、の手順を使用します "ルートボリュームが暗号化されている場合のキー管理のリカバリ"。

スイッチバックを実行しています

MetroCluster 構成の修復が完了したら、 MetroCluster のスイッチバック処理を実行できます。MetroCluster のスイッチバック処理を実行すると、構成が通常の動作状態に戻ります。ディザスタサイトにある同期元の Storage Virtual Machine （ SVM ）がアクティブになり、ローカルディスクプールからデータを提供します。

作業を開始する前に

- ディザスタクラスタからサバイバークラスタへのスイッチオーバーが正常に完了している必要があります。
- データアグリゲートとルートアグリゲートに対して修復が実行されている必要があります。
- サバイバークラスタノードが HA フェイルオーバー状態ではない（各 HA ペアのすべてのノードが稼働中である）必要があります。
- ディザスタサイトのコントローラモジュールが完全にブートしていること、および HA テイクオーバーモードでないことが必要です。
- ルートアグリゲートがミラーされている必要があります。
- スイッチ間リンク（ ISL ）がオンラインになっている必要があります。
- 必要なライセンスがシステムにインストールされている必要があります。

手順

1. すべてのノードの状態が enabled であることを確認します。

   MetroCluster node show

   次の例は、ノードが有効な状態であることを表示します。

```
cluster_B::>  metrocluster node show

DR                         Configuration  DR
Group Cluster Node         State          Mirroring Mode
----- ------- ----------- -------------- --------- --------------------
1     cluster_A
              node_A_1    configured     enabled   heal roots completed
              node_A_2    configured     enabled   heal roots completed
      cluster_B
              node_B_1    configured     enabled   waiting for
switchback recovery
              node_B_2    configured     enabled   waiting for
switchback recovery
4 entries were displayed.
```

2. すべての SVM で再同期が完了したことを確認します。

   MetroCluster vserver show

3. 修復処理で実行される LIF の自動移行が完了していることを確認します。

   MetroCluster check lif show

4. サバイバークラスタ内の任意のノードから MetroCluster switchback コマンドを実行して、スイッチバックを実行します。
5. スイッチバック処理の進捗を確認します。

   「 MetroCluster show 」

   出力に「 waiting - for-switchback 」と表示されている場合は、スイッチバック処理をまだ実行中です。

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                switchover
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                waiting-for-switchback
                          AUSO Failure Domain -
```

   出力に「 normal 」と表示された場合、スイッチバック処理は完了しています。

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
```

スイッチバックの完了に時間がかかる場合は、 advanced 権限レベルで次のコマンドを使用して、進行中のベースライン転送のステータスを確認できます。

「 MetroCluster config-replication resync-status show 」を参照してください

6. SnapMirror 構成または SnapVault 構成があれば、再確立します。

   ONTAP 8.3 では、失われた SnapMirror 構成を MetroCluster スイッチバック処理のあとに手動で再確立する必要があります。ONTAP 9.0 以降では、関係が自動的に再確立されます。

スイッチバックが成功したことを確認する

スイッチバックの実行後に、すべてのアグリゲートと Storage Virtual Machine （ SVM ）がスイッチバックされてオンラインになっていることを確認します。

手順

1. スイッチオーバーされたデータアグリゲートがスイッチバックされたことを確認します。

   「 storage aggregate show

   次の例では、ノード B2 の aggr_b2 がスイッチバックされています。

```
node_B_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 node_B_2   raid_dp,

mirrored,

normal

node_A_1::> aggr show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2          -         -     - unknown      - node_A_1
```

ディザスタサイトにミラーされていないアグリゲートが含まれていて、ミラーされていないアグリゲートが存在しない場合、 storage aggregate show コマンドの出力に「 unknown 」という状態が表示されることがあります。ミラーされていないアグリゲートの古いエントリを削除する方法については、テクニカルサポートにお問い合わせください。サポート技術情報アーティクルを参照してください "ストレージが失われた場合にMetroCluster でミラーされていない古いアグリゲートエントリを削除する方法"

2. サバイバークラスタの同期先のすべてのSVMが休止状態であることを確認します（動作状態が「stopped」と表示されています）。

   `vserver show -subtype sync-destination`

```
node_B_1::> vserver show -subtype sync-destination
                                 Admin    Operational  Root
Vserver       Type    Subtype    State    State        Volume
Aggregate
-----------   ------- ---------- -------- ----------   --------
----------
...
cluster_A-vs1a-mc data sync-destination
                               running    stopped    vs1a_vol   aggr_b2
```

MetroCluster 構成の同期先アグリゲートの名前には、識別しやすいように「 -mc 」というサフィックスが自動的に付加されます。

3. ディザスタクラスタの同期元SVMが稼働していることを確認します。

「 vserver show -subtype sync-source 」のようになります

```
node_A_1::> vserver show -subtype sync-source
                                  Admin    Operational  Root
Vserver        Type    Subtype    State    State        Volume
Aggregate
-----------    ------- ---------- -------- ----------   --------
----------
...
vs1a           data    sync-source
                                  running  running    vs1a_vol  aggr_b2
```

4. MetroCluster operation show コマンドを使用して、スイッチバック操作が成功したことを確認します。

出力内容	作業
スイッチバック処理の状態が「 successful 」である	スイッチバックプロセスは完了しており、システムの処理を続行できます。
スイッチバック処理またはスイッチバック継続エージェントの処理が「 partially successful 」である	MetroCluster operation show コマンドの出力に記載されている推奨修正を実行します。

完了後

上記の手順を繰り返して、逆方向へのスイッチバックを実行する必要があります。site_A が site_B のスイッチオーバーを行った場合は、 site_B で site_A のスイッチオーバーを行います

交換用ノードのルートアグリゲートをミラーリング

ディスクを交換した場合は、ディザスタサイトで新しいノードのルートアグリゲートをミラーする必要があります。

手順

1. ディザスタサイトで、ミラーリングされていないアグリゲートを特定します。

「 storage aggregate show

```
cluster_A::> storage aggregate show

Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_A_1_aggr0
            1.49TB   74.12GB   95% online       1 node_A_1
raid4,

normal
node_A_2_aggr0
            1.49TB   74.12GB   95% online       1 node_A_2
raid4,

normal
node_A_1_aggr1
            1.49TB   74.12GB   95% online       1 node_A_1         raid
4, normal

mirrored
node_A_2_aggr1
            1.49TB   74.12GB   95% online       1 node_A_2         raid
4, normal

mirrored
4 entries were displayed.

cluster_A::>
```

2. 1 つのルートアグリゲートをミラーします。

   「 storage aggregate mirror -aggregate root-aggregate 」のように表示されます

   次の例は、アグリゲートをミラーするコマンドでディスクを選択し、確認を求めるプロンプトを表示する方法を示しています。

```
cluster_A::> storage aggregate mirror -aggregate node_A_2_aggr0

Info: Disks would be added to aggregate "node_A_2_aggr0" on node
"node_A_2" in
      the following manner:

      Second Plex

        RAID Group rg0, 3 disks (block checksum, raid4)
          Position   Disk                      Type
Size
          ---------- ------------------------- ----------
---------------
          parity     2.10.0                    SSD
-
          data       1.11.19                   SSD
894.0GB
          data       2.10.2                    SSD
894.0GB

      Aggregate capacity available for volume use would be 1.49TB.

Do you want to continue? {y|n}: y

cluster_A::>
```

3. ルートアグリゲートのミラーリングが完了したことを確認します。

   「 storage aggregate show

   次の例は、ルートアグリゲートがミラーされたことを示しています。

```
cluster_A::> storage aggregate show

Aggregate     Size Available Used% State   #Vols  Nodes       RAID
Status
--------- -------- --------- ----- ------- ------ ----------
------------
node_A_1_aggr0
            1.49TB   74.12GB   95% online       1 node_A_1    raid4,
                                                               mirrored,
                                                               normal
node_A_2_aggr0
            2.24TB   838.5GB   63% online       1 node_A_2    raid4,
                                                               mirrored,
                                                               normal
node_A_1_aggr1
            1.49TB   74.12GB   95% online       1 node_A_1    raid4,
                                                               mirrored,
                                                               normal
node_A_2_aggr1
            1.49TB   74.12GB   95% online       1 node_A_2    raid4
                                                               mirrored,
                                                               normal
4 entries were displayed.

cluster_A::>
```

4. 他のルートアグリゲートについても、上記の手順を繰り返します。

   ステータスがミラーリングされていないルートアグリゲートはミラーリングする必要があります。

ONTAP Mediator（MetroCluster IP構成）の再構成

ONTAP Mediator を使用して設定された MetroCluster IP 構成がある場合は、ONTAP Mediator との関連付けを削除して再設定する必要があります。

作業を開始する前に

- ONTAP Mediator の IP アドレス、ユーザー名、パスワードが必要です。
- ONTAP Mediator が Linux ホスト上で設定され、動作している必要があります。

手順

1. 既存の ONTAP メディエーター設定を削除します。

   MetroCluster 構成設定のメディエーターが削除されました

2. ONTAP メディエーター設定を再設定します。

MetroCluster 構成設定メディエーターの追加メディエーターのアドレスメディエータの IP アドレス

MetroCluster 構成の健全性の確認

MetroCluster 構成の健全性をチェックして、正常に動作することを確認する必要があります。

手順

1. 各クラスタで MetroCluster が設定されており、通常モードであることを確認します。

   「 MetroCluster show 」

```
cluster_A::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-disaster
Remote: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-disaster
```

2. 各ノードでミラーリングが有効であることを確認します。

   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_1       configured     enabled   normal
2 entries were displayed.
```

3. 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 」のようになります

```
cluster_A::> metrocluster check run

Last Checked On: 10/1/2014 16:03:37

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
4 entries were displayed.

Command completed. Use the `metrocluster check show -instance` command
or sub-commands in `metrocluster check` directory for detailed results.
To check if the nodes are ready to do a switchover or switchback
operation, run `metrocluster switchover -simulate` or `metrocluster
switchback -simulate`, respectively.
```

4. ヘルスアラートがないことを確認します。

   「 system health alert show 」というメッセージが表示されます

5. スイッチオーバー処理をシミュレートします。

   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 モードで続けるかどうかを尋ねられたら、「 y 」と入力して応答する必要があります。advanced モードのプロンプトが表示されます（ * > ）。

   a. 「 -simulate 」パラメータを指定して、スイッチオーバー操作を実行します。

      MetroCluster switchover -simulate

   b. admin 権限レベルに戻ります。

      「特権管理者」

6. ONTAP Mediator を使用した MetroCluster IP 構成の場合は、ONTAP Mediator が起動して動作していることを確認します。

   a. メディエーターディスクがシステムから認識されていることを確認します。

      「 storage failover mailbox-disk show 」をクリックします

      次の例は、メールボックスディスクが認識されていることを示しています。

```
node_A_1::*> storage failover mailbox-disk show
                 Mailbox
Node             Owner     Disk    Name        Disk UUID
-------------     ------   -----   -----        ---------------
sti113-vsim-ucs626g
.
.
     local     0m.i2.3L26
7BBA77C9:AD702D14:831B3E7E:0B0730EE:00000000:00000000:00000000:000000
00:00000000:00000000
     local     0m.i2.3L27
928F79AE:631EA9F9:4DCB5DE6:3402AC48:00000000:00000000:00000000:000000
00:00000000:00000000
     local     0m.i1.0L60
B7BCDB3C:297A4459:318C2748:181565A3:00000000:00000000:00000000:000000
00:00000000:00000000
.
.
.
     partner   0m.i1.0L14
EA71F260:D4DD5F22:E3422387:61D475B2:00000000:00000000:00000000:000000
00:00000000:00000000
     partner   0m.i2.3L64
4460F436:AAE5AB9E:D1ED414E:ABF811F7:00000000:00000000:00000000:000000
00:00000000:00000000
28 entries were displayed.
```

b. advanced 権限レベルに切り替えます。

   「 advanced 」の権限が必要です

c. メールボックス LUN がシステムから認識されていることを確認します。

   「 storage iscsi-initiator show 」のように表示されます

   メールボックス LUN があることを示す出力が表示されます。

```
Node    Type        Label      Target Portal     Target Name
Admin/Op
----    ----        --------   ---------    ---------
--------------------------------       --------
.
.
.
.node_A_1
               mailbox
                     mediator 172.16.254.1    iqn.2012-
05.local:mailbox.target.db5f02d6-e3d3    up/up
.
.
.
17 entries were displayed.
```

a. admin 権限レベルに戻ります。

「特権管理者」

コントローラ以外の障害からのリカバリ

ディザスタサイトの機器に対して必要なメンテナンスまたは交換を実施し、その際にコントローラを交換しなかった場合は、続けて MetroCluster 構成を完全に冗長な状態に戻す手順を開始できます。これには、設定の修復（データアグリゲート、ルートアグリゲートの順）とスイッチバック処理が含まれます。

作業を開始する前に

- ディザスタクラスタのすべての MetroCluster ハードウェアが動作している必要があります。
- MetroCluster 構成全体がスイッチオーバー中である必要があります。
- ファブリック接続 MetroCluster 構成では、 MetroCluster サイト間で ISL が稼働している必要があります。

コンソールログを有効にする

NetAppでは、使用しているデバイスでコンソールロギングをイネーブルにし、この手順を実行する際に次のアクションを実行することを強く推奨します。

- メンテナンス中はAutoSupportを有効のままにします。
- メンテナンスの前後にメンテナンスAutoSupportメッセージをトリガーして、メンテナンスアクティビティ中にケースの作成を無効にします。

  ナレッジベースの記事を参照してください "スケジュールされたメンテナンス時間中にケースの自動作成を停止する方法"。

- 任意のCLIセッションのセッションロギングをイネーブルにします。セッションログを有効にする方法については、ナレッジベースの記事の「セッション出力のログ」セクションを参照してください "ONTAPシステムへの接続を最適化するためのPuTTYの設定方法"。

MetroCluster構成での構成の修復

MetroCluster FC構成では、特定の順序で修復処理を実行して、スイッチオーバー後にMetroCluster機能をリストアします。

MetroCluster IP構成では、スイッチオーバー後に修復処理が自動的に開始されます。サポートされていない場合は、修復処理を手動で実行できます。

作業を開始する前に

- スイッチオーバーを実行済みで、サバイバーサイトがデータを提供している必要があります。
- ディザスタサイトのノードが停止しているか、電源がオフのままになっている必要があります。

  修復プロセスでは、これらのノードを完全にブートしないでください。

- ディザスタサイトのストレージにアクセスできる（シェルフは電源がオンで稼働しており、アクセス可能である）必要があります。
- ファブリック接続 MetroCluster 構成では、スイッチ間リンク（ ISL ）が稼働している必要があります。
- 4 ノード MetroCluster 構成では、サバイバーサイトのノードが HA フェイルオーバー状態でない（各 HA ペアのすべてのノードが稼働中である）必要があります。

このタスクについて

修復処理は、最初にデータアグリゲートで実行し、次にルートアグリゲートで実行する必要があります。

データアグリゲートの修復

ディザスタサイトのハードウェアを修理および交換したら、データアグリゲートを修復する必要があります。この処理では、データアグリゲートを再同期し、（修復された）ディザスタサイトを通常の動作用に準備します。データアグリゲートの修復は、ルートアグリゲートの修復の前に行う必要があります。

このタスクについて

次の例は、強制スイッチオーバーを示しており、スイッチオーバーされたアグリゲートをオンラインにします。リモートクラスタでの構成の更新はすべてローカルクラスタにレプリケートされます。この手順の一部としてディザスタサイトのストレージに電源を投入しますが、ディザスタサイトにあるコントローラモジュールの電源はオンにしないでください。

手順

1. スイッチオーバーが完了したことを確認します。

   「 MetroCluster operation show 」を参照してください

```
controller_A_1::> metrocluster operation show
  Operation: switchover
      State: successful
 Start Time: 7/25/2014 20:01:48
   End Time: 7/25/2014 20:02:14
     Errors: -
```

2. サバイバークラスタから次のコマンドを実行して、データアグリゲートを再同期します。

「 MetroCluster heal-phase aggregates 」

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

修復が拒否された場合は '--overriding-siding’parameter を指定して MetroCluster heal-(修復) コマンドを再実行できますこのオプションパラメータを使用すると、修復処理を妨げるソフトな拒否はすべて無視されます。

3. 処理が完了したことを確認します。

「 MetroCluster operation show 」を参照してください

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2014 18:45:55
   End Time: 7/25/2014 18:45:56
     Errors: -
```

4. アグリゲートの状態を確認します。

「 storage aggregate show 」コマンドを実行します。

```
controller_A_1::> storage aggregate show
Aggregate Size     Available Used% State   #Vols  Nodes        RAID
Status
--------- -------- --------- ----- ------- ------ ------------
------------
...
aggr_b2   227.1GB  227.1GB   0%    online  0      mcc1-a2      raid_dp,
mirrored, normal...
```

5. ディザスタサイトのストレージを交換した場合は、アグリゲートの再ミラーリングが必要になることがあ

ります。

災害発生後のルートアグリゲートの修復

データアグリゲートの修復が完了したら、スイッチバック処理に備えてルートアグリゲートを修復する必要があります。

作業を開始する前に

MetroCluster 修復プロセスのデータアグリゲートの修復が完了している必要があります。

手順

1. ミラーされたアグリゲートをスイッチバックします。

   「 MetroCluster heal-phase root-aggregates 」

   ```
   mcc1A::> metrocluster heal -phase root-aggregates
   [Job 137] Job succeeded: Heal Root Aggregates is successful
   ```

   修復が拒否された場合は '--overriding-siding’parameter を指定して MetroCluster heal-(修復) コマンドを再実行できますこのオプションパラメータを使用すると、修復処理を妨げるソフトな拒否はすべて無視されます。

2. デスティネーションクラスタで次のコマンドを実行して、修復処理が完了していることを確認します。

   「 MetroCluster operation show 」を参照してください

   ```
   mcc1A::> metrocluster operation show
     Operation: heal-root-aggregates
         State: successful
    Start Time: 7/29/2014 20:54:41
      End Time: 7/29/2014 20:54:42
        Errors: -
   ```

スイッチバックに向けたシステムの事前チェック

システムがすでにスイッチオーバー状態にある場合は、「 -simulate 」オプションを使用して、スイッチバック処理の結果をプレビューできます。

手順

1. ディザスタサイトの各コントローラモジュールに電源を投入します。

ノードの電源がオフになっている場合：
ノードの電源をオンにします

ノードに**LOADER**プロンプトが表示されている場合：
次のコマンドを実行します。 `boot_ontap`

2. ノードのブートが完了したら、ルートアグリゲートがミラーされていることを確認します。

プレックスに障害が発生した場合:

a. 障害が発生したプレックスを破棄します。

```
storage aggregate plex delete -aggregate <aggregate_name> -plex
<plex_name>
```

b. ミラーを再作成してミラー関係を再確立します。

「 storage aggregate mirror -aggregate <aggregate-name> 」の形式で指定します

プレックスがオフラインの場合:
プレックスをオンラインにする:

```
storage aggregate plex online -aggregate <aggregate_name> -plex <plex_name>
```

両方のプレックスが存在する場合:
再同期が自動的に開始されます

3. スイッチバック処理をシミュレートします。

a. どちらかのサバイバー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 モードで続けるかどうかを尋ねられたら、「 y 」と入力して応答する必要があります。
advanced モードのプロンプトが表示されます（ * > ）。

a. 「 -simulate 」パラメータを指定して、スイッチバック操作を実行します。

MetroCluster switchback -simulate

b. admin 権限レベルに戻ります。

「特権管理者」

4. 返された出力を確認します。

出力には、スイッチバック処理でエラーが発生するかどうかが示されます。

検証結果の例

次の例は、スイッチバック処理を正常に実行できる場合の出力を示しています。

```
cluster4::*> metrocluster switchback -simulate
  (metrocluster switchback)
[Job 130] Setting up the nodes and cluster components for the switchback
operation...DBG:backup_api.c:327:backup_nso_sb_vetocheck : MetroCluster
Switch Back
[Job 130] Job succeeded: Switchback simulation is successful.

cluster4::*> metrocluster op show
  (metrocluster operation show)
  Operation: switchback-simulate
      State: successful
 Start Time: 5/15/2014 16:14:34
   End Time: 5/15/2014 16:15:04
     Errors: -

cluster4::*> job show -name Me*
                            Owning
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
130    MetroCluster Switchback
                            cluster4
                                       cluster4-01
                                                      Success
       Description: MetroCluster Switchback Job - Simulation
```

スイッチバックを実行しています

MetroCluster 構成の修復が完了したら、 MetroCluster のスイッチバック処理を実行できます。MetroCluster のスイッチバック処理を実行すると、構成が通常の動作状態に戻ります。ディザスタサイトにある同期元の Storage Virtual Machine （ SVM ）がアクティブになり、ローカルディスクプールからデータを提供します。

作業を開始する前に

- ディザスタクラスタからサバイバークラスタへのスイッチオーバーが正常に完了している必要があります。
- データアグリゲートとルートアグリゲートに対して修復が実行されている必要があります。
- サバイバークラスタノードが HA フェイルオーバー状態ではない（各 HA ペアのすべてのノードが稼働中である）必要があります。
- ディザスタサイトのコントローラモジュールが完全にブートしていること、および HA テイクオーバーモードでないことが必要です。
- ルートアグリゲートがミラーされている必要があります。
- スイッチ間リンク（ ISL ）がオンラインになっている必要があります。

- 必要なライセンスがシステムにインストールされている必要があります。

手順

1. すべてのノードの状態が enabled であることを確認します。

   MetroCluster node show

   次の例は、「 enabled 」状態のノードを表示します。

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- ------------ -------------- --------- --------------------
1     cluster_A
              node_A_1     configured     enabled   heal roots completed
              node_A_2     configured     enabled   heal roots completed
      cluster_B
              node_B_1     configured     enabled   waiting for
switchback recovery
              node_B_2     configured     enabled   waiting for
switchback recovery
4 entries were displayed.
```

2. すべての SVM で再同期が完了したことを確認します。

   MetroCluster vserver show

3. 修復処理で実行される LIF の自動移行が完了していることを確認します。

   MetroCluster check lif show

4. サバイバークラスタ内の任意のノードから次のコマンドを実行して、スイッチバックを実行します。

   MetroCluster スイッチバック

5. スイッチバック処理の進捗を確認します。

   「 MetroCluster show 」

   出力に「 waiting - for-switchback 」と表示されている場合は、スイッチバック処理をまだ実行中です。

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                switchover
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                waiting-for-switchback
                          AUSO Failure Domain -
```

出力に「 normal 」と表示された場合、スイッチバック処理は完了しています。

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
```

スイッチバックの完了に時間がかかる場合は、次のコマンドを advanced 権限レベルで使用して、進行中のベースライン転送のステータスを確認できます。

「 MetroCluster config-replication resync-status show 」を参照してください

6. SnapMirror 構成または SnapVault 構成があれば、再確立します。

   ONTAP 8.3 では、失われた SnapMirror 構成を MetroCluster スイッチバック処理のあとに手動で再確立する必要があります。ONTAP 9.0 以降では、関係が自動的に再確立されます。

スイッチバックが成功したことを確認する

スイッチバックの実行後に、すべてのアグリゲートと Storage Virtual Machine （ SVM ）がスイッチバックされてオンラインになっていることを確認します。

手順

1. スイッチオーバーされたデータアグリゲートがスイッチバックされたことを確認します。

   「 storage aggregate show

   次の例では、ノード B2 の aggr_b2 がスイッチバックされています。

```
node_B_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 node_B_2   raid_dp,

mirrored,

normal

node_A_1::> aggr show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2          -         -     - unknown      - node_A_1
```

ディザスタサイトにミラーされていないアグリゲートが含まれていて、ミラーされていないアグリゲートが存在しない場合、「 storage aggregate show 」コマンドの出力に「 unknown 」と表示されることがあります。ミラーされていないアグリゲートの古いエントリを削除する方法については、テクニカルサポートにお問い合わせください。また、技術情報アーティクルも参照してください "ストレージが失われた場合にMetroCluster でミラーされていない古いアグリゲートエントリを削除する方法"

2. サバイバークラスタの同期先のすべてのSVMが休止状態であることを確認します（動作状態が「stopped」と表示されています）。

   `vserver show -subtype sync-destination`

```
node_B_1::> vserver show -subtype sync-destination
                                 Admin    Operational  Root
Vserver       Type    Subtype    State    State        Volume
Aggregate
-----------   ------- ---------- -------- ----------   --------
----------
...
cluster_A-vs1a-mc data sync-destination
                               running    stopped    vs1a_vol   aggr_b2
```

MetroCluster 構成の同期先アグリゲートの名前には、識別しやすいように「 -mc 」というサフィックスが自動的に付加されます。

3. ディザスタクラスタの同期元SVMが稼働していることを確認します。

「 vserver show -subtype sync-source 」のようになります

```
node_A_1::> vserver show -subtype sync-source
                                  Admin    Operational  Root
Vserver        Type    Subtype    State    State        Volume
Aggregate
-----------    ------- ---------- -------- ----------   --------
----------
...
vs1a           data    sync-source
                                  running  running    vs1a_vol  aggr_b2
```

4. スイッチバック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

出力内容	作業
スイッチバック処理の状態が「 successful 」である	スイッチバックプロセスは完了しており、システムの処理を続行できます。
スイッチバック操作または 'witchback-tile-agent' 操作が部分的に成功していること	MetroCluster operation show コマンドの出力に記載されている推奨修正を実行します

完了後

上記の手順を繰り返して、逆方向へのスイッチバックを実行する必要があります。site_A が site_B のスイッチオーバーを行った場合は、 site_B で site_A のスイッチオーバーを行います

スイッチバック後の古いアグリゲートリストの削除

スイッチバック後に古いアグリゲートが残っていることがあります。古いアグリゲートとは、 ONTAP からは削除されたものの、情報がまだディスクに記録されたままのアグリゲートのことです。古いアグリゲートは「 nodeshell aggr status -r 」コマンドで表示されますが、「 storage aggregate show 」コマンドでは表示されません。これらのレコードを削除して、表示されないようにすることができます。

このタスクについて

古いアグリゲートは、 MetroCluster 構成のスイッチオーバー中にアグリゲートを再配置すると発生する可能性があります。例：

1. サイト A がサイト B にスイッチオーバーします
2. 負荷分散のため、アグリゲートのミラーリングを削除し、 node_B_1 から node_B_2 にアグリゲートを再配置します。
3. アグリゲートの修復を実行します。

この時点では、アグリゲートそのものは node_B_1 から削除されているにもかかわらず、古いアグリゲートがこのノードに表示されます。このアグリゲートは、「 nodeshell aggr status -r 」コマンドの出力に表示され

ます。「 storage aggregate show 」コマンドの出力には表示されません。

1. 次のコマンドの出力を比較します。

   「 storage aggregate show

   'run local aggr status -r を実行します

   古いアグリゲートは「 run local aggr status -r 」の出力には表示されますが、「 storage aggregate show 」の出力には表示されません。たとえば、次のアグリゲートが「 run local aggr status -r 」の出力に表示される場合があります。

```
Aggregate aggr05 (failed, raid_dp, partial) (block checksums)
Plex /aggr05/plex0 (offline, failed, inactive)
  RAID group /myaggr/plex0/rg0 (partial, block checksums)

 RAID Disk Device  HA  SHELF BAY CHAN Pool Type  RPM  Used (MB/blks)
Phys (MB/blks)
 --------- ------  ------------- ---- ---- ----  ----- --------------
--------------
 dparity   FAILED          N/A                        82/ -
 parity    0b.5    0b    -   -   SA:A   0 VMDISK  N/A 82/169472
88/182040
 data      FAILED          N/A                        82/ -
 data      FAILED          N/A                        82/ -
 data      FAILED          N/A                        82/ -
 data      FAILED          N/A                        82/ -
 data      FAILED          N/A                        82/ -
 data      FAILED          N/A                        82/ -
 Raid group is missing 7 disks.
```

2. 古いアグリゲートを削除します。

   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 モードで続けるかどうかを尋ねられたら、「 y 」と入力して応答する必要があります。advanced モードのプロンプトが表示されます（ * > ）。

   a. 古いアグリゲートを削除します。

      「 aggregate remove-stale-record -aggregate aggregate_name 」のようになります

   b. admin 権限レベルに戻ります。

      「特権管理者」

3. 古いアグリゲートのレコードが削除されたことを確認します。

'run local aggr status -r を実行します

法的通知

著作権に関する声明、商標、特許などにアクセスできます。

著作権

"https://www.netapp.com/company/legal/copyright/"

商標

NetApp 、 NetApp のロゴ、および NetApp の商標ページに記載されているマークは、 NetApp, Inc. の商標です。その他の会社名および製品名は、それぞれの所有者の商標である場合があります。

"https://www.netapp.com/company/legal/trademarks/"

特許

ネットアップが所有する特許の最新リストは、次のサイトで入手できます。

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

プライバシーポリシー

"https://www.netapp.com/company/legal/privacy-policy/"

安全に関する情報と規制に関する通知

https://library.netapp.com/ecm/ecm_download_file/ECMP12475945

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権を有し、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権については、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。