



アップグレードを準備

ONTAP MetroCluster

NetApp
February 13, 2026

目次

アップグレードを準備	1
このMetroCluster IPアップグレード手順を使用するための要件	1
この手順でサポートされているプラットフォーム	1
要件	1
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	2
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）	3
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	3
ステップ2: 古いコントローラに設定するbootargを決定する	3
ステップ3: 古いコントローラに必要なbootargを設定する	4
MetroCluster IPシステムのアップグレードを準備	5
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	5
古いノードから新しいノードへのポートのマッピング	7
新しいコントローラをネットブート	8
コントローラモジュールの設定をクリアします	10
サイトをアップグレードする前に MetroCluster の健全性を確認	10
アップグレード前に情報を収集	12
メディエーターまたは Tiebreaker の監視を削除します	14
カスタム AutoSupport メッセージをメンテナンス前に送信する	15

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、["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"](#)で、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ロット数が元のシステムの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 \(9.15.1以降で導入されたシステムにアップグレードする場合\)"](#) で、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、ONTAPIはnode_A_1-oldと同じポートでLIFをホストしようとしてします。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ットの物理ポート		
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。 <code>ifconfig e0M -auto</code>
静的	手動接続を設定します。 <code>ifconfig e0M -addr= ip_addr-mask= netmask _ -gw= _gateway`</code>

- 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へ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. 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

- 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](#)"。

- 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。
- 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

- 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.
```

メディアエーターまたは **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 またはメディア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

- 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、メディアエーター、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"
メディアエーター	ONTAP プロンプトで次のコマンドを問題に設定します。 MetroCluster 構成設定のメディア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。

著作権に関する情報

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および/または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。