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

Upgrade controllers

NetApp
March 11, 2026

目次

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

ARLアップグレード手順について学ぶ

コントローラハードウェアをアップグレードするには、アグリゲート再配置（ARL）の方法が複数あります。この手順では、ONTAP 9.8以降を実行しているシステムで、「システムコントローラ置換コマンド」を使用してアグリゲート再配置（ARL）を行い、コントローラハードウェアをアップグレードする方法について説明します。

手順の実行中に、交換用コントローラハードウェアを使用して元のコントローラハードウェアをアップグレードし、ルート以外のアグリゲートの所有権を切り替えます。アグリゲートをノードからノードに複数回移行して、アップグレード手順 全体を通じて、少なくとも 1 つのノードがアグリゲートからデータを提供していることを確認します。また、処理を続行する前に、データ論理インターフェイス（ LIF ）を移行し、新しいコントローラのネットワークポートをインターフェイスグループに割り当てます。

この情報で使用される用語

この情報では、元のノードの名前は「 node1 」と「 node2 」になり、新しいノードの名前は「 node3 」と「 node4 」になります。この手順では、ノード1をノード3に、ノード2をノード4に置き換えます。

「 node1 」、「 node2 」、「 node3 」、および「 node4 」は、元のノードと新しいノードを区別するためだけに使用されます。手順を実行するときは、元のノードと新しいノードの実際の名前に置き換える必要があります。ただし実際には、コントローラハードウェアのアップグレード後もノードの名前は変わりません。ノード3の名前はnode1になり、ノード4の名前はnode2になります。

重要な情報：

- この手順は複雑で、 ONTAP の高度な管理スキルがあることを前提としています。また、以下の内容を読んで理解する必要があります。 "ARLを使用したコントローラのアップグレードに関するガイドライン"そして"ARLアップグレードシーケンス"アップグレードを開始する前に。
- この手順は、交換用コントローラハードウェアが新しく購入され、使用されていないことを前提としています。使用済みのコントローラを「 wipeconfig 」コマンドで準備するために必要な手順は、この手順には含まれていません。交換用コントローラハードウェアを以前に使用していた場合は、テクニカルサポートに問い合わせる必要があります。特に、コントローラが Data ONTAP 7-Mode を実行していた場合は、テクニカルサポートにお問い合わせください。
- ARL を使用すると、システムを停止することなく、アップグレードするクラスタよりも新しいバージョンの ONTAP を実行する新しいコントローラへのアップグレードを実行できます。古いコントローラと新しいコントローラの ONTAP バージョンの組み合わせは、 ONTAP ソフトウェアリリースの NDU モデルによって決まります。たとえば、 ONTAP 9.8 を実行しているコントローラがあり、そのコントローラで最後にサポートされていたバージョンである場合は、 ONTAP 9.8 より後のバージョンの ONTAP を実行している新しいコントローラにアップグレードできます。

  このアップグレード手順では、交換するコントローラモデルで ONTAP の新しいバージョンがサポートされておらず、新しいコントローラで以前のバージョンの ONTAP がサポートされていない主な環境アップグレードシナリオを使用します。

- この手順を使用して、ノードが 3 つ以上あるクラスタでコントローラハードウェアをアップグレードでき

ます。ただし、クラスタ内のハイアベイラビリティ（ HA ）ペアごとに手順を個別に実行する必要があります。

- この手順は、 FASシステムとAFFシステムに適用されます。
- この手順環境システムは、 4 ノードの NetApp MetroCluster 構成以上を実行しています。MetroCluster 構成サイトは物理的に異なる場所に設置できるため、 HA ペアの場合は各 MetroCluster サイトでコントローラの自動アップグレードを個別に実行する必要があります。
- HA クラスタなどの MetroCluster 以外手順のシステムでは、 ARL アップグレードのみがサポートされます。
- AFF A320 システムからアップグレードする場合は、ボリューム移動を使用してコントローラハードウェアをアップグレードするか、テクニカルサポートにお問い合わせください。を参照してください "参考資料" をクリックして、ボリュームまたは storage _ を移動して _ Upgrade にリンクします。

コントローラのアップグレードプロセスを自動化する

コントローラのアップグレード時に、コントローラは、より新しい、またはより強力なプラットフォームを実行する別のコントローラに交換されます。このコンテンツの以前のバージョンには、完全に手動で実行するだけで構成されるコントローラの無停止更新プロセスの手順が含まれていました。このコンテンツでは、新しい自動手順の手順を紹介します。自動化された新しい では、ネットワークポートの到達可能性チェックが自動化され、コントローラのアップグレードがさらに簡単になります。

手動での作業は時間がかかり複雑でしたが、この簡易化された手順 では、アグリゲートの再配置を使用してコントローラの更新を実装できるため、 HA ペアの無停止アップグレードをより効率的に実行できます。特に、検証、情報収集、および事後チェックに関連する手動手順は大幅に少なくなります。

この集約再配置手順を使用するかどうかを決定します

コントローラハードウェアをアップグレードするには、アグリゲート再配置（ARL）の方法が複数あります。この手順では、ONTAP 9.8以降を実行しているシステムで、「システムコントローラ置換コマンド」を使用してアグリゲート再配置（ARL）を行い、コントローラハードウェアをアップグレードする方法について説明します。この複雑な手順は、経験豊富なONTAP管理者のみが実行できます。

この ARL 手順がコントローラ ハードウェアのアップグレードに適しているかどうかを判断するには、サポートされているアップグレードについて次の状況をすべて確認する必要があります。

- ONTAP 9.8以降を実行している。
- 新しいコントローラを新しいHAペアとしてクラスタに追加したり、ボリューム移動を使用してデータを移行したりすることはありません。
- ONTAPの管理経験があり、diagnostic権限モードで作業する場合のリスクを十分に理解していること。
- MetroCluster構成をアップグレードする場合は、4ノード以上のFC構成で、すべてのノードでONTAP 9.8以降が実行されています。

  MetroCluster IP構成のアップグレードについては、MetroCluster Upgrade and Expansion_へのリンクを参照してください"参考資料"。

- 同じシャーシ内のコントローラモジュールを交換してシステムをアップグレードする場合、例えば AFF A800 または AFF C800 、NetApp は"ARLを使用してコントローラモデルをアップグレードし、既存のシステムシャーシ、ディスク、データを維持します"アップグレード手順の使用を強く推奨します。この ARL 手順には、アップグレード手順中にコントローラを取り外したり取り付けたりするときに、内部ディスクがシャーシ内で安全な状態を保つための手順が含まれています。

  "既存のシステムシャーシ、ディスク、データを維持しながら、ARLを使用してサポートされているシステムアップグレードの組み合わせについて学習します"。

- この手順 では、NetApp Storage Encryption（NSE）、NetApp Volume Encryption（NVE）、およびNetApp Aggregate Encryption（NAE）を使用できます。

サポートされているシステムアップグレードの組み合わせ

次の表は、この ARL 手順を使用してコントローラのアップグレードを実行する場合にサポートされるシステム マトリックスを示しています。

古いコントローラ	交換用コントローラ
FAS8020 [3]、FAS8040 [3]、FAS8060、FAS8080	FAS8200 、 FAS8300 、 FAS8700 、 FAS9000
FAS8060 [4]、FAS8080 [4]	FAS9500
AFF8020[3]、AFF8040[3]、AFF8060、AFF8080を参照してください	AFF A300 、 AFF A400 、 AFF A700 、 AFF A800^1
AFF8060 [4]、AFF8080 [4]	AFF A900 の略
FAS8200	FAS8300 [2]、FAS8700、FAS9000、FAS9500
FAS8300、FAS8700、FAS9000	FAS9500
AFF A300	AFF A400 [2]、AFF A700、AFF A800^1 ^、AFF A900
AFF A320 [4]	AFF A400
AFF A400 、 AFF A700	AFF A900 の略
FAS2620[4]、FAS2720[4]	FAS2820

コントローラのアップグレードモデルの組み合わせが上記の表にない場合は、テクニカルサポートにお問い合わせください。

[1] AFF A800システムに必要なその他の手順については、セクション"ノード1のディスクをノード3に再割り当て（手順9）"、またはのA800に関する説明に記載されている手順に進みます"ノード2のディスクをノード4に再割り当て（手順9）"。

[2]2ノードスイッチレスクラスタ構成でAFF A300からAFF A400、またはFAS8200からFAS8300システムにアップグレードする場合は、コントローラのアップグレード用に一時的なクラスタポートを選択する必要があります。AFF A400 および FAS8300 システムは、イーサネットバンドルとして、メザニンカードポートはイーサネットタイプ、 FC タイプの FC バンドルとして、 2 種類の構成で提供されます。

- AFF A400 または FAS8300 では、イーサネットタイプの構成の場合、 2 つのメザニンポートのいずれかを一時的なクラスタポートとして使用できます。

- AFF A400 または FC タイプの構成で FAS8300 を使用する場合は、 4 ポートの 10GbE ネットワークインターフェイスカード（パーツ番号 X1147A ）を追加して一時的なクラスタポートを提供する必要があります。
- 一時的なクラスタポートを使用したコントローラのアップグレードが完了したら、クラスタ LIF を無停止で e3a および e3b 、 AFF A400 システムの 100GbE ポート、 FAS8300 システムの e0c および e0d 、 100GbE ポートに移行できます。

^3FAS8020、FAS8040、AFF8020、およびAFF8040のシステムを上記の表のターゲット交換コントローラにアップグレードする場合、交換用コントローラが古いコントローラと同じONTAP バージョンを実行している必要があります。FAS8020、FAS8040、AFF8020、およびAFF8040のシステムは、ONTAP 9.8以降のONTAPバージョンをサポートしていません。

[4]次の表は、コントローラのアップグレードの組み合わせでサポートされているONTAPバージョンを示しています。

古いコントローラ		交換用コントローラ	
システム	ONTAP バージョン	システム	ONTAP バージョン
FAS2720	9.13.1以降	FAS2820	9.13.1以降
FAS2760	9.11.1P7以前	FAS2820	9.13.1以降
AFF8060の場合	9.8P13以降のパッチ	AFF A900 の略	9.10.1から9.12.1
AFF8080	9.8P10以降のパッチ	AFF A900 の略	9.10.1から9.12.1
FAS8060	9.8P13以降のパッチ	FAS9500	9.10.1P3～9.12.1
FAS8080	9.8P12以降のパッチ	FAS9500	9.10.1P3～9.12.1
AFF A320	9.9.1以降	AFF A400	9.9.1以降

上記の表にあるアップグレードの組み合わせについては、次の点に注意してください。

- 既存のコントローラと交換用コントローラで同じバージョンのONTAPを使用する必要はありません。ONTAP ソフトウェアのアップグレードは、コントローラのアップグレード時に実行されます。
- アップグレードするときは、サポートされているONTAP バージョンとパッチレベルで交換用コントローラを取り付ける必要があります。
- 手順を開始して最初のノードをアップグレードすると、コントローラのアップグレードをキャンセルしたり元に戻したりすることはできません。

別のハードウェアアップグレード手順を選択する

- "コントローラハードウェアのアップグレードに使用できる代替ARL方法を確認します"です。
- コントローラハードウェアを別の方法でアップグレードして、ボリュームの移動を希望する場合は、を参照してください "参考資料" をクリックして、ボリュームまたは storage _ を移動して _ Upgrade にリンクします。

関連情報

参照"参考資料" _ONTAP 9 ドキュメント_にリンクします。

必要な工具とドキュメント

新しいハードウェアを設置するための特別なツールが必要です。また、アップグレードプロセス中に他のドキュメントを参照する必要があります。

アップグレードを実行するには、次の工具が必要です。

- アーススストラップ
- No.2 プラスドライバ

にアクセスします "参考資料" セクションでは、このアップグレードに必要な参照ドキュメントと参照サイトのリストを参照できます

ARL を使用したコントローラのアップグレードに関するガイドライン

ARL を使用して ONTAP 9.8 以降を実行するコントローラのペアをアップグレードできるかどうかは、プラットフォームおよび元のコントローラと交換用コントローラの両方の構成によって異なります。

ARL のアップグレードがサポートされます

ARL 手順 for ONTAP 9.8 以降を使用してノードのペアをアップグレードする場合は、 ARL が元のコントローラおよび交換用コントローラで実行されていることを確認する必要があります。

元のシステムでサポートされるすべての定義済みアグリゲートのサイズとディスク数を確認する必要があります。次に、サポートされるアグリゲートサイズとディスク数を、新しいシステムでサポートされるアグリゲートサイズとディスク数と比較する必要があります。を参照してください "参考資料" この情報がある Hardware Universe にリンクするには、次の手順を実行します。新しいシステムでサポートされるアグリゲートサイズとディスク数は、元のシステムでサポートされるアグリゲートサイズとディスク数以上であることが必要です。

元のコントローラを交換したときに、新しいノードが既存のノードとクラスタの一部になることができるかどうかは、クラスタ混在ルールで検証する必要があります。クラスタ混在ルールの詳細については、を参照してください "参考資料" Hardware Universe にリンクするには、次の手順を実行します。

> 内蔵ドライブをサポートするシステム（ FAS2700 または AFF A250 など）をアップグレードする場合でも内蔵ドライブがないときは、を参照してください "参考資料" および、 _ アグリゲートの再配置に含まれる手順を使用して、使用している ONTAP のバージョンに適したコントローラ Hardware_content を手動でアップグレードします。

FAS8080 や AFF8080 システムなど、ノードあたり 3 つ以上のクラスタポートを備えたシステムは、アップグレードを開始する前に、ノードあたり 2 つのクラスタポートにクラスタ LIF を移行してホームに戻す必要があります。ノードごとに 3 つ以上のクラスタポートを使用してコントローラのアップグレードを実行すると、アップグレード後に新しいコントローラのクラスタ LIF がなくなる可能性があります。

ARL を使用したコントローラのアップグレードは、 SnapLock Enterprise ボリュームおよび SnapLock Compliance ボリュームが設定されたシステムでサポートされます。

2 ノードスイッチレスクラスタ

2 ノードスイッチレスクラスタのノードをアップグレードする場合は、アップグレードの実行中もスイッチレスクラスタのノードをそのまま使用できます。スイッチクラスタに変換する必要はありません。

ARL のアップグレードはサポートされていません

次のアップグレードは実行できません。

- 元のコントローラに接続されたディスクシェルフをサポートしない交換用コントローラへの接続

  を参照してください "参考資料" ディスクサポート情報の Hardware Universe にリンクするには、次の手順を実行します。

- 内蔵ドライブを搭載したエントリレベルのコントローラ。たとえば、 FAS 2500 などです。

  内蔵ドライブを搭載したエントリレベルの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 "参考資料" ボリュームまたは storage を移動して _Upgrade にリンクし、 Data ONTAP に移動して、clustered 手順を実行するノードのペアをアップグレードする _ に進みます。

MetroCluster FC 構成

MetroCluster FC構成では、できるだけ早くディザスタリカバリ/フェイルオーバーサイトのノードを交換する必要があります。コントローラモデルの不一致が原因で原因ディザスタリカバリのミラーリングがオフラインになる可能性があるため、 MetroCluster 内のコントローラモデルの不一致はサポートされません。2つ目のサイトでノードを交換する場合は、コマンドを使用し `-skip-metrocluster-check true` てMetroClusterチェックをバイパスします。

トラブルシューティングを行う

ノードペアのアップグレード中に障害が発生する可能性があります。ノードがクラッシュする、アグリゲートが再配置されない、または LIF が移行されない可能性があります。障害の原因とその解決策は、アップグレード手順の実行中に障害が発生したタイミングによって異なります。

問題が発生した場合は、 "トラブルシューティングを行う"詳細情報と可能な解決策については、手順の最後にあるセクションをご覧ください。発生する可能性のある障害に関する情報は、手順のフェーズごとに記載されています。 "ARLアップグレードシーケンス" 。

発生した問題に対する解決策 が見つからない場合は、テクニカルサポートにお問い合わせください。

MetroCluster 構成の健全性を確認

Fabric MetroCluster 構成でアップグレードを開始する前に、 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. 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

```
metrocluster_siteA::*> metrocluster check run
```

この処理はバックグラウンドで実行されます。

2. MetroCluster チェックの実行操作が完了したら ' 結果を表示します

   MetroCluster チェックショー

   約 5 分後に、次の結果が表示されます。

```
metrocluster_siteA::*> metrocluster check show
Last Checked On: 4/7/2019 21:15:05
Component             Result
---------------       -------
nodes                 ok
lifs                  ok
config-replication    ok
aggregates            warning
clusters              ok
connections           not-applicable
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 オペレーション履歴 show -job-id 38`

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

MetroCluster 構成エラーがないかどうかを確認します

ネットアップサポートサイトで入手できる Active IQ Config Advisor ツールを使用して、代表的な構成エラーがないかどうかを確認できます。

MetroCluster 構成を使用していない場合は、このセクションを省略できます。

このタスクについて

Active IQ 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. をダウンロードします "Active IQ Config Advisor" ツール。

2. Active IQ Config Advisor を実行し、出力を確認して推奨された方法で問題に対処します。

スイッチオーバー、修復、スイッチバックを検証

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。

を参照してください "参考資料" MetroCluster の管理とディザスタリカバリのコンテンツにリンクし、ネゴシエートスイッチオーバー、修復、スイッチバックについて記載された手順を使用するには、次の手順を実行します。

ARLアップグレードシーケンスについて学ぶ

ARL を使用してノードをアップグレードする前に、手順の動作について理解しておく必要があります。このコンテンツでは、手順はいくつかの段階に分かれています。

ノードペアをアップグレードします

ノードペアをアップグレードするには、元のノードを準備し、元のノードと新しいノードの両方で一連の手順を実行する必要があります。その後、元のノードの運用を停止できます。

ARL アップグレードシーケンスの概要

手順では、交換用コントローラハードウェアを使用して元のコントローラハードウェアを一度に 1 台ずつアップグレードし、 HA ペア構成を利用してルート以外のアグリゲートの所有権を切り替えます。すべてのルート以外のアグリゲートで、アップグレード後の正しいノードである最終デスティネーションに到達するために、 2 つの再配置を実行する必要があります。

各アグリゲートにはホーム所有者と現在の所有者があります。ホーム所有者はアグリゲートの実際の所有者であり、現在の所有者は一時的な所有者です。

次の表に、各フェーズで実行するタスクの概要と、そのフェーズの最後で実行したアグリゲートの所有権の状態を示します。詳細な手順については、手順の後半で説明します。

段階	説明
"ステージ 1 ：アップグレードを準備"	ステージ1では、事前確認を実行し、必要に応じてアグリゲートの所有権を修正します。OKMを使用してストレージ暗号化を管理し、SnapMirror関係を休止できる場合は、特定の情報を記録する必要があります。 ステージ 1 終了時のアグリゲートの所有権： • node1 は、 node1 アグリゲートのホーム所有者と現在の所有者です。 • node2 には、 node2 アグリゲートのホーム所有者と現在の所有者を指定します。

段階	説明
"ステージ 2 ：移行してノード 1 を撤去"	ステージ2で、ノード1の非ルートアグリゲートとNASデータLIFをノード2に再配置します。このプロセスは主に自動化されており、ステータスを確認するために処理が一時停止します。この処理は手動で再開する必要があります。必要に応じて、障害が発生したアグリゲートまたは拒否されたアグリゲートを再ノード1を撤去する前に、手順 の後半で使用するために情報をメモしておきます。ネットブートnode3とnode4には、あとで手順 で準備することもできます。 ステージ 2 終了時のアグリゲートの所有権： • node2 には、 node1 アグリゲートの現在の所有者を指定します。 • node2 には、 node2 アグリゲートのホーム所有者と現在の所有者を指定します。
"ステージ 3 ：node3 をインストールしてブートします"	ステージ3では、ノード3をインストールしてブートし、ノード1のクラスタポートとノード管理ポートがノード3でオンラインになったことを確認し、ノード1のディスクをノード3に再割り当てして、ノード3のインストールを確認します。NetApp Volume Encryption（NVE）を使用している場合は、キー管理ツールの設定をリストアします。必要に応じて、ノード3にFCまたはUTA / UTA2設定を設定します。さらに、node1のNASデータLIFとルート以外のアグリゲートをnode2からnode3に再配置し、SAN LIFがnode3にあることを確認します。 ステージ 3 終了時のアグリゲートの所有権： • node3 は、 node1 アグリゲートのホームの所有者であること、および現在の所有者であること。 • node2 には、 node2 アグリゲートのホーム所有者と現在の所有者を指定します。
"ステージ 4 ：ノード 2 の移動と撤去"	ステージ4で、ルート以外のアグリゲートとNASデータLIFをnode2からnode3に再配置します。node2の情報は、あとで手順 で使用するために記録してから、node2を撤去することもできます。 ステージ 4 終了時のアグリゲートの所有権： • node3 は、 node1 に属していたアグリゲートのホーム所有者および現在の所有者です。 • node2 には、 node2 アグリゲートのホーム所有者を指定します。 • node3 は、 node2 アグリゲートの現在の所有者です。

段階	説明
"ステージ 5 ：ノード 4 をインストールしてブートします"	ステージ5では、ノード4をインストールしてブートし、ノード2のクラスタポートとノード管理ポートがノード4でオンラインになったことを確認し、ノード2のディスクをノード4に再割り当てして、ノード4のインストールを確認します。NVEを使用している場合は、key-manager configurationをリストアします。必要に応じて、ノード4でFCまたはUTA / UTA2設定を設定します。node2のNASデータLIFとルート以外のアグリゲートもnode3からnode4に再配置し、SAN LIFがnode4にあることを確認します。 ステージ 5 終了時のアグリゲートの所有権： • node3 は、 node1 に属していたアグリゲートのホーム所有者および現在の所有者です。 • node4 は、 node2 に属していたアグリゲートのホーム所有者および現在の所有者です。
"ステージ 6 ：アップグレードを完了します"	ステージ6では、新しいノードが正しくセットアップされていることを確認し、暗号化が有効な新しいノードがある場合はストレージ暗号化またはNVEを設定してセットアップします。また、古いノードの運用を停止し、SnapMirrorの処理を再開する必要があります。

ステージ 1 ：アップグレードを準備

ノードをアップグレードする準備をします

コントローラの交換プロセスでは、まず一連の事前確認が実行されます。また、手順の後半で使用するために元のノードに関する情報を収集し、必要に応じて使用中の自己暗号化ドライブのタイプを特定します。

手順

1. ONTAP コマンドラインで次のコマンドを入力して、コントローラの交換プロセスを開始します。

   'system controller replace start-nodes_node_name _`

   ◦ ONTAP 9.10.1 以降では、 4 ノードの MetroCluster FC 構成のデフォルトの自動ネゴシエートスイッチオーバー（ NSO ）ベースのアップグレード手順が使用されます。4 ノード MetroCluster FC 構成をアップグレードする場合、「 system controller replace start 」コマンドを問題するときに、「 -nso 」パラメータを「 false 」に設定して、 NSO ベースの手順の起動を禁止する必要があります。

   'system controller replace start-nodes _node_name --nso false

   ◦ このコマンドは、advanced権限レベルでのみ実行でき `system controller replace start` ます。

   「 advanced 」の権限が必要です

次の出力が表示されます。

```
Warning:
1. Current ONTAP version is 9.x
Before starting controller replacement operation, ensure that the new
controllers are running the version 9.x

2. Verify that NVMEM or NVRAM batteries of the new nodes are charged,
and charge them if they are not. You need to physically check the new
nodes to see if the NVMEM or NVRAM  batteries are charged. You can check
the battery status either by connecting to a serial console or using
SSH, logging into the Service Processor (SP) or Baseboard Management
Controller (BMC) for your system, and use the system sensors to see if
the battery has a sufficient charge.

Attention: Do not try to clear the NVRAM contents. If there is a need to
clear the contents of NVRAM, contact NetApp technical support.

3. If a controller was previously part of a different cluster, run
wipeconfig before using it as the replacement controller.

Do you want to continue? {y|n}: y
```

2. 「 y 」キーを押すと、次の出力が表示されます。

```
Controller replacement operation: Prechecks in progress.
Controller replacement operation has been paused for user intervention.
```

システムでは次の事前確認が実行され、あとで手順で使用するために各事前確認の出力が記録されます。

事前チェック	説明
クラスタの健常性チェック	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。
MCC クラスタチェック	システムが MetroCluster 構成かどうかを確認します。MetroCluster 構成かどうかが自動的に検出され、特定の事前確認と検証チェックが実行されます。4 ノードの MetroCluster FC 構成のみがサポートされます。2 ノード MetroCluster 構成と 4 ノード MetroCluster の IP 構成では、チェックが失敗します。MetroCluster 構成がスイッチオーバーされている場合、チェックは失敗します。
アグリゲートの再配置ステータスチェック	アグリゲートの再配置がすでに実行中であるかどうかを確認します。別のアグリゲートの再配置を実行中の場合、チェックは失敗します。
モデル名のチェック（ Model Name Check	この手順でコントローラモデルがサポートされているかどうかを確認します。モデルがサポートされていない場合、タスクは失敗します。

事前チェック	説明
クラスタクォーラムチェック	交換するノードがクォーラムにあることを確認します。ノードがクォーラムを構成していない場合は、タスクが失敗します。
イメージのバージョンチェック	交換するノードで同じバージョンの ONTAP が実行されていることを確認します。ONTAP イメージのバージョンが異なると、タスクは失敗します。新しいノードには、元のノードと同じバージョンの ONTAP 9.x がインストールされている必要があります。新しいノードに別のバージョンの ONTAP がインストールされている場合は、設置後に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。ONTAP のアップグレード方法については、を参照してください "参考資料" リンク先： ONTAP のアップグレード _ 。
HA ステータスチェック	交換する両方のノードがハイアベイラビリティ（ HA ）ペア構成になっているかどうかを確認します。コントローラでストレージフェイルオーバーが有効になっていない場合、タスクは失敗します。
アグリゲートステータスチェック	ホーム所有者でないアグリゲートを交換するノードが所有している場合、そのタスクは失敗します。ローカル以外のアグリゲートを所有するノードは使用しないでください。
ディスクステータスチェック	交換するノードに不足しているディスクまたは障害が発生しているディスクがある場合、タスクは失敗します。見つからないディスクがある場合は、CLI_を使用したディスクへのリンクとアグリゲートの管理、CLI_を使用した論理ストレージの管理、および_HAペアのMANAGEMENT_を参照して"参考資料"、HAペアのストレージを設定してください。
データ LIF ステータスチェック	交換するノードにローカル以外のデータ LIF があるかどうかを確認します。ホーム所有者でないデータ LIF がノードに含まれないようにしてください。ローカル以外のデータ LIF がいずれかのノードに含まれている場合、タスクは失敗します。
クラスタ LIF ステータス	両方のノードでクラスタ LIF が動作しているかどうかを確認します。クラスタ LIF が停止している場合は、タスクは失敗します。
ASUP ステータスチェック	ASUP 通知が設定されていないと、タスクは失敗します。コントローラの交換用手順を開始する前に ASUP を有効にする必要があります。
CPU 利用率チェック	交換するノードの CPU 利用率が 50% を超えていないかどうかを確認します。CPU 使用率がかなりの時間にわたって 50% を超えると、タスクは失敗します。
アグリゲートの再構築チェック	いずれかのデータアグリゲートで再構築が実行されているかどうかを確認しますアグリゲートの再構築を実行中の場合、タスクは失敗します。
ノードアフィニティジョブチェック	ノードアフィニティジョブが実行されているかどうかを確認します。ノードアフィニティジョブが実行中の場合、チェックは失敗します。

3. コントローラの交換処理が開始されて事前確認が完了すると、処理が一時停止するため、ノード 3 の設定時にあとで必要になる可能性がある出力情報を収集できます。

FAS8080 や AFF8080 システムなど、ノードあたり 3 つ以上のクラスタポートを備えたシステムは、アップグレードを開始する前に、ノードあたり 2 つのクラスタポートにクラスタ LIF を移行してホームに戻す必要があります。ノードごとに 3 つ以上のクラスタポートを使用してコントローラのアップグレードを実行すると、アップグレード後に新しいコントローラのクラスタ LIF がなくなる可能性があります。

4. システムコンソールで、コントローラの交換用手順の指示に従って、次のコマンドセットを実行します。

   各ノードに接続されているシリアルポートで、次のコマンドの出力を個別に実行して保存します。

   - vserver services name-service dns show
   - `network interface show -curr-node local -role cluster,intercluster,node-mgmt,cluster-mgmt,data`
   - `network port show -node local -type physical`
   - `service-processor show -node local -instance`
   - `network fcp adapter show -node local`
   - `network port ifgrp show -node local`
   - `system node show -instance -node local`
   - `run -node local sysconfig`
   - `storage aggregate show -node local`
   - `volume show -node local`
   - storage array config show -switch_switch_name_`
   - `system license show -owner local`
   - 「 storage encryption disk show 」のように表示されます
   - 「 securitykey manager onboard show-backup 」を参照してください
   - 「 security key-manager external show 」と入力します
   - 「 security key-manager external show-status 」
   - `network port reachability show -detail -node local`

   オンボードキーマネージャ（OKM）を使用したNetApp Volume Encryption（NVE）またはNetApp Aggregate Encryption（NAE）を使用している場合は、手順の後半の工程でキー管理ツールの再同期を実行できるように、キー管理ツールのパスフレーズを準備しておいてください。

5. システムで自己暗号化ドライブを使用している場合は、Knowledge Baseの文書を参照してください "ドライブがFIPS認定かどうかを確認する方法" アップグレード対象のHAペアで使用されている自己暗号化ドライブのタイプを確認する。ONTAP ソフトウェアは、次の2種類の自己暗号化ドライブをサポートしています。

   - FIPS認定のNetApp Storage Encryption（NSE）SASドライブまたはNVMeドライブ
   - FIPS非対応の自己暗号化NVMeドライブ（SED）

FIPSドライブは、同じノードまたはHAペアで他のタイプのドライブと混在させることはできません。

SEDと非暗号化ドライブを同じノードまたはHAペアで混在させることができます。

"サポートされている自己暗号化ドライブの詳細を確認できます"。

ARL の事前確認に失敗した場合は、アグリゲートの所有権を修正

アグリゲートステータスチェックに失敗した場合は、パートナーノードが所有するアグリゲートをホーム所有者ノードに戻し、事前確認プロセスを再度開始する必要があります。

手順

1. パートナーノードが現在所有しているアグリゲートをホーム所有者ノードに戻します。

   storage aggregate relocation start -node-source_node__ destination_destination-node-aggregate-list *

2. node1 と node2 のどちらも現在の所有者（ホーム所有者ではない）アグリゲートを所有していないことを確認します。

   storage aggregate show -nodes_node_name -is-home false -fields owner-name、home-name、stateを指定します

   次の例は、アグリゲートの現在の所有者とホーム所有者の両方がノードにある場合のコマンドの出力例を示しています。

```
cluster::> storage aggregate show -nodes node1 -is-home true -fields
owner-name,home-name,state
aggregate   home-name  owner-name  state
---------   ---------  ----------  ------
aggr1       node1      node1       online
aggr2       node1      node1       online
aggr3       node1      node1       online
aggr4       node1      node1       online

4 entries were displayed.
```

完了後

コントローラの交換プロセスを再開する必要があります。

'system controller replace start-nodes_node_name _`

使用許諾

一部の機能にはライセンスが必要ですが、1つ以上の機能を含む_packages_として発行されます。クラスタで使用する各機能のキーは、クラスタ内の各ノードに独自に設定する必要があります。

新しいライセンスキーがない場合は、クラスタで現在ライセンスされている機能を新しいコントローラで使用できます。ただし、ライセンスされていない機能をコントローラ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、アップグレードの完了後に新しいコントローラのライセンスキーをインストールする必要があります。

を参照してください "参考資料" ONTAPの新しい28文字のライセンスキーを取得できる_ NetApp Support Site _にリンクします。キーは、 _ ソフトウェアライセンス _ の _ マイサポート _ セクションにあります。必要なライセンスキーがサイトにない場合は、ネットアップの営業担当者にお問い合わせください。

ライセンスの詳細については、を参照してください "参考資料" をクリックして、 *System Administration Reference*(システム管理リファレンス) にリンクします。

オンボードキーマネージャを使用してストレージ暗号化を管理します

オンボードキーマネージャ（OKM）を使用して暗号化キーを管理できます。OKMをセットアップした場合は、アップグレードを開始する前にパスフレーズとバックアップ資料を記録しておく必要があります。

手順

1. クラスタ全体のパスフレーズを記録します。

   これは、CLIまたはREST APIを使用してOKMを設定または更新したときに入力したパスフレーズです。

2. を実行して、キー管理ツールの情報をバックアップします `security key-manager onboard show-backup` コマンドを実行します

SnapMirror 関係を休止します（オプション）。

手順を続行する前に、すべての SnapMirror 関係が休止状態になっていることを確認する必要があります。休止された SnapMirror 関係は、リブート後およびフェイルオーバー後も休止状態のままです。

手順

1. デスティネーションクラスタの SnapMirror 関係のステータスを確認します。

   「 Snapmirror show 」のように表示されます

   > このステータスが「Transferring」の場合は、転送を中止する必要があります。snapmirror abort -destination -vserver _vserver_name _`

   SnapMirror 関係の状態が「 Transferring 」でない場合は、中止は失敗します。

2. クラスタ間のすべての関係を休止します。

   ```
   snapmirror quiesce -destination-vserver *
   ```

ステージ 2 ：移行してノード 1 を撤去

ノード **1** が所有するルート以外のアグリゲートと **NAS** データ **LIF** をノード **2** に再配置します

ノード 1 をノード 3 に交換する前に、ルート以外のアグリゲートと NAS データ LIF をノード 1 からノード 2 に移動してから、ノード 1 のリソースをノード 3 に移動する必要があります。

作業を開始する前に

この処理は、タスクの開始時にすでに一時停止されている必要があります。手動で再開する必要があります。

このタスクについて

アグリゲートと LIF の移行が完了すると、検証のために処理が一時停止されます。この段階で、ルート以外のアグリゲートと SAN 以外のデータ LIF がすべて node3 に移行されているかどうかを確認する必要があります。

アグリゲートおよび LIF のホーム所有者は変更されません。現在の所有者のみが変更されます。

手順

1. アグリゲートの再配置処理と NAS データ LIF の移動処理を再開します。

   「システムコントローラの交換が再開」

   ルート以外のアグリゲートと NAS データ LIF はすべて、 node1 から node2 に移行されます。

   処理が一時停止することで、ノード 1 のルート以外のアグリゲートと SAN 以外のデータ LIF がすべて node2 に移行されているかどうかを確認できます。

2. アグリゲートの再配置処理と NAS データ LIF の移動処理のステータスを確認します。

   「 system controller replace show-sdetails 」というエラーが表示されます

3. 処理が一時停止したまま、ルート以外のすべてのアグリゲートが node2 でそれぞれの状態でオンラインになっていることを確認します。

   ```
   storage aggregate show -node <node2> -state online -root false
   ```

   次の例は、 node2 のルート以外のアグリゲートがオンラインになっていることを示しています。

```
cluster::> storage aggregate show -node node2 -state online -root false

Aggregate  Size     Available  Used%  State  #Vols  Nodes  RAID Status
---------  -------  ---------  -----  ------ -----  ------
--------------
aggr_1     744.9GB  744.8GB    0%     online     5  node2
raid_dp,normal
aggr_2     825.0GB  825.0GB    0%     online     1  node2
raid_dp,normal
2 entries were displayed.
```

アグリゲートがオフラインになった場合、または node2 で外部になった場合は、各アグリゲートに対して 1 回、 node2 で次のコマンドを使用してアグリゲートをオンラインにします。

```
storage aggregate online -aggregate <aggregate_name>
```

4. node2 で次のコマンドを使用し、出力を調べて、すべてのボリュームがオンラインであることを確認します。

```
volume show -node <node2> -state offline
```

node2 上にオフラインのボリュームがある場合は、各ボリュームに対して 1 回、 node2 で次のコマンドを使用してオンラインにします。

```
volume online -vserver <vserver_name> -volume <volume_name>
```

その `vserver_name`このコマンドで使用する方法は、前の出力で確認できます。 `volume show`指示。

5. [[step5] いずれかの LIF が停止している場合は、次のコマンドを使用して、各 LIF に対して 1 回ずつ LIF の管理ステータスを「 up 」に設定します。

「network interface modify -vserver *vserver_name* _ lif_lif_name_-home-nodename_-status-admin up

障害が発生した、または拒否されたアグリゲートをノード**2**に再配置します。

集約の再配置に失敗したり、拒否されたりした場合は、集約を手動でノード 2 に再配置するか、必要に応じて拒否または宛先チェックのいずれかをオーバーライドする必要があります。

このタスクについて

エラーのため、システムは再配置操作を一時停止します。

手順

1. イベント管理システム（ EMS ）のログで、アグリゲートの再配置に失敗した理由や拒否された理由を確認します。
2. 障害が発生したアグリゲートまたは拒否されたアグリゲートを

```
storage aggregate relocation start -node <node1> -destination <node2>
-aggregate-list <aggregate_name> -ndo-controller-upgrade true
```

3. プロンプトが表示されたら、「 y 」と入力します。
4. 再配置は、次のいずれかの方法で強制的に実行できます。

オプション	説明
拒否チェックの無視	次のコマンドを使用します。 `storage aggregate relocation start -node node1 -destination node2 -aggregate-list <aggregate_list> -ndo-controller-upgrade true -override-vetoes true`
デスティネーションチェックの無効化	次のコマンドを使用します。 `storage aggregate relocation start -node node1 -destination node2 -aggregate-list <aggregate_list> -ndo-controller-upgrade true -override-vetoes true -override-destination-checks true`

ノード **1** を撤去

ノード 1 を撤去するには、自動処理を再開して、ノード 2 と HA ペアを無効にし、ノード 1 を正しくシャットダウンします。手順の後半の工程で、ノード1をラックまたはシャーシから取り外します。

手順

1. 処理を再開します。

   「システムコントローラの交換が再開」

2. ノード 1 が停止されたことを確認します。

   「 system controller replace show-sdetails 」というエラーが表示されます

完了後

アップグレードが完了したら、 node1 の運用を停止できます。を参照してください "古いシステムの運用を停止"。

ネットブートを準備

ノード 3 とノード 4 を手順の後半で物理的にラックに設置したあと、ネットブートが必要になることがあります。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配置します。

作業を開始する前に

- 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。
- を参照してください "参考資料" からネットアップサポートサイトにリンクして、使用しているプラットフォームに必要なシステムファイルと、適切なバージョンの ONTAP をダウンロードします。

このタスクについて

元のコントローラと同じバージョンの ONTAP 9 がインストールされていない場合は、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. ネットアップサポートサイトにアクセスして、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。

用途	作業
FAS/AFF8000 シリーズシステム	「 ONTAP_version_image.tgz 」ファイルの内容をターゲットディレクトリ「 tar -zxvf ONTAP_version_image.tgz 」に展開します 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は、カーネル・ファイル「 netboot/ kernel 」を含むネットブート・フォルダが含まれている必要があります
その他すべてのシステム	ディレクトリの一覧に次のファイルが表示されます。 `<ontap_version>_image.tgz` 「 ONTAP_version_image.tgz 」ファイルの内容を抽出する必要はありません。

のディレクトリの情報を使用します "ステージ 3"。

ステージ 3 ：node3 をインストールしてブートします

node3 をインストールしてブートします

ノード 3 をラックに設置し、ノード 1 の接続をノード 3 に転送し、ノード 3 をブートして、 ONTAP をインストールする必要があります。そのあと、このセクションで説明するように、ノード 1 のスペアディスク、ルートボリュームに属するディスク、およびその前の手順でノード 2 に再配置されなかったルート以外のアグリゲートを再割り当てす

る必要があります。

このタスクについて

再配置処理はこのフェーズの開始時に一時停止されます。このプロセスは主に自動化されており、ステータスを確認するために処理が一時停止します。この処理は手動で再開する必要があります。また、 SAN LIF がノード 3 に正常に移動したことを確認する必要があります。

ノード 1 にインストールされている ONTAP 9 のバージョンが異なる場合は、ノード 3 をネットブートする必要があります。node3 のインストールが完了したら、 Web サーバに保存されている ONTAP 9 イメージからブートします。その後、の手順に従って、後続のシステムのブートに使用する正しいファイルをブートメディアデバイスにダウンロードできます "ネットブートを準備"。

- AFF A800またはAFF C800コントローラのアップグレードの場合、ノード 1 を取り外す前に、シャーシ内のすべてのドライブがミッドプレーンにしっかりと固定されていることを確認する必要があります。詳細については、 "AFF A800またはAFF C800コントローラモジュールを交換"。
- ストレージディスクが搭載されたシステムをアップグレードする場合は、このセクション全体を完了して、にアクセスする必要があります "ノード 3 の FC ポートを設定" および "ノード 3 の UTA / UTA2 ポートを確認して設定してください" セクションで、クラスタ・プロンプトでコマンドを入力します。

手順

1. [[auto_install3_step1] ノード 3 のラックスペースがあることを確認します。

   ノード 1 とノード 2 が別々のシャーシに搭載されている場合は、ノード 3 をノード 1 と同じラックの場所に設置できます。ただし、 node1 が node2 の同じシャーシに設置されている場合は、 node3 を専用のラックスペースに配置する必要があります。その場合は、 node1 の場所に近い場所に配置することを推奨します。

2. [[auto_install3_step2] ノードモデルの *Installation and Setup Instructions* に従って、ラックにノード 3 をインストールします。

   両方のノードが同じシャーシ内にあるシステムにアップグレードする場合は、シャーシに node4 と node3 をインストールします。両方のノードを同じシャーシにインストールしないと、ノード 3 を起動するとデュアルシャーシ構成のように動作し、ノード 4 を起動するとノード間の相互接続が確立されません。

3. ケーブルノード 3 を接続し、ノード 1 からノード 3 に接続を移動します。

   node3 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」、適切なディスク シェルフ ドキュメント、および「HA ペア管理」ドキュメントを使用して、次の接続をケーブル接続します。

   参照"参考資料"_HAペア管理_にリンクします。

   - コンソール（リモート管理ポート）
   - クラスタポート
   - データポート
   - クラスタポートとノード管理ポート
   - ストレージ

◦ SAN 構成： iSCSI イーサネットおよび FC スイッチポート

ほとんどのプラットフォームモデルには一意のインターコネクトカードモデルがあるため、インターコネクトカードまたはクラスタインターコネクトケーブルの接続を node1 から node3 に移動する必要はない場合があります。MetroCluster 構成の場合、 FC-VI ケーブルの接続を node1 から node3 に移動する必要があります。新しいホストに FC-VI カードがない場合は、 FC-VI カードの移動が必要になることがあります。

4. ノード 3 の電源をオンにしてから、コンソール端末で Ctrl+C 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。

両方のノードを同じシャーシに搭載したシステムにアップグレードする場合は、 node4 もリブートします。ただし、 node4 のブートはあとで破棄することができます。

node3 をブートすると、次の警告メッセージが表示される場合があります。

```
WARNING: The battery is unfit to retain data during a power outage. This
is likely because the battery is discharged but could be due to other
temporary conditions.
When the battery is ready, the boot process will complete and services
will be engaged.
To override this delay, press 'c' followed by 'Enter'
```

5. で警告メッセージが表示される場合 手順 4を使用して、次の操作を実行します。

a. NVRAM バッテリ低下以外の問題を示すコンソールメッセージがないか確認し、必要に応じて対処します。

b. バッテリの充電と起動プロセスが完了するまで待ちます。

遅延を無視しないでください。バッテリーの充電が不十分だと、データが失われる可能性があります。

を参照してください "ネットブートを準備"。

6. [[step6] 次のいずれかの操作を選択して、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。データLIF IPは使用しないでください。使用しないと、アップグレードの実行中にデータ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

動的ホスト構成プロトコル（ **DHCP** ）の状態	作業
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（必須）。 *`netmask`* は、ストレージシステムのネットワークマスクです（必須）。 *`gateway`* は、ストレージシステムのゲートウェイです（必須）。 *`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（オプション）。 *`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（オプション）。 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。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。

7. [[step7] node3 でネットブートを実行します。

用途	作業
FAS/AFF8000 シリーズシステム	netboot\http://<web_server_ip/path_to_web-accessible_directory>/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_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 "ネットブートを準備"。

トランクを中断しないでください。

8. ブートメニューからオプション [(7) 新しいソフトウェアを最初にインストールする] 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 procedure is not supported for Non-Disruptive Upgrade on an HA pair
```

コントローラのアップグレードではなく、 ONTAP による環境の無停止アップグレードも記録されています。

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 リリースオプションを指定してネットブート手順 を実行する `(7) Install new software` ブートメディアを消去して、両方のイメージパーティションに同じONTAP バージョンを配置します。

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場合は、「 y 」と入力し、パッケージのプロンプトが表示されたら URL を入力します。

   http://<web_server_ip/path_to_web-accessible_directory>/<ontap_version>_image.tgz` にアクセスします

10. [[step10] コントローラモジュールをリブートするには、次の手順を実行します。

    a. 次のプロンプトが表示されたら 'n' を入力してバックアップ・リカバリをスキップします

       バックアップ設定を今すぐ復元しますか？{y|n}`

    b. 次のプロンプトが表示されたら 'y' と入力して再起動します

       ' 新しくインストールしたソフトウェアの使用を開始するには ' ノードを再起動する必要があります今すぐリブートしますか？{y|n}`

    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、構成データをリストアする必要があるためです。

11. ブートメニューからメンテナンスモード「 5 」を選択し、起動を続行するように求めるプロンプトが表示されたら「 y 」と入力します。

12. コントローラとシャーシが HA として構成されていることを確認します。

    「 ha-config show 」

    次に 'ha-config show コマンドの出力例を示します

    ```
    Chassis HA configuration: ha
    Controller HA configuration: ha
    ```

    システムは、 HA ペア構成かスタンドアロン構成かを PROM に記録します。状態は、スタンドアロンシステムまたは HA ペア内のすべてのコンポーネントで同じである必要があります。

13. コントローラとシャーシが HA として設定されていない場合は、次のコマンドを使用して構成を修正します。

    「 ha-config modify controller ha 」を参照してください

    「 ha-config modify chassis ha 」を参照してください

    MetroCluster 構成の場合は、次のコマンドを使用してコントローラとシャーシを変更します。

「 ha-config modify controller mcc 」

「 ha-config modify chassis mcc 」

14. メンテナンスモードを終了します。

「 halt 」

ブート環境のプロンプトでCtrl+Cキーを押して、AUTOBOOTを中断します。

15. node2 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。

「食事」

16. [step16]] on node3 で、ブート環境のプロンプトで次のコマンドを使用して日付を確認します。

「日付」

17. 必要に応じて、 node3 の日付を設定します。

'set date_mm/dd/yyyy_`

18. [step18]] on node3 で、ブート環境のプロンプトで次のコマンドを使用して時間を確認します。

「時間」

19. 必要に応じて、ノード 3 の時刻を設定します。

'set time_hh:mm:ss_`

20. ブートローダーで、node3のパートナーシステムIDを設定します。

setsetenv partner-sysid_node2 *sysid*`

ノード3の場合、 `partner-sysid` node2のものである必要があります。

a. 設定を保存します。

'aveenv

21. [[auto_install3_step21]を確認します `partner-sysid` ノード3の場合：

printenv partner-sysid

1. NetApp Storage Encryption (NSE) ドライブがインストールされている場合は、次の手順を実行します。

手順 でこれまでに行ったことがない場合は、Knowledge Baseの記事を参照してください "ドライブがFIPS認定かどうかを確認する方法" 使用している自己暗号化ドライブのタイプを確認するため。

a. 設定 `bootarg.storageencryption.support` 終了： `true` または `false` ：

次のドライブが使用中の場合	次に、
FIPS 140-2レベル2の自己暗号化要件に準拠したNSEドライブ	`setenv bootarg.storageencryption.support **true**`
ネットアップの非FIPS SED	`setenv bootarg.storageencryption.support **false**`

> FIPSドライブは、同じノードまたはHAペアで他のタイプのドライブと混在させることはできません。SEDと非暗号化ドライブを同じノードまたはHAペアで混在させることができます。

b. 特別なブートメニューに移動してオプションを選択します `(10) Set Onboard Key Manager recovery secrets`。

手順の前半で記録したパスフレーズとバックアップ情報を入力します。"オンボードキーマネージャを使用してストレージ暗号化を管理します"を参照してください。

2. ノードをブートメニューでブートします。

「 boot_ontap menu

次の手順

- FCまたはUTA/UTA2構成のシステムをお持ちの場合は、"ノード3のFCまたはUTA/UTA2ポートを設定および構成する" 。
- FCまたはUTA/UTA2構成がない場合は、"ノード1のディスクをノード3に再割り当てする、ステップ1"ノード3がノード1のディスクを認識できるようにする。
- MetroCluster構成の場合、"ノード3のFCまたはUTA/UTA2ポートを設定および構成する"ノードに接続されているディスクを検出します。

ノード 3 で FC または UTA / UTA2 設定を設定します

ノード 3 にオンボードの FC ポート、オンボードのユニファイドターゲットアダプタ（ UTA / UTA2 ）ポート、または UTA / UTA2 カードがある場合は、残りの手順を完了する前に設定を行う必要があります。

このタスクについて

セクションの完了が必要な場合があります ノード 3 の FC ポートを設定、を参照してください ノード 3 の UTA / UTA2 ポートを確認して設定してください、または両方のセクション。

> ネットアップのマーケティング資料では、 Converged Network Adapter （ CNA ；統合ネットワークアダプタ）アダプタおよびポートを UTA2 と呼ぶ場合があります。ただし、 CLI では CNA という用語が使用されます。

ノード3にオンボードFCポート、オンボードUTA/UTA2ポート、またはUTA/UTA2カード（たとえば、 ONTAP 9.15.1以降に導入されたAFFおよびFASシステム）がなく、ストレージディスクを備えたシステムをアップグレードする場合は、"ノード1のディスクをノード3に再割り当て" 。

ノード 3 の FC ポートを設定

node3 にオンボードまたはアドオン FC アダプタ上の FC ポートがある場合、システムの出荷時にポートが事前構成されていないため、ノードをサービスに投入する前にノード上でポート構成を設定する必要があります。ポートを設定しないと、サービスが中断される可能性があります。

作業を開始する前に

セクションに保存した FC ポート設定の値を node1 で確認しておく必要があります "ノードをアップグレードする準備をします"。

このタスクについて

システムに FC 構成がない場合は、このセクションをスキップしてかまいません。システムにオンボード UTA / UTA2 ポートまたは UTA / UTA2 カードがある場合は、で設定します ノード 3 の UTA / UTA2 ポートを確認して設定してください。

このセクションのコマンドをメンテナンス モードのシェル プロンプトで入力します。

手順

1. ノード 3 の FC 設定を、先ほどノード 1 からキャプチャした設定と比較します。
2. 必要に応じて、次のいずれかのアクションを実行して、ノード 3 の FC ポートを変更します。

   メンテナンス モードの場合 (ブート メニューのオプション 5):

   - ターゲット ポートとしてプログラムするには:

     `ucadmin modify -m fc -t target <adapter>`

     例えば： `ucadmin modify -m fc -t target 2a`

   - イニシエータポートをプログラミングする場合：

     `ucadmin modify -m fc -t initiator <adapter>`

   例えば： `ucadmin modify -m fc -t initator 2b`

3. 次のコマンドを使用して出力を調べ、新しい設定を確認します。

   ucadmin show

4. ノードを停止します。

   「 halt 」

5. LOADERプロンプトからシステムをブートします。

   「 boot_ontap menu

6. コマンドを入力したら、ブート環境のプロンプトでシステムが停止するまで待ちます。
7. 保守モードのブート・メニューからオプション「 5 」を選択します。
8. [[auto_check3_step8] 次のいずれかの操作を実行します

ノード 3 の場合...	作業
UTA/UTA2 カードまたは UTA/UTA2 オンボード ポートを搭載	へ移動ノード 3 の UTA / UTA2 ポートを確認して設定してください
UTA/UTA2 カードまたは UTA/UTA2 オンボード ポートがありません	_ノード3のUTA/UTA2ポートの確認と設定_をスキップして、"ノード1のディスクをノード3に再割り当て" 。

ノード 3 の UTA / UTA2 ポートを確認して設定してください

ノード 3 にオンボード UTA / UTA2 ポートまたは UTA / UTA2 カードが搭載されている場合は、アップグレードしたシステムの使用方法によって、ポートの設定を確認し、場合によっては再設定する必要があります。

作業を開始する前に

UTA / UTA2 ポートに対応する正しい SFP+ モジュールが必要です。

このタスクについて

FC にユニファイドターゲットアダプタ（ UTA / UTA2 ）ポートを使用する場合は、まずポートの設定を確認する必要があります。

ネットアップのマーケティング資料では、 UTA2 という用語を CNA アダプタとポートという意味で使用している場合があります。ただし、 CLI では CNA という用語が使用されます。

使用することができます `ucadmin show`次の出力例に示すように、現在のポート構成を表示または確認するには、コマンドを使用します。

```
*> ucadmin show
          Current  Current    Pending   Pending      Admin
Adapter   Mode     Type       Mode      Type         Status
-------   -------  -------    --------  ----------   --------
0e        fc       target     -         initiator    offline
0f        fc       target     -         initiator    offline
0g        fc       target     -         initiator    offline
0h        fc       target     -         initiator    offline
1a        fc       target     -         -            online
1b        fc       target     -         -            online
6 entries were displayed.
```

UTA / UTA2 ポートは、ネイティブの FC モードまたは UTA / UTA2 モードに設定できます。FC モードでは FC イニシエータと FC ターゲットがサポートされます。 UTA / UTA2 モードを使用すると、同じ 10GbE SFP+ インターフェイスを共有する NIC と FCoE のトラフィックを同時に処理でき、 FC ターゲットをサポートできます。

アドオン アダプタまたはコントローラ マザーボード上に UTA/UTA2 ポートがあり、次の構成になっている場合がありますが、ノード 3 の UTA/UTA2 ポートの構成を確認し、必要に応じて変更する必要があります。

- コントローラを注文した UTA / UTA2 カードは、注文したパーソナリティを指定するために出荷前に設定されます。
- コントローラとは別に発注した UTA / UTA2 カードは、デフォルトの FC ターゲットパーソナリティとして出荷されます。
- 新しいコントローラのオンボード UTA / UTA2 ポートは、希望するパーソナリティを持つように出荷する前に設定されます。

UTA/UTA2 ポートを構成するには、メンテナンス モードになっている必要があります。このセクションのコマンドをメンテナンス モードのシェル プロンプトで入力します。

手順

1. 現在の SFP+ モジュールが目的の用途と一致しない場合は、正しい SFP+ モジュールに交換します。

   ネットアップの担当者に連絡して、正しい SFP+ モジュールを入手します。

2. UTA/UTA2 ポート設定を確認します。

   ucadmin show

   出力を調べて、UTA/UTA2 ポートに必要な特性があるかどうかを判断します。

   次の例の出力は、アダプタ「1b」のタイプがイニシエーターに変更され、アダプタ「2a」と「2b」のモードが「cna」に変更されていることを示しています。 CNA モードでは、カードをネットワーク アダプタとして使用できます。

```
*> ucadmin show
         Current    Current     Pending  Pending     Admin
Adapter  Mode       Type        Mode     Type        Status
-------  --------   ----------  -------  --------    --------
1a       fc         initiator   -        -           online
1b       fc         target      -        initiator   online
2a       fc         target      cna      -           online
2b       fc         target      cna      -           online
*>
```

3. 次のいずれかを実行します。

UTA / UTA2 ポート	次に、
希望するパーソナリティがない	行きます 手順 4。
あなたがほしい人格を持っている	ステップ4からステップ8をスキップして、手順 9 。

4. 次のいずれかのアクションを実行します。

を設定する場合	次に、
UTA / UTA2 カードのポート	へ移動手順 5
オンボードの UTA/UTA2 ポート	ステップ5をスキップして手順 6。

5. アダプタがイニシエーターモードであり、UTA/UTA2 ポートがオンラインの場合は、UTA/UTA2 ポートをオフラインにします。

   ```
   storage disable adapter <adapter_name>
   ```

   ターゲットモードのアダプタは、メンテナンスモードで自動的にオフラインになります。

6. 現在の構成が目的の用途と一致しない場合は、必要に応じて構成を変更します。

   ```
   ucadmin modify -m fc|cna -t initiator|target <adapter_name>
   ```

   - 「 -m 」はパーソナリティ・モードで、「 fc 」または「 cna 」です。
   - `-t` は FC4 のタイプ、「 target 」または「 initiator 」です。

   > テープ ドライブおよびMetroCluster構成には FC イニシエーターを使用する必要があります。 SAN クライアントには FC ターゲットを使用する必要があります。

7. 各ポートに対して次のコマンドを 1 回ずつ入力して、ターゲット ポートをオンラインにします。

   ```
   storage enable adapter <adapter_name>
   ```

8. ポートをケーブル接続します。

1. メンテナンスモードを終了します。

   「 halt 」

2. ノードをブートメニューでブートします。

   「 boot_ontap menu

次の手順

- AFF A800システムにアップグレードする場合は、"ノード1のディスクをノード3に再割り当て（手順9）"。
- その他のシステムアップグレードについては、"ノード1のディスクをノード3に再割り当て（手順1）"。

ノード1のディスクをノード3に再割り当て

ノード3のインストールを検証する前に、ノード1に属していたディスクをノード3に再割り当てする必要があります。

手順

1. ノード1がブートメニューで停止していることを確認します。ノード1のディスクをノード3に再割り当

てします。

```
boot_after_controller_replacement
```

少し待機したあと、交換するノードの名前を入力するように求められます。共有ディスク（Advanced Disk Partitioning（ADP；アドバンストディスクパーティショニング）またはパーティショニングされたディスクとも呼ばれます）がある場合は、HAパートナーのノード名を入力するように求められます。

これらのプロンプトは、コンソールメッセージに埋もれている可能性があります。ノード名を入力しなかった場合や間違った名前を入力した場合は、名前をもう一度入力するように求められます。

コンソールの出力例を展開します

```
LOADER-A> boot_ontap menu
.
<output truncated>
.
All rights reserved.
*******************************
*                             *
* Press Ctrl-C for Boot Menu. *
*                             *
*******************************
.
<output truncated>
.
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)? 22/7
(22/7) Print this secret List
(25/6) Force boot with multiple filesystem disks missing.
(25/7) Boot w/ disk labels forced to clean.
(29/7) Bypass media errors.
(44/4a) Zero disks if needed and create new flexible root volume.
(44/7) Assign all disks, Initialize all disks as SPARE, write DDR
labels
.
<output truncated>
.
(wipeconfig)                        Clean all configuration on boot
device
(boot_after_controller_replacement) Boot after controller upgrade
(boot_after_mcc_transition)         Boot after MCC transition
(9a)                                Unpartition all disks and remove
their ownership information.
(9b)                                Clean configuration and
```

```
initialize node with partitioned disks.
(9c)                                Clean configuration and
initialize node with whole disks.
(9d)                                Reboot the node.
(9e)                                Return to main boot menu.
The boot device has changed. System configuration information could
be lost. Use option (6) to restore the system configuration, or
option (4) to initialize all disks and setup a new system.
Normal Boot is prohibited.
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)? boot_after_controller_replacement
This will replace all flash-based configuration with the last backup
to disks. Are you sure you want to continue?: yes
.
<output truncated>
.
Controller Replacement: Provide name of the node you would like to
replace:<nodename of the node being replaced>
Controller Replacement: Provide High Availability partner of node1:
<nodename of the partner of the node being replaced>
Changing sysid of node node1 disks.
Fetched sanown old_owner_sysid = 536940063 and calculated old sys id
= 536940063
Partner sysid = 4294967295, owner sysid = 536940063
.
<output truncated>
.
varfs_backup_restore: restore using /mroot/etc/varfs.tgz
varfs_backup_restore: attempting to restore /var/kmip to the boot
device
varfs_backup_restore: failed to restore /var/kmip to the boot device
varfs_backup_restore: attempting to restore env file to the boot
device
varfs_backup_restore: successfully restored env file to the boot
device wrote key file "/tmp/rndc.key"
```

```
varfs_backup_restore: timeout waiting for login
varfs_backup_restore: Rebooting to load the new varfs
Terminated
<node reboots>
System rebooting...
.
Restoring env file from boot media...
copy_env_file:scenario = head upgrade
Successfully restored env file from boot media...
Rebooting to load the restored env file...
.
System rebooting...
.
<output truncated>
.
WARNING: System ID mismatch. This usually occurs when replacing a
boot device or NVRAM cards!
Override system ID? {y|n} y
.
Login:
```

上記のコンソールの出力例では、アドバンストディスクパーティショニング（ADP）ディスクを使用するシステムの場合は ONTAP からパートナーノード名の入力を求められます。

2. システムが再起動ループに入り、メッセージが表示された場合は `no disks found`これは、システムが FC または UTA/UTA2 ポートをターゲット モードにリセットしたため、ディスクが認識されないことを示します。この問題を解決するには、次のいずれかのタスクを選択してください。
   - 実行する手順 3に手順 8ノード3上
   - セクションへ移動"ノード 3 のインストールを確認します"
3. [reassign-node1-node3-app-step3]]自動ブート中にCtrl+Cキーを押して、Loader >プロンプトでノードを停止します。
4. LOADERプロンプトで、メンテナンスモードに切り替えます。

   「 boot_ontap maint 」を使用してください
5. 保守モードで、以前に設定したすべてのイニシエータポートをターゲットモードで表示します。

   ucadmin show

   ポートをイニシエータモードに戻します。

   ucadmin modify -m fc -t initiator -f adapter name_`
6. ポートがイニシエータモードに変更されたことを確認します。

ucadmin show

7. メンテナンスモードを終了します。

「 halt 」

> 外付けディスクをサポートするシステムから外付けディスクもサポートするシステムにアップグレードする場合は、に進みます手順 8。
>
> 外付けディスクをサポートするシステムから、内蔵ディスクと外付けディスクの両方をサポートするシステム（AFF A800システムなど）にアップグレードする場合は、に進みます。手順 9

8. Loaderプロンプトでブートします。

「 boot_ontap menu

これで、ブート時に以前に割り当てられていたすべてのディスクをノードで検出できるようになり、想定どおりにブートできるようになります。

交換するクラスタノードがルートボリューム暗号化を使用している場合、ONTAPはディスクからボリューム情報を読み取ることができません。ルートボリュームのキーをリストアします。

> これは、ルートボリュームでNetAppボリューム暗号化を使用している場合にのみ該当します。

a. 特別なブートメニューに戻ります。

```
LOADER> boot_ontap menu
```

```
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)? 10
```

a. （10）Set Onboard Key Manager Recovery secrets（オンボードキーマネージャリカバリシークレットの設定）*を選択します

b. 入力するコマンド y 次のプロンプトが表示されます。

```
This option must be used only in disaster recovery procedures. Are you sure?
(y or n): y
```

c. プロンプトで、キー管理ツールのパスフレーズを入力します。

d. プロンプトが表示されたら、バックアップデータを入力します。

> でパスフレーズとバックアップデータを入手しておく必要があります "ノードをアップグレードする準備をします" この手順のセクション。

e. システムが再度特別な起動メニューを起動したら、オプション*（1）Normal Boot *を実行します

> この段階でエラーが発生する場合があります。エラーが発生した場合は、システムが正常にブートするまでの手順を繰り返し 手順 8 ます。

9. [reassign-node1-node3-app-step9]]外付けディスクを搭載したシステムから、内蔵ディスクと外付けディスクをサポートするシステム（AFF A800システムなど）にアップグレードする場合は、node1のアグリゲートをルートアグリゲートとして設定し、node3がnode1のルートアグリゲートからブートすることを確認します。ルートアグリゲートを設定するには、ブートメニューに移動し、メンテナンスモードに切り替えるオプションを選択します 5。

> * ここに示す順序で以下の手順を実行する必要があります。正しく実行しないと、原因が停止したり、データが失われたりする可能性があります。 *

次の手順は、 node3 を node1 のルートアグリゲートからブートするように設定します。

a. メンテナンスモードに切り替えます。

「 boot_ontap maint 」を使用してください

b. node1 アグリゲートの RAID 、プレックス、およびチェックサムの情報を確認します。

「 aggr status -r 」

c. node1 アグリゲートのステータスを確認します。

「 aggr status 」を入力します

d. 必要に応じて、 node1 アグリゲートをオンラインにします。

「aggr_online root_aggr_from__」を参照してください

e. node3 を元のルートアグリゲートからブートできないようにします。

「aggr offline_root_aggr_on_node3」を参照してください

f. node1 ルートアグリゲートを、 node3 の新しいルートアグリゲートとして設定します。

'aggr options aggr_from *node1* root

g. ノード 3 のルートアグリゲートがオフラインになっていること、およびノード 1 からテイクオーバーされたディスクのルートアグリゲートがオンラインになっていて root に設定されていることを確認し

ます。

「 aggr status 」を入力します

前の手順を実行しないと、原因 node3 を内部ルートアグリゲートからブートするか、原因システムで新しいクラスタ構成が存在すると想定するか、あるいはクラスタ構成を特定するように求められる可能性があります。

次の例は、コマンドの出力を示しています。

```
---------------------------------------------------------------------
Aggr                    State    Status              Options

aggr0_nst_fas8080_15 online   raid_dp, aggr       root, nosnap=on
                              fast zeroed
                              64-bit

aggr0                   offline  raid_dp, aggr       diskroot
                              fast zeroed
                              64-bit
---------------------------------------------------------------------
```

ノード 3 のインストールを確認します

node1 の物理ポートが、 node3 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、 node3 は、アップグレード後に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

を参照してください "参考資料" Hardware Universe にリンクして新しいノードのポートに関する情報を取得するには、次の手順を実行します。このセクションの後半の情報を使用します。

物理ポートのレイアウトは、ノードのモデルによって異なる場合があります。新しいノードがブートすると、 ONTAP は、自動的にクォーラムに参加するためにクラスタ LIF をホストするポートを判別しようとします。

node1 の物理ポートが node3 の物理ポートに直接マッピングされていない場合は、次のセクションを参照してください ノード 3 でネットワーク設定をリストア ネットワーク接続を修復するために使用する必要があります。

node3 のインストールとブートが完了したら、正しくインストールされていることを確認する必要があります。node3 がクォーラムに参加するのを待ってから、再配置処理を再開する必要があります。

手順のこの時点で、 node3 がクォーラムに参加する間、処理が一時停止します。

手順

1. ノード 3 がクォーラムに参加していることを確認し

cluster show -node node3 -fields health`

「 health 」フィールドの出力は「 true 」でなければなりません。

2. ノード 3 が node2 と同じクラスタに含まれており、ノード 3 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

3. アップグレードするHAペアで実行しているONTAPのバージョンに応じて、次のいずれかの操作を実行します。

ONTAP のバージョン	作業
9.8 ~ 9.11.1	クラスタ LIF がポート 7700 をリスンしていることを確認します。 `::> network connections listening show -vserver Cluster`
9.12.1以降	この手順をスキップして、 手順 5。

次の 2 ノードクラスタの例に示すように、クラスタポートでリスンしているポート 7700 は想定される結果です。

```
Cluster::> network connections listening show -vserver Cluster
Vserver Name     Interface Name:Local Port     Protocol/Service
---------------- ----------------------------  -------------------
Node: NodeA
Cluster          NodeA_clus1:7700               TCP/ctlopcp
Cluster          NodeA_clus2:7700               TCP/ctlopcp
Node: NodeB
Cluster          NodeB_clus1:7700               TCP/ctlopcp
Cluster          NodeB_clus2:7700               TCP/ctlopcp
4 entries were displayed.
```

4. ポート7700をリスンしていない各クラスタLIFについて、LIFの管理ステータスをに設定します。 `down` 次に `up`：

`::> net int modify -vserver Cluster-lif cluster_lif_cluster-status-admin down；net int modify -vserver Cluster-lif cluster_lif_-status-admin up

手順 3 を繰り返して、クラスタ LIF がポート 7700 でリスンしていることを確認します。

5. advanced権限モードに切り替えます。

「高度」

6. コントローラ交換処理のステータスを確認し、ノード 1 を停止する前と同じ状態で一時停止状態になっていることを確認して、新しいコントローラの設置とケーブルの移動の物理的なタスクを実行します。

「 system controller replace show 」と表示されます

「 system controller replace show-sdetails 」というエラーが表示されます

7. MetroCluster システムを使用している場合は、交換したコントローラが MetroCluster 構成に対して正しく設定されていることを確認します。 MetroCluster 構成が正常な状態である必要があります。を参照してください "MetroCluster 構成の健全性を確認"。

   手順 6 に進む前に、 MetroCluster ノード node3 でクラスタ間 LIF を再設定し、クラスタピアリングを調べて MetroCluster ノード間の通信をリストアすることを確認します。

   MetroCluster ノードのステータスを確認します。

   MetroCluster node show

8. コントローラの交換処理を再開します。

   「システムコントローラの交換が再開」

9. コントローラの交換は一時停止し、次のメッセージが表示されます。

```
Cluster::*> system controller replace show
Node              Status                       Error-Action
----------------- ------------------------
-----------------------------------
Node1(now node3) Paused-for-intervention      Follow the instructions
given in
                                               Step Details
Node2                       None

Step Details:
--------------------------------------------
To complete the Network Reachability task, the ONTAP network
configuration must be manually adjusted to match the new physical
network configuration of the hardware. This includes:

1. Re-create the interface group, if needed, before restoring VLANs. For
detailed commands and instructions, refer to the "Re-creating VLANs,
ifgrps, and broadcast domains" section of the upgrade controller
hardware guide for the ONTAP version running on the new controllers.
2. Run the command "cluster controller-replacement network displaced-
vlans show" to check if any VLAN is displaced.
3. If any VLAN is displaced, run the command "cluster controller-
replacement network displaced-vlans restore" to restore the VLAN on the
desired port.

2 entries were displayed.
```

この手順では、 VLAN 、 ifgrp 、およびブロードキャストドメインの作成に関するセクションの名前が、 node3 のネットワーク設定の名前が _Restore に変更されています。

10. コントローラの交換を一時停止状態にした状態で次のセクションに進んで、ノードのネットワーク設定をリストアします。

ノード **3** でネットワーク設定をリストア

node3 がクォーラムにあり、 node2 と通信できることを確認したら、 node1 の VLAN 、インターフェイスグループ、およびブロードキャストドメインが node3 にあることを確認します。また、 node3 のすべてのネットワークポートが正しいブロードキャストドメインに設定されていることを確認します。

このタスクについて

VLAN 、インターフェイスグループ、およびブロードキャストドメインの作成と再作成の詳細については、を参照してください "参考資料" をクリックして _ ネットワーク管理 _ にリンクします。

AFF A800またはAFF C800システムでクラスタポートe0aおよびe1aのポート速度を変更すると、速度変換後に不正な形式のパケットを受信することがあります。を参照してください "NetApp Bugs OnlineのバグID1570339" ナレッジベースの記事 "40GbEから100GbEへの変換後のT6ポートのCRCエラー" を参照してください。

手順

1. [[step1] アップグレードした node1 （ node3 ）上のすべての物理ポートを表示します。

   network port show -node node3

   ノードのすべての物理ネットワークポート、 VLAN ポート、およびインターフェイスグループポートが表示されます。この出力から、 ONTAP によって「 Cluster 」ブロードキャストドメインに移動された物理ポートを確認できます。この出力を使用して、 LIF をホストするためにインターフェイスグループメンバーポート、 VLAN ベースポート、またはスタンドアロンの物理ポートとして使用するポートを決定できます。

2. [step2] クラスタ上のブロードキャストドメインの一覧を表示します。

   「 network port broadcast-domain show 」

3. node3 のすべてのポートの到達可能性をリストします。

   「 network port reachability show 」のように表示されます

   次の例のような出力が表示されます。

```
clusterA::*> reachability show -node node1_node3
(network port reachability show)
Node         Port       Expected Reachability   Reachability Status
-----------  ---------  ----------------------  ----------------------
node1_node3
             a0a        Default:Default         no-reachability
             a0a-822    Default:822             no-reachability
             a0a-823    Default:823             no-reachability
             e0M        Default:Mgmt            ok
             e0a        Cluster:Cluster         misconfigured-
reachability
             e0b        Cluster:Cluster         no-reachability
             e0c        Cluster:Cluster         no-reachability
             e0d        Cluster:Cluster         no-reachability
             e0e        Cluster:Cluster         ok
             e0e-822    -                       no-reachability
             e0e-823    -                       no-reachability
             e0f        Default:Default         no-reachability
             e0f-822    Default:822             no-reachability
             e0f-823    Default:823             no-reachability
             e0g        Default:Default         misconfigured-
reachability
             e0h        Default:Default         ok
             e0h-822    Default:822             ok
             e0h-823    Default:823             ok
18 entries were displayed.
```

上記の例では、 node1 _node3 はコントローラの交換後にブートしたばかりです。一部のポートは想定されるブロードキャストドメインに到達できないため、修復が必要です。

4. 'node3 の各ポートの到達可能性を 'OK' 以外の到達可能性ステータスで修復します次のコマンドを最初に任意の物理ポートで実行し、次に任意の VLAN ポートで一度に 1 つずつ実行します。

   'network port reachability repair-Node_node_name — port_port_port_name_`

   次の例のような出力が表示されます。

```
Cluster ::> reachability repair -node node1_node3 -port e0h
```

```
Warning: Repairing port "node1_node3: e0h" may cause it to move into a
different broadcast domain, which can cause LIFs to be re-homed away
from the port. Are you sure you want to continue? {y|n}:
```

上記の警告メッセージは、到達可能性ステータスのポートで、現在配置されているブロードキャストドメ

インの到達可能性ステータスとは異なる可能性がある場合に表示されます。ポートと回答 'y' または 'n' の接続を適宜確認します

すべての物理ポートに想定される到達可能性があることを確認します。

「 network port reachability show 」のように表示されます

到達可能性の修復が実行されると、 ONTAP は正しいブロードキャストドメインにポートを配置しようとします。ただし、ポートの到達可能性を判別できず、既存のどのブロードキャストドメインにも属していない場合、 ONTAP はこれらのポート用に新しいブロードキャストドメインを作成します。

5. [[step5] インターフェイスグループの設定が新しいコントローラの物理ポートレイアウトと一致しない場合は、次の手順に従って変更します。

   a. 最初に、インターフェイスグループのメンバーポートにする物理ポートを、それぞれのブロードキャストドメインメンバーシップから削除する必要があります。これを行うには、次のコマンドを使用します。

      「network port broadcast-domain remove-ports -broadcast-domain broadcast_domain_name」 -ports_node_name -ports_node_name：port_name

   b. インターフェイスグループにメンバーポートを追加します。

      「network port ifgrp add -port -node node_name」-ifgrp_-port_port_port_name_`

   c. インターフェイスグループは、最初のメンバーポートが追加されてから約 1 分後にブロードキャストドメインに自動的に追加されます。

   d. インターフェイスグループが適切なブロードキャストドメインに追加されたことを確認します。

      「network port reachability show -node node_name --port_ifgrp_`」という形式で表示されます

      インターフェイスグループの到達可能性ステータスが「 OK 」でない場合は、適切なブロードキャストドメインに割り当てます。

「network port broadcast-domain add-ports -broadcast-domain broadcast_domain_name」-ports_node ：port_

6. [step6] 適切な物理ポートを 'Cluster' ブロードキャストドメインに割り当てるには ' 次の手順に従います

   a. 'Cluster' ブロードキャスト・ドメインに到達可能なポートを判別します

      「 network port reachability show-reachable-broadcast-domain Cluster ： Cluster 」

   b. 到達可能性ステータスが「 OK 」でない場合は、「 Cluster 」ブロードキャストドメインに到達可能なすべてのポートを修復します。

      'network port reachability repair-Node_node_name — port_port_port_name_`

7. [[step7] 次のいずれかのコマンドを使用して、残りの物理ポートを正しいブロードキャストドメインに移動します。

   'network port reachability repair-Node_node_name — port_port_port_name_`

「 network port broadcast-domain remove-port 」のようになります

「 network port broadcast-domain add-port 」と入力します

到達不能または予期しないポートが存在しないことを確認します。次のコマンドを使用してすべての物理ポートの到達可能性ステータスをチェックし、出力を調べてステータスが「 OK 」であることを確認します。

「 network port reachability show-detail` 」と表示されます

8. [[step8] 次の手順を使用して、取り外された可能性のある VLAN を復元します。

   a. 取り外された VLAN のリスト：

      「cluster controller -replacement network変位- VLANs show」と表示されます

      次のような出力が表示されます。

```
Cluster::*> displaced-vlans show
(cluster controller-replacement network displaced-vlans show)
          Original
Node      Base Port   VLANs
--------  ----------  ----------------------------------------
Node1       a0a       822, 823
            e0e       822, 823
2 entries were displayed.
```

   b. 以前のベースポートから取り外された VLAN を復元します。

      クラスタ・コントローラ交換ネットワークが取り外されましたVLANがリストアされました

      次に、インターフェイスグループ a0a から削除された VLAN を同じインターフェイスグループにリストアする例を示します。

```
Cluster::*> displaced-vlans restore -node node1_node3 -port a0a
-destination-port a0a
```

      次に、ポート「 e0e 」上の取り外された VLAN を「 E0h 」にリストアする例を示します。

```
Cluster::*> displaced-vlans restore -node node1_node3 -port e0e
-destination-port e0h
```

      VLAN の復元が成功すると、指定された宛先ポートに、取り外された VLAN が作成されます。デスティネーションポートがインターフェイスグループのメンバーである場合、またはデスティネーションポートがダウンしている場合、 VLAN のリストアは失敗します。

新しくリストアした VLAN が適切なブロードキャストドメインに配置されるまで約 1 分待ちます。

a. 必要に応じて'クラスタコントローラ交換ネットワークではないVLANポート用に新しいVLANポートを作成しますが'VLANは出力を示しますが'他の物理ポート上で構成する必要があります

9. [[step9] すべてのポート修復が完了したら、空のブロードキャストドメインを削除します。

   `network port broadcast-domain delete -broadcast-domain broadcast_domain_name`

10. [[step10]] ポートの到達可能性を確認します。

    「 network port reachability show 」のように表示されます

    すべてのポートが正しく設定され、正しいブロードキャストドメインに追加されている場合、「 network port reachability show 」コマンドは、接続されているすべてのポートの到達可能性ステータスを「 ok 」、物理的に接続されていないポートのステータスを「 no-reachability 」と報告する必要があります。この 2 つ以外のステータスが報告されたポートがある場合は、到達可能性修復を実行し、の手順に従ってブロードキャストドメインにポートを追加または削除します 手順 4。

11. すべてのポートがブロードキャストドメインに配置されたことを確認します。

    「 network port show 」のように表示されます

12. ブロードキャストドメインのすべてのポートで、正しい Maximum Transmission Unit （ MTU ；最大伝送ユニット）が設定されていることを確認します。

    「 network port broadcast-domain show 」

13. 次の手順に従って、リストアが必要な SVM および LIF のホームポートがある場合は、それらを指定して LIF のホームポートをリストアします。

    a. 移動された LIF を表示します。

       「 dispaced-interface show 」

    b. LIF のホームノードとホームポートをリストアします。

       「cluster controller -replacement network変位-interface restore-home-node-node_node_name *-vserver_vserver_name _-lif - name_lif_name*`

14. すべての LIF にホームポートがあり、意図的に稼働状態になっていることを確認します。

    network interface show -fields home-port、status-admin

ノード **3** でキー管理ツールの設定をリストアします

NetApp Volume Encryption（NVE）およびNetApp Aggregate Encryption（NAE）を使用してアップグレードするシステムのボリュームを暗号化する場合は、暗号化設定を新しいノードに同期する必要があります。キー管理ツールを同期しない場合、ARLを使用してノード1のアグリゲートをノード2からノード3に再配置すると、ノード3に暗号化されたボリュームとアグリゲートをオンラインにするための必要な暗号化キーがないために障害が発生することがあります。

このタスクについて

次の手順を実行して、暗号化設定を新しいノードに同期します。

手順

1. ノード3から次のコマンドを実行します。

   「セキュリティキーマネージャオンボード同期」

2. データアグリゲートを再配置する前に、ノード3のSVM-KEKキーが「true」にリストアされたことを確認します。

```
::> security key-manager key query -node node3 -fields restored -key
-type SVM-KEK
```

例

```
::> security key-manager key query -node node3 -fields restored -key
-type SVM-KEK

node     vserver   key-server   key-id
restored
-------- --------- -----------  ----------------------------------------
--------
node3    svm1      ""           000000000000000020000000000a008a81976
true
                                2190178f9350e071fbb90f00000000000000000
```

ノード **1** で所有されているルート以外のアグリゲートと **NAS** データ **LIF** を、ノード **2** からノード **3** に移動します

ノード 3 のネットワーク設定を確認し、ノード 2 からノード 3 にアグリゲートを再配置する前に、ノード 2 に現在あるノード 1 に属する NAS データ LIF が node2 からノード 3 に再配置されたことを確認する必要があります。また、ノード 3 に SAN LIF が存在することも確認する必要があります。

このタスクについて

アップグレード手順の実行中、リモート LIF は SAN LUN へのトラフィックを処理します。アップグレード時にクラスタやサービスの健全性を維持するために、 SAN LIF を移動する必要はありません。SAN LIF は、新しいポートにマッピングする必要がないかぎり移動されません。ノード 3 をオンラインにしたあと、 LIF が正常に機能しており、適切なポートに配置されていることを確認します。

T6ベースのイーサネットネットワークインターフェイスカードまたはマザーボードポートのポート速度を変更すると、速度変換後に不正な形式のパケットが受信されることがあります。を参照してください "NetApp Bugs OnlineのバグID1570339" ナレッジベースの記事 "40GbEから100GbEへの変換後のT6ポートのCRCエラー" を参照してください。

手順

1. 再配置処理を再開します。

```
system controller replace resume
```

システムは次のタスクを実行します。

- クラスタクォーラムチェック
- システム ID の確認
- イメージのバージョンチェック
- ターゲットプラットフォームのチェック
- ネットワーク到達可能性チェック

ネットワーク到達可能性チェックのこの段階で処理が一時停止します。

2. 再配置処理を再開します。

```
system controller replace resume
```

システムは次のチェックを実行します。

- クラスタの健全性チェック
- クラスタ LIF のステータスを確認します

これらのチェックの実行後、 node1 で所有されているルート以外のアグリゲートと NAS データ LIF が新しいコントローラ node3 に再配置されます。リソースの再配置が完了すると、コントローラの交換処理が一時停止します。

3. アグリゲートの再配置処理と NAS データ LIF の移動処理のステータスを確認します。

```
system controller replace show-details
```

コントローラ交換用手順が一時停止している場合は、エラーがある場合はチェックして修正し、次に「問題 re sume 」をクリックして操作を続行します。

4. 必要に応じて、移動された LIF を復元して元に戻すか、自動的に再配置できなかったノード 1 LIF をノード 3 に手動で移行して変更します。

移動した**LIF**を復元して元に戻す

a. 移動した LIF をリストします。

```
cluster controller-replacement network displaced-interface show
```

b. LIF が表示されなくなった場合は、ホームノードをノード 3 にリストアします。

```
cluster controller-replacement network displaced-interface
restore-home-node -node <node3_nodename> -vserver <vserver name>
-lif-name <lif_name>
```

LIFを手動で移行および変更する

a. 自動的に再配置できなかった LIF をノード 3 に移行します。

```
network interface migrate -vserver <vserver name> -lif <lif_name>
-destination-node <node3_nodename> -destination-port
<port_on_node3>
```

b. 移行された LIF のホーム ノードとホーム ポートを変更します。

```
network interface modify -vserver <vserver_name> -lif
<data_lif_name> -home-node <node3_nodename> -home-port
<home_port>
```

5. この処理を再開すると、必要なポストチェックの実行をシステムに求めるプロンプトが表示されます。

```
system controller replace resume
```

次のポストチェックが実行されます。

- クラスタクォーラムチェック
- クラスタの健全性チェック
- アグリゲートの再構築チェック
- アグリゲートのステータスを確認します
- ディスクのステータスを確認します
- クラスタ LIF のステータスを確認します
- ボリュームチェック

ステージ 4 ：ノード 2 の移動と撤去

ルート以外のアグリゲートと NAS データ LIF を node2 から node3 に再配置します

ノード2をノード4に交換する前に、ノード2が所有するルート以外のアグリゲートとNASデータLIFをノード3に再配置します。

作業を開始する前に

前の段階で確認したあとに、 node2 のリソースリリースが自動的に開始されます。ルート以外のアグリゲートと SAN 以外のデータ LIF が node2 から node3 に移行されます。

このタスクについて

アップグレード手順の実行中、リモート LIF は SAN LUN へのトラフィックを処理します。アップグレード時にクラスタやサービスの健全性を維持するために、 SAN LIF を移動する必要はありません。

アグリゲートと LIF の移行が完了すると、検証のために処理が一時停止されます。この段階で、ルート以外のアグリゲートと SAN 以外のデータ LIF がすべて node3 に移行されているかどうかを確認する必要があります。

アグリゲートおよび LIF のホーム所有者は変更されません。現在の所有者のみが変更されます。

手順

1. ルート以外のすべてのアグリゲートがオンラインで、ノード 3 でそれらの状態になっていることを確認します。

   ```
   storage aggregate show -node <node3> -state online -root false
   ```

   次の例は、 node2 のルート以外のアグリゲートがオンラインになっていることを示しています。

   ```
   cluster::> storage aggregate show -node node3 state online -root false

   Aggregate      Size         Available   Used%   State   #Vols  Nodes
   RAID     Status
   ----------     ---------    ---------   ------  -----   -----  ------
   -------  ------
   aggr_1         744.9GB      744.8GB      0%     online  5      node2
   raid_dp  normal
   aggr_2         825.0GB      825.0GB      0%     online  1      node2
   raid_dp  normal
   2 entries were displayed.
   ```

   アグリゲートがオフラインになった場合、または node3 で外部になった場合は、各アグリゲートに対して次のコマンドを実行してそれらのアグリゲートをオンラインにします。

   ```
   storage aggregate online -aggregate <aggregate_name>
   ```

2. node3 で次のコマンドを実行し、出力を調べて、すべてのボリュームがノード 3 でオンラインになっていることを確認します。

   ```
   volume show -node <node3> -state offline
   ```

   node3 にオフラインのボリュームがある場合は、各ボリュームに対して次のコマンドを実行してそれらのボリュームをオンラインにします。

   ```
   volume online -vserver <vserver_name> -volume <volume_name>
   ```

   その `vserver_name`このコマンドで使用する方法は、前の出力で確認できます。 `volume show`指示。

3. LIF が正しいポートに移動され、ステータスが「 up 」になっていることを確認します。LIF が 1 つでも停止している場合は、次のコマンドを LIF ごとに 1 回入力して、 LIF の管理ステータスを「 up 」に設定します。

   ```
   network interface modify -vserver <vserver_name> -lif <LIF_name> -home-node
   <node_name> -status-admin up
   ```

4. データ LIF を現在ホストしているポートが新しいハードウェアに存在しない場合は、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 」と入力します

5. [[Step5]] 次のコマンドを入力し、出力を調べて、 node2 にデータ LIF が残っていないことを確認します。

   network interface show -curr-node _node2 -role data

障害が発生した、または拒否されたアグリゲートをノード**3**に再配置します。

集約の再配置に失敗したり、拒否されたりした場合は、集約を手動でノード 3 に再配置するか、必要に応じて拒否または宛先チェックのいずれかをオーバーライドする必要があります。

このタスクについて

エラーのため、システムは再配置操作を一時停止します。

手順

1. イベント管理システム（ EMS ）のログで、アグリゲートの再配置に失敗した理由や拒否された理由を確認します。
2. 障害が発生したアグリゲートまたは拒否されたアグリゲートを

   ```
   storage aggregate relocation start -node <node2> -destination <node3>
   -aggregate-list <aggregate_name> -ndo-controller-upgrade true
   ```

3. プロンプトが表示されたら、「 y 」と入力します。
4. 再配置は、次のいずれかの方法で強制的に実行できます。

オプション	説明
拒否チェックの無視	次のコマンドを使用します。 `storage aggregate relocation start -node node2 -destination node3 -aggregate-list <aggregate_list> -ndo-controller-upgrade true -override-vetoes true`
デスティネーションチェックの無効化	次のコマンドを使用します。 `storage aggregate relocation start -node node2 -destination node3 -aggregate-list <aggregate_list> -ndo-controller-upgrade true -override-vetoes true -override-destination-checks true`

ノード 2 を撤去

node2 を廃止するには、node2 を適切にシャットダウンし、ラックまたはシャーシから取り外します。

手順

1. 処理を再開します。

   「システムコントローラの交換が再開」

   ノードは自動的に停止します。

完了後

アップグレードの完了後に、 node2 の運用を停止できます。を参照してください "古いシステムの運用を停止"。

ステージ 5 ：ノード 4 をインストールしてブートします

ノード 4 をインストールしてブートします

ノード 4 をラックに設置し、ノード 2 の接続をノード 4 に転送し、ノード 4 をブートして、 ONTAP をインストールする必要があります。次に、このセクションで説明するように、ノード 2 のスペアディスク、ルートボリュームに属するディスク、およびプロセスの前にノード 3 に再配置されなかったルート以外のアグリゲートを再割り当てする必要があります。

このタスクについて

再配置処理はこのフェーズの開始時に一時停止されます。このプロセスはほとんどが自動化されており、処理は一時停止してステータスを確認できます。この処理は手動で再開する必要があります。

node4 のONTAPバージョンが node2 のONTAPバージョンと異なる場合は、node4 をネットブートする必要があります。node4 をインストールしたら、Web サーバーに保存されているONTAP 9 イメージから起動します。その後、次の手順に従って、次回以降のシステム起動時に正しいファイルをブートメディアデバイスにダ

ウンロードすることができます。 "ネットブートを準備"。

- AFF A800またはAFF C800コントローラのアップグレードの場合、ノード 2 を取り外す前に、シャーシ内のすべてのドライブがミッドプレーンにしっかりと固定されていることを確認する必要があります。詳細については、 "AFF A800またはAFF C800コントローラモジュールを交換"。
- ストレージディスクを備えたシステムをアップグレードする場合は、このセクション全体を完了してから、 "ノード 4 で FC または UTA / UTA2 設定を設定します"クラスタープロンプトでコマンドを入力します。

手順

1. [[auto_install4_stp1] ノード 4 に十分なラックスペースがあることを確認します。

   node4 が node2 とは別のシャーシにある場合は、 node3 と同じ場所に node4 を配置できます。node2 と node4 が同じシャーシにある場合は、 node4 が適切なラックの場所にすでに存在しているとします。

2. ノードモデルの _Installation and Setup Instructions _ の手順に従って、ノード 4 をラックに設置します。
3. ノード 4 をケーブル接続します。 node2 から node4 に接続を移動します。

   node4 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」、適切なディスク シェルフ ドキュメント、および「HA ペア管理」ドキュメントを使用して、次の接続をケーブル接続します。

   参照"参考資料"_HAペア管理_にリンクします。

   - コンソール（リモート管理ポート）
   - クラスタポート
   - データポート
   - クラスタポートとノード管理ポート
   - ストレージ
   - SAN 構成： iSCSI イーサネットおよび FC スイッチポート

   ほとんどのプラットフォームモデルには一意のインターコネクトカードモデルがあるため、インターコネクトカード / FC-VI カードまたはインターコネクト / FC-VI ケーブルの接続を node2 から node4 に移動する必要はありません。MetroCluster 構成の場合は、 FC-VI ケーブルの接続を node2 から node4 に移動する必要があります。新しいホストに FC-VI カードがない場合は、 FC-VI カードの移動が必要になることがあります。

4. ノード 4 の電源をオンにしてから、コンソール端末で 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。

   node4 をブートすると、次の警告メッセージが表示される場合があります。

```
WARNING: The battery is unfit to retain data during a power outage. This
is likely
         because the battery is discharged but could be due to other
temporary
         conditions.
         When the battery is ready, the boot process will complete
         and services will be engaged. To override this delay, press 'c'
followed
         by 'Enter'
```

5. 手順 4 で警告メッセージが表示された場合は、次の操作を実行します。

   a. NVRAM バッテリ低下以外の問題を示すコンソールメッセージがないか確認し、必要に応じて対処します。

   b. バッテリの充電と起動プロセスが完了するまで待ちます。

      遅延を無視しないでください。バッテリーの充電が不十分だと、データが失われる可能性があります。

   を参照してください "ネットブートを準備"。

6. [[step6] 次のいずれかの操作を選択して、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。データLIF IPは使用しないでください。使用しないと、アップグレードの実行中にデータ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

動的ホスト構成プロトコル（**DHCP**）の状態	作業
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入力して、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（必須）。 *netmask* は、ストレージシステムのネットワークマスクです（必須）。 *gateway* は、ストレージシステムのゲートウェイです（必須）。 *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（オプション）。 *dns_domain* は、DNSドメイン名です（オプション）。 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。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。

7. ノード 4 でネットブートを実行します。

用途	作業
FAS/AFF8000 シリーズシステム	netboot\http://<web_server_ip/path_to_web-accessible_directory>/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_the_web-accessible_directory> 」は、手順 1 の「 <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 "ネットブートを準備"。

トランクを中断しないでください。

8. 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 procedure is not supported for Non-Disruptive Upgrade on an HA pair
   ```

   コントローラのアップグレードではなく、 ONTAP による環境の無停止アップグレードも記録されています。

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 リリースオプションを指定してネットブート手順 を実行する `(7) Install new software` ブートメディアを消去して、両方のイメージパーティションに同じONTAP バージョンを配置します。

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、「 y 」と入力し、パッケージの入力を求められたら URL を入力します。

   http://<web_server_ip/path_to_web-accessible_directory>/<ontap_version>_image.tgz` にアクセスします

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. 次のプロンプトが表示されたら 'n' を入力してバックアップ・リカバリをスキップします

    ```
    Do you want to restore the backup configuration now? {y|n}
    ```

    b. 次の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}
    ```

    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、構成データをリストアする必要があるためです。

11. ブート・メニューからメンテナンス・モード「 5 」を選択し、ブートを続行するように求めるプロンプトが表示されたら「 y 」と入力します。
12. コントローラとシャーシが HA 構成になっていることを確認します。

    「 ha-config show 」

    次に 'ha-config show コマンドの出力例を示します

    ```
    Chassis HA configuration: ha
    Controller HA configuration: ha
    ```

    システムは、 HA ペア構成かスタンドアロン構成かを PROM に記録します。状態は、スタンドアロンシステムまたは HA ペア内のすべてのコンポーネントで同じである必要があります。

13. コントローラとシャーシが HA として構成されていない場合は、次のコマンドを使用して構成を修正します。

    「 ha-config modify controller ha 」を参照してください

    「 ha-config modify chassis ha 」を参照してください

MetroCluster 構成の場合は、次のコマンドを使用してコントローラとシャーシを変更します。

「 ha-config modify controller mcc 」

「 ha-config modify chassis mcc 」

14. メンテナンスモードを終了します。

    「 halt 」

    ブート環境のプロンプトでCtrl+Cキーを押して、AUTOBOOTを中断します。

15. [auto_install4_step15]] ノード 3 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。

    「食事」

16. node4 で、ブート環境のプロンプトで次のコマンドを使用して日付を確認します。

    「日付」

17. 必要に応じて、 node4 に日付を設定します。

    'set date_mm/dd/yyyy_`

18. node4 で、ブート環境のプロンプトで次のコマンドを使用して時間を確認します。

    「時間」

19. 必要に応じて、 node4 に時間を設定します。

    'set time_hh:mm:ss_`

20. ブートローダーのnode4にあるパートナーシステムIDを設定します。

    setsetenv partner-sysid_node3 *sysid*`

    ノード4の場合、 `partner-sysid` node3のノードである必要があります。

    設定を保存します。

    'aveenv

21. [[auto_install4_step21]を確認します `partner-sysid` ノード4の場合：

    printenv partner-sysid

22. NetApp Storage Encryption (NSE) ドライブがインストールされている場合は、次の手順を実行します。

    手順 でこれまでに行ったことがない場合は、Knowledge Baseの記事を参照してください "ドライブがFIPS認定かどうかを確認する方法" 使用している自己暗号化ドライブのタイプを確認するため。

a. 設定 `bootarg.storageencryption.support` 終了： `true` または `false`：

次のドライブが使用中の場合	次に、
FIPS 140-2レベル2の自己暗号化要件に準拠したNSEドライブ	`setenv bootarg.storageencryption.support` **`true`**
ネットアップの非FIPS SED	`setenv bootarg.storageencryption.support` **`false`**

FIPSドライブは、同じノードまたはHAペアで他のタイプのドライブと混在させることはできません。SEDと非暗号化ドライブを同じノードまたはHAペアで混在させることができます。

b. 特別なブートメニューに移動してオプションを選択します `(10) Set Onboard Key Manager recovery secrets`。

手順の前半で記録したパスフレーズとバックアップ情報を入力します。"オンボードキーマネージャを使用してストレージ暗号化を管理します"を参照してください。

23. ノードをブートメニューでブートします。

「 boot_ontap menu

次の手順

- FCまたはUTA/UTA2構成の場合、"ノード4のFCまたはUTA/UTA2ポートを設定および構成する" 。
- FCまたはUTA/UTA2構成がない場合は、"ノード2のディスクをノード4に再割り当てする、ステップ1" ノード4がノード2のディスクを認識できるようにする。
- MetroCluster構成の場合、"ノード4のFCまたはUTA/UTA2ポートを設定および構成する"ノードに接続されているディスクを検出します。

ノード 4 で FC または UTA / UTA2 設定を設定します

ノード 4 でオンボードの FC ポート、オンボードのユニファイドターゲットアダプタ（ UTA / UTA2 ）ポート、または UTA / UTA2 カードが使用されている場合は、残りの手順を完了する前に設定する必要があります。

このタスクについて

完了する必要があるかもしれませんノード 4 の FC ポートを設定しますまたはノード 4 の UTA / UTA2 ポートを確認して設定してください、または両方のセクション。

ノード4にオンボードFCポート、オンボードUTA/UTA2ポート、またはUTA/UTA2カード（たとえば、 ONTAP 9.15.1以降に導入されたAFFおよびFASシステム）がなく、ストレージディスクを備えたシステムをアップグレードする場合は、"ノード2のディスクをノード4に再割り当てします。" 。

ノード 4 に十分なラックスペースがあることを確認してください。node4 と node2 が別々のシャーシにある場合は、 node4 を node3 と同じ場所に配置できます。node2 と node4 が同じシャーシにある場合は、 node4 が適切なラックの場所にすでに存在しているとします。

ノード 4 の FC ポートを設定します

node4 にオンボードまたはアドオン FC アダプタ上の FC ポートがある場合、システムの出荷時にポートが事前構成されていないため、ノードをサービスに投入する前にノード上でポート構成を設定する必要があります。必要に応じてポートを構成しないと、サービスが中断される可能性があります。

作業を開始する前に

セクションに保存した node2 の FC ポート設定の値を確認しておく必要があります "ノードをアップグレードする準備をします"。

このタスクについて

システムに FC 構成がない場合は、このセクションをスキップしてかまいません。システムにオンボード UTA / UTA2 ポートまたは UTA / UTA2 アダプタが搭載されている場合は、で設定します ノード 4 の UTA / UTA2 ポートを確認して設定してください。

このセクションのコマンドをメンテナンス モードのシェル プロンプトで入力します。

手順

1. システム上のすべての FC および統合ネットワーク アダプタに関する情報を表示します。

   「 system node hardware unified-connect show 」を参照してください

2. ノード 4 の FC 設定とノード 1 から前に取得した設定を比較します。
3. 必要に応じて、ノード 4 の FC ポートを変更します。

   ◦ ターゲット ポートとしてプログラムするには:

   ucadmin modify -m fc -t target_adapter_`

   例えば： `ucadmin modify -m fc -t target 2a`

   ◦ イニシエータポートをプログラミングする場合：

   ucadmin modify -m fc -t initiator_adapter_`

   `-t` は FC4 のタイプで ' ターゲットまたはイニシエータです

   例えば： `ucadmin modify -m fc -t initator 2b`

4. ノードを停止します。

   「 halt 」

5. LOADERプロンプトからシステムをブートします。

   「 boot_ontap menu

6. コマンドを入力したら、ブート環境のプロンプトでシステムが停止するまで待ちます。
7. 保守モードのブート・メニューからオプション「 5 」を選択します。
8. 次のいずれかの操作を実行します。

- に進みます ノード 4 の UTA / UTA2 ポートを確認して設定してください ノード 4 に UTA / UTA2 カードまたは UTA / UTA2 オンボードポートがある場合
- ノード4にUTA/UTA2カードまたはUTA/UTA2オンボードポートがない場合は、「ノード4のUTA/UTA2ポートの確認と設定」をスキップして、"ノード2のディスクをノード4に再割り当てします。" 。

ノード **4** の **UTA / UTA2** ポートを確認して設定してください

ノード 4 でオンボード UTA / UTA2 ポートまたは UTA / UTA2A カードが使用されている場合は、アップグレードしたシステムの使用方法に応じて、ポートの設定を確認して設定する必要があります。

作業を開始する前に

UTA / UTA2 ポートに対応する正しい SFP+ モジュールが必要です。

このタスクについて

UTA / UTA2 ポートは、ネイティブの FC モードまたは UTA / UT2A モードに設定できます。FC モードでは FC イニシエータと FC ターゲットがサポートされます。 UTA / UTA2 モードを使用すると、 NIC と FCoE の同時トラフィックで同じ 10GbE SFP+ インターフェイスを共有し、 FC ターゲットをサポートすることができます。

ネットアップのマーケティング資料では、 UTA2 という用語を CNA アダプタとポートという意味で使用している場合があります。ただし、 CLI では CNA という用語が使用されます。

UTA / UTA2 ポートはアダプタまたはコントローラ上に次の構成で配置されます。

- UTA / UTA2 カードは、コントローラと同時に注文しても、希望するパーソナリティを持つ未設定の状態で出荷されます。
- コントローラとは別に発注した UTA / UTA2 カードは、デフォルトの FC ターゲットパーソナリティとして出荷されます。
- 新しいコントローラのオンボード UTA / UTA2 ポートは、要求したパーソナリティを持つように（出荷前に）設定されています。

ただし、ノード 4 の UTA / UTA2 ポートの設定を確認し、必要に応じて変更してください。

このセクションのコマンドをメンテナンス モードのシェル プロンプトで入力します。

手順

1. ノード 4 でポートが現在どのように構成されているかを確認します。

   「 system node hardware unified-connect show 」を参照してください

   次の例のような出力が表示されます。

```
*> ucadmin show
                Current  Current    Pending   Pending   Admin
Node   Adapter  Mode     Type       Mode      Type      Status
----   -------  ---      ---------  -------   --------  -------
f-a    0e       fc       initiator  -          -        online
f-a    0f       fc       initiator  -          -        online
f-a    0g       cna      target     -          -        online
f-a    0h       cna      target     -          -        online
f-a    0e       fc       initiator  -          -        online
f-a    0f       fc       initiator  -          -        online
f-a    0g       cna      target     -          -        online
f-a    0h       cna      target     -          -        online
*>
```

2. 現在の SFP+ モジュールが目的の用途と一致しない場合は、正しい SFP+ モジュールに交換します。

   ネットアップの担当者に連絡して、正しい SFP+ モジュールを入手します。

3. 設定を確認します。

   ucadmin show

   ucadmin show コマンドの出力結果を調べ、 UTA / UTA2 ポートが希望するパーソナリティに対応しているかどうかを確認します。

   次の例の出力は ' アダプタ「 1b 」の FC4 タイプがイニシエータに変更され ' アダプタ「 2a 」および「 2b 」のモードが「 cna' 」に変更されていることを示しています

```
*> ucadmin show
Node  Adapter  Current Mode  Current Type  Pending Mode  Pending Type
Admin Status
----  -------  ------------  ------------  ------------  ------------
------------
f-a   1a       fc             initiator    -             -
online
f-a   1b       fc             target       -             initiator
online
f-a   2a       fc             target       cna           -
online
f-a   2b       fc             target       cna           -
online
4 entries were displayed.
*>
```

4. 次のいずれかを実行します。

CNA ポートの状況	次に、
希望するパーソナリティがない	に進みます 手順 5。
あなたがほしい人格を持っている	ステップ5からステップ9をスキップして、手順 10 。

5. [[auto_check_4_step5] 次のいずれかの操作を実行します。

を設定する場合	次に、
UTA / UTA2 カードのポート	へ移動手順 6
オンボードの UTA/UTA2 ポート	ステップ6をスキップして手順 7。

6. アダプタがイニシエーターモードであり、UTA/UTA2 ポートがオンラインの場合は、UTA/UTA2 ポートをオフラインにします。

   storage disable adapter_adapter_adapter_adapter_name_`

   ターゲットモードのアダプタは、メンテナンスモードで自動的にオフラインになります。

7. [[auto_check_4_step7] 現在の構成が目的の用途に一致しない場合は、必要に応じて構成を変更します。

   ```
   ucadmin modify -m fc|cna -t initiator|target <adapter_name>
   ```

   - 「 -m 」はパーソナリティ・モード、 FC または 10GbE UTA です。
   - `-t` は FC4 のタイプ、「 target 」または「 initiator 」です。

   > テープ ドライブおよびMetroCluster構成には FC イニシエーターを使用する必要があります。 SAN クライアントには FC ターゲットを使用する必要があります。

8. 次のコマンドを各ポートごとに 1 回入力して、ターゲット ポートをオンラインにします。

   ```
   storage enable adapter <adapter_name>
   ```

9. ポートをケーブル接続します。
10. メンテナンスモードを終了:

    「 halt 」

11. ノードをブートメニューでブートします。

    「 boot_ontap menu

次の手順

- AFF A800システムにアップグレードする場合は、に進みます"ノード2のディスクをノード4に再割り当て（手順9）"。
- その他のシステムアップグレードについては、"ノード2のディスクをノード4の手順1に再割り当てしま

す。"。

ノード**2**のディスクをノード**4**に再割り当てします。

ノード2に属していたディスクをノード4に再割り当てしてから、ノード4のインストールを確認する必要があります。

手順

1. ノード2がブートメニューで停止していることを確認し、ノード2のディスクをノード4に再割り当てします。

   ```
   boot_after_controller_replacement
   ```

   少し待機したあと、交換するノードの名前を入力するように求められます。共有ディスク（Advanced Disk Partitioning（ADP；アドバンストディスクパーティショニング）またはパーティショニングされたディスクとも呼ばれます）がある場合は、HAパートナーのノード名を入力するように求められます。

   これらのプロンプトは、コンソールメッセージに埋もれている可能性があります。ノード名を入力しなかった場合や間違った名前を入力した場合は、名前をもう一度入力するように求められます。

コンソールの出力例を展開します

```
LOADER-A> boot_ontap menu
.
.
<output truncated>
.
All rights reserved.
*****************************
*                           *
* Press Ctrl-C for Boot Menu. *
*                           *
*****************************
.
<output truncated>
.
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)? 22/7
(22/7)                          Print this secret List
(25/6)                          Force boot with multiple filesystem
disks missing.
(25/7)                          Boot w/ disk labels forced to clean.
(29/7)                          Bypass media errors.
(44/4a)                         Zero disks if needed and create new
flexible root volume.
(44/7)                          Assign all disks, Initialize all
disks as SPARE, write DDR labels
.
.
<output truncated>
.
.
(wipeconfig)                        Clean all configuration on boot
device
```

```
(boot_after_controller_replacement) Boot after controller upgrade
(boot_after_mcc_transition)         Boot after MCC transition
(9a)                                Unpartition all disks and remove
their ownership information.
(9b)                                Clean configuration and
initialize node with partitioned disks.
(9c)                                Clean configuration and
initialize node with whole disks.
(9d)                                Reboot the node.
(9e)                                Return to main boot menu.
The boot device has changed. System configuration information could
be lost. Use option (6) to
restore the system configuration, or option (4) to initialize all
disks and setup a new system.
Normal Boot is prohibited.
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)? boot_after_controller_replacement
This will replace all flash-based configuration with the last backup
to disks. Are you sure
you want to continue?: yes
.
.
<output truncated>
.
.
Controller Replacement: Provide name of the node you would like to
replace:
<nodename of the node being replaced>
Controller Replacement: Provide High Availability partner of node1:
<nodename of the partner of the node being replaced>
Changing sysid of node node2 disks.
Fetched sanown old_owner_sysid = 536940063 and calculated old sys id
= 536940063
Partner sysid = 4294967295, owner sysid = 536940063
.
```

```
.
<output truncated>
.
.
varfs_backup_restore: restore using /mroot/etc/varfs.tgz
varfs_backup_restore: attempting to restore /var/kmip to the boot
device
varfs_backup_restore: failed to restore /var/kmip to the boot device
varfs_backup_restore: attempting to restore env file to the boot
device
varfs_backup_restore: successfully restored env file to the boot
device wrote
    key file "/tmp/rndc.key"
varfs_backup_restore: timeout waiting for login
varfs_backup_restore: Rebooting to load the new varfs
Terminated
<node reboots>
System rebooting...
.
.
Restoring env file from boot media...
copy_env_file:scenario = head upgrade
Successfully restored env file from boot media...
Rebooting to load the restored env file...
.
System rebooting...
.
.
.
<output truncated>
.
.
.
.
WARNING: System ID mismatch. This usually occurs when replacing a
boot device or NVRAM cards!
Override system ID? {y|n} y
.
.
.
.
Login:
```

上記のコンソールの出力例では、アドバンストディスクパーティショニング（ADP）ディスクを使用するシステムの場合は ONTAP からパートナーノード名の入力を求められます。

2. システムが再起動ループに入り、メッセージが表示された場合は `no disks found`これは、システムが FC または UTA/UTA2 ポートをターゲット モードにリセットしたため、ディスクが認識されないことを示します。この問題を解決するには、次のいずれかのタスクを選択してください。
   - 実行する手順 3に手順 8ノード4上
   - セクションへ移動"ノード 4 のインストールを確認します"
3. [reassign-node2-node4-app-step3]]自動ブート中にCtrl+Cキーを押して、Loader >プロンプトでノードを停止します。
4. LOADERプロンプトで、メンテナンスモードに切り替えます。

   「 boot_ontap maint 」を使用してください
5. 保守モードで、以前に設定したすべてのイニシエータポートをターゲットモードで表示します。

   ucadmin show

   ポートをイニシエータモードに戻します。

   ucadmin modify -m fc -t initiator -f adapter name_`
6. ポートがイニシエータモードに変更されたことを確認します。

   ucadmin show
7. メンテナンスモードを終了します。

   「 halt 」

   外付けディスクをサポートするシステムから外付けディスクもサポートするシステムにアップグレードする場合は、に進みます手順 8。

   外付けディスクを使用するシステムから、内蔵ディスクと外付けディスクの両方をサポートするシステム（AFF A800システムなど）にアップグレードする場合は、に進みます。手順 9
8. Loaderプロンプトでブートします。

   「 boot_ontap menu

   これで、ブート時に以前に割り当てられていたすべてのディスクをノードで検出できるようになり、想定どおりにブートできるようになります。

   交換するクラスタノードがルートボリューム暗号化を使用している場合、ONTAPはディスクからボリューム情報を読み取ることができません。ルートボリュームのキーをリストアします。

   これは、ルートボリュームでNetAppボリューム暗号化を使用している場合にのみ該当します。

a. 特別なブートメニューに戻ります。

```
LOADER> boot_ontap menu
```

```
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)? 10
```

a. （10）Set Onboard Key Manager Recovery secrets（オンボードキーマネージャリカバリシークレットの設定）*を選択します

b. 入力するコマンド `y` 次のプロンプトが表示されます。

```
This option must be used only in disaster recovery procedures. Are you sure?
(y or n): y
```

c. プロンプトで、キー管理ツールのパスフレーズを入力します。

d. プロンプトが表示されたら、バックアップデータを入力します。

でパスフレーズとバックアップデータを入手しておく必要があります "ノードをアップグレードする準備をします" この手順のセクション。

e. システムが再度特別な起動メニューを起動したら、オプション*（1）Normal Boot *を実行します

この段階でエラーが発生する場合があります。エラーが発生した場合は、システムが正常にブートするまでの手順を繰り返し 手順 8 ます。

9. 外部ディスクを備えたシステムから内部ディスクと外部ディスクをサポートするシステム（AFF A800システムなど）にアップグレードする場合は、node2 アグリゲートをルート アグリゲートとして設定し、node4 が node2 のルート アグリゲートから起動するようにします。ルートアグリゲートを設定するには、ノード4のブートメニューに移動し、オプションを選択します。 `5`メンテナンスモードに入ります。

* ここに示す順序で以下の手順を実行する必要があります。正しく実行しないと、原因が停止したり、データが失われたりする可能性があります。 *

次の手順では、 node4 に node2 のルートアグリゲートからブートするよう設定しています。

a. メンテナンスモードに切り替えます。

「 boot_ontap maint 」を使用してください

b. node2 アグリゲートの RAID 、プレックス、およびチェックサムの情報を確認します。

「 aggr status -r 」

c. node2 アグリゲートのステータスを確認します。

「 aggr status 」を入力します

d. 必要に応じて、 node2 アグリゲートをオンラインにします。

「aggr_online root_aggr_from__」に設定します

e. ノード 4 が元のルートアグリゲートからブートしないようにします。

'aggr offline_root_aggr_on_node4

f. node2 のルートアグリゲートを node4 の新しいルートアグリゲートとして設定します。

'aggr options aggr_from__ node2 _root

g. ノード 4 のルートアグリゲートがオフラインになっていること、および node2 から提供されたディスクのルートアグリゲートがオンラインになっていて root に設定されていることを確認します。

「 aggr status 」を入力します

> ⓘ 前の手順を実行しない場合は、原因 node4 から内部ルートアグリゲートをブートするか、原因システムが新しいクラスタ構成が存在すると想定するか、あるいはクラスタ構成を特定するように求められる可能性があります。

次の例は、コマンドの出力を示しています。

```
---------------------------------------------------------------------
Aggr State                          Status               Options
aggr 0_nst_fas8080_15 online        raid_dp, aggr        root, nosnap=on
                                    fast zeroed
                                    64-bit
aggr0 offline                       raid_dp, aggr        diskroot
                                    fast zeroed`
                                    64-bit
---------------------------------------------------------------------
```

ノード **4** のインストールを確認します

node2 の物理ポートが node4 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、 node4 はアップグレード後に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

を参照してください "参考資料" Hardware Universe にリンクして新しいノードのポートに関する情報を取得するには、次の手順を実行します。このセクションの後半の情報を使用します。

物理ポートのレイアウトは、ノードのモデルによって異なる場合があります。新しいノードがブートすると、ONTAP は、自動的にクォーラムに参加するためにクラスタ LIF をホストするポートを判別しようとします。

node2 の物理ポートが node4 の物理ポートに直接マッピングされない場合は、次のセクションに続きます ノード 4 のネットワーク設定をリストアします ネットワーク接続を修復するために使用する必要があります。

ノード 4 のインストールとブートが完了したら、ノード 4 が正しくインストールされていることを確認する必要があります。ノード 4 がクォーラムに参加するのを待ってから、再配置処理を再開する必要があります。

手順のこの時点で、ノード 4 がクォーラムに参加する間、処理が一時停止します。

手順

1. ノード 4 がクォーラムに参加していることを確認し

   cluster show -node node4 -fields health`

   「 health 」フィールドの出力は「 true 」でなければなりません。

2. ノード 4 がノード 3 と同じクラスタに含まれていること、およびノード 4 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

3. アップグレードするHAペアで実行しているONTAPのバージョンに応じて、次のいずれかの操作を実行します。

ONTAP のバージョン	作業
9.8 ~ 9.11.1	クラスタ LIF がポート 7700 をリスンしていることを確認します。 `::> network connections listening show -vserver Cluster`
9.12.1以降	この手順をスキップして、 手順 5。

   次の 2 ノードクラスタの例に示すように、クラスタポートでリスンしているポート 7700 は想定される結果です。

```
Cluster::> network connections listening show -vserver Cluster
Vserver Name     Interface Name:Local Port     Protocol/Service
---------------- ----------------------------  -------------------
Node: NodeA
Cluster          NodeA_clus1:7700               TCP/ctlopcp
Cluster          NodeA_clus2:7700               TCP/ctlopcp
Node: NodeB
Cluster          NodeB_clus1:7700               TCP/ctlopcp
Cluster          NodeB_clus2:7700               TCP/ctlopcp
4 entries were displayed.
```

4. ポート7700をリスンしていない各クラスタLIFについて、LIFの管理ステータスをに設定します。 `down` 次に `up`：

   `::> net int modify -vserver Cluster-lif cluster_lif_cluster-status-admin down；net int modify -vserver Cluster-lif cluster_lif_-status-admin up

   手順 3 を繰り返して、クラスタ LIF がポート 7700 でリスンしていることを確認します。

5. advanced権限モードに切り替えます。

   「高度」

6. コントローラ交換処理のステータスを確認し、 node2 を停止する前と同じ状態で一時停止状態になっていることを確認して、新しいコントローラの取り付けやケーブルの移動の物理タスクを実行します。

   「 system controller replace show 」と表示されます

   「 system controller replace show-sdetails 」というエラーが表示されます

7. MetroCluster システムを使用している場合は、交換したコントローラが MetroCluster 構成に対して正しく設定されていることを確認します。 MetroCluster 構成が正常な状態である必要があります。を参照してください "MetroCluster 構成の健全性を確認"。

   MetroCluster ノード node4 にあるクラスタ間 LIF を再設定し、 MetroCluster ノード間の通信をリストアするクラスタピアリングをチェックします 手順 6。

   MetroCluster ノードのステータスを確認します。

   MetroCluster node show

8. コントローラ交換操作を再開します。

   「システムコントローラの交換が再開」

9. コントローラの交換は一時停止し、次のメッセージが表示されます。

```
Cluster::*> system controller replace show
Node             Status                        Error-Action
---------------- ------------------------
-----------------------------------
Node2(now node4) Paused-for-intervention      Follow the instructions
given in
                                               Step Details
Node2

Step Details:
-------------------------------------------
To complete the Network Reachability task, the ONTAP network
configuration must be
manually adjusted to match the new physical network configuration of the
hardware.
This includes:

1. Re-create the interface group, if needed, before restoring VLANs. For
detailed
commands and instructions, refer to the "Re-creating VLANs, ifgrps, and
broadcast
domains" section of the upgrade controller hardware guide for the ONTAP
version
running on the new controllers.
2. Run the command "cluster controller-replacement network displaced-
vlans show"
to check if any VLAN is displaced.
3. If any VLAN is displaced, run the command "cluster controller-
replacement
network displaced-vlans restore" to restore the VLAN on the desired
port.
2 entries were displayed.
```

この手順では、 VLAN 、 ifgrp 、およびブロードキャストドメインの作成に関するセクションの名前が「 _node4 にあるネットワーク設定のリストア」に変更されています。

10. コントローラの交換を一時停止状態にした状態で次のセクションに進んで、ノードのネットワーク設定をリストアします。

ノード **4** のネットワーク設定をリストアします

node4 がクォーラムにあり、 node3 と通信できることを確認したら、 node2 の VLAN 、インターフェイスグループ、およびブロードキャストドメインが node4 にあることを確認します。また、ノード 4 のすべてのネットワークポートが正しいブロードキャストドメインに設定されていることを確認します。

このタスクについて

VLAN 、インターフェイスグループ、およびブロードキャストドメインの作成と再作成の詳細については、を参照してください "参考資料" をクリックして _ ネットワーク管理 _ にリンクします。

AFF A800またはAFF C800システムでクラスタポートe0aおよびe1aのポート速度を変更すると、速度変換後に不正な形式のパケットを受信することがあります。を参照してください "NetApp Bugs OnlineのバグID1570339" ナレッジベースの記事 "40GbEから100GbEへの変換後のT6ポートのCRCエラー" を参照してください。

手順

1. アップグレードされた node2 （ node4 ）にある物理ポートをすべて一覧表示します。

   「 network port show -node node4 」

   ノードのすべての物理ネットワークポート、 VLAN ポート、およびインターフェイスグループポートが表示されます。この出力から、 ONTAP によって「 Cluster 」ブロードキャストドメインに移動された物理ポートを確認できます。この出力を使用して、インターフェイスグループメンバーポート、 VLAN ベースポート、または LIF をホストするスタンドアロンの物理ポートとして使用するポートを決定できます。

2. クラスタのブロードキャストドメインの一覧を表示します。

   「 network port broadcast-domain show 」

3. node4 にあるすべてのポートの到達可能性をリストします。

   「 network port reachability show 」のように表示されます

   コマンドの出力例を次に示します。

```
clusterA::*> reachability show -node node2_node4
  (network port reachability show)
Node         Port       Expected Reachability       Reachability Status
---------    --------  --------------------------
---------------------
node2_node4
             a0a        Default:Default             no-reachability
             a0a-822    Default:822                 no-reachability
             a0a-823    Default:823                 no-reachability
             e0M        Default:Mgmt                ok
             e0a        Cluster:Cluster             misconfigured-
reachability
             e0b        Cluster:Cluster             no-reachability
             e0c        Cluster:Cluster             no-reachability
             e0d        Cluster:Cluster             no-reachability
             e0e        Cluster:Cluster             ok
             e0e-822    -                           no-reachability
             e0e-823    -                           no-reachability
             e0f        Default:Default             no-reachability
             e0f-822    Default:822                 no-reachability
             e0f-823    Default:823                 no-reachability
             e0g        Default:Default             misconfigured-
reachability
             e0h        Default:Default             ok
             e0h-822    Default:822                 ok
             e0h-823    Default:823                 ok
18 entries were displayed.
```

上記の例では、 node2 _node4 がコントローラの交換後にブートされたとします。到達可能性のない複数のポートがあり、到達可能性スキャンを保留しています。

4. ノード 4 の各ポートの到達可能性を 'OK' 以外の到達可能性ステータスで修復します次のコマンドを最初に任意の物理ポートで実行し、次に任意の VLAN ポートで一度に 1 つずつ実行します。

   'network port reachability repair-Node_node_name — port_port_port_name_`

   次のような出力が表示されます。

```
Cluster ::> reachability repair -node node2_node4 -port e0h
```

```
Warning: Repairing port "node2_node4: e0h" may cause it to move into a
different broadcast domain, which can cause LIFs to be re-homed away
from the port. Are you sure you want to continue? {y|n}:
```

上記の警告メッセージは、到達可能性ステータスのポートで、現在配置されているブロードキャストドメインの到達可能性ステータスとは異なる可能性がある場合に表示されます。

ポートと回答 'y' または 'n' の接続を適宜確認します

すべての物理ポートに想定される到達可能性があることを確認します。

「 network port reachability show 」のように表示されます

到達可能性の修復が実行されると、 ONTAP は正しいブロードキャストドメインにポートを配置しようとします。ただし、ポートの到達可能性を判別できず、既存のどのブロードキャストドメインにも属していない場合、 ONTAP はこれらのポート用に新しいブロードキャストドメインを作成します。

5. インターフェイスグループの設定が新しいコントローラの物理ポートレイアウトと一致しない場合は、次の手順に従って設定を変更します。

   a. 最初に、インターフェイスグループのメンバーポートにする物理ポートを、それぞれのブロードキャストドメインメンバーシップから削除する必要があります。これを行うには、次のコマンドを使用します。

      「network port broadcast-domain remove-ports -broadcast-domain broadcast_domain_name」-ports_node_name -ports_node_name：port_name」

   b. インターフェイスグループにメンバーポートを追加します。

      「network port ifgrp add -port -node node_name」-ifgrp_-port_port_port_name_`

   c. インターフェイスグループは、最初のメンバーポートが追加されてから約 1 分後にブロードキャストドメインに自動的に追加されます。

   d. インターフェイスグループが適切なブロードキャストドメインに追加されたことを確認します。

      「network port reachability show -node node_name --port_ifgrp_`」という形式で表示されます

      インターフェイスグループの到達可能性ステータスが「 OK 」でない場合は、適切なブロードキャストドメインに割り当てます。

   「network port broadcast-domain add-ports -broadcast-domain broadcast_domain_name」-ports_node：port_

6. 適切な物理ポートを Cluster ブロードキャスト・ドメインに割り当てます

   a. 'Cluster' ブロードキャスト・ドメインに到達可能なポートを判別します

      「 network port reachability show-reachable-broadcast-domain Cluster ： Cluster 」

   b. 到達可能性ステータスが「 OK 」でない場合は、「 Cluster 」ブロードキャストドメインに到達可能なすべてのポートを修復します。

      'network port reachability repair-Node_node_name — port_port_port_name_`

7. 次のいずれかのコマンドを使用して、残りの物理ポートを正しいブロードキャストドメインに移動します。

   'network port reachability repair-Node_node_name — port_port_port_name_`

「 network port broadcast-domain remove-port 」のようになります

「 network port broadcast-domain add-port 」と入力します

到達不能または予期しないポートが存在しないことを確認します。次のコマンドを使用してすべての物理ポートの到達可能性ステータスをチェックし、出力を調べてステータスが「 OK 」であることを確認します。

「 network port reachability show-detail` 」と表示されます

8. 次の手順を実行して、取り外された可能性のある VLAN を復元します。

   a. 取り外された VLAN のリスト：

      「cluster controller -replacement network変位- VLANs show」と表示されます

      次のような出力が表示されます。

      ```
      Cluster::*> displaced-vlans show
      (cluster controller-replacement network displaced-vlans show)
                  Original
      Node        Base Port     VLANs
      ---------   ---------
      ------------------------------------------------------
      Node1       a0a           822, 823
                  e0e           822, 823
      ```

   b. 以前のベースポートから取り外された VLAN を復元します。

      クラスタ・コントローラ交換ネットワークが取り外されましたVLANがリストアされました

      次に、インターフェイスグループ a0a から削除された VLAN を同じインターフェイスグループにリストアする例を示します。

      ```
      Cluster::*> displaced-vlans restore -node node2_node4 -port a0a
      -destination-port a0a
      ```

      次に、ポート「 e0e 」上の取り外された VLAN を「 E0h 」にリストアする例を示します。

      ```
      Cluster::*> displaced-vlans restore -node node2_node4 -port e0e
      -destination-port e0h
      ```

      VLAN の復元が成功すると、指定された宛先ポートに、取り外された VLAN が作成されます。デスティネーションポートがインターフェイスグループのメンバーである場合、またはデスティネーションポートがダウンしている場合、 VLAN のリストアは失敗します。

新しくリストアした VLAN が適切なブロードキャストドメインに配置されるまで約 1 分待ちます。

a. 必要に応じて'クラスタコントローラ交換ネットワークではないVLANポート用に新しいVLANポートを作成しますが'VLANは出力を示しますが'他の物理ポート上で構成する必要があります

9. ポートの修復がすべて完了したら、空のブロードキャストドメインを削除します。

   `network port broadcast-domain delete -broadcast-domain broadcast_domain_name`

10. ポートの到達可能性を確認します

    「 network port reachability show 」のように表示されます

    すべてのポートが正しく設定され、正しいブロードキャストドメインに追加されている場合、「 network port reachability show 」コマンドは、接続されているすべてのポートの到達可能性ステータスを「 ok 」、物理的に接続されていないポートのステータスを「 no-reachability 」と報告する必要があります。この 2 つ以外のステータスが報告されるポートがある場合は、到達可能性修復を実行し、の手順に従ってブロードキャストドメインにポートを追加または削除します 手順 4。

11. すべてのポートがブロードキャストドメインに配置されたことを確認します。

    「 network port show 」のように表示されます

12. ブロードキャストドメインのすべてのポートで、正しい Maximum Transmission Unit （ MTU ；最大伝送ユニット）が設定されていることを確認します。

    「 network port broadcast-domain show 」

13. SVM のホームポートと LIF のホームポート（ある場合）をリストアする必要がある場合は、それらを指定して LIF のホームポートをリストアします。

    a. 移動された LIF を表示します。

       「 dispaced-interface show 」

    b. LIF のホームポートをリストアします。

       「変位インターフェイスのリストア-home-node-node-node_node_name - *vserver_vserver_name _-lif - name_lif_name_name*」のように指定します

14. すべての LIF にホームポートがあり、意図的に稼働状態になっていることを確認します。

    network interface show -fields home-port、status-admin

ノード 4 でキー管理ツールの設定をリストアします

NetApp Volume Encryption（NVE）およびNetApp Aggregate Encryption（NAE）を使用してアップグレードするシステムのボリュームを暗号化する場合は、暗号化設定を新しいノードに同期する必要があります。キー管理ツールを同期しない場合は、ARLを使用してノード2のアグリゲートをノード3からノード4に再配置すると、ノード4に暗号化されたボリュームとアグリゲートをオンラインにするために必要な暗号化キーがないと処理が失敗することがあります。

このタスクについて

次の手順を実行して、暗号化設定を新しいノードに同期します。

手順

1. ノード4から次のコマンドを実行します。

   「セキュリティキーマネージャオンボード同期」

2. データアグリゲートを再配置する前に、ノード4でSVMのKEKキーが「true」にリストアされたことを確認します。

```
::> security key-manager key query -node node4 -fields restored -key
-type SVM-KEK
```

例

```
::> security key-manager key query -node node4 -fields restored -key
-type SVM-KEK

node     vserver   key-server   key-id
restored
-------- --------- -----------  ----------------------------------------
--------
node4    svm1      ""           000000000000000002000000000000a008a81976
true
                                2190178f9350e071fbb90f00000000000000000
```

node2 によって所有されているルート以外のアグリゲートと NAS データ LIF を、node3 から node4 に移動します

ノード 4 のネットワーク構成を確認した後、ノード 2 が所有する NAS データ LIF をノード 3 からノード 4 に再配置し、SAN LIF がノード 4 に存在することを確認する必要があります。

このタスクについて

リモート LIF は、アップグレード手順中に SAN LUN へのトラフィックを処理します。アップグレード中のクラスタまたはサービスの健全性のために、SAN LIF を移動する必要はありません。SAN LIF は、新しいポートにマッピングする必要がある場合を除き、移動されません。

node4 をオンラインにした後、LIF が正常であり、正しいポートに配置されていることを確認します。

> T6ベースのイーサネットネットワークインターフェイスカードまたはマザーボードポートのポート速度を変更すると、速度変換後に不正な形式のパケットが受信されることがあります。を参照してください "NetApp Bugs OnlineのバグID1570339" ナレッジベースの記事 "40GbEから100GbEへの変換後のT6ポートのCRCエラー" を参照してください。

手順

1. 再配置処理を再開します。

```
system controller replace resume
```

システムは次のタスクを実行します。

- クラスタクォーラムチェック
- システム ID の確認
- イメージのバージョンチェック
- ターゲットプラットフォームのチェック
- ネットワーク到達可能性チェック

ネットワーク到達可能性チェックのこの段階で、システムは操作を一時停止します。

2. 再配置処理を再開します。

```
system controller replace resume
```

システムは次のチェックを実行します。

- クラスタの健全性チェック
- クラスタ LIF のステータスを確認します

これらのチェックの実行後、システムによって、 node2 によって所有されているルート以外のアグリゲートと NAS データ LIF が新しいコントローラ node4 に再配置されます。リソースの再配置が完了すると、コントローラの交換処理が一時停止します。

3. アグリゲートの再配置処理と NAS データ LIF の移動処理のステータスを確認します。

```
system controller replace show-details
```

コントローラ交換用手順が一時停止している場合は、エラーがある場合はチェックして修正し、次に「問題 re sume 」をクリックして操作を続行します。

4. 必要に応じて、移動された LIF を復元して元に戻すか、自動的に再配置できなかったノード 2 LIF をノード 4 に手動で移行して変更します。

移動した**LIF**を復元して元に戻す

a. 移動した LIF をリストします。

```
cluster controller-replacement network displaced-interface show
```

b. LIF が取り外された場合は、ホームノードをノード 4 にリストアします。

```
cluster controller-replacement network displaced-interface
restore-home-node -node <node4_nodename> -vserver <vserver name>
-lif-name <lif_name>
```

LIFを手動で移行および変更する

a. 自動的に再配置できなかった LIF をノード 4 に移行します。

```
network interface migrate -vserver <vserver name> -lif <lif_name>
-destination-node <node4_nodename> -destination-port
<port_on_node4>
```

b. 移行された LIF のホーム ノードとホーム ポートを変更します。

```
network interface modify -vserver <vserver_name> -lif
<data_lif_name> -home-node <node4_nodename> -home-port
<home_port>
```

5. この処理を再開すると、必要なポストチェックの実行をシステムに求めるプロンプトが表示されます。

```
system controller replace resume
```

次のポストチェックが実行されます。

- クラスタクォーラムチェック
- クラスタの健全性チェック
- アグリゲートの再構築チェック
- アグリゲートのステータスを確認します
- ディスクのステータスを確認します
- クラスタ LIF のステータスを確認します
- ボリュームチェック

ステージ 6 ：アップグレードを完了します

KMIP サーバを使用して認証を管理します

ONTAP 9.8 以降では、 Key Management Interoperability Protocol （ KMIP ）サーバを使用して認証キーを管理できます。

手順

1. 新しいコントローラを追加します。

   「 security key-manager external enable 」と入力します

2. キー管理ツールを追加します。

   「security key-manager external add-servers -key-servers_key_manager_server_ip_address _」のように指定します

3. キー管理サーバが設定され、クラスタ内のすべてのノードで使用できることを確認します。

   「 security key-manager external show-status 」

4. リンクされたすべてのキー管理サーバの認証キーを新しいノードにリストアします。

   'security key-manager external restore -node *new_controller_name*`

新しいコントローラが正しくセットアップされていることを確認します

正しいセットアップを確認するには、 HA ペアを有効にする必要があります。さらに、 node3 と node4 が相互のストレージにアクセスできること、およびクラスタ内の他のノードに属するデータ LIF を所有していないことを確認する必要があります。また、 node3 が node1 のアグリゲートを所有しており、 node4 が node2 のアグリゲートを所有していること、および両方のノードのボリュームがオンラインであることを確認する必要があります。

手順

1. node2 のチェック後、 node2 クラスタのストレージフェイルオーバーとクラスタ HA ペアが有効になります。処理が完了すると、両方のノードに「 Completed 」と表示され、クリーンアップ処理が実行されます。
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

   次の例は、ストレージフェイルオーバーが有効になっている場合のコマンドの出力例を示しています。

```
cluster::> storage failover show
                    Takeover
Node      Partner   Possible    State Description
--------- -----     -------     ------------------
node3     node4     true        Connected to node4
node4     node3     true        Connected to node3
```

3. 次のコマンドを使用して、 node3 と node4 が同じクラスタに属していることを確認します。出力を確認します。

   「 cluster show 」を参照してください

4. 次のコマンドを使用して、 node3 と node4 が相互のストレージにアクセスできることを確認します。出力を確認します。

   「storage failover show -fields local-missing-disks、partner-missing-disks」

5. 次のコマンドを使用して、 node3 と node4 がクラスタ内の他のノードによってホーム所有されているデータ LIF を所有していないことを確認します。

   「 network interface show 」を参照してください

   node3 と node4 がクラスタ内の他のノードによってホーム所有されているデータ LIF を所有していない場合は、データ LIF をホーム所有者にリバートします。

   「 network interface revert 」の略

6. ノード 3 がノード 1 のアグリゲートを所有していること、およびノード 4 がノード 2 のアグリゲートを所有していることを確認します。

   ```
   storage aggregate show -owner-name <node3>

   storage aggregate show -owner-name <node4>
   ```

7. オフラインになっているボリュームがないかを確認します。

   ```
   volume show -node <node3> -state offline

   volume show -node <node4> -state offline
   ```

8. オフラインになっているボリュームがある場合は、セクションで取得したオフラインボリュームのリストと比較します "ノードをアップグレードする準備をします"必要に応じて、次のコマンドを使用して、ボリュームごとに 1 回、オフラインボリュームをオンラインにします。

   ```
   volume online -vserver <vserver_name> -volume <volume_name>
   ```

9. ノードごとに次のコマンドを使用して、新しいノードの新しいライセンスをインストールします。

   ```
   system license add -license-code <license_code,license_code,license_code…>
   ```

license-code パラメータには、アルファベットの文字キーをアルファベットの大文字 28 個まで入力できます。ライセンスは一度に 1 つずつ追加することも、複数追加することもできます。各ライセンスキーをカンマで区切って指定することもできます。

10. 次のいずれかのコマンドを使用して、元のノードから古いライセンスをすべて削除します。

    「システムライセンスのクリーンアップ - 未使用 - 期限切れ」

    ```
    system license delete -serial-number <node_serial_number> -package
    <licensable_package>
    ```

    - 期限切れのライセンスをすべて削除します。

      「システムライセンスのクリーンアップ - 期限切れ」

    - 未使用のライセンスをすべて削除します。

      'System license clean-up-unused （システムライセンスのクリーンアップ - 未使用） '

    - クラスタから特定のライセンスを削除するには、ノードで次のコマンドを使用します。

      ```
      system license delete -serial-number <node1_serial_number> -package *

      system license delete -serial-number <node2_serial_number> -package *
      ```

    次の出力が表示されます。

    ```
    Warning: The following licenses will be removed:
    <list of each installed package>
    Do you want to continue? {y|n}: y
    ```

    すべてのパッケージを削除するには 'y' を入力します

11. 次のコマンドを使用して出力を調べ、ライセンスが正しくインストールされていることを確認します。

    「 system license show 」を参照してください

    出力を、セクションでキャプチャした出力と比較できます "ノードをアップグレードする準備をします"。

12. 自己暗号化ドライブが構成で使用されており、 `kmip.init.maxwait`変数に `off（例えば、"ノード4のインストールと起動、ステップ22" ）の場合は、変数を設定解除する必要があります。

    ```
    set diag; systemshell -node-node_name --コマンドsudo kenv -u -p
    kmip.init.maxwait
    ```

13. 両方のノードで次のコマンドを使用して、 SP を設定します。

    system service-processor network modify -node _node_name _`

    "参考資料"を参照して、SPに関する情報については_System Administration Reference_に、system `service-processor network modify`コマンドの詳細については_ONTAP 9 Command reference_にリンクし

てください。

14. 新しいノードにスイッチレスクラスタをセットアップする場合は、を参照してください "参考資料" ネットアップサポートサイトへのリンクを設定するには、 _2 ノードスイッチレスクラスタへの移行の手順に従ってください。

完了後

ノード 3 とノード 4 でストレージ暗号化が有効になっている場合は、セクションを完了します "新しいコントローラモジュールで Storage Encryption をセットアップします"。それ以外の場合は、の項を実行します "古いシステムの運用を停止"。

新しいコントローラモジュールで **Storage Encryption** をセットアップします

交換したコントローラまたは新しいコントローラの HA パートナーで Storage Encryption が使用されている場合は、 SSL 証明書のインストールやキー管理サーバのセットアップなど、新しいコントローラモジュールを Storage Encryption 用に設定する必要があります。

このタスクについて

この手順には、新しいコントローラモジュールで実行する手順が含まれています。コマンドは正しいノードで入力する必要があります。

手順

1. キー管理サーバがまだ使用可能であり、ステータスと認証キー情報が正しいことを確認します。

   「 security key-manager external show-status 」

   「 securitykey manager onboard show-backup 」を参照してください

2. 前の手順で確認したキー管理サーバを、新しいコントローラのキー管理サーバのリストに追加します。
   a. キー管理サーバを追加します。

      「security key-manager external add-servers -key-servers_key_manager_server_ip_address _」のように指定します

   b. リストされている各キー管理サーバについて、同じ手順を繰り返します。最大 4 台のキー管理サーバをリンクできます。
   c. キー管理サーバが正常に追加されたことを確認します。

      「 security key-manager external show 」と入力します

3. 新しいコントローラモジュールで、キー管理セットアップウィザードを実行して、キー管理サーバをセットアップしてインストールします。

   既存のコントローラモジュールと同じキー管理サーバをインストールする必要があります。

   a. 新しいノードでキー管理サーバセットアップウィザードを起動します。

      「 security key-manager external enable 」と入力します

b. ウィザードの手順に従って、キー管理サーバを設定します。

4. リンクされたすべてのキー管理サーバから新しいノードに認証キーをリストアします。

'security key-manager external restore -node *new_controller_name*`

新しいコントローラモジュールで**NetApp Volume**または**Aggregate Encryption**をセットアップします

新しいコントローラの交換したコントローラまたはハイアベイラビリティ（HA）パートナーがNetApp Volume Encryption（NVE）またはNetApp Aggregate Encryption（NAE）を使用している場合は、新しいコントローラモジュールをNVEまたはNAE用に設定する必要があります。

このタスクについて

この手順には、新しいコントローラモジュールで実行する手順が含まれています。コマンドは正しいノードで入力する必要があります。

オンボードキーマネージャ

オンボードキーマネージャを使用してNVEまたはNAEを設定します。

手順

1. リンクされたすべてのキー管理サーバから新しいノードに認証キーをリストアします。

   「セキュリティキーマネージャオンボード同期」

外部キー管理

外部キー管理を使用してNVEまたはNAEを設定します。

手順

1. キー管理サーバがまだ使用可能であり、ステータスと認証キー情報が正しいことを確認します。

   「 securitykey manager key query -node node 」を参照してください

2. 前の手順で確認したキー管理サーバを新しいコントローラのキー管理サーバリストに追加します。

   a. キー管理サーバを追加します。

      「security key-manager external add-servers -key-servers_key_manager_server_ip_address _」のように指定します

   b. リストされている各キー管理サーバについて、同じ手順を繰り返します。最大 4 台のキー管理サーバをリンクできます。

   c. キー管理サーバが正常に追加されたことを確認します。

      「 security key-manager external show 」と入力します

3. 新しいコントローラモジュールで、キー管理セットアップウィザードを実行して、キー管理サーバをセットアップしてインストールします。

   既存のコントローラモジュールと同じキー管理サーバをインストールする必要があります。

   a. 新しいノードでキー管理サーバセットアップウィザードを起動します。

      「 security key-manager external enable 」と入力します

   b. ウィザードの手順に従って、キー管理サーバを設定します。

4. リンクされたすべてのキー管理サーバから新しいノードに認証キーをリストアします。

   「セキュリティキーマネージャの外部リストア」

   このコマンドには、OKMのパスフレーズが必要です

   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 "ONTAP ブートメニューから外部キー管理サーバの設定をリストアする方法"。

完了後

認証キーを使用できなかったか、 EKM サーバに到達できなかったためにボリュームがオフラインになっていないか確認してください。volume online コマンドを使用して ' これらのボリュームをオンラインに戻します

古いシステムの運用を停止

アップグレード後は、ネットアップサポートサイトから古いシステムの運用を停止できます。システムの運用を停止すると、そのシステムは動作していないことがネットアップに通知され、サポートデータベースから削除されます。

手順

1. を参照してください "参考資料" からネットアップサポートサイトにリンクしてログインします。
2. メニューから [製品]>[マイ製品] を選択します。
3. [インストール済みシステムの表示 **]** ページで、システムに関する情報の表示に使用する ***Selection Criteria** を選択します。

   次のいずれかを選択してシステムを検索できます。

   - シリアル番号（ユニットの背面に記載）
   - 所在地のシリアル番号
4. 「 * Go ！ * 」を選択します

   シリアル番号を含むクラスタ情報が表に表示されます。
5. テーブルでクラスタを見つけ、 Product Tool Set （製品ツールセット）ドロップダウンメニューから * Decommission this system * （このシステムのデコミッション）を選択します。

SnapMirror 処理を再開します

アップグレード前に休止していた SnapMirror 転送を再開し、 SnapMirror 関係を再開できます。更新はアップグレードの完了後にスケジュールどおりに実行されます。

手順

1. デスティネーションで SnapMirror のステータスを確認します。

   「 Snapmirror show 」のように表示されます
2. SnapMirror 関係を再開します。

   snapmirror resume -destination–vserver_vserver_name _`

トラブルシューティングを行う

アグリゲートの再配置に失敗しまし

アグリゲートの再配置（ ARL ）がアップグレード中に別のポイントで失敗することがあ

ります。

アグリゲートの再配置に失敗していないかどうか

手順の処理中に、ステージ 2 、ステージ 3 、またはステージ 5 で ARL が失敗することがあります。

手順

1. 次のコマンドを入力し、出力を確認します。

   「 storage aggregate relocation show 」を参照してください

   「 storage aggregate relocation show 」コマンドを実行すると、正常に再配置されたアグリゲートと再配置されなかったアグリゲート、および障害の原因が表示されます。

2. コンソールで EMS メッセージを確認します。
3. 次のいずれかを実行します。
   - 「 storage aggregate relocation show 」コマンドの出力と EMS メッセージの出力に応じて、適切な方法を実行します。
   - 「 storage aggregate relocation start 」コマンドの「 override-vetoes 」オプションまたは「 override-vetoes destination-checks 」オプションを使用して、アグリゲートまたはアグリゲートの強制的な再配置を実行します。

     `storage aggregate relocation start`、 `override-vetoes`、 `override-destination-checks`
     オプションの詳細については、link:other_references.html["参考資料"]を参照して_ONTAP 9 Command reference_にリンクしてください。

アグリゲートは、アップグレードの完了後、ノード **1** にもともと存在していたものとノード **4** によって所有されます

アップグレード手順の最後に、 node3 は、元々ホームノードとしてノード 1 を使用していたアグリゲートの新しいホームノードである必要があります。このパスはアップグレード後に再配置できます。

このタスクについて

次の状況で、アグリゲートを正しく再配置できず、ノード 1 がノード 3 ではなくホームノードになっている可能性があります。

- ステージ 3 で、アグリゲートが node2 から node3 に再配置されている場合。再配置する一部のアグリゲートのホームノードが node1 に含まれている。たとえば、このようなアグリゲートのことを aggr_node_A_1 と呼びます。ステージ 3 で aggr_node_A_1 の再配置が失敗し、強制的に再配置を実行できない場合、アグリゲートは node2 で残ります。
- ステージ 4 のあとで、 node2 を node4 に置き換える場合。node2 を交換すると、 aggr_node_A_1 が、node3 ではなく node4 にあるホームノードとしてオンラインになります。

ストレージフェイルオーバーを有効にしたあとに、ステージ 6 に続けて誤った所有権の問題を修正するには、次の手順を実行します。

手順

1. 次のコマンドを入力して、アグリゲートのリストを表示します。

   storage aggregate show -nodes_node4 --is-home true

   正しく再配置されていないアグリゲートを特定するには、セクションで取得した node1 のホーム所有者を含むアグリゲートのリストを参照してください "ノードをアップグレードする準備をします" コマンドの出力と比較してください。

2. 手順 1 の出力と、セクションで確認した node1 用の出力を比較します "ノードをアップグレードする準備をします" 再配置されていないアグリゲートがあることを確認します。

3. [[auto_aggr_relocate_fail_Step3] ノード 4 の背後にあるアグリゲートの再配置：

   「storage aggregate relocation start -NODE_node4」-aggr_aggr_node_A_1 -destination_node3 _」を入力します

   この再配置中は '-nd-controller-upgrade パラメータを使用しないでください

4. node3 がアグリゲートのホームの所有者になったことを確認します。

   storage aggregate show -aggregate aggr1、aggr2、aggr3_-fields home-name

   「*aggr1*、*aggr2*、*aggr3_*」は、node1が元のホーム所有者であるアグリゲートのリストです。

   ノード 3 をホーム所有者としないアグリゲートは、の同じ再配置コマンドを使用してノード 3 に再配置できます 手順 3。

リブート、パニック、電源再投入

アップグレードの各段階で、システムがクラッシュする（リブート、パニック状態、または電源の再投入）場合があります。

これらの問題の解決策は、状況によって異なります。

事前チェックフェーズでのリブート、パニック、電源再投入

HA ペアを有効にして事前チェックフェーズの前にノード 1 またはノード 2 がクラッシュした場合

事前チェックフェーズの前にノード 1 またはノード 2 がクラッシュした場合は、再配置されたアグリゲートがなく、 HA ペア構成が有効なままになります。

このタスクについて

テイクオーバーとギブバックは正常に実行されます。

手順

1. コンソールで、システムで発行された EMS メッセージを確認し、推奨される対処方法を実行します。
2. ノードペアのアップグレード用手順に進みます。

最初のリソースリリースフェーズでリブート、パニック、電源再投入が発生した場合

HA ペアを有効にすると、リソースの最初のリリースフェーズでノード 1 がクラッシュします

一部またはすべてのアグリゲートがノード 1 からノード 2 に再配置されており、 HA ペアが有効なままです。node2 は、ノード 1 のルートボリュームと再配置されていないルート以外のアグリゲートをテイクオーバーします。

このタスクについて

再配置されたアグリゲートの所有権は、ホーム所有者が変更されていないためにテイクオーバーされたルート以外のアグリゲートの所有権と同じになります。

node1 の状態が「 waiting for giveback 」になると、 node2 はノード 1 のルート以外のすべてのアグリゲートをギブバックします。

手順

1. ノード 1 がブートすると、ノード 1 のルート以外のすべてのアグリゲートがノード 1 に戻されます。アグリゲートの手動での再配置を、node1からnode2に実行する必要があります。storage aggregate relocation start -node node1 -destination node2 -aggregate-list *-ndocontroller -upgrade true
2. ノードペアのアップグレード用手順に進みます。

HA ペアを無効にすると、リソースの最初のリリースフェーズでノード 1 がクラッシュします

node2 はテイクオーバーしませんが、ルート以外のすべてのアグリゲートから引き続きデータを提供しています。

手順

1. ノード 1 を起動します。
2. ノードペアのアップグレード用手順に進みます。

リソースの最初のリリースフェーズで HA ペアを有効にした状態で node2 に障害が発生する

ノード 1 の一部またはすべてのアグリゲートが node2 に再配置されています。HA ペアが有効になります。

このタスクについて

ノード 1 で、ノード 2 のすべてのアグリゲートと、ノード 2 に再配置された独自のアグリゲートがテイクオーバーされます。ノード 2 がブートすると、アグリゲートの再配置が自動的に完了します。

手順

1. node2 を起動します。
2. ノードペアのアップグレード用手順に進みます。

リソースの最初のリリースフェーズと HA ペアの無効化後に、ノード 2 がクラッシュします

ノード 1 ではテイクオーバーが実行されません。

手順

1. node2 を起動します。

   node2 のブート中に、すべてのアグリゲートでクライアントが停止します。

2. 残りのノードペアのアップグレード用手順に進みます。

最初の検証フェーズでリブート、パニック、または電源の再投入が発生した場合

HA ペアを無効にして最初の検証フェーズで node2 がクラッシュします

HA ペアがすでに無効になっているため、ノード 2 のクラッシュ後にノード 3 はテイクオーバーしません。

手順

1. node2 を起動します。

   node2 のブート中に、すべてのアグリゲートでクライアントが停止します。

2. ノードペアのアップグレード用手順に進みます。

HA ペアを無効にして初回の検証フェーズでノード 3 がクラッシュした場合

node2 はテイクオーバーしませんが、ルート以外のすべてのアグリゲートから引き続きデータを提供しています。

手順

1. ノード 3 を起動します。
2. ノードペアのアップグレード用手順に進みます。

最初のリソース再取得フェーズでのリブート、パニック、電源再投入

アグリゲートの再配置中にリソースを再取得する最初のフェーズでノード 2 がクラッシュする

node2 の一部またはすべてのアグリゲートがノード 1 からノード 3 に再配置されています。node3 は、再配置されたアグリゲートからデータを提供します。HA ペアが無効になっているため、テイクオーバーはありません。

このタスクについて

再配置されなかったアグリゲートのクライアントが停止しています。ノード 2 のブート時に、ノード 1 のアグリゲートがノード 3 に再配置されます。

手順

1. node2 を起動します。
2. ノードペアのアップグレード用手順に進みます。

アグリゲートの再配置中に、最初のリソースのリ回復フェーズでノード 3 がクラッシュする

node2 によるアグリゲートのノード 3 への再配置中にノード 3 がクラッシュした場合、ノード 3 のブート後も処理が続行されます。

このタスクについて

node2 では残りのアグリゲートの処理が続行されますが、 node3 の起動中にすでに node3 に再配置されたアグリゲートでクライアントが停止する可能性があります。

手順

1. ノード 3 を起動します。
2. コントローラのアップグレードに進みます。

チェック後のフェーズでリブート、パニック、電源再投入が発生した場合

チェック後のフェーズで **node2** または **node3** がクラッシュする

HA ペアが無効になっているため、テイクオーバーは行われません。リブートしたノードに属するアグリゲートでクライアントが停止しています。

手順

1. ノードを起動します。
2. ノードペアのアップグレード用手順に進みます。

リソースの **2** つ目のリリースフェーズでリブート、パニック、電源の再投入が発生した場合

リソースの **2** つ目のリリースフェーズでノード **3** がクラッシュする

node2 によるアグリゲートの再配置中にノード 3 がクラッシュした場合、ノード 3 のブート後もタスクは続行されます。

このタスクについて

node2 で残りのアグリゲートの処理は続行されますが、 node3 と node3 の独自のアグリゲートにすでに再配置されたアグリゲートでは、 node3 のブート中にクライアントが停止することがあります。

手順

1. ノード 3 を起動します。
2. コントローラのアップグレード手順に進みます。

2 番目のリソースリリースフェーズで **node2** がクラッシュします

アグリゲートの再配置時にノード 2 がクラッシュした場合、ノード 2 はテイクオーバーされません。

このタスクについて

ノード 3 は再配置されたアグリゲートを引き続き提供しますが、ノード 2 が所有するアグリゲートではクライアントの停止が発生します。

手順

1. node2 を起動します。
2. コントローラのアップグレード手順に進みます。

2 回目の検証フェーズで、リブート、パニック、または電源の再投入が発生した場合

2 回目の検証フェーズでノード **3** がクラッシュした場合

このフェーズで node3 がクラッシュした場合は、 HA ペアがすでに無効になっているため、テイクオーバーは実行されません。

このタスクについて

node3 がリブートするまでは、すべてのアグリゲートのクライアントが停止します。

手順

1. ノード 3 を起動します。
2. ノードペアのアップグレード用手順に進みます。

2 番目の検証フェーズ中にノード 4 がクラッシュした場合

このフェーズでノード 4 がクラッシュした場合は、テイクオーバーは実行されません。node3 は、アグリゲートからデータを提供します。

このタスクについて

ノード 4 のリブートまでルート以外のアグリゲートがすでに再配置されています。

手順

1. ノード 4 を起動します。
2. ノードペアのアップグレード用手順に進みます。

手順の複数の段階で発生する可能性のある問題

手順のさまざまな段階で問題が発生する可能性があります。

予期しない「 **storage failover show** 」コマンドの出力が表示されます

手順の実行中に、すべてのデータアグリゲートをホストするノードがパニック状態になったり、誤ってリブートされたりした場合は、リブート、パニック状態、電源再投入の前後に「 storage failover show 」コマンドの出力が想定外に表示されることがあります。

このタスクについて

ステージ 2 、ステージ 3 、ステージ 4 、またはステージ 5 の「 storage failover show 」コマンドの出力結果に予期しないものが表示されることがあります。

次の例は、すべてのデータアグリゲートをホストするノードでリブートやパニックが発生していない場合の「 storage failover show 」コマンドの出力を示しています。

```
cluster::> storage failover show

                    Takeover
Node     Partner    Possible  State Description
-------  --------   --------- -----------------
node1    node2      false     Unknown
node2    node1      false     Node owns partner aggregates as part of the
non-disruptive head upgrade procedure. Takeover is not possible: Storage
failover is disabled.
```

次の例は、リブートまたはパニック後の「 storage failover show 」コマンドの出力例を示しています。

```
cluster::> storage failover show

                    Takeover
Node      Partner   Possible  State Description
--------  --------  --------- -----------------
node1     node2     -         Unknown
node2     node1     false     Waiting for node1, Partial giveback, Takeover
is not possible: Storage failover is disabled
```

ノードが部分的なギブバック状態にあること、およびストレージフェイルオーバーが無効になっていることを示す出力が表示されますが、このメッセージは無視してもかまいません。

手順

対処は不要です。ノードペアのアップグレード手順に進みます。

LIF の移行が失敗しました

LIF の移行後、ステージ 2 、ステージ 3 、またはステージ 5 で移行後にオンラインにならない場合があります。

手順

1. ポートの MTU サイズがソースノードと同じであることを確認します。

   たとえば、ソースノードのクラスタポートの MTU サイズが 9000 の場合、デスティネーションノードは 9000 にする必要があります。

2. ポートの物理的な状態が「所有」である場合は、ネットワークケーブルの物理的な接続を確認します。

参考資料

このコンテンツの手順を実行するときは、参照コンテンツを参照するか、参照 Web サイトにアクセスする必要があります。

参照コンテンツ

このアップグレードに固有のコンテンツを次の表に示します。

内容	説明
"CLI での管理の概要"	ONTAP システムの管理方法、 CLI インターフェイスの使用方法、クラスタへのアクセス方法、ノードの管理方法などについて説明します
"クラスタセットアップで System Manager と ONTAP CLI のどちらを使用するかを決定します"	ONTAP をセットアップおよび設定する方法について説明します。

内容	説明
"CLI によるディスクおよびアグリゲートの管理"	CLI を使用して ONTAP 物理ストレージを管理する方法について説明します。アグリゲートを作成、拡張、管理する方法、 Flash Pool アグリゲートを使用する方法、ディスクを管理する方法、および RAID ポリシーを管理する方法を示します。
"HAペアの管理"	ストレージフェイルオーバー、テイクオーバー / ギブバックなどのハイアベイラビリティクラスタ構成をインストールおよび管理する方法について説明します。
"CLI を使用した論理ストレージ管理"	ボリューム、 FlexClone ボリューム、ファイル、 LUN を使用して論理ストレージリソースを効率的に管理する方法について説明します。 FlexCache 、重複排除、圧縮、 qtree 、およびクォータ
"MetroCluster の管理とディザスタリカバリ"	計画的なメンテナンス時または災害発生時の両方のケースにおける、 MetroCluster のスイッチオーバーとスイッチバック処理の実行方法について説明します。
"MetroCluster のアップグレードと拡張"	MetroCluster 構成でコントローラとストレージモデルをアップグレードし、 MetroCluster FC 構成から MetroCluster IP 構成に移行し、ノードを追加して MetroCluster 構成を拡張する手順について説明します。
"Network Management の略"	クラスタで物理 / 仮想ネットワークポート（ VLAN およびインターフェイスグループ）、 LIF 、ルーティング、およびホスト解決サービスを設定および管理する方法、ロードバランシングでネットワークトラフィックを最適化する方法、および SNMP を使用してクラスタを監視する方法について説明します。
"ONTAP 9 コマンドリファレンス"	サポートされているONTAPコマンドの構文と使用法について説明します。
"CLI での SAN 管理"	iSCSI および FC プロトコルを使用して LUN 、 igroup 、ターゲットを設定および管理する方法、 NVMe/FC プロトコルを使用してネームスペースとサブシステムを設定および管理する方法について説明します。
"SAN 構成リファレンス"	FC と iSCSI のトポロジと配線方式について説明します
"ボリュームまたはストレージを移動してアップグレードします"	ストレージまたはボリュームを移動してクラスタ内のコントローラハードウェアを簡単にアップグレードする方法について説明します。サポートされるモデルをディスクシェルフに変換する方法についても説明します。
"ONTAP をアップグレードします"	ONTAP のダウンロードとアップグレードの手順については、を参照してください
"ONTAP 9.15.1以降で導入された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。"	ONTAP 9.15.1以降で「system controller replace」コマンドを使用してコントローラを無停止でアップグレードするために必要なアグリゲートの再配置手順について説明します。
"「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"	古いシステムシャーシとディスクをそのまま使用して、システムを無停止でアップグレードするために必要なアグリゲートの再配置手順について説明します。

内容	説明
"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"	ONTAP 9.8 を実行するコントローラを、 system controller replace コマンドを使用して無停止でアップグレードする場合に必要なアグリゲートの再配置手順について説明します。
"ONTAP 9.8 以降を実行しているコントローラハードウェアは、アグリゲートの再配置を使用して手動でアップグレードします"	ONTAP 9.8 以降を実行するコントローラの手動無停止アップグレードを実行するために必要なアグリゲートの再配置手順について説明します。
"「 system controller replace 」コマンドを使用して、 ONTAP 9.5 を実行するコントローラハードウェアを ONTAP 9.7 にアップグレードします"	ONTAP 9.5 を実行するコントローラを ONTAP 9.7 に無停止でアップグレードする場合に、「 system controller replace 」コマンドを使用してアグリゲートの再配置手順を説明します。
"ONTAP 9.7 以前を実行しているコントローラハードウェアは、アグリゲートの再配置を使用して手動でアップグレードします"	ONTAP 9.7 以前を実行しているコントローラの手動による無停止アップグレードを実行するために必要なアグリゲートの再配置手順について説明します。

参照サイト

。 "ネットアップサポートサイト" また、システムで使用する可能性のあるネットワークインターフェイスカード（ NIC ）やその他のハードウェアに関するドキュメントも含まれています。また、にも含まれています "Hardware Universe"をクリックします。このコマンドは、新しいシステムでサポートされるハードウェアに関する情報を提供します。

にアクセスします "ONTAP 9 のドキュメント"。

にアクセスします "Active IQ Config Advisor" ツール。

著作権に関する情報

商標に関する情報