



ONTAP

9.15.1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。

Upgrade controllers

NetApp
July 05, 2024

目次

ONTAP 9.15.1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。	1
概要	1
コントローラのアップグレードプロセスを自動化する	2
アグリゲートの再配置手順を使用するかどうかを決定します	2
必要な工具とドキュメント	3
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	3
ARL アップグレードの概要	5
ステージ 1：アップグレードを準備	7
ステージ 2：移行してノード 1 を撤去	12
ステージ 3：node3 をインストールしてブートします	16
ステージ 4：ノード 2 の移動と撤去	36
ステージ 5：ノード 4 をインストールしてブートします	38
ステージ 6：アップグレードを完了します	58
トラブルシューティングを行う	65
参考資料	72

ONTAP 9.15.1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。

概要

この手順では、次のシステム構成で Aggregate Relocation（ARL；アグリゲートの再配置）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方法について説明します。

メソッド	ONTAP バージョン	サポートされるシステム
「system controller replace」コマンドを使用します	9.15.1以降	"サポートされているシステムマトリックスへのリンク"



この手順を使用して、MetroClusterのFCまたはIP構成をアップグレードすることはできません。MetroCluster構成をアップグレードするには、MetroClusterのアップグレードおよび拡張に関するドキュメント_へのリンクを参照してください ["参考資料"](#)。

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、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"](#) および ["ARLアップグレードの概要"](#) アップグレード開始前のセクション。
- 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。この手順には、コマンドを使用して使用済みコントローラを準備するために必要な手順 `wipeconfig` 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た場合は、テクニカルサポートにお問い合わせください。
- 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。
- ONTAP 9.15.1で導入されたAFF A70、AFF A90、またはAFF A1Kシステムにアップグレードする

と、ONTAPでは、Storage Efficiencyを使用していないボリュームも含め、既存のシンプロビジョニングされたすべてのボリュームのストレージ効率化が変換され、ハードウェアオフロード機能を使用する新しいStorage Efficiency機能が適用されます。これは自動バックグラウンドプロセスであり、システムのパフォーマンスへの明らかな影響はありません。"詳細はこちら。"です。

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。ここでは一部自動化された手順について説明します。この手順では、ネットワークポートの到達可能性チェックが自動で行われるため、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。

アグリゲートの再配置手順を使用するかどうかを決定します

この手順では、既存のデータとディスクを残したまま、HAペアのストレージコントローラを新しいコントローラにアップグレードする方法について説明します。これは複雑な手順であり、経験豊富な管理者のみが使用する必要があります。

この手順は、次の状況で使用できます。

- ONTAP 9.15.1 以降を実行している必要があります。
- 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、ボリューム移動手順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が十分にあります。



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。

次の状況では、この手順を使用できません。

- AFF A800をAFF A70またはAFF A90にアップグレードする。AFF A800のこのアップグレードを実行するには、「to_use "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する」を参照してください "[参考資料](#)"。
- バックエンドストレージに外付けアレイを使用して、VシリーズシステムまたはFlexArray仮想化ストレージシステムをアップグレードする場合。VシリーズまたはFlexArrayシステムのアップグレードオプションについては、テクニカルサポートにお問い合わせください。
- MetroClusterのFCまたはIP構成をアップグレードする。MetroCluster構成をアップグレードするには、MetroClusterのアップグレードおよび拡張に関するドキュメント_へのリンクを参照してください "[参考資料](#)"。

次の表は、コントローラのアップグレードでサポートされるモデルマトリックスを示しています。

既存のコントローラ	交換用コントローラ
AFF A300	AFF A70、AFF A90、およびAFF A1K
AFF A400	AFF A70、AFF A90、およびAFF A1K

既存のコントローラ	交換用コントローラ
AFF A700の略	AFF A70、AFF A90、およびAFF A1K
AFF A900 の略	AFF A90およびAFF A1K



AFF A70およびAFF A90は、オンボードディスクを搭載した統合システムです。2台のコントローラとディスクを1台のシャーシに搭載します。新しいコントローラに内蔵ドライブが搭載されている場合は、既存のシステムをアップグレードできません。

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。

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。

を参照してください ["参考資料"](#) から ONTAP 9 ドキュメントセンターにリンクして、ONTAP 9 製品ドキュメントにアクセスできます。

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

ONTAP 9.15.1以降を実行するコントローラのペアをARLを使用してアップグレードできるかどうかを理解するには、プラットフォームと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

このARLの手順を使用してノードのペアをアップグレードする前に、次の要件を確認して、構成がサポートされていることを確認してください。

- 元のコントローラと交換用コントローラでARLを実行できることを確認します。
- 定義済みのすべてのアグリゲートのサイズと、元のシステムでサポートされているディスク数を確認します。次に、サポートされるアグリゲートの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

リゲートのサイズとディスク数と比較します。この情報が利用可能な [_ Hardware Universe _](#) へのリンクについては、を参照して ["参考資料"](#) ください。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、クラスタに新しいノードが既存のノードと一緒にクラスタに追加できるかどうかを混在ルールで検証します。クラスタ混在ルールの詳細については、[_ Hardware Universe _](#) へのリンクを参照して ["参考資料"](#) ください。
- 次の構成のAFF 700などのシステムを使用している場合は、ノードごとに2つのクラスタポートにクラスタLIFを移行し、ホームポートを変更します。
- ノードごとに2つ以上のクラスタポート
- ポートe4a、e4b、e4c、e4dを作成するためのブレイクアウトモードのslot4のクラスタインターコネクトカードと、ポートe4e、e4f、e4g、およびe4h



ノードごとにクラスタポートが2つ以上ある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が失われる可能性があります。

詳細については、ナレッジベースの記事を参照して ["不要なクラスタLIFや不要なクラスタLIFを削除する方法"](#) ください。

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

元のコントローラに接続されているディスクシェルフがサポートされない交換用コントローラはアップグレードできません。

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をアップグレードする場合は、ボリュームまたはストレージの移動によるアップグレード [_](#) へのリンクを参照し、「[_ ボリュームの移動による clustered Data ONTAP を実行するノードのペアのアップグレード](#)」の手順を参照して ["参考資料"](#) ください。

トラブルシューティングを行う

コントローラのアップグレード中に問題が発生した場合の詳細と考えられる解決方法については、を参照して ["トラブルシューティングを行う"](#) ください。

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。

ARL アップグレードの概要

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"	<p>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。</p> <p>ステージ 1 終了時のアグリゲートの所有権：</p> <ul style="list-style-type: none">• 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
<p>"ステージ 2：移行してノード 1 を撤去"</p>	<p>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。</p> <p>ステージ 2 終了時のアグリゲートの所有権：</p> <ul style="list-style-type: none"> • 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。
<p>"ステージ 3：node3 をインストールしてブートします"</p>	<p>ステージ 3 で、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 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。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。</p> <p>ステージ 3 終了時のアグリゲートの所有権：</p> <ul style="list-style-type: none"> • 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。
<p>"ステージ 4：ノード 2 の移動と撤去"</p>	<p>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。</p> <p>ステージ 4 終了時のアグリゲートの所有権：</p> <ul style="list-style-type: none"> • 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"	<p>ステージ 5 で、node4 をインストールしてブートした場合、node2 のクラスタポートとノード管理ポートがオンラインになっていることを確認し、node4 のインストールがあることを確認します。NVE を使用している場合は、key-manager configuration をリストアします。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。</p> <p>ステージ 5 終了時のアグリゲートの所有権：</p> <ul style="list-style-type: none"> • 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"	<p>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。</p>

ステージ 1 : アップグレードを準備

ステージ1の概要

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。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ていて、SnapMirror関係を休止するように選択できる場合は、特定の情報も記録しておきます。

手順

1. "ノードをアップグレードする準備をします"
2. "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"

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_names>
```



system controller replace start コマンドは、advanced 権限レベルでのみ実行できます。set -privilege advanced

次の例のような出力が表示されます。出力には、クラスタで実行されているONTAPのバージョンが表示されます。

```
Warning: 1. Current ONTAP version is 9.15.1
```

```
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.
```

```
4. Note: This is not a MetroCluster configuration. Controller replacement supports only ARL based procedure.
```

```
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
クラスタの健全性チェック	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。
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。
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。

事前チェック	説明
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。足りないディスクがある場合は、を参照してください " 参考資料 " CLI でディスクおよびアグリゲートの管理にリンクするには、CLI _、_ で論理ストレージの管理に使用します。HA ペアのストレージを構成するには、_、_ ハイアベイラビリティ管理 _ を使用します。
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。

次の構成のAFF 700などのシステムを使用している場合は、アップグレードを開始する前に、クラスタLIFをノードごとに2つのクラスタポートに移行してホームポートに戻します。



- ノードごとに2つ以上のクラスタポート
- ポートe4a、e4b、e4c、e4dを作成するためのブレイクアウトモードのslot4のクラスタインターコネクトカードと、ポートe4e、e4f、e4g、およびe4h

ノードごとにクラスタポートが2つ以上ある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が失われる可能性があります。

詳細については、ナレッジベースの記事を参照して ["不要なクラスタLIFや不要なクラスタLIFを削除する方法"](#) ください。

4. システムコンソールで、コントローラの交換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 -r`
- `storage aggregate show -node <local>`
- `volume show -node <local>`
- `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ワード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](#)

[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)

["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

アグリゲータ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

ONTAPライセンスの詳細については、を参照してください ["ライセンス管理"](#)。



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ります。

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ズ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. クラスタ全体のパズ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ズフレーズです。

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、リポ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

ステージ2の概要

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また、必要なノード1の情報を記録してノード1を撤去し、あとで手順でノード3とノード4をネットブートする準備をします。

手順

1. "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"
2. "障害が発生したアグリゲートを再配置するか"
3. "ノード 1 を撤去"
4. "ネットブートを準備"

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せん。

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 aggr_name`
```

- 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 --状態オフライン
```

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_name_-volume_name_`
```

このコマンドで使用する'vserver_name'は'前のvolume showコマンドの出力にあります

- [[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
```

障害が発生したアグリゲートを再配置するか

いずれかのアグリゲートに再配置が失敗した場合、または拒否されている場合は、アグリゲートを手動で再配置するか、必要に応じて拒否またはデスティネーションのチェックを無視する必要があります。

このタスクについて

エラーが原因で再配置処理が一時停止します。

手順

- 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。
- 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 -node1_-destination_node2」 -aggregate-list_aggr_name --nd
```

-controller-upgrade true」を指定します

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_aggr_list --nd -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_aggr_list --nd -controller-upgrade true -override-vetoes true -override-vetoes true -override-vetoes 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。

USB ブートオプションを使用してネットブートを実行することもできます。サポート技術情報の記事を参照してください "[システムの初期セットアップのために ONTAP をインストールするために boot_recovery loader コマンドを使用する方法](#)"。

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。

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

ステージ3の概要

ステージ 3 で、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 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。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。

手順

1. ["node3 をインストールしてブートします"](#)
2. ["ノード 3 のインストールを確認します"](#)
3. ["ノード 3 でキー管理ツールの設定をリストアします"](#)
4. ["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"](#)

node3 をインストールしてブートします

ノード3をラックに取り付け、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を取り付けます。次に、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、および以前にノード2に再配置されていなかったルート以外のアグリゲートを再割り当てします。

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が正常にオンラインになり、ノード3の正しいFC物理ポートに割り当てられている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"**。

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。

新しいノードのスペースと高さの要件は、既存のノードと異なる場合があります。アップグレードシナリオのスペース要件を計画します。

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。
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。

ONTAP 9.15.1以降では、新しいコントローラモデルにベースボード管理コントローラ (BMC) および管理接続用の「レンチ」ポートが1つだけ搭載されています。それに応じてケーブル配線の変更を計画します。

- コンソール (リモート管理ポート)
- クラスタポートとHA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
- Serial-Attached SCSI (SAS) およびEthernetストレージポート
- SAN構成: iSCSIイーサネット、FC、NVMe/FCスイッチポート

異なるコントローラモデルやカードモデル間で相互運用性を確保するために、新旧のコントローラ間のインターコネクトケーブルの変更が必要になる場合があります。ご使用のシステムのイーサネットストレージシェルフのケーブル接続マップについては、を参照して **"システムのインストール手順"** ください。



ONTAP 9.15.1以降で導入されたコントローラでは、クラスタインターコネクトとHAインターコネクトで同じポートが使用されます。スイッチ接続構成では、同様のポートを同じクラスタスイッチに接続する必要があります。たとえば、既存のコントローラからAFF A1Kにアップグレードする場合は、両方のノードのe1aポートを一方のスイッチに接続し、両方のノードのe7aポートをもう一方のスイッチに接続する必要があります。

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。



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。



* 注意：遅延は無視しないでください。バッテリーの充電に失敗すると、データが失われるおそれがあります。 *



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。アップグレードの実行中にデータ LIF IP を使用しないでください。データ LIF が停止する可能性があります。

動的ホスト構成プロトコル (DHCP) の状態	作業
実行中です	ブート環境プロンプトで次のコマンドを使用して、自動的に接続を設定します。 <code>ifconfig e0M -auto</code>

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	<p>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。</p> <pre>ifconfig e0M -addr=filer_addr -mask=netmask -gw=gateway -dns=dns_addr -domain=dns_domain</pre> <p><i>filer_addr</i> は、ストレージシステムのIPアドレスです (必須)。 <i>netmask</i> は、ストレージシステムのネットワークマスクです (必須)。 <i>gateway</i> は、ストレージシステムのゲートウェイです (必須)。 <i>dns_addr</i> 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)。 <i>dns_domain</i> 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)。</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p> 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。</p> </div>

7. [[step7] node3 でネットブートを実行します。

```
netboot/http://<web_server_ip/path_to_web-accessible_directory>/<ontap_version>_image.tgz`
```

「<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せん。

 新しいノードを希望するイメージに更新する場合は、必ずネットブートを使用してください。別の方法で新しいコントローラにイメージをインストールした場合、正しいイメージがインストールされないことがあります。この問題環境 All ONTAP リリース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`](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

14. イーサネットシェルフへの接続に使用するすべてのイーサネットポートがストレージとして構成されていることを確認します。

```
storage port show
```

表示される出力は、システム構成によって異なります。次の出力例は、スロット11にストレージカードが1つ搭載されたノードに対するものです。システムの出力は異なる場合があります。

```
*> storage port show
Port Type Mode      Speed (Gb/s) State      Status  VLAN ID
-----
e11a ENET storage 100 Gb/s    enabled  online  30
e11b ENET storage 100 Gb/s    enabled  online  30
```

15. ストレージに設定されていないポートを変更します。

```
storage port modify -p <port> -m storage
```

ストレージシェルフに接続されたすべてのイーサネットポートは、ディスクとシェルフにアクセスできるようにストレージとして構成する必要があります。

16. メンテナンスモードを終了します。

「halt」

ブート環境プロンプトで Ctrl+C キーを押して'自動ブートを中断します

17. 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」

18. node3 で、ブート環境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」

19. 必要に応じて、node3 で日付を設定します。

```
set date <mm/dd/yyyy>
```

20. 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刻を確認します。

「時間」

21. 必要に応じて、node3 で時刻を設定します。

```
set time <hh:mm:ss>
```

22. ブートローダーのnode3にあるパートナーシステムIDを設定します。

```
setenv 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
```

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

24. NetApp Storage Encryption (NSE) ドライブを搭載している場合は、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	<code>setenv bootarg.storageencryption.support true</code>
ネットアップの非FIPS SED	<code>setenv bootarg.storageencryption.support false</code>

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。

パスフレーズと、前の手順で手順 に記録しておいたバックアップ情報を入力します。を参照してください "[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](#)"。

25. ノードをブートメニューに追加します。

「 `boot_ontap menu`

26. ノード3で、ブートメニューに移動し、22 / 7を使用して隠しオプションを選択します `boot_after_controller_replacement`。プロンプトで、`node1` のディスクを `node3` に再割り当てするには、次の例のように入力します。

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>
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せん。

27. というメッセージが表示されてシステムのリブートループが発生した場合は `no disks found`、ディスクの再割り当てで問題が発生したことを示しています。問題を解決するには、[を参照してください"トラブルシューティングを行う"](#)。
28. 自動ブート中にを押して、プロンプトで `Ctrl-C` ノードを停止し `LOADER>` ます。
29. `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

30. ディスクの接続、コントローラのモデル文字列、HA構成、およびその他のハードウェアの接続に関する詳細を確認します。
31. メンテナンスモードを終了します。

「`halt`」

32. `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
```

- b. (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
- c. 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
```

- d. 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。
- e. 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。

- f. 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 [ステップ32](#) ます。

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. advanced権限モードに切り替えます。

「高度」

4. 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

5. 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」

6. 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。

7. 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。

手順

1. アップグレードされた node1 (node3) にある物理ポートをすべて一覧表示します。

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せん。

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. node3 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

次の例のような出力が表示されます。

```
ClusterA::*> network port reachability show
Node      Port      Expected Reachability      Reachability
Status
-----
node1_node3
      e0M      Default:Mgmt      ok
      e10a     Default:Default   ok
      e10b     -                 no-reachability
      e10c     Default:Default   ok
      e10d     -                 no-reachability
      e1a      Cluster:Cluster   ok
      e1b      -                 no-reachability
      e7a      Cluster:Cluster   ok
      e7b      -                 no-reachability
node2_node4
      e0M      Default:Mgmt      ok
      e4a      Default:Default   ok
      e4b      -                 no-reachability
      e4c      Default:Default   ok
      e4d      -                 no-reachability
      e3a      Cluster:Cluster   ok
      e3b      Cluster:Cluster   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_name>
```

次の例のような出力が表示されます。

```
Cluster ::> reachability repair -node nodel_node3 -port e4a
```

```
Warning: Repairing port "nodel_node3: e4a" 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: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 <ifgrp> -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>
```

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. 次の手順に従って、ブロードキャストドメインに適切な物理ポートを割り当て cluster 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_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_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
      e4a         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。

クラスター・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「e9a」で削除されたVLANを「e9d」にリストアする例を示します。

```
Cluster::*> displaced-vlans restore -node node1_node3 -port e9a
-destination-port e9d
```

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. [[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 displaced-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	""	0000000000000000200000000000a008a81976
true			2190178f9350e071fbb90f000000000000000

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。

手順

1. 到達可能性スキャンを使用して、iSCSI LIFが正しいホームポートを自動的に検出します。FCおよびNVMe/FC SAN LIFは自動的に移動しません。アップグレード前のホームポートは引き続き表示されます。

ノード3のSAN LIFを確認します。

- a. 「停止」処理ステータスを報告しているiSCSI SAN LIFを新しいデータポートに変更します。

```
network interface modify -vserver <vserver> -lif <iscsi_san_lif> admin down
```

```
network interface modify -vserver <vserver> -lif <iscsi_san_lif> port  
<new_port> node <node>
```

```
network interface modify -vserver <vserver> -lif <iscsi_san_lif>
```

- b. 新しいコントローラのホームにあるFCおよびNVMe/FC SAN LIFを変更し、新しいコントローラのFCPポートに「停止」の動作ステータスを報告します。

```
network interface modify -vserver <vserver> -lif <fc_san_lif> admin down
```

```
network interface modify -vserver <vserver> -lif <fc_san_lif> port  
<new_port> node <node>
```

```
network interface modify -vserver <vserver> -lif <fc_san_lif>
```

2. 再配置処理を再開します。

「システムコントローラの交換が再開」

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。

3. 再配置処理を再開します。

「システムコントローラの交換が再開」

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。

4. 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

コントローラ交換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。

5. 必要に応じて、取り外した LIF をリストアしてリポートします。取り外した LIF を表示します。

cluster controller -replacement network ヒエラー（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） -interface show

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。

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インタフェース・リストア -home-node

6. 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。

「システムコントローラの交換が再開」

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

ステージ4の概要

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。あとで手順で使用するために必要なノード2の情報も記録しておき、ノード2を撤去します。

手順

1. "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"
2. "ノード 2 を撤去"

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せん。

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 aggr_name
```

- 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 _name -volume _name'
```

このコマンドで使用する '*vserver_name*' は '前の volume show コマンドの出力にあります

- 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 _name __-status-admin up
```

- 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
```

- [[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
```

ノード 2 を撤去

ノード2を撤去するには、まずノード2を正しくシャットダウンし、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

ステージ5の概要

ステージ 5 で、node4 をインストールしてブートした場合、node2 のクラスタポートとノード管理ポートがオンラインになっていることを確認し、node4 のインストールがあることを確認します。NVEを使用している場合は、key-manager configurationをリストアします。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。

手順

1. "ノード 4 をインストールしてブートします"
2. "ノード 4 のインストールを確認します"
3. "ノード 4 でキー管理ツールの設定をリストアします"
4. "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 をインストールしてブートします

ノード4をラックに取り付け、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をインストールします。次に、このセクションで説明するように、ノード2の任意のスペアディスク、ルートボリュームに属するディスク、および以前にノード3に再配置されていなかったルート以外のアグリゲートを再割り当てします。

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。

node2 に同じバージョンの ONTAP 9 がインストールされていない場合は、node4 をネットブートする必要があります。node4 のインストールが完了したら、Web サーバに格納されている ONTAP 9 イメージからブートします。その後、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"](#)。

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。

各ノード 4 のプラットフォームについて、『Installation and Setup Instructions』または『FlexArray Virtualization Installation Requirements and Reference_for the node4』、該当するディスクシェルフのドキュメント、および `_High Availability management_` の手順に従って、次の接続をケーブル接続します。

を参照してください ["参考資料" FlexArray 仮想化インストール要件およびリファレンスとハイアベイラビリティ管理へのリンク](#)。

- コンソール（リモート管理ポート）
- クラスタポートとHA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
- Serial-Attached SCSI（SAS）およびEthernetストレージポート
- SAN構成：iSCSIイーサネット、FC、NVMe/FCスイッチポート

異なるコントローラモデルやカードモデル間で相互運用性を確保するために、新旧のコントローラ間のインターコネクトケーブルの変更が必要になる場合があります。ご使用のシステムのイーサネットストレージシェルフのケーブル接続マップについては、を参照して ["システムのインストール手順"](#) ください。



ONTAP 9.15.1以降で導入されたコントローラでは、クラスタインターコネクトとHAインターコネクトで同じポートが使用されます。スイッチ接続構成では、同様のポートを同じクラスタスイッチに接続する必要があります。たとえば、既存のコントローラからAFF A1Kにアップグレードする場合は、両方のノードのe1aポートを一方のスイッチに接続し、両方のノードのe7aポートをもう一方のスイッチに接続する必要があります。

4. node4 への電源を入れてから、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。



* 注意：遅延は無視しないでください。バッテリーの充電に失敗すると、データが失われるおそれがあります。 *



を参照してください ["ネットブートを準備"](#)。

6. 次のいずれかを実行してネットブート接続を設定します。



ネットブート接続として管理ポートおよび IP を使用する必要があります。アップグレードの実行中にデータ LIF IP を使用しないでください。データ LIF が停止する可能性があります。

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。 <code>ifconfig e0M -auto</code>

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	<p>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。</p> <pre>ifconfig e0M -addr=filer_addr -mask=netmask -gw=gateway -dns=dns_addr -domain=dns_domain</pre> <p><i>filer_addr</i> は、ストレージシステムのIPアドレスです (必須)。 <i>netmask</i> は、ストレージシステムのネットワークマスクです (必須)。 <i>gateway</i> は、ストレージシステムのゲートウェイです (必須)。 <i>dns_addr</i> 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)。 <i>dns_domain</i> は、DNSドメイン名です (オプション)。</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p> 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。</p> </div>

7. ノード 4 でネットブートを実行します。

```
netboot\http://<web_server_ip/path_to_web-accessible_directory>/<ontap_version>_image.tgz`
```

「<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ポートします。
 - 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ポートしますが、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

14. イーサネットシェルフへの接続に使用するすべてのイーサネットポートがストレージとして構成されていることを確認します。

storage port show

表示される出力は、システム構成によって異なります。次の出力例は、スロット11にストレージカードが1つ搭載されたノードに対するものです。システムの出力は異なる場合があります。

```
*> storage port show
Port Type Mode      Speed (Gb/s) State      Status  VLAN ID
-----
e11a ENET storage 100 Gb/s    enabled  online  30
e11b ENET storage 100 Gb/s    enabled  online  30
```

15. ストレージに設定されていないポートを変更します。

```
storage port modify -p <port> -m storage
```

ストレージシェルフに接続されたすべてのイーサネットポートは、ディスクとシェルフにアクセスできるようにストレージとして構成する必要があります。

16. 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 を押し、AUTOBOOT を中断します。

17. [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」

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日付を確認します。

「日付」

19. 必要に応じて、node4 に日付を設定します。

```
set date <mm/dd/yyyy>
```

20. 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」

21. 必要に応じて、node4 に時間を設定します。

```
set time <hh:mm:ss>
```

22. 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。

```
setenv 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
```

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

24. NetAppストレージ暗号化（NSE）ドライブが取り付けられている場合は、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	<code>setenv bootarg.storageencryption.support true</code>
ネットアップの非FIPS SED	<code>setenv bootarg.storageencryption.support false</code>

- 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。

パスフレーズと、前の手順で手順 に記録しておいたバックアップ情報を入力します。を参照してください "[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](#)"。

25. ノードをブートメニューに追加します。

「 boot_ontap menu

26. node4で、ブートメニューに移動し、22/7を使用して隠しオプションを選択します `boot_after_controller_replacement`。プロンプトで `node2` と入力し、次の例のように `node2` のディスクを `node4` に再割り当てします。

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>

Changing sysid of node node2 disks.

Fetches 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せん。

27. 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。

ルートボリュームが暗号化されている場合は、システムがルートボリュームを検出できるように、オンボードキー管理シークレットをリカバリします。

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
```

b. (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

c. 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
```

d. 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。

e. 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。

f. 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 [ステップ27](#) ます。

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. advanced 権限モードに切り替えます。

「高度」

4. 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

5. 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」

6. 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。

7. 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。

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::*> network port reachability show
Node      Port      Expected Reachability      Reachability
Status
-----
node1_node3
    e0M      Default:Mgmt      ok
    e10a     Default:Default  ok
    e10b     -                no-reachability
    e10c     Default:Default  ok
    e10d     -                no-reachability
    e1a      Cluster:Cluster  ok
    e1b      -                no-reachability
    e7a      Cluster:Cluster  ok
    e7b      -                no-reachability
node2_node4
    e0M      Default:Mgmt      ok
    e10a     Default:Default  ok
    e10b     -                no-reachability
    e10c     Default:Default  ok
    e10d     -                no-reachability
    e1a      Cluster:Cluster  ok
    e1b      -                no-reachability
    e7a      Cluster:Cluster  ok
    e7b      -                no-reachability
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_name>
```

次のような出力が表示されます。

```
Cluster ::> reachability repair -node node2_node4 -port e10a
```

```
Warning: Repairing port "node2_node4: e10a" 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: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 <ifgrp> -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>
```

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_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_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
      e10a         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「e10a」で削除されたVLANを「e10b」にリストアする例を示します。

```
Cluster::*> displaced-vlans restore -node node2_node4 -port e10a
-destination-port e10b
```

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。

「displaced-interface show」

- b. LIF のホームポートをリストアします。

```
displaced-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 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       ""          0000000000000000020000000000a008a81976  
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 のネットワーク設定を確認し、ノード 3 からノード 4 にアグリゲートを再配置する前に、ノード 2 に現在ノード 3 に属する NAS データ LIF が、ノード 3 からノード 4 に再配置されていることを確認する必要があります。また、ノード 4 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ー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 4 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。

手順

1. 到達可能性スキャンを使用して、iSCSI LIFが正しいホームポートを自動的に検出します。FCおよびNVMe/FC SAN LIFは自動的に移動しません。アップグレード前のホームポートは引き続き表示されます。

ノード4のSAN LIFを確認します。

- a. 「停止」処理ステータスを報告しているiSCSI SAN LIFを新しいデータポートに変更します。

```
network interface modify -vserver <vserver> -lif <iscsi_san_lif> admin down
```

```
network interface modify -vserver <vserver> -lif <iscsi_san_lif> port  
<new_port> node <node>
```

```
network interface modify -vserver <vserver> -lif <iscsi_san_lif>
```

- b. 新しいコントローラのホームにあるFCおよびNVMe/FC SAN LIFを変更し、新しいコントローラのFCPポートに「停止」の動作ステータスを報告します。

```
network interface modify -vserver <vserver> -lif <fc_san_lif> admin down
```

```
network interface modify -vserver <vserver> -lif <fc_san_lif> port  
<new_port> node <node>
```

```
network interface modify -vserver <vserver> -lif <fc_san_lif>
```

2. 再配置処理を再開します。

「システムコントローラの交換が再開」

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。

3. 再配置処理を再開します。

「システムコントローラの交換が再開」

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。

4. 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

コントローラ交換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 resume」をクリックして操作を続行します。

5. 必要に応じて、取り外した LIF をリストアしてリポートします。取り外した LIF を表示します。

cluster controller -replacement network ヒエラー（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） -interface show

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。

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インタフェース・リストア -home-node

6. 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。

「システムコントローラの交換が再開」

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

ステージ6の概要

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NetApp Volume Encryptionを設定および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。

手順

1. "KMIP サーバを使用して認証を管理します"
2. "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"
3. "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"
4. "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"
5. "古いシステムの運用を停止"
6. "SnapMirror 処理を再開します"

KMIP サーバを使用して認証を管理します

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

- 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

- 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」

- 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ポートします。

「network interface revert」の略

- 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>
```

- 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
```

- 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>
```

- 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. 構成で自己暗号化ドライブを使用している場合は、変数をに設定して `kmip.init.maxwait off` (のように) "[Node4 をインストールしてブートします \(手順 24\)](#)"、変数の設定を解除する必要があります。

```
set diag; systemshell -node <node_name> -command 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>
```

を参照してください "[参考資料](#)" SP および `_SP ONTAP 9.8` コマンドの詳細については 'システム管理リフ

ァレンスにリンクするには ' マニュアルページリファレンスを参照してください system の service-processor network modify コマンドの詳細については ' を参照してください

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、技術情報アート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

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

ユする、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。

手順の各フェーズについては、セクションの表を参照してください "[ARL アップグレードの概要](#)"。発生する可能性のある障害の情報は、手順のフェーズ別に表示されます。

アグリゲートの再配置に失敗しました

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」、および「override-vetoes destination-checks」オプションの詳細については、を参照してください "[参考資料](#)" ONTAP 9.8 コマンド：マニュアルページリファレンスにリンクするには、次の手順を実行します。

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ポート、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ポート、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継続されます。

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継続されますが、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ポート、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。リポ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ポート、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継続されます。

このタスクについて

node2 で残りのアグリゲートの処理は継続されますが、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
```

Node	Partner	Takeover 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
```

Node	Partner	Takeover 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]

• [参照サイト]

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。
"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。
"FlexArray 仮想化インストール要件およびリファレンスガイド"	FlexArray 仮想化システムのケーブル接続手順とその他の情報について説明します
"高可用性管理"	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 9.13.1 コマンド：マニュアルページリファレンス"	サポートされる ONTAP 9.13.1 コマンドの構文と使用法について説明します。
"ONTAP 9.14.1 コマンド：マニュアルページリファレンス"	サポートされる ONTAP 9.14.1 コマンドの構文と使用法について説明します。
"ONTAP 9.15.1 コマンド：マニュアルページリファレンス"	サポートされる ONTAP 9.15.1 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。

内容	説明
"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セ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
"「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。
"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。

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

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

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

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

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

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

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

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

商標に関する情報

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