



ステージ 1 : アップグレードを準備

Upgrade controllers

NetApp
February 22, 2024

目次

ステージ 1：アップグレードを準備	1
概要	1
ノードをアップグレードする準備をします	1
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	6

ステージ 1：アップグレードを準備

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_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'
```

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

「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。
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。
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。



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 *
```


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权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

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