ステージ 3 ：交換用システムモジュールでノード1をブートします

Upgrade controllers

NetApp
March 11, 2026

This PDF was generated from https://docs.netapp.com/ja-jp/ontap-systems-upgrade/upgrade-arl-auto-in-chassis/cable-node1-for-shared-cluster-HA-storage.html on March 11, 2026. Always check docs.netapp.com for the latest.

目次

ステージ 3 ：交換用システムモジュールでノード1をブートします . . . 1
共有クラスタHAとストレージのノード1をケーブル接続します。 . . . 1
e0MポートとBMCポートを接続 . . . 1
2ノードスイッチレスクラスタに接続 . . . 1
スイッチ接続クラスタへの接続 . . . 2
交換用システムモジュールでノード1をブートします . . . 3
アップグレードした node1 でキー管理ツールの設定をリストアします . . . 9
ノード1のルート以外のアグリゲートとNASデータLIFをノード2からアップグレード後のノード1に移動します。 . . . 10

ステージ 3 ：交換用システムモジュールでノード1をブートします

共有クラスタHAとストレージのノード1をケーブル接続します。

次のいずれかのアップグレードを実行する場合は、以前に既存のシステムのnode1に接続していたクラスタ、HA、ストレージ、データ、および管理の接続を、交換用システムの新しくインストールしたnode1に接続する必要があります。

既存のシステム	交換用システム
AFF A250用	AFF A30、AFF A50
AFF C250用	AFF C30、AFF C60
AFF A800用	AFF A70、AFF A90
AFF C800用	AFF C80用

e0MポートとBMCポートを接続

既存のシステムに管理ポート（e0M）とBMCポートがある場合は、e0MポートとBMCポートが組み合わされ、交換用システムの「レンチ」ポートからアクセスされます。交換用システムに接続する前に、e0MポートとBMCポートが既存システムの同じスイッチとサブネットに接続されていることを確認する必要があります。

状況	作業
e0MとBMCのIPアドレスが同じIPサブネット上にある	既存システムのe0MポートまたはBMCポートを、交換用システムの「レンチ」ポートに接続します。
e0MとBMCのIPアドレスが別 々 のサブネットにあります	1. e0MとBMCのIPアドレスを1つのIPサブネットにマージします。 2. 既存システムのe0MポートまたはBMCポートを、交換用システムの「レンチ」ポートに接続します。

2ノードスイッチレスクラスタに接続

次の表に、2ノードスイッチレスクラスタ構成でのスイッチポートの用途を示します。

ポートタイプ	AFF A800、AFF C800	AFF A90用	AFF A70、AFF C80
クラスタ	e0a	e1a	e1a
クラスタ	e1a	e7a（e7aがない場合はe1bを使用）	e1b
はあ	e0b	接続しないでください	接続しないでください
はあ	e1b	接続しないでください	接続しないでください

ポートタイプ	**AFF A800、AFF C800**	**AFF A90用**	**AFF A70、AFF C80**
SASストレージポート（存在し、使用している場合）	使用可能な任意のポート	使用可能な任意のポート	使用可能な任意のポート
NS224シェルフのイーサネットストレージポート	使用可能な任意のポート	イーサネットストレージ接続のマッピングを参照	イーサネットストレージ接続のマッピングを参照

ポート	**AFF A250、AFF C250**	**AFF A30、AFF C30、AFF C60**	**AFF A50用**
クラスタ	e0c	e1a (一時的なクラスタ相互接続には e1a を使用)	e1a (一時的なクラスタ相互接続には e1a を使用)
クラスタ	e0d	e1b (一時的なクラスタ相互接続には e1b を使用)	e1b (一時的なクラスタ相互接続には e1b を使用)
はあ	不要	ノード1のアップグレードにはHAポートは必要ありません	ノード1のアップグレードにはHAポートは必要ありません
イーサネットストレージポート	使用可能な任意のポート	e3a、e3b	e3a、e3b
SASストレージポート	使用可能な任意のポート	3a、3b	3a、3b

スイッチ接続クラスタへの接続

スイッチ接続クラスタの場合は、AFF A30、AFF A50、AFF A70、AFF A90、AFF C30、AFF C60、またはAFF C80（交換用）ノードの次の要件を満たしていることを確認します。

- 交換用ノードの同一のクラスタポートが同じスイッチ上にあります。たとえば、アップグレードが完了したら、node1のe1aとnode2のe1aを1つのクラスタスイッチに接続する必要があります。同様に、両方のノードの2番目のクラスタポートを2番目のクラスタスイッチに接続する必要があります。共有クラスタHAポート（ノード1のe1aがスイッチAに接続され、ノード2のe1aがスイッチBに接続されている）をクロス接続すると、HA通信に障害が発生します。
- 交換用ノードは、共有のクラスタHAイーサネットポートを使用します。
- クラスタスイッチに、共有クラスタHAポートをサポートするリファレンス構成ファイル（RCF）がインストールされていることを確認します。

  a. スイッチの既存の設定を削除します。

スイッチのモデル	手順
Cisco Nexus	ナレッジベースの記事"リモート接続を維持したままCiscoインターコネクトスイッチの設定をクリアする方法"
Broadcom BES-53248	ナレッジベースの記事"リモート接続を維持したままBroadcomインターコネクトスイッチの設定をクリアする方法"

  b. スイッチのセットアップを設定して確認します。

スイッチのモデル	手順
Cisco Nexus 9336C-FX2	"リファレンス構成ファイル（RCF）のアップグレード"
Broadcom BES-53248	"リファレンス構成ファイル（RCF）のアップグレード"
NVIDIA SN2100	"リファレンス構成ファイル（RCF）スクリプトのインストールまたはアップグレード"

クラスタ スイッチが 10/25 GbE の速度のみをサポートしている場合は、クラスタ相互接続の交換システムのスロット 1 またはスロット 2 で X60130A、4 ポート 10/25GbE カードを使用する必要があります。

交換用システムモジュールでノード1をブートします

交換用モジュールを搭載した Node1 の起動準備が完了しました。サポートされている交換モジュールは、"サポートされるシステムマトリックス"に記載されています。

コントローラモジュールを交換する場合は、すべての接続を古いコントローラモジュールから交換用コントローラモジュールに移動します。

コントローラモジュールとNVRAMモジュールを交換する場合は、コンソール接続と管理接続のみを移動します。

手順

1. （AFF A250、AFF C250、AFF A800、またはAFF C800アップグレードのみ）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

   a. 答え `y`混合プラットフォームの確認プロンプトが表示されます。

   b. 確認プロンプトに応答し `yes` ます。

   c. 100GbEインターフェイスの状態を表示します。

      `storage port show`です。

      次の出力例に示すように、NS224シェルフまたはストレージスイッチに接続されたすべての100GbEポートがポートとして報告されます `storage` 。

```
*> storage port show
Port Type Mode    Speed(Gb/s) State    Status  VLAN ID
---- ---- ------- ----------- -------- ------- -------
e8a  ENET storage 100 Gb/s    enabled  online  30
e8b  ENET storage 100 Gb/s    enabled  online  30
e11a ENET storage 100 Gb/s    enabled  online  30
e11b ENET storage 100 Gb/s    enabled  online  30
```

a. メンテナンスモードを終了します。

「 halt 」

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

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

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

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

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

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

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

3. ノードをブートメニューでブートします。

「 boot_ontap menu

4. ノードがブート メニューで停止した場合は、node1 で次のコマンドを実行して、古い node1 ディスクを交換用の node1 に再割り当てします。

`boot_after_controller_replacement`

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

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

「[localhost:disk.encryptNoSupport:alert]: FIPS認定暗号化ドライブと」、または「[localhost:diskown.errorDuringIO: error]: Error」がディスクエラーで発生した場合は、次の手順を実行します。

a. LOADERプロンプトでノードを停止します。
b. に記載されているストレージ暗号化のbootargを確認してリセットします 手順 2。
c. LOADERプロンプトでブートします。

「 boot_ontap 」

次の例を参考にしてください。

コンソールの出力例を展開します

```
LOADER-A> boot_ontap menu
.
.
<output truncated>
.
All rights reserved.
*******************************
*                             *
* Press Ctrl-C for Boot Menu. *
*                             *
*******************************
.
<output truncated>
.
Please choose one of the following:

(1)  Normal Boot.
(2)  Boot without /etc/rc.
(3)  Change password.
(4)  Clean configuration and initialize all disks.
(5)  Maintenance mode boot.
(6)  Update flash from backup config.
(7)  Install new software first.
(8)  Reboot node.
(9)  Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? 22/7

(22/7)                          Print this secret List
(25/6)                          Force boot with multiple filesystem
disks missing.
(25/7)                          Boot w/ disk labels forced to clean.
(29/7)                          Bypass media errors.
(44/4a)                         Zero disks if needed and create new
flexible root volume.
(44/7)                          Assign all disks, Initialize all
disks as SPARE, write DDR labels
.
.
<output truncated>
.
.
(wipeconfig)                        Clean all configuration on boot
```

```
device
(boot_after_controller_replacement) Boot after controller upgrade
(boot_after_mcc_transition)         Boot after MCC transition
(9a)                                Unpartition all disks and remove
their ownership information.
(9b)                                Clean configuration and
initialize node with partitioned disks.
(9c)                                Clean configuration and
initialize node with whole disks.
(9d)                                Reboot the node.
(9e)                                Return to main boot menu.



The boot device has changed. System configuration information could
be lost. Use option (6) to restore the system configuration, or
option (4) to initialize all disks and setup a new system.
Normal Boot is prohibited.

Please choose one of the following:

(1)  Normal Boot.
(2)  Boot without /etc/rc.
(3)  Change password.
(4)  Clean configuration and initialize all disks.
(5)  Maintenance mode boot.
(6)  Update flash from backup config.
(7)  Install new software first.
(8)  Reboot node.
(9)  Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? boot_after_controller_replacement

This will replace all flash-based configuration with the last backup
to disks. Are you sure you want to continue?: yes

.
.
<output truncated>
.
.
Controller Replacement: Provide name of the node you would like to
replace:<nodename of the node being replaced>
Controller Replacement: Provide High Availability partner of node1:
<nodename of the partner of the node being replaced>
```

```
Changing sysid of node node1 disks.
Fetched sanown old_owner_sysid = 536940063 and calculated old sys id
= 536940063
Partner sysid = 4294967295, owner sysid = 536940063
.
.
<output truncated>
.
.
varfs_backup_restore: restore using /mroot/etc/varfs.tgz
varfs_backup_restore: attempting to restore /var/kmip to the boot
device
varfs_backup_restore: failed to restore /var/kmip to the boot device
varfs_backup_restore: attempting to restore env file to the boot
device
varfs_backup_restore: successfully restored env file to the boot
device wrote key file "/tmp/rndc.key"
varfs_backup_restore: timeout waiting for login
varfs_backup_restore: Rebooting to load the new varfs
Terminated
<node reboots>

System rebooting...

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

```
.
Login:
```

上記の例のシステム ID は一例です。アップグレードするノードの実際のシステム ID は異なります。

プロンプトでノード名を入力するかログインプロンプトを表示するまで、ノードが数回リブートして環境変数をリストアし、システムのカードでファームウェアを更新し、他の ONTAP 更新を実行します。

アップグレードした **node1** でキー管理ツールの設定をリストアします

NetApp Aggregate Encryption（NAE）またはNetApp Volume Encryption（NVE）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。キー管理ツールを再同期しない場合、ARLを使用してノード1のアグリゲートをノード2からアップグレードしたノード1に再配置すると、ノード1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. node1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1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 node1 -fields restored -key
-type SVM-KEK
```

例

```
::> security key-manager key query -node node1 -fields restored -key
-type SVM-KEK

node     vserver   key-server   key-id
restored
-------- --------- -----------  ----------------------------------------
--------
node1    svm1      ""           000000000000000002000000000000a008a81976
true
                                2190178f9350e071fbb90f00000000000000000
```

ノード1のルート以外のアグリゲートとNASデータLIFをノード2からアップグレード後のノード1に移動します。

ノード 1 のネットワーク構成を確認した後、ノード 1 が所有する NAS データ LIF をノード 2 からノード 1 に再配置し、SAN LIF がノード 1 に存在することを確認する必要があります。

このタスクについて

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

node1 をオンラインにした後、LIF が正常であり、正しいポートに配置されていることを確認します。

手順

1. 再配置処理を再開します。

```
system controller replace resume
```

システムは次のタスクを実行します。

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

システムはネットワーク到達可能性チェックのこの段階で操作を一時停止します。

2. ネットワーク到達可能性チェックを実行します。

```
network port reachability show -node node1
```

インターフェイスグループポートおよび VLAN ポートを含むすべての接続ポートのステータスが「 OK 」であることを確認します。

3. 次のアップグレードでは、FCP SAN LIFを再割り当てする必要があります。

既存のシステム	交換用システム
AFF A250用	AFF A30、AFF A50
AFF C250用	AFF C30、AFF C60
AFF A800用	AFF A70、AFF A90
AFF C800用	AFF C80用

その他のすべてのシステムのアップグレードについては、に進みます手順 4。

a. FCPまたはFC-NVMeデータアクセスに使用するFCP SAN LIFを正しいホームポートに再割り当てします。

```
network interface show -vserver <vserver_hosting_fcp_lifs>
```

b. 現在のノードがアップグレード後のノード1であり、現在のポートが「status oper」になっているLIFについては（ポートはAFF A800ノードに存在していたがAFF A90ノードには存在しないため）、現在のポートをオンラインにする前に変更します。

FC LIFを移動する必要があるFCターゲットポートへの物理的な接続が確立されていることを確認します。

i. LIF のステータスを「 down 」に設定します。

```
network interface modify -vserver <vserver_name> -lif <lif_name>
-status-admin down
```

ii. LIFのホームポートを変更します。

```
network interface modify -vserver <vserver_name> -lif <lif_name> -
home-node <node1> -home-port <FC_target_port>
```

iii. LIFのステータスを「up」に設定します。

```
network interface modify -vserver <vserver> -lif <lif_name>  -status
-admin up
```

+
node1のホームにあるFC SAN LIFごとに手順aとbを繰り返します。

4. 再配置操作を再開します

```
system controller replace resume
```

システムは次のチェックを実行します。

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

これらのチェックの実行後、システムは、 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 を新しい node1 に再配置します。

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。

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

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

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

6. 必要に応じて、移動された LIF を復元して元に戻すか、または node1 への自動再配置に失敗した node1 LIF を手動で移行して変更します。

移動した**LIF**を復元して元に戻す

a. 移動した LIF をリストします。

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

b. LIF が表示されなくなった場合は、ホームノードをノード 1 にリストアします。

```
cluster controller-replacement network displaced-interface
restore-home-node -node <node1_nodename> -vserver <vserver name>
-lif-name <lif_name>
```

LIFを手動で移行および変更する

a. 自動的に再配置できなかった LIF をノード 1 に移行します。

```
network interface migrate -vserver <vserver name> -lif <lif_name>
-destination-node <node1_nodename> -destination-port
<port_on_node1>
```

b. 移行された LIF のホーム ノードとホーム ポートを変更します。

```
network interface modify -vserver <vserver_name> -lif
<data_lif_name> -home-node <node1_nodename> -home-port
<home_port>
```

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

```
system controller replace resume
```

次のポストチェックが実行されます。

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

著作権に関する情報

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

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

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

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

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

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

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

商標に関する情報

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