



ブートメディア - 手動リカバリ

Install and maintain

NetApp
February 20, 2026

目次

ブートメディア - 手動リカバリ	1
ブートメディアの手動リカバリワークフロー - FAS50	1
手動ブートメディアリカバリの要件 - FAS50	2
手動ブートメディアリカバリの暗号化サポートを確認する - FAS50	2
ステップ1: NVEのサポートを確認し、正しいONTAPイメージをダウンロードする	2
ステップ2: キーマネージャーのステータスを確認し、構成をバックアップする	3
手動ブートメディアリカバリのためにコントローラをシャットダウンする - FAS50	7
ブートメディアを交換し、手動ブートリカバリの準備をします - FAS50	10
このタスクについて	10
手順 1 : コントローラを取り外す	10
手順 2 : ブートメディアを交換します	12
手順 3 : コントローラを再度取り付けます	13
手順 4 : ブートイメージをブートメディアに転送します	14
USBドライブからの手動ブートメディアリカバリ - FAS50	16
手動ブートリカバリ後の暗号化キーの復元 - FAS50	18
障害が発生したパーティションをNetApp - FAS50に返却します。	28

ブートメディア - 手動リカバリ

ブートメディアの手動リカバリワークフロー - FAS50

ブートイメージを手動でリカバリするには、USBドライブを使用して、FAS50システムの交換用ブートメディアにONTAPを再インストールする必要があります。NetApp NetApp サイトから適切なONTAPリカバリイメージをダウンロードし、USB ドライブにコピーする必要があります。この準備したUSB ドライブを使用してリカバリを実行し、システムを稼働状態に復元します。

システムがONTAP 9.17.1以降で実行されている場合は、["自動ブート回復手順"](#)。

開始するには、回復要件を確認し、コントローラーをシャットダウンし、ブート メディアを交換し、USB ドライブを使用してイメージを復元し、必要に応じて暗号化設定を再適用します。

1

"ブートメディア要件を確認"

ブートメディアの交換要件を確認します。

2

"オンボード暗号化キーを確認"

システムでセキュリティキー管理機能が有効になっているか暗号化されたディスクがあるかを確認します。

3

"障害のあるコントローラをシャットダウンします"

ブートメディアの交換が必要になったときは、コントローラをシャットダウンします。

4

"ブートメディアの交換"

障害が発生したコントローラから障害が発生したブート メディアを取り外し、交換用のブート メディアをインストールし、USB フラッシュ ドライブを使用してONTAPイメージを転送します。

5

"リカバリイメージをブートします"

USB ドライブからONTAPイメージをブートし、ファイルシステムをリストアして、環境変数を確認します。

6

"アンコウカノ"

ONTAPブート メニューからオンボード キー マネージャ構成または外部キー マネージャを復元します。

7

"障害のあるパーツをネットアップに返却します"

障害のある部品は、キットに付属する RMA 指示書に従ってネットアップに返却してください。

手動ブートメディアリカバリの要件 - FAS50

FAS50ストレージシステムのブートメディアを交換する前に、交換を正常に行うために必要な要件を満たしていることを確認してください。これには、適切なストレージ容量のUSBフラッシュドライブがあること、および交換用のブートデバイスが正しいことの確認が含まれます。

USB フラッシュ ドライブ

- USB フラッシュ ドライブが FAT32 にフォーマットされていることを確認します。
- USBには十分な保存容量が必要です `image_xxx.tgz` ファイル。

ファイルの準備

コピー `image_xxx.tgz` ファイルをUSBフラッシュドライブに保存します。このファイルは、USBフラッシュ ドライブを使用してONTAPイメージを転送するときに使用されます。

部品交換

故障したコンポーネントをNetAppが提供する交換用コンポーネントと交換します。

コントローラー識別

障害のあるブート メディアを交換するときは、正しいコントローラにコマンドを適用することが重要です。

- 障害のあるコントローラー は、メンテナンスを実行しているコントローラーです。
- 正常なコントローラ は、障害のあるコントローラの HA パートナーです。

次の手順

ブートメディアの交換要件を確認したら、を実行する必要があり["暗号化キーのサポートとブートメディアのステータスを確認する"](#)ます。

手動ブートメディアリカバリの暗号化サポートを確認する - FAS50

ストレージシステムのデータセキュリティを確保するには、暗号化キーのサポートとブートメディアのステータスを確認する必要があります。ONTAPのバージョンでNetApp Volume Encryption (NVE) がサポートされているかどうかを確認し、コントローラをシャットダウンする前にキー管理ツールがアクティブになっているかどうかを確認してください。

ステップ1: NVEのサポートを確認し、正しいONTAPイメージをダウンロードする

ブート メディアの交換に適切なONTAPイメージをダウンロードできるように、ONTAPバージョンがNetApp Volume Encryption (NVE) をサポートしているかどうかを確認します。

手順

- ONTAPバージョンが暗号化をサポートしているかどうかを確認します。

```
version -v
```

出力に含まれている場合、`1Ono-DARE` クラスタのバージョンではNVEがサポートされていません。

2. NVE サポートに基づいて適切なONTAPイメージをダウンロードします。

- NVEがサポートされている場合: NetApp Volume Encryptionを含むONTAPイメージをダウンロードします
- NVEがサポートされていない場合: NetAppボリューム暗号化なしのONTAPイメージをダウンロードします



NetAppサポートサイトからONTAPイメージを HTTP または FTP サーバーまたはローカル フォルダーにダウンロードします。ブート メディアの交換手順中にこのイメージファイルが必要になります。

ステップ2: キーマネージャーのステータスを確認し、構成をバックアップする

障害のあるコントローラをシャットダウンする前に、キー マネージャの構成を確認し、必要な情報をバックアップしてください。

手順

1. システムで有効になっているキー管理ツールを確認します。

ONTAP バージョン	実行するコマンド
ONTAP 9.14.1以降	<pre>security key-manager keystore show</pre> <ul style="list-style-type: none">◦ EKMが有効になっている場合は、`EKM`がコマンド出力に表示されます。◦ OKMが有効になっている場合は、`OKM`がコマンド出力に表示されます。◦ 有効になっているキー管理ツールがない場合は `No key manager keystores configured`、コマンドの出力にと表示されます。
ONTAP 9.13.1 以前	<pre>security key-manager show-key-store</pre> <ul style="list-style-type: none">◦ EKMが有効になっている場合は、`external`がコマンド出力に表示されます。◦ OKMが有効になっている場合は、`onboard`がコマンド出力に表示されます。◦ 有効になっているキー管理ツールがない場合は `No key managers configured`、コマンドの出力にと表示されます。

2. システムにキー マネージャーが設定されているかどうかに応じて、次のいずれかを実行します。

キーマネージャーが設定されていない場合:

障害のあるコントローラを安全にシャットダウンし、シャットダウン手順に進むことができます。

キーマネージャーが設定されている場合（**EKM**または**OKM**）：

- a. キー マネージャー内の認証キーのステータスを表示するには、次のクエリ コマンドを入力します。

```
security key-manager key query
```

- b. 出力を確認し、`Restored`カラム。この列には、キー マネージャー (EKM または OKM) の認証キーが正常に復元されたかどうかが表示されます。

3. キー マネージャーのタイプに応じて適切な手順を完了します。

外部キーマネージャ（**EKM**）

以下の値に基づいてこれらの手順を完了します。`Restored`カラム。

すべてのキーが表示された場合 `true` 復元された列に：

障害のあるコントローラーを安全にシャットダウンし、シャットダウン手順に進むことができます。

いずれかのキーに以下の値が表示されていない場合は `true` 復元された列に：

- 外部キー管理認証キーをクラスター内のすべてのノードに復元します。

```
security key-manager external restore
```

このコマンドが失敗した場合は、NetAppサポートにお問い合わせください。

- すべての認証キーが復元されたことを確認します。

```
security key-manager key query
```

確認する `Restored` 列表示 `true` すべての認証キーに対して。

- すべてのキーが復元された場合は、障害のあるコントローラーを安全にシャットダウンし、シャットダウン手順に進むことができます。

オンボードキーマネージャ（**OKM**）

以下の値に基づいてこれらの手順を完了します。`Restored`カラム。

すべてのキーが表示された場合 `true` 復元された列に：

- OKM 情報をバックアップします。

- 高度な権限モードに切り替える:

```
set -priv advanced
```

入力 `y` 続行するように求められた場合。

- キー管理のバックアップ情報を表示します。

```
security key-manager onboard show-backup
```

- バックアップ情報を別のファイルまたはログ ファイルにコピーします。

交換手順中に OKM を手動で回復する必要がある場合は、このバックアップ情報を必要になります。

- 管理者モードに戻る:

```
set -priv admin
```

- 障害のあるコントローラーを安全にシャットダウンし、シャットダウン手順に進むことができます。

す。

いずれかのキーに以下の値が表示されていない場合は `true` 復元された列に：

- オンボード キー マネージャーを同期します。

```
security key-manager onboard sync
```

プロンプトが表示されたら、32 文字の英数字のオンボード キー管理パスフレーズを入力します。



これは、オンボード キー マネージャーを最初に構成したときに作成したクラスタ全体のパスフレーズです。このパスフレーズがない場合は、NetAppサポートにお問い合わせください。

- すべての認証キーが復元されたことを確認します。

```
security key-manager key query
```

確認する Restored` 列表示 `true`、すべての認証キーと `Key Manager` タイプ表示 `onboard`。

- OKM 情報をバックアップします。

- 高度な権限モードに切り替える:

```
set -priv advanced
```

入力 `y` 続行するように求められた場合。

- キー管理のバックアップ情報を表示します。

```
security key-manager onboard show-backup
```

- バックアップ情報を別のファイルまたはログ ファイルにコピーします。

交換手順中に OKM を手動で回復する必要がある場合は、このバックアップ情報を必要になります。

- 管理者モードに戻る:

```
set -priv admin
```

- 障害のあるコントローラーを安全にシャットダウンし、シャットダウン手順に進むことができます。

次の手順

ブートメディアで暗号化キーのサポートとステータスを確認したら、を実行する必要があります "[コントローラをシャットダウン](#)"。

手動ブートメディアリカバリのためにコントローラをシャットダウンする - FAS50

手動ブート メディア回復プロセス中にデータの損失を防ぎ、システムの安定性を維持するために、FAS50 ストレージ システム内の障害のあるコントローラをシャットダウンします。

オプション 1：ほとんどのシステム

障害のあるコントローラをシャットダウンするには、コントローラのステータスを確認し、必要に応じて正常なコントローラが障害のあるコントロラストレージからデータを引き続き提供できるようにコントローラをテイクオーバーする必要があります。

このタスクについて

- SANシステムを使用している場合は、障害コントローラのSCSIブレードのイベントメッセージを確認しておく必要があります(`cluster kernel-service show`します)。コマンド (priv advancedモードから) を実行すると、`cluster kernel-service show`そのノードのノード名、そのノードの可用性ステータス、およびそのノードの動作ステータスが表示され"[クオーラムステータス](#)"ます。

各 SCSI ブレードプロセスは、クラスタ内の他のノードとクオーラムを構成している必要があります。交換を進める前に、すべての問題を解決しておく必要があります。

- ノードが 3 つ以上あるクラスタは、クオーラムを構成している必要があります。クラスタがクオーラムを構成していない場合、または正常なコントローラで適格性と正常性についてfalseと表示される場合は、障害のあるコントローラをシャットダウンする前に問題を修正する必要があります。を参照してください "[ノードをクラスタと同期します](#)"。

手順

1. AutoSupportが有効になっている場合は、AutoSupportメッセージを呼び出してケースの自動作成を停止します。

```
system node autosupport invoke -node * -type all -message MAINT=<# of hours>h
```

次のAutoSupport メッセージは、ケースの自動作成を2時間停止します。

```
cluster1:> system node autosupport invoke -node * -type all -message MAINT=2h
```

2. 自動ギブバックを無効にする:

- a. 正常なコントローラのコンソールから次のコマンドを入力します。

```
storage failover modify -node impaired_node_name -auto-giveback false
```

- b. 入力 y 「自動ギブバックを無効にしますか?」というプロンプトが表示されたら、

3. 障害のあるコントローラに LOADER プロンプトを表示します。

障害のあるコントローラの表示	作業
LOADER プロンプト	次の手順に進みます。
ギブバックを待っています	Ctrl キーを押しながら C キーを押し'プロンプトが表示されたら y と入力します

障害のあるコントローラの表示	作業
システムプロンプトまたはパスワードプロンプト	<p>正常なコントローラから障害コントローラをテイクオーバーまたは停止します。</p> <pre>storage failover takeover -ofnode impaired_node_name -halt true</pre> <p><code>_halt true</code> パラメータを指定すると、Loaderプロンプトが表示されます。</p>

オプション 2：コントローラが MetroCluster に搭載されている

障害のあるコントローラをシャットダウンするには、コントローラのステータスを確認し、必要に応じて正常なコントローラが障害のあるコントローラストレージからデータを引き続き提供できるようにコントローラをテイクオーバーする必要があります。

- ノードが 3 つ以上あるクラスタは、クオーラムを構成している必要があります。クラスタがクオーラムを構成していない場合、または正常なコントローラで適格性と正常性についてfalseと表示される場合は、障害のあるコントローラをシャットダウンする前に問題を修正する必要があります。を参照してください "[ノードをクラスタと同期します](#)"。
- MetroClusterの設定状態が「設定済み」になっていること、およびノードが有効かつ正常な状態であることを確認しておく必要があります。

```
metrocluster node show
```

手順

- AutoSupportが有効になっている場合は、AutoSupportメッセージを呼び出してケースの自動作成を停止します。

```
system node autosupport invoke -node * -type all -message
MAINT=number_of_hours_downh
```

次のAutoSupport メッセージは、ケースの自動作成を2時間停止します。

```
cluster1:> system node autosupport invoke -node * -type all -message
MAINT=2h
```

- 自動ギブバックを無効にする:

- 正常なコントローラのコンソールから次のコマンドを入力します。

```
storage failover modify -node local -auto-giveback false
```

- 入力 `y` 「自動ギブバックを無効にしますか?」というプロンプトが表示されたら、

- 障害のあるコントローラに LOADER プロンプトを表示します。

障害のあるコントローラの表示	作業
LOADER プロンプト	次のセクションに進みます。

障害のあるコントローラの表示	作業
ギブバックを待っています	Ctrl キーを押しながら C キーを押し、プロンプトが表示されたら y と入力します
システムプロンプトまたはパスワードプロンプト（システムパスワードの入力）	正常なコントローラから障害コントローラをテイクオーバーまたは停止します。 <pre>storage failover takeover -ofnode impaired_node_name -halt true</pre> _-halt true パラメータを指定すると、Loaderプロンプトが表示されます。

次の手順

コントローラをシャットダウンしたら、を実行する必要があり["ブートメディアの交換"](#)ます。

ブートメディアを交換し、手動ブートリカバリの準備をします - FAS50

FAS50システムのブートメディアには、重要なファームウェアと構成データが保存されています。交換プロセスでは、コントローラモジュールの取り外し、損傷したブートメディアの取り外し、交換用ブートメディアのインストール、そしてUSBフラッシュドライブを使用してONTAPイメージを交換用ブートメディアに手動で転送する必要があります。

このタスクについて

該当するプラットフォームの物理的な位置を特定するために、必要に応じてプラットフォームシャーシロケーション（青色）LEDを点灯できます。SSHを使用してBMCにログインし、コマンドを入力し `system location-led on` ます。

プラットフォームシャーシにはロケーションLEDが3つあります。1つはオペレータ用ディスプレイパネルに、もう1つは各コントローラにあります。ロケーションLEDは30分間点灯したままになります。

無効にするには、コマンドを入力し `system location-led off` ます。LEDが点灯しているか消灯しているかが不明な場合は、コマンドを入力して LED の状態を確認できます `system location-led show`。

手順 1：コントローラを取り外す

コントローラを交換するとき、またはコントローラ内部のコンポーネントを交換するときは、コントローラをシャーシから取り外す必要があります。

作業を開始する前に

ストレージシステムの他のすべてのコンポーネントが正常に動作していることを確認します。正常に動作していない場合は、この手順を続行する前にに連絡する必要があります ["ネットアップサポート"](#)。

手順

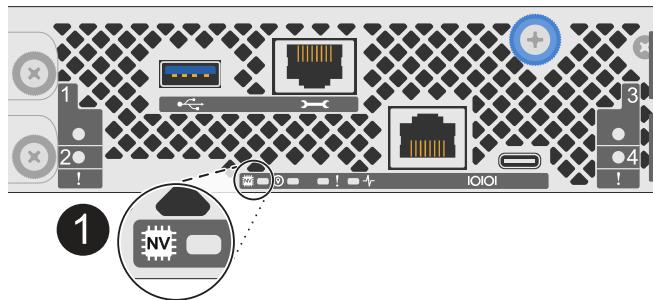
- 障害のあるコントローラで、NV LEDが消灯していることを確認します。

NV LEDが消灯するとデステージが完了し、障害のあるコントローラを安全に取り外すことができます。



NV LEDが緑色で点滅している場合は、デステージを実行中です。NV LEDが消灯するまで待つ必要があります。ただし、点滅が5分以上続く場合は、に連絡してからこの手順を続行してください "ネットアップサポート"。

NV LEDは、コントローラのNVアイコンの横にあります。



1

コントローラのNVアイコンとLED



設置およびメンテナンス手順中は、検証済みの接地点に接続された接地リストラップを常に着用してください。適切なESD予防措置に従わないと、コントローラーノード、ストレージシェルフ、およびネットワークスイッチに永久的な損傷が発生する可能性があります。

- 障害コントローラの電源を切断します。



電源装置 (PSU) には電源スイッチはありません。

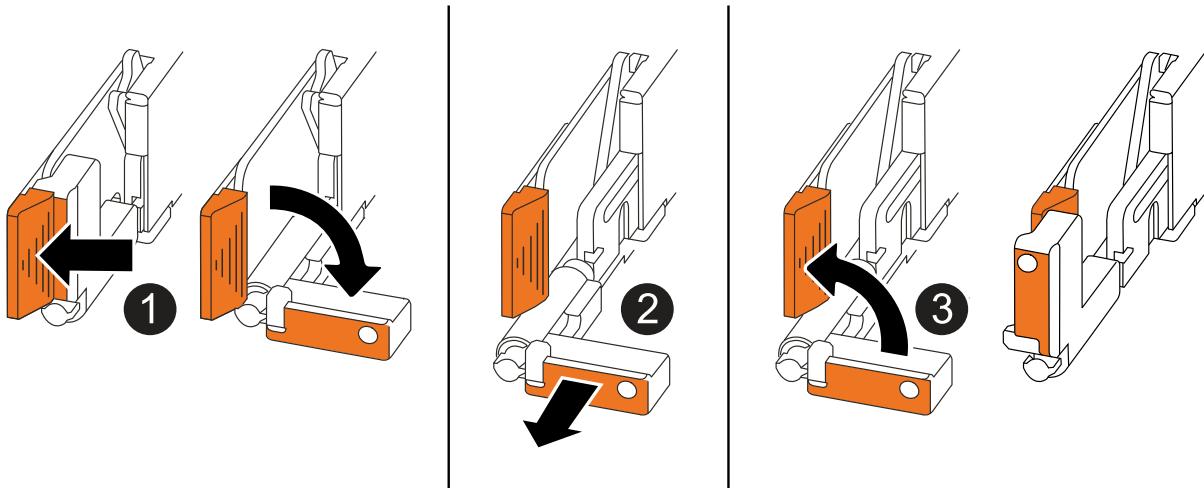
切断対象	作業
AC PSU	a. 電源コード固定クリップを開きます。 b. PSUから電源コードを抜き、脇に置きます。
DC PSU	a. D-SUB DC電源コードコネクタの2本の蝶ネジを外します。 b. PSUから電源コードを抜き、脇に置きます。

- 障害のあるコントローラからすべてのケーブルを取り外します。

ケーブルがどこに接続されていたかを記録します。

- 障害コントローラを取り外します。

次の図は、コントローラを取り外す際のコントローラハンドル（コントローラの左側から）の動作を示しています。



①	コントローラの両端で、垂直方向の固定ツメを外側に押してハンドルを外します。
②	<ul style="list-style-type: none"> ハンドルを手前に引いて、コントローラをミッドプレーンから外します。 引っ張ると、ハンドルがコントローラから引き出され、抵抗を感じて引っ張り続けます。 コントローラの底面を支えながらコントローラをシャーシから引き出し、平らで安定した場所に置きます。
③	必要に応じて、タブの横にあるハンドルを垂直に回転させて邪魔にならないようにします。

4. コントローラを帯電防止マットの上に置きます。
5. 取り付けネジを反時計回りに回して緩め、カバーを開きます。

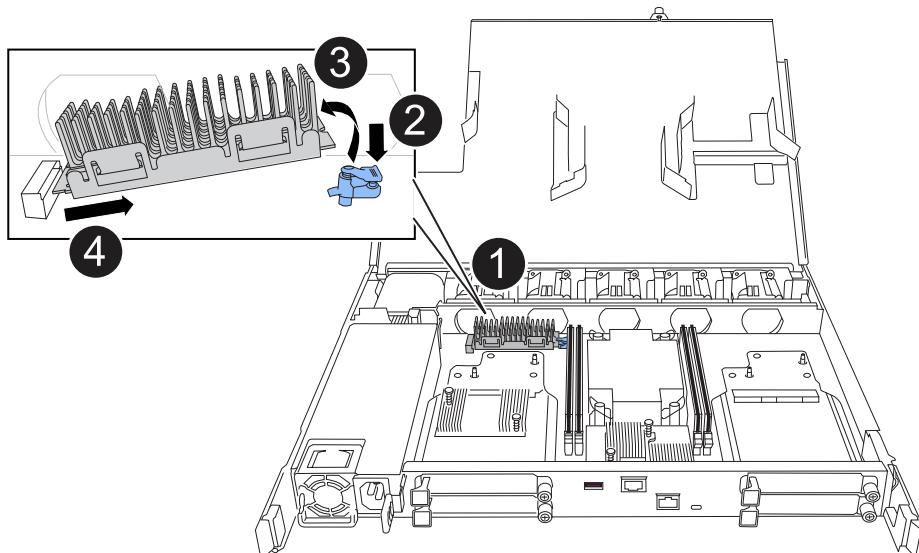
手順 2：ブートメディアを交換します

ブートメディアを交換するには、コントローラ内部でブートメディアの場所を確認し、特定の手順を実行します。



設置およびメンテナンス手順中は、検証済みの接地点に接続された接地リストラップを常に着用してください。適切なESD予防措置に従わないと、コントローラーノード、ストレージシェルフ、およびネットワークスイッチに永久的な損傷が発生する可能性があります。

1. ブートメディアを取り外します。



①	ブートメディアの場所
②	青いタブを押してブートメディアの右端を外します。
③	ブートメディアの右端を少し傾けて持ち上げ、ブートメディアの側面をしっかりとつかみます。
④	ブートメディアの左端をソケットからゆっくりと引き出します。

2. 交換用ブートメディアを取り付けます。

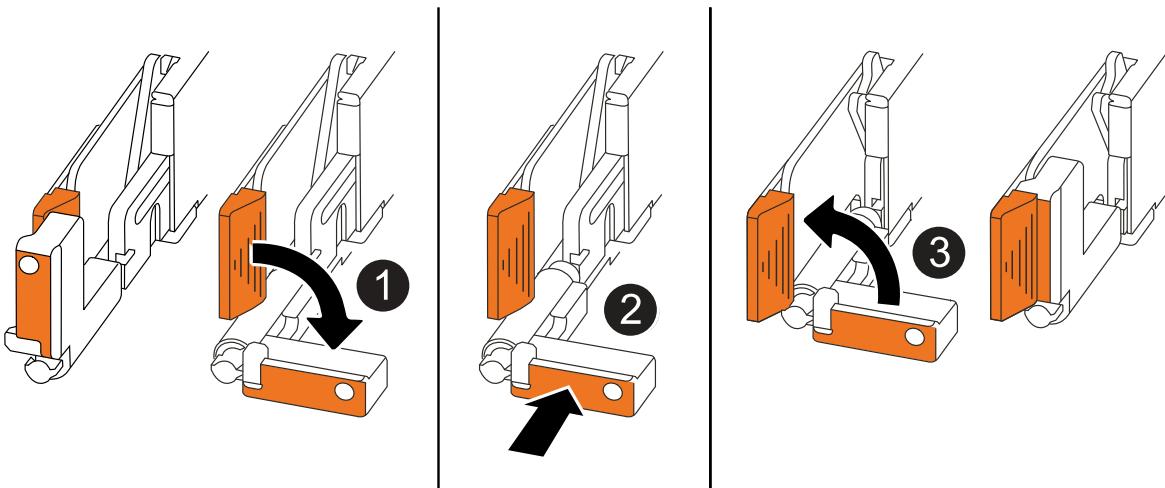
- パッケージからブートメディアを取り外します。
- ブートメディアのソケット側をソケットに挿入します。
- ブートメディアの反対側の端で、青いタブ（開いた状態）を押したまま、ブートメディアの端が止まるまでそっと押し下げ、タブを放してブートメディアを所定の位置にロックします。

手順 3：コントローラを再度取り付けます

コントローラをシャーシに再度取り付けますが、リブートは行わないでください。

このタスクについて

次の図は、コントローラを再取り付けする際のコントローラハンドル（コントローラの左側から）の動作を示しています。以降のコントローラの再取り付け手順の参考として使用できます。



1	作業中にコントローラのハンドルを垂直（タブの横）に回転させて邪魔にならない場所に移動した場合は、ハンドルを水平位置まで下に回転させます。
2	ハンドルを押してコントローラをシャーシに再度挿入し、指示が表示されたらコントローラが完全に装着されるまで押し込みます。
3	ハンドルを直立位置まで回転させ、ロックタブで所定の位置にロックします。

手順

1. コントローラのカバーを閉じ、固定されるまで取り付けネジを時計回りに回します。
2. コントローラをシャーシの途中まで挿入します。

コントローラの背面をシャーシの開口部に合わせ、ハンドルを使用してコントローラをそっと押し込みます。



この手順の後半で指示されるまで、コントローラをシャーシに完全に挿入しないでください。

3. ケーブルをコントローラに再接続します。ただし、この時点では電源装置（PSU）に電源コードを接続しないでください。



コントローラをシャーシに完全に装着してブートが開始されたときにブートメディアの交換手順の後半でブートシーケンスを確認して記録するため、コンソールケーブルがコントローラに接続されていることを確認してください。

手順 4：ブートイメージをブートメディアに転送します

取り付けた交換用ブートメディアにはONTAPイメージがないため、USBフラッシュドライブを使用してONTAPイメージを転送する必要があります。

作業を開始する前に

- FAT32 にフォーマットされた、4GB 以上の容量の USB フラッシュドライブが必要です。

- 障害コントローラで実行されていたバージョンのONTAPイメージのコピーが必要です。NetAppサポートサイトのセクションから該当するイメージをダウンロードできます。["ダウンロード"](#)
 - NVEがサポートされている場合は、NetApp Volume Encryptionを含むイメージをダウンロードします。
 - NVEがサポートされない場合は、NetAppボリューム暗号化なしのイメージをダウンロードします（ダウンロードボタンに表示されます）。
- コントローラのノード管理ポート（通常はe0Mインターフェイス）間にネットワーク接続が必要です。

手順

- 適切なサービスイメージをからUSBフラッシュドライブにダウンロードしてコピーし["ネットアップサポートサイト"](#)ます。
 - ページの[Downloads]リンクから、ラップトップのワークスペースにサービスイメージをダウンロードします。
 - サービスイメージを解凍します。



Windows を使用して内容を展開する場合は、winzip を使用してネットブートイメージを展開しないでください。7-Zip や WinRAR など、別の抽出ツールを使用します。

- USBフラッシュドライブに、障害のあるコントローラで実行されている適切なONTAPイメージが格納されている必要があります。
- USB フラッシュドライブをラップトップから取り外します。
- 障害のあるコントローラのUSB-AポートにUSBフラッシュドライブを挿入します。
- USB フラッシュドライブは、USB コンソールポートではなく、USB デバイス用のラベルが付いたスロットに取り付けてください。
- 障害のあるコントローラをシャーシに完全に挿入します。

- コントローラがミッドプレーンに接触して完全に装着されるまで、ハンドルをしっかりと押し込みます。



コントローラをシャーシに挿入する際に力を入れすぎないように注意してください。コネクタが破損する可能性があります。



コントローラをシャーシに完全に装着するとブートします。パートナーコントローラから電力を取得します。

- コントローラのハンドルを上に回転させ、タブで所定の位置に固定します。

- Ctrl+C キーを押してブートプロセスを中断し、LOADER プロンプトで停止します。

このメッセージが表示されない場合は、Ctrl+C キーを押し、メンテナンスマードでブートするオプションを選択してから、コントローラを停止して LOADER プロンプトを表示します。

- 障害のあるコントローラの電源装置（PSU）に電源コードを再接続します。

PSUへの電源が復旧すると、STATUS LEDがグリーンに点灯します。

再接続の対象	作業
AC PSU	<p>a. 電源コードをPSUに接続します。</p> <p>b. 電源コード固定クリップを使用して電源コードを固定します。</p>
DC PSU	<p>a. D-SUB DC電源コードコネクタをPSUに接続します。</p> <p>b. 2本の蝶ネジを締めて、D-SUB DC電源コードコネクタをPSUに固定します。</p>

次の手順

ブートメディアを交換したら、を行う必要があり["リカバリイメージのブート"](#)ます。

USB ドライブからの手動ブートメディアリカバリ - FAS50

FAS50ストレージシステムに新しいブートメディアデバイスをインストールした後、USB ドライブからリカバリ イメージを手動でブートして、パートナー ノードから構成を復元できます。

作業を開始する前に

- コンソールが障害のあるコントローラに接続されていることを確認します。
- リカバリイメージが保存された USB フラッシュ ドライブがあることを確認します。
- システムで暗号化が使用されているかどうかを判断します。暗号化が有効になっているかどうかに応じて、手順 3 で適切なオプションを選択する必要があります。

手順

- 障害のあるコントローラの LOADER プロンプトから、USB フラッシュ ドライブからリカバリ イメージを起動します。

`boot_recovery`

リカバリイメージは USB フラッシュ ドライブからダウンロードされます。

- プロンプトが表示されたら、画像の名前を入力するか、**Enter** キーを押して括弧内に表示されるデフォルトの画像を受け入れます。
- ONTAPバージョンの手順を使用して、var ファイル システムを復元します。

ONTAP 9.16.0 以前

障害のあるコントローラーとパートナー コントローラーで次の手順を実行します。

- 障害のあるコントローラーの場合: 押す Y`見ると `Do you want to restore the backup configuration now?
- 障害のあるコントローラーの場合: プロンプトが表示されたら、 Y /etc/ssh/ssh_host_ecdsa_key を上書きします。
- パートナー コントローラで: 障害のあるコントローラを高度な権限レベルに設定します。

```
set -privilege advanced
```

- パートナー コントローラで: 復元バックアップ コマンドを実行します。

```
system node restore-backup -node local -target-address
impaired_node_IP_address
```



復元成功以外のメッセージが表示された場合は、 NetAppサポートにお問い合わせください。

- パートナー コントローラで: 管理者レベルに戻ります:

```
set -privilege admin
```

- 障害のあるコントローラの場合: 押す Y`見ると `Was the restore backup procedure successful?
- 障害のあるコントローラの場合: 押す Y`見ると `...would you like to use this restored copy now?
- 障害のあるコントローラの場合: 押す `Y`再起動を求められたら、 `Ctrl-C`ブートメニューが表示されたら。
 - 障害のあるコントローラで: 次のいずれかを実行します。
 - システムで暗号化が使用されていない場合は、ブートメニューから [オプション 1 通常ブート] を選択します。
 - システムが暗号化を使用している場合は、 "アンコウカノ"。

ONTAP 9.16.1以降

障害のあるコントローラで次の手順を実行します。

- バックアップ設定の復元を求めるプロンプトが表示されたら、と入力し `Y` ます。

復元手順が成功すると、次のメッセージが表示されます。 syncflash_partner: Restore from partner complete

- プレス `Y` バックアップの復元が成功したかどうかを確認するプロンプトが表示されたら。
- プレス `Y` 復元された構成を使用するように求められた場合。
- プレス `Y` ノードを再起動するように求められた場合。

- e. プレス 'Y' 再起動を求められた場合は、'Ctrl-C' ブートメニューが表示されたら。
- f. 次のいずれかを実行します。
 - システムで暗号化が使用されていない場合は、ブートメニューから [オプション 1 通常ブート] を選択します。
 - システムが暗号化を使用している場合は、["アンコウカノ"](#)。

4. パートナーコントローラにコンソールケーブルを接続します。
5. コントローラのストレージをギブバックして、コントローラを通常動作に戻します。

```
storage failover giveback -fromnode local
```

6. 自動ギブバックを無効にした場合は、再度有効にします。

```
storage failover modify -node local -auto-giveback true
```

7. AutoSupportが有効になっている場合は、ケースの自動作成をリストアします。

```
system node autosupport invoke -node * -type all -message MAINT=END
```

次の手順

リカバリイメージを起動したら、を実行する必要があり["ブートメディアで暗号化をリストアする"](#)ます。

手動ブートリカバリ後の暗号化キーの復元 - FAS50

FAS50ストレージシステムの交換用ブートメディアで暗号化を復元し、データ保護を継続してください。交換プロセスでは、キーの可用性の確認、暗号化設定の再適用、データへの安全なアクセスの確認が行われます。

キー マネージャーの種類に応じて適切な手順を実行し、システムの暗号化を復元します。システムで使用されているキー マネージャーが不明な場合は、ブート メディアの交換手順の開始時にキャプチャした設定を確認してください。

オンボードキーマネージャ（OKM）

ONTAPブートメニューからオンボードキーマネージャ（OKM）設定をリストアします。

作業を開始する前に

次の情報を用意してください。

- ・クラスタ全体のパスフレーズを入力 "[オンボードキー管理の有効化](#)"
- ・"[オンボードキーマネージャのバックアップ情報](#)"
- ・正しいパスフレーズとバックアップデータがあることを確認するには、"[オンボードキー管理のバックアップとクラスタ全体のパスフレーズを検証する方法](#)"手順

手順

障害のあるコントローラーの場合:

1. コンソールケーブルを障害のあるコントローラーに接続します。
2. ONTAPブートメニューから適切なオプションを選択します。

ONTAP バージョン	このオプションを選択します。
ONTAP 9.8 以降	<p>オプション10を選択します。</p> <p>ブートメニューの例を表示します。</p> <div style="border: 1px solid black; padding: 10px; background-color: #f9f9f9;"><p>Please choose one of the following:</p><ul style="list-style-type: none">(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.<p>Selection (1-11)? 10</p></div>

ONTAP バージョン	このオプションを選択します。
ONTAP 9.7以前	<p>非表示オプションを選択します recover_onboard_keymanager</p> <p>ブートメニューの例を表示します。</p> <pre>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. Selection (1-19)? recover_onboard_keymanager</pre>

3. プロンプトが表示されたら、回復プロセスを続行することを確認します。

プロンプトの例を表示

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

4. クラスタ全体のパスフレーズを2回入力します。

パスフレーズを入力している間、コンソールに入力内容が表示されません。

プロンプトの例を表示

```
Enter the passphrase for onboard key management:
```

```
Enter the passphrase again to confirm:
```

5. バックアップ情報を入力します。

- a. ダッシュを含め、BEGIN BACKUP 行から END BACKUP 行までのコンテンツ全体を貼り付けます。

プロンプトの例を表示

Enter the backup data:

```
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
0123456789012345678901234567890123456789012345678901
23
1234567890123456789012345678901234567890123456789012
34
2345678901234567890123456789012345678901234567890123
45
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA

-----END
BACKUP-----
```

- b. 入力の最後に Enter キーを 2 回押します。

回復プロセスが完了し、次のメッセージが表示されます。

```
Successfully recovered keymanager secrets.
```

プロンプトの例を表示

```
Trying to recover keymanager secrets....  
Setting recovery material for the onboard key manager  
Recovery secrets set successfully  
Trying to delete any existing km_onboard.wkeydb file.  
  
Successfully recovered keymanager secrets.  
  
*****  
*****  
* Select option "(1) Normal Boot." to complete recovery process.  
*  
* Run the "security key-manager onboard sync" command to  
synchronize the key database after the node reboots.  
*****  
*****
```

+



表示された出力が以下の場合、続行しないでください。Successfully recovered keymanager secrets。トラブルシューティングを実行してエラーを修正します。

6. オプションを選択 `1` ブートメニューからONTAPのブートを続行します。

プロンプトの例を表示

```
*****
*****
* Select option "(1) Normal Boot." to complete the recovery
process.
*
*****
*****
(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)? 1
```

7. コントローラーのコンソールに次のメッセージが表示されていることを確認します。

```
Waiting for giveback...(Press Ctrl-C to abort wait)
```

パートナーコントローラーの場合:

8. 障害のあるコントローラーを返却します。

```
storage failover giveback -fromnode local -only-cfo-aggregates true
```

障害のあるコントローラーの場合:

9. CFO アグリゲートのみで起動した後、キー マネージャーを同期します。

```
security key-manager onboard sync
```

10. プロンプトが表示されたら、オンボード キー マネージャーのクラスター全体のパスフレーズを入力します。

プロンプトの例を表示

```
Enter the cluster-wide passphrase for the Onboard Key Manager:
```

All offline encrypted volumes will be brought online and the corresponding volume encryption keys (VEKs) will be restored automatically within 10 minutes. If any offline encrypted volumes are not brought online automatically, they can be brought online manually using the "volume online -vserver <vserver> -volume <volume_name>" command.



同期が成功すると、追加のメッセージなしでクラスター プロンプトが返されます。同期が失敗した場合、クラスター プロンプトに戻る前にエラー メッセージが表示されます。エラーが修正され、同期が正常に実行されるまで続行しないでください。

11. すべてのキーが同期されていることを確認します。

```
security key-manager key query -restored false
```

コマンドは結果を返さないはずです。結果が表示された場合は、結果が返されなくなるまで同期コマンドを繰り返します。

パートナーコントローラーの場合:

12. 障害のあるコントローラーを返却します。

```
storage failover giveback -fromnode local
```

13. 自動ギブバックを無効にした場合はリストアします。

```
storage failover modify -node local -auto-giveback true
```

14. AutoSupportが有効になっている場合は、ケースの自動作成をリストアします。

```
system node autosupport invoke -node * -type all -message MAINT=END
```

外部キーマネージャ (EKM)

ONTAP ブートメニューから外部キーマネージャの設定をリストアします。

作業を開始する前に

別のクラスター ノードまたはバックアップから次のファイルを収集します。

- `/cfcard/kmip/servers.cfg` ファイルまたはKMIPサーバーのアドレスとポート
- `/cfcard/kmip/certs/client.crt` ファイル (クライアント証明書)
- `/cfcard/kmip/certs/client.key` ファイル (クライアントキー)

- `/cfcard/kmip/certs/CA.pem` ファイル (KMIP サーバー CA 証明書)

手順

障害のあるコントローラーの場合:

1. コンソール ケーブルを障害のあるコントローラーに接続します。
2. オプションを選択 `11` ONTAP ブート メニューから。

ブートメニューの例を表示します。

```
(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)? 11
```

3. プロンプトが表示されたら、必要な情報を収集したことを確認します。

プロンプトの例を表示

```
Do you have a copy of the /cfcard/kmip/certs/client.crt file?
{y/n}
Do you have a copy of the /cfcard/kmip/certs/client.key file?
{y/n}
Do you have a copy of the /cfcard/kmip/certs/CA.pem file? {y/n}
Do you have a copy of the /cfcard/kmip/servers.cfg file? {y/n}
```

4. プロンプトが表示されたら、クライアントとサーバーの情報を入力します。

- a. BEGIN 行と END 行を含むクライアント証明書 (client.crt) ファイルの内容を入力します。
- b. BEGIN 行と END 行を含むクライアント キー (client.key) ファイルの内容を入力します。
- c. BEGIN 行と END 行を含む KMIP サーバー CA (CA.pem) ファイルの内容を入力します。
- d. KMIP サーバーの IP アドレスを入力します。
- e. KMIP サーバー ポートを入力します (デフォルトのポート 5696 を使用するには Enter キーを押します)。

例を示します

```
Enter the client certificate (client.crt) file contents:  
-----BEGIN CERTIFICATE-----  
<certificate_value>  
-----END CERTIFICATE-----  
  
Enter the client key (client.key) file contents:  
-----BEGIN RSA PRIVATE KEY-----  
<key_value>  
-----END RSA PRIVATE KEY-----  
  
Enter the KMIP server CA(s) (CA.pem) file contents:  
-----BEGIN CERTIFICATE-----  
<certificate_value>  
-----END CERTIFICATE-----  
  
Enter the IP address for the KMIP server: 10.10.10.10  
Enter the port for the KMIP server [5696]:  
  
System is ready to utilize external key manager(s).  
Trying to recover keys from key servers....  
kmip_init: configuring ports  
Running command '/sbin/ifconfig e0M'  
..  
..  
kmip_init: cmd: ReleaseExtraBSDPort e0M
```

回復プロセスが完了し、次のメッセージが表示されます。

Successfully recovered keymanager secrets.

例を示します

```
System is ready to utilize external key manager(s).  
Trying to recover keys from key servers....  
Performing initialization of OpenSSL  
Successfully recovered keymanager secrets.
```

5. オプションを選択`1`ブートメニューからONTAPのブートを続行します。

プロンプトの例を表示

```
*****
*****
* Select option "(1) Normal Boot." to complete the recovery
process.
*
*****
*****
(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)? 1
```

6. 自動ギブバックを無効にした場合はリストアします。

```
storage failover modify -node local -auto-giveback true
```

7. AutoSupportが有効になっている場合は、ケースの自動作成をリストアします。

```
system node autosupport invoke -node * -type all -message MAINT=END
```

次の手順

ブートメディアで暗号化をリストアしたら、を実行する必要があり["故障した部品をNetAppに返却します。"](#)ま
す。

障害が発生したパーティションをNetApp - FAS50に返却します。

FAS50システムのコンポーネントに障害が発生した場合は、障害が発生した部品
をNetAppに返却してください。["パーティションの返品と交換"詳細](#)については、ページを参照し
てください。

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隨時、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 5225.227-19（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。