



ブートメディア Install and maintain

NetApp
February 13, 2026

目次

ブートメディア	1
ブートメディアの交換の概要- FAS9000	1
暗号化キーのサポートおよびステータスの確認	1
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	1
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	2
障害のあるコントローラのシャットダウン- FAS9000	5
オプション 1：ほとんどのシステム	6
オプション 3：コントローラは 2 ノード MetroCluster に搭載されています	7
ブートメディアの交換- FAS9000	8
手順 1：コントローラを取り外す	8
手順 2：ブートメディアを交換します	10
手順 3：ブートイメージをブートメディアに転送します	11
リカバリイメージのブート- FAS9000	13
オプション1：ほとんどのシステムでリカバリイメージをブートする	13
オプション 2：2 ノード MetroCluster 構成でリカバリイメージをブートする	16
2ノードMetroCluster構成でのアグリゲートのスイッチバック- FAS9000	17
リストア暗号化- FAS9000	18
障害が発生したパーツをNetApp - FAS9000に返却します。	28

ブートメディア

ブートメディアの交換の概要- FAS9000

ブート メディアには、システムの起動時に使用されるプライマリおよびセカンダリのシステム (ブート イメージ) ファイル セットが保存されます。FAS9000システムは、手動のブート メディア回復手順のみをサポートします。自動ブート メディア リカバリはサポートされていません。

ブートメディアには、システムがブート時に使用するシステムファイル (ブートイメージ) のプライマリセットとセカンダリセットが格納されています。ネットワーク構成に応じて、無停止または停止を伴う交換を実行できます。

「image_xxx.tgz」を格納できる適切な容量のストレージを搭載した、FAT32 にフォーマットされた USB フラッシュドライブが必要です。

また ' この手順で後で使用するために 'image_xxx.tgz ファイルを USB フラッシュドライブにコピーする必要があります

- ブート・メディアを交換するための無停止かつ停止を伴う方法では 'var' ファイル・システムをリストアする必要があります
 - 無停止交換の場合 'HA ペアはネットワークに接続して 'var' ファイル・システムをリストアする必要はありません単一シャーシ内の HA ペアには内部 e0S 接続があり ' これを使用して 'var'config をそれらの間で転送します
 - 停止を伴う交換の場合 'var' ファイル・システムをリストアするためにネットワーク接続は必要ありませんが ' 再起動が 2 回必要です
- 障害が発生したコンポーネントは、プロバイダから受け取った交換用 FRU コンポーネントと交換する必要があります。
- 以下の手順のコマンドを正しいノードに適用することが重要です。
 - impaired_node は、保守を実行しているノードです。
 - Healthy node_name は、障害が発生したノードの HA パートナーです。

暗号化キーのサポートおよびステータスの確認

ストレージ システム上のデータ セキュリティを確保するには、ブート メディア上の暗号化キーのサポートとステータスを確認する必要があります。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、コントローラをシャットダウンする前にキー マネージャがアクティブかどうかを確認します。FAS9000システムは、手動のブート メディア回復手順のみをサポートします。自動ブート メディア リカバリはサポートされていません。

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

1. 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
```

出力にが含まれている場合、`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。

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：

- a. 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。

- b. 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。

- c. 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：

- a. OKM 情報をバックアップします。

- i. 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。

- i. 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
```

- ii. 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が必要になります。

- iii. 管理者モードに戻る：

```
set -priv admin
```

- b. 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：

- a. 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ー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。

- b. 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`。

- c. OKM 情報をバックアップします。

- i. 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。

- i. 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
```

- ii. 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が必要になります。

- iii. 管理者モードに戻る：

```
set -priv admin
```

- d. 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。

障害のあるコントローラーのシャットダウン- FAS9000

構成に適した手順を使用して、障害のあるコントローラーをシャットダウンするか、引き継ぎます。FAS9000システムは、手動のブート メディア回復手順のみをサポートしま

す。自動ブート メディア リカバリはサポートされていません。

オプション 1：ほとんどのシステム

NVE タスクまたは NSE タスクが完了したら、障害のあるコントローラをシャットダウンする必要があります。

手順

1. 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が表示された場合	作業
LOADER プロンプト	コントローラモジュールの取り外しに進みます。
ギブバックを待機しています	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）	<p>正常なコントローラから障害のあるコントローラをテイクオーバーまたは停止します。 <code>storage failover takeover -ofnode impaired_node_name</code></p> <p>障害のあるコントローラに「Waiting for giveback...」と表示されたら、Ctrl+C キーを押し、「y」と入力します。</p>

2. LOADER プロンプトで「printenv」と入力し、すべてのブート環境変数をキャプチャします。出力をログファイルに保存します。



ブートデバイスが壊れているか機能していない場合、このコマンドは機能しない可能性があります。

オプション 2：コントローラが **MetroCluster** に搭載されている

NVE タスクまたは NSE タスクを完了したら、障害ノードのシャットダウンを完了する必要があります。注：2 ノード MetroCluster 構成のシステムでは、この手順を使用しないでください。

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、クォーラムを構成する必要があります。クラスタがクォ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 構成を使用している場合は、MetroCluster 構成状態が構成済みで、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

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抑制

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`

2. 正常なコントローラのコンソールから自動ギブバックを無効にします。storage failover modify – node local-auto-giveback false
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
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）	<p>正常なコントローラから障害のあるコントローラをテイクオーバーまたは停止します。「storage failover takeover -ofnode impaired_node_name _</p> <p>障害のあるコントローラに「Waiting for giveback...」と表示されたら、Ctrl+C キーを押し、「y」と入力します。</p>

オプション 3：コントローラは 2 ノード **MetroCluster** に搭載されています

NVE タスクまたは NSE タスクを完了したら、障害ノードのシャットダウンを完了する必要があります。



2 ノード MetroCluster 構成のシステムでは、この手順を使用しないでください。

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、クォーラムを構成する必要があります。クラスタがクォ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 構成を使用している場合は、MetroCluster 構成状態が構成済みで、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

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抑制します。「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`

2. 正常なコントローラのコンソールから自動ギブバックを無効にします。 `storage failover modify – node local-auto-giveback false`
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
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）	<p>正常なコントローラから障害のあるコントローラをテイクオーバーまたは停止します。「 <code>storage failover takeover -ofnode impaired_node_name _</code></p> <p>障害のあるコントローラに「 <code>Waiting for giveback...</code> 」と表示されたら、Ctrl+C キーを押し、「 <code>y</code> 」と入力します。</p>

ブートメディアの交換- FAS9000

ブート メディアを交換するには、障害のあるコントローラ モジュールを取り外し、交換用のブート メディアをインストールし、ブート イメージを USB フラッシュドライブに転送する必要があります。FAS9000システムは、手動のブート メディア回復手順のみをサポートします。自動ブート メディア リカバリはサポートされていません。

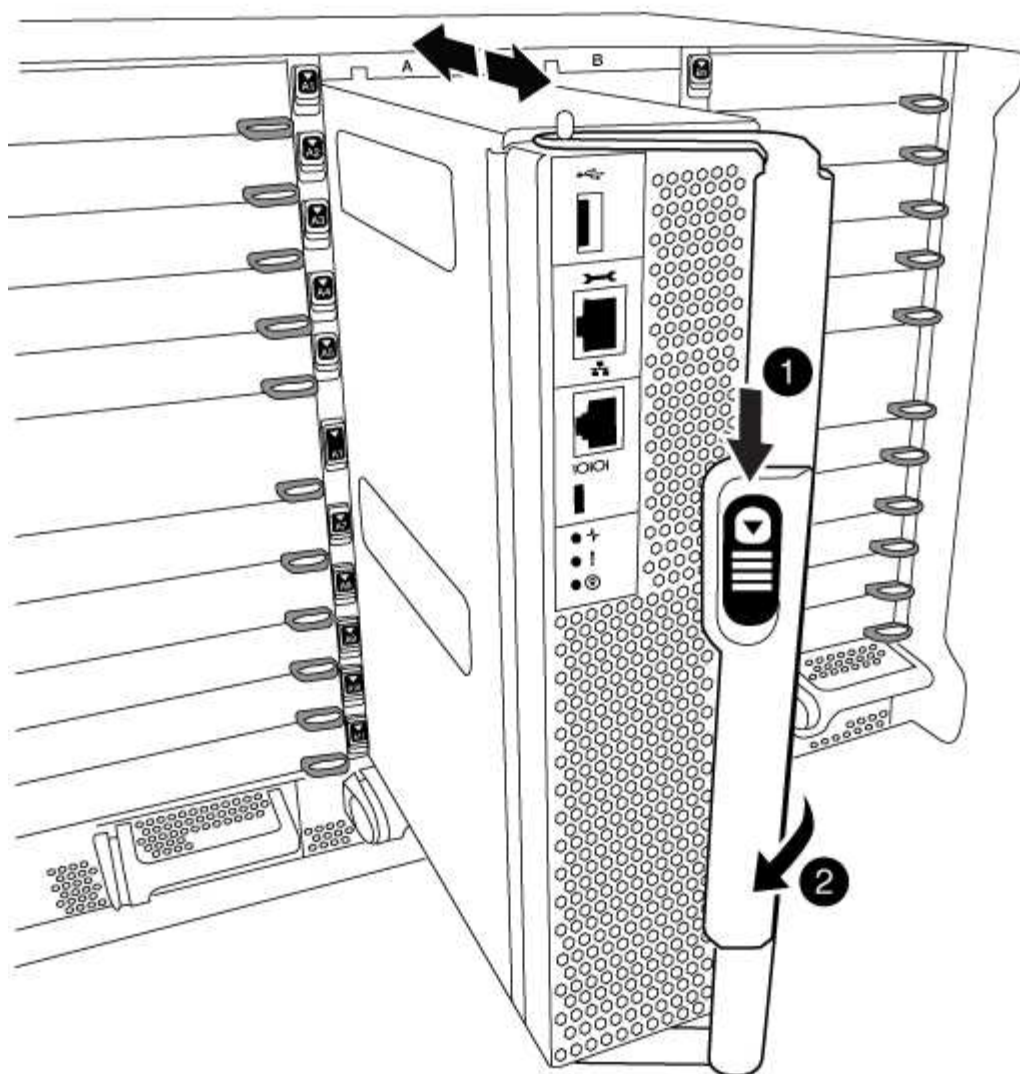
ブートメディアを交換するには、障害のあるコントローラモジュールを取り外し、交換用ブートメディアを取り付けて、ブートイメージを USB フラッシュドライブに転送する必要があります。

手順 1：コントローラを取り外す

コントローラ内部のコンポーネントにアクセスするには、まずコントローラモジュールをシステムから取り外し、続いてコントローラモジュールのカバーを外す必要があります。

手順

1. 接地対策がまだの場合は、自身で適切に実施します。
2. 障害のあるコントローラモジュールからケーブルを外し、どのケーブルが何に接続されていたかを記録します。
3. カムハンドルのオレンジ色のボタンを下にスライドさせてロックを解除します。



①

カムハンドルのリリースボタン

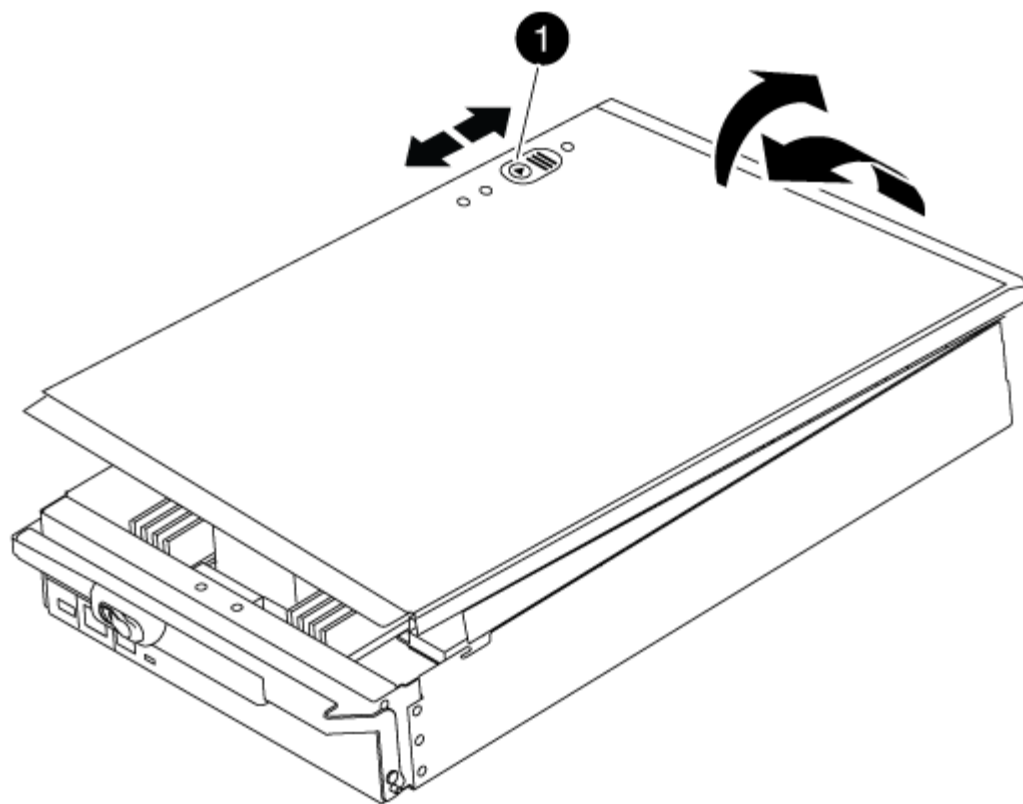
②

カムハンドル

4. カムハンドルを回転させて、コントローラモジュールをシャーシから完全に外し、コントローラモジュールをシャーシから引き出します。

このとき、空いている手でコントローラモジュールの底面を支えてください。

5. コントローラモジュールのふた側を上にして、平らで安定した場所に置きます。カバーの青いボタンを押し、コントローラモジュールの背面にカバーをスライドさせてから、カバーを上動かしてコントローラモジュールから外します。

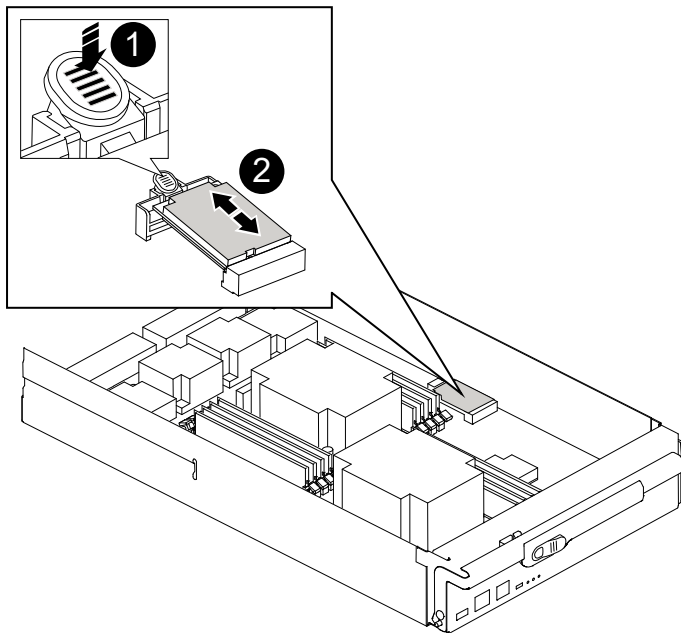


1

コントローラモジュールのカバーの固定ボタン

手順 2：ブートメディアを交換します

次の図またはコントローラモジュールの FRU マップを使用して、ブートメディアの場所を確認します。



1

リリースタブを押します

2

ブートメディア

1. ブートメディアケースの青いボタンを押してブートメディアをケースからリリースし、ブートメディアソケットからゆっくりと引き出します。



ソケットやブートメディアが損傷する可能性があるため、ブートメディアをねじったり、真上に引き出したりしないでください。

2. 交換用ブートメディアの端をブートメディアソケットに合わせ、ソケットにゆっくりと押し込みます。
3. ブートメディアが正しい向きでソケットに完全に装着されたことを確認します。

必要に応じて、ブートメディアを取り外してソケットへの装着をやり直します。

4. ブートメディアを押し下げて、ブートメディアケースの固定ボタンをはめ込みます。
5. コントローラモジュールのカバーにあるピンをマザーボードキャリアのスロットに合わせてカバーを再び取り付け、所定の位置に収まるまでスライドさせます。

手順 3：ブートイメージをブートメディアに転送します

イメージがインストールされた USB フラッシュドライブを使用して、交換用ブートメディアにシステムイメージをインストールできます。ただし、この手順の実行中に 'var' ファイル・システムをリストアする必要があります。

- 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。
- 障害のあるコントローラが実行していたバージョンの ONTAP イメージのコピー。該当するイメージは、ネットアップサポートサイトのダウンロードセクションからダウンロードできます
 - NVE が有効な場合は、ダウンロードボタンの指示に従って、NetApp Volume Encryption を使用してイメージをダウンロードします。
 - NVE が有効になっていない場合は、ダウンロードボタンの指示に従って、NetApp Volume Encryption なしでイメージをダウンロードします。
- スタンドアロン・システムの場合 ' ネットワーク接続は必要ありませんが 'var' ファイル・システムをリストアする場合は ' 追加の再起動を実行する必要があります

手順

1. コントローラモジュールの端をシャーシの開口部に合わせ、コントローラモジュールをシステムに半分までそっと押し込みます。
2. 必要に応じて、コントローラモジュールにケーブルを再接続します。
3. USB フラッシュドライブをコントローラモジュールの USB スロットに挿入します。

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。

4. コントローラモジュールをシステムに最後まで押し込み、カムハンドルの位置が USB フラッシュドライブに干渉していないことを確認します。カムハンドルを強く押し込んでコントローラモジュールを装着し、カムハンドルを閉じます。

ノードは、シャーシに完全に取り付けられるとすぐにブートを開始します。

5. ブートを開始するときに Ctrl+C キーを押し、ブートプロセスを中断して LOADER プロンプトで停止します。「Starting autoboot」というメッセージが表示されたら、Ctrl+C を押して中止します

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

6. LOADER プロンプトでネットワーク接続タイプを設定します。

- DHCP を構成している場合： `ifconfig e0a-auto`



設定するターゲットポートは、正常なノードから障害ノードへの通信に使用するターゲットポートで、ネットワーク接続を使用した /var/file system restore の実行時に指定します。このコマンドでは e0M ポートを使用することもできます。

- 手動接続を設定する場合は、「 `ifconfig e0a-addr= filer_addr-mask= netmask -gw= gateway -dns= dns_addr-domain= dns_domain'` 」のように入力します
 - `filer_addr` は、ストレージシステムの IP アドレスです。
 - `netmask` は、HA パートナーに接続されている管理ネットワークのネットワークマスクです。
 - `gateway` は、ネットワークのゲートウェイです。
 - `dns_addr` は、ネットワーク上のネームサーバの IP アドレスです。
 - `dns_domain` は、DNS ドメイン名です。

このオプションパラメータを使用する場合は、ネットブートサーバの URL に完全修飾ドメイン名を指定する必要はありません。必要なのはサーバのホスト名だけです。



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、詳細を確認できます。

7. コントローラがストレッチまたはファブリック接続の MetroCluster に含まれている場合は、FC アダプタの構成をリストアする必要があります。

- a. 保守モードでブート：`boot_ontap maint`
- b. MetroCluster ポートをイニシエータとして設定します。`ucadmin modify -m fc -t initiator adapter_name _``
- c. 停止して保守モードに戻ります：「halt」

変更はシステムのブート時に実装されます。

リカバリイメージのブート- FAS9000

障害のあるノードをリカバリ イメージから起動する手順は、システムが 2 ノードの MetroCluster 構成になっているかどうかによって異なります。FAS9000 システムは、手動のブート メディア回復手順のみをサポートします。自動ブート メディア リカバリはサポートされていません。

障害ノードをリカバリイメージからブートするための手順は、システムが 2 ノード MetroCluster 構成かどうかによって異なります。

オプション1：ほとんどのシステムでリカバリイメージをブートする

ONTAP イメージを USB ドライブからブートし、ファイルシステムをリストアして、環境変数を確認する必要があります。

この手順環境システムは 2 ノード MetroCluster 構成には含まれません。

手順

1. LOADER プロンプトから、USB フラッシュドライブ「boot_recovery」からリカバリ・イメージをブートします

イメージが USB フラッシュドライブからダウンロードされます。

2. プロンプトが表示されたら、イメージの名前を入力するか、画面に表示されたデフォルトのイメージをそのまま使用します。
3. var' ファイルシステムを復元します

システム構成	作業
ネットワーク接続	<ul style="list-style-type: none"> a. バックアップ構成を復元するかどうかを確認するメッセージが表示されたら 'y' を押します b. 正常なノードを advanced 権限レベルに設定します。「set -privilege advanced」 c. リストア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_name -' d. ノードを admin レベルに戻します。「set -privilege admin」 e. 復元された構成を使用するかどうかを確認するメッセージが表示されたら 'y' を押します f. ノードの再起動を求めるプロンプトが表示されたら 'y' を押します
ネットワーク接続がありません	<ul style="list-style-type: none"> a. バックアップ構成を復元するよう求められたら 'n' を押します b. プロンプトが表示されたら、システムをリブートします。 c. 表示されたメニューから「* Update flash from backup config * (sync flash)」オプションを選択します。 <p>更新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」を押します。</p>

システム構成	作業
ネットワークに接続されておらず、MetroCluster IP 構成になっています	<p>a. バックアップ構成を復元するよう求められたら 'n' を押します</p> <p>b. プロンプトが表示されたら、システムをリブートします。</p> <p>c. iSCSI ストレージ接続が確立されるまで待ちます。</p> <p>次のメッセージが表示されたら、次の手順に進みます。</p> <pre> date-and-time [node- name:iscsi.session.stateChanged:notice]: iSCSI session state is changed to Connected for the target iSCSI-target (type: dr_auxiliary, address: ip-address). date-and-time [node- name:iscsi.session.stateChanged:notice]: iSCSI session state is changed to Connected for the target iSCSI-target (type: dr_partner, address: ip-address). date-and-time [node- name:iscsi.session.stateChanged:notice]: iSCSI session state is changed to Connected for the target iSCSI-target (type: dr_auxiliary, address: ip-address). date-and-time [node- name:iscsi.session.stateChanged:notice]: iSCSI session state is changed to Connected for the target iSCSI-target (type: dr_partner, address: ip-address). </pre> <p>d. 表示されたメニューから「* Update flash from backup config * (sync flash)」オプションを選択します。</p> <p>更新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」を押します。</p>

4. 環境変数が正しく設定されていることを確認します。

- ノードに LOADER プロンプトを表示します。
- printenv コマンドを使用して ' 環境変数の設定を確認します
- 環境変数が正しく設定されていない場合は 'setenv_environment-variable-name__ changed-value_' コマンドで変更します
- 「savenv」コマンドを使用して、変更内容を保存します。

5. 次の手順は、システム構成によって異なります。

- システムにオンボードキーマネージャ、NSE、または NVE が設定されている場合は、に進みます [必](#)

要に応じて、OKM、NSE、NVE をリストアします

- 。システムにオンボードキーマネージャ、NSE、または NVE が設定されていない場合は、このセクションの手順を実行します。

6. LOADER プロンプトで「boot_ontap」コマンドを入力します。

* 表示内容	... *
ログインプロンプト	次の手順に進みます。
ギブバックを待っています	a. パートナーノードにログインします。 b. 「storage failover show」コマンドを使用して、ターゲットノードでギブバックの準備が完了していることを確認します。

7. パートナーノードにコンソールケーブルを接続します。

8. 「storage failover giveback -fromnode local」コマンドを使用してノードをギブバックします。

9. クラスタ・プロンプトで 'net int-is-home false' コマンドを使用して論理インターフェイスを確認します

"false" と表示されているインターフェイスがある場合は、net int revert コマンドを使用して、これらのインターフェイスをホームポートに戻します。

10. コンソールケーブルを修復されたノードに移動し、「version-v」コマンドを実行して ONTAP のバージョンを確認します。

11. 「storage failover modify -node local-auto-giveback true」コマンドを使用して自動ギブバックを無効にした場合は、自動ギブバックをリストアします。

オプション 2：2 ノード MetroCluster 構成でリカバリイメージをブートする

ONTAP イメージを USB ドライブからブートし、環境変数を確認する必要があります。

この手順環境システムは、2 ノード MetroCluster 構成です。

手順

1. LOADER プロンプトから、USB フラッシュドライブ「boot_recovery」からリカバリ・イメージをブートします

イメージが USB フラッシュドライブからダウンロードされます。

2. プロンプトが表示されたら、イメージの名前を入力するか、画面に表示されたデフォルトのイメージをそのまま使用します。

3. イメージがインストールされたら、リストアプロセスを開始します。

a. バックアップ構成を復元するよう求められたら 'n' を押します

b. 再起動を求めるプロンプトが表示されたら 'y' を押して '新しくインストールされたソフトウェアの使用を開始します

プロンプトが表示されたら、ブートプロセスを中断できるように準備しておく必要があります。

4. システムの起動時に 'Press Ctrl-C for Boot Menu' というメッセージが表示されたら 'Ctrl-C' を押します起動メニューが表示されたら 'Option 6' を選択します
5. 環境変数が正しく設定されていることを確認します。
 - a. ノードに LOADER プロンプトを表示します。
 - b. printenv コマンドを使用して '環境変数の設定を確認します
 - c. 環境変数が正しく設定されていない場合は 'setenv_environment-variable-name__ changed-value_' コマンドで変更します
 - d. 「savenv」コマンドを使用して、変更内容を保存します。
 - e. ノードをリブートします。

2 ノード MetroCluster 構成でのアグリゲートのスイッチバック-FAS9000

ブート メディアの交換が完了したら、MetroCluster スイッチバック操作を実行します。FAS9000 システムは、手動のブート メディア回復手順のみをサポートします。自動ブート メディア リカバリはサポートされていません。

このタスクでは、環境の 2 ノード MetroCluster 構成のみを実行します。

手順

1. すべてのノードの状態が「enabled」であることを確認します。 MetroCluster node show

```
cluster_B::> metrocluster node show
```

DR	Configuration	DR
Group Cluster Node	State	Mirroring Mode
1 cluster_A	controller_A_1 configured	enabled heal roots
completed cluster_B	controller_B_1 configured	enabled waiting for switchback recovery

2 entries were displayed.

2. すべての SVM で再同期が完了したことを確認します。「MetroCluster vserver show」
3. 修復処理によって実行される LIF の自動移行が正常に完了したことを確認します。 MetroCluster check lif show
4. サバイバークラスタ内の任意のノードから MetroCluster switchback コマンドを使用して、スイッチバックを実行します。
5. スイッチバック処理が完了したことを確認します MetroCluster show

クラスタの状態が waiting-for-switchback の場合は、スイッチバック処理がまだ実行中です。

```
cluster_B::> metrocluster show
Cluster              Configuration State      Mode
-----
Local: cluster_B configured          switchover
Remote: cluster_A configured          waiting-for-switchback
```

クラスタが「normal」状態のとき、スイッチバック処理は完了しています。

```
cluster_B::> metrocluster show
Cluster              Configuration State      Mode
-----
Local: cluster_B configured          normal
Remote: cluster_A configured          normal
```

スイッチバックが完了するまでに時間がかかる場合は、「MetroCluster config-replication resync-status show」コマンドを使用することで、進行中のベースラインのステータスを確認できます。

6. SnapMirror 構成または SnapVault 構成があれば、再確立します。

リストア暗号化- FAS9000

交換用ブート メディアで暗号化を復元します。FAS9000システムは、手動のブート メディア回復手順のみをサポートします。自動ブート メディア リカバリはサポートされていません。

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><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> <div> <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> </div>

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:

-----BEGIN

BACKUP-----

01234567890123456789012345678901234567890123456789012345678901

23

12345678901234567890123456789012345678901234567890123456789012

34

23456789012345678901234567890123456789012345678901234567890123

45

34567890123456789012345678901234567890123456789012345678901234

56

45678901234567890123456789012345678901234567890123456789012345

67

AA

AA

AA

AA

AA

AA

AA

AA

AA

AA

AA

AA

AA

AA

AA

AA

AA

AA

AA

AA

AA

AA

AA

AA

AA

AA

AA

AA

AA

```
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
01234567890123456789012345678901234567890123456789012345678901
23
12345678901234567890123456789012345678901234567890123456789012
34
23456789012345678901234567890123456789012345678901234567890123
45
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
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が、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
```

障害が発生したパーツをNetApp - FAS9000に返却します。

キットに同梱されている RMA 手順に従って、故障した部品をNetAppに返送してください。参照 ["パーツの返品と交換"](#) 詳細については、ページをご覧ください。FAS9000システムは、手動のブート メディア回復手順のみをサポートします。自動ブート メディアリカバリはサポートされていません。

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。