



# 手動

## Install and maintain

NetApp  
September 25, 2024

# 目次

手動 .....	1
ブートメディアの交換ワークフロー- ASA A70およびASA A90 .....	1
ブートメディアの交換要件- ASA A70およびASA A90 .....	1
オンボード暗号化キーの確認- ASA A70およびASA A90 .....	2
コントローラのシャットダウン- ASA A70およびASA A90 .....	3
ブートメディアの交換- ASA A70およびASA A90 .....	4
リカバリイメージのブート (ASA A70およびASA A90) .....	8
暗号化のリストア- ASA A70およびASA A90 .....	10
故障した部品をNetApp (ASA A70およびASA A90) に返却します。 .....	19

# 手動

## ブートメディアの交換ワークフロー- ASA A70およびASA A90

ブートメディアを交換するには、次のワークフロー手順を実行します。

1

"ブートメディア要件を確認"

ブートメディアを交換するには、一定の要件を満たす必要があります。

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"

障害のあるコントローラをシャットダウンまたはテイクオーバーして、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引き続きデータを提供できるようにします。

4

"ブートメディアの交換"

障害が発生したブートメディアをシステム管理モジュールから取り外し、交換用ブートメディアを取り付けてから、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"

ONATPブートメニューからオンボードキーマネージャの設定または外部キーマネージャをリストアします。

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。

## ブートメディアの交換要件- ASA A70およびASA A90

ブートメディアを交換する前に、次の要件を確認してください。

- 「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。
- この手順であとで使用できるように、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

image\_xxx.tgz。

- 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。
- これらの手順のコマンドを正しいコントローラに適用することが重要です。
  - `impaired_controller` は、メンテナンスを実行しているコントローラです。
  - `healthy_controller` は、障害のあるコントローラの HA パートナーです。

## オンボード暗号化キーの確認- ASA A70およびASA A90

障害のあるコントローラをシャットダウンしてオンボード暗号化キーのステータスを確認する前に、障害のあるコントローラのステータスを確認し、自動ギブバックを無効にして、実行中の ONTAP のバージョンを確認する必要があります。

ノードが3つ以上あるクラスタは、クォーラムを構成している必要があります。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](#)"。

### システムのNVEまたはNSEを確認する

障害のあるコントローラをシャットダウンする前に、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ディスクが暗号化されているかを確認する必要があります。

### セキュリティキー管理ツールの設定を確認

手順


1. `security key-manager keystore show_` コマンドを使用して、キー管理ツールがアクティブかどうかを確認します。詳細については、 "[security key-manager keystore showのマニュアルページ](#)"



他にもキー管理ツールのタイプがある場合があります。タイプは `KMIP`、`AKV`、および `GCP`` です。これらのタイプを確認するプロセスは、キー管理ツールのタイプを確認するプロセスと同じ ``external onboard` です。

- 出力が表示されない場合は、に進み、障害ノードをシャットダウンします "[障害コントローラをシャットダウン](#)"。
  - コマンドで出力が表示された場合は、システムがアクティブで `security key-manager` あるため、タイプとステータスを表示する必要があります `Key Manager` ます。
2. `security key-manager key query_` コマンド を使用して、アクティブな情報を表示します `Key Manager`。
    - タイプにと表示され、列にと表示されていれば、 `Key Manager external Restored `true`` 障害のあるコントローラを安全にシャットダウンできます。
    - タイプがと表示され、列にが表示された場合は `Key Manager onboard Restored true`、いくつかの手順を追加で実行する必要があります。
    - タイプがと表示され、列に以外の値が表示されている場合は `Key Manager external Restored true`、いくつかの手順を追加で実行する必要があります。

- タイプがと表示され、列に以外の値が表示されている場合は Key Manager onboard Restored true、いくつかの手順を追加で実行する必要があります。
3. タイプがと表示され、列にと表示された場合は Key Manager onboard Restored true、OKM情報を手動でバックアップします。
    - a. 続行するかどうかを尋ねられたら、と入力し y ます `set -priv advanced`
    - b. 次のコマンドを入力して、キー管理情報を表示します。 `security key-manager onboard show -backup`
    - c. バックアップ情報の内容を別のファイルまたはログファイルにコピーします。OKM は手動でリカバリする必要がある災害シナリオで必要になります。
    - d. 障害のあるコントローラを安全にシャットダウンできます。
  4. タイプがと表示され、列に次の以外が表示されている場合 Key Manager onboard Restored true :
    - a. onboard security key-manager syncコマンドを入力します。 `security key-manager onboard sync`

 プロンプトで、32文字のオンボードキー管理のパスフレーズを英数字で入力します。パスフレーズを指定できない場合は、NetAppサポートにお問い合わせください。  
"[mysupport.netapp.com](https://mysupport.netapp.com)"
    - b. すべての認証キーの列にと表示されていることを確認し Restored true ます。 `security key-manager key query`
    - c. タイプが表示されていることを確認し Key Manager onboard、OKM情報を手動でバックアップします。
    - d. 次のコマンドを入力して、キー管理バックアップ情報を表示します。 `security key-manager onboard show -backup`
    - e. バックアップ情報の内容を別のファイルまたはログファイルにコピーします。OKM は手動でリカバリする必要がある災害シナリオで必要になります。
    - f. コントローラは安全にシャットダウンできます。
  5. タイプがと表示され、列に次の以外が表示されている場合 Key Manager external Restored true :
    - a. 外部キー管理の認証キーをクラスタ内のすべてのノードにリストアします：「 `securitykey-manager external restore`

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 "[mysupport.netapp.com](https://mysupport.netapp.com)".
    - b. すべての認証キーの列にと表示されていることを確認します Restored true 。 `security key-manager key query`
    - c. 障害のあるコントローラを安全にシャットダウンできます。

## コントローラのシャットダウン- ASA A70およびASA A90

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。障害のあるコントローラをシャットダウンするかテイクオーバーします。

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。

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`ます)。コマンド (priv advancedモードから) を実行すると、`cluster kernel-service show ノード名、そのノードのクォーラムステータス、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ォ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、クォーラムを構成している必要があります。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](#)"。

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. 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



自動ギブバックを無効にしますか?\_と表示されたら'y'を入力します

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	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 _  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。

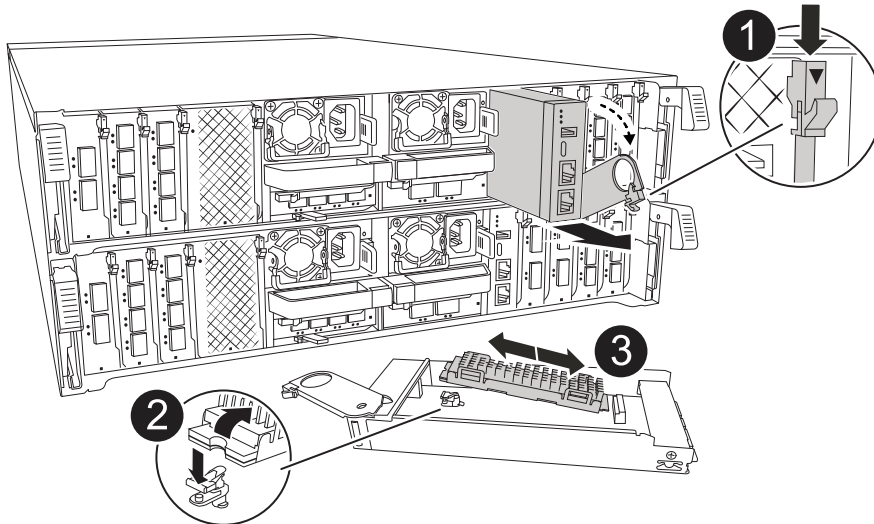
## ブートメディアの交換- ASA A70およびASA A90

ブートメディアを交換するには、システムの背面からシステム管理モジュールを取り外

し、障害のあるブートメディアを取り外して、交換用ブートメディアをシステム管理モジュールに取り付ける必要があります。

### 手順 1：ブートメディアを交換します

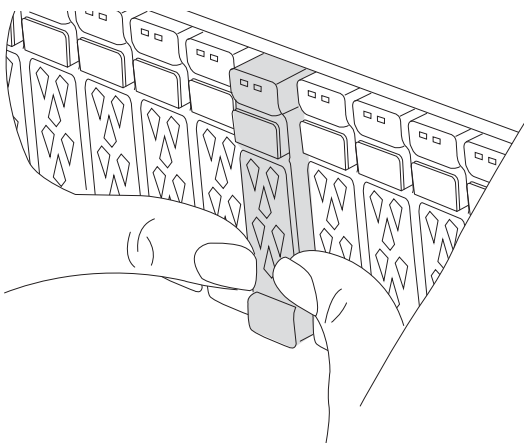
ブートメディアはシステム管理モジュールの内部にあり、モジュールをシステムから取り外すとアクセスできます。



	システム管理モジュールのカムラッチ
	ブートメディアロックボタン
	ブートメディア

1. シャーシの前面で、プラスのストッパーになるまで、親指で各ドライブをしっかりと押し込みます。これ

により、ドライブがシャーシのミッドプレーンにしっかりと装着されます。



2. シャーシの背面に移動します。接地対策がまだの場合は、自身で適切に実施します。
3. コントローラモジュールを約3インチ引き出して、コントローラモジュールの電源を切断します。
  - a. コントローラモジュールの両方のロックラッチを押し下げ、両方のラッチを同時に下に回転させます。
  - b. コントローラモジュールをシャーシから約3インチ引き出して、電源を外します。
  - c. システム管理モジュールに接続されているケーブルをすべて取り外します。モジュールを再度取り付けるときに正しいポートにケーブルを接続できるように、ケーブルが接続されていた場所にラベルを付けてください。
  - d. ケーブルマネジメントトレイ内部の両側にあるボタンを引いてケーブルマネジメントトレイを下に回転させ、トレイを下に回転させます。
  - e. システム管理カムボタンを押します。カムレバーがシャーシから離れます。
  - f. カムレバーを完全に下に回転させ、システム管理モジュールをコントローラモジュールから取り外します。
  - g. システム管理モジュールを静電気防止用マットの上に置き、ブートメディアにアクセスできるようにします。
4. 管理モジュールからブートメディアを取り外します。
  - a. 青色のロックボタンを押します。
  - b. ブートメディアを上回転させ、ソケットから引き出して脇に置きます。
5. 交換用ブートメディアをシステム管理モジュールに取り付けます。
  - a. ブートメディアの端をソケットケースに合わせ、ソケットに対して垂直にゆっくりと押し込みます。
  - b. ブートメディアをロックボタンの方に回転させます。
  - c. 固定ボタンを押し、ブートメディアを最後まで回転させて固定ボタンを放します。
6. システム管理モジュールを取り付け直します。
  - a. ケーブルマネジメントトレイを上回転させて閉じます。
  - b. システム管理モジュールにケーブルを再接続します。



## 手順 2 : 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）。
- HAペアのシステムの場合は、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を確立する必要があります。

手順

1. 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。
  - a. 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。
  - b. 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。

- c. 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。
2. USBフラッシュドライブをシステム管理モジュールのUSB-Aポートに挿入します。

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。

3. コントローラモジュールに電源を再接続します。
  - a. コントローラモジュールをシャーシに挿入し、ミッドプレーンまでしっかりと押し込んで完全に装着します。

コントローラモジュールが完全に装着されると、ロックラッチが上がります。

- b. ロックラッチを上方向に回してロック位置にします。

コントローラは、システムに電源を再接続するとすぐにブートを開始します。

4. 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、メンテナンスモードでブートするオプション

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。

#### 5. 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を設定する場合：`ifconfig e0M -auto`



設定するターゲットポートは、正常なコントローラから障害コントローラへの通信に使用するポートで、var ファイルシステムのリストア時にネットワーク接続で使用します。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：`ifconfig e0M -addr=filer_addr -mask=netmask -gw=gateway`
  - `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。



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。詳細については、ファームウェアのプロンプトで「`help ifconfig`」と入力してください。

## リカバリイメージのブート (ASA A70およびASA A90)

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。

### 手順

1. LOADERプロンプトで、USBフラッシュドライブからリカバリイメージをブートします。`boot_recovery` 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。

システムで実行しているバージョン	作業
ONTAP 9.16.0 以前	<p>a. 障害コントローラで、次のメッセージが表示されたら <code>_Y_</code> を押します。Do you want to restore the backup configuration now?</p> <p>b. 障害コントローラで、上書きするかどうかを確認するメッセージが表示されたら <code>_Y_</code> を押します  <code>/etc/ssh/ssh_host_ecdsa_key</code>。</p> <p>c. 正常なパートナーコントローラで、障害コントローラを advanced 権限レベルに設定します。<code>_set -privilege advanced _</code>。</p> <p>d. 正常なパートナーコントローラで、restore backup コマンド <code>_system node restore -backup -node local-target-address impaired_node_IP_address_</code> を実行します。</p> <p>*注：*リストアが正常に完了した以外のメッセージが表示された場合は、にお問い合わせください <a href="#">"ネットアップサポート"</a>。</p> <p>e. 正常なパートナーコントローラで、障害のあるコントローラを admin レベルに戻します。<code>set -privilege admin</code>。</p> <p>f. 障害コントローラで、というメッセージが表示されたら、<code>_y_</code> を押します Was the restore backup procedure successful?。</p> <p>g. 障害コントローラで、というメッセージが表示されたら、<code>_y_</code> を押します ...would you like to use this restored copy now?。</p> <p>h. 障害コントローラで、障害コントローラのリブートを求めるプロンプトが表示されたら <code>_y_</code> を押し、ブートメニューとして <code>_Ctrl+C_</code> を押します。</p> <p>i. システムで暗号化が使用されていない場合は、<code>_option 1 Normal Boot</code> を選択します。使用されていない場合は、に進みます。"<a href="#">キー管理ツールのリストア</a>"</p> <p>j. 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。</p> <p>k. <code>storage failover giveback -fromnode local_</code> コマンドを使用してコントローラをギブバックします。</p> <p>l. 自動ギブバックを無効にした場合は、<code>_storage failover modify -node local-auto-giveback true_</code> コマンドを使用してリストアします。</p> <p>m. AutoSupport が有効になっている場合は、<code>_system node AutoSupport invoke -node *-type all -message MAINT=end_command</code> を使用して、ケースの自動作成をリストアまたは抑制解除します。</p> <p>*注意：*プロセスが失敗した場合は、ご連絡してください <a href="#">"ネットアップサポート"</a>。</p>

システムで実行しているバージョン	作業
ONTAP 9.16.1以降	<p>a. 障害コントローラで、バックアップ構成をリストアするかどうかを確認するメッセージが表示されたら、<code>_y_</code>を押します。</p> <p>リストア手順が正常に完了すると、コンソールにこのメッセージが表示されます <code>syncflash_partner: Restore from partner complete.</code></p> <p>b. 障害のあるコントローラで、リストアバックアップ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、<code>_y_</code>を押します。</p> <p>c. 障害コントローラで、リストアし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、<code>_y_</code>を押します。</p> <p>d. 障害コントローラで、ノードをリブートするように求められたら、<code>_y_</code>を押します。</p> <p>e. 障害コントローラで、障害コントローラのリブートを求めるプロンプトが表示されたら <code>_y_</code> を押し、ブートメニューとして <code>_Ctrl+C_</code> を押します。</p> <p>f. システムで暗号化が使用されていない場合は、<code>_option 1 Normal Boot</code> を選択します。使用されていない場合は、に進みます。"<a href="#">キー管理ツールのリストア</a>"</p> <p>g. 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。</p> <p>h. <code>storage failover giveback -fromnode local_</code> コマンドを使用してコントローラをギブバックします。</p> <p>i. 自動ギブバックを無効にした場合は、<code>_storage failover modify -node local-auto-giveback true_</code> コマンドを使用してリストアします。</p> <p>j. AutoSupportが有効になっている場合は、<code>_system node AutoSupport invoke -node *-type all -message MAINT=end_</code> commandを使用して、ケースの自動作成をリストアまたは抑制解除します。</p> <p>*注意：*プロセスが失敗した場合は、に連絡してください "<a href="#">ネットアップサポート</a>"。</p>

## 暗号化のリストア- ASA A70およびASA A90

交換用ブートメディアで暗号化をリストアします。

### 手順1：オンボードキーマネージャをリストアする

この手順で最初を取得した設定を使用して、オンボードキーマネージャ（OKM）、NetAppストレージ暗号化（NSE）、またはNetAppボリューム暗号化（NVE）が有効になっているシステムに固有の手順を実行する必要があります。



オンボードまたは外部のキーマネージャと一緒にNSEまたはNVEが有効になっている場合は、この手順の最初に取得した設定をリストアする必要があります。

#### 手順

1. コンソールケーブルをターゲットコントローラに接続します。
2. 次のいずれかのオプションを選択して、ONATPブートメニューからオンボードキーマネージャの設定をリストアします。

## オプション1：オンボードキーマネージャサーバ構成のシステム

ONATPブートメニューからオンボード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

OKM設定をリストアするには、次の情報が必要です。

- クラスタ全体のパスフレーズが入力されました "オンボードキー管理の有効化時"。
- "オンボードキーマネージャのバックアップ情報"です。
- 続行する前に手順を実行して "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" ください。

手順

1. ONTAPのブートメニューからオプション10を選択します。

```
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
```

2. プロセスの継続を確認してください。`This option must be used only in disaster recovery procedures. Are you sure? (y or n):`y
3. クラスタ全体のパスフレーズを2回入力します。



パスフレーズの入力中、コンソールに入力内容は表示されません。

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

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

4. バックアップ情報を入力します。BEGIN BACKUP行からEND BACKUP行まで、すべての内容を貼り付けます。

入力の最後にあるENTERキーを2回押します。



```
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外の場合は、先に進まない `Successfully recovered keymanager secrets` でください。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. ブートメニューからオプション1を選択して、ONTAPのブートを続行します。

```
*****
*****
* 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. コントローラのコンソールに Waiting for giveback...(Press Ctrl-C to abort wait)



8. パートナーノードから、パートナーコントローラをギブバックします。 `storage failover giveback -fromnode local-only-cfo-aggregates true`
9. CFOアグリゲートでのみ起動したら、`_security key-manager onboard sync`コマンドを実行します。
10. オンボードキーマネージャのクラスタ全体のパスフレーズを入力します。

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.

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`

There are no entries matching your query.



restoredパラメータでfalseをフィルタする場合、結果は表示されません。

12. パートナーからのノードのギブバック: `storage failover giveback -fromnode local`

オプション2: 外部キー管理サーバが設定されたシステム

ONATPブートメニューから外部キー管理ツールの設定をリストアします。

作業を開始する前に

外部キー管理ツール (EKM) の設定をリストアするには、次の情報が必要です。

- 別のクラスタノードから/cfcard/kmip/servers.cfgファイルのコピー、または次の情報が必要です。
- KMIPサーバのアドレス。
- KMIPポート。
- 別のクラスタノードの/cfcard/kmip/certs/client.crtファイルのコピー、またはクライアント証明書。
- 別のクラスタノードからの/cfcard/kmip/certs/client.keyファイルのコピー、またはクライアントキー。
- 別のクラスタノード (KMIPサーバCA) の/cfcard/kmip/certs/CA.pemファイルのコピー。

手順

1. ONTAPのブートメニューからオプション11を選択します。

```
(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
```

2. 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。

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

代わりに次のプロンプトを使用することもできます。

- e. Do you have a copy of the /cfcard/kmip/servers.cfg file? {y/n} *n*
  - i. Do you know the KMIP server address? {y/n} *y*
  - ii. Do you know the KMIP Port? {y/n} *y*

3. 次の各プロンプトの情報を入力します。

- a. Enter the client certificate (client.crt) file contents:
- b. Enter the client key (client.key) file contents:
- c. Enter the KMIP server CA(s) (CA.pem) file contents:
- d. Enter the server configuration (servers.cfg) file contents:

## Example

Enter the client certificate (client.crt) file contents:

```
-----BEGIN CERTIFICATE-----
MIIDvjCCAqagAwIBAgICN3gwDQYJKoZIhvcNAQELBQAwwY8xCzAJBgNVBAYTA1VT
MRMwEQYDVQQIEwpDYWxpZm9ybmlhMQwwCgYDVQQHEwNTVkwxDzANBgNVBAoTBk51
MSUubQusvzAFs8G3P54GG32iIRvaCFnj2gQpCxcilJ0qB2foiBGx5XVQ/Mtk+rlap
Pk4ECW/wqSOUXDYtJs1+RB+w0+SHx8mzxpbz3mXF/X/1PC3YOzVNCq5eieek62si
Fp8=
-----END CERTIFICATE-----
```

Enter the client key (client.key) file contents:

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAoUleajEG6QC2h2Zih0jEaGVtQUexNeoCFwKPoMSePmjDNtrU
MSB1SlX3VgCuElHk57XPdq6xSbYlBkIb4bAgLztHEmUDOkGmXYAkblQ=
-----END RSA PRIVATE KEY-----
```

Enter the KMIP server CA(s) (CA.pem) file contents:

```
-----BEGIN CERTIFICATE-----
MIIEIzCCA3OgAwIBAgIBADANBgkqhkiG9w0BAQsFADCBjzELMAkGA1UEBhMVCVMx
7yaumMQETNrpMfP+nQMd34y4AmseWYGM6qG0z37BRnYU0Wf2qDL61cQ3/jkm7Y94
EQBKG1NY8dVyjphmYZv+
-----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
```

## 4. リカバリプロセスが完了します。

```
System is ready to utilize external key manager(s).
Trying to recover keys from key servers....
[Aug 29 21:06:28]: 0x808806100: 0: DEBUG: kmip2::main:
[initOpenssl]:460: Performing initialization of OpenSSL
Successfully recovered keymanager secrets.
```

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

```

*****
*****
* 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

```

**手順2：ブートメディアの交換が完了します。**

通常のブート後に最終チェックを実行してストレージをギブバックし、ブートメディアの交換プロセスを完了します。

1. コンソールの出力を確認します。

| コンソールに表示される内容 | 作業                                                                                                                                                                       |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ログインプロンプト     | 手順6に進みます。                                                                                                                                                                |
| ギブバックを待っています  | <ul style="list-style-type: none"> <li>a. パートナーコントローラにログインします。</li> <li>b. <code>storage failover show_</code> コマンドを使用して、ターゲットコントローラでギブバックの準備が完了していることを確認します。</li> </ul> |

2. 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、`_storage failover giveback -fromnode local-only -cfo-aggregates true_` コマンドを使用してターゲットコントローラストレージをギブバックします。

- ディスク障害のためにコマンドが失敗した場合は、ディスクを物理的に取り外します。ただし、交換用のディスクを受け取るまでは、ディスクをスロットに残しておきます。
- パートナーの準備ができていないためにコマンドが失敗した場合は、HAサブシステムがパートナー間

で同期されるまで5分待ちます。

- NDMP、SnapMirror、または SnapVault のプロセスが原因でコマンドが失敗する場合は、そのプロセスを無効にします。詳細については、該当するドキュメントセンターを参照してください。

- 3分待ってから、`_storage failover show_` コマンドを使用してフェイルオーバーステータスを確認します。
- clustershellプロンプトで `_network interface show -is-home false_` commandを入力して、ホームコントローラおよびポートにない論理インターフェイスを一覧表示します。

と表示されるインターフェイスがある場合は `false_`、`_net int revert -vserver Cluster -lif_nodename_` コマンドを使用して、それらのインターフェイスをホームポートに戻します。

- ターゲットコントローラにコンソールケーブルを接続し、`_version -v_` コマンドを実行してONTAPのバージョンを確認します。
- を使用し `storage encryption disk show` で出力を確認します。
- `security key-manager key query_` コマンド を使用して、キー管理サーバに格納されている認証キーのキーIDを表示します。
  - リストアされたカラム = 'yes/true' の場合は '終了し' 交換プロセスを完了することができます
  - =と列が以外の場合 `Key Manager type external Restored `yes/true`` は、`_security key-manager external restore_` commandを使用して認証キーのキーIDをリストアします。



コマンドが失敗した場合は、カスタマーサポートにお問い合わせください。

- =と列が以外の場合 `Key Manager type onboard Restored `yes/true`` は、`_security key-manager onboard sync_` コマンドを使用して、修復されたノードで不足しているオンボードキーを同期します。

`security key-manager key query_` commandを使用して、すべての認証キーの列が=であることを確認します `Restored yes/true` 。

- 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。
- `storage failover giveback -fromnode local` コマンドを使用して、コントローラをギブバックします。
- 自動ギブバックを無効にした場合は、`_storage failover modify -node local-auto-giveback true_` コマンドを使用してリストアします。
- AutoSupportが有効になっている場合は、`_system node AutoSupport invoke -node *-type all -message MAINT=end_` commandを使用して、ケースの自動作成をリストアまたは抑制解除します。

## 故障した部品をNetApp (ASA A70およびASA A90) に返却します。

障害が発生したパーツは、キットに付属のRMA指示書に従ってNetAppに返却してください。"[パーツの返品と交換](#)"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 © 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。