ブートメディア
Install and maintain

NetApp
September 25, 2024

目次

ブートメディア

ブートメディアの交換ワークフロー- FAS70およびFAS90

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. "ブートメディアの交換要件の確認"

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- FAS70およびFAS90

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- FAS70およびFAS90

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"。

NVEまたはNSEの確認

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 Key Manager ます。
2. security key-manager key query_コマンド を使用して、アクティブなの情報を表示します 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"

   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"。

   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。

障害のあるコントローラ **FAS70** および **FAS90** をシャットダウンします

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。構成に応じた適切な手順 を使用して、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 `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。

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"。
- 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。

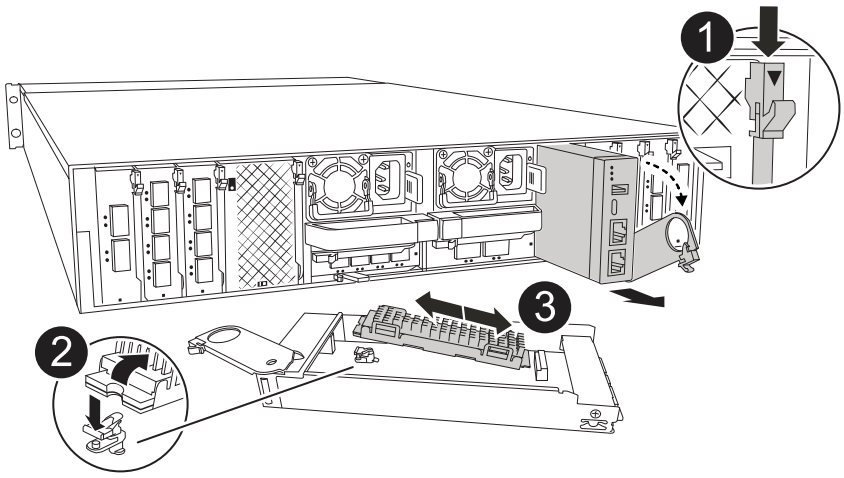
障害のあるコントローラの表示	作業
LOADER プロンプト	次の手順に進みます。
ギブバックを待っています	Ctrl キーを押しながら C キーを押し ' プロンプトが表示されたら y と入力します
システムプロンプトまたはパスワードプロンプト（システムパスワードの入力）	正常なコントローラから障害のあるコントローラをテイクオーバーまたは停止します。「 storage failover takeover -ofnode impaired_node_name _ 障害のあるコントローラに「 Waiting for giveback… 」と表示されたら、 Ctrl+C キーを押し、「 y 」と入力します。

ブートメディア - **FAS70** および **FAS90** を交換します

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、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。



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

1. 接地対策がまだの場合は、自身で適切に実施します。
2. コントローラからPSUから電源装置ケーブルを抜きます。

ストレージシステムにDC電源装置が搭載されている場合は、電源装置（PSU）から電源ケーブルブロックを外します。

a. 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、ケーブルの接続先にラベルを付けておいてください。

b. 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。

c. システム管理カムボタンを押します。

d. カムラッチをできるだけ下に回転させます。

e. カムレバーの開口部に指をはさみ、モジュールをエンクロージャから引き出して、システム管理モジュールをエンクロージャから取り外します。

f. 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。

3. 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に回転させ、ソケットから引き出して脇に置きます。

4. 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。

5. システム管理モジュールを取り付け直します。

a. モジュールをエンクロージャスロット開口部の端に合わせます。

b. モジュールをスロットにゆっくりと挿入してエンクロージャの奥まで押し込み、カムラッチを上に回転させてモジュールを所定の位置にロックします。

6. ケーブルマネジメントトレイを上に回転させて閉じます。

a. 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：ONTAPイメージをブートメディアに転送する

取り付けた交換用ブートメディアにONTAPイメージがない場合は、適切なONTAPサービスイメージをから "ネットアップサポートサイト"USBフラッシュドライブにダウンロードしてから交換用ブートメディアにダウンロードすることで、ONTAPイメージを交換用ブートメディアに転送できます。

作業を開始する前に

- 4GB以上の容量がある、FAT32にフォーマットされた空の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。
3. 電源装置に電源ケーブルを接続し、電源ケーブル固定クリップを再度取り付けます。

   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- FAS70およびFAS90

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	a. 障害コントローラで、次のメッセージが表示されたら_Y_を押します。 `Do you want to restore the backup configuration now?` 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_Y_を押します `/etc/ssh/ssh_host_ecdsa_key`。 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。_set -privilege advanced _。 d. 正常なパートナーコントローラで、restore backupコマンド_system node restore -backup -node local-target-address impaired_node_IP_address_を実行します。 *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 "ネットアップサポート"。 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。*set -privilege admin*。 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、_y_を押します `Was the restore backup procedure successful?`。 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、_y_を押します `…would you like to use this restored copy now?`。 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_y_を押し、ブートメニューとして_Ctrl+C_を押します。 i. システムで暗号化が使用されていない場合は、_option 1 Normal Bootを選択します。使用されていない場合は、に進みます。 "キー管理ツールのリストア" 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。 k. 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。 l. 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。 m. 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。 *注意：*プロセスが失敗した場合は、に連絡してください "ネットアップサポート"。

システムで実行しているバージョン	作業
ONTAP 9 .16.1以降	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、_y_を押します。 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 `syncflash_partner: Restore from partner complete`。 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、_y_を押します。 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、_y_を押します。 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、_y_を押します。 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_y_を押し、ブートメニューとして_Ctrl+C_を押します。 f. システムで暗号化が使用されていない場合は、_option 1 Normal Bootを選択します。使用されていない場合は、に進みます。 "キー管理ツールのリストア" 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。 h. 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。 i. 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。 j. 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。 *注意：*プロセスが失敗した場合は、に連絡してください "ネットアップサポート"。

リストアの暗号化- FAS70およびFAS90

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

この手順で最初に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。

```
Enter the backup data:

--------------------------BEGIN BACKUP--------------------------
0123456789012345678901234567890123456789012345678901234567890123
1234567890123456789012345678901234567890123456789012345678901234
2345678901234567890123456789012345678901234567890123456789012345
3456789012345678901234567890123456789012345678901234567890123456
4567890123456789012345678901234567890123456789012345678901234567
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
0123456789012345678901234567890123456789012345678901234567890123
1234567890123456789012345678901234567890123456789012345678901234
2345678901234567890123456789012345678901234567890123456789012345
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

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

5. リカバリプロセスが完了します。

```
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-----
MIIDvjCCAqagAwIBAgICN3gwDQYJKoZIhvcNAQELBQAwgY8xCzAJBgNVBAYTAlVT
MRMwEQYDVQQIEwpDYWxpZm9ybmlhMQwwCgYDVQQHEwNTVkwxDzANBgNVBAoTBk5l
MSUbQusvzAFs8G3P54GG32iIRvaCFnj2gQpCxciLJ0qB2foiBGx5XVQ/Mtk+rlap
Pk4ECW/wqSOUXDYtJs1+RB+w0+SHx8mzxpbz3mXF/X/1PC3YOzVNCq5eieek62si
Fp8=
-----END CERTIFICATE-----

Enter the client key (client.key) file contents:
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAoU1eajEG6QC2h2Zih0jEaGVtQUexNeoCFwKPoMSePmjDNtrU
MSB1SlX3VgCuElHk57XPdq6xSbYlbkIb4bAgLztHEmUDOkGmXYAkblQ=
-----END RSA PRIVATE KEY-----

Enter the KMIP server CA(s) (CA.pem) file contents:
-----BEGIN CERTIFICATE-----
MIIEizCCA3OgAwIBAgIBADANBgkqhkiG9w0BAQsFADCBjzELMAkGA1UEBhMCVVMx
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	a. パートナーコントローラにログインします。 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。

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. 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。
4. 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。

5. 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。
6. を使用し `storage encryption disk show` て出力を確認します。
7. 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` 。

8. 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。
9. 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。
10. 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。
11. 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。

障害が発生したパーツをNetApp - FAS70およびFAS90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

商標に関する情報