



Suporte de arranque

Install and maintain

NetApp
January 10, 2025

Índice

- Suporte de arranque 1
 - Descrição geral da substituição do suporte de arranque - AFF A200 1
 - Verifique o suporte e o status da chave de criptografia - AFF A200 1
 - Desligue o controlador desativado - AFF A200 5
 - Substitua o suporte de arranque - AFF A200 6
 - Inicie a imagem de recuperação - AFF A200 9
 - Restaurar encriptação - AFF A200 11
 - Devolva a peça com falha ao NetApp - AFF A200 21

Suporte de arranque

Descrição geral da substituição do suporte de arranque - AFF A200

A Mídia de inicialização armazena um conjunto primário e secundário de arquivos do sistema (imagem de inicialização) que o sistema usa quando ele é inicializado. Dependendo da configuração da rede, você pode realizar uma substituição sem interrupções ou disruptiva.

O que você vai precisar

Tem de ter uma unidade flash USB, formatada para FAT32, com a quantidade de armazenamento adequada para guardar o `image_XXX.tgz` ficheiro.

Antes de começar

- Os métodos sem interrupções e disruptivos para substituir uma Mídia de inicialização exigem que você restaure o sistema de arquivos var:
 - Para substituição sem interrupções, o par de HA deve ser conetado a uma rede para restaurar o sistema de arquivos var.
 - Para a substituição disruptiva, não é necessário uma ligação de rede para restaurar o sistema de ficheiros var, mas o processo requer duas reinicializações.
- Você deve substituir o componente com falha por um componente FRU de substituição que você recebeu de seu provedor.
- É importante que você aplique os comandos nestas etapas no controlador correto:
 - O controlador *prejudicado* é o controlador no qual você está realizando a manutenção.
 - O controlador *Healthy* é o parceiro de HA do controlador prejudicado.

Verifique o suporte e o status da chave de criptografia - AFF A200

Antes de desligar o controlador desativado, verifique se a sua versão do ONTAP suporta encriptação de volume NetApp (NVE) e se o sistema de gestão de chaves está corretamente configurado.

Passo 1: Verifique se a sua versão do ONTAP suporta encriptação de volume NetApp

Verifique se sua versão do ONTAP suporta criptografia de volume NetApp (NVE). Esta informação é crucial para transferir a imagem ONTAP correta.

1. Determine se sua versão do ONTAP suporta criptografia executando o seguinte comando:

```
version -v
```

Se a saída incluir `1Ono-DARE`, o NVE não é suportado na versão do cluster.

2. Dependendo se o NVE é compatível com o seu sistema, execute uma das seguintes ações:
 - Se for suportado NVE, transfira a imagem ONTAP com encriptação de volume NetApp.
 - Se a NVE não for suportada, transfira a imagem ONTAP **sem** encriptação de volume NetApp.

Passo 2: Determine se é seguro desligar o controlador

Para desligar um controlador com segurança, primeiro identifique se o External Key Manager (EKM) ou o Onboard Key Manager (OKM) está ativo. Em seguida, verifique o gerenciador de chaves em uso, exiba as informações de chave apropriadas e tome medidas com base no status das chaves de autenticação.

1. Determine qual gerenciador de chaves está habilitado em seu sistema:

Versão de ONTAP	Execute este comando
ONTAP 9.14,1 ou posterior	<pre data-bbox="621 611 1192 638">security key-manager keystore show</pre> <ul style="list-style-type: none"> • Se EKM estiver ativado, EKM é listado na saída do comando. • Se OKM estiver ativado, OKM o será listado na saída do comando. • Se nenhum gerenciador de chaves estiver habilitado, No key manager keystores configured o será listado na saída do comando.
ONTAP 9.13,1 ou anterior	<pre data-bbox="621 947 1208 974">security key-manager show-key-store</pre> <ul style="list-style-type: none"> • Se EKM estiver ativado, external é listado na saída do comando. • Se OKM estiver ativado, onboard o será listado na saída do comando. • Se nenhum gerenciador de chaves estiver habilitado, No key managers configured o será listado na saída do comando.

2. Dependendo se um gerenciador de chaves está configurado no sistema, selecione uma das opções a seguir.

Nenhum gerenciador de chaves configurado

Pode desligar o controlador com segurança. Vá para ["desligue o controlador desativado"](#).

Gestor de chaves externo ou integrado configurado

- a. Digite o seguinte comando de consulta para exibir o status das chaves de autenticação no gerenciador de chaves.

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

- b. Verifique a saída para o valor na `Restored` coluna do seu gerenciador de chaves.

Esta coluna indica se as chaves de autenticação do seu gerenciador de chaves (EKM ou OKM) foram restauradas com êxito.

3. Dependendo se o sistema estiver usando o Gerenciador de chaves Externo ou o Gerenciador de chaves integrado, selecione uma das opções a seguir.

Gerenciador de chaves externo

Dependendo do valor de saída exibido na `Restored` coluna, siga as etapas apropriadas.

Valor de saída <code>Restored</code> na coluna	Siga estes passos...
<code>true</code>	Pode desligar o controlador com segurança. Vá para "desligue o controlador desativado" .
Qualquer outra coisa que não <code>true</code>	<ol style="list-style-type: none">Restaure as chaves de autenticação de gerenciamento de chaves externas para todos os nós no cluster usando o seguinte comando: <pre>security key-manager external restore</pre><p>Se o comando falhar, contactar "Suporte à NetApp".</p>Verifique se a <code>Restored</code> coluna é exibida <code>true</code> para todas as chaves de autenticação inserindo o <code>security key-manager key query</code> comando. Se todas as chaves de autenticação forem <code>true</code>, pode desligar o controlador com segurança. Vá para "desligue o controlador desativado".

Gerenciador de chaves integrado

Dependendo do valor de saída exibido na `Restored` coluna, siga as etapas apropriadas.

Valor de saída <code>Restored</code> na coluna	Siga estes passos...
<code>true</code>	<p>Faça backup manual das informações OKM.</p> <ol style="list-style-type: none">Vá para o modo avançado entrando <code>set -priv advanced</code> e, em seguida, entre <code>Y</code> quando solicitado.Digite o seguinte comando para exibir as informações de gerenciamento de chaves: <pre>security key-manager onboard show-backup</pre>Copie o conteúdo das informações de backup para um arquivo separado ou seu arquivo de log. Você vai precisar dele em cenários de desastre onde você pode precisar recuperar manualmente OKM.Pode desligar o controlador com segurança. Vá para "desligue o controlador desativado".

Valor de saída Restored na coluna	Siga estes passos...
Qualquer outra coisa que não true	<p>a. Digite o comando Onboard security key-manager sync:</p> <pre>security key-manager onboard sync</pre> <p>b. Digite a senha alfanumérica de gerenciamento de chaves integradas de 32 caracteres quando solicitado.</p> <p>Se a frase-passe não puder ser fornecida, "Suporte à NetApp" contacte .</p> <p>c. Verifique se a Restored coluna exibe true todas as chaves de autenticação:</p> <pre>security key-manager key query</pre> <p>d. Verifique se o Key Manager tipo é exibido onboard e, em seguida, faça backup manual das informações OKM.</p> <p>e. Digite o comando para exibir as informações de backup de gerenciamento de chaves:</p> <pre>security key-manager onboard show-backup</pre> <p>f. Copie o conteúdo das informações de backup para um arquivo separado ou seu arquivo de log.</p> <p>Você vai precisar dele em cenários de desastre onde você pode precisar recuperar manualmente OKM.</p> <p>g. Pode desligar o controlador com segurança. Vá para "desligue o controlador desativado".</p>

Desligue o controlador desativado - AFF A200

Depois de concluir as tarefas NVE ou NSE, você precisa concluir o desligamento do controlador desativado.

Passos

1. Leve o controlador prejudicado para o prompt Loader:

Se o controlador afetado apresentar...	Então...
O prompt Loader	Vá para Remove módulo do controlador.
Waiting for giveback...	Pressione Ctrl-C e responda y quando solicitado.

Se o controlador afetado apresentar...	Então...
Prompt do sistema ou prompt de senha (digite a senha do sistema)	<p>Assuma ou interrompa o controlador prejudicado do controlador saudável: <code>storage failover takeover -ofnode impaired_node_name</code></p> <p>Quando o controlador prejudicado mostrar aguardando a giveback..., pressione Ctrl-C e responda <code>y</code>.</p>

- No prompt Loader, digite: `printenv` Para capturar todas as variáveis ambientais de inicialização. Salve a saída no arquivo de log.



Este comando pode não funcionar se o dispositivo de inicialização estiver corrompido ou não funcional.

Substitua o suporte de arranque - AFF A200

Para substituir o suporte de arranque, tem de remover o módulo do controlador afetado, instalar o suporte de arranque de substituição e transferir a imagem de arranque para uma unidade flash USB.

Passo 1: Remova o controlador

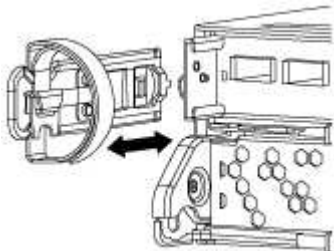
Para aceder aos componentes no interior do controlador, tem de remover primeiro o módulo do controlador do sistema e, em seguida, remover a tampa do módulo do controlador.

Passos

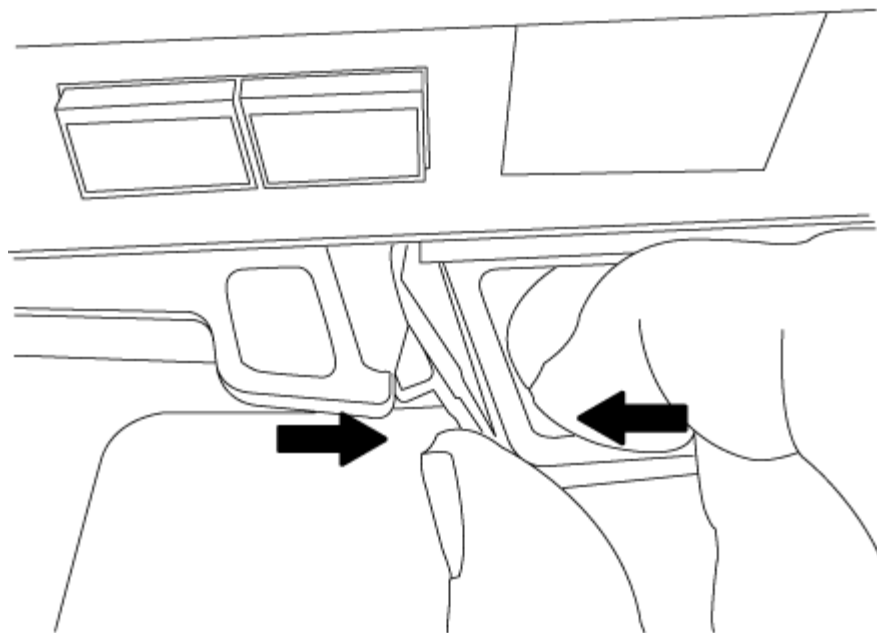
- Se você ainda não está aterrado, aterre-se adequadamente.
- Solte o gancho e a alça de loop que prendem os cabos ao dispositivo de gerenciamento de cabos e, em seguida, desconete os cabos do sistema e os SFPs (se necessário) do módulo do controlador, mantendo o controle de onde os cabos estavam conectados.

Deixe os cabos no dispositivo de gerenciamento de cabos para que, ao reinstalar o dispositivo de gerenciamento de cabos, os cabos sejam organizados.

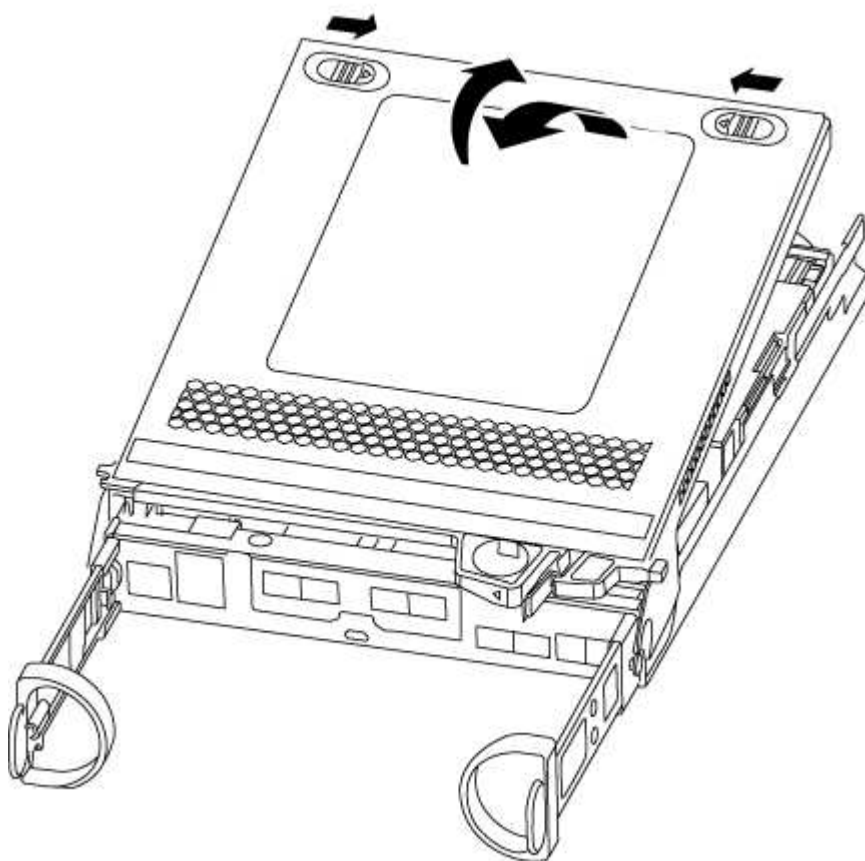
- Retire e reserve os dispositivos de gerenciamento de cabos dos lados esquerdo e direito do módulo do controlador.



- Aperte o trinco na pega do excêntrico até que este se solte, abra totalmente o manípulo do excêntrico para libertar o módulo do controlador do plano médio e, em seguida, utilizando duas mãos, puxe o módulo do controlador para fora do chassis.



5. Vire o módulo do controlador ao contrário e coloque-o numa superfície plana e estável.
6. Abra a tampa deslizando as patilhas azuis para soltar a tampa e, em seguida, rode a tampa para cima e abra-a.



Passo 2: Substitua o suporte de arranque

Você deve localizar o suporte de inicialização no controlador e seguir as instruções para substituí-lo.

Passos

1. Se você ainda não está aterrado, aterre-se adequadamente.
2. Localize a Mídia de inicialização usando a ilustração a seguir ou o mapa da FRU no módulo do controlador:
3. Prima o botão azul no alojamento do suporte do suporte de arranque para soltar o suporte de arranque do respectivo alojamento e, em seguida, puxe-o cuidadosamente para fora do suporte de suporte de arranque.



Não torça nem puxe o suporte de arranque diretamente para cima, pois isto pode danificar o suporte ou o suporte de arranque.

4. Alinhe as extremidades do suporte de arranque de substituição com a tomada de suporte de arranque e, em seguida, empurre-o cuidadosamente para dentro do encaixe.
5. Verifique o suporte de arranque para se certificar de que está encaixado corretamente e completamente no encaixe.

Se necessário, retire o suporte de arranque e volte a colocá-lo no socket.

6. Prima o suporte de arranque para baixo para engatar o botão de bloqueio no alojamento do suporte de suporte de arranque.
7. Feche a tampa do módulo do controlador.

Passo 3: Transfira a imagem de arranque para o suporte de arranque

Pode instalar a imagem do sistema no suporte de arranque de substituição utilizando uma unidade flash USB com a imagem instalada. No entanto, tem de restaurar o sistema de ficheiros var durante este procedimento.

O que você vai precisar

- Você deve ter uma unidade flash USB, formatada para FAT32, com pelo menos 4GBGB de capacidade.
- Uma cópia da mesma versão de imagem do ONTAP que a que o controlador afetado estava a executar. Você pode baixar a imagem apropriada da seção Downloads no site de suporte da NetApp
 - Se a NVE estiver ativada, transfira a imagem com encriptação de volume NetApp, conforme indicado no botão de transferência.
 - Se a NVE não estiver ativada, transfira a imagem sem encriptação de volume NetApp, conforme indicado no botão de transferência.
- Se o seu sistema for um par de HA, tem de ter uma ligação de rede.
- Se o seu sistema for um sistema autónomo, não necessita de uma ligação de rede, mas tem de efetuar uma reinicialização adicional ao restaurar o sistema de ficheiros var.

Passos

1. Alinhe a extremidade do módulo do controlador com a abertura no chassis e, em seguida, empurre cuidadosamente o módulo do controlador até meio do sistema.
2. Reinstale o dispositivo de gerenciamento de cabos e reconete o sistema, conforme necessário.

Ao reativar, lembre-se de reinstalar os conversores de Mídia (SFPs) se eles foram removidos.

3. Introduza a unidade flash USB na ranhura USB do módulo do controlador.

Certifique-se de que instala a unidade flash USB na ranhura identificada para dispositivos USB e não na porta da consola USB.

- Empurre o módulo do controlador totalmente para dentro do sistema, certificando-se de que a alça da came limpa a unidade flash USB, empurre firmemente a alça da came para terminar de assentar o módulo do controlador, empurre a alça da came para a posição fechada e, em seguida, aperte o parafuso de aperto manual.

O controlador começa a arrancar assim que é completamente instalado no chassis.

- Interrompa o processo de inicialização para parar no prompt DO Loader pressionando Ctrl-C quando você vir iniciando o AUTOBOOT pressione Ctrl-C para abortar....

Se você perder essa mensagem, pressione Ctrl-C, selecione a opção para inicializar no modo Manutenção e, em seguida, interrompa o controlador para inicializar NO Loader.

- Para sistemas com um controlador no chassi, reconete a alimentação e ligue as fontes de alimentação.

O sistema começa a inicializar e pára no prompt DO Loader.

- Defina o tipo de conexão de rede no prompt DO Loader:

- Se estiver a configurar DHCP: `ifconfig e0a -auto`



A porta de destino configurada é a porta de destino utilizada para comunicar com o controlador afetado a partir do controlador saudável durante a restauração do sistema de ficheiros var com uma ligação de rede. Você também pode usar a porta e0M neste comando.

- Se estiver a configurar ligações manuais: `ifconfig e0a -addr=filer_addr -mask=netmask -gw=gateway-dns=dns_addr-domain=dns_domain`

- `filer_addr` É o endereço IP do sistema de armazenamento.
- `netmask` É a máscara de rede da rede de gerenciamento conetada ao parceiro HA.
- `gateway` é o gateway para a rede.
- `dns_addr` É o endereço IP de um servidor de nomes na rede.
- `dns_domain` É o nome de domínio do sistema de nomes de domínio (DNS).

Se você usar esse parâmetro opcional, não precisará de um nome de domínio totalmente qualificado no URL do servidor netboot. Você só precisa do nome de host do servidor.



Outros parâmetros podem ser necessários para sua interface. Você pode digitar `help ifconfig` no prompt do firmware para obter detalhes.

Inicie a imagem de recuperação - AFF A200

Você deve inicializar a imagem ONTAP a partir da unidade USB, restaurar o sistema de arquivos e verificar as variáveis ambientais.

Passos

- A partir do prompt Loader, inicialize a imagem de recuperação da unidade flash USB: `boot_recovery`

A imagem é transferida da unidade flash USB.

2. Quando solicitado, insira o nome da imagem ou aceite a imagem padrão exibida dentro dos colchetes na tela.
3. Restaure o `var` sistema de arquivos:

Se o seu sistema tem...	Então...
Uma ligação de rede	<ol style="list-style-type: none">a. Pressione <code>y</code> quando solicitado para restaurar a configuração de backup.b. Defina o controlador saudável para nível de privilégio avançado: <code>set -privilege advanced</code>c. Execute o comando Restore backup: <code>system node restore-backup -node local -target-address <i>impaired_node_IP_address</i></code>d. Retorne o controlador ao nível de administração: <code>set -privilege admin</code>e. Pressione <code>y</code> quando solicitado a usar a configuração restaurada.f. Pressione <code>y</code> quando solicitado para reiniciar o controlador.
Sem ligação à rede	<ol style="list-style-type: none">a. Pressione <code>n</code> quando solicitado para restaurar a configuração de backup.b. Reinicie o sistema quando solicitado pelo sistema.c. Selecione a opção Update flash from backup config (Sync flash) no menu exibido. <p>Se for solicitado que você continue com a atualização, <code>y</code> pressione <code>.</code></p>

4. Certifique-se de que as variáveis ambientais estão definidas como esperado:
 - a. Leve o controlador para o prompt Loader.
 - b. Verifique as configurações de variáveis de ambiente com o `printenv` comando.
 - c. Se uma variável de ambiente não for definida como esperado, modifique-a com o `setenv environment-variable-name changed-value` comando.
 - d. Salve suas alterações usando o `saveenv` comando.
5. O próximo depende da configuração do sistema:
 - Se o sistema tiver o gerenciador de chaves integrado, NSE ou NVE configurado, vá para [Restaure OKM, NSE e NVE conforme necessário](#)
 - Se o sistema não tiver o gerenciador de chaves integrado, NSE ou NVE configurado, execute as etapas nesta seção.
6. No prompt Loader, digite o `boot_ontap` comando.

Se você ver...	Então...
O aviso de início de sessão	Vá para a próxima etapa.
A aguardar pela giveback...	<ol style="list-style-type: none"> Faça login no controlador do parceiro. Confirme se o controlador de destino está pronto para giveback com o <code>storage failover show</code> comando.

- Conete o cabo do console ao controlador do parceiro.
- Devolva o controlador usando o `storage failover giveback -fromnode local` comando.
- No prompt do cluster, verifique as interfaces lógicas com o `net int -is-home false` comando.

Se alguma interface estiver listada como "false", reverta essas interfaces de volta para sua porta inicial usando o `net int revert` comando.

- Mova o cabo do console para o controlador reparado e execute o `version -v` comando para verificar as versões do ONTAP.
- Restaurar o giveback automático se você o desativou usando o `storage failover modify -node local -auto-giveback true` comando.

Restaurar encriptação - AFF A200

Restaurar a encriptação no suporte de arranque de substituição.

Você deve concluir etapas específicas para sistemas que tenham o Gerenciador de chaves integrado (OKM), a criptografia de armazenamento NetApp (NSE) ou a criptografia de volume NetApp (NVE) habilitados usando as configurações capturadas no início do procedimento de substituição de Mídia de inicialização.

Dependendo de qual um gerenciador de chaves está configurado no sistema, selecione uma das seguintes opções para restaurá-lo no menu de inicialização.

- "[Opção 1: Restaurar a configuração do Gerenciador de chaves integrado](#)"
- "[Opção 2: Restaurar a configuração do Gerenciador de chaves Externo](#)"

Opção 1: Restaurar a configuração do Gerenciador de chaves integrado

Restaurar a configuração OKM (Onboard Key Manager) no menu de inicialização do ONTAP.

Antes de começar

- Certifique-se de que tem as seguintes informações enquanto restaura a configuração OKM:
 - Frase-passe de todo o cluster introduzida "[ao ativar o gerenciamento de chaves integradas](#)".
 - "[Informações de cópia de segurança para o Gestor de chaves integrado](#)".
- Execute o "[Como verificar o backup integrado do gerenciamento de chaves e a senha em todo o cluster](#)" procedimento antes de prosseguir.

Passos

1. Conecte o cabo do console ao controlador de destino.
2. No menu de inicialização do ONTAP, selecione a opção apropriada no menu de inicialização.

Versão de ONTAP	Selecione esta opção
ONTAP 9 .8 ou posterior	<p data-bbox="621 279 901 310">Selecione a opção 10.</p> <p data-bbox="621 342 1153 373">Mostrar exemplo de menu de inicialização</p> <div data-bbox="654 415 1456 1197" style="border: 1px solid #ccc; padding: 10px;"><pre data-bbox="686 447 1372 1165">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</pre></div>

Versão de ONTAP	Selecione esta opção
ONTAP 9 F.7 e anteriores	<p data-bbox="621 163 1377 195">Selecione a opção oculta <code>recover_onboard_keymanager</code></p> <p data-bbox="621 233 1154 264">Mostrar exemplo de menu de inicialização</p> <div data-bbox="654 306 1455 968" style="border: 1px solid #ccc; padding: 10px; background-color: #f9f9f9;"> <pre data-bbox="683 342 1369 932"> 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. Confirme se deseja continuar o processo de recuperação.

Mostrar prompt de exemplo

```

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

```

4. Introduza duas vezes a frase-passe de todo o cluster.

Ao inserir a senha, o console não mostrará nenhuma entrada.

Mostrar prompt de exemplo

```

Enter the passphrase for onboard key management:

Enter the passphrase again to confirm:

```

5. Introduza as informações de cópia de segurança.

- a. Cole todo o conteúdo da linha DE BACKUP INICIAL através da linha DE BACKUP FINAL.

Mostrar prompt de exemplo

Enter the backup data:

```
-----BEGIN BACKUP-----  
01234567890123456789012345678901234567890123456789012345678901234567890123  
12345678901234567890123456789012345678901234567890123456789012345678901234  
23456789012345678901234567890123456789012345678901234567890123456789012345  
34567890123456789012345678901234567890123456789012345678901234567890123456  
45678901234567890123456789012345678901234567890123456789012345678901234567  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
01234567890123456789012345678901234567890123456789012345678901234567890123  
12345678901234567890123456789012345678901234567890123456789012345678901234  
23456789012345678901234567890123456789012345678901234567890123456789012345  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
-----END BACKUP-----
```

b. Pressione a tecla Enter duas vezes no final da entrada.

O processo de recuperação é concluído.

Mostrar prompt de exemplo

```
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.
*****
*****
```



Não prossiga se a saída exibida for diferente `Successfully recovered keymanager secrets` de . Execute a solução de problemas para corrigir o erro.

6. Selecione a opção 1 no menu de inicialização para continuar inicializando no ONTAP.

Mostrar prompt de exemplo

```
*****
*****
* 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. Confirme se o console do controlador exibe a seguinte mensagem.

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

8. A partir do nó do parceiro, giveback do controlador do parceiro inserindo o seguinte comando.

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

9. Depois de inicializar apenas com o agregado CFO, execute o seguinte comando.

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

10. Introduza a frase-passe de todo o cluster para o Gestor de chaves integrado.

Mostrar prompt de exemplo

```
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.
```



Se a sincronização for bem-sucedida, o prompt do cluster será retornado sem mensagens adicionais. Se a sincronização falhar, uma mensagem de erro será exibida antes de retornar ao prompt do cluster. Não continue até que o erro seja corrigido e a sincronização seja executada com êxito.

11. Certifique-se de que todas as chaves são sincronizadas digitando o seguinte comando.

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

```
There are no entries matching your query.
```



Nenhum resultado deve aparecer ao filtrar para FALSE no parâmetro restaurado.

12. Troque o nó do parceiro digitando o seguinte comando.

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

13. Restaure o giveback automático, se você o desativou, digitando o seguinte comando.

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

14. Se o AutoSupport estiver ativado, restaure a criação automática de casos inserindo o seguinte comando.

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

Opção 2: Restaure a configuração do Gerenciador de chaves Externo

Restaure a configuração do Gerenciador de chaves Externo no menu de inicialização do ONTAP.

Antes de começar

Você precisa das seguintes informações para restaurar a configuração do EKM (External Key Manager).

- Uma cópia do arquivo `/cfcard/kmip/servers.cfg` de outro nó de cluster ou as seguintes informações:
 - O endereço do servidor KMIP.
 - A porta KMIP.

- Uma cópia do `/cfcard/kmip/certs/client.crt` arquivo de outro nó de cluster ou do certificado do cliente.
- Uma cópia do `/cfcard/kmip/certs/client.key` arquivo de outro nó de cluster ou da chave do cliente.
- Cópia `/cfcard/kmip/certs/CA.pem` do arquivo de outro nó de cluster ou CA(s) do servidor KMIP.

Passos

1. Conete o cabo do console ao controlador de destino.
2. Selecione a opção 11 no menu de inicialização do ONTAP.

Mostrar exemplo de menu de inicialização

```
(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. Quando solicitado, confirme que você reuniu as informações necessárias.

Mostrar prompt de exemplo

```
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. Quando solicitado, insira as informações do cliente e do servidor.

Mostrar prompt

```
Enter the client certificate (client.crt) file contents:
Enter the client key (client.key) file contents:
Enter the KMIP server CA(s) (CA.pem) file contents:
Enter the server configuration (servers.cfg) file contents:
```

Mostrar exemplo

```
Enter the client certificate (client.crt) file contents:
-----BEGIN CERTIFICATE-----
MIIDvjCCAqagAwIBAgICN3gwDQYJKoZIhvcNAQELBQAwY8xCzAJBgNVBAYTA1VT
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-----
<key_value>
-----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....
kmp_init: configuring ports
Running command '/sbin/ifconfig e0M'
..
..
kmp_init: cmd: ReleaseExtraBSDPort e0M
```

Depois de inserir as informações do cliente e do servidor, o processo de recuperação é concluído.

Mostrar exemplo

```
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. Selecione a opção 1 no menu de inicialização para continuar inicializando no ONTAP.

Mostrar prompt de exemplo

```
*****
*****
* 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. Restaure o giveback automático, se você o desativou, digitando o seguinte comando.

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

7. Se o AutoSupport estiver ativado, restaure a criação automática de casos inserindo o seguinte comando.

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

Devolva a peça com falha ao NetApp - AFF A200

Devolva a peça com falha ao NetApp, conforme descrito nas instruções de RMA fornecidas com o kit. Consulte a "[Devolução de peças e substituições](#)" página para obter mais informações.

Informações sobre direitos autorais

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.