



Suporte de arranque

Install and maintain

NetApp
January 10, 2025

Índice

- Suporte de arranque 1
 - Descrição geral da substituição do suporte de arranque - AFF A400 1
 - Verifique o suporte e o status da chave de criptografia - AFF A400 1
 - Desligue o controlador desativado - AFF A400 5
 - Substitua o suporte de arranque - AFF A400 9
 - Inicie a imagem de recuperação - AFF A400 14
 - Altere agregados em uma configuração de MetroCluster de dois nós - AFF A400 17
 - Restaurar encriptação - AFF A400 18
 - Devolva a peça com falha ao NetApp - AFF A400 28

Suporte de arranque

Descrição geral da substituição do suporte de arranque - AFF A400

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.

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

Você também deve copiar o `image_xxx.tgz` arquivo para a unidade flash USB para uso posterior neste procedimento.

- Os métodos sem interrupções e disruptivos para substituir uma Mídia de inicialização exigem que você restaure o `var` sistema de arquivos:
 - Para substituição sem interrupções, o par de HA deve estar conetado a uma rede para restaurar o `var` sistema de arquivos.
 - Para a substituição disruptiva, não é necessário uma ligação de rede para restaurar o `var` sistema de ficheiros, 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 nessas etapas no nó correto:
 - O nó *prejudicado* é o nó no qual você está realizando a manutenção.
 - O nó *Healthy* é o parceiro de HA do nó prejudicado.

Verifique o suporte e o status da chave de criptografia - AFF A400

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>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>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> Se o comando falhar, contactar "Suporte à NetApp".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 A400

Depois de concluir as tarefas NVE ou NSE, você precisa concluir o desligamento do controlador desativado. Encerre ou assuma o controlador afetado utilizando o procedimento adequado para a sua configuração.

Opção 1: A maioria das configurações

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 Remover módulo do controlador. |
| Waiting for giveback... | Pressione Ctrl-C e responda <code>y</code> quando solicitado. |
| Prompt do sistema ou prompt de senha (digite a senha do sistema) | Assuma ou interrompa o controlador prejudicado do controlador saudável: <code>storage failover takeover -ofnode impaired_node_name</code> Quando o controlador prejudicado mostrar aguardando a giveback..., pressione Ctrl-C e responda <code>y</code> . |

- 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.

Opção 2: O controlador está em uma configuração MetroCluster



Não use este procedimento se o sistema estiver em uma configuração de MetroCluster de dois nós.

Para encerrar o controlador com deficiência, você deve determinar o status do controlador e, se necessário, assumir o controlador para que o controlador saudável continue fornecendo dados do armazenamento do controlador com deficiência.

- Se você tiver um cluster com mais de dois nós, ele deverá estar no quórum. Se o cluster não estiver em quórum ou se um controlador íntegro exibir `false` para qualificação e integridade, você deverá corrigir o problema antes de encerrar o controlador prejudicado; "[Sincronize um nó com o cluster](#)" consulte .
- Se você tiver uma configuração MetroCluster, você deve ter confirmado que o estado de configuração do MetroCluster está configurado e que os nós estão em um estado ativado e normal (`metrocluster node show`).

Passos

- Se o AutoSupport estiver ativado, suprimir a criação automática de casos invocando uma mensagem AutoSupport: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

A seguinte mensagem AutoSupport suprime a criação automática de casos por duas horas:

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

- Desative a giveback automática a partir da consola do controlador saudável: `storage failover modify -node local -auto-giveback false`
- Leve o controlador prejudicado para o prompt Loader:

| Se o controlador afetado estiver a apresentar... | Então... |
|--|---|
| O prompt Loader | Vá para a próxima etapa. |
| A aguardar pela giveback... | Pressione Ctrl-C e responda <code>y</code> quando solicitado. |
| Prompt do sistema ou prompt de senha (digite a senha do sistema) | Assuma ou interrompa o controlador prejudicado do controlador saudável: <code>storage failover takeover -ofnode <i>impaired_node_name</i></code> Quando o controlador prejudicado mostrar aguardando a giveback..., pressione Ctrl-C e responda <code>y</code> . |

Opção 3: O controlador está em um MetroCluster de dois nós

Para desligar o controlador desativado, você deve determinar o status do controlador e, se necessário, trocar o controlador para que o controlador saudável continue fornecendo dados do armazenamento do controlador prejudicado.

Sobre esta tarefa

- Você deve deixar as fontes de alimentação ligadas no final deste procedimento para fornecer energia ao controlador de integridade.

Passos

1. Verifique o estado do MetroCluster para determinar se o controlador afetado mudou automaticamente para o controlador saudável: `metrocluster show`
2. Dependendo se ocorreu uma mudança automática, proceda de acordo com a seguinte tabela:

| Se o controlador deficiente... | Então... |
|--|--|
| Mudou automaticamente | Avance para o passo seguinte. |
| Não mudou automaticamente | Execute uma operação de comutação planejada a partir do controlador íntegro: <code>metrocluster switchover</code> |
| Não mudou automaticamente, tentou mudar com o comando e o <code>switchover metrocluster switchover</code> foi vetado | Reveja as mensagens de veto e, se possível, resolva o problema e tente novamente. Se você não conseguir resolver o problema, entre em Contato com o suporte técnico. |

3. Ressincronize os agregados de dados executando o `metrocluster heal -phase aggregates` comando do cluster sobrevivente.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

Se a cura for vetada, você tem a opção de reemitir o `metrocluster heal` comando com o `-override -vetoes` parâmetro. Se você usar esse parâmetro opcional, o sistema substituirá quaisquer vetos de software que impeçam a operação de recuperação.

4. Verifique se a operação foi concluída usando o comando `MetroCluster operation show`.

```
controller_A_1::> metrocluster operation show
  Operation: heal-aggregates
  State: successful
Start Time: 7/25/2016 18:45:55
End Time: 7/25/2016 18:45:56
Errors: -
```

5. Verifique o estado dos agregados utilizando o `storage aggregate show` comando.

```
controller_A_1::> storage aggregate show
Aggregate      Size Available Used% State   #Vols  Nodes           RAID
Status
-----
...
aggr_b2       227.1GB   227.1GB   0% online    0  mcc1-a2
raid_dp, mirrored, normal...
```

6. Curar os agregados raiz usando o `metrocluster heal -phase root-aggregates` comando.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

Se a recuperação for vetada, você terá a opção de reemitir o `metrocluster heal` comando com o parâmetro `-override-vetos`. Se você usar esse parâmetro opcional, o sistema substituirá quaisquer vetos de software que impeçam a operação de recuperação.

7. Verifique se a operação `heal` está concluída usando o `metrocluster operation show` comando no cluster de destino:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
  State: successful
Start Time: 7/29/2016 20:54:41
End Time: 7/29/2016 20:54:42
Errors: -
```

8. No módulo do controlador desativado, desligue as fontes de alimentação.

Substitua o suporte de arranque - AFF A400

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 módulo do controlador

Para aceder aos componentes no interior do módulo do controlador, tem de remover o módulo do controlador do chassis.

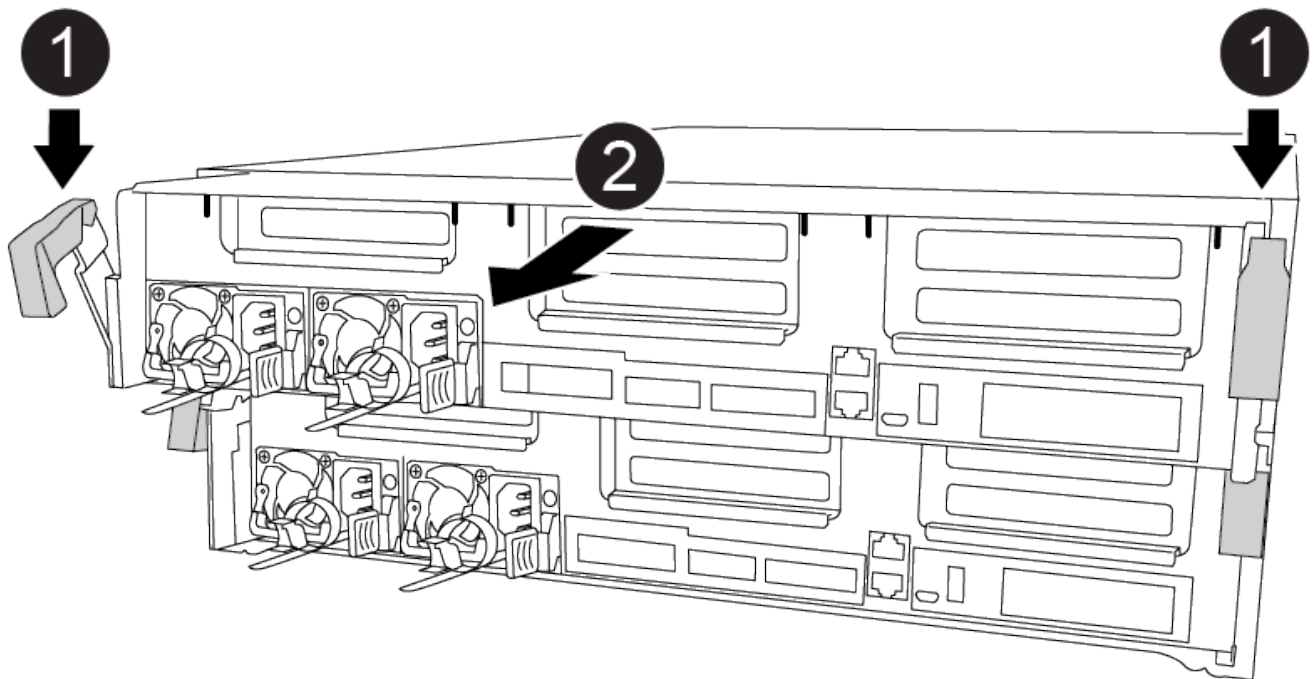
Passos

1. Se você ainda não está aterrado, aterre-se adequadamente.
2. Solte os fixadores do cabo de alimentação e, em seguida, desconecte os cabos das fontes de alimentação.
3. Solte o gancho e a alça de loop que prendem os cabos ao dispositivo de gerenciamento de cabos e, em seguida, desconecte 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.

4. Retire o dispositivo de gestão de cabos do módulo do controlador e coloque-o de lado.
5. Prima ambos os trincos de bloqueio para baixo e, em seguida, rode ambos os trincos para baixo ao mesmo tempo.

O módulo do controlador desloca-se ligeiramente para fora do chassis.



1

Trincos de bloqueio

2

O controlador se move ligeiramente para fora do chassi

6. Faça deslizar o módulo do controlador para fora do chassis.

Certifique-se de que suporta a parte inferior do módulo do controlador enquanto o desliza para fora do chassis.

7. Coloque o módulo do controlador numa superfície estável e plana.

Passo 2: Substitua o suporte de arranque

Deve localizar o suporte de arranque no módulo do controlador (consulte o mapa da FRU no módulo do controlador) e, em seguida, seguir as instruções para o substituir.

Antes de começar

Embora o conteúdo da Mídia de inicialização seja criptografado, é uma prática recomendada apagar o conteúdo da Mídia de inicialização antes de substituí-la. Para obter mais informações, consulte "[Declaração de volatilidade](#)" para o seu sistema no site de suporte da NetApp.



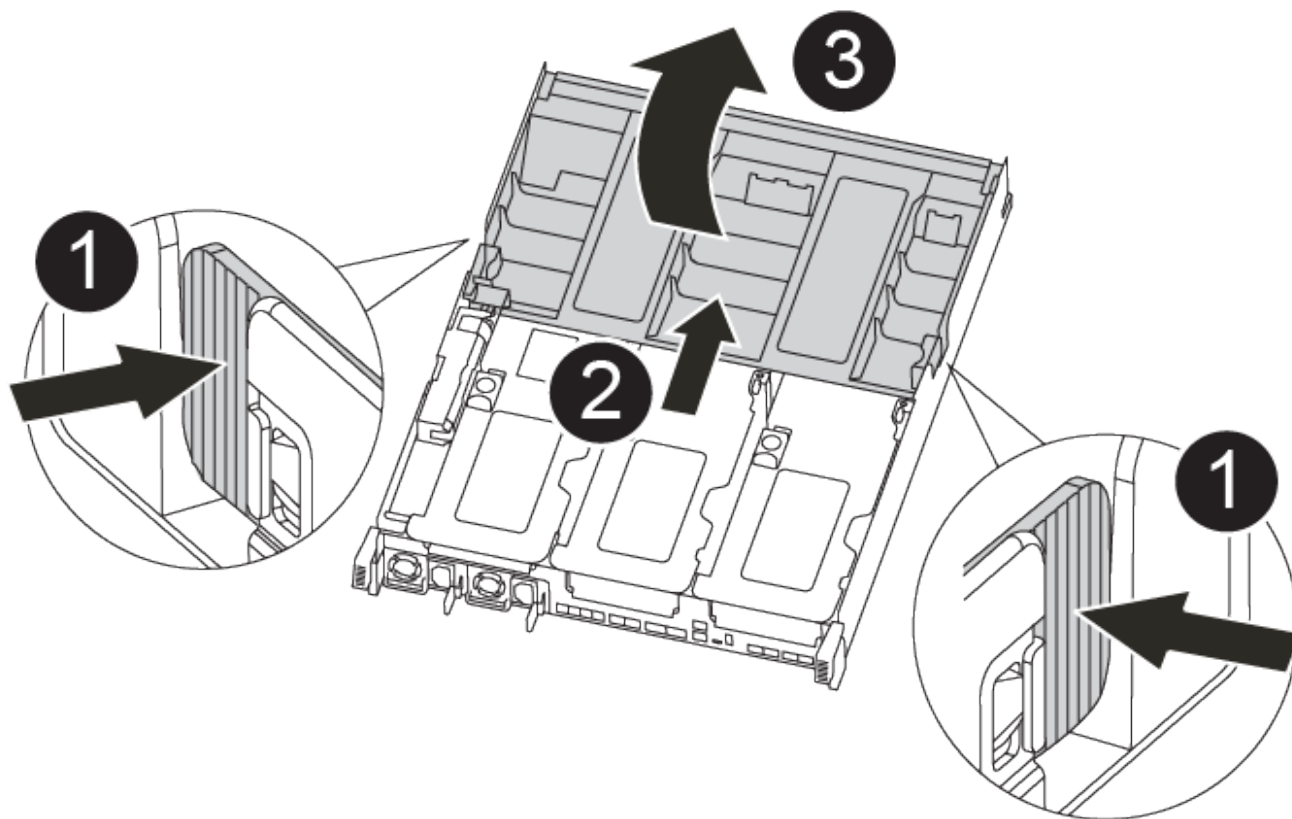
Você deve fazer login no site de suporte da NetApp para exibir a *Declaração de volatilidade* para o seu sistema.

Você pode usar a animação, ilustração ou as etapas escritas a seguir para substituir o suporte de inicialização.

[Animação - substitua o suporte de arranque](#)

Passos

1. Abrir a conduta de ar:



1

Patilhas de bloqueio

2

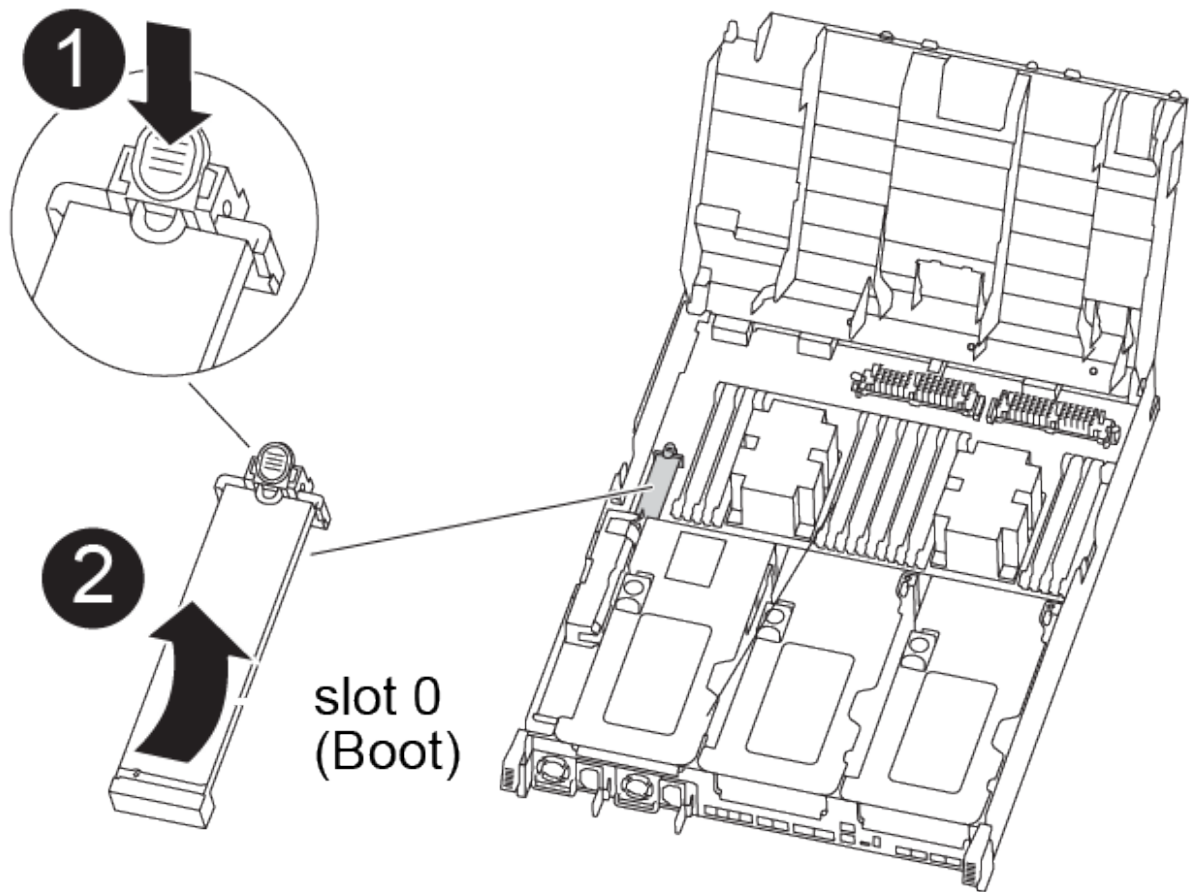
Deslize o duto de ar em direção à parte traseira do controlador

3

Rode a conduta de ar para cima

- a. Pressione as patilhas de bloqueio nas laterais da conduta de ar para dentro, em direção ao centro do módulo do controlador.
- b. Faça deslizar a conduta de ar em direção à parte de trás do módulo do controlador e, em seguida, rode-a para cima até à posição completamente aberta.

2. Localize e remova o suporte de arranque do módulo do controlador:



1

Prima o botão azul

2

Rode o suporte de arranque para cima e retire-o da tomada

- a. Pressione o botão azul na extremidade do suporte de inicialização até que o lábio do suporte de inicialização apague o botão azul.
 - b. Rode o suporte de arranque para cima e puxe cuidadosamente o suporte de arranque para fora do encaixe.
3. 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.
 4. 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.

5. Bloquee o suporte de arranque no devido lugar:
 - a. Rode o suporte de arranque para baixo em direção à placa-mãe.

- b. Colocando um dedo na extremidade do suporte de arranque com o botão azul, prima a extremidade do suporte de arranque para engatar o botão de bloqueio azul.
 - c. Enquanto pressiona o suporte de arranque, levante o botão azul de bloqueio para bloquear o suporte de arranque no lugar.
6. Feche a conduta de ar.

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

A Mídia de inicialização de substituição que você instalou não tem uma imagem de inicialização, então você precisa transferir uma imagem de inicialização usando uma unidade flash USB.

Antes de começar

- Você deve ter uma unidade flash USB, formatada para MBR/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 `var` sistema de ficheiros.

Passos

1. Transfira e copie a imagem de serviço apropriada do site de suporte da NetApp para a unidade flash USB.
 - a. Transfira a imagem de serviço para o seu espaço de trabalho no seu computador portátil.
 - b. Descompacte a imagem de serviço.



Se você estiver extraindo o conteúdo usando o Windows, não use o WinZip para extrair a imagem netboot. Use outra ferramenta de extração, como 7-Zip ou WinRAR.

Há duas pastas no arquivo de imagem de serviço descompactado:

- `boot`
- `efi`

- c. Copie a `efi` pasta para o diretório superior da unidade flash USB.



Se a imagem de serviço não tiver uma pasta efi, "[Pasta EFI ausente do arquivo de download de imagem de serviço usado para recuperação de dispositivo de inicialização para modelos FAS e AFF](#)" consulte .

A unidade flash USB deve ter a pasta efi e a mesma versão de imagem de serviço (BIOS) do que o controlador deficiente está executando.

- a. Retire a unidade flash USB do seu computador portátil.

2. Se ainda não o tiver feito, feche a conduta de ar.
3. 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.
4. Reinstale o dispositivo de gerenciamento de cabos e reconete o sistema, conforme necessário.

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

5. Ligue o cabo de alimentação à fonte de alimentação e volte a instalar o fixador do cabo de alimentação.
6. 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.

7. Conclua a instalação do módulo do controlador:
 - a. Ligue o cabo de alimentação à fonte de alimentação, volte a instalar o anel de bloqueio do cabo de alimentação e, em seguida, ligue a fonte de alimentação à fonte de alimentação.
 - b. Empurre firmemente o módulo do controlador para dentro do chassi até que ele atenda ao plano médio e esteja totalmente assentado.

Os trincos de bloqueio sobem quando o módulo do controlador está totalmente assente.



Não utilize força excessiva ao deslizar o módulo do controlador para dentro do chassis para evitar danificar os conectores.

O módulo do controlador começa a arrancar assim que estiver totalmente assente no chassis. Esteja preparado para interromper o processo de inicialização.

- a. Rode os trincos de bloqueio para cima, inclinando-os de forma a que estes limpem os pinos de bloqueio e, em seguida, baixe-os para a posição de bloqueio.
 - b. Se ainda não o tiver feito, reinstale o dispositivo de gerenciamento de cabos.
8. Interrompa o processo de inicialização pressionando Ctrl-C para parar no prompt DO Loader.

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

9. Se o controlador estiver em um MetroCluster elástico ou conectado à malha, será necessário restaurar a configuração do adaptador FC:
 - a. Arranque para o modo de manutenção: `boot_ontap maint`
 - b. Defina as portas MetroCluster como iniciadores: `ucadmin modify -m fc -t initiator adapter_name`
 - c. Parar para voltar ao modo de manutenção: `halt`

As alterações serão implementadas quando o sistema for inicializado.

Inicie a imagem de recuperação - AFF A400

Você deve inicializar a imagem ONTAP a partir da unidade USB, restaurar o sistema de

arquivos e verificar as variáveis ambientais.

Passos

1. 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 sistema de ficheiros var:

Opção 1: ONTAP 9.16,0 ou anterior

- a. No controlador para deficientes, prima Y quando vir `Do you want to restore the backup configuration now?`
- b. No controlador prejudicado, Y pressione quando solicitado a substituir `/etc/ssh/ssh_host_ecdsa_key`.
- c. No controlador de parceiro saudável, defina o controlador prejudicado para nível de privilégio avançado: `set -privilege advanced`.
- d. No controlador do parceiro saudável, execute o comando `Restore backup: system node restore-backup -node local -target-address impaired_node_IP_address`.

NOTA: se você vir qualquer mensagem que não seja uma restauração bem-sucedida, entre em Contato "[Suporte à NetApp](#)" com .

- e. No controlador do parceiro saudável, devolva o controlador afetado ao nível de administração: `set -privilege admin`.
- f. No controlador para deficientes, prima Y quando vir `Was the restore backup procedure successful?`.
- g. No controlador para deficientes, prima Y quando vir `...would you like to use this restored copy now?`.
- h. No controlador desativado, Y prima quando for solicitado que reinicie o controlador desativado e prima `ctrl-c` para aceder ao Menu de arranque.
- i. Se o sistema não usar criptografia, selecione *opção 1 Inicialização normal.*, caso contrário, vá para "[Restaure a criptografia](#)".

Opção 2: ONTAP 9.16,1 ou posterior

- a. No controlador afetado, prima Y quando for solicitado que restaure a configuração de cópia de segurança.

Depois que o procedimento de restauração for bem-sucedido, essa mensagem será exibida no console - `syncflash_partner: Restore from partner complete`.

- b. No controlador desativado, Y prima quando solicitado para confirmar se a cópia de segurança de restauro foi bem sucedida.
- c. No controlador prejudicado, Y pressione quando solicitado a usar a configuração restaurada.
- d. No controlador prejudicado, Y pressione quando solicitado a reinicializar o nó.
- e. No controlador desativado, Y prima quando for solicitado que reinicie o controlador desativado e prima `ctrl-c` para aceder ao Menu de arranque.
- f. Se o sistema não usar criptografia, selecione *opção 1 Inicialização normal.*, caso contrário, vá para "[Restaure a criptografia](#)".

4. Conete o cabo do console ao controlador do parceiro.
5. Devolva o controlador usando o `storage failover giveback -fromnode local` comando.
6. Restaure o giveback automático se você o desativou usando o `storage failover modify -node local -auto-giveback true` comando.

7. Se o AutoSupport estiver ativado, restaure/dessuprimir a criação automática de casos usando o `system node autosupport invoke -node * -type all -message MAINT=END` comando.

NOTA: se o processo falhar, entre em Contato ["Suporte à NetApp"](#) com .

Alterne agregados em uma configuração de MetroCluster de dois nós - AFF A400

Depois de concluir a substituição da FRU em uma configuração de MetroCluster de dois nós, você pode executar a operação de switchback do MetroCluster. Isso retorna a configuração ao seu estado operacional normal, com as máquinas virtuais de armazenamento de origem sincronizada (SVMs) no site anteriormente prejudicado agora ativo e fornecendo dados dos pools de discos locais.

Esta tarefa só se aplica a configurações de MetroCluster de dois nós.

Passos

1. Verifique se todos os nós estão no `enabled` estado: `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. Verifique se a ressincronização está concluída em todos os SVMs: `metrocluster vserver show`
3. Verifique se todas as migrações automáticas de LIF que estão sendo executadas pelas operações de recuperação foram concluídas com sucesso: `metrocluster check lif show`
4. Execute o switchback usando o `metrocluster switchback` comando de qualquer nó no cluster sobrevivente.
5. Verifique se a operação de comutação foi concluída: `metrocluster show`

A operação de switchback ainda está em execução quando um cluster está no `waiting-for-switchback` estado:

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

A operação de switchback é concluída quando os clusters estão no normal estado.:

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

Se um switchback estiver demorando muito tempo para terminar, você pode verificar o status das linhas de base em andamento usando o `metrocluster config-replication resync-status show` comando.

6. Restabelecer qualquer configuração SnapMirror ou SnapVault.

Restaurar encriptação - AFF A400

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

Opção 1: Restaure 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="626 281 899 310">Selecione a opção 10.</p> <p data-bbox="626 344 1153 373">Mostrar exemplo de menu de inicialização</p> <div data-bbox="656 415 1455 1197" style="border: 1px solid #ccc; padding: 10px;"><pre data-bbox="685 453 1370 1163">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

```
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 A400

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.