



Suporte de arranque

Install and maintain

NetApp
January 10, 2025

Índice

- Suporte de arranque 1
 - Descrição geral da substituição do suporte de arranque - FAS500f 1
 - Verifique o suporte e o status da chave de criptografia - FAS500f 1
 - Desligue o controlador - FAS500f 4
 - Substitua o suporte de arranque - FAS500f 6
 - Inicie a imagem de recuperação - FAS500f 13
 - Restaurar encriptação - FAS500f 16
 - Devolva a peça com falha ao NetApp - FAS500f 26

Suporte de arranque

Descrição geral da substituição do suporte de arranque - FAS500f

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.

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

- 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 - FAS500f

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><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. <p>Se todas as chaves de autenticação forem <code>true</code>, pode desligar o controlador com segurança. Vá para "desligue o controlador desativado".</p>

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. <p>Você vai precisar dele em cenários de desastre onde você pode precisar recuperar manualmente OKM.</p>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 - FAS500f

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 um 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)	<p>Assuma ou interrompa o controlador prejudicado do controlador saudável: <code>storage failover takeover -ofnode <i>impaired_node_name</i></code></p> <p>Quando o controlador prejudicado mostrar aguardando a giveback..., pressione Ctrl-C e responda <code>y</code>.</p>

Substitua o suporte de arranque - FAS500f

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

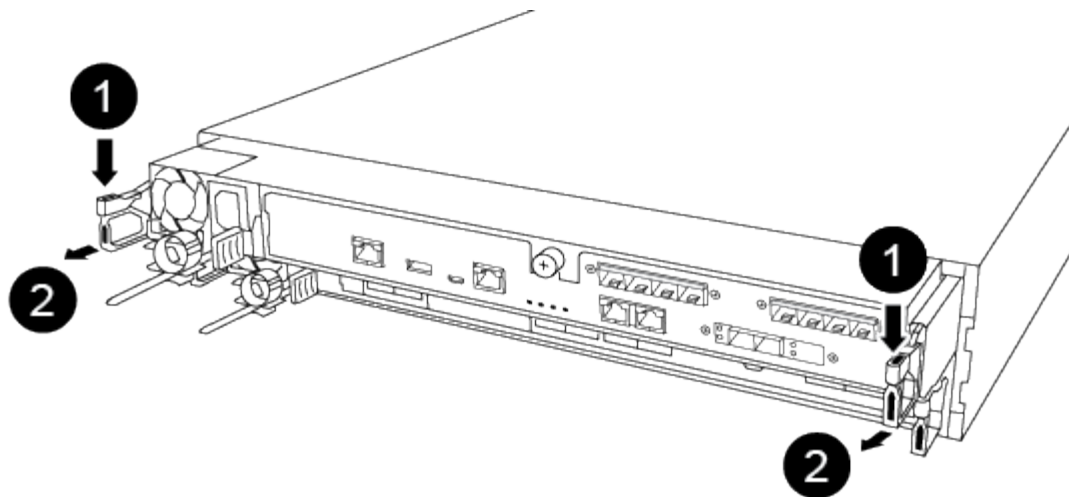
Deve remover o módulo do controlador do chassis quando substituir um componente no interior do módulo do controlador.

Certifique-se de etiquetar os cabos para que saiba de onde vieram.

1. Se você ainda não está aterrado, aterre-se adequadamente.
2. Desconete as fontes de alimentação do módulo do controlador da fonte.
3. Solte os fixadores do cabo de alimentação e, em seguida, desconete os cabos das fontes de alimentação.
4. Insira o dedo indicador no mecanismo de travamento em ambos os lados do módulo do controlador, pressione a alavanca com o polegar e puxe o controlador cuidadosamente alguns centímetros para fora do chassi.

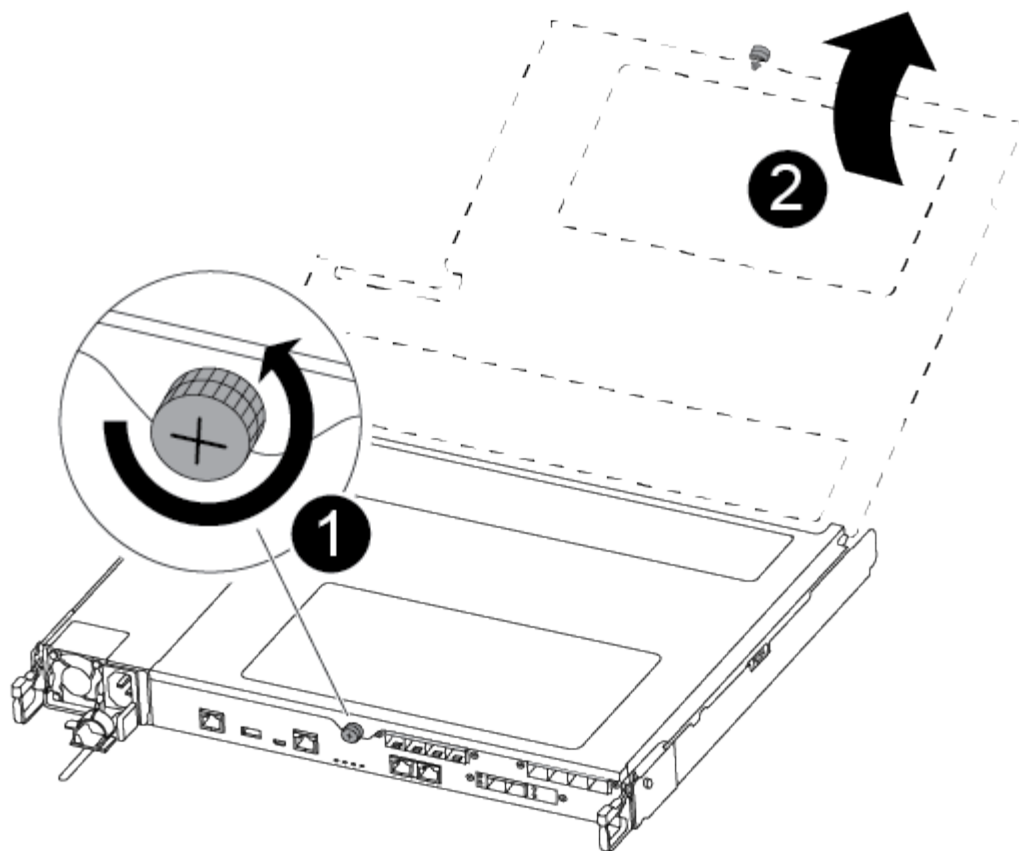


Se tiver dificuldade em remover o módulo do controlador, coloque os dedos indicadores através dos orifícios dos dedos a partir do interior (cruzando os braços).



1
Alavanca
2
Mecanismo de bloqueio

5. Usando ambas as mãos, segure os lados do módulo do controlador e puxe-o suavemente para fora do chassi e coloque-o em uma superfície plana e estável.
6. Rode o parafuso de aperto manual na parte frontal do módulo do controlador no sentido contrário ao dos ponteiros do relógio e abra a tampa do módulo do controlador.



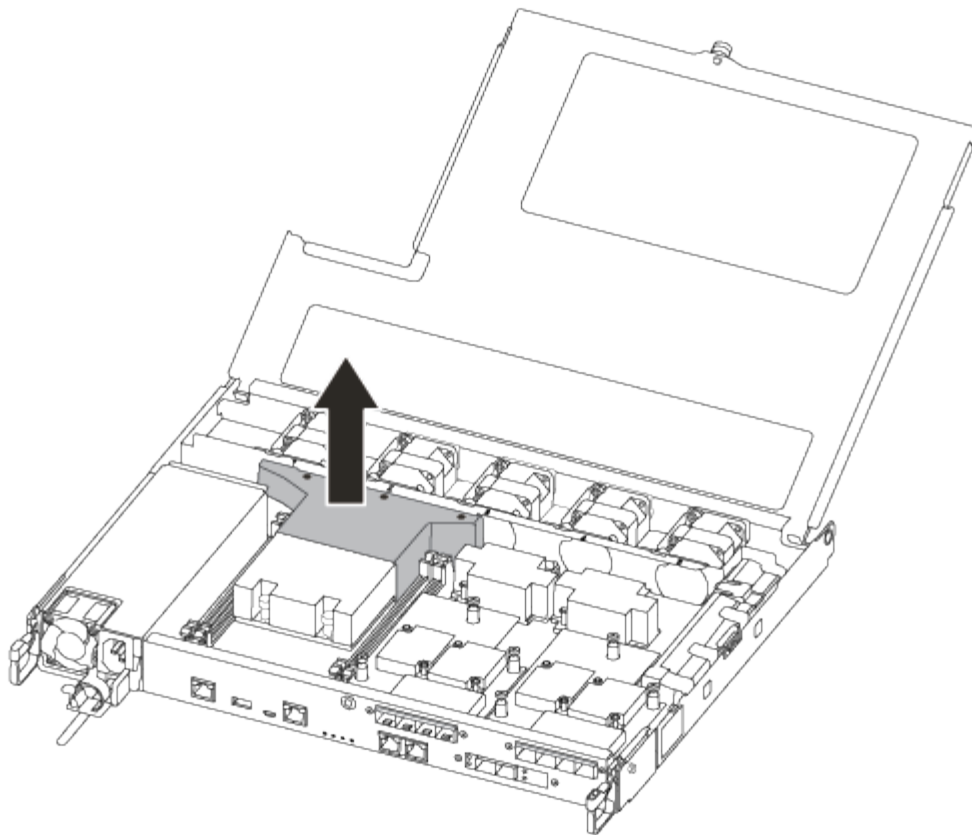
1

Parafuso de aperto manual

2

Tampa do módulo do controlador.

7. Levante a tampa da conduta de ar.



Passo 2: Substitua o suporte de arranque

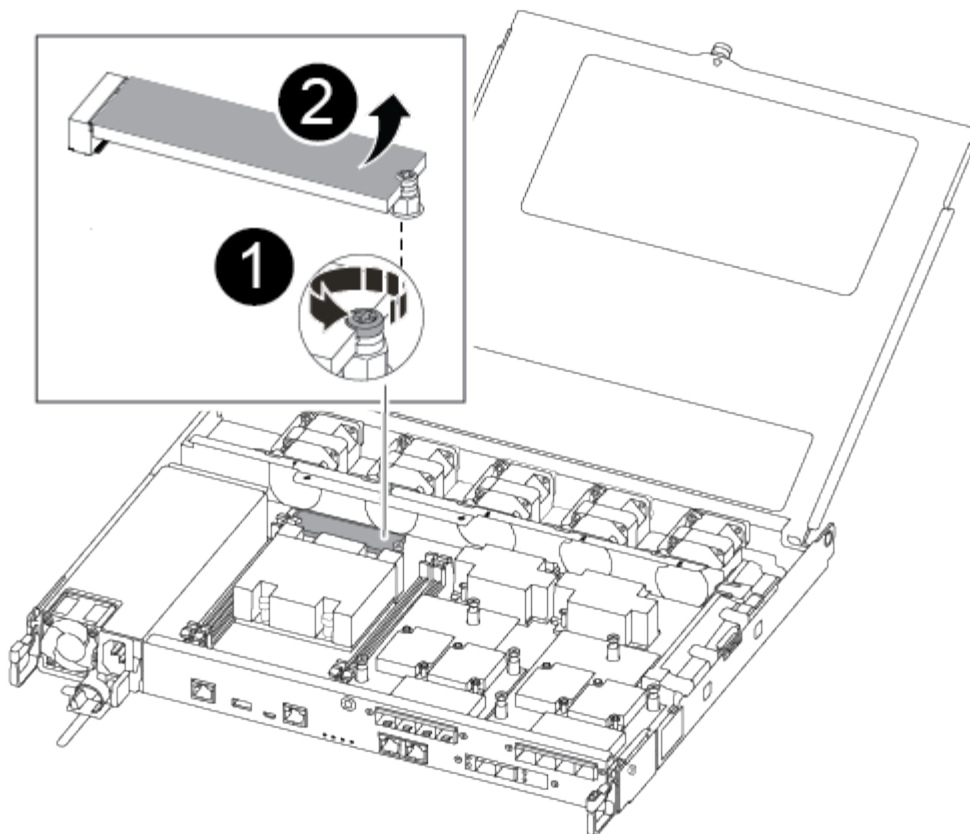
Pode localizar o suporte de arranque avariado no módulo do controlador removendo a conduta de ar no módulo do controlador antes de poder substituir o suporte de arranque.

Você precisa de uma chave de fenda Phillips magnética nº 1 para remover o parafuso que prende o suporte de inicialização no lugar. Devido às restrições de espaço dentro do módulo do controlador, você também deve ter um ímã para transferir o parafuso para para que você não o solte.

Pode utilizar o seguinte vídeo ou as etapas tabuladas para substituir o suporte de arranque:

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

1. Localize e substitua os suportes de arranque danificados a partir do módulo do controlador.



1

Retire o parafuso que fixa o suporte de arranque à placa-mãe no módulo do controlador.

2

Levante o suporte de arranque para fora do módulo do controlador.

- a. Utilizando a chave de fendas magnética nº 1, retire o parafuso do suporte de arranque danificado e coloque-o de lado com segurança no íman.
- b. Levante cuidadosamente o suporte da bagageira danificado diretamente para fora da tomada e coloque-o de lado.
- c. Retire o suporte de substituição da bolsa de transporte antiestática e alinhe-o no lugar no módulo da controladora.
- d. Utilizando a chave de fendas magnética nº 1, introduza e aperte o parafuso no suporte de arranque.



Não aplique força ao apertar o parafuso na Mídia de inicialização; você pode quebrá-lo.

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

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

- 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 sistema de ficheiros var.

Passos

1. Transfira e copie a imagem de serviço apropriada do site de suporte da NetApp para a unidade flash USB.
2. Transfira a imagem de serviço para o seu espaço de trabalho no seu computador portátil.
3. 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.

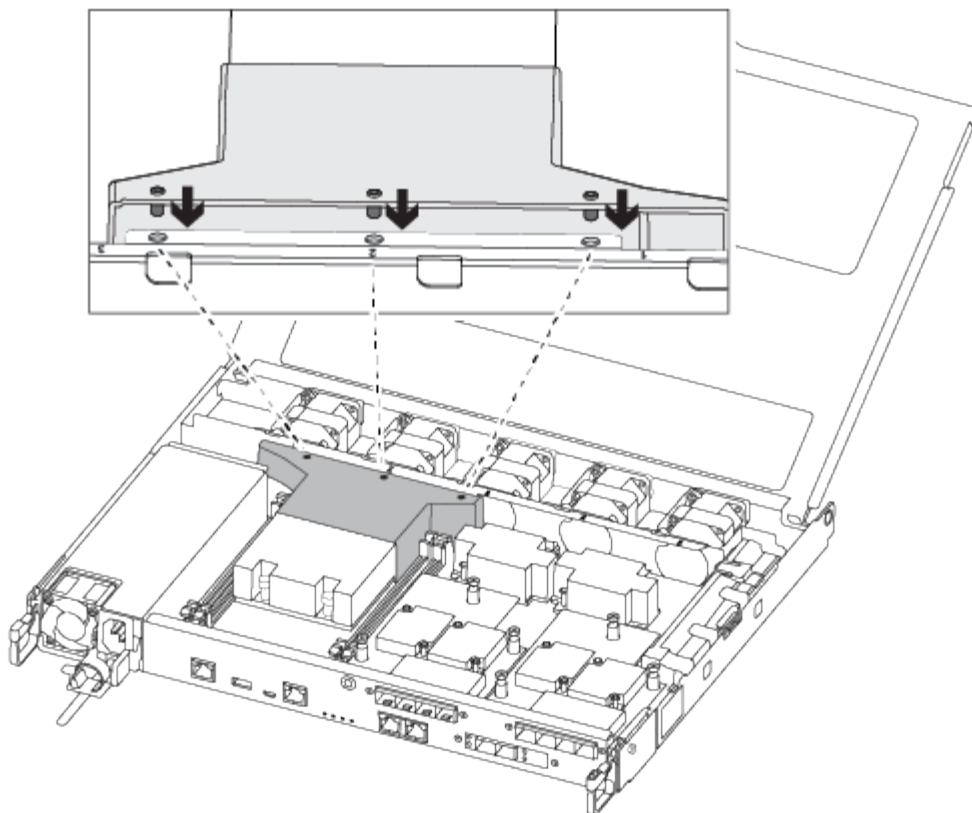
Há duas pastas no arquivo de imagem de serviço descompactado:

- boot
- efi

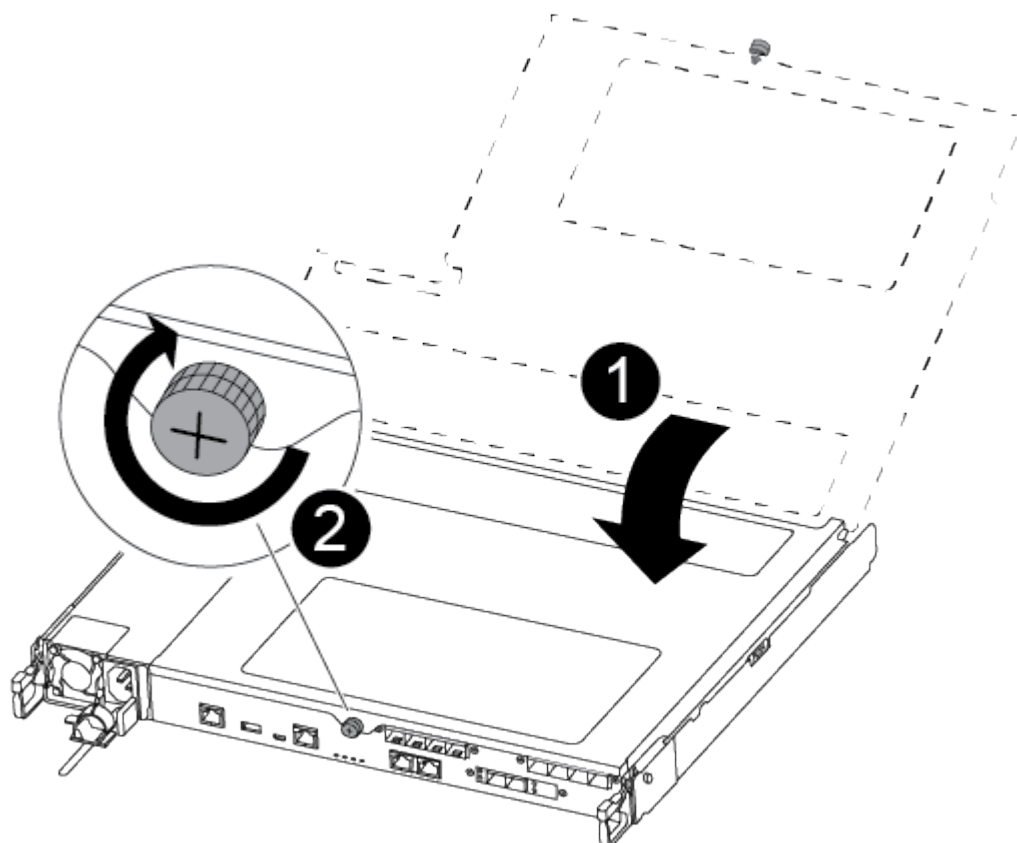
4. Copie a `efi` pasta para o diretório superior da unidade flash USB.

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.

5. Retire a unidade flash USB do seu computador portátil.
6. Se ainda não o tiver feito, instale a conduta de ar.



7. Feche a tampa do módulo do controlador e aperte o parafuso de aperto manual.



1

Tampa do módulo do controlador

2

Parafuso de aperto manual

8. 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.
9. Ligue o cabo de alimentação à fonte de alimentação e volte a instalar o fixador do cabo de alimentação.
10. 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.

11. Empurre o módulo do controlador até ao chassis:
12. Coloque os dedos indicadores através dos orifícios dos dedos a partir do interior do mecanismo de bloqueio.
13. Pressione os polegares para baixo nas patilhas cor-de-laranja na parte superior do mecanismo de bloqueio e empurre suavemente o módulo do controlador sobre o batente.
14. Solte os polegares da parte superior dos mecanismos de travamento e continue empurrando até que os mecanismos de travamento se encaixem no lugar.

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

O módulo do controlador deve ser totalmente inserido e alinhado com as bordas do chassi.

Inicie a imagem de recuperação - FAS500f

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:

Se o seu sistema tem...	Então...
Uma ligação de rede	<ul 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	<ul 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>

Se o seu sistema tem...	Então...
Sem conexão de rede e está em uma configuração IP MetroCluster	<p>a. Pressione n quando solicitado para restaurar a configuração de backup.</p> <p>b. Reinicie o sistema quando solicitado pelo sistema.</p> <p>c. Aguarde que as ligações de armazenamento iSCSI se liguem.</p> <p>Você pode prosseguir depois de ver as seguintes mensagens:</p> <pre data-bbox="672 428 1489 1289"> date-and-time [node- name:iscsi.session.stateChanged:notice]: iSCSI session state is changed to Connected for the target iSCSI-target (type: dr_auxiliary, address: ip-address). date-and-time [node- name:iscsi.session.stateChanged:notice]: iSCSI session state is changed to Connected for the target iSCSI-target (type: dr_partner, address: ip-address). date-and-time [node- name:iscsi.session.stateChanged:notice]: iSCSI session state is changed to Connected for the target iSCSI-target (type: dr_auxiliary, address: ip-address). date-and-time [node- name:iscsi.session.stateChanged:notice]: iSCSI session state is changed to Connected for the target iSCSI-target (type: dr_partner, address: ip-address). </pre> <p>d. Selecione a opção Update flash from backup config (Sync flash) no menu exibido.</p> <p>Se for solicitado que você continue com a atualização, y pressione .</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 `savenv` 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...	a. Faça login no controlador do parceiro. b. Confirme se o controlador de destino está pronto para giveback com o <code>storage failover show</code> comando.

7. Conete o cabo do console ao controlador do parceiro.
8. Devolva o controlador usando o `storage failover giveback -fromnode local` comando.
9. 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.

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

Restaurar encriptação - FAS500f

Restaure 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

Restaure 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. Conete 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="620 466 901 499">Selecione a opção 10.</p> <p data-bbox="620 535 1153 569">Mostrar exemplo de menu de inicialização</p> <div data-bbox="656 604 1455 1390" style="border: 1px solid #ccc; padding: 10px; background-color: #f9f9f9;"> <p data-bbox="683 646 1295 680">Please choose one of the following:</p> <ul style="list-style-type: none"> <li data-bbox="683 726 971 760">(1) Normal Boot. <li data-bbox="683 768 1133 802">(2) Boot without /etc/rc. <li data-bbox="683 810 1052 844">(3) Change password. <li data-bbox="683 852 1367 919">(4) Clean configuration and initialize all disks. <li data-bbox="683 928 1156 961">(5) Maintenance mode boot. <li data-bbox="683 970 1328 1003">(6) Update flash from backup config. <li data-bbox="683 1012 1247 1045">(7) Install new software first. <li data-bbox="683 1054 977 1087">(8) Reboot node. <li data-bbox="683 1096 1188 1163">(9) Configure Advanced Drive Partitioning. <li data-bbox="683 1171 1334 1239">(10) Set Onboard Key Manager recovery secrets. <li data-bbox="683 1247 1318 1314">(11) Configure node for external key management. <p data-bbox="683 1323 1036 1356">Selection (1-11)? 10</p> </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 - FAS500f

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.