Suporte de arranque

Install and maintain

NetApp
January 10, 2025

Índice

Suporte de arranque

Visão geral e requisitos ASA A250

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.

Antes de começar

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

Sobre esta tarefa

- 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 nestas etapas no controlador correto:
  - O nó *prejudicado* é o controlador no qual você está realizando a manutenção.
  - O nó *Healthy* é o parceiro de HA do controlador prejudicado.

Verifique o suporte e o status da chave de criptografia - ASA A250

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	`security key-manager keystore show` • 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	`security key-manager show-key-store` • 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 `Restored` na coluna	**Siga estes passos…**
`true`	Pode desligar o controlador com segurança. Vá para "desligue o controlador desativado".
Qualquer outra coisa que não `true`	a. Restaure as chaves de autenticação de gerenciamento de chaves externas para todos os nós no cluster usando o seguinte comando: `security key-manager external restore` Se o comando falhar, contactar "Suporte à NetApp". b. Verifique se a `Restored` coluna é exibida `true` para todas as chaves de autenticação inserindo o `security key-manager key query` comando. Se todas as chaves de autenticação forem `true`, 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 `Restored` na coluna	**Siga estes passos…**
`true`	Faça backup manual das informações OKM. a. Vá para o modo avançado entrando `set -priv advanced` e, em seguida, entre `Y` quando solicitado. b. Digite o seguinte comando para exibir as informações de gerenciamento de chaves: `security key-manager onboard show-backup` c. 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. d. 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`	a. Digite o comando Onboard security key-manager sync:
	
	`security key-manager onboard sync`
	
	b. Digite a senha alfanumérica de gerenciamento de chaves integradas de 32 carateres quando solicitado.
	
	Se a frase-passe não puder ser fornecida, "Suporte à NetApp" contacte .
	
	c. Verifique se a `Restored` coluna exibe `true` todas as chaves de autenticação:
	
	`security key-manager key query`
	
	d. Verifique se o `Key Manager` tipo é exibido `onboard` e, em seguida, faça backup manual das informações OKM.
	e. Digite o comando para exibir as informações de backup de gerenciamento de chaves:
	
	`security key-manager onboard show-backup`
	
	f. 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.
	
	g. Pode desligar o controlador com segurança. Vá para "desligue o controlador desativado".

Desligue o controlador - ASA A250

Encerre ou assuma o controlador afetado utilizando o procedimento adequado para a sua configuração.

Opção 1: A maioria dos sistemas

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 `y` quando solicitado.
Prompt do sistema ou prompt de senha (digite a senha do sistema)	Assuma ou interrompa o controlador prejudicado do controlador saudável: `storage failover takeover -ofnode impaired_node_name` Quando o controlador prejudicado mostrar aguardando a giveback…, pressione Ctrl-C e responda `y`.

2. 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: Sistemas em um MetroCluster

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

> 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

1. 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`

2. Desative a giveback automática a partir da consola do controlador saudável: `storage failover modify –node local -auto-giveback false`
3. 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 `y` quando solicitado.
Prompt do sistema ou prompt de senha (digite a senha do sistema)	Assuma ou interrompa o controlador prejudicado do controlador saudável: `storage failover takeover -ofnode` *`impaired_node_name`* Quando o controlador prejudicado mostrar aguardando a giveback…, pressione Ctrl-C e responda `y`.

Substitua o suporte de arranque - ASA A250

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.

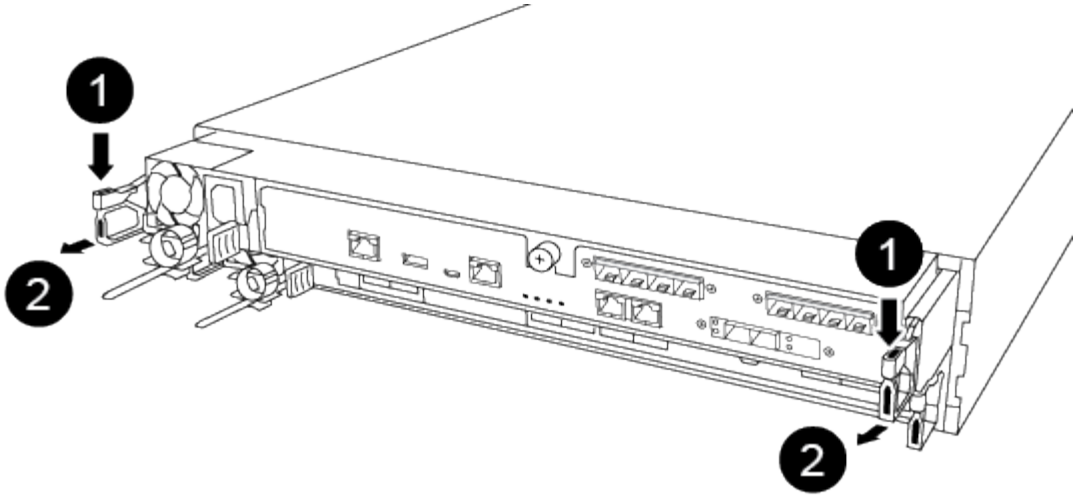
Passo 1: Remova o módulo do controlador

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

Passos

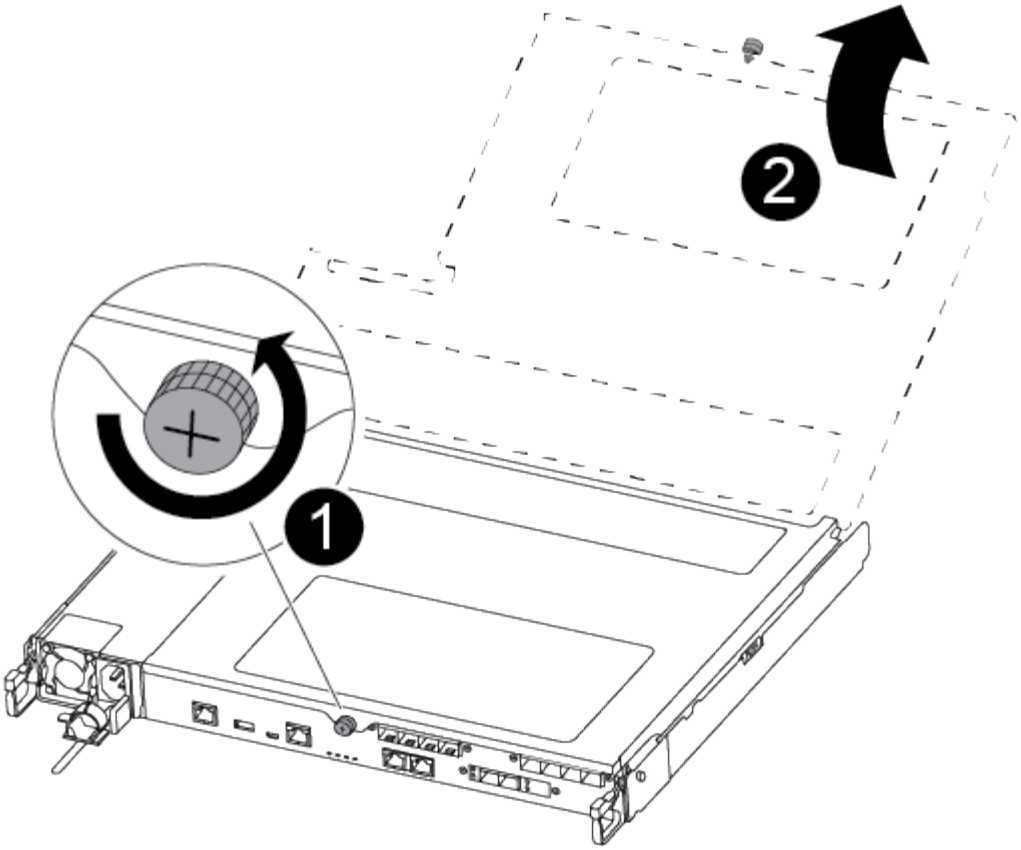
1. Se você ainda não está aterrado, aterre-se adequadamente.
2. Desconete as fontes de alimentação do módulo do controlador da fonte.
3. Solte os fixadores do cabo de alimentação e, em seguida, desconete os cabos das fontes de alimentação.
4. Insira o dedo indicador no mecanismo de travamento em ambos 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).



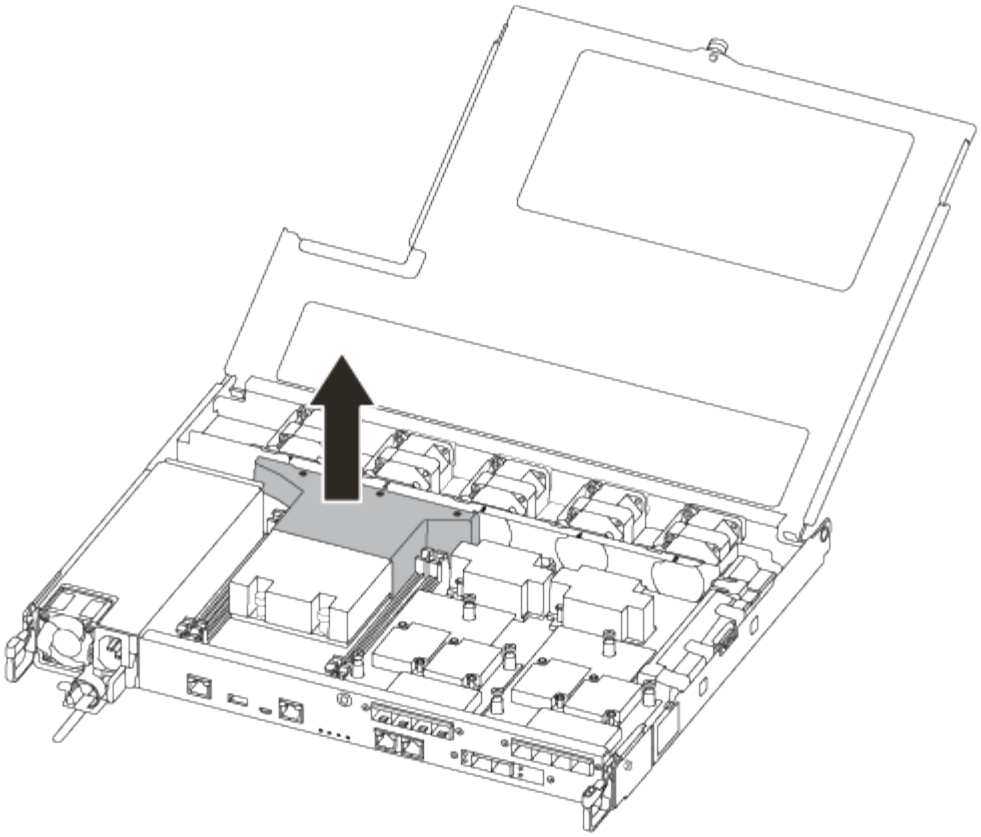
1	
Alavanca	
2	
Mecanismo de bloqueio	

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

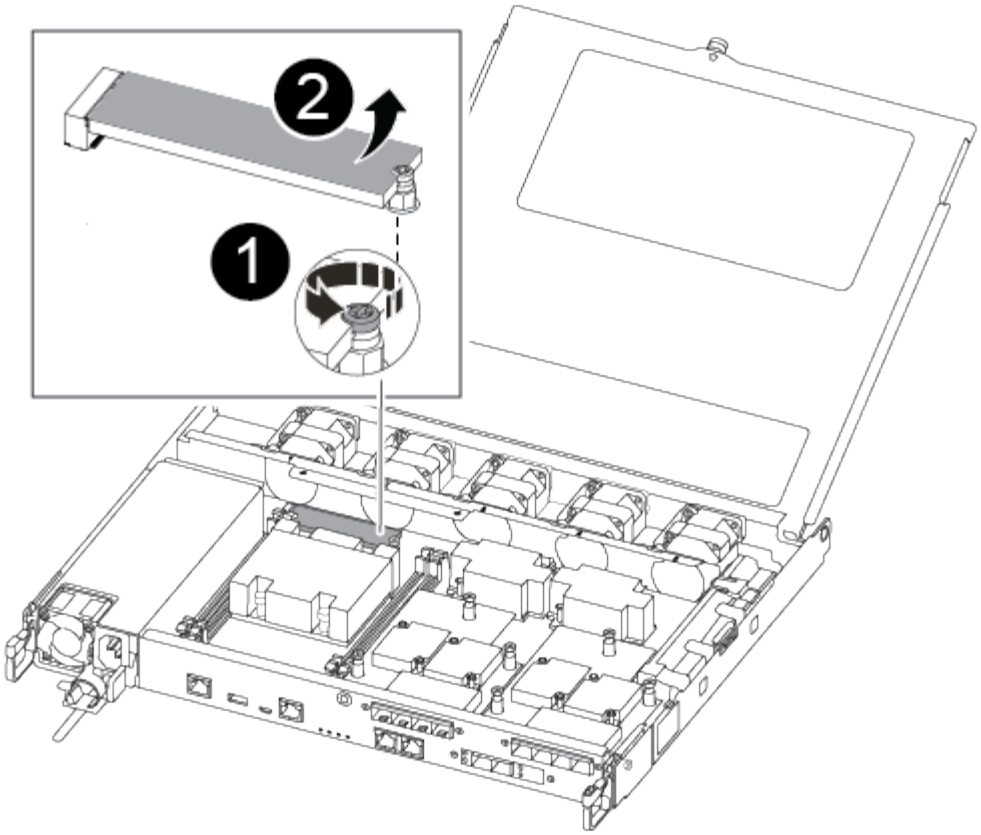
Pode localizar o suporte de arranque avariado no módulo do controlador removendo a conduta de ar no módulo do controlador antes de poder substituir o suporte de arranque.

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 que você não o perca.

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.

2. 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.
3. Levante cuidadosamente o suporte da bagageira danificado diretamente para fora da tomada e coloque-o de lado.
4. Retire o suporte de substituição da bolsa de transporte antiestática e alinhe-o no lugar no módulo da controladora.
5. 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.

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

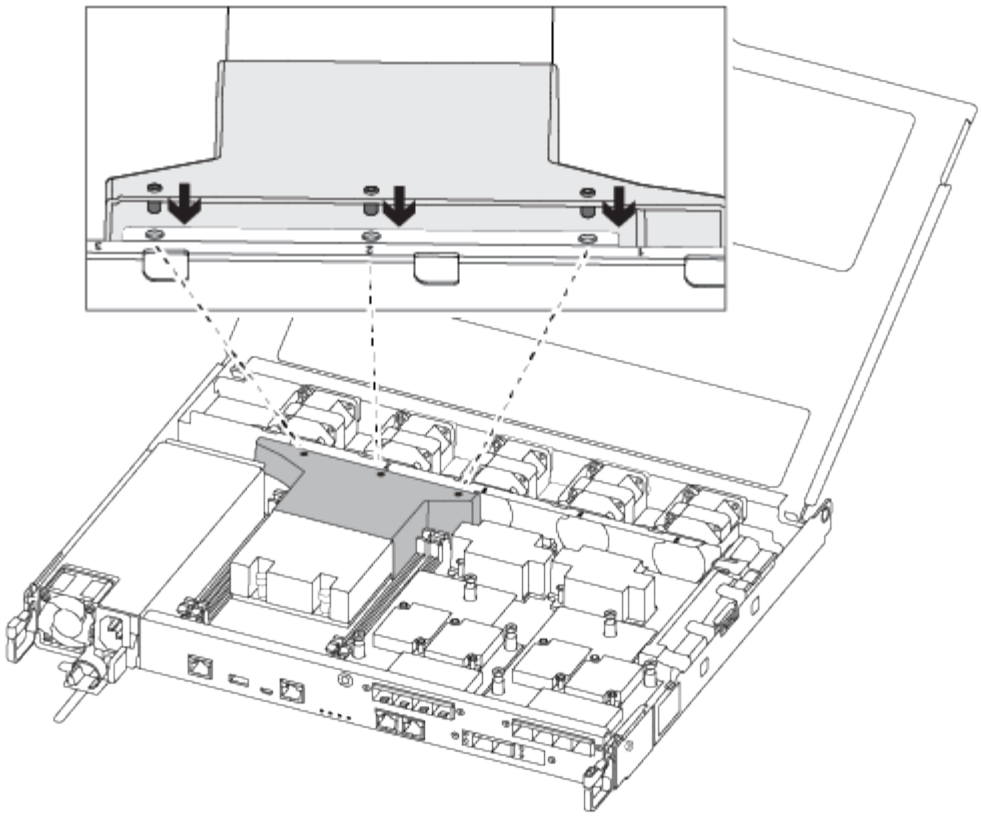
- inicialização
- efi

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

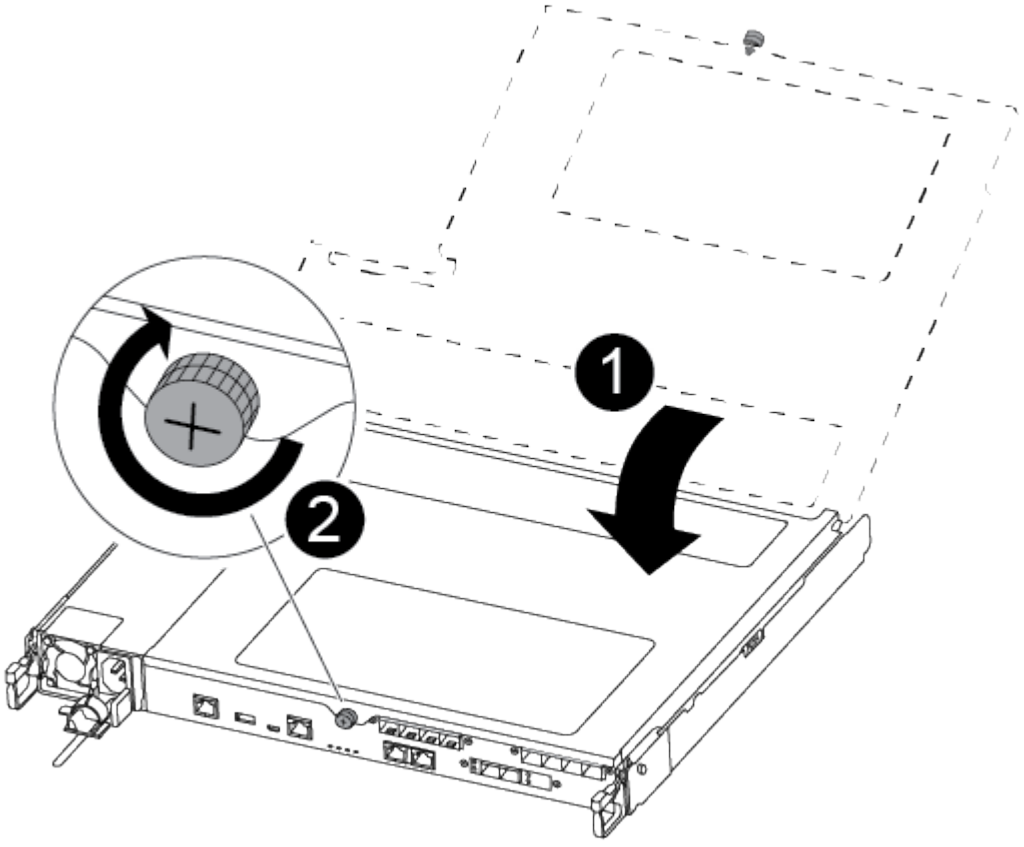
> Se a imagem de serviço não tiver uma pasta efi, "Pasta EFI ausente do arquivo de download de imagem de serviço usado para recuperação de dispositivo de inicialização para modelos FAS e AFF"consulte .

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.

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



g. 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

h. 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.

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

j. 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.

k. Empurre o módulo do controlador até ao chassis:

l. Coloque os dedos indicadores através dos orifícios dos dedos a partir do interior do mecanismo de bloqueio.

m. 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.

n. 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.

o. 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.

p. 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.

q. 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 - ASA A250

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 .

Restaurar encriptação - ASA A250

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	Selecione a opção 10. **Mostrar exemplo de menu de inicialização** ``` 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 ```

Versão de ONTAP	Selecione esta opção

ONTAP 9 F.7 e anteriores	Selecione a opção oculta `recover_onboard_keymanager`
	
	Mostrar exemplo de menu de inicialização
	
	`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`

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--------------------------
0123456789012345678901234567890123456789012345678901234567890123
1234567890123456789012345678901234567890123456789012345678901234
2345678901234567890123456789012345678901234567890123456789012345
3456789012345678901234567890123456789012345678901234567890123456
4567890123456789012345678901234567890123456789012345678901234567
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
0123456789012345678901234567890123456789012345678901234567890123
1234567890123456789012345678901234567890123456789012345678901234
2345678901234567890123456789012345678901234567890123456789012345
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

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

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

Enter the client key (client.key) file contents:
-----BEGIN RSA PRIVATE KEY-----
<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....
kmip_init: configuring ports
Running command '/sbin/ifconfig e0M'
..
..
kmip_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 - ASA A250

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

Informações sobre marcas comerciais