Suporte de arranque

Install and maintain

NetApp
January 10, 2025

Índice

Suporte de arranque 1
Substitua o suporte de arranque - FAS9500 1
Verifique o suporte e o status da chave de criptografia - FAS9500 1
Remova o controlador, substitua o suporte de arranque e transfira a imagem de arranque - FAS9500 5
Inicie a imagem de recuperação - FAS9500 11
Restaurar encriptação - FAS9500 14
Devolva a peça com falha ao NetApp - FAS9500 24

Suporte de arranque

Substitua o suporte de arranque - FAS9500

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 manter o `image_xxx.tgz`.

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 não requer conexão com uma rede para restaurar o `var` sistema de arquivos. O par de HA em um único chassi tem uma conexão e0S interna, que é usada para transferir `var` a configuração entre eles.
  - 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 - FAS9500

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".

Remova o controlador, substitua o suporte de arranque e transfira a imagem de arranque - FAS9500

Tem de remover e abrir o módulo do controlador, localizar e substituir o suporte de arranque no controlador e, em seguida, transferir a imagem para o suporte de arranque de substituição.

Passo 1: Remova o módulo do controlador

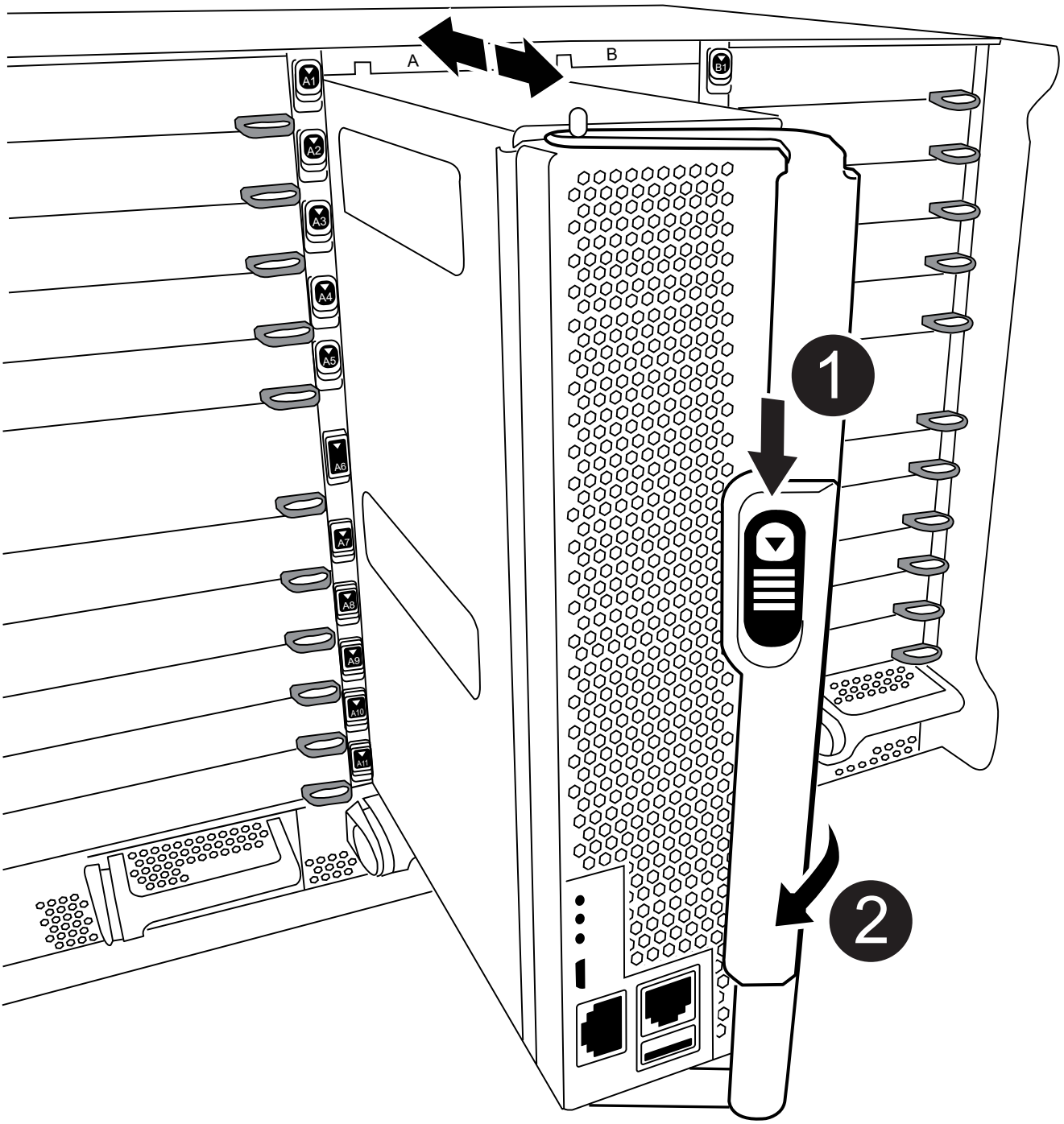
Para aceder aos componentes no interior do controlador, tem de remover primeiro o módulo do controlador do sistema e, em seguida, remover a tampa do módulo do controlador.

Passos

1. Se você ainda não está aterrado, aterre-se adequadamente.

2. Desconete os cabos do módulo do controlador desativado e mantenha o controle de onde os cabos foram conetados.
3. Deslize o botão terra cotta na pega do came para baixo até que este se destranque.

Animação - Remover módulo do controlador



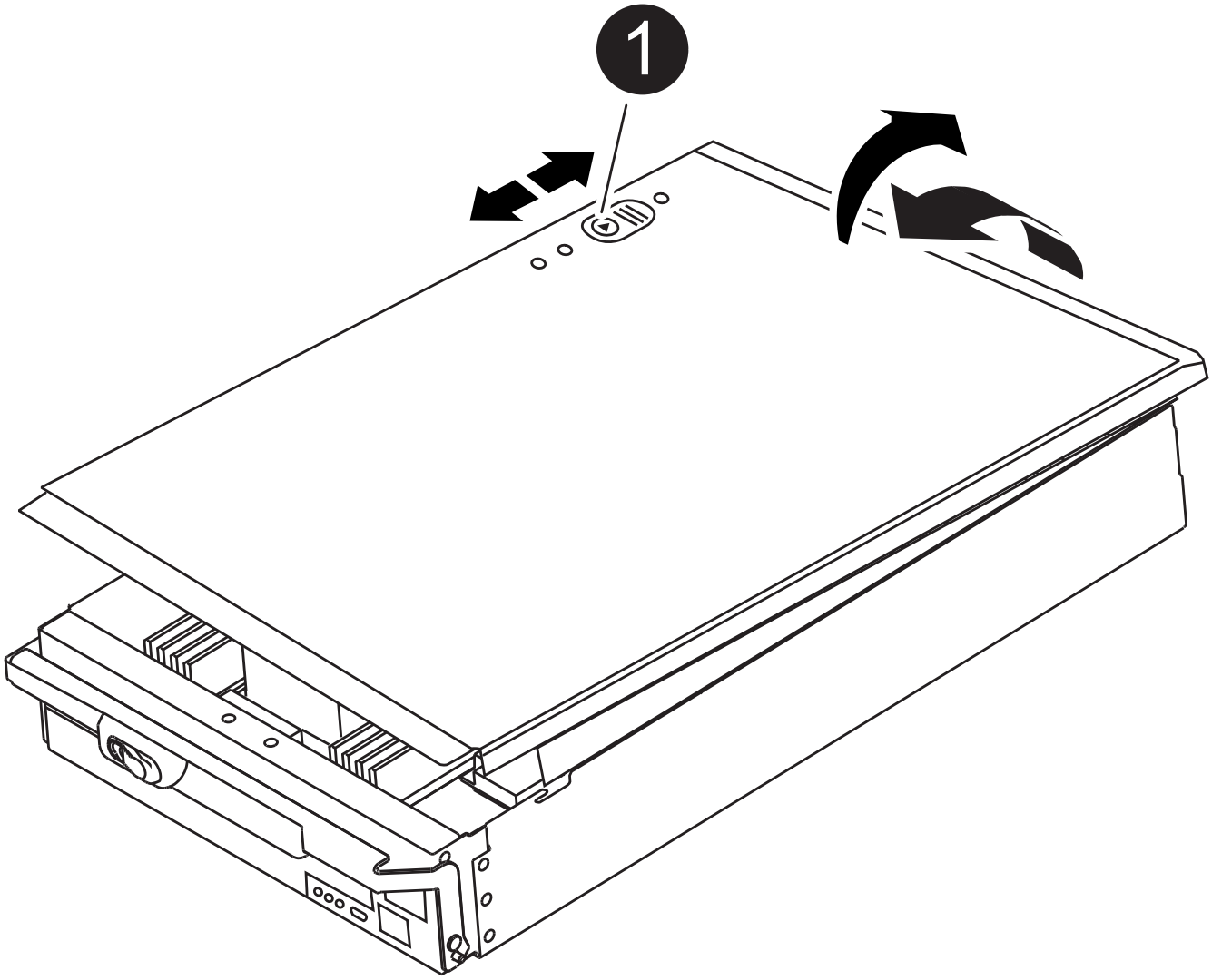
1	Botão de libertação do manípulo do excêntrico

2	Pega do came

4. Rode o manípulo do excêntrico de forma a desengatar completamente o módulo do controlador do chassis e, em seguida, deslize 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.

5. Coloque a tampa do módulo do controlador para cima sobre uma superfície estável e plana, pressione o botão azul na tampa, deslize a tampa para a parte traseira do módulo do controlador e, em seguida, gire a tampa para cima e levante-a do módulo do controlador.



1	Botão de bloqueio da tampa do módulo do controlador

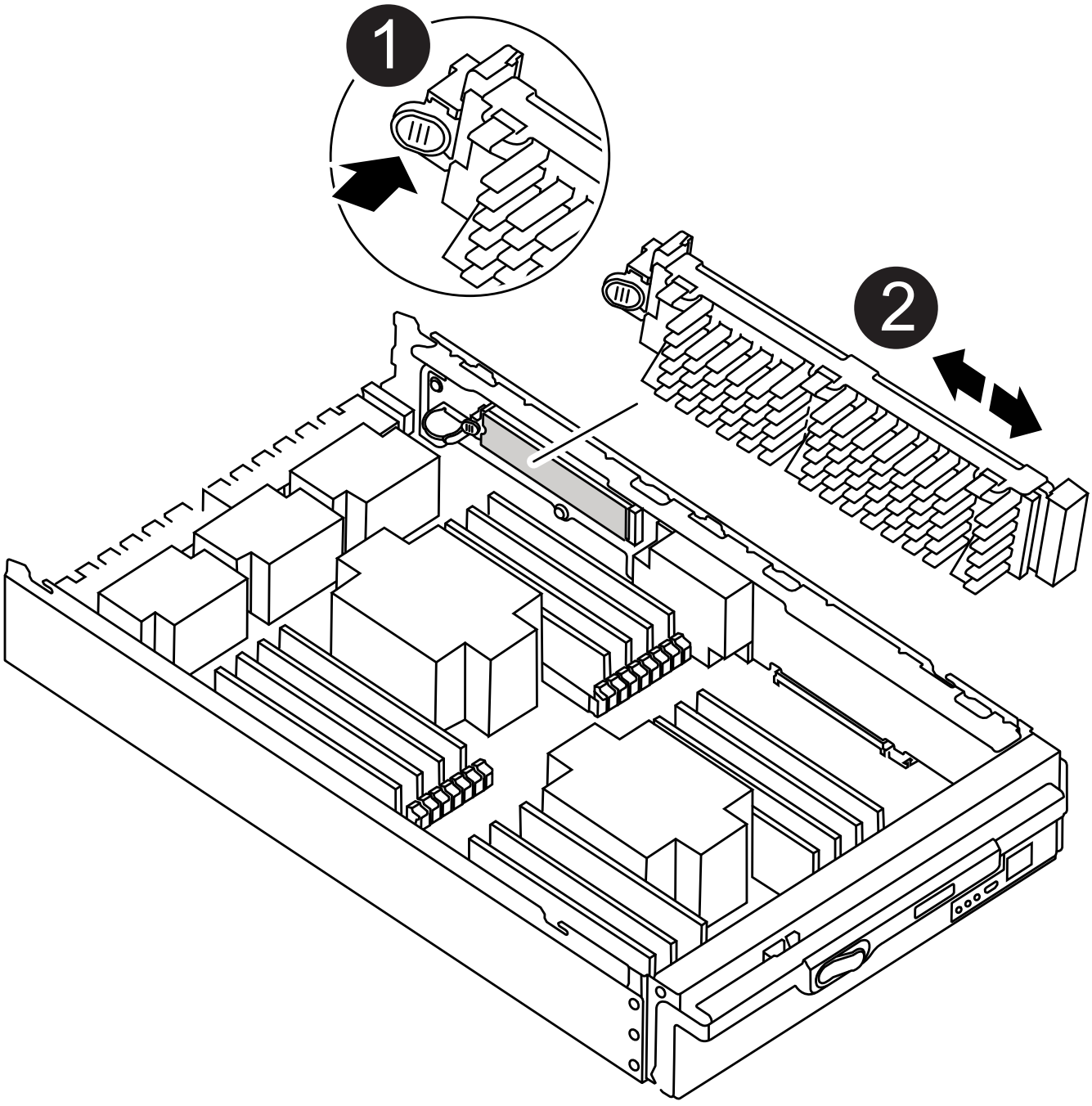
Passo 2: Substitua o suporte de arranque

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

Passos

1. Levante a conduta de ar preta na parte de trás do módulo do controlador e, em seguida, localize o suporte de arranque utilizando a ilustração a seguir ou o mapa da FRU no módulo do controlador:

   Animação - Substituir Mídia de inicialização



1	Prima o separador de libertação
2	Suporte de arranque

2. Prima o botão azul no alojamento do suporte do suporte de arranque para soltar o suporte de arranque do

respetivo alojamento e, em seguida, puxe-o cuidadosamente para fora do suporte de suporte de arranque.

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

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. Prima o suporte de arranque para baixo para engatar o botão de bloqueio no alojamento do suporte de suporte de arranque.
6. Reinstale a tampa do módulo do controlador alinhando os pinos na tampa com os slots no suporte da placa-mãe e, em seguida, deslize a tampa para o lugar.

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

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

Antes de começar

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

Passos

1. Alinhe a extremidade do módulo do controlador com a abertura no chassis e, em seguida, empurre cuidadosamente o módulo do controlador até meio do sistema.
2. Recable o módulo do controlador, conforme necessário.
3. Introduza a unidade flash USB na ranhura USB do módulo do controlador.

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

4. Empurre o módulo do controlador totalmente para dentro do sistema, certificando-se de que a pega da câmara limpa a unidade flash USB, empurre firmemente a pega da câmara para terminar de assentar o módulo do controlador e, em seguida, empurre a pega da câmara para a posição fechada.

   O nó começa a inicializar assim que é completamente instalado no chassi.

5. 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 nó para inicializar NO Loader.

6. Embora as variáveis de ambiente e bootargs sejam mantidas, você deve verificar se todas as variáveis de ambiente de inicialização necessárias e bootargs estão corretamente definidas para o seu tipo de sistema e configuração usando o `printenv bootarg name` comando e corrigir quaisquer erros usando o `setenv variable-name <value>` comando.
   a. Verifique as variáveis de ambiente de inicialização:
      - bootarg.init.boot_clustered
      - sistema de parceiro
      - bootarg.init.flash_optimized para AFF
      - bootarg.init.san_optimized para AFF
      - bootarg.init.switchless_cluster.enable
   b. Se o Gerenciador de chaves Externo estiver habilitado, verifique os valores de inicialização listados na `kenv` saída ASUP:
      - bootarg.storageencryption.support <value>
      - bootarg.keymanager.support <value>
      - kmip.init.interface <value>
      - kmip.init.ipaddr <value>
      - kmip.init.netmask <value>
      - kmip.init.gateway <value>
   c. Se o Gerenciador de chaves integrado estiver habilitado, verifique os valores de bootarg listados na `kenv` saída ASUP:
      - bootarg.storageencryption.support <value>
      - bootarg.keymanager.support <value>
      - bootarg.onboard_keymanager <value>
   d. Salve as variáveis de ambiente que você alterou com o `savenv` comando
   e. Confirme as alterações usando o `printenv variable-name` comando.
7. 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 usada para se comunicar com o nó prejudicado do nó saudável durante a restauração do sistema de arquivos var com uma conexão 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 da rede.
- DNS_addr é o endereço IP de um servidor de nomes em sua 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 inserir a ajuda ifconfig no prompt do firmware para obter detalhes.

8. Se o controlador estiver em um MetroCluster elástico ou conetado 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 iniitator 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 - FAS9500

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

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	a. Pressione `y` quando solicitado para restaurar a configuração de backup. b. Pressione `y` quando solicitado a substituir `/etc/ssh/ssh_host_ecdsa_key`. c. Pressione `y` quando solicitado para confirmar se o backup de restauração foi bem-sucedido. d. Pressione `Y` quando solicitado para a cópia de configuração restaurada. e. Defina o nó saudável para nível de privilégio avançado: `set -privilege advanced` f. Execute o comando Restore backup: `system node restore-backup -node local -target-address impaired_node_IP_address` g. Retorne o nó ao nível de administrador: `set -privilege admin` h. Pressione `y` quando solicitado a usar a configuração restaurada. i. Pressione `y` quando solicitado para reinicializar o nó.
Sem ligação à rede	a. Pressione `n` 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. Se for solicitado que você continue com a atualização, `y` pressione .

Se o seu sistema tem…	Então…

Sem conexão de rede e está em uma configuração IP MetroCluster	a. Pressione `n` quando solicitado para restaurar a configuração de backup.
	b. Reinicie o sistema quando solicitado pelo sistema.
	c. Aguarde que as ligações de armazenamento iSCSI se liguem.
	Você pode prosseguir depois de ver as seguintes mensagens:
	`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).`
	d. Selecione a opção **Update flash from backup config** (Sync flash) no menu exibido.
	Se for solicitado que você continue com a atualização, `y` pressione .

4. Certifique-se de que as variáveis ambientais estão definidas como esperado:
   a. Leve o nó para o prompt Loader.
   b. Verifique as configurações de variáveis de ambiente com o `printenv` comando.
   c. Se uma variável de ambiente não for definida como esperado, modifique-a com o `setenv` *`environment_variable_name changed_value`* comando.
   d. Salve suas alterações usando o `saveenv` comando.
5. O próximo depende da configuração do sistema:

- Se o sistema tiver o gerenciador de chaves integrado, NSE ou NVE configurado, vá para Etapas de substituição de Mídia de pós-inicialização para OKM, NSE e NVE
- 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 nó do parceiro. b. Confirme se o nó de destino está pronto para giveback com o `storage failover show` comando.

7. Conete o cabo do console ao nó do parceiro.
8. Devolva o nó 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 nó 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 - FAS9500

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 - FAS9500

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