



Suporte de arranque

Install and maintain

NetApp
August 18, 2025

This PDF was generated from <https://docs.netapp.com/pt-br/ontap-systems/fas2800/bootmedia-replace-overview.html> on August 18, 2025. Always check docs.netapp.com for the latest.

Índice

Suporte de arranque	1
Descrição geral da substituição do suporte de arranque - FAS2820	1
Verifique o suporte e o status da chave de criptografia - FAS2820	1
Passo 1: Verifique se a sua versão do ONTAP suporta encriptação de volume NetApp	1
Passo 2: Determine se é seguro desligar o controlador	2
Desligue o controlador desativado - FAS2820	5
Substitua o suporte de arranque - FAS2820	6
Passo 1: Remova o módulo do controlador	6
Passo 2: Substitua o suporte de arranque	7
Passo 3: Transfira a imagem de arranque para o suporte de arranque	9
Inicie a imagem de recuperação - FAS2820	10
Restaurar encriptação - FAS2820	12
Opção 1: Restaure a configuração do Gerenciador de chaves integrado	12
Opção 2: Restaure a configuração do Gerenciador de chaves Externo	18
Devolva a peça com falha ao NetApp - FAS2820	22

Suporte de arranque

Descrição geral da substituição do suporte de arranque - FAS2820

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

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

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

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

Verifique o suporte e o status da chave de criptografia - FAS2820

Para garantir a segurança dos dados no sistema de armazenamento, é necessário verificar o suporte e o status da chave de criptografia na Mídia de inicialização. Verifique se sua versão do ONTAP suporta criptografia de volume NetApp (NVE) e, antes de desligar a controladora, verifique se o gerenciador de chaves está ativo.

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.

Passos

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.

Passos

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

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

O que se segue?

Depois de verificar o suporte e o status da chave de criptografia na Mídia de inicialização, é necessário "[desligue o controlador](#)".

Desligue o controlador desativado - FAS2820

Desligue ou assuma o controlador desativado.

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: <code>storage failover takeover -ofnode impaired_node_name</code> 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.

O que se segue?

Depois de desligar o controlador, é necessário "[substitua o suporte de arranque](#)".

Substitua o suporte de arranque - FAS2820

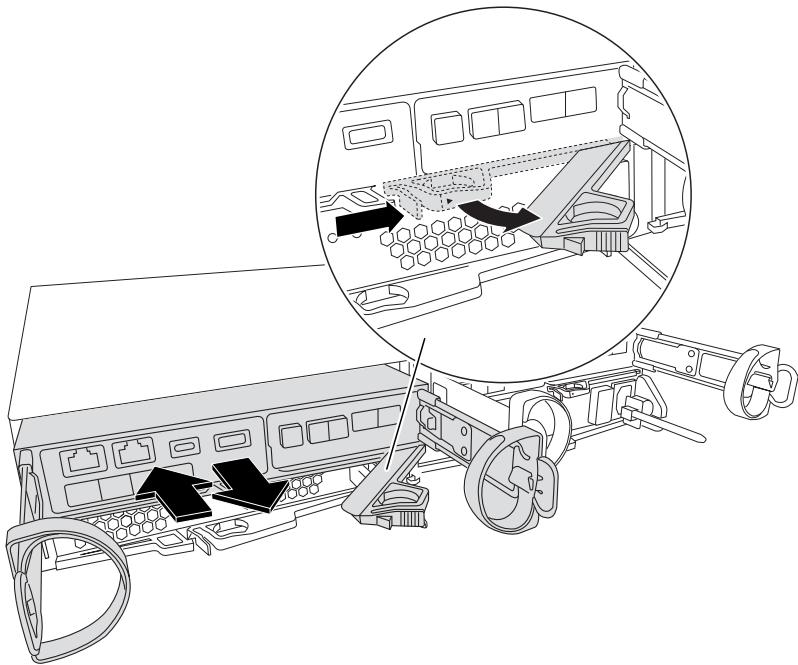
Você deve remover e abrir o módulo do controlador danificado, localizar e recolocar a mídia de inicialização no controlador, transferir a imagem de inicialização para uma unidade USB, inserir a unidade USB no controlador e, em seguida, inicializar o controlador.

Passo 1: Remova o módulo do controlador

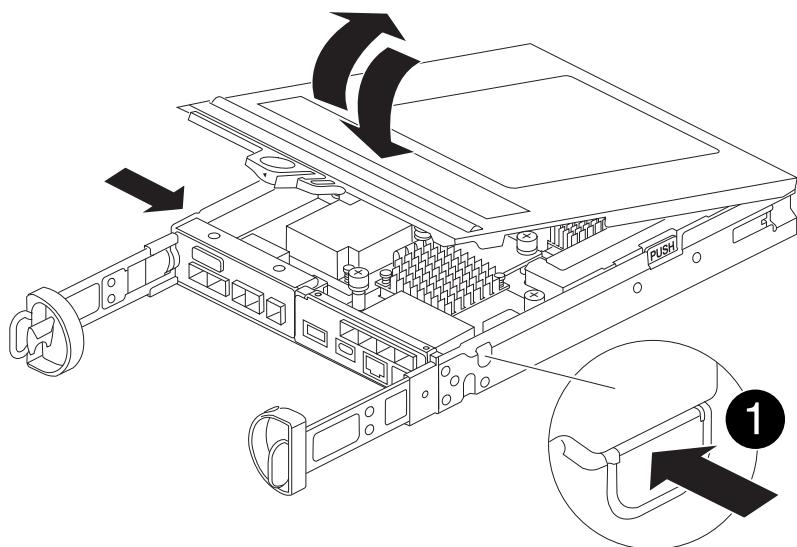
Passos

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.

1. Se você ainda não está aterrado, aterre-se adequadamente.
2. Solte o gancho e a alça de loop que prendem os cabos ao dispositivo de gerenciamento de cabos e, em seguida, desconecte os cabos do sistema e os SFPs (se necessário) do módulo do controlador, mantendo o controle de onde os cabos estavam conectados.
3. Aperte o trinco na pega do excêntrico até que este se solte, abra totalmente o manípulo do excêntrico para libertar o módulo do controlador do plano médio e, em seguida, utilizando duas mãos, puxe o módulo do controlador para fora do chassis.



4. Vire o módulo do controlador ao contrário e coloque-o numa superfície plana e estável.
5. Abra a tampa pressionando os botões azuis nas laterais do módulo do controlador para soltar a tampa e, em seguida, gire a tampa para cima e para fora do módulo do controlador.

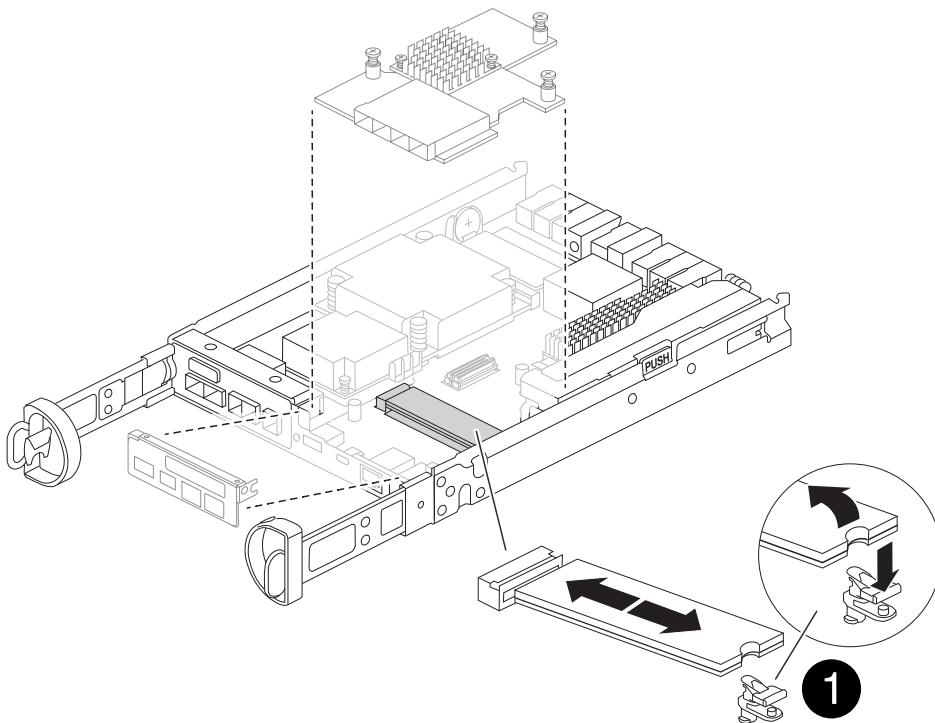


1

Botão de liberação da tampa do módulo do controlador

Passo 2: Substitua o suporte de arranque

Localize a Mídia de inicialização no módulo do controlador, localizado sob a placa mezzanine e siga as instruções para substituí-la.



1

Patilha de bloqueio do suporte de arranque

Passos

1. Se você ainda não está aterrado, aterre-se adequadamente.
2. Remova a placa mezzanine usando a ilustração a seguir ou o mapa da FRU no módulo do controlador:
 - a. Remova a placa de e/S deslizando-a diretamente para fora do módulo do controlador.
 - b. Desaperte os parafusos de aperto manual na placa do mezanino.
 - c. Levante a placa do mezanino para cima.

i Você pode soltar os parafusos com os dedos ou uma chave de fenda. Se utilizar os dedos, poderá ter de rodar a bateria NV para cima para obter uma melhor compra com o dedo no parafuso de aperto manual ao lado.
3. Substitua o suporte de arranque:
 - a. Prima o botão azul no alojamento do suporte de arranque para soltar o suporte de arranque do respetivo alojamento, rode o suporte de arranque para cima e, em seguida, puxe-o suavemente para fora do suporte de arranque.
 - b. 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. Verifique a Mídia de inicialização para se certificar de que ela está encaixada corretamente e completamente no soquete e, se necessário, remova a Mídia de inicialização e recoloque-a no soquete.
 - c. Prima o botão de bloqueio azul, rode o suporte de arranque até ao fim e, em seguida, solte o botão de bloqueio para bloquear o suporte de arranque no lugar.

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

4. Reinstate a placa mezzanine:
 - a. Alinhe o soquete na placa-mãe com o soquete na placa mezzanine e, em seguida, encaixe a placa com cuidado no soquete.
 - b. Aperte os três parafusos de aperto manual na placa do mezanino.
 - c. Volte a instalar a placa de e/S.
5. Volte a instalar a tampa do módulo do controlador e bloqueeie-a no lugar.

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

Instale a imagem do sistema no suporte de arranque de substituição utilizando uma unidade flash USB com a imagem instalada. Tem de restaurar o sistema de ficheiros var durante este procedimento.

Antes de começar

- Você deve ter uma unidade flash USB, formatada para MBR/FAT32, com pelo menos 4GBGB de capacidade.
- Tem de ter uma ligação de rede.

Passos

1. Transfira a versão de imagem apropriada do ONTAP para a unidade flash USB formatada:
 - a. ["Como determinar se a versão do ONTAP em execução suporta encriptação de volume NetApp \(NVE\)"](#) Use para determinar se a criptografia de volume é atualmente suportada.
 - Se o NVE for suportado no cluster, transfira a imagem com encriptação de volume NetApp.
 - Se a NVE não for suportada no cluster, transfira a imagem sem encriptação de volume NetApp. ["Qual imagem do ONTAP devo baixar? Com ou sem criptografia de volume?"](#) Consulte para obter mais detalhes.
 2. Retire a unidade flash USB do seu computador portátil.
 3. Instale o módulo do controlador:
 - a. 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.
 - b. Recable o módulo do controlador.

Ao reativar, lembre-se de reinstalar os conversores de Mídia (SFPs) se eles foram removidos.
 4. 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.
5. Empurre o módulo do controlador totalmente para dentro do sistema, certificando-se de que a alça da came limpa a unidade flash USB, empurre firmemente a alça da came para terminar de assentar o módulo do controlador, empurre a alça da came para a posição fechada e, em seguida, aperte o parafuso de aperto manual.

O controlador começa a inicializar assim que é completamente instalado no chassi e para no prompt LOADER.

O que se segue?

Depois de substituir a Mídia de inicialização, você precisa ["inicie a imagem de recuperação"](#).

Inicie a imagem de recuperação - FAS2820

Depois de instalar o novo dispositivo multimédia de arranque no seu sistema, pode arrancar a imagem de recuperação a partir de uma unidade USB e restaurar a configuração a partir do nó do parceiro.

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. Se solicitado no controlador prejudicado, pressione Y para 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 reiniciar 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 .

O que se segue?

Depois de inicializar a imagem de recuperação, você precisa "[restaure a encriptação no suporte de arranque](#)".

Restaurar encriptação - FAS2820

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>Selecione a opção 10.</p> <p>Mostrar exemplo de menu de inicialização</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>Please choose one of the following:</p> <ul style="list-style-type: none"> (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. <p>Selection (1-11)? 10</p> </div>

Versão de ONTAP	Selecione esta opção
ONTAP 9 F.7 e anteriores	<p>Selecione a opção oculta <code>recover_onboard_keymanager</code></p> <p>Mostrar exemplo de menu de inicialização</p> <div data-bbox="649 297 1465 988" style="border: 1px solid #ccc; padding: 10px;"> <pre>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:

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-----  
<certificate_value>  
-----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-----  
<certificate_value>  
-----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....  
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 a giveback automática se a tiver desativado.

```
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
```

O que se segue?

Depois de restaurar a encriptação no suporte de arranque, tem de ["Devolva a peça com falha ao NetApp"](#).

Devolva a peça com falha ao NetApp - FAS2820

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 DESTE DOCUMENTO. 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 SOBRESSAENTES; 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 DESTE SOFTWARE, 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.