



# Suporte de arranque

## Install and maintain

NetApp  
January 09, 2026

# Índice

|   |    |
|---|----|
| Suporte de arranque .....   | 1  |
| Descrição geral da substituição do suporte de arranque - AFF C250 .....                 | 1  |
| Verifique o suporte e o status da chave de criptografia - AFF C250 .....                | 1  |
| Passo 1: Verifique a compatibilidade com NVE e baixe a imagem ONTAP correta.....        | 1  |
| Etapa 2: Verifique o status do gerenciador de chaves e faça backup da configuração..... | 2  |
| Desligue o controlador - AFF C250 .....   | 5  |
| Opção 1: A maioria dos sistemas .....   | 6  |
| Opção 2: Sistemas em um MetroCluster .....  | 6  |
| Substitua o suporte de arranque - AFF C250 .....  | 7  |
| Passo 1: Remova o módulo do controlador.....  | 7  |
| Passo 2: Substitua o suporte de arranque.....   | 9  |
| Passo 3: Transfira a imagem de arranque para o suporte de arranque .....                | 10 |
| Inicie a imagem de recuperação - AFF C250.....  | 13 |
| Restaurar encriptação - AFF C250 .....  | 16 |
| Devolva a peça com falha ao NetApp - AFF C250 .....                                     | 26 |

# Suporte de arranque

## Descrição geral da substituição do suporte de arranque - AFF C250

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 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 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 - AFF C250

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 a compatibilidade com NVE e baixe a imagem ONTAP correta.

Verifique se a sua versão do ONTAP é compatível com a Criptografia de Volume NetApp (NVE) para que você possa baixar a imagem correta do ONTAP para a substituição da mídia de inicialização.

#### Passos

1. Verifique se a sua versão do ONTAP suporta criptografia:

```
version -v
```

Se a saída incluir `1Ono-DARE`, o NVE não é suportado na versão do cluster.

2. Faça o download da imagem ONTAP apropriada com base no suporte a NVE:
  - Se o NVE for compatível: Baixe a imagem do ONTAP com o NetApp Volume Encryption.
  - Se o NVE não for compatível: Baixe a imagem do ONTAP sem o NetApp Volume Encryption.



Faça o download da imagem do ONTAP do site de suporte da NetApp para o seu servidor HTTP ou FTP ou para uma pasta local. Você precisará deste arquivo de imagem durante o procedimento de substituição da mídia de inicialização.

## Etapa 2: Verifique o status do gerenciador de chaves e faça backup da configuração.

Antes de desligar o controlador com defeito, verifique a configuração do gerenciador de chaves e faça backup das informações necessárias.

### 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"><li>• Se EKM estiver ativado, EKM é listado na saída do comando.</li><li>• Se OKM estiver ativado, OKM o será listado na saída do comando.</li><li>• Se nenhum gerenciador de chaves estiver habilitado, <code>No key manager keystores configured</code> o será listado na saída do comando.</li></ul>                            |
| ONTAP 9.13,1 ou anterior  | <pre>security key-manager show-key-store</pre> <ul style="list-style-type: none"><li>• Se EKM estiver ativado, <code>external</code> é listado na saída do comando.</li><li>• Se OKM estiver ativado, <code>onboard</code> o será listado na saída do comando.</li><li>• Se nenhum gerenciador de chaves estiver habilitado, <code>No key managers configured</code> o será listado na saída do comando.</li></ul> |

2. Dependendo se um gerenciador de chaves estiver configurado em seu sistema, faça um dos seguintes procedimentos:

#### Se nenhum gerenciador de chaves estiver configurado:

Você pode desligar com segurança o controlador com defeito e prosseguir com o procedimento de desligamento.

#### Se um gerenciador de chaves estiver configurado (EKM ou OKM):

- a. Insira o seguinte comando de consulta para exibir o status das chaves de autenticação no seu gerenciador de chaves:

```
security key-manager key query
```

- b. Analise a saída e verifique o valor em `Restored` coluna. Esta coluna indica se as chaves de autenticação do seu gerenciador de chaves (EKM ou OKM) foram restauradas com sucesso.
3. Conclua o procedimento adequado com base no seu tipo de gestor de chaves:

### Gerenciador de chaves externo (EKM)

Complete estas etapas com base no valor em `Restored` coluna.

#### Se todas as chaves estiverem visíveis `true` na coluna Restaurado:

Você pode desligar com segurança o controlador com defeito e prosseguir com o procedimento de desligamento.

#### Se alguma chave apresentar um valor diferente de `true` na coluna Restaurado:

- a. Restaure as chaves de autenticação de gerenciamento de chaves externas em todos os nós do cluster:

```
security key-manager external restore
```

Se o comando falhar, entre em contato com o Suporte da NetApp .

- b. Verifique se todas as chaves de autenticação foram restauradas:

```
security key-manager key query
```

Confirme que o `Restored` exibição de coluna `true` para todas as chaves de autenticação.

- c. Se todas as teclas forem restauradas, você poderá desligar o controlador com defeito em segurança e prosseguir com o procedimento de desligamento.

### Gerenciador de chaves integrado (OKM)

Complete estas etapas com base no valor em `Restored` coluna.

#### Se todas as chaves estiverem visíveis `true` na coluna Restaurado:

- a. Faça backup das informações do OKM:

- i. Alternar para o modo de privilégios avançados:

```
set -priv advanced
```

Digitar `y` quando solicitado a continuar.

- i. Exibir as informações de backup do gerenciamento de chaves:

```
security key-manager onboard show-backup
```

- ii. Copie as informações de backup para um arquivo separado ou para o seu arquivo de registro.

Você precisará dessas informações de backup caso precise recuperar o OKM manualmente durante o procedimento de substituição.

- iii. Voltar ao modo administrador:

```
set -priv admin
```

- b. Você pode desligar com segurança o controlador com defeito e prosseguir com o procedimento de desligamento.

**Se alguma chave apresentar um valor diferente de `true` na coluna Restaurado:**

- a. Sincronizar o gerenciador de chaves integrado:

```
security key-manager onboard sync
```

Digite a senha alfanumérica de 32 caracteres para gerenciamento da chave de bordo quando solicitado.



Esta é a senha de todo o cluster que você criou ao configurar inicialmente o Gerenciador de Chaves Integrado. Caso não possua essa senha, entre em contato com o Suporte da NetApp .

- b. Verifique se todas as chaves de autenticação foram restauradas:

```
security key-manager key query
```

Confirme que o Restored exibição de coluna `true` para todas as chaves de autenticação e o Key Manager tipo mostra `onboard` .

- c. Faça backup das informações do OKM:

- i. Alternar para o modo de privilégios avançados:

```
set -priv advanced
```

Digitar `y` quando solicitado a continuar.

- i. Exibir as informações de backup do gerenciamento de chaves:

```
security key-manager onboard show-backup
```

- ii. Copie as informações de backup para um arquivo separado ou para o seu arquivo de registro.

Você precisará dessas informações de backup caso precise recuperar o OKM manualmente durante o procedimento de substituição.

- iii. Voltar ao modo administrador:

```
set -priv admin
```

- d. Você pode desligar com segurança o controlador com defeito e prosseguir com o procedimento de desligamento.

## Desligue o controlador - AFF C250

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

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

## Substitua o suporte de arranque - AFF C250

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

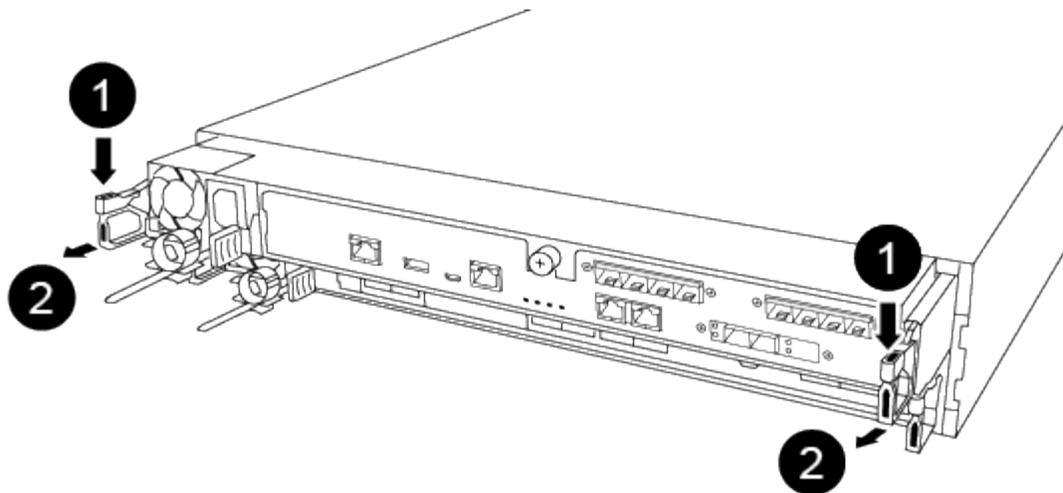
Para aceder aos componentes no interior do módulo do controlador, tem de remover primeiro o módulo do controlador do sistema e, em seguida, remover a tampa do módulo do controlador.

#### 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. Desconete os cabos de e/S do módulo do controlador.
5. 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.

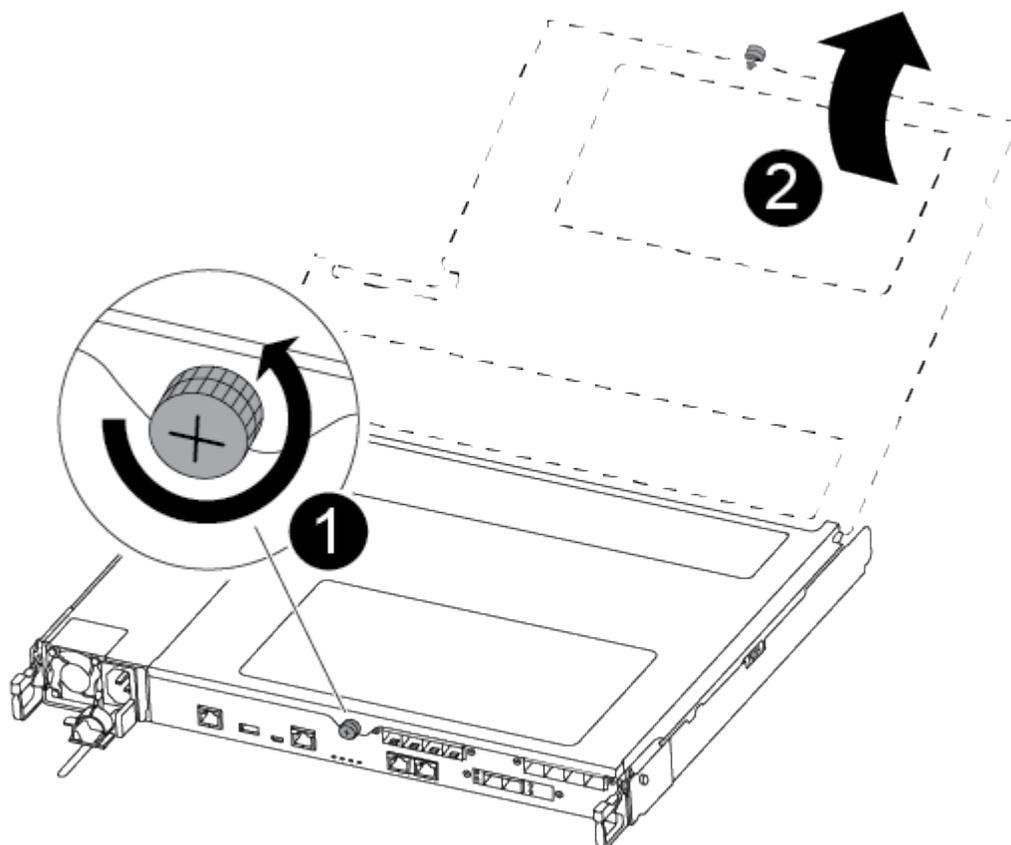


Se tiver dificuldade em remover o módulo do controlador, coloque os dedos indicadores através dos orifícios dos dedos a partir do interior (cruzando os braços).



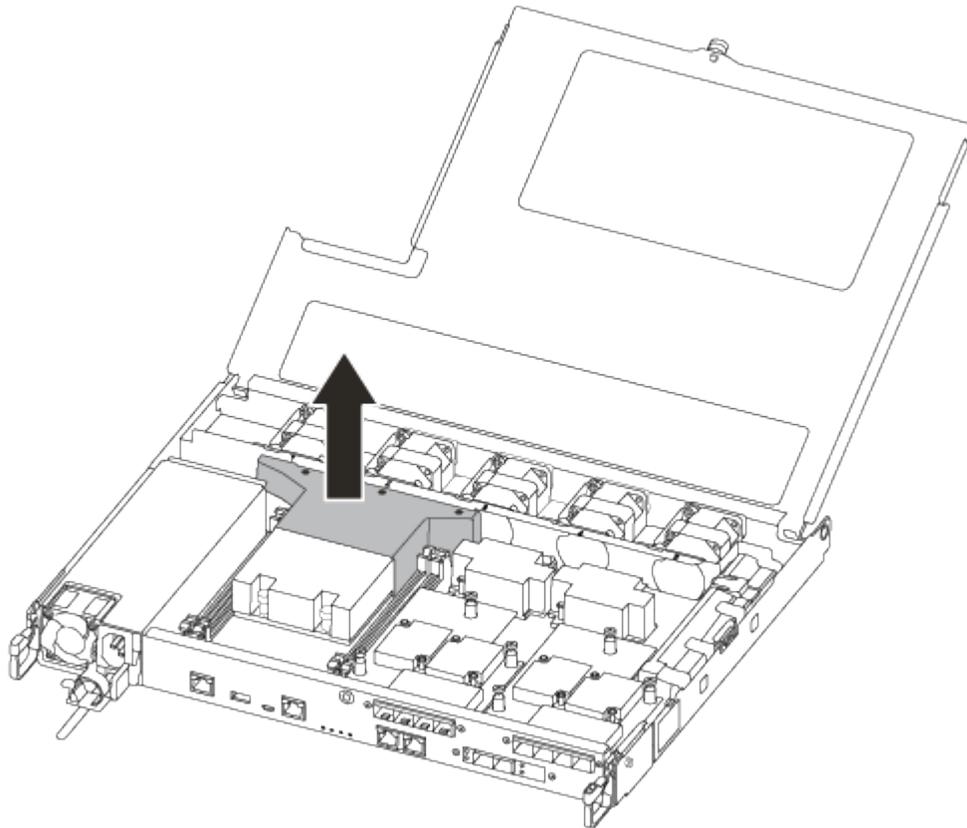
|   |                       |
|---|-----------------------|
| 1 | Alavanca              |
| 2 | Mecanismo de bloqueio |

6. 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.
7. 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. |

8. Levante a tampa da conduta de ar.



## Passo 2: Substitua o suporte de arranque

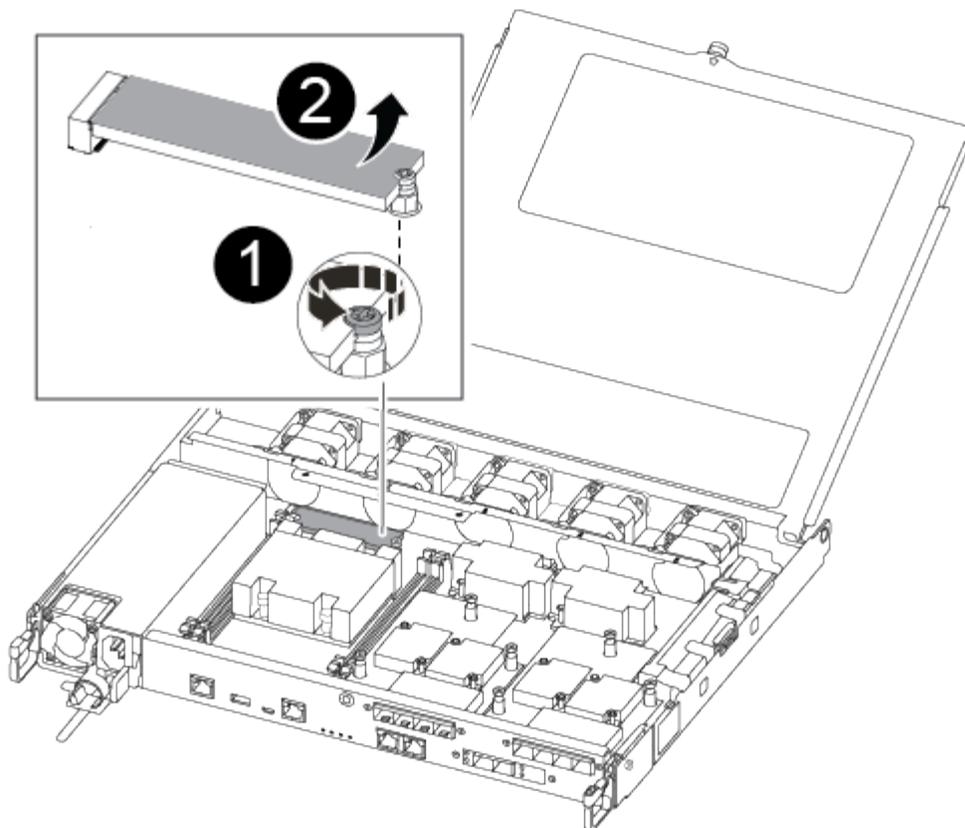
Pode localizar o suporte de arranque avariado no módulo do controlador removendo a conduta de ar no módulo do controlador antes de poder substituir o suporte de arranque.

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.



|                 |   |
|-----------------|---|
| <p><b>1</b></p> | <p>Retire o parafuso que fixa o suporte de arranque à placa-mãe no módulo do controlador.</p> |
| <p><b>2</b></p> | <p>Levante o suporte de arranque para fora do módulo do controlador.</p>                      |

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:

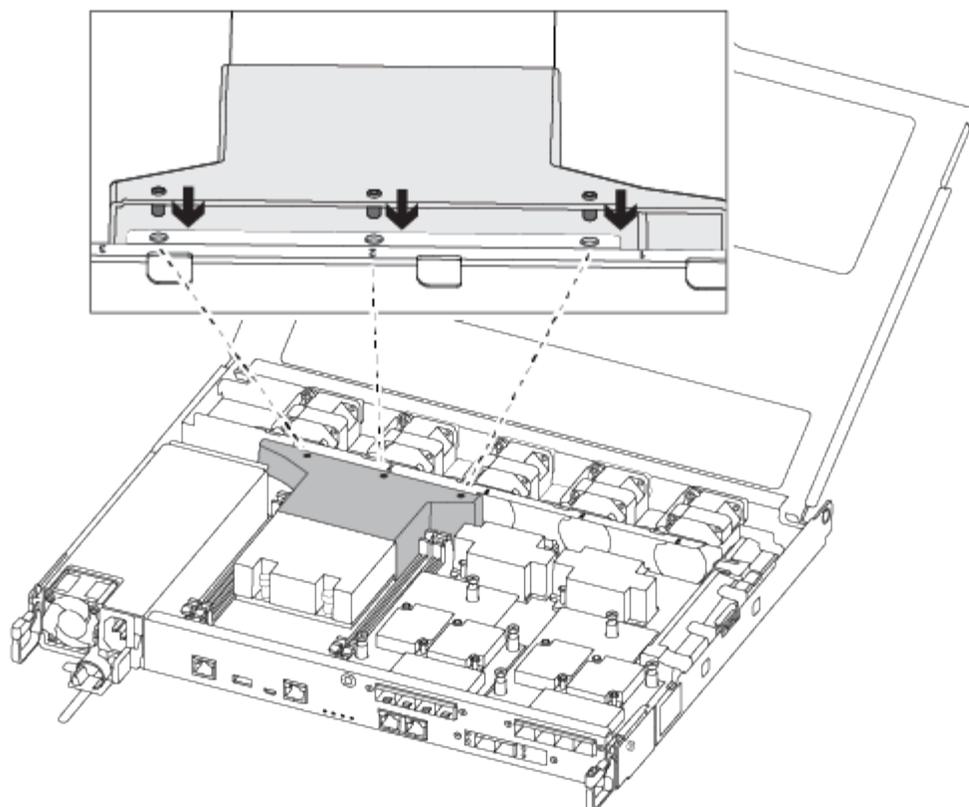
- inicialização
  - efi
- d. Copie a pasta efi para o diretório superior da unidade flash USB.



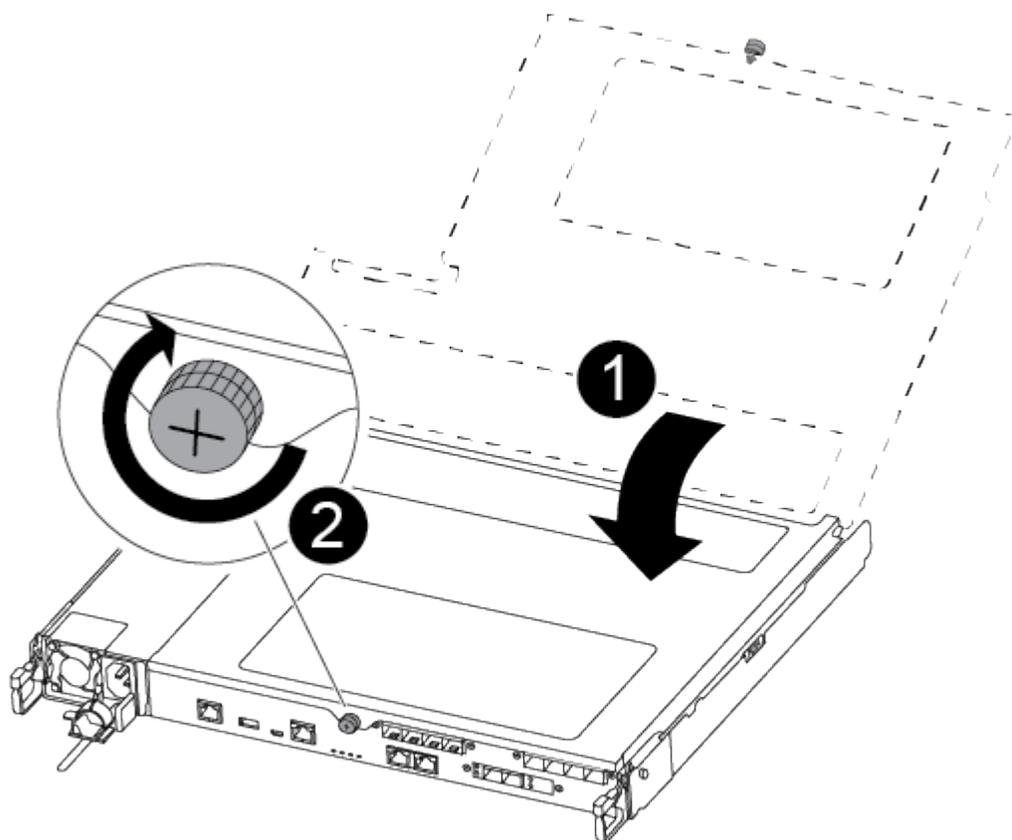
Se a imagem de serviço não tiver uma pasta efi, "[Pasta EFI ausente do arquivo de download de imagem de serviço usado para recuperação de dispositivo de inicialização para modelos FAS e AFF](#)" consulte .

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.



|          |                                |
|----------|--------------------------------|
| <b>1</b> | Tampa do módulo do controlador |
| <b>2</b> | Parafuso de aperto manual      |

- 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. 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.

- c. Empurre o módulo do controlador até ao chassis:
- d. Coloque os dedos indicadores através dos orifícios dos dedos a partir do interior do mecanismo de bloqueio.
- e. 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.
- f. 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 deve ser totalmente inserido e alinhado com as bordas do chassi.

- g. Volte a ligar os cabos de e/S do módulo do controlador.
- h. Conete os cabos de alimentação às fontes de alimentação, reinstale o colar de travamento do cabo de alimentação e, em seguida, conete as fontes de alimentação à fonte de alimentação.

O módulo do controlador começa a inicializar assim que a energia é restaurada. Esteja preparado para interromper o processo de inicialização.

- i. 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.

- j. 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.

## Inicie a imagem de recuperação - AFF C250

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.

### Antes de começar

- Certifique-se de que seu console esteja conectado ao controle com defeito.

- Verifique se você possui um pen drive com a imagem de recuperação.
- Verifique se o seu sistema utiliza criptografia. Você precisará selecionar a opção apropriada na etapa 3, dependendo se a criptografia está ativada ou não.

### Passos

1. A partir do prompt LOADER no controlador com defeito, inicialize a imagem de recuperação a partir da unidade flash USB:

```
boot_recovery
```

A imagem de recuperação é baixada da unidade flash USB.

2. Quando solicitado, digite o nome da imagem ou pressione **Enter** para aceitar a imagem padrão exibida entre colchetes.
3. Restaure o sistema de arquivos var usando o procedimento para sua versão do ONTAP :

### ONTAP 9.16,0 ou anterior

Conclua as seguintes etapas no controlador incapacitado e no controlador parceiro:

- a. **No controlador com defeito:** Pressione Y quando você vê `Do you want to restore the backup configuration now?`
- b. **No controlador com defeito:** Se solicitado, pressione Y para sobrescrever `/etc/ssh/ssh_host_ecdsa_key`.
- c. **No controlador parceiro:** Defina o controlador com problemas para o nível de privilégio avançado:

```
set -privilege advanced
```

- d. **No controlador parceiro:** Execute o comando de restauração de backup:

```
system node restore-backup -node local -target-address  
impaired_node_IP_address
```



Se você vir qualquer mensagem diferente de uma restauração bem-sucedida, entre em contato com o Suporte da NetApp .

- e. **No controlador de parceiros:** Retornar ao nível de administrador:

```
set -privilege admin
```

- f. **No controlador com defeito:** Pressione Y quando você vê `Was the restore backup procedure successful?`
- g. **No controlador com defeito:** Pressione Y quando você vê `...would you like to use this restored copy now?`
- h. **No controlador com defeito:** Pressione Y Quando solicitado a reiniciar, pressione Ctrl-C quando você vir o Menu de Inicialização.
- i. **No controlador inoperante:** Faça um dos seguintes procedimentos:
  - Se o sistema não usar criptografia, selecione *Opção 1 Inicialização Normal* no Menu de Inicialização.
  - Se o sistema usar criptografia, acesse "[Restaure a criptografia](#)".

### ONTAP 9.16.1 ou posterior

Conclua os seguintes passos no controlador comprometido:

- a. Pressione Y quando solicitado para restaurar a configuração de backup.

Após o procedimento de restauração ser concluído com sucesso, esta mensagem é exibida:  
`syncflash_partner: Restore from partner complete`

- b. Imprensa Y quando solicitado a confirmar que a restauração do backup foi bem-sucedida.
- c. Imprensa Y quando solicitado a usar a configuração restaurada.
- d. Imprensa Y quando solicitado a reiniciar o nó.

- e. Imprensa Y Quando solicitado a reiniciar novamente, pressione `Ctrl-C` quando você vir o Menu de Inicialização.
- f. Execute um dos seguintes procedimentos:
  - Se o sistema não usar criptografia, selecione *Opção 1 Inicialização Normal* no Menu de Inicialização.
  - Se o sistema usar criptografia, acesse "[Restaure a criptografia](#)".

4. Conecte o cabo do console ao controlador do parceiro.

5. Volte a colocar o controlador em funcionamento normal, devolvendo o respectivo armazenamento:

```
storage failover giveback -fromnode local
```

6. Se você desativou a devolução automática, reative-a:

```
storage failover modify -node local -auto-giveback true
```

7. Se o AutoSupport estiver ativado, restaure a criação automática de casos:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

## Restaurar encriptação - AFF C250

Restaure a encriptação no suporte de arranque de substituição.

Siga os passos adequados para restaurar a criptografia no seu sistema, de acordo com o tipo de gerenciador de chaves utilizado. Se você não tiver certeza de qual gerenciador de chaves seu sistema utiliza, verifique as configurações que você registrou no início do procedimento de substituição da mídia de inicialização.

## Gerenciador de chaves integrado (OKM)

Restaure a configuração OKM (Onboard Key Manager) no menu de inicialização do ONTAP.

### Antes de começar

Certifique-se de ter as seguintes informações disponíveis:

- Senha global do cluster inserida enquanto "[habilitando o gerenciamento de chaves a bordo](#)"
- "[Informações de cópia de segurança para o Gestor de chaves integrado](#)"
- Verificação de que você possui a senha correta e os dados de backup usando o "[Como verificar o backup integrado do gerenciamento de chaves e a senha em todo o cluster](#)" procedimento

### Passos

#### No controlador incapacitado:

1. Conecte o cabo do console ao controle com defeito.
2. No menu de inicialização do ONTAP , selecione a opção apropriada:

| Versão de ONTAP         | Selecione esta opção   |
|-------------------------|--|
| ONTAP 9 .8 ou posterior | <p>Selecione a opção 10.</p> <p><b>Mostrar exemplo de menu de inicialização</b></p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"><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. (10) Set Onboard Key Manager recovery secrets. (11) Configure node for external key management. Selection (1-11)? 10</pre></div> |

| Versão de ONTAP          | Selecione esta opção  |
|--------------------------|---|
| ONTAP 9 F.7 e anteriores | <p data-bbox="634 155 1390 197">Selecione a opção oculta <code>recover_onboard_keymanager</code></p> <p data-bbox="634 226 1162 268"><b>Mostrar exemplo de menu de inicialização</b></p> <div data-bbox="667 302 1422 968" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <pre data-bbox="695 338 1382 932"> Please choose one of the following:  (1) Normal Boot. (2) Boot without /etc/rc. (3) Change password. (4) Clean configuration and initialize all disks. (5) Maintenance mode boot. (6) Update flash from backup config. (7) Install new software first. (8) Reboot node. (9) Configure Advanced Drive Partitioning. Selection (1-19)? recover_onboard_keymanager </pre> </div> |

3. Confirme que deseja continuar o processo de recuperação quando solicitado:

**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 digitar a senha, o console não exibe nenhuma entrada.

**Mostrar prompt de exemplo**

```

Enter the passphrase for onboard key management:

Enter the passphrase again to confirm:

```

5. Insira as informações de backup:

- a. Cole todo o conteúdo da linha BEGIN BACKUP até a linha END BACKUP, incluindo os traços.



```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
01234567890123456789012345678901234567890123456789012345678901
23
12345678901234567890123456789012345678901234567890123456789012
34
23456789012345678901234567890123456789012345678901234567890123
45
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
-----END
BACKUP-----
```

b. Pressione Enter duas vezes ao final da entrada de dados.

O processo de recuperação é concluído e exibe a seguinte mensagem:

Successfully recovered keymanager secrets.

### 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 de `Successfully recovered keymanager secrets`. Realize a resolução de problemas para corrigir o erro.

6. Selecione a opção 1 a partir do menu de inicialização para continuar a inicialização 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)
```

### No controlador parceiro:

8. Devolva o controle remoto com defeito:

```
storage failover giveback -fromnode local -only-cfo-aggregates true
```

### No controlador incapacitado:

9. Após inicializar apenas com o agregado CFO, sincronize o gerenciador de chaves:

```
security key-manager onboard sync
```

10. Quando solicitado, insira a senha de acesso ao Onboard Key Manager, que será aplicada em todo o cluster.

## 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 prossiga até que o erro seja corrigido e a sincronização seja concluída com sucesso.

11. Verifique se todas as chaves estão sincronizadas:

```
security key-manager key query -restored false
```

O comando não deve retornar nenhum resultado. Se algum resultado aparecer, repita o comando de sincronização até que nenhum resultado seja retornado.

### No controlador parceiro:

12. Devolva o controle remoto com defeito:

```
storage failover giveback -fromnode local
```

13. Restaure a giveback automática se você a tiver desativado:

```
storage failover modify -node local -auto-giveback true
```

14. Se o AutoSupport estiver ativado, restaure a criação automática de casos:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

## Gerenciador de chaves externo (EKM)

Restaure a configuração do Gerenciador de chaves Externo no menu de inicialização do ONTAP.

### Antes de começar

Reúna os seguintes arquivos de outro nó do cluster ou do seu backup:

- ``/cfcard/kmip/servers.cfg`` arquivo ou o endereço e porta do servidor KMIP
- ``/cfcard/kmip/certs/client.crt`` arquivo (certificado do cliente)
- ``/cfcard/kmip/certs/client.key`` arquivo (chave do cliente)
- ``/cfcard/kmip/certs/CA.pem`` arquivo (certificados CA do servidor KMIP)

## Passos

### No controlador incapacitado:

1. Conecte o cabo do console ao controle com defeito.
2. Selecione a opção 11 a partir do 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. Confirme que reuniu as informações necessárias quando solicitado:

#### 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. Insira as informações do cliente e do servidor quando solicitado:
  - a. Insira o conteúdo do arquivo de certificado do cliente (client.crt), incluindo as linhas BEGIN e END.
  - b. Insira o conteúdo do arquivo de chave do cliente (client.key), incluindo as linhas BEGIN e END.
  - c. Insira o conteúdo do arquivo CA.pem do servidor KMIP, incluindo as linhas BEGIN e END.
  - d. Insira o endereço IP do servidor KMIP.
  - e. Digite a porta do servidor KMIP (pressione Enter para usar a porta padrão 5696).

### 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
```

O processo de recuperação é concluído e exibe a seguinte mensagem:

```
Successfully recovered keymanager secrets.
```

### 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 a partir do menu de inicialização para continuar a inicialização 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 você a tiver desativado:

```
storage failover modify -node local -auto-giveback true
```

7. Se o AutoSupport estiver ativado, restaure a criação automática de casos:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

## Devolva a peça com falha ao NetApp - AFF C250

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 © 2026 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

## Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.