# Mídia de inicialização - recuperação manual

Install and maintain

NetApp
February 13, 2026

This PDF was generated from https://docs.netapp.com/pt-br/ontap-systems/a70-90/bootmedia-replace-workflow.html on February 13, 2026. Always check docs.netapp.com for the latest.

# Índice

Mídia de inicialização - recuperação manual . . . 1
Fluxo de trabalho de recuperação manual de mídia de inicialização - AFF A70 e AFF A90 . . . 1
Requisitos para recuperação manual de mídia de inicialização - AFF A70 e AFF A90 . . . 2
Verifique o suporte de criptografia para recuperação manual de mídia de inicialização - AFF A70 e AFF A90 . . . 2
Passo 1: Verifique a compatibilidade com NVE e baixe a imagem ONTAP correta. . . . 3
Etapa 2: Verifique o status do gerenciador de chaves e faça backup da configuração. . . . 3
Desligue o controlador para recuperação manual da mídia de inicialização - AFF A70 e AFF A90 . . . 7
Substitua a mídia de inicialização e prepare-se para recuperação de inicialização manual - AFF A70 e AFF A90 . . . 10
Passo 1: Substitua o suporte de arranque . . . 10
Passo 2: Transfira a imagem de arranque para o suporte de arranque . . . 11
Recuperação manual de mídia de inicialização de uma unidade USB - AFF A70 e AFF A90 . . . 13
Restaurar chaves de criptografia após recuperação de inicialização manual - AFF A70 e AFF A90 . . . 15
Devolva a peça com falha ao NetApp - AFF A70 e AFF A90 . . . 25

# Mídia de inicialização - recuperação manual

## Fluxo de trabalho de recuperação manual de mídia de inicialização - AFF A70 e AFF A90

A recuperação manual da imagem de inicialização envolve o uso de uma unidade USB para reinstalar o ONTAP na mídia de inicialização de substituição do sistema AFF A70 ou AFF A90 . Você deve baixar a imagem de recuperação do ONTAP apropriada no site de suporte da NetApp e copiá-la para uma unidade USB. Essa unidade USB preparada é então usada para executar a recuperação e restaurar o sistema ao status operacional.

Se o seu sistema de armazenamento estiver executando o ONTAP 9.17.1 ou posterior, use o"procedimento automatizado de recuperação de inicialização" . Se o seu sistema estiver executando uma versão anterior do ONTAP, use o procedimento de recuperação de inicialização manual.

Para começar, revise os requisitos de recuperação, desligue o controlador, substitua a mídia de inicialização, use a unidade USB para restaurar a imagem e reaplique as configurações de criptografia, se necessário.

1. **"Reveja os requisitos para substituir o suporte de arranque"**

Reveja os requisitos para substituir o suporte de arranque.

2. **"Verifique o suporte e o status da chave de criptografia"**

Determine se o sistema tem o gerenciador de chaves de segurança ativado ou discos criptografados.

3. **"Desligue o controlador"**

Desligue o controlador quando precisar de substituir o suporte de arranque.

4. **"Substitua o suporte de arranque"**

Remova o suporte de arranque com falha do módulo de gestão do sistema e instale o suporte de arranque de substituição e, em seguida, transfira uma imagem ONTAP utilizando uma unidade flash USB.

5. **"Inicie a imagem de recuperação"**

Inicie a imagem ONTAP a partir da unidade USB, restaure o sistema de ficheiros e verifique as variáveis ambientais.

6. **"Restaure a criptografia"**

Restaure a configuração do gerenciador de chaves integrado ou do gerenciador de chaves externo no menu de inicialização do ONTAP .

7 **"Devolva a peça com falha ao NetApp"**

Devolva a peça com falha ao NetApp, conforme descrito nas instruções de RMA fornecidas com o kit.

# Requisitos para recuperação manual de mídia de inicialização - AFF A70 e AFF A90

Antes de substituir o suporte de arranque no sistema AFF A70 ou AFF A90, certifique-se de que cumpre os requisitos necessários para uma substituição bem-sucedida. Isso inclui garantir que você tenha uma unidade flash USB com a quantidade adequada de armazenamento e verificar se você tem o dispositivo de inicialização de substituição correto.

Se o seu sistema estiver executando o ONTAP 9.17.1 e posterior, use o "procedimento de recuperação de inicialização automática" .

**Pen drive USB**

- Certifique-se de ter uma unidade flash USB formatada para FAT32.
- O USB deve ter capacidade de armazenamento suficiente para armazenar o `image_xxx.tgz` arquivo.

**Preparação do arquivo**

Copie o `image_xxx.tgz` arquivo para o pen drive USB. Este arquivo será usado quando você transferir a imagem ONTAP usando o pen drive USB.

**Substituição de componentes**

Substitua o componente com falha pelo componente de substituição fornecido pela NetApp.

**Identificação do controlador**

É fundamental aplicar os comandos ao controlador correto ao substituir a mídia de inicialização danificada:

- O *controlador danificado* é o controlador no qual você está executando a manutenção.
- O *controlador saudável* é o parceiro HA do controlador prejudicado.

**O que se segue?**

Depois de rever os requisitos para substituir o suporte de arranque, tem de "verifique o suporte e o status da chave de criptografia na mídia de inicialização".

# Verifique o suporte de criptografia para recuperação manual de mídia de inicialização - AFF A70 e AFF A90

Para garantir a segurança dos dados no sistema de armazenamento AFF A70 ou AFF A90, 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.

Se o seu sistema estiver executando o ONTAP 9.17.1 e posterior, use o "procedimento de recuperação de

inicialização automática" .

## 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 | `security key-manager keystore show`<br>• Se EKM estiver ativado, `EKM` é listado na saída do comando.<br>• Se OKM estiver ativado, `OKM` o será listado na saída do comando.<br>• Se nenhum gerenciador de chaves estiver habilitado, `No key manager keystores configured` o será listado na saída do comando. |

| Versão de ONTAP | Execute este comando |
| --- | --- |
| ONTAP 9.13,1 ou anterior | `security key-manager show-key-store`<br>• Se EKM estiver ativado, `external` é listado na saída do comando.<br>• Se OKM estiver ativado, `onboard` o será listado na saída do comando.<br>• 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 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.

**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 para recuperação manual da mídia de inicialização - AFF A70 e AFF A90

Desligue o controlador danificado no seu sistema de armazenamento AFF A70 ou AFF A90 para evitar perda de dados e manter a estabilidade do sistema durante o processo automatizado de recuperação da mídia de inicialização.

**Opção 1: A maioria dos sistemas**

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.

**Sobre esta tarefa**

- Se você tiver um sistema SAN, você deve ter verificado mensagens de `cluster kernel-service show`evento ) para o blade SCSI do controlador afetado. O `cluster kernel-service show` comando (do modo avançado priv) exibe o nome do nó, "status do quorum"desse nó, o status de disponibilidade desse nó e o status operacional desse nó.

  Cada processo SCSI-blade deve estar em quórum com os outros nós no cluster. Qualquer problema deve ser resolvido antes de prosseguir com a substituição.

- 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 .

**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=<# of hours>h
   ```

   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. Desabilitar devolução automática:

   a. Digite o seguinte comando no console do controlador íntegro:

      ```
      storage failover modify -node impaired_node_name -auto-giveback false
      ```

   b. Digitar `y` quando você vê o prompt *Você quer desabilitar o retorno automático?*

3. Leve o controlador prejudicado para o prompt Loader:

| Se o controlador afetado estiver a apresentar… | Então… |
|---|---|
| O prompt Loader | Vá para a próxima etapa. |
| A aguardar pela giveback… | Pressione Ctrl-C e responda `y` quando solicitado. |

| Se o controlador afetado estiver a apresentar… | Então… |
| --- | --- |
| Prompt do sistema ou prompt de senha | Assuma ou interrompa o controlador prejudicado do controlador saudável:<br><br>`storage failover takeover -ofnode` *`impaired_node_name`* `-halt` *`true`*<br><br>O parâmetro *-halt True* traz para o prompt Loader. |

**Opção 2: O controlador está em um MetroCluster**

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 .
- 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. Desabilitar devolução automática:
   a. Digite o seguinte comando no console do controlador íntegro:

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

   b. Digitar `y` quando você vê o prompt *Você quer desabilitar o retorno automático?*
3. Leve o controlador prejudicado para o prompt Loader:

| Se o controlador afetado estiver a apresentar… | Então… |
| --- | --- |
| O prompt Loader | Vá para a próxima seção. |

| Se o controlador afetado estiver a apresentar… | Então… |
| --- | --- |
| A aguardar pela giveback… | Pressione Ctrl-C e responda `y` quando solicitado. |
| Prompt do sistema ou prompt de senha (digite a senha do sistema) | Assuma ou interrompa o controlador prejudicado do controlador saudável:<br><br>`storage failover takeover -ofnode` *`impaired_node_name`* `-halt` *`true`*<br><br>O parâmetro *-halt True* traz para o prompt Loader. |

**O que se segue?**

Depois de desligar o controlador, é necessário "substitua o suporte de arranque".

# Substitua a mídia de inicialização e prepare-se para recuperação de inicialização manual - AFF A70 e AFF A90

A mídia de inicialização do seu sistema AFF A70 ou AFF A90 armazena dados essenciais de firmware e configuração. O processo de substituição envolve a remoção do módulo de Gerenciamento do Sistema, a remoção da mídia de inicialização danificada, a instalação da mídia de inicialização de substituição e a transferência manual da imagem ONTAP para a mídia de inicialização de substituição usando um pen drive USB.

## Passo 1: Substitua o suporte de arranque

O suporte de arranque encontra-se no interior do módulo de gestão do sistema e é acedido removendo o módulo do sistema.

**Passos**

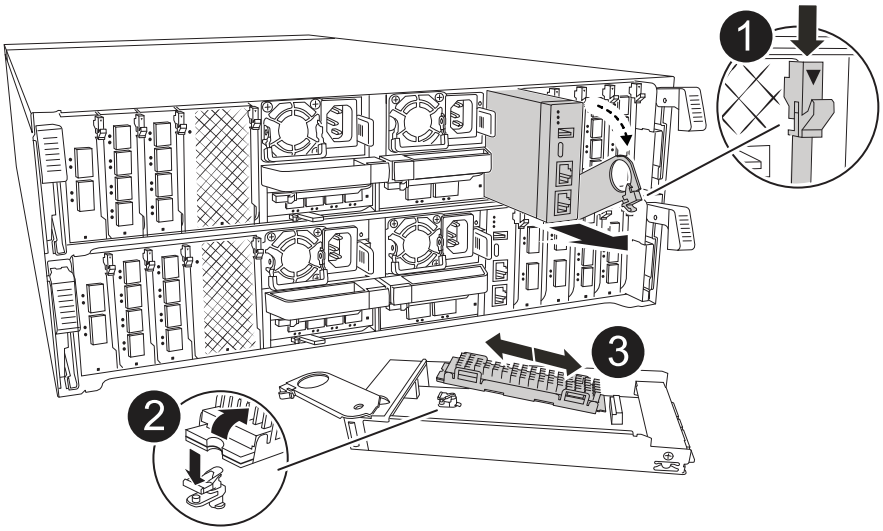
1. Vá para a parte traseira do chassis. Se você ainda não está aterrado, aterre-se adequadamente.
2. Desconecte as PSUs do controlador.

   Se o sistema tiver alimentação CC, desligue o bloco de alimentação das PSUs.

   a. Retire todos os cabos ligados ao módulo de gestão do sistema. Certifique-se de identificar onde os cabos foram conetados, para que você possa conectá-los às portas corretas quando reinstalar o módulo.
   b. Gire a bandeja de gerenciamento de cabos para baixo puxando os botões de ambos os lados no interior da bandeja de gerenciamento de cabos e, em seguida, gire a bandeja para baixo.
   c. Prima o botão do came de gestão do sistema. A alavanca do excêntrico afasta-se do chassis.
   d. Rode a alavanca do excêntrico totalmente para baixo e retire o módulo de gestão do sistema do módulo do controlador.

e. Coloque o módulo de gestão do sistema num tapete anti-estático, de forma a que o suporte de arranque fique acessível.

3. Retire o suporte de arranque do módulo de gestão:




| | |
|---|---|
| 1 | Trinco do excêntrico do módulo de gestão do sistema |
| 2 | Botão de bloqueio do suporte de arranque |
| 3 | Suporte de arranque |

a. Prima o botão azul de trancamento.

b. Rode o suporte de arranque para cima, deslize-o para fora do encaixe e coloque-o de lado.

4. Instale o suporte de arranque de substituição no módulo de gestão do sistema:

a. Alinhe as extremidades do suporte de arranque com o alojamento do encaixe e, em seguida, empurre-o suavemente no encaixe.

b. Rode o suporte de arranque para baixo em direção ao botão de bloqueio.

c. Prima o botão de bloqueio, rode o suporte de arranque totalmente para baixo e, em seguida, solte o botão de bloqueio.

5. Reinstale o módulo de gerenciamento do sistema:

a. Rode o tabuleiro de gestão de cabos para cima até à posição fechada.

b. Recable o módulo de Gestão do sistema.

## Passo 2: Transfira a imagem de arranque para o suporte de arranque

A Mídia de inicialização de substituição que você instalou é sem uma imagem ONTAP. Pode transferir a imagem ONTAP para o suporte de arranque de substituição, transferindo a imagem de serviço ONTAP adequada da "Site de suporte da NetApp" para uma unidade flash USB e, em seguida, para o suporte de arranque de substituição.

**Antes de começar**

- Você deve ter uma unidade flash USB, formatada para FAT32, com pelo menos 4GBGB de capacidade.
- Faça o download de uma cópia da mesma versão de imagem do ONTAP que a controladora prejudicada estava sendo executada. Você pode baixar a imagem apropriada da seção Downloads no site de suporte da NetApp. Use o `version -v` comando para exibir se sua versão do ONTAP oferece suporte a NVE. Se o comando output for exibido `<10no- DARE>`, sua versão do ONTAP não suporta NVE.
  - Se a NVE for suportada pela sua versão do ONTAP, transfira a imagem com encriptação de volume NetApp, conforme indicado no botão de transferência.
  - Se não for suportado NVE, transfira a imagem sem encriptação de volume NetApp, conforme indicado no botão de transferência.
- Se o sistema for um par de HA, você precisará ter uma conexão de rede entre as portas de gerenciamento de nós dos controladores (normalmente as interfaces e0M).

**Passos**

1. Transfira e copie a imagem de serviço adequada do "Site de suporte da NetApp" para a unidade flash USB.

   a. Transfira a imagem de serviço a partir do link Downloads na página, para o seu espaço de trabalho no seu computador portátil.

   b. 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.

   A unidade flash USB deve ter a imagem ONTAP apropriada do que o controlador afetado está a executar.

   a. Retire a unidade flash USB do seu computador portátil.

2. Insira a unidade flash USB na porta USB-A no módulo de gerenciamento do sistema.

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

3. Conete os cabos de alimentação às fontes de alimentação. O controlador reinicia assim que a energia é restaurada.

   > Se você tiver fontes de alimentação CC, reconecte o bloco de energia às fontes de alimentação.

4. Interrompa o processo de inicialização pressionando Ctrl-C para parar no prompt DO Loader.

   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.

**O que se segue?**

Depois de substituir a Mídia de inicialização, você precisa "inicie a imagem de recuperação".

# Recuperação manual de mídia de inicialização de uma unidade USB - AFF A70 e AFF A90

Depois de instalar o novo dispositivo de mídia de inicialização no seu sistema AFF A70 ou AFF A90 , você pode inicializar a imagem de recuperação manualmente a partir de uma unidade USB para restaurar a configuração do nó parceiro.

Se o seu sistema estiver executando o ONTAP 9.17.1 e posterior, use o "procedimento de recuperação de inicialização automática" .

**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. Conete o cabo do console ao controlador do parceiro.
5. Volte a colocar o controlador em funcionamento normal, devolvendo o respetivo 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
```

**O que se segue?**

Depois de inicializar a imagem de recuperação, você precisa "restaure a encriptação no suporte de arranque".

# Restaurar chaves de criptografia após recuperação de inicialização manual - AFF A70 e AFF A90

Restaure a criptografia na Mídia de inicialização de substituição em seu sistema AFF A70 ou AFF A90 para garantir a proteção contínua dos dados. O processo de substituição envolve verificar a disponibilidade das chaves, reaplicar as configurações de criptografia e confirmar o acesso seguro aos seus dados.

Se o seu sistema estiver executando o ONTAP 9.17.1 e posterior, use o "procedimento de recuperação de inicialização automática" .

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 | Selecione a opção 10.<br><br>**Mostrar exemplo de menu de inicialização**<br><br>`Please choose one of the following:`<br><br>`(1) Normal Boot.`<br>`(2) Boot without /etc/rc.`<br>`(3) Change password.`<br>`(4) Clean configuration and initialize all disks.`<br>`(5) Maintenance mode boot.`<br>`(6) Update flash from backup config.`<br>`(7) Install new software first.`<br>`(8) Reboot node.`<br>`(9) Configure Advanced Drive Partitioning.`<br>`(10) Set Onboard Key Manager recovery secrets.`<br>`(11) Configure node for external key management.`<br>`Selection (1-11)? 10` |

| Versão de ONTAP | Selecione esta opção |
| --- | --- |
| ONTAP 9 F.7 e anteriores | Selecione a opção oculta `recover_onboard_keymanager`<br><br>**Mostrar exemplo de menu de inicialização**<br><br>`Please choose one of the following:`<br><br>`(1) Normal Boot.`<br>`(2) Boot without /etc/rc.`<br>`(3) Change password.`<br>`(4) Clean configuration and initialize all disks.`<br>`(5) Maintenance mode boot.`<br>`(6) Update flash from backup config.`<br>`(7) Install new software first.`<br>`(8) Reboot node.`<br>`(9) Configure Advanced Drive Partitioning.`<br>`Selection (1-19)?`<br>`recover_onboard_keymanager` |

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.

**Mostrar prompt de exemplo**

```
Enter the backup data:

---------------------------BEGIN
BACKUP---------------------------
0123456789012345678901234567890123456789012345678901234567890123456789901
23
1234567890123456789012345678901234567890123456789012345678901234567890123
4
2345678901234567890123456789012345678901234567890123456789012345678901234
5
3456789012345678901234567890123456789012345678901234567890123456789012345
6
4567890123456789012345678901234567890123456789012345678901234567890123456
7
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
```

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
0123456789012345678901234567890123456789012345678901234567890123456789
23
1234567890123456789012345678901234567890123456789012345678901234567890
34
2345678901234567890123456789012345678901234567890123456789012345678901
45
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
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
   ```

**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 - AFF A70 e AFF A90

Se um componente do seu sistema de armazenamento AFF A70 ou AFF A90 falhar, devolva a peça com defeito à NetApp. Consulte a "Devolução de peças e substituições" página para 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 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 SOBRESSALENTES; 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.