# Proteja aplicativos

## Astra Control Center

NetApp
August 11, 2025

# Índice


Proteja aplicativos . . . 1
Visão geral da proteção . . . 1
Fluxo de trabalho de proteção de aplicações . . . 1
Proteja aplicativos com snapshots e backups . . . 2
Configurar uma política de proteção . . . 2
Criar um instantâneo . . . 6
Crie uma cópia de segurança . . . 8
Habilite o backup e a restauração de operações de economia de ONTAP nas . . . 10
Crie um backup imutável . . . 11
Visualizar instantâneos e backups . . . 12
Eliminar instantâneos . . . 12
Cancelar cópias de segurança . . . 13
Eliminar cópias de segurança . . . 13
[Tech Preview] Proteja um cluster inteiro . . . 14
Como funciona . . . 14
Crie um backup programado de todos os namespaces . . . 14
Crie um backup programado de namespaces específicos . . . 15
Restaurar aplicações . . . 15
Restaure dados do backup ou do snapshot usando a IU da Web . . . 16
[Visualização técnica] Restaurar a partir da cópia de segurança utilizando um recurso personalizado (CR) . . . 17
[Visualização técnica] Restaurar a partir de instantâneos utilizando um recurso personalizado (CR) . . . 20
Filtre recursos durante uma restauração de aplicativos . . . 24
Complicações de restauração no local para um aplicativo que compartilha recursos com outro aplicativo . . . 25
Replique aplicativos entre back-ends de storage usando a tecnologia SnapMirror . . . 25
Pré-requisitos de replicação . . . 26
Configure uma relação de replicação . . . 28
Colocar um aplicativo replicado on-line no cluster de destino (failover) . . . 29
Ressincronizar uma falha na replicação . . . 30
Replicação reversa da aplicação . . . 30
Falha de aplicativos para o cluster de origem original . . . 31
Excluir uma relação de replicação de aplicativos . . . 31
Estado de integridade da relação de replicação e estados do ciclo de vida da relação . . . 32
Clonar e migrar aplicações . . . 33
Gerenciar ganchos de execução de aplicativos . . . 36
Tipos de ganchos de execução . . . 36
Filtros de gancho de execução . . . 36
Notas importantes sobre ganchos de execução personalizados . . . 37
Exemplos de gancho de execução . . . 40
Ative o recurso ganchos de execução . . . 40
Desative o recurso ganchos de execução . . . 40
Ver ganchos de execução existentes . . . 40

Exibir scripts existentes . . . 41
Adicione um script . . . 41
Excluir um script . . . 42
Crie um gancho de execução personalizado . . . 42
Verifique o estado de um gancho de execução . . . 43
Exibir o uso do script . . . 44
Edite um gancho de execução . . . 44
Desativar um gancho de execução . . . 44
Excluir um gancho de execução . . . 45
Para mais informações . . . 45
Proteger o Astra Control Center usando o Astra Control Center . . . 45
Etapa 1 opção: Faça backup e restauração do Astra Control Center . . . 47
Etapa 1 opção: Proteger o Astra Control Center usando a replicação . . . 49
Etapa 2: Restaure o Operador do Centro de Controle Astra . . . 52
Solução de problemas . . . 53

# Proteja aplicativos

## Visão geral da proteção

Você pode criar backups, clones, snapshots e políticas de proteção para suas aplicações usando o Astra Control Center. O backup de seus aplicativos ajuda seus serviços e dados associados a estarem o mais disponíveis possível; durante um cenário de desastre, a restauração do backup pode garantir a recuperação completa de um aplicativo e seus dados associados com o mínimo de interrupções. Backups, clones e snapshots podem ajudar a proteger contra ameaças comuns, como ransomware, perda acidental de dados e desastres ambientais. "Saiba mais sobre os tipos de proteção de dados disponíveis no Astra Control Center e quando usá-los".

Além disso, é possível replicar aplicações para um cluster remoto para se preparar para a recuperação de desastres.

### Fluxo de trabalho de proteção de aplicações

Você pode usar o fluxo de trabalho de exemplo a seguir para começar a proteger seus aplicativos.

#### [Um] Proteja todas as aplicações

Para garantir que seus aplicativos estejam protegidos imediatamente"crie um backup manual de todos os aplicativos", .

#### [Dois] Configure uma política de proteção para cada aplicativo

Para automatizar backups e snapshots futuros, "configure uma política de proteção para cada aplicativo". Por exemplo, você pode começar com backups semanais e snapshots diários, com retenção de um mês para ambos. A automação de backups e snapshots com uma política de proteção é altamente recomendada em backups e snapshots manuais.

#### [Três] Ajustar as políticas de proteção

À medida que as aplicações e os seus padrões de utilização mudam, ajuste as políticas de proteção conforme necessário para proporcionar a melhor proteção.

#### [Quatro] Replique aplicações para um cluster remoto

"Replicar aplicações" Para um cluster remoto usando a tecnologia NetApp SnapMirror. O Astra Control replica snapshots para um cluster remoto, fornecendo funcionalidade assíncrona de recuperação de desastres.

#### [Cinco] Em caso de desastre, restaure seus aplicativos com o backup ou replicação mais recente para o sistema remoto

Se a perda de dados ocorrer, você pode se recuperar "restaurar a cópia de segurança mais recente"primeiro para cada aplicativo. Em seguida, você pode restaurar o instantâneo mais recente (se disponível). Ou, você pode usar a replicação para um sistema remoto.

# Proteja aplicativos com snapshots e backups

Proteja todos os aplicativos tirando snapshots e backups usando uma política de proteção automatizada ou ad hoc. Você pode usar a IU do Astra Control Center ou "API Astra Control" para proteger aplicações.

**Sobre esta tarefa**

- **Aplicativos implantados pelo Helm**: Se você usar o Helm para implantar aplicativos, o Astra Control Center precisará do Helm versão 3. O gerenciamento e clonagem de aplicativos implantados com o Helm 3 (ou atualizados do Helm 2 para o Helm 3) são totalmente compatíveis. As aplicações implementadas com o Helm 2 não são suportadas.
- **(somente clusters OpenShift) Adicionar políticas**: Quando você cria um projeto para hospedar um aplicativo em um cluster OpenShift, o projeto (ou namespace Kubernetes) recebe um UID SecurityContext. Para ativar o Astra Control Center para proteger seu aplicativo e mover o aplicativo para outro cluster ou projeto no OpenShift, você precisa adicionar políticas que permitam que o aplicativo seja executado como qualquer UID. Como exemplo, os seguintes comandos OpenShift CLI concedem as políticas apropriadas a um aplicativo WordPress.

```
oc new-project wordpress
oc adm policy add-scc-to-group anyuid system:serviceaccounts:wordpress
oc adm policy add-scc-to-user privileged -z default -n wordpress
```

Você pode executar as seguintes tarefas relacionadas à proteção dos dados do aplicativo:

- Configurar uma política de proteção
- Criar um instantâneo
- Crie uma cópia de segurança
- Habilite o backup e a restauração de operações de economia de ONTAP nas
- Crie um backup imutável
- Visualizar instantâneos e backups
- Eliminar instantâneos
- Cancelar cópias de segurança
- Eliminar cópias de segurança

## Configurar uma política de proteção

Uma política de proteção protege um aplicativo criando snapshots, backups ou ambos em um cronograma definido. Você pode optar por criar snapshots e backups por hora, diariamente, semanalmente e mensalmente, e especificar o número de cópias a reter. Você pode definir uma política de proteção usando a IU da Web do Astra Control ou um arquivo de recurso personalizado (CR).

Se precisar de backups ou snapshots para executar com mais frequência do que uma vez por hora, você pode "Use a API REST do Astra Control para criar snapshots e backups".

Se você estiver definindo uma política de proteção que crie backups imutáveis para gravar buckets WORM (uma vez leitura muitas), verifique se o tempo de retenção dos backups não é menor do que o período de retenção configurado para o bucket.

Offset programações de backup e replicação para evitar sobreposições de agendamento. Por exemplo, execute backups no topo da hora a cada hora e programe a replicação para começar com um deslocamento de 5 minutos e um intervalo de 10 minutos.

### Configurar uma política de proteção usando a IU da Web

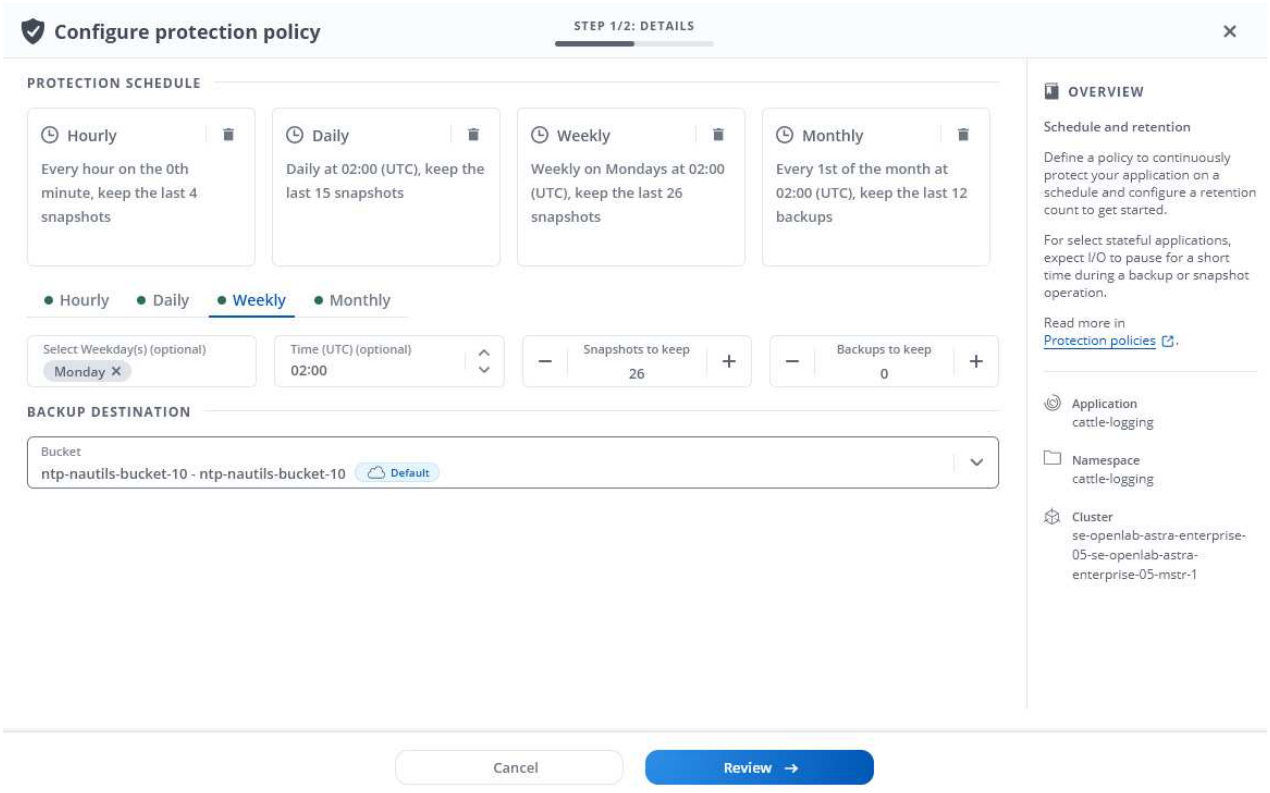
**Passos**

1. Selecione **aplicativos** e, em seguida, selecione o nome de um aplicativo.
2. Selecione **proteção de dados**.
3. Selecione **Configurar política de proteção**.
4. Defina um cronograma de proteção escolhendo o número de snapshots e backups para manter a hora, o dia, a semana e o mês.

   Você pode definir as programações por hora, diária, semanal e mensal simultaneamente. Uma programação não ficará ativa até que você defina um nível de retenção.

   Ao definir um nível de retenção para backups, você pode escolher o intervalo onde deseja armazenar os backups.

   O exemplo a seguir define quatro programações de proteção: Por hora, por dia, por semana e por mês para snapshots e backups.




5. [**Tech Preview**] escolha um intervalo de destino para os backups ou snapshots da lista de buckets de armazenamento.
6. Selecione **Revisão**.
7. Selecione **Definir política de proteção.**

### [Tech Preview] Configure uma política de proteção usando um CR

**Passos**

1. Crie o arquivo de recurso personalizado (CR) e nomeie-o `astra-control-schedule-cr.yaml`. Atualize os valores entre parêntesis> para atender às necessidades de proteção de dados,

configuração de cluster e ambiente Astra Control:

- <CR_NAME>: O nome deste recurso personalizado; escolha um nome único e sensato para o seu ambiente.
- <APPLICATION_NAME>: O nome do Kubernetes da aplicação para fazer backup.
- <APPVAULT_NAME>: O nome do AppVault onde o conteúdo de backup deve ser armazenado.
- <BACKUPS_RETAINED>: O número de backups a reter. Zero indica que nenhum backup deve ser criado.
- <SNAPSHOTS_RETAINED>: O número de instantâneos a reter. Zero indica que nenhum instantâneo deve ser criado.
- <GRANULARITY>: A frequência em que o horário deve ser executado. Valores possíveis, juntamente com campos associados obrigatórios:
  - `hourly` (requer que você `spec.minute` especifique )
  - `daily` (requer que você especifique `spec.minute` e `spec.hour`)
  - `weekly` (requer que você especifique `spec.minute`, `spec.hour` e `spec.dayOfWeek`)
  - `monthly` (requer que você especifique `spec.minute`, `spec.hour` e `spec.dayOfMonth`)
- <DAY_OF_MONTH>: *(Opcional)* o dia do mês (1 - 31) que o cronograma deve ser executado. Este campo é necessário se a granularidade estiver definida como `monthly`.
- <DAY_OF_WEEK>: *(Opcional)* o dia da semana (0 - 7) que o cronograma deve ser executado. Os valores de 0 ou 7 indicam domingo. Este campo é necessário se a granularidade estiver definida como `weekly`.
- <HOUR_OF_DAY>: *(Opcional)* a hora do dia (0 - 23) em que o horário deve ser executado. Este campo é necessário se a granularidade estiver definida como `daily`, `weekly` `monthly` ou .
- <MINUTE_OF_HOUR>: *(Opcional)* o minuto da hora (0 - 59) que o cronograma deve ser executado. Este campo é necessário se a granularidade estiver definida como `hourly`, , `daily` `weekly` , ou `monthly`.

```
apiVersion: astra.netapp.io/v1
kind: Schedule
metadata:
  namespace: astra-connector
  name: <CR_NAME>
spec:
  applicationRef: <APPLICATION_NAME>
  appVaultRef: <APPVAULT_NAME>
  backupRetention: "<BACKUPS_RETAINED>"
  snapshotRetention: "<SNAPSHOTS_RETAINED>"
  granularity: <GRANULARITY>
  dayOfMonth: "<DAY_OF_MONTH>"
  dayOfWeek: "<DAY_OF_WEEK>"
  hour: "<HOUR_OF_DAY>"
  minute: "<MINUTE_OF_HOUR>"
```

2. Depois de preencher o `astra-control-schedule-cr.yaml` ficheiro com os valores corretos, aplique o CR:

```
kubectl apply -f astra-control-schedule-cr.yaml
```

**Resultado**

O Astra Control implementa a política de proteção de dados criando e retendo snapshots e backups usando o cronograma e a política de retenção definidos por você.

## Criar um instantâneo

Você pode criar um snapshot sob demanda a qualquer momento.

**Sobre esta tarefa**

O Astra Control é compatível com a criação de snapshot usando classes de storage com o respaldo dos seguintes drivers:

- `ontap-nas`
- `ontap-san`
- `ontap-san-economy`

> Se o aplicativo usar uma classe de armazenamento suportada pelo `ontap-nas-economy` driver, os snapshots não poderão ser criados. Use uma classe de armazenamento alternativa para instantâneos.

**Crie um instantâneo usando a IU da Web**

**Passos**

1. Selecione **aplicações**.
2. No menu Opções na coluna **ações** para o aplicativo desejado, selecione **Instantâneo**.
3. Personalize o nome do instantâneo e selecione **Next**.
4. [**Tech Preview**] escolha um intervalo de destino para o instantâneo na lista de intervalos de armazenamento.
5. Reveja o resumo do instantâneo e selecione **Snapshot**.

**[Tech preview] Crie um instantâneo usando um CR**

**Passos**

1. Crie o arquivo de recurso personalizado (CR) e nomeie-o `astra-control-snapshot-cr.yaml`. Atualize os valores entre parêntesis> para corresponder ao seu ambiente Astra Control e à configuração de cluster:
   - <CR_NAME>: O nome deste recurso personalizado; escolha um nome único e sensato para o seu ambiente.
   - <APPLICATION_NAME>: O nome do Kubernetes da aplicação para snapshot.
   - <APPVAULT_NAME>: O nome do AppVault onde o conteúdo do snapshot deve ser armazenado.
   - <RECLAIM_POLICY>: *(Opcional)* define o que acontece com um snapshot quando o snapshot CR é excluído. Opções válidas:
     - `Retain`
     - `Delete` (predefinição)

     ```
     apiVersion: astra.netapp.io/v1
     kind: Snapshot
     metadata:
       namespace: astra-connector
       name: <CR_NAME>
     spec:
       applicationRef: <APPLICATION_NAME>
       appVaultRef: <APPVAULT_NAME>
       reclaimPolicy: <RECLAIM_POLICY>
     ```

2. Depois de preencher o `astra-control-snapshot-cr.yaml` ficheiro com os valores corretos, aplique o CR:

   ```
   kubectl apply -f astra-control-snapshot-cr.yaml
   ```

**Resultado**

O processo de instantâneo é iniciado. Um instantâneo é bem-sucedido quando o status é **saudável** na coluna **Estado** na página **proteção de dados** > **instantâneos**.

## Crie uma cópia de segurança

Você pode fazer backup de um aplicativo a qualquer momento.

**Sobre esta tarefa**

Buckets no Astra Control não relatam a capacidade disponível. Antes de fazer backup ou clonar aplicativos gerenciados pelo Astra Control, verifique as informações do bucket no sistema de gerenciamento de storage apropriado.

Se o seu aplicativo usa uma classe de armazenamento suportada pelo `ontap-nas-economy` driver, você precisa ativar cópia de segurança e restaurode funcionalidade. Certifique-se de que definiu um `backendType` parâmetro no "Objeto de storage do Kubernetes" com um valor de `ontap-nas-economy` antes de executar quaisquer operações de proteção.

O Astra Control é compatível com a criação de backup usando classes de storage com o respaldo dos seguintes drivers:

- `ontap-nas`
- `ontap-nas-economy`
- `ontap-san`
- `ontap-san-economy`

**Crie um backup usando a IU da Web**

**Passos**

1. Selecione **aplicações**.
2. No menu Opções na coluna **ações** para o aplicativo desejado, selecione **Backup**.
3. Personalize o nome da cópia de segurança.
4. Escolha se deseja fazer backup do aplicativo a partir de um snapshot existente. Se selecionar esta opção, pode escolher entre uma lista de instantâneos existentes.
5. [**Tech Preview**] escolha um intervalo de destino para o backup na lista de buckets de armazenamento.
6. Selecione **seguinte**.
7. Reveja o resumo da cópia de segurança e selecione **cópia de segurança**.

**[Tech Preview] Crie uma cópia de segurança utilizando um CR**

**Passos**

1. Crie o arquivo de recurso personalizado (CR) e nomeie-o `astra-control-backup-cr.yaml`. Atualize os valores entre parêntesis> para corresponder ao seu ambiente Astra Control e à configuração de cluster:
   - <CR_NAME>: O nome deste recurso personalizado; escolha um nome único e sensato para o seu ambiente.
   - <APPLICATION_NAME>: O nome do Kubernetes da aplicação para fazer backup.
   - <APPVAULT_NAME>: O nome do AppVault onde o conteúdo de backup deve ser armazenado.

   ```
   apiVersion: astra.netapp.io/v1
   kind: Backup
   metadata:
     namespace: astra-connector
     name: <CR_NAME>
   spec:
     applicationRef: <APPLICATION_NAME>
     appVaultRef: <APPVAULT_NAME>
   ```

2. Depois de preencher o `astra-control-backup-cr.yaml` ficheiro com os valores corretos, aplique o CR:

   ```
   kubectl apply -f astra-control-backup-cr.yaml
   ```

**Resultado**

O Astra Control cria um backup da aplicação.

- Se a sua rede tiver uma interrupção ou estiver anormalmente lenta, uma operação de backup pode acabar com o tempo limite. Isso faz com que o backup falhe.
- Se for necessário cancelar uma cópia de segurança em execução, utilize as instruções em Cancelar cópias de segurança. Para excluir o backup, aguarde até que ele esteja concluído e, em seguida, use as instruções na Eliminar cópias de segurança.
- Após uma operação de proteção de dados (clone, backup, restauração) e subsequente redimensionamento persistente de volume, há até vinte minutos de atraso antes que o novo tamanho de volume seja exibido na IU. A operação de proteção de dados é bem-sucedida em minutos. Você pode usar o software de gerenciamento do back-end de storage para confirmar a alteração no tamanho do volume.

## Habilite o backup e a restauração de operações de economia de ONTAP nas

O Astra Control Provisioner oferece funcionalidade de backup e restauração que pode ser habilitada para back-ends de storage que usam a `ontap-nas-economy` classe de storage.

**Antes de começar**

- Você "Ativou o Astra Control Provisioner"tem .
- Você definiu uma aplicação no Astra Control. Esta aplicação terá uma funcionalidade de proteçãoão limitada até concluir este procedimento.
- Você `ontap-nas-economy` selecionou como a classe de armazenamento padrão para o back-end de armazenamento.

**Passos**

1. Faça o seguinte no back-end de storage do ONTAP:
   a. Encontre o SVM que hospeda os `ontap-nas-economy` volumes baseados na aplicação.
   b. Faça login em um terminal conetado ao ONTAP onde os volumes são criados.
   c. Ocultar o diretório de snapshot para o SVM:

      Essa alteração afeta todo o SVM. O diretório oculto continuará acessível.

```
nfs modify -vserver <svm name> -v3-hide-snapshot enabled
```

+

Verifique se o diretório de snapshot no back-end de storage do ONTAP está oculto. A falha em ocultar esse diretório pode levar à perda de acesso ao aplicativo, especialmente se estiver usando NFSv3.

2. Faça o seguinte no Astra Control Provisioner:
   a. Ative o diretório instantâneo para cada PV que está `ontap-nas-economy` baseado e associado ao aplicativo:

```
tridentctl update volume <pv name> --snapshot-dir=true --pool-level
=true -n trident
```

b. Confirme se o diretório instantâneo foi ativado para cada PV associado:

```
tridentctl get volume <pv name> -n trident -o yaml | grep snapshotDir
```

Resposta:

```
snapshotDirectory: "true"
```

3. No Astra Control, atualize a aplicação depois de ativar todos os diretórios snapshot associados para que o Astra Control reconheça o valor alterado.

**Resultado**

A aplicação está pronta para fazer backup e restauração com o Astra Control. Cada PVC também está disponível para ser usado por outras aplicações para backups e restaurações.

## Crie um backup imutável

Um backup imutável não pode ser modificado, excluído ou substituído, desde que a política de retenção no bucket que armazena o backup o proíba. Você pode criar backups imutáveis fazendo backup de aplicativos em buckets que tenham uma política de retenção configurada. "Proteção de dados"Consulte para obter informações importantes sobre como trabalhar com backups imutáveis.

**Antes de começar**

Você precisa configurar o intervalo de destino com uma política de retenção. A forma como você faz isso será diferente dependendo do provedor de armazenamento que você usa. Consulte a documentação do fornecedor de armazenamento para obter mais informações:

- **Amazon Web Services**: "Ative o bloqueio de objetos S3D ao criar o bucket e defina um modo de retenção padrão de "governança" com um período de retenção padrão".
- **NetApp StorageGRID**: "Ative o bloqueio de objetos S3D ao criar o bucket e defina um modo de retenção padrão de "conformidade" com um período de retenção padrão".

> Buckets no Astra Control não relatam a capacidade disponível. Antes de fazer backup ou clonar aplicativos gerenciados pelo Astra Control, verifique as informações do bucket no sistema de gerenciamento de storage apropriado.

> Se o aplicativo usar uma classe de armazenamento apoiada pelo `ontap-nas-economy` driver, certifique-se de que você definiu um `backendType` parâmetro no "Objeto de storage do Kubernetes" com um valor de `ontap-nas-economy` antes de executar qualquer operação de proteção.

**Passos**

1. Selecione **aplicações**.

2. No menu Opções na coluna **ações** para o aplicativo desejado, selecione **Backup**.
3. Personalize o nome da cópia de segurança.
4. Escolha se deseja fazer backup do aplicativo a partir de um snapshot existente. Se selecionar esta opção, pode escolher entre uma lista de instantâneos existentes.
5. Escolha um intervalo de destino para o backup na lista de buckets de armazenamento. Um bucket WORM (write once read many) é indicado com um status de "bloqueado" ao lado do nome do bucket.

   Se o balde for um tipo não suportado, isso é indicado quando você passa o Mouse sobre ou seleciona o balde.

6. Selecione **seguinte**.
7. Reveja o resumo da cópia de segurança e selecione **cópia de segurança**.

**Resultado**

O Astra Control cria um backup imutável do aplicativo.

- Se a sua rede tiver uma interrupção ou estiver anormalmente lenta, uma operação de backup pode acabar com o tempo limite. Isso faz com que o backup falhe.
- Se você tentar criar dois backups imutáveis do mesmo aplicativo no mesmo bucket ao mesmo tempo, o Astra Control impede que o segundo backup seja iniciado. Aguarde até que o primeiro backup esteja concluído antes de iniciar outro.
- Não é possível cancelar um backup imutável em execução.
- Após uma operação de proteção de dados (clone, backup, restauração) e subsequente redimensionamento persistente de volume, há até vinte minutos de atraso antes que o novo tamanho de volume seja exibido na IU. A operação de proteção de dados é bem-sucedida em minutos. Você pode usar o software de gerenciamento do back-end de storage para confirmar a alteração no tamanho do volume.

## Visualizar instantâneos e backups

Você pode exibir os snapshots e backups de um aplicativo na guia proteção de dados.

Um backup imutável é indicado com um status de "bloqueado" ao lado do intervalo que está usando.

**Passos**

1. Selecione **aplicativos** e, em seguida, selecione o nome de um aplicativo.
2. Selecione **proteção de dados**.

   Os instantâneos são apresentados por predefinição.

3. Selecione **backups** para ver a lista de backups.

## Eliminar instantâneos

Exclua os snapshots programados ou sob demanda que você não precisa mais.

Não é possível excluir um instantâneo que está sendo replicado no momento.

**Passos**

1. Selecione **aplicativos** e, em seguida, selecione o nome de um aplicativo gerenciado.
2. Selecione **proteção de dados**.
3. No menu Opções na coluna **ações** para o instantâneo desejado, selecione **Excluir instantâneo**.
4. Digite a palavra "delete" para confirmar a exclusão e selecione **Yes, Delete snapshot**.

**Resultado**

O Astra Control exclui o Snapshot.

## Cancelar cópias de segurança

Pode cancelar uma cópia de segurança em curso.

Para cancelar uma cópia de segurança, a cópia de segurança tem de estar `Running` no estado. Não é possível cancelar uma cópia de segurança que esteja `Pending` no estado.

Não é possível cancelar um backup imutável em execução.

**Passos**

1. Selecione **aplicativos** e, em seguida, selecione o nome de um aplicativo.
2. Selecione **proteção de dados**.
3. Selecione **backups**.
4. No menu Opções na coluna **ações** para o backup desejado, selecione **Cancelar**.
5. Digite a palavra "cancelar" para confirmar a operação e selecione **Sim, cancelar backup**.

## Eliminar cópias de segurança

Exclua os backups programados ou sob demanda que você não precisa mais. Não é possível excluir um backup feito em um bucket imutável até que a política de retenção do bucket o permita fazer.

Você não pode excluir um backup imutável antes que o período de retenção expire.

Se for necessário cancelar uma cópia de segurança em execução, utilize as instruções em Cancelar cópias de segurança. Para excluir o backup, aguarde até que ele esteja concluído e, em seguida, use estas instruções.

**Passos**

1. Selecione **aplicativos** e, em seguida, selecione o nome de um aplicativo.
2. Selecione **proteção de dados**.
3. Selecione **backups**.
4. No menu Opções na coluna **ações** para o backup desejado, selecione **Excluir backup**.
5. Digite a palavra "delete" para confirmar a exclusão e selecione **Yes, Delete backup**.

**Resultado**

O Astra Control exclui o backup.

# [Tech Preview] Proteja um cluster inteiro

Você pode criar um backup automático e agendado de qualquer um ou todos os namespaces não gerenciados em um cluster. Esses fluxos de trabalho são fornecidos pelo NetApp como uma conta de serviço do Kubernetes, vinculações de função e um trabalho cron, orquestrado com um script Python.

## Como funciona

Quando você configura e instala o fluxo de trabalho de backup de cluster completo, uma tarefa cron é executada periodicamente e protege qualquer namespace que ainda não seja gerenciado, criando automaticamente políticas de proteção com base nos horários escolhidos durante a instalação.

Se você não quiser proteger todos os namespace não gerenciados no cluster com o fluxo de trabalho completo de backup do cluster, pode utilizar o fluxo de trabalho de backup baseado em rótulos. O fluxo de trabalho de backup baseado em rótulos também usa uma tarefa cron, mas em vez de proteger todos os namespaces não gerenciados, ele identifica namespaces por rótulos que você fornece para proteger opcionalmente os namespaces com base em políticas de backup bronze, prata ou ouro.

Quando um novo namespace é criado que se enquadra no escopo do fluxo de trabalho escolhido, ele é protegido automaticamente, sem qualquer ação do administrador. Esses fluxos de trabalho são implementados por cluster para que diferentes clusters possam usar qualquer fluxo de trabalho com níveis de proteção exclusivos, dependendo da importância do cluster.

#### Exemplo: Proteção total do cluster

Por exemplo, quando você configura e instala o fluxo de trabalho completo de backup do cluster, todos os aplicativos em qualquer namespace são gerenciados e protegidos periodicamente, sem mais esforço do administrador. O namespace não precisa existir no momento em que você instala o fluxo de trabalho; se um namespace for adicionado no futuro, ele será protegido.

#### Exemplo: Proteção baseada em etiquetas

Para obter mais granularidade, você pode usar o fluxo de trabalho baseado em rótulos. Por exemplo, você pode instalar esse fluxo de trabalho e dizer aos usuários para aplicar um dos vários rótulos a qualquer namespaces que eles querem proteger, dependendo do nível de proteção que eles precisam. Isso permite que os usuários criem o namespace com um desses rótulos, e eles não precisam notificar um administrador. Seu novo namespace e todos os aplicativos dentro dele são protegidos automaticamente.

## Crie um backup programado de todos os namespaces

Você pode criar um backup agendado de todos os namespaces em um cluster usando o fluxo de trabalho completo de backup do cluster.

#### Passos

1. Transfira os seguintes ficheiros para uma máquina que tenha acesso à rede ao cluster:
   - "Arquivo CRD Components.yaml"
   - "protectCluster.py Python script"
2. Para configurar e instalar o kit de ferramentas, "siga as instruções incluídas".

### Crie um backup programado de namespaces específicos

Você pode criar um backup agendado de namespaces específicos por seus rótulos usando o fluxo de trabalho de backup baseado em rótulos.

**Passos**

1. Transfira os seguintes ficheiros para uma máquina que tenha acesso à rede ao cluster:
   - "Arquivo CRD Components.yaml"
   - "protectCluster.py Python script"
2. Para configurar e instalar o kit de ferramentas, "siga as instruções incluídas".

# Restaurar aplicações

O Astra Control pode restaurar sua aplicação a partir de um snapshot ou backup. A restauração a partir de um instantâneo existente será mais rápida ao restaurar o aplicativo para o mesmo cluster. Você pode usar a IU do Astra Control ou "API Astra Control" restaurar aplicações.

**Antes de começar**

- * Proteja seus aplicativos primeiro *: É altamente recomendável que você tire um instantâneo ou backup de seu aplicativo antes de restaurá-lo. Isso permitirá clonar a partir do snapshot ou backup se a restauração não for bem-sucedida.
- **Verificar volumes de destino**: Se você restaurar para uma classe de armazenamento diferente, verifique se a classe de armazenamento usa o mesmo modo de acesso de volume persistente (por exemplo, ReadWriteMany). A operação de restauração falhará se o modo de acesso ao volume persistente de destino for diferente. Por exemplo, se o volume persistente de origem usar o modo de acesso RWX, selecionar uma classe de armazenamento de destino que não seja capaz de fornecer RWX, como discos gerenciados do Azure, AWS EBS, Google Persistent Disk ou `ontap-san`, fará com que a operação de restauração falhe. Para obter mais informações sobre os modos de acesso de volume persistente, consulte "Kubernetes" a documentação.
- **Planejar necessidades de espaço**: Quando você executa uma restauração no local de um aplicativo que usa armazenamento NetApp ONTAP, o espaço usado pelo aplicativo restaurado pode dobrar. Depois de executar uma restauração no local, remova todos os snapshots indesejados do aplicativo restaurado para liberar espaço de armazenamento.
- **(somente clusters Red Hat OpenShift) Adicionar políticas**: Quando você cria um projeto para hospedar um aplicativo em um cluster OpenShift, o projeto (ou namespace Kubernetes) recebe um UID SecurityContext. Para ativar o Astra Control Center para proteger seu aplicativo e mover o aplicativo para outro cluster ou projeto no OpenShift, você precisa adicionar políticas que permitam que o aplicativo seja executado como qualquer UID. Como exemplo, os seguintes comandos OpenShift CLI concedem as políticas apropriadas a um aplicativo WordPress.

  ```
  oc new-project wordpress
  oc adm policy add-scc-to-group anyuid system:serviceaccounts:wordpress
  oc adm policy add-scc-to-user privileged -z default -n wordpress
  ```

- **Drivers de classe de armazenamento suportados**: O Astra Control suporta a restauração de backups usando classes de armazenamento suportadas pelos seguintes drivers:
  - `ontap-nas`

- `ontap-nas-economy`
- `ontap-san`
- `ontap-san-economy`

- * (Somente driver ONTAP-nas-Economy) backups e restaurações*: Antes de fazer backup ou restaurar um aplicativo que usa uma classe de armazenamento apoiada pelo `ontap-nas-economy` driver, verifique se o "O diretório snapshot no back-end de storage do ONTAP está oculto". A falha em ocultar esse diretório pode levar à perda de acesso ao aplicativo, especialmente se estiver usando NFSv3.
- **Aplicativos implantados pelo Helm**: Os aplicativos implantados com o Helm 3 (ou atualizados do Helm 2 para o Helm 3) são totalmente suportados. As aplicações implementadas com o Helm 2 não são suportadas.

> Executar uma operação de restauração no local em um aplicativo que compartilhe recursos com outro aplicativo pode ter resultados não desejados. Todos os recursos compartilhados entre os aplicativos são substituídos quando uma restauração no local é executada em um dos aplicativos. Para obter mais informações, este exemploconsulte .

Execute as etapas a seguir, dependendo do tipo de arquivo que você deseja restaurar:

## Restaure dados do backup ou do snapshot usando a IU da Web

Você pode restaurar os dados usando a IU da Web Astra Control.

**Passos**

1. Selecione **aplicativos** e, em seguida, selecione o nome de um aplicativo.
2. No menu Opções na coluna ações, selecione **Restaurar**.
3. Escolha o tipo de restauração:
   - **Restaurar para namespaces originais**: Use este procedimento para restaurar o aplicativo no local para o cluster original.

     > Se o aplicativo usar uma classe de armazenamento apoiada pelo `ontap-nas-economy` driver, você deverá restaurar o aplicativo usando as classes de armazenamento originais. Você não pode especificar uma classe de armazenamento diferente se estiver restaurando o aplicativo para o mesmo namespace.

     i. Selecione o instantâneo ou o backup a ser usado para restaurar o aplicativo no local, o que reverte o aplicativo para uma versão anterior de si mesmo.

     ii. Selecione **seguinte**.

     > Se você restaurar para um namespace que foi excluído anteriormente, um novo namespace com o mesmo nome será criado como parte do processo de restauração. Todos os usuários que tinham direitos para gerenciar aplicativos no namespace excluído anteriormente precisam restaurar manualmente os direitos para o namespace recém-criado.

   - * Restaurar para novos namespaces*: Use este procedimento para restaurar o aplicativo para outro cluster ou com namespaces diferentes da origem.

     i. Especifique o nome do aplicativo restaurado.

ii. Escolha o cluster de destino para o aplicativo que você pretende restaurar.

iii. Insira um namespace de destino para cada namespace de origem associado ao aplicativo.

> O Astra Control cria novos namespaces de destino como parte dessa opção de restauração. Namespaces de destino que você especificar não devem estar presentes no cluster de destino.

iv. Selecione **seguinte**.

v. Selecione o instantâneo ou a cópia de segurança a utilizar para restaurar a aplicação.

vi. Selecione **seguinte**.

vii. Escolha uma das seguintes opções:

- **Restaurar usando classes de armazenamento originais**: O aplicativo usa a classe de armazenamento originalmente associada, a menos que não exista no cluster de destino. Neste caso, a classe de armazenamento padrão para o cluster será usada.
- **Restaurar usando uma classe de armazenamento diferente**: Selecione uma classe de armazenamento existente no cluster de destino. Todos os volumes de aplicativos, independentemente de suas classes de armazenamento originalmente associadas, serão migrados para essa classe de armazenamento diferente como parte da restauração.

viii. Selecione **seguinte**.

4. Escolha quaisquer recursos para filtrar:
   - **Restaurar todos os recursos**: Restaure todos os recursos associados ao aplicativo original.
   - **Filtrar recursos**: Especifique regras para restaurar um sub-conjunto dos recursos originais do aplicativo:
     i. Escolha incluir ou excluir recursos do aplicativo restaurado.
     ii. Selecione **Adicionar regra de inclusão** ou **Adicionar regra de exclusão** e configure a regra para filtrar os recursos corretos durante a restauração do aplicativo. Você pode editar uma regra ou removê-la e criar uma regra novamente até que a configuração esteja correta.

> Para saber mais sobre como configurar regras de inclusão e exclusão, Filtre recursos durante uma restauração de aplicativosconsulte .

5. Selecione **seguinte**.
6. Revise os detalhes sobre a ação de restauração cuidadosamente, digite "restaurar" (se solicitado) e selecione **Restaurar**.

## [Visualização técnica] Restaurar a partir da cópia de segurança utilizando um recurso personalizado (CR)

Você pode restaurar dados de um backup usando um arquivo de recurso personalizado (CR) para um namespace diferente ou para o namespace de origem original.

**Restaurar a partir de uma cópia de segurança utilizando um CR**

**Passos**

1. Crie o arquivo de recurso personalizado (CR) e nomeie-o `astra-control-backup-restore-cr.yaml`. Atualize os valores entre parêntesis> para corresponder ao seu ambiente Astra Control e à configuração de cluster:
   - <CR_NAME>: O nome desta operação de CR; escolha um nome sensato para o seu ambiente.
   - <APPVAULT_NAME>: O nome do AppVault onde o conteúdo de backup é armazenado.
   - <BACKUP_PATH>: O caminho dentro do AppVault onde o conteúdo do backup é armazenado. Por exemplo:

     ```
     ONTAP-S3_1343ff5e-4c41-46b5-af00/backups/schedule-
     20231213023800_94347756-9d9b-401d-a0c3
     ```

   - <SOURCE_NAMESPACE>: O namespace de origem da operação de restauração.
   - <DESTINATION_NAMESPACE>: O namespace de destino da operação de restauração.

     ```
     apiVersion: astra.netapp.io/v1
     kind: BackupRestore
     metadata:
       name: <CR_NAME>
       namespace: astra-connector
     spec:
       appVaultRef: <APPVAULT_NAME>
       appArchivePath: <BACKUP_PATH>
       namespaceMapping: [{"source": "<SOURCE_NAMESPACE>",
     "destination": "<DESTINATION_NAMESPACE>"}]
     ```

2. (Opcional) se você precisar selecionar apenas determinados recursos do aplicativo para restaurar, adicione filtragem que inclua ou exclua recursos marcados com rótulos específicos:
   - "<INCLUDE-EXCLUDE>": *(obrigatório para filtragem)* Use `include` ou `exclude` para incluir ou excluir um recurso definido em resourceMatchers. Adicione os seguintes parâmetros resourceMatchers para definir os recursos a serem incluídos ou excluídos:
     - <GROUP>: *(Opcional)* Grupo do recurso a ser filtrado.
     - <KIND>: *(Opcional)* tipo do recurso a ser filtrado.
     - <VERSION>: *(Opcional)* versão do recurso a ser filtrado.
     - <NAMES>: Nomes *(Opcional)* no campo Kubernetes metadata.name do recurso a ser filtrado.
     - <NAMESPACES>: *(Opcional)* namespaces no campo Kubernetes metadata.name do recurso a ser filtrado.
     - <SELECTORS>: *(Opcional)* string de seletor de rótulos no campo Kubernetes metadata.name do recurso conforme definido em "Documentação do Kubernetes". exemplo: . `"trident.netapp.io/os=linux"`

Exemplo:

```
spec:
    resourceFilter:
        resourceSelectionCriteria: "<INCLUDE-EXCLUDE>"
        resourceMatchers:
           group: <GROUP>
           kind: <KIND>
           version: <VERSION>
           names: <NAMES>
           namespaces: <NAMESPACES>
           labelSelectors: <SELECTORS>
```

3. Depois de preencher o `astra-control-backup-restore-cr.yaml` ficheiro com os valores corretos, aplique o CR:

```
kubectl apply -f astra-control-backup-restore-cr.yaml
```

**Restaure do backup para o namespace original usando um CR**

**Passos**

1. Crie o arquivo de recurso personalizado (CR) e nomeie-o `astra-control-backup-ipr-cr.yaml`. Atualize os valores entre parêntesis> para corresponder ao seu ambiente Astra Control e à configuração de cluster:
   - <CR_NAME>: O nome desta operação de CR; escolha um nome sensato para o seu ambiente.
   - <APPVAULT_NAME>: O nome do AppVault onde o conteúdo de backup é armazenado.
   - <BACKUP_PATH>: O caminho dentro do AppVault onde o conteúdo do backup é armazenado. Por exemplo:

     ```
     ONTAP-S3_1343ff5e-4c41-46b5-af00/backups/schedule-
     20231213023800_94347756-9d9b-401d-a0c3
     ```

     ```
     apiVersion: astra.netapp.io/v1
     kind: BackupInplaceRestore
     metadata:
       name: <CR_NAME>
       namespace: astra-connector
     spec:
       appVaultRef: <APPVAULT_NAME>
       appArchivePath: <BACKUP_PATH>
     ```

2. (Opcional) se você precisar selecionar apenas determinados recursos do aplicativo para restaurar, adicione filtragem que inclua ou exclua recursos marcados com rótulos específicos:

- "<INCLUDE-EXCLUDE>": *(obrigatório para filtragem)* Use `include` ou `exclude` para incluir ou excluir um recurso definido em resourceMatchers. Adicione os seguintes parâmetros resourceMatchers para definir os recursos a serem incluídos ou excluídos:
  - <GROUP>: *(Opcional)* Grupo do recurso a ser filtrado.
  - <KIND>: *(Opcional)* tipo do recurso a ser filtrado.
  - <VERSION>: *(Opcional)* versão do recurso a ser filtrado.
  - <NAMES>: Nomes *(Opcional)* no campo Kubernetes metadata.name do recurso a ser filtrado.
  - <NAMESPACES>: *(Opcional)* namespaces no campo Kubernetes metadata.name do recurso a ser filtrado.
  - <SELECTORS>: *(Opcional)* string de seletor de rótulos no campo Kubernetes metadata.name do recurso conforme definido em "Documentação do Kubernetes". exemplo: . `"trident.netapp.io/os=linux"`

    Exemplo:

```
spec:
    resourceFilter:
        resourceSelectionCriteria: "<INCLUDE-EXCLUDE>"
        resourceMatchers:
           group: <GROUP>
           kind: <KIND>
           version: <VERSION>
           names: <NAMES>
           namespaces: <NAMESPACES>
           labelSelectors: <SELECTORS>
```

3. Depois de preencher o `astra-control-backup-ipr-cr.yaml` ficheiro com os valores corretos, aplique o CR:

```
kubectl apply -f astra-control-backup-ipr-cr.yaml
```

## [Visualização técnica] Restaurar a partir de instantâneos utilizando um recurso personalizado (CR)

É possível restaurar dados de um snapshot usando um arquivo de recurso personalizado (CR) para um namespace diferente ou namespace de origem original.

**Restaurar a partir de instantâneos usando um CR**

**Passos**

1. Crie o arquivo de recurso personalizado (CR) e nomeie-o `astra-control-snapshot-restore-cr.yaml`. Atualize os valores entre parêntesis> para corresponder ao seu ambiente Astra Control e à configuração de cluster:
   - <CR_NAME>: O nome desta operação de CR; escolha um nome sensato para o seu ambiente.
   - <APPVAULT_NAME>: O nome do AppVault onde o conteúdo de backup é armazenado.
   - <BACKUP_PATH>: O caminho dentro do AppVault onde o conteúdo do backup é armazenado. Por exemplo:

     ```
     ONTAP-S3_1343ff5e-4c41-46b5-af00/backups/schedule-
     20231213023800_94347756-9d9b-401d-a0c3
     ```

   - <SOURCE_NAMESPACE>: O namespace de origem da operação de restauração.
   - <DESTINATION_NAMESPACE>: O namespace de destino da operação de restauração.

     ```
     apiVersion: astra.netapp.io/v1
     kind: SnapshotRestore
     metadata:
       name: <CR_NAME>
       namespace: astra-connector
     spec:
       appArchivePath: <BACKUP_PATH>
       appVaultRef: <APPVAULT_NAME>
       namespaceMapping: [{"source": "<SOURCE_NAMESPACE>",
     "destination": "<DESTINATION_NAMESPACE>"}]
     ```

2. (Opcional) se você precisar selecionar apenas determinados recursos do aplicativo para restaurar, adicione filtragem que inclua ou exclua recursos marcados com rótulos específicos:
   - "<INCLUDE-EXCLUDE>": *(obrigatório para filtragem)* Use `include` ou `exclude` para incluir ou excluir um recurso definido em resourceMatchers. Adicione os seguintes parâmetros resourceMatchers para definir os recursos a serem incluídos ou excluídos:
     - <GROUP>: *(Opcional)* Grupo do recurso a ser filtrado.
     - <KIND>: *(Opcional)* tipo do recurso a ser filtrado.
     - <VERSION>: *(Opcional)* versão do recurso a ser filtrado.
     - <NAMES>: Nomes *(Opcional)* no campo Kubernetes metadata.name do recurso a ser filtrado.
     - <NAMESPACES>: *(Opcional)* namespaces no campo Kubernetes metadata.name do recurso a ser filtrado.
     - <SELECTORS>: *(Opcional)* string de seletor de rótulos no campo Kubernetes metadata.name do recurso conforme definido em "Documentação do Kubernetes". exemplo: . `"trident.netapp.io/os=linux"`

Exemplo:

```
spec:
    resourceFilter:
        resourceSelectionCriteria: "<INCLUDE-EXCLUDE>"
        resourceMatchers:
           group: <GROUP>
           kind: <KIND>
           version: <VERSION>
           names: <NAMES>
           namespaces: <NAMESPACES>
           labelSelectors: <SELECTORS>
```

3. Depois de preencher o `astra-control-snapshot-restore-cr.yaml` ficheiro com os valores corretos, aplique o CR:

```
kubectl apply -f astra-control-snapshot-restore-cr.yaml
```

**Restaure do instantâneo para o namespace original usando um CR**

**Passos**

1. Crie o arquivo de recurso personalizado (CR) e nomeie-o `astra-control-snapshot-ipr-cr.yaml`. Atualize os valores entre parêntesis> para corresponder ao seu ambiente Astra Control e à configuração de cluster:
   - <CR_NAME>: O nome desta operação de CR; escolha um nome sensato para o seu ambiente.
   - <APPVAULT_NAME>: O nome do AppVault onde o conteúdo de backup é armazenado.
   - <BACKUP_PATH>: O caminho dentro do AppVault onde o conteúdo do backup é armazenado. Por exemplo:

```
ONTAP-S3_1343ff5e-4c41-46b5-af00/backups/schedule-
20231213023800_94347756-9d9b-401d-a0c3
```

```
apiVersion: astra.netapp.io/v1
kind: SnapshotInplaceRestore
metadata:
  name: <CR_NAME>
  namespace: astra-connector
spec:
  appArchivePath: <BACKUP_PATH>
  appVaultRef: <APPVAULT_NAME>
```

2. (Opcional) se você precisar selecionar apenas determinados recursos do aplicativo para restaurar, adicione filtragem que inclua ou exclua recursos marcados com rótulos específicos:

- "<INCLUDE-EXCLUDE>": *(obrigatório para filtragem)* Use `include` ou `exclude` para incluir ou excluir um recurso definido em resourceMatchers. Adicione os seguintes parâmetros resourceMatchers para definir os recursos a serem incluídos ou excluídos:
  - <GROUP>: *(Opcional)* Grupo do recurso a ser filtrado.
  - <KIND>: *(Opcional)* tipo do recurso a ser filtrado.
  - <VERSION>: *(Opcional)* versão do recurso a ser filtrado.
  - <NAMES>: Nomes *(Opcional)* no campo Kubernetes metadata.name do recurso a ser filtrado.
  - <NAMESPACES>: *(Opcional)* namespaces no campo Kubernetes metadata.name do recurso a ser filtrado.
  - <SELECTORS>: *(Opcional)* string de seletor de rótulos no campo Kubernetes metadata.name do recurso conforme definido em "Documentação do Kubernetes". exemplo: . `"trident.netapp.io/os=linux"`

    Exemplo:

```
spec:
    resourceFilter:
        resourceSelectionCriteria: "<INCLUDE-EXCLUDE>"
        resourceMatchers:
           group: <GROUP>
           kind: <KIND>
           version: <VERSION>
           names: <NAMES>
           namespaces: <NAMESPACES>
           labelSelectors: <SELECTORS>
```

3. Depois de preencher o `astra-control-snapshot-ipr-cr.yaml` ficheiro com os valores corretos, aplique o CR:

```
kubectl apply -f astra-control-snapshot-ipr-cr.yaml
```

**Resultado**

O Astra Control restaura a aplicação com base nas informações fornecidas. Se você restaurou o aplicativo no local, o conteúdo dos volumes persistentes existentes será substituído pelo conteúdo de volumes persistentes do aplicativo restaurado.

> Após uma operação de proteção de dados (clone, backup ou restauração) e subsequente redimensionamento persistente de volume, há um atraso de até vinte minutos antes que o novo tamanho de volume seja exibido na IU da Web. A operação de proteção de dados é bem-sucedida em minutos. Você pode usar o software de gerenciamento do back-end de storage para confirmar a alteração no tamanho do volume.

Qualquer usuário membro com restrições de namespace por nome/ID de namespace ou por rótulos de namespace pode clonar ou restaurar um aplicativo para um novo namespace no mesmo cluster ou para qualquer outro cluster na conta da organização. No entanto, o mesmo usuário não pode acessar o aplicativo clonado ou restaurado no novo namespace. Após uma operação de clone ou restauração criar um novo namespace, o administrador/proprietário da conta pode editar a conta de usuário membro e atualizar as restrições de função para o usuário afetado conceder acesso ao novo namespace.

## Filtre recursos durante uma restauração de aplicativos

Você pode adicionar uma regra de filtro a uma "restaurar" operação que especificará os recursos existentes do aplicativo a serem incluídos ou excluídos do aplicativo restaurado. Você pode incluir ou excluir recursos com base em um namespace, rótulo ou GVK (GroupVersionKind) especificado.

**Expanda para obter mais informações sobre incluir e excluir cenários**

- **Você seleciona uma regra include com namespaces originais (in-place restore)**: Os recursos de aplicativo existentes que você definir na regra serão excluídos e substituídos por aqueles do snapshot selecionado ou backup que você está usando para a restauração. Quaisquer recursos que você não especificar na regra incluir permanecerão inalterados.
- **Você seleciona uma regra de inclusão com novos namespaces**: Use a regra para selecionar os recursos específicos desejados no aplicativo restaurado. Quaisquer recursos que você não especificar na regra incluir não serão incluídos no aplicativo restaurado.
- **Você seleciona uma regra de exclusão com namespaces originais (in-loco restore)**: Os recursos que você especificar para serem excluídos não serão restaurados e permanecerão inalterados. Os recursos que você não especificar para excluir serão restaurados do snapshot ou backup. Todos os dados em volumes persistentes serão excluídos e recriados se o StatefulSet correspondente fizer parte dos recursos filtrados.
- **Você seleciona uma regra de exclusão com novos namespaces**: Use a regra para selecionar os recursos específicos que deseja remover do aplicativo restaurado. Os recursos que você não especificar para excluir serão restaurados do snapshot ou backup.

As regras são incluir ou excluir tipos. Regras que combinem inclusão e exclusão de recursos não estão disponíveis.

**Passos**

1. Depois de escolher filtrar recursos e selecionar uma opção incluir ou excluir no assistente Restaurar aplicativo, selecione **Adicionar regra de inclusão** ou **Adicionar regra de exclusão**.

   Não é possível excluir quaisquer recursos com escopo de cluster que sejam incluídos automaticamente pelo Astra Control.

2. Configure a regra de filtro:

   Você deve especificar pelo menos um namespace, rótulo ou GVK. Certifique-se de que todos os recursos que você mantém após as regras de filtro são suficientes para manter o aplicativo restaurado em um estado saudável.

   a. Selecione um namespace específico para a regra. Se você não fizer uma seleção, todos os namespaces serão usados no filtro.

Se o seu aplicativo originalmente continha vários namespaces e você o restaura para novos namespaces, todos os namespaces serão criados mesmo que eles não contenham recursos.

b. (Opcional) Digite um nome de recurso.

c. (Opcional) **Seletor de etiquetas**: Inclua a "seletor de etiquetas" para adicionar à regra. O seletor de etiquetas é utilizado para filtrar apenas os recursos que correspondem à etiqueta selecionada.

d. (Opcional) Selecione **Use GVK (GroupVersionKind) definido para filtrar recursos** para opções de filtragem adicionais.

Se você usar um filtro GVK, você deve especificar versão e tipo.

i. (Opcional) **Group**: Na lista suspensa, selecione o grupo da API do Kubernetes.

ii. **Kind**: Na lista suspensa, selecione o esquema de objeto para o tipo de recurso do Kubernetes a ser usado no filtro.

iii. **Versão**: Selecione a versão da API do Kubernetes.

3. Revise a regra criada com base em suas entradas.
4. Selecione **Adicionar**.

Você pode criar quantos recursos incluir e excluir regras quiser. As regras aparecem no resumo do aplicativo de restauração antes de iniciar a operação.

### Complicações de restauração no local para um aplicativo que compartilha recursos com outro aplicativo

Você pode executar uma operação de restauração no local em um aplicativo que compartilhe recursos com outro aplicativo e produza resultados não intencionais. Todos os recursos compartilhados entre os aplicativos são substituídos quando uma restauração no local é executada em um dos aplicativos.

O seguinte é um cenário de exemplo que cria uma situação indesejável ao usar a replicação do NetApp SnapMirror para uma restauração:

1. Você define o aplicativo `app1` usando o namespace `ns1`.
2. Você configura uma relação de replicação para `app1`o .
3. Você define o `app2` aplicativo (no mesmo cluster) usando os namespaces e `ns1` `ns2`.
4. Você configura uma relação de replicação para `app2`o .
5. Inverta a replicação para `app2`o . Isso faz com que o `app1` aplicativo no cluster de origem seja desativado.

# Replique aplicativos entre back-ends de storage usando a tecnologia SnapMirror

Com o Astra Control, você pode criar continuidade dos negócios para suas aplicações com RPO baixo (objetivo do ponto de recuperação) e rto baixo (objetivo do tempo de recuperação) usando funcionalidades de replicação assíncrona da tecnologia NetApp

SnapMirror. Uma vez configurados, isso permite que as aplicações repliquem alterações de dados e aplicações de um back-end de storage para outro, no mesmo cluster ou entre clusters diferentes.

Para obter uma comparação entre backups/restaurações e replicação, "Conceitos de proteção de dados"consulte .

Você pode replicar aplicativos em diferentes cenários, como os seguintes cenários somente no local, híbridos e multicloud:

- Local A para local A.
- Local A para local B no local
- On-premises para a nuvem com o Cloud Volumes ONTAP
- Nuvem com Cloud Volumes ONTAP no local
- Nuvem com Cloud Volumes ONTAP para nuvem (entre diferentes regiões no mesmo fornecedor de nuvem ou para diferentes fornecedores de nuvem)

O Astra Control pode replicar aplicações entre clusters no local, no local para a nuvem (usando o Cloud Volumes ONTAP) ou entre nuvens (Cloud Volumes ONTAP para Cloud Volumes ONTAP).

> Você pode replicar simultaneamente um aplicativo diferente na direção oposta. Por exemplo, os aplicativos A, B, C podem ser replicados do Datacenter 1 para o Datacenter 2; e os aplicativos X, Y, Z podem ser replicados do Datacenter 2 para o Datacenter 1.

Com o Astra Control, você pode fazer as seguintes tarefas relacionadas a replicação de aplicações:

- Configure uma relação de replicação
- Colocar um aplicativo replicado on-line no cluster de destino (failover)
- Ressincronizar uma falha na replicação
- Replicação reversa da aplicação
- Falha de aplicativos para o cluster de origem original
- Excluir uma relação de replicação de aplicativos

## Pré-requisitos de replicação

A replicação de aplicações Astra Control requer que os seguintes pré-requisitos sejam atendidos antes de começar:

**Clusters de ONTAP**

- * Astra Control Provisioner ou Astra Trident*: O Astra Control Provisioner ou o Astra Trident devem existir nos clusters de Kubernetes de origem e destino que utilizam o ONTAP como back-end. O Astra Control é compatível com replicação com tecnologia NetApp SnapMirror usando classes de storage com os seguintes drivers:
  - `ontap-nas`
  - `ontap-san`
- **Licenças**: As licenças assíncronas do ONTAP SnapMirror usando o pacote proteção de dados devem estar ativadas nos clusters ONTAP de origem e destino. "Visão geral do licenciamento do SnapMirror no

ONTAP"Consulte para obter mais informações.

**Peering**

- **Cluster e SVM**: Os backends de storage do ONTAP devem ser colocados em Contato. "Visão geral do peering de cluster e SVM"Consulte para obter mais informações.

  Certifique-se de que os nomes do SVM usados na relação de replicação entre dois clusters ONTAP sejam exclusivos.

- **Astra Control Provisioner ou Astra Trident e SVM**: Os SVMs remotas em peering precisam estar disponíveis para o Astra Control Provisioner ou Astra Trident no cluster de destino.

  **Astra Control Center**

  "Implante o Astra Control Center" em um domínio de terceira falha ou local secundário para recuperação de desastres otimizada.

- **Backends gerenciados**: Você precisa adicionar e gerenciar backends de storage do ONTAP no Astra Control Center para criar uma relação de replicação.

  Adicionar e gerenciar back-ends de storage do ONTAP no Astra Control Center é opcional se você ativou o Astra Control Provisioner.

- **Clusters gerenciados**: Adicione e gerencie os seguintes clusters com o Astra Control, de preferência em diferentes domínios ou locais de falha:
  - Fonte do cluster do Kubernetes
  - Cluster de destino Kubernetes
  - Clusters associados do ONTAP
- **Contas de usuário**: Quando você adiciona um back-end de storage do ONTAP ao Centro de Controle Astra, aplique credenciais de usuário com a função "admin". Essa função tem métodos de acesso `http` e `ontapi` é habilitada nos clusters de origem e destino do ONTAP. "Gerenciar contas de usuário na documentação do ONTAP"Consulte para obter mais informações.

  Com a funcionalidade Astra Control Provisioner, você não precisa definir especificamente uma função de "administrador" para gerenciar clusters no Astra Control Center, pois essas credenciais não são exigidas pelo Astra Control Center.

O Astra Control Center não oferece suporte à replicação NetApp SnapMirror para back-ends de storage que usam o protocolo NVMe em TCP.

**Configuração Astra Trident/ONTAP**

O Astra Control Center exige que você configure pelo menos um back-end de storage compatível com a replicação para os clusters de origem e destino. Se os clusters de origem e destino forem iguais, o aplicativo de destino deverá usar um back-end de storage diferente do aplicativo de origem para obter a melhor resiliência.

A replicação do Astra Control é compatível com aplicações que usam uma única classe de storage. Ao adicionar um aplicativo a um namespace, verifique se o aplicativo tem a mesma classe de armazenamento que outros aplicativos no namespace. Ao adicionar um PVC a um aplicativo replicado, verifique se o novo PVC tem a mesma classe de armazenamento que outros PVCs no namespace.

## Configure uma relação de replicação

A configuração de uma relação de replicação envolve o seguinte:

- Escolhendo com que frequência você deseja que o Astra Control tire um snapshot de aplicativo (que inclui os recursos do Kubernetes da aplicação, bem como os snapshots de volume de cada um dos volumes da aplicação)
- Escolha do cronograma de replicação (incluindo recursos do Kubernetes e dados de volume persistente)
- Definir o tempo para a captura instantânea

**Passos**

1. Na navegação à esquerda do Astra Control, selecione **Applications**.
2. Selecione a guia **proteção de dados** > **replicação**.
3. Selecione **Configurar política de replicação**. Ou, na caixa proteção do aplicativo, selecione a opção ações e selecione **Configurar política de replicação**.
4. Introduza ou selecione as seguintes informações:
   - **Cluster de destino**: Insira um cluster de destino (pode ser o mesmo que o cluster de origem).
   - **Classe de armazenamento de destino**: Selecione ou insira a classe de armazenamento que usa o SVM com ponteiro no cluster ONTAP de destino. Como prática recomendada, a classe de armazenamento de destino deve apontar para um back-end de storage diferente da classe de armazenamento de origem.
   - **Replication type**: `Asynchronous` É atualmente o único tipo de replicação disponível.
   - * Namespace de destino*: Insira namespaces de destino novos ou existentes para o cluster de destino.
   - (Opcional) Adicione namespaces adicionais selecionando **Add namespace** e escolhendo o namespace na lista suspensa.
   - **Frequência de replicação**: Defina com que frequência deseja que o Astra Control faça um snapshot e replique-o para o destino.
   - **Offset**: Defina o número de minutos a partir do topo da hora em que deseja que o Astra Control faça uma captura instantânea. Você pode querer usar um deslocamento para que ele não coincida com outras operações agendadas.

     Offset programações de backup e replicação para evitar sobreposições de agendamento. Por exemplo, execute backups no topo da hora a cada hora e programe a replicação para começar com um deslocamento de 5 minutos e um intervalo de 10 minutos.

5. Selecione **seguinte**, reveja o resumo e selecione **Guardar**.

   No início, o status exibe "APP-mirror" antes que a primeira programação ocorra.

O Astra Control cria um snapshot de aplicação usado para replicação.

6. Para ver o status do instantâneo do aplicativo, selecione a guia **aplicativos** > **instantâneos**.

   O nome do instantâneo usa o formato `replication-schedule-<string>` do . O Astra Control retém o último snapshot usado para replicação. Quaisquer instantâneos de replicação mais antigos são excluídos após a conclusão bem-sucedida da replicação.

**Resultado**

Isso cria a relação de replicação.

O Astra Control conclui as seguintes ações como resultado do estabelecimento do relacionamento:

- Cria um namespace no destino (se ele não existir)
- Cria um PVC no namespace de destino correspondente aos PVCs do aplicativo de origem.
- Obtém um snapshot inicial consistente com o aplicativo.
- Estabelece a relação do SnapMirror para volumes persistentes usando o snapshot inicial.

A página **proteção de dados** mostra o estado e o estado da relação de replicação: <Health status> | estado do ciclo de vida da relação>

Por exemplo: Normal | estabelecido

Saiba mais sobre os estados de replicação e o status no final deste tópico.

## Colocar um aplicativo replicado on-line no cluster de destino (failover)

Com o Astra Control, você pode fazer failover de aplicações replicadas para um cluster de destino. Este procedimento interrompe a relação de replicação e coloca a aplicação online no cluster de destino. Este procedimento não pára a aplicação no cluster de origem se estiver operacional.

**Passos**

1. Na navegação à esquerda do Astra Control, selecione **Applications**.
2. Selecione a guia **proteção de dados** > **replicação**.
3. No menu ações, selecione **failover**.
4. Na página failover, revise as informações e selecione **failover**.

**Resultado**

As seguintes ações ocorrem como resultado do procedimento de failover:

- O aplicativo de destino é iniciado com base no instantâneo replicado mais recente.
- O cluster de origem e a aplicação (se operacional) não são interrompidos e continuarão a ser executados.
- O estado de replicação muda para "failover" e, em seguida, para "failover" quando ele for concluído.
- A política de proteção do aplicativo de origem é copiada para o aplicativo de destino com base nas programações presentes no aplicativo de origem no momento do failover.
- Se o aplicativo de origem tiver um ou mais ganchos de execução pós-restauração ativados, esses ganchos de execução serão executados para o aplicativo de destino.
- O Astra Control mostra a aplicação nos clusters de origem e destino e sua respetiva integridade.

## Ressincronizar uma falha na replicação

A operação ressincronizada restabelece a relação de replicação. Você pode escolher a origem da relação para reter os dados no cluster de origem ou destino. Esta operação restabelece as relações SnapMirror para iniciar a replicação de volume na direção da escolha.

O processo pára o aplicativo no novo cluster de destino antes de restabelecer a replicação.

Durante o processo de ressincronização, o estado do ciclo de vida mostra como "estabelecendo".

**Passos**

1. Na navegação à esquerda do Astra Control, selecione **Applications**.
2. Selecione a guia **proteção de dados** > **replicação**.
3. No menu ações, selecione **Resync**.
4. Na página Resync, selecione a instância do aplicativo de origem ou destino que contém os dados que você deseja preservar.

   Escolha a fonte ressincronizada cuidadosamente, pois os dados no destino serão sobrescritos.

5. Selecione **Resync** para continuar.
6. Digite "ressync" para confirmar.
7. Selecione **Sim, ressincronizar** para concluir.

**Resultado**

- A página replicação mostra "estabelecer" como o status da replicação.
- O Astra Control interrompe a aplicação no novo cluster de destino.
- O Astra Control restabelece a replicação de volume persistente na direção selecionada usando o SnapMirror Resync.
- A página replicação mostra a relação atualizada.

## Replicação reversa da aplicação

Esta é a operação planejada para mover o aplicativo para o back-end de storage de destino e continuar replicando de volta para o back-end de storage de origem original. O Astra Control interrompe a aplicação de origem e replica os dados para o destino antes de fazer failover para a aplicação de destino.

Nesta situação, você está trocando a origem e o destino.

**Passos**

1. Na navegação à esquerda do Astra Control, selecione **Applications**.
2. Selecione a guia **proteção de dados** > **replicação**.
3. No menu ações, selecione **Reverse replication**.
4. Na página Reverse Replication (Reverse Replication), reveja as informações e selecione **Reverse replication** (Reverse replication) para continuar.

**Resultado**

As seguintes ações ocorrem como resultado da replicação reversa:

- Um snapshot é obtido dos recursos do Kubernetes do aplicativo de origem original.
- Os pods do aplicativo de origem original são interrompidos graciosamente ao excluir os recursos do Kubernetes do aplicativo (deixando PVCs e PVS no lugar).
- Depois que os pods são desativados, snapshots dos volumes do aplicativo são feitos e replicados.
- As relações do SnapMirror são quebradas, tornando os volumes de destino prontos para leitura/gravação.
- Os recursos do Kubernetes do aplicativo são restaurados a partir do snapshot de pré-encerramento, usando os dados de volume replicados após o desligamento do aplicativo de origem original.
- A replicação é restabelecida na direção inversa.

## Falha de aplicativos para o cluster de origem original

Com o Astra Control, você pode obter "failback" após uma operação de failover usando a seguinte sequência de operações. Nesse fluxo de trabalho para restaurar a direção de replicação original, o Astra Control replica (ressincrones) qualquer aplicação muda de volta para a aplicação de origem original antes de reverter a direção de replicação.

Esse processo começa a partir de um relacionamento que concluiu um failover para um destino e envolve as seguintes etapas:

- Comece com um estado com falha em excesso.
- Ressincronizar o relacionamento.
- Inverta a replicação.

**Passos**

1. Na navegação à esquerda do Astra Control, selecione **Applications**.
2. Selecione a guia **proteção de dados** > **replicação**.
3. No menu ações, selecione **Resync**.
4. Para uma operação de failback, escolha o aplicativo failover com falha como a origem da operação ressincronizada (preservando qualquer failover pós-escrito de dados).
5. Digite "ressync" para confirmar.
6. Selecione **Sim, ressincronizar** para concluir.
7. Após a conclusão da ressincronização, na guia proteção de dados > replicação, no menu ações, selecione **Reverse replication**.
8. Na página Reverse Replication (Reverse Replication), reveja as informações e selecione **Reverse replication**.

**Resultado**

Isso combina os resultados das operações "ressincronização" e "relação reversa" para colocar o aplicativo on-line no cluster de origem original com replicação retomada para o cluster de destino original.

## Excluir uma relação de replicação de aplicativos

A exclusão do relacionamento resulta em dois aplicativos separados sem relação entre eles.

**Passos**

1. Na navegação à esquerda do Astra Control, selecione **Applications**.
2. Selecione a guia **proteção de dados** > **replicação**.
3. Na caixa proteção do aplicativo ou no diagrama de relacionamento, selecione **Excluir relação de replicação**.

**Resultado**

As seguintes ações ocorrem como resultado da exclusão de uma relação de replicação:

- Se o relacionamento for estabelecido, mas o aplicativo ainda não tiver sido colocado on-line no cluster de destino (failover), o Astra Control manterá os PVCs criados durante a inicialização, deixará um aplicativo gerenciado "vazio" no cluster de destino e manterá o aplicativo de destino para manter todos os backups que possam ter sido criados.
- Se o aplicativo for colocado on-line no cluster de destino (failover), o Astra Control manterá PVCs e aplicativos de destino. Os aplicativos de origem e destino agora são tratados como aplicativos independentes. As programações de backup permanecem em ambos os aplicativos, mas não estão associadas umas às outras.

## Estado de integridade da relação de replicação e estados do ciclo de vida da relação

Astra Control exibe a integridade do relacionamento e os estados do ciclo de vida da relação de replicação.

### Estados de integridade da relação de replicação

Os seguintes Estados indicam a integridade da relação de replicação:

- **Normal**: O relacionamento está estabelecendo ou estabeleceu, e o snapshot mais recente foi transferido com sucesso.
- **Aviso**: O relacionamento está falhando ou falhou (e, portanto, não está mais protegendo o aplicativo de origem).
- **Crítica**
  - A relação está estabelecendo ou falhou e a última tentativa de reconciliar falhou.
  - A relação é estabelecida, e a última tentativa de reconciliar a adição de um novo PVC está falhando.
  - A relação é estabelecida (para que um snapshot bem-sucedido seja replicado e o failover seja possível), mas o snapshot mais recente falhou ou não conseguiu replicar.

### estados do ciclo de vida da replicação

Os seguintes estados refletem as diferentes fases do ciclo de vida de replicação:

- * Estabelecimento*: Uma nova relação de replicação está sendo criada. O Astra Control cria um namespace, se necessário, cria declarações de volume persistentes (PVCs) em novos volumes no cluster de destino e cria relações SnapMirror. Esse status também pode indicar que a replicação está ressincronizando ou invertendo a replicação.
- **Estabelecido**: Existe uma relação de replicação. O Astra Control verifica periodicamente se os PVCs estão disponíveis, verifica o relacionamento de replicação, cria periodicamente snapshots do aplicativo e identifica quaisquer novos PVCs de origem no aplicativo. Nesse caso, o Astra Control cria os recursos para incluí-los na replicação.
- * Com falha*: O Astra Control quebra os relacionamentos do SnapMirror e restaura os recursos do

Kubernetes do aplicativo a partir do último snapshot do aplicativo replicado com sucesso.

- * Failover*: O Astra Control pára de replicar a partir do cluster de origem, usa o snapshot do aplicativo replicado mais recente (bem-sucedido) no destino e restaura os recursos do Kubernetes.
- **Ressincronização**: O Astra Control ressincroniza os novos dados na origem ressincronizada para o destino ressincronizado usando o SnapMirror Resync. Esta operação pode substituir alguns dos dados no destino com base na direção da sincronização. O Astra Control interrompe a execução da aplicação no namespace de destino e remove a aplicação Kubernetes. Durante o processo de ressincronização, o status mostra como "estabelecendo".
- **Reversing**: A é a operação planejada para mover o aplicativo para o cluster de destino, continuando a replicar de volta para o cluster de origem original. O Astra Control interrompe a aplicação no cluster de origem, replica os dados para o destino antes de fazer failover da aplicação para o cluster de destino. Durante a replicação reversa, o status é exibido como "estabelecendo".
- **Excluindo**:
  - Se a relação de replicação tiver sido estabelecida, mas ainda não tiver falha, o Astra Control removerá PVCs criados durante a replicação e excluirá o aplicativo gerenciado de destino.
  - Se a replicação já tiver falhado, o Astra Control manterá os PVCs e a aplicação de destino.

# Clonar e migrar aplicações

Você pode clonar um aplicativo existente para criar um aplicativo duplicado no mesmo cluster do Kubernetes ou em outro cluster. Quando o Astra Control clona uma aplicação, ele cria um clone de sua configuração de aplicação e storage persistente.

A clonagem pode ajudar se você precisar mover aplicações e storage de um cluster Kubernetes para outro. Por exemplo, você pode querer mover workloads por meio de um pipeline de CI/CD e entre namespaces do Kubernetes. Você pode usar a IU do Astra Control Center ou "API Astra Control" clonar e migrar aplicações.

**Antes de começar**

- **Verificar volumes de destino**: Se você clonar para uma classe de armazenamento diferente, verifique se a classe de armazenamento usa o mesmo modo de acesso de volume persistente (por exemplo, ReadWriteMany). A operação de clone falhará se o modo de acesso ao volume persistente de destino for diferente. Por exemplo, se o volume persistente de origem usar o modo de acesso RWX, selecionar uma classe de armazenamento de destino que não seja capaz de fornecer RWX, como discos gerenciados do Azure, AWS EBS, Google Persistent Disk ou `ontap-san`, fará com que a operação de clone falhe. Para obter mais informações sobre os modos de acesso de volume persistente, consulte "Kubernetes" a documentação.
- Para clonar aplicativos para um cluster diferente, você precisa garantir que as instâncias de nuvem que contêm os clusters de origem e destino (se não forem os mesmos) tenham um bucket padrão. Você precisará atribuir um bucket padrão para cada instância da nuvem.
- Durante as operações de clone, os aplicativos que precisam de um recurso do IngressClass ou webhooks para funcionar corretamente não devem ter esses recursos já definidos no cluster de destino.

Durante a clonagem de aplicativos em ambientes OpenShift, o Astra Control Center precisa permitir que o OpenShift monte volumes e altere a propriedade dos arquivos. Por causa disso, você precisa configurar uma política de exportação de volume ONTAP para permitir essas operações. Você pode fazer isso com os seguintes comandos:

1. `export-policy rule modify -vserver <storage virtual machine name> -policyname <policy name> -ruleindex 1 -superuser sys`
2. `export-policy rule modify -vserver <storage virtual machine name> -policyname <policy name> -ruleindex 1 -anon 65534`

**Limitações de clone**

- **Classes de armazenamento explícitas**: Se você implantar um aplicativo com uma classe de armazenamento explicitamente definida e precisar clonar o aplicativo, o cluster de destino deverá ter a classe de armazenamento especificada originalmente. Clonar um aplicativo com uma classe de storage definida explicitamente para um cluster que não tenha a mesma classe de storage falhará.
- **Aplicativos suportados pelo ONTAP-nas-Economy**: Você não pode usar operações de clonagem se a classe de armazenamento do aplicativo for apoiada pelo `ontap-nas-economy` driver. Você pode, no entanto"habilite o backup e a restauração de operações de economia de ONTAP nas", .
- **Clones e restrições de usuário**: Qualquer usuário membro com restrições de namespace por nome/ID de namespace ou por rótulos de namespace pode clonar ou restaurar um aplicativo para um novo namespace no mesmo cluster ou para qualquer outro cluster na conta de sua organização. No entanto, o mesmo usuário não pode acessar o aplicativo clonado ou restaurado no novo namespace. Após uma operação de clone ou restauração criar um novo namespace, o administrador/proprietário da conta pode editar a conta de usuário membro e atualizar as restrições de função para o usuário afetado conceder acesso ao novo namespace.
- **Os clones usam buckets padrão**: Durante um backup do aplicativo ou restauração do aplicativo, você pode especificar opcionalmente um ID de bucket. Uma operação de clone de aplicativo, no entanto, sempre usa o bucket padrão que foi definido. Não há opção de alterar buckets para um clone. Se você quiser controlar qual balde é usado, você pode "altere o intervalo padrão"ou fazer um "backup" seguido por um "restaurar" separadamente.
- **Com o Jenkins CI**: Se você clonar uma instância implantada pelo operador do Jenkins CI, precisará restaurar manualmente os dados persistentes. Esta é uma limitação do modelo de implantação do aplicativo.
- **Com buckets do S3**: Os buckets do S3 no Astra Control Center não relatam a capacidade disponível. Antes de fazer backup ou clonar aplicativos gerenciados pelo Astra Control Center, verifique as informações do bucket no sistema de gerenciamento ONTAP ou StorageGRID.
- **Com uma versão específica do PostgreSQL**: Os clones de aplicativos dentro do mesmo cluster falham consistentemente com o gráfico Bitnami PostgreSQL 11.5.0. Para clonar com sucesso, use uma versão anterior ou posterior do gráfico.

**Considerações sobre OpenShift**

- * Clusters e versões OpenShift*: Se você clonar um aplicativo entre clusters, os clusters de origem e destino devem ser a mesma distribuição do OpenShift. Por exemplo, se você clonar um aplicativo de um cluster OpenShift 4,7, use um cluster de destino que também é OpenShift 4,7.
- * Projetos e UIDs*: Quando você cria um projeto para hospedar um aplicativo em um cluster OpenShift, o projeto (ou namespace Kubernetes) recebe um UID SecurityContext. Para ativar o Astra Control Center para proteger seu aplicativo e mover o aplicativo para outro cluster ou projeto no OpenShift, você precisa adicionar políticas que permitam que o aplicativo seja executado como qualquer UID. Como exemplo, os seguintes comandos OpenShift CLI concedem as políticas apropriadas a um aplicativo WordPress.

```
oc new-project wordpress
oc adm policy add-scc-to-group anyuid system:serviceaccounts:wordpress
oc adm policy add-scc-to-user privileged -z default -n wordpress
```

**Passos**

1. Selecione **aplicações**.
2. Execute um dos seguintes procedimentos:
   - Selecione o menu Opções na coluna **ações** para o aplicativo desejado.
   - Selecione o nome da aplicação pretendida e selecione a lista pendente de estado no canto superior direito da página.
3. Selecione **Clone**.
4. Especifique detalhes para o clone:
   - Introduza um nome.
   - Escolha um cluster de destino para o clone.
   - Insira namespaces de destino para o clone. Cada namespace de origem associado ao aplicativo mapeia para o namespace de destino que você define.

     O Astra Control cria novos namespaces de destino como parte da operação clone. Namespaces de destino que você especificar não devem estar presentes no cluster de destino.

   - Selecione **seguinte**.
   - Escolha manter a classe de armazenamento original associada ao aplicativo ou selecionar uma classe de armazenamento diferente.

     Você pode migrar a classe de armazenamento de um aplicativo para uma classe de armazenamento de provedor de nuvem nativa ou outra classe de armazenamento suportada, migrar um aplicativo de uma classe de armazenamento suportada por `ontap-nas-economy` para uma classe de armazenamento suportada pelo `ontap-nas` mesmo cluster ou copiar o aplicativo para outro cluster com uma classe de armazenamento suportada `ontap-nas-economy` pelo driver.

   Se você selecionar uma classe de armazenamento diferente e essa classe de armazenamento não existir no momento da restauração, um erro será retornado.

5. Selecione **seguinte**.
6. Reveja as informações sobre o clone e selecione **Clone**.

**Resultado**

O Astra Control clona a aplicação com base nas informações fornecidas por você. A operação de clone é bem-sucedida quando o novo clone de aplicativo está `Healthy` no estado na página **aplicativos**.

Após uma operação de clone ou restauração criar um novo namespace, o administrador/proprietário da conta pode editar a conta de usuário membro e atualizar as restrições de função para o usuário afetado conceder acesso ao novo namespace.

Após uma operação de proteção de dados (clone, backup ou restauração) e subsequente redimensionamento persistente de volume, há até vinte minutos de atraso antes que o novo tamanho de volume seja exibido na IU. A operação de proteção de dados é bem-sucedida em minutos. Você pode usar o software de gerenciamento do back-end de storage para confirmar a alteração no tamanho do volume.

# Gerenciar ganchos de execução de aplicativos

Um gancho de execução é uma ação personalizada que você pode configurar para ser executada em conjunto com uma operação de proteção de dados de um aplicativo gerenciado. Por exemplo, se você tiver um aplicativo de banco de dados, poderá usar um gancho de execução para pausar todas as transações de banco de dados antes de um snapshot e retomar as transações após a conclusão do snapshot. Isso garante snapshots consistentes com aplicativos.

## Tipos de ganchos de execução

O Astra Control Center dá suporte aos seguintes tipos de ganchos de execução, com base em quando eles podem ser executados:

- Pré-instantâneo
- Pós-snapshot
- Pré-backup
- Pós-backup
- Pós-restauração
- Pós-failover

## Filtros de gancho de execução

Quando você adiciona ou edita um gancho de execução a um aplicativo, você pode adicionar filtros a um gancho de execução para gerenciar quais contentores o gancho corresponderá. Os filtros são úteis para aplicativos que usam a mesma imagem de contentor em todos os contentores, mas podem usar cada imagem para um propósito diferente (como o Elasticsearch). Os filtros permitem criar cenários onde os ganchos de execução são executados em alguns, mas não necessariamente em todos os contentores idênticos. Se você criar vários filtros para um único gancho de execução, eles serão combinados com um operador LÓGICO E. Você pode ter até 10 filtros ativos por gancho de execução.

Cada filtro que você adicionar a um gancho de execução usa uma expressão regular para corresponder a containers em seu cluster. Quando um gancho corresponde a um recipiente, o gancho executará o script associado nesse recipiente. As expressões regulares para filtros usam a sintaxe da expressão regular 2 (RE2), que não suporta a criação de um filtro que exclui contentores da lista de correspondências. Para obter informações sobre a sintaxe que o Astra Control suporta para expressões regulares em filtros de gancho de execução, "Suporte à sintaxe da expressão regular 2 (RE2)" consulte .

Se você adicionar um filtro de namespace a um gancho de execução que é executado após uma operação de restauração ou clone e a origem e destino de restauração ou clone estiverem em namespaces diferentes, o filtro de namespace será aplicado somente ao namespace de destino.

## Notas importantes sobre ganchos de execução personalizados

Considere o seguinte ao Planejar ganchos de execução para seus aplicativos.

> Como os ganchos de execução geralmente reduzem ou desativam completamente a funcionalidade do aplicativo em que estão sendo executados, você deve sempre tentar minimizar o tempo que seus ganchos de execução personalizados demoram para serem executados. Se você iniciar uma operação de backup ou snapshot com ganchos de execução associados, mas depois cancelá-la, os ganchos ainda poderão ser executados se a operação de backup ou snapshot já tiver começado. Isso significa que a lógica usada em um gancho de execução pós-backup não pode assumir que o backup foi concluído.

- O recurso ganchos de execução é desativado por padrão para novas implantações do Astra Control.
  - Você precisa ativar o recurso de ganchos de execução antes de usar ganchos de execução.
  - Os usuários proprietários ou administradores podem ativar ou desativar o recurso ganchos de execução para todos os usuários definidos na conta atual do Astra Control. Ative o recurso ganchos de execuçãoConsulte e Desative o recurso ganchos de execução para obter instruções.
  - O status de capacitação do recurso é preservado durante as atualizações do Astra Control.
- Um gancho de execução deve usar um script para executar ações. Muitos ganchos de execução podem referenciar o mesmo script.
- O Astra Control requer que os scripts que os ganchos de execução usam sejam escritos no formato de scripts shell executáveis.
- O tamanho do script está limitado a 96kbMB.
- O Astra Control usa configurações de gancho de execução e quaisquer critérios correspondentes para determinar quais ganchos são aplicáveis a uma operação de snapshot, backup ou restauração.
- Todas as falhas no gancho de execução são falhas suaves; outros ganchos e a operação de proteção de dados ainda são tentados, mesmo que um gancho falhe. No entanto, quando um gancho falha, um evento de aviso é registrado no log de eventos da página **atividade**.
- Para criar, editar ou excluir ganchos de execução, você deve ser um usuário com permissões de proprietário, administrador ou membro.
- Se um gancho de execução demorar mais de 25 minutos para ser executado, o gancho falhará, criando uma entrada de log de eventos com um código de retorno de "N/A". Qualquer instantâneo afetado expira e será marcado como falhou, com uma entrada de log de eventos resultante anotando o tempo limite.
- Para operações de proteção de dados sob demanda, todos os eventos de gancho são gerados e salvos no log de eventos da página **atividade**. No entanto, para operações agendadas de proteção de dados, apenas eventos de falha de gancho são registrados no log de eventos (eventos gerados pelas próprias operações de proteção de dados agendadas ainda são registrados).
- Se o Astra Control Center falhar em um aplicativo de origem replicado para o aplicativo de destino, todos os ganchos de execução pós-failover habilitados para o aplicativo de origem serão executados para o aplicativo de destino após a conclusão do failover.

> Se você tiver executado ganchos pós-restauração com Astra Control Center 23,04 e atualizado seu Astra Control Center para 23,07 ou posterior, os ganchos de execução pós-restauração não serão mais executados após uma replicação de failover. Você precisa criar novos ganchos de execução pós-failover para seus aplicativos. Alternativamente, você pode alterar o tipo de operação de ganchos pós-restauração existentes destinados a failovers de "pós-restauração" para "pós-failover".

### Ordem de execução

Quando uma operação de proteção de dados é executada, os eventos de gancho de execução ocorrem na seguinte ordem:

1. Todos os ganchos de execução personalizados de pré-operação aplicáveis são executados nos contentores apropriados. Você pode criar e executar quantos ganchos de pré-operação personalizados você precisar, mas a ordem de execução desses ganchos antes da operação não é garantida nem configurável.
2. A operação de proteção de dados é realizada.
3. Todos os ganchos de execução pós-operação personalizados aplicáveis são executados nos contentores apropriados. Você pode criar e executar quantos ganchos de pós-operação personalizados você precisar, mas a ordem de execução desses ganchos após a operação não é garantida nem configurável.

Se você criar vários ganchos de execução do mesmo tipo (por exemplo, pré-snapshot), a ordem de execução desses ganchos não será garantida. No entanto, a ordem de execução de ganchos de diferentes tipos é garantida. Por exemplo, a ordem de execução de uma configuração que tenha todos os tipos diferentes de ganchos seria assim:

1. Ganchos pré-backup executados
2. Ganchos pré-instantâneos executados
3. Ganchos pós-snapshot executados
4. Ganchos pós-backup executados
5. Ganchos pós-restauração executados

Você pode ver um exemplo dessa configuração no cenário número 2 da tabela em Determine se um gancho vai funcionar.

> Você deve sempre testar seus scripts de gancho de execução antes de habilitá-los em um ambiente de produção. Você pode usar o comando 'kubectl exec' para testar convenientemente os scripts. Depois de habilitar os ganchos de execução em um ambiente de produção, teste os snapshots e backups resultantes para garantir que eles sejam consistentes. Você pode fazer isso clonando o aplicativo para um namespace temporário, restaurando o snapshot ou o backup e testando o aplicativo.

### Determine se um gancho vai funcionar

Use a tabela a seguir para ajudar a determinar se um gancho de execução personalizado será executado para seu aplicativo.

Observe que todas as operações de aplicativos de alto nível consistem em executar uma das operações básicas de snapshot, backup ou restauração. Dependendo do cenário, uma operação de clone pode consistir em várias combinações dessas operações, portanto, o que os ganchos de execução executados por uma operação de clone variará.

As operações de restauração no local exigem um snapshot ou backup existente, portanto, essas operações não executam snapshots ou ganchos de backup.

Se você iniciar, mas cancelar um backup que inclua um snapshot e houver ganchos de execução associados, alguns ganchos podem ser executados e outros podem não. Isso significa que um gancho de execução pós-backup não pode assumir que o backup foi concluído. Tenha em mente os seguintes pontos para backups cancelados com ganchos de execução associados:

- Os ganchos de pré-backup e pós-backup são sempre executados.
- Se o backup incluir um novo snapshot e o snapshot tiver iniciado, os ganchos pré-snapshot e pós-snapshot serão executados.
- Se o backup for cancelado antes do início do snapshot, os ganchos pré-snapshot e pós-snapshot não serão executados.

| Cenário | Operação | Snapshot existente | Backup existente | Namespace | Cluster | Os ganchos instantâneos funcionam | Ganchos de segurança executados | Restaurar os ganchos de funcionamento | Ganchos de failover executados |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Clone | N | N | Novo | O mesmo | Y | N | Y | N |
| 2 | Clone | N | N | Novo | Diferente | Y | Y | Y | N |
| 3 | Clone ou restauração | Y | N | Novo | O mesmo | N | N | Y | N |
| 4 | Clone ou restauração | N | Y | Novo | O mesmo | N | N | Y | N |
| 5 | Clone ou restauração | Y | N | Novo | Diferente | N | N | Y | N |
| 6 | Clone ou restauração | N | Y | Novo | Diferente | N | N | Y | N |
| 7 | Restaurar | Y | N | Existente | O mesmo | N | N | Y | N |
| 8 | Restaurar | N | Y | Existente | O mesmo | N | N | Y | N |
| 9 | Snapshot | N/A. | N/A. | N/A. | N/A. | Y | N/A. | N/A. | N |
| 10 | Backup | N | N/A. | N/A. | N/A. | Y | Y | N/A. | N |
| 11 | Backup | Y | N/A. | N/A. | N/A. | N | N | N/A. | N |
| 12 | Failover | Y | N/A. | Criado pela replicação | Diferente | N | N | N | Y |
| 13 | Failover | Y | N/A. | Criado pela replicação | O mesmo | N | N | N | Y |

## Exemplos de gancho de execução

Visite o "Projeto NetApp Verda GitHub" para baixar ganchos de execução reais para aplicativos populares, como Apache Cassandra e Elasticsearch. Você também pode ver exemplos e obter ideias para estruturar seus próprios ganchos de execução personalizados.

## Ative o recurso ganchos de execução

Se você é um usuário proprietário ou administrador, você pode ativar o recurso ganchos de execução. Quando você ativa o recurso, todos os usuários definidos nesta conta do Astra Control podem usar ganchos de execução e exibir ganchos de execução e scripts de gancho existentes.

**Passos**

1. Vá para **aplicativos** e selecione o nome de um aplicativo gerenciado.
2. Selecione a guia **ganchos de execução**.
3. Selecione **Ativar ganchos de execução**.

   A guia **Account** > **Feature settings** é exibida.
4. No painel **ganchos de execução**, selecione o menu de configurações.
5. Selecione **Ativar**.
6. Observe o aviso de segurança exibido.
7. Selecione **Sim, ative os ganchos de execução**.

## Desative o recurso ganchos de execução

Se você é um usuário proprietário ou administrador, você pode desativar o recurso ganchos de execução para todos os usuários definidos nesta conta Astra Control. Você deve excluir todos os ganchos de execução existentes antes de desativar o recurso ganchos de execução. Excluir um gancho de execuçãoConsulte para obter instruções sobre como excluir um gancho de execução existente.

**Passos**

1. Vá para **Account** e selecione a guia **Feature settings**.
2. Selecione a guia **ganchos de execução**.
3. No painel **ganchos de execução**, selecione o menu de configurações.
4. Selecione **Desativar**.
5. Observe o aviso que aparece.
6. Digite `disable` para confirmar que deseja desativar o recurso para todos os usuários.
7. Selecione **Sim, desativar**.

## Ver ganchos de execução existentes

Você pode exibir ganchos de execução personalizados existentes para um aplicativo.

**Passos**

1. Vá para **aplicativos** e selecione o nome de um aplicativo gerenciado.
2. Selecione a guia **ganchos de execução**.

Pode visualizar todos os ganchos de execução ativados ou desativados na lista resultante. Você pode ver o status de um gancho, quantos contentores ele corresponde, o tempo de criação e quando ele é executado (pré ou pós-operação). Você pode selecionar o + ícone ao lado do nome do gancho para expandir a lista de contentores em que ele será executado. Para ver os logs de eventos ao redor dos ganchos de execução para este aplicativo, vá para a guia **atividade**.

## Exibir scripts existentes

Você pode visualizar os scripts carregados existentes. Você também pode ver quais scripts estão em uso, e quais ganchos estão usando, nesta página.

**Passos**

1. Vá para **conta**.
2. Selecione a guia **Scripts**.

   Você pode ver uma lista de scripts carregados existentes nesta página. A coluna **usada por** mostra quais ganchos de execução estão usando cada script.

## Adicione um script

Cada gancho de execução deve usar um script para executar ações. Você pode adicionar um ou mais scripts que os ganchos de execução podem referenciar. Muitos ganchos de execução podem referenciar o mesmo script; isso permite que você atualize muitos ganchos de execução alterando apenas um script.

**Passos**

1. Certifique-se de que o recurso de ganchos de execução é ativado.
2. Vá para **conta**.
3. Selecione a guia **Scripts**.
4. Selecione **Adicionar**.
5. Execute um dos seguintes procedimentos:
   - Carregue um script personalizado.
     i. Selecione a opção **Upload file**.
     ii. Navegue até um arquivo e carregue-o.
     iii. Dê ao script um nome exclusivo.
     iv. (Opcional) Digite quaisquer notas que outros administradores devem saber sobre o script.
     v. Selecione **Salvar script**.
   - Cole em um script personalizado da área de transferência.
     i. Selecione a opção **Colar ou tipo**.
     ii. Selecione o campo de texto e cole o texto do script no campo.
     iii. Dê ao script um nome exclusivo.
     iv. (Opcional) Digite quaisquer notas que outros administradores devem saber sobre o script.
6. Selecione **Salvar script**.

**Resultado**

O novo script aparece na lista na guia **Scripts**.

## Excluir um script

Você pode remover um script do sistema se ele não for mais necessário e não for usado por nenhum hooks de execução.

**Passos**

1. Vá para **conta**.
2. Selecione a guia **Scripts**.
3. Escolha um script que você deseja remover e selecione o menu na coluna **ações**.
4. Selecione **Eliminar**.

> Se o script estiver associado a um ou mais ganchos de execução, a ação **Delete** não estará disponível. Para excluir o script, primeiro edite os ganchos de execução associados e associe-os a um script diferente.

## Crie um gancho de execução personalizado

Você pode criar um gancho de execução personalizado para um aplicativo e adicioná-lo ao Astra Control. Exemplos de gancho de execuçãoConsulte para obter exemplos de gancho. Você precisa ter permissões de proprietário, administrador ou membro para criar ganchos de execução.

> Quando você cria um script shell personalizado para usar como um gancho de execução, lembre-se de especificar o shell apropriado no início do arquivo, a menos que você esteja executando comandos específicos ou fornecendo o caminho completo para um executável.

**Passos**

1. Certifique-se de que o recurso de ganchos de execução é ativado.
2. Selecione **aplicativos** e, em seguida, selecione o nome de um aplicativo gerenciado.
3. Selecione a guia **ganchos de execução**.
4. Selecione **Adicionar**.
5. Na área **Detalhes do gancho**:
   a. Determine quando o gancho deve funcionar selecionando um tipo de operação no menu suspenso **operação**.
   b. Introduza um nome exclusivo para o gancho.
   c. (Opcional) Digite quaisquer argumentos para passar para o gancho durante a execução, pressionando a tecla Enter após cada argumento que você inserir para gravar cada um.
6. (Opcional) na área **Hook Filter Details** (Detalhes do filtro do gancho), você pode adicionar filtros para controlar em quais contentores o gancho de execução é executado:
   a. Selecione **Adicionar filtro**.
   b. Na coluna **tipo de filtro gancho**, escolha um atributo no qual filtrar no menu suspenso.
   c. Na coluna **Regex**, insira uma expressão regular para usar como filtro. O Astra Control usa o "Sintaxe regular expressão 2 (RE2) regex".

Se você filtrar o nome exato de um atributo (como um nome do pod) sem nenhum outro texto no campo de expressão regular, uma correspondência de subcadeia será executada. Para corresponder a um nome exato e apenas a esse nome, use a sintaxe exata de correspondência de cadeia de carateres (por exemplo, `^exact_podname$` ).

d. Para adicionar mais filtros, selecione **Adicionar filtro**.

Vários filtros para um gancho de execução são combinados com um operador LÓGICO E. Você pode ter até 10 filtros ativos por gancho de execução.

7. Quando terminar, selecione **seguinte**.
8. Na área **Script**, execute um dos seguintes procedimentos:
   - Adicione um novo script.
     i. Selecione **Adicionar**.
     ii. Execute um dos seguintes procedimentos:
       - Carregue um script personalizado.
         I. Selecione a opção **Upload file**.
         II. Navegue até um arquivo e carregue-o.
         III. Dê ao script um nome exclusivo.
         IV. (Opcional) Digite quaisquer notas que outros administradores devem saber sobre o script.
         V. Selecione **Salvar script**.
       - Cole em um script personalizado da área de transferência.
         I. Selecione a opção **Colar ou tipo**.
         II. Selecione o campo de texto e cole o texto do script no campo.
         III. Dê ao script um nome exclusivo.
         IV. (Opcional) Digite quaisquer notas que outros administradores devem saber sobre o script.
   - Selecione um script existente na lista.

     Isso instrui o gancho de execução a usar este script.
9. Selecione **seguinte**.
10. Reveja a configuração do gancho de execução.
11. Selecione **Adicionar**.

## Verifique o estado de um gancho de execução

Depois que uma operação de snapshot, backup ou restauração terminar de ser executada, você pode verificar o estado dos ganchos de execução executados como parte da operação. Você pode usar essas informações de status para determinar se deseja manter o gancho de execução, modificá-lo ou excluí-lo.

**Passos**

1. Selecione **aplicativos** e, em seguida, selecione o nome de um aplicativo gerenciado.
2. Selecione a guia **proteção de dados**.

3. Selecione **Snapshots** para ver os snapshots em execução ou **backups** para ver os backups em execução.

   O estado **Hook** mostra o status da execução do hook run após a conclusão da operação. Você pode passar o Mouse sobre o estado para obter mais detalhes. Por exemplo, se houver falhas de gancho de execução durante um instantâneo, passar o Mouse sobre o estado de gancho para esse instantâneo fornece uma lista de ganchos de execução com falha. Para ver os motivos de cada falha, você pode verificar a página **atividade** na área de navegação do lado esquerdo.

## Exibir o uso do script

Você pode ver quais ganchos de execução usam um script específico na IU da Web do Astra Control.

**Passos**

1. Selecione **conta**.
2. Selecione a guia **Scripts**.

   A coluna **usada por** na lista de scripts contém detalhes sobre os ganchos que estão usando cada script na lista.

3. Selecione as informações na coluna **usado por** para um script em que você está interessado.

   Uma lista mais detalhada é exibida, com os nomes de ganchos que estão usando o script e o tipo de operação com os quais eles estão configurados para executar.

## Edite um gancho de execução

Você pode editar um gancho de execução se quiser alterar seus atributos, filtros ou o script que ele usa. Você precisa ter permissões de proprietário, administrador ou membro para editar ganchos de execução.

**Passos**

1. Selecione **aplicativos** e, em seguida, selecione o nome de um aplicativo gerenciado.
2. Selecione a guia **ganchos de execução**.
3. Selecione o menu Opções na coluna **ações** para um gancho que você deseja editar.
4. Selecione **Editar**.
5. Faça as alterações necessárias, selecionando **Next** após concluir cada seção.
6. Selecione **Guardar**.

## Desativar um gancho de execução

Você pode desativar um gancho de execução se quiser impedir temporariamente que ele seja executado antes ou depois de um instantâneo de um aplicativo. Você precisa ter permissões de proprietário, Administrador ou Membro para desativar os ganchos de execução.

**Passos**

1. Selecione **aplicativos** e, em seguida, selecione o nome de um aplicativo gerenciado.
2. Selecione a guia **ganchos de execução**.
3. Selecione o menu Opções na coluna **ações** para um gancho que você deseja desativar.

4. Selecione **Desativar**.

## Excluir um gancho de execução

Você pode remover um gancho de execução inteiramente se você não precisar mais dele. Você precisa ter permissões de proprietário, administrador ou membro para excluir ganchos de execução.

**Passos**

1. Selecione **aplicativos** e, em seguida, selecione o nome de um aplicativo gerenciado.
2. Selecione a guia **ganchos de execução**.
3. Selecione o menu Opções na coluna **ações** para um gancho que você deseja excluir.
4. Selecione **Eliminar**.
5. Na caixa de diálogo resultante, digite "delete" para confirmar.
6. Selecione **Sim, excluir o gancho de execução**.

## Para mais informações

- "Projeto NetApp Verda GitHub"

# Proteger o Astra Control Center usando o Astra Control Center

Para garantir mais resiliência contra erros fatais no cluster do Kubernetes onde o Astra Control Center está sendo executado, proteja a própria aplicação Astra Control Center. Você pode fazer backup e restaurar o Astra Control Center usando uma instância secundária do Astra Control Center ou usar a replicação Astra se o storage subjacente estiver usando o ONTAP.

Nesses cenários, uma segunda instância do Astra Control Center é implantada e configurada em um domínio de falha diferente e executada em um segundo cluster Kubernetes diferente da instância primária do Astra Control Center. A segunda instância do Astra Control é usada para fazer backup e potencialmente restaurar a instância primária do Astra Control Center. Uma instância restaurada ou replicada do Astra Control Center continuará fornecendo gerenciamento de dados de aplicações para as aplicações de cluster de aplicações e restaurará a acessibilidade a backups e snapshots dessas aplicações.

**Antes de começar**

Antes de configurar cenários de proteção para o Astra Control Center, certifique-se de que você tenha o seguinte:

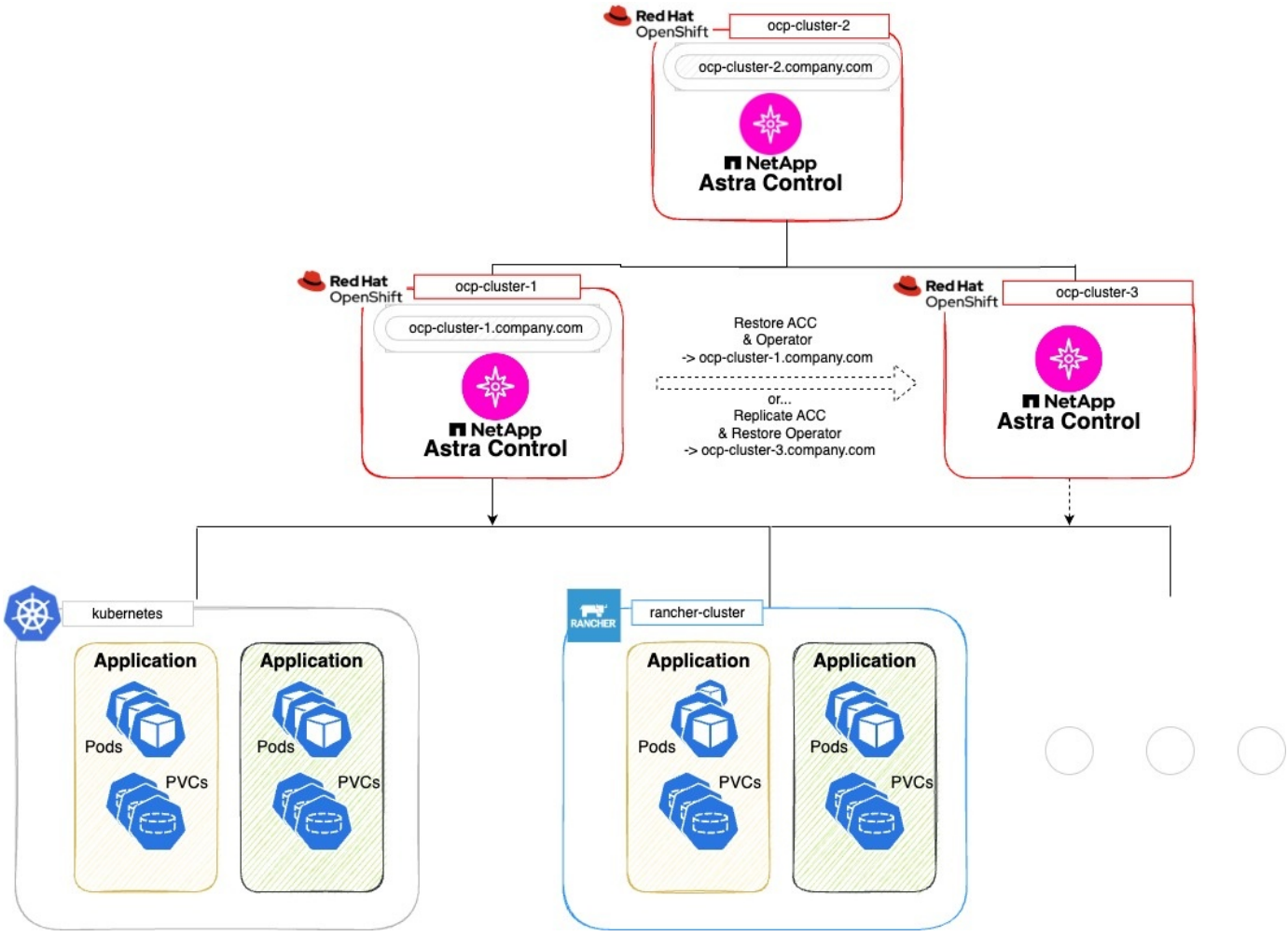
- **Um cluster Kubernetes executando a instância primária do Astra Control Center**: Esse cluster hospeda a instância primária do Astra Control Center que gerencia clusters de aplicações.
- **Um segundo cluster Kubernetes do mesmo tipo de distribuição Kubernetes que o primário que está executando a instância secundária Astra Control Center**: Esse cluster hospeda a instância Astra Control Center que gerencia a instância primária Astra Control Center.
- **Um terceiro cluster do Kubernetes com o mesmo tipo de distribuição do Kubernetes que o primário**: Esse cluster hospedará a instância restaurada ou replicada do Astra Control Center. Ele precisa ter o mesmo namespace Astra Control Center disponível que está implantado atualmente no primário. Por exemplo, se o Astra Control Center for implantado em namespace `netapp-acc` no cluster de origem, o

namespace `netapp-acc` precisará estar disponível e não usado por nenhuma aplicação no cluster do Kubernetes de destino.

- **Buckets compatíveis com S3**: Cada instância do Astra Control Center tem um bucket de armazenamento de objetos compatível com S3 acessível.
- **Um balanceador de carga configurado**: O balanceador de carga fornece um endereço IP para o Astra e deve ter conetividade de rede com os clusters de aplicativos e os buckets do S3.
- **Os clusters atendem aos requisitos do Astra Control Center**: Cada cluster usado na proteção do Astra Control Center atende "Requisitos gerais do Astra Control Center"ao .

**Sobre esta tarefa**

Esses procedimentos descrevem as etapas necessárias para restaurar o Astra Control Center para um novo cluster usando backup e restauraçãoou replicação. As etapas são baseadas no exemplo de configuração descrito aqui:




Neste exemplo de configuração, é apresentado o seguinte:

- **Um cluster Kubernetes executando a instância primária do Astra Control Center**:
  - Cluster OpenShift: `ocp-cluster-1`
  - Instância principal do Astra Control Center: `ocp-cluster-1.company.com`
  - Esse cluster gerencia os clusters de aplicações.

- **O segundo cluster do Kubernetes do mesmo tipo de distribuição do Kubernetes que o primário que está executando a instância secundária Astra Control Center**:
  - Cluster OpenShift: `ocp-cluster-2`
  - Instância secundária Astra Control Center: `ocp-cluster-2.company.com`
  - Esse cluster será usado para fazer backup da instância primária do Astra Control Center ou configurar a replicação para um cluster diferente (neste exemplo, o `ocp-cluster-3` cluster).
- **Um terceiro cluster do Kubernetes do mesmo tipo de distribuição do Kubernetes que o primário que será usado para operações de restauração**:
  - Cluster OpenShift: `ocp-cluster-3`
  - Terceira instância do Astra Control Center: `ocp-cluster-3.company.com`
  - Esse cluster será usado para restauração ou failover de replicação do Astra Control Center.

> Idealmente, o cluster de aplicativos deve estar situado fora dos três clusters do Astra Control Center, conforme descrito pelos clusters kureau e rancher na imagem acima.

Não representado no diagrama:

- Todos os clusters têm back-ends ONTAP com Astra Trident ou Astra Control Provisioner instalado.
- Nesta configuração, os clusters OpenShift estão usando o MetalLB como balanceador de carga.
- O controlador instantâneo e o VolumeSnapshotClass também são instalados em todos os clusters, conforme descrito no "pré-requisitos".

## Etapa 1 opção: Faça backup e restauração do Astra Control Center

Este procedimento descreve as etapas necessárias para restaurar o Astra Control Center para um novo cluster usando backup e restauração.

Neste exemplo, o Astra Control Center é sempre instalado sob `netapp-acc` o namespace e o operador é instalado sob `netapp-acc-operator` o namespace.

> Embora não seja descrito, o operador Astra Control Center também pode ser implantado no mesmo namespace que o Astra CR.

**Antes de começar**

- Você instalou o Astra Control Center primário em um cluster.
- Você instalou o Astra Control Center secundário em um cluster diferente.

**Passos**

1. Gerencie o cluster de aplicação e destino primário Astra Control Center a partir da instância secundária Astra Control Center (em execução `ocp-cluster-2` no cluster):
   a. Faça login na instância secundária do Astra Control Center.
   b. "Adicione o cluster primário Astra Control Center" (`ocp-cluster-1`).
   c. "Adicione o terceiro cluster de destino" (`ocp-cluster-3`) que será usado para a restauração.
2. Gerencie o Astra Control Center e o operador Astra Control Center no Astra Control Center secundário:

a. Na página aplicativos, selecione **Definir**.

b. Na janela **Definir aplicativo**, insira o novo nome da aplicação (`netapp-acc`).

c. Escolha o cluster que está executando o Astra Control Center primário (`ocp-cluster-1`) na lista suspensa **Cluster**.

d. Escolha `netapp-acc` o namespace para Astra Control Center na lista suspensa **namespace**.

e. Na página recursos de cluster, marque **incluir recursos adicionais com escopo de cluster**.

f. Selecione **Adicionar regra de inclusão**.

g. Selecione estas entradas e selecione **Adicionar**:

- Seletor de etiquetas: <label name>
- Grupo: Apipextensions.k8s.io
- Versão: V1
- Tipo: CustomResourceDefinição

h. Confirme as informações da aplicação.

i. Selecione **Definir**.

Depois de selecionar **define**, repita o processo de definir aplicativo para o operador `netapp-acc-operator`) e selecione o `netapp-acc-operator` namespace no assistente Definir aplicativo.

3. Faça backup do Astra Control Center e do operador:

a. No Astra Control Center secundário, navegue até a página aplicações selecionando a guia aplicações.

b. "Faça backup" A aplicação Astra Control Center (`netapp-acc`).

c. "Faça backup" o operador (`netapp-acc-operator`).

4. Depois de fazer backup do Astra Control Center e do operador, simule um cenário de recuperação de desastres (DR) a "Desinstalação do Astra Control Center" partir do cluster primário.

> Você restaurará o Astra Control Center para um novo cluster (o terceiro cluster Kubernetes descrito neste procedimento) e usará o mesmo DNS que o cluster primário para o Astra Control Center recém-instalado.

5. Usando o Astra Control Center secundário, "restaurar" a instância principal da aplicação Astra Control Center a partir do seu backup:

a. Selecione **aplicações** e, em seguida, selecione o nome da aplicação Astra Control Center.

b. No menu Opções na coluna ações, selecione **Restaurar**.

c. Escolha **Restaurar para novos namespaces** como o tipo de restauração.

d. Introduza o nome da restauração (`netapp-acc`).

e. Escolha o terceiro cluster de (`ocp-cluster-3`destino ).

f. Atualize o namespace de destino para que ele seja o mesmo namespace do original.

g. Na página Restaurar origem, selecione a cópia de segurança da aplicação que será utilizada como fonte de restauro.

h. Selecione **Restaurar usando classes de armazenamento originais**.

i. Selecione **Restaurar todos os recursos**.

j. Revise as informações de restauração e selecione **Restaurar** para iniciar o processo de restauração que restaura o Astra Control Center ao cluster de destino (`ocp-cluster-3`). A restauração é concluída quando o aplicativo entra `available` no estado.

6. Configurar o Astra Control Center no cluster de destino:

a. Abra um terminal e conete usando kubeconfig ao cluster de destino (`ocp-cluster-3`) que contém o Astra Control Center restaurado.

b. Confirme se a `ADDRESS` coluna na configuração do Astra Control Center faz referência ao nome DNS do sistema primário:

```
kubectl get acc -n netapp-acc
```

Resposta:

```
NAME  UUID                                   VERSION    ADDRESS
READY
astra 89f4fd47-0cf0-4c7a-a44e-43353dc96ba8 24.02.0-69 ocp-cluster-
1.company.com           True
```

a. Se o `ADDRESS` campo na resposta acima não tiver o FQDN da instância primária do Astra Control Center, atualize a configuração para fazer referência ao Astra Control Center DNS:

```
kubectl edit acc -n netapp-acc
```

i. Altere `astraAddress` o em `spec:` para FQDN (`ocp-cluster-1.company.com`neste exemplo) da instância primária do Astra Control Center.

ii. Salve a configuração.

iii. Confirme se o endereço foi atualizado:

```
kubectl get acc -n netapp-acc
```

b. Vá para a Restaure o Operador do Centro de Controle Astra seção deste documento para concluir o processo de restauração.

## Etapa 1 opção: Proteger o Astra Control Center usando a replicação

Este procedimento descreve as etapas necessárias para configurar "Replicação do Astra Control Center" para proteger a instância primária do Astra Control Center.

Neste exemplo, o Astra Control Center é sempre instalado sob `netapp-acc` o namespace e o operador é instalado sob `netapp-acc-operator` o namespace.

**Antes de começar**

- Você instalou o Astra Control Center primário em um cluster.

- Você instalou o Astra Control Center secundário em um cluster diferente.

**Passos**

1. Gerencie o cluster de destino e a aplicação Astra Control Center primário a partir da instância secundária Astra Control Center:
   a. Faça login na instância secundária do Astra Control Center.
   b. "Adicione o cluster primário Astra Control Center" (`ocp-cluster-1`).
   c. "Adicione o terceiro cluster de destino" (`ocp-cluster-3`) que será usado para a replicação.
2. Gerencie o Astra Control Center e o operador Astra Control Center no Astra Control Center secundário:
   a. Selecione **clusters** e selecione o cluster que contém o Astra Control Center primário (`ocp-cluster-1`).
   b. Selecione a guia **namespaces**.
   c. `netapp-acc`Selecione e `netapp-acc-operator` namespaces.
   d. Selecione o menu ações e selecione **Definir como aplicações**.
   e. Selecione **Exibir em aplicativos** para ver os aplicativos definidos.
3. Configurar backends para replicação:

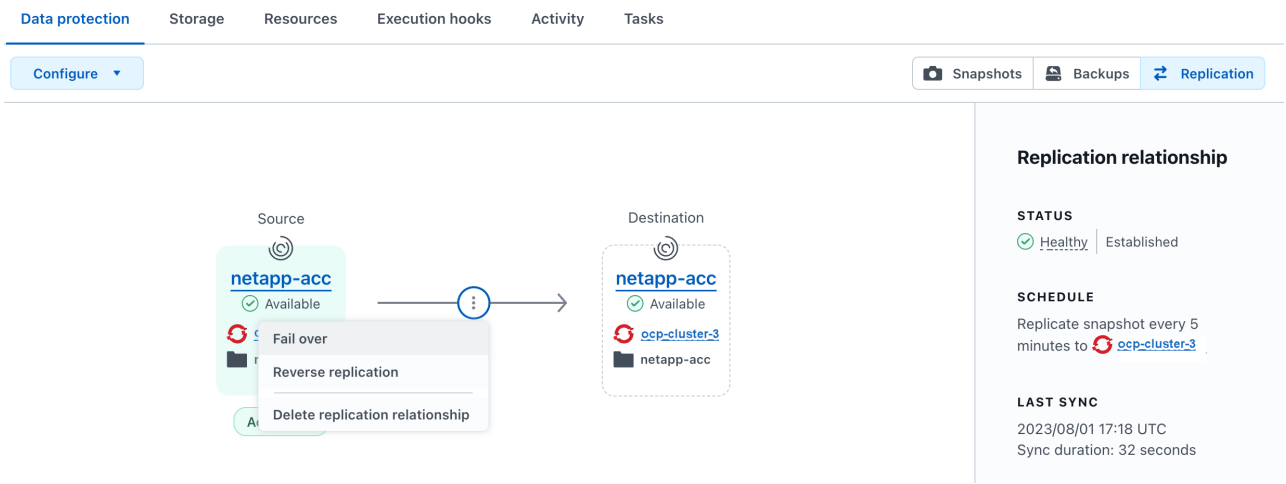
   A replicação requer que o cluster primário do Centro de Controle Astra e o cluster de (`ocp-cluster-3`destino ) usem diferentes back-ends de storage ONTAP com peering. Depois que cada back-end é peered e adicionado ao Astra Control, o back-end aparece na guia **descoberto** da página backends.

   a. "Adicione um back-end com peered" Para Astra Control Center no cluster primário.
   b. "Adicione um back-end com peered" Para Astra Control Center no cluster de destino.
4. Configurar replicação:
   a. No ecrã aplicações, selecione a `netapp-acc` aplicação.
   b. Selecione **Configurar política de replicação**.
   c. `ocp-cluster-3`Selecione como o cluster de destino.
   d. Selecione a classe de armazenamento.
   e. `netapp-acc`Insira como namespace de destino.
   f. Altere a frequência de replicação, se desejado.
   g. Selecione **seguinte**.
   h. Confirme se a configuração está correta e selecione **Guardar**.

      A relação de replicação passa de `Establishing` para `Established`. Quando ativa, essa replicação ocorrerá a cada cinco minutos até que a configuração de replicação seja excluída.
5. Faça failover da replicação para o outro cluster se o sistema primário estiver corrompido ou não estiver mais acessível:

   Certifique-se de que o cluster de destino não tenha o Astra Control Center instalado para garantir um failover bem-sucedido.

a. Selecione o ícone de elipses verticais e selecione **failover**.




b. Confirme os detalhes e selecione **failover** para iniciar o processo de failover.

   O status da relação de replicação muda para `Failing over` e depois `Failed over` quando concluído.

6. Conclua a configuração de failover:

   a. Abra um terminal e conete-se usando o kubeconfig do terceiro cluster (`ocp-cluster-3`). Agora, esse cluster tem o Astra Control Center instalado.

   b. Determine o FQDN do Centro de Controle Astra no terceiro (`ocp-cluster-3`cluster ).

   c. Atualize a configuração para fazer referência ao Astra Control Center DNS:

```
kubectl edit acc -n netapp-acc
```

      i. Altere `astraAddress` o em `spec:` com o FQDN (`ocp-cluster-3.company.com`) do terceiro cluster de destino.

      ii. Salve a configuração.

      iii. Confirme se o endereço foi atualizado:

```
kubectl get acc -n netapp-acc
```

   d. Confirme que todos os CRDs traefik necessários estão presentes:

```
kubectl get crds | grep traefik
```

   CRDS traefik necessário:

```
ingressroutes.traefik.containo.us
ingressroutes.traefik.io
ingressroutetcps.traefik.containo.us
ingressroutetcps.traefik.io
ingressrouteudps.traefik.containo.us
ingressrouteudps.traefik.io
middlewares.traefik.containo.us
middlewares.traefik.io
middlewaretcps.traefik.containo.us
middlewaretcps.traefik.io
serverstransports.traefik.containo.us
serverstransports.traefik.io
tlsoptions.traefik.containo.us
tlsoptions.traefik.io
tIsstores.traefik.containo.us
tIsstores.traefik.io
traefikservices.traefik.containo.us
traefikservices.traefik.io
```

a. Se algumas das CRDs acima estiverem ausentes:
   i. Vá para "documentação traefik".
   ii. Copie a área "Definições" em um arquivo.
   iii. Aplicar alterações:

```
kubectl apply -f <file name>
```

   iv. Reiniciar traefik:

```
kubectl get pods -n netapp-acc | grep -e "traefik" | awk '{print
$1}' | xargs kubectl delete pod -n netapp-acc
```

b. Vá para a Restaure o Operador do Centro de Controle Astra seção deste documento para concluir o processo de restauração.

## Etapa 2: Restaure o Operador do Centro de Controle Astra

Usando o Astra Control Center secundário, restaure o operador principal do Astra Control Center a partir do backup. O namespace de destino deve ser o mesmo que o namespace de origem. No caso em que o Astra Control Center foi excluído do cluster de origem principal, ainda haverá backups para executar as mesmas etapas de restauração.

**Passos**

1. Selecione **aplicativos** e, em seguida, selecione o nome do aplicativo operador (`netapp-acc-operator`).

2. No menu Opções na coluna ações, selecione **Restaurar**
3. Escolha **Restaurar para novos namespaces** como o tipo de restauração.
4. Escolha o terceiro cluster de (`ocp-cluster-3`destino ).
5. Altere o namespace para ser o mesmo que o namespace associado ao cluster de origem primária (`netapp-acc-operator`).
6. Selecione o backup que foi feito anteriormente como a origem de restauração.
7. Selecione **Restaurar usando classes de armazenamento originais**.
8. Selecione **Restaurar todos os recursos**.
9. Revise os detalhes e clique em **Restaurar** para iniciar o processo de restauração.

   A página aplicativos mostra o operador do Astra Control Center sendo restaurado para o terceiro cluster de destino (`ocp-cluster-3`). Quando o processo estiver concluído, o estado será exibido como `Available`. Dentro de dez minutos, o endereço DNS deve ser resolvido na página.

**Resultado**

O Astra Control Center, seus clusters registrados e aplicações gerenciadas com seus snapshots e backups agora estão disponíveis no terceiro cluster de destino (`ocp-cluster-3`). Quaisquer políticas de proteção que você tenha no original também estão presentes na nova instância. Você pode continuar fazendo backups e snapshots programados ou sob demanda.

## Solução de problemas

Determine a integridade do sistema e se os processos de proteção foram bem-sucedidos.

- **Os pods não estão em execução**: Confirme se todos os pods estão ativos e em execução:

  ```
  kubectl get pods -n netapp-acc
  ```

  Se alguns pods estiverem `CrashLookBackOff` no estado, reinicie-os e eles devem fazer a transição para `Running` o estado.

- **Confirmar status do sistema**: Confirme se o sistema Astra Control Center está `ready` no estado:

  ```
  kubectl get acc -n netapp-acc
  ```

  Resposta:

  ```
  NAME  UUID                                   VERSION    ADDRESS
  READY
  astra 89f4fd47-0cf0-4c7a-a44e-43353dc96ba8 24.02.0-69 ocp-cluster-
  1.company.com           True
  ```

- **Confirmar status de implantação**: Mostrar informações de implantação do Astra Control Center para confirmar que `Deployment State` é `Deployed`.

```
kubectl describe acc astra -n netapp-acc
```

- **A IU do Astra Control Center restaurada retorna um erro 404**: Se isso acontecer quando você selecionou `AccTraefik` como uma opção de entrada, verifique a CRDs traefik para garantir que todos estão instalados.

## Informações sobre direitos autorais



## Informações sobre marcas comerciais