Use o Astra Control Center

Astra Control Center

NetApp
August 11, 2025

Índice

Use o Astra Control Center

Comece a gerenciar aplicativos

Depois de "Adicionar um cluster ao gerenciamento do Astra Control"instalar aplicativos no cluster (fora do Astra Control) e, em seguida, vá para a página aplicações no Astra Control para definir as aplicações e seus recursos.

Você pode definir e gerenciar aplicativos que incluem recursos de storage com pods em execução ou aplicativos que incluem recursos de storage sem pods em execução. Os aplicativos que não têm pods em execução são conhecidos como aplicativos somente de dados.

Requisitos de gerenciamento de aplicativos

O Astra Control tem os seguintes requisitos de gerenciamento de aplicações:

- **Licenciamento**: Para gerenciar aplicações usando o Astra Control Center, você precisa da licença de avaliação do Astra Control Center incorporada ou de uma licença completa.
- **Namespaces**: Os aplicativos podem ser definidos em um ou mais namespaces especificados em um único cluster usando o Astra Control. Um aplicativo pode conter recursos que abrangem vários namespaces dentro do mesmo cluster. O Astra Control não dá suporte à capacidade de definir aplicações em vários clusters.
- **Storage class**: Se você instalar um aplicativo com uma classe de armazenamento explicitamente definida e precisar clonar o aplicativo, o cluster de destino para a operação clone deve 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.
- **Recursos do Kubernetes**: As aplicações que usam recursos do Kubernetes não coletados pelo Astra Control podem não ter recursos completos de gerenciamento de dados do aplicativo. O Astra Control coleta os seguintes recursos do Kubernetes:

`ClusterRole`	`ClusterRoleBinding`	`ConfigMap`
`CronJob`	`CustomResourceDefinition`	`CustomResource`
`DaemonSet`	`DeploymentConfig`	`HorizontalPodAutoscaler`
`Ingress`	`MutatingWebhook`	`NetworkPolicy`
`PersistentVolumeClaim`	`Pod`	`PodDisruptionBudget`
`PodTemplate`	`ReplicaSet`	`Role`
`RoleBinding`	`Route`	`Secret`
`Service`	`ServiceAccount`	`StatefulSet`
`ValidatingWebhook`		

Métodos de instalação de aplicativos suportados

O Astra Control é compatível com os seguintes métodos de instalação de aplicações:

- **Arquivo manifesto**: O Astra Control suporta aplicativos instalados a partir de um arquivo manifesto usando kubectl. Por exemplo:

```
kubectl apply -f myapp.yaml
```

- **Helm 3**: Se você usar o Helm para instalar aplicativos, o Astra Control requer o Helm versão 3. O gerenciamento e clonagem de aplicativos instalados com o Helm 3 (ou atualizados do Helm 2 para o Helm 3) é totalmente compatível. O gerenciamento de aplicativos instalados com o Helm 2 não é suportado.
- **Aplicativos implantados pelo operador**: O Astra Control suporta aplicativos instalados com operadores com escopo de namespace que são, em geral, projetados com uma arquitetura "pass-by-value" em vez de "pass-by-reference". Um operador e o aplicativo que ele instala devem usar o mesmo namespace; talvez seja necessário modificar o arquivo YAML de implantação para o operador para garantir que esse seja o caso.

  A seguir estão alguns aplicativos de operador que seguem estes padrões:

  - "Apache K8ssandra"

    > Para K8ssandra, são suportadas as operações de restauração no local. Uma operação de restauração para um novo namespace ou cluster requer que a instância original do aplicativo seja removida. Isto destina-se a garantir que as informações do grupo de pares transportadas não conduzam à comunicação entre instâncias. A clonagem da aplicação não é suportada.

  - "Jenkins CI"
  - "Cluster Percona XtraDB"

  O Astra Control pode não ser capaz de clonar um operador projetado com uma arquitetura "pass-by-reference" (por exemplo, o operador CockroachDB). Durante esses tipos de operações de clonagem, o operador clonado tenta consultar os segredos do Kubernetes do operador de origem, apesar de ter seu próprio novo segredo como parte do processo de clonagem. A operação de clone pode falhar porque o Astra Control não conhece os segredos do Kubernetes no operador de origem.

Instale aplicativos no cluster

Depois de "adicionado o cluster" acessar o Astra Control, você poderá instalar aplicações ou gerenciar aplicações existentes no cluster. Qualquer aplicativo com escopo para um ou mais namespaces pode ser gerenciado.

Definir aplicações

Depois que o Astra Control descobrir namespaces em seus clusters, você pode definir as aplicações que deseja gerenciar. Você pode escolher para gerencie um aplicativo abrangendo um ou mais namespaces ou gerencie um namespace inteiro como uma única aplicação. Tudo se resume ao nível de granularidade de que você precisa para operações de proteção de dados.

Embora o Astra Control permita que você gerencie separadamente ambos os níveis da hierarquia (o namespace e os aplicativos nesse namespace ou spanning Namespaces), a prática recomendada é escolher um ou outro. As ações que você executa no Astra Control podem falhar se as ações ocorrerem ao mesmo tempo no nível do namespace e da aplicação.

Como exemplo, você pode querer definir uma política de backup para "maria" que tenha uma cadência semanal, mas você pode precisar fazer backup do "mariadb" (que está no mesmo namespace) com mais frequência do que isso. Com base nessas necessidades, você precisaria gerenciar os aplicativos separadamente e não como um aplicativo de namespace único.

Antes de começar

- Um cluster de Kubernetes adicionado ao Astra Control.
- Um ou mais aplicativos instalados no cluster. Leia mais sobre os métodos de instalação de aplicativos suportados.
- Namespaces existentes no cluster do Kubernetes que você adicionou ao Astra Control.
- (Opcional) Um rótulo do Kubernetes em qualquer "Recursos do Kubernetes compatíveis".

Um rótulo é um par de chave/valor que você pode atribuir a objetos Kubernetes para identificação. Os rótulos facilitam a ordenação, organização e localização de objetos do Kubernetes. Para saber mais sobre rótulos do Kubernetes, "Consulte a documentação oficial do Kubernetes".

Sobre esta tarefa

- Antes de começar, você também deve entender "gerenciamento de namespaces padrão e do sistema".
- Se você planeja usar vários namespaces com suas aplicações no Astra Control, "modifique as funções do usuário com restrições de namespace" depois de atualizar para uma versão do Astra Control Center com suporte a vários namespace.
- Para obter instruções sobre como gerenciar aplicativos usando a API Astra Control, consulte o "Informações de API e automação do Astra".

Opções de gerenciamento de aplicativos

- Definir recursos para gerenciar como um aplicativo
- Defina um namespace para gerenciar como um aplicativo

Definir recursos para gerenciar como um aplicativo

Você pode especificar o "Recursos do Kubernetes que compõem uma aplicação" que deseja gerenciar com o Astra Control. A definição de um aplicativo permite agrupar elementos do cluster do Kubernetes em um único aplicativo. Essa coleção de recursos do Kubernetes é organizada por critérios de seleção de namespace e rótulo.

A definição de uma aplicação oferece controle mais granular sobre o que incluir em uma operação do Astra Control, incluindo clone, snapshot e backups.

Ao definir aplicativos, certifique-se de que você não inclua um recurso Kubernetes em vários aplicativos com políticas de proteção. A sobreposição de políticas de proteção em recursos do Kubernetes pode causar conflitos de dados. Leia mais em um exemplo.

Expanda para saber mais sobre como adicionar recursos com escopo de cluster aos namespaces do aplicativo.

É possível importar recursos de cluster associados aos recursos de namespace, além dos recursos do Astra Control incluídos automaticamente. Você pode adicionar uma regra que incluirá recursos de um grupo específico, tipo, versão e, opcionalmente, rótulo. Você pode querer fazer isso se houver recursos que o Astra Control não inclui automaticamente.

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

Você pode adicionar o seguinte `apiVersions` (que são os grupos combinados com a versão da API):

Tipo de recurso	ApiVersions (versão do grupo)
`ClusterRole`	rbac.authorization.k8s.io/v1
`ClusterRoleBinding`	rbac.authorization.k8s.io/v1
`CustomResource`	apipextensions.k8s.io/v1, apipextensions.k8s.io/v1beta1
`CustomResourceDefinition`	apipextensions.k8s.io/v1, apipextensions.k8s.io/v1beta1
`MutatingWebhookConfiguration`	admissionregistration.k8s.io/v1
`ValidatingWebhookConfiguration`	admissionregistration.k8s.io/v1

Passos

1. Na página aplicativos, selecione **Definir**.
2. Na janela **Definir aplicativo**, insira o nome do aplicativo.
3. Escolha o cluster no qual seu aplicativo está sendo executado na lista suspensa **Cluster**.
4. Escolha um namespace para sua aplicação na lista suspensa **namespace**.

> As aplicações podem ser definidas em um ou mais namespaces especificados em um único cluster usando o Astra Control. Um aplicativo pode conter recursos que abrangem vários namespaces dentro do mesmo cluster. O Astra Control não dá suporte à capacidade de definir aplicações em vários clusters.

5. (Opcional) Insira um rótulo para os recursos do Kubernetes em cada namespace. Você pode especificar um único rótulo ou critério de seleção de rótulo (consulta).

> Para saber mais sobre rótulos do Kubernetes, "Consulte a documentação oficial do Kubernetes".

6. (Opcional) Adicione namespaces adicionais para o aplicativo selecionando **Adicionar namespace** e escolhendo o namespace na lista suspensa.
7. (Opcional) Digite critérios de seleção de rótulo ou rótulo único para quaisquer namespaces adicionais que você adicionar.
8. (Opcional) para incluir recursos com escopo de cluster além daqueles que o Astra Control inclui

automaticamente, marque **incluir recursos adicionais com escopo de cluster** e conclua o seguinte:

a. Selecione **Adicionar regra de inclusão**.
b. **Group**: Na lista suspensa, selecione o grupo de recursos da API.
c. **Kind**: Na lista suspensa, selecione o nome do esquema do objeto.
d. **Versão**: Insira a versão da API.
e. * Seletor de etiquetas*: Opcionalmente, inclua um rótulo para adicionar à regra. Este rótulo é usado para recuperar apenas os recursos correspondentes a esse rótulo. Se você não fornecer um rótulo, o Astra Control coletará todas as instâncias do tipo de recurso especificado para esse cluster.
f. Revise a regra criada com base em suas entradas.
g. Selecione **Adicionar**.

> Você pode criar quantas regras de recursos com escopo de cluster quiser. As regras aparecem no Resumo da aplicação definida.

9. Selecione **Definir**.
10. Depois de selecionar **define**, repita o processo para outros aplicativos, conforme necessário.

Depois de concluir a definição de uma aplicação, a aplicação aparece `Healthy` no estado na lista de aplicações na página aplicações. Agora você pode cloná-lo e criar backups e snapshots.

> O aplicativo que você acabou de adicionar pode ter um ícone de aviso na coluna protegido, indicando que ele ainda não foi feito backup e ainda não está programado para backups.

> Para ver os detalhes de uma aplicação específica, selecione o nome da aplicação.

Para ver os recursos adicionados a este aplicativo, selecione a guia **recursos**. Selecione o número após o nome do recurso na coluna recurso ou insira o nome do recurso na Pesquisa para ver os recursos adicionais com escopo de cluster incluídos.

Defina um namespace para gerenciar como um aplicativo

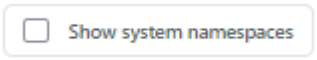
É possível adicionar todos os recursos do Kubernetes em um namespace ao gerenciamento do Astra Control definindo os recursos desse namespace como uma aplicação. Esse método é preferível à definição de aplicativos individualmente se você pretende gerenciar e proteger todos os recursos em um namespace específico de uma maneira semelhante e em intervalos comuns.

Passos

1. Na página clusters, selecione um cluster.
2. Selecione a guia **namespaces**.
3. Selecione o menu ações para o namespace que contém os recursos do aplicativo que você deseja gerenciar e selecione **Definir como aplicativo**.

> Se você quiser definir vários aplicativos, selecione na lista namespaces e selecione o botão **ações** no canto superior esquerdo e selecione **Definir como aplicativo**. Isso definirá vários aplicativos individuais em seus namespaces individuais. Para aplicações com vários namespace, Definir recursos para gerenciar como um aplicativoconsulte .

Marque a caixa de seleção **Mostrar namespaces do sistema** para revelar namespaces do sistema que geralmente não são usados no gerenciamento de aplicativos por padrão.



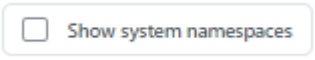
"Leia mais".

Após a conclusão do processo, os aplicativos associados ao namespace aparecem na `Associated applications` coluna.

E quanto aos namespaces do sistema?

O Astra Control também descobre namespaces do sistema em um cluster do Kubernetes. Nós não mostramos esses namespaces do sistema por padrão, porque é raro que você precise fazer backup dos recursos do aplicativo do sistema.

Você pode exibir namespaces do sistema na guia namespaces para um cluster selecionado selecionando a caixa de seleção **Mostrar namespaces do sistema**.



O Astra Control Center não é mostrado por padrão como uma aplicação que pode ser gerenciada, mas é possível fazer backup e restaurar uma instância do Astra Control Center usando outra instância do Astra Control Center.

Exemplo: Política de proteção separada para versões diferentes

Neste exemplo, a equipe de devops está gerenciando uma implantação de versão "canário". O cluster da equipe tem três pods executando o nginx. Dois dos pods são dedicados à liberação estável. O terceiro pod é para o lançamento canário.

O administrador do Kubernetes da equipe de devops adiciona o rótulo `deployment=stable` aos pods de versão estáveis. A equipe adiciona o rótulo `deployment=canary` ao pod de lançamento canário.

A versão estável da equipe inclui um requisito para instantâneos por hora e backups diários. O lançamento canário é mais efêmero, então eles querem criar uma política de proteção menos agressiva e de curto prazo para qualquer coisa rotulada . `deployment=canary`

Para evitar possíveis conflitos de dados, o administrador criará dois aplicativos: Um para a versão "canary" e outro para a versão "stable". Isso mantém os backups, snapshots e operações de clone separados para os dois grupos de objetos Kubernetes.

Encontre mais informações

- "Use a API Astra Control"
- "Desgerenciar um aplicativo"

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.

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.

Passos

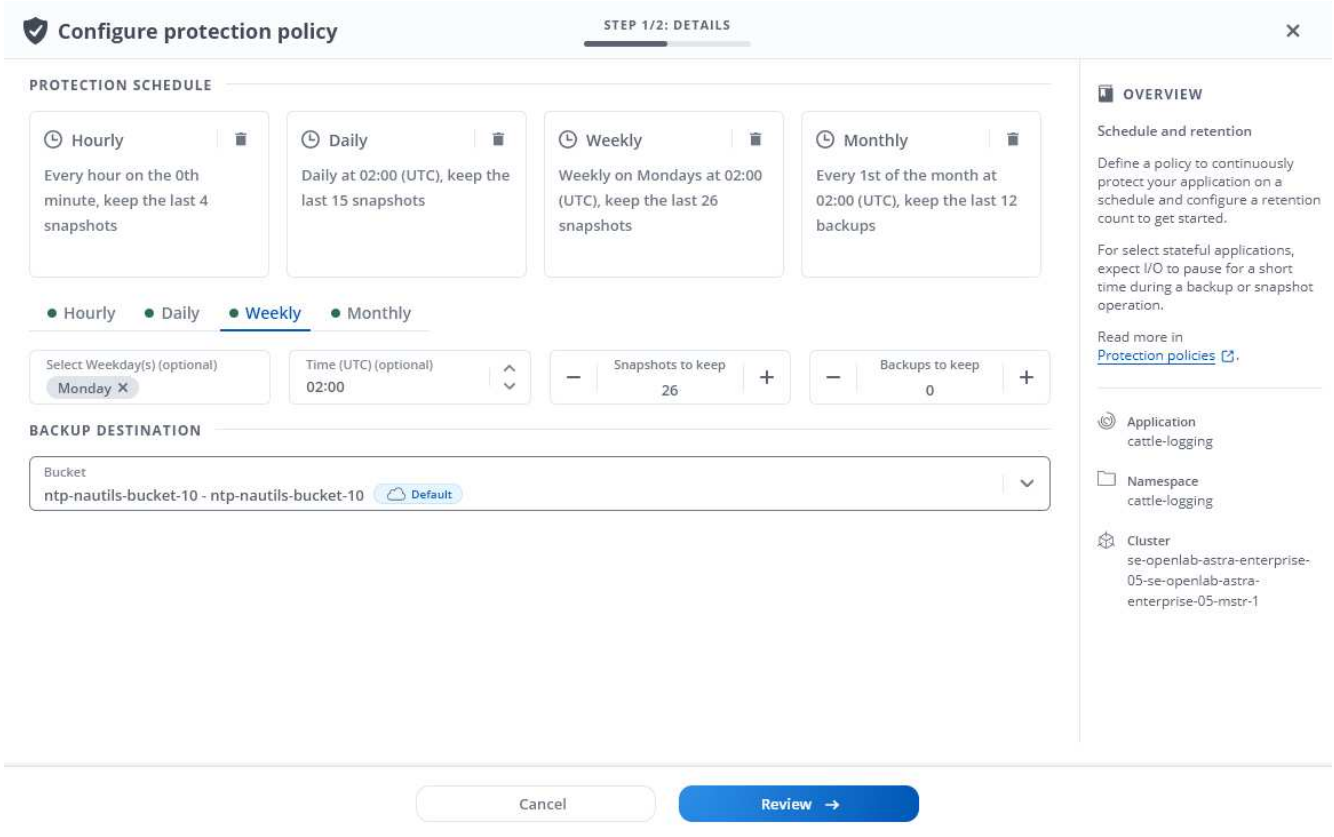
1. Selecione **aplicativos** e, em seguida, selecione o nome de um aplicativo.
2. Selecione **proteção de dados**.

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. Selecione **Revisão**.
6. Selecione **Definir política de proteção.**

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.

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. Reveja o resumo do instantâneo e selecione **Snapshot**.

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`

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

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.

Expanda para obter as etapas de configuração

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 Trident:

   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.

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 .

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**.

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 no local B para local B
- No local 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 Trident**: O Astra Trident versão 22,10 ou posterior deve existir nos clusters do 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 Trident e SVM**: Os SVMs remotas em peering precisam estar disponíveis para o Astra Trident no cluster de destino.

Astra Control Center

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

  somente divisioner: Adicionar e gerenciar back-ends de storage do ONTAP no Astra Control Center é opcional se você tiver ativado o Astra Control Provisioner para Astra Control Center 23,10 ou posterior.

- **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.

  Astra Control Provisioner Only: Se você ativou a funcionalidade Astra Control Provisioner, não será mais necessário definir especificamente uma função de "admin" para gerenciar clusters no Astra Control Center, já que essas credenciais não são mais necessárias no Astra Control Center.

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

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 ad hoc, 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

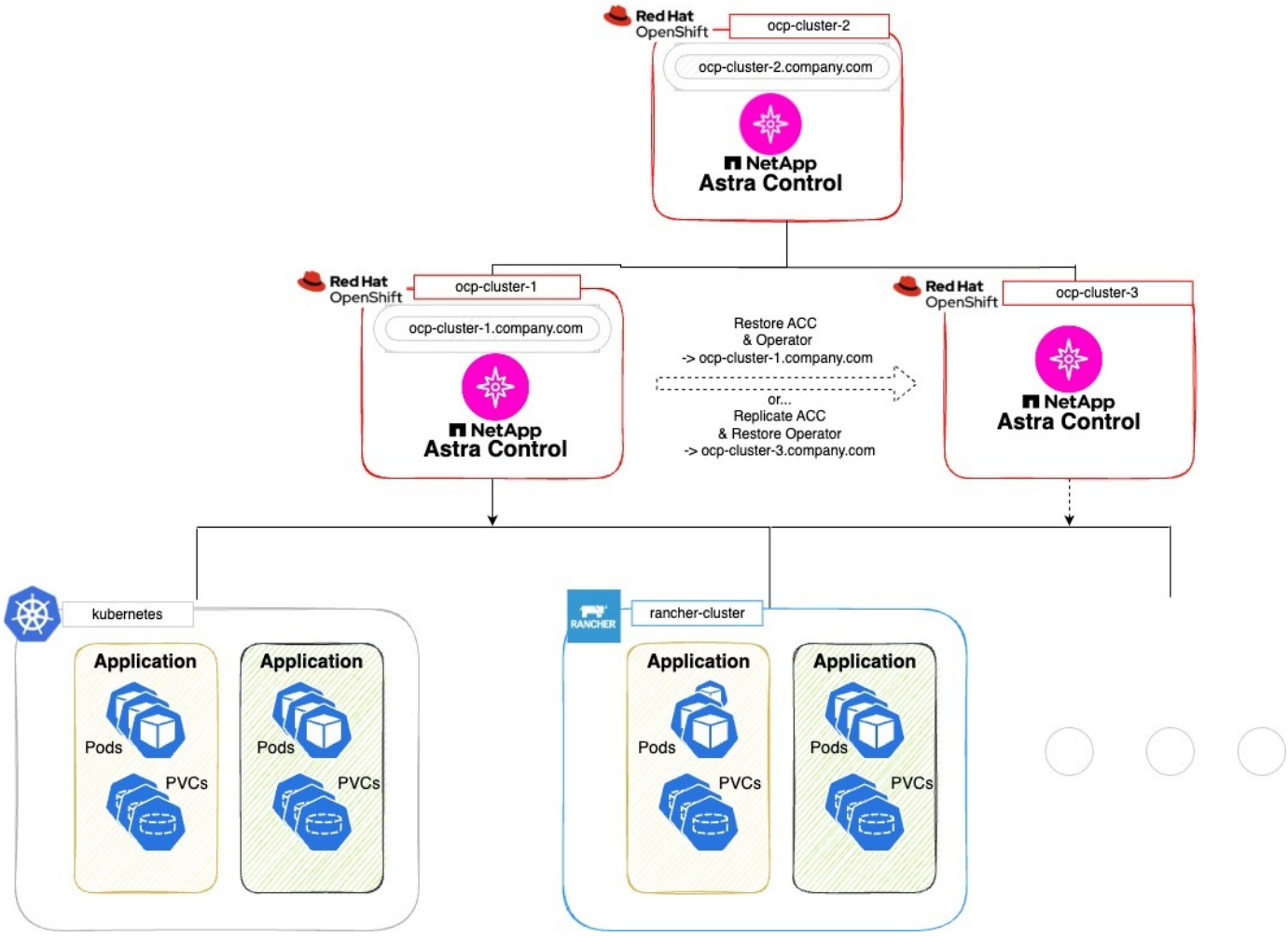
Antes de configurar cenários de proteção para o Astra Control Center, certifique-se de que você tenha o seguinte:

- **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 backends ONTAP com o Trident 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 23.10.0-68 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**.

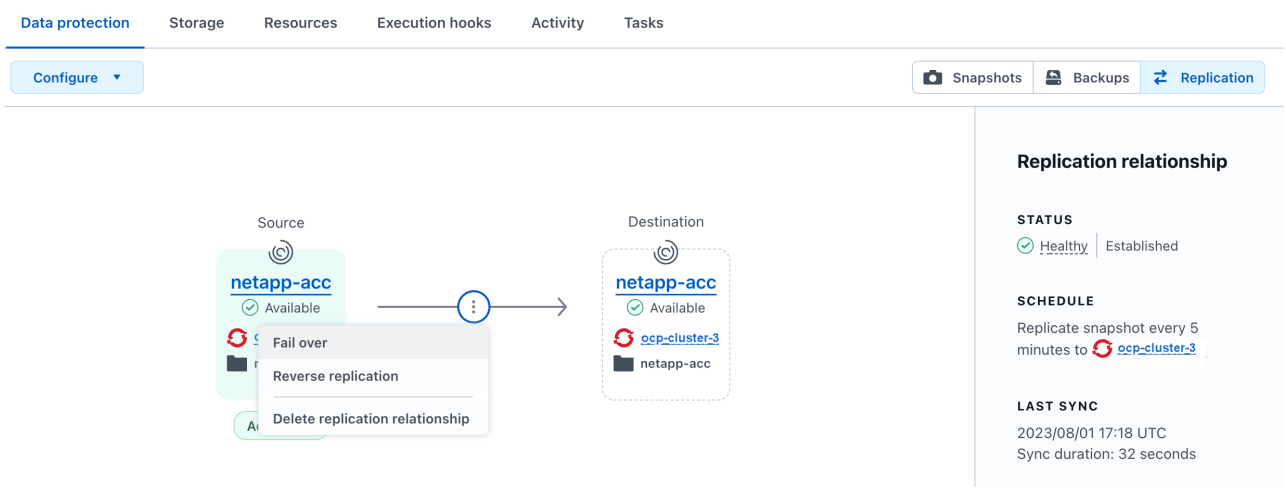
h. Confirme se a configuração está correta e selecione **Guardar**.

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 23.10.0-68 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.

Monitorar a integridade do aplicativo e do cluster

Exibir um resumo da integridade do aplicativo e do cluster

Selecione o **Dashboard** para ver uma visualização de alto nível de seus aplicativos, clusters, back-ends de armazenamento e sua integridade.

Estes não são apenas números estáticos ou status - você pode detalhar de cada um. Por exemplo, se os aplicativos não estiverem totalmente protegidos, você pode passar o Mouse sobre o ícone para identificar quais aplicativos não estão totalmente protegidos, o que inclui um motivo.

Mosaico de aplicações

O bloco **Applications** ajuda você a identificar o seguinte:

- Quantas aplicações você está gerenciando atualmente com o Astra.
- Se esses aplicativos gerenciados estão saudáveis.
- Se os aplicativos estão totalmente protegidos (eles são protegidos se os backups recentes estiverem disponíveis).
- O número de aplicativos que foram descobertos, mas ainda não são gerenciados.

  Idealmente, esse número seria zero porque você gerenciaria ou ignoraria aplicativos depois que eles forem descobertos. E então você monitoraria o número de aplicativos descobertos no Dashboard para identificar quando os desenvolvedores adicionam novos aplicativos a um cluster.

Blocos de clusters

O bloco **clusters** fornece detalhes semelhantes sobre a integridade dos clusters que você está gerenciando usando o Astra Control Center, e você pode detalhar para obter mais detalhes da mesma forma que pode com um aplicativo.

Azulejo dos backends de armazenamento

O bloco **Storage Backends** fornece informações para ajudá-lo a identificar a integridade dos backends de armazenamento, incluindo:

- Quantos backends de armazenamento são gerenciados
- Se esses backends gerenciados são saudáveis
- Se os backends estão totalmente protegidos
- O número de backends que são descobertos, mas ainda não são gerenciados.

Visualize a integridade do cluster e gerencie classes de armazenamento

Depois de adicionar clusters a serem gerenciados pelo Astra Control Center, é possível exibir detalhes sobre o cluster, como localização, nós de trabalho, volumes persistentes e classes de storage. Você também pode alterar a classe de storage padrão para clusters gerenciados.

Exibir integridade e detalhes do cluster

É possível exibir detalhes sobre o cluster, como sua localização, os nós de trabalho, volumes persistentes e classes de storage.

Passos

1. Na IU do Astra Control Center, selecione **clusters**.
2. Na página **clusters**, selecione o cluster cujos detalhes deseja exibir.

> Se um cluster ainda estiver `removed` no estado de cluster e a conetividade de rede parecer saudável (tentativas externas de acessar o cluster usando APIs do Kubernetes são bem-sucedidas), o kubeconfig que você forneceu ao Astra Control pode não ser mais válido. Isto pode dever-se à rotação ou expiração do certificado no cluster. Para corrigir esse problema, atualize as credenciais associadas ao cluster no Astra Control usando o "API Astra Control".

3. Veja as informações nas guias **Visão geral**, **armazenamento** e **atividade** para encontrar as informações que você está procurando.
   - **Visão geral**: Detalhes sobre os nós de trabalho, incluindo seu estado.
   - **Storage**: Os volumes persistentes associados à computação, incluindo a classe de armazenamento e o estado.
   - **Atividade**: Mostra as atividades relacionadas ao cluster.

> Você também pode exibir informações de cluster a partir do Astra Control Center **Dashboard**. Na guia **clusters** em **Resumo de recursos**, você pode selecionar os clusters gerenciados, que o levam à página **clusters**. Depois de acessar a página **clusters**, siga as etapas descritas acima.

Altere a classe de armazenamento padrão

Você pode alterar a classe de armazenamento padrão para um cluster. Quando o Astra Control gerencia um cluster, ele controla a classe de storage padrão do cluster.

> Não altere a classe de armazenamento usando comandos kubectl. Em vez disso, utilize este procedimento. O Astra Control reverterá as alterações se feitas usando kubectl.

Passos

1. Na IU da Web do Astra Control Center, selecione **clusters**.
2. Na página **clusters**, selecione o cluster que deseja alterar.
3. Selecione a guia **armazenamento**.
4. Selecione a categoria **Storage classes**.

5. Selecione o menu **ações** para a classe de armazenamento que você deseja definir como padrão.
6. Selecione **Definir como padrão**.

Veja a saúde e os detalhes de um aplicativo

Depois de começar a gerenciar uma aplicação, o Astra Control fornece detalhes sobre a aplicação que permite identificar seu status de comunicação (se o Astra Control pode se comunicar com a aplicação), seu status de proteção (se ele está totalmente protegido em caso de falha), os pods, storage persistente e muito mais.

Passos

1. Na IU do Astra Control Center, selecione **Applications** e, em seguida, selecione o nome de um aplicativo.
2. Reveja as informações.

   Estado da aplicação
   Fornece um status que reflete se o Astra Control pode se comunicar com a aplicação.

   - **Status da proteção do aplicativo**: Fornece um status de quão bem o aplicativo está protegido:
     - **Totalmente protegido**: O aplicativo tem um agendamento de backup ativo e um backup bem-sucedido com menos de uma semana de idade
     - **Parcialmente protegido**: O aplicativo tem um agendamento de backup ativo, um agendamento de snapshot ativo ou um backup ou snapshot bem-sucedido
     - **Desprotegido**: Aplicativos que não estão totalmente protegidos ou parcialmente protegidos.

       Você não pode estar totalmente protegido até ter um backup recente. Isso é importante porque os backups são armazenados em um armazenamento de objetos longe dos volumes persistentes. Se uma falha ou acidente apagar o cluster e seu armazenamento persistente, então você precisa de um backup para recuperar. Um instantâneo não permitiria que você se recuperasse.
   - **Visão geral**: Informações sobre o estado dos pods associados ao aplicativo.
   - **Proteção de dados**: Permite configurar uma política de proteção de dados e visualizar os instantâneos e backups existentes.
   - **Storage**: Mostra os volumes persistentes no nível do aplicativo. O estado de um volume persistente é da perspetiva do cluster do Kubernetes.
   - **Recursos**: Permite verificar quais recursos estão sendo copiados e gerenciados.
   - **Actividade**: Mostra as atividades relacionadas com a aplicação.

   > Você também pode visualizar informações de aplicativos a partir do Astra Control Center **Dashboard**. Na guia **aplicativos** em **Resumo de recursos**, você pode selecionar os aplicativos gerenciados, que o levam à página **aplicativos**. Depois de acessar a página **aplicativos**, siga as etapas descritas acima.

Gerencie sua conta

Gerencie usuários e funções locais

Você pode adicionar, remover e editar usuários da instalação do Astra Control Center usando a IU do Astra Control. Você pode usar a IU do Astra Control ou "API Astra Control" gerenciar usuários.

Você também pode usar LDAP para executar a autenticação para usuários selecionados.

Utilize LDAP

O LDAP é um protocolo padrão do setor para acessar informações de diretórios distribuídos e uma escolha popular para autenticação empresarial. Você pode conetar o Astra Control Center a um servidor LDAP para executar a autenticação para usuários selecionados do Astra Control. Em alto nível, a configuração envolve a integração do Astra com LDAP e a definição dos usuários e grupos do Astra Control correspondentes às definições LDAP. Você pode usar a API Astra Control ou a IU da Web para configurar a autenticação LDAP e usuários e grupos LDAP. Consulte a seguinte documentação para obter mais informações:

- "Use a API Astra Control para gerenciar usuários e autenticação remota"
- "Use a IU do Astra Control para gerenciar usuários e grupos remotos"
- "Use a IU do Astra Control para gerenciar a autenticação remota"

Adicionar utilizadores

Os proprietários e administradores de contas podem adicionar mais usuários à instalação do Astra Control Center.

Passos

1. Na área de navegação **Gerenciar sua conta**, selecione **conta**.
2. Selecione a guia **usuários**.
3. Selecione **Adicionar usuário**.
4. Introduza o nome do utilizador, o endereço de correio eletrónico e uma palavra-passe temporária.

   O utilizador terá de alterar a palavra-passe no primeiro início de sessão.

5. Selecione uma função de usuário com as permissões de sistema apropriadas.

   Cada função fornece as seguintes permissões:

   - Um **Viewer** pode visualizar recursos.
   - Um **Membro** tem permissões de função Visualizador e pode gerenciar aplicativos e clusters, desgerenciar aplicativos e excluir snapshots e backups.
   - Um **Admin** tem permissões de função de Membro e pode adicionar e remover quaisquer outros usuários, exceto o proprietário.
   - Um **proprietário** tem permissões de função Admin e pode adicionar e remover quaisquer contas de usuário.

6. Para adicionar restrições a um utilizador com uma função Membro ou Visualizador, ative a caixa de verificação **restringir função a restrições**.

   Para obter mais informações sobre como adicionar restrições, "Gerencie usuários e funções locais"consulte .

7. Selecione **Adicionar**.

Gerenciar senhas

Você pode gerenciar senhas para contas de usuário no Astra Control Center.

Altere a sua palavra-passe

Você pode alterar a senha da sua conta de usuário a qualquer momento.

Passos

1. Selecione o ícone Utilizador no canto superior direito do ecrã.
2. Selecione **Perfil**.
3. No menu Opções na coluna **ações** e selecione **alterar senha**.
4. Introduza uma palavra-passe que esteja em conformidade com os requisitos de palavra-passe.
5. Introduza novamente a palavra-passe para confirmar.
6. Selecione **alterar palavra-passe**.

Repor a palavra-passe de outro utilizador

Se a sua conta tiver permissões de função de Administrador ou proprietário, você pode redefinir senhas para outras contas de usuário, bem como suas próprias. Ao redefinir uma senha, você atribui uma senha temporária que o usuário terá que alterar ao fazer login.

Passos

1. Na área de navegação **Gerenciar sua conta**, selecione **conta**.
2. Selecione a lista suspensa **ações**.
3. Selecione **Redefinir senha**.
4. Introduza uma palavra-passe temporária que esteja em conformidade com os requisitos de palavra-passe.
5. Introduza novamente a palavra-passe para confirmar.

   Da próxima vez que o usuário fizer login, será solicitado que o usuário altere a senha.

6. Selecione **Redefinir senha**.

Remover usuários

Os usuários com a função proprietário ou Admin podem remover outros usuários da conta a qualquer momento.

Passos

1. Na área de navegação **Gerenciar sua conta**, selecione **conta**.
2. Na guia **usuários**, marque a caixa de seleção na linha de cada usuário que você deseja remover.
3. No menu Opções na coluna **ações**, selecione **Remover usuário(s)**.
4. Quando for solicitado, confirme a exclusão digitando a palavra "remover" e selecione **Sim, Remover usuário**.

Resultado

O Astra Control Center remove o usuário da conta.

Gerenciar funções

Você pode gerenciar funções adicionando restrições de namespace e restringindo funções de usuário a essas restrições. Isso permite que você controle o acesso a recursos dentro de sua organização. Você pode usar a IU do Astra Control ou "API Astra Control" gerenciar funções.

Adicione uma restrição de namespace a uma função

Um usuário Admin ou proprietário pode adicionar restrições de namespace às funções Membro ou Visualizador.

Passos

1. Na área de navegação **Gerenciar sua conta**, selecione **conta**.
2. Selecione a guia **usuários**.
3. Na coluna **ações**, selecione o botão de menu para um usuário com a função Membro ou Visualizador.
4. Selecione **Editar função**.
5. Ative a caixa de verificação **restringir função a restrições**.

   A caixa de verificação só está disponível para funções Membro ou Visualizador. Você pode selecionar uma função diferente na lista suspensa **Role**.

6. Selecione **Adicionar restrição**.

   Você pode ver a lista de restrições disponíveis por namespace ou por rótulo de namespace.

7. Na lista suspensa **tipo de restrição**, selecione **namespace do Kubernetes** ou **rótulo do namespace do Kubernetes** dependendo de como seus namespaces são configurados.
8. Selecione um ou mais namespaces ou rótulos da lista para compor uma restrição que restrinja funções a esses namespaces.
9. Selecione **Confirm**.

   A página **Editar função** exibe a lista de restrições que você escolheu para essa função.

10. Selecione **Confirm**.

    Na página **conta**, você pode visualizar as restrições para qualquer função de Membro ou Visualizador na coluna **função**.

> ⓘ Se você habilitar restrições para uma função e selecionar **Confirm** sem adicionar nenhuma restrição, a função será considerada como tendo restrições completas (a função é negada acesso a quaisquer recursos atribuídos a namespaces).

Remova uma restrição de namespace de uma função

Um usuário Admin ou proprietário pode remover uma restrição de namespace de uma função.

Passos

1. Na área de navegação **Gerenciar sua conta**, selecione **conta**.

2. Selecione a guia **usuários**.
3. Na coluna **ações**, selecione o botão de menu para um usuário com a função Membro ou Visualizador que tem restrições ativas.
4. Selecione **Editar função**.

   A caixa de diálogo **Editar função** exibe as restrições ativas para a função.

5. Selecione **X** à direita da restrição que você precisa remover.
6. Selecione **Confirm**.

Para mais informações

- "Funções de usuário e namespaces"

Gerenciar a autenticação remota

O LDAP é um protocolo padrão do setor para acessar informações de diretórios distribuídos e uma escolha popular para autenticação empresarial. Você pode conetar o Astra Control Center a um servidor LDAP para executar a autenticação para usuários selecionados do Astra Control.

Em alto nível, a configuração envolve a integração do Astra com LDAP e a definição dos usuários e grupos do Astra Control correspondentes às definições LDAP. Você pode usar a API Astra Control ou a IU da Web para configurar a autenticação LDAP e usuários e grupos LDAP.

> ⓘ O Astra Control Center usa o atributo de login do usuário, configurado quando a autenticação remota está ativada, para pesquisar e acompanhar usuários remotos. Um atributo de um endereço de e-mail ("mail") ou nome principal do usuário ("userPrincipalName") deve existir neste campo para qualquer usuário remoto que você deseja aparecer no Astra Control Center. Este atributo é usado como o nome de usuário no Astra Control Center para autenticação e em pesquisas de usuários remotos.

Adicione um certificado para autenticação LDAPS

Adicione o certificado TLS privado para o servidor LDAP para que o Astra Control Center possa se autenticar com o servidor LDAP quando você usa uma conexão LDAPS. Você só precisa fazer isso uma vez, ou quando o certificado que você instalou expirar.

Passos

1. Vá para **conta**.
2. Selecione a guia **certificados**.
3. Selecione **Adicionar**.
4. Carregue o `.pem` arquivo ou cole o conteúdo do arquivo da área de transferência.
5. Marque a caixa de seleção **Trusted**.
6. Selecione **Adicionar certificado**.

Ativar autenticação remota

Você pode ativar a autenticação LDAP e configurar a conexão entre o Astra Control e o servidor LDAP remoto.

Antes de começar

Se você planeja usar o LDAPS, verifique se o certificado TLS privado para o servidor LDAP está instalado no Astra Control Center para que o Astra Control Center possa se autenticar com o servidor LDAP. Adicione um certificado para autenticação LDAPSConsulte para obter instruções.

Passos

1. Aceda a **conta > ligações**.
2. No painel **Autenticação remota**, selecione o menu de configuração.
3. Selecione **Connect**.
4. Introduza o endereço IP do servidor, a porta e o protocolo de ligação preferido (LDAP ou LDAPS).

   Como prática recomendada, use o LDAPS ao se conetar ao servidor LDAP. Você precisa instalar o certificado TLS privado do servidor LDAP no Astra Control Center antes de se conetar ao LDAPS.

5. Insira as credenciais da conta de serviço no formato de e-mail (administrator@example.com). O Astra Control usará essas credenciais ao se conetar ao servidor LDAP.
6. Na seção **User Match**, faça o seguinte:
   a. Insira o DN base e um filtro de pesquisa de usuário apropriado para usar ao recuperar informações do usuário do servidor LDAP.
   b. (Opcional) se o diretório usar o atributo de login do usuário `userPrincipalName` em vez `mail` de , digite `userPrincipalName` o atributo correto no campo **atributo de login do usuário**.
7. Na seção **correspondência de grupo**, insira o DN da base de pesquisa de grupo e um filtro de pesquisa de grupo personalizado apropriado.

   Certifique-se de usar o DN (Nome distinto) base correto e um filtro de pesquisa apropriado para **User Match** e **Group Match**. O DN base informa ao Astra Control em que nível da árvore de diretórios iniciar a pesquisa e o filtro de pesquisa limita as partes da árvore de diretórios do Astra Control.

8. Selecione **Enviar**.

Resultado

O status do painel **Autenticação remota** é movido para **pendente** e depois para **conectado** quando a conexão com o servidor LDAP é estabelecida.

Desativar a autenticação remota

Pode desativar temporariamente uma ligação ativa ao servidor LDAP.

Quando você desativa uma conexão com um servidor LDAP, todas as configurações são salvas e todos os usuários remotos e grupos que foram adicionados ao Astra Control a partir desse servidor LDAP são retidos. Você pode se reconetar a este servidor LDAP a qualquer momento.

Passos

1. Aceda a **conta > ligações**.
2. No painel **Autenticação remota**, selecione o menu de configuração.
3. Selecione **Desativar**.

Resultado

O status do painel **Autenticação remota** é movido para **Desativado**. Todas as configurações de autenticação remota, usuários remotos e grupos remotos são preservados e você pode reativar a conexão a qualquer momento.

Editar definições de autenticação remota

Se tiver desativado a ligação ao servidor LDAP ou se o painel **Autenticação remota** estiver no estado "erro de ligação", pode editar as definições de configuração.

Não é possível editar o URL ou o endereço IP do servidor LDAP quando o painel **Autenticação remota** estiver no estado "Desativado". Você precisa Desconete a autenticação remotaprimeiro.

Passos

1. Aceda a **conta > ligações**.
2. No painel **Autenticação remota**, selecione o menu de configuração.
3. Selecione **Editar**.
4. Faça as alterações necessárias e selecione **Editar**.

Desconete a autenticação remota

Você pode se desconetar de um servidor LDAP e remover as configurações do Astra Control.

Se você for um usuário LDAP e desconetar, sua sessão terminará imediatamente Quando você se desconeta do servidor LDAP, todas as configurações desse servidor LDAP são removidas do Astra Control, bem como quaisquer usuários e grupos remotos que foram adicionados desse servidor LDAP.

Passos

1. Aceda a **conta > ligações**.
2. No painel **Autenticação remota**, selecione o menu de configuração.
3. Selecione **Disconnect**.

Resultado

O status do painel **Autenticação remota** é movido para **desconectada**. As configurações de autenticação remota, usuários remotos e grupos remotos são removidos do Astra Control.

Gerenciar usuários e grupos remotos

Se você ativou a autenticação LDAP no sistema Astra Control, poderá pesquisar usuários e grupos LDAP e incluí-los nos usuários aprovados do sistema.

Adicionar um utilizador remoto

Proprietários e administradores de contas podem adicionar usuários remotos ao Astra Control. O Astra Control Center dá suporte a até 10.000 usuários remotos LDAP.

> O Astra Control Center usa o atributo de login do usuário, configurado quando a autenticação remota está ativada, para pesquisar e acompanhar usuários remotos. Um atributo de um endereço de e-mail ("mail") ou nome principal do usuário ("userPrincipalName") deve existir neste campo para qualquer usuário remoto que você deseja aparecer no Astra Control Center. Este atributo é usado como o nome de usuário no Astra Control Center para autenticação e em pesquisas de usuários remotos.

> Você não pode adicionar um usuário remoto se um usuário local com o mesmo endereço de e-mail (com base no atributo "e-mail" ou "nome principal do usuário") já existir no sistema. Para adicionar o utilizador como utilizador remoto, primeiro elimine o utilizador local do sistema.

Passos

1. Vá para a área **conta**.
2. Selecione a guia **usuários e grupos**.
3. No canto direito da página, selecione **usuários remotos**.
4. Selecione **Adicionar**.
5. Opcionalmente, procure um usuário LDAP inserindo o endereço de e-mail do usuário no campo **Filtrar por e-mail**.
6. Selecione um ou mais utilizadores na lista.
7. Atribua uma função ao utilizador.

> Se você atribuir funções diferentes a um usuário e ao grupo do usuário, a função mais permissiva terá precedência.

8. Opcionalmente, atribua uma ou mais restrições de namespace a este usuário e selecione **restringir função a restrições** para aplicá-las. Você pode adicionar uma nova restrição de namespace selecionando **Add constraint**.

> Quando um usuário recebe várias funções por meio da associação ao grupo LDAP, as restrições na função mais permissiva são as únicas que entram em vigor. Por exemplo, se um utilizador com uma função Visualizador local juntar três grupos que estão ligados à função Membro, a soma das restrições das funções Membro entra em vigor e quaisquer restrições da função Visualizador são ignoradas.

9. Selecione **Adicionar**.

Resultado

O novo utilizador aparece na lista de utilizadores remotos. Nesta lista, você pode ver restrições ativas no usuário, bem como gerenciar o usuário no menu **ações**.

Adicionar um grupo remoto

Para adicionar muitos usuários remotos de uma só vez, os proprietários e administradores de contas podem adicionar grupos remotos ao Astra Control. Quando você adiciona um grupo remoto, todos os usuários

remotos desse grupo estarão disponíveis para fazer login no Astra Control e herdarão a mesma função que o grupo.

O Astra Control Center é compatível com até 5.000 grupos remotos LDAP.

Passos

1. Vá para a área **conta**.
2. Selecione a guia **usuários e grupos**.
3. No canto direito da página, selecione **grupos remotos**.
4. Selecione **Adicionar**.

   Nesta janela, você pode ver uma lista dos nomes comuns e nomes distintos dos grupos LDAP que o Astra Control recuperou do diretório.

5. Opcionalmente, procure um grupo LDAP inserindo o nome comum do grupo no campo **Filtrar por nome comum**.
6. Selecione um ou mais grupos na lista.
7. Atribua uma função aos grupos.

   A função selecionada é atribuída a todos os usuários deste grupo. Se você atribuir funções diferentes a um usuário e ao grupo do usuário, a função mais permissiva terá precedência.

8. Opcionalmente, atribua uma ou mais restrições de namespace a esse grupo e selecione **restringir função a restrições** para aplicá-las. Você pode adicionar uma nova restrição de namespace selecionando **Add constraint**.

   Quando um usuário recebe várias funções por meio da associação ao grupo LDAP, as restrições na função mais permissiva são as únicas que entram em vigor. Por exemplo, se um utilizador com uma função Visualizador local juntar três grupos que estão ligados à função Membro, a soma das restrições das funções Membro entra em vigor e quaisquer restrições da função Visualizador são ignoradas.

9. Selecione **Adicionar**.

Resultado

O novo grupo aparece na lista de grupos remotos. Os utilizadores remotos deste grupo não aparecem na lista de utilizadores remotos até que cada utilizador remoto inicie sessão. Nesta lista, pode ver detalhes sobre o grupo, bem como gerir o grupo a partir do menu **ações**.

Ver e gerir notificações

O Astra notifica você quando as ações forem concluídas ou falhadas. Por exemplo, você verá uma notificação se um backup de um aplicativo for concluído com êxito.

Você pode gerenciar essas notificações no canto superior direito da interface:

Passos

1. Selecione o número de notificações não lidas no canto superior direito.
2. Reveja as notificações e selecione **Marcar como lidas** ou **Mostrar todas as notificações**.

   Se você selecionou **Mostrar todas as notificações**, a página notificações será carregada.

3. Na página **notificações**, visualize as notificações, selecione as que deseja marcar como lidas, selecione **Ação** e selecione **Marcar como lidas**.

Adicione e remova credenciais

Adicione e remova credenciais de fornecedores de nuvem privada locais, como o ONTAP S3, clusters do Kubernetes gerenciados com o OpenShift ou clusters do Kubernetes não gerenciados da sua conta a qualquer momento. O Astra Control Center usa essas credenciais para descobrir clusters de Kubernetes e as aplicações nos clusters e para provisionar recursos em seu nome.

Observe que todos os usuários do Astra Control Center compartilham os mesmos conjuntos de credenciais.

Adicionar credenciais

Você pode adicionar credenciais ao Astra Control Center ao gerenciar clusters. Para adicionar credenciais adicionando um novo cluster, "Adicionar um cluster do Kubernetes"consulte .

> Se você criar seu próprio arquivo kubeconfig, você deve definir apenas um elemento de contexto * nele. "Documentação do Kubernetes"Consulte para obter informações sobre a criação de arquivos kubeconfig.

Remover credenciais

Remova as credenciais de uma conta a qualquer momento. Você só deve remover credenciais após "desgerenciar todos os clusters associados"o .

> O primeiro conjunto de credenciais que você adiciona ao Astra Control Center está sempre em uso porque o Astra Control Center usa as credenciais para se autenticar no bucket do backup. É melhor não remover essas credenciais.

Passos

1. Selecione **conta**.
2. Selecione a guia **Credentials**.
3. Selecione o menu Opções na coluna **Estado** para as credenciais que você deseja remover.
4. Selecione **Remover**.
5. Digite a palavra "remove" para confirmar a exclusão e selecione **Yes, Remove Credential**.

Resultado

O Astra Control Center remove as credenciais da conta.

Monitorar a atividade da conta

Você pode ver detalhes sobre as atividades na sua conta do Astra Control. Por exemplo, quando novos usuários foram convidados, quando um cluster foi adicionado ou quando um snapshot foi tirado. Você também pode exportar a atividade da sua conta para um arquivo CSV.

Se você gerenciar clusters de Kubernetes do Astra Control e do Astra Control estiver conetado ao Cloud Insights, o Astra Control enviará logs de eventos para o Cloud Insights. As informações de log, incluindo informações sobre implantação de pod e anexos de PVC, são exibidas no log de atividades do Astra Control. Use essas informações para identificar quaisquer problemas nos clusters do Kubernetes que você está gerenciando.

Ver todas as atividades da conta no Astra Control

1. Selecione **atividade**.
2. Use os filtros para restringir a lista de atividades ou use a caixa de pesquisa para encontrar exatamente o que você está procurando.
3. Selecione **Exportar para CSV** para fazer o download da atividade da sua conta para um arquivo CSV.

Exibir atividade da conta para um aplicativo específico

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

Ver atividade da conta dos clusters

1. Selecione **clusters** e, em seguida, selecione o nome do cluster.
2. Selecione **atividade**.

Tome medidas para resolver eventos que exigem atenção

1. Selecione **atividade**.
2. Selecione um evento que exija atenção.
3. Selecione a opção suspensa **Take Action**.

   Nesta lista, você pode visualizar possíveis ações corretivas que você pode executar, exibir a documentação relacionada ao problema e obter suporte para ajudar a resolver o problema.

Atualizar uma licença existente

Você pode converter uma licença de avaliação para uma licença completa ou atualizar uma avaliação existente ou uma licença completa com uma nova licença. Se você não tiver uma licença completa, trabalhe com seu Contato de vendas da NetApp para obter uma licença completa e um número de série. Você pode usar a IU do Astra Control Center ou "API Astra Control" atualizar uma licença existente.

Passos

1. Inicie sessão no "Site de suporte da NetApp".
2. Acesse a página de download do Centro de Controle Astra, insira o número de série e baixe o arquivo de licença NetApp completo (NLF).

3. Faça login na IU do Astra Control Center.
4. Na navegação à esquerda, selecione **conta** > **Licença**.
5. Na página **conta** > **Licença**, selecione o menu suspenso status da licença existente e selecione **Substituir**.
6. Navegue até o arquivo de licença que você baixou.
7. Selecione **Adicionar**.

A página **Account** > **Licenses** exibe as informações da licença, data de validade, número de série da licença, ID da conta e unidades CPU usadas.

Para mais informações

- "Licenciamento do Astra Control Center"

Gerenciar buckets

Um fornecedor de bucket do armazenamento de objetos é essencial para fazer backup das aplicações e do storage persistente ou para clonar aplicações entre clusters. Usando o Astra Control Center, adicione um provedor de armazenamento de objetos como destino de backup externo para seus aplicativos.

Não é necessário um bucket se estiver clonando a configuração da aplicação e o storage persistente para o mesmo cluster.

Use um dos seguintes provedores de bucket do Amazon Simple Storage Service (S3):

- NetApp ONTAP S3
- NetApp StorageGRID S3
- Microsoft Azure
- Genérico S3

> A Amazon Web Services (AWS) e o Google Cloud Platform (GCP) usam o tipo de bucket Generic S3.

> Embora o Astra Control Center ofereça suporte ao Amazon S3 como um provedor de bucket do Generic S3, o Astra Control Center pode não oferecer suporte a todos os fornecedores de armazenamento de objetos que claim o suporte ao S3 da Amazon.

Um balde pode estar em um destes estados:

- Pendente: O bucket está programado para descoberta.
- Disponível: O balde está disponível para uso.
- Removido: O balde não está atualmente acessível.

Para obter instruções sobre como gerenciar buckets usando a API Astra Control, consulte o "Informações de API e automação do Astra".

Você pode executar estas tarefas relacionadas ao gerenciamento de buckets:

- "Adicione um balde"
- Edite um balde
- Defina o intervalo predefinido
- Gire ou remova as credenciais do bucket
- Retire um balde

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.

Edite um balde

Você pode alterar as informações de credenciais de acesso para um bucket e alterar se um bucket selecionado é o bucket padrão.

Quando você adiciona um bucket, selecione o provedor de bucket correto e forneça as credenciais certas para esse provedor. Por exemplo, a IU aceita o NetApp ONTAP S3 como o tipo e aceita credenciais StorageGRID; no entanto, isso fará com que todos os backups e restaurações futuros de aplicativos que usam esse bucket falhem. Consulte "Notas de versão".

Passos

1. Na navegação à esquerda, selecione **Buckets**.
2. No menu da coluna **ações**, selecione **Editar**.
3. Altere qualquer informação que não seja o tipo de balde.

   Não é possível modificar o tipo de bucket.

4. Selecione **Atualizar**.

Defina o intervalo predefinido

Quando você executa um clone nos clusters, o Astra Control requer um bucket padrão. Siga estas etapas para definir um bucket padrão para todos os clusters.

Passos

1. Vá para **instâncias da nuvem**.
2. Selecione o menu na coluna **ações** para a instância de nuvem na lista.
3. Selecione **Editar**.
4. Na lista **Bucket**, selecione o bucket que deseja ser o padrão.
5. Selecione **Guardar**.

Gire ou remova as credenciais do bucket

O Astra Control usa credenciais de bucket para obter acesso e fornecer chaves secretas para um bucket do S3, para que o Astra Control Center possa se comunicar com o bucket.

Gire as credenciais do bucket

Se você girar credenciais, gire-as durante uma janela de manutenção quando nenhum backup estiver em andamento (agendado ou sob demanda).

Etapas para editar e girar credenciais

1. Na navegação à esquerda, selecione **Buckets**.
2. No menu Opções na coluna **ações**, selecione **Editar**.
3. Crie a nova credencial.
4. Selecione **Atualizar**.

Remova as credenciais do bucket

Você só deve remover credenciais de bucket se novas credenciais tiverem sido aplicadas a um bucket ou se o bucket não for mais usado ativamente.

O primeiro conjunto de credenciais que você adiciona ao Astra Control está sempre em uso porque o Astra Control usa as credenciais para autenticar o bucket do backup. Não remova essas credenciais se o bucket estiver em uso ativo, pois isso levará a falhas de backup e indisponibilidade de backup.

Se você remover credenciais de bucket ativas, "solução de problemas na remoção de credenciais do balde"consulte .

Para obter instruções sobre como remover credenciais do S3 usando a API Astra Control, consulte o "Informações de API e automação do Astra".

Retire um balde

Você pode remover um balde que não está mais em uso ou não está saudável. Você pode querer fazer isso para manter a configuração do armazenamento de objetos simples e atualizada.

- Não é possível remover um balde predefinido. Se você quiser remover esse balde, primeiro selecione outro balde como padrão.
- Não é possível remover um bucket do WORM (write once read many) antes do período de retenção do fornecedor de nuvem do bucket expirar. Os baldes SEM-FIM são indicados com "bloqueado" junto ao nome do balde.

- Não é possível remover um balde predefinido. Se você quiser remover esse balde, primeiro selecione outro balde como padrão.

Antes de começar

- Você deve verificar se não há backups em execução ou concluídos para esse bucket antes de começar.
- Você deve verificar se o balde não está sendo usado em nenhuma política de proteção ativa.

Se houver, você não será capaz de continuar.

Passos

1. Na navegação à esquerda, selecione **baldes**.

2. No menu **ações**, selecione **Remover**.

> O Astra Control garante primeiro que não haja políticas de agendamento usando o bucket dos backups e que não haja backups ativos no bucket que você está prestes a remover.

3. Digite "remove" para confirmar a ação.
4. Selecione **Sim, remova o balde**.

Encontre mais informações

- "Use a API Astra Control"

Gerenciar o back-end de storage

O gerenciamento de clusters de storage no Astra Control como um back-end de storage permite que você tenha vínculos entre volumes persistentes (PVS) e o back-end de storage, bem como métricas de storage adicionais. Você pode monitorar os detalhes de integridade e capacidade de storage, incluindo a performance se o Astra Control Center estiver conetado ao Cloud Insights.

Para obter instruções sobre como gerenciar back-ends de storage usando a API Astra Control, consulte o "Informações de API e automação do Astra".

Você pode concluir as seguintes tarefas relacionadas ao gerenciamento de um back-end de storage:

- "Adicionar um back-end de storage"
- Veja os detalhes do back-end de armazenamento
- Editar detalhes de autenticação de back-end de armazenamento
- Gerenciar um back-end de storage descoberto
- Desgerenciar um back-end de storage
- Remover um back-end de storage

Veja os detalhes do back-end de armazenamento

Você pode exibir informações de back-end de armazenamento no Dashboard ou na opção backends.

Veja os detalhes do back-end do storage no Dashboard

Passos

1. Na navegação à esquerda, selecione **Dashboard**.
2. Revise o painel de back-end do Storage do Dashboard que mostra o estado:
   - **Insalubre**: O armazenamento não está em um estado ideal. Isso pode ser devido a um problema de latência ou um aplicativo é degradado devido a um problema de contentor, por exemplo.
   - **Todos saudáveis**: O armazenamento foi gerenciado e está em um estado ideal.
   - **Descoberto**: O storage foi descoberto, mas não gerenciado pelo Astra Control.

Veja os detalhes do back-end de armazenamento na opção backends

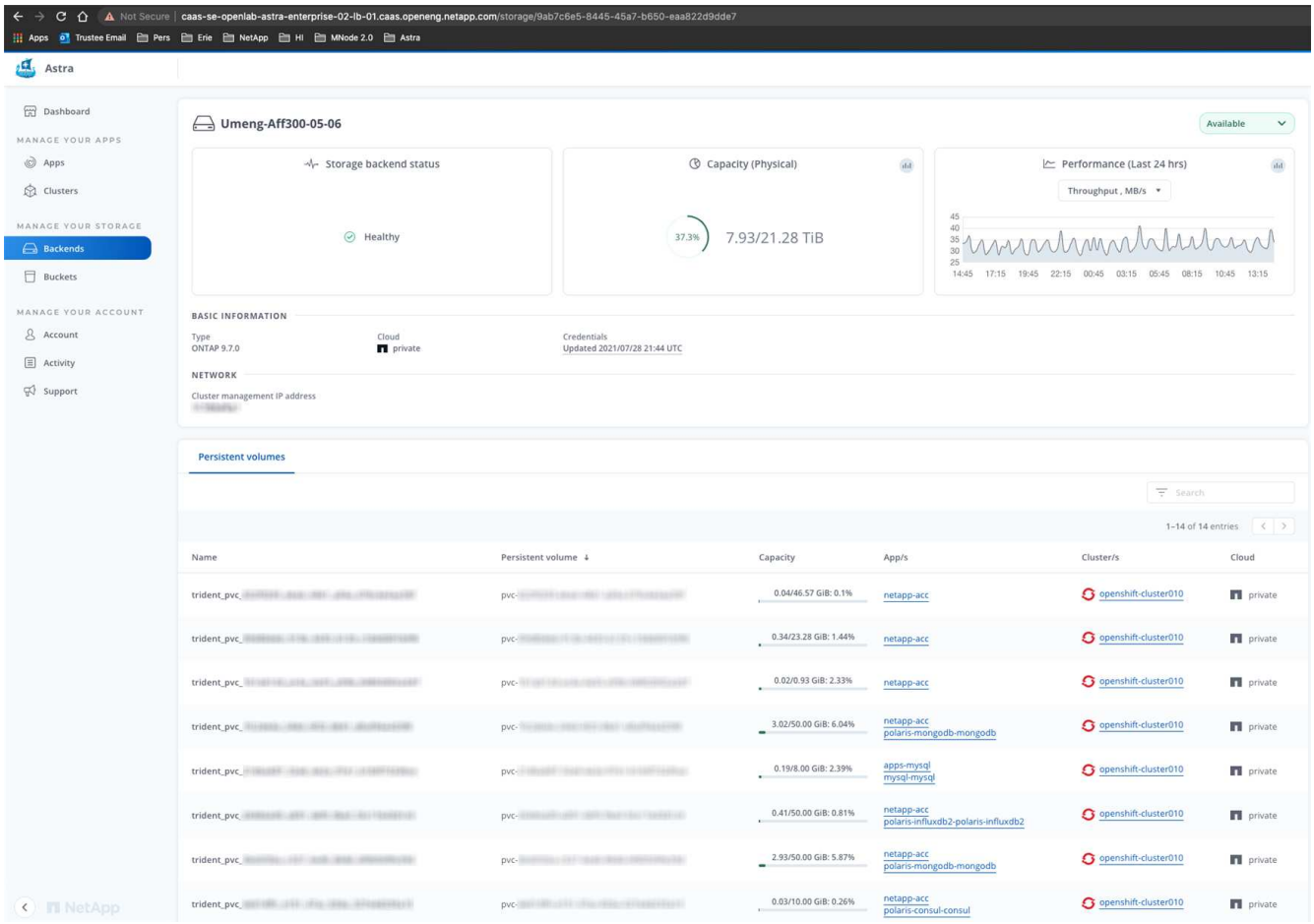
Veja informações sobre a integridade, a capacidade e a performance do back-end (taxa de transferência de IOPS e/ou latência).

Você pode ver os volumes que os aplicativos Kubernetes estão usando, que são armazenados em um back-end de storage selecionado. Com o Cloud Insights, você pode ver informações adicionais. "Documentação do Cloud Insights"Consulte .

Passos

1. Na área de navegação à esquerda, selecione **backends**.
2. Selecione o back-end de armazenamento.

> Se você se conetou ao NetApp Cloud Insights, trechos de dados do Cloud Insights aparecerão na página de backends.



3. Para ir diretamente ao Cloud Insights, selecione o ícone **Cloud Insights** ao lado da imagem de métricas.

Editar detalhes de autenticação de back-end de armazenamento

O Astra Control Center oferece dois modos de autenticação de um back-end do ONTAP.

- **Autenticação baseada em credenciais**: O nome de usuário e senha para um usuário do ONTAP com as permissões necessárias. Você deve usar uma função de login de segurança predefinida, como admin, para garantir a máxima compatibilidade com versões do ONTAP.

- **Autenticação baseada em certificado**: O Astra Control Center também pode se comunicar com um cluster ONTAP usando um certificado instalado no back-end. Você deve usar o certificado de cliente, a chave e o certificado de CA confiável, se usado (recomendado).

Você pode atualizar os backends existentes para passar de um tipo de autenticação para outro método. Apenas um método de autenticação é suportado de cada vez.

Para obter detalhes sobre como ativar a autenticação baseada em certificado, "Ativar a autenticação no back-end de storage do ONTAP"consulte .

Passos

1. Na navegação à esquerda, selecione **backends**.
2. Selecione o back-end de armazenamento.
3. No campo credenciais, selecione o ícone **Editar**.
4. Na página Editar, selecione uma das seguintes opções.
   - **Use as credenciais de administrador**: Insira o endereço IP e as credenciais de administrador de gerenciamento de cluster do ONTAP. As credenciais devem ser credenciais de todo o cluster.

     O usuário cujas credenciais você inserir aqui deve ter o `ontapi` método de acesso de login de usuário habilitado no Gerenciador de sistema do ONTAP no cluster do ONTAP. Se você planeja usar a replicação do SnapMirror, aplique credenciais de usuário com a função "admin", que tem os métodos de acesso `ontapi` e `http`, nos clusters ONTAP de origem e destino. "Gerenciar contas de usuário na documentação do ONTAP"Consulte para obter mais informações.

   - **Use um certificado**: Carregue o arquivo de certificado `.pem`, o arquivo de chave de certificado `.key` e, opcionalmente, o arquivo de autoridade de certificação.
5. Selecione **Guardar**.

Gerenciar um back-end de storage descoberto

Você pode optar por gerenciar um back-end de storage não gerenciado, mas descoberto. Quando você gerencia um back-end de storage, o Astra Control indica se um certificado de autenticação expirou.

Passos

1. Na navegação à esquerda, selecione **backends**.
2. Selecione a opção **descoberto**.
3. Selecione o back-end de armazenamento.
4. No menu Opções na coluna **ações**, selecione **Gerenciar**.
5. Faça as alterações.
6. Selecione **Guardar**.

Desgerenciar um back-end de storage

Você pode desgerenciar o backend.

Passos

1. Na navegação à esquerda, selecione **backends**.

2. Selecione o back-end de armazenamento.
3. No menu Opções na coluna **ações**, selecione **Desgerenciar**.
4. Digite "Unmanage" (Desgerenciar) para confirmar a ação.
5. Selecione **Sim, desgerencie o back-end de armazenamento**.

Remover um back-end de storage

Você pode remover um back-end de storage que não está mais em uso. Você pode querer fazer isso para manter sua configuração simples e atualizada.

Antes de começar

- Certifique-se de que o back-end de armazenamento não é gerenciado.
- Certifique-se de que o back-end de storage não tenha nenhum volume associado ao cluster.

Passos

1. Na navegação à esquerda, selecione **backends**.
2. Se o back-end for gerenciado, desfaça-o.
   a. Selecione **Managed**.
   b. Selecione o back-end de armazenamento.
   c. Na opção **ações**, selecione **Desgerenciar**.
   d. Digite "Unmanage" (Desgerenciar) para confirmar a ação.
   e. Selecione **Sim, desgerencie o back-end de armazenamento**.
3. Selecione **descoberto**.
   a. Selecione o back-end de armazenamento.
   b. Na opção **ações**, selecione **Remover**.
   c. Digite "remove" para confirmar a ação.
   d. Selecione **Sim, remova o back-end de armazenamento**.

Encontre mais informações

- "Use a API Astra Control"

Monitorar tarefas em execução

Você pode ver detalhes sobre tarefas e tarefas executadas que foram concluídas, falhadas ou canceladas nas últimas 24 horas no Astra Control. Por exemplo, você pode exibir o status de uma operação de backup, restauração ou clone em execução e ver detalhes como porcentagem concluída e tempo restante estimado. Você pode exibir o status de uma operação agendada que foi executada ou uma operação iniciada manualmente.

Ao exibir uma tarefa em execução ou concluída, você pode expandir os detalhes da tarefa para ver o status de cada uma das subtarefas. A barra de progresso da tarefa está verde para tarefas em curso ou concluídas, azul para tarefas canceladas e vermelha para tarefas que falharam devido a um erro.

Para operações de clone, as subtarefas consistem em uma operação de restauração de snapshot e snapshot.

Para ver mais informações sobre tarefas com falha, "Monitorar a atividade da conta"consulte .

Passos

1. Enquanto uma tarefa estiver em execução, vá para **aplicativos**.
2. Selecione o nome de uma aplicação na lista.
3. Nos detalhes do aplicativo, selecione a guia **tarefas**.

   Você pode exibir detalhes de tarefas atuais ou passadas e filtrar por estado da tarefa.

As tarefas são mantidas na lista **tarefas** por até 24 horas. Pode configurar este limite e outras definições do monitor de tarefas utilizando o "API Astra Control".

Monitore a infraestrutura com conexões Cloud Insights, Prometheus ou Fluentd

Você pode configurar várias configurações opcionais para aprimorar sua experiência com o Astra Control Center. Para monitorar e obter informações sobre sua infraestrutura completa, crie uma conexão com o NetApp Cloud Insights, configure Prometheus ou adicione uma conexão Fluentd.

Se a rede em que você está executando o Astra Control Center exigir um proxy para conexão à Internet (para carregar pacotes de suporte para o site de suporte da NetApp ou estabelecer uma conexão com o Cloud Insights), você deverá configurar um servidor proxy no Astra Control Center.

- Conete-se ao Cloud Insights
- Conete-se ao Prometheus
- Ligar ao Fluentd

Adicione um servidor proxy para conexões ao Cloud Insights ou ao site de suporte da NetApp

Se a rede em que você está executando o Astra Control Center exigir um proxy para conexão à Internet (para carregar pacotes de suporte para o site de suporte da NetApp ou estabelecer uma conexão com o Cloud Insights), você deverá configurar um servidor proxy no Astra Control Center.

O Astra Control Center não valida os detalhes inseridos para o servidor proxy. Certifique-se de que introduz os valores corretos.

Passos

1. Faça login no Astra Control Center usando uma conta com privilégio **admin**/**owner**.
2. Selecione **conta** > **conexões**.
3. Selecione **Connect** na lista suspensa para adicionar um servidor proxy.

4. Introduza o nome do servidor proxy ou o endereço IP e o número da porta proxy.
5. Se o servidor proxy exigir autenticação, marque a caixa de seleção e insira o nome de usuário e a senha.
6. Selecione **Connect**.

Resultado

Se as informações do proxy que você inseriu foram salvas, a seção **Proxy HTTP** da página **Account** > **Connections** indica que ela está conetada e exibe o nome do servidor.

Edite as configurações do servidor proxy

Você pode editar as configurações do servidor proxy.

Passos

1. Faça login no Astra Control Center usando uma conta com privilégio **admin**/**owner**.
2. Selecione **conta** > **conexões**.
3. Selecione **Editar** na lista suspensa para editar a conexão.
4. Edite os detalhes do servidor e as informações de autenticação.
5. Selecione **Guardar**.

Desative a conexão do servidor proxy

Você pode desativar a conexão do servidor proxy. Você será avisado antes de desativar que pode ocorrer uma possível interrupção para outras conexões.

Passos

1. Faça login no Astra Control Center usando uma conta com privilégio **admin**/**owner**.
2. Selecione **conta** > **conexões**.
3. Selecione **Disconnect** na lista pendente para desativar a ligação.
4. Na caixa de diálogo que se abre, confirme a operação.

Conete-se ao Cloud Insights

Para monitorar e ter insights sobre toda a sua infraestrutura, conecte o NetApp Cloud Insights à sua instância do Astra Control Center. O Cloud Insights está incluído na sua licença do Astra Control Center.

O Cloud Insights deve ser acessível a partir da rede que o Centro de Controle Astra usa, ou indiretamente, por meio de um servidor proxy.

Quando o Centro de Controle Astra está conetado ao Cloud Insights, um pod de unidade de aquisição é criado. Esse pod coleta dados dos back-ends de storage gerenciados pelo Astra Control Center e envia-los para o Cloud Insights. Este pod requer 8 GB de RAM e 2 núcleos de CPU.

Quando o Astra Control Center estiver emparelhado com o Cloud Insights, você não deve usar a opção **Modificar implantação** no Cloud Insights.

Depois de ativar a conexão Cloud Insights, você pode exibir informações de taxa de transferência na página **backends**, bem como se conetar ao Cloud Insights após selecionar um back-end de armazenamento. Você também pode encontrar as informações no **Painel** na seção Cluster e se conetar ao Cloud Insights a partir daí.

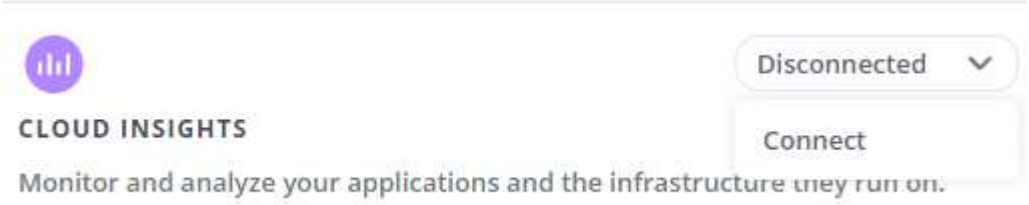
Antes de começar

- Uma conta do Centro de Controle Astra com **admin**/**owner** Privileges.
- Uma licença válida do Astra Control Center.
- Um servidor proxy se a rede onde você está executando o Astra Control Center exigir um proxy para conexão à Internet.

Se você é novo no Cloud Insights, familiarize-se com os recursos e capacidades. "Documentação do Cloud Insights"Consulte a .

Passos

1. Faça login no Astra Control Center usando uma conta com privilégio **admin**/**owner**.
2. Selecione **conta** > **conexões**.
3. Selecione **Connect** onde mostrar **Disconnected** na lista suspensa para adicionar a conexão.



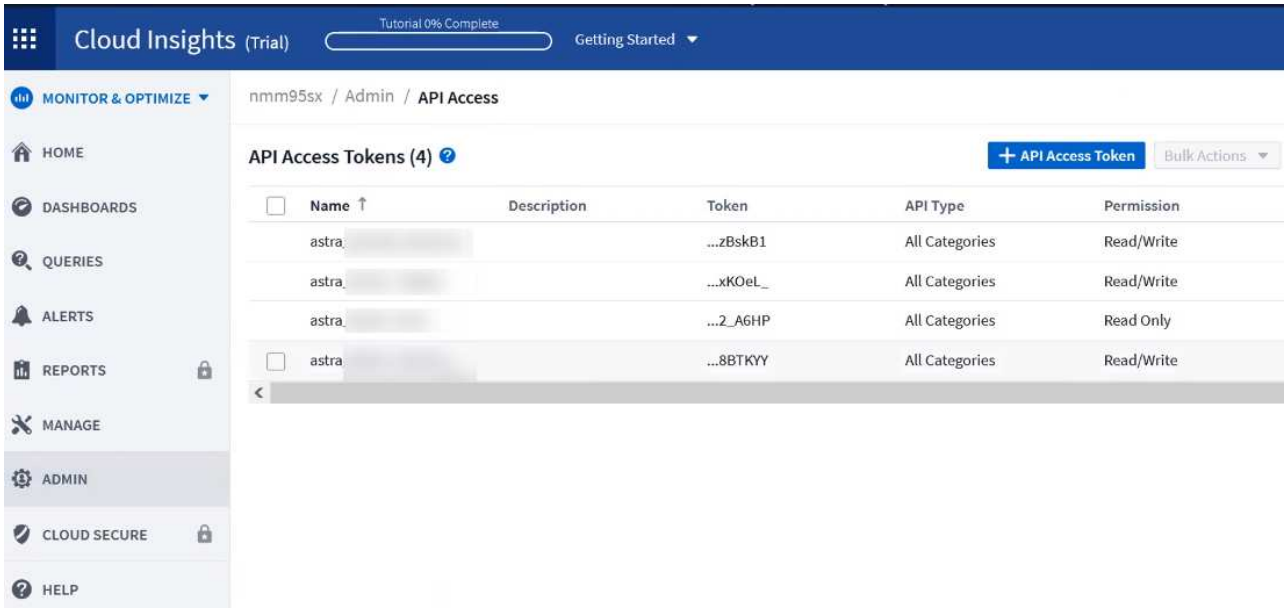
4. Insira os tokens da API do Cloud Insights e o URL do locatário. A URL do locatário tem o seguinte formato, como exemplo:

```
https://<environment-name>.c01.cloudinsights.netapp.com/
```

Você obtém o URL do locatário quando você recebe a licença do Cloud Insights. Se você não tiver o URL do locatário, consulte o "Documentação do Cloud Insights".

a. Para obter o "Token de API", faça login no URL de locatário do Cloud Insights.

b. No Cloud Insights, gere um token de acesso à API **Read/Write** e **Read Only** clicando em **Admin** > **API Access**.



c. Copie a tecla **somente leitura**. Você precisará colá-lo na janela Centro de Controle Astra para ativar a conexão Cloud Insights. Para obter as permissões de chave de token de acesso à API de leitura, selecione: Ativos, Alertas, Unidade de aquisição e coleta de dados.

d. Copie a tecla **Read/Write**. Você precisará colá-lo na janela do Centro de Controle Astra **Connect Cloud Insights**. Para obter as permissões de chave de token de acesso à API de leitura/gravação, selecione: Ingestão de dados, ingestão de log, Unidade de aquisição e coleta de dados.

> Recomendamos que você gere uma tecla **somente leitura** e uma tecla **leitura/gravação**, e não use a mesma chave para ambos os fins. Por padrão, o período de expiração do token é definido como um ano. Recomendamos que você mantenha a seleção padrão para dar ao token a duração máxima antes que ele expire. Se o token expirar, a telemetria parará.

e. Cole as chaves que você copiou do Cloud Insights para o Centro de Controle Astra.

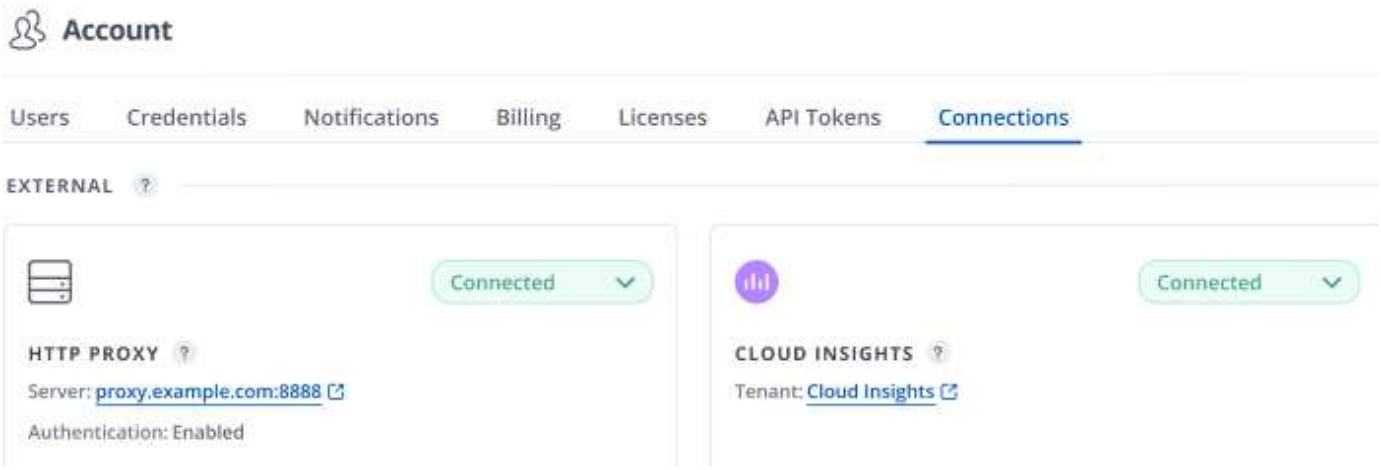
5. Selecione **Connect**.

> Depois de selecionar **conetar**, o status da conexão muda para **pendente** na seção **Cloud Insights** da página **conta** > **conexões**. Pode ser ativado alguns minutos para a ligação e o estado mudar para **Connected**.

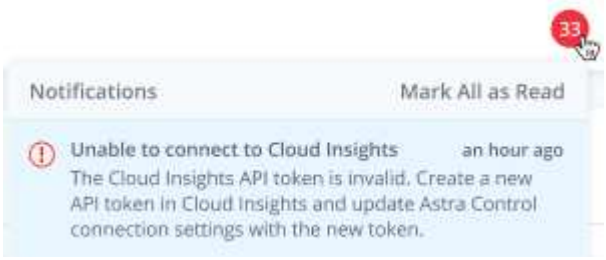
> Para ir e voltar facilmente entre o Centro de Controle Astra e as UIs do Cloud Insights, certifique-se de que você esteja conetado a ambos.

Exibir dados no Cloud Insights

Se a conexão foi bem-sucedida, a seção **Cloud Insights** da página **Account** > **Connections** indica que ela está conetada e exibe o URL do locatário. Você pode visitar o Cloud Insights para ver os dados sendo recebidos e exibidos com êxito.

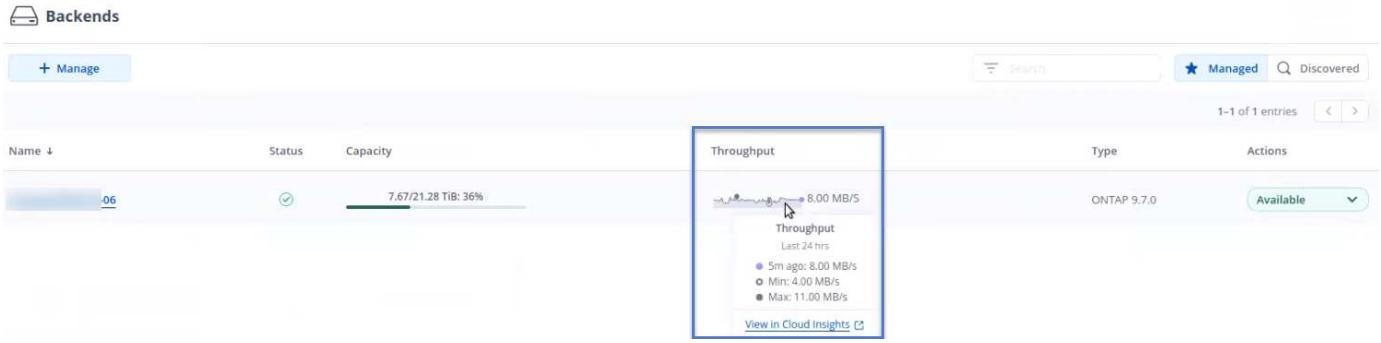


Se a conexão falhou por algum motivo, o status mostra **Failed**. Você pode encontrar o motivo da falha em **notificações** no lado superior direito da interface do usuário.



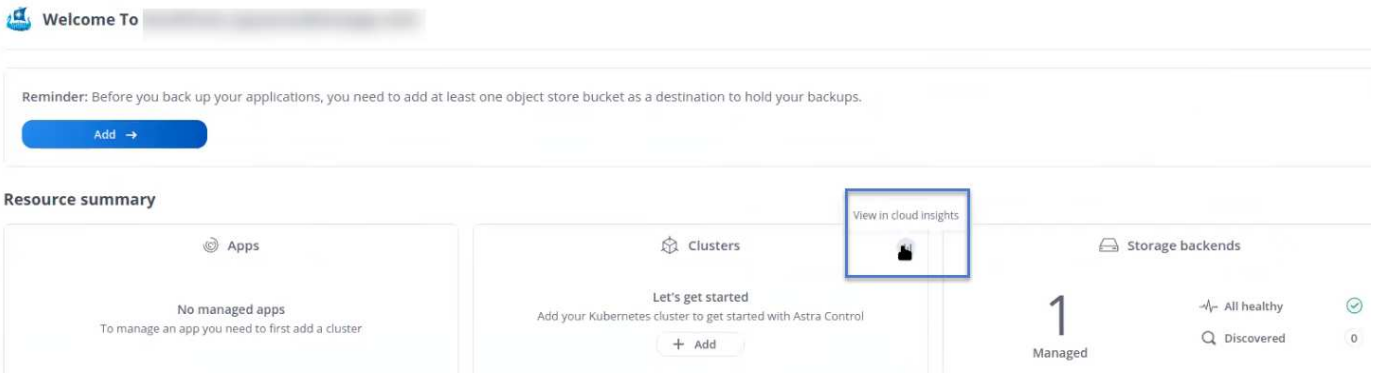
Você também pode encontrar as mesmas informações em **conta** > **notificações**.

A partir do Centro de Controle Astra, você pode visualizar informações de throughput na página **backends**, bem como se conetar ao Cloud Insights a partir daqui, depois de selecionar um back-end de armazenamento.



Para ir diretamente ao Cloud Insights, selecione o ícone **Cloud Insights** ao lado da imagem de métricas.

Você também pode encontrar as informações no **Dashboard**.



Depois de ativar a conexão Cloud Insights, se você remover os backends que adicionou no Centro de Controle Astra, os backends param de gerar relatórios para o Cloud Insights.

Editar ligação à Cloud Insights

Pode editar a ligação Cloud Insights.

Você só pode editar as chaves da API. Para alterar o URL de locatário do Cloud Insights, recomendamos que você desconete a conexão Cloud Insights e conete-se ao novo URL.

Passos

1. Faça login no Astra Control Center usando uma conta com privilégio **admin**/**owner**.
2. Selecione **conta** > **conexões**.
3. Selecione **Editar** na lista suspensa para editar a conexão.
4. Edite as definições de ligação Cloud Insights.
5. Selecione **Guardar**.

Desativar a ligação Cloud Insights

Você pode desativar a conexão Cloud Insights para um cluster Kubernetes gerenciado pelo Astra Control Center. A desativação da conexão Cloud Insights não exclui os dados de telemetria já carregados no Cloud Insights.

Passos

1. Faça login no Astra Control Center usando uma conta com privilégio **admin**/**owner**.
2. Selecione **conta** > **conexões**.
3. Selecione **Disconnect** na lista pendente para desativar a ligação.
4. Na caixa de diálogo que se abre, confirme a operação. Depois de confirmar a operação, na página **conta** > **conexões**, o status do Cloud Insights muda para **pendente**. Demora alguns minutos para que o status mude para **desconectada**.

Conete-se ao Prometheus

Você pode monitorar os dados do Astra Control Center com Prometheus. Você pode configurar o Prometheus para reunir métricas do endpoint de métricas do cluster do Kubernetes e usar o Prometheus também para visualizar os dados das métricas.

Para obter detalhes sobre como usar Prometheus, consulte sua documentação em "Começando com

Prometheus".

O que você vai precisar

Certifique-se de ter baixado e instalado o pacote Prometheus no cluster Astra Control Center ou em um cluster diferente que possa se comunicar com o cluster Astra Control Center.

Siga as instruções na documentação oficial para "Instale Prometheus".

Prometeu precisa ser capaz de se comunicar com o cluster do Kubernetes do Astra Control Center. Se Prometheus não estiver instalado no cluster Astra Control Center, você precisará garantir que eles possam se comunicar com o serviço de métricas em execução no cluster Astra Control Center.

Configure Prometheus

O Astra Control Center expõe um serviço de métricas na porta TCP 9090 no cluster Kubernetes. Você precisa configurar Prometheus para coletar métricas deste serviço.

Passos

1. Faça login no servidor Prometheus.
2. Adicione a entrada do cluster ao `prometheus.yml` arquivo. No `yml` arquivo, adicione uma entrada semelhante à seguinte para o cluster no `scrape_configs section`:

```
job_name: '<Add your cluster name here. You can abbreviate. It just
needs to be a unique name>'
  metrics_path: /accounts/<replace with your account ID>/metrics
  authorization:
     credentials: <replace with your API token>
  tls_config:
     insecure_skip_verify: true
  static_configs:
    - targets: ['<replace with your astraAddress. If using FQDN, the
prometheus server has to be able to resolve it>']
```

> Se você definir `tls_config insecure_skip_verify` como `true`, o protocolo de criptografia TLS não será necessário.

3. Reinicie o serviço Prometheus:

```
sudo systemctl restart prometheus
```

Acesse Prometheus

Acesse a URL Prometheus.

Passos

1. Em um navegador, insira o URL Prometheus com a porta 9090.

2. Verifique a sua ligação selecionando **Status** > **Targets**.

Ver dados em Prometheus

Você pode usar Prometheus para visualizar os dados do Astra Control Center.

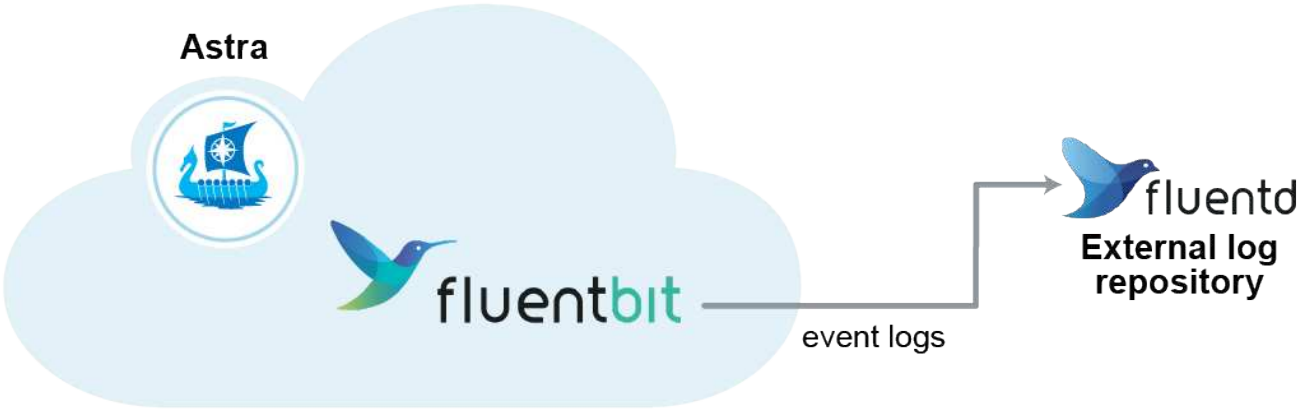
Passos

1. Em um navegador, insira o URL Prometheus.
2. No menu Prometheus, selecione **Graph**.
3. Para usar o Metrics Explorer, selecione o ícone ao lado de **execute**.
4. `scrape_samples_scraped`Selecione e selecione **Executar**.
5. Para ver a raspagem de amostra ao longo do tempo, selecione **Gráfico**.

Se vários dados de cluster foram coletados, as métricas de cada cluster aparecem em uma cor diferente.

Ligar ao Fluentd

Você pode enviar logs (eventos do Kubernetes) de um sistema monitorado pelo Astra Control Center para o seu ponto de extremidade do Fluentd. A ligação Fluentd está desativada por predefinição.



Somente os logs de eventos de clusters gerenciados são encaminhados para o Fluentd.

Antes de começar

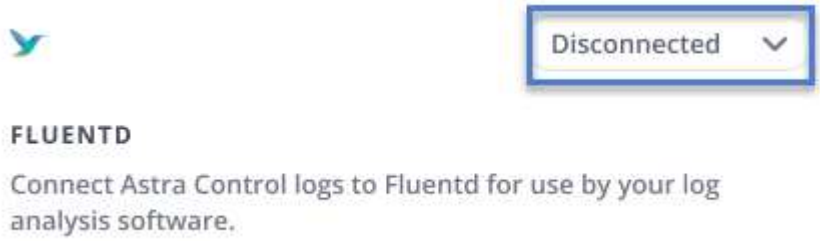
- Uma conta do Centro de Controle Astra com **admin**/**owner** Privileges.
- Astra Control Center instalado e executado em um cluster Kubernetes.

O Astra Control Center não valida os detalhes inseridos para o seu servidor Fluentd. Certifique-se de que introduz os valores corretos.

Passos

1. Faça login no Astra Control Center usando uma conta com privilégio **admin**/**owner**.
2. Selecione **conta** > **conexões**.

3. Selecione **Connect** na lista suspensa onde mostra **Disconnected** para adicionar a conexão.



4. Insira o endereço IP do host, o número da porta e a chave compartilhada para o servidor Fluentd.
5. Selecione **Connect**.

Resultado

Se os detalhes inseridos para o servidor Fluentd foram salvos, a seção **Fluentd** da página **Account** > **Connections** indica que ele está conetado. Agora você pode visitar o servidor Fluentd conetado e visualizar os logs de eventos.

Se a conexão falhou por algum motivo, o status mostra **Failed**. Você pode encontrar o motivo da falha em **notificações** no lado superior direito da interface do usuário.

Você também pode encontrar as mesmas informações em **conta** > **notificações**.

Se você estiver tendo problemas com a coleta de logs, faça login no nó de trabalho e verifique se os logs estão disponíveis no `/var/log/containers/`.

Edite a ligação Fluentd

Você pode editar a conexão Fluentd para sua instância do Astra Control Center.

Passos

1. Faça login no Astra Control Center usando uma conta com privilégio **admin**/**owner**.
2. Selecione **conta** > **conexões**.
3. Selecione **Editar** na lista suspensa para editar a conexão.
4. Altere as definições de ponto final Fluentd.
5. Selecione **Guardar**.

Desative a conexão Fluentd

Você pode desativar a conexão Fluentd com sua instância do Astra Control Center.

Passos

1. Faça login no Astra Control Center usando uma conta com privilégio **admin**/**owner**.
2. Selecione **conta** > **conexões**.
3. Selecione **Disconnect** na lista pendente para desativar a ligação.
4. Na caixa de diálogo que se abre, confirme a operação.

Desgerenciar aplicativos e clusters

Remova todas as aplicações ou clusters que você não deseja mais gerenciar do Astra Control Center.

Desgerenciar um aplicativo

Pare de gerenciar aplicações que não deseja mais fazer backup, snapshot ou clonar a partir do Astra Control Center.

Quando você desgerencia um aplicativo:

- Todos os backups e snapshots existentes serão excluídos.
- Aplicativos e dados permanecem disponíveis.

Passos

1. Na barra de navegação à esquerda, selecione **aplicações**.
2. Selecione a aplicação.
3. No menu Opções na coluna ações, selecione **Desgerenciar**.
4. Reveja as informações.
5. Digite "Unmanage" (Desgerenciar) para confirmar.
6. Selecione **Sim, desgerenciar o aplicativo**.

Resultado

O Astra Control Center deixa de gerenciar a aplicação.

Desgerenciar um cluster

Pare de gerenciar o cluster que não deseja mais gerenciar a partir do Astra Control Center.

Antes de desgerenciar o cluster, você deve desgerenciar os aplicativos associados ao cluster.

Quando você desgerencia um cluster:

- Essa ação impede que o cluster seja gerenciado pelo Astra Control Center. Ele não faz alterações na configuração do cluster e não exclui o cluster.
- O Astra Trident não será desinstalado do cluster. "Saiba como desinstalar o Astra Trident".

Passos

1. Na barra de navegação à esquerda, selecione **clusters**.
2. Marque a caixa de seleção do cluster que você não deseja mais gerenciar.
3. No menu Opções na coluna **ações**, selecione **Desgerenciar**.
4. Confirme se deseja desgerenciar o cluster e selecione **Sim, desgerenciar o cluster**.

Resultado

O status do cluster muda para **Remover**. Depois disso, o cluster será removido da página **clusters** e não será mais gerenciado pelo Astra Control Center.

Se o Centro de Controle Astra e o Cloud Insights não estiverem conetados, o desgerenciamento do cluster removerá todos os recursos instalados para o envio de dados de telemetria. **Se o Centro de Controle Astra e o Cloud Insights estiverem conetados**, o desgerenciamento do cluster excluirá somente os `fluentbit` pods e. `event-exporter`

Atualizar o Astra Control Center

Para atualizar o Astra Control Center, faça o download do pacote de instalação no site de suporte da NetApp e siga estas instruções. Você pode usar este procedimento para atualizar o Astra Control Center em ambientes conetados à Internet ou com conexão via rede.

Estas instruções descrevem o processo de atualização para o Astra Control Center da segunda versão mais recente para esta versão atual. Você não pode atualizar diretamente de uma versão que seja duas ou mais versões por trás da versão atual. Se a versão instalada do Astra Control Center for muitas versões atrás da versão mais recente, talvez seja necessário realizar atualizações em cadeia para versões mais recentes até que o Astra Control Center instalado esteja apenas uma versão atrás da versão mais recente. Para obter uma lista completa das versões lançadas, consulte "notas de lançamento".

Antes de começar

Antes de atualizar, certifique-se de que o seu ambiente ainda atende ao "Requisitos mínimos para implantação do Astra Control Center". Seu ambiente deve ter o seguinte:

- **"suportado"Versão Astra Trident**

  Expanda para obter passos

  Determine a versão do Trident que você está executando:

  ```
  kubectl get tridentversion -n trident
  ```

  Atualizar o Astra Trident, se necessário, usando "instruções" estes .

O lançamento de 23,10 é o último lançamento do Astra Control Center que será compatível com o Astra Trident. É altamente recomendável que você "Habilite o Astra Control Provisioner"acesse os recursos de gerenciamento avançado e provisionamento de storage além daqueles fornecidos pelo Astra Trident. Você precisa atualizar para o Astra Control Center 23,10 e habilitar o Astra Control Provisioner a usar essa funcionalidade estendida. O Astra Control Provisioner não funcionará com versões anteriores do Astra Control Center.

- **Uma distribuição do Kubernetes suportada**

Expanda para obter passos

Determine a versão do Kubernetes que você está executando:

```
kubectl get nodes -o wide
```

- **Recursos de cluster suficientes**

  Expanda para obter passos

  Determine os recursos disponíveis do cluster:

  ```
  kubectl describe node <node name>
  ```

- * Um Registro que você pode usar para enviar e carregar imagens do Astra Control Center*
- **Uma classe de armazenamento padrão**

  Expanda para obter passos

  Determine sua classe de armazenamento padrão:

  ```
  kubectl get storageclass
  ```

- **Serviços API saudáveis e disponíveis**

  Expanda para obter passos

  Certifique-se de que todos os serviços de API estão em um estado saudável e disponíveis:

  ```
  kubectl get apiservices
  ```

- **(apenas OpenShift) operadores de cluster saudáveis e disponíveis**

  Expanda para obter passos

  Certifique-se de que todos os operadores de cluster estão em um estado saudável e disponíveis.

  ```
  kubectl get clusteroperators
  ```

- **Acesse o Registro de imagem do NetApp Astra Control**: Você tem a opção de obter imagens de

instalação e melhorias de funcionalidade para o Astra Control, como o Astra Control Provisioner, a partir do Registro de imagens do NetApp.

Expanda para obter passos

a. Registre seu ID de conta Astra Control que você precisará fazer login no Registro.

   Você pode ver o ID da conta na IU da Web do Astra Control Service. Selecione o ícone de figura no canto superior direito da página, selecione **Acesso à API** e anote o ID da sua conta.

b. Na mesma página, selecione **Generate API token** e copie a cadeia de token da API para a área de transferência e salve-a no seu editor.

c. Faça login no Registro do Astra Control:

```
docker login cr.astra.netapp.io -u <account-id> -p <api-token>
```

Sobre esta tarefa

O processo de atualização do Astra Control Center orienta você pelas seguintes etapas de alto nível:

Saia da IU do Astra Control Center antes de iniciar a atualização.

- Faça download e extraia Astra Control Center
- Remova o plug-in NetApp Astra kubectl e instale-o novamente
- Adicione as imagens ao seu registo local
- Instale o operador Astra Control Center atualizado
- Atualizar o Astra Control Center
- Verifique o status do sistema

Não exclua o operador Astra Control Center (por exemplo, `kubectl delete -f astra_control_center_operator_deploy.yaml`) a qualquer momento durante a atualização ou operação do Astra Control Center para evitar a exclusão de pods.

Faça atualizações em uma janela de manutenção quando programações, backups e snapshots não estiverem sendo executados.

Faça download e extraia Astra Control Center

Você pode optar por baixar o pacote Astra Control Center do site de suporte da NetApp ou usar o Docker para extrair o pacote do Registro de imagem do serviço Astra Control.

Site de suporte da NetApp

1. Faça o download do pacote que contém o Astra Control Center (`astra-control-center-[version].tar.gz`) no "Página de downloads do Astra Control Center".
2. (Recomendado, mas opcional) Faça o download do pacote certificados e assinaturas para o Astra Control Center (`astra-control-center-certs-[version].tar.gz`) para verificar a assinatura do pacote.

   Expanda para obter detalhes

   ```
   tar -vxzf astra-control-center-certs-[version].tar.gz
   ```

   ```
   openssl dgst -sha256 -verify certs/AstraControlCenter-public.pub
   -signature certs/astra-control-center-[version].tar.gz.sig
   astra-control-center-[version].tar.gz
   ```

   A saída será `Verified OK` exibida após a verificação bem-sucedida.

3. Extraia as imagens do pacote Astra Control Center:

   ```
   tar -vxzf astra-control-center-[version].tar.gz
   ```

Registro de imagem Astra Control

1. Faça login no Astra Control Service.
2. No Dashboard, selecione **Deploy a self-managed instance of Astra Control**.
3. Siga as instruções para fazer login no Registro de imagens do Astra Control, extrair a imagem de instalação do Astra Control Center e extrair a imagem.

Remova o plug-in NetApp Astra kubectl e instale-o novamente

Você pode usar o plugin de linha de comando NetApp Astra kubectl para enviar imagens para um repositório local do Docker.

1. Determine se você tem o plug-in instalado:

   ```
   kubectl astra
   ```

2. Execute uma destas ações:
   - Se o plugin estiver instalado, o comando deve retornar a ajuda do plugin kubectl e você pode remover a versão existente do kubectl-astra: `delete /usr/local/bin/kubectl-astra`.
   - Se o comando retornar um erro, o plugin não está instalado e você pode prosseguir para a próxima

etapa para instalá-lo.

3. Instale o plugin:

   a. Liste os binários disponíveis do plug-in NetApp Astra kubectl e observe o nome do arquivo que você precisa para o seu sistema operacional e arquitetura de CPU:

      A biblioteca de plugins kubectl faz parte do pacote tar e é extraída para a pasta `kubectl-astra`.

```
ls kubectl-astra/
```

   a. Mova o binário correto para o caminho atual e renomeie-o para `kubectl-astra`:

```
cp kubectl-astra/<binary-name> /usr/local/bin/kubectl-astra
```

Adicione as imagens ao seu registo local

1. Complete a sequência de passos adequada para o seu motor de contentores:

Docker

1. Mude para o diretório raiz do tarball. Você deve ver o `acc.manifest.bundle.yaml` arquivo e estes diretórios:

   ```
   acc/
   kubectl-astra/
   acc.manifest.bundle.yaml
   ```

2. Envie as imagens do pacote no diretório de imagens do Astra Control Center para o Registro local. Faça as seguintes substituições antes de executar o `push-images` comando:

   - Substitua o <BUNDLE_FILE> pelo nome do arquivo do pacote Astra Control (`acc.manifest.bundle.yaml`).
   - Substitua o <MY_FULL_REGISTRY_PATH> pela URL do repositório Docker; por exemplo"<a href="https://<docker-registry>"" class="bare">https://<docker-registry>", .
   - Substitua o <MY_REGISTRY_USER> pelo nome de usuário.
   - Substitua o <MY_REGISTRY_TOKEN> por um token autorizado para o Registro.

     ```
     kubectl astra packages push-images -m <BUNDLE_FILE> -r
     <MY_FULL_REGISTRY_PATH> -u <MY_REGISTRY_USER> -p
     <MY_REGISTRY_TOKEN>
     ```

Podman

1. Mude para o diretório raiz do tarball. Você deve ver este arquivo e diretório:

   ```
   acc/
   kubectl-astra/
   acc.manifest.bundle.yaml
   ```

2. Inicie sessão no seu registo:

   ```
   podman login <YOUR_REGISTRY>
   ```

3. Prepare e execute um dos seguintes scripts personalizados para a versão do Podman que você usa. Substitua o <MY_FULL_REGISTRY_PATH> pela URL do seu repositório que inclui quaisquer subdiretórios.

   ```
   <strong>Podman 4</strong>
   ```

```
export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=23.10.0-68
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*/::')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done
```

```
<strong>Podman 3</strong>
```

```
export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=23.10.0-68
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*/::')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done
```

O caminho da imagem que o script cria deve ser semelhante ao seguinte, dependendo da configuração do Registro:

```
https://downloads.example.io/docker-astra-control-
prod/netapp/astra/acc/23.10.0-68/image:version
```

Instale o operador Astra Control Center atualizado

1. Altere o diretório:

```
cd manifests
```

2. Edite a implantação do operador Astra Control Center yaml)
(`astra_control_center_operator_deploy.yaml`para consultar o Registro local e o segredo.

```
vim astra_control_center_operator_deploy.yaml
```

   a. Se você usar um Registro que requer autenticação, substitua ou edite a linha padrão do `imagePullSecrets: []` com o seguinte:

```
imagePullSecrets: [{name: astra-registry-cred}]
```

   b. Altere `ASTRA_IMAGE_REGISTRY` para a `kube-rbac-proxy` imagem para o caminho do registo onde as imagens foram empurradas para um passo anterior.

   c. Altere `ASTRA_IMAGE_REGISTRY` para a `acc-operator` imagem para o caminho do registo onde as imagens foram empurradas para um passo anterior.

   d. Adicione os seguintes valores à `env` seção:

```
- name: ACCOP_HELM_UPGRADETIMEOUT
  value: 300m
```

Exemplo de astra_control_center_operator_deploy.yaml:

```
apiVersion: apps/v1
kind: Deployment
metadata:
  labels:
    control-plane: controller-manager
  name: acc-operator-controller-manager
  namespace: netapp-acc-operator
spec:
  replicas: 1
  selector:
    matchLabels:
      control-plane: controller-manager
  strategy:
    type: Recreate
  template:
    metadata:
      labels:
        control-plane: controller-manager
    spec:
      containers:
      - args:
        - --secure-listen-address=0.0.0.0:8443
        - --upstream=http://127.0.0.1:8080/
        - --logtostderr=true
        - --v=10
        image: ASTRA_IMAGE_REGISTRY/kube-rbac-proxy:v4.8.0
        name: kube-rbac-proxy
        ports:
        - containerPort: 8443
          name: https
      - args:
        - --health-probe-bind-address=:8081
        - --metrics-bind-address=127.0.0.1:8080
        - --leader-elect
        env:
        - name: ACCOP_LOG_LEVEL
          value: "2"
        - name: ACCOP_HELM_UPGRADETIMEOUT
          value: 300m
        image: ASTRA_IMAGE_REGISTRY/acc-operator:23.10.72
        imagePullPolicy: IfNotPresent
        livenessProbe:
          httpGet:
            path: /healthz
```

```
            port: 8081
          initialDelaySeconds: 15
          periodSeconds: 20
        name: manager
        readinessProbe:
          httpGet:
            path: /readyz
            port: 8081
          initialDelaySeconds: 5
          periodSeconds: 10
        resources:
          limits:
            cpu: 300m
            memory: 750Mi
          requests:
            cpu: 100m
            memory: 75Mi
        securityContext:
          allowPrivilegeEscalation: false
      imagePullSecrets: []
      securityContext:
        runAsUser: 65532
      terminationGracePeriodSeconds: 10
```

3. Instale o operador Astra Control Center atualizado:

```
kubectl apply -f astra_control_center_operator_deploy.yaml
```

Resposta da amostra:

```
namespace/netapp-acc-operator unchanged
customresourcedefinition.apiextensions.k8s.io/astracontrolcenters.as
tra.netapp.io configured
role.rbac.authorization.k8s.io/acc-operator-leader-election-role
unchanged
clusterrole.rbac.authorization.k8s.io/acc-operator-manager-role
configured
clusterrole.rbac.authorization.k8s.io/acc-operator-metrics-reader
unchanged
clusterrole.rbac.authorization.k8s.io/acc-operator-proxy-role
unchanged
rolebinding.rbac.authorization.k8s.io/acc-operator-leader-election-
rolebinding unchanged
clusterrolebinding.rbac.authorization.k8s.io/acc-operator-manager-
rolebinding configured
clusterrolebinding.rbac.authorization.k8s.io/acc-operator-proxy-
rolebinding unchanged
configmap/acc-operator-manager-config unchanged
service/acc-operator-controller-manager-metrics-service unchanged
deployment.apps/acc-operator-controller-manager configured
```

4. Verifique se os pods estão em execução:

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

Atualizar o Astra Control Center

1. Edite o recurso personalizado do Astra Control Center (CR):

```
kubectl edit AstraControlCenter -n [netapp-acc or custom namespace]
```

2. Altere o número da versão Astra (`astraVersion`dentro de `spec`) de `23.07.0` para `23.10.0`:

> Você não pode atualizar diretamente de uma versão que seja duas ou mais versões por trás da versão atual. Para obter uma lista completa das versões lançadas, consulte "notas de lançamento".

```
spec:
  accountName: "Example"
  astraVersion: "[Version number]"
```

3. Verifique se o caminho do Registro de imagens corresponde ao caminho do Registro para o qual você enviou as imagens em um passo anterior. Atualize `imageRegistry` dentro de `spec` se o Registro foi alterado desde sua última instalação.

```
  imageRegistry:
    name: "[your_registry_path]"
```

4. Adicione o seguinte à `crds` sua configuração dentro do `spec`:

```
crds:
  shouldUpgrade: true
```

5. Adicione as seguintes linhas dentro `additionalValues` do `spec` no Astra Control Center CR:

```
additionalValues:
    nautilus:
      startupProbe:
        periodSeconds: 30
        failureThreshold: 600
    keycloak-operator:
      livenessProbe:
        initialDelaySeconds: 180
      readinessProbe:
        initialDelaySeconds: 180
```

6. Salve e saia do editor de arquivos. As alterações serão aplicadas e a atualização começará.
7. (Opcional) Verifique se os pods terminam e ficam disponíveis novamente:

```
watch kubectl get pods -n [netapp-acc or custom namespace]
```

8. Aguarde que as condições de status do Astra Control indiquem que a atualização está concluída e pronta (`True`):

```
kubectl get AstraControlCenter -n [netapp-acc or custom namespace]
```

Resposta:

```
NAME    UUID                                   VERSION     ADDRESS
READY
astra   9aa5fdae-4214-4cb7-9976-5d8b4c0ce27f   23.10.0-68
10.111.111.111  True
```

Para monitorar o status de atualização durante a operação, execute o seguinte comando: `kubectl get AstraControlCenter -o yaml -n [netapp-acc or custom namespace]`

Para inspecionar os logs do operador do Centro de Controle Astra, execute o seguinte comando: `kubectl logs deploy/acc-operator-controller-manager -n netapp-acc-operator -c manager -f`

Verifique o status do sistema

1. Faça login no Astra Control Center.
2. Verifique se a versão foi atualizada. Consulte a página **suporte** na IU.
3. Verifique se todos os clusters e aplicativos gerenciados ainda estão presentes e protegidos.

Habilite o Astra Control Provisioner

O Astra Trident versões 23,10 e posteriores incluem a opção de usar o Astra Control Provisioner, que permite que usuários licenciados do Astra Control acessem o recurso avançado de provisionamento de storage. O Astra Control Provisioner fornece essa funcionalidade estendida, além da funcionalidade padrão baseada em CSI Astra Trident.

Nas próximas atualizações do Astra Control, o parceiro Astra Control substituirá o Astra Trident como provisionador de storage e orquestrador na arquitetura Astra Control. Por isso, é altamente recomendável que os usuários do Astra Control habilitem o Astra Control Provisioner. O Astra Trident continuará a ser de código aberto e será lançado, mantido, suportado e atualizado com o novo CSI e outros recursos do NetApp.

Sobre esta tarefa

Você deve seguir este procedimento se você for um usuário licenciado do Astra Control Center e estiver procurando usar a funcionalidade Astra Control Provisioner. Você também deve seguir este procedimento se você for um usuário do Astra Trident e quiser usar a funcionalidade adicional que o Astra Control Provisioner fornece sem usar também o Astra Control.

Para cada caso, a funcionalidade de provisionador não é habilitada por padrão no Astra Trident 23,10, mas pode ser habilitada usando esse processo.

Antes de começar

Se você estiver habilitando o Astra Control Provisioner, faça o seguinte primeiro:

Astra Control visioners usuários com o Astra Control Center

- **Obter uma licença do Astra Control Center**: Você precisará de um "Licença do Astra Control Center" para habilitar o Astra Control Provisioner e acessar a funcionalidade que ele oferece.
- **Instalar ou atualizar para o Astra Control Center 23,10**: Você precisará desta versão se estiver planejando usar o Astra Control Provisioner com o Astra Control.
- **Confirme que seu cluster tem uma arquitetura de sistema AMD64**: A imagem Astra Control Provisioner é fornecida em arquiteturas de CPU AMD64 e ARM64, mas apenas AMD64 é compatível com o Astra Control Center.
- **Obtenha uma conta do Serviço Astra Control para acesso ao Registro**: Se você pretende usar o Registro Astra Control em vez do site de suporte da NetApp para fazer o download da imagem do programa Astra Control, preencha o Registro para um "Conta do Astra Control Service". após concluir e enviar o formulário e criar uma conta do BlueXP , você receberá um e-mail de boas-vindas do Serviço Astra Control.
- **Se você tiver o Astra Trident instalado, confirme que sua versão está dentro de uma janela de quatro versões**: Você pode fazer uma atualização direta para o Astra Trident 23,10 com o Astra Control Provisioner se o seu Astra Trident estiver dentro de uma janela de quatro versões da versão 23,10. Por exemplo, você pode fazer o upgrade diretamente do Astra Trident 22,10 para o 23,10.

Apenas usuários do Astra Control Provisioner

- **Obter uma licença do Astra Control Center**: Você precisará de um "Licença do Astra Control Center" para habilitar o Astra Control Provisioner e acessar a funcionalidade que ele oferece.
- **Se você tiver o Astra Trident instalado, confirme que sua versão está dentro de uma janela de quatro versões**: Você pode fazer uma atualização direta para o Astra Trident 23,10 com o Astra Control Provisioner se o seu Astra Trident estiver dentro de uma janela de quatro versões da versão 23,10. Por exemplo, você pode fazer o upgrade diretamente do Astra Trident 22,10 para o 23,10.
- **Obtenha uma conta do Astra Control Service para acesso ao Registro**: Você precisará de acesso ao Registro para baixar imagens do Astra Control Provisioner. Para começar, preencha o Registro para um "Conta do Astra Control Service". depois de preencher e enviar o formulário e criar uma conta do BlueXP , você receberá um e-mail de boas-vindas do Serviço Astra Control.

(Passo 1) Faça o download e extraia Astra Control Provisioner

Os usuários do Centro de Controle Astra podem baixar a imagem usando o site de suporte da NetApp ou o método de Registro Astra Control. Os usuários do Astra Trident que desejam usar o Astra Control Provisioner sem o Astra Control devem usar o método de Registro.

(Opção) Site de suporte da NetApp

1. Faça o download do pacote Astra Control Provisioner (`trident-acp-[version].tar`) no "Página de downloads do Astra Control Center".
2. (Recomendado, mas opcional) Faça o download do pacote de certificados e assinaturas para o Centro de Controle Astra (astra-control-center-certs-[version].tar.gz) para verificar a assinatura do pacote tar Trident-acp-[version].

Expanda para obter detalhes

```
tar -vxzf astra-control-center-certs-[version].tar.gz
```

```
openssl dgst -sha256 -verify certs/AstraControlCenterDockerImages-public.pub -signature certs/trident-acp-[version].tar.sig trident-acp-[version].tar
```

3. Carregue a imagem do Astra Control Provisioner:

```
docker load < trident-acp-23.10.0.tar
```

Resposta:

```
Loaded image: trident-acp:23.10.0-linux-amd64
```

4. Marque a imagem:

```
docker tag trident-acp:23.10.0-linux-amd64 <my_custom_registry>/trident-acp:23.10.0
```

5. Envie a imagem para o seu registo personalizado:

```
docker push <my_custom_registry>/trident-acp:23.10.0
```

(Opção) Registro de imagem Astra Control

Você pode usar Podman em vez de Docker para os comandos neste procedimento. Se você estiver usando um ambiente Windows, o PowerShell é recomendado.

1. Acesse o Registro de imagem do NetApp Astra Control:
   a. Faça logon na IU da Web do Astra Control Service e selecione o ícone de figura no canto superior direito da página.
   b. Selecione **Acesso à API**.
   c. Anote o seu ID de conta.
   d. Na mesma página, selecione **Generate API token** e copie a cadeia de token da API para a área de transferência e salve-a no seu editor.
   e. Faça login no Registro Astra Control usando seu método preferido:

```
docker login cr.astra.netapp.io -u <account-id> -p <api-token>
```

```
crane auth login cr.astra.netapp.io -u <account-id> -p <api-token>
```

2. Se você tiver um Registro personalizado, siga estas etapas para o método preferido para mover a imagem para o Registro personalizado. Se você não estiver usando um Registro, siga as etapas do operador Trident no "próxima seção".

> Você pode usar Podman em vez de Docker para os seguintes comandos. Se você estiver usando um ambiente Windows, o PowerShell é recomendado.

Docker

a. Extraia a imagem Astra Control Provisioner do Registro:

> A imagem puxada não suportará múltiplas plataformas e só suportará a mesma plataforma que o host que puxou a imagem, como o Linux AMD64.

```
docker pull cr.astra.netapp.io/astra/trident-acp:23.10.0
--platform <cluster platform>
```

Exemplo:

```
docker pull cr.astra.netapp.io/astra/trident-acp:23.10.0
--platform linux/amd64
```

b. Marque a imagem:

```
docker tag cr.astra.netapp.io/astra/trident-acp:23.10.0
<my_custom_registry>/trident-acp:23.10.0
```

c. Envie a imagem para o seu registo personalizado:

```
docker push <my_custom_registry>/trident-acp:23.10.0
```

Grua

a. Copie o manifesto Astra Control Provisioner para o seu Registro personalizado:

```
crane copy cr.astra.netapp.io/astra/trident-acp:23.10.0
<my_custom_registry>/trident-acp:23.10.0
```

(Etapa 2) ative o Astra Control Provisioner no Astra Trident

Determine se o método de instalação original usou um e conclua as etapas apropriadas de acordo com o método original.

> Não use o Helm para ativar o Astra Control Provisioner. Se você usou o Helm para a instalação original e está atualizando para o 23,10, precisará usar o operador Trident ou o tridentctl para executar a habilitação do Provisioner do Astra Control.

Operador do Astra Trident

1. "Baixe o instalador do Astra Trident e extraia-o.".
2. Siga estas etapas se você ainda não tiver instalado o Astra Trident ou se tiver removido o operador da sua implantação original do Astra Trident:
   a. Crie o CRD:

```
kubectl create -f
deploy/crds/trident.netapp.io_tridentorchestrators_crd_post1.16.y
aml
```

   b. Crie o namespace Trident (`kubectl create namespace trident`) ou confirme se o namespace Trident ainda existe (`kubectl get all -n trident`). Se o namespace tiver sido removido, crie-o novamente.
3. Atualize o Astra Trident para 23.10.0:

> Para clusters que executam o Kubernetes 1,24 ou anterior, `bundle_pre_1_25.yaml` use o . Para clusters que executam o Kubernetes 1,25 ou posterior, `bundle_post_1_25.yaml` use o .

```
kubectl -n trident apply -f trident-installer-
23.10.0/deploy/<bundle-name.yaml>
```

4. Verifique se o Astra Trident está em execução:

```
kubectl get torc -n trident
```

   Resposta:

```
NAME      AGE
trident   21m
```

5. se você tem um Registro que usa segredos, crie um segredo para usar para puxar a imagem Astra Control Provisioner:

```
kubectl create secret docker-registry <secret_name> -n trident
--docker-server=<my_custom_registry> --docker-username=<username>
--docker-password=<token>
```

6. Edite o TridentOrchestrator CR e faça as seguintes edições:

```
kubectl edit torc trident -n trident
```

a. Defina um local de Registro personalizado para a imagem Astra Trident ou extraia-a do Registro Astra Control (`tridentImage: <my_custom_registry>/trident:23.10.0`ou `tridentImage: netapp/trident:23.10.0`).

b. Ative o Astra Control Provisioner (`enableACP: true`).

c. Defina o local de Registro personalizado para a imagem Astra Control Provisioner ou extraia-a do Registro Astra Control (`acpImage: <my_custom_registry>/trident-acp:23.10.0`ou `acpImage: cr.astra.netapp.io/astra/trident-acp:23.10.0`).

d. Se tiver estabelecido a imagem puxa segredos anteriormente neste procedimento, pode defini-los aqui (`imagePullSecrets: - <secret_name>`). Use o mesmo nome secreto que você estabeleceu nas etapas anteriores.

```
apiVersion: trident.netapp.io/v1
kind: TridentOrchestrator
metadata:
  name: trident
spec:
  debug: true
  namespace: trident
  tridentImage: <registry>/trident:23.10.0
  enableACP: true
  acpImage: <registry>/trident-acp:23.10.0
  imagePullSecrets:
  - <secret_name>
```

7. Salve e saia do arquivo. O processo de implantação começará automaticamente.
8. Verifique se o operador, a implantação e as replicasets são criados.

```
kubectl get all -n trident
```

Deve haver apenas **uma instância** do operador em um cluster do Kubernetes. Não crie várias implantações do operador Astra Trident.

9. Verifique se o `trident-acp` contentor está em execução e se `acpVersion` está `23.10.0` com um status de `Installed`:

```
kubectl get torc -o yaml
```

Resposta:

```
status:
  acpVersion: 23.10.0
  currentInstallationParams:
    ...
    acpImage: <registry>/trident-acp:23.10.0
    enableACP: "true"
    ...
  ...
  status: Installed
```

tridentctl

1. "Baixe o instalador do Astra Trident e extraia-o.".
2. "Se você tiver um Astra Trident existente, desinstale-o do cluster que o hospeda".
3. Instalar o Astra Trident com a previsão de controle Astra ativada (`--enable-acp=true`):

```
./tridentctl -n trident install --enable-acp=true --acp
-image=mycustomregistry/trident-acp:23.10
```

4. Confirme se o Astra Control Provisioner foi ativado:

```
./tridentctl -n trident version
```

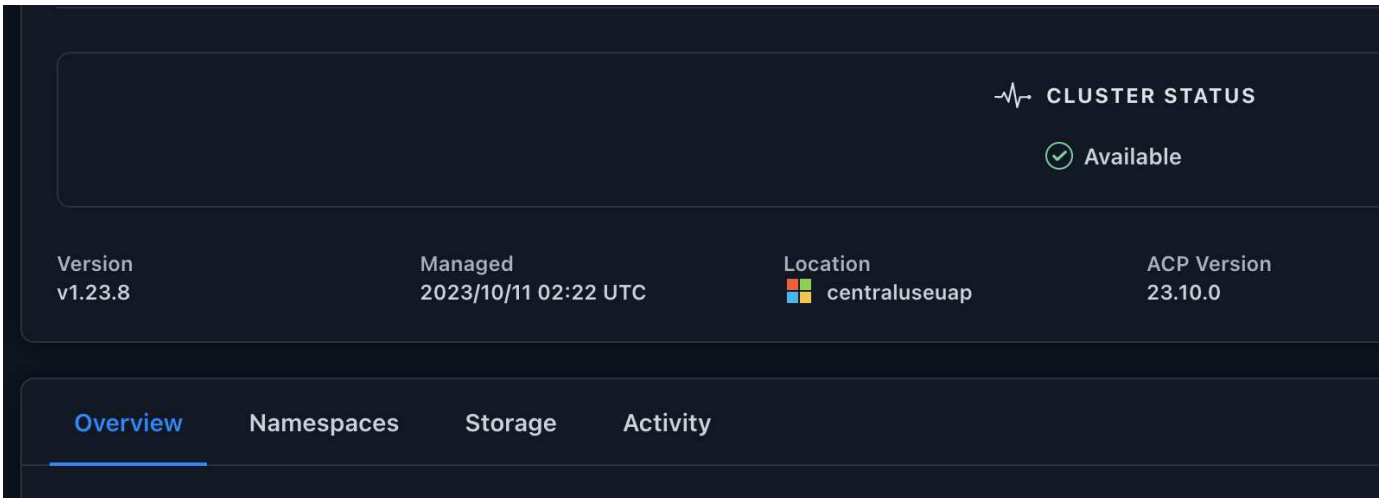
Resposta:

```
+----------------+----------------+-------------+ | SERVER VERSION |
CLIENT VERSION | ACP VERSION | +----------------+----------------
+-------------+ | 23.10.0 | 23.10.0 | 23.10.0. | +----------------
+----------------+-------------+
```

Resultado

A funcionalidade Astra Control Provisioner está ativada e você pode usar todos os recursos disponíveis para a versão em execução.

(Somente para usuários do Astra Control Center) após a instalação do Astra Control Provisioner, o cluster que hospeda o provisionador na IU do Astra Control Center mostrará um `ACP version` número de versão instalado em vez `Trident version` de campo e atual.



Para mais informações

- "O Astra Trident atualiza a documentação"

Desinstale o Astra Control Center

Talvez seja necessário remover componentes do Astra Control Center se você estiver atualizando de uma versão de avaliação para uma versão completa do produto. Para remover o Centro de Controle Astra e o Operador do Centro de Controle Astra, execute os comandos descritos neste procedimento em sequência.

Se tiver algum problema com a desinstalação, Solução de problemas de desinstalaçãoconsulte .

Antes de começar

1. "Desgerenciar todos os aplicativos" nos clusters.
2. "Desgerenciar todos os clusters".

Passos

1. Excluir Astra Control Center. O seguinte comando de exemplo é baseado em uma instalação padrão. Modifique o comando se você fez configurações personalizadas.

   ```
   kubectl delete -f astra_control_center.yaml -n netapp-acc
   ```

   Resultado:

   ```
   astracontrolcenter.astra.netapp.io "astra" deleted
   ```

2. Use o seguinte comando para excluir o `netapp-acc` namespace (ou nome personalizado):

   ```
   kubectl delete ns [netapp-acc or custom namespace]
   ```

   Resultado de exemplo:

```
namespace "netapp-acc" deleted
```

3. Use o seguinte comando para excluir componentes do sistema do operador Astra Control Center:

```
kubectl delete -f astra_control_center_operator_deploy.yaml
```

Resultado:

```
namespace/netapp-acc-operator deleted
customresourcedefinition.apiextensions.k8s.io/astracontrolcenters.astra.
netapp.io deleted
role.rbac.authorization.k8s.io/acc-operator-leader-election-role deleted
clusterrole.rbac.authorization.k8s.io/acc-operator-manager-role deleted
clusterrole.rbac.authorization.k8s.io/acc-operator-metrics-reader
deleted
clusterrole.rbac.authorization.k8s.io/acc-operator-proxy-role deleted
rolebinding.rbac.authorization.k8s.io/acc-operator-leader-election-
rolebinding deleted
clusterrolebinding.rbac.authorization.k8s.io/acc-operator-manager-
rolebinding deleted
clusterrolebinding.rbac.authorization.k8s.io/acc-operator-proxy-
rolebinding deleted
configmap/acc-operator-manager-config deleted
service/acc-operator-controller-manager-metrics-service deleted
deployment.apps/acc-operator-controller-manager deleted
```

Solução de problemas de desinstalação

Use as soluções alternativas a seguir para resolver quaisquer problemas que você tenha com a desinstalação do Astra Control Center.

A desinstalação do Astra Control Center não consegue limpar o pod do operador de monitoramento no cluster gerenciado

Se você não desgerenciou os clusters antes de desinstalar o Astra Control Center, poderá excluir manualmente os pods no namespace NetApp-monitoring e no namespace com os seguintes comandos:

Passos

1. Eliminar `acc-monitoring` agente:

```
kubectl delete agents acc-monitoring -n netapp-monitoring
```

Resultado:

```
agent.monitoring.netapp.com "acc-monitoring" deleted
```

2. Excluir o namespace:

```
kubectl delete ns netapp-monitoring
```

Resultado:

```
namespace "netapp-monitoring" deleted
```

3. Confirmar recursos removidos:

```
kubectl get pods -n netapp-monitoring
```

Resultado:

```
No resources found in netapp-monitoring namespace.
```

4. Confirmar o agente de monitoramento removido:

```
kubectl get crd|grep agent
```

Resultado da amostra:

```
agents.monitoring.netapp.com                    2021-07-21T06:08:13Z
```

5. Excluir informações de definição de recursos personalizados (CRD):

```
kubectl delete crds agents.monitoring.netapp.com
```

Resultado:

```
customresourcedefinition.apiextensions.k8s.io
"agents.monitoring.netapp.com" deleted
```

A desinstalação do Astra Control Center não consegue limpar CRDs do Traefik

Você pode excluir manualmente as CRDs do Traefik. CRDs são recursos globais e excluí-los pode afetar outros aplicativos no cluster.

Passos

1. Listar CRDs Traefik instalados no cluster:

```
kubectl get crds |grep -E 'traefik'
```

Resposta

```
ingressroutes.traefik.containo.us             2021-06-23T23:29:11Z
ingressroutetcps.traefik.containo.us          2021-06-23T23:29:11Z
ingressrouteudps.traefik.containo.us          2021-06-23T23:29:12Z
middlewares.traefik.containo.us               2021-06-23T23:29:12Z
middlewaretcps.traefik.containo.us            2021-06-23T23:29:12Z
serverstransports.traefik.containo.us         2021-06-23T23:29:13Z
tlsoptions.traefik.containo.us                2021-06-23T23:29:13Z
tlsstores.traefik.containo.us                 2021-06-23T23:29:14Z
traefikservices.traefik.containo.us           2021-06-23T23:29:15Z
```

2. Eliminar as CRDs:

```
kubectl delete crd ingressroutes.traefik.containo.us
ingressroutetcps.traefik.containo.us
ingressrouteudps.traefik.containo.us middlewares.traefik.containo.us
serverstransports.traefik.containo.us tlsoptions.traefik.containo.us
tlsstores.traefik.containo.us traefikservices.traefik.containo.us
middlewaretcps.traefik.containo.us
```

Encontre mais informações

- "Problemas conhecidos para desinstalar"

Informações sobre direitos autorais

Informações sobre marcas comerciais