Conceitos

Astra Control Center

NetApp
August 11, 2025

Índice

Conceitos

Arquitetura e componentes

O Astra Control é uma solução de gerenciamento do ciclo de vida de dados de aplicativos Kubernetes que simplifica as operações para aplicativos com estado e ajuda você a armazenar, proteger e mover suas cargas de trabalho do Kubernetes entre ambientes híbridos.

Recursos

O Astra Control oferece funcionalidades essenciais para o gerenciamento do ciclo de vida dos dados da aplicação Kubernetes:

Loja:

- Provisionamento de storage dinâmico para workloads em contêineres
- Criptografia em trânsito de dados do contêiner para volumes persistentes
- Replicação entre regiões, entre zonas
- Proteger*:
- Detecção automatizada e proteção com reconhecimento de aplicações de toda uma aplicação e seus dados
- Recuperação instantânea de um aplicativo a partir de qualquer versão de snapshot com base nas necessidades da sua organização
- Failover rápido em zonas, regiões e fornecedores de nuvem

Mover:

- Mobilidade de dados e aplicações entre clusters do Kubernetes e nuvens
- Clones instantâneos de aplicações e dados inteiros
- Migração de aplicativos com um clique por meio de IU e API consistentes da Web

Arquitetura

A arquitetura do Astra Control permite que a TI forneça recursos avançados de gerenciamento de dados que aprimoram o recurso e a disponibilidade das aplicações Kubernetes, simplifica o gerenciamento, a proteção e a movimentação de workloads em contêineres entre nuvens públicas e ambientes locais, além de fornecer recursos de automação por meio de sua API REST e SDK, permitindo acesso programático para integração aprimorada com workflows existentes.

O Astra Control é nativo em Kubernetes, permitindo workflows de proteção de dados que utilizam recursos personalizados e, ao mesmo tempo, permanecem compatíveis com a API e o SDK existentes. A proteção de dados nativa do Kubernetes oferece vantagens significativas. Ao integrar de forma otimizada às APIs e aos recursos do Kubernetes, a proteção de dados pode se tornar uma parte inerente do ciclo de vida do aplicativo por meio das ferramentas existentes de CI/CD e/ou GitOps de uma organização.

O Astra Control foi desenvolvido com base em quatro componentes complementares:

- **Astra Control**: O Astra Control é o serviço de gerenciamento centralizado para todos os clusters gerenciados, fornecendo cargas de trabalho orquestradas para proteção e mobilidade de aplicativos locais, bem como os seguintes recursos:
  - Visão combinada de vários clusters
  - Proteção de fluxos de trabalho orquestrados
  - Visualização e seleção granular de recursos
- **Astra Connector**: O Astra Connector combina com o Astra Control para fornecer uma conexão segura a cada cluster gerenciado, oferecendo execução local de operações agendadas independentemente do status da conexão, bem como as seguintes funcionalidades:
  - Execução local de operações agendadas independentemente do status da conexão
  - Operações locais que distribuem e otimizam o uso de recursos do sistema do Astra entre clusters
  - Instalação local que permite o menor acesso de privilégios ao cluster para maior segurança
- **Astra Control Provisioner**: O Astra Control Provisioner oferece a funcionalidade de provisionamento de CSI básico e recursos avançados de gerenciamento de storage para configuração adicional de segurança e recuperação de desastres, bem como os seguintes recursos:
  - Provisionamento de storage dinâmico para workloads em contêineres
  - Gerenciamento avançado de storage:
    - Criptografia em trânsito de dados do contêiner para o PV
    - Funcionalidade de nuvem SnapMirror com replicação entre regiões e entre zonas
- **Recursos personalizados do Astra**: Os recursos personalizados usados em cada cluster fornecem uma abordagem nativa do Kubernetes para executar operações localmente, simplificando a integração com outras ferramentas e automação compatíveis com o Kubernetes, além de fornecer os seguintes recursos:
  - Workflows de automação e integração direta de ferramentas de ecossistema
  - Primitivas de nível inferior que permitem fluxos de trabalho personalizados

Modelos de implantação

O Astra Control está disponível em um único modelo de implantação.

Astra Control Center: Software autogerenciado que oferece gerenciamento de dados com reconhecimento de aplicações dos clusters Kubernetes executados em seu ambiente local. O Astra Control Center também pode ser instalado em vários ambientes de fornecedor de nuvem com um back-end de storage da NetApp Cloud Volumes ONTAP.

"Documentação do Astra Control Center"

	Astra Control Center
Como é oferecido?	Como software que você pode baixar, instalar e gerenciar
Onde está hospedado?	No seu próprio cluster Kubernetes
Como é atualizado?	Você gerencia quaisquer atualizações

	Astra Control Center
Quais são as distribuições compatíveis do Kubernetes?	• Serviço Kubernetes do Azure no Azure Stack HCI • Google Anthos • Kubernetes (upstream) • Rancher Kubernetes Engine (RKE) • Red Hat OpenShift Container Platform
Quais são os backends de armazenamento suportados?	• Sistemas NetApp ONTAP AFF e FAS • NetApp ONTAP Select • "Cloud Volumes ONTAP" • "Longhorn"

Para mais informações

- "Documentação do Astra Control Center"
- "Documentação do Astra Trident"
- "API Astra Control"
- "Documentação do Cloud Insights"
- "Documentação do ONTAP"

Proteção de dados

Saiba mais sobre os tipos de proteção de dados disponíveis no Astra Control Center e a melhor forma de usá-los para proteger suas aplicações.

Snapshots, backups e políticas de proteção

Os snapshots e os backups protegem os seguintes tipos de dados:

- A aplicação em si
- Volumes de dados persistentes associados à aplicação
- Quaisquer artefactos de recurso pertencentes à aplicação

Um *snapshot* é uma cópia pontual de um aplicativo que é armazenado no mesmo volume provisionado que o aplicativo. Eles geralmente são rápidos. Você pode usar snapshots locais para restaurar o aplicativo para um ponto anterior no tempo. Os snapshots são úteis para clones rápidos. Os snapshots incluem todos os objetos Kubernetes da aplicação, incluindo arquivos de configuração. Os snapshots são úteis para clonar ou restaurar um aplicativo no mesmo cluster.

Um *backup* é baseado em um snapshot. Ele é armazenado no armazenamento de objetos externo e, por causa disso, pode ser mais lento de tirar em comparação com snapshots locais. Você pode restaurar um backup de aplicativo para o mesmo cluster ou pode migrar um aplicativo restaurando seu backup para um cluster diferente. Você também pode escolher um período de retenção mais longo para backups. Como eles são armazenados no armazenamento de objetos externo, os backups geralmente oferecem melhor proteção do que os snapshots em casos de falha de servidor ou perda de dados.

Uma *política de proteção* é uma maneira de proteger um aplicativo criando automaticamente snapshots, backups ou ambos de acordo com uma programação que você define para esse aplicativo. Uma política de proteção também permite escolher quantos snapshots e backups devem ser mantidos na programação e definir diferentes níveis de granularidade do agendamento. Automatizar seus backups e snapshots com uma política de proteção é a melhor maneira de garantir que cada aplicativo seja protegido de acordo com as necessidades de sua organização e requisitos de SLA (Service Level Agreement).

> *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 associado, então você precisa de um backup para recuperar. Um instantâneo não permitiria que você se recuperasse.

Backups imutáveis

Um backup imutável é um backup que não pode ser alterado ou excluído durante um período especificado. Quando você cria um backup imutável, o Astra Control verifica para garantir que o bucket que você está usando seja um bucket do WORM (write once read many) e, nesse caso, garante que o backup seja imutável a partir do Astra Control. O Astra Control Center dá suporte à criação de backups imutáveis com as seguintes plataformas e tipos de bucket:

- Amazon Web Services usando um bucket do Amazon S3 com o bloqueio de objetos S3 configurado
- NetApp StorageGRID usando um bucket S3 com bloqueio de objeto S3 configurado

Observe o seguinte ao trabalhar com backups imutáveis:

- Se você fizer backup em um bucket do WORM em uma plataforma não suportada ou em um tipo de bucket não suportado, poderá obter resultados imprevisíveis, como falha na exclusão de backup, mesmo que o tempo de retenção tenha decorrido.
- O Astra Control não é compatível com políticas de gerenciamento de ciclo de vida dos dados nem com a exclusão manual de objetos nos buckets que você usa com backups imutáveis. Verifique se o back-end de storage não está configurado para gerenciar o ciclo de vida dos snapshots do Astra Control ou dos dados de backup.

Clones

Um *clone* é uma cópia exata de um aplicativo, sua configuração e seus volumes de dados persistentes. Você pode criar manualmente um clone no mesmo cluster do Kubernetes ou em outro cluster. Clonar uma aplicação pode ser útil se você precisar mover aplicações e storage de um cluster Kubernetes para outro.

Replicação entre backends de armazenamento

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.

É possível replicar entre dois SVMs ONTAP no mesmo cluster ONTAP ou em clusters ONTAP diferentes.

O Astra Control replica de forma assíncrona as cópias snapshot de aplicações para um cluster de destino. O processo de replicação inclui dados nos volumes persistentes replicados pelo SnapMirror e os metadados da aplicação protegidos pelo Astra Control.

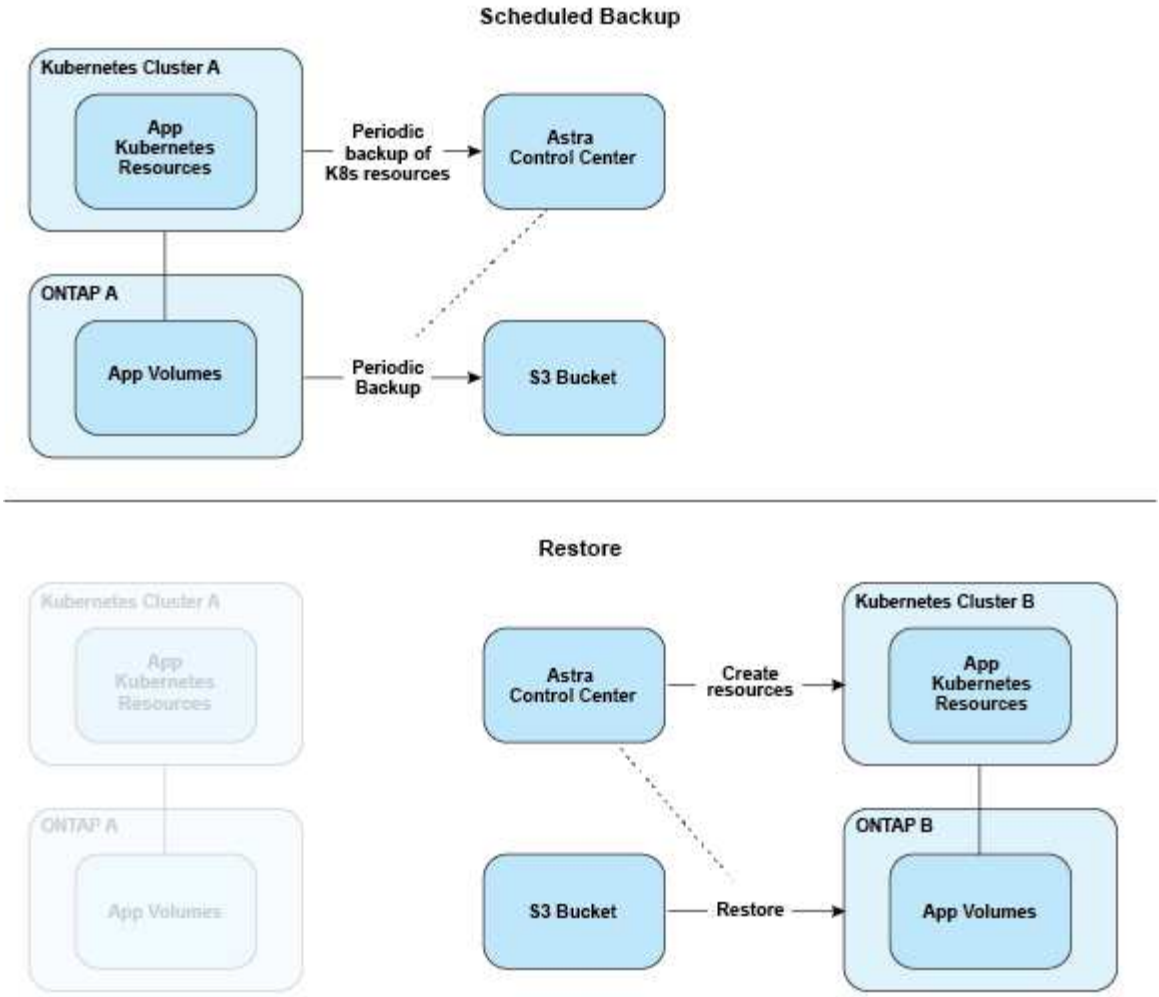
A replicação de aplicativos é diferente do backup e restauração de aplicativos das seguintes maneiras:

- **Replicação de aplicativos**: O Astra Control requer que os clusters de Kubernetes de origem e destino (que podem ser o mesmo cluster) estejam disponíveis e gerenciados com seus respectivos back-ends de storage do ONTAP configurados para habilitar o NetApp SnapMirror. O Astra Control tira o snapshot da aplicação orientada por políticas e replica-o no back-end de storage de destino. A tecnologia NetApp SnapMirror é usada para replicar dados de volume persistente. Para fazer failover, o Astra Control pode colocar a aplicação replicada online recriando os objetos da aplicação no cluster de Kubernetes de destino com os volumes replicados no cluster do ONTAP de destino. Como os dados de volume persistente já estão presentes no cluster de destino ONTAP, o Astra Control pode oferecer tempos de recuperação rápidos para failover.
- **Backup e restauração de aplicativos**: Ao fazer backup de aplicações, o Astra Control cria um snapshot dos dados do aplicativo e os armazena em um bucket de armazenamento de objetos. Quando uma restauração é necessária, os dados no bucket devem ser copiados para um volume persistente no cluster do ONTAP. A operação de backup/restauração não exige que o cluster secundário Kubernetes/ONTAP esteja disponível e gerenciado, mas a cópia de dados adicional pode resultar em tempos de restauração mais longos.

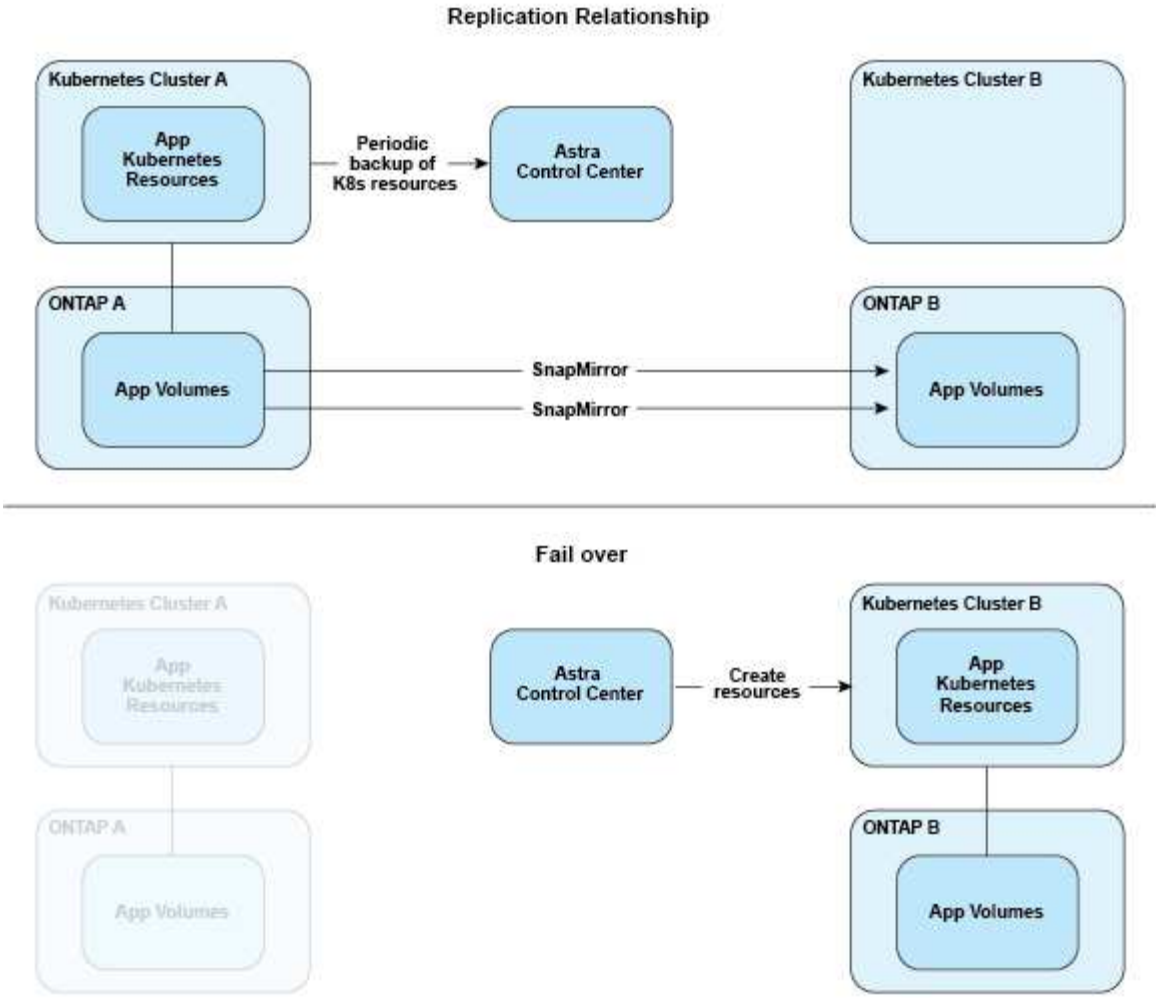
Para saber como replicar aplicativos, "Replique aplicativos para um sistema remoto usando a tecnologia SnapMirror"consulte .

As imagens a seguir mostram o processo de backup e restauração agendado em comparação com o processo de replicação.

O processo de backup copia dados para buckets do S3 e restaurações dos buckets do S3:



Por outro lado, a replicação é feita com replicação para o ONTAP e, em seguida, um failover cria os recursos do Kubernetes:



Backups, snapshots e clones com uma licença expirada

Se a licença expirar, você poderá adicionar uma nova aplicação ou executar operações de proteção de aplicações (como snapshots, backups, clones e operações de restauração) somente se a aplicação que você está adicionando ou protegendo for outra instância do Astra Control Center.

Licenciamento

Ao implantar o Astra Control Center, ele é instalado com uma licença de avaliação incorporada de 90 dias para 4.800 unidades de CPU. Se você precisar de mais capacidade ou um período de avaliação mais longo ou quiser atualizar para uma licença completa, você pode obter uma licença de avaliação diferente ou uma licença completa da NetApp.

Você obtém uma licença de uma das seguintes maneiras:

- Se você estiver avaliando o Centro de Controle Astra e precisar de termos de avaliação diferentes dos incluídos na licença de avaliação incorporada, entre em Contato com a NetApp para solicitar um arquivo de licença de avaliação diferente.
- "Se você já comprou o Astra Control Center, gere seu arquivo de licença do NetApp (NLF)" Ao iniciar sessão no site de suporte da NetApp e navegar para as suas licenças de software no menu sistemas.

Para obter detalhes sobre as licenças necessárias para backends de armazenamento ONTAP, "backends de armazenamento suportados"consulte .

> Certifique-se de que sua licença ativa pelo menos quantas unidades de CPU forem necessárias. Se o número de unidades de CPU que o Astra Control Center está gerenciando atualmente exceder as unidades de CPU disponíveis na nova licença que está sendo aplicada, você não poderá aplicar a nova licença.

Licenças de avaliação e licenças completas

Uma licença de avaliação incorporada é fornecida com uma nova instalação do Astra Control Center. Uma licença de avaliação permite os mesmos recursos e recursos que uma licença completa por um período limitado (90 dias). Após o período de avaliação, é necessária uma licença completa para continuar com a funcionalidade completa.

Expiração da licença

Se a licença ativa do Astra Control Center expirar, a funcionalidade de IU e API dos seguintes recursos não estará disponível:

- Instantâneos e backups locais manuais
- Snapshots e backups locais programados
- Restaurar a partir de um instantâneo ou cópia de segurança
- Clonagem a partir de um instantâneo ou estado atual
- Gerenciamento de novas aplicações
- Configurando políticas de replicação

Como o consumo de licença é calculado

Quando você adiciona um novo cluster ao Astra Control Center, ele não conta para licenças consumidas até que pelo menos uma aplicação executada no cluster seja gerenciada pelo Astra Control Center.

Quando você começa a gerenciar um aplicativo em um cluster, todas as unidades de CPU desse cluster são incluídas no consumo de licença do Astra Control Center, exceto unidades de CPU de nó de cluster Red Hat OpenShift relatadas por um usando o rótulo `node-role.kubernetes.io/infra: ""`.

> Os nós de infraestrutura do Red Hat OpenShift não consomem licenças no Astra Control Center. Para marcar um nó como um nó de infraestrutura, aplique o rótulo `node-role.kubernetes.io/infra: ""` ao nó.

Encontre mais informações

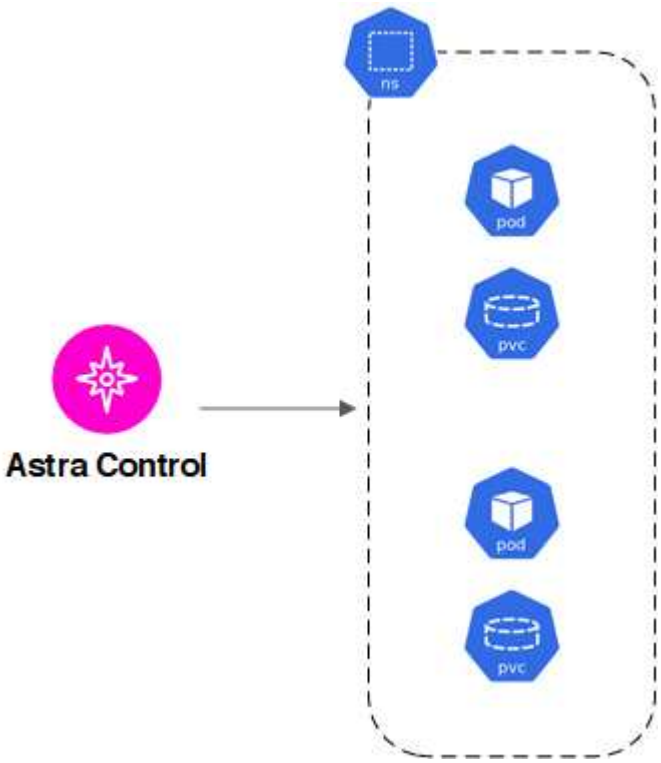
- "Adicione uma licença ao configurar o Astra Control Center pela primeira vez"
- "Atualizar uma licença existente"

Gerenciamento de aplicativos

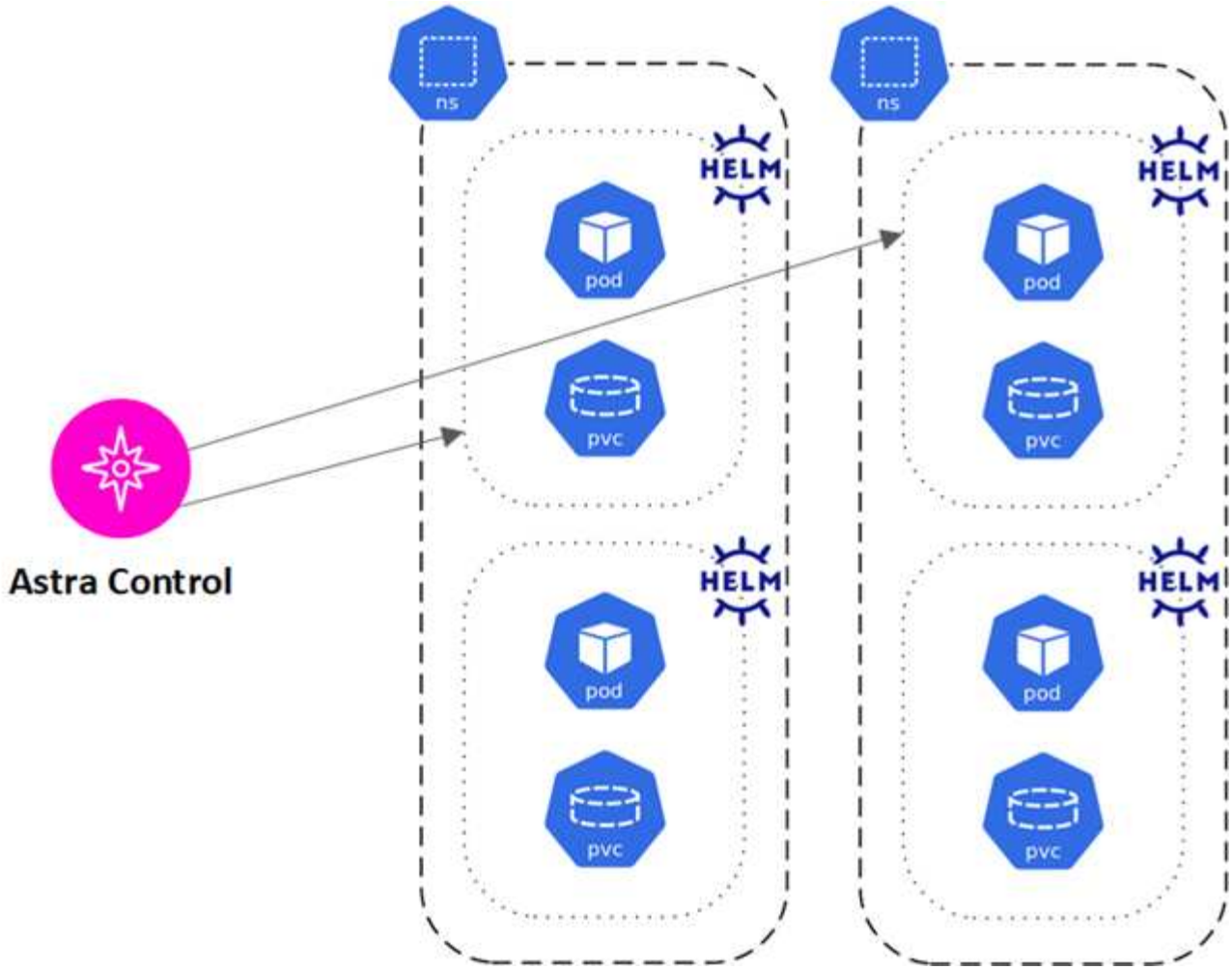
Quando o Astra Control descobre seus clusters, as aplicações nesses clusters não são

gerenciadas até que você escolha como deseja gerenciá-los. Uma aplicação gerenciada no Astra Control pode ser uma das seguintes opções:

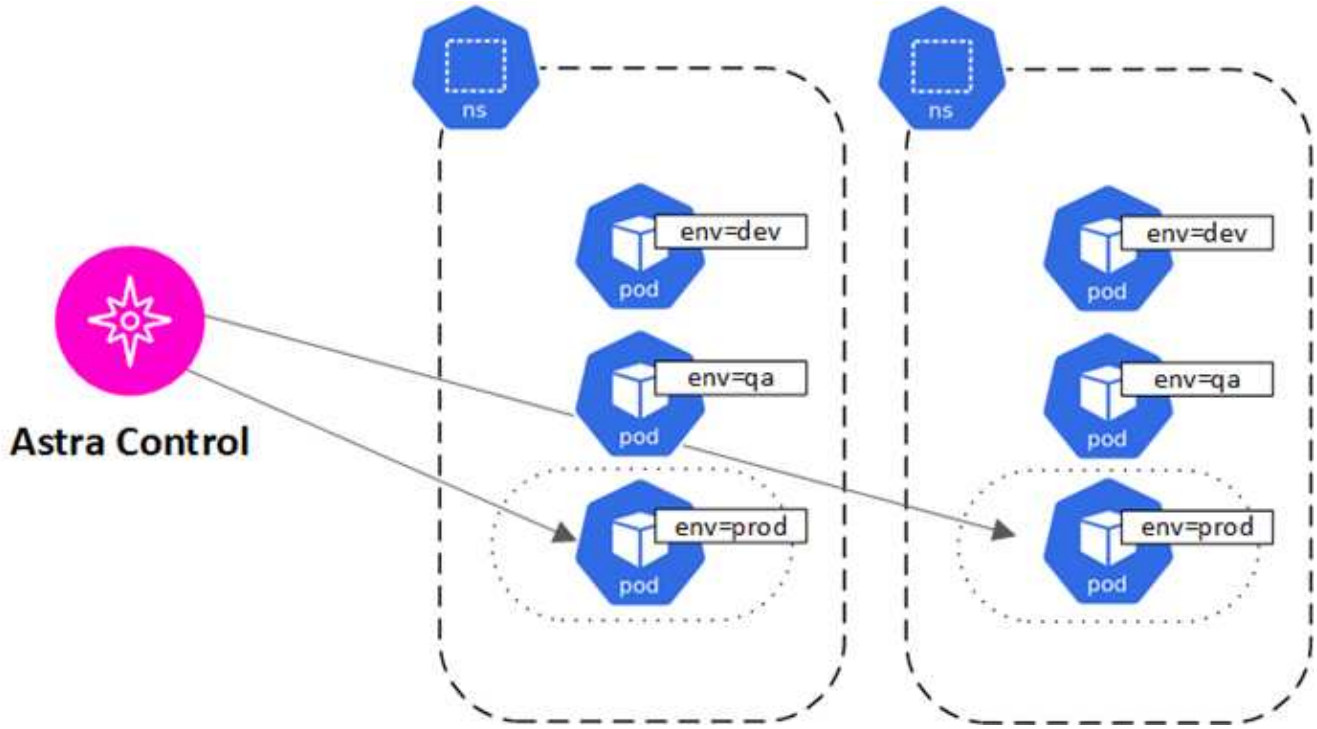
- Namespace, incluindo todos os recursos nesse namespace



- Um aplicativo individual implantado em um ou mais namespaces (helm3 é usado neste exemplo)



- Um grupo de recursos identificados por um rótulo do Kubernetes em um ou mais namespaces



Classes de armazenamento e tamanho de volume persistente

O Centro de Controle Astra é compatível com NetApp ONTAP e Longhorn como back-ends de armazenamento.

Visão geral

O Astra Control Center é compatível com o seguinte:

- * Classes de storage com suporte de armazenamento ONTAP*: Se você estiver usando um back-end do ONTAP, o Centro de Controle Astra oferece a capacidade de importar o back-end do ONTAP para relatar informações de monitoramento.
- * Classes de armazenamento baseadas em CSI apoiadas pela Longhorn*: Você pode usar Longhorn com o driver Longhorn Container Storage Interface (CSI).

As classes de storage devem estar "configurado" usando o Astra Control Provisioner.

Classes de armazenamento

Quando você adiciona um cluster ao Astra Control Center, será solicitado que você selecione uma classe de storage configurada anteriormente nesse cluster como a classe de storage padrão. Essa classe de armazenamento será usada quando nenhuma classe de armazenamento for especificada em uma reivindicação de volume persistente (PVC). A classe de armazenamento padrão pode ser alterada a qualquer momento no Astra Control Center e qualquer classe de armazenamento pode ser usada a qualquer momento especificando o nome da classe de armazenamento dentro do gráfico PVC ou Helm. Certifique-se de que você tenha apenas uma única classe de storage padrão definida para o cluster do Kubernetes.

Funções de usuário e namespaces

Saiba mais sobre funções de usuário e namespaces no Astra Control e como usá-los para controlar o acesso a recursos na sua organização.

Funções de utilizador

Você pode usar funções para controlar o acesso que os usuários têm a recursos ou funcionalidades do Astra Control. Veja a seguir as funções de usuário no Astra Control:

- 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.

Pode adicionar restrições a um utilizador Membro ou Visualizador para restringir o utilizador a um ou mais Namespaces.

Namespaces

Um namespace é um escopo que você pode atribuir a recursos específicos em um cluster gerenciado pelo Astra Control. O Astra Control descobre os namespaces de um cluster quando você adiciona o cluster ao Astra Control. Uma vez descoberto, os namespaces estão disponíveis para atribuir como restrições aos usuários. Somente os membros que têm acesso a esse namespace podem usar esse recurso. Você pode usar namespaces para controlar o acesso a recursos usando um paradigma que faz sentido para sua organização; por exemplo, por regiões físicas ou divisões dentro de uma empresa. Quando você adiciona restrições a um usuário, você pode configurar esse usuário para ter acesso a todos os namespaces ou apenas um conjunto específico de namespaces. Você também pode atribuir restrições de namespace usando rótulos de namespace.

Encontre mais informações

"Gerencie usuários e funções locais"

Informações sobre direitos autorais

Informações sobre marcas comerciais