Conceitos

Astra Control Center

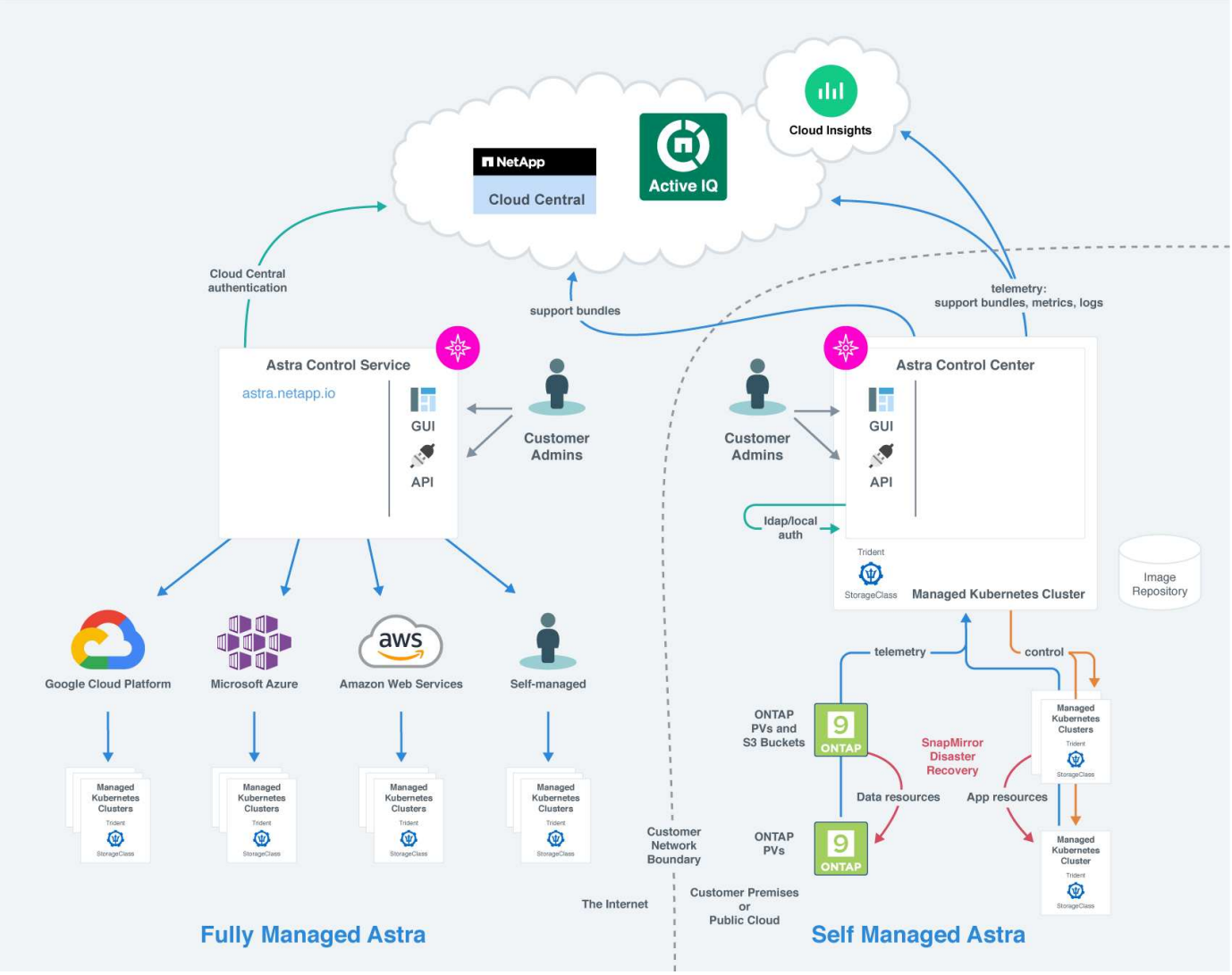
NetApp
August 11, 2025

Índice

Conceitos

Arquitetura e componentes

Aqui está uma visão geral dos vários componentes do ambiente Astra Control.



Componentes do Astra Control

- **Clusters do Kubernetes**: O Kubernetes é uma plataforma portátil, extensível e de código aberto para gerenciar cargas de trabalho e serviços em contêineres, que facilita tanto a configuração declarativa quanto a automação. O Astra fornece serviços de gerenciamento para aplicações hospedadas em um cluster Kubernetes.
- **Astra Trident**: Como um provisionador de storage de código aberto e orquestrador totalmente compatível mantido pelo NetApp, o Astra Trident permite que você crie volumes de storage para aplicações em contêiner gerenciadas pelo Docker e Kubernetes. Quando implantado com o Astra Control Center, o Astra Trident inclui um back-end de storage ONTAP configurado.
- **Backend de armazenamento**:
  - O Astra Control Service usa os seguintes back-ends de storage:

        - "NetApp Cloud Volumes Service para Google Cloud" Ou Google Persistent Disk como o back-end de storage para clusters GKE
        - "Azure NetApp Files" Ou discos gerenciados do Azure como o back-end de storage para clusters AKS.
        - "Amazon Elastic Block Store (EBS)" Ou "Amazon FSX para NetApp ONTAP" como opções de storage no back-end para clusters do EKS.
    - O Astra Control Center usa os seguintes back-ends de storage:
        - ONTAP AFF, FAS e ASA. Como uma plataforma de software e hardware de storage, o ONTAP fornece serviços básicos de storage, suporte para vários protocolos de acesso ao storage e recursos de gerenciamento de storage, como snapshots e espelhamento.
        - Cloud Volumes ONTAP
- **Cloud Insights**: Uma ferramenta de monitoramento de infraestrutura de nuvem da NetApp, o Cloud Insights permite que você monitore a performance e a utilização dos clusters do Kubernetes gerenciados pelo Astra Control Center. O Cloud Insights correlaciona o uso do storage com as cargas de trabalho. Quando você ativa a conexão Cloud Insights no Centro de Controle Astra, as informações de telemetria são exibidas nas páginas de IU do Centro de Controle Astra.

Interfaces Astra Control

Você pode concluir tarefas usando diferentes interfaces:

- * Interface de usuário da Web (UI)*: O Astra Control Service e o Astra Control Center usam a mesma interface de usuário baseada na Web onde você pode gerenciar, migrar e proteger aplicativos. Use a IU também para gerenciar contas de usuário e configurações.
- **API**: O Astra Control Service e o Astra Control Center usam a mesma API Astra Control. Usando a API, você pode executar as mesmas tarefas que você usaria a IU.

O Astra Control Center também permite gerenciar, migrar e proteger clusters de Kubernetes executados em ambientes de VM.

Para mais informações

- "Documentação do Astra Control Service"
- "Documentação do Astra Control Center"
- "Documentação do Astra Trident"
- "Use a 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.

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 para um cluster remoto

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 configurado, isso permite que as aplicações repliquem alterações de dados e aplicações de um cluster para outro.

O Astra Control replica de forma assíncrona as cópias Snapshot do aplicativo para um cluster remoto. 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 estejam disponíveis e gerenciados com seus respetivos back-ends de storage do ONTAP configurados para habilitar o NetApp SnapMirror. Astra Control elimina a aplicação orientada por políticas e replica-a para o cluster remoto. A tecnologia NetApp SnapMirror é usada para replicar dados de volume persistente.

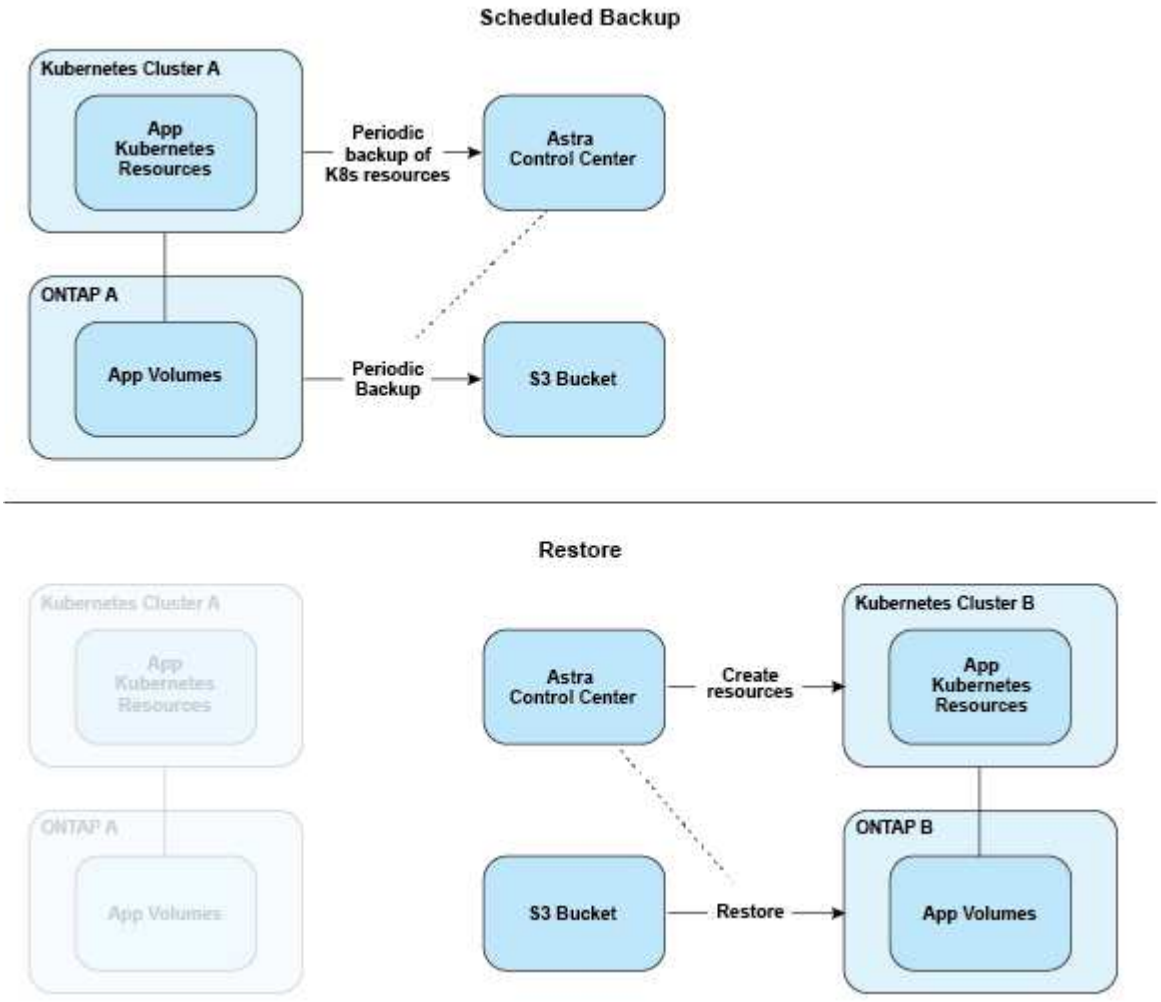
Para fazer failover, o Astra Control pode colocar a aplicação replicada online recriando os objetos da aplicação no cluster de Kubernetes de destino com os volumes replicados no cluster do ONTAP de destino. Como os dados de volume persistente já estão presentes no cluster de destino ONTAP, o Astra Control pode oferecer tempos de recuperação rápidos para failover.

- **Backup e restauração de aplicações**: 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.

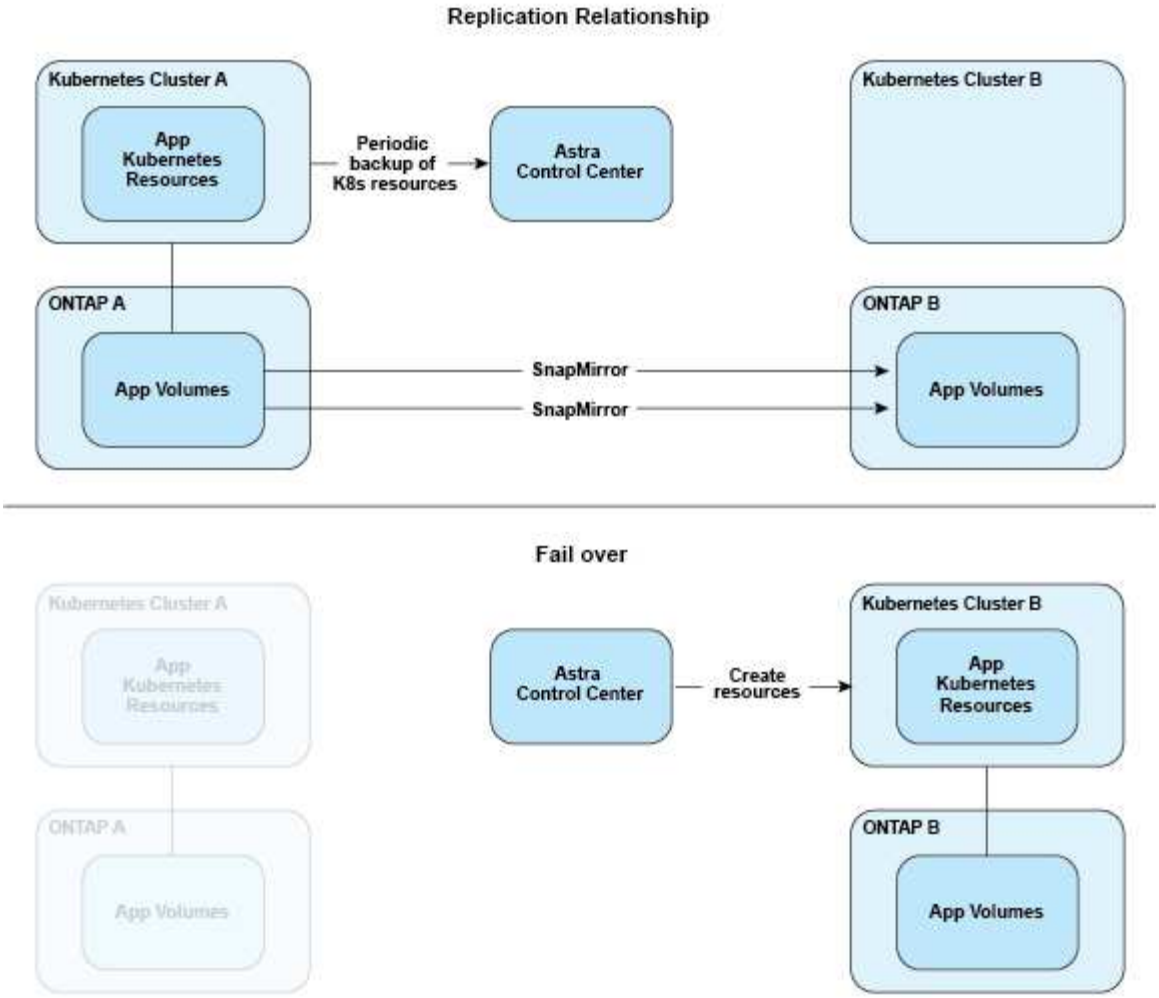
Para saber como replicar aplicativos, "Replique aplicativos para um sistema remoto usando a tecnologia SnapMirror"consulte .

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

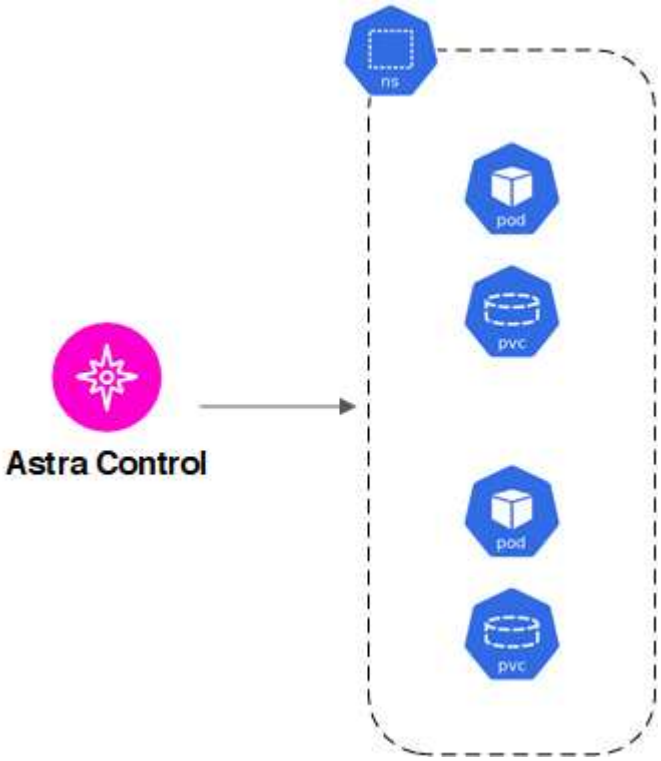
- "Adicione uma licença ao configurar o Astra Control Center pela primeira vez"
- "Atualizar uma licença existente"

Gerenciamento de aplicativos

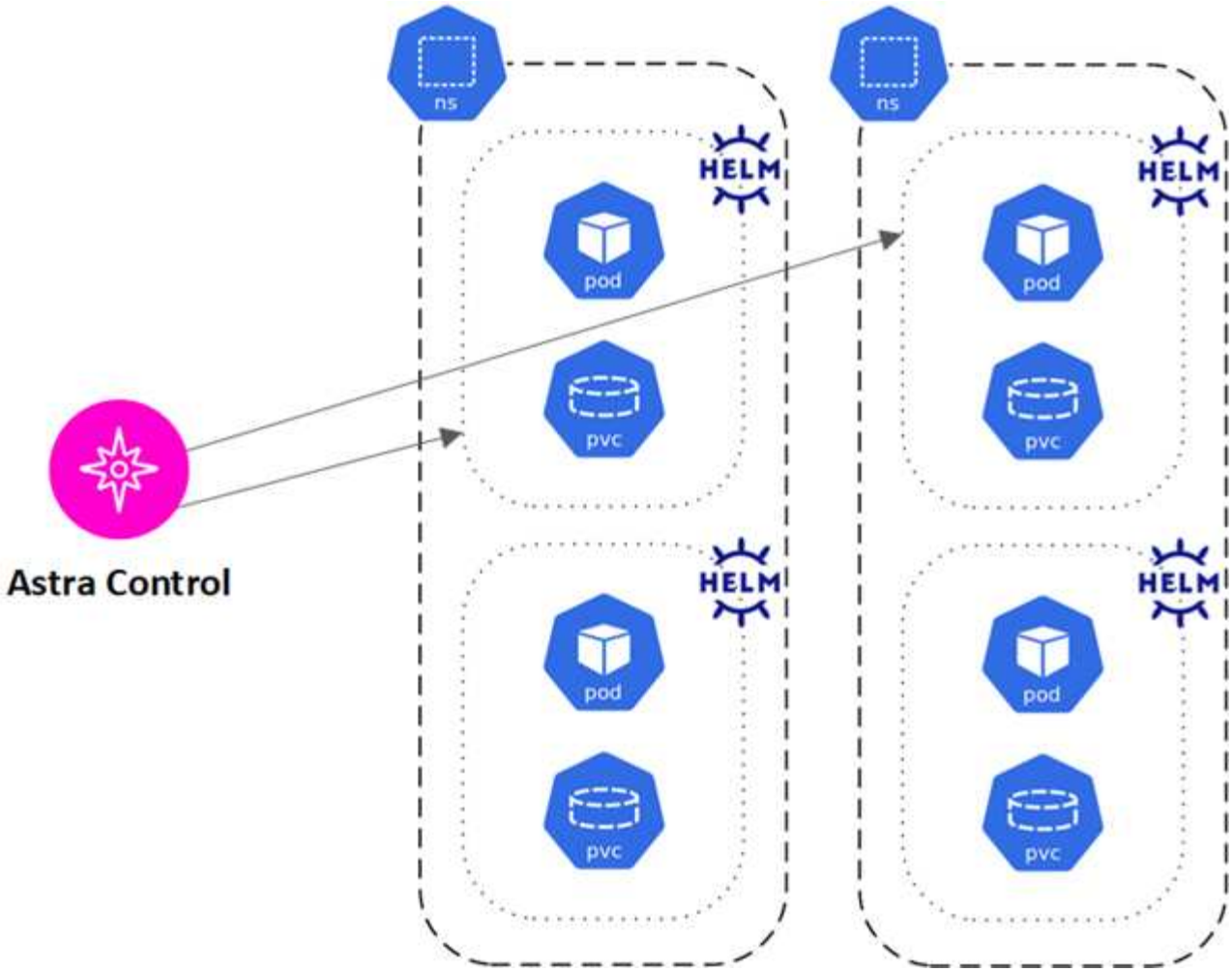
Quando o Astra Control descobre seus clusters, as aplicações nesses clusters não são

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

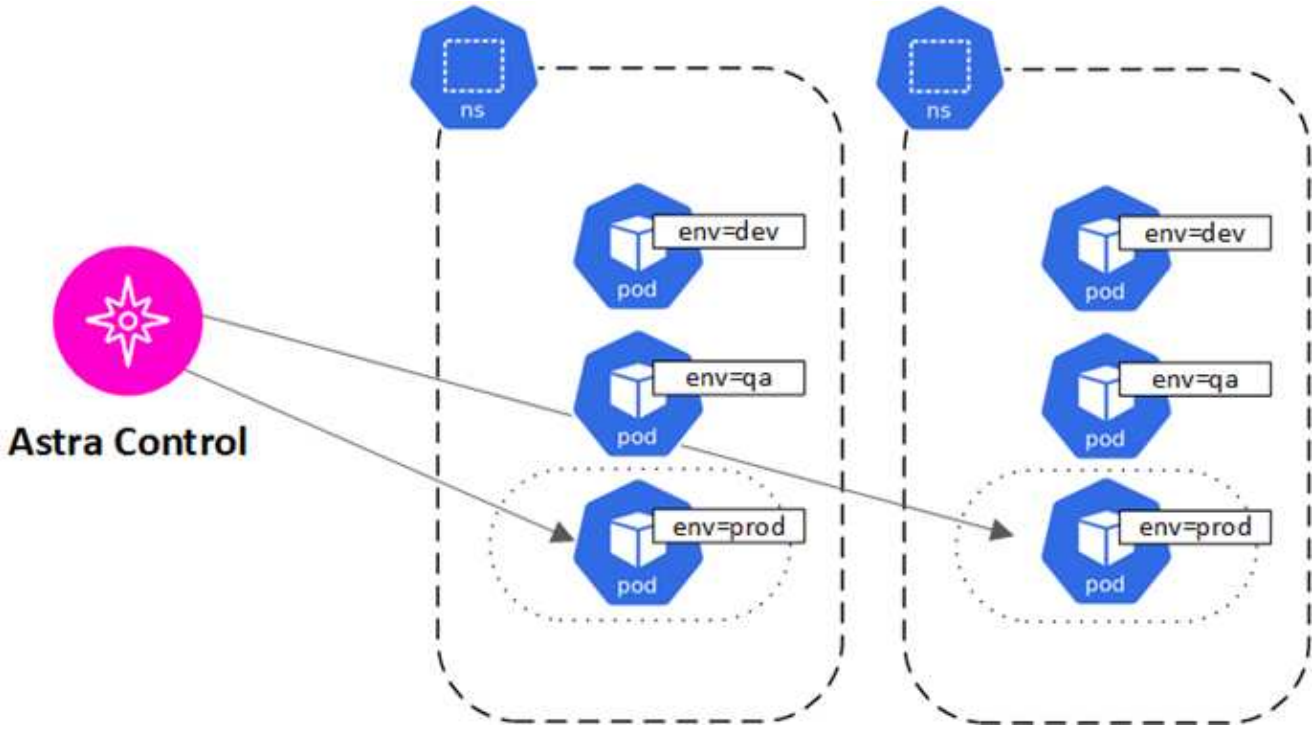
- Namespace, incluindo todos os recursos nesse namespace



- 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 Astra Control Center é compatível com o ONTAP como back-end de storage.

Visão geral

O Astra Control Center é compatível com o seguinte:

- **Classes de storage Astra Trident com suporte do ONTAP storage**: Se você estiver usando um back-end do ONTAP, o Astra Control Center oferece a capacidade de importar o back-end do ONTAP para relatar várias informações de monitoramento.

> As classes de storage do Astra Trident devem ser pré-configuradas fora do Centro de Controle Astra.

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.

Para mais informações

- "Documentação do Astra Trident"

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"

Segurança do pod

O Astra Control Center oferece suporte à limitação de privilégios por meio de políticas de segurança de pod (PSPs) e admissão de segurança de pod (PSA). Essas estruturas permitem limitar o que usuários ou grupos podem executar contêineres e o que Privileges esses contêineres podem ter.

Algumas distribuições do Kubernetes podem ter uma configuração de segurança de pod padrão que é muito restritiva e causa problemas ao instalar o Astra Control Center.

Você pode usar as informações e exemplos incluídos aqui para entender as alterações de segurança de pod que o Astra Control Center faz e usar uma abordagem de segurança de pod que fornece a proteção necessária sem interferir nas funções do Astra Control Center.

PSAs aplicados pelo Astra Control Center

Durante a instalação, o Astra Control Center permite a aplicação de uma admissão de segurança de pod, adicionando o seguinte rótulo ao `netapp-acc` namespace personalizado ou a um namespace personalizado:

```
pod-security.kubernetes.io/enforce: privileged
```

PSPs instalados pelo Astra Control Center

Quando você instala o Astra Control Center no Kubernetes 1,23 ou 1,24, várias políticas de segurança de pod são criadas durante a instalação. Alguns deles são permanentes, e alguns deles são criados durante certas operações e são removidos assim que a operação estiver concluída. O Astra Control Center não tenta instalar PSPs quando o cluster de host está executando o Kubernetes 1,25 ou posterior, pois não é compatível com essas versões.

PSP criados durante a instalação

Durante a instalação do Astra Control Center, o operador Astra Control Center instala uma política de

segurança de pod personalizada, um `Role` objeto e `RoleBinding` um objeto para oferecer suporte à implantação de serviços Astra Control Center no namespace Astra Control Center.

A nova política e os objetos têm os seguintes atributos:

```
kubectl get psp

NAME                            PRIV    CAPS          SELINUX    RUNASUSER
FSGROUP     SUPGROUP    READONLYROOTFS   VOLUMES
netapp-astra-deployment-psp    false                 RunAsAny   RunAsAny
RunAsAny    RunAsAny    false            *

kubectl get role -n <namespace_name>

NAME                                      CREATED AT
netapp-astra-deployment-role              2022-06-27T19:34:58Z

kubectl get rolebinding -n <namespace_name>

NAME                                      ROLE
AGE
netapp-astra-deployment-rb                Role/netapp-astra-deployment-role
32m
```

PSP criados durante operações de cópia de segurança

Durante as operações de backup, o Astra Control Center cria uma política de segurança de pod dinâmico, um `ClusterRole` objeto e um `RoleBinding` objeto. Isso dá suporte ao processo de backup, que acontece em um namespace separado.

A nova política e os objetos têm os seguintes atributos:

```
kubectl get psp

NAME                              PRIV    CAPS
SELINUX    RUNASUSER          FSGROUP     SUPGROUP    READONLYROOTFS
VOLUMES
netapp-astra-backup            false   DAC_READ_SEARCH
RunAsAny   RunAsAny           RunAsAny    RunAsAny    false           *

kubectl get role -n <namespace_name>

NAME                   CREATED AT
netapp-astra-backup   2022-07-21T00:00:00Z

kubectl get rolebinding -n <namespace_name>

NAME                   ROLE                         AGE
netapp-astra-backup   Role/netapp-astra-backup   62s
```

PSP criados durante a gestão de clusters

Quando você gerencia um cluster, o Astra Control Center instala o operador de monitoramento de NetApp no cluster gerenciado. Esse operador cria uma política de segurança de pod, um `ClusterRole` objeto e `RoleBinding` um objeto para implantar serviços de telemetria no namespace Astra Control Center.

A nova política e os objetos têm os seguintes atributos:

```
kubectl get psp

NAME                              PRIV    CAPS
SELINUX    RUNASUSER          FSGROUP     SUPGROUP    READONLYROOTFS
VOLUMES
netapp-monitoring-psp-nkmo     true    AUDIT_WRITE,NET_ADMIN,NET_RAW
RunAsAny   RunAsAny           RunAsAny    RunAsAny    false           *

kubectl get role -n <namespace_name>

NAME                                          CREATED AT
netapp-monitoring-role-privileged             2022-07-21T00:00:00Z

kubectl get rolebinding -n <namespace_name>

NAME                                                ROLE
AGE
netapp-monitoring-role-binding-privileged           Role/netapp-
monitoring-role-privileged             2m5s
```

Informações sobre direitos autorais

Informações sobre marcas comerciais