Documentação do Astra Control Center 22,04

Astra Control Center

NetApp
October 22, 2024

Índice

Documentação do Astra Control Center 22,04

Notas de lançamento

Temos o prazer de anunciar a versão 22.04.0 do Astra Control Center.

- "O que há nesta versão do Astra Control Center"
- "Problemas conhecidos"
- "Problemas conhecidos com o Astra Data Store e este lançamento do Astra Control Center"
- "Limitações conhecidas"

Siga-nos no Twitter. Envie feedback sobre a documentação tornando-se um "Colaborador do GitHub" ou enviando um e-mail para NetApp.com.

Novidades nesta versão do Astra Control Center

Temos o prazer de anunciar a mais recente versão 22.04.0 do Astra Control Center.

26 de abril de 2022 (22.04.0)

Novos recursos e suporte

- "Implantação do Astra Data Store a partir do Astra Control Center"
- "Controles de acesso baseados em função do namespace (RBAC)"
- "Suporte para Cloud Volumes ONTAP"
- "Capacitação genérica de ingresso para Astra Control Center"
- "Remoção do balde do Astra Control"
- "Suporte ao portfólio VMware Tanzu"

Problemas e limitações conhecidos

- "Problemas conhecidos para esta versão"
- "Problemas conhecidos com o Astra Data Store e este lançamento do Astra Control Center"
- "Limitações conhecidas para esta versão"

14 de dezembro de 2021 (21,12)

Novos recursos e suporte

- "Restauração de aplicativo"
- "Ganchos de execução"
- "Suporte para aplicativos implantados com operadores com escopo de namespace"
- "Suporte adicional para Kubernetes e Rancher upstream"
- "Pré-visualização do gerenciamento e monitoramento de back-end do Astra Data Store"
- "Atualizações do Astra Control Center"
- "Opção Red Hat OperatorHub para instalação"

Problemas resolvidos

- "Problemas resolvidos para esta versão"

Problemas e limitações conhecidos

- "Problemas conhecidos para esta versão"
- "Problemas conhecidos com a prévia do Astra Data Store e este lançamento do Astra Control Center"
- "Limitações conhecidas para esta versão"

5 de agosto de 2021 (21,08)

Lançamento inicial do Astra Control Center.

- "O que é"
- "Compreender a arquitetura e os componentes"
- "O que é preciso para começar"
- "Instale" e "configuração"
- "Gerenciar" e "proteger" aplicações
- "Gerenciar buckets" e "back-ends de armazenamento"
- "Gerenciar contas"
- "Automatize com API"

Encontre mais informações

- "Problemas conhecidos para esta versão"
- "Limitações conhecidas para esta versão"
- "Documentação do Astra Data Store"
- "Versões anteriores da documentação do Astra Control Center"

Problemas conhecidos

Problemas conhecidos identificam problemas que podem impedi-lo de usar esta versão do produto com sucesso.

Os seguintes problemas conhecidos afetam a versão atual:

Aplicações

- A restauração de um aplicativo resulta em tamanho PV maior do que o PV original
- Os clones de aplicativos falham usando uma versão específica do PostgreSQL
- Os clones do aplicativo falham ao usar as restrições de contexto de segurança do OCP (SCC) no nível da conta de serviço
- Os clones do aplicativo falham após a implantação de uma aplicação com uma classe de storage definida

Clusters

- O gerenciamento de um cluster com Astra Control Center falha quando o arquivo kubeconfig padrão contém mais de um contexto

Outras questões

- As operações de gerenciamento de dados da aplicação falham com erro de serviço interno (500) quando o Astra Trident está off-line

- Os instantâneos podem falhar com o controlador de instantâneos versão 4.2.0

A restauração de um aplicativo resulta em tamanho PV maior do que o PV original

Se você redimensionar um volume persistente após criar um backup e restaurar a partir desse backup, o tamanho do volume persistente corresponderá ao novo tamanho do PV em vez de usar o tamanho do backup.

Os clones de aplicativos falham usando uma versão específica do PostgreSQL

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.

Os clones do aplicativo falham ao usar as restrições de contexto de segurança do OCP (SCC) no nível da conta de serviço

Um clone de aplicativo pode falhar se as restrições de contexto de segurança originais forem configuradas no nível da conta de serviço dentro do namespace no cluster OpenShift Container Platform. Quando o clone de aplicação falha, ele aparece na área de aplicações gerenciadas no Astra Control Center com status `Removed`. Consulte "artigo da base de conhecimento" para obter mais informações.

Os clones do aplicativo falham após a implantação de uma aplicação com uma classe de storage definida

Depois que um aplicativo é implantado com uma classe de armazenamento explicitamente definida (por exemplo, `helm install …-set global.storageClass=netapp-cvs-perf-extreme`), as tentativas subsequentes de clonar o aplicativo exigem que o cluster de destino tenha 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. Não há etapas de recuperação neste cenário.

O gerenciamento de um cluster com Astra Control Center falha quando o arquivo kubeconfig padrão contém mais de um contexto

Você não pode usar um kubeconfig com mais de um cluster e contexto nele. Consulte "artigo da base de conhecimento" para obter mais informações.

As operações de gerenciamento de dados da aplicação falham com erro de serviço interno (500) quando o Astra Trident está off-line

Se o Astra Trident em um cluster de aplicações ficar offline (e for colocado novamente online) e se forem encontrados 500 erros de serviço interno ao tentar o gerenciamento de dados de aplicações, reinicie todos os nós do Kubernetes no cluster de aplicações para restaurar a funcionalidade.

Os instantâneos podem falhar com o controlador de instantâneos versão 4.2.0

Quando você usa a controladora de snapshot do Kubernetes (também conhecida como Snapshotter externo) versão 4.2.0 com Kubernetes 1,20 ou 1,21, os snapshots podem começar a falhar. Para evitar isso, use uma ferramenta diferente "versão suportada" de snapshotter externo, como a versão 4,2.1, com as versões 1,20 ou 1,21 do Kubernetes.

1. Execute uma chamada POST para adicionar um arquivo kubeconfig atualizado ao `/credentials` endpoint e recuperar o atribuído `id` do corpo de resposta.

2. Execute uma chamada PUT do `/clusters` ponto de extremidade usando o ID de cluster apropriado e defina o `credentialID` para o `id` valor da etapa anterior.

Depois de concluir estas etapas, a credencial associada ao cluster é atualizada e o cluster deve se reconetar e atualizar seu estado para `available`.

Encontre mais informações

- "Problemas conhecidos com a revisão do Astra Data Store e este lançamento do Astra Control Center"
- "Limitações conhecidas"

Problemas conhecidos com o Astra Data Store e este lançamento do Astra Control Center

Problemas conhecidos identificam problemas que podem impedi-lo de usar esta versão do produto com sucesso.

"Veja estes problemas conhecidos" Isso pode afetar o gerenciamento do Astra Data Store com o lançamento atual do Astra Control Center.

Encontre mais informações

- "Problemas conhecidos"
- "Limitações conhecidas"

Limitações conhecidas

As limitações conhecidas identificam plataformas, dispositivos ou funções que não são suportadas por esta versão do produto ou que não interoperam corretamente com ele. Revise essas limitações com cuidado.

Limitações do gerenciamento de clusters

- O mesmo cluster não pode ser gerenciado por duas instâncias do Astra Control Center
- O Astra Control Center não pode gerenciar dois clusters com nomes idênticos

Limitações de controle de acesso baseado em função (RBAC)

- Um usuário com restrições de namespace RBAC pode adicionar e desgerenciar um cluster
- Um membro com restrições de namespace não pode acessar os aplicativos clonados ou restaurados até que o administrador adicione o namespace à restrição

Limitações de gerenciamento de aplicativos

- Os backups de aplicativos em andamento não podem ser interrompidos
- Clones de aplicativos instalados usando operadores pass-by-referência podem falhar
- As operações de restauração no local de aplicativos que usam um gerenciador de certificados não são suportadas
- O operador habilitado para OLM e com escopo de cluster implantaram aplicativos não suportados
- As aplicações implementadas com o Helm 2 não são suportadas

Limitações gerais

- Os buckets do S3 no Astra Control Center não relatam a capacidade disponível
- O Astra Control Center não valida os detalhes inseridos para o servidor proxy
- As conexões existentes com um pod Postgres causam falhas
- Backups e snapshots podem não ser retidos durante a remoção de uma instância do Astra Control Center

O mesmo cluster não pode ser gerenciado por duas instâncias do Astra Control Center

Se você quiser gerenciar um cluster em outra instância do Astra Control Center, primeiro você deve "desgerenciar o cluster"usar a instância na qual ele é gerenciado antes de gerenciá-lo em outra instância. Depois de remover o cluster do gerenciamento, verifique se o cluster não é gerenciado executando este comando:

```
oc get pods n -netapp-monitoring
```

Não deve haver pods em execução nesse namespace ou o namespace não deve existir. Se qualquer um deles for verdadeiro, o cluster não será gerenciado.

O Astra Control Center não pode gerenciar dois clusters com nomes idênticos

Se você tentar adicionar um cluster com o mesmo nome de um cluster que já existe, a operação falhará. Esse problema ocorre na maioria das vezes em um ambiente padrão do Kubernetes se você não tiver alterado o nome padrão do cluster nos arquivos de configuração do Kubernetes.

Como solução alternativa, faça o seguinte:

1. Edite seu kubeadm-config ConfigMap:

   ```
   kubectl edit configmaps -n kube-system kubeadm-config
   ```

2. Altere o `clusterName` valor do campo `kubernetes` de (o nome padrão do Kubernetes) para um nome personalizado exclusivo.
3. Editar kubeconfig (`.kube/config`).
4. Atualizar nome do cluster de `kubernetes` para um nome personalizado exclusivo (`xyz-cluster`é usado nos exemplos abaixo). Faça a atualização em ambas `clusters` as seções e `contexts`, conforme mostrado neste exemplo:

```
apiVersion: v1
clusters:
- cluster:
    certificate-authority-data:
ExAmPLERb2tCcjZ5K3E2Njk4eQotLExAMpLEORCBDRVJUSUZJQ0FURS0txxxxXX==
    server: https://x.x.x.x:6443
  name: xyz-cluster
contexts:
- context:
    cluster: xyz-cluster
    namespace: default
    user: kubernetes-admin
  name: kubernetes-admin@kubernetes
current-context: kubernetes-admin@kubernetes
```

Um usuário com restrições de namespace RBAC pode adicionar e desgerenciar um cluster

Um usuário com restrições de namespace RBAC não deve ter permissão para adicionar ou desgerenciar clusters. Devido a uma limitação atual, o Astra não impede que tais usuários desgerenciem clusters.

Um membro com restrições de namespace não pode acessar os aplicativos clonados ou restaurados até que o administrador adicione o namespace à restrição

Qualquer `member` usuário com restrições RBAC 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. Depois que um novo namespace é criado por uma operação de clone ou restauração, o administrador/proprietário da conta pode editar a `member` conta de usuário e atualizar as restrições de função para o usuário afetado conceder acesso ao novo namespace.

Os backups de aplicativos em andamento não podem ser interrompidos

Não há como parar um backup em execução. Se precisar excluir o backup, aguarde até que ele esteja concluído e use as instruções em "Eliminar cópias de segurança". Para eliminar uma cópia de segurança com falha, utilize o "API Astra Control".

Clones de aplicativos instalados usando operadores pass-by-referência podem falhar

O Astra Control é compatível com aplicativos instalados com operadores com escopo de namespace. Esses operadores são geralmente projetados com uma arquitetura "pass-by-value" em vez de "pass-by-reference". 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"

Observe que 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.

As operações de restauração no local de aplicativos que usam um gerenciador de certificados não são suportadas

Esta versão do Astra Control Center não oferece suporte à restauração local de aplicativos com gerentes de certificados. Operações de restauração para um namespace diferente e operações de clone são compatíveis.

O operador habilitado para OLM e com escopo de cluster implantaram aplicativos não suportados

O Astra Control Center não oferece suporte a atividades de gerenciamento de aplicações com operadores com escopo de cluster.

As aplicações implementadas com o Helm 2 não são suportadas

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) é totalmente compatível. Para obter mais informações, "Requisitos do Astra Control Center"consulte .

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.

O Astra Control Center não valida os detalhes inseridos para o servidor proxy

Certifique-se de que você "introduza os valores corretos" ao estabelecer uma conexão.

As conexões existentes com um pod Postgres causam falhas

Quando você executa operações nos pods Postgres, você não deve se conetar diretamente dentro do pod para usar o comando psql. O Astra Control requer acesso psql para congelar e descongelar os bancos de dados. Se houver uma conexão pré-existente, o snapshot, o backup ou o clone falhará.

Backups e snapshots podem não ser retidos durante a remoção de uma instância do Astra Control Center

Se você tiver uma licença de avaliação, certifique-se de armazenar o ID da conta para evitar perda de dados em caso de falha do Astra Control Center se você não estiver enviando ASUPs.

Encontre mais informações

- "Problemas conhecidos"
- "Problemas conhecidos com o Astra Data Store e este lançamento do Astra Control Center"

Conceitos

Saiba mais sobre o Astra Control

O Astra Control é uma solução de gerenciamento de ciclo de vida de dados de aplicações Kubernetes que simplifica as operações de aplicações com estado monitorado. Proteja, faça backup e migre workloads do Kubernetes com facilidade e crie clones de aplicações em funcionamento instantaneamente.

Caraterísticas

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

- Gerencie automaticamente o storage persistente
- Crie backups e snapshots sob demanda com reconhecimento de aplicações
- Automatizar operações de backup e snapshot orientadas por políticas
- Migrar aplicações e dados entre clusters do Kubernetes
- Clonar facilmente uma aplicação da produção ao preparo
- Visualize a integridade e o status de proteção da aplicação
- Use uma interface de usuário ou uma API para implementar seus fluxos de trabalho de backup e migração

O Astra Control vigia continuamente sua computação em busca de mudanças de estado, por isso está ciente de quaisquer novas aplicações que você adicionar ao longo do caminho.

Modelos de implantação

O Astra Control está disponível em dois modelos de implantação:

- **Astra Control Service**: Um serviço gerenciado pelo NetApp que fornece gerenciamento de dados com reconhecimento de aplicações dos clusters do Kubernetes no Google Kubernetes Engine (GKE) e no Azure Kubernetes Service (AKS).
- **Astra Control Center**: Software autogerenciado que oferece gerenciamento de dados com reconhecimento de aplicações dos clusters Kubernetes executados em seu ambiente local.

	Astra Control Service	Astra Control Center
Como é oferecido?	Como um serviço de nuvem totalmente gerenciado da NetApp	Como software que você baixa, instala e gerencia
Onde está hospedado?	Em uma nuvem pública de escolha da NetApp	No cluster Kubernetes fornecido
Como é atualizado?	Gerenciado por NetApp	Você gerencia quaisquer atualizações
Quais são os recursos de gerenciamento de dados do aplicativo?	Mesmas funcionalidades em ambas as plataformas, com exceções ao back-end de storage ou a serviços externos	Mesmas funcionalidades em ambas as plataformas, com exceções ao back-end de storage ou a serviços externos

	Astra Control Service	Astra Control Center
Qual é o suporte de back-end de storage?	Ofertas de serviço de nuvem da NetApp	• Sistemas NetApp ONTAP AFF e FAS • Astra Data Store como back-end de storage • Back-end de storage do Cloud Volumes ONTAP

Aplicações suportadas

O NetApp validou alguns aplicativos para garantir a segurança e a consistência dos snapshots e backups.

- "Saiba a diferença entre um aplicativo validado e um aplicativo padrão no Astra Control".

Não importa qual tipo de aplicação que você use com o Astra Control, você deve sempre testar o fluxo de trabalho de backup e restauração para garantir que atenda aos requisitos de recuperação de desastres.

Como funciona o Astra Control Service

O Astra Control Service é um serviço de nuvem gerenciado pela NetApp que está sempre ativo e atualizado com as funcionalidades mais recentes. Ele utiliza vários componentes para habilitar o gerenciamento do ciclo de vida dos dados das aplicações.

Em um alto nível, o Astra Control Service funciona assim:

- Você começa a usar o Astra Control Service configurando seu fornecedor de nuvem e registrando-se em uma conta Astra.
  - Para clusters GKE, o Astra Control Service usa "NetApp Cloud Volumes Service para Google Cloud" ou discos persistentes do Google como back-end de storage para volumes persistentes.
  - Para clusters AKS, o Astra Control Service usa "Azure NetApp Files" ou o Azure Disk Storage como o back-end de storage para seus volumes persistentes.
- Você adiciona sua primeira computação do Kubernetes ao Astra Control Service. Em seguida, o Astra Control Service faz o seguinte:
  - Cria um armazenamento de objetos na sua conta de fornecedor de nuvem, que é onde as cópias de backup são armazenadas.

    No Azure, o Astra Control Service também cria um grupo de recursos, uma conta de storage e chaves para o contêiner de Blob.
  - Cria uma nova função de administrador e conta de serviço do Kubernetes no cluster.
  - Usa essa nova função de administrador para instalar "Astra Trident" no cluster e criar uma ou mais classes de armazenamento.
  - Se você usa o Azure NetApp Files ou o NetApp Cloud Volumes Service para Google Cloud como back-end de storage, o Astra Control Service usa o Astra Trident para provisionar volumes persistentes para suas aplicações.
- Neste ponto, você pode adicionar aplicativos ao cluster. Volumes persistentes serão provisionados na nova classe de armazenamento padrão.
- Depois, você usa o Astra Control Service para gerenciar essas aplicações e começar a criar snapshots, backups e clones.

O Astra Control Service vigia continuamente sua computação em busca de mudanças de estado, de modo que esteja ciente de quaisquer novas aplicações adicionadas ao longo do caminho.

O Plano Gratuito do Astra Control permite gerenciar até 10 aplicativos em sua conta. Se você quiser gerenciar mais de 10 aplicativos, precisará configurar o faturamento atualizando do Plano Gratuito para o Plano Premium.

Como funciona o Astra Control Center

Astra Control Center é executado localmente em sua própria nuvem privada.

O Astra Control Center é compatível com clusters OpenShift Kubernetes com:

- Armazenamento Trident backends com ONTAP 9 .5 e superior
- Back-ends de storage do Astra Data Store

Em um ambiente conectado à nuvem, o Astra Control Center usa o Cloud Insights para fornecer monitoramento avançado e telemetria. Na ausência de uma conexão Cloud Insights, monitoramento e telemetria limitados (7 dias de métricas) estão disponíveis no Centro de Controle Astra e também exportados para ferramentas de monitoramento nativas do Kubernetes (como Prometheus e Grafana) por meio de pontos finais de métricas abertas.

O Astra Control Center é totalmente integrado ao ecossistema de consultores digitais da AutoSupport e Active IQ (também conhecido como consultor digital) para fornecer aos usuários e ao suporte da NetApp informações de solução de problemas e uso.

Você pode experimentar o Astra Control Center usando uma licença de avaliação de 90 dias. A versão de avaliação é suportada por meio de opções de e-mail e comunidade (canal Slack). Além disso, você tem acesso a artigos e documentação da base de conhecimento a partir do painel de suporte do produto.

Para instalar e usar o Astra Control Center, você precisará atender a determinados "requisitos".

Em um alto nível, o Astra Control Center funciona assim:

- Você instala o Astra Control Center em seu ambiente local. Saiba mais sobre como "Instale o Astra Control Center" .
- Você conclui algumas tarefas de configuração, como estas:
  - Configure o licenciamento.
  - Adicione o primeiro cluster.
  - Adicione o back-end de storage descoberto quando você adicionou o cluster.
  - Adicione um bucket do armazenamento de objetos que armazenará os backups do aplicativo.

Saiba mais sobre como "Configure o Astra Control Center" .

O Astra Control Center faz o seguinte:

- Descobre detalhes sobre os clusters gerenciados do Kubernetes.
- Descobre a configuração do armazenamento de dados Astra Trident ou Astra nos clusters que você escolher gerenciar e permite monitorar os back-ends de storage.
- Descobre aplicações nesses clusters e permite-lhe gerir e proteger as aplicações.

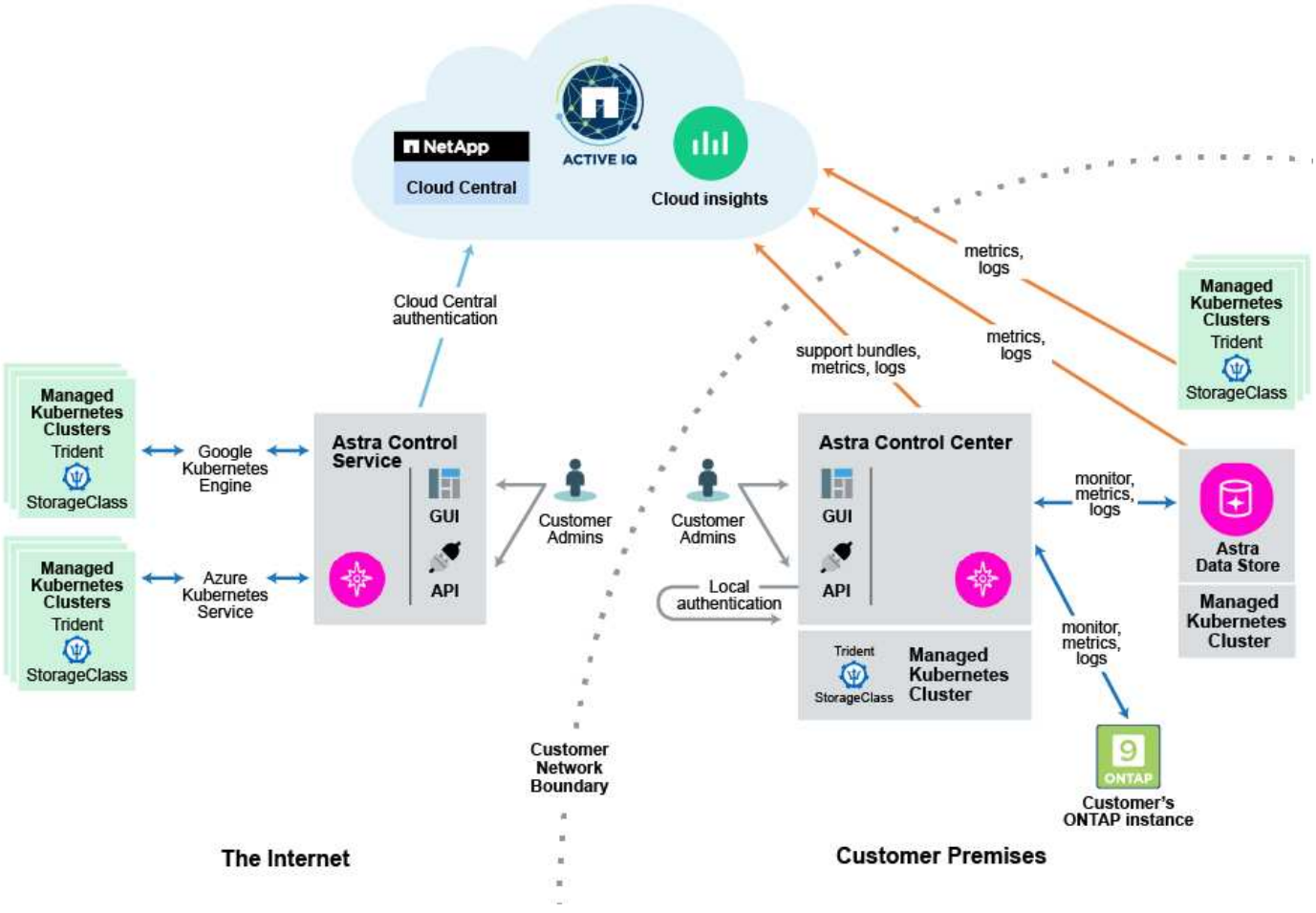
Você pode adicionar aplicativos ao cluster. Ou, se você já tiver algumas aplicações no cluster sendo gerenciado, poderá usar o Astra Control Center para detectá-las e gerenciá-las. Depois, use o Astra Control Center para criar snapshots, backups e clones.

Para mais informações

- "Documentação do Astra Control Service"
- "Documentação do Astra Control Center"
- "Documentação do Astra Data Store"
- "Documentação do Astra Trident"
- "Use a API Astra Control"
- "Documentação do Cloud Insights"
- "Documentação do ONTAP"

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 Trident permite que você crie volumes de storage para aplicações em contêiner gerenciadas pelo Docker e Kubernetes. Quando implantado com Astra Control Center, o Trident inclui um back-end de storage ONTAP configurado e também dá suporte ao Astra Data Store como um back-end de storage.
- **Backend de armazenamento**:
  - O Astra Control Service usa "NetApp Cloud Volumes Service para Google Cloud" como back-end de storage para clusters GKE e "Azure NetApp Files" como back-end de storage para clusters AKS.
  - O Astra Control Service também é compatível com discos gerenciados do Azure e o Google Persistent Disk como opções de storage de back-end.
  - O Astra Control Center usa os seguintes back-ends de storage:
    - Back-end de storage Astra Data Store
    - Back-end de storage ONTAP AFF e FAS. 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.
    - Back-end de storage do 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

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.

Um *backup* é armazenado no armazenamento de objetos externo e 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 que você escolha quantos snapshots e backups devem ser mantidos na programação. 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 da sua organização.

> *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 seu armazenamento persistente. 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.

Licenciamento

O Astra Control Center requer que seja instalada uma licença para que a funcionalidade completa de gerenciamento de dados do aplicativo seja ativada. Quando você implementa o Astra Control Center sem uma licença, um banner é exibido na IU da Web, avisando que a funcionalidade do sistema é limitada.

As seguintes operações requerem uma licença válida:

- Gerenciamento de novas aplicações
- Criação de instantâneos ou backups
- Configuração de uma política de proteção para agendar snapshots ou backups
- Restaurar a partir de um instantâneo ou cópia de segurança

- Clonagem a partir de um instantâneo ou estado atual

> Você pode adicionar um cluster, adicionar um bucket e gerenciar um back-end de storage do Astra Data Store sem licença. No entanto, você precisa de uma licença válida do Astra Control Center para gerenciar aplicações usando o Astra Data Store como um back-end de storage.

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. Você também pode adicionar um back-end de storage Astra Data Store ao Astra Control Center sem afetar o consumo de licença. Isso permite que você gerencie um back-end do Astra Data Store a partir de um sistema Astra Control Center não licenciado.

Quando você começa a gerenciar um aplicativo em um cluster, as unidades de CPU do cluster são incluídas no cálculo de consumo de licença do Astra Control Center.

Encontre mais informações

- "Atualizar uma licença existente"

Aplicativos validados vs padrão

Há dois tipos de aplicações que você pode trazer para o Astra Control: Validadas e padrão. Conheça a diferença entre essas duas categorias e os impactos potenciais em seus projetos e estratégia.

> É tentador pensar nessas duas categorias como "suportadas" e "não suportadas". Mas, como você verá, não há um aplicativo "não suportado" no Astra Control. É possível adicionar qualquer aplicação ao Astra Control, embora as aplicações validadas tenham mais infraestrutura desenvolvida em torno dos workflows do Astra Control em comparação com as aplicações padrão.

Aplicações validadas

As aplicações validadas para Astra Control incluem o seguinte:

- MySQL 8.0.25
- MariaDB 10.5.9
- PostgreSQL 11,12
- Jenkins 2.277.4 LTS e 2.289.1 LTS

A lista de aplicações validadas representa as aplicações que o Astra Control reconhece. A equipe do Astra Control analisou e confirmou que essas aplicações foram totalmente testadas para serem restauradas. O Astra Control executa workflows personalizados para garantir a consistência de snapshots e backups no nível da aplicação.

Se um aplicativo for validado, a equipe do Astra Control identificou e implementou etapas que podem ser executadas para desativar o aplicativo antes de tirar um snapshot para obter um snapshot consistente com a aplicação. Por exemplo, quando o Astra Control faz um backup de um banco de dados PostgreSQL, ele primeiro desativa o banco de dados. Após a conclusão do backup, o Astra Control restaura o banco de dados para uma operação normal.

Não importa qual tipo de aplicação você usa com o Astra Control, sempre teste o fluxo de trabalho de backup e restauração para garantir que você atenda aos requisitos de recuperação de desastres.

Aplicações padrão

Outros aplicativos, incluindo programas personalizados, são considerados aplicativos padrão. Você pode adicionar e gerenciar aplicações padrão por meio do Astra Control. Você também pode criar snapshots e backups básicos e consistentes com falhas de um aplicativo padrão. No entanto, eles não foram totalmente testados para restaurar o aplicativo para o seu estado original.

O Astra Control em si não é um aplicativo padrão; é um "aplicativo do sistema". O próprio Astra Control não é mostrado por padrão para gerenciamento. Você não deve tentar gerenciar o Astra Control por si só.

Classes de armazenamento e tamanho de volume persistente

O Astra Control Center é compatível com o ONTAP ou o Astra Data Store como back-end de storage.

Visão geral

O Astra Control Center é compatível com o seguinte:

- **Classes de storage do Trident com suporte do armazenamento de dados Astra**: Se você instalou um ou mais clusters de armazenamento de dados Astra manualmente, o Astra Control Center oferece a capacidade de importar e recuperar a topologia (nós, discos), bem como vários status.

  O Astra Control Center exibe o cluster subjacente do Kubernetes na configuração Astra Data Store, na nuvem à qual o cluster Kubernetes pertence, em quaisquer volumes persistentes provisionados pelo Astra Data Store, no nome do volume interno correspondente, na aplicação que usa o volume persistente e no cluster que contém a aplicação.

- **Classes de storage 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 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.

Quando você usa o Astra Control Center integrado a um back-end de storage Astra Data Store, após a instalação, nenhuma classe de storage será definida. Você precisará criar a classe de storage padrão do

Trident e aplicá-la ao back-end de storage. Consulte "Primeiros passos do Astra Data Store" para criar uma classe de storage padrão do Astra Data Store.

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

"Gerenciar funções"

Comece agora

Requisitos do Astra Control Center

Comece verificando a prontidão do seu ambiente operacional, clusters de aplicativos, aplicativos, licenças e navegador da Web.

Requisitos do ambiente operacional

O Astra Control Center requer um dos seguintes tipos de ambientes operacionais:

- Kubernetes 1,20 a 1,23
- Rancher 2,5.8, 2,5.9, ou 2,6 com RKE1
- Red Hat OpenShift Container Platform 4,6.8, 4,7, 4,8 ou 4,9
- VMware Tanzu Kubernetes Grid 1,4
- VMware Tanzu Kubernetes Grid Integrated Edition 1.12.2

Certifique-se de que o ambiente operacional escolhido para hospedar o Astra Control Center atenda aos requisitos básicos de recursos descritos na documentação oficial do ambiente. O Astra Control Center requer os seguintes recursos, além dos requisitos de recursos do ambiente:

Componente	Requisito
Capacidade de back-end de storage	Pelo menos 500GB disponível
Nós de trabalho	Pelo menos 3 nós de trabalho no total, com 4 núcleos de CPU e 12GB GB de RAM cada
Endereço FQDN	Um endereço FQDN para o Astra Control Center
Astra Trident	• Astra Trident 21,04 ou mais recente instalado e configurado • Astra Trident 21.10.1 ou mais recente instalado e configurado se o armazenamento de dados Astra for usado como um back-end de storage

Esses requisitos presumem que o Astra Control Center é a única aplicação em execução no ambiente operacional. Se o ambiente estiver executando aplicativos adicionais, ajuste esses requisitos mínimos de acordo.

- **Registro de imagem**: Você deve ter um Registro de imagem Docker privado existente para o qual você pode enviar imagens de compilação do Astra Control Center. Você precisa fornecer o URL do Registro de imagens onde você vai carregar as imagens.
- **Configuração Astra Trident / ONTAP**: O Astra Control Center requer que uma classe de storage seja criada e definida como a classe de storage padrão. O Astra Control Center é compatível com os seguintes drivers ONTAP fornecidos pelo Astra Trident:
  - ONTAP-nas
  - ONTAP-san

- ONTAP-são-economia

> 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`

> Se você pretende adicionar um segundo ambiente operacional do OpenShift como um recurso de computação gerenciado, precisa garantir que o recurso Snapshot de volume do Astra Trident esteja ativado. Para habilitar e testar snapshots de volume com o Astra Trident, "Consulte as instruções oficiais do Astra Trident".

Requisitos de cluster do VMware Tanzu Kubernetes Grid

Ao hospedar o Astra Control Center em um cluster do VMware Tanzu Kubernetes Grid (TKG) ou Tanzu Kubernetes Grid Integrated Edition (TKGI), tenha em mente as seguintes considerações.

- Desative a aplicação da classe de armazenamento padrão TKG ou TKGI em qualquer cluster de aplicativos que seja gerenciado pelo Astra Control. Você pode fazer isso editando o `TanzuKubernetesCluster` recurso no cluster do namespace.
- Você deve criar uma política de segurança que permita que o Astra Control Center crie pods no cluster. Você pode fazer isso usando os seguintes comandos:

```
kubectl config use-context <context-of-workload-cluster>
kubectl create clusterrolebinding default-tkg-admin-privileged-binding
--clusterrole=psp:vmware-system-privileged --group=system:authenticated
```

- Esteja ciente dos requisitos específicos do Astra Trident ao implantar o Centro de Controle Astra em um ambiente TKG ou TKGi. Para obter mais informações, consulte "Documentação do Astra Trident" .

> O token de arquivo de configuração padrão do VMware TKG e TKGI expira dez horas após a implantação. Se você usa produtos do portfólio Tanzu, precisará gerar um arquivo de configuração de cluster do Kubernetes da Tanzu com um token sem expiração para evitar problemas de conexão entre o Astra Control Center e os clusters de aplicativos gerenciados. Para obter instruções, visite "Documentação do produto do data center VMware NSX-T."

Backends de armazenamento suportados

O Astra Control Center é compatível com os seguintes back-ends de storage.

- Armazenamento de dados Astra
- NetApp ONTAP 9 .5 ou sistemas AFF e FAS mais recentes
- NetApp Cloud Volumes ONTAP

Requisitos do cluster de aplicativos

O Astra Control Center tem os seguintes requisitos para clusters que você planeja gerenciar a partir do Astra Control Center. Esses requisitos também se aplicam se o cluster que você planeja gerenciar for o cluster do ambiente operacional que hospeda o Astra Control Center.

- A versão mais recente do Kubernetes "componente do controlador snapshot" é instalada
- Um Astra Trident "volumesnapshotclass objeto" foi definido por um administrador
- Existe uma classe de storage padrão do Kubernetes no cluster
- Pelo menos uma classe de storage está configurada para usar o Astra Trident

Seu cluster de aplicativos deve ter um `kubeconfig.yaml` arquivo que define apenas um elemento *context*. Visite a documentação do Kubernetes para "informações sobre a criação de arquivos kubeconfig".

Ao gerenciar clusters de aplicativos em um ambiente Rancher, modifique o contexto padrão do cluster de aplicativos no `kubeconfig` arquivo fornecido pelo Rancher para usar um contexto de plano de controle em vez do contexto do servidor da API Rancher. Isso reduz a carga no servidor de API Rancher e melhora o desempenho.

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 de uma licença do Astra Control Center.
- **Namespaces**: O Astra Control requer que um aplicativo não abranja mais do que um namespace único, mas um namespace pode conter mais de um aplicativo.
- **StorageClass**: Se você instalar um aplicativo com um StorageClass explicitamente definido e precisar clonar o aplicativo, o cluster de destino para a operação clone deverá ter o StorageClass especificado originalmente. Clonar um aplicativo com um StorageClass explicitamente definido para um cluster que não tenha o mesmo StorageClass 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
Entrada	MutatingWebhook	NetworkPolicy
PersistentVolumeClaim	Pod	PodDisruptionBudget
PodTemplate	ReplicaSet	Função
RoleBinding	Rota	Segredo
Serviço	Contagem de serviço	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. A seguir estão alguns aplicativos que foram validados para este modelo de instalação:
  - "Apache K8ssandra"
  - "Jenkins CI"
  - "Cluster Percona XtraDB"

> Um operador e o aplicativo que ele instala devem usar o mesmo namespace; talvez seja necessário modificar o arquivo .yaml de implantação para que o operador garanta que esse seja o caso.

Acesso à internet

Você deve determinar se você tem acesso externo à Internet. Se não o fizer, algumas funcionalidades poderão ser limitadas, como receber dados de monitorização e métricas do NetApp Cloud Insights, ou enviar pacotes de suporte para o "Site de suporte da NetApp".

Licença

O Astra Control Center requer uma licença do Astra Control Center para todos os recursos. Obtenha uma licença de avaliação ou uma licença completa da NetApp. Sem uma licença, você não poderá:

- Definir aplicações personalizadas
- Criar snapshots ou clones de aplicações existentes
- Configurar políticas de proteção de dados

Se você quiser experimentar o Astra Control Center, você pode "use uma licença de avaliação de 90 dias".

Para saber mais sobre como as licenças funcionam, "Licenciamento"consulte .

Entrada para clusters do Kubernetes no local

Você pode escolher o tipo de entrada de rede que o Astra Control Center usa. Por padrão, o Astra Control Center implanta o gateway Astra Control Center (Service/traefik) como um recurso em todo o cluster. O Astra Control Center também é compatível com o uso de um balanceador de carga de serviço, se permitido no seu ambiente. Se você preferir usar um balanceador de carga de serviço e ainda não tiver um configurado, você pode usar o balanceador de carga MetalLB para atribuir automaticamente um endereço IP externo ao serviço.

Na configuração do servidor DNS interno, você deve apontar o nome DNS escolhido para o Astra Control Center para o endereço IP com balanceamento de carga.

> Se você estiver hospedando o Astra Control Center em um cluster Tanzu Kubernetes Grid, use o `kubectl get nsxlbmonitors -A` comando para ver se você já tem um monitor de serviço configurado para aceitar o tráfego de entrada. Se existir um, não deve instalar o MetalLB, porque o monitor de serviço existente substituirá qualquer nova configuração do balanceador de carga.

Para obter mais informações, "Configure a entrada para o balanceamento de carga"consulte .

Requisitos de rede

O ambiente operacional que hospeda o Astra Control Center se comunica usando as seguintes portas TCP. Você deve garantir que essas portas sejam permitidas por meio de firewalls e configurar firewalls para permitir qualquer tráfego de saída HTTPS proveniente da rede Astra. Algumas portas exigem conectividade entre o ambiente que hospeda o Astra Control Center e cada cluster gerenciado (observado quando aplicável).

> É possível implantar o Astra Control Center em um cluster de Kubernetes de duas stack e o Astra Control Center pode gerenciar aplicações e back-ends de storage configurados para operação de duas stack. Para obter mais informações sobre os requisitos de cluster de pilha dupla, consulte o "Documentação do Kubernetes".

Fonte	Destino	Porta	Protocolo	Finalidade
PC do cliente	Astra Control Center	443	HTTPS	Acesso de IU / API - garanta que essa porta esteja aberta de ambas as maneiras entre o cluster que hospeda o Astra Control Center e cada cluster gerenciado
Consumidor de métricas	Nó de trabalho do Astra Control Center	9090	HTTPS	Comunicação de dados de métricas - garanta que cada cluster gerenciado possa acessar essa porta no cluster que hospeda o Astra Control Center (comunicação bidirecional necessária)
Astra Control Center	Serviço Cloud Insights hospedado (https://cloudinsights.netapp.com)	443	HTTPS	Comunicação Cloud Insights

Fonte	Destino	Porta	Protocolo	Finalidade
Astra Control Center	Fornecedor de bucket de armazenamento Amazon S3 (https://my-bucket.s3.us-west-2.amazonaws.com/)	443	HTTPS	Comunicação de armazenamento Amazon S3
Astra Control Center	NetApp AutoSupport (https://support.netapp.com)	443	HTTPS	Comunicação NetApp AutoSupport

Navegadores da Web suportados

O Astra Control Center suporta versões recentes do Firefox, Safari e Chrome com uma resolução mínima de 1280 x 720.

O que vem a seguir

Veja a "início rápido" visão geral.

Início rápido para Astra Control Center

Esta página fornece uma visão geral de alto nível das etapas necessárias para começar a usar o Astra Control Center. Os links em cada etapa levam você a uma página que fornece mais detalhes.

Experimente! Se você quiser experimentar o Astra Control Center, você pode usar uma licença de avaliação de 90 dias. "informações de licenciamento"Consulte para obter detalhes.

Analisar os requisitos do cluster do Kubernetes

- O Astra funciona com clusters Kubernetes com um back-end de storage ONTAP configurado pela Trident ou um back-end de storage do Astra Data Store.
- Os clusters devem estar em execução em um estado saudável, com pelo menos três nós de trabalho on-line.
- O cluster precisa estar executando o Kubernetes.

"Saiba mais sobre os requisitos do Astra Control Center".

Baixe e instale o Astra Control Center

- Faça o download do Astra Control Center no "Página de download do site de suporte da NetApp".
- Instalar o Astra Control Center no seu ambiente local.

  Opcionalmente, instale o Astra Control Center usando o Red Hat OperatorHub.

"Saiba mais sobre a instalação do Astra Control Center".

3 Conclua algumas tarefas de configuração inicial

- Adicione uma licença.
- Adicionar um cluster Kubernetes e o Astra Control Center descobre detalhes.
- Adicionar um ONTAP ou "Armazenamento de dados Astra" back-end de storage.
- Opcionalmente, adicione um bucket do armazenamento de objetos que armazenará seus backups do aplicativo.

"Saiba mais sobre o processo de configuração inicial".

4 Use o Astra Control Center

Depois de concluir a configuração do Astra Control Center, veja o que você pode fazer a seguir:

- Gerenciar um aplicativo. "Saiba mais sobre como gerenciar aplicativos".
- Opcionalmente, conecte-se ao NetApp Cloud Insights para exibir métricas sobre a integridade do sistema, capacidade e taxa de transferência na IU do Centro de Controle Astra. "Saiba mais sobre como conetar-se ao Cloud Insights".

5 Continue a partir deste Quick Start

"Instale o Astra Control Center".

Encontre mais informações

- "Use a API Astra Control"

Visão geral da instalação

Escolha e conclua um dos seguintes procedimentos de instalação do Astra Control Center:

- "Instale o Astra Control Center usando o processo padrão"
- "(Se você usar o Red Hat OpenShift) instale o Astra Control Center usando o OpenShift OperatorHub"
- "Instalar o Astra Control Center com um back-end de storage do Cloud Volumes ONTAP"

Instale o Astra Control Center usando o processo padrão

Para instalar o Centro de Controle Astra, baixe o pacote de instalação no site de suporte da NetApp e execute as etapas a seguir para instalar o Operador do Centro de Controle Astra e o Centro de Controle Astra em seu ambiente. Você pode usar este procedimento para instalar o Astra Control Center em ambientes conetados à Internet ou com conexão via rede.

Para ambientes Red Hat OpenShift, você também pode usar um "procedimento alternativo" para instalar o Astra Control Center usando o OpenShift OperatorHub.

O que você vai precisar

- "Antes de começar a instalação, prepare seu ambiente para a implantação do Astra Control Center".

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

  Exemplo do OpenShift:

  ```
  oc get clusteroperators
  ```

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

  Exemplo do OpenShift:

  ```
  oc get apiservices
  ```

- O Astra FQDN que você pretende usar precisa ser roteável para esse cluster. Isso significa que você tem uma entrada DNS no seu servidor DNS interno ou está usando uma rota URL principal que já está registrada.

Sobre esta tarefa

O processo de instalação do Astra Control Center faz o seguinte:

- Instala os componentes do Astra no `netapp-acc` namespace (ou nome personalizado).
- Cria uma conta padrão.
- Estabelece um endereço de e-mail do usuário administrativo padrão e uma senha única padrão para `ACC-<UUID_of_installation>` esta instância do Astra Control Center. Esse usuário é atribuído a função proprietário no sistema e é necessário para fazer login pela primeira vez na IU.
- Ajuda você a determinar que todos os pods do Astra Control Center estão em execução.
- Instala a IU do Astra.

(Aplica-se apenas à versão EAP (Astra Data Store Early Access Program)) se você pretende gerenciar o Astra Data Store usando o Astra Control Center e habilitar workflows da VMware, implante o Astra Control Center somente no `pcloud` namespace e não no `netapp-acc` namespace ou namespace personalizado descrito nas etapas deste procedimento.

Não execute o seguinte comando durante todo o processo de instalação para evitar a exclusão de todos os pods do Astra Control Center: `kubectl delete -f astra_control_center_operator_deploy.yaml`

Se você estiver usando o Podman do Red Hat em vez do Docker Engine, os comandos Podman podem ser usados no lugar dos comandos Docker.

Passos

Para instalar o Astra Control Center, siga estas etapas:

- Faça o download e descompacte o pacote Astra Control Center
- Instale o plug-in NetApp Astra kubectl
- Adicione as imagens ao seu registo local

- Configure namespace e segredo para Registros com requisitos de autenticação
- Instale o operador do Centro de Controle Astra
- Configurar o Astra Control Center
- Instalação completa do operador e do Centro de Controle Astra
- Verifique o status do sistema
- Configure a entrada para o balanceamento de carga
- Faça login na IU do Astra Control Center

Faça o download e descompacte o pacote Astra Control Center

1. Faça o download do pacote Astra Control Center (`astra-control-center-[version].tar.gz`) no "Site de suporte da NetApp".
2. Faça o download do zip dos certificados e chaves do Astra Control Center no "Site de suporte da NetApp".
3. (Opcional) Use o seguinte comando para verificar a assinatura do pacote:

```
openssl dgst -sha256 -verify astra-control-center[version].pub
-signature <astra-control-center[version].sig astra-control-
center[version].tar.gz
```

4. Extraia as imagens:

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

Instale o plug-in NetApp Astra kubectl

O plug-in da linha de comando NetApp Astra `kubectl` economiza tempo ao executar tarefas comuns associadas à implantação e atualização do Astra Control Center.

O que você vai precisar

O NetApp fornece binários para o plugin para diferentes arquiteturas de CPU e sistemas operacionais. Você precisa saber qual CPU e sistema operacional você tem antes de executar esta tarefa. Em sistemas operacionais Linux e Mac, você pode usar o `uname -a` comando para coletar essas informações.

Passos

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

```
ls kubectl-astra/
```

2. Copie o arquivo para o mesmo local que o utilitário padrão `kubectl`. Neste exemplo, o `kubectl` utilitário está localizado no `/usr/local/bin` diretório. Substitua `<binary-name>` pelo nome do arquivo que você precisa:

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

Adicione as imagens ao seu registo local

1. Mude para o diretório Astra:

```
cd acc
```

2. Adicione os arquivos no diretório de imagem do Astra Control Center ao seu Registro local.

   Veja exemplos de scripts para o carregamento automático de imagens abaixo.

   a. Inicie sessão no seu registo:

      Docker:

```
docker login [your_registry_path]
```

      Podman:

```
podman login [your_registry_path]
```

   b. Use o script apropriado para carregar as imagens, marcar as imagens e enviar as imagens para seu Registro local:

      Docker:

```
export REGISTRY=[Docker_registry_path]
for astraImageFile in $(ls images/*.tar) ; do
  # Load to local cache. And store the name of the loaded image
trimming the 'Loaded images: '
  astraImage=$(docker load --input ${astraImageFile} | sed 's/Loaded
image: //')
  astraImage=$(echo ${astraImage} | sed 's!localhost/!!')
  # Tag with local image repo.
  docker tag ${astraImage} ${REGISTRY}/${astraImage}
  # Push to the local repo.
  docker push ${REGISTRY}/${astraImage}
done
```

      Podman:

```
export REGISTRY=[Registry_path]
for astraImageFile in $(ls images/*.tar) ; do
  # Load to local cache. And store the name of the loaded image trimming
the 'Loaded images: '
  astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image(s): //')
  astraImage=$(echo ${astraImage} | sed 's!localhost/!!')
  # Tag with local image repo.
  podman tag ${astraImage} ${REGISTRY}/${astraImage}
  # Push to the local repo.
  podman push ${REGISTRY}/${astraImage}
done
```

Configure namespace e segredo para Registros com requisitos de autenticação

1. Se você usar um Registro que requer autenticação, você precisará fazer o seguinte:

   a. Crie o `netapp-acc-operator` namespace:

   ```
   kubectl create ns netapp-acc-operator
   ```

   Resposta:

   ```
   namespace/netapp-acc-operator created
   ```

   b. Crie um segredo para o `netapp-acc-operator` namespace. Adicione informações do Docker e execute o seguinte comando:

   ```
   kubectl create secret docker-registry astra-registry-cred -n netapp-
   acc-operator --docker-server=[your_registry_path] --docker
   -username=[username] --docker-password=[token]
   ```

   Resposta da amostra:

   ```
   secret/astra-registry-cred created
   ```

   c. Crie o `netapp-acc` namespace (ou nome personalizado).

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

   Resposta da amostra:

```
namespace/netapp-acc created
```

d. Crie um segredo para o `netapp-acc` namespace (ou nome personalizado). Adicione informações do Docker e execute o seguinte comando:

```
kubectl create secret docker-registry astra-registry-cred -n [netapp-
acc or custom namespace] --docker-server=[your_registry_path]
--docker-username=[username] --docker-password=[token]
```

Resposta

```
secret/astra-registry-cred created
```

a. (Opcional) se você quiser que o cluster seja gerenciado automaticamente pelo Astra Control Center após a instalação, certifique-se de fornecer o kubeconfig como um segredo dentro do namespace Astra Control Center que você pretende implantar usando este comando:

```
kubectl create secret generic [acc-kubeconfig-cred or custom secret
name] --from-file=<path-to-your-kubeconfig> -n [netapp-acc or custom
namespace]
```

Instale o operador do Centro de Controle Astra

1. 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 a linha padrão de `imagePullSecrets: []` pelo seguinte:

```
imagePullSecrets:
- name: <name_of_secret_with_creds_to_local_registry>
```

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

c. Altere `[your_registry_path]` para a `acc-operator-controller-manager` imagem para o caminho do registo onde as imagens foram empurradas para um passo anterior.

d. (Para instalações que usam a pré-visualização do Astra Data Store) consulte este problema conhecido relacionado "Provisionadores de classe de storage e alterações adicionais que você precisará fazer no YAML"ao .

```
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
  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: [your_registry_path]/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
        command:
        - /manager
        env:
        - name: ACCOP_LOG_LEVEL
          value: "2"
        image: [your_registry_path]/acc-operator:[version x.y.z]
        imagePullPolicy: IfNotPresent
      imagePullSecrets: []
```

2. Instale o operador do Centro de Controle Astra:

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

Resposta da amostra:

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

Configurar o Astra Control Center

1. Edite o arquivo de recursos personalizados do Astra Control Center (CR) (`astra_control_center_min.yaml`) para criar contas, AutoSupport, Registro e outras configurações necessárias:

> Se forem necessárias personalizações adicionais para o seu ambiente, pode utilizar `astra_control_center.yaml` como CR alternativo. `astra_control_center_min.yaml` É o CR padrão e é adequado para a maioria das instalações.

```
vim astra_control_center_min.yaml
```

> As propriedades configuradas pelo CR não podem ser alteradas após a implantação inicial do Astra Control Center.

> Se você estiver usando um Registro que não requer autorização, você deve excluir a `secret` linha dentro `imageRegistry` ou a instalação falhará.

   a. Mude `[your_registry_path]` para o caminho do registo onde empurrou as imagens no passo anterior.

   b. Altere a `accountName` cadeia de carateres para o nome que deseja associar à conta.

   c. Altere a `astraAddress` cadeia de carateres para o FQDN que deseja usar no navegador para acessar o Astra. Não use `http://` ou `https://` no endereço. Copie este FQDN para uso em um

passo posterior.

d. Altere a `email` cadeia de carateres para o endereço de administrador inicial padrão. Copie este endereço de e-mail para uso em um passo posterior.

e. Alterar `enrolled` para AutoSupport para `false` sites sem conetividade com a Internet ou manter `true` para sites conetados.

f. (Opcional) Adicione um nome `firstName` e sobrenome `lastName` do usuário associado à conta. Você pode executar esta etapa agora ou mais tarde dentro da IU.

g. (Opcional) altere o `storageClass` valor para outro recurso de storageClass do Trident, se necessário pela sua instalação.

h. (Opcional) se você quiser que o cluster seja gerenciado automaticamente pelo Astra Control Center após a instalação e já tiver criou o segredo que contém o kubeconfig para este cluster, forneça o nome do segredo adicionando um novo campo a esse arquivo YAML chamado `astraKubeConfigSecret: "acc-kubeconfig-cred or custom secret name"`

i. Execute um dos seguintes passos:

- **Outro controlador de entrada (ingressType:Generic)**: Esta é a ação padrão com o Astra Control Center. Depois que o Astra Control Center for implantado, você precisará configurar o controlador Ingress para expor o Astra Control Center com um URL.

  A instalação padrão do Astra Control Center configura seu gateway (`service/traefik`) para ser do tipo `ClusterIP`. Essa instalação padrão requer que você configure adicionalmente um controlador/ingresso do Kubernetes para rotear o tráfego para ele. Se pretender utilizar uma entrada, "Configure a entrada para o balanceamento de carga"consulte .

- **Balanceador de carga de serviço (ingressType:AccTraefik)**: Se você não quiser instalar um IngressController ou criar um recurso de entrada, defina `ingressType` como `AccTraefik`.

  Isso implanta o gateway Astra Control Center `traefik` como um serviço do tipo Kubernetes LoadBalancer.

  O Astra Control Center usa um serviço do tipo "LoadBalancer" (`svc/traefik` no namespace Astra Control Center) e exige que seja atribuído um endereço IP externo acessível. Se os balanceadores de carga forem permitidos em seu ambiente e você ainda não tiver um configurado, você poderá usar o MetalLB ou outro balanceador de carga de serviço externo para atribuir um endereço IP externo ao serviço. Na configuração do servidor DNS interno, você deve apontar o nome DNS escolhido para o Astra Control Center para o endereço IP com balanceamento de carga.

> Para obter detalhes sobre o tipo de serviço "LoadBalancer" e Ingress, "Requisitos"consulte .

```
apiVersion: astra.netapp.io/v1
kind: AstraControlCenter
metadata:
  name: astra
spec:
  accountName: "Example"
  astraVersion: "ASTRA_VERSION"
  astraAddress: "astra.example.com"
  astraKubeConfigSecret: "acc-kubeconfig-cred or custom secret name"
  ingressType: "Generic"
  autoSupport:
    enrolled: true
  email: "[admin@example.com]"
  firstName: "SRE"
  lastName: "Admin"
  imageRegistry:
    name: "[your_registry_path]"
    secret: "astra-registry-cred"
  storageClass: "ontap-gold"
```

Instalação completa do operador e do Centro de Controle Astra

1. Se você ainda não fez isso em uma etapa anterior, crie o `netapp-acc` namespace (ou personalizado):

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

Resposta da amostra:

```
namespace/netapp-acc created
```

2. Instale o Astra Control Center no `netapp-acc` namespace (ou personalizado):

```
kubectl apply -f astra_control_center_min.yaml -n [netapp-acc or custom
namespace]
```

Resposta da amostra:

```
astracontrolcenter.astra.netapp.io/astra created
```

Verifique o status do sistema

Se você preferir usar OpenShift, você pode usar comandos oc comparáveis para etapas de verificação.

1. Verifique se todos os componentes do sistema foram instalados com êxito.

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

Cada pod deve ter um status de `Running`. Pode levar alguns minutos até que os pods do sistema sejam implantados.

Resposta da amostra:

```
NAME                                     READY   STATUS    RESTARTS
AGE
acc-helm-repo-5f75c5f564-bzqmt           1/1     Running   0
11m
activity-6b8f7cccb9-mlrn4                1/1     Running   0
9m2s
api-token-authentication-6hznt           1/1     Running   0
8m50s
api-token-authentication-qpfgb           1/1     Running   0
8m50s
api-token-authentication-sqnb7           1/1     Running   0
8m50s
asup-5578bbdd57-dxkbp                    1/1     Running   0
9m3s
authentication-56bff4f95d-mspmq          1/1     Running   0
7m31s
bucketservice-6f7968b95d-9rrrl           1/1     Running   0
8m36s
cert-manager-5f6cf4bc4b-82khn            1/1     Running   0
6m19s
cert-manager-cainjector-76cf976458-sdrbc 1/1     Running   0
6m19s
cert-manager-webhook-5b7896bfd8-2n45j    1/1     Running   0
6m19s
cloud-extension-749d9f684c-8bdhq         1/1     Running   0
9m6s
cloud-insights-service-7d58687d9-h5tzw   1/1     Running   2
8m56s
composite-compute-968c79cb5-nv7l4        1/1     Running   0
9m11s
composite-volume-7687569985-jg9gg        1/1     Running   0
8m33s
```

```
credentials-5c9b75f4d6-nx9cz                1/1     Running   0
8m42s
entitlement-6c96fd8b78-zt7f8                1/1     Running   0
8m28s
features-5f7bfc9f68-gsjnl                   1/1     Running   0
8m57s
fluent-bit-ds-h88p7                         1/1     Running   0
7m22s
fluent-bit-ds-krhnj                         1/1     Running   0
7m23s
fluent-bit-ds-l5bjj                         1/1     Running   0
7m22s
fluent-bit-ds-lrclb                         1/1     Running   0
7m23s
fluent-bit-ds-s5t4n                         1/1     Running   0
7m23s
fluent-bit-ds-zpr6v                         1/1     Running   0
7m22s
graphql-server-5f5976f4bd-vbb4z             1/1     Running   0
7m13s
identity-56f78b8f9f-8h9p9                   1/1     Running   0
8m29s
influxdb2-0                                 1/1     Running   0
11m
krakend-6f8d995b4d-5khkl                    1/1     Running   0
7m7s
license-5b5db87c97-jmxzc                    1/1     Running   0
9m
login-ui-57b57c74b8-6xtv7                   1/1     Running   0
7m10s
loki-0                                      1/1     Running   0
11m
monitoring-operator-9dbc9c76d-8znck         2/2     Running   0
7m33s
nats-0                                      1/1     Running   0
11m
nats-1                                      1/1     Running   0
10m
nats-2                                      1/1     Running   0
10m
nautilus-6b9d88bc86-h8kfb                   1/1     Running   0
8m6s
nautilus-6b9d88bc86-vn68r                   1/1     Running   0
8m35s
openapi-b87d77dd8-5dz9h                     1/1     Running   0
9m7s
```

```
polaris-consul-consul-5ljfb                1/1     Running   0
11m
polaris-consul-consul-s5d5z                1/1     Running   0
11m
polaris-consul-consul-server-0             1/1     Running   0
11m
polaris-consul-consul-server-1             1/1     Running   0
11m
polaris-consul-consul-server-2             1/1     Running   0
11m
polaris-consul-consul-twmpq                1/1     Running   0
11m
polaris-mongodb-0                          2/2     Running   0
11m
polaris-mongodb-1                          2/2     Running   0
10m
polaris-mongodb-2                          2/2     Running   0
10m
polaris-ui-84dc87847f-zrg8w                1/1     Running   0
7m12s
polaris-vault-0                            1/1     Running   0
11m
polaris-vault-1                            1/1     Running   0
11m
polaris-vault-2                            1/1     Running   0
11m
public-metrics-657698b66f-67pgt            1/1     Running   0
8m47s
storage-backend-metrics-6848b9fd87-w7x8r   1/1     Running   0
8m39s
storage-provider-5ff5868cd5-r9hj7          1/1     Running   0
8m45s
telegraf-ds-dw4hg                          1/1     Running   0
7m23s
telegraf-ds-k92gn                          1/1     Running   0
7m23s
telegraf-ds-mmxjl                          1/1     Running   0
7m23s
telegraf-ds-nhs8s                          1/1     Running   0
7m23s
telegraf-ds-rj7lw                          1/1     Running   0
7m23s
telegraf-ds-tqrkb                          1/1     Running   0
7m23s
telegraf-rs-9mwgj                          1/1     Running   0
7m23s
```

```
telemetry-service-56c49d689b-ffrzx          1/1     Running   0
8m42s
tenancy-767c77fb9d-g9ctv                    1/1     Running   0
8m52s
traefik-5857d87f85-7pmx8                    1/1     Running   0
6m49s
traefik-5857d87f85-cpxgv                    1/1     Running   0
5m34s
traefik-5857d87f85-lvmlb                    1/1     Running   0
4m33s
traefik-5857d87f85-t2xlk                    1/1     Running   0
4m33s
traefik-5857d87f85-v9wpf                    1/1     Running   0
7m3s
trident-svc-595f84dd78-zb816                1/1     Running   0
8m54s
vault-controller-86c94fbf4f-krttq           1/1     Running   0
9m24s
```

2. (Opcional) para garantir que a instalação esteja concluída, você pode assistir os `acc-operator` logs usando o seguinte comando.

```
kubectl logs deploy/acc-operator-controller-manager -n netapp-acc-
operator -c manager -f
```

> ⓘ `accHost` o registro de cluster é uma das últimas operações e, se falhar, não causará falha na implantação. No caso de uma falha de Registro de cluster indicada nos logs, você pode tentar o Registro novamente por meio do fluxo de trabalho ou da API de adicionar cluster"Na IU".

3. Quando todos os pods estiverem em execução, verifique o sucesso da instalação recuperando a `AstraControlCenter` instância instalada pelo Operador do Centro de Controle Astra.

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

4. No YAML, marque o `status.deploymentState` campo na resposta para o `Deployed` valor. Se a implantação não tiver êxito, uma mensagem de erro será exibida.
5. Para obter a senha única que você usará quando fizer login no Astra Control Center, copie o `status.uuid` valor. A palavra-passe é `ACC-` seguida pelo valor UUID (`ACC-[UUID]`ou, neste exemplo, `ACC-9aa5fdae-4214-4cb7-9976-5d8b4c0ce27f`).

Amostra YAML Detalhes

```
name: astra
   namespace: netapp-acc
   resourceVersion: "104424560"
   selfLink: /apis/astra.netapp.io/v1/namespaces/netapp-
acc/astracontrolcenters/astra
   uid: 9aa5fdae-4214-4cb7-9976-5d8b4c0ce27f
 spec:
   accountName: Example
   astraAddress: astra.example.com
   astraVersion: 21.12.60
   autoSupport:
     enrolled: true
     url: https://support.netapp.com/asupprod/post/1.0/postAsup
   crds: {}
   email: admin@example.com
   firstName: SRE
   imageRegistry:
     name: registry_name/astra
     secret: astra-registry-cred
   lastName: Admin
 status:
   accConditionHistory:
     items:
     - astraVersion: 21.12.60
       condition:
         lastTransitionTime: "2021-11-23T02:23:59Z"
         message: Deploying is currently in progress.
         reason: InProgress
         status: "False"
         type: Ready
       generation: 2
       observedSpec:
         accountName: Example
         astraAddress: astra.example.com
         astraVersion: 21.12.60
         autoSupport:
           enrolled: true
           url: https://support.netapp.com/asupprod/post/1.0/postAsup
         crds: {}
         email: admin@example.com
         firstName: SRE
         imageRegistry:
           name: registry_name/astra
           secret: astra-registry-cred
```

```
      lastName: Admin
    timestamp: "2021-11-23T02:23:59Z"
  - astraVersion: 21.12.60
    condition:
      lastTransitionTime: "2021-11-23T02:23:59Z"
      message: Deploying is currently in progress.
      reason: InProgress
      status: "True"
      type: Deploying
    generation: 2
    observedSpec:
      accountName: Example
      astraAddress: astra.example.com
      astraVersion: 21.12.60
      autoSupport:
        enrolled: true
        url: https://support.netapp.com/asupprod/post/1.0/postAsup
      crds: {}
      email: admin@example.com
      firstName: SRE
      imageRegistry:
        name: registry_name/astra
        secret: astra-registry-cred
      lastName: Admin
    timestamp: "2021-11-23T02:23:59Z"
  - astraVersion: 21.12.60
    condition:
      lastTransitionTime: "2021-11-23T02:29:41Z"
      message: Post Install was successful
      observedGeneration: 2
      reason: Complete
      status: "True"
      type: PostInstallComplete
    generation: 2
    observedSpec:
      accountName: Example
      astraAddress: astra.example.com
      astraVersion: 21.12.60
      autoSupport:
        enrolled: true
        url: https://support.netapp.com/asupprod/post/1.0/postAsup
      crds: {}
      email: admin@example.com
      firstName: SRE
      imageRegistry:
        name: registry_name/astra
```

```
      secret: astra-registry-cred
    lastName: Admin
  timestamp: "2021-11-23T02:29:41Z"
- astraVersion: 21.12.60
  condition:
    lastTransitionTime: "2021-11-23T02:29:41Z"
    message: Deploying succeeded.
    reason: Complete
    status: "False"
    type: Deploying
  generation: 2
  observedGeneration: 2
  observedSpec:
    accountName: Example
    astraAddress: astra.example.com
    astraVersion: 21.12.60
    autoSupport:
      enrolled: true
      url: https://support.netapp.com/asupprod/post/1.0/postAsup
    crds: {}
    email: admin@example.com
    firstName: SRE
    imageRegistry:
      name: registry_name/astra
      secret: astra-registry-cred
    lastName: Admin
  observedVersion: 21.12.60
  timestamp: "2021-11-23T02:29:41Z"
- astraVersion: 21.12.60
  condition:
    lastTransitionTime: "2021-11-23T02:29:41Z"
    message: Astra is deployed
    reason: Complete
    status: "True"
    type: Deployed
  generation: 2
  observedGeneration: 2
  observedSpec:
    accountName: Example
    astraAddress: astra.example.com
    astraVersion: 21.12.60
    autoSupport:
      enrolled: true
      url: https://support.netapp.com/asupprod/post/1.0/postAsup
    crds: {}
    email: admin@example.com
```

```
        firstName: SRE
        imageRegistry:
          name: registry_name/astra
          secret: astra-registry-cred
        lastName: Admin
      observedVersion: 21.12.60
      timestamp: "2021-11-23T02:29:41Z"
    - astraVersion: 21.12.60
      condition:
        lastTransitionTime: "2021-11-23T02:29:41Z"
        message: Astra is deployed
        reason: Complete
        status: "True"
        type: Ready
      generation: 2
      observedGeneration: 2
      observedSpec:
        accountName: Example
        astraAddress: astra.example.com
        astraVersion: 21.12.60
        autoSupport:
          enrolled: true
          url: https://support.netapp.com/asupprod/post/1.0/postAsup
        crds: {}
        email: admin@example.com
        firstName: SRE
        imageRegistry:
          name: registry_name/astra
          secret: astra-registry-cred
        lastName: Admin
      observedVersion: 21.12.60
      timestamp: "2021-11-23T02:29:41Z"
  certManager: deploy
  cluster:
    type: OCP
    vendorVersion: 4.7.5
    version: v1.20.0+bafe72f
  conditions:
  - lastTransitionTime: "2021-12-08T16:19:55Z"
    message: Astra is deployed
    reason: Complete
    status: "True"
    type: Ready
  - lastTransitionTime: "2021-12-08T16:19:55Z"
    message: Deploying succeeded.
    reason: Complete
```

```
      status: "False"
      type: Deploying
    - lastTransitionTime: "2021-12-08T16:19:53Z"
      message: Post Install was successful
      observedGeneration: 2
      reason: Complete
      status: "True"
      type: PostInstallComplete
    - lastTransitionTime: "2021-12-08T16:19:55Z"
      message: Astra is deployed
      reason: Complete
      status: "True"
      type: Deployed
    deploymentState: Deployed
    observedGeneration: 2
    observedSpec:
      accountName: Example
      astraAddress: astra.example.com
      astraVersion: 21.12.60
      autoSupport:
        enrolled: true
        url: https://support.netapp.com/asupprod/post/1.0/postAsup
      crds: {}
      email: admin@example.com
      firstName: SRE
      imageRegistry:
        name: registry_name/astra
        secret: astra-registry-cred
      lastName: Admin
    observedVersion: 21.12.60
    postInstall: Complete
    uuid: 9aa5fdae-4214-4cb7-9976-5d8b4c0ce27f
kind: List
metadata:
 resourceVersion: ""
 selfLink: ""
```

Configure a entrada para o balanceamento de carga

Você pode configurar uma controladora de entrada de Kubernetes que gerencia o acesso externo a serviços, como balanceamento de carga em um cluster.

Este procedimento explica como configurar um controlador de entrada (`ingressType:Generic`). Essa é a ação padrão do Astra Control Center. Depois que o Astra Control Center for implantado, você precisará configurar o controlador Ingress para expor o Astra Control Center com um URL.

Se não pretender configurar um controlador de entrada, pode configurar `ingressType:AccTraefik)`o . O Astra Control Center usa um serviço do tipo "LoadBalancer" (`svc/traefik` no namespace Astra Control Center) e exige que seja atribuído um endereço IP externo acessível. Se os balanceadores de carga forem permitidos em seu ambiente e você ainda não tiver um configurado, você poderá usar o MetalLB ou outro balanceador de carga de serviço externo para atribuir um endereço IP externo ao serviço. Na configuração do servidor DNS interno, você deve apontar o nome DNS escolhido para o Astra Control Center para o endereço IP com balanceamento de carga. Para obter detalhes sobre o tipo de serviço "LoadBalancer" e Ingress, "Requisitos"consulte .

Os passos diferem consoante o tipo de controlador de entrada que utiliza:

- Controlador de entrada nginx
- Controlador de entrada OpenShift

O que você vai precisar

- O necessário "controlador de entrada" já deve ser implantado.
- O "classe de entrada" correspondente ao controlador de entrada já deve ser criado.
- Você está usando versões do Kubernetes entre o v1,19 e o v1,22, inclusive.

Etapas para o controlador nginx Ingress

1. Crie um segredo do tipo[`kubernetes.io/tls`] para uma chave privada TLS e um certificado no `netapp-acc` namespace (ou nome personalizado), conforme descrito em "Segredos TLS".
2. Implante um recurso de entrada no `netapp-acc` namespace (ou nome personalizado) usando o `v1beta1` tipo de recurso (obsoleto na versão do Kubernetes menor que ou 1,22) ou `v1` para um esquema obsoleto ou novo:
   a. Para um `v1beta1` esquema obsoleto, siga esta amostra:

```
apiVersion: extensions/v1beta1
kind: Ingress
metadata:
  name: ingress-acc
  namespace: [netapp-acc or custom namespace]
  annotations:
    kubernetes.io/ingress.class: [class name for nginx controller]
spec:
  tls:
  - hosts:
    - <ACC address>
    secretName: [tls secret name]
  rules:
  - host: [ACC address]
    http:
      paths:
      - backend:
        serviceName: traefik
        servicePort: 80
        pathType: ImplementationSpecific
```

b. Para o `v1` novo esquema, siga esta amostra:

```
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: netapp-acc-ingress
  namespace: [netapp-acc or custom namespace]
spec:
  ingressClassName: [class name for nginx controller]
  tls:
  - hosts:
    - <ACC address>
    secretName: [tls secret name]
  rules:
  - host: <ACC addess>
    http:
      paths:
        - path:
          backend:
            service:
              name: traefik
              port:
                number: 80
          pathType: ImplementationSpecific
```

Passos para o controlador OpenShift Ingress

1. Procure seu certificado e prepare os arquivos de chave, certificado e CA para uso pela rota OpenShift.
2. Crie a rota OpenShift:

```
oc create route edge --service=traefik
--port=web -n [netapp-acc or custom namespace]
--insecure-policy=Redirect --hostname=<ACC address>
--cert=cert.pem --key=key.pem
```

Faça login na IU do Astra Control Center

Depois de instalar o Astra Control Center, você alterará a senha do administrador padrão e fará login no painel da IU do Astra Control Center.

Passos

1. Em um navegador, insira o FQDN usado no no `astraAddress` `astra_control_center_min.yaml`CR quando Você instalou o Astra Control Center.
2. Aceite os certificados autoassinados quando solicitado.

> Você pode criar um certificado personalizado após o login.

3. Na página de login do Astra Control Center, insira o valor usado `email` no `astra_control_center_min.yaml` CR quando Você instalou o Astra Control Center, seguido da senha única (`ACC-[UUID]`).

> Se você digitar uma senha incorreta três vezes, a conta de administrador será bloqueada por 15 minutos.

4. Selecione **Login**.
5. Altere a senha quando solicitado.

> Se este for o seu primeiro login e você esquecer a senha e nenhuma outra conta de usuário administrativo ainda tiver sido criada, entre em Contato com o suporte da NetApp para obter assistência de recuperação de senha.

6. (Opcional) Remova o certificado TLS autoassinado existente e substitua-o por um "Certificado TLS personalizado assinado por uma autoridade de certificação (CA)".

Solucionar problemas da instalação

Se algum dos serviços estiver `Error` no estado, pode inspecionar os registos. Procure códigos de resposta da API na faixa 400 a 500. Eles indicam o lugar onde uma falha aconteceu.

Passos

1. Para inspecionar os logs do operador do Centro de Controle Astra, digite o seguinte:

```
kubectl logs --follow -n netapp-acc-operator $(kubectl get pods -n
netapp-acc-operator -o name)  -c manager
```

O que vem a seguir

Conclua a implantação executando "tarefas de configuração"o .

Instale o Astra Control Center usando o OpenShift OperatorHub

Se você usar o Red Hat OpenShift, poderá instalar o Astra Control Center usando o operador certificado Red Hat. Use este procedimento para instalar o Astra Control Center a partir do "Catálogo de ecossistemas da Red Hat" ou usando o Red Hat OpenShift Container Platform.

Depois de concluir este procedimento, terá de voltar ao procedimento de instalação para concluir o para verificar o "passos restantes"êxito da instalação e iniciar sessão.

O que você vai precisar

- "Antes de começar a instalação, prepare seu ambiente para a implantação do Astra Control Center".
- A partir do cluster OpenShift, certifique-se de que todos os operadores de cluster estão em um estado saudável (`available`é `true`):

```
oc get clusteroperators
```

- A partir do cluster OpenShift, certifique-se de que todos os serviços de API estão em um estado saudável (`available`é `true`):

```
oc get apiservices
```

- Você criou um endereço FQDN para o Astra Control Center em seu data center.
- Você tem as permissões necessárias e acesso à Red Hat OpenShift Container Platform para executar as etapas de instalação descritas.

Passos

- Faça o download e descompacte o pacote Astra Control Center
- Instale o plug-in NetApp Astra kubectl
- Adicione as imagens ao seu registo local
- Localize a página de instalação do operador
- Instale o operador
- Instale o Astra Control Center

Faça o download e descompacte o pacote Astra Control Center

1. Faça o download do pacote Astra Control Center (`astra-control-center-[version].tar.gz`) no "Site de suporte da NetApp".
2. Faça o download do zip dos certificados e chaves do Astra Control Center no "Site de suporte da NetApp".
3. (Opcional) Use o seguinte comando para verificar a assinatura do pacote:

```
openssl dgst -sha256 -verify astra-control-center[version].pub
-signature <astra-control-center[version].sig astra-control-
center[version].tar.gz
```

4. Extraia as imagens:

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

Instale o plug-in NetApp Astra kubectl

O plug-in da linha de comando NetApp Astra `kubectl` economiza tempo ao executar tarefas comuns associadas à implantação e atualização do Astra Control Center.

O que você vai precisar

O NetApp fornece binários para o plugin para diferentes arquiteturas de CPU e sistemas operacionais. Você precisa saber qual CPU e sistema operacional você tem antes de executar esta tarefa. Em sistemas operacionais Linux e Mac, você pode usar o `uname -a` comando para coletar essas informações.

Passos

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

```
ls kubectl-astra/
```

2. Copie o arquivo para o mesmo local que o utilitário padrão `kubectl`. Neste exemplo, o `kubectl` utilitário está localizado no `/usr/local/bin` diretório. Substitua `<binary-name>` pelo nome do arquivo que você precisa:

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

Adicione as imagens ao seu registo local

1. Mude para o diretório Astra:

```
cd acc
```

2. Adicione os arquivos no diretório de imagem do Astra Control Center ao seu Registro local.

   Veja exemplos de scripts para o carregamento automático de imagens abaixo.

   a. Inicie sessão no seu registo:

      Docker:

```
docker login [your_registry_path]
```

      Podman:

```
podman login [your_registry_path]
```

   b. Use o script apropriado para carregar as imagens, marcar as imagens e enviar as imagens para seu Registro local:

      Docker:

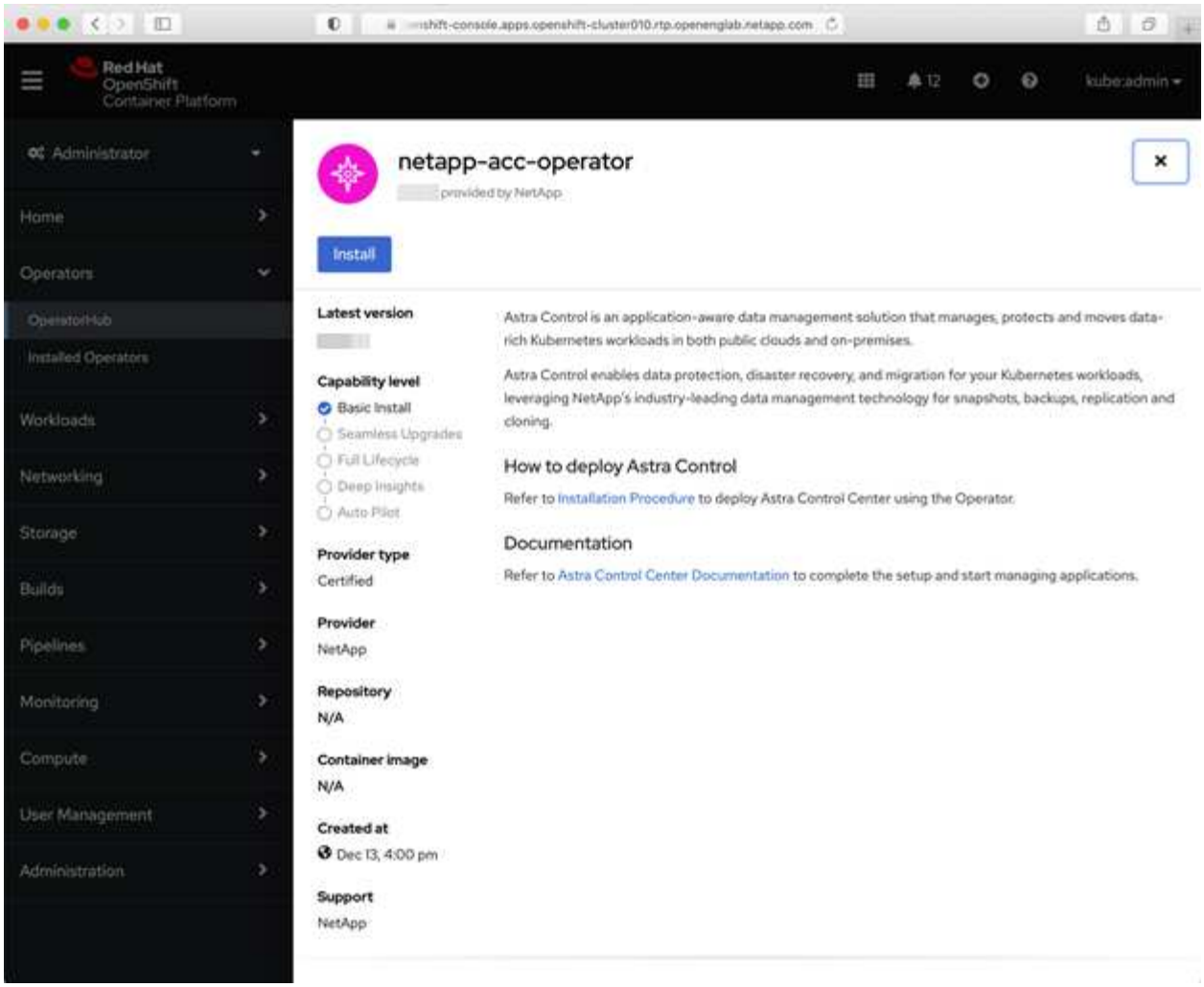
```
export REGISTRY=[Docker_registry_path]
for astraImageFile in $(ls images/*.tar) ; do
  # Load to local cache. And store the name of the loaded image
trimming the 'Loaded images: '
  astraImage=$(docker load --input ${astraImageFile} | sed 's/Loaded
image: //')
  astraImage=$(echo ${astraImage} | sed 's!localhost/!!')
  # Tag with local image repo.
  docker tag ${astraImage} ${REGISTRY}/${astraImage}
  # Push to the local repo.
  docker push ${REGISTRY}/${astraImage}
done
```

Podman:

```
export REGISTRY=[Registry_path]
for astraImageFile in $(ls images/*.tar) ; do
  # Load to local cache. And store the name of the loaded image trimming
the 'Loaded images: '
  astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image(s): //')
  astraImage=$(echo ${astraImage} | sed 's!localhost/!!')
  # Tag with local image repo.
  podman tag ${astraImage} ${REGISTRY}/${astraImage}
  # Push to the local repo.
  podman push ${REGISTRY}/${astraImage}
done
```

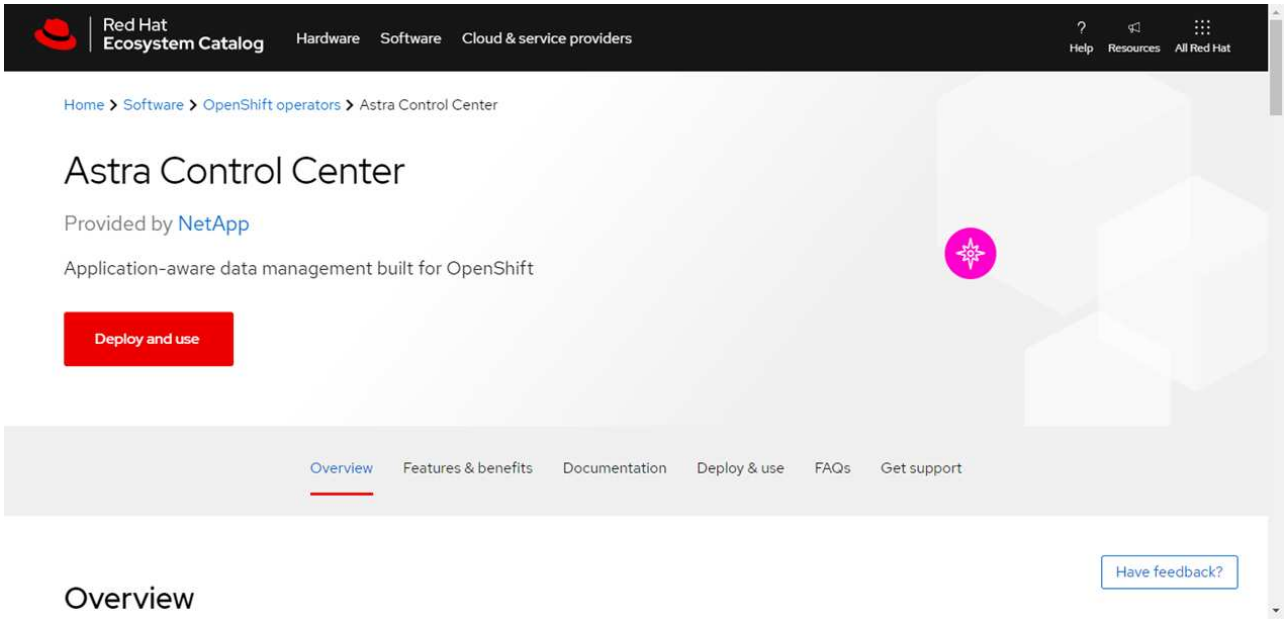
Localize a página de instalação do operador

1. Execute um dos seguintes procedimentos para acessar a página de instalação do operador:
   - A partir do console web Red Hat OpenShift:



i. Faça login na IU da OpenShift Container Platform.
ii. No menu lateral, selecione **operadores > OperatorHub**.
iii. Selecione o operador do Centro de Controle NetApp Astra.
iv. Selecione **Instalar**.

◦ No Red Hat Ecosystem Catalog:



i. Selecione o Centro de Controle NetApp Astra "operador" .

ii. Selecione **Deploy and use**.

Instale o operador

1. Preencha a página **Instalar Operador** e instale o operador:

   O operador estará disponível em todos os namespaces de cluster.

   a. Selecione o namespace do operador ou `netapp-acc-operator` o namespace será criado automaticamente como parte da instalação do operador.

   b. Selecione uma estratégia de aprovação manual ou automática.

   Recomenda-se a aprovação manual. Você deve ter apenas uma única instância de operador em execução por cluster.

   c. Selecione **Instalar**.

   Se selecionou uma estratégia de aprovação manual, ser-lhe-á pedido que aprove o plano de instalação manual para este operador.

2. No console, vá para o menu OperatorHub e confirme se o operador instalou com êxito.

Instale o Astra Control Center

1. No console na exibição de detalhes do operador Astra Control Center, selecione `Create instance` na seção APIs fornecidas.
2. Preencha o `Create AstraControlCenter` campo do formulário:
   a. Mantenha ou ajuste o nome do Astra Control Center.
   b. (Opcional) ative ou desative o suporte automático. Recomenda-se a manutenção da funcionalidade de suporte automático.

c. Insira o endereço do Astra Control Center. Não introduza `http://` ou `https://` no endereço.

d. Digite a versão do Astra Control Center; por exemplo, 21.12.60.

e. Insira um nome de conta, endereço de e-mail e sobrenome do administrador.

f. Mantenha a política de recuperação de volume padrão.

g. Em **Image Registry**, insira seu caminho de Registro de imagem de contentor local. Não introduza `http://` ou `https://` no endereço.

h. Se você usar um Registro que requer autenticação, digite o segredo.

i. Introduza o nome do administrador.

j. Configurar o dimensionamento de recursos.

k. Guarde a classe de armazenamento padrão.

l. Definir preferências de tratamento de CRD.

3. `Create`Selecione .

O que vem a seguir

Verifique a instalação bem-sucedida do Astra Control Center e conclua o "passos restantes" para fazer login. Além disso, você concluirá a implantação executando também "tarefas de configuração"o .

Instalar o Astra Control Center com um back-end de storage do Cloud Volumes ONTAP

Com o Astra Control Center, você pode gerenciar suas aplicações em um ambiente de nuvem híbrida com clusters Kubernetes autogerenciados e instâncias do Cloud Volumes ONTAP. É possível implantar o Astra Control Center nos clusters do Kubernetes no local ou em um dos clusters do Kubernetes autogerenciado no ambiente de nuvem.

Em uma dessas implantações, você pode executar operações de gerenciamento de dados de aplicações usando o Cloud Volumes ONTAP como um back-end de storage. Você também pode configurar um bucket do S3 como o destino de backup.

Para instalar o Astra Control Center na Amazon Web Services (AWS) e no Microsoft Azure com um back-end de storage do Cloud Volumes ONTAP, execute as etapas a seguir, dependendo do seu ambiente de nuvem.

- Implante o Astra Control Center na Amazon Web Services
- Implante o Astra Control Center no Microsoft Azure

Implante o Astra Control Center na Amazon Web Services

É possível implantar o Astra Control Center em um cluster Kubernetes autogerenciado hospedado em uma nuvem pública da Amazon Web Services (AWS).

Somente clusters autogerenciados do OpenShift Container Platform (OCP) são compatíveis com a implantação do Astra Control Center.

O que você precisará para a AWS

Antes de implantar o Astra Control Center na AWS, você precisará dos seguintes itens:

- Licença do Astra Control Center. "Requisitos de licenciamento do Astra Control Center"Consulte .

- "Atender aos requisitos do Astra Control Center".
- Conta do NetApp Cloud Central
- Permissões do Red Hat OpenShift Container Platform (OCP) (no nível do namespace para criar pods)
- Credenciais da AWS, ID de acesso e chave secreta com permissões que permitem criar buckets e conetores
- Acesso e login do AWS Account Elastic Container Registry (ECR)
- A zona hospedada da AWS e a entrada do Route 53 são necessárias para acessar a IU do Astra Control

Requisitos de ambiente operacional para a AWS

O Astra Control Center requer o seguinte ambiente operacional para a AWS:

- Red Hat OpenShift Container Platform 4,8

> Certifique-se de que o ambiente operacional escolhido para hospedar o Astra Control Center atenda aos requisitos básicos de recursos descritos na documentação oficial do ambiente.

O Astra Control Center requer os seguintes recursos, além dos requisitos de recursos do ambiente:

Componente	Requisito
Capacidade de storage do NetApp Cloud Volumes ONTAP no back-end	Pelo menos 300GB disponível
Nós de trabalho (requisito AWS EC2)	No total, pelo menos 3 nós de trabalho, com 4 núcleos vCPU e 12GB GB de RAM cada
Balanceador de carga	Tipo de serviço "LoadBalancer" disponível para envio de tráfego de entrada para serviços no cluster do ambiente operacional
FQDN	Um método para apontar o FQDN do Astra Control Center para o endereço IP balanceado de carga
Astra Trident (instalado como parte da descoberta de clusters do Kubernetes no NetApp Cloud Manager)	Astra Trident 21,04 ou mais recente instalado e configurado e o NetApp ONTAP versão 9,5 ou mais recente como um back-end de storage
Registo de imagens	Você precisa ter um Registro privado existente, como o AWS Elastic Container Registry, para o qual você pode enviar imagens de compilação do Astra Control Center. Você precisa fornecer o URL do Registro de imagens onde você vai carregar as imagens. O cluster hospedado do Astra Control Center e o cluster gerenciado devem ter acesso ao mesmo Registro de imagem para poder fazer backup e restaurar aplicativos usando a imagem baseada em Restic.

Componente	Requisito
Configuração Astra Trident/ONTAP	O Astra Control Center exige que uma classe de storage seja criada e definida como a classe de storage padrão. O Astra Control Center é compatível com as seguintes classes de storage do ONTAP Kubernetes criadas quando você importa o cluster do Kubernetes para o NetApp Cloud Manager. Eles são fornecidos pelo Astra Trident: • `vsaworkingenvironment-<>-ha-nas csi.trident.netapp.io` • `vsaworkingenvironment-<>-ha-san csi.trident.netapp.io` • `vsaworkingenvironment-<>-single-nas csi.trident.netapp.io` • `vsaworkingenvironment-<>-single-san csi.trident.netapp.io`

Esses requisitos presumem que o Astra Control Center é a única aplicação em execução no ambiente operacional. Se o ambiente estiver executando aplicativos adicionais, ajuste esses requisitos mínimos de acordo.

O token de Registro da AWS expira em 12 horas, após o qual você terá que renovar o segredo de Registro de imagem do Docker.

Visão geral da implantação para AWS

Aqui está uma visão geral do processo de instalação do Astra Control Center for AWS com o Cloud Volumes ONTAP como um back-end de storage.

Cada uma destas etapas é explicada em mais detalhes abaixo.

1. Certifique-se de que tem permissões IAM suficientes.
2. Instale um cluster RedHat OpenShift na AWS.
3. Configurar a AWS.
4. Configure o NetApp Cloud Manager.
5. Instale o Astra Control Center.

Certifique-se de que tem permissões IAM suficientes

Verifique se você tem funções e permissões suficientes do IAM que permitem instalar um cluster do RedHat OpenShift e um conetor do NetApp Cloud Manager.

```
https://docs.netapp.com/us-en/cloud-manager-setup-admin/concept-accounts-aws.html#initial-aws-credentials["Credenciais iniciais da AWS"^]Consulte .
```

Instale um cluster RedHat OpenShift na AWS

Instale um cluster do RedHat OpenShift Container Platform na AWS.

Para obter instruções de instalação, "Instalar um cluster na AWS no OpenShift Container Platform" consulte .

Configurar a AWS

Em seguida, configure a AWS para criar uma rede virtual, configurar instâncias de computação EC2, criar um bucket do AWS S3, criar um ECR (Elastic Container Register) para hospedar as imagens do Astra Control Center e enviar as imagens para esse Registro.

Siga a documentação da AWS para concluir as etapas a seguir. "Documentação de instalação da AWS"Consulte .

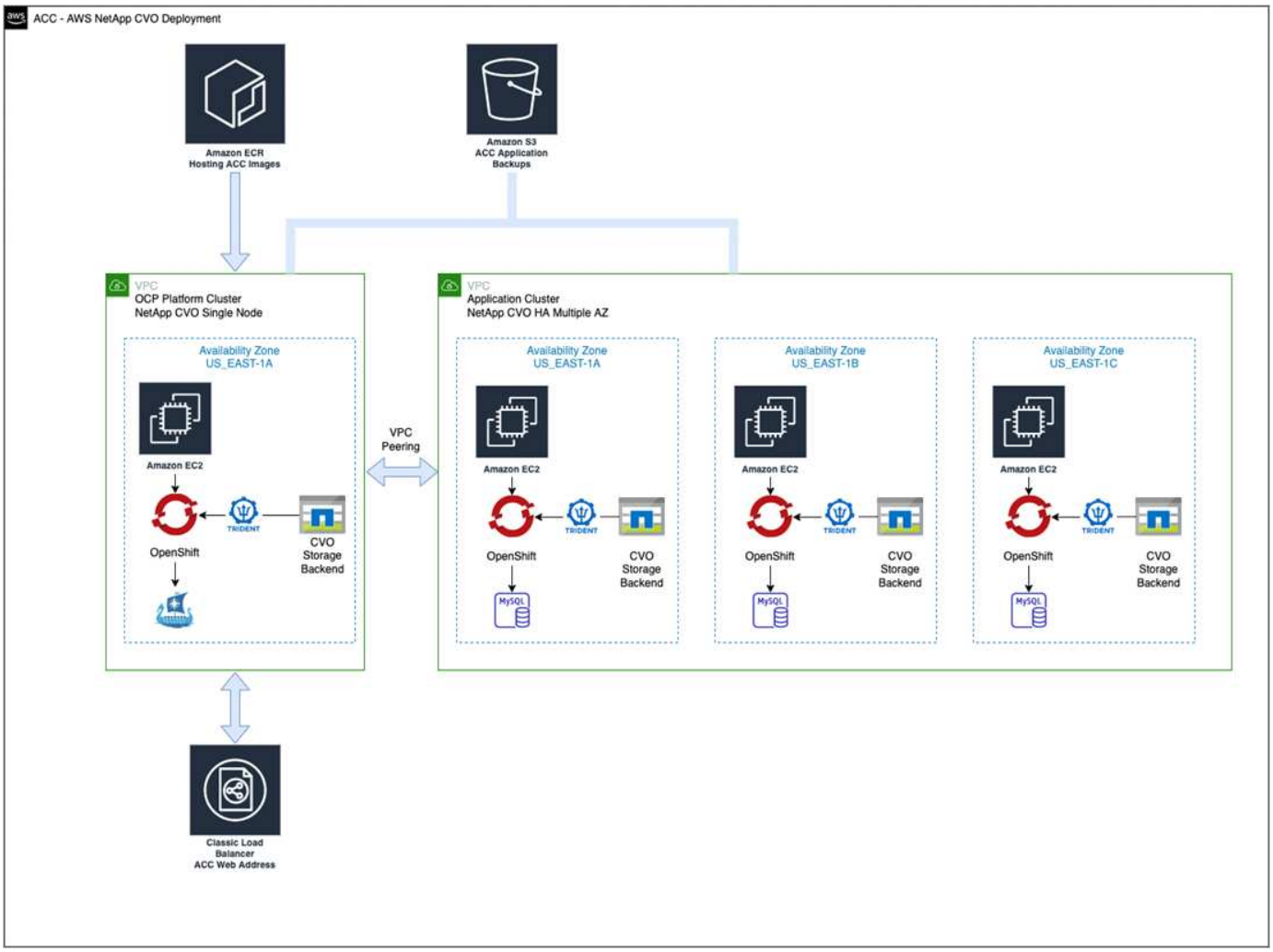
1. Crie uma rede virtual da AWS.
2. Analise as instâncias de computação do EC2. Isso pode ser um servidor bare metal ou VMs na AWS.
3. Se o tipo de instância ainda não corresponder aos requisitos mínimos de recursos do Astra para nós mestres e trabalhadores, altere o tipo de instância na AWS para atender aos requisitos do Astra. "Requisitos do Astra Control Center"Consulte .
4. Crie pelo menos um bucket do AWS S3 para armazenar seus backups.
5. Crie um AWS Elastic Container Registry (ECR) para hospedar todas as imagens do ACC.

> Se você não criar o ECR, o Astra Control Center não poderá acessar dados de monitoramento de um cluster que contém o Cloud Volumes ONTAP com um back-end da AWS. O problema é causado quando o cluster que você tenta descobrir e gerenciar usando o Astra Control Center não tem acesso ao AWS ECR.

6. Envie as imagens ACC para o registo definido.

> O token AWS Elastic Container Registry (ECR) expira após 12 horas e faz com que as operações de clone entre clusters falhem. Esse problema ocorre ao gerenciar um back-end de storage do Cloud Volumes ONTAP configurado para AWS. Para corrigir esse problema, autentique novamente com o ECR e gere um novo segredo para que as operações de clone sejam retomadas com sucesso.

Veja um exemplo de implantação da AWS:



Configure o NetApp Cloud Manager

Usando o Cloud Manager, crie uma área de trabalho, adicione um conetor à AWS, crie um ambiente de trabalho e importe o cluster.

Siga a documentação do Cloud Manager para concluir as etapas a seguir. Veja o seguinte:

- "Introdução ao Cloud Volumes ONTAP na AWS".
- "Crie um conetor na AWS usando o Cloud Manager"

Passos

1. Adicione suas credenciais ao Cloud Manager.
2. Criar um espaço de trabalho.
3. Adicione um conetor para a AWS. Escolha a AWS como o provedor.
4. Crie um ambiente de trabalho para seu ambiente de nuvem.
   a. Localização: "Amazon Web Services (AWS)"
   b. Tipo: "Cloud Volumes ONTAP HA"
5. Importe o cluster OpenShift. O cluster se conetará ao ambiente de trabalho que você acabou de criar.
   a. Veja os detalhes do cluster do NetApp selecionando **K8s** > **Lista de clusters** > **Detalhes do cluster**.

b. No canto superior direito, observe a versão do Trident.

c. Observe as classes de storage de cluster do Cloud Volumes ONTAP que mostram o NetApp como o provisionador.

   Isso importa seu cluster Red Hat OpenShift e atribui a ele uma classe de armazenamento padrão. Você seleciona a classe de armazenamento. O Trident é instalado automaticamente como parte do processo de importação e descoberta.

6. Observe todos os volumes e volumes persistentes nessa implantação do Cloud Volumes ONTAP.

O Cloud Volumes ONTAP pode operar como um único nó ou em alta disponibilidade. Se a HA estiver ativada, observe o status da HA e o status da implantação do nó em execução na AWS.

Instale o Astra Control Center

Siga o padrão "Instruções de instalação do Astra Control Center".

Implante o Astra Control Center no Microsoft Azure

É possível implantar o Astra Control Center em um cluster Kubernetes autogerenciado, hospedado em uma nuvem pública do Microsoft Azure.

O que você precisará para o Azure

Antes de implantar o Astra Control Center no Azure, você precisará dos seguintes itens:

- Licença do Astra Control Center. "Requisitos de licenciamento do Astra Control Center"Consulte .
- "Atender aos requisitos do Astra Control Center".
- Conta do NetApp Cloud Central
- Red Hat OpenShift Container Platform (OCP) 4,8
- Permissões do Red Hat OpenShift Container Platform (OCP) (no nível do namespace para criar pods)
- Credenciais do Azure com permissões que permitem criar buckets e conetores

Requisitos de ambiente operacional para o Azure

Certifique-se de que o ambiente operacional escolhido para hospedar o Astra Control Center atenda aos requisitos básicos de recursos descritos na documentação oficial do ambiente.

O Astra Control Center requer os seguintes recursos, além dos requisitos de recursos do ambiente:

"Requisitos do ambiente operacional do Astra Control Center"Consulte .

Componente	Requisito
Capacidade de storage do NetApp Cloud Volumes ONTAP no back-end	Pelo menos 300GB disponível
Nós de trabalho (requisito de computação do Azure)	No total, pelo menos 3 nós de trabalho, com 4 núcleos vCPU e 12GB GB de RAM cada

Componente	Requisito
Balanceador de carga	Tipo de serviço "LoadBalancer" disponível para envio de tráfego de entrada para serviços no cluster do ambiente operacional
FQDN (zona DNS do Azure)	Um método para apontar o FQDN do Astra Control Center para o endereço IP balanceado de carga
Astra Trident (instalado como parte da descoberta de clusters do Kubernetes no NetApp Cloud Manager)	O Astra Trident 21,04 ou mais recente instalado e configurado e o NetApp ONTAP versão 9,5 ou mais recente serão usados como um back-end de storage
Registo de imagens	Você deve ter um Registro privado existente, como o Azure Container Registry (ACR), para o qual você pode enviar imagens de compilação do Astra Control Center. Você precisa fornecer o URL do Registro de imagens onde você vai carregar as imagens. Você precisa habilitar o acesso anônimo para extrair imagens Restic para backups.
Configuração Astra Trident/ONTAP	O Astra Control Center exige que uma classe de storage seja criada e definida como a classe de storage padrão. O Astra Control Center é compatível com as seguintes classes de storage do ONTAP Kubernetes criadas quando você importa o cluster do Kubernetes para o NetApp Cloud Manager. Eles são fornecidos pelo Astra Trident: • `vsaworkingenvironment-<>-ha-nas csi.trident.netapp.io` • `vsaworkingenvironment-<>-ha-san csi.trident.netapp.io` • `vsaworkingenvironment-<>-single-nas csi.trident.netapp.io` • `vsaworkingenvironment-<>-single-san csi.trident.netapp.io`

Esses requisitos presumem que o Astra Control Center é a única aplicação em execução no ambiente operacional. Se o ambiente estiver executando aplicativos adicionais, ajuste esses requisitos mínimos de acordo.

Visão geral da implantação para o Azure

Aqui está uma visão geral do processo para instalar o Astra Control Center para Azure.

Cada uma destas etapas é explicada em mais detalhes abaixo.

1. Instale um cluster RedHat OpenShift no Azure.
2. Criar grupos de recursos do Azure.

3. Certifique-se de que tem permissões IAM suficientes.
4. Configurar o Azure.
5. Configure o NetApp Cloud Manager.
6. Instalar e configurar o Astra Control Center.

Instale um cluster RedHat OpenShift no Azure

O primeiro passo é instalar um cluster RedHat OpenShift no Azure.

Para obter instruções de instalação, consulte a documentação do RedHat em "Instalando o cluster OpenShift no Azure" e "Instalando uma conta do Azure".

Criar grupos de recursos do Azure

Crie pelo menos um grupo de recursos do Azure.

> OpenShift pode criar seus próprios grupos de recursos. Além disso, você também deve definir grupos de recursos do Azure. Consulte a documentação do OpenShift.

Você pode querer criar um grupo de recursos de cluster de plataforma e um grupo de recursos de cluster OpenShift de aplicativo de destino.

Certifique-se de que tem permissões IAM suficientes

Verifique se você tem funções e permissões suficientes do IAM que permitem instalar um cluster do RedHat OpenShift e um conetor do NetApp Cloud Manager.

```
https://docs.netapp.com/us-en/cloud-manager-setup-admin/concept-accounts-
azure.html["Credenciais e permissões do Azure"^]Consulte .
```

Configurar o Azure

Em seguida, configure o Azure para criar uma rede virtual, configurar instâncias de computação, criar um contentor Blob do Azure, criar um ACR (Registro de contentor do Azure) para hospedar as imagens do Astra Control Center e enviar as imagens para esse Registro.

Siga a documentação do Azure para concluir as etapas a seguir. "Instalando o cluster OpenShift no Azure"Consulte .

1. Crie uma rede virtual do Azure.
2. Revise as instâncias de computação. Isso pode ser um servidor bare metal ou VMs no Azure.
3. Se o tipo de instância ainda não corresponder aos requisitos mínimos de recursos do Astra para nós mestres e trabalhadores, altere o tipo de instância no Azure para atender aos requisitos do Astra. "Requisitos do Astra Control Center"Consulte .
4. Crie pelo menos um contêiner do Blob do Azure para armazenar seus backups.
5. Crie uma conta de armazenamento. Você precisará de uma conta de storage para criar um contêiner para ser usado como um bucket no Astra Control Center.
6. Crie um segredo, que é necessário para o acesso ao bucket.

7. Crie um ACR (Azure Container Registry) para hospedar todas as imagens do Astra Control Center.
8. Configure o acesso ACR para o Docker push/pull de todas as imagens do Astra Control Center.
9. Empurre as imagens ACC para este registo introduzindo o seguinte script:

```
az acr login -n <AZ ACR URL/Location>
This script requires ACC manifest file and your Azure ACR location.
```

Exemplo:

```
manifestfile=astra-control-center-<version>.manifest
AZ_ACR_REGISTRY=<target image repository>
ASTRA_REGISTRY=<source ACC image repository>

while IFS= read -r image; do
    echo "image: $ASTRA_REGISTRY/$image $AZ_ACR_REGISTRY/$image"
    root_image=${image%:*}
    echo $root_image
    docker pull $ASTRA_REGISTRY/$image
    docker tag $ASTRA_REGISTRY/$image $AZ_ACR_REGISTRYY/$image
    docker push $AZ_ACR_REGISTRY/$image
done < astra-control-center-22.04.41.manifest
```

10. Configurar zonas DNS.

Configure o NetApp Cloud Manager

Usando o Cloud Manager, crie uma área de trabalho, adicione um conetor ao Azure, crie um ambiente de trabalho e importe o cluster.

Siga a documentação do Cloud Manager para concluir as etapas a seguir. "Introdução ao Cloud Manager no Azure"Consulte .

O que você vai precisar

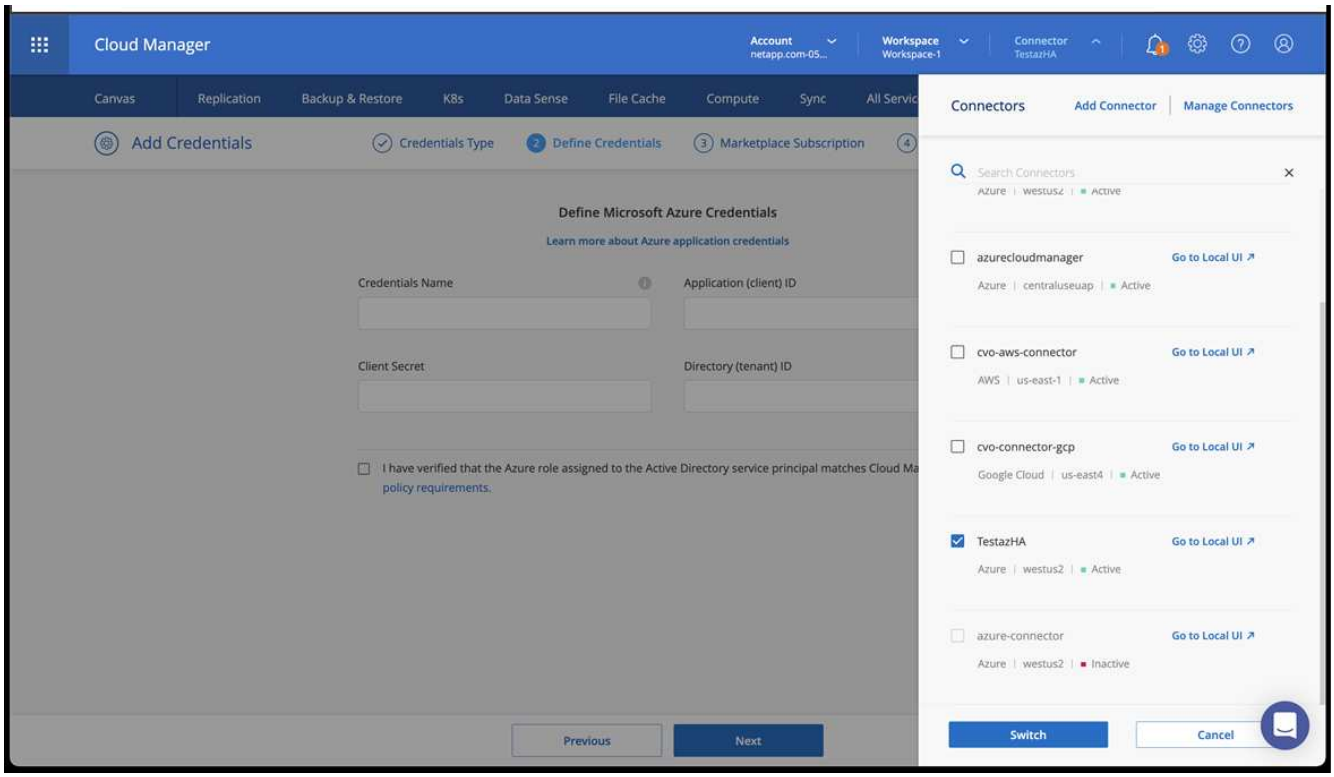
Acesso à conta do Azure com as permissões e funções necessárias do IAM

Passos

1. Adicione suas credenciais ao Cloud Manager.
2. Adicione um conetor para o Azure. "Políticas do Cloud Manager"Consulte .
   a. Escolha **Azure** como Provedor.
   b. Insira as credenciais do Azure, incluindo o ID do aplicativo, o segredo do cliente e o ID do diretório (locatário).

```
https://docs.netapp.com/us-
en/occm/task_creating_connectors_azure.html["Criando um conetor no
Azure a partir do Cloud Manager"^]Consulte .
```

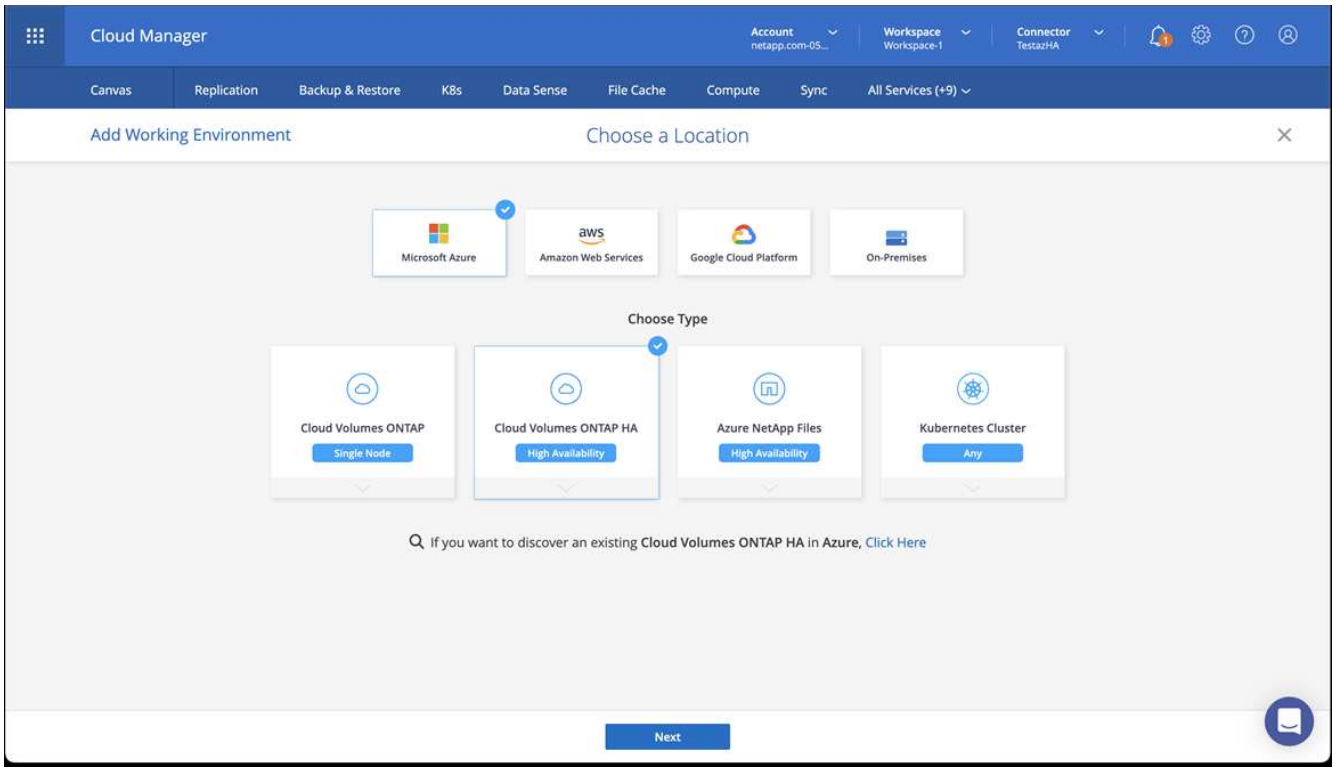
3. Certifique-se de que o conetor está a funcionar e mude para esse conetor.



4. Crie um ambiente de trabalho para seu ambiente de nuvem.

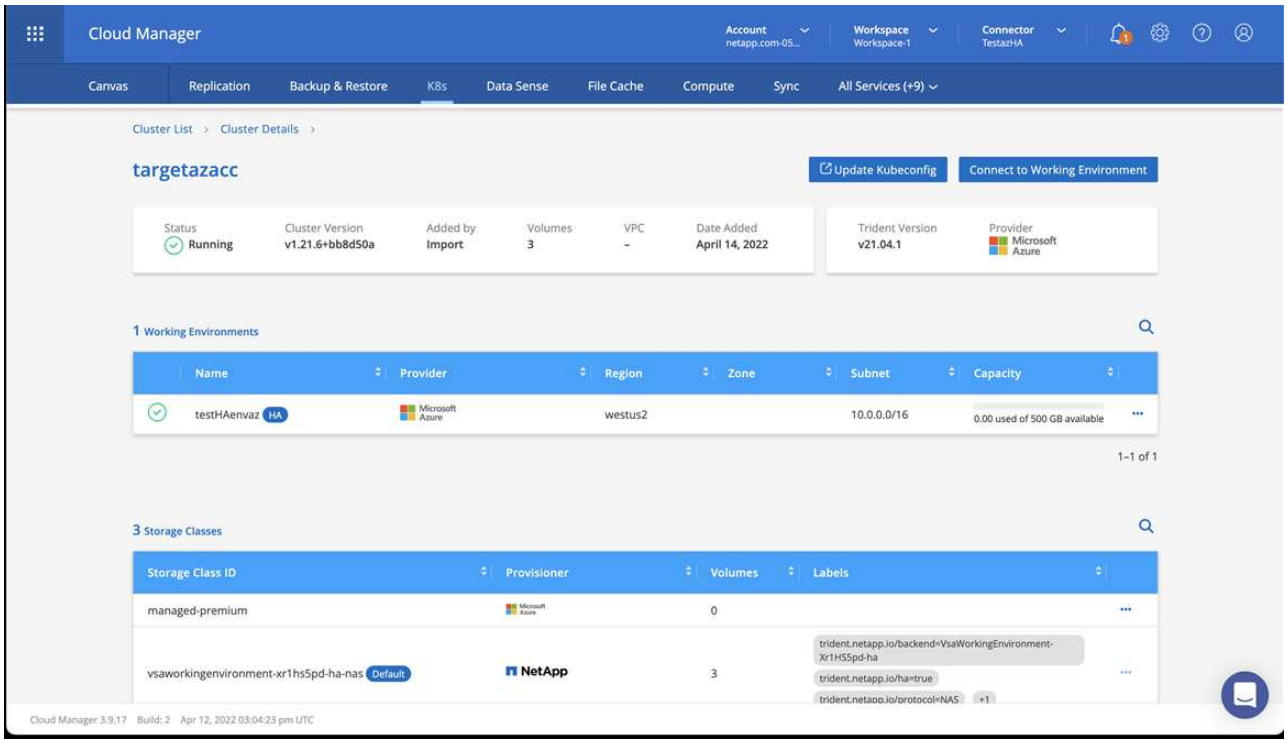
   a. Localização: "Microsoft Azure".

   b. Tipo: "Cloud Volumes ONTAP HA".



5. Importe o cluster OpenShift. O cluster se conetará ao ambiente de trabalho que você acabou de criar.

   a. Veja os detalhes do cluster do NetApp selecionando **K8s** > **Lista de clusters** > **Detalhes do cluster**.



   b. No canto superior direito, observe a versão do Trident.

   c. Observe as classes de storage de cluster do Cloud Volumes ONTAP que mostram o NetApp como o provisionador.

Isso importa seu cluster Red Hat OpenShift e atribui uma classe de armazenamento padrão. Você

seleciona a classe de armazenamento. O Trident é instalado automaticamente como parte do processo de importação e descoberta.

6. Observe todos os volumes e volumes persistentes nessa implantação do Cloud Volumes ONTAP.
7. O Cloud Volumes ONTAP pode operar como um único nó ou em alta disponibilidade. Se a HA estiver ativada, observe o status da HA e o status da implantação do nó em execução no Azure.

Instalar e configurar o Astra Control Center

Instalar o Astra Control Center com o padrão "instruções de instalação".

Usando o Astra Control Center, adicione um bucket do Azure. "Configure o Astra Control Center e adicione buckets"Consulte .

Configure o Astra Control Center

O Astra Control Center dá suporte e monitora o ONTAP e o Astra Data Store como o back-end de storage. Depois de instalar o Astra Control Center, fazer login na IU e alterar sua senha, você deseja configurar uma licença, adicionar clusters, gerenciar storage e adicionar buckets.

Tarefas

- Adicione uma licença para o Astra Control Center
- Adicionar cluster
- Adicionar um back-end de storage
- Adicione um balde

Adicione uma licença para o Astra Control Center

Você pode adicionar uma nova licença usando a IU ou "API" obter a funcionalidade completa do Astra Control Center. Sem licença, seu uso do Astra Control Center se limita ao gerenciamento de usuários e à adição de novos clusters.

Para obter mais informações sobre como as licenças são calculadas, "Licenciamento"consulte .

> Para atualizar uma avaliação existente ou uma licença completa, "Atualizar uma licença existente"consulte .

As licenças do Astra Control Center medem recursos de CPU usando unidades de CPU Kubernetes. A licença precisa ter em conta os recursos de CPU atribuídos aos nós de trabalho de todos os clusters do Kubernetes gerenciados. Antes de adicionar uma licença, você precisa obter o arquivo de licença (NLF) do "Site de suporte da NetApp".

Você também pode experimentar o Astra Control Center com uma licença de avaliação, que permite usar o Astra Control Center por 90 dias a partir da data em que você baixar a licença. Você pode se inscrever para uma avaliação gratuita registrando "aqui"o .

> Se a instalação aumentar para exceder o número licenciado de unidades de CPU, o Astra Control Center impedirá que você gerencie novas aplicações. É apresentado um alerta quando a capacidade é ultrapassada.

O que você vai precisar

Quando você baixou o Centro de Controle Astra do "Site de suporte da NetApp", você também baixou o arquivo de licença NetApp (NLF). Certifique-se de que tem acesso a este ficheiro de licença.

Passos

1. Faça login na IU do Astra Control Center.
2. Selecione **conta** > **Licença**.
3. Selecione **Adicionar licença**.
4. Navegue até o arquivo de licença (NLF) que você baixou.
5. Selecione **Adicionar licença**.

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

Se você tiver uma licença de avaliação, certifique-se de armazenar o ID da conta para evitar perda de dados em caso de falha do Astra Control Center se você não estiver enviando ASUPs.

Adicionar cluster

Para começar a gerenciar suas aplicações, adicione um cluster do Kubernetes e gerencie-o como um recurso de computação. Você precisa adicionar um cluster para Astra Control Center para descobrir suas aplicações Kubernetes. No Astra Data Store, você deseja adicionar o cluster de aplicações Kubernetes que contém aplicações que estão usando volumes provisionados pelo Astra Data Store.

Recomendamos que o Astra Control Center gerencie o cluster em que ele é implantado primeiro antes de adicionar outros clusters ao Astra Control Center para gerenciar. Ter o cluster inicial sob gerenciamento é necessário enviar dados do Kubemetrics e dados associados ao cluster para métricas e solução de problemas. Você pode usar o recurso **Adicionar cluster** para gerenciar um cluster com o Astra Control Center.

Quando o Astra Control gerencia um cluster, ele controla a classe de storage padrão do cluster. Se você alterar a classe de armazenamento usando `kubectl` comandos, o Astra Control reverte a alteração. Para alterar a classe de storage padrão em um cluster gerenciado pelo Astra Control, use um dos seguintes métodos:

- Use o endpoint da API Astra Control `PUT /managedClusters` e atribua uma classe de storage padrão diferente com o `DefaultStorageClass` parâmetro.
- Use a IU da Web Astra Control para atribuir uma classe de storage padrão diferente. Altere a classe de armazenamento padrãoConsulte .

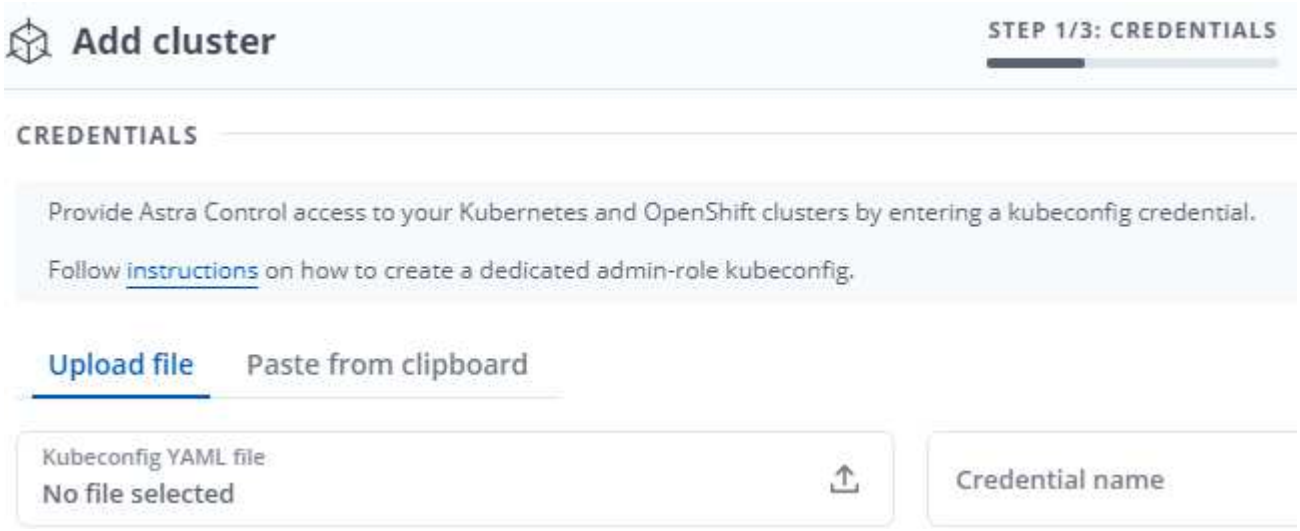
O que você vai precisar

- Antes de adicionar um cluster, revise e execute o "tarefas pré-requisitos"necessário .

Passos

1. No **Dashboard** na IU do Astra Control Center, selecione **Add** na seção clusters.
2. Na janela **Add Cluster** que se abre, carregue um `kubeconfig.yaml` ficheiro ou cole o conteúdo de um `kubeconfig.yaml` ficheiro.

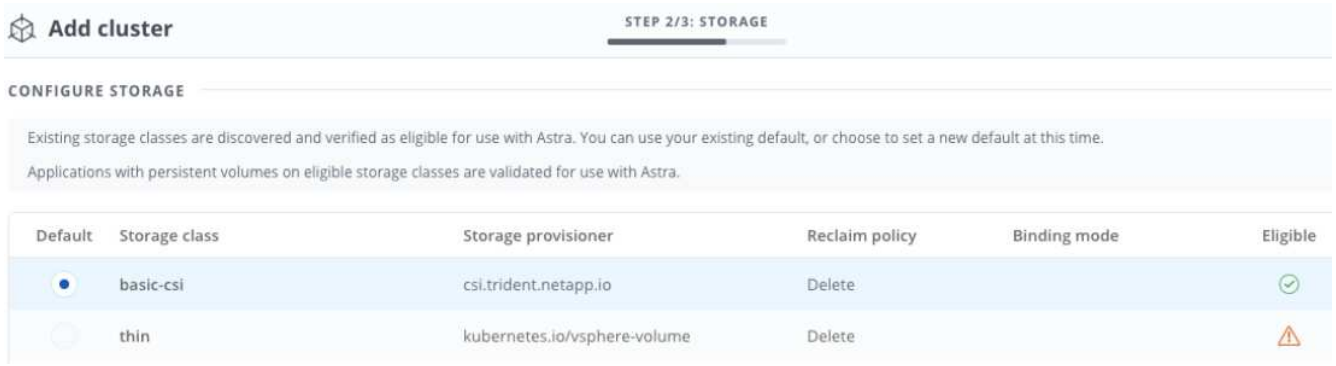
O `kubeconfig.yaml` arquivo deve incluir **somente a credencial de cluster para um cluster**.



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

3. Forneça um nome de credencial. Por padrão, o nome da credencial é preenchido automaticamente como o nome do cluster.
4. Selecione **Configurar armazenamento**.
5. Selecione a classe de armazenamento a ser usada para este cluster do Kubernetes e selecione **Review**.

Você deve selecionar uma classe de storage do Trident com o suporte do ONTAP Storage ou do Astra Data Store.



6. Revise as informações e, se tudo estiver bem, selecione **Adicionar cluster**.

Resultado

O cluster insere o status **Descobrindo** e, em seguida, muda para **Running**. Você adicionou com sucesso um cluster do Kubernetes e agora o está gerenciando no Astra Control Center.

Depois de adicionar um cluster a ser gerenciado no Astra Control Center, talvez demore alguns minutos para implantar o operador de monitoramento. Até então, o ícone de notificação fica vermelho e Registra um evento **Falha na verificação do status do agente de monitoramento**. Você pode ignorar isso, porque o problema resolve quando o Astra Control Center obtém o status correto. Se o problema não resolver em alguns minutos, vá para o cluster e execute `oc get pods -n netapp-monitoring` como ponto de partida. Você precisará examinar os logs do operador de monitoramento para depurar o problema.

Adicionar um back-end de storage

Você pode adicionar um back-end de storage para que o Astra Control possa gerenciar seus recursos. Você pode implantar um back-end de storage em um cluster gerenciado ou usar um back-end de storage existente.

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.

O que você precisará para implantações atuais do Astra Data Store

- Você adicionou o cluster de aplicações Kubernetes e o cluster de computação subjacente.

Depois de adicionar o cluster de aplicações Kubernetes para Astra Data Store e ser gerenciado pelo Astra Control, o cluster aparece como `unmanaged` na lista de back-ends descobertos. Em seguida, adicione o cluster de computação que contém o Astra Data Store e que está subjacente ao cluster de aplicações Kubernetes. Você pode fazer isso a partir de **backends** na interface do usuário. Selecione o menu ações do cluster, selecione `Manage`, e "adicione o cluster". Após o estado do cluster `unmanaged` das alterações no nome do cluster do Kubernetes, você pode continuar adicionando um back-end.

O que você precisará para novas implantações do Astra Data Store

- Você "carregou a versão do pacote de instalação que pretende implementar" precisa de um local acessível para o Astra Control.
- Você adicionou o cluster do Kubernetes que pretende usar para implantação.
- Você carregou o Licença do Astra Data Store para sua implantação em um local acessível ao Astra Control.

Opções

- Implantar recursos de storage
- Usar um back-end de storage existente

Implantar recursos de storage

Você pode implantar um novo Astra Data Store e gerenciar o back-end de storage associado.

Passos

1. Navegue no Dashboard ou no menu backends:
   - Em **Painel**: No Resumo de recursos, selecione um link no painel de back-ends de armazenamento e selecione **Adicionar** na seção backends.
   - De **backends**:
     i. Na área de navegação à esquerda, selecione **backends**.

ii. Selecione **Adicionar**.

2. Selecione a opção de implantação **Astra Data Store** na guia **Deploy**.
3. Selecione o pacote Astra Data Store a ser implantado:
   a. Insira um nome para a aplicação Astra Data Store.
   b. Escolha a versão do Astra Data Store que você deseja implantar.

> Se ainda não tiver carregado a versão que pretende implementar, pode utilizar a opção **Adicionar pacote** ou sair do assistente e utilizar "gerenciamento de pacotes" para carregar o pacote de instalação.

4. Selecione uma licença do Astra Data Store que você tenha carregado anteriormente ou use a opção **Adicionar licença** para carregar uma licença para usar com o aplicativo.

> As licenças do Astra Data Store com permissões completas estão associadas ao cluster do Kubernetes, e esses clusters associados devem aparecer automaticamente. Se não houver cluster gerenciado, você poderá selecionar a opção **Adicionar um cluster** para adicionar um ao gerenciamento do Astra Control. Para licenças Astra Data Store, se não tiver sido feita nenhuma associação entre a licença e o cluster, você poderá definir essa associação na próxima página do assistente.

5. Se você não adicionou um cluster Kubernetes ao gerenciamento do Astra Control, precisará fazê-lo na página **cluster Kubernetes**. Selecione um cluster existente na lista ou selecione **Adicionar o cluster subjacente** para adicionar um cluster ao gerenciamento do Astra Control.
6. Selecione o tamanho do modelo de implantação para o cluster do Kubernetes que fornecerá recursos para o Astra Data Store.

> Ao escolher um modelo, selecione nós maiores com mais memória e núcleos para cargas de trabalho maiores ou um número maior de nós para cargas de trabalho menores. Você deve selecionar um modelo com base no que sua licença permite. Cada opção de modelo sugere o número de nós elegíveis que satisfazem o padrão de modelo para memória e núcleos e capacidade para cada nó.

7. Configure os nós:
   a. Adicione um rótulo de nó para identificar o pool de nós de trabalho compatível com este cluster Astra Data Store.

> O rótulo deve ser adicionado a cada nó individual no cluster que será usado para a implantação do Astra Data Store antes do início da implantação ou da implantação falhar.

   b. Configure a capacidade (GiB) por nó manualmente ou selecione a capacidade máxima do nó permitida.
   c. Configure um número máximo de nós permitidos no cluster ou permita o número máximo de nós no cluster.
8. (Somente licenças completas do Astra Data Store) Insira a chave do rótulo que deseja usar para domínios de proteção.

Crie pelo menos três rótulos exclusivos para a chave para cada nó. Por exemplo, se a chave for `astra.datastore.protection.domain`, você poderá criar os seguintes rótulos: `astra.datastore.protection.domain=domain1` ,`astra.datastore.protection.domain=domain2`, E `astra.datastore.protection.domain=domain3`.

9. Configure a rede de gerenciamento:
   a. Insira um endereço IP de gerenciamento para o gerenciamento interno do Astra Data Store que esteja na mesma sub-rede que os endereços IP do nó de trabalho.
   b. Escolha usar a mesma NIC para redes de gerenciamento e dados ou configurá-las separadamente.
   c. Insira o pool de endereços IP da rede de dados, a máscara de sub-rede e o gateway para acesso ao armazenamento.
10. Revise a configuração e selecione **Deploy** para iniciar a instalação.

Resultado

Após uma instalação bem-sucedida, o back-end aparece `available` no estado na lista de backends junto com informações de desempenho ativo.

Talvez seja necessário atualizar a página para que o backend apareça.

Usar um back-end de storage existente

Você pode trazer um back-end de storage descoberto do ONTAP ou Astra Data Store para o gerenciamento do Astra Control Center.

Passos

1. Navegue no Dashboard ou no menu backends:
   - Em **Painel**: No Resumo de recursos, selecione um link no painel de back-ends de armazenamento e selecione **Adicionar** na seção backends.
   - De **backends**:
     i. Na área de navegação à esquerda, selecione **backends**.
     ii. Selecione **Gerenciar** em um back-end descoberto no cluster gerenciado ou selecione **Adicionar** para gerenciar um back-end existente adicional.
2. Selecione a guia **usar existente**.
3. Siga um destes procedimentos dependendo do tipo de back-end:
   - **Astra Data Store**:
     i. Selecione **Astra Data Store**.
     ii. Selecione o cluster de computação gerenciada e selecione **Next**.
     iii. Confirme os detalhes do back-end e selecione **Add storage backend**.
   - **ONTAP**:
     i. Selecione **ONTAP**.
     ii. Insira as credenciais de administrador do ONTAP e selecione **Revisão**.
     iii. Confirme os detalhes do back-end e selecione **Add storage backend**.

Resultado

O backend aparece `available` no estado na lista com informações de resumo.

Talvez seja necessário atualizar a página para que o backend apareça.

Adicione um balde

Adicionar fornecedores de bucket do armazenamento de objetos é essencial para fazer backup das aplicações e do storage persistente ou clonar aplicações entre clusters. O Astra Control armazena os backups ou clones nos buckets do armazenamento de objetos que você define.

Quando você adiciona um bucket, o Astra Control marca um bucket como o indicador padrão do bucket. O primeiro bucket que você criar se torna o bucket padrão.

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

Utilize qualquer um dos seguintes tipos de balde:

- NetApp ONTAP S3
- NetApp StorageGRID S3
- Genérico 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.

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

Passos

1. Na área de navegação à esquerda, selecione **Buckets**.
   a. Selecione **Adicionar**.
   b. Selecione o tipo de balde.

      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.

   c. Crie um novo nome de bucket ou insira um nome de bucket existente e uma descrição opcional.

      O nome e a descrição do bucket aparecem como um local de backup que você pode escolher mais tarde ao criar um backup. O nome também aparece durante a configuração da política de proteção.

   d. Introduza o nome ou endereço IP do endpoint S3.
   e. Se você quiser que esse bucket seja o bucket padrão para todos os backups, marque a `Make this bucket the default bucket for this private cloud` opção.

Esta opção não aparece para o primeiro bucket criado.

f. Continue adicionando informações de credenciais.

Adicionar credenciais de acesso S3

Adicione credenciais de acesso S3 a qualquer momento.

Passos

1. Na caixa de diálogo baldes, selecione a guia **Adicionar** ou **usar existente**.
   a. Insira um nome para a credencial que a distingue de outras credenciais no Astra Control.
   b. Insira a ID de acesso e a chave secreta colando o conteúdo da área de transferência.

Altere a classe de armazenamento padrão

Você pode alterar a classe de armazenamento padrão para um cluster.

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**.

O que se segue?

Agora que você fez login e adicionou clusters ao Astra Control Center, está pronto para começar a usar os recursos de gerenciamento de dados de aplicações do Astra Control Center.

- "Gerenciar usuários"
- "Comece a gerenciar aplicativos"
- "Proteja aplicativos"
- "Clonar aplicações"
- "Gerenciar notificações"
- "Conete-se ao Cloud Insights"
- "Adicione um certificado TLS personalizado"

Encontre mais informações

- "Use a API Astra Control"
- "Problemas conhecidos"

Pré-requisitos para adicionar um cluster

Você deve garantir que as condições de pré-requisito sejam atendidas antes de adicionar um cluster. Você

também deve executar as verificações de qualificação para garantir que seu cluster esteja pronto para ser adicionado ao Astra Control Center.

O que você precisará antes de adicionar um cluster

- Um dos seguintes tipos de clusters:
  - Clusters executando OpenShift 4,6.8, 4,7, 4,8 ou 4,9
  - Clusters executando Rancher 2,5.8, 2,5.9, ou 2,6 com RKE1
  - Clusters que executam o Kubernetes 1,20 a 1,23
  - Clusters executando o VMware Tanzu Kubernetes Grid 1,4
  - Clusters executando o VMware Tanzu Kubernetes Grid Integrated Edition 1.12.2

    Verifique se os clusters têm um ou mais nós de trabalho com pelo menos 1GB GB de RAM disponíveis para executar serviços de telemetria.

> Se você pretende adicionar um segundo cluster do OpenShift 4,6, 4,7 ou 4,8 como um recurso de computação gerenciado, certifique-se de que o recurso Snapshot de volume do Astra Trident esteja ativado. Consulte o Astra Trident oficial "instruções" para habilitar e testar snapshots de volume com o Astra Trident.

- StorageClasses Astra Trident configurados com a "back-end de storage compatível" (necessários para qualquer tipo de cluster)
- O superusuário e ID de usuário definidos no sistema ONTAP de backup para fazer backup e restaurar aplicativos com o Centro de Controle Astra. Execute o seguinte comando na linha de comando ONTAP: `export-policy rule modify -vserver <storage virtual machine name> -policyname <policy name> -ruleindex 1 -superuser sysm --anon 65534`
- Um objeto Astra Trident `volumesnapshotclass` definido por um administrador. Consulte o Astra Trident "instruções" para habilitar e testar snapshots de volume com o Astra Trident.
- Certifique-se de que você tenha apenas uma única classe de storage padrão definida para o cluster do Kubernetes.

Execute verificações de qualificação

Execute as seguintes verificações de qualificação para garantir que o cluster esteja pronto para ser adicionado ao Astra Control Center.

Passos

1. Verifique a versão do Trident.

```
kubectl get tridentversions -n trident
```

   Se o Trident existir, você verá uma saída semelhante à seguinte:

```
NAME      VERSION
trident   21.04.0
```

Se o Trident não existir, você verá uma saída semelhante à seguinte:

```
error: the server doesn't have a resource type "tridentversions"
```

Se o Trident não estiver instalado ou a versão instalada não for a mais recente, você precisará instalar a versão mais recente do Trident antes de continuar. Consulte "Documentação do Trident" para obter instruções.

2. Verifique se as classes de armazenamento estão usando os drivers Trident suportados. O nome do provisionador deve ser `csi.trident.netapp.io`. Veja o exemplo a seguir:

```
kubectl get sc
NAME                     PROVISIONER                    RECLAIMPOLICY
VOLUMEBINDINGMODE   ALLOWVOLUMEEXPANSION   AGE
ontap-gold (default)   csi.trident.netapp.io          Delete
Immediate           true                   5d23h
thin                   kubernetes.io/vsphere-volume   Delete
Immediate           false                  6d
```

Crie uma função admin kubeconfig

Certifique-se de que tem o seguinte na sua máquina antes de executar os passos:

- `kubectl` v1,19 ou posterior instalado
- Um kubeconfig ativo com direitos de administrador de cluster para o contexto ativo

Passos

1. Crie uma conta de serviço da seguinte forma:

   a. Crie um arquivo de conta de serviço `astracontrol-service-account.yaml`chamado .

      Ajuste o nome e o namespace conforme necessário. Se as alterações forem feitas aqui, você deve aplicar as mesmas alterações nas etapas a seguir.

```
<strong>astracontrol-service-account.yaml</strong>
```

+

```
apiVersion: v1
kind: ServiceAccount
metadata:
  name: astracontrol-service-account
  namespace: default
```

a. Aplique a conta de serviço:

```
kubectl apply -f astracontrol-service-account.yaml
```

2. (Opcional) se o cluster usar uma política de segurança de pod restritiva que não permita a criação de pod privilegiados ou permitir que processos nos contentores de pod sejam executados como usuário raiz, crie uma política de segurança de pod personalizada para o cluster que permita que o Astra Control crie e gerencie pods. Para obter instruções, "Crie uma política de segurança de pod personalizada"consulte .
3. Conceda permissões de administrador do cluster da seguinte forma:

a. Crie um `ClusterRoleBinding` arquivo chamado `astracontrol-clusterrolebinding.yaml`.

Ajuste quaisquer nomes e namespaces modificados ao criar a conta de serviço conforme necessário.

```
<strong>astracontrol-clusterrolebinding.yaml</strong>
```

+

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: astracontrol-admin
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: cluster-admin
subjects:
- kind: ServiceAccount
  name: astracontrol-service-account
  namespace: default
```

a. Aplicar a vinculação de funções do cluster:

```
kubectl apply -f astracontrol-clusterrolebinding.yaml
```

4. Liste os segredos da conta de serviço, substituindo `<context>` pelo contexto correto para sua instalação:

```
kubectl get serviceaccount astracontrol-service-account --context
<context> --namespace default -o json
```

O final da saída deve ser semelhante ao seguinte:

```
"secrets": [
{ "name": "astracontrol-service-account-dockercfg-vhz87"},
{ "name": "astracontrol-service-account-token-r59kr"}
]
```

Os índices para cada elemento no `secrets` array começam com 0. No exemplo acima, o índice para `astracontrol-service-account-dockercfg-vhz87` seria 0 e o índice para `astracontrol-service-account-token-r59kr` seria 1. Em sua saída, anote o índice do nome da conta de serviço que tem a palavra "token" nele.

5. Gere o kubeconfigo da seguinte forma:
   a. Crie um `create-kubeconfig.sh` arquivo. Substitua `TOKEN_INDEX` no início do script a seguir pelo valor correto.

```
<strong>create-kubeconfig.sh</strong>
```

```
# Update these to match your environment.
# Replace TOKEN_INDEX with the correct value
# from the output in the previous step. If you
# didn't change anything else above, don't change
# anything else here.

SERVICE_ACCOUNT_NAME=astracontrol-service-account
NAMESPACE=default
NEW_CONTEXT=astracontrol
KUBECONFIG_FILE='kubeconfig-sa'

CONTEXT=$(kubectl config current-context)

SECRET_NAME=$(kubectl get serviceaccount ${SERVICE_ACCOUNT_NAME} \
  --context ${CONTEXT} \
  --namespace ${NAMESPACE} \
  -o jsonpath='{.secrets[TOKEN_INDEX].name}')
TOKEN_DATA=$(kubectl get secret ${SECRET_NAME} \
  --context ${CONTEXT} \
  --namespace ${NAMESPACE} \
  -o jsonpath='{.data.token}')

TOKEN=$(echo ${TOKEN_DATA} | base64 -d)

# Create dedicated kubeconfig
# Create a full copy
kubectl config view --raw > ${KUBECONFIG_FILE}.full.tmp
```

```
# Switch working context to correct context
kubectl --kubeconfig ${KUBECONFIG_FILE}.full.tmp config use-context
${CONTEXT}

# Minify
kubectl --kubeconfig ${KUBECONFIG_FILE}.full.tmp \
  config view --flatten --minify > ${KUBECONFIG_FILE}.tmp

# Rename context
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  rename-context ${CONTEXT} ${NEW_CONTEXT}

# Create token user
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  set-credentials ${CONTEXT}-${NAMESPACE}-token-user \
  --token ${TOKEN}

# Set context to use token user
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  set-context ${NEW_CONTEXT} --user ${CONTEXT}-${NAMESPACE}-token
-user

# Set context to correct namespace
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  set-context ${NEW_CONTEXT} --namespace ${NAMESPACE}

# Flatten/minify kubeconfig
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  view --flatten --minify > ${KUBECONFIG_FILE}

# Remove tmp
rm ${KUBECONFIG_FILE}.full.tmp
rm ${KUBECONFIG_FILE}.tmp
```

b. Forneça os comandos para aplicá-los ao cluster do Kubernetes.

```
source create-kubeconfig.sh
```

6. (**Opcional**) Renomear o kubeconfig para um nome significativo para o cluster. Proteja a credencial do cluster.

```
chmod 700 create-kubeconfig.sh
mv kubeconfig-sa.txt YOUR_CLUSTER_NAME_kubeconfig
```

O que se segue?

Agora que você verificou que os pré-requisitos são atendidos, você está pronto para "adicione um cluster".

Encontre mais informações

- "Documentação do Trident"
- "Use a API Astra Control"

Adicione um certificado TLS personalizado

Você pode remover o certificado TLS autoassinado existente e substituí-lo por um certificado TLS assinado por uma autoridade de certificação (CA).

O que você vai precisar

- Cluster do Kubernetes com Astra Control Center instalado
- Acesso administrativo a um shell de comando no cluster para executar `kubectl` comandos
- Arquivos de chave privada e certificado da CA

Remova o certificado autoassinado

Remova o certificado TLS autoassinado existente.

1. Usando SSH, faça login no cluster do Kubernetes que hospeda o Astra Control Center como usuário administrativo.
2. Localize o segredo TLS associado ao certificado atual usando o seguinte comando, substituindo `<ACC-deployment-namespace>` pelo namespace de implantação do Astra Control Center:

```
kubectl get certificate -n <ACC-deployment-namespace>
```

3. Exclua o segredo e o certificado atualmente instalados usando os seguintes comandos:

```
kubectl delete cert cert-manager-certificates -n <ACC-deployment-
namespace>
kubectl delete secret secure-testing-cert -n <ACC-deployment-namespace>
```

Adicione um novo certificado

Adicione um novo certificado TLS assinado por uma CA.

1. Use o comando a seguir para criar o novo segredo TLS com a chave privada e os arquivos de certificado da CA, substituindo os argumentos entre colchetes> pelas informações apropriadas:

```
kubectl create secret tls <secret-name> --key <private-key-filename>
--cert <certificate-filename> -n <ACC-deployment-namespace>
```

2. Use o comando e exemplo a seguir para editar o arquivo CRD (Custom Resource Definition) do cluster e altere o `spec.selfSigned` valor para `spec.ca.secretName` se referir ao segredo TLS criado anteriormente:

```
kubectl edit clusterissuers.cert-manager.io/cert-manager-certificates -n
<ACC-deployment-namespace>
....

#spec:
#  selfSigned: {}

spec:
  ca:
    secretName: <secret-name>
```

3. Use o comando e exemplo de saída a seguir para validar se as alterações estão corretas e o cluster está pronto para validar certificados, substituindo `<ACC-deployment-namespace>` pelo namespace de implantação do Astra Control Center:

```
kubectl describe clusterissuers.cert-manager.io/cert-manager-
certificates -n <ACC-deployment-namespace>
....

Status:
  Conditions:
    Last Transition Time:  2021-07-01T23:50:27Z
    Message:               Signing CA verified
    Reason:                KeyPairVerified
    Status:                True
    Type:                  Ready
Events:                    <none>
```

4. Crie o `certificate.yaml` arquivo usando o exemplo a seguir, substituindo os valores de espaço reservado entre colchetes> por informações apropriadas:

```
apiVersion: cert-manager.io/v1
kind: Certificate
metadata:
  name: <certificate-name>
  namespace: <ACC-deployment-namespace>
spec:
  secretName: <certificate-secret-name>
  duration: 2160h # 90d
  renewBefore: 360h # 15d
  dnsNames:
  - <astra.dnsname.example.com> #Replace with the correct Astra Control
Center DNS address
  issuerRef:
    kind: ClusterIssuer
    name: cert-manager-certificates
```

5. Crie o certificado usando o seguinte comando:

```
kubectl apply -f certificate.yaml
```

6. Usando o comando a seguir e exemplo de saída, valide que o certificado foi criado corretamente e com os argumentos especificados durante a criação (como nome, duração, prazo de renovação e nomes DNS).

```
kubectl describe certificate -n <ACC-deployment-namespace>
....

Spec:
  Dns Names:
    astra.example.com
  Duration:  125h0m0s
  Issuer Ref:
    Kind:        ClusterIssuer
    Name:        cert-manager-certificates
  Renew Before:  61h0m0s
  Secret Name:   <certificate-secret-name>
Status:
  Conditions:
    Last Transition Time:  2021-07-02T00:45:41Z
    Message:               Certificate is up to date and has not expired
    Reason:                Ready
    Status:                True
    Type:                  Ready
  Not After:               2021-07-07T05:45:41Z
  Not Before:              2021-07-02T00:45:41Z
  Renewal Time:            2021-07-04T16:45:41Z
  Revision:                1
Events:                    <none>
```

7. Edite a opção TLS de CRD de entrada para apontar para o novo segredo de certificado usando o comando e o exemplo a seguir, substituindo os valores de espaço reservado entre colchetes> por informações apropriadas:

```
kubectl edit ingressroutes.traefik.containo.us -n <ACC-deployment-
namespace>
....

# tls:
#    options:
#      name: default
#    secretName: secure-testing-cert
#    store:
#      name: default

 tls:
    options:
      name: default
    secretName: <certificate-secret-name>
    store:
      name: default
```

8. Usando um navegador da Web, navegue até o endereço IP de implantação do Astra Control Center.
9. Verifique se os detalhes do certificado correspondem aos detalhes do certificado que você instalou.
10. Exporte o certificado e importe o resultado para o gerenciador de certificados no navegador da Web.

Crie uma política de segurança de pod personalizada

O Astra Control precisa criar e gerenciar pods do Kubernetes nos clusters que ele gerencia. Se o cluster usar uma política de segurança de pod restritiva que não permita a criação de pod privilegiados ou permitir que processos nos contentores de pod sejam executados como usuário raiz, você precisará criar uma política de segurança de pod menos restritiva para permitir que o Astra Control crie e gerencie esses pods.

Passos

1. Crie uma diretiva de segurança de pod para o cluster que seja menos restritiva do que a padrão e salve-a em um arquivo. Por exemplo:

```
apiVersion: policy/v1beta1
kind: PodSecurityPolicy
metadata:
  name: astracontrol
  annotations:
    seccomp.security.alpha.kubernetes.io/allowedProfileNames: '*'
spec:
  privileged: true
  allowPrivilegeEscalation: true
  allowedCapabilities:
  - '*'
  volumes:
  - '*'
  hostNetwork: true
  hostPorts:
  - min: 0
    max: 65535
  hostIPC: true
  hostPID: true
  runAsUser:
    rule: 'RunAsAny'
  seLinux:
    rule: 'RunAsAny'
  supplementalGroups:
    rule: 'RunAsAny'
  fsGroup:
    rule: 'RunAsAny'
```

2. Crie uma nova função para a diretiva de segurança do pod.

```
kubectl-admin create role psp:astracontrol \
    --verb=use \
    --resource=podsecuritypolicy \
    --resource-name=astracontrol
```

3. Vincule a nova função à conta de serviço.

```
kubectl-admin create rolebinding default:psp:astracontrol \
    --role=psp:astracontrol \
    --serviceaccount=astracontrol-service-account:default
```

Perguntas mais frequentes para o Astra Control Center

Este FAQ pode ajudar se você está apenas procurando uma resposta rápida para uma pergunta.

Visão geral

As seções a seguir fornecem respostas a algumas perguntas adicionais que você pode encontrar ao usar o Astra Control Center. Para esclarecimentos adicionais, entre em Contato com o NetApp.com

Acesso ao Astra Control Center

Qual é a URL do Astra Control?

O Astra Control Center usa autenticação local e uma URL específica para cada ambiente.

Para o URL, em um navegador, digite o nome de domínio totalmente qualificado (FQDN) definido no campo spec.astraAddress no arquivo Astra_control_center_min.yaml Custom resource definition (CRD) quando você instalou o Astra Control Center. O e-mail é o valor definido no campo spec.email no CRD astra_control_center_min.yaml.

Estou usando a licença de avaliação. Como posso mudar para a licença completa?

Você pode facilmente mudar para uma licença completa obtendo o arquivo de licença NetApp (NLF).

Passos

- Na navegação à esquerda, selecione **conta** > **Licença**.
- Selecione **Adicionar licença**.
- Navegue até o arquivo de licença que você baixou e selecione **Adicionar**.

Estou usando a licença de avaliação. Ainda posso gerenciar aplicativos?

Sim, você pode testar a funcionalidade de gerenciamento de aplicativos com a licença avaliação.

Registrando clusters do Kubernetes

Eu preciso adicionar nós de trabalho ao meu cluster do Kubernetes depois de adicionar ao Astra Control. O que devo fazer?

Novos nós de trabalho podem ser adicionados a pools existentes. Eles serão descobertos automaticamente pelo Astra Control. Se os novos nós não estiverem visíveis no Astra Control, verifique se os novos nós de trabalho estão executando o tipo de imagem suportado. Você também pode verificar a integridade dos novos nós de trabalho usando o `kubectl get nodes` comando.

Como faço para desgerenciar corretamente um cluster?

1. "Desgerenciar as aplicações do Astra Control".
2. "Desgerenciar o cluster a partir do Astra Control".

O que acontece com minhas aplicações e dados após a remoção do cluster Kubernetes do Astra Control?

A remoção de um cluster do Astra Control não fará alterações na configuração do cluster (aplicações e

storage persistente). Todos os snapshots ou backups do Astra Control feitos de aplicações nesse cluster não estarão disponíveis para restauração. Os backups de storage persistente criados pelo Astra Control permanecem no Astra Control, mas não estão disponíveis para restauração.

> Sempre remova um cluster do Astra Control antes de excluí-lo por meio de outros métodos. A exclusão de um cluster usando outra ferramenta enquanto ele ainda está sendo gerenciado pelo Astra Control pode causar problemas para sua conta Astra Control.

O NetApp Trident é desinstalado automaticamente de um cluster quando eu desgerencio? Quando você desgerencia um cluster do Astra Control Center, o Trident não é desinstalado automaticamente do cluster. Para desinstalar o Trident, você precisará "Siga estas etapas na documentação do Trident".

Gerenciamento de aplicações

O Astra Control pode implantar uma aplicação?

O Astra Control não implanta aplicações. As aplicações precisam ser implantadas fora do Astra Control.

O que acontece com as aplicações depois de parar de gerenciá-las do Astra Control?

Quaisquer backups ou snapshots existentes serão excluídos. Aplicativos e dados permanecem disponíveis. As operações de gerenciamento de dados não estarão disponíveis para aplicativos não gerenciados ou backups ou snapshots que pertençam a eles.

O Astra Control pode gerenciar uma aplicação que esteja em um storage que não seja da NetApp?

Não. Embora o Astra Control possa descobrir aplicações que estão usando storage que não é NetApp, ele não pode gerenciar uma aplicação que esteja usando storage que não seja NetApp.

Devo gerenciar o próprio Astra Control? Não, você não deve gerenciar o Astra Control por ser um "aplicativo do sistema".

Os pods não saudáveis afetam o gerenciamento de aplicativos? Se um aplicativo gerenciado tiver pods em um estado de integridade, o Astra Control não poderá criar novos backups e clones.

Operações de gerenciamento de dados

Há instantâneos na minha conta que eu não criei. De onde vieram?

Em algumas situações, o Astra Control criará automaticamente um snapshot como parte de um processo de backup, clone ou restauração.

Meu aplicativo usa vários PVS. O Astra Control fará snapshots e backups de todos esses PVCs?

Sim. Uma operação de snapshot em uma aplicação do Astra Control inclui o snapshot de todos os PVs vinculados aos PVCs da aplicação.

Posso gerenciar snapshots feitos pelo Astra Control diretamente por meio de uma interface ou storage de objetos diferente?

Não. Os snapshots e backups feitos pelo Astra Control só podem ser gerenciados com o Astra Control.

Use o Astra

Gerir aplicações

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 aplicativos no Astra Control para começar a gerenciar os aplicativos e seus recursos.

Para obter mais informações, "Requisitos de gerenciamento de aplicativos"consulte .

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) são totalmente compatíveis. 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. Esses operadores são geralmente projetados com uma arquitetura "pass-by-value" em vez de "pass-by-reference". A seguir estão alguns aplicativos de operador que seguem estes padrões:
  - "Apache K8ssandra"
  - "Jenkins CI"
  - "Cluster Percona XtraDB"

Observe que 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.

> Um operador e o aplicativo que ele instala devem usar o mesmo namespace; talvez seja necessário modificar o arquivo .yaml de implantação para que o operador garanta que esse seja o caso.

Instale aplicativos no cluster

Agora que você adicionou seu cluster ao Astra Control, você pode instalar aplicações ou gerenciar aplicações existentes no cluster. Qualquer aplicativo com escopo para um namespace pode ser gerenciado. Depois que os pods estiverem online, você poderá gerenciar a aplicação com o Astra Control.

Para obter ajuda com a implantação de aplicativos validados a partir de gráficos Helm, consulte o seguinte:

- "Implante o MariaDB a partir de um gráfico Helm"
- "Implante o MySQL a partir de um gráfico Helm"
- "Implante Postgres a partir de um gráfico Helm"
- "Implante Jenkins a partir de um gráfico Helm"

Gerir aplicações

Com o Astra Control, você gerencia suas aplicações no nível de namespace ou por rótulo Kubernetes.

As aplicações instaladas com o Helm 2 não são suportadas.

Você pode executar as seguintes atividades para gerenciar aplicativos:

- Gerir aplicações
  - Gerenciar aplicativos por namespace
  - Gerenciar aplicativos por etiqueta do Kubernetes
- Ignore as aplicações
- Desgerenciar aplicativos

O Astra Control em si não é um aplicativo padrão; é um "aplicativo do sistema". Você não deve tentar gerenciar o Astra Control por si só. O próprio Astra Control não é mostrado por padrão para gerenciamento. Para ver as aplicações do sistema, utilize o filtro "Mostrar aplicações do sistema".

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

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.

Gerenciar aplicativos por namespace

A seção **descoberto** da página Apps mostra namespaces e quaisquer aplicativos instalados pelo Helm ou aplicativos personalizados nesses namespaces. Você pode optar por gerenciar cada aplicativo individualmente ou no nível do namespace. Tudo se resume ao nível de granularidade de que você precisa para operações de proteção de dados.

Por 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 sob um único namespace.

Embora o Astra Control permita gerenciar separadamente os dois níveis da hierarquia (o namespace e os aplicativos nesse namespace), 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.

Passos

1. Na barra de navegação à esquerda, selecione **aplicações**.
2. Selecione o filtro **descoberto**.

3. Veja a lista de namespaces descobertos. Expanda o namespace para exibir os aplicativos e os recursos associados.

   O Astra Control mostra os aplicativos Helm e os aplicativos personalizados no namespace. Se os rótulos Helm estiverem disponíveis, eles serão designados com um ícone de tag.

4. Olhe para a coluna **Group** para ver em qual namespace o aplicativo está sendo executado (ele é designado com o ícone de pasta).
5. Decida se você deseja gerenciar cada aplicativo individualmente ou no nível do namespace.
6. Encontre o aplicativo desejado no nível desejado na hierarquia e selecione **Gerenciar** no menu Opções na coluna **ações**.
7. Se você não quiser gerenciar um aplicativo, selecione **Ignorar** no menu Opções na coluna **ações**.

   Por exemplo, se você quiser gerenciar todos os aplicativos sob o namespace "maria" juntos para que eles tenham as mesmas políticas de snapshot e backup, você gerenciaria o namespace e ignoraria os aplicativos no namespace.

8. Para ver a lista de aplicativos gerenciados, selecione **gerenciados** como o filtro de exibição.

> 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.

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

Resultado

Os aplicativos que você escolheu gerenciar agora estão disponíveis na guia **gerenciado**. Quaisquer aplicativos ignorados serão movidos para a guia **ignorado**. Idealmente, a guia descoberta mostrará zero aplicativos, de modo que, à medida que novos aplicativos são instalados, eles são mais fáceis de encontrar e gerenciar.

Gerenciar aplicativos por etiqueta do Kubernetes

O Astra Control inclui uma ação no topo da página Apps chamada **Definir aplicativo personalizado**. Você pode usar essa ação para gerenciar aplicativos identificados com um rótulo Kubernetes. "Saiba mais sobre como definir aplicativos personalizados pelo rótulo do Kubernetes".

Passos

1. Na barra de navegação à esquerda, selecione **aplicações**.
2. Selecione **Definir**.
3. Na caixa de diálogo **Definir aplicativo personalizado**, forneça as informações necessárias para gerenciar o aplicativo:
   a. **Novo aplicativo**: Insira o nome de exibição do aplicativo.

b. **Cluster**: Selecione o cluster onde o aplicativo reside.

c. * Namespace:* Selecione o namespace para o aplicativo.

d. **Label:** Digite um rótulo ou selecione um rótulo dos recursos abaixo.

e. **Recursos selecionados**: Visualize e gerencie os recursos do Kubernetes selecionados que você gostaria de proteger (pods, segredos, volumes persistentes e muito mais).

- Exiba os rótulos disponíveis expandindo um recurso e selecionando o número de rótulos.
- Selecione uma das etiquetas.

  Depois de escolher um rótulo, ele será exibido no campo **Label**. O Astra Control também atualiza a seção **recursos não selecionados** para mostrar os recursos que não correspondem ao rótulo selecionado.

f. **Recursos não selecionados**: Verifique os recursos do aplicativo que você não deseja proteger.

4. Selecione **Definir aplicação personalizada**.

Resultado

O Astra Control permite o gerenciamento da aplicação. Agora você pode encontrá-lo na guia **gerenciado**.

Ignore as aplicações

Se um aplicativo foi descoberto, ele aparece na lista descoberta. Nesse caso, você pode limpar a lista descoberta para que novos aplicativos recém-instalados sejam mais fáceis de encontrar. Ou, você pode ter aplicativos que você está gerenciando e, mais tarde, decidir que não deseja mais gerenciá-los. Se você não quiser gerenciar esses aplicativos, você pode indicar que eles devem ser ignorados.

Além disso, você pode querer gerenciar aplicativos em um namespace juntos (gerenciado por namespace). Você pode ignorar aplicativos que deseja excluir do namespace.

Passos

1. Na barra de navegação à esquerda, selecione **aplicações**.
2. Selecione **descoberto** como filtro.
3. Selecione a aplicação.
4. No menu Opções na coluna **ações**, selecione **Ignorar**.
5. Para ignorar, selecione **Unignore**.

Desgerenciar aplicativos

Quando você não quiser mais fazer backup, snapshot ou clonar um aplicativo, pode parar de gerenciá-lo.

Se você desgerenciar um aplicativo, todos os backups ou snapshots criados anteriormente serão perdidos.

Passos

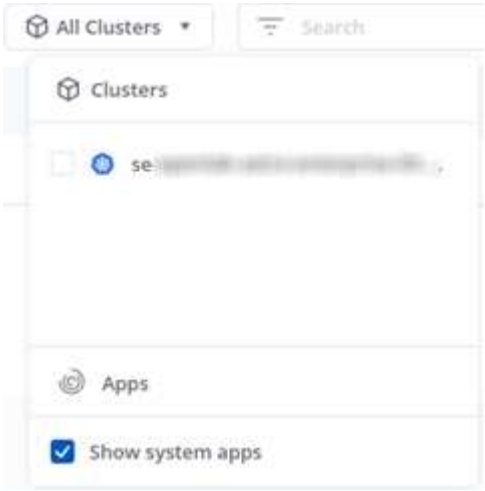
1. Na barra de navegação à esquerda, selecione **aplicações**.
2. Selecione **Managed** como filtro.
3. Selecione a aplicação.
4. No menu Opções na coluna **ações**, selecione **Desgerenciar**.

5. Reveja as informações.
6. Digite "Unmanage" (Desgerenciar) para confirmar.
7. Selecione **Sim, Desgerenciar aplicativo**.

E quanto aos aplicativos do sistema?

O Astra Control também descobre as aplicações de sistema executadas em um cluster Kubernetes. Não mostramos esses aplicativos de sistema por padrão, porque é raro que você precise fazer backup deles.

Você pode exibir aplicativos do sistema na página aplicativos selecionando a caixa de seleção **Mostrar aplicativos do sistema** sob o filtro clusters na barra de ferramentas.



O Astra Control em si não é um aplicativo padrão; é um "aplicativo do sistema". Você não deve tentar gerenciar o Astra Control por si só. O próprio Astra Control não é mostrado por padrão para gerenciamento.

Encontre mais informações

- "Use a API Astra Control"

Defina um exemplo de aplicativo personalizado

A criação de um aplicativo personalizado permite agrupar elementos do cluster do Kubernetes em um único aplicativo. Essa coleção de recursos do Kubernetes é baseada em um namespace e um rótulo.

Uma aplicação personalizada oferece controle mais granular sobre o que incluir em uma operação do Astra Control, incluindo:

- Clone
- Snapshot
- Backup
- Política de proteção

Na maioria dos casos, você deseja usar os recursos do Astra Control em todo o aplicativo. No entanto, você também pode criar um aplicativo personalizado para usar esses recursos pelos rótulos atribuídos a objetos

Kubernetes em um namespace.

> Aplicativos personalizados podem ser criados somente dentro de um namespace especificado em um único cluster. O Astra Control não dá suporte à capacidade de uma aplicação personalizada abranger vários namespaces ou clusters.

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".

> A sobreposição de políticas para o mesmo recurso sob nomes diferentes pode causar conflitos de dados. Se você criar um aplicativo personalizado para um recurso, certifique-se de que ele não está sendo clonado ou feito backup em nenhuma outra política.

O que você vai precisar

- Um cluster adicionado ao Astra Control

Passos

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

   A janela Custom App (aplicação personalizada) mostra quais recursos serão incluídos ou excluídos do seu aplicativo personalizado. Isso ajuda você a ter certeza de que está escolhendo os critérios corretos para definir seu aplicativo personalizado.

2. Na janela pop-up, insira o nome do aplicativo, escolha o cluster no menu suspenso **Cluster** e escolha o namespace do aplicativo no menu suspenso **namespace**.
3. Na lista suspensa **Label**, selecione um rótulo para os aplicativos e namespace.
4. Depois de definir o aplicativo personalizado para uma implantação, repita o processo para outras implantações, conforme necessário.

Quando você terminar de criar os dois aplicativos personalizados, você pode tratar esses recursos como qualquer outra aplicação Astra Control. Eles podem cloná-los, criar backups e snapshots e criar uma política de proteção personalizada para cada grupo de recursos com base nos rótulos do Kubernetes.

Exemplo: Política de proteção separada para versões diferentes

Neste exemplo, a equipe de devops está gerenciando uma implantação de lançamento do canary. Seu cluster 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 personalizados: 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.

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".

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] Faça backup de todos os aplicativos

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] Opcional: Ajuste 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] Em caso de desastre, restaure seus aplicativos

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).

Proteja aplicativos com snapshots e backups

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

> 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.

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
```

Configurar uma política de proteção

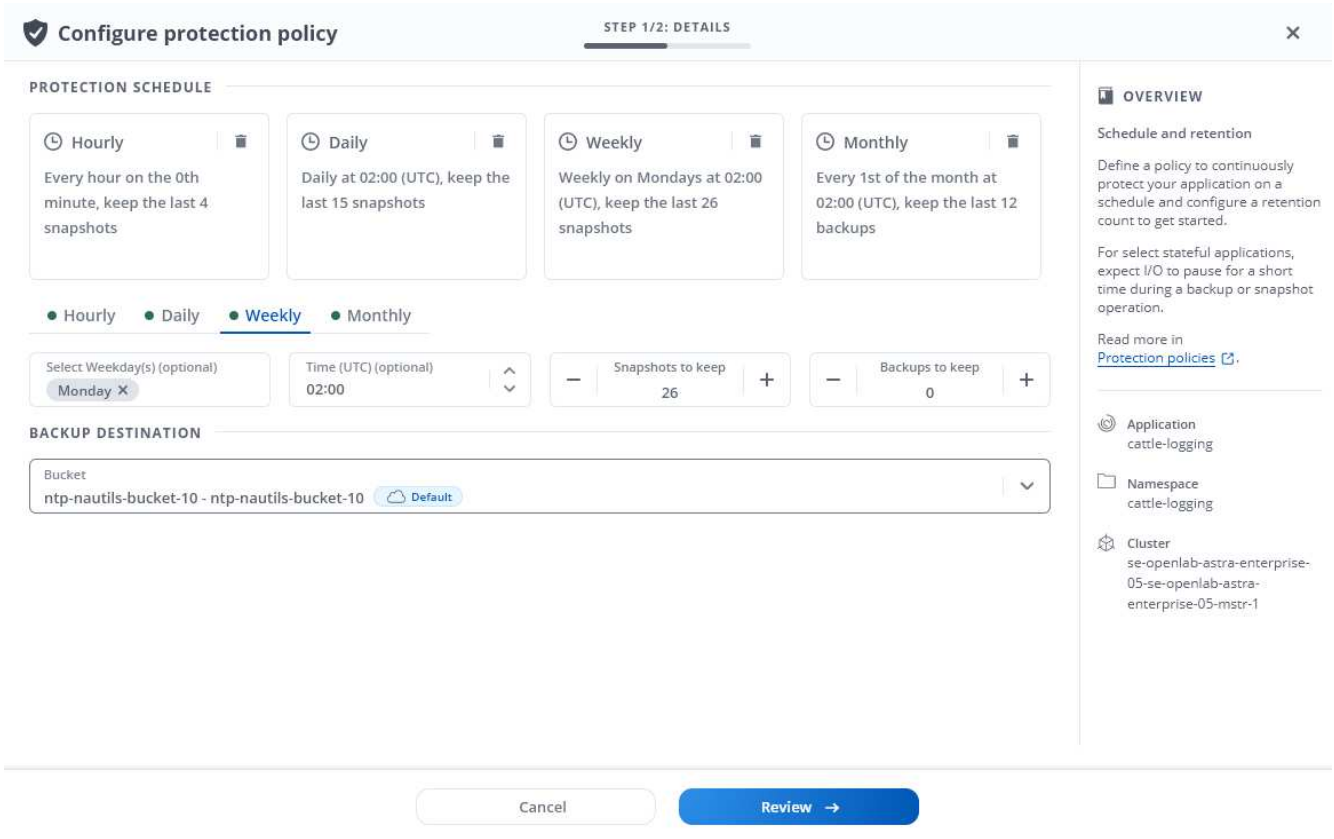
Uma política de proteção protege um aplicativo criando snapshots, backups ou ambos em um cronograma definido. Você pode optar por criar snapshots e backups por hora, diariamente, semanalmente e mensalmente, e especificar o número de cópias a reter. Por exemplo, uma política de proteção pode criar backups semanais e snapshots diários e reter os backups e snapshots por um mês. A frequência com que você cria snapshots e backups e quanto tempo você os retém depende das necessidades de sua organização.

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.

   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 Center implementa a política de proteção de dados criando e retendo snapshots e backups usando a programação e a política de retenção que você definiu.

Criar um instantâneo

Você pode criar um snapshot sob demanda a qualquer momento.

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 **Review**.
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 **disponível** na coluna **ações** na página **proteção de dados** > **instantâneos**.

Crie uma cópia de segurança

Você também pode fazer backup de um aplicativo a qualquer momento.

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.

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 destino para o backup selecionando na lista de buckets de armazenamento.
6. Selecione **Revisão**.
7. Reveja o resumo da cópia de segurança e selecione **Backup**.

Resultado

O Astra Control Center 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.

Não há como parar um backup em execução. Se precisar excluir o backup, aguarde até que ele esteja concluído e use as instruções em Eliminar cópias de segurança. Para eliminar uma cópia de segurança com falha, "Use a API Astra Control".

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.

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.

Passos

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

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 Center exclui o snapshot.

Eliminar cópias de segurança

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

> Não há como parar um backup em execução. Se você precisar excluir o backup, aguarde até que ele esteja concluído e, em seguida, use estas instruções. Para eliminar uma cópia de segurança com falha, "Use a API Astra Control".

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 Center 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.

Sobre esta tarefa

- É altamente recomendável tirar um instantâneo ou fazer backup do aplicativo antes de restaurá-lo. Isso permitirá clonar a partir do instantâneo ou backup, caso a restauração não seja bem-sucedida.
- 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.
- Se você restaurar para um cluster diferente, verifique se o cluster está usando 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.
- 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. Depois que um novo namespace é criado por uma operação de clone ou restauração, 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.
- 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 **aplicativos** e, em seguida, selecione o nome de um aplicativo.
2. Selecione **proteção de dados**.
3. Se você quiser restaurar a partir de um instantâneo, mantenha o ícone **Snapshots** selecionado. Caso contrário, selecione o ícone **backups** para restaurar a partir de um backup.
4. No menu Opções na coluna **ações** para o instantâneo ou backup a partir do qual você deseja restaurar, selecione **Restaurar aplicativo**.
5. **Restaurar detalhes**: Especifique detalhes para o aplicativo restaurado. Por padrão, o cluster e o namespace atuais são exibidos. Deixe esses valores intactos para restaurar um aplicativo no local, o que reverte o aplicativo para uma versão anterior de si mesmo. Altere esses valores se quiser restaurar para um cluster ou namespace diferente.
   - Introduza um nome e um namespace para a aplicação.
   - Escolha o cluster de destino para a aplicação.
   - Selecione **Revisão**.

   > 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.

6. **Restore Summary**: Revise os detalhes sobre a ação de restauração, digite "Restore" e selecione **Restore**.

Resultado

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

> Após uma operação de proteção de dados (clone, backup, 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.

Clonar e migrar aplicações

Clone um aplicativo existente para criar um aplicativo duplicado no mesmo cluster do Kubernetes ou em outro cluster. Quando o Astra Control Center clones 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 ou "API Astra Control" clonar e migrar aplicações.

O que você vai precisar

Para clonar aplicativos para um cluster diferente, você precisa de um bucket padrão. Quando você adiciona seu primeiro bucket, ele se torna o bucket padrão.

Sobre esta tarefa

- Se você implantar um aplicativo com um StorageClass explicitamente definido e precisar clonar o aplicativo, o cluster de destino precisará ter o StorageClass originalmente especificado. Clonar um aplicativo com um StorageClass explicitamente definido para um cluster que não tenha o mesmo StorageClass falhará.
- Se você clonar uma instância implantada por operador do Jenkins CI, precisará restaurar manualmente os dados persistentes. Esta é uma limitação do modelo de implantação do aplicativo.
- 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.
- Durante um backup de aplicativo ou restauração de 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.
- 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. Depois que um novo namespace é criado por uma operação de clone ou restauração, 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.

Considerações sobre 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.
- 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. **Detalhes do clone**: Especifique detalhes para o clone:
   ◦ Introduza um nome.
   ◦ Insira um namespace para o clone.
   ◦ Escolha um cluster de destino para o clone.
   ◦ Escolha se deseja criar o clone a partir de um instantâneo ou backup existente. Se você não selecionar essa opção, o Astra Control Center criará o clone a partir do estado atual do aplicativo.
5. **Fonte**: Se você optar por clonar de um instantâneo ou backup existente, escolha o instantâneo ou o backup que deseja usar.
6. Selecione **Revisão**.
7. **Clone Summary**: Revise os detalhes sobre o clone e selecione **Clone**.

Resultado

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

> 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.

Gerenciar ganchos de execução de aplicativos

Um gancho de execução é um script personalizado que você pode executar antes ou depois de um instantâneo de um aplicativo gerenciado. Por exemplo, se você tiver um aplicativo de banco de dados, poderá usar ganchos 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.

Ganchos de execução padrão e expressões regulares

Para alguns aplicativos, o Astra Control vem com ganchos de execução padrão, fornecidos pelo NetApp, que lidam com operações de congelamento e descongelamento antes e depois dos snapshots. O Astra Control usa expressões regulares para corresponder a imagem de contêiner de um aplicativo a essas aplicações:

- MariaDB
  ◦ Expressão regular correspondente
- MySQL
  ◦ Expressão regular correspondente: Mysql
- PostgreSQL
  ◦ Expressão regular correspondente

Se houver uma correspondência, os ganchos de execução padrão fornecidos pelo NetApp para esse

aplicativo aparecerão na lista de ganchos de execução ativos do aplicativo e esses ganchos serão executados automaticamente quando os snapshots desse aplicativo forem obtidos. Se um dos seus aplicativos personalizados tiver um nome de imagem semelhante que corresponda a uma das expressões regulares (e você não quiser usar os ganchos de execução padrão), você pode alterar o nome da imagem ou desativar o gancho de execução padrão para esse aplicativo e usar um gancho personalizado.

Não é possível excluir ou modificar os ganchos de execução padrão.

Notas importantes sobre ganchos de execução personalizados

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

- O Astra Control requer que ganchos de execução sejam escritos no formato de scripts shell executáveis.
- O tamanho do script está limitado a 128KBMB.
- O Astra Control usa configurações de gancho de execução e quaisquer critérios de correspondência para determinar quais ganchos são aplicáveis a um instantâneo.
- Todas as falhas no gancho de execução são falhas suaves; outros ganchos e o instantâneo 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.

> 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 levam para serem executados.

Quando um instantâneo é executado, os eventos de gancho de execução ocorrem na seguinte ordem:

1. Todos os ganchos de execução pré-snapshot padrão fornecidos pelo NetApp são executados nos contentores apropriados.
2. Todos os ganchos de execução pré-snapshot personalizados aplicáveis são executados nos contentores apropriados. Você pode criar e executar quantos ganchos pré-snapshot personalizados forem necessários, mas a ordem de execução desses ganchos antes do snapshot não é garantida nem configurável.
3. O instantâneo é executado.
4. Todos os ganchos de execução pós-snapshot personalizados aplicáveis são executados nos contentores apropriados. Você pode criar e executar quantos ganchos pós-snapshot personalizados forem necessários, mas a ordem de execução desses ganchos após o snapshot não é garantida nem configurável.
5. Todos os ganchos de execução pós-snapshot padrão fornecidos pelo NetApp são executados nos contentores apropriados.

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 resultantes para garantir que eles sejam consistentes. Você pode fazer isso clonando o aplicativo para um namespace temporário, restaurando o snapshot e testando o aplicativo.

Ver ganchos de execução existentes

Você pode exibir ganchos de execução padrão personalizados ou fornecidos pelo NetApp 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, a origem e quando um gancho é executado (pré ou pós-snapshot). Para ver os registos de eventos em torno dos ganchos de execução, aceda à página **Activity** na área de navegação do lado esquerdo.

Crie um gancho de execução personalizado

Você pode criar um gancho de execução personalizado para um aplicativo. "Exemplos de gancho de execução"Consulte 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 linux ou fornecendo o caminho completo para um executável.

Passos

1. Selecione **aplicativos** e, em seguida, selecione o nome de um aplicativo gerenciado.
2. Selecione a guia **ganchos de execução**.
3. Selecione **Adicionar um novo gancho**.
4. Na área **Detalhes do gancho**, dependendo de quando o gancho deve ser executado, escolha **Pré-instantâneo** ou **Pós-instantâneo**.
5. Introduza um nome exclusivo para o gancho.
6. (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.
7. Na área **Container Images**, se o gancho for executado contra todas as imagens de contentor contidas no aplicativo, ative a caixa de seleção **Apply to all container images** (aplicar a todas as imagens de contentor). Se, em vez disso, o gancho deve agir apenas em uma ou mais imagens de contentor especificadas, insira os nomes de imagem de contentor no campo **nomes de imagem de contentor a corresponder**.
8. Na área **Script**, 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.

- Cole em um script personalizado da área de transferência.
  i. Selecione a opção **Colar da área de transferência**.
  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.

9. Selecione **Adicionar gancho**.

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**.

Exemplos de gancho de execução

Use os exemplos a seguir para ter uma ideia de como estruturar seus ganchos de execução. Você pode usar esses ganchos como modelos ou como scripts de teste.

Exemplo simples de sucesso

Este é um exemplo de um gancho simples que é bem-sucedido e grava uma mensagem na saída padrão e erro padrão.

```
#!/bin/sh
```

```
# success_sample.sh
#
# A simple noop success hook script for testing purposes.
#
# args: None
#


#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# main
#

# log something to stdout
info "running success_sample.sh"

# exit with 0 to indicate success
info "exit 0"
```

```
exit 0
```

Exemplo de sucesso simples (versão bash)

Este é um exemplo de um gancho simples que é bem-sucedido e escreve uma mensagem para saída padrão e erro padrão, escrito para bash.

```
#!/bin/bash

# success_sample.bash
#
# A simple noop success hook script for testing purposes.
#
# args: None


#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
```

```
# main
#

# log something to stdout
info "running success_sample.bash"

# exit with 0 to indicate success
info "exit 0"
exit 0
```

Exemplo de sucesso simples (versão zsh)

Este é um exemplo de um gancho simples que é bem-sucedido e escreve uma mensagem para saída padrão e erro padrão, escrito para shell Z.

```
#!/bin/zsh

# success_sample.zsh
#
# A simple noop success hook script for testing purposes.
#
# args: None
#


#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
```

```
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}

#
# main
#

# log something to stdout
info "running success_sample.zsh"

# exit with 0 to indicate success
info "exit 0"
exit 0
```

Sucesso com argumentos exemplo

O exemplo a seguir demonstra como você pode usar args em um gancho.

```
#!/bin/sh

# success_sample_args.sh
#
# A simple success hook script with args for testing purposes.
#
# args: Up to two optional args that are echoed to stdout

#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
```

```
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# main
#

# log something to stdout
info "running success_sample_args.sh"


# collect args
arg1=$1
arg2=$2

# output args and arg count to stdout
info "number of args: $#"
info "arg1 ${arg1}"
info "arg2 ${arg2}"

# exit with 0 to indicate success
info "exit 0"
exit 0
```

Exemplo de gancho pré-instantâneo/pós-instantâneo

O exemplo a seguir demonstra como o mesmo script pode ser usado tanto para um gancho pré-snapshot quanto para um gancho pós-snapshot.

```
#!/bin/sh

# success_sample_pre_post.sh
#
# A simple success hook script example with an arg for testing purposes
# to demonstrate how the same script can be used for both a prehook and
posthook
```

```
#
# args: [pre|post]

# unique error codes for every error case
ebase=100
eusage=$((ebase+1))
ebadstage=$((ebase+2))
epre=$((ebase+3))
epost=$((ebase+4))


#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# Would run prehook steps here
#
prehook() {
    info "Running noop prehook"
    return 0
```

```
}

#
# Would run posthook steps here
#
posthook() {
    info "Running noop posthook"
    return 0
}


#
# main
#

# check arg
stage=$1
if [ -z "${stage}" ]; then
    echo "Usage: $0 <pre|post>"
    exit ${eusage}
fi

if [ "${stage}" != "pre" ] && [ "${stage}" != "post" ]; then
    echo "Invalid arg: ${stage}"
    exit ${ebadstage}
fi

# log something to stdout
info "running success_sample_pre_post.sh"

if [ "${stage}" = "pre" ]; then
    prehook
    rc=$?
    if [ ${rc} -ne 0 ]; then
        error "Error during prehook"
    fi
fi

if [ "${stage}" = "post" ]; then
    posthook
    rc=$?
    if [ ${rc} -ne 0 ]; then
        error "Error during posthook"
    fi
fi
```

```
exit ${rc}
```

Exemplo de falha

O exemplo a seguir demonstra como você pode lidar com falhas em um gancho.

```
#!/bin/sh

# failure_sample_arg_exit_code.sh
#
# A simple failure hook script for testing purposes.
#
# args: [the exit code to return]
#


#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
```

```
# main
#

# log something to stdout
info "running failure_sample_arg_exit_code.sh"

argexitcode=$1

# log to stderr
error "script failed, returning exit code ${argexitcode}"

# exit with specified exit code
exit ${argexitcode}
```

Exemplo de falha verbosa

O exemplo a seguir demonstra como você pode lidar com falhas em um gancho, com Registro mais detalhado.

```
#!/bin/sh

# failure_sample_verbose.sh
#
# A simple failure hook script with args for testing purposes.
#
# args: [The number of lines to output to stdout]


#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}
```

```
#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# main
#

# log something to stdout
info "running failure_sample_verbose.sh"


# output arg value to stdout
linecount=$1
info "line count ${linecount}"

# write out a line to stdout based on line count arg
i=1
while [ "$i" -le ${linecount} ]; do
    info "This is line ${i} from failure_sample_verbose.sh"
    i=$(( i + 1 ))
done

error "exiting with error code 8"
exit 8
```

Falha com um exemplo de código de saída

O exemplo a seguir demonstra uma falha de gancho com um código de saída.

```
#!/bin/sh

# failure_sample_arg_exit_code.sh
#
# A simple failure hook script for testing purposes.
#
# args: [the exit code to return]
#
```

```
#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# main
#

# log something to stdout
info "running failure_sample_arg_exit_code.sh"

argexitcode=$1

# log to stderr
error "script failed, returning exit code ${argexitcode}"

# exit with specified exit code
exit ${argexitcode}
```

Exemplo de sucesso após falha

O exemplo a seguir demonstra um gancho falhando na primeira vez que é executado, mas sucedendo após a segunda corrida.

```
#!/bin/sh

# failure_then_success_sample.sh
#
# A hook script that fails on initial run but succeeds on second run for
testing purposes.
#
# Helpful for testing retry logic for post hooks.
#
# args: None
#

#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
```

```
# main
#

# log something to stdout
info "running failure_success sample.sh"


if [ -e /tmp/hook-test.junk ] ; then
    info "File does exist.  Removing /tmp/hook-test.junk"
    rm /tmp/hook-test.junk
    info "Second run so returning exit code 0"
    exit 0
else
    info "File does not exist.  Creating /tmp/hook-test.junk"
    echo "test" > /tmp/hook-test.junk
    error "Failed first run, returning exit code 5"
    exit 5
fi
```

Ver a integridade da aplicação 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.

Ver a integridade e os detalhes dos clusters

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.

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.

Veja a saúde e os detalhes de um aplicativo

Depois de começar a gerenciar uma aplicação, o Astra fornece detalhes sobre a aplicação que permite identificar seu status (integridade), seu status de proteção (totalmente protegido em caso de falha), os pods, o 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. Encontre as informações que você está procurando:

Estado da aplicação
Fornece um status que reflete o estado do aplicativo no Kubernetes. Por exemplo, os pods e os volumes persistentes estão online? Se um aplicativo não estiver saudável, você precisará solucionar o problema no cluster observando os logs do Kubernetes. O Astra não fornece informações para ajudá-lo a corrigir um aplicativo quebrado.

Estado de proteção da aplicação
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 exibir os snapshots e backups existentes.

Armazenamento
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 armazenados em backup e gerenciados.

Atividade
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

Gerenciar usuários

Você pode convidar, 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.

Convide usuários

Proprietários e administradores de contas podem convidar novos usuários para o Astra Control Center.

Passos

1. Na área de navegação **Gerenciar sua conta**, selecione **conta**.
2. Selecione a guia **usuários**.
3. Selecione **convidar usuário**.
4. Introduza o nome e o endereço de correio eletrónico do utilizador.
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, "Gerenciar funções"consulte .
7. Selecione **convidar utilizadores**.

   O usuário recebe um e-mail informando que foi convidado para o Astra Control Center. O e-mail inclui senha temporária, que eles precisarão alterar no primeiro login.

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, "Gerenciar funções"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**.

Altere a função de um usuário

Os usuários com a função proprietário podem alterar a função de todos os usuários, enquanto os usuários

com a função Admin podem alterar a função de usuários que têm a função Admin, Member ou Viewer.

Passos

1. Na área de navegação **Gerenciar sua conta**, selecione **conta**.
2. Selecione a lista suspensa **ações**.
3. Selecione **Editar função**.
4. Selecione uma nova função.
5. Para aplicar restrições à função, ative a caixa de verificação **restringir função a restrições** e selecione uma restrição na lista.

   Se não houver restrições, você pode adicionar uma restrição. Para obter mais informações, "Gerenciar funções"consulte .

6. Selecione **Confirm**.

Resultado

O Astra Control Center atualiza as permissões do usuário com base na nova função selecionada.

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.

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"

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 `kubeconfig` arquivo, você deve definir apenas **um** elemento de contexto nele. Consulte "Documentação do Kubernetes" para obter informações sobre como criar `kubeconfig` arquivos.

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.

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 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 conexões de repositório

Você pode conetar repositórios ao Astra Control para usar como referência para imagens e artefatos de instalação de pacotes de software. Quando você importa pacotes de software, o Astra Control faz referência a imagens de instalação no repositório de imagens e binários e outros artefatos no repositório de artefatos.

O que você vai precisar

- Cluster do Kubernetes com Astra Control Center instalado
- Um repositório Docker em execução que você pode acessar
- Um repositório de artefatos em execução (como Artifactory) que você pode acessar

Conete um repositório de imagens do Docker

Você pode conetar um repositório de imagens do Docker para armazenar imagens de instalação de pacotes, como as do Astra Data Store. Quando você instala pacotes, o Astra Control importa os arquivos de imagem do pacote do repositório de imagens.

Passos

1. Na área de navegação **Gerenciar sua conta**, selecione **conta**.
2. Selecione a guia **conexões**.
3. Na seção **Docker Image Repository**, selecione o menu no canto superior direito.
4. Selecione **Connect**.
5. Adicione a URL e a porta para o repositório.
6. Insira as credenciais do repositório.
7. Selecione **Connect**.

Resultado

O repositório está conetado. Na seção **Docker Image Repository**, o repositório deve mostrar um status conetado.

Desconete um repositório de imagens do Docker

Você pode remover a conexão a um repositório de imagens do Docker se ele não for mais necessário.

Passos

1. Na área de navegação **Gerenciar sua conta**, selecione **conta**.
2. Selecione a guia **conexões**.
3. Na seção **Docker Image Repository**, selecione o menu no canto superior direito.

4. Selecione **Disconnect**.
5. Selecione **Sim, desconete o repositório de imagens do Docker**.

Resultado

O repositório está desconetado. Na seção **Docker Image Repository**, o repositório deve mostrar um status desconetado.

Conete um repositório de artefatos

Você pode conetar um repositório de artefatos a artefatos de host, como binários de pacotes de software. Quando você instala pacotes, o Astra Control importa os artefatos dos pacotes de software do repositório de imagens.

Passos

1. Na área de navegação **Gerenciar sua conta**, selecione **conta**.
2. Selecione a guia **conexões**.
3. Na seção **Artifact Repository**, selecione o menu no canto superior direito.
4. Selecione **Connect**.
5. Adicione a URL e a porta para o repositório.
6. Se a autenticação for necessária, ative a caixa de verificação **Use Authentication** e introduza as credenciais para o repositório.
7. Selecione **Connect**.

Resultado

O repositório está conetado. Na seção **Artifact Repository**, o repositório deve mostrar um status conetado.

Desconete um repositório de artefatos

Você pode remover a conexão a um repositório de artefatos se ele não for mais necessário.

Passos

1. Na área de navegação **Gerenciar sua conta**, selecione **conta**.
2. Selecione a guia **conexões**.
3. Na seção **Artifact Repository**, selecione o menu no canto superior direito.
4. Selecione **Disconnect**.
5. Selecione **Sim, desconete o repositório de artefatos**.

Resultado

O repositório está desconetado. Na seção **Artifact Repository**, o repositório deve mostrar um status conetado.

Encontre mais informações

- "Gerenciar pacotes de software"

Gerenciar pacotes de software

O NetApp oferece recursos adicionais para o Centro de Controle Astra com pacotes de software que podem

ser baixados no site de suporte da NetApp. Depois de conetar repositórios Docker e artefato, você pode carregar e importar pacotes para adicionar essa funcionalidade ao Astra Control Center. Você pode usar a interface da Web CLI ou a interface da Web do Astra Control Center para gerenciar pacotes de software.

O que você vai precisar

- Cluster do Kubernetes com Astra Control Center instalado
- Um repositório de imagem Docker conetado para armazenar imagens de pacotes de software. Para obter mais informações, "Gerenciar conexões de repositório"consulte .
- Um repositório de artefatos conetado para armazenar binários e artefatos de pacotes de software. Para obter mais informações, "Gerenciar conexões de repositório"consulte .
- Um pacote de software do site de suporte da NetApp

Carregue imagens de pacotes de software para os repositórios

O Astra Control Center faz referência a imagens de pacotes e artefatos em repositórios conetados. Você pode fazer upload de imagens e artefatos para os repositórios usando a CLI.

Passos

1. Baixe o pacote de software do site de suporte da NetApp e salve-o em uma máquina que tenha o `kubectl` utilitário instalado.
2. Extraia o arquivo de pacote compactado e altere o diretório para o local do arquivo de pacote Astra Control (por exemplo, `acc.manifest.bundle.yaml`).
3. Envie as imagens do pacote para o repositório Docker. Faça as seguintes substituições:
   - Substitua BUNDLE_FILE pelo nome do arquivo de pacote Astra Control.
   - Substitua my_REGISTRY pela URL do repositório Docker.
   - Substitua my_REGISTRY_user e my_REGISTRY_PASSWORD pelas credenciais do repositório.

   ```
   kubectl astra packages push-images -m BUNDLE_FILE -r MY_REGISTRY -u
   MY_REGISTRY_USER -p MY_REGISTRY_PASSWORD
   ```

4. Se o pacote tiver artefatos, copie os artefatos para o repositório de artefatos. Substitua BUNDLE_FILE pelo nome do arquivo de pacote Astra Control e network_LOCATION pelo local de rede para copiar os arquivos de artefato para:

   ```
   kubectl astra packages copy-artifacts -m BUNDLE_FILE -n NETWORK_LOCATION
   ```

Adicione um pacote de software

Você pode importar pacotes de software usando um arquivo de pacote Astra Control Center. Isso instala o pacote e disponibiliza o software para uso do Astra Control Center.

Adicione um pacote de software usando a IU da Web Astra Control

Você pode usar a IU da Web do Astra Control Center para adicionar um pacote de software que foi carregado para os repositórios conetados.

Passos

1. Na área de navegação **Gerenciar sua conta**, selecione **conta**.
2. Selecione a guia **Pacotes**.
3. Selecione o botão **Add**.
4. Na caixa de diálogo de seleção de ficheiros, selecione o ícone de carregamento.
5. Escolha um arquivo de pacote Astra Control, em `.yaml` formato, para upload.
6. Selecione **Adicionar**.

Resultado

Se o arquivo do pacote for válido e as imagens e artefatos do pacote estiverem localizados nos repositórios conetados, o pacote será adicionado ao Astra Control Center. Quando o status na coluna **Status** mudar para **disponível**, você pode usar o pacote. Você pode passar o Mouse sobre o status de um pacote para obter mais informações.

Se uma ou mais imagens ou artefatos de um pacote não forem encontrados no repositório, uma mensagem de erro será exibida para esse pacote.

Adicione um pacote de software usando a CLI

Você pode usar a CLI para importar um pacote de software que você carregou para os repositórios conetados. Para fazer isso, primeiro você precisa Registrar seu ID de conta do Astra Control Center e um token de API.

Passos

1. Usando um navegador da Web, faça login na IU da Web do Astra Control Center.
2. No Painel, selecione o ícone do usuário no canto superior direito.
3. Selecione **Acesso à API**.
4. Observe o ID da conta perto da parte superior da tela.
5. Selecione **Generate API token**.
6. Na caixa de diálogo resultante, selecione **Generate API token**.
7. Observe o token resultante e selecione **Fechar**. Na CLI, altere os diretórios para o local `.yaml` do arquivo de pacote no conteúdo do pacote extraído.
8. Importe o pacote usando o arquivo bundle, fazendo as seguintes substituições:
   - Substitua BUNDLE_FILE pelo nome do arquivo de pacote Astra Control.
   - Substitua O SERVIDOR pelo nome DNS da instância Astra Control.
   - Substitua account_ID e TOKEN pelo ID da conta e token da API que você gravou anteriormente.

```
kubectl astra packages import -m BUNDLE_FILE -u SERVER -a ACCOUNT_ID
-k TOKEN
```

Resultado

Se o arquivo do pacote for válido e as imagens e artefatos do pacote estiverem localizados nos repositórios conetados, o pacote será adicionado ao Astra Control Center.

Se uma ou mais imagens ou artefatos de um pacote não forem encontrados no repositório, uma mensagem de erro será exibida para esse pacote.

Remova um pacote de software

Você pode usar a IU da Web do Astra Control Center para remover um pacote de software importado anteriormente no Astra Control Center.

Passos

1. Na área de navegação **Gerenciar sua conta**, selecione **conta**.
2. Selecione a guia **Pacotes**.

   Você pode ver a lista de pacotes instalados e seus status nesta página.

3. Na coluna **ações** para o pacote, abra o menu ações.
4. Selecione **Eliminar**.

Resultado

O pacote é excluído do Astra Control Center, mas as imagens e artefatos do pacote permanecem em seus repositórios.

Encontre mais informações

- "Gerenciar conexões de repositório"

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
- Genérico S3
- Microsoft Azure

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
- 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 Opções na 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**.

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.

O que você vai precisar

- 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
- Desgerenciar um back-end de storage
- Atualizar uma licença de back-end de armazenamento
- Adicionar nós a um cluster de 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.

Na página Detalhes do back-end de storage, para o Astra Data Store, você pode ver as seguintes informações:

- Cluster Astra Data Store
  - Taxa de transferência, IOPS e latência
  - Capacidade utilizada em comparação com a capacidade total
- Para cada volume de cluster Astra Data Store
  - Capacidade utilizada em comparação com a capacidade total
  - Taxa de transferência

Veja os detalhes do back-end do storage no Dashboard

Passos

1. Na navegação à esquerda, selecione **Dashboard**.
2. Revise a seção de back-end de armazenamento 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

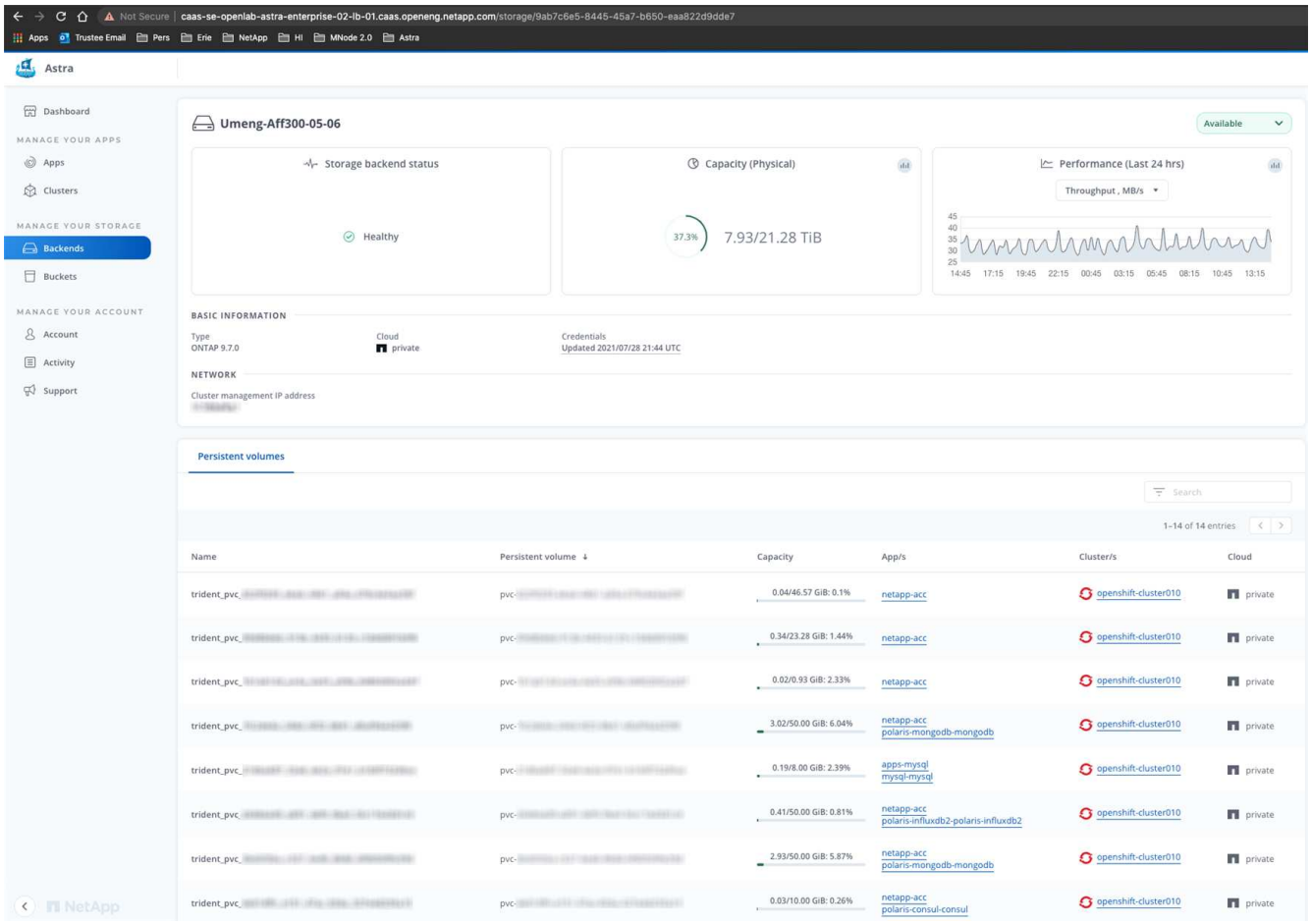
Veja informações sobre a integridade, a capacidade e a performance do back-end (taxa de transferência de IOPS e/ou latência).

Com uma conexão com o Cloud Insights, você pode ver os volumes que os aplicativos Kubernetes estão usando, que são armazenados em um back-end de storage selecionado.

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.

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.

Se você estiver removendo um back-end do Astra Data Store, ele não deverá ter sido criado pelo vCenter.

O que você vai precisar

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

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**.

Atualizar uma licença de back-end de armazenamento

Você pode atualizar a licença de um back-end de storage do Astra Data Store para dar suporte a uma implantação maior ou recursos aprimorados.

O que você vai precisar

- Um back-end de storage Astra Data Store implantado e gerenciado
- Um arquivo de licença do Astra Data Store (entre em Contato com seu representante de vendas da NetApp para adquirir uma licença do Astra Data Store)

Passos

1. Na navegação à esquerda, selecione **backends**.
2. Selecione o nome de um back-end de armazenamento.
3. Em **Informação básica**, você pode ver o tipo de licença instalada.

   Se você passar o Mouse sobre as informações da licença, um pop-up será exibido com mais informações, como informações de expiração e direito.

4. Em **Licença**, selecione o ícone de edição ao lado do nome da licença.

5. Na página **Atualizar licença**, execute um dos seguintes procedimentos:

Status da licença	Ação
Pelo menos uma licença foi adicionada ao Astra Data Store.	Selecione uma licença na lista.
Nenhuma licença foi adicionada ao Astra Data Store.	a. Selecione o botão **Add**. b. Selecione um ficheiro de licença para carregar. c. Selecione **Add** para carregar o ficheiro de licença.

6. Selecione **Atualizar**.

Adicionar nós a um cluster de back-end de storage

Você pode adicionar nós a um cluster Astra Data Store, até o número de nós suportados pelo tipo de licença instalada para Astra Data Store.

O que você vai precisar

- Um back-end de storage Astra Data Store implantado e licenciado
- Você adicionou o pacote de software Astra Data Store ao Astra Control Center
- Um ou mais nós novos a serem adicionados ao cluster

Passos

1. Na navegação à esquerda, selecione **backends**.
2. Selecione o nome de um back-end de armazenamento.
3. Em informações básicas, você pode ver o número de nós nesse cluster de back-end de storage.
4. Em **nós**, selecione o ícone de edição ao lado do número de nós.
5. Na página **Add Nodes**, insira informações sobre o novo nó ou nós:
   a. Atribua um rótulo de nó para cada nó.
   b. Execute um dos seguintes procedimentos:
      - Se quiser que o Astra Data Store utilize sempre o número máximo de nós disponível de acordo com a sua licença, ative a caixa de verificação **sempre use até o número máximo de nós permitidos**.
      - Se você não quiser que o Astra Data Store use sempre o número máximo de nós disponíveis, selecione o número desejado de nós totais a serem usados.
   c. Se você implantou o Astra Data Store com Protection Domains habilitado, atribua o novo nó ou nós aos domínios de proteção.
6. Selecione **seguinte**.
7. Insira o endereço IP e as informações de rede para cada novo nó. Insira um único endereço IP para um único nó novo ou um pool de endereços IP para vários nós novos.

   Se o Astra Data Store puder usar os endereços IP configurados durante a implantação, não será necessário inserir informações de endereço IP.

8. Selecione **seguinte**.
9. Revise a configuração do novo nó ou nós.
10. Selecione **Adicionar nós**.

Encontre mais informações

- "Use a API Astra Control"

Monitorar e proteger a infraestrutura

Você pode configurar várias configurações opcionais para aprimorar sua experiência com o Astra Control Center. 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. Para monitorar e obter insights sobre toda a sua infraestrutura, crie uma conexão com o NetApp Cloud Insights. Para coletar eventos do Kubernetes de sistemas monitorados pelo Astra Control Center, adicione uma conexão Fluentd.

Adicione um servidor proxy

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.

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

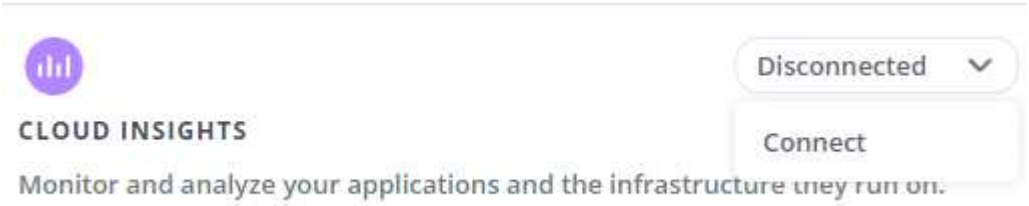
O que você vai precisar

- 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 .

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.

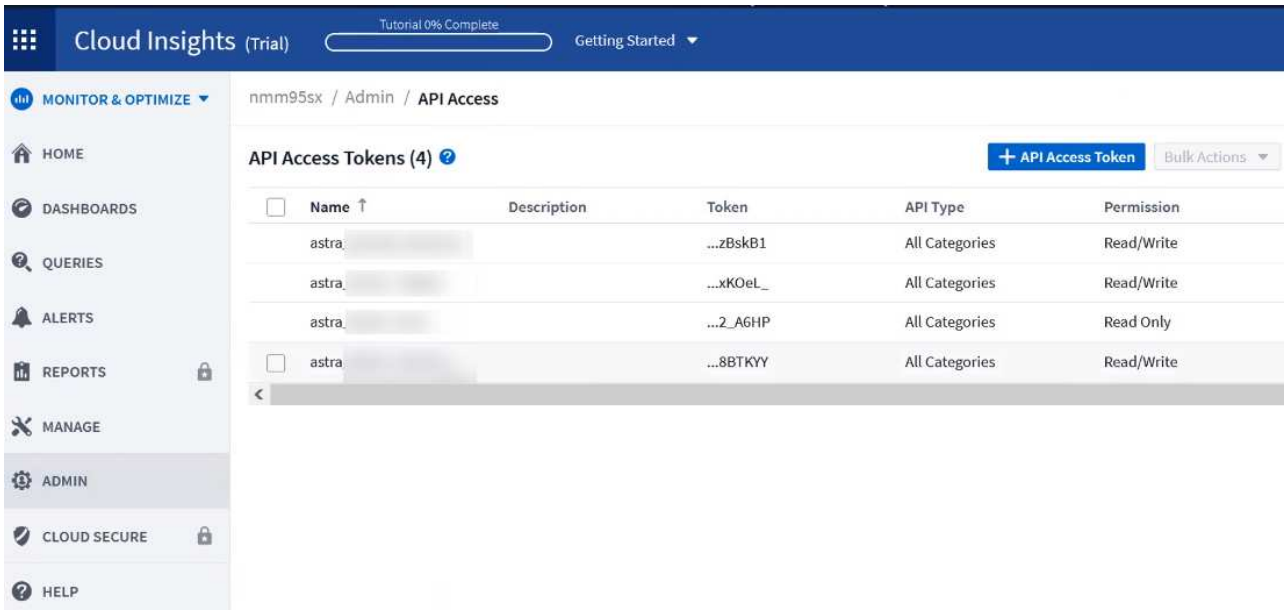


4. Insira os tokens da API do Cloud Insights e o URL do locatário. A URL do locatário tem o seguinte formato, como exemplo:

```
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: Ativos, 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.

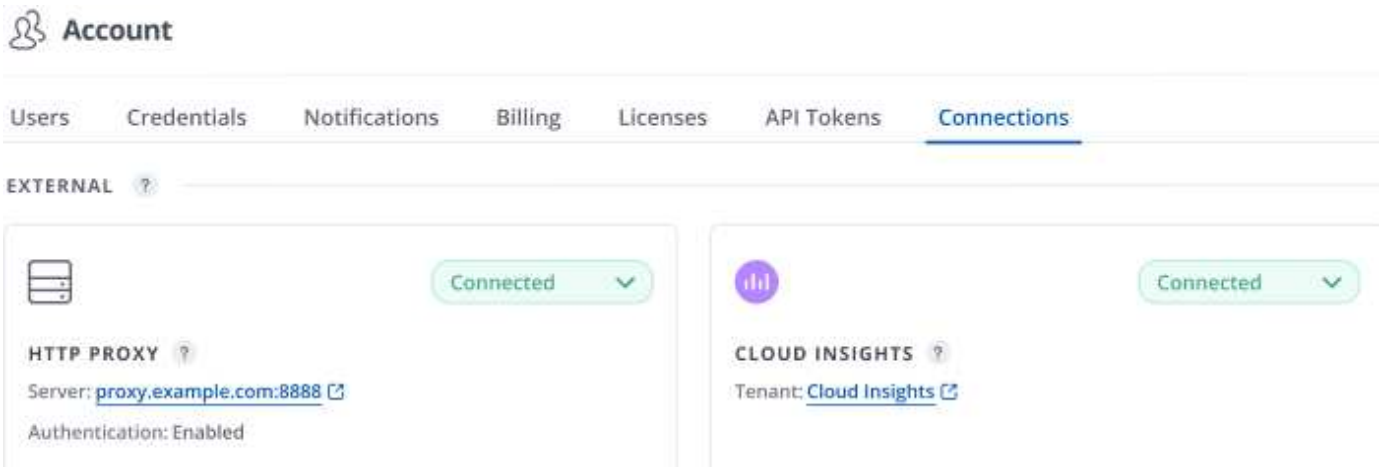
5. Selecione **Connect**.

> 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**.

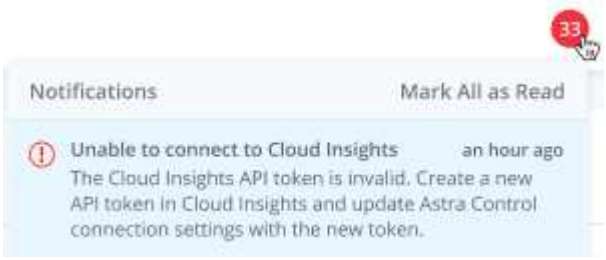
> Para ir e voltar facilmente entre o Centro de Controle Astra e as UIs do Cloud Insights, certifique-se de que você esteja conetado a ambos.

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.

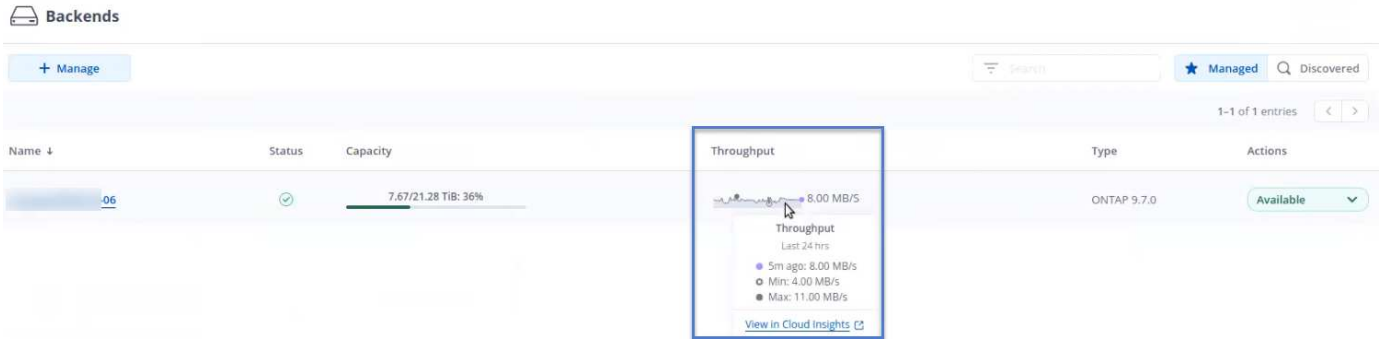


Se a conexão falhou por algum motivo, o status mostra **Failed**. Você pode encontrar o motivo da falha em **notificações** no lado superior direito da interface do usuário.



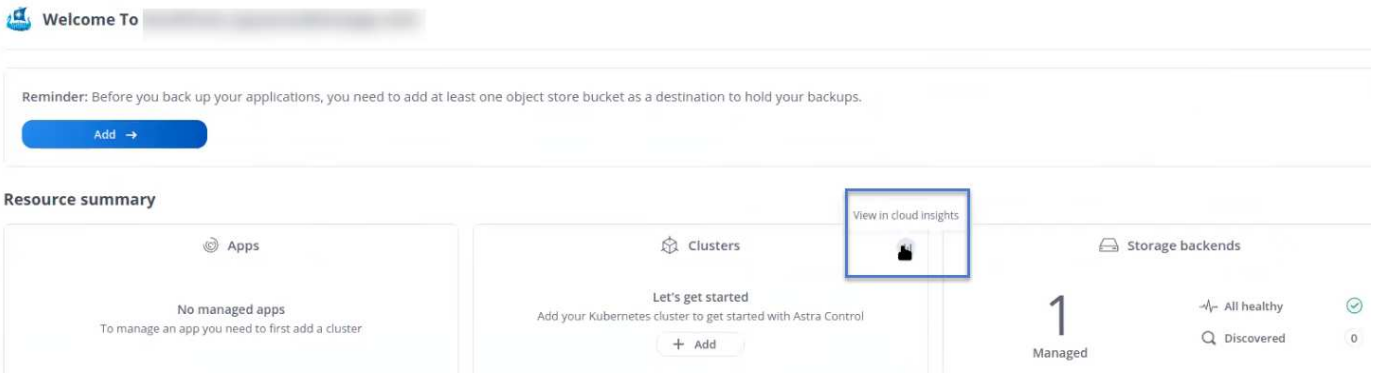
Você também pode encontrar as mesmas informações em **conta** > **notificações**.

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

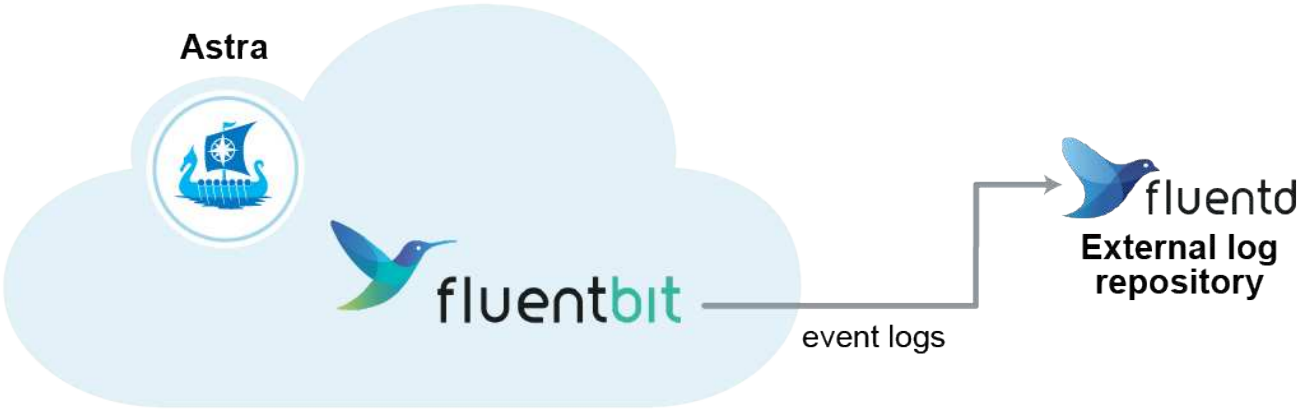
Você pode desativar a conexão Cloud Insights para um cluster Kubernetes gerenciado pelo Astra Control Center. A desativação da conexão Cloud Insights não exclui os dados de telemetria já carregados no Cloud Insights.

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**.

Ligar ao Fluentd

Você pode enviar logs (eventos Kubernetes) do 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.

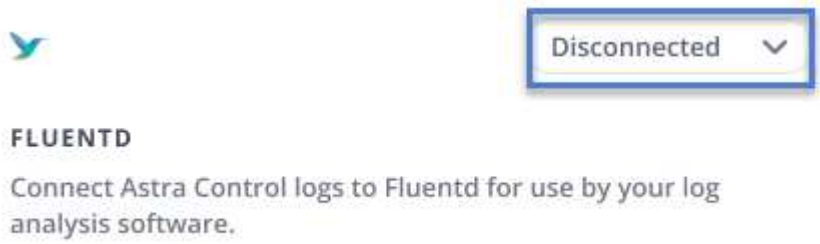
O que você vai precisar

- 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.

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

Passos

1. Na barra de navegação à esquerda, selecione **aplicações**.
2. Marque a caixa de seleção dos aplicativos que você não deseja mais gerenciar.
3. No menu **Action**, selecione **Unmanage**.
4. Digite "Unmanage" (Desgerenciar) para confirmar.
5. Confirme se deseja desgerenciar os aplicativos e selecione **Sim, desgerenciar o aplicativo**.

Resultado

O Astra Control Center deixa de gerenciar a aplicação.

Desgerenciar um cluster

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

- 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 Trident não será desinstalado do cluster. "Saiba como desinstalar o Trident".

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

Passos

1. Na barra de navegação à esquerda, selecione **clusters**.
2. Marque a caixa de seleção do cluster que não deseja mais gerenciar no Astra Control Center.
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** e, depois disso, o cluster será removido da página **clusters**, e ele 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 para atualizar os componentes do Astra Control Center em seu ambiente. Você pode usar este procedimento para atualizar o Astra Control Center em ambientes conetados à Internet ou com conexão via rede.

O que você vai precisar

- "Antes de começar a atualização, verifique se seu ambiente ainda atende aos requisitos mínimos para implantação do Astra Control Center".
- Certifique-se de que todos os operadores de cluster estão em um estado saudável e disponíveis.

  Exemplo do OpenShift:

  ```
  oc get clusteroperators
  ```

- Certifique-se de que todos os serviços de API estejam em um estado saudável e disponíveis.

  Exemplo do OpenShift:

  ```
  oc get apiservices
  ```

- Saia do seu Astra Control Center.

Sobre esta tarefa

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

- Faça o download do pacote Astra Control Center
- Desembale o pacote e mude o diretório
- Adicione as imagens ao seu registo local
- Instale o operador Astra Control Center atualizado
- Atualizar o Astra Control Center
- Atualizar serviços de terceiros (opcional)
- Verifique o status do sistema
- Configure a entrada para o balanceamento de carga

Não execute o seguinte comando durante todo o processo de atualização para evitar a exclusão de todos os pods do Astra Control Center: `kubectl delete -f astra_control_center_operator_deploy.yaml`

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

Os comandos do Podman podem ser usados no lugar dos comandos do Docker se você estiver usando o Podman do Red Hat em vez do Docker Engine.

Faça o download do pacote Astra Control Center

1. Faça o download do pacote de atualização do Astra Control Center (`astra-control-center-[version].tar.gz`) no "Site de suporte da NetApp".
2. (Opcional) Use o seguinte comando para verificar a assinatura do pacote:

```
openssl dgst -sha256 -verify astra-control-center[version].pub
-signature <astra-control-center[version].sig astra-control-
center[version].tar.gz
```

Desembale o pacote e mude o diretório

1. Extraia as imagens:

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

2. Mude para o diretório Astra.

```
cd astra-control-center-[version]
```

Adicione as imagens ao seu registo local

1. Adicione os arquivos no diretório de imagem do Astra Control Center ao seu Registro local.

   Veja um script de exemplo para o carregamento automático de imagens abaixo.

   a. Faça login no seu Registro do Docker:

   ```
   docker login [your_registry_path]
   ```

   b. Carregue as imagens no Docker.

   c. Marque as imagens.

   d. empurre as imagens para o seu Registro local.

   ```
   export REGISTRY=[your_registry_path]
   for astraImageFile in $(ls images/*.tar)
     # Load to local cache. And store the name of the loaded image
   trimming the 'Loaded images: '
     do astraImage=$(docker load --input ${astraImageFile} | sed
   's/Loaded image: //')
     astraImage=$(echo ${astraImage} | sed 's!localhost/!!')
     # Tag with local image repo.
     docker tag ${astraImage} ${REGISTRY}/${astraImage}
     # Push to the local repo.
     docker push ${REGISTRY}/${astraImage}
   done
   ```

Instale o operador Astra Control Center atualizado

1. 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 a linha padrão de `imagePullSecrets: []` pelo seguinte:

```
imagePullSecrets:
- name: <name_of_secret_with_creds_to_local_registry>
```

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

c. Altere `[your_registry_path]` para a `acc-operator-controller-manager` 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
```

```
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
  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: [your_registry_path]/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
        command:
        - /manager
        env:
        - name: ACCOP_LOG_LEVEL
          value: "2"
        - name: ACCOP_HELM_UPGRADETIMEOUT
          value: 300m
        image: [your_registry_path]/acc-operator:[version x.y.z]
        imagePullPolicy: IfNotPresent
      imagePullSecrets: []
```

2. 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.astra.
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
```

Atualizar o Astra Control Center

1. Edite o recurso personalizado do Astra Control Center (CR(`astra_control_center_min.yaml`)) e altere a versão do Astra (`astraVersion`dentro `Spec` do número do) para o mais recente:

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

> Seu caminho do Registro deve corresponder ao caminho do Registro onde você enviou as imagens em um passo anterior.

2. Adicione as seguintes linhas dentro `additionalValues` do `Spec` no Astra Control Center CR:

```
additionalValues:
    nautilus:
      startupProbe:
        periodSeconds: 30
        failureThreshold: 600
```

3. Execute um dos seguintes procedimentos:
   a. Se você não tiver seu próprio IngressController ou IngressController e estiver usando o Astra Control Center com seu gateway Traefik como um serviço do tipo LoadBalancer e gostaria de continuar com essa configuração, especifique outro campo `ingressType` (se ainda não estiver presente) e defina-o como `AccTraefik`.

      ```
      ingressType: AccTraefik
      ```

   b. Se você quiser mudar para a implantação de entrada genérica padrão do Astra Control Center, forneça sua própria configuração de IngressController/IngressController (com terminação TLS, etc.), abra uma rota para o Astra Control Center e defina `ingressType` como `Generic`.

      ```
      ingressType: Generic
      ```

      Se você omitir o campo, o processo se tornará a implantação genérica. Se você não quiser a implantação genérica, certifique-se de adicionar o campo.

4. (Opcional) Verifique se os pods terminam e ficam disponíveis novamente:

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

5. Aguarde que as condições de status Astra indiquem que o upgrade esteja concluído e pronto:

   ```
   kubectl get -o yaml -n [netapp-acc or custom namespace]
   astracontrolcenters.astra.netapp.io astra
   ```

   Resposta:

   ```
   conditions:
     - lastTransitionTime: "2021-10-25T18:49:26Z"
       message: Astra is deployed
       reason: Complete
       status: "True"
       type: Ready
     - lastTransitionTime: "2021-10-25T18:49:26Z"
       message: Upgrading succeeded.
       reason: Complete
       status: "False"
       type: Upgrading
   ```

6. Faça login novamente e verifique se todos os clusters gerenciados e aplicativos ainda estão presentes e protegidos.

7. Se o operador não tiver atualizado o Cert-manager, atualize os serviços de terceiros, em seguida.

Atualizar serviços de terceiros (opcional)

Os serviços de terceiros Traefik e Cert-manager não são atualizados durante etapas anteriores de atualização. Você pode, opcionalmente, atualizá-los usando o procedimento descrito aqui ou manter versões de serviço existentes se o seu sistema exigir isso.

- **Traefik**: Por padrão, o Astra Control Center gerencia o ciclo de vida da implantação do Traefik. Definir `externalTraefik` como `false` (padrão) indica que não existe Traefik externo no sistema e o Traefik está sendo instalado e gerenciado pelo Astra Control Center. Neste caso, `externalTraefik`está definido como `false`.

  Por outro lado, se você tiver sua própria implantação do Traefik, defina `externalTraefik` como `true`. Nesse caso, você mantém a implantação e o Astra Control Center não atualizará as CRDs, a menos `shouldUpgrade` que esteja definido como `true`.

- **Cert-manager**: Por padrão, o Astra Control Center instala o cert-manager (e CRDs), a menos que você defina `externalCertManager` como `true`. Defina `shouldUpgrade` como `true` para que o Astra Control Center atualize as CRDs.

O Traefik é atualizado se qualquer uma das seguintes condições for cumprida:

- ExternalTraefik: FALSO OR
- ExternalTraefik: TRUE E shouldUpgrade: True.

Passos

1. Editar o `acc` CR:

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

2. Altere o `externalTraefik` campo e o `shouldUpgrade` campo para `true` ou `false` conforme necessário.

```
crds:
    externalTraefik: false
    externalCertManager: false
    shouldUpgrade: false
```

Verifique o status do sistema

1. Faça login no Astra Control Center.
2. Verifique se todos os clusters e aplicativos gerenciados ainda estão presentes e protegidos.

Configure a entrada para o balanceamento de carga

Você pode configurar um objeto de entrada do Kubernetes que gerencia o acesso externo aos serviços, como balanceamento de carga em um cluster.

- A atualização padrão usa a implantação genérica de entrada. Nesse caso, você também precisará configurar um controlador de entrada ou um recurso de entrada.
- Se você não quiser um controlador de entrada e quiser manter o que já tem, defina `ingressType` como `AccTraefik`.

> Para obter detalhes adicionais sobre o tipo de serviço "LoadBalancer" e Ingress, "Requisitos"consulte .

Os passos diferem consoante o tipo de controlador de entrada que utiliza:

- Controlador de entrada nginx
- Controlador de entrada OpenShift

O que você vai precisar

- Na especificação CR,
  - Se `crd.externalTraefik` estiver presente, deve ser definido como `false` OU
  - Se `crd.externalTraefik` for `true`, `crd.shouldUpgrade` também deve ser `true`.
- O necessário "controlador de entrada" já deve ser implantado.
- O "classe de entrada" correspondente ao controlador de entrada já deve ser criado.
- Você está usando versões do Kubernetes entre o v1,19 e o v1,21, inclusive.

Etapas para o controlador nginx Ingress

1. Use o segredo existente `secure-testing-cert` ou crie um segredo do tipo[`kubernetes.io/tls`] para uma chave privada TLS e um certificado no `netapp-acc` namespace (ou nome personalizado), conforme descrito em "Segredos TLS".
2. Implante um recurso de entrada no `netapp-acc` namespace (ou nome personalizado) para um esquema obsoleto ou novo:

   a. Para um esquema obsoleto, siga esta amostra:

```
apiVersion: extensions/v1beta1
kind: Ingress
metadata:
  name: ingress-acc
  namespace: [netapp-acc or custom namespace]
  annotations:
    kubernetes.io/ingress.class: nginx
spec:
  tls:
  - hosts:
    - <ACC address>
    secretName: [tls secret name]
  rules:
  - host: [ACC address]
    http:
      paths:
      - backend:
        serviceName: traefik
        servicePort: 80
        pathType: ImplementationSpecific
```

b. Para um novo esquema, siga este exemplo:

```
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: netapp-acc-ingress
  namespace: [netapp-acc or custom namespace]
spec:
  ingressClassName: [class name for nginx controller]
  tls:
  - hosts:
    - <ACC address>
    secretName: [tls secret name]
  rules:
  - host: <ACC address>
    http:
      paths:
        - path:
          backend:
            service:
              name: traefik
              port:
                number: 80
          pathType: ImplementationSpecific
```

Passos para o controlador OpenShift Ingress

1. Procure seu certificado e prepare os arquivos de chave, certificado e CA para uso pela rota OpenShift.
2. Crie a rota OpenShift:

```
oc create route edge --service=traefik
--port=web -n [netapp-acc or custom namespace]
--insecure-policy=Redirect --hostname=<ACC address>
--cert=cert.pem --key=key.pem
```

Verifique a configuração da entrada

Pode verificar a configuração de entrada antes de continuar.

1. Certifique-se de que o Traefik foi alterado para `clusterIP` de Loadbalancer:

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

2. Verifique as rotas em Traefik:

```
Kubectl get ingressroute ingressroutetls -n [netapp-acc or custom
namespace]
-o yaml | grep "Host("
```

O resultado deve estar vazio.

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 .

O que você vai precisar

- Use a IU do Astra Control Center para desgerenciar tudo "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_min.yaml -n netapp-acc
   ```

   Resultado:

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

2. Use o seguinte comando para excluir o `netapp-acc` namespace:

   ```
   kubectl delete ns netapp-acc
   ```

   Resultado:

   ```
   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"

Automatize com a API REST

Automação com a API REST do Astra Control

O Astra Control tem uma API REST que permite acessar diretamente a funcionalidade Astra Control usando uma linguagem de programação ou utilitário como o Curl. Também é possível gerenciar implantações do Astra Control usando o Ansible e outras tecnologias de automação.

Para configurar e gerenciar suas aplicações Kubernetes, você pode usar a IU do Astra ou a API Astra Control.

Para saber mais, acesse "Documentação de automação do Astra" .

Implantar aplicativos

Implante Jenkins a partir de um gráfico Helm

Saiba como implantar o Jenkins a partir do "Gráfico de Bitnami Helm". Depois de implantar o Jenkins no cluster, é possível Registrar a aplicação com o Astra Control.

Jenkins é uma aplicação validada para Astra Control.

- "Saiba a diferença entre um aplicativo validado e um aplicativo padrão no Astra Control".

Essas instruções se aplicam ao Astra Control Service e ao Astra Control Center.

> Os aplicativos implantados no Google Marketplace não foram validados. Alguns usuários relatam problemas com descoberta e/ou backup com implantações do Google Marketplace de Postgres, MariaDB e MySQL.

Requisitos

- Um cluster que foi adicionado ao Astra Control.

  > No Astra Control Center, você pode adicionar primeiro o cluster ao Astra Control Center ou adicionar primeiro a aplicação.

- Versões atualizadas do Helm (versão 3,2) e do Kubectl instaladas em uma máquina local com o kubeconfig adequado para o cluster

No momento, o Astra Control não oferece suporte ao "Plug-in do Kubernetes para Jenkins". Você pode executar o Jenkins em um cluster do Kubernetes sem o plugin. O plugin fornece escalabilidade para o seu cluster Jenkins.

Instale o Jenkins

Duas notas importantes sobre este processo:

- Você precisa implantar a aplicação depois que o cluster for adicionado ao Astra Control Service, não antes. O Astra Control Center aceitará aplicações antes ou depois que o cluster for adicionado ao Astra Control Center.
- Você deve implantar o gráfico Helm em um namespace diferente do padrão.

Passos

1. Adicione o repositório do gráfico Bitnami:

   ```
   helm repo add bitnami https://charts.bitnami.com/bitnami
   ```

2. Crie o `jenkins` namespace e implante o Jenkins nele com o comando:

```
helm install <name> bitnami/jenkins --namespace <namespace> --create
-namespace
--set global.storageClass=<storage_class_name>
```

Se o tamanho do volume for alterado, use as unidades Kibibibyte (Ki), Mebibyte (mi) ou Gibibyte (GI).

Você precisa definir a classe de armazenamento somente nessas situações:

- Você está usando o Astra Control Service e não quer usar a classe de storage padrão.
- Você está usando o Astra Control Center e ainda não importou o cluster para o Astra Control Center. Ou você importou o cluster, mas não deseja usar a classe de armazenamento padrão.

Resultado

Isso faz o seguinte:

- Cria um namespace.
- Define a classe de armazenamento correta.

Depois que os pods estiverem online, você poderá gerenciar a aplicação com o Astra Control. O Astra Control permite gerenciar um aplicativo no nível de namespace ou usando uma etiqueta de leme.

Implante o MariaDB a partir de um gráfico Helm

Saiba como implantar o MariaDB a partir do "Gráfico de Bitnami Helm". Depois de implantar o MariaDB no cluster, você poderá gerenciar a aplicação com o Astra Control.

O MariaDB é uma aplicação validada para Astra.

- "Saiba a diferença entre um aplicativo validado e um aplicativo padrão no Astra Control".

Essas instruções se aplicam ao Astra Control Service e ao Astra Control Center.

Os aplicativos implantados no Google Marketplace não foram validados. Alguns usuários relatam problemas com descoberta e/ou backup com implantações do Google Marketplace de Postgres, MariaDB e MySQL.

Requisitos

- Um cluster que foi adicionado ao Astra Control.

No Astra Control Center, você pode adicionar primeiro o cluster ao Astra Control Center ou adicionar primeiro a aplicação.

- Versões atualizadas do Helm (versão 3,2) e do Kubectl instaladas em uma máquina local com o kubeconfig adequado para o cluster

Instale o MariaDB

Duas notas importantes sobre este processo:

- Você precisa implantar a aplicação depois que o cluster for adicionado ao Astra Control Service, não antes. O Astra Control Center aceitará aplicações antes ou depois que o cluster for adicionado ao Astra Control Center.
- Você deve implantar o gráfico Helm em um namespace diferente do padrão.

Passos

1. Adicione o repositório do gráfico Bitnami:

```
helm repo add bitnami https://charts.bitnami.com/bitnami
```

2. Implante o MariaDB com o comando:

```
helm install <name> bitnami/MariaDB --namespace <namespace> --create
-namespace
--set global.storageClass=<storage_class_name>
```

> Se o tamanho do volume for alterado, use as unidades Kibibibyte (Ki), Mebibyte (mi) ou Gibibyte (GI).

Você precisa definir a classe de armazenamento somente nessas situações:

- Você está usando o Astra Control Service e não quer usar a classe de storage padrão.
- Você está usando o Astra Control Center e ainda não importou o cluster para o Astra Control Center. Ou você importou o cluster, mas não deseja usar a classe de armazenamento padrão.

Resultado

Isso faz o seguinte:

- Cria um namespace.
- Implanta o MariaDB no namespace.
- Cria um banco de dados.

> Este método de configuração da senha na implantação é inseguro. Não recomendamos isso para um ambiente de produção.

Depois que os pods estiverem online, você poderá gerenciar a aplicação com o Astra Control. O Astra Control permite gerenciar um aplicativo no nível de namespace ou usando uma etiqueta de leme.

Implante o MySQL a partir de um gráfico Helm

Saiba como implantar o MySQL a partir do "Gráfico de Bitnami Helm". Depois de implantar o MySQL no cluster Kubernetes, você pode gerenciar a aplicação com o Astra Control.

O MySQL é uma aplicação validada para Astra Control.

- "Saiba a diferença entre um aplicativo validado e um aplicativo padrão no Astra Control".

Essas instruções se aplicam ao Astra Control Service e ao Astra Control Center.

> Os aplicativos implantados no Google Marketplace não foram validados. Alguns usuários relatam problemas com descoberta e/ou backup com implantações do Google Marketplace de Postgres, MariaDB e MySQL.

Requisitos

- Um cluster que foi adicionado ao Astra Control.

  > No Astra Control Center, você pode adicionar primeiro o cluster ao Astra Control Center ou adicionar primeiro a aplicação.

- Versões atualizadas do Helm (versão 3,2) e do Kubectl instaladas em uma máquina local com o kubeconfig adequado para o cluster

Instale o MySQL

Duas notas importantes sobre este processo:

- Você precisa implantar a aplicação depois que o cluster for adicionado ao Astra Control Service, não antes. O Astra Control Center aceitará aplicações antes ou depois que o cluster for adicionado ao Astra Control Center.
- Recomendamos que você implante o gráfico Helm em um namespace diferente do padrão.

Passos

1. Adicione o repositório do gráfico Bitnami:

   ```
   helm repo add bitnami https://charts.bitnami.com/bitnami
   ```

2. Implemente MySQL com o comando:

   ```
   helm install <name> bitnami/mysql --namespace <namespace> --create
   -namespace
   --set global.storageClass=<storage_class_name>
   ```

   > Se o tamanho do volume for alterado, use as unidades Kibibibyte (Ki), Mebibyte (mi) ou Gibibyte (GI).

   Você precisa definir a classe de armazenamento somente nessas situações:

   - Você está usando o Astra Control Service e não quer usar a classe de storage padrão.
   - Você está usando o Astra Control Center e ainda não importou o cluster para o Astra Control Center. Ou você importou o cluster, mas não deseja usar a classe de armazenamento padrão.

Resultado

Isso faz o seguinte:

- Cria um namespace.
- Implanta MySQL no namespace.

Depois que os pods estiverem online, você poderá gerenciar a aplicação com o Astra Control. O Astra Control permite gerenciar um aplicativo com seu nome, no nível do namespace ou usando uma etiqueta de leme.

Implante Postgres a partir de um gráfico Helm

Saiba como implantar Postgres a partir do "Gráfico de Bitnami Helm". Depois de implantar o Postgres no cluster, você pode Registrar a aplicação com o Astra Control.

Postgres é um aplicativo validado para Astra.

- "Saiba a diferença entre um aplicativo validado e um aplicativo padrão no Astra Control".

Essas instruções se aplicam ao Astra Control Service e ao Astra Control Center.

> Os aplicativos implantados no Google Marketplace não foram validados. Alguns usuários relatam problemas com descoberta e/ou backup com implantações do Google Marketplace de Postgres, MariaDB e MySQL.

Requisitos

- Um cluster que foi adicionado ao Astra Control.

> No Astra Control Center, você pode adicionar primeiro o cluster ao Astra Control Center ou adicionar primeiro a aplicação.

- Versões atualizadas do Helm (versão 3,2) e do Kubectl instaladas em uma máquina local com o kubeconfig adequado para o cluster

Instale Postgres

Duas notas importantes sobre este processo:

- Você precisa implantar a aplicação depois que o cluster for adicionado ao Astra Control Service, não antes. O Astra Control Center aceitará aplicações antes ou depois que o cluster for adicionado ao Astra Control Center.
- Você deve implantar o gráfico Helm em um namespace diferente do padrão.

Passos

1. Adicione o repositório do gráfico Bitnami:

```
helm repo add bitnami https://charts.bitnami.com/bitnami
```

2. Implante Postgres com o comando:

```
helm install <name> bitnami/postgresql --namespace <namespace> --create
-namespace
--set global.storageClass=<storage_class_name>
```

Se o tamanho do volume for alterado, use as unidades Kibibibyte (Ki), Mebibyte (mi) ou Gibibyte (GI).

Você precisa definir a classe de armazenamento somente nessas situações:

- Você está usando o Astra Control Service e não quer usar a classe de storage padrão.
- Você está usando o Astra Control Center e ainda não importou o cluster para o Astra Control Center. Ou você importou o cluster, mas não deseja usar a classe de armazenamento padrão.

Resultado

Isso faz o seguinte:

- Cria um namespace.
- Implanta Postgres no namespace.

Depois que os pods estiverem online, você poderá gerenciar a aplicação com o Astra Control. O Astra Control permite gerenciar um aplicativo no nível de namespace ou usando uma etiqueta de leme.

Conhecimento e apoio

Solução de problemas

Aprenda a contornar alguns problemas comuns que você pode encontrar.

https://kb.netapp.com/Advice_and_Troubleshooting/Cloud_Services/Astra

Encontre mais informações

- "Como carregar um arquivo para o NetApp (login necessário)"
- "Como fazer upload manual de um arquivo para o NetApp (login necessário)"

Obtenha ajuda

O NetApp é compatível com o Astra Control de várias maneiras. Amplas opções gratuitas de suporte autônomo estão disponíveis 24 horas por dia, 7 dias por semana, como artigos da base de conhecimento (KB) e um canal Slack. Sua conta Astra Control inclui suporte técnico remoto por meio de tíquetes na Web.

Se você tiver uma licença de avaliação para o Astra Control Center, poderá obter suporte técnico. No entanto, a criação de casos através do site de suporte da NetApp (NSS) não está disponível. Você pode entrar em Contato com o suporte por meio da opção de feedback ou usar o canal Slack para autoatendimento.

Você deve primeiro "Ative o suporte para o seu número de série NetApp" para usar essas opções de suporte que não são de autoatendimento. É necessária uma conta SSO do site de suporte da NetApp (NSS) para chat e emissão de bilhetes na Web, juntamente com o gerenciamento de casos.

Opções de auto-suporte

Você pode acessar as opções de suporte na IU do Astra Control Center selecionando a guia **Support** no menu principal.

Estas opções estão disponíveis gratuitamente, 24x7:

- "**Base de conhecimento** (login necessário)": Procure artigos, perguntas frequentes ou informações sobre Break Fix relacionadas ao Astra Control.
- **Centro de documentação**: Este é o site de documentação que você está vendo atualmente.
- "**Obter ajuda via Slack**": Vá para o canal Containers no espaço de trabalho thePub para se conetar com colegas e especialistas.
- * Criar um caso de suporte*: Gere pacotes de suporte para fornecer ao suporte NetApp para solução de problemas.
- **Dê feedback sobre o Astra Control**: Envie um e-mail para NetApp.com para nos informar seus pensamentos, ideias ou preocupações.

Habilite o upload diário do pacote de suporte programado para o suporte da NetApp

Durante a instalação do Astra Control Center, se você especificar `enrolled: true` `autoSupport` no arquivo CRD (Custom Resource Definition) do Astra Control Center (`astra_control_center_min.yaml`, os pacotes de suporte diários serão automaticamente carregados para o "Site de suporte da NetApp".

Gerar pacote de suporte para fornecer ao suporte da NetApp

O Astra Control Center permite que o usuário administrativo gere pacotes, que incluem informações úteis para o suporte da NetApp, incluindo logs, eventos para todos os componentes da implantação do Astra, métricas e informações de topologia sobre clusters e aplicações em gerenciamento. Se você estiver conetado à Internet, poderá fazer o upload de pacotes de suporte para o site de suporte da NetApp (NSS) diretamente a partir da IU do Centro de Controle Astra.

> O tempo gasto pelo Astra Control Center para gerar o pacote depende do tamanho da instalação do Astra Control Center, bem como dos parâmetros do pacote de suporte solicitado. O tempo de duração especificado ao solicitar um pacote de suporte determina o tempo necessário para que o pacote seja gerado (por exemplo, um período de tempo mais curto resulta em geração de pacotes mais rápida).

Antes de começar

Determine se uma conexão proxy será necessária para carregar pacotes para o NSS. Se for necessária uma conexão proxy, verifique se o Astra Control Center foi configurado para usar um servidor proxy.

1. Selecione **Contas** > **conexões**.
2. Verifique as configurações de proxy em **Configurações de conexão**.

Passos

1. Crie um caso no portal do NSS usando o número de série da licença listado na página **suporte** da IU do Astra Control Center.
2. Execute as etapas a seguir para gerar o pacote de suporte usando a IU do Astra Control Center:
   a. Na página **suporte**, no bloco Pacote suporte, selecione **gerar**.
   b. Na janela **Generate a Support Bundle** (gerar um pacote de suporte), selecione o período de tempo.

      Você pode escolher entre prazos rápidos ou personalizados.

      > Você pode escolher um intervalo de datas personalizado, bem como especificar um período de tempo personalizado durante o intervalo de datas.

   c. Depois de fazer as seleções, selecione **Confirm**.
   d. Marque a caixa de seleção **carregar o pacote para o site de suporte da NetApp quando gerado**.
   e. Selecione **Generate Bundle**.

      Quando o pacote de suporte estiver pronto, uma notificação aparece na página **Contas** > **notificação** na área Alertas, na página **atividade** e também na lista de notificações (acessível selecionando o ícone no lado superior direito da interface do usuário).

Se a geração falhar, um ícone será exibido na página gerar pacote. Selecione o ícone para ver a mensagem.

O ícone de notificações no canto superior direito da interface do usuário fornece informações sobre eventos relacionados ao pacote de suporte, como quando o pacote é criado com êxito, quando a criação do pacote falha, quando o pacote não pôde ser carregado, quando o pacote não pôde ser baixado, e assim por diante.

Se você tiver uma instalação com ar-gapped

Se você tiver uma instalação com conexão via rede, execute as seguintes etapas após a geração do pacote suporte. Quando o pacote está disponível para download, o ícone Download aparece ao lado de **Generate** na seção **Support Bundles** da página **Support**.

Passos

1. Selecione o ícone Transferir para transferir o pacote localmente.
2. Carregue manualmente o pacote para o NSS.

   Você pode usar um dos seguintes métodos para fazer isso:

   - "Carregamento de ficheiro autenticado NetApp (necessário iniciar sessão)"Use .
   - Fixe o pacote ao estojo diretamente no NSS.
   - Use o Digital Advisor.

Encontre mais informações

- "Como carregar um arquivo para o NetApp (login necessário)"
- "Como fazer upload manual de um arquivo para o NetApp (login necessário)"

Versões anteriores da documentação do Astra Control Center

A documentação para versões anteriores está disponível.

- "Documentação do Astra Control Center 21,12"
- "Documentação do Astra Control Center 21,08"

Avisos legais

Avisos legais fornecem acesso a declarações de direitos autorais, marcas registradas, patentes e muito mais.

Direitos de autor

"https://www.netapp.com/company/legal/copyright/"

Marcas comerciais

NetApp, o logotipo DA NetApp e as marcas listadas na página de marcas comerciais da NetApp são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respetivos proprietários.

"https://www.netapp.com/company/legal/trademarks/"

Patentes

Uma lista atual de patentes de propriedade da NetApp pode ser encontrada em:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Política de privacidade

"https://www.netapp.com/company/legal/privacy-policy/"

Código aberto

Os arquivos de aviso fornecem informações sobre direitos autorais de terceiros e licenças usadas no software NetApp.

- "Aviso para Astra Control Center"
- "Aviso para Astra Data Store"

Licença de API Astra Control

https://docs.netapp.com/us-en/astra-automation-2204/media/astra-api-license.pdf

Informações sobre direitos autorais

Informações sobre marcas comerciais