Documentação do Astra Control Center 21,08

Astra Control Center

NetApp
October 23, 2024

Índice

Documentação do Astra Control Center 21,08

Notas de lançamento

Temos o prazer de anunciar o lançamento inicial do Astra Control Center.

- "O que há nesta versão do Astra Control Center"
- "Problemas conhecidos"
- "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.

Conteúdo desta versão do Astra Control Center

Temos o prazer de anunciar o lançamento do Astra Control Center.

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"

Problemas conhecidos com esta versão

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

Os seguintes problemas conhecidos afetam a versão atual:

- ClusterRoleBinding incorreto criado pelo Astra Control Center CRD durante a instalação
- Aplicativo com rótulo definido pelo usuário entra no estado "removido"
- Não é possível parar de executar a cópia de segurança da aplicação
- Falha de backup ou clone em aplicativos que usam PVCs com unidades decimais no Astra Control Center
- como alterações de volume persistente

- Durante a restauração do aplicativo a partir do backup Trident cria um PV maior do que o PV original
- Desempenho de clones afetado por grandes volumes persistentes
- 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 buckets do S3 no Astra Control Center não relatam a capacidade disponível
- A reutilização de buckets entre instâncias do Astra Control Center causa falhas
- Selecionar um tipo de provedor de bucket com credenciais para outro tipo causa falhas na proteção de dados
- Backups e snapshots podem não ser retidos durante a remoção de uma instância do Astra Control Center
- Backups extras são mantidos como parte do backup agendado
- "A operação clone não pode usar outros buckets além do padrão"
- O gerenciamento de um cluster com Astra Control Center falha quando o arquivo kubeconfig padrão contém mais de um contexto
- "Não é possível determinar o status do pacote tar ASUP em ambiente dimensionado"
- A desinstalação do Astra Control Center não consegue limpar o pod do operador de monitoramento no cluster gerenciado
- A desinstalação do Astra Control Center não consegue limpar CRDs do Traefik
- Coleção ASUP presa em um estado de geração ou upload

ClusterRoleBinding incorreto criado pelo Astra Control Center CRD durante a instalação

Aplique o patch a seguir a todos os clusters do Kubernetes onde a versão 21.08.65 do operador acc foi implantada. Também deve ser aplicado se o operador acc for reativado.

Para resolver este problema:

1. Substitua `ACC_NAMESPACE` no script abaixo pelo namespace que você usou para "Implante o Astra Control Center".

```
cat <<EOF | kubectl apply -f -
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: acc-operator-manager-rolebinding
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: acc-operator-manager-role
subjects:
- kind: ServiceAccount
  name: default
  namespace: netapp-acc-operator
- apiGroup: rbac.authorization.k8s.io
  kind: Group
  name: system:serviceaccounts:ACC_NAMESPACE
EOF
```

2. Execute o script.

O patch remove os dois assuntos a seguir `ClusterRoleBinding: "acc-operator-manager-rolebinding"`

```
- apiGroup: rbac.authorization.k8s.io
  kind: Group
  name: system:serviceaccounts
- apiGroup: ""
  kind: Group
  name: system:serviceaccounts
```

Aplicativo com rótulo definido pelo usuário entra no estado "removido"

Se você definir um aplicativo com um rótulo k8s inexistente, o Astra Control Center criará, gerenciará e removerá imediatamente o aplicativo. Para evitar isso, adicione o rótulo k8s aos pods e recursos depois que o aplicativo for gerenciado pelo Astra Control Center.

Não é possível parar de executar a cópia de segurança da aplicação

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 do Astra".

Falha de backup ou clone em aplicativos que usam PVCs com unidades decimais no Astra Control Center

Os volumes criados com unidades decimais falham usando o processo de backup ou clone do Astra Control

Center. Consulte "artigo da base de conhecimento" para obter mais informações.

A IU do Astra Control Center fica lenta para mostrar alterações nos recursos da aplicação, como alterações de volume persistente

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. Esse atraso na IU também pode ocorrer quando quaisquer recursos do aplicativo são adicionados ou modificados. Nesse caso, uma operação de proteção de dados é bem-sucedida em minutos e você pode usar o software de gerenciamento do back-end de storage para confirmar a alteração no tamanho do volume.

Durante a restauração do aplicativo a partir do backup Trident cria um PV maior do que o PV original

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

Desempenho de clones afetado por grandes volumes persistentes

Clones de volumes persistentes muito grandes e consumidos podem ser lentos intermitentemente, dependendo do acesso do cluster ao armazenamento de objetos. Se o clone estiver suspenso e nenhum dado tiver sido copiado por mais de 30 minutos, o Astra Control encerrará a ação do clone.

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 OCP. 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 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.

A reutilização de buckets entre instâncias do Astra Control Center causa falhas

Se você tentar reutilizar um bucket usado por outra instalação ou anterior do Astra Control Center, o backup e a restauração falharão. Deve utilizar um balde diferente ou limpar completamente o balde anteriormente utilizado. Não é possível compartilhar buckets entre instâncias do Astra Control Center.

Selecionar um tipo de provedor de bucket com credenciais para outro tipo causa falhas na proteção de dados

Quando você adicionar um bucket, selecione o tipo correto de provedor de bucket com credenciais corretas para esse provedor. Por exemplo, a IU aceita o NetApp ONTAP S3 como o tipo com credenciais

StorageGRID; no entanto, isso fará com que todos os backups e restaurações futuros de aplicativos que usam esse bucket falhem.

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.

Backups extras são mantidos como parte do backup agendado

Às vezes, um ou mais backups no Astra Control Center são retidos além do número especificado para serem retidos no cronograma de backup. Esses backups extras devem ser excluídos como parte de um backup agendado, mas não são excluídos e estão presos em um `pending` estado. Para resolver o problema, "forçar a eliminação" os backups extras.

A operação clone não pode usar outros buckets além do padrão

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.

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.

Não é possível determinar o status do pacote tar ASUP em ambiente dimensionado

Durante a coleção ASUP, o status do bundle na IU é relatado como `collecting` `done` ou . A coleta pode levar até uma hora para ambientes grandes. Durante o download do ASUP, a velocidade de transferência do arquivo de rede para o pacote pode ser insuficiente, e o download pode ter tempo limite após 15 minutos sem qualquer indicação na IU. Os problemas de download dependem do tamanho do ASUP, do tamanho do cluster dimensionado e se o tempo de coleta ultrapassar o limite de sete dias.

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:

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

   Resultado:

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

2. Excluir o namespace:

```
oc delete ns netapp-monitoring
```

Resultado:

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

3. Confirmar recursos removidos:

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

Resultado:

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

4. Confirmar o agente de monitoramento removido:

```
oc 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):

```
oc 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:

Passos

1. Confirme quais CRDs não foram excluídos pelo processo de desinstalação:

```
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
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
```

Coleção ASUP presa em um estado de geração ou upload

Se um pod ASUP for morto ou reiniciado, uma coleção ASUP pode ficar presa em um estado de geração ou upload. Execute a seguinte "API REST do Astra Control" chamada para iniciar novamente a coleta manual:

Método HTTP	Caminho
POST	/AccountID/core/v1/asups

Esta solução alternativa da API só funciona se for executada mais de 10 minutos após o ASUP ser iniciado.

Encontre mais informações

- "Limitações conhecidas para esta versão"

Limitações conhecidas com esta versão

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.

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 cluster está `removed` no estado, embora o cluster e a rede estejam funcionando conforme esperado

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":

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`.

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

O Astra Control Center não oferece suporte a aplicativos que são implantados com operadores habilitados para o Operator Lifecycle Manager (OLM) ou operadores com escopo de cluster.

A clonagem de aplicações só pode ser feita com a mesma distribuição do K8s

Se você clonar uma aplicação entre clusters, os clusters de origem e destino precisam ser a mesma distribuição do Kubernetes. Por exemplo, se você clonar um aplicativo de um cluster OpenShift 4,7, use um cluster de destino que também é OpenShift 4,7.

OpenShift 4,8 não é suportado

O OpenShift 4,8 não é compatível com o lançamento de julho do Astra Control Center. Para obter mais informações, "Requisitos do Astra Control Center"consulte .

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) são totalmente compatíveis. Para obter mais informações, "Requisitos do Astra Control Center"consulte .

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.

Proteção de dados para Astra Control Center como aplicação ainda não disponível

Esta versão não é compatível com a capacidade de gerenciar o Astra como aplicativo usando opções de snapshot, backup ou restauração.

Pods pouco 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.

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.

O Trident não é desinstalado de um cluster

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".

Encontre mais informações

- "Problemas conhecidos para esta versão"

Conceitos

Introdução ao 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 storage de back-end ou a serviços externos	Mesmas funcionalidades em ambas as plataformas, com exceções ao storage de back-end ou a serviços externos

	Astra Control Service	Astra Control Center
Qual é o suporte ao storage no back-end?	Ofertas de serviço de nuvem da NetApp	Sistemas NetApp ONTAP AFF e FAS

Aplicações suportadas

O Astra Control Center não oferece suporte a aplicativos que são implantados com operadores habilitados para o Operator Lifecycle Manager (OLM) ou operadores com escopo de cluster.

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

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

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 é usado "NetApp Cloud Volumes Service para Google Cloud" como storage de back-end para volumes persistentes.
  - Para clusters AKS, o Astra Control Service usa "Azure NetApp Files" como storage de back-end 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.
  - 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.

No primeiro lançamento, o Astra Control Center será compatível com clusters do Kubernetes do OpenShift e com os back-ends de storage do Trident com o ONTAP 9.5 e superior.

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 NetApp suporte com 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 armazenamento de back-end 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 Astra Trident 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.

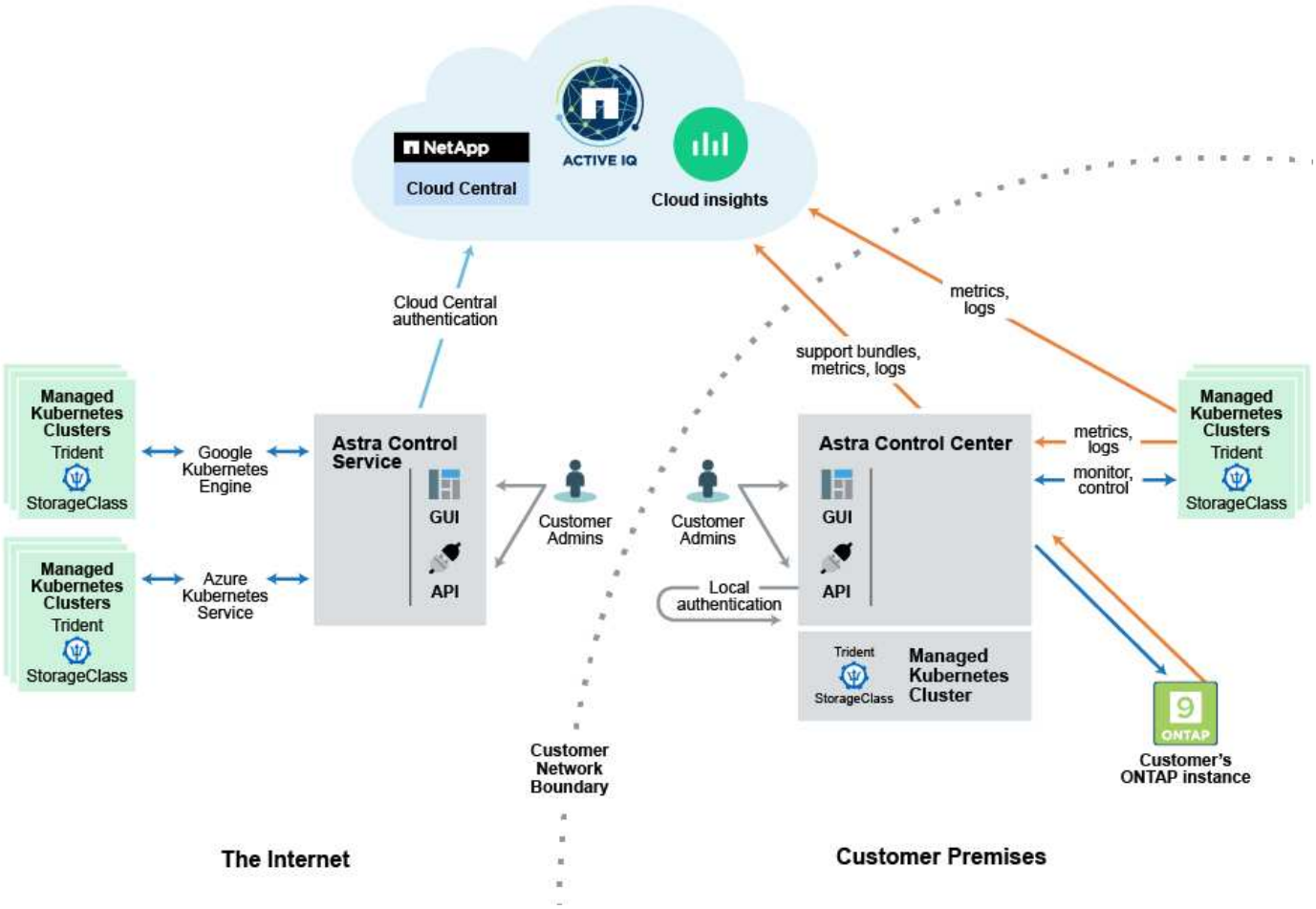
Você pode adicionar aplicativos ao cluster. Ou, se você já tiver algumas aplicações no cluster sendo gerenciado, poderá usar o Astra Control Center para detectá-las e gerenciá-las. Depois, use o Astra Control Center para criar snapshots, backups e clones.

Para mais informações

- "Documentação do Astra Control Service"
- "Documentação do Astra Control Center"
- "Documentação do Astra Trident"
- "Use a API Astra"
- "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 o Astra Control Center, o Trident inclui

um back-end de storage ONTAP configurado.

- * Storage backend*: O Astra Control Service usa "NetApp Cloud Volumes Service para Google Cloud" como armazenamento de back-end para clusters GKE e "Azure NetApp Files" como armazenamento de back-end para clusters AKS.

  O Astra Control Center usa um 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.

- **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 Control Control"
- "Documentação do Astra Trident"
- "Use a API Astra"
- "Documentação do Cloud Insights"
- "Documentação do ONTAP"

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 como storage de back-end. Você deve entender como a classe de armazenamento e o tamanho do volume persistente (PV) podem ajudá-lo a atingir seus objetivos de desempenho.

Visão geral

No momento, o Astra Control Center dá suporte apenas às classes de storage Trident com o suporte de storage ONTAP. O Astra Control Center detecta e usa os recursos já implantados, incluindo ONTAP, Trident e classes de storage associadas.

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

Classes de armazenamento

Quando você adiciona clusters ao Astra Control Center, será solicitado a escolher uma das classes de storage descobertas anteriormente para volumes persistentes. Os níveis de serviço nas classes de armazenamento são projetados para diferentes necessidades de capacidade e largura de banda. Essas classes de storage descobertas estão qualificadas para uso no Astra Control Center.

Tamanho do volume persistente e performance

Consulte as informações do Trident que fornecem comparações de custos e exemplos que podem ajudá-lo a entender melhor como acoplar um nível de serviço com tamanho de volume para atender aos seus objetivos de desempenho.

Encontre mais informações

- "Documentação do Trident sobre configuração de armazenamento"

Comece agora

Requisitos do Astra Control Center

Comece verificando o suporte para clusters, aplicativos, licenças e navegador da Web do Kubernetes.

Requisitos gerais do cluster do Kubernetes

Um cluster de Kubernetes precisa atender aos requisitos gerais a seguir para que você possa descobri-lo e gerenciá-lo no Astra Control Center.

- **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. Tem de ter a URL do registo de imagens onde irá carregar as imagens e tem de ter marcado as imagens para o registo de contentores privado.
- **Configuração de storage Trident / ONTAP**: O Astra Control Center requer que o Trident versão 21,01 ou 21,04 já esteja instalado e configurado para funcionar com o NetApp ONTAP versão 9,5 ou mais recente como o back-end de storage. 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 os seguintes drivers ONTAP fornecidos pelo Trident:
  - ONTAP-nas
  - ONTAP-nas-FlexGroup
  - ONTAP-san
  - ONTAP-são-economia

Se você está planejando gerenciar o cluster do Kubernetes a partir do Astra Control Center e usar o cluster para hospedar a instalação do Astra Control Center, o cluster terá os seguintes requisitos adicionais:

- A versão mais recente do Kubernetes "componente do controlador snapshot" é instalada
- Um Trident "volumesnapshotclass objeto" foi definido por um administrador
- Existe uma classe de storage padrão do Kubernetes no cluster
- Pelo menos uma classe de armazenamento está configurada para usar o Trident
- Um método para apontar o FQDN do Astra Control Center para o endereço IP externo do serviço Astra Control Center

Clusters OpenShift

O Astra Control Center requer um cluster Red Hat OpenShift Container Platform 4.6.8 ou 4,7 que tenha classes de storage Trident com suporte do ONTAP 9.5 ou mais recente, com os seguintes atributos:

- Pelo menos 300GB GB de capacidade de armazenamento ONTAP disponível
- 3 nós de controladora com 4 núcleos de CPU, 16GB GB de RAM e 120GB GB de storage disponível cada
- 3 nós de trabalho com pelo menos 12 núcleos de CPU, 32GB GB de RAM e 50GB GB de armazenamento disponível cada
- Kubernetes versão 1,19 ou 1,20
- Tipo de serviço "LoadBalancer" disponível para o tráfego de entrada a ser enviado para serviços no cluster OpenShift

- Um método para apontar o FQDN do Astra Control Center para o endereço IP balanceado de carga

Esses requisitos mínimos presumem que o Astra Control Center é a única aplicação em execução no cluster OpenShift. Se o cluster estiver executando aplicações adicionais, você precisará ajustar esses requisitos mínimos de acordo.

Certifique-se de que seu cluster atenda aos requisitos mínimos e que você siga as práticas recomendadas do Kubernetes para que o Astra Control Center fique altamente disponível no cluster do Kubernetes.

OpenShift 4,8 não é suportado.

Durante a clonagem de aplicativos, o Astra Control Center precisa permitir que o OpenShift monte volumes e altere a propriedade dos arquivos. Devido a isso, o ONTAP precisa ser configurado para permitir que operações de volume sejam concluídas com sucesso usando os seguintes comandos:

1. `export-policy rule modify -vserver svm0 -policyname default -ruleindex 1 -superuser sys`
2. `export-policy rule modify -policyname default -ruleindex 1 -anon 65534`

Se você pretende adicionar um segundo cluster do OpenShift 4,6 ou 4,7 como um recurso de computação gerenciado, você precisa garantir que o recurso Snapshot de volume do Trident esteja ativado. Consulte o Trident oficial "instruções" para ativar e testar instantâneos de volume com o Trident.

Requisitos de gerenciamento de aplicativos

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

- **Licenciamento**: Você precisa de uma licença do Astra Control Center para gerenciar aplicativos usando o Astra Control Center.
- **Helm 3**: 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.
- **Gerenciamento do operador**: O Astra Control Center não oferece suporte a aplicativos implantados com operadores habilitados para o Operator Lifecycle Manager (OLM) ou operadores com escopo de cluster.

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 da 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".

Tipo de serviço "LoadBalancer" para clusters do Kubernetes no local

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. Para clusters OpenShift locais, você pode usar "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.

Requisitos de rede

O cluster 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 de ambos os lados entre o cluster que hospeda o Astra Control Center e cada cluster gerenciado (observado quando aplicável).

Produto	Porta	Protocolo	Direção	Finalidade
Astra Control Center	443	HTTPS	Entrada	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
Astra Control Center	9090	HTTPS	• Ingresso (para cluster que hospeda o Astra Control Center) • Saída (porta aleatória do endereço IP do nó de cada nó de trabalho de cada cluster gerenciado)	Dados de métricas para o consumidor de métricas - garanta que cada cluster gerenciado possa acessar essa porta no cluster que hospeda o Astra Control Center
Trident	34571	HTTPS	Entrada	Comunicação do pod do nó
Trident	9220	HTTP	Entrada	Endpoint de métricas

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.
- 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 download do Astra Control Center no site de suporte da NetApp.
- Instalar o Astra Control Center no seu ambiente local.
- Descubra sua configuração do Trident com o back-end de storage do ONTAP.

  Para nossa primeira versão, você instalará as imagens em um Registro OpenShift ou usará seu Registro local.

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

Conclua algumas tarefas de configuração inicial

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

"Saiba mais sobre o processo de configuração inicial".

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"

Instale o Astra Control Center

Para instalar o Astra Control Center, siga estas etapas:

- Instale o Astra Control Center
- Faça login na IU do Astra Control Center

Instale o Astra Control Center

Para instalar o Centro de Controle Astra, baixe o pacote de instalação no site de suporte da NetApp e execute uma série de comandos 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.

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
```

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.

> Os comandos Podman podem ser usados no lugar dos comandos Docker se você estiver usando o repositório Podman da Red Hat.

Passos

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 em "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
```

5. Mude para o diretório Astra.

```
cd astra-control-center-[version]
```

6. 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 [Docker_registry_path]
```

   b. Carregue as imagens no Docker.
   c. Marque as imagens.
   d. Envie as imagens para o seu registo local.

```
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
```

7. (Apenas para Registros com requisitos de autenticação) se você usar um Registro que requer autenticação, você precisa 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=[Docker_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]
      ```

      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] --docker-server=[Docker_registry_path] --docker
-username=[username] --docker-password=[token]
```

Resposta

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

8. 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: astra-registry-cred
```

b. Altere `[Docker_registry_path]` para a `kube-rbac-prox` imagem para o caminho do registo onde as imagens foram empurradas numa etapa anterior.

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

```
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: [Docker_registry_path]/kube-rbac-proxy:v0.5.0
        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: [Docker_registry_path]/acc-operator:[version x.y.z]
        imagePullPolicy: IfNotPresent
      imagePullSecrets: []
```

9. Edite o arquivo de recurso personalizado (CR) do Astra Control Center (`astra_control_center_min.yaml`):

```
vim astra_control_center_min.yaml
```

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.

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

a. Mude `[Docker_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. Se você não estiver usando um Registro que requer autorização, exclua a `secret` linha.

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

10. 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
```

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

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

Resposta da amostra:

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

12. Execute o seguinte patch para corrigir "binding de função do cluster".
13. Instale o Astra Control Center no `netapp-acc` namespace (ou personalizado):

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

Resposta da amostra:

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

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

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

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-5fdfff786f-gkv6z            1/1     Running   0
4m58s
activity-649f869bf7-jn5gs                 1/1     Running   0
3m14s
asup-79846b5fdc-s9s97                     1/1     Running   0
3m10s
authentication-84c78f5cf4-qhx9t           1/1     Running   0
118s
billing-9b8496787-v8rzv                   1/1     Running   0
2m54s
bucketservice-5fb876d9d5-wkfvz            1/1     Running   0
3m26s
cloud-extension-f9f4f59c6-dz6s6           1/1     Running   0
3m
cloud-insights-service-5676b8c6d4-6q7lv   1/1     Running   0
2m52s
composite-compute-7dcc9c6d6c-lxdr6        1/1     Running   0
2m50s
composite-volume-74dbfd7577-cd42b         1/1     Running   0
3m2s
credentials-75dbf46f9d-5qm2b              1/1     Running   0
3m32s
entitlement-6cf875cb48-gkvhp              1/1     Running   0
3m12s
features-74fd97bb46-vss2n                 1/1     Running   0
3m6s
fluent-bit-ds-2g9jb                       1/1     Running   0
113s
fluent-bit-ds-5tg5h                       1/1     Running   0
113s
fluent-bit-ds-qfxb8                       1/1     Running   0
113s
graphql-server-7769f98b86-p4qrv           1/1     Running   0
90s
```

```
identity-566c566cd5-ntfj6                    1/1     Running   0
3m16s
influxdb2-0                                  1/1     Running   0
4m43s
krakend-5cb8d56978-44q66                     1/1     Running   0
93s
license-66cbbc6f48-27kgf                     1/1     Running   0
3m4s
login-ui-584f7fd84b-dmdrp                    1/1     Running   0
87s
loki-0                                       1/1     Running   0
4m44s
metrics-ingestion-service-6dcfddf45f-mhnvh   1/1     Running   0
3m8s
monitoring-operator-78d67b4d4-nxs6v          2/2     Running   0
116s
nats-0                                       1/1     Running   0
4m40s
nats-1                                       1/1     Running   0
4m26s
nats-2                                       1/1     Running   0
4m15s
nautilus-9b664bc55-rn9t8                     1/1     Running   0
2m56s
openapi-dc5ddfb7d-6q8vh                      1/1     Running   0
3m20s
polaris-consul-consul-5tjs7                  1/1     Running   0
4m43s
polaris-consul-consul-5wbnx                  1/1     Running   0
4m43s
polaris-consul-consul-bfvl7                  1/1     Running   0
4m43s
polaris-consul-consul-server-0               1/1     Running   0
4m43s
polaris-consul-consul-server-1               1/1     Running   0
4m43s
polaris-consul-consul-server-2               1/1     Running   0
4m43s
polaris-mongodb-0                            2/2     Running   0
4m49s
polaris-mongodb-1                            2/2     Running   0
4m22s
polaris-mongodb-arbiter-0                    1/1     Running   0
4m49s
polaris-ui-6648875998-75d98                  1/1     Running   0
92s
```

```
polaris-vault-0                                1/1     Running   0
4m41s
polaris-vault-1                                1/1     Running   0
4m41s
polaris-vault-2                                1/1     Running   0
4m41s
storage-backend-metrics-69546f4fc8-m7lfj       1/1     Running   0
3m22s
storage-provider-5d46f755b-qfv89               1/1     Running   0
3m30s
support-5dc579865c-z4pwq                       1/1     Running   0
3m18s
telegraf-ds-4452f                              1/1     Running   0
113s
telegraf-ds-gnqxl                              1/1     Running   0
113s
telegraf-ds-jhw74                              1/1     Running   0
113s
telegraf-rs-gg6m4                              1/1     Running   0
113s
telemetry-service-6dcc875f98-zft26             1/1     Running   0
3m24s
tenancy-7f7f77f699-q7l6w                       1/1     Running   0
3m28s
traefik-769d846f9b-c9crt                       1/1     Running   0
83s
traefik-769d846f9b-l9n4k                       1/1     Running   0
67s
trident-svc-8649c8bfc5-pdj79                   1/1     Running   0
2m57s
vault-controller-745879f98b-49c5v              1/1     Running   0
4m51s
```

15. (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
```

16. Quando todos os pods estiverem em execução, verifique o sucesso da instalação recuperando a instância do AstraControlCenter instalada pelo Operador do ACC.

```
kubectl get acc -o yaml -n netapp-acc
```

17. Verifique o `status.deploymentState` campo na resposta para o `Deployed` valor. Se a implantação não tiver êxito, uma mensagem de erro será exibida.

    Irá utilizar o `uuid` no passo seguinte.

```
apiVersion: v1
items:
- apiVersion: astra.netapp.io/v1
  kind: AstraControlCenter
  metadata:
    creationTimestamp: "2021-07-28T21:36:49Z"
    finalizers:
    - astracontrolcenter.netapp.io/finalizer
   generation: 1
    name: astra
    namespace: netapp-acc
    resourceVersion: "27797604"
    selfLink: /apis/astra.netapp.io/v1/namespaces/netapp-
acc/astracontrolcenters/astra
    uid: 61cd8b65-047b-431a-ba35-510afcb845f1
  spec:
    accountName: Example
    astraAddress: astra.example.com
    astraResourcesScaler: "Off"
    astraVersion: 21.08.52
    autoSupport:
      enrolled: false
    email: admin@example.com
    firstName: SRE
    lastName: Admin
    imageRegistry:
      name: registry_name/astra
  status:
    certManager: deploy
    deploymentState: Deployed
    observedGeneration: 1
    observedVersion: 21.08.52
    postInstall: Complete
    uuid: c49008a5-4ef1-4c5d-a53e-830daf994116
kind: List
metadata:
  resourceVersion: ""
  selfLink: ""
```

18. Para obter a senha única que você usará quando fizer login no Astra Control Center, copie o

`status.uuid` valor da resposta na etapa anterior. A palavra-passe é `ACC-` seguida pelo valor UUID (`ACC-[UUID]`ou, neste exemplo, `ACC-c49008a5-4ef1-4c5d-a53e-830daf994116`).

Faça login na IU do Astra Control Center

Depois de instalar o ACC, irá alterar a palavra-passe do administrador predefinido e iniciar sessão no painel de controlo da IU do ACC.

Passos

1. Em um navegador, insira o FQDN usado no no `astraAddress` `astra_control_center_min.yaml`CR quando Instalou o ACC.
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 Instalou o ACC, 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 .

Configure o Astra Control Center

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.

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.

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

Adicione uma licença completa ou de avaliação

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.

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.

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.

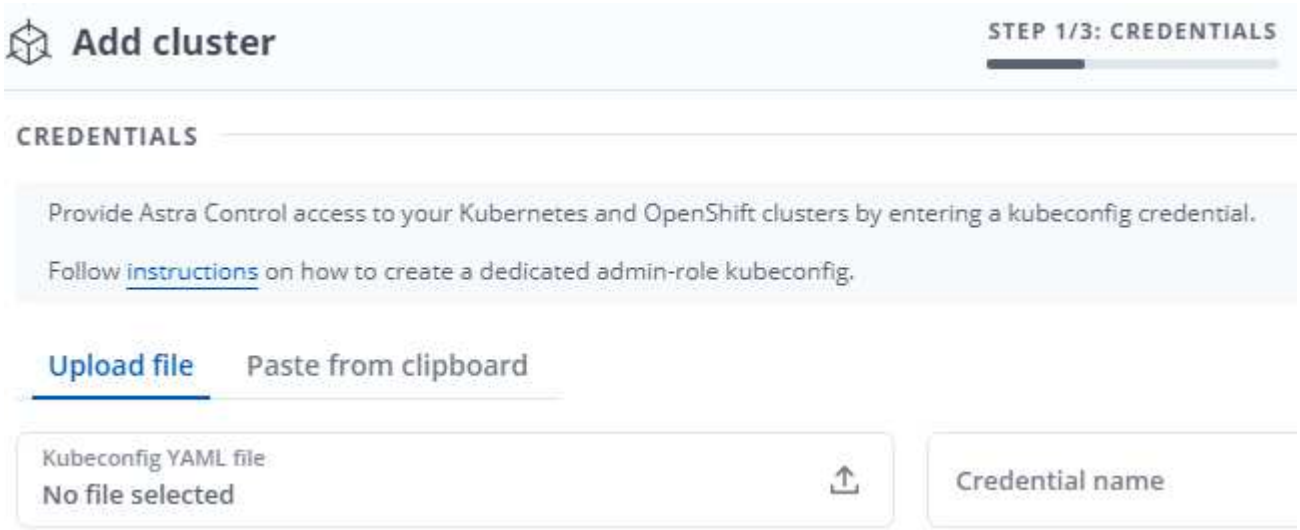
O que você precisa. 8217

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**.

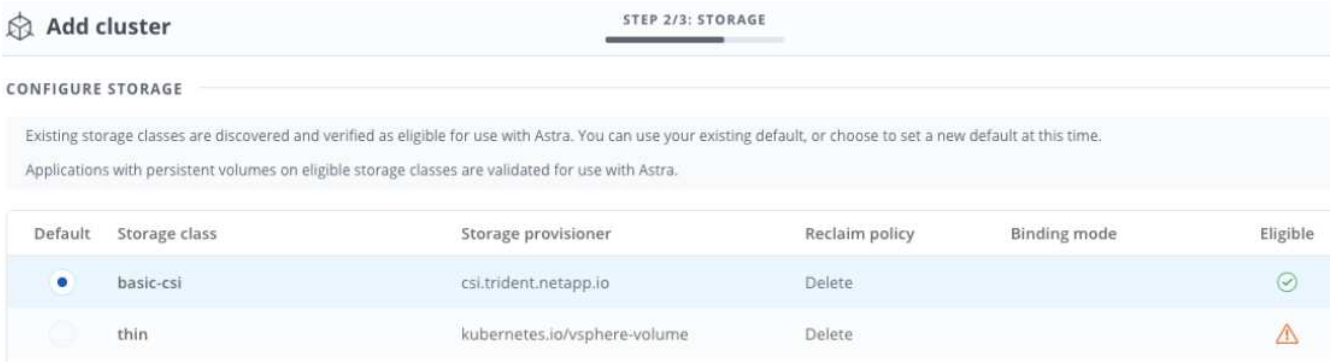


Se você criar seu próprio `kubeconfig` arquivo, você deve definir apenas **um** elemento de contexto nele. Consulte "Documentação do Kubernetes" para obter informações sobre como criar `kubeconfig` arquivos.

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 armazenamento do Trident com o suporte do armazenamento do ONTAP.



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. 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 adicionar um back-end de storage das seguintes maneiras:

- Configure o armazenamento quando estiver adicionando um cluster. "Adicionar cluster"Consulte .
- Adicione um back-end de armazenamento descoberto usando a opção Dashboard ou backends.

Você pode adicionar um back-end de armazenamento já descoberto usando estas opções:

- Adicionar back-end de storage usando o Dashboard
- Adicionar back-end de armazenamento usando backends opção

Adicionar back-end de storage usando o Dashboard

1. No Dashboard, execute um dos seguintes procedimentos:
   a. Na seção de back-end do Dashboard Storage, selecione **Manage**.

b. Na seção Resumo de recursos do Painel > backends de armazenamento, selecione **Adicionar**.

2. Insira as credenciais de administrador do ONTAP e selecione **Revisão**.
3. Confirme os detalhes do backend e selecione **Manage**.

   O backend aparece na lista com informações de resumo.

Adicionar back-end de armazenamento usando backends opção

1. Na área de navegação à esquerda, selecione **backends**.
2. Selecione **Gerenciar**.
3. Insira as credenciais de administrador do ONTAP e selecione **Revisão**.
4. Confirme os detalhes do backend e selecione **Manage**.

   O backend aparece na lista com informações de resumo.

5. Para ver detalhes do armazenamento de back-end, selecione-o.

Volumes persistentes usados por aplicativos no cluster de computação gerenciada também são exibidos.

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, "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 adicionar um bucket, selecione o tipo correto de provedor de bucket com credenciais corretas para esse provedor. Por exemplo, a IU aceita o NetApp ONTAP S3 como o tipo com 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 servidor 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.

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"
- "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 cluster que executa o OpenShift 4,6 ou 4,7, que tem o Trident StorageClasses apoiado pelo ONTAP 9.5 ou posterior.
  - Um ou mais nós de trabalho com pelo menos 1GB GB de RAM disponíveis para executar serviços de telemetria.

> ⓘ Se você planeja adicionar um segundo cluster do OpenShift 4,6 ou 4,7 como um recurso de computação gerenciado, verifique se o recurso Snapshot de volume do Trident está ativado. Consulte o Trident oficial "instruções" para ativar e testar instantâneos de volume com o Trident.

- O superusuário e ID de usuário definidos no sistema ONTAP de backup para fazer backup e restaurar aplicativos com o Centro de Controle Astra (ACC). Execute os seguintes comandos na linha de comando ONTAP:
  `export policy rule modify -vserver svm0 -policyname default -ruleindex 1 -superuser sys`
  `export-policy rule modify -policyname default -ruleindex 1 -anon 65534` (Este é o valor padrão)

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 storageClass -A
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. 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
```

3. 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.

4. Gere o kubeconfigo da seguinte forma:

   a. Crie um `create-kubeconfig.sh` arquivo. Se o índice de token que você observou na etapa anterior não for 0, substitua o valor `TOKEN_INDEX` no início do script a seguir pelo valor correto.

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

```
# Update these to match your environment. Replace the value for
TOKEN_INDEX from
# the output in the previous step if it was not 0. 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'
TOKEN_INDEX=0

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
```

5. (**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"

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

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

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.

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 será desinstalado quando eu remover um cluster Kubernetes do Astra Control?

O Trident não será desinstalado de um cluster ao removê-lo do Astra Control.

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".

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.

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 implementadas 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, 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

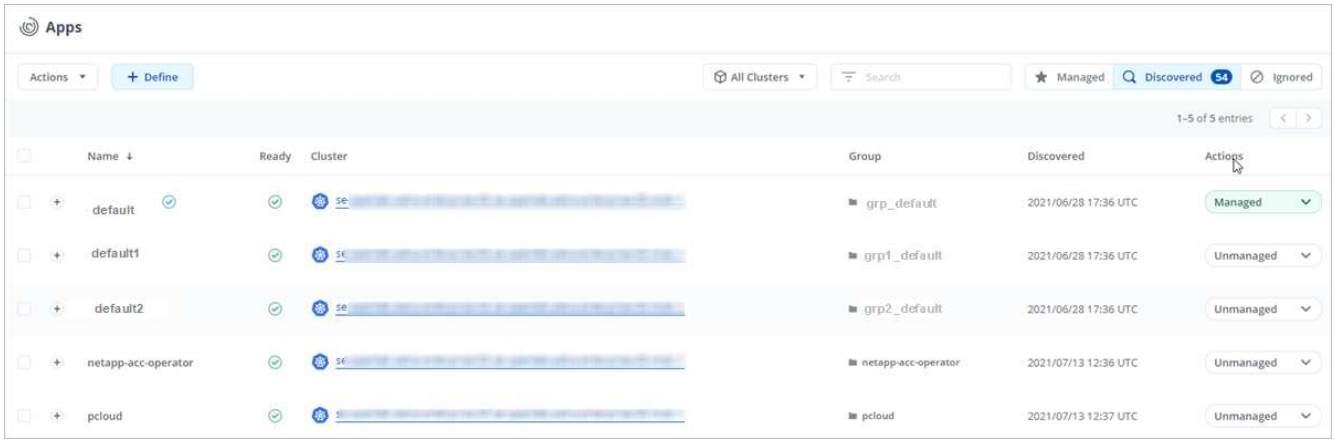
A seção **descoberto** da página Apps mostra namespaces e quaisquer aplicativos instalados pelo Helm ou aplicativos personalizados nesses namespaces. Você pode optar por gerenciar cada aplicativo individualmente ou no nível do namespace. Tudo se resume ao nível de granularidade de que você precisa para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



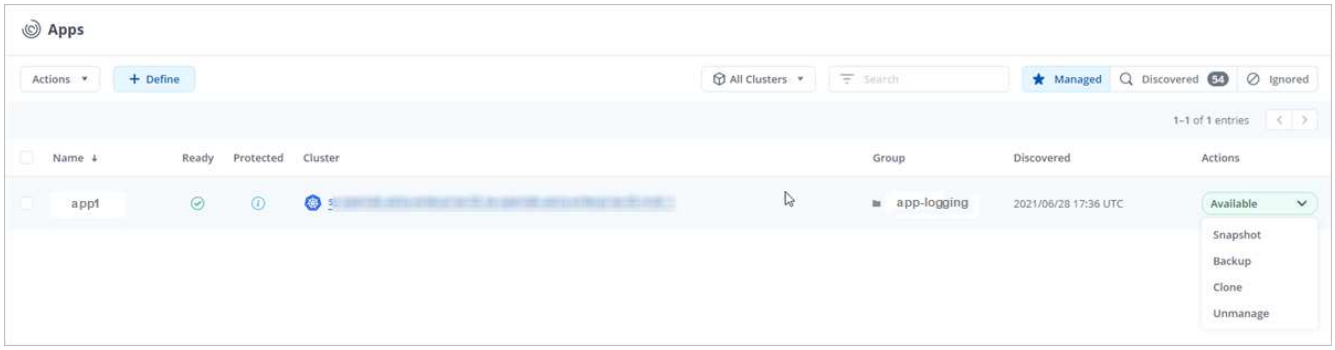
3. Veja a lista de namespaces descobertos. Expanda o namespace para exibir os aplicativos e os recursos associados.

   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, no menu ações, selecione **Gerenciar**.
7. Se você não quiser gerenciar um aplicativo, no menu ações ao lado do aplicativo, selecione **Ignorar**.

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.



Observe que o aplicativo que você acabou de adicionar tem um ícone de aviso sob a 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

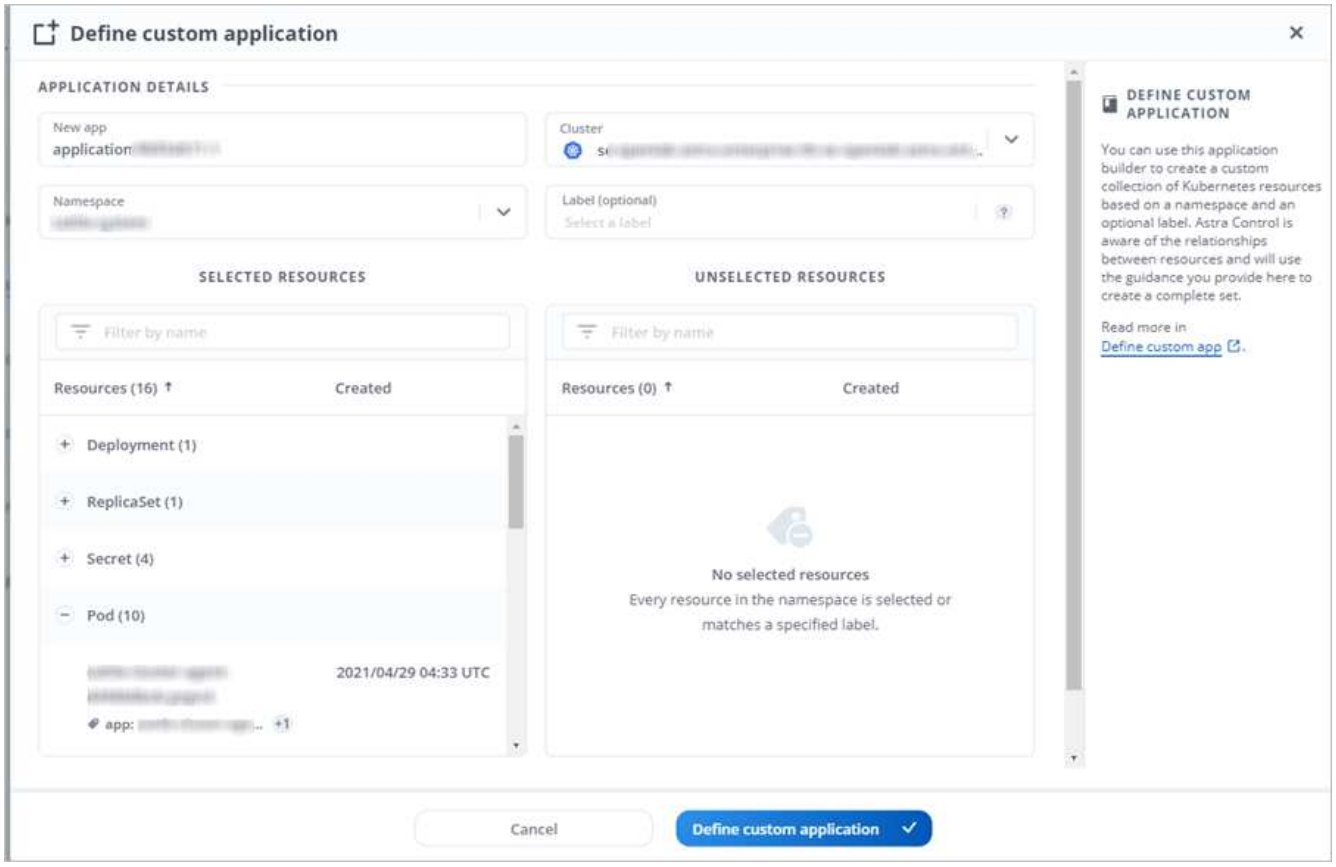
Os aplicativos que você escolheu gerenciar agora estão disponíveis na guia **gerenciado**. Quaisquer aplicativos ignorados serão movidos para a guia **ignorado**. Idealmente, a guia descoberta mostrará zero aplicativos, de modo que, à medida que novos aplicativos são instalados, eles são mais fáceis 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 **Apps**.
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 clicando no 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. Clique em **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 **Apps**.
2. Selecione **descoberto** como filtro.
3. Selecione a aplicação.
4. No menu ações, selecione **Ignorar**.
5. Para ignorar, no menu ações, selecione **Unignore**.

Desgerenciar aplicativos

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

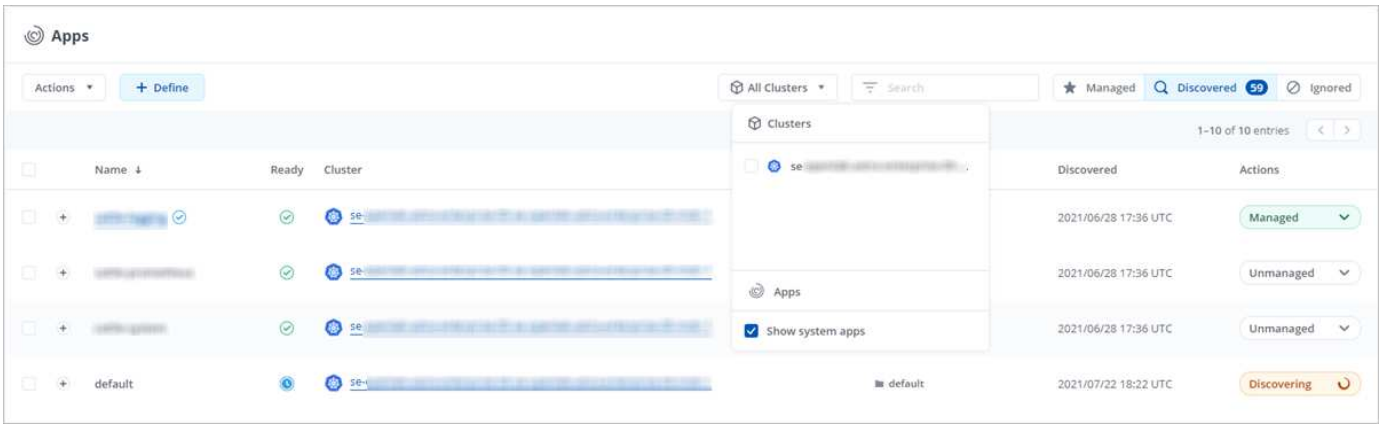
> Se você desgerenciar um aplicativo, todos os backups ou snapshots criados anteriormente serão perdidos.

Passos

1. Na barra de navegação à esquerda, selecione **Apps**.
2. Selecione **Managed** como filtro.
3. Selecione a aplicação.
4. No menu ações, selecione **Unmanage**.
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. Você pode exibir aplicativos do sistema selecionando a caixa de seleção **Mostrar aplicativos do sistema** sob o filtro Cluster na barra de ferramentas.



Não mostramos esses aplicativos de sistema por padrão, porque é raro que você precise fazer backup deles.

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".

Encontre mais informações

- "Use a API Astra"

Defina um exemplo de aplicativo personalizado

A criação de um aplicativo personalizado permite agrupar elementos do cluster do Kubernetes em um único aplicativo.

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.

Para criar um aplicativo personalizado, vá para a página aplicativos e clique em **Definir**.

À medida que você faz suas seleções, a janela aplicativo personalizado 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.

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.

Exemplo: Política de proteção separada para liberação canário

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 canário e outro para a versão estável. Isso mantém os backups, snapshots e operações de clone separados para os dois grupos de objetos Kubernetes.

Passos

1. Depois que a equipe adicionar o cluster ao Astra Control, a próxima etapa é definir um aplicativo personalizado. Para fazer isso, a equipe clica no botão **Definir** na página aplicativos.
2. Na janela pop-up exibida, a equipe define `devops-canary-deployment` como o nome do aplicativo. A equipe escolhe o cluster na lista suspensa **Cluster** e, em seguida, o namespace do aplicativo na lista suspensa **namespace**.
3. A equipe pode digitar `deployment=canary` no campo **rótulos** ou selecionar esse rótulo nos recursos listados abaixo.
4. Depois de definir o aplicativo personalizado para a implantação do canary, a equipe repete o processo para a implantação estável.

Quando a equipe terminar de criar os dois aplicativos personalizados, eles podem 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.

Proteja aplicativos

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 "A API Astra" 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
```

Snapshots e backups

Um *snapshot* é uma cópia pontual de um aplicativo que é armazenado no mesmo volume provisionado que o aplicativo. Eles geralmente são rápidos. Os instantâneos locais são usados para restaurar o aplicativo para um ponto no tempo anterior. 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. Uma cópia de segurança pode ser mais lenta em comparação com instantâneos locais. Você pode migrar um aplicativo restaurando seu backup para um cluster diferente. Você também pode escolher um período de retenção mais longo para backups.

> *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.

Configurar uma política de proteção

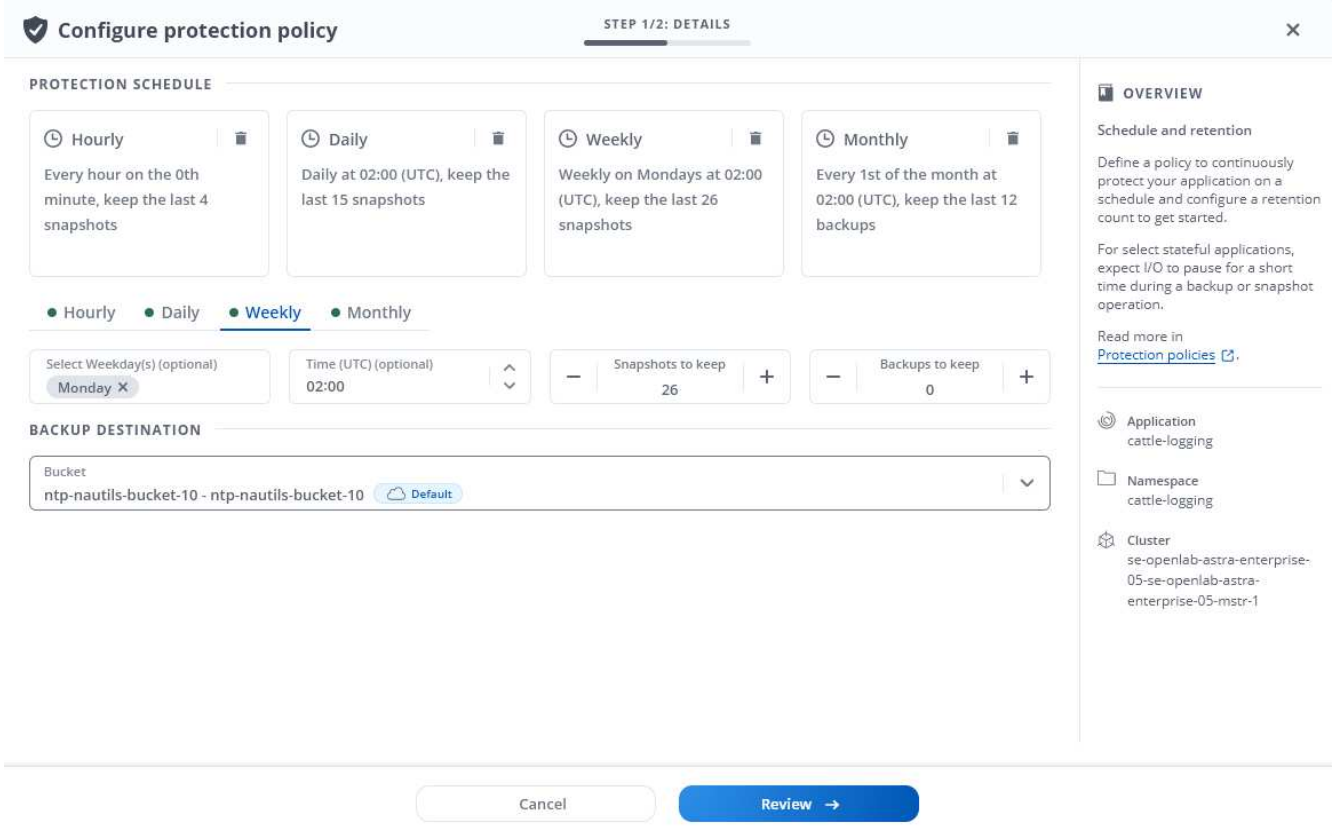
Uma política de proteção protege um aplicativo criando snapshots, backups ou ambos em um cronograma definido. Você pode optar por criar snapshots e backups por hora, diariamente, semanalmente e mensalmente, e especificar o número de cópias a reter.

Passos

1. Clique em **Apps** e, em seguida, clique no nome de um aplicativo.
2. Clique em **proteção de dados**.
3. Clique em **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. Clique em **Revisão**.
6. Clique em **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. Clique em **Apps**.
2. Clique na lista suspensa na coluna **ações** para o aplicativo desejado.
3. Clique em **Snapshot**.
4. Personalize o nome do instantâneo e, em seguida, clique em **Review**.
5. Reveja o resumo do instantâneo e clique em **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. Clique em **Apps**.
2. Clique na lista suspensa na coluna **ações** para o aplicativo desejado.
3. Clique em **Backup**.
4. Personalize o nome da cópia de segurança.
5. 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.
6. Escolha um destino para o backup selecionando na lista de buckets de armazenamento.
7. Clique em **Revisão**.
8. Revise o resumo do backup e clique em **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".

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. Clique em **Apps** e, em seguida, clique no nome de um aplicativo.
2. Clique em **proteção de dados**.

   Os instantâneos são apresentados por predefinição.

3. Clique em **backups** para ver a lista de backups.

Eliminar instantâneos

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

Passos

1. Clique em **Apps** e, em seguida, clique no nome de um aplicativo.
2. Clique em **proteção de dados**.
3. Clique na lista suspensa na coluna **ações** para o instantâneo desejado.
4. Clique em **Eliminar instantâneo**.
5. Digite a palavra "delete" para confirmar a exclusão e clique em **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".

1. Clique em **Apps** e, em seguida, clique no nome de um aplicativo.
2. Clique em **proteção de dados**.
3. Clique em **backups**.
4. Clique na lista suspensa na coluna **ações** para o backup desejado.
5. Clique em **Excluir backup**.
6. Digite a palavra "delete" para confirmar a exclusão e clique em **Yes, Delete backup**.

Resultado

O Astra Control Center exclui o backup.

Restaurar aplicações

O Astra Control Center pode restaurar sua aplicação a partir de um snapshot ou backup. Backups e snapshots de armazenamento persistentes são transferidos do seu armazenamento de objetos, portanto, a restauração de um snapshot existente para o mesmo cluster será mais rápida do que outros métodos. Você pode usar a IU do Astra ou "A API Astra" para restaurar 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.

> 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.

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. Clique em **Apps** e, em seguida, clique no nome de um aplicativo.
2. Clique em **proteção de dados**.
3. Se você quiser restaurar a partir de um instantâneo, mantenha o ícone **Snapshots** selecionado. Caso contrário, clique no ícone **backups** para restaurar a partir de um backup.
4. Clique na lista suspensa na coluna **ações** para o instantâneo ou backup a partir do qual você deseja restaurar.
5. Clique em **Restaurar aplicativo**.
6. **Restaurar detalhes**: Especifique detalhes para a restauração:
   - Introduza um nome e um namespace para a aplicação.

     Se você estiver restaurando um aplicativo que foi excluído, escolha um nome e um namespace diferentes para o aplicativo que o nome original. Se o nome do aplicativo restaurado for o mesmo que o aplicativo excluído, a operação de restauração falhará.

   - Escolha o cluster de destino para a aplicação.
   - Clique em **Revisão**.
7. **Restore Summary**: Revise os detalhes sobre a ação de restauração e clique em **Restore**.

Resultado

O Astra Control Center restaura a aplicação com base nas informações fornecidas.

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.

Clonar e migrar aplicações

Clone um aplicativo existente para criar um aplicativo duplicado no mesmo cluster do Kubernetes ou em outro cluster. 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 "A API Astra" clonar e migrar aplicações.

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 o Astra Control Center clones uma aplicação, ele cria um clone de sua configuração de aplicação e storage persistente.

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.

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
```

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.

Passos

1. Clique em **Apps**.
2. Execute um dos seguintes procedimentos:
   - Clique na lista suspensa na coluna **ações** para o aplicativo desejado.
   - Clique no nome do aplicativo desejado e selecione a lista suspensa status no canto superior direito da página.
3. Clique em **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. Clique em **Revisão**.
7. **Clone Summary**: Revise os detalhes sobre o clone e clique em **Clone**.

Resultado

O Astra Control Center clones essa aplicação com base nas informações fornecidas por você. A operação de

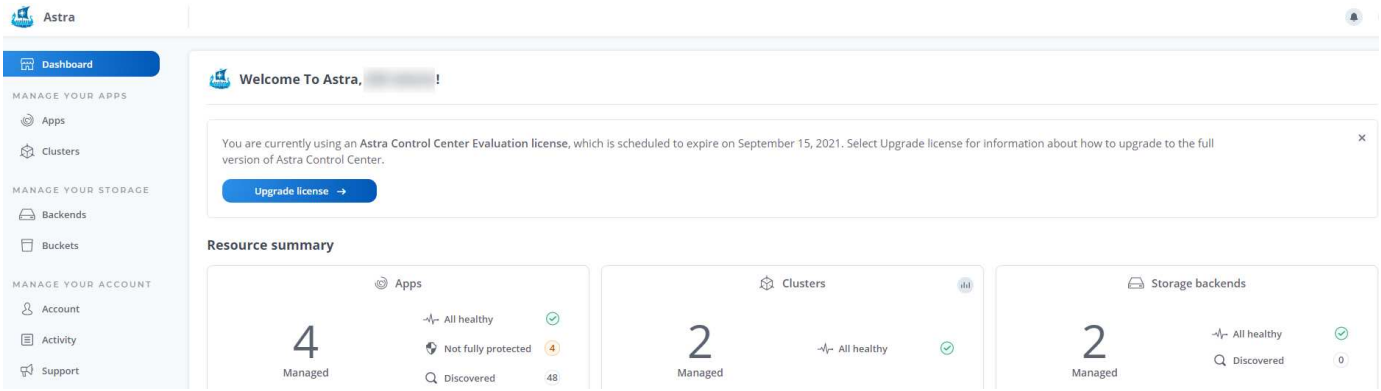
clone é bem-sucedida quando o novo clone de aplicativo está no `Available` estado na página **Apps**.

> 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.

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 cada um deles. 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 **Apps** ajuda 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.
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 **Apps** e, em seguida, selecione o nome de um aplicativo.
2. Clique ao redor para encontrar 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 **Apps** em **Resumo de recursos**, você pode selecionar os aplicativos gerenciados, que o levam à página **Apps**. Depois de chegar à página **Apps**, siga os passos descritos acima.

Gerencie sua conta

Gerenciar usuários

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

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**, clique em **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, mas não pode desgerenciar aplicativos ou clusters, nem excluir snapshots ou 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. Clique em **Add**.

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. Clique no ícone Usuário no canto superior direito da tela.
2. Selecione **Perfil**.
3. Clique na lista suspensa **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. Clique em **alterar senha**.

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**, clique em **conta**.
2. Na guia **usuários**, selecione a lista suspensa na coluna **Estado** para o usuário.
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, o usuário será solicitado a alterar a senha.

6. Clique em **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**, clique em **conta**.
2. Na guia **usuários**, selecione a lista suspensa na coluna **função** para o usuário.
3. Selecione uma nova função e clique em **alterar função** quando solicitado.

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**, clique em **conta**.
2. Na guia **usuários**, marque a caixa de seleção na linha de cada usuário que você deseja remover.
3. Clique em **ações** e selecione **Remover usuário(s)**.
4. Quando você for solicitado, confirme a exclusão digitando a palavra "remover" e clique em **Sim, Remover usuário**.

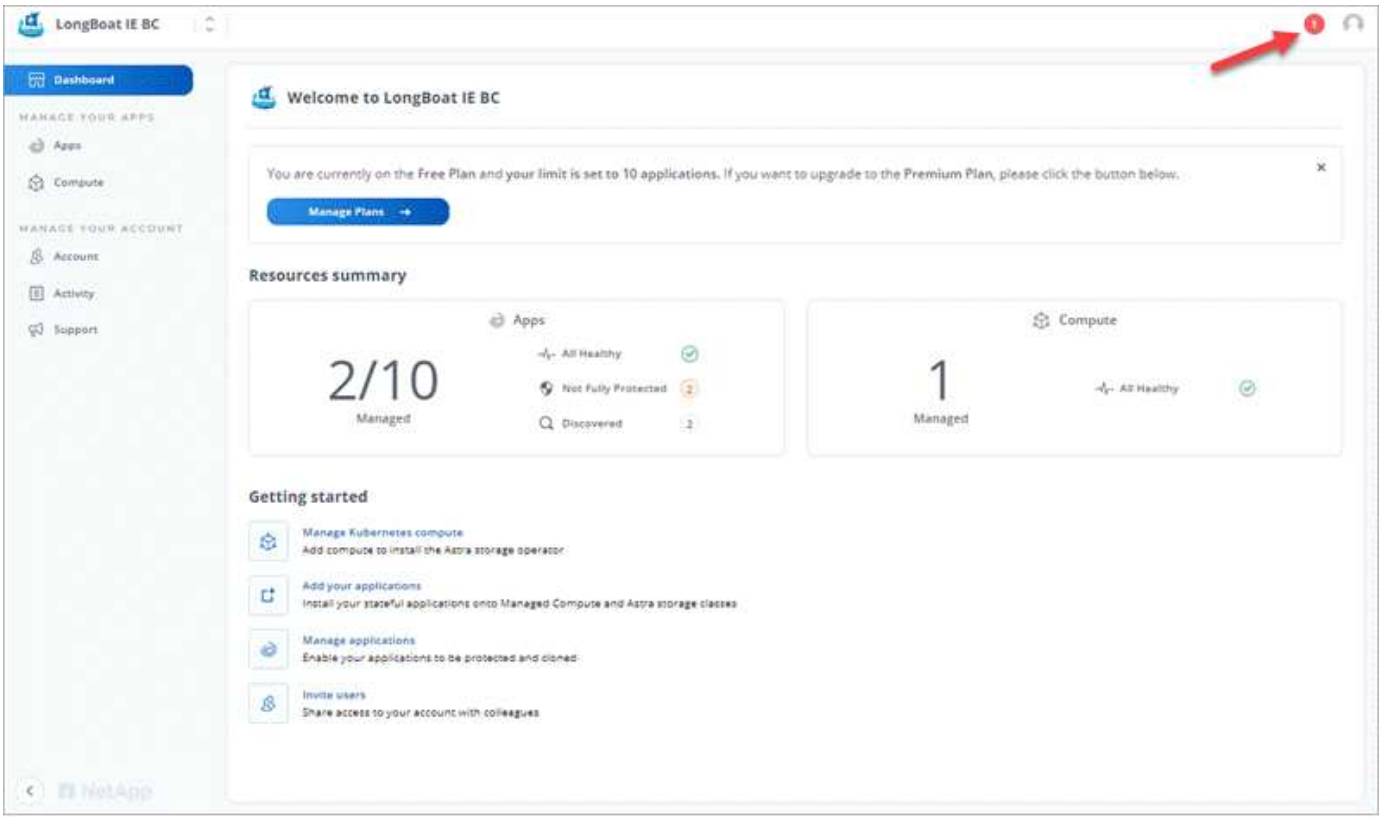
Resultado

O Astra Control Center remove o usuário da conta.

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.

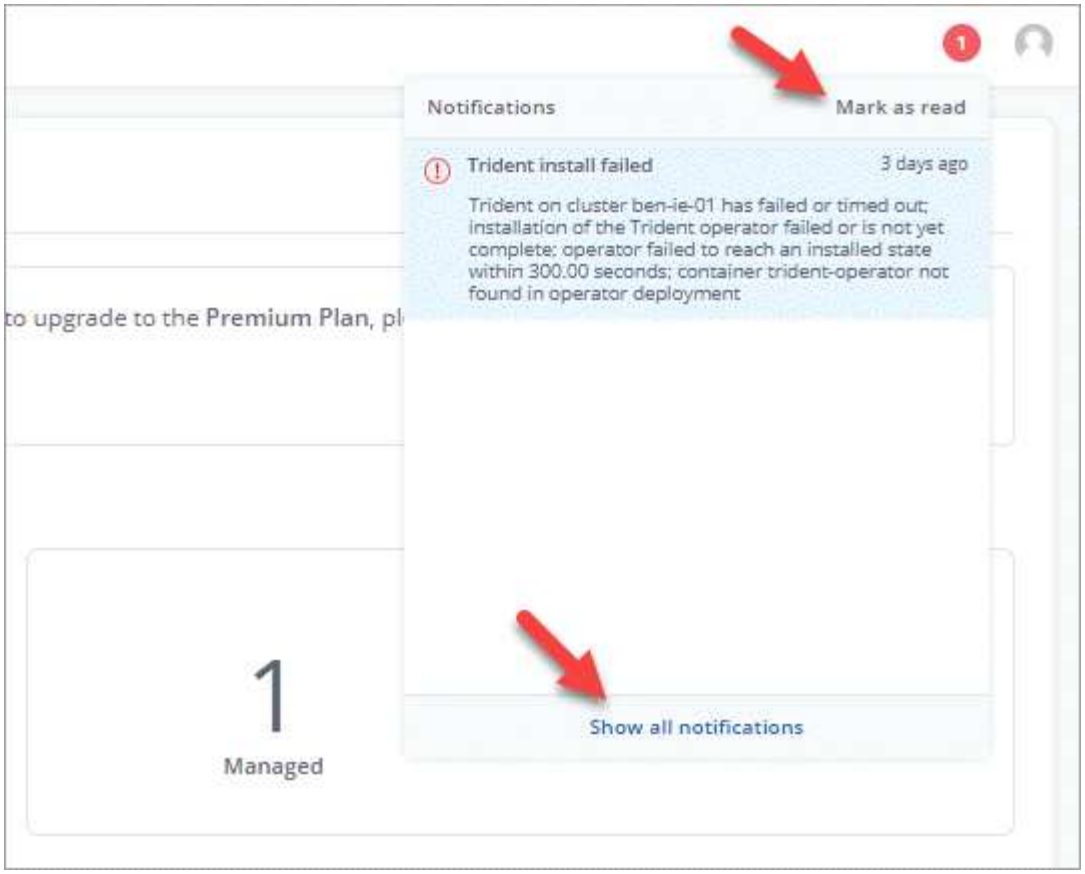
O número de notificações não lidas está disponível no canto superior direito da interface:



Você pode ver essas notificações e marcá-las como lidas (isso pode ser útil se você quiser limpar notificações não lidas como nós).

Passos

1. Clique no número de notificações não lidas no canto superior direito.



2. Revise as notificações e clique em **Marcar como lidas** ou **Mostrar todas as notificações**.

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

3. Na página **notificações**, visualize as notificações, selecione as que deseja marcar como lidas, clique em **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.

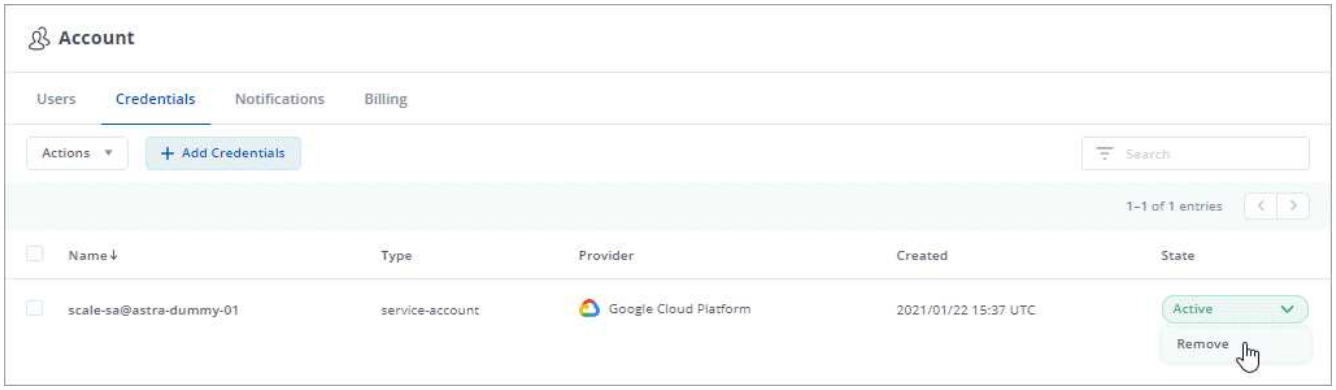
Remover credenciais

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. Clique em **conta > credenciais**.
2. Clique na lista suspensa na coluna **Estado** para obter as credenciais que deseja remover.
3. Clique em **Remover**.



4. Digite a palavra "remove" para confirmar a exclusão e clique em **Yes, Remove Credential**.

Resultado

O Astra Control Center remove as credenciais da conta.

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 "A API Astra" atualizar uma licença existente.

Passos

1. Faça login 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**, clique no 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.

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 qualquer um dos seguintes provedores de bucket:

- 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.

Você não pode excluir um bucket; no entanto, você pode editá-lo.

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, 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

> 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.

Remover credenciais

Remova as credenciais do S3 de uma conta a qualquer momento usando a API Astra Control.

Para obter detalhes, "Use a API Astra Control" consulte .

> 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. É melhor não remover essas credenciais.

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 adicionar um bucket, selecione o tipo correto de provedor de bucket com credenciais corretas para esse provedor. Por exemplo, a IU aceita o NetApp ONTAP S3 como o tipo com 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 **baldes**.
2. No menu 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**.

Encontre mais informações

- "Use a API Astra"

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, 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

Veja os detalhes do back-end de armazenamento

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

Veja os detalhes do back-end do storage no Dashboard

Passos

1. Na navegação à esquerda, selecione **Dashboard**.
2. Revise 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

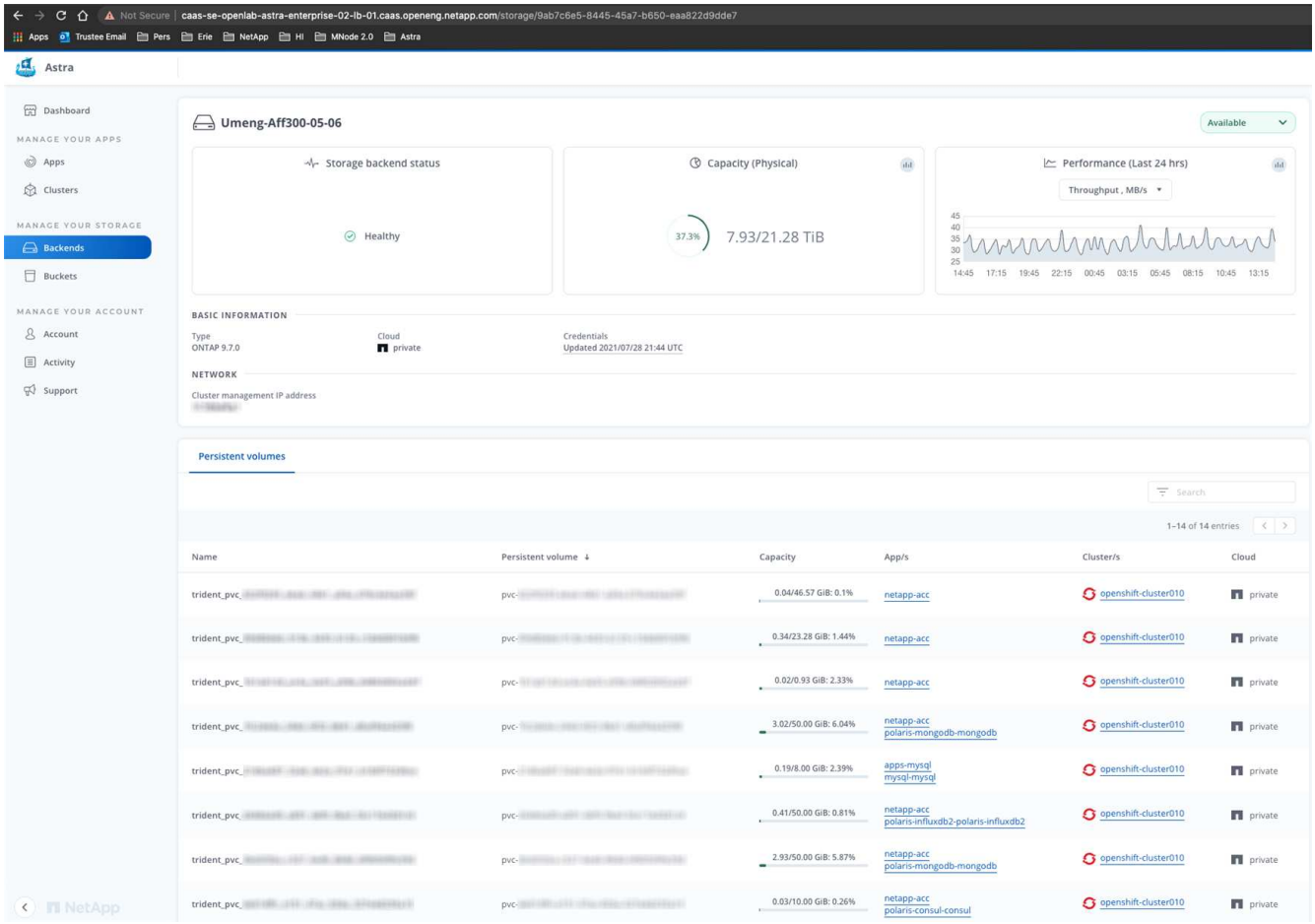
Veja informações sobre a integridade, a capacidade e a performance do back-end (taxa de transferência de IOPS e/ou latência).

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, clique no 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 armazenamento de back-end.
3. No menu ações, selecione **Unmanage**.
4. Digite "Unmanage" para confirmar a remoção.
5. Selecione **Sim, remova o back-end de armazenamento**.

Encontre mais informações

- "Use a API Astra"

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.

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 daqui.

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

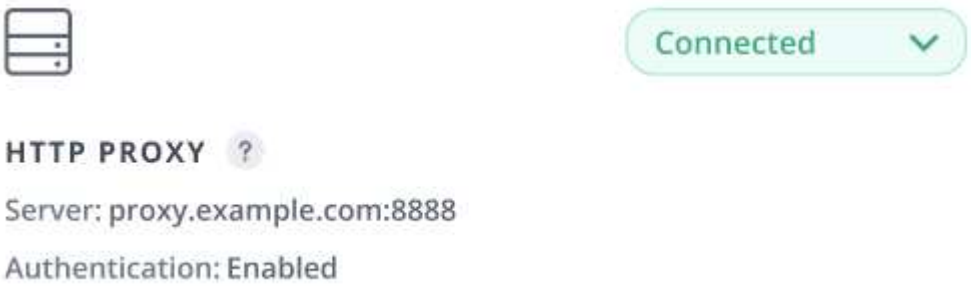
1. Faça login no Astra Control Center usando uma conta com privilégio **admin**/**owner**.
2. Selecione **conta** > **conexões**.
3. Selecione **Connect** na lista suspensa para adicionar um servidor proxy.

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.

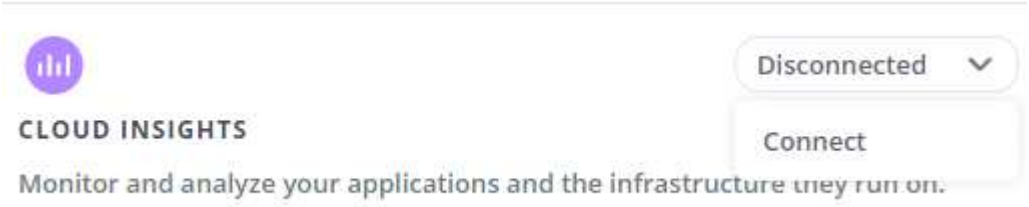
O que você vai precisar

- 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 "aqui".

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.

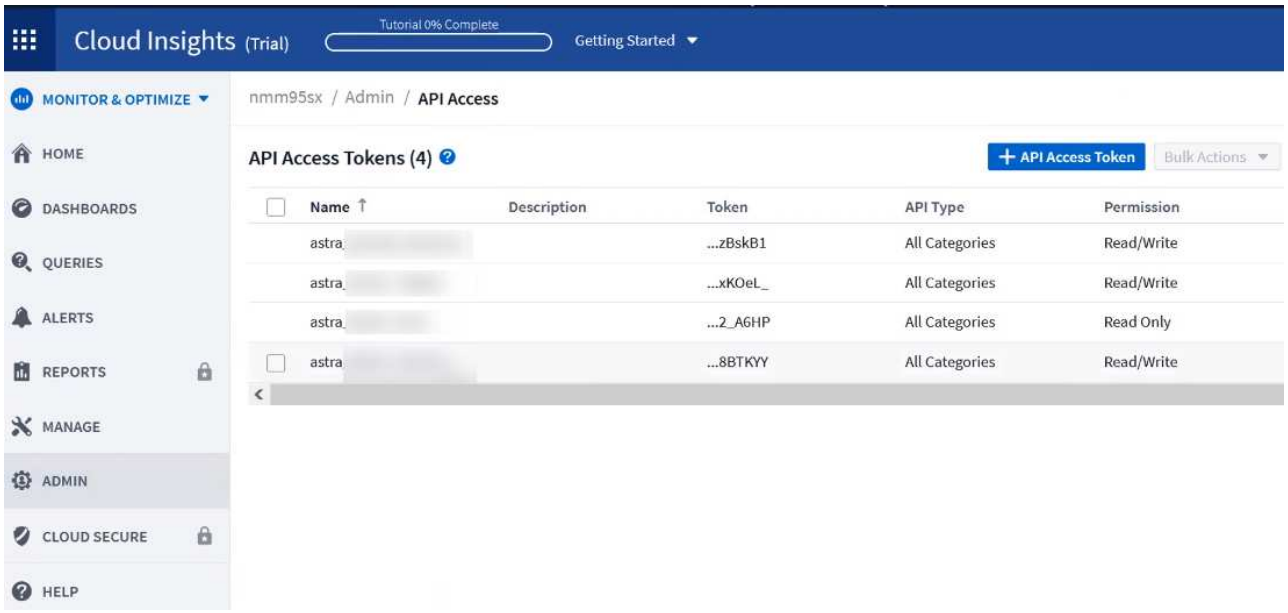


4. Insira os tokens da API do Cloud Insights e o URL do locatário. A URL do locatário tem o seguinte formato, como exemplo:

```
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 API do tipo **somente leitura**.



c. Copie a tecla **somente leitura**. Você precisará colá-lo na janela Centro de Controle Astra para ativar a conexão Cloud Insights.

d. No Cloud Insights, gere um token de API do tipo **Read/Write**.

e. Copie a tecla **Read/Write**. Você precisará colá-lo na janela do Centro de Controle Astra **Connect Cloud Insights**.

> 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.

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

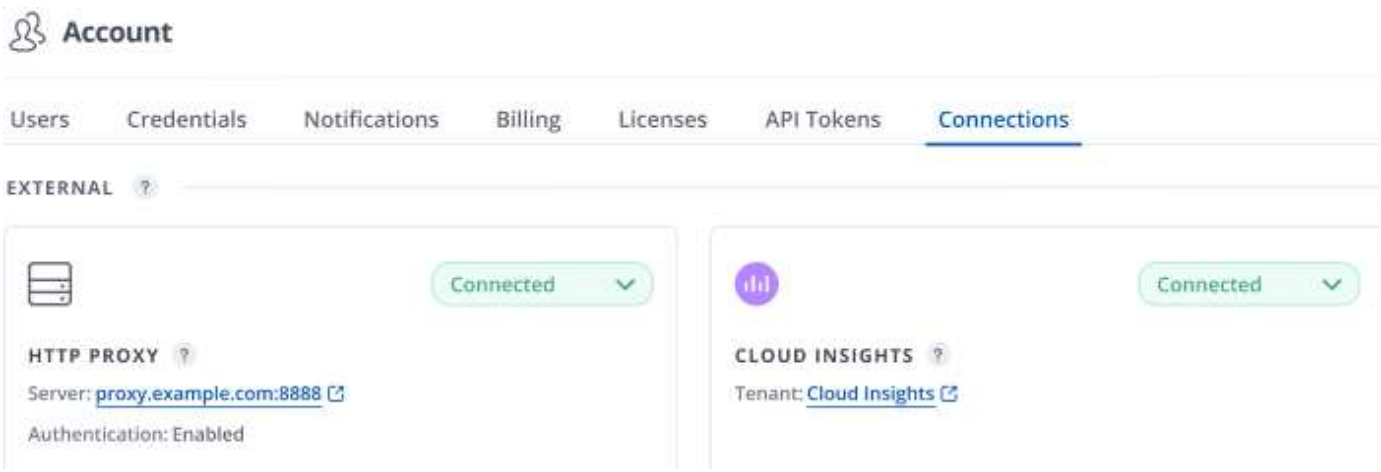
5. Selecione **Connect**.

> 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**.

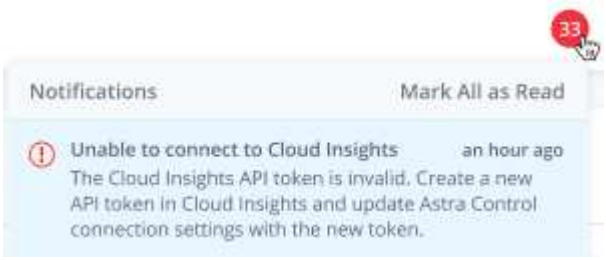
> Para ir e voltar facilmente entre o Centro de Controle Astra e as UIs do Cloud Insights, certifique-se de que você esteja conetado a ambos.

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.

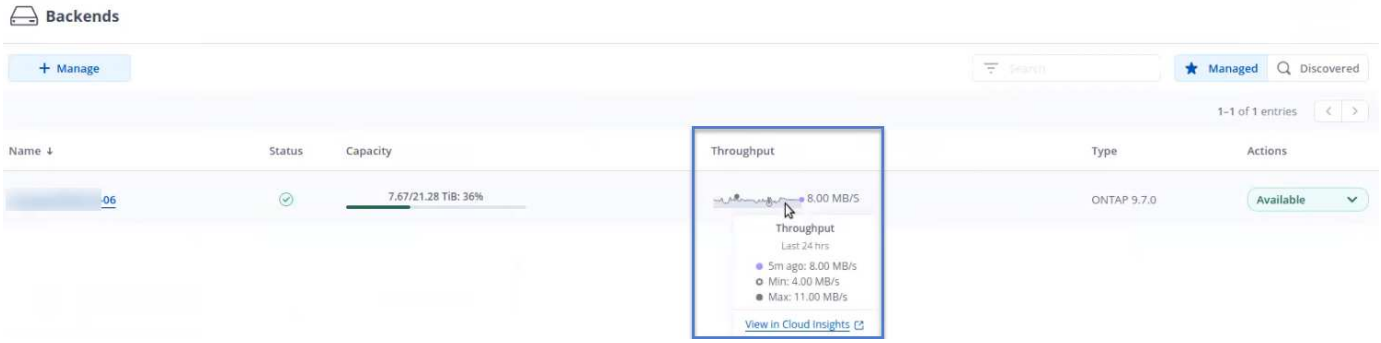


Se a conexão falhou por algum motivo, o status mostra **Failed**. Você pode encontrar o motivo da falha em **notificações** no lado superior direito da interface do usuário.



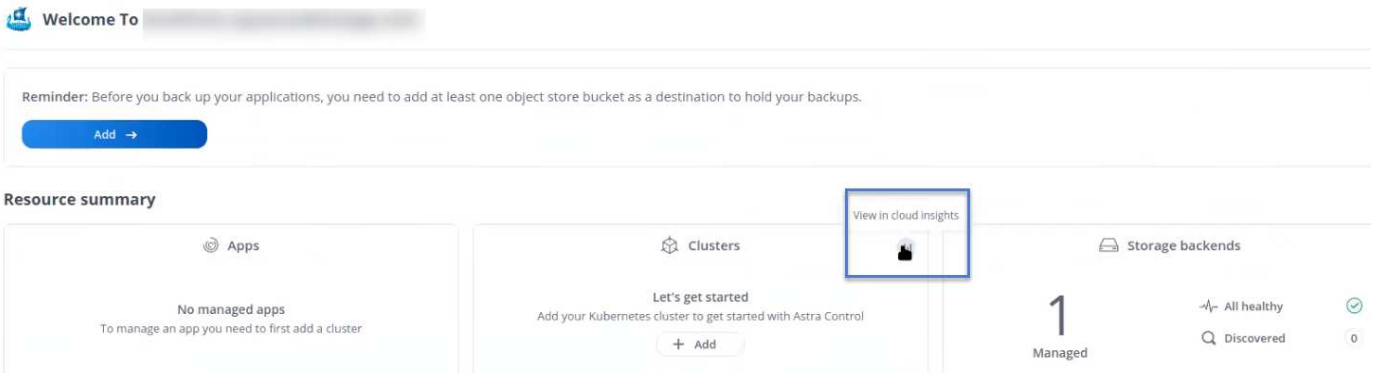
Você também pode encontrar as mesmas informações em **conta** > **notificações**.

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

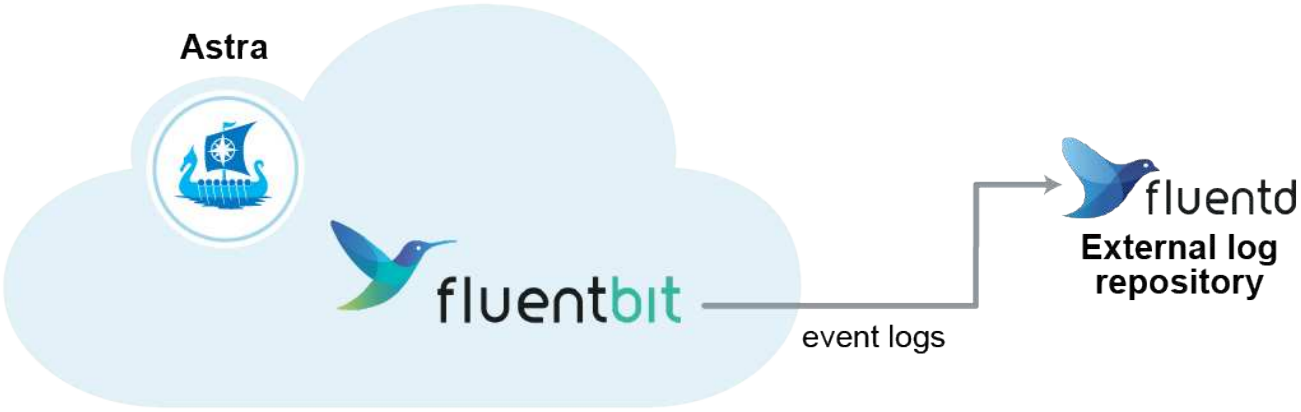
Você pode desativar a conexão Cloud Insights para um cluster Kubernetes gerenciado pelo Astra Control Center. A desativação da conexão Cloud Insights não exclui os dados de telemetria já carregados no Cloud Insights.

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.

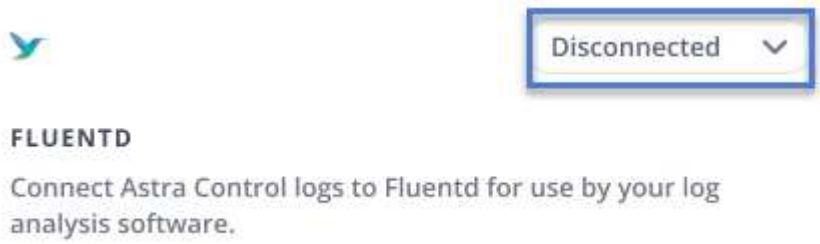
O que você vai precisar

- 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.

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 "A API Astra" atualizar uma licença existente.

Passos

1. Faça login 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**, clique no 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.

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 **Apps**.
2. Selecione a caixa de verificação para as aplicações que já não pretende gerir.
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 **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`

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.

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
```

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.

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

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> --namespace <namespace> --create-namespace --set
persistence.storageClass=<storage_class>
```

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.

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

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> --namespace <namespace> --create-namespace --set
persistence.storageClass=<storage_class>
```

> 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.

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

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> --namespace <namespace> --create-namespace --set
   persistence.storageClass=<storage_class>
   ```

   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.

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

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> --namespace <namespace> --create-namespace --set
persistence.storageClass=<storage_class>
```

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

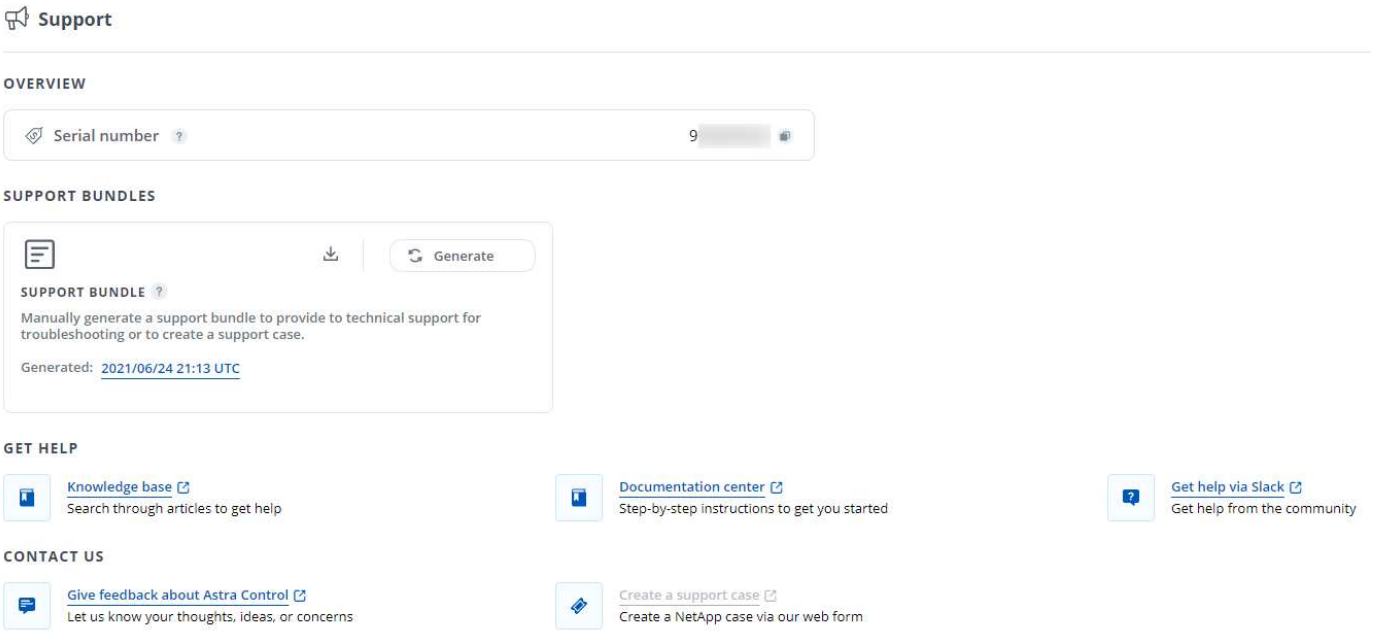
Obtenha ajuda

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.

Você pode acessar as opções de suporte na IU do Astra Control Center selecionando a guia **Support** no menu principal.



Opções de auto-suporte

Estas opções estão disponíveis gratuitamente 24x7:

- "Base de conhecimento (login necessário)"

  PESQUISE artigos, perguntas frequentes ou informações sobre Break Fix relacionadas ao Astra Control.

- Documentação

  Este é o site de documentação que você está vendo atualmente.

- "Folga"

  Vá para o canal Containers no espaço de trabalho thePub para se conetar com colegas e especialistas.

- Gere pacotes de suporte para fornecer ao suporte da NetApp para solução de problemas
- E-mail de feedback

  Envie um e-mail para NetApp.com para nos informar sobre 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 de definição de recursos personalizados (CRD) do Astra Control Center (`astra_control_center_min.yaml`, os pacotes de suporte diários serão automaticamente carregados no 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. Verifique o **carregue o pacote para o site de suporte da NetApp quando gerado**.

e. Selecione **Generate Bundle**.

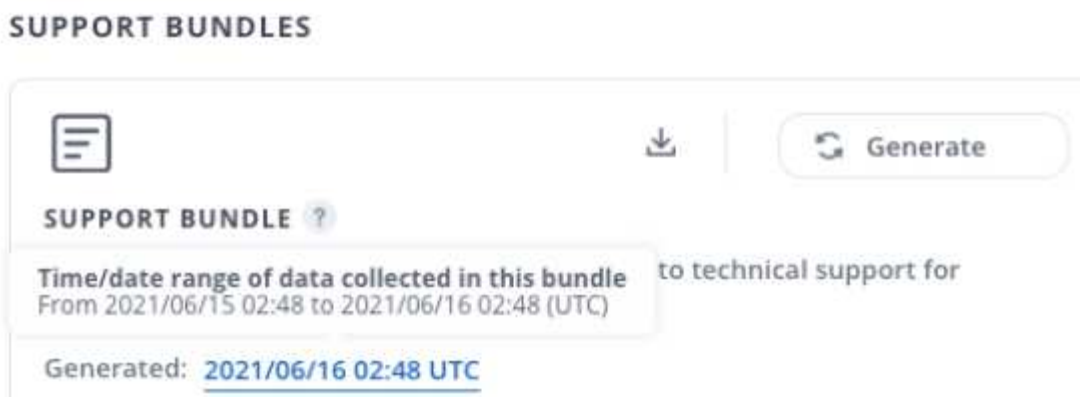
Quando o pacote de suporte estiver pronto, uma notificação aparece na página **Contas** > **notificação** na área Alertas, na página **atividade** e também na lista de notificações (acessível selecionando o ícone no lado superior direito da interface do usuário).

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, ele aparece ao lado de **Generated** na seção **Support Bundles** da página **Support**, conforme mostrado:



1. Selecione o ícone **Download** para fazer o download do 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 NetApp AIQ.

Encontre mais informações

- "Como carregar um arquivo para o NetApp (login necessário)"
- "Como fazer upload manual de um arquivo para o NetApp (login necessário)"

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 a versão Astra Control Center 21,08"

Licença de API Astra Control

https://docs.netapp.com/us-en/astra-automation-2108/media/astra-api-license.pdf

Informações sobre direitos autorais

Informações sobre marcas comerciais