



Documentação do Astra Control Center 23,04

Astra Control Center

NetApp
October 23, 2024

Índice

Documentação do Astra Control Center 23,04	1
Notas de lançamento	2
Novidades nesta versão do Astra Control Center	2
Problemas conhecidos	5
Limitações conhecidas	9
Comece agora	14
Saiba mais sobre o Astra Control	14
Requisitos do Astra Control Center	17
Início rápido para Astra Control Center	22
Visão geral da instalação	23
Configure o Astra Control Center	90
Perguntas mais frequentes para o Astra Control Center	110
Conceitos	113
Arquitetura e componentes	113
Proteção de dados	114
Licenciamento	117
Gerenciamento de aplicativos	118
Classes de armazenamento e tamanho de volume persistente	121
Funções de usuário e namespaces	121
Segurança do pod	122
Use o Astra Control Center	125
Comece a gerenciar aplicativos	125
Proteja aplicativos	130
Monitorar a integridade do aplicativo e do cluster	158
Gerencie sua conta	161
Gerenciar buckets	171
Gerenciar o back-end de storage	174
Monitorar tarefas em execução	177
Monitore a infraestrutura com conexões Cloud Insights, Prometheus ou Fluentd	178
Desgerenciar aplicativos e clusters	187
Atualizar o Astra Control Center	188
Desinstale o Astra Control Center	197
Automatize com a API REST do Astra Control	201
Automação com a API REST do Astra Control	201
Conhecimento e apoio	202
Solução de problemas	202
Obtenha ajuda	202
Versões anteriores da documentação do Astra Control Center	205
Avisos legais	206
Direitos de autor	206
Marcas comerciais	206
Patentes	206
Política de privacidade	206

Código aberto	206
Licença de API Astra Control	206

Documentação do Astra Control Center 23,04

Notas de lançamento

Temos o prazer de anunciar a última versão 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.

Novidades nesta versão do Astra Control Center

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

18 de maio de 2023 (23.04.2)

Esta versão de patch (23.04.2) para Astra Control Center (23.04.0) fornece suporte ["Snapshotter externo do Kubernetes v6, 1.0"](#) e corrige o seguinte:

- Um bug com restauração de aplicativos no local ao usar ganchos de execução
- Problemas de conexão com o serviço do balde

25 de abril de 2023 (23.04.0)

Novos recursos e suporte

- ["Licença de avaliação de 90 dias habilitada por padrão para novas instalações do Astra Control Center"](#)
- ["Funcionalidade aprimorada de ganchos de execução com opções de filtragem adicionais"](#)
- ["Agora, os ganchos de execução podem ser executados após failover de replicação com o Astra Control Center"](#)
- ["Suporte para migrar volumes da classe 'ONTAP-nas-economy storage' para a classe de armazenamento 'ONTAP-nas'"](#)
- ["Suporte para incluir ou excluir recursos de aplicativos durante operações de restauração"](#)
- ["Suporte para gerenciamento de aplicações somente de dados"](#)

Problemas e limitações conhecidos

- ["Problemas conhecidos para esta versão"](#)
- ["Limitações conhecidas para esta versão"](#)

22 de novembro de 2022 (22.11.0)

Detalhes

Novos recursos e suporte

- ["Suporte para aplicações que abrangem vários namespaces"](#)
- ["Suporte para incluir recursos de cluster em uma definição de aplicativo"](#)
- ["Autenticação LDAP aprimorada com integração com controle de acesso baseado em função \(RBAC\)"](#)
- ["Adicionado suporte para Kubernetes 1,25 e admissão de segurança de Pod \(PSA\)"](#)
- ["Relatórios de progresso aprimorados para suas operações de backup, restauração e clone"](#)

Problemas e limitações conhecidos

- ["Problemas conhecidos para esta versão"](#)
- ["Limitações conhecidas para esta versão"](#)

8 de setembro de 2022 (22.08.1)

Detalhes

Esta versão de patch (22.08.1) para o Centro de Controle Astra (22.08.0) corrige pequenos bugs na replicação de aplicativos usando o NetApp SnapMirror.

10 de agosto de 2022 (22.08.0)

Detalhes

Novos recursos e suporte

- ["Replicação de aplicativos usando a tecnologia NetApp SnapMirror"](#)
- ["Fluxo de trabalho de gerenciamento de aplicativos aprimorado"](#)
- ["Funcionalidade aprimorada de ganchos de execução provide-your-own"](#)



O NetApp forneceu ganchos de execução pré e pós-snapshot padrão para aplicativos específicos foram removidos nesta versão. Se você atualizar para esta versão e não fornecer seus próprios ganchos de execução para snapshots, o Astra Control tirará somente snapshots consistentes com falhas. Visite o ["NetApp Verda"](#) repositório do GitHub para scripts de gancho de execução de exemplo que você pode modificar para se adequar ao seu ambiente.

- ["Suporte para o VMware Tanzu Kubernetes Grid Integrated Edition \(TKGI\)"](#)
- ["Suporte para Google Anthos"](#)
- ["Configuração LDAP \(via API Astra Control\)"](#)

Problemas e limitações conhecidos

- ["Problemas conhecidos para esta versão"](#)
- ["Limitações conhecidas para esta versão"](#)

26 de abril de 2022 (22.04.0)

Detalhes

Novos recursos e suporte

- ["Controles de acesso baseados em função do namespace \(RBAC\)"](#)
- ["Suporte para Cloud Volumes ONTAP"](#)
- ["Capacitação genérica de ingresso para Astra Control Center"](#)
- ["Remoção do balde do Astra Control"](#)
- ["Suporte ao portfólio VMware Tanzu"](#)

Problemas e limitações conhecidos

- ["Problemas conhecidos para esta versão"](#)
- ["Limitações conhecidas para esta versão"](#)

14 de dezembro de 2021 (21,12)

Detalhes

Novos recursos e suporte

- ["Restauração de aplicativo"](#)
- ["Ganchos de execução"](#)
- ["Suporte para aplicativos implantados com operadores com escopo de namespace"](#)
- ["Suporte adicional para Kubernetes e Rancher upstream"](#)
- ["Atualizações do Astra Control Center"](#)
- ["Opção Red Hat OperatorHub para instalação"](#)

Problemas resolvidos

- ["Problemas resolvidos para esta versão"](#)

Problemas e limitações conhecidos

- ["Problemas conhecidos para esta versão"](#)
- ["Limitações conhecidas para esta versão"](#)

5 de agosto de 2021 (21,08)

Detalhes

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"](#)
- ["Versões anteriores da documentação do Astra Control Center"](#)

Problemas conhecidos

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

Os seguintes problemas conhecidos afetam a versão atual:

Aplicações

- [A restauração de um aplicativo resulta em tamanho PV maior do que o PV original](#)
- [Os clones de aplicativos falham usando uma versão específica do PostgreSQL](#)
- [Os clones do aplicativo falham ao usar as restrições de contexto de segurança do OCP \(SCC\) no nível da conta de serviço](#)
- [Os clones do aplicativo falham após a implantação de uma aplicação com uma classe de storage definida](#)
- [Backups e snapshots de aplicativos falharão se a volumessnapshotclass for adicionada após o gerenciamento de um cluster](#)

Clusters

- [O gerenciamento de um cluster com Astra Control Center falha quando o arquivo kubeconfig padrão contém mais de um contexto](#)
- [04](#)
- [04 para 23.04.2](#)
- [Um pod de monitoramento pode falhar em ambientes do Istio](#)

Outras questões

- [Os clusters gerenciados não aparecem no NetApp Cloud Insights ao se conectar por meio de um proxy](#)

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

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

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

Os clones de aplicativos falham usando uma versão específica do PostgreSQL

Clones de aplicativos dentro do mesmo cluster falham consistentemente com o gráfico Bitnami PostgreSQL 11.5.0. Para clonar com sucesso, use uma versão anterior ou posterior do gráfico.

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

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

Backups e snapshots de aplicativos falharão se a `volumesnapshotclass` for adicionada após o gerenciamento de um cluster

Backups e snapshots falham `UI 500 error` nesse cenário. Como solução alternativa, atualize a lista de aplicativos.

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

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

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

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

Alguns pods não conseguem iniciar após a atualização para o Astra Control Center 23,04

Depois de atualizar para o Astra Control Center 23,04, alguns pods podem não ser iniciados. Como solução alternativa, reinicie manualmente os pods afetados usando as seguintes etapas:

1. Localize os pods afetados, substituindo o `<namespace>` pelo namespace atual:

```
kubectl get pods -n <namespace> | grep au-pod
```

Os pods afetados terão resultados semelhantes aos seguintes:

```
pcloud-astra-control-center-au-pod-0 0/1 CreateContainerConfigError 0  
13s
```

2. Reinicie cada pod afetado, substituindo o <namespace> pelo namespace atual:

```
kubectl delete pod pcloud-astra-control-center-au-pod-0 -n <namespace>
```

Alguns pods mostram um estado de erro após o estágio de limpeza da atualização de 23.04 para 23.04.2

Depois de atualizar para o Astra Control Center 23.04.2, alguns pods podem mostrar um erro nos logs relacionados `task-service-task-purge` ao :

```
kubectl get all -n netapp-acc -o wide|grep purge  
  
pod/task-service-task-purge-28282828-ab1cd      0/1      Error      0  
48m      10.111.0.111      openshift-clstr-ol-07-zwlj8-worker-jhp2b      <none>  
<none>
```

Este estado de erro significa que uma etapa de limpeza não foi executada corretamente. A atualização geral para o 23.04.2 é bem-sucedida. Execute o seguinte comando para limpar a tarefa e remover o estado de erro:

```
kubectl delete job task-service-task-purge-[system-generated task ID] -n  
<netapp-acc or custom namespace>
```

Um pod de monitoramento pode falhar em ambientes do Istio

Se você emparelhar o Astra Control Center com o Cloud Insights em um ambiente Istio, o `telegraf-rs` pod poderá falhar. Como solução alternativa, execute as seguintes etapas:

1. Encontre o pod avariado:

```
kubectl -n netapp-monitoring get pod | grep Error
```

Você deve ver saída semelhante ao seguinte:

```
NAME READY STATUS RESTARTS AGE
telegraf-rs-fhhrh 1/2 Error 2 (26s ago) 32s
```

2. Reinicie o pod avariado, substituindo <pod_name_from_output> pelo nome do pod afetado:

```
kubectl -n netapp-monitoring delete pod <pod_name_from_output>
```

Você deve ver saída semelhante ao seguinte:

```
pod "telegraf-rs-fhhrh" deleted
```

3. Verifique se o pod foi reiniciado e não está em um estado de erro:

```
kubectl -n netapp-monitoring get pod
```

Você deve ver saída semelhante ao seguinte:

```
NAME READY STATUS RESTARTS AGE
telegraf-rs-rrnsb 2/2 Running 0 11s
```

Os clusters gerenciados não aparecem no NetApp Cloud Insights ao se conectar por meio de um proxy

Quando o Astra Control Center se conecta ao NetApp Cloud Insights por meio de um proxy, os clusters gerenciados podem não aparecer no Cloud Insights. Como solução alternativa, execute os seguintes comandos em cada cluster gerenciado:

```
kubectl get cm telegraf-conf -o yaml -n netapp-monitoring | sed
'/\[\[outputs.http\]\]/c\ \[\[outputs.http\]\n\ use_system_proxy =
true' | kubectl replace -f -
```

```
kubectl get cm telegraf-conf-rs -o yaml -n netapp-monitoring | sed
'/\[\[outputs.http\]\]/c\ \[\[outputs.http\]\n\ use_system_proxy =
true' | kubectl replace -f -
```

```
kubectl get pods -n netapp-monitoring --no-headers=true | grep 'telegraf-
ds\|telegraf-rs' | awk '{print $1}' | xargs kubectl delete -n netapp-
monitoring pod
```

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

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

Encontre mais informações

- ["Limitações conhecidas"](#)

Limitações conhecidas

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

Limitações do gerenciamento de clusters

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

Limitações de controle de acesso baseado em função (RBAC)

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

Limitações de gerenciamento de aplicativos

- [Vários aplicativos em um único namespace não podem ser restaurados coletivamente para um namespace diferente](#)
- [O Astra Control não é compatível com aplicações que usam várias classes de storage por namespace](#)
- [O Astra Control não atribui automaticamente buckets padrão nas instâncias da nuvem](#)
- [Clones de aplicativos instalados usando operadores pass-by-referência podem falhar](#)
- [As operações de restauração no local de aplicativos que usam um gerenciador de certificados não são suportadas](#)
- [O operador habilitado para OLM e com escopo de cluster implantaram aplicativos não suportados](#)
- [As aplicações implementadas com o Helm 2 não são suportadas](#)

Limitações gerais

- [Os buckets do S3 no Astra Control Center não relatam a capacidade disponível](#)
- [O Astra Control Center não valida os detalhes inseridos para o servidor proxy](#)
- [As conexões existentes com um pod Postgres causam falhas](#)
- [Backups e snapshots podem não ser retidos durante a remoção de uma instância do Astra Control Center](#)
- [Limitações de usuário e grupo LDAP](#)
- [A página atividade exibe até 100000 eventos](#)
- [25 ou em clusters posteriores com certas versões de controladora de snapshot](#)

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

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

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

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

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

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

Como solução alternativa, faça o seguinte:

1. Edite seu kubeadm-config ConfigMap:

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

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

```
apiVersion: v1
clusters:
- cluster:
  certificate-authority-data:
  ExAmPLERb2tCcJZ5K3E2Njk4eQotLExAMpLEORCBDRVJUSUZJQ0FURS0txxxxXX==
  server: https://x.x.x.x:6443
  name: xyz-cluster
contexts:
- context:
  cluster: xyz-cluster
  namespace: default
  user: kubernetes-admin
  name: kubernetes-admin@kubernetes
current-context: kubernetes-admin@kubernetes
```

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

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

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

Qualquer `member` usuário com restrições RBAC por nome/ID de namespace pode clonar ou restaurar um aplicativo para um novo namespace no mesmo cluster ou para qualquer outro cluster na conta da organização. No entanto, o mesmo usuário não pode acessar o aplicativo clonado ou restaurado no novo namespace. Depois que um novo namespace é criado por uma operação de clone ou restauração, o administrador/proprietário da conta pode editar a `member` conta de usuário e atualizar as restrições de função para o usuário afetado conceder acesso ao novo namespace.

Vários aplicativos em um único namespace não podem ser restaurados coletivamente para um namespace diferente

Se você gerenciar várias aplicações em um único namespace (criando várias definições de aplicações no Astra Control), não poderá restaurar todas as aplicações para um namespace único diferente. Você precisa restaurar cada aplicativo para seu próprio namespace separado.

O Astra Control não é compatível com aplicações que usam várias classes de storage por namespace

O Astra Control é compatível com aplicações que usam uma única classe de storage por namespace. Ao adicionar um aplicativo a um namespace, verifique se o aplicativo tem a mesma classe de armazenamento que outros aplicativos no namespace.

O Astra Control não atribui automaticamente buckets padrão nas instâncias da nuvem

O Astra Control não atribui automaticamente um bucket padrão a nenhuma instância de nuvem. Você precisa definir manualmente um intervalo padrão para uma instância de nuvem. Se um bucket padrão não estiver definido, você não poderá executar operações de clone de aplicativo entre dois clusters.

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

O Astra Control é compatível com aplicativos instalados com operadores com escopo de namespace. Esses operadores são geralmente projetados com uma arquitetura "pass-by-value" em vez de "pass-by-reference". A seguir estão alguns aplicativos de operador que seguem estes padrões:

- ["Apache K8ssandra"](#)



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

- ["Jenkins CI"](#)
- ["Cluster Percona XtraDB"](#)

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



Durante as operações de clone, os aplicativos que precisam de um recurso do IngressClass ou webhooks para funcionar corretamente não devem ter esses recursos já definidos no cluster de destino.

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

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

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

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

As aplicações implementadas com o Helm 2 não são suportadas

Se você usar o Helm para implantar aplicativos, o Astra Control Center precisará do Helm versão 3. O gerenciamento e clonagem de aplicativos implantados com o Helm 3 (ou atualizados do Helm 2 para o Helm 3) é totalmente compatível. Para obter mais informações, ["Requisitos do Astra Control Center"](#) consulte .

Os buckets do S3 no Astra Control Center não relatam a capacidade disponível

Antes de fazer backup ou clonar aplicativos gerenciados pelo Astra Control Center, verifique as informações do bucket no sistema de gerenciamento ONTAP ou StorageGRID.

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

Certifique-se de que você ["introduza os valores corretos"](#) ao estabelecer uma conexão.

As conexões existentes com um pod Postgres causam falhas

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

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

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

Limitações de usuário e grupo LDAP

O Astra Control Center é compatível com até 5.000 grupos remotos e 10.000 usuários remotos.

A página atividade exibe até 100000 eventos

A página atividade do Astra Control pode exibir até 100.000 eventos. Para ver todos os eventos registrados, recupere os eventos utilizando o ["API REST do Astra Control"](#).

Os snapshots podem falhar no Kubernetes 1,25 ou em clusters posteriores com certas versões de controladora de snapshot

Os snapshots para clusters do Kubernetes que executam a versão 1,25 ou posterior podem falhar se a versão v1beta1 das APIs do controlador de snapshot estiver instalada no cluster.

Como solução alternativa, faça o seguinte ao atualizar instalações existentes do Kubernetes 1,25 ou posteriores:

1. Remova quaisquer CRDs de Snapshot existentes e qualquer controladora de snapshot existente.
2. ["Desinstale o Astra Trident"](#).
3. ["Instale as CRDs de snapshot e o controlador de snapshot"](#).
4. ["Instale a versão mais recente do Astra Trident"](#).
5. ["Crie um VolumeSnapshotClass"](#).

Encontre mais informações

- ["Problemas conhecidos"](#)

Comece agora

Saiba mais sobre o Astra Control

O Astra Control é uma solução de gerenciamento de ciclo de vida de dados de aplicações Kubernetes que simplifica as operações de aplicações com estado monitorado. Proteja, faça backup, replique 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
- Replique aplicações para um sistema remoto usando a tecnologia NetApp SnapMirror (Astra Control Center)
- Clonar aplicações da preparação para a produção
- Visualize a integridade e o status de proteção da aplicação
- Trabalhe com uma IU da Web ou uma API para implementar seus fluxos de trabalho de backup e migração

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

	Astra Control Service	Astra Control Center
Como é oferecido?	Como um serviço de nuvem totalmente gerenciado da NetApp	Como software que você pode baixar, instalar e gerenciar
Onde está hospedado?	Em uma nuvem pública de escolha da NetApp	No seu próprio cluster Kubernetes
Como é atualizado?	Gerenciado por NetApp	Você gerencia quaisquer atualizações

	Astra Control Service	Astra Control Center
Quais são os backends de armazenamento suportados?	<ul style="list-style-type: none"> • Amazon Web Services: <ul style="list-style-type: none"> ◦ Amazon EBS ◦ Amazon FSX para NetApp ONTAP ◦ "Cloud Volumes ONTAP" • Google Cloud: <ul style="list-style-type: none"> ◦ Persistent Disk do Google ◦ NetApp Cloud Volumes Service ◦ "Cloud Volumes ONTAP" • Microsoft Azure: <ul style="list-style-type: none"> ◦ Discos gerenciados do Azure ◦ Azure NetApp Files ◦ "Cloud Volumes ONTAP" • Clusters autogerenciados: <ul style="list-style-type: none"> ◦ Amazon EBS ◦ Persistent Disk do Google ◦ Discos gerenciados do Azure ◦ "Cloud Volumes ONTAP" 	<ul style="list-style-type: none"> • Sistemas NetApp ONTAP AFF e FAS • "Cloud Volumes ONTAP"

Como funciona o Astra Control Service

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

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

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

No Azure, o Astra Control Service também cria um grupo de recursos, uma conta de storage e chaves para o contêiner de Blob.

- Cria uma nova função de administrador e conta de serviço do Kubernetes no cluster.
- Usa essa nova função de administrador para instalar "[Astra Trident](#)" no cluster e criar uma ou mais classes de armazenamento.
- Se você usar uma oferta de storage de serviço de nuvem da NetApp como back-end de storage, o Astra Control Service usará o Astra Trident para provisionar volumes persistentes para suas aplicações. Se você usar os discos gerenciados do Amazon EBS ou Azure como back-end de armazenamento, precisará instalar um driver CSI específico do provedor. As instruções de instalação são fornecidas na "[Configurar o Amazon Web Services](#)" e "[Configurar o Microsoft Azure com discos gerenciados do Azure](#)".
- 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 Plano Gratuito do Astra Control permite gerenciar até 10 namespaces em sua conta. Se você quiser gerenciar mais de 10, precisará configurar o faturamento atualizando do Plano Gratuito para o Plano Premium.

Como funciona o Astra Control Center

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

O Astra Control Center é compatível com clusters Kubernetes com classe de storage baseado no Astra Trident com um back-end ONTAP 9.5 ou 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 AutoSupport e Active IQ para fornecer aos usuários e ao suporte NetApp informações de solução de problemas e utilização.

Você pode experimentar o Astra Control Center usando uma licença de avaliação incorporada de 90 dias. Enquanto você está avaliando o Astra Control Center, pode obter suporte por meio de e-mail e opções da comunidade. Além disso, você tem acesso a artigos e documentação da base de conhecimento a partir do painel de suporte do produto.

Para instalar e usar o Astra Control Center, você precisará atender a determinados "[requisitos](#)".

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

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

Saiba mais sobre como ["Configure o Astra Control Center"](#) .

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

Para mais informações

- ["Documentação do Astra Control Service"](#)
- ["Documentação do Astra Control Center"](#)
- ["Documentação do Astra Trident"](#)
- ["Use a API Astra Control"](#)
- ["Documentação do Cloud Insights"](#)
- ["Documentação do ONTAP"](#)

Requisitos do Astra Control Center

Comece verificando a prontidão do seu ambiente operacional, clusters de aplicativos, aplicativos, licenças e navegador da Web. Garanta que seu ambiente atenda a esses requisitos para implantar e operar o Astra Control Center.

- [Ambientes de Kubernetes do cluster de host compatíveis](#)
- [Requisitos de recursos de cluster de host](#)
- [Requisitos do Astra Trident](#)
- [Back-ends de armazenamento](#)
- [Registo de imagens](#)
- [Licença do Astra Control Center](#)
- [Licenças ONTAP](#)
- [Requisitos de rede](#)
- [Entrada para clusters do Kubernetes no local](#)
- [Navegadores da Web suportados](#)
- [Requisitos adicionais para clusters de aplicações](#)

Ambientes de Kubernetes do cluster de host compatíveis

O Astra Control Center foi validado com os seguintes ambientes de host do Kubernetes:



Garantir que o ambiente do Kubernetes que você escolher hospedar o Astra Control Center atenda aos requisitos básicos de recursos descritos na documentação oficial do ambiente.

Distribuição do Kubernetes no cluster de host	Versões suportadas
Serviço Kubernetes do Azure no Azure Stack HCI	Azure Stack HCI 21H2 e 22H2 com AKS 1,23 e 1,24
Google Anthos	1,12 a 1,14 (Requisitos de entrada do Google Anthos consulte)

Distribuição do Kubernetes no cluster de host	Versões suportadas
Kubernetes (upstream)	1,24 a 1,26 (o Astra Trident 22,10 ou mais recente é necessário para Kubernetes 1,25 ou mais recente)
Rancher Kubernetes Engine (RKE)	RKE 1,3 com Rancher 2,6 RKE 1,4 com Rancher 2,7 RKE 2 (v1,23.x) com Rancher 2,6 RKE 2 (v1,24.x) com Rancher 2,7
Red Hat OpenShift Container Platform	4,10 a 4,12
VMware Tanzu Kubernetes Grid	1,6 (Requisitos de recursos de cluster de host consulte)
VMware Tanzu Kubernetes Grid Integrated Edition	1,14 e 1,15 (Requisitos de recursos de cluster de host consulte)

Requisitos de recursos de cluster de host

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



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

- * Extensões de CPU*: As CPUs em todos os nós do ambiente de hospedagem devem ter extensões AVX ativadas.
- **Worker Nodes**: Pelo menos 3 worker node total, com 4 núcleos de CPU e 12GB GB de RAM cada
- **Requisitos de cluster do VMware Tanzu Kubernetes Grid**: Ao hospedar o Astra Control Center em um cluster do VMware Tanzu Kubernetes Grid (TKG) ou Tanzu Kubernetes Grid Integrated Edition (TKGI), tenha em mente as seguintes considerações.
 - O token de arquivo de configuração padrão do VMware TKG e TKGI expira dez horas após a implantação. Se você usa produtos do portfólio Tanzu, precisará gerar um arquivo de configuração de cluster do Kubernetes da Tanzu com um token sem expiração para evitar problemas de conexão entre o Astra Control Center e os clusters de aplicativos gerenciados. Para obter instruções, visite "[Documentação do produto do data center VMware NSX-T](#)."
 - Use o `kubect1 get nsxlbmonitors -A` comando para ver se você já tem um monitor de serviço configurado para aceitar o tráfego de entrada. Se existir um, não deve instalar o MetalLB, porque o monitor de serviço existente substituirá qualquer nova configuração do balanceador de carga.
 - Desative a aplicação da classe de armazenamento padrão TKG ou TKGI em qualquer cluster de aplicativos que seja gerenciado pelo Astra Control. Você pode fazer isso editando o `TanzuKubernetesCluster` recurso no cluster do namespace.
 - Esteja ciente dos requisitos específicos do Astra Trident ao implantar o Centro de Controle Astra em um ambiente TKG ou TKGI. Para obter mais informações, consulte "[Documentação do Astra Trident](#)".

Requisitos do Astra Trident

Garanta o atendimento aos seguintes requisitos do Astra Trident específicos para as necessidades do seu ambiente:

- **Versão mínima para uso com o Astra Control Center**: Astra Trident 22,04 ou mais recente instalado e configurado.

- **Replicação SnapMirror:** Astra Trident 22,07 ou mais recente instalado para replicação de aplicações baseada em SnapMirror.
- **Para suporte a Kubernetes 1,25 ou mais recente:** Astra Trident 22,10 ou mais recente instalado para Kubernetes 1,25 ou clusters mais recentes (é necessário atualizar para Astra Trident 22,10 antes da atualização para Kubernetes 1,25 ou mais recente)
- **Configuração do ONTAP com o Astra Trident:**
 - **Storage class:** Configure pelo menos uma classe de armazenamento Astra Trident no cluster. Se uma classe de armazenamento padrão estiver configurada, verifique se ela é a única classe de armazenamento com a designação padrão.
 - **Drivers de armazenamento e nós de trabalho:** Certifique-se de que os nós de trabalho no cluster estejam configurados com os drivers de armazenamento apropriados para que os pods possam interagir com o armazenamento de back-end. O Astra Control Center é compatível com os seguintes drivers ONTAP fornecidos pelo Astra Trident:
 - `ontap-nas`
 - `ontap-san`
 - `ontap-san-economy` (a replicação de aplicativos não está disponível com esse tipo de classe de armazenamento)
 - `ontap-nas-economy` (snapshots, políticas de replicação e políticas de proteção não estão disponíveis com esse tipo de classe de storage)

Back-ends de armazenamento

Certifique-se de ter um back-end compatível com capacidade suficiente.

- **Backends compatíveis:** O Astra Control Center é compatível com os seguintes back-ends de storage:
 - NetApp ONTAP 9 .8 ou sistemas AFF, FAS e ASA mais recentes
 - NetApp ONTAP Select 9,8 ou mais recente
 - NetApp Cloud Volumes ONTAP 9,8 ou mais recente
- **Capacidade de back-end de armazenamento necessária:** Pelo menos 500GB GB disponíveis

Licenças ONTAP

Para usar o Astra Control Center, verifique se você tem as seguintes licenças do ONTAP, dependendo do que você precisa realizar:

- FlexClone
- SnapMirror: Opcional. Necessário apenas para replicação para sistemas remotos usando a tecnologia SnapMirror. Consulte a ["Informações de licença do SnapMirror"](#).
- Licença S3: Opcional. Necessário apenas para buckets do ONTAP S3

Para verificar se o sistema ONTAP tem as licenças necessárias, ["Gerenciar licenças do ONTAP"](#) consulte .

Registro de imagens

Você deve ter um Registro de imagem privada do Docker existente para o qual você pode enviar imagens de compilação do Astra Control Center. Você precisa fornecer o URL do Registro de imagens onde você vai carregar as imagens.

Licença do Astra Control Center

O Astra Control Center requer uma licença do Astra Control Center. Quando você instala o Astra Control Center, uma licença de avaliação incorporada de 90 dias para 4.800 unidades CPU já está ativada. Se você precisar de mais capacidade ou termos de avaliação diferentes ou quiser atualizar para uma licença completa, você pode obter uma licença de avaliação diferente ou uma licença completa da NetApp. Você precisa de uma licença para proteger seus aplicativos e dados.

Você pode experimentar o Astra Control Center inscrevendo-se para uma avaliação gratuita. Você pode se inscrever registrando ["aqui"](#).

Para configurar a licença, ["use uma licença de avaliação de 90 dias"](#) consulte a .

Para saber mais sobre como as licenças funcionam, ["Licenciamento"](#) consulte .

Requisitos de rede

Configure seu ambiente operacional para garantir que o Astra Control Center possa se comunicar corretamente. São necessárias as seguintes configurações de rede:

- **Endereço FQDN:** Você deve ter um endereço FQDN para o Astra Control Center.
- **Acesso à internet:** Você deve determinar se tem acesso externo à internet. Se não o fizer, algumas funcionalidades poderão ser limitadas, como receber dados de monitorização e métricas do NetApp Cloud Insights, ou enviar pacotes de suporte para o ["Site de suporte da NetApp"](#).
- **Acesso à porta:** O ambiente operacional que hospeda o Astra Control Center se comunica usando as seguintes portas TCP. Você deve garantir que essas portas sejam permitidas por meio de firewalls e configurar firewalls para permitir qualquer tráfego de saída HTTPS proveniente da rede Astra. Algumas portas exigem conectividade entre o ambiente que hospeda o Astra Control Center e cada cluster gerenciado (observado quando aplicável).



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

Fonte	Destino	Porta	Protocolo	Finalidade
PC do cliente	Astra Control Center	443	HTTPS	Acesso de IU / API - garanta que essa porta esteja aberta de ambas as maneiras entre o cluster que hospeda o Astra Control Center e cada cluster gerenciado

Fonte	Destino	Porta	Protocolo	Finalidade
Consumidor de métricas	Nó de trabalho do Astra Control Center	9090	HTTPS	Comunicação de dados de métricas - garante que cada cluster gerenciado possa acessar essa porta no cluster que hospeda o Astra Control Center (comunicação bidirecional necessária)
Astra Control Center	Serviço Cloud Insights hospedado (https://www.netapp.com/cloud-services/cloud-insights/)	443	HTTPS	Comunicação Cloud Insights
Astra Control Center	Fornecedor de bucket de storage do Amazon S3	443	HTTPS	Comunicação de armazenamento Amazon S3
Astra Control Center	NetApp AutoSupport (https://support.netapp.com)	443	HTTPS	Comunicação NetApp AutoSupport

Entrada para clusters do Kubernetes no local

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



O balanceador de carga deve usar um endereço IP localizado na mesma sub-rede que os endereços IP do nó de trabalho do Astra Control Center.

Para obter mais informações, "[Configure a entrada para o balanceamento de carga](#)" consulte .

Requisitos de entrada do Google Anthos

Ao hospedar o Astra Control Center em um cluster do Google Anthos, observe que o Google Anthos inclui o balanceador de carga MetalLB e o serviço de ingresso Istio por padrão, permitindo que você simplesmente use os recursos genéricos de entrada do Astra Control Center durante a instalação. "[Configurar o Astra Control Center](#)" Consulte para obter detalhes.

Navegadores da Web suportados

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

Requisitos adicionais para clusters de aplicações

Tenha em mente esses requisitos se você planeja usar esses recursos do Astra Control Center:

- * Requisitos de cluster de aplicativos*: ["Requisitos de gerenciamento de clusters"](#)
 - **Requisitos de aplicação gerenciada**: ["Requisitos de gerenciamento de aplicativos"](#)
 - **Requisitos adicionais para replicação de aplicativos**: ["Pré-requisitos de replicação"](#)

O que vem a seguir

Veja a ["início rápido"](#) visão geral.

Início rápido para Astra Control Center

Aqui está uma visão geral 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.

1

Analisar os requisitos do cluster do Kubernetes

Certifique-se de que seu ambiente atenda a esses requisitos:

Cluster do Kubernetes

- ["Certifique-se de que o cluster de host atenda aos requisitos do ambiente operacional"](#)
- ["Configurar o ingresso para balanceamento de carga de clusters do Kubernetes no local"](#)

Integração de armazenamento

- ["Garanta que seu ambiente inclua a versão compatível com o Astra Trident"](#)
- ["Prepare os nós de trabalho"](#)
- ["Configurar o back-end de storage do Astra Trident"](#)
- ["Configurar as classes de storage do Astra Trident"](#)
- ["Instalar a controladora Snapshot de volume Astra Trident"](#)
- ["Crie uma classe de instantâneo de volume"](#)

Credenciais ONTAP

- ["Configurar credenciais do ONTAP"](#)

2

Baixe e instale o Astra Control Center

Conclua estas tarefas de instalação:

- ["Faça download do Centro de Controle Astra na página de downloads do site de suporte da NetApp"](#)
- Obtenha o ficheiro de licença NetApp:
 - Se você estiver avaliando o Astra Control Center, uma licença de avaliação incorporada já estará incluída

- ["Se você já comprou o Astra Control Center, gere seu arquivo de licença"](#)
- ["Instale o Astra Control Center"](#)
- ["Execute etapas de configuração opcionais adicionais"](#)

3

Conclua algumas tarefas de configuração inicial

Conclua algumas tarefas básicas para começar:

- ["Adicione uma licença"](#)
- ["Prepare seu ambiente para o gerenciamento de clusters"](#)
- ["Adicione um cluster"](#)
- ["Adicionar um back-end de storage"](#)
- ["Adicione um balde"](#)

4

Use o Astra Control Center

Depois de concluir a configuração do Astra Control Center, use a IU do Astra Control ou a ["API Astra Control"](#) para começar a gerenciar e proteger aplicações:

- ["Gerir aplicações"](#): Defina recursos para gerenciar.
- ["Proteja aplicativos"](#): Configurar políticas de proteção e replicar, clonar e migrar aplicativos.
- ["Gerenciar contas"](#): Usuários, funções, LDAP, credenciais e muito mais.
- ["Opcionalmente, conecte-se ao Cloud Insights"](#): Visualizar métricas sobre a integridade do seu sistema.

Para mais informações

- ["API Astra Control"](#)
- ["Atualizar o Astra Control Center"](#)
- ["Obtenha ajuda com o Astra Control"](#)

Visão geral da instalação

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

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

Dependendo do seu ambiente, pode haver configuração adicional necessária após a instalação do Astra Control Center:

- ["Configure o Astra Control Center após a instalação"](#)

Instale o Astra Control Center usando o processo padrão

Para instalar o Astra Control Center, faça o download do pacote de instalação no site de suporte da NetApp e execute as etapas a seguir. Você pode usar este procedimento para instalar o Astra Control Center em ambientes conectados à Internet ou com conexão via rede.

Outros procedimentos de instalação

- **Instalar com RedHat OpenShift OperatorHub:** Use isso ["procedimento alternativo"](#) para instalar o Astra Control Center no OpenShift usando o OperatorHub.
- **Instalar na nuvem pública com o Cloud Volumes ONTAP backend:** Use ["estes procedimentos"](#) para instalar o Astra Control Center no Amazon Web Services (AWS), no Google Cloud Platform (GCP) ou no Microsoft Azure com um back-end de storage do Cloud Volumes ONTAP.

Para uma demonstração do processo de instalação do Astra Control Center, ["este vídeo"](#) consulte .

Antes de começar

- ["Antes de começar a instalação, prepare seu ambiente para a implantação do Astra Control Center"](#).
- Se você configurou ou deseja configurar políticas de segurança de pod no seu ambiente, familiarize-se com as políticas de segurança de pod e como elas afetam a instalação do Astra Control Center. ["Compreender as restrições da política de segurança do pod"](#)Consulte a .
- Certifique-se de que todos os serviços de API estão em um estado saudável e disponíveis:

```
kubectl get apiservices
```

- Certifique-se de que o Astra FQDN que pretende utilizar está roteável para este cluster. Isso significa que você tem uma entrada DNS no seu servidor DNS interno ou está usando uma rota URL principal que já está registrada.
- Se um gerenciador de cert já existir no cluster, você precisará executar alguns ["etapas de pré-requisito"](#) para que o Astra Control Center não tente instalar seu próprio gerenciador de cert. Por padrão, o Astra Control Center instala seu próprio gerenciador de cert durante a instalação.



Implante o Astra Control Center em um domínio de terceiros ou local secundário. Isso é recomendado para replicação de aplicativos e recuperação de desastres aprimorada.

Sobre esta tarefa

O processo de instalação do Astra Control Center ajuda você a fazer o seguinte:

- Instale os componentes do Astra no `netapp-acc` namespace (ou nome personalizado).
- Crie uma conta de administrador padrão do Astra Control Owner.
- Estabeleça um endereço de e-mail de usuário administrativo e uma senha de configuração inicial padrão. Este usuário é atribuído a função proprietário que é necessária para o primeiro login na IU.
- Determine se todos os pods do Astra Control Center estão em execução.
- Instale a IU do Astra Control Center.



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

Passos

Para instalar o Astra Control Center, siga estas etapas:

- [Faça download e extraia Astra Control Center](#)
- [Instale o plug-in NetApp Astra kubectl](#)
- [Adicione as imagens ao seu registo local](#)
- [Configure namespace e segredo para Registros com requisitos de autenticação](#)
- [Instale o operador do Centro de Controle Astra](#)
- [Configurar o Astra Control Center](#)
- [Instalação completa do operador e do Centro de Controle Astra](#)
- [Verifique o status do sistema](#)
- [Configure a entrada para o balanceamento de carga](#)
- [Faça login na IU do Astra Control Center](#)

Faça download e extraia Astra Control Center

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

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

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

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

4. Extraia as imagens do pacote Astra Control Center:

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

Instale o plug-in NetApp Astra kubectl

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

Antes de começar

O NetApp fornece binários de plug-in para diferentes arquiteturas de CPU e sistemas operacionais. Você precisa saber qual CPU e sistema operacional você tem antes de executar esta tarefa.

Se você já tiver o plugin instalado a partir de uma instalação anterior, "[certifique-se de que tem a versão mais recente](#)" antes de concluir estas etapas.

Passos

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



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

```
ls kubectl-astra/
```

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

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

Adicione as imagens ao seu registo local

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

Docker

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

```
acc.manifest.bundle.yaml
acc/
```

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

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

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

Podman

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

```
acc.manifest.bundle.yaml
acc/
```

2. Inicie sessão no seu registro:

```
podman login <YOUR_REGISTRY>
```

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

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

```

export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=23.04.2-7
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //'')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*/:::')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done

```

Podman 3

```

export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=23.04.2-7
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //'')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*/:::')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done

```



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

```

https://netappdownloads.jfrog.io/docker-astra-control-
prod/netapp/astra/acc/23.04.2-7/image:version

```

Configure namespace e segredo para Registros com requisitos de autenticação

1. Exporte o KUBECONFIG para o cluster host do Astra Control Center:

```
export KUBECONFIG=[file path]
```



Antes de concluir a instalação, certifique-se de que o KUBECONFIG está apontando para o cluster onde você deseja instalar o Astra Control Center. O KUBECONFIG pode conter apenas um contexto.

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

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

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

Resposta:

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

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



O marcador de posição `your_registry_path` deve corresponder à localização das imagens que carregou anteriormente (por exemplo, `[Registry_URL]/netapp/astra/astracc/23.04.2-7`).

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

Resposta da amostra:

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



Se você excluir o namespace depois que o segredo é gerado, recrie o namespace e, em seguida, regenere o segredo para o namespace.

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

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

Resposta da amostra:

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

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

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

Resposta

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

Instale o operador do Centro de Controle Astra

1. Altere o diretório:

```
cd manifests
```

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

```
vim astra_control_center_operator_deploy.yaml
```



Uma amostra anotada YAML segue estes passos.

- a. Se você usar um Registro que requer autenticação, substitua a linha padrão de imagePullSecrets: [] pelo seguinte:

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

- b. Altere [your_registry_path] para a kube-rbac-proxy imagem para o caminho do registo onde as imagens foram empurradas para um [passo anterior](#).
- c. Altere [your_registry_path] para a acc-operator-controller-manager imagem para o caminho do registo onde as imagens foram empurradas para um [passo anterior](#).

```
<strong>astra_control_center_operator_deploy.yaml</strong>
```

```
apiVersion: apps/v1
```

```

kind: Deployment
metadata:
  labels:
    control-plane: controller-manager
  name: acc-operator-controller-manager
  namespace: netapp-acc-operator
spec:
  replicas: 1
  selector:
    matchLabels:
      control-plane: controller-manager
  strategy:
    type: Recreate
  template:
    metadata:
      labels:
        control-plane: controller-manager
    spec:
      containers:
        - args:
            - --secure-listen-address=0.0.0.0:8443
            - --upstream=http://127.0.0.1:8080/
            - --logtostderr=true
            - --v=10
          image: [your_registry_path]/kube-rbac-proxy:v4.8.0
          name: kube-rbac-proxy
          ports:
            - containerPort: 8443
              name: https
        - args:
            - --health-probe-bind-address=:8081
            - --metrics-bind-address=127.0.0.1:8080
            - --leader-elect
          env:
            - name: ACCOP_LOG_LEVEL
              value: "2"
            - name: ACCOP_HELM_INSTALLTIMEOUT
              value: 5m
          image: [your_registry_path]/acc-operator:23.04.36
          imagePullPolicy: IfNotPresent
          livenessProbe:
            httpGet:
              path: /healthz
              port: 8081
            initialDelaySeconds: 15
            periodSeconds: 20

```

```

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

```

3. Instale o operador 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

```

4. Verifique se os pods estão em execução:

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

Configurar o Astra Control Center

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

```
vim astra_control_center.yaml
```



Uma amostra anotada YAML segue estes passos.

2. Modifique ou confirme as seguintes definições:

`<code>accountName</code>`

Definição	Orientação	Tipo	Exemplo
accountName	Altere a <code>accountName</code> cadeia de caracteres para o nome que deseja associar à conta Astra Control Center. Só pode haver uma <code>accountName</code> .	cadeia de caracteres	Example

`<code>astraVersion</code>`

Definição	Orientação	Tipo	Exemplo
astraVersion	A versão do Astra Control Center para implantação. Não é necessária nenhuma ação para esta definição, uma vez que o valor será pré-preenchido.	cadeia de caracteres	23.04.2-7

<code> </code>

Definição	Orientação	Tipo	Exemplo
astraAddress	Altere a astraAddress cadeia de caracteres para o endereço FQDN (recomendado) ou IP que você deseja usar em seu navegador para acessar o Astra Control Center. Esse endereço define como o Astra Control Center será encontrado em seu data center e será o mesmo FQDN ou endereço IP que você provisionou do balanceador de carga quando concluir "Requisitos do Astra Control Center" . NOTA: Não use http:// nem https:// no endereço. Copie este FQDN para uso em um passo posterior .	cadeia de caracteres	astra.example.com

<code> AutoSupport </code>

Suas seleções nesta seção determinam se você participará do aplicativo de suporte Pro-ativo da NetApp, NetApp Active IQ e onde os dados são enviados. É necessária uma ligação à Internet (porta 442) e todos os dados de suporte são anonimizados.

Definição	Utilização	Orientação	Tipo	Exemplo
<code>autoSupport.enrolled</code>	enrolled`Os campos ou `url têm de ser selecionados	Alterar enrolled para AutoSupport para false sites sem conectividade com a Internet ou manter true para sites conectados. Uma configuração de true permite que dados anônimos sejam enviados para o NetApp para fins de suporte. A eleição padrão é false e indica que nenhum dado de suporte será enviado para o NetApp.	Booleano	false (este valor é o padrão)
<code>autoSupport.url</code>	enrolled`Os campos ou `url têm de ser selecionados	Esta URL determina onde os dados anônimos serão enviados.	cadeia de caracteres	https://support.netapp.com/asupprod/post/1.0/postAsup

`<code> email</code>`

Definição	Orientação	Tipo	Exemplo
email	Altere a email cadeia de caracteres para o endereço de administrador inicial padrão. Copie este endereço de e-mail para uso em um passo posterior . Este endereço de e-mail será usado como o nome de usuário da conta inicial para fazer login na IU e será notificado de eventos no Astra Control.	cadeia de caracteres	admin@example.com

`<code>firstName</code>`

Definição	Orientação	Tipo	Exemplo
firstName	O primeiro nome do administrador inicial padrão associado à conta Astra. O nome usado aqui será visível em um cabeçalho na IU após seu primeiro login.	cadeia de caracteres	SRE

`<code>LastName</code>`

Definição	Orientação	Tipo	Exemplo
lastName	O sobrenome do administrador inicial padrão associado à conta Astra. O nome usado aqui será visível em um cabeçalho na IU após seu primeiro login.	cadeia de caracteres	Admin

`<code> imageRegistry</code>`

Suas seleções nesta seção definem o Registro de imagem de contendor que hospeda as imagens do aplicativo Astra, o Operador do Centro de Controle Astra e o repositório do Astra Control Center Helm.

Definição	Utilização	Orientação	Tipo	Exemplo
<code>imageRegistry.name</code>	Obrigatório	O nome do registo de imagens onde as imagens foram enviadas para o passo anterior . Não utilize <code>http://</code> ou <code>https://</code> no nome do registo.	cadeia de caracteres	<code>example.registry.com/astra</code>
<code>imageRegistry.secret</code>	Obrigatório se a cadeia de caracteres inserida para <code>imageRegistry.name</code> requires a secret. IMPORTANT: If you are using a registry that does not require authorization, you must delete this <code>secret</code> a linha <code>imageRegistry</code> ou a instalação falhar.	O nome do segredo do Kubernetes usado para autenticar com o Registro de imagens.	cadeia de caracteres	<code>astra-registry-cred</code>

`<code>storageClass</code>`

Definição	Orientação	Tipo	Exemplo
<code>storageClass</code>	Altere <code>storageClass</code> o valor de <code>ontap-gold</code> para outro recurso de <code>storageClass</code> do Astra Trident, conforme exigido pela sua instalação. Execute o comando <code>kubectl get sc</code> para determinar suas classes de armazenamento configuradas existentes. Uma das classes de storage baseadas no Astra Trident deve ser inserida no arquivo MANIFEST (<code>astra-control-center-<version>.manifest</code>) e será usada para PVS Astra. Se não estiver definida, a classe de armazenamento padrão será usada. Nota: Se uma classe de armazenamento padrão estiver configurada, certifique-se de que é a única classe de armazenamento que tem a anotação padrão.	cadeia de caracteres	<code>ontap-gold</code>

`<code> volume ReclaimPolicy</code>`

Definição	Orientação	Tipo	Opções
<code>volumeReclaimPolicy</code>	Isso define a política de recuperação para PVS do Astra. Definir essa política para <code>Retain</code> reter volumes persistentes depois que o Astra for excluído. Definir essa política para <code>Delete</code> excluir volumes persistentes depois que o Astra for excluído. Se este valor não for definido, os PVS são retidos.	cadeia de caracteres	<ul style="list-style-type: none">• <code>Retain</code> (Este é o valor padrão)• <code>Delete</code>

`<code>ingressType</code>`





Definição	Orientação	Tipo	Opções
ingressType	<p>Use um dos seguintes tipos de entrada:</p> <p>Generic (ingressType: "Generic") (Padrão) Use esta opção quando tiver outro controlador de entrada em uso ou preferir usar seu próprio controlador de entrada. Depois que o Astra Control Center for implantado, você precisará configurar o "controlador de entrada" para expor o Astra Control Center com um URL. AccTraefik (ingressType: "AccTraefik") Utilize esta opção quando preferir não configurar um controlador de entrada. Isso implanta o gateway Astra Control Center traefik como um serviço do tipo Kubernetes LoadBalancer. O Astra Control Center usa um serviço do tipo "LoadBalancer" (svc/traefik no namespace Astra Control Center) e exige que seja atribuído um endereço IP externo acessível. Se os balanceadores de carga forem permitidos em seu ambiente e você ainda não tiver um configurado, você poderá usar o MetalLB ou outro balanceador de carga de serviço externo para atribuir um endereço IP externo ao serviço. Na configuração do servidor DNS interno, você deve apontar o nome DNS escolhido</p>	cadeia de caracteres	<ul style="list-style-type: none"> • Generic (este é o valor padrão) • AccTraefik

`scaleSize`

Definição	Orientação	Tipo	Opções
<code>scaleSize</code>	Por padrão, o Astra usará alta disponibilidade (HA <code>scaleSize</code>) do Medium, que implanta a maioria dos serviços no HA e implanta várias réplicas para redundância. Com <code>scaleSize</code> as <code>Small</code> , o Astra reduzirá o número de réplicas para todos os serviços, exceto para serviços essenciais para reduzir o consumo. Dica: Medium As implantações consistem em cerca de 100 pods (não incluindo cargas de trabalho transitórias. os pods do 100 são baseados em uma configuração de três nós mestre e três nós de trabalho). Esteja ciente das restrições de limite de rede por pod que podem ser um problema em seu ambiente, especialmente ao considerar cenários de recuperação de desastres.	cadeia de caracteres	<ul style="list-style-type: none">• <code>Small</code>• <code>Medium</code> (Este é o valor padrão)

`<code>astraResourcesScaler</code>`

Definição	Orientação	Tipo	Opções
<code>astraResourcesScaler</code>	<p>Opções de escala para os limites de recursos do AstraControlCenter. Por padrão, o Astra Control Center é implantado com solicitações de recursos definidas para a maioria dos componentes no Astra. Essa configuração permite que a pilha de software Astra Control Center tenha melhor desempenho em ambientes com maior carga e escalabilidade de aplicações. No entanto, em cenários que usam clusters de desenvolvimento ou teste menores, o campo <code>CR</code> <code>astraResourcesScaler</code> pode ser definido como <code>Off</code>. Isso desativa as solicitações de recursos e permite a implantação em clusters menores.</p>	cadeia de caracteres	<ul style="list-style-type: none">• Default (Este é o valor padrão)• Off

`<code> AdditionalValues</code>`

- Para a comunicação Astral Control Center e Cloud Insights, a verificação de certificado TLS é desativada por padrão. Você pode habilitar a verificação de certificação TLS para comunicação entre o Cloud Insights e o cluster de host e o cluster gerenciado do Astra Control Center adicionando a seguinte seção em `additionalValues`.

```
additionalValues:
  netapp-monitoring-operator:
    config:
      ciSkipTlsVerify: false
  cloud-insights-service:
    config:
      ciSkipTlsVerify: false
  telemetry-service:
    config:
      ciSkipTlsVerify: false
```

`<code> crds</code>`

Suas seleções nesta seção determinam como o Astra Control Center deve lidar com CRDs.

Definição	Orientação	Tipo	Exemplo
<code>crds.externalCertManager</code>	Se você usar um gerenciador cert externo, <code>externalCertManager</code> altere para <code>true</code> . O padrão <code>false</code> faz com que o Astra Control Center instale seus próprios CRDs de gerenciador de cert durante a instalação. CRDs são objetos de todo o cluster e instalá-los pode ter um impactos em outras partes do cluster. Você pode usar esse sinalizador para sinalizar para o Astra Control Center que essas CRDs serão instaladas e gerenciadas pelo administrador do cluster fora do Astra Control Center.	Booleano	<code>False</code> (este valor é o padrão)
<code>crds.externalTraefik</code>	Por padrão, o Astra Control Center instalará CRDs Traefik necessários. CRDs são objetos de todo o cluster e instalá-los pode ter um impactos em outras partes do cluster. Você pode usar esse sinalizador para sinalizar para o Astra Control Center que essas CRDs serão instaladas e gerenciadas pelo administrador do cluster fora do Astra Control Center.	Booleano	<code>False</code> (este valor é o padrão)



Certifique-se de que selecionou a classe de armazenamento e o tipo de entrada corretos para a sua configuração antes de concluir a instalação.

```
<strong>astra_control_center.yaml</strong>
```

```
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: "[your_registry_path]"
    secret: "astra-registry-cred"
  storageClass: "ontap-gold"
  volumeReclaimPolicy: "Retain"
  ingressType: "Generic"
  scaleSize: "Medium"
  astraResourcesScaler: "Default"
  additionalValues: {}
  crds:
    externalTraefik: false
    externalCertManager: false
```

Instalação completa do operador e do Centro de Controle Astra

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

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

Resposta da amostra:

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

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

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

Resposta da amostra:

```
astracenter.astra.netapp.io/astra created
```



O operador do Astra Control Center executará uma verificação automática dos requisitos de ambiente. A falta "requisitos" pode fazer com que a instalação falhe ou o Astra Control Center não funcione corretamente. [próxima seção](#) Consulte para verificar se existem mensagens de aviso relacionadas com a verificação automática do sistema.

Verifique o status do sistema

Você pode verificar o status do sistema usando comandos kubectl. Se você preferir usar OpenShift, você pode usar comandos oc comparáveis para etapas de verificação.

Passos

1. Verifique se o processo de instalação não produziu mensagens de avisos relacionadas às verificações de validação:

```
kubectl get acc [astra or custom Astra Control Center CR name] -n [netapp-acc or custom namespace] -o yaml
```



Mensagens de aviso adicionais também são relatadas nos logs do operador do Centro de Controle Astra.

2. Corrija quaisquer problemas com seu ambiente que foram relatados pelas verificações automatizadas de requisitos.



Você pode corrigir problemas garantindo que seu ambiente atenda ao do "requisitos" para Astra Control Center.

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

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

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

Resposta da amostra

NAME	READY	STATUS	
RESTARTS AGE			
acc-helm-repo-6cc7696d8f-pmhm8 9h	1/1	Running	0
activity-597fb656dc-5rd4l 9h	1/1	Running	0
activity-597fb656dc-mqmcw 9h	1/1	Running	0
api-token-authentication-62f84 9h	1/1	Running	0
api-token-authentication-68nlf 9h	1/1	Running	0
api-token-authentication-ztgrm 9h	1/1	Running	0
asup-669d4ddbc4-fnmwp (9h ago) 9h	1/1	Running	1
authentication-78789d7549-lk686 9h	1/1	Running	0
bucket-service-65c7d95496-24x7l (9h ago) 9h	1/1	Running	3
cert-manager-c9f9fbf9f-k8zq2 9h	1/1	Running	0
cert-manager-c9f9fbf9f-qj1zm 9h	1/1	Running	0
cert-manager-cainjector-dbbbd8447-b5q1l 9h	1/1	Running	0
cert-manager-cainjector-dbbbd8447-p5whs 9h	1/1	Running	0
cert-manager-webhook-6f97bb7d84-4722b 9h	1/1	Running	0
cert-manager-webhook-6f97bb7d84-86kv5 9h	1/1	Running	0
certificates-59d9f6f4bd-2j899 9h	1/1	Running	0
certificates-59d9f6f4bd-9d9k6 9h	1/1	Running	0
certificates-expiry-check-28011180--1-81kxz 9h	0/1	Completed	0
cloud-extension-5c9c9958f8-jdhrp 9h	1/1	Running	0
cloud-insights-service-5cdd5f7f-pp8r5 9h	1/1	Running	0
composite-compute-66585789f4-hxn5w 9h	1/1	Running	0

composite-volume-68649f68fd-tb7p4 9h	1/1	Running	0
credentials-dfc844c57-jsx92 9h	1/1	Running	0
credentials-dfc844c57-xw26s 9h	1/1	Running	0
entitlement-7b47769b87-4jb6c 9h	1/1	Running	0
features-854d8444cc-c24b7 9h	1/1	Running	0
features-854d8444cc-dv6sm 9h	1/1	Running	0
fluent-bit-ds-9tlv4 9h	1/1	Running	0
fluent-bit-ds-bpkcb 9h	1/1	Running	0
fluent-bit-ds-cxmxw 9h	1/1	Running	0
fluent-bit-ds-jgnhc 9h	1/1	Running	0
fluent-bit-ds-vtr6k 9h	1/1	Running	0
fluent-bit-ds-vxqd5 9h	1/1	Running	0
graphql-server-7d4b9d44d5-zdbf5 9h	1/1	Running	0
identity-6655c48769-4pwk8 9h	1/1	Running	0
influxdb2-0 9h	1/1	Running	0
keycloak-operator-55479d6fc6-slvmt 9h	1/1	Running	0
krakend-f487cb465-78679 9h	1/1	Running	0
krakend-f487cb465-rjsxx 9h	1/1	Running	0
license-64cbc7cd9c-qxsr8 9h	1/1	Running	0
login-ui-5db89b5589-ndb96 9h	1/1	Running	0
loki-0 9h	1/1	Running	0
metrics-facade-8446f64c94-x8h7b 9h	1/1	Running	0
monitoring-operator-6b44586965-pvcl4 9h	2/2	Running	0

nats-0 9h	1/1	Running	0
nats-1 9h	1/1	Running	0
nats-2 9h	1/1	Running	0
nautilus-85754d87d7-756qb 9h	1/1	Running	0
nautilus-85754d87d7-q8j7d 9h	1/1	Running	0
openapi-5f9cc76544-7fnjm 9h	1/1	Running	0
openapi-5f9cc76544-vzr7b 9h	1/1	Running	0
packages-5db49f8b5-lrzhd 9h	1/1	Running	0
polaris-consul-consul-server-0 9h	1/1	Running	0
polaris-consul-consul-server-1 9h	1/1	Running	0
polaris-consul-consul-server-2 9h	1/1	Running	0
polaris-keycloak-0 (9h ago) 9h	1/1	Running	2
polaris-keycloak-1 9h	1/1	Running	0
polaris-keycloak-2 9h	1/1	Running	0
polaris-keycloak-db-0 9h	1/1	Running	0
polaris-keycloak-db-1 9h	1/1	Running	0
polaris-keycloak-db-2 9h	1/1	Running	0
polaris-mongodb-0 9h	1/1	Running	0
polaris-mongodb-1 9h	1/1	Running	0
polaris-mongodb-2 9h	1/1	Running	0
polaris-ui-66fb99479-qp9gq 9h	1/1	Running	0
polaris-vault-0 9h	1/1	Running	0
polaris-vault-1 9h	1/1	Running	0

polaris-vault-2 9h	1/1	Running	0
public-metrics-76fbf9594d-zmxzw 9h	1/1	Running	0
storage-backend-metrics-7d7fbc9cb9-lmd25 9h	1/1	Running	0
storage-provider-5bdd456c4b-2fftc 9h	1/1	Running	0
task-service-87575df85-dnn2q (9h ago) 9h	1/1	Running	3
task-service-task-purge-28011720--1-q6w4r 28m	0/1	Completed	0
task-service-task-purge-28011735--1-vk6pd 13m	1/1	Running	0
telegraf-ds-2r2kw 9h	1/1	Running	0
telegraf-ds-6s9d5 9h	1/1	Running	0
telegraf-ds-96jl7 9h	1/1	Running	0
telegraf-ds-hbp84 9h	1/1	Running	0
telegraf-ds-plwzv 9h	1/1	Running	0
telegraf-ds-sr22c 9h	1/1	Running	0
telegraf-rs-4sbg8 9h	1/1	Running	0
telemetry-service-fb9559f7b-mk917 (9h ago) 9h	1/1	Running	3
tenancy-559bbc6b48-5msgg 9h	1/1	Running	0
traefik-d997b8877-7xpf4 9h	1/1	Running	0
traefik-d997b8877-9xv96 9h	1/1	Running	0
trident-svc-585c97548c-d25z5 9h	1/1	Running	0
vault-controller-88484b454-2d6sr 9h	1/1	Running	0
vault-controller-88484b454-fc5cz 9h	1/1	Running	0
vault-controller-88484b454-jktld 9h	1/1	Running	0

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

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



`accHost` o registro de cluster é uma das últimas operações e, se falhar, não causará falha na implantação. No caso de uma falha de Registro de cluster indicada nos logs, você pode tentar o Registro novamente por meio da ["Adicione fluxo de trabalho de cluster na IU"](#) API ou.

5. Quando todos os pods estiverem em execução, verifique se a instalação foi bem-sucedida (`READY` é `True`) e obtenha a senha de configuração inicial que você usará quando fizer login no Astra Control Center:

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

Resposta:

NAME	UUID	VERSION	ADDRESS
READY			
astra	9aa5fdae-4214-4cb7-9976-5d8b4c0ce27f	23.04.2-7	10.111.111.111
True			



Copie o valor UUID. A palavra-passe é `ACC-` seguida pelo valor UUID (`ACC-[UUID]` ou, neste exemplo, `ACC-9aa5fdae-4214-4cb7-9976-5d8b4c0ce27f`).

Configure a entrada para o balanceamento de carga

Você pode configurar uma controladora de ingresso do Kubernetes que gerencia o acesso externo a serviços. Esses procedimentos fornecem exemplos de configuração para um controlador de entrada se você usou o padrão do no recurso personalizado do `ingressType: "Generic"` Astra Control Center (`astra_control_center.yaml`). Não é necessário usar este procedimento se você especificou `ingressType: "AccTraefik"` no recurso personalizado do Astra Control Center (`astra_control_center.yaml`).

Depois que o Astra Control Center for implantado, você precisará configurar o controlador Ingress para expor o Astra Control Center com um URL.

As etapas de configuração diferem dependendo do tipo de controlador de entrada que você usa. O Astra Control Center é compatível com muitos tipos de controlador de entrada. Estes procedimentos de configuração fornecem passos de exemplo para os seguintes tipos de controlador de entrada:

- Entrada de Istio
- Controlador de entrada nginx

- Controlador de entrada OpenShift

Antes de começar

- O necessário "[controlador de entrada](#)" já deve ser implantado.
- O "[classe de entrada](#)" correspondente ao controlador de entrada já deve ser criado.

Etapas para a entrada do Istio

1. Configurar a entrada do Istio.



Este procedimento pressupõe que o Istio é implantado usando o perfil de configuração "padrão".

2. Reúna ou crie o certificado e o arquivo de chave privada desejados para o Ingress Gateway.

Você pode usar um certificado assinado pela CA ou autoassinado. O nome comum deve ser o endereço Astra (FQDN).

Exemplo de comando:

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout tls.key -out  
tls.crt
```

3. Crie um segredo `tls secret name` do tipo `kubernetes.io/tls` para uma chave privada TLS e um certificado, `istio-system` namespace conforme descrito em `segredos TLS`.

Exemplo de comando:

```
kubectl create secret tls [tls secret name] --key="tls.key"  
--cert="tls.crt" -n istio-system
```



O nome do segredo deve corresponder ao `spec.tls.secretName` fornecido no `istio-ingress.yaml` arquivo.

4. Implante um recurso de entrada no `netapp-acc` namespace (ou nome personalizado) usando o tipo de recurso `v1` para um esquema (`istio-Ingress.yaml` é usado neste exemplo):

```

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

```

5. Aplicar as alterações:

```
kubectl apply -f istio-Ingress.yaml
```

6. Verifique o estado da entrada:

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

Resposta:

NAME	CLASS	HOSTS	ADDRESS	PORTS	AGE
ingress	istio	astra.example.com	172.16.103.248	80, 443	1h

7. Concluir a instalação do Astra Control Center.

Etapas para o controlador nginx Ingress

1. Crie um segredo do tipo `kubernetes.io/tls` para uma chave privada TLS e um certificado no `netapp-acc` namespace (ou nome personalizado), conforme descrito em "[Segredos TLS](#)".
2. Implantar um recurso de entrada no `netapp-acc` namespace (ou nome personalizado) usando o tipo de recurso `v1` para um esquema (`nginx-Ingress.yaml` é usado neste exemplo):

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

3. Aplicar as alterações:

```
kubectl apply -f nginx-Ingress.yaml
```



O NetApp recomenda a instalação do controlador nginx como uma implementação em vez de um `daemonSet`.

Passos para o controlador OpenShift Ingress

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

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

Faça login na IU do Astra Control Center

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

Passos

1. Em um navegador, insira o FQDN (incluindo o `https://` prefixo) usado no `astraAddress` `astra_control_center.yaml` CR quando [Você instalou o Astra Control Center](#).
2. Aceite os certificados autoassinados, se 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.yaml` CR quando [Você instalou o Astra Control Center](#), seguido da senha de configuração inicial (`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 ["Suporte à 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 registros. Procure códigos de resposta da API na faixa 400 a 500. Eles indicam o lugar onde uma falha aconteceu.

Opções

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

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

- Para verificar a saída do Astra Control Center CR:

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

O que vem a seguir

- (Opcional) dependendo do seu ambiente, conclua a pós-instalação "[etapas de configuração](#)".
- Conclua a implantação executando "[tarefas de configuração](#)"o .

Configurar um gerenciador de cert externo

Se um gerenciador de cert já existir no cluster do Kubernetes, você precisará executar algumas etapas de pré-requisito para que o Astra Control Center não instale seu próprio gerenciador de cert.

Passos

1. Confirme se você tem um gerenciador cert instalado:

```
kubectl get pods -A | grep 'cert-manager'
```

Resposta da amostra:

```
cert-manager   essential-cert-manager-84446f49d5-sf2zd   1/1
Running        0      6d5h
cert-manager   essential-cert-manager-cainjector-66dc99cc56-9ldmt   1/1
Running        0      6d5h
cert-manager   essential-cert-manager-webhook-56b76db9cc-fjqrq     1/1
Running        0      6d5h
```

2. Crie um par de certificados/chaves para o `astraAddress` FQDN:

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout tls.key -out
tls.crt
```

Resposta da amostra:

```
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'tls.key'
```

3. Crie um segredo com arquivos gerados anteriormente:

```
kubectl create secret tls selfsigned-tls --key tls.key --cert tls.crt -n
<cert-manager-namespace>
```

Resposta da amostra:

```
secret/selfsigned-tls created
```

4. Crie um ClusterIssuer arquivo que seja **exatamente** a seguir, mas inclua o local do namespace onde seus cert-manager pods estão instalados:

```
apiVersion: cert-manager.io/v1
kind: ClusterIssuer
metadata:
  name: astra-ca-clusterissuer
  namespace: <cert-manager-namespace>
spec:
  ca:
    secretName: selfsigned-tls
```

```
kubectl apply -f ClusterIssuer.yaml
```

Resposta da amostra:

```
clusterissuer.cert-manager.io/astra-ca-clusterissuer created
```

5. Verifique se o ClusterIssuer foi apresentado corretamente. Ready deve ser True antes que você possa prosseguir:

```
kubectl get ClusterIssuer
```

Resposta da amostra:

NAME	READY	AGE
astra-ca-clusterissuer	True	9s

6. Preencha "[Processo de instalação do Astra Control Center](#)"o . Há um "[Etapa de configuração necessária para o cluster Astra Control Center YAML](#)" em que você altera o valor CRD para indicar que o gerenciador cert está instalado externamente. Você deve concluir esta etapa durante a instalação para que o Astra Control Center reconheça o gerenciador de cert externo.

Instale o Astra Control Center usando o OpenShift OperatorHub

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

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

Antes de começar

- * Pré-requisitos ambientais atendidos*: ["Antes de começar a instalação, prepare seu ambiente para a implantação do Astra Control Center"](#).
- * Operadores de cluster e serviços de API saudáveis*:
 - A partir do cluster OpenShift, certifique-se de que todos os operadores de cluster estão em um estado saudável:

```
oc get clusteroperators
```

- A partir do cluster OpenShift, certifique-se de que todos os serviços de API estão em um estado saudável:

```
oc get apiservices
```

- **Endereço FQDN**: Obtenha um endereço FQDN para o Astra Control Center em seu data center.
- **Permissões OpenShift**: Obtenha as permissões necessárias e o acesso à Red Hat OpenShift Container Platform para executar as etapas de instalação descritas.
- **Gerenciador de cert configurado**: Se um gerenciador de cert já existir no cluster, você precisará executar alguns ["etapas de pré-requisito"](#) para que o Astra Control Center não instale seu próprio gerenciador de cert. Por padrão, o Astra Control Center instala seu próprio gerenciador de cert durante a instalação.
- * Controlador de entrada de Kubernetes*: Se você tiver uma controladora de entrada de Kubernetes que gerencia o acesso externo a serviços, como balanceamento de carga em um cluster, será necessário configurá-la para uso com o Astra Control Center:
 - a. Crie o namespace do operador:

```
oc create namespace netapp-acc-operator
```

- b. ["Conclua a configuração"](#) para o seu tipo de controlador de entrada.

Passos

- [Faça download e extraia Astra Control Center](#)
- [Instale o plug-in NetApp Astra kubectl](#)
- [Adicione as imagens ao seu registo local](#)

- [Localize a página de instalação do operador](#)
- [Instale o operador](#)
- [Instale o Astra Control Center](#)

Faça download e extraia Astra Control Center

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

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

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

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

4. Extraia as imagens do pacote Astra Control Center:

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

Instale o plug-in NetApp Astra kubectl

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

Antes de começar

O NetApp fornece binários de plug-in para diferentes arquiteturas de CPU e sistemas operacionais. Você precisa saber qual CPU e sistema operacional você tem antes de executar esta tarefa.

Passos

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



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

```
ls kubectl-astra/
```

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

```
cp kubect1-astra/<binary-name> /usr/local/bin/kubect1-astra
```

Adicione as imagens ao seu registo local

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

Docker

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

```
acc.manifest.bundle.yaml
acc/
```

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

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

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

Podman

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

```
acc.manifest.bundle.yaml
acc/
```

2. Inicie sessão no seu registro:

```
podman login <YOUR_REGISTRY>
```

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

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

```

export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=23.04.2-7
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //'')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*/::')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done

```

Podman 3

```

export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=23.04.2-7
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //'')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*/::')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done

```



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

```

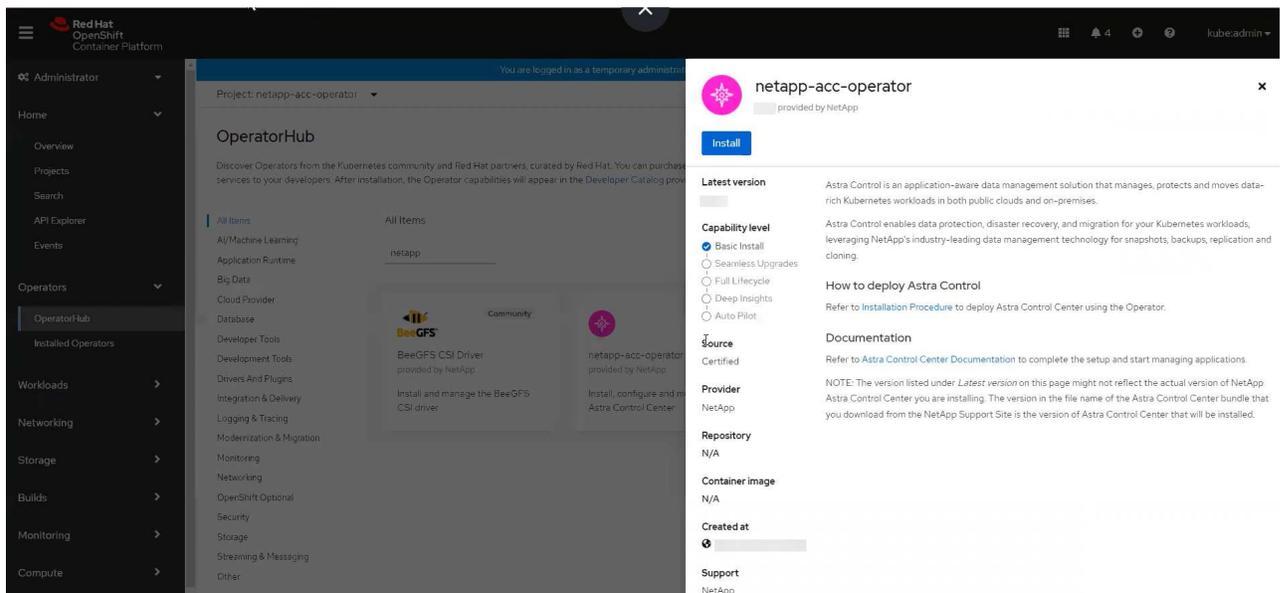
https://netappdownloads.jfrog.io/docker-astra-control-
prod/netapp/astra/acc/23.04.2-7/image:version

```

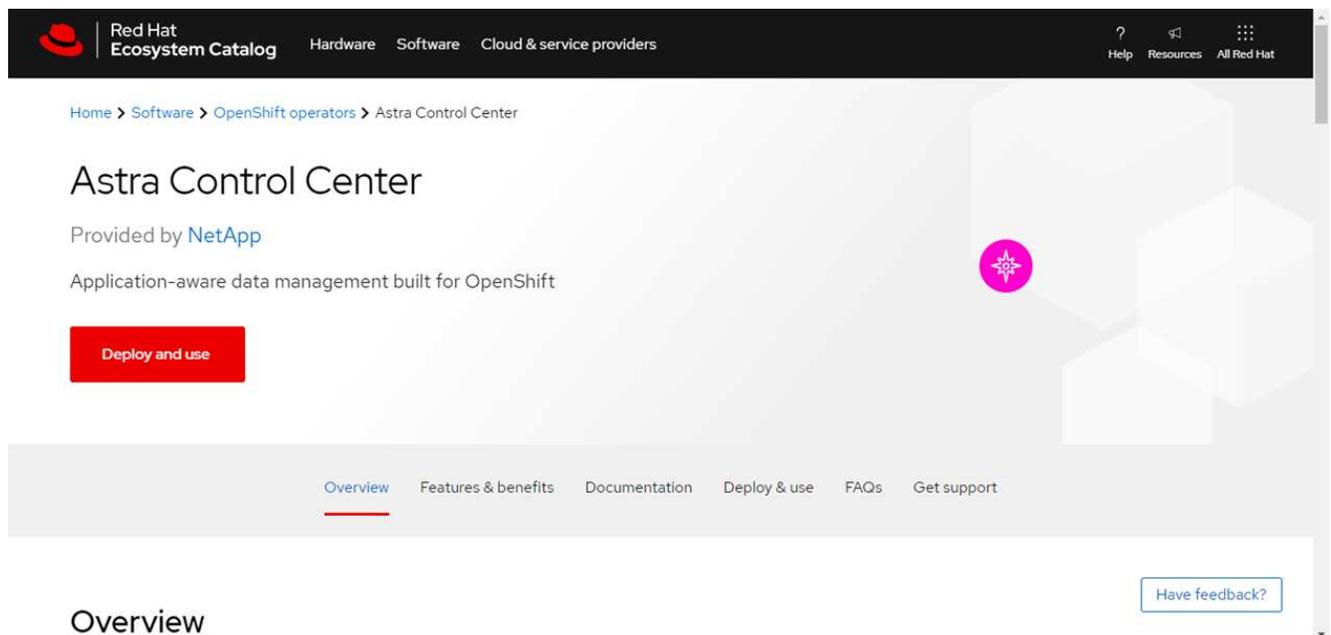
Localize a página de instalação do operador

1. Execute um dos seguintes procedimentos para acessar a página de instalação do operador:

- A partir do console web Red Hat OpenShift:
 - i. Faça login na IU da OpenShift Container Platform.
 - ii. No menu lateral, selecione **operadores > OperatorHub**.
 - iii. Procure e selecione o operador do Centro de Controle NetApp Astra.



- No Red Hat Ecosystem Catalog:
 - i. Seleção o Centro de Controle NetApp Astra "operador" .
 - ii. Seleção **Deploy and use**.



Instale o operador

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



O operador estará disponível em todos os namespaces de cluster.

- a. Selecione o namespace do operador ou `netapp-acc-operator` o namespace será criado automaticamente como parte da instalação do operador.
- b. Selecione uma estratégia de aprovação manual ou automática.



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

- c. Selecione **Instalar**.



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

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

Instale o Astra Control Center

1. No console dentro da guia **Astra Control Center** do operador Astra Control Center, selecione **Create AstraControlCenter**.

Project: netapp-acc-operator

Installed Operators > Operator details

netapp-acc-operator
23.4.0 provided by NetApp

Actions

Details YAML Subscription Events Astra Control Center

AstraControlCenters Show operands in: All namespaces Current namespace only [Create AstraControlCenter](#)

No operands found

Operands are declarative components used to define the behavior of the application.

2. Preencha o `Create AstraControlCenter` campo do formulário:
 - a. Mantenha ou ajuste o nome do Astra Control Center.
 - b. Adicione etiquetas para o Astra Control Center.
 - c. Ative ou desative o suporte automático. Recomenda-se a manutenção da funcionalidade de suporte automático.
 - d. Insira o FQDN ou o endereço IP do Centro de Controle Astra. Não introduza `http://` ou `https://` no campo de endereço.
 - e. Digite a versão do Astra Control Center; por exemplo, `23.04.2-7`.
 - f. Insira um nome de conta, endereço de e-mail e sobrenome do administrador.
 - g. Escolha uma política de recuperação de volume de `Retain`, `Recycle` ou `Delete`. O valor padrão é `Retain`.
 - h. Selecione o `scaleSize` da instalação.



Por padrão, o Astra usará alta disponibilidade (HA `scaleSize`) do `Medium`, que implanta a maioria dos serviços no HA e implanta várias réplicas para redundância. Com `scaleSize` as `Small`, o Astra reduzirá o número de réplicas para todos os serviços, exceto para serviços essenciais para reduzir o consumo.

i. Selecione o tipo de entrada:

▪ **Generic**(`ingressType: "Generic"`) (Predefinição)

Utilize esta opção quando tiver outro controlador de entrada em utilização ou preferir utilizar o seu próprio controlador de entrada. Depois que o Astra Control Center for implantado, você precisará configurar o "[controlador de entrada](#)" para expor o Astra Control Center com um URL.

▪ **AccTraefik**(`ingressType: "AccTraefik"`)

Utilize esta opção quando preferir não configurar um controlador de entrada. Isso implanta o gateway Astra Control Center `traefik` como um serviço do tipo "LoadBalancer" do Kubernetes.

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



Para obter detalhes sobre o tipo de serviço "LoadBalancer" e Ingress, "[Requisitos](#)" consulte .

- a. Em **Image Registry**, insira seu caminho de Registro de imagem de contentor local. Não introduza `http://` ou `https://` no campo de endereço.
- b. Se utilizar um registo de imagens que necessite de autenticação, introduza o segredo da imagem.



Se você usar um Registro que requer autenticação, [crie um segredo no cluster](#).

- c. Introduza o nome do administrador.
- d. Configurar o dimensionamento de recursos.
- e. Forneça a classe de armazenamento padrão.



Se uma classe de armazenamento padrão estiver configurada, certifique-se de que é a única classe de armazenamento que tem a anotação padrão.

f. Definir preferências de tratamento de CRD.

3. Selecione a vista YAML para rever as definições selecionadas.
4. `Create` Selecione .

Crie um segredo de Registro

Se você usar um Registro que requer autenticação, crie um segredo no cluster OpenShift e insira o nome secreto no `Create AstraControlCenter` campo formulário.

1. Crie um namespace para o operador Astra Control Center:

```
oc create ns [netapp-acc-operator or custom namespace]
```

2. Crie um segredo neste namespace:

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



O Astra Control suporta apenas segredos de registo do Docker.

3. Preencha os campos restantes em [O campo criar formulário AstraControlCenter](#).

O que vem a seguir

Preencha o "[passos restantes](#)" para verificar se o Astra Control Center foi instalado com sucesso, configure um controlador de entrada (opcional) e faça login na IU. Além disso, você precisará executar "[tarefas de configuração](#)" depois de concluir a instalação.

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

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

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

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

- [Implante o Astra Control Center na Amazon Web Services](#)
- [Implante o Astra Control Center no Google Cloud Platform](#)
- [Implante o Astra Control Center no Microsoft Azure](#)

Você pode gerenciar seus aplicativos em distribuições com clusters do Kubernetes autogerenciados, como o OpenShift Container Platform (OCP). Somente clusters de OCP autogeridos são validados para implantar o Astra Control Center.

Implante o Astra Control Center na Amazon Web Services

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

O que você precisará para a AWS

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

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

Requisitos de ambiente operacional para a AWS

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

- Red Hat OpenShift Container Platform 4,8



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

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

Componente	Requisito
Capacidade de storage do NetApp Cloud Volumes ONTAP no back-end	Pelo menos 300GB disponível
Nós de trabalho (requisito AWS EC2)	No total, pelo menos 3 nós de trabalho, com 4 núcleos vCPU e 12GB GB de RAM cada
Balancedor de carga	Tipo de serviço "LoadBalancer" disponível para envio de tráfego de entrada para serviços no cluster do ambiente operacional
FQDN	Um método para apontar o FQDN do Astra Control Center para o endereço IP balanceado de carga
Astra Trident (instalado como parte da descoberta de clusters do Kubernetes no NetApp BlueXP , anteriormente chamado Gerenciador de nuvem)	Astra Trident 21,04 ou mais recente instalado e configurado e o NetApp ONTAP versão 9,5 ou mais recente como um back-end de storage

Componente	Requisito
Registo de imagens	<p>Você precisa ter um Registro privado existente, como o AWS Elastic Container Registry, para o qual você pode enviar imagens de compilação do Astra Control Center. Você precisa fornecer o URL do Registro de imagens onde você vai carregar as imagens.</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;">  <p>O cluster hospedado do Astra Control Center e o cluster gerenciado devem ter acesso ao mesmo Registro de imagem para poder fazer backup e restaurar aplicativos usando a imagem baseada em Restic.</p> </div>
Configuração Astra Trident/ONTAP	<p>O Astra Control Center exige que uma classe de storage seja criada e definida como a classe de storage padrão. O Astra Control Center é compatível com as seguintes classes de storage do ONTAP Kubernetes criadas quando você importa o cluster do Kubernetes para o NetApp BlueXP (anteriormente conhecido como Cloud Manager). Eles são fornecidos pelo Astra Trident:</p> <ul style="list-style-type: none"> • <code>vsaworkingenvironment-<>-ha-nas</code> <code>csi.trident.netapp.io</code> • <code>vsaworkingenvironment-<>-ha-san</code> <code>csi.trident.netapp.io</code> • <code>vsaworkingenvironment-<>-single-nas</code> <code>csi.trident.netapp.io</code> • <code>vsaworkingenvironment-<>-single-san</code> <code>csi.trident.netapp.io</code>



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



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

Visão geral da implantação para AWS

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

Cada uma destas etapas é explicada em mais detalhes abaixo.

1. [Certifique-se de que tem permissões IAM suficientes.](#)
2. [Instale um cluster RedHat OpenShift na AWS.](#)
3. [Configurar a AWS.](#)
4. [Configure o NetApp BlueXP para AWS.](#)
5. [Instalar o Astra Control Center for AWS.](#)

Certifique-se de que tem permissões IAM suficientes

Certifique-se de que você tenha funções e permissões suficientes do IAM que permitam instalar um cluster do RedHat OpenShift e um conector do NetApp BlueXP (antigo Gerenciador de nuvem).

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

Instale um cluster RedHat OpenShift na AWS

Instale um cluster do RedHat OpenShift Container Platform na AWS.

Para obter instruções de instalação, "[Instalar um cluster na AWS no OpenShift Container Platform](#)" consulte .

Configurar a AWS

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

Siga a documentação da AWS para concluir as etapas a seguir. "[Documentação de instalação da AWS](#)"Consulte .

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



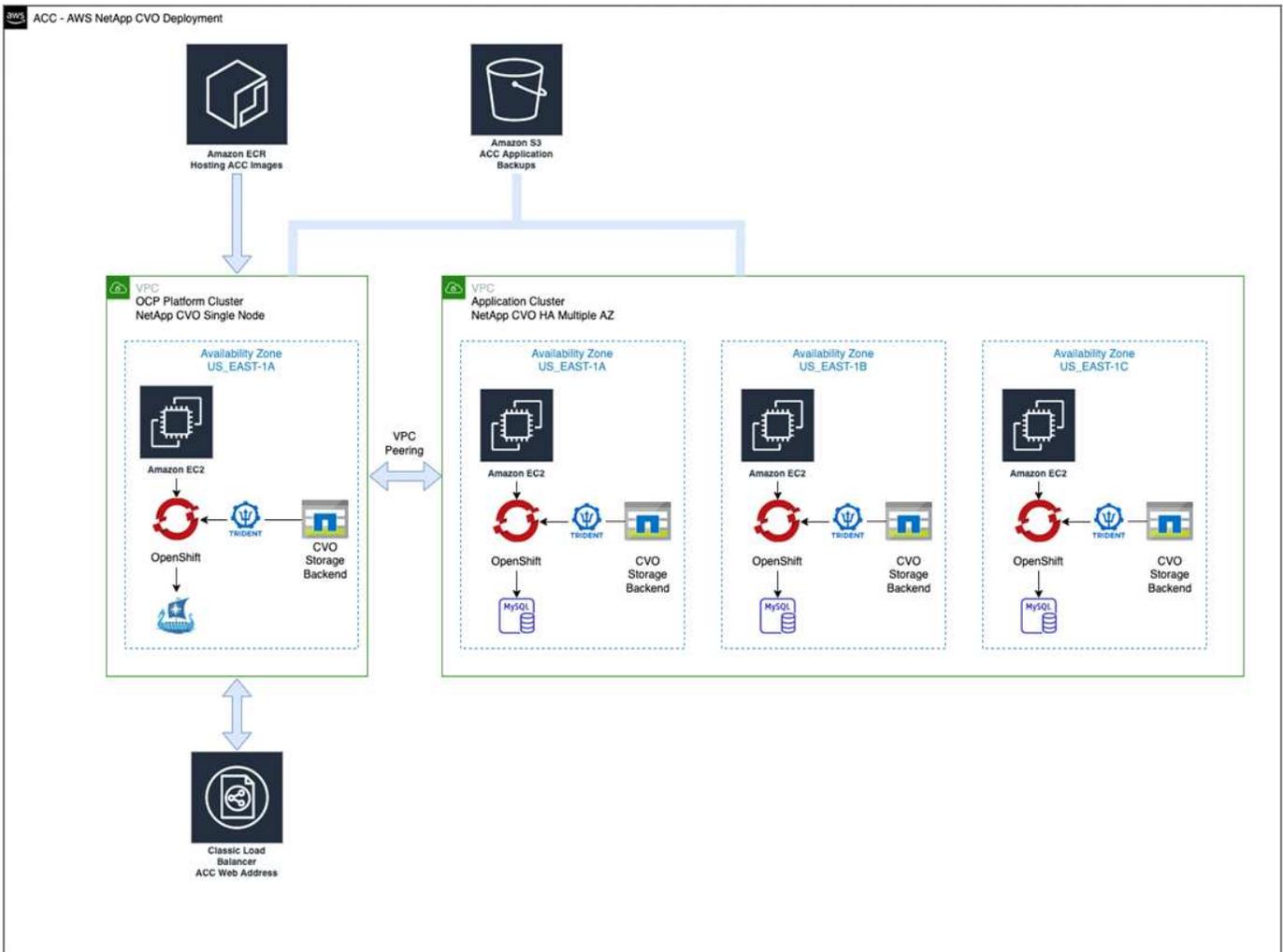
Se você não criar o ECR, o Astra Control Center não poderá acessar dados de monitoramento de um cluster que contém o Cloud Volumes ONTAP com um back-end da AWS. O problema é causado quando o cluster que você tenta descobrir e gerenciar usando o Astra Control Center não tem acesso ao AWS ECR.

6. Envie as imagens ACC para o registro definido.



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

Veja um exemplo de implantação da AWS:



Configure o NetApp BlueXP para AWS

Usando o NetApp BlueXP, crie uma área de trabalho, adicione um conector à AWS, crie um ambiente de trabalho e importe o cluster.

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

- ["Introdução ao Cloud Volumes ONTAP na AWS"](#).
- ["Crie um conector na AWS usando o BlueXP"](#)

Passos

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

- b. No canto superior direito, observe a versão Astra Trident.
- c. Observe as classes de storage de cluster do Cloud Volumes ONTAP que mostram o NetApp como o provisionador.

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

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



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

Instalar o Astra Control Center for AWS

Siga o padrão "[Instruções de instalação do Astra Control Center](#)".



A AWS usa o tipo de bucket Generic S3.

Implante o Astra Control Center no Google Cloud Platform

É possível implantar o Astra Control Center em um cluster autogerenciado do Kubernetes hospedado em uma nuvem pública do Google Cloud Platform (GCP).

O que você precisará para o GCP

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

- Licença do Astra Control Center. "[Requisitos de licenciamento do Astra Control Center](#)" Consulte a .
- "[Atender aos requisitos do Astra Control Center](#)".
- Conta do NetApp Cloud Central
- Se estiver usando OCP, Red Hat OpenShift Container Platform (OCP) 4,10
- Se estiver usando OCP, permissões do Red Hat OpenShift Container Platform (OCP) (no nível do namespace para criar pods)
- Conta de serviço do GCP com permissões que permitem criar buckets e conetores

Requisitos do ambiente operacional do GCP



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

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

Componente	Requisito
Capacidade de storage do NetApp Cloud Volumes ONTAP no back-end	Pelo menos 300GB disponível

Componente	Requisito
Nós de trabalho (requisito de computação do GCP)	No total, pelo menos 3 nós de trabalho, com 4 núcleos vCPU e 12GB GB de RAM cada
Balancedor de carga	Tipo de serviço "LoadBalancer" disponível para envio de tráfego de entrada para serviços no cluster do ambiente operacional
FQDN (ZONA DNS DO GCP)	Um método para apontar o FQDN do Astra Control Center para o endereço IP balanceado de carga
Astra Trident (instalado como parte da descoberta de clusters do Kubernetes no NetApp BlueXP , anteriormente chamado Gerenciador de nuvem)	Astra Trident 21,04 ou mais recente instalado e configurado e o NetApp ONTAP versão 9,5 ou mais recente como um back-end de storage
Registo de imagens	<p>Você deve ter um Registro privado existente, como o Google Container Registry, para o qual você pode enviar imagens de compilação do Astra Control Center. Você precisa fornecer o URL do Registro de imagens onde você vai carregar as imagens.</p> <div style="display: flex; align-items: center; margin-top: 10px;">  <p>Você precisa habilitar o acesso anônimo para extrair imagens Restic para backups.</p> </div>
Configuração Astra Trident/ONTAP	<p>O Astra Control Center exige que uma classe de storage seja criada e definida como a classe de storage padrão. O Astra Control Center é compatível com as seguintes classes de storage do ONTAP Kubernetes criadas quando você importa o cluster do Kubernetes para o NetApp BlueXP . Eles são fornecidos pelo Astra Trident:</p> <ul style="list-style-type: none"> • <code>vsaworkingenvironment-<>-ha-nas csi.trident.netapp.io</code> • <code>vsaworkingenvironment-<>-ha-san csi.trident.netapp.io</code> • <code>vsaworkingenvironment-<>-single-nas csi.trident.netapp.io</code> • <code>vsaworkingenvironment-<>-single-san csi.trident.netapp.io</code>



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

Visão geral da implantação do GCP

Veja a seguir uma visão geral do processo de instalação do Astra Control Center em um cluster de OCP autogerenciado no GCP, com o Cloud Volumes ONTAP como um back-end de storage.

Cada uma destas etapas é explicada em mais detalhes abaixo.

1. [Instale um cluster RedHat OpenShift no GCP.](#)
2. [Crie um projeto do GCP e uma nuvem privada virtual.](#)
3. [Certifique-se de que tem permissões IAM suficientes.](#)
4. [Configurar o GCP.](#)
5. [Configurar o NetApp BlueXP para GCP.](#)
6. [Instalar o Astra Control Center no GCP.](#)

Instale um cluster RedHat OpenShift no GCP

A primeira etapa é instalar um cluster do RedHat OpenShift no GCP.

Para obter instruções de instalação, consulte o seguinte:

- ["Instalação de um cluster OpenShift no GCP"](#)
- ["Criando uma conta de serviço do GCP"](#)

Crie um projeto do GCP e uma nuvem privada virtual

Crie pelo menos um projeto do GCP e a Virtual Private Cloud (VPC).



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

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

Certifique-se de que tem permissões IAM suficientes

Certifique-se de que você tenha funções e permissões suficientes do IAM que permitam instalar um cluster do RedHat OpenShift e um conector do NetApp BlueXP (antigo Gerenciador de nuvem).

```
https://docs.netapp.com/us-en/cloud-manager-setup-admin/task-creating-connectors-gcp.html#setting-up-permissions["Credenciais e permissões iniciais do GCP"^]Consulte .
```

Configurar o GCP

Em seguida, configure o GCP para criar uma VPC, configurar instâncias de computação, criar um Google Cloud Object Storage, criar um Google Container Register para hospedar as imagens do Astra Control Center e enviar as imagens para esse Registro.

Siga a documentação do GCP para concluir as etapas a seguir. Consulte [Instalando o cluster OpenShift no GCP](#).

1. Crie um projeto do GCP e uma VPC no GCP que você planeja usar para o cluster do OCP com o back-end do CVO.
2. Revise as instâncias de computação. Isso pode ser um servidor bare metal ou VMs no GCP.

3. Se o tipo de instância ainda não corresponder aos requisitos mínimos de recursos do Astra para nós mestres e trabalhadores, altere o tipo de instância no GCP para atender aos requisitos do Astra. ["Requisitos do Astra Control Center"](#)Consulte a .
4. Crie pelo menos um bucket do GCP Cloud Storage para armazenar seus backups.
5. Crie um segredo, que é necessário para o acesso ao bucket.
6. Crie um Registro de contêiner do Google para hospedar todas as imagens do Astra Control Center.
7. Configure o acesso do Google Container Registry para push/pull do Docker para todas as imagens do Astra Control Center.

Exemplo: As imagens ACC podem ser enviadas para este registo introduzindo o seguinte script:

```
gcloud auth activate-service-account <service account email address>
--key-file=<GCP Service Account JSON file>
```

Este script requer um arquivo de manifesto Astra Control Center e sua localização do Registro de imagens do Google.

Exemplo:

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

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

8. Configurar zonas DNS.

Configurar o NetApp BlueXP para GCP

Usando o NetApp BlueXP , crie uma área de trabalho, adicione um conector ao GCP, crie um ambiente de trabalho e importe o cluster.

Siga a documentação do BlueXP para concluir as etapas a seguir. ["Introdução ao Cloud Volumes ONTAP no GCP"](#)Consulte .

Antes de começar

- Acesso à conta do serviço do GCP com as permissões e funções necessárias do IAM

Passos

1. Adicione suas credenciais ao BlueXP . ["Adicionando contas do GCP"](#)Consulte .

2. Adicione um conector para o GCP.
 - a. Escolha "GCP" como Provedor.
 - b. Insira as credenciais do GCP. ["Criando um conector no GCP a partir do BlueXP"](#)Consulte .
 - c. Certifique-se de que o conector está a funcionar e mude para esse conector.
3. Crie um ambiente de trabalho para seu ambiente de nuvem.
 - a. Localização: "GCP"
 - b. Tipo: "Cloud Volumes ONTAP HA"
4. Importe o cluster OpenShift. O cluster se conectará ao ambiente de trabalho que você acabou de criar.
 - a. Veja os detalhes do cluster do NetApp selecionando **K8s > Lista de clusters > Detalhes do cluster**.
 - b. No canto superior direito, observe a versão do Trident.
 - c. Observe as classes de storage de cluster do Cloud Volumes ONTAP que mostram "NetApp" como o provisionador.

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

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



O Cloud Volumes ONTAP pode operar como um nó único ou em alta disponibilidade (HA). Se a HA estiver ativada, observe o status de HA e o status de implantação de nós em execução no GCP.

Instalar o Astra Control Center no GCP

Siga o padrão ["Instruções de instalação do Astra Control Center"](#).



O GCP usa o tipo de bucket Generic S3.

1. Gere o segredo do Docker para extrair imagens para a instalação do Astra Control Center:

```
kubectl create secret docker-registry <secret name> --docker
-server=<Registry location> --docker-username=_json_key --docker
-password="$(cat <GCP Service Account JSON file>)" --namespace=pcloud
```

Implante o Astra Control Center no Microsoft Azure

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

O que você precisará para o Azure

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

- Licença do Astra Control Center. ["Requisitos de licenciamento do Astra Control Center"](#)Consulte a .
- ["Atender aos requisitos do Astra Control Center"](#).

- Conta do NetApp Cloud Central
- Se estiver usando OCP, Red Hat OpenShift Container Platform (OCP) 4,8
- Se estiver usando OCP, permissões do Red Hat OpenShift Container Platform (OCP) (no nível do namespace para criar pods)
- Credenciais do Azure com permissões que permitem criar buckets e conetores

Requisitos de ambiente operacional para o Azure

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

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

"[Requisitos do ambiente operacional do Astra Control Center](#)"Consulte a .

Componente	Requisito
Capacidade de storage do NetApp Cloud Volumes ONTAP no back-end	Pelo menos 300GB disponível
Nós de trabalho (requisito de computação do Azure)	No total, pelo menos 3 nós de trabalho, com 4 núcleos vCPU e 12GB GB de RAM cada
Balancedor de carga	Tipo de serviço "LoadBalancer" disponível para envio de tráfego de entrada para serviços no cluster do ambiente operacional
FQDN (zona DNS do Azure)	Um método para apontar o FQDN do Astra Control Center para o endereço IP balanceado de carga
Astra Trident (instalado como parte da descoberta de clusters do Kubernetes no NetApp BlueXP)	O Astra Trident 21,04 ou mais recente instalado e configurado e o NetApp ONTAP versão 9,5 ou mais recente serão usados como um back-end de storage
Registo de imagens	<p>Você deve ter um Registro privado existente, como o Azure Container Registry (ACR), para o qual você pode enviar imagens de compilação do Astra Control Center. Você precisa fornecer o URL do Registro de imagens onde você vai carregar as imagens.</p> <div style="display: flex; align-items: center;">  <p>Você precisa habilitar o acesso anônimo para extrair imagens Restic para backups.</p> </div>

Componente	Requisito
Configuração Astra Trident/ONTAP	<p>O Astra Control Center exige que uma classe de storage seja criada e definida como a classe de storage padrão. O Astra Control Center é compatível com as seguintes classes de storage do ONTAP Kubernetes criadas quando você importa o cluster do Kubernetes para o NetApp BlueXP . Eles são fornecidos pelo Astra Trident:</p> <ul style="list-style-type: none"> • <code>vsaworkingenvironment-<>-ha-nas</code> <code>csi.trident.netapp.io</code> • <code>vsaworkingenvironment-<>-ha-san</code> <code>csi.trident.netapp.io</code> • <code>vsaworkingenvironment-<>-single-nas</code> <code>csi.trident.netapp.io</code> • <code>vsaworkingenvironment-<>-single-san</code> <code>csi.trident.netapp.io</code>



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

Visão geral da implantação para o Azure

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

Cada uma destas etapas é explicada em mais detalhes abaixo.

1. [Instale um cluster RedHat OpenShift no Azure.](#)
2. [Criar grupos de recursos do Azure.](#)
3. [Certifique-se de que tem permissões IAM suficientes.](#)
4. [Configurar o Azure.](#)
5. [Configure o NetApp BlueXP \(anteriormente Gerenciador de nuvem\) para Azure.](#)
6. [Instalar e configurar o Astra Control Center para Azure.](#)

Instale um cluster RedHat OpenShift no Azure

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

Para obter instruções de instalação, consulte o seguinte:

- ["Instalando o cluster OpenShift no Azure"](#).
- ["Instalando uma conta do Azure"](#).

Criar grupos de recursos do Azure

Crie pelo menos um grupo de recursos do Azure.



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

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

Certifique-se de que tem permissões IAM suficientes

Verifique se você tem funções e permissões suficientes do IAM que permitem instalar um cluster do RedHat OpenShift e um NetApp BlueXP Connector.

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

Configurar o Azure

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

Siga a documentação do Azure para concluir as etapas a seguir. ["Instalando o cluster OpenShift no Azure"](#)Consulte .

1. Crie uma rede virtual do Azure.
2. Revise as instâncias de computação. Isso pode ser um servidor bare metal ou VMs no Azure.
3. Se o tipo de instância ainda não corresponder aos requisitos mínimos de recursos do Astra para nós mestres e trabalhadores, altere o tipo de instância no Azure para atender aos requisitos do Astra. ["Requisitos do Astra Control Center"](#)Consulte a .
4. Crie pelo menos um contêiner do Blob do Azure para armazenar seus backups.
5. Crie uma conta de armazenamento. Você precisará de uma conta de storage para criar um contêiner para ser usado como um bucket no Astra Control Center.
6. Crie um segredo, que é necessário para o acesso ao bucket.
7. Crie um ACR (Azure Container Registry) para hospedar todas as imagens do Astra Control Center.
8. Configure o acesso ACR para o Docker push/pull de todas as imagens do Astra Control Center.
9. Empurre as imagens ACC para este registo introduzindo o seguinte script:

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

Exemplo:

```

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

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

```

10. Configurar zonas DNS.

Configure o NetApp BlueXP (anteriormente Gerenciador de nuvem) para Azure

Usando o BlueXP (antigo Gerenciador de nuvem), crie uma área de trabalho, adicione um conector ao Azure, crie um ambiente de trabalho e importe o cluster.

Siga a documentação do BlueXP para concluir as etapas a seguir. ["Introdução ao BlueXP no Azure"](#) Consulte

Antes de começar

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

Passos

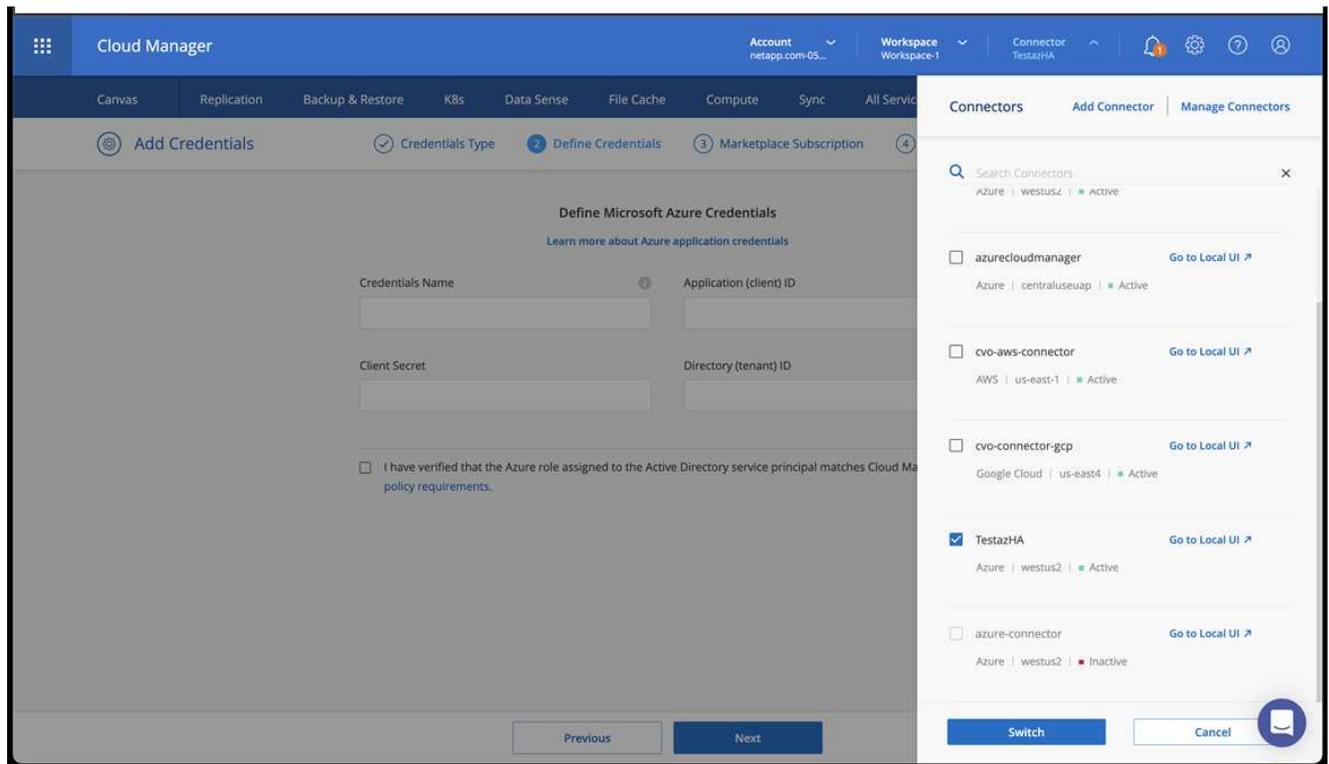
1. Adicione suas credenciais ao BlueXP .
2. Adicione um conector para o Azure. ["Políticas da BlueXP"](#)Consulte .
 - a. Escolha **Azure** como Provedor.
 - b. Insira as credenciais do Azure, incluindo o ID do aplicativo, o segredo do cliente e o ID do diretório (locatário).

```

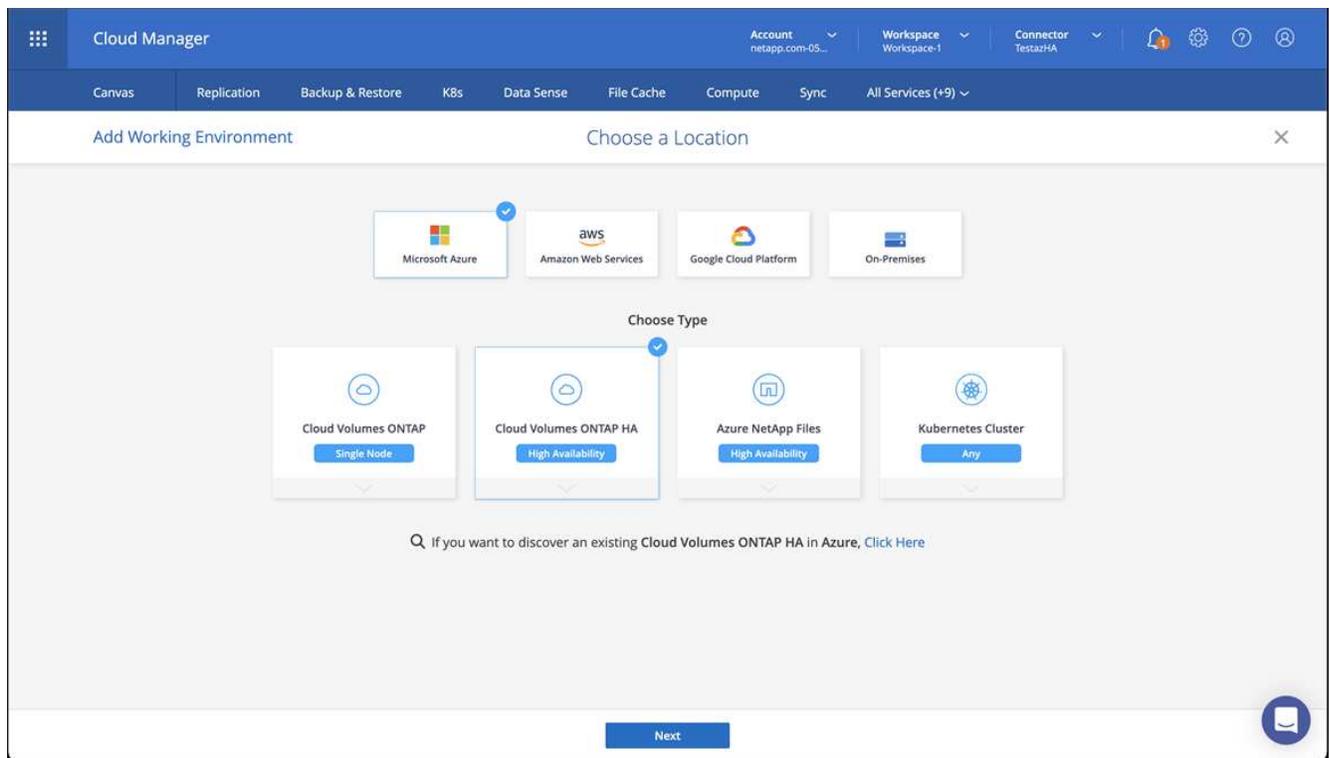
https://docs.netapp.com/us-
en/occm/task_creating_connectors_azure.html["Criando um conector no
Azure a partir do BlueXP"]Consulte .

```

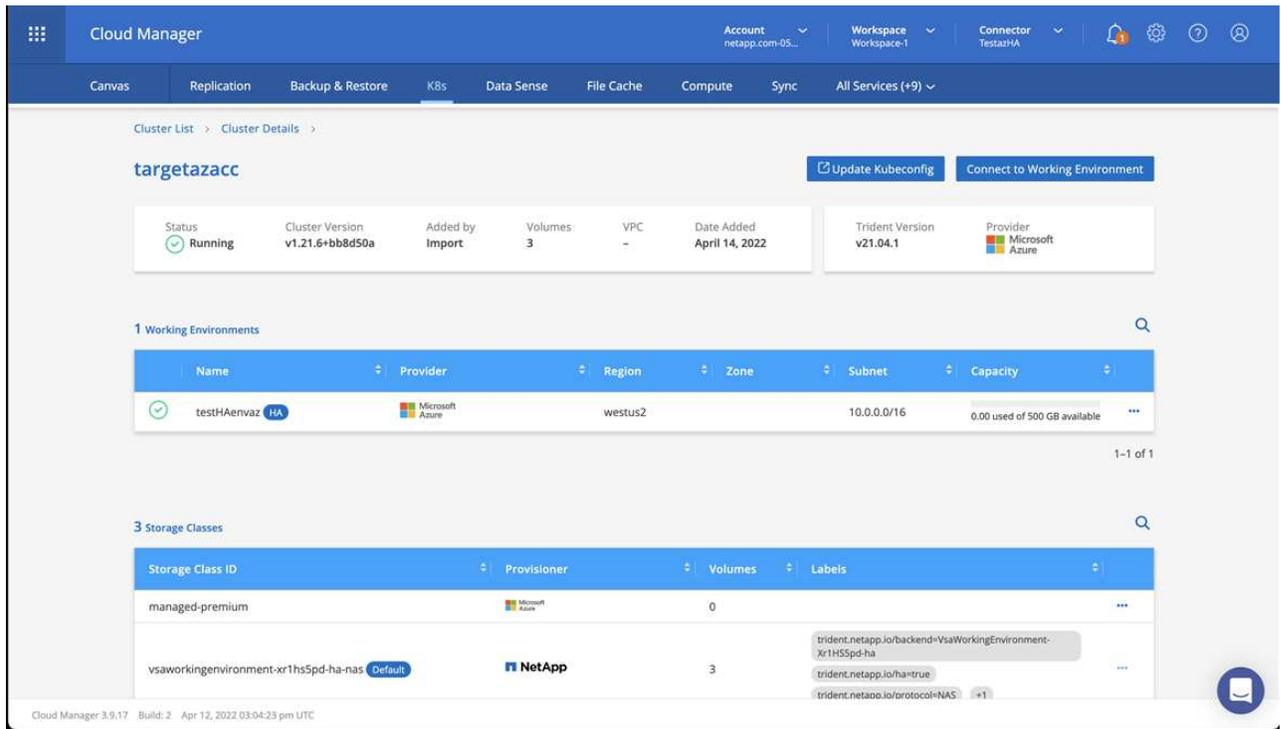
3. Certifique-se de que o conector está a funcionar e mude para esse conector.



4. Crie um ambiente de trabalho para seu ambiente de nuvem.
 - a. Localização: "Microsoft Azure".
 - b. Tipo: "Cloud Volumes ONTAP HA".



5. Importe o cluster OpenShift. O cluster se conetará ao ambiente de trabalho que você acabou de criar.
 - a. Veja os detalhes do cluster do NetApp selecionando **K8s > Lista de clusters > Detalhes do cluster**.



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

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

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

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

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

Instalar e configurar o Astra Control Center para Azure

Instalar o Astra Control Center com o padrão "[instruções de instalação](#)".

Usando o Astra Control Center, adicione um bucket do Azure. "[Configure o Astra Control Center e adicione buckets](#)" Consulte a .

Configure o Astra Control Center após a instalação

Dependendo do seu ambiente, pode haver configuração adicional necessária após a instalação do Astra Control Center.

Remover limitações de recursos

Alguns ambientes usam os objetos ResourceQuotes e LimitRanges para impedir que os recursos em um namespace consumam toda a CPU e memória disponíveis no cluster. O Astra Control Center não define limites máximos, por isso não estará em conformidade com esses recursos. Se o seu ambiente estiver configurado dessa forma, você precisará remover esses recursos dos namespaces onde você planeja instalar o Astra Control Center.

Você pode usar as etapas a seguir para recuperar e remover essas cotas e limites. Nestes exemplos, a saída do comando é mostrada imediatamente após o comando.

Passos

1. Obtenha as cotas de recursos no `netapp-acc` namespace (ou nome personalizado):

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

Resposta:

```
NAME          AGE   REQUEST                                     LIMIT
pods-high     16s   requests.cpu: 0/20, requests.memory: 0/100Gi
limits.cpu: 0/200, limits.memory: 0/1000Gi
pods-low      15s   requests.cpu: 0/1, requests.memory: 0/1Gi
limits.cpu: 0/2, limits.memory: 0/2Gi
pods-medium   16s   requests.cpu: 0/10, requests.memory: 0/20Gi
limits.cpu: 0/20, limits.memory: 0/200Gi
```

2. Excluir todas as cotas de recursos por nome:

```
kubectl delete resourcequota pods-high -n [netapp-acc or custom namespace]
```

```
kubectl delete resourcequota pods-low -n [netapp-acc or custom namespace]
```

```
kubectl delete resourcequota pods-medium -n [netapp-acc or custom namespace]
```

3. Obtenha os intervalos de limite no `netapp-acc` namespace (ou nome personalizado):

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

Resposta:

```
NAME             CREATED AT
cpu-limit-range  2022-06-27T19:01:23Z
```

4. Eliminar os intervalos de limite por nome:

```
kubectl delete limitrange cpu-limit-range -n [netapp-acc or custom namespace]
```

Ative a comunicação de rede entre namespaces

Alguns ambientes usam construções NetworkPolicy para restringir o tráfego entre namespaces. O operador Astra Control Center e o Astra Control Center estão em diferentes namespaces. Os serviços nesses diferentes namespaces precisam ser capazes de se comunicar uns com os outros. Para ativar esta comunicação, siga estes passos.

Passos

1. Exclua todos os recursos da NetworkPolicy que existem no namespace Astra Control Center:

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

2. Para cada objeto NetworkPolicy retornado pelo comando anterior, use o seguinte comando para excluí-lo. Substitua [OBJECT_NAME] pelo nome do objeto retornado:

```
kubectl delete networkpolicy [OBJECT_NAME] -n [netapp-acc or custom namespace]
```

3. Aplique o seguinte arquivo de recurso para configurar o `acc-avp-network-policy` objeto para permitir que os serviços de plug-in Astra façam solicitações aos serviços do Astra Control Center. Substitua as informações entre parêntesis > por informações do seu ambiente:

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: acc-avp-network-policy
  namespace: <ACC_NAMESPACE_NAME> # REPLACE THIS WITH THE ASTRA CONTROL
CENTER NAMESPACE NAME
spec:
  podSelector: {}
  policyTypes:
    - Ingress
  ingress:
    - from:
      - namespaceSelector:
          matchLabels:
            kubernetes.io/metadata.name: <PLUGIN_NAMESPACE_NAME> #
REPLACE THIS WITH THE ASTRA PLUGIN NAMESPACE NAME
```

4. Aplique o seguinte arquivo de recurso para configurar o `acc-operator-network-policy` objeto para

permitir que o operador Astra Control Center se comunique com os serviços Astra Control Center. Substitua as informações entre parêntesis> por informações do seu ambiente:

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: acc-operator-network-policy
  namespace: <ACC_NAMESPACE_NAME> # REPLACE THIS WITH THE ASTRA CONTROL
CENTER NAMESPACE NAME
spec:
  podSelector: {}
  policyTypes:
    - Ingress
  ingress:
    - from:
      - namespaceSelector:
          matchLabels:
            kubernetes.io/metadata.name: <NETAPP-ACC-OPERATOR> #
REPLACE THIS WITH THE OPERATOR NAMESPACE NAME
```

Adicione um certificado TLS personalizado

O Astra Control Center usa um certificado TLS autoassinado por padrão para o tráfego do controlador de entrada (somente em certas configurações) e autenticação da IU da Web com navegadores da Web. Você pode remover o certificado TLS autoassinado existente e substituí-lo por um certificado TLS assinado por uma autoridade de certificação (CA).

O certificado auto-assinado padrão é usado para dois tipos de conexões:

- Conexões HTTPS com a IU da Web do Astra Control Center
- Tráfego do controlador de entrada (somente se a `ingressType: "AccTraefik"` propriedade foi definida no `astra_control_center.yaml` arquivo durante a instalação do Astra Control Center)



A substituição do certificado TLS padrão substitui o certificado usado para autenticação dessas conexões.

Antes de começar

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

Remova o certificado autoassinado

Remova o certificado TLS autoassinado existente.

1. Usando SSH, faça login no cluster do Kubernetes que hospeda o Astra Control Center como usuário

administrativo.

2. Localize o segredo TLS associado ao certificado atual usando o seguinte comando, substituindo <ACC-deployment-namespace> pelo namespace de implantação do Astra Control Center:

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

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

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

Adicione um novo certificado usando a linha de comando

Adicione um novo certificado TLS assinado por uma CA.

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

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

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

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

#spec:
# selfSigned: {}

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

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

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

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

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

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

5. Crie o certificado usando o seguinte comando:

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

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

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

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

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

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

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

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

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

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, habilitar a autenticação, gerenciar armazenamento e adicionar buckets.

Tarefas

- [Adicione uma licença para o Astra Control Center](#)
- [Prepare seu ambiente para gerenciamento de clusters com o Astra Control](#)
- [Adicionar cluster](#)
- [Ativar a autenticação no back-end de storage do ONTAP](#)
- [Adicionar um back-end de storage](#)
- [Adicione um balde](#)

Adicione uma licença para o Astra Control Center

Quando você instala o Astra Control Center, uma licença de avaliação incorporada já está instalada. Se você estiver avaliando o Astra Control Center, ignore esta etapa.

Você pode adicionar uma nova licença usando a IU do Astra Control ou ["API"](#)o .

As licenças do Astra Control Center medem recursos de CPU usando unidades de CPU Kubernetes e contam os recursos de CPU atribuídos aos nós de trabalho de todos os clusters gerenciados do Kubernetes. As

licenças são baseadas no uso do vCPU. Para obter mais informações sobre como as licenças são calculadas, "[Licenciamento](#)" consulte .



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



Para atualizar uma avaliação existente ou uma licença completa, "[Atualizar uma licença existente](#)" consulte .

Antes de começar

- Acesso a uma instância recém-instalada do Astra Control Center.
- Permissões de função de administrador.
- A "[Ficheiro de licença do NetApp](#)" (NLF).

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 e não estiver enviando dados para o AutoSupport, lembre-se de armazenar o ID da conta para evitar a perda de dados em caso de falha do Centro de Controle Astra.

Prepare seu ambiente para gerenciamento de clusters com o Astra Control

Você deve garantir que as seguintes condições de pré-requisito sejam atendidas antes de adicionar um cluster. Você também deve executar verificações de qualificação para garantir que seu cluster esteja pronto para ser adicionado ao Astra Control Center e criar funções para gerenciamento de clusters.

Antes de começar

- Verifique se os nós de trabalho no cluster estão configurados com os drivers de armazenamento apropriados para que os pods possam interagir com o armazenamento de back-end.
- Seu ambiente atende ao "[requisitos do ambiente operacional](#)" Astra Trident e Astra Control Center.
- Uma versão do Astra Trident "[Compatível com Astra Control Center](#)" instalada:



Você pode "[Implante o Astra Trident](#)" usar o operador Astra Trident (manualmente ou usando o gráfico Helm) ou `tridentctl`. Antes de instalar ou atualizar o Astra Trident, revise o "[interfaces suportadas, backends e configurações de host](#)".

- **Back-end de storage do Astra Trident configurado:** Pelo menos um back-end de storage do Astra Trident precisa estar "[configurado](#)" no cluster.

- **Classes de storage Astra Trident configuradas:** Pelo menos uma classe de storage Astra Trident deve estar "**configurado**" no cluster. Se uma classe de armazenamento padrão estiver configurada, certifique-se de que é a única classe de armazenamento que tem a anotação padrão.
- **Controlador de volume e classe de snapshot de volume Astra Trident instalado e configurado:** A controladora de volume deve ser "**instalado**" para que os snapshots possam ser criados no Astra Control. Pelo menos um Astra Trident `VolumeSnapshotClass` foi "**configuração**" feito por um administrador.
- **Kubeconfig acessível:** Você tem acesso ao "**cluster kubeconfig**" que inclui apenas um elemento de contexto.
- *** Credenciais ONTAP*:** Você precisa de credenciais ONTAP e um superusuário e ID de usuário definidos no sistema ONTAP de backup para fazer backup e restaurar aplicativos com o Astra Control Center.

Execute os seguintes comandos na linha de comando ONTAP:

```
export-policy rule modify -vserver <storage virtual machine name>
-policyname <policy name> -ruleindex 1 -superuser sys
export-policy rule modify -vserver <storage virtual machine name>
-policyname <policy name> -ruleindex 1 -anon 65534
```

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

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 Astra Trident.

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

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

```
NAME          VERSION
trident       22.10.0
```

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

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



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

2. Certifique-se de que os pods estão em execução:

```
kubectl get pods -n trident
```

3. Determine se as classes de storage estão usando os drivers Astra Trident compatíveis. O nome do provisionador deve ser `csi.trident.netapp.io`. Veja o exemplo a seguir:

```
kubectl get sc
```

Resposta da amostra:

NAME	PROVISIONER	RECLAIMPOLICY
VOLUMEBINDINGMODE	ALLOWVOLUMEEXPANSION	AGE
ontap-gold (default)	csi.trident.netapp.io	Delete
true	5d23h	Immediate

Crie uma função de cluster limitada kubeconfig

Você pode, opcionalmente, criar uma função de administrador limitada para o Astra Control Center. Este não é um procedimento necessário para a configuração do Astra Control Center. Esse procedimento ajuda a criar um kubeconfig separado que limita as permissões do Astra Control nos clusters gerenciados.

Antes de começar

Certifique-se de que tem o seguinte para o cluster que pretende gerir antes de concluir as etapas do procedimento:

- kubectl v1,23 ou posterior instalado
- Acesso kubectl ao cluster que você pretende adicionar e gerenciar com o Astra Control Center



Para esse procedimento, você não precisa de acesso kubectl ao cluster que está executando o Astra Control Center.

- Um kubeconfig ativo para o cluster que pretende gerir com direitos de administrador de cluster para o contexto ativo

Passos

1. Criar uma conta de serviço:

- 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. Crie uma função de cluster limitada com as permissões mínimas necessárias para que um cluster seja gerenciado pelo Astra Control:

- a. Crie um `ClusterRole` arquivo chamado `astra-admin-account.yaml`.

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>astra-admin-account.yaml</strong>
```

+

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: astra-admin-account
rules:

# Get, List, Create, and Update all resources
# Necessary to backup and restore all resources in an app
- apiGroups:
```

```
- '*'
resources:
- '*'
verbs:
- get
- list
- create
- patch

# Delete Resources
# Necessary for in-place restore and AppMirror failover
- apiGroups:
- ""
- apps
- autoscaling
- batch
- crd.projectcalico.org
- extensions
- networking.k8s.io
- policy
- rbac.authorization.k8s.io
- snapshot.storage.k8s.io
- trident.netapp.io
resources:
- configmaps
- cronjobs
- daemonsets
- deployments
- horizontalpodautoscalers
- ingresses
- jobs
- namespaces
- networkpolicies
- persistentvolumeclaims
- poddisruptionbudgets
- pods
- podtemplates
- podsecuritypolicies
- replicaset
- replicationcontrollers
- replicationcontrollers/scale
- rolebindings
- roles
- secrets
- serviceaccounts
- services
```

```

- statefulsets
- tridentmirrorrelationships
- tridentnapshotinfos
- volumesnapshots
- volumesnapshotcontents
verbs:
- delete

# Watch resources
# Necessary to monitor progress
- apiGroups:
  - ""
  resources:
  - pods
  - replicationcontrollers
  - replicationcontrollers/scale
  verbs:
  - watch

# Update resources
- apiGroups:
  - ""
  - build.openshift.io
  - image.openshift.io
  resources:
  - builds/details
  - replicationcontrollers
  - replicationcontrollers/scale
  - imagestreams/layers
  - imagestreamtags
  - imagetags
  verbs:
  - update

# Use PodSecurityPolicies
- apiGroups:
  - extensions
  - policy
  resources:
  - podsecuritypolicies
  verbs:
  - use

```

a. Aplique a função de cluster:

```
kubectl apply -f astra-admin-account.yaml
```

3. Crie a vinculação de função de cluster para a função de cluster à conta de serviço:

- 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: astra-admin-account
subjects:
- kind: ServiceAccount
  name: astracontrol-service-account
  namespace: default
```

- a. Aplicar a vinculação de funções do cluster:

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

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

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

O final da saída deve ser semelhante ao seguinte:

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

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

5. Gere o kubeconfig da seguinte forma:

- a. Crie um `create-kubeconfig.sh` arquivo. Substitua `TOKEN_INDEX` no início do script a seguir pelo valor correto.

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

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

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

CONTEXT=$(kubectl config current-context)

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

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

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

```

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

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

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

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

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

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

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

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

```

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

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

6. (Opcional) Renomear o kubeconfig para um nome significativo para o cluster.

```
mv kubeconfig-sa YOUR_CLUSTER_NAME_kubeconfig
```

O que se segue?

Agora que você verificou que os pré-requisitos foram atendidos, você está pronto para [adicione um cluster](#).

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.

Antes de começar

- Antes de adicionar um cluster, revise e execute o [tarefas pré-requisitos](#) necessário .

Passos

1. Navegue pelo menu Dashboard ou clusters:
 - Em **Dashboard** no Resumo de recursos, selecione **Add** no painel clusters.
 - Na área de navegação à esquerda, selecione **clusters** e, em seguida, selecione **Adicionar cluster** na página 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. "[Documentação do Kubernetes](#)" Consulte para obter informações sobre a criação `kubeconfig` de ficheiros. Se você criou um `kubeconfig` para uma função de cluster limitada usando o [processo acima](#) , certifique-se de carregar ou colar esse `kubeconfig` nesta etapa.

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



Você deve selecionar uma classe de storage Astra Trident com o suporte de storage ONTAP.

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

Resultado

O cluster entra no estado **Descobrendo** e depois muda para **saudável**. Agora você está gerenciando o cluster com 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.

Ativar a autenticação no back-end de storage do ONTAP

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

- **Autenticação baseada em credenciais:** O nome de usuário e senha para um usuário do ONTAP com as permissões necessárias. Você deve usar uma função de login de segurança pré-definida, como `admin` ou `vsadmin` para garantir a máxima compatibilidade com as versões do ONTAP.
- **Autenticação baseada em certificado:** O Astra Control Center também pode se comunicar com um cluster ONTAP usando um certificado instalado no back-end. Você deve usar o certificado de cliente, a chave e o certificado de CA confiável, se usado (recomendado).

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

Ative a autenticação baseada em credenciais

O Astra Control Center requer as credenciais para um cluster com escopo `admin` para se comunicar com o back-end do ONTAP. Você deve usar funções padrão e predefinidas, `admin` como `.` Isso garante compatibilidade direta com futuras versões do ONTAP que podem expor APIs de recursos a serem usadas por futuras versões do Astra Control Center.



Uma função de login de segurança personalizada pode ser criada e usada com o Astra Control Center, mas não é recomendada.

Uma definição de backend de exemplo se parece com esta:

```
{
  "version": 1,
  "backendName": "ExampleBackend",
  "storageDriverName": "ontap-nas",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.2",
  "svm": "svm_nfs",
  "username": "admin",
  "password": "secret"
}
```

A definição de back-end é o único lugar onde as credenciais são armazenadas em texto simples. A criação ou atualização de um backend é a única etapa que requer conhecimento das credenciais. Como tal, é uma operação somente de administração, realizada pelo Kubernetes ou pelo administrador de storage.

Ativar autenticação baseada em certificado

O Centro de Controle Astra pode usar certificados para se comunicar com backends ONTAP novos e existentes. Você deve inserir as seguintes informações na definição de back-end.

- `clientCertificate`: Certificado do cliente.
- `clientPrivateKey`: Chave privada associada.
- `trustedCACertificate`: Certificado de CA confiável. Se estiver usando uma CA confiável, esse parâmetro deve ser fornecido. Isso pode ser ignorado se nenhuma CA confiável for usada.

Você pode usar um dos seguintes tipos de certificados:

- Certificado auto-assinado
- Certificado de terceiros

Ative a autenticação com um certificado autoassinado

Um fluxo de trabalho típico envolve as etapas a seguir.

Passos

1. Gerar um certificado e chave de cliente. Ao gerar, defina o Nome Comum (CN) para o usuário ONTAP para autenticar como.

```
openssl req -x509 -nodes -days 1095 -newkey rsa:2048 -keyout k8senv.key  
-out k8senv.pem -subj "/C=US/ST=NC/L=RTP/O=NetApp/CN=<common-name>"
```

2. Instale o certificado de cliente de tipo `client-ca` e chave no cluster do ONTAP.

```
security certificate install -type client-ca -cert-name <certificate-  
name> -vserver <vserver-name>  
security ssl modify -vserver <vserver-name> -client-enabled true
```

3. Confirme se a função de login de segurança do ONTAP suporta o método de autenticação de certificado.

```
security login create -user-or-group-name vsadmin -application ontapi  
-authentication-method cert -vserver <vserver-name>  
security login create -user-or-group-name vsadmin -application http  
-authentication-method cert -vserver <vserver-name>
```

4. Teste a autenticação usando o certificado gerado. Substitua o ONTAP Management LIF> e o <vserver name> pelo IP de LIF de gerenciamento e nome da SVM. Você deve garantir que o LIF tenha sua política de serviço definida como `default-data-management`.

```
curl -X POST -Lk https://<ONTAP-Management-LIF>/servlets/netapp.servlets.admin.XMLrequest_filer --key k8senv.key --cert ~/k8senv.pem -d '<?xml version="1.0" encoding="UTF-8"?><netapp xmlns=http://www.netapp.com/filer/admin version="1.21" vfiler="<vserver-name>"><vserver-get></vserver-get></netapp>
```

5. Usando os valores obtidos na etapa anterior, adicione o back-end de storage na IU do Astra Control Center.

Ative a autenticação com um certificado de terceiros

Se você tiver um certificado de terceiros, poderá configurar a autenticação baseada em certificado com estas etapas.

Passos

1. Gerar a chave privada e CSR:

```
openssl req -new -newkey rsa:4096 -nodes -sha256 -subj "/" -outform pem -out ontap_cert_request.csr -keyout ontap_cert_request.key -addext "subjectAltName = DNS:<ONTAP_CLUSTER_FQDN_NAME>,IP:<ONTAP_MGMT_IP>"
```

2. Passe o CSR para a CA do Windows (CA de terceiros) e emita o certificado assinado.
3. Baixe o certificado assinado e nomeie-o como "ONTAP_signed_cert.crt"
4. Exporte o certificado raiz da CA do Windows (CA de terceiros).
5. Nomeie este arquivo `ca_root.crt`

Agora você tem os seguintes três arquivos:

- **Chave privada:** `ontap_signed_request.key` (Esta é a chave correspondente para o certificado do servidor no ONTAP. É necessário ao instalar o certificado do servidor.)
 - **Certificado assinado:** `ontap_signed_cert.crt` (Isso também é chamado de *certificado do servidor* no ONTAP.)
 - **Certificado CA raiz:** (Também é chamado de *certificado CA* `ca_root.crt` *Server-CA* no ONTAP.)
6. Instale estes certificados no ONTAP. Gerar, instalar `server` e `server-ca` certificados no ONTAP.

Detalhes em `Sample.yaml`

```
# Copy the contents of ca_root.crt and use it here.
```

```
security certificate install -type server-ca
```

```
Please enter Certificate: Press <Enter> when done
```

```
-----BEGIN CERTIFICATE-----
```

```
<certificate details>
```

```
-----END CERTIFICATE-----
```

You should keep a copy of the CA-signed digital certificate for future reference.

The installed certificate's CA and serial number for reference:

CA:

serial:

The certificate's generated name for reference:

===

```
# Copy the contents of ontap_signed_cert.crt and use it here. For key, use the contents of ontap_cert_request.key file.
```

```
security certificate install -type server
```

```
Please enter Certificate: Press <Enter> when done
```

```
-----BEGIN CERTIFICATE-----
```

```
<certificate details>
```

```
-----END CERTIFICATE-----
```

```
Please enter Private Key: Press <Enter> when done
```

```
-----BEGIN PRIVATE KEY-----
```

```
<private key details>
```

```
-----END PRIVATE KEY-----
```

Enter certificates of certification authorities (CA) which form the certificate chain of the server certificate. This starts with the issuing CA certificate of the server certificate and can range up to the root CA certificate.

Do you want to continue entering root and/or intermediate certificates {y|n}: n

The provided certificate does not have a common name in the subject field.

Enter a valid common name to continue installation of the certificate: <ONTAP_CLUSTER_FQDN_NAME>

You should keep a copy of the private key and the CA-signed digital certificate for future reference.

The installed certificate's CA and serial number for reference:

CA:

serial:

The certificate's generated name for reference:

==

```
# Modify the vsserver settings to enable SSL for the installed certificate
```

```
ssl modify -vsserver <vsserver_name> -ca <CA> -server-enabled true  
-serial <serial number> (security ssl modify)
```

==

```
# Verify if the certificate works fine:
```

```
openssl s_client -CAfile ca_root.crt -showcerts -servername server  
-connect <ONTAP_CLUSTER_FQDN_NAME>:443
```

```
CONNECTED(00000005)
```

```
depth=1 DC = local, DC = umca, CN = <CA>
```

```
verify return:1
```

```
depth=0
```

```
verify return:1
```

```
write W BLOCK
```

```
---
```

```
Certificate chain
```

```
0 s:
```

```
  i:/DC=local/DC=umca/<CA>
```

```
-----BEGIN CERTIFICATE-----
```

```
<Certificate details>
```

7. Crie o certificado de cliente para o mesmo host para comunicação sem senha. O Centro de Controle Astra usa esse processo para se comunicar com o ONTAP.

8. Gerar e instalar os certificados de cliente no ONTAP:

Detalhes em Sample.yaml

```
# Use /CN=admin or use some other account which has privileges.
openssl req -x509 -nodes -days 1095 -newkey rsa:2048 -keyout
ontap_test_client.key -out ontap_test_client.pem -subj "/CN=admin"
```

Copy the content of ontap_test_client.pem file and use it in the below command:

```
security certificate install -type client-ca -vserver <vserver_name>
```

Please enter Certificate: Press <Enter> when done

```
-----BEGIN CERTIFICATE-----
```

```
<Certificate details>
```

```
-----END CERTIFICATE-----
```

You should keep a copy of the CA-signed digital certificate for future reference.

The installed certificate's CA and serial number for reference:

CA:

serial:

The certificate's generated name for reference:

==

```
ssl modify -vserver <vserver_name> -client-enabled true
(security ssl modify)
```

```
# Setting permissions for certificates
```

```
security login create -user-or-group-name admin -application ontapi
-authentication-method cert -role admin -vserver <vserver_name>
```

```
security login create -user-or-group-name admin -application http
-authentication-method cert -role admin -vserver <vserver_name>
```

==

```
#Verify passwordless communication works fine with the use of only
certificates:
```

```
curl --cacert ontap_signed_cert.crt --key ontap_test_client.key
--cert ontap_test_client.pem
```

```
https://<ONTAP_CLUSTER_FQDN_NAME>/api/storage/aggregates
```

```
{
```

```
"records": [
```

```

{
  "uuid": "f84e0a9b-e72f-4431-88c4-4bf5378b41bd",
  "name": "<aggr_name>",
  "node": {
    "uuid": "7835876c-3484-11ed-97bb-d039ea50375c",
    "name": "<node_name>",
    "_links": {
      "self": {
        "href": "/api/cluster/nodes/7835876c-3484-11ed-97bb-d039ea50375c"
      }
    }
  },
  "_links": {
    "self": {
      "href": "/api/storage/aggregates/f84e0a9b-e72f-4431-88c4-4bf5378b41bd"
    }
  }
},
  "num_records": 1,
  "_links": {
    "self": {
      "href": "/api/storage/aggregates"
    }
  }
}
}

```

9. Adicione o back-end de storage à IU do Astra Control Center e forneça os seguintes valores:

- **Certificado do cliente:** ONTAP_test_client.pem
- **Chave privada:** ONTAP_test_client.key
- **Certificado de CA confiável:** ONTAP_signed_cert.crt

Adicionar um back-end de storage

Você pode adicionar um back-end de storage do ONTAP existente ao Astra Control Center para 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.

Depois de configurar as credenciais ou as informações de autenticação de certificado, você poderá adicionar um back-end de storage do ONTAP existente ao Astra Control Center para gerenciar seus recursos.

Passos

1. No Painel na área de navegação à esquerda, selecione **backends**.
2. Selecione **Adicionar**.
3. Na seção usar existente da página Adicionar storage backend, selecione **ONTAP**.
4. Selecione uma das seguintes opções:
 - **Use as credenciais de administrador:** Insira o endereço IP e as credenciais de administrador de gerenciamento de cluster do ONTAP. As credenciais devem ser credenciais de todo o cluster.



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

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

5. Selecione **seguinte**.
6. Confirme os detalhes do backend e selecione **Manage**.

Resultado

O backend aparece no `online` estado da lista com informações de resumo.



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

Adicione um balde

Você pode adicionar um bucket usando a IU do Astra Control ou ["API"](#)o . 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.

Você não precisa de um bucket no Astra Control se estiver clonando a configuração da aplicação e o storage persistente para o mesmo cluster. A funcionalidade de instantâneos de aplicações não requer um intervalo.

Antes de começar

- Um bucket que pode ser acessado a partir dos clusters gerenciados pelo Astra Control Center.
- Credenciais para o bucket.
- Um balde dos seguintes tipos:
 - NetApp ONTAP S3
 - NetApp StorageGRID S3
 - Microsoft Azure
 - Genérico S3



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



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

Passos

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



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

4. 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.

5. Introduza o nome ou endereço IP do endpoint S3.
6. Em **Selecionar credenciais**, escolha a guia **Adicionar** ou **usar existente**.
 - Se você escolheu **Add**:
 - i. Insira um nome para a credencial que a distingue de outras credenciais no Astra Control.
 - ii. Insira a ID de acesso e a chave secreta colando o conteúdo da área de transferência.
 - Se você escolheu **Use existing**:
 - i. Selecione as credenciais existentes que você deseja usar com o bucket.
7. `Add` Selecione .



Quando você adiciona um balde, o Astra Control marca um balde com o indicador de balde padrão. O primeiro bucket que você criar se torna o bucket padrão. À medida que você adiciona buckets, você pode decidir mais tarde "[defina outro intervalo padrão](#)".

O que se segue?

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

- "[Gerencie usuários e funções locais](#)"
- "[Comece a gerenciar aplicativos](#)"
- "[Proteja aplicativos](#)"
- "[Gerenciar notificações](#)"
- "[Conecte-se ao Cloud Insights](#)"
- "[Adicione um certificado TLS personalizado](#)"

- ["Altere a classe de armazenamento padrão"](#)

Encontre mais informações

- ["Use a API Astra Control"](#)
- ["Problemas conhecidos"](#)

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.yaml` custom resource (CR) quando você instalou o Astra Control Center. O e-mail é o valor definido no campo `spec.email` no `astra_control_center.yaml` CR.

Licenciamento

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

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

Passos

1. Na navegação à esquerda, selecione **conta > Licença**.
2. Na visão geral da licença, à direita das informações da licença, selecione o menu Opções.
3. Selecione **Substituir**.
4. Navegue até o arquivo de licença que você baixou e selecione **Adicionar**.

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

Sim, você pode testar a funcionalidade de gerenciamento de aplicativos com uma licença de avaliação (incluindo a licença de avaliação incorporada instalada por padrão). Não há diferença em recursos ou recursos entre uma licença de avaliação e uma licença completa; a licença de avaliação simplesmente tem uma vida útil mais curta. ["Licenciamento"](#) Consulte para obter mais informações.

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 Astra Trident é desinstalado automaticamente de um cluster quando eu o desgerencio?

Quando você desgerencia um cluster do Astra Control Center, o Astra Trident não é desinstalado automaticamente do cluster. Para desinstalar o Astra Trident, você precisará ["Siga estas etapas na documentação do Astra Trident"](#).

Gerenciamento de aplicações

O Astra Control pode implantar uma aplicação?

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

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

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

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

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

Devo gerenciar o próprio Astra Control?

Não, você não deve gerenciar o Astra Control por ser uma "aplicação do sistema".

Os pods não saudáveis afetam o gerenciamento de aplicativos?

Não, a integridade dos pods não afeta o gerenciamento de aplicativos.

Operações de gerenciamento de dados

Meu aplicativo usa vários PVS. O Astra Control fará snapshots e backups desses PVS?

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

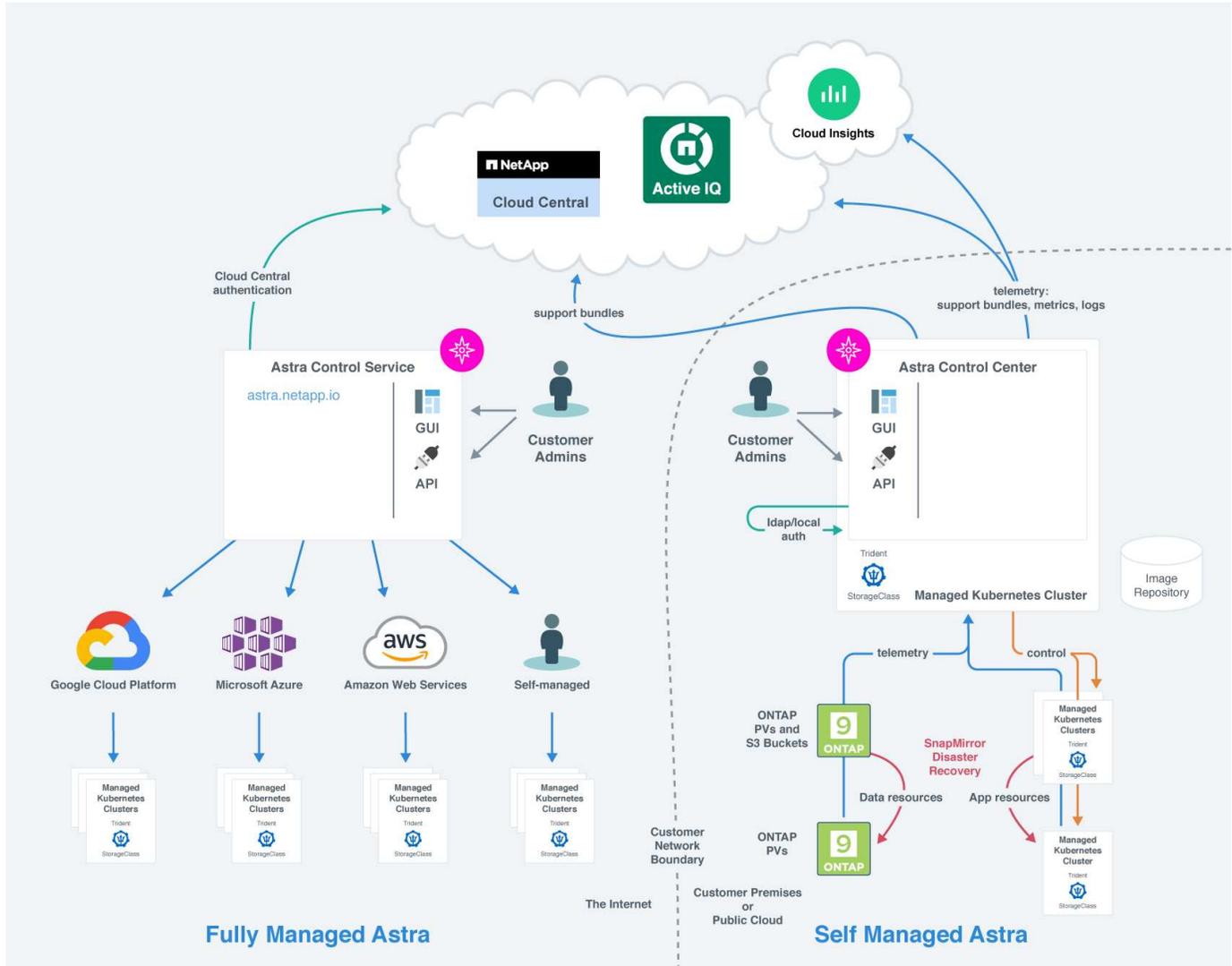
Posso gerenciar snapshots feitos pelo Astra Control diretamente por meio de uma interface ou storage de objetos diferente?

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

Conceitos

Arquitetura e componentes

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



Componentes do Astra Control

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

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

Interfaces Astra Control

Você pode concluir tarefas usando diferentes interfaces:

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

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

Para mais informações

- ["Documentação do Astra Control Service"](#)
- ["Documentação do Astra Control Center"](#)
- ["Documentação do Astra Trident"](#)
- ["Use a API Astra Control"](#)
- ["Documentação do Cloud Insights"](#)
- ["Documentação do ONTAP"](#)

Proteção de dados

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

Snapshots, backups e políticas de proteção

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

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

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

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

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



Você não pode estar totalmente protegido até ter um backup recente. Isso é importante porque os backups são armazenados em um armazenamento de objetos longe dos volumes persistentes. Se uma falha ou acidente apagar o cluster e seu armazenamento persistente associado, então você precisa de um backup para recuperar. Um instantâneo não permitiria que você se recuperasse.

Clones

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

Replicação para um cluster remoto

Com o Astra Control, você pode criar continuidade dos negócios para suas aplicações com RPO baixo (objetivo do ponto de recuperação) e rto baixo (objetivo do tempo de recuperação) usando funcionalidades de replicação assíncrona da tecnologia NetApp SnapMirror. Uma vez configurado, isso permite que as aplicações repliquem alterações de dados e aplicações de um cluster para outro.

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

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

- **Replicação de aplicativos:** O Astra Control requer que os clusters de Kubernetes de origem e destino estejam disponíveis e gerenciados com seus respectivos back-ends de storage do ONTAP configurados para habilitar o NetApp SnapMirror. Astra Control elimina a aplicação orientada por políticas e replica-a para o cluster remoto. A tecnologia NetApp SnapMirror é usada para replicar dados de volume persistente.

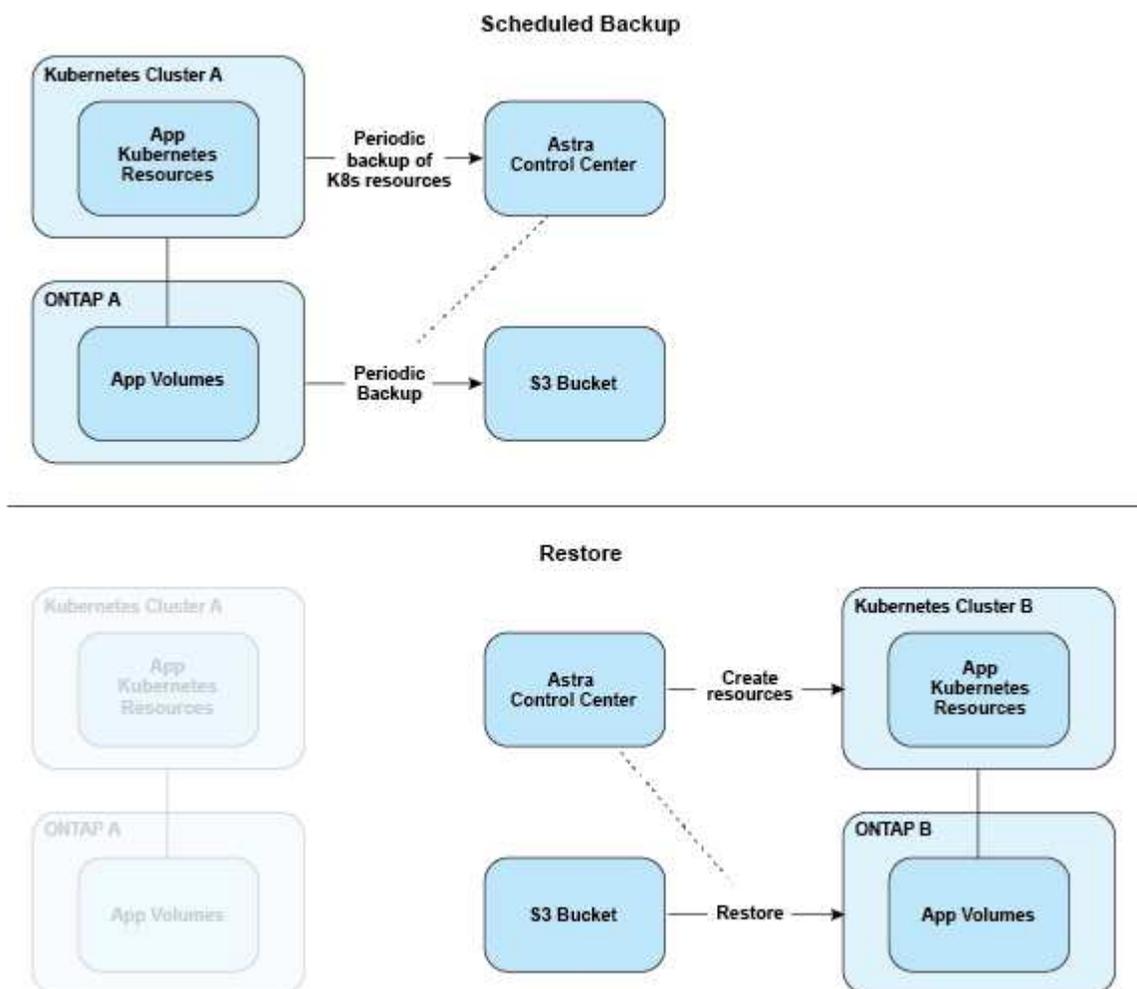
Para fazer failover, o Astra Control pode colocar a aplicação replicada online recriando os objetos da aplicação no cluster de Kubernetes de destino com os volumes replicados no cluster do ONTAP de destino. Como os dados de volume persistente já estão presentes no cluster de destino ONTAP, o Astra Control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

- **Backup e restauração de aplicações:** Ao fazer backup de aplicações, o Astra Control cria um Snapshot dos dados do aplicativo e os armazena em um bucket de armazenamento de objetos. Quando uma restauração é necessária, os dados no bucket devem ser copiados para um volume persistente no cluster do ONTAP. A operação de backup/restauração não exige que o cluster secundário Kubernetes/ONTAP esteja disponível e gerenciado, mas a cópia de dados adicional pode resultar em tempos de restauração mais longos.

Para saber como replicar aplicativos, "[Replique aplicativos para um sistema remoto usando a tecnologia SnapMirror](#)" consulte .

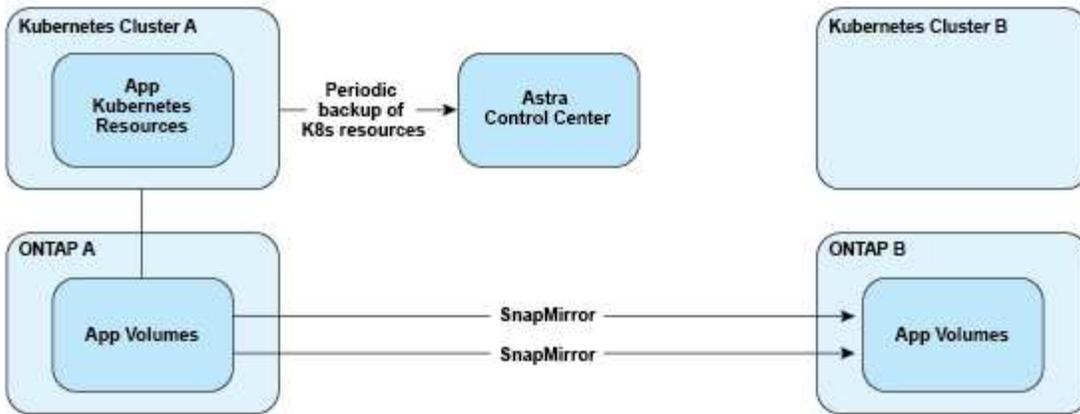
As imagens a seguir mostram o processo de backup e restauração agendado em comparação com o processo de replicação.

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

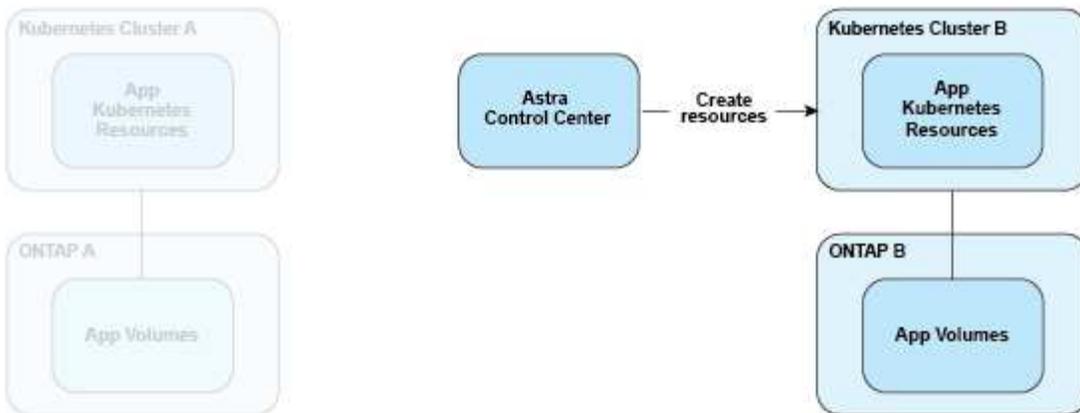


Por outro lado, a replicação é feita com replicação para o ONTAP e, em seguida, um failover cria os recursos do Kubernetes:

Replication Relationship



Fail over



Backups, snapshots e clones com uma licença expirada

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

Licenciamento

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

Você obtém uma licença de uma das seguintes maneiras:

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

Para obter detalhes sobre as licenças necessárias para backends de armazenamento ONTAP, "[backends de armazenamento suportados](#)" consulte .



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

Licenças de avaliação e licenças completas

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

Expiração da licença

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

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

Como o consumo de licença é calculado

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

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



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

Encontre mais informações

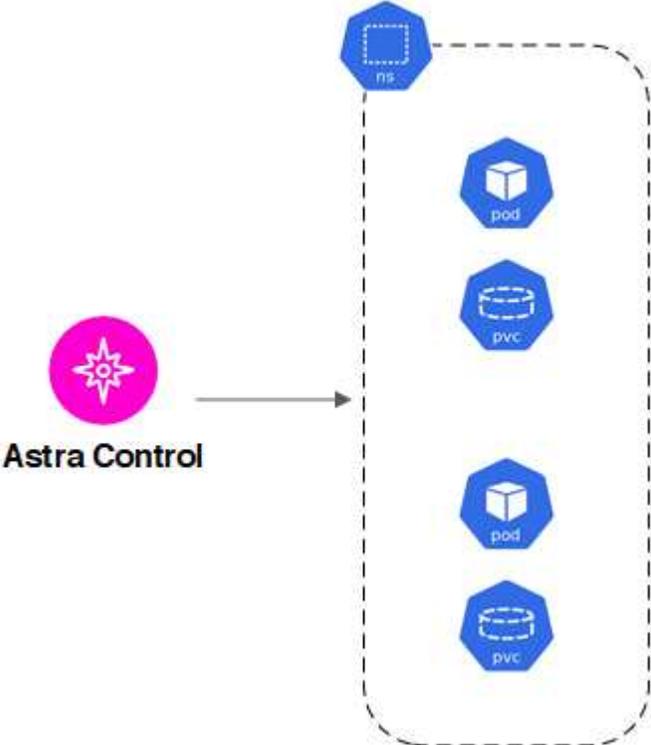
- "[Adicione uma licença ao configurar o Astra Control Center pela primeira vez](#)"
- "[Atualizar uma licença existente](#)"

Gerenciamento de aplicativos

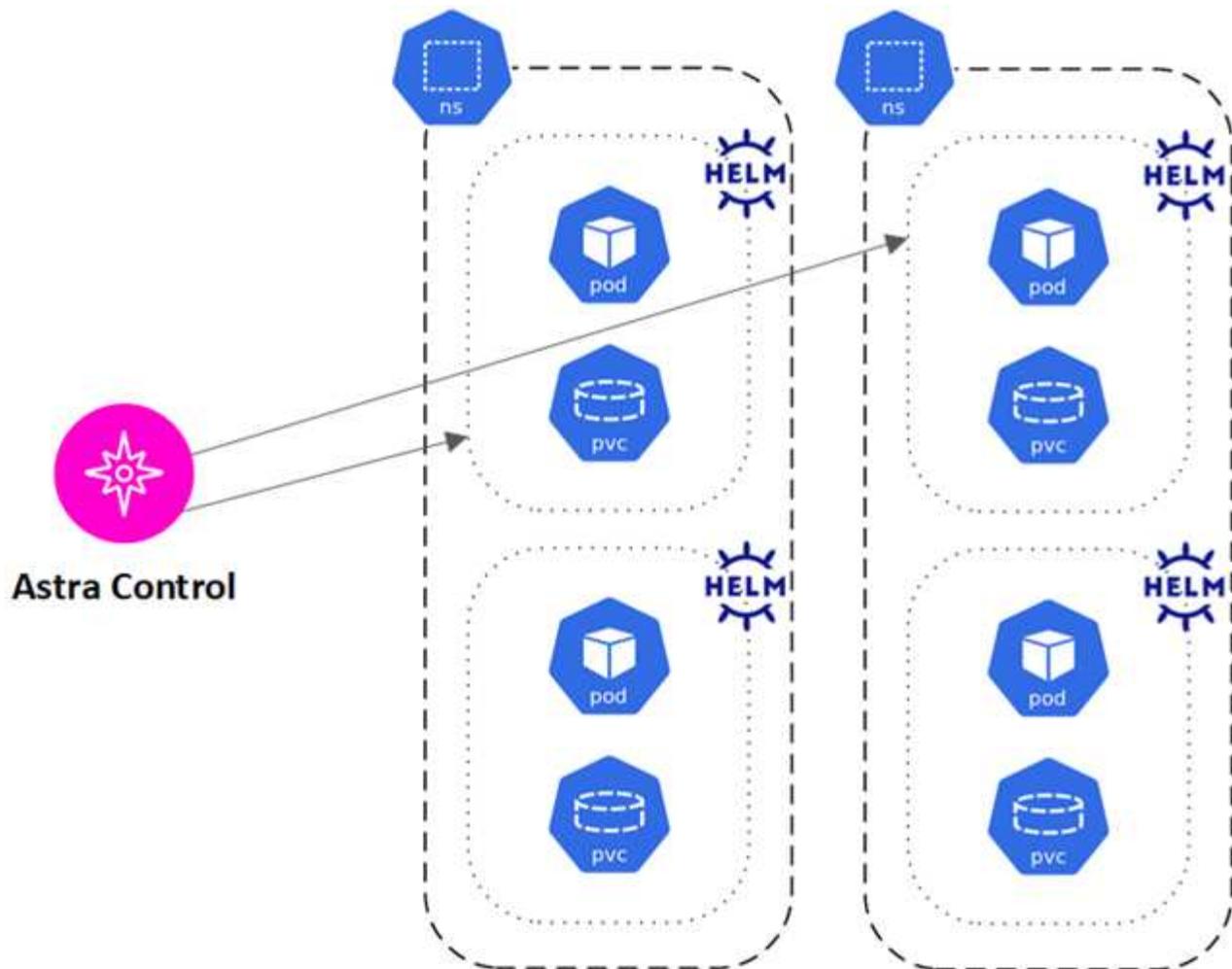
Quando o Astra Control descobre seus clusters, as aplicações nesses clusters não são

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

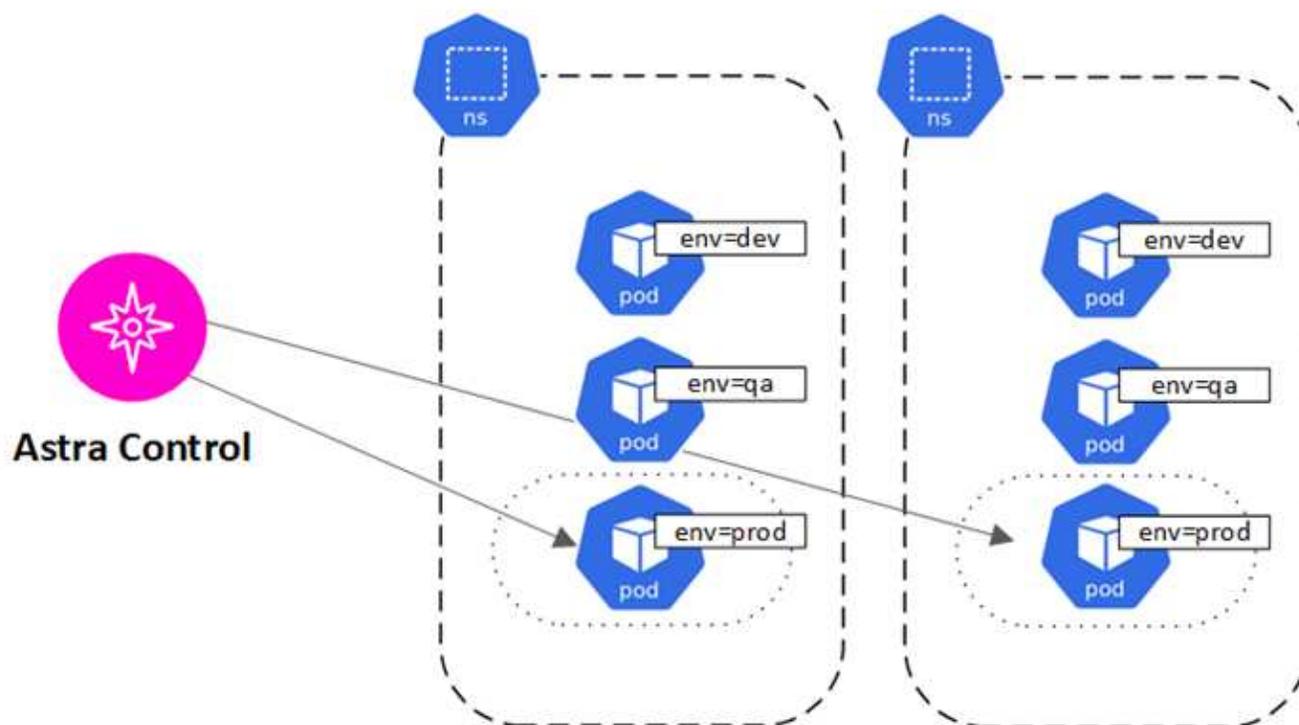
- Namespace, incluindo todos os recursos nesse namespace



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



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



Classes de armazenamento e tamanho de volume persistente

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

Visão geral

O Astra Control Center é compatível com o seguinte:

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



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

Classes de armazenamento

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

Para mais informações

- ["Documentação do Astra Trident"](#)

Funções de usuário e namespaces

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

Funções de utilizador

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

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

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

Namespaces

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

Encontre mais informações

["Gerencie usuários e funções locais"](#)

Segurança do pod

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

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

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

PSAs aplicados pelo Astra Control Center

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

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

PSPs instalados pelo Astra Control Center

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

PSP criados durante a instalação

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

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

A nova política e os objetos têm os seguintes atributos:

```
kubectl get psp
```

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

```
kubectl get role -n <namespace_name>
```

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

```
kubectl get rolebinding -n <namespace_name>
```

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

PSP criados durante operações de cópia de segurança

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

A nova política e os objetos têm os seguintes atributos:

```
kubectl get psp
```

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

```
kubectl get role -n <namespace_name>
```

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

```
kubectl get rolebinding -n <namespace_name>
```

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

PSP criados durante a gestão de clusters

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

A nova política e os objetos têm os seguintes atributos:

```
kubectl get psp
```

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

```
kubectl get role -n <namespace_name>
```

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

```
kubectl get rolebinding -n <namespace_name>
```

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

Use o Astra Control Center

Comece a gerenciar aplicativos

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

Requisitos de gerenciamento de aplicativos

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

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

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

Métodos de instalação de aplicativos suportados

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

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

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

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

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

- ["Apache K8ssandra"](#)



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

- ["Jenkins CI"](#)
- ["Cluster Percona XtraDB"](#)

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

Instale aplicativos no cluster

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

Definir aplicações

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

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



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

Antes de começar

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



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

Sobre esta tarefa

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

Opções de gerenciamento de aplicativos

- [Definir recursos para gerenciar como um aplicativo](#)
- [Defina um namespace para gerenciar como um aplicativo](#)

Definir recursos para gerenciar como um aplicativo

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

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



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

Leia mais sobre como adicionar recursos com escopo de cluster aos namespaces do aplicativo.

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

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

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

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

Passos

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



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

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



Para saber mais sobre rótulos do Kubernetes, "[Consulte a documentação oficial do Kubernetes](#)".

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

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



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

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

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



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



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

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

Defina um namespace para gerenciar como um aplicativo

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

Passos

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



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



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



Show system namespaces

["Leia mais"](#).

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

E quanto aos namespaces do sistema?

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

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



Show system namespaces



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.

Exemplo: Política de proteção separada para versões diferentes

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

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

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

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

Encontre mais informações

- ["Use a API Astra Control"](#)
- ["Desgerenciar um aplicativo"](#)

Proteja aplicativos

Visão geral da proteção

Você pode criar backups, clones, snapshots e políticas de proteção para suas aplicações usando o Astra Control Center. O backup de seus aplicativos ajuda seus serviços e dados associados a estarem o mais disponíveis possível; durante um cenário de desastre, a restauração do backup pode garantir a recuperação completa de um aplicativo e seus dados associados com o mínimo de interrupções. Backups, clones e snapshots podem ajudar a proteger contra ameaças comuns, como ransomware, perda acidental de dados e desastres ambientais. ["Saiba mais sobre os tipos de proteção de dados disponíveis no Astra Control Center e quando usá-los"](#).

Além disso, é possível replicar aplicações para um cluster remoto para se preparar para a recuperação de desastres.

Fluxo de trabalho de proteção de aplicações

Você pode usar o fluxo de trabalho de exemplo a seguir para começar a proteger seus aplicativos.

[Um] Proteja todas as aplicações

Para garantir que seus aplicativos estejam protegidos imediatamente ["crie um backup manual de todos os aplicativos"](#), .

[Dois] Configure uma política de proteção para cada aplicativo

Para automatizar backups e snapshots futuros, ["configure uma política de proteção para cada aplicativo"](#). Por exemplo, você pode começar com backups semanais e snapshots diários, com retenção de um mês para ambos. A automação de backups e snapshots com uma política de proteção é altamente recomendada em backups e snapshots manuais.

[Três] Ajustar as políticas de proteção

À medida que as aplicações e os seus padrões de utilização mudam, ajuste as políticas de proteção conforme necessário para proporcionar a melhor proteção.

[Quatro] Replique aplicações para um cluster remoto

["Replicar aplicações"](#) Para um cluster remoto usando a tecnologia NetApp SnapMirror. O Astra Control replica snapshots para um cluster remoto, fornecendo funcionalidade assíncrona de recuperação de desastres.

[Cinco] Em caso de desastre, restaure seus aplicativos com o backup ou replicação mais recente para o sistema remoto

Se a perda de dados ocorrer, você pode se recuperar ["restaurar a cópia de segurança mais recente"](#) primeiro para cada aplicativo. Em seguida, você pode restaurar o instantâneo mais recente (se disponível). Ou, você pode usar a replicação para um sistema remoto.

Proteja aplicativos com snapshots e backups

Proteja todos os aplicativos tirando snapshots e backups usando uma política de proteção automatizada ou ad hoc. Você pode usar a IU do Astra Control Center ou ["API Astra Control"](#) para proteger aplicações.

Sobre esta tarefa

- **Aplicativos implantados pelo Helm:** Se você usar o Helm para implantar aplicativos, o Astra Control Center precisará do Helm versão 3. O gerenciamento e clonagem de aplicativos implantados com o Helm 3 (ou atualizados do Helm 2 para o Helm 3) são totalmente compatíveis. As aplicações implementadas com o Helm 2 não são suportadas.
- **(somente clusters OpenShift) Adicionar políticas:** Quando você cria um projeto para hospedar um aplicativo em um cluster OpenShift, o projeto (ou namespace Kubernetes) recebe um UID SecurityContext. Para ativar o Astra Control Center para proteger seu aplicativo e mover o aplicativo para outro cluster ou projeto no OpenShift, você precisa adicionar políticas que permitam que o aplicativo seja executado como qualquer UID. Como exemplo, os seguintes comandos OpenShift CLI concedem as políticas apropriadas a um aplicativo WordPress.

```
oc new-project wordpress
oc adm policy add-scc-to-group anyuid system:serviceaccounts:wordpress
oc adm policy add-scc-to-user privileged -z default -n wordpress
```

Você pode executar as seguintes tarefas relacionadas à proteção dos dados do aplicativo:

- [Configurar uma política de proteção](#)
- [Criar um instantâneo](#)
- [Crie uma cópia de segurança](#)
- [Visualizar instantâneos e backups](#)
- [Eliminar instantâneos](#)
- [Cancelar cópias de segurança](#)
- [Eliminar cópias de segurança](#)

Configurar uma política de proteção

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

Se precisar de backups ou snapshots para executar com mais frequência do que uma vez por hora, você pode "[Use a API REST do Astra Control para criar snapshots e backups](#)".



Offset programações de backup e replicação para evitar sobreposições de agendamento. Por exemplo, execute backups no topo da hora a cada hora e programe a replicação para começar com um deslocamento de 5 minutos e um intervalo de 10 minutos.



Se o aplicativo usar uma classe de armazenamento apoiada pelo `ontap-nas-economy` driver, as políticas de proteção não poderão ser usadas. Migre para uma classe de storage com suporte do Astra Control se quiser agendar backups e snapshots.

Passos

1. Selecione **aplicativos** e, em seguida, selecione o nome de um aplicativo.
2. Selecione **proteção de dados**.
3. Selecione **Configurar política de proteção**.
4. Defina um cronograma de proteção escolhendo o número de snapshots e backups para manter a hora, o

dia, a semana e o mês.

Você pode definir as programações por hora, diária, semanal e mensal simultaneamente. Uma programação não ficará ativa até que você defina um nível de retenção.

Ao definir um nível de retenção para backups, você pode escolher o intervalo onde deseja armazenar os backups.

O exemplo a seguir define quatro programações de proteção: Por hora, por dia, por semana e por mês para snapshots e backups.

Configure protection policy STEP 1/2: DETAILS

PROTECTION SCHEDULE

- Hourly**: Every hour on the 0th minute, keep the last 4 snapshots
- Daily**: Daily at 02:00 (UTC), keep the last 15 snapshots
- Weekly**: Weekly on Mondays at 02:00 (UTC), keep the last 26 snapshots
- Monthly**: Every 1st of the month at 02:00 (UTC), keep the last 12 backups

● Hourly ● Daily ● **Weekly** ● Monthly

Select Weekday(s) (optional): Monday X

Time (UTC) (optional): 02:00

Snapshots to keep: 26

Backups to keep: 0

BACKUP DESTINATION

Bucket: ntp-nautilus-bucket-10 - ntp-nautilus-bucket-10 (Default)

OVERVIEW

Schedule and retention

Define a policy to continuously protect your application on a schedule and configure a retention count to get started.

For select stateful applications, expect I/O to pause for a short time during a backup or snapshot operation.

Read more in [Protection policies](#)

Application: cattle-logging

Namespace: cattle-logging

Cluster: se-openlab-astra-enterprise-05-se-openlab-astra-enterprise-05-mstr-1

Cancel Review ->

5. Selecione **Revisão**.

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

Resultado

O Astra Control implementa a política de proteção de dados criando e retendo snapshots e backups usando o cronograma e a política de retenção definidos por você.

Criar um instantâneo

Você pode criar um snapshot sob demanda a qualquer momento.



Se o aplicativo usar uma classe de armazenamento suportada pelo `ontap-nas-economy` driver, os snapshots não poderão ser criados. Use uma classe de armazenamento alternativa para instantâneos.

Passos

1. Selecione **aplicações**.

2. No menu Opções na coluna **ações** para o aplicativo desejado, selecione **Instantâneo**.
3. Personalize o nome do instantâneo e selecione **Next**.
4. Reveja o resumo do instantâneo e selecione **Snapshot**.

Resultado

O processo de instantâneo é iniciado. Um instantâneo é bem-sucedido quando o status é **saudável** na coluna **Estado** na página **proteção de dados > instantâneos**.

Crie uma cópia de segurança

Você 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.



Se o aplicativo usar uma classe de armazenamento apoiada pelo `ontap-nas-economy` driver, certifique-se de que você definiu um `backendType` parâmetro no "[Objeto de storage do Kubernetes](#)" com um valor de `ontap-nas-economy` antes de executar qualquer operação de proteção. Os backups de aplicativos suportados pelo `ontap-nas-economy` são disruptivos e o aplicativo ficará indisponível até que a operação de backup seja concluída.

Passos

1. Selecione **aplicações**.
2. No menu Opções na coluna **ações** para o aplicativo desejado, selecione **Backup**.
3. Personalize o nome da cópia de segurança.
4. Escolha se deseja fazer backup do aplicativo a partir de um snapshot existente. Se selecionar esta opção, pode escolher entre uma lista de instantâneos existentes.
5. Escolha um intervalo de destino para o backup na lista de buckets de armazenamento.
6. Selecione **seguinte**.
7. Reveja o resumo da cópia de segurança e selecione **cópia de segurança**.

Resultado

O Astra Control cria um backup da aplicação.



Se a sua rede tiver uma interrupção ou estiver anormalmente lenta, uma operação de backup pode acabar com o tempo limite. Isso faz com que o backup falhe.



Se for necessário cancelar uma cópia de segurança em execução, utilize as instruções em [Cancelar cópias de segurança](#). Para excluir o backup, aguarde até que ele esteja concluído e, em seguida, use as instruções na [Eliminar cópias de segurança](#).



Após uma operação de proteção de dados (clone, backup, restauração) e subsequente redimensionamento persistente de volume, há até vinte minutos de atraso antes que o novo tamanho de volume seja exibido na IU. A operação de proteção de dados é bem-sucedida em minutos. Você pode usar o software de gerenciamento do back-end de storage para confirmar a alteração no tamanho do volume.

Visualizar instantâneos e backups

Você pode exibir os snapshots e backups de um aplicativo na guia proteção de dados.

Passos

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

Os instantâneos são apresentados por predefinição.

3. Selecione **backups** para ver a lista de backups.

Eliminar instantâneos

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



Não é possível excluir um instantâneo que está sendo replicado no momento.

Passos

1. Selecione **aplicativos** e, em seguida, selecione o nome de um aplicativo gerenciado.
2. Selecione **proteção de dados**.
3. No menu Opções na coluna **ações** para o instantâneo desejado, selecione **Excluir instantâneo**.
4. Digite a palavra "delete" para confirmar a exclusão e selecione **Yes, Delete snapshot**.

Resultado

O Astra Control exclui o Snapshot.

Cancelar cópias de segurança

Pode cancelar uma cópia de segurança em curso.



Para cancelar uma cópia de segurança, a cópia de segurança tem de estar `Running` no estado. Não é possível cancelar uma cópia de segurança que esteja `Pending` no estado.

Passos

1. Selecione **aplicativos** e, em seguida, selecione o nome de um aplicativo.
2. Selecione **proteção de dados**.
3. Selecione **backups**.
4. No menu Opções na coluna **ações** para o backup desejado, selecione **Cancelar**.
5. Digite a palavra "cancelar" para confirmar a operação e selecione **Sim, cancelar backup**.

Eliminar cópias de segurança

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



Se for necessário cancelar uma cópia de segurança em execução, utilize as instruções em [Cancelar cópias de segurança](#). Para excluir o backup, aguarde até que ele esteja concluído e, em seguida, use estas instruções.

Passos

1. Selecione **aplicativos** e, em seguida, selecione o nome de um aplicativo.
2. Selecione **proteção de dados**.
3. Selecione **backups**.
4. No menu Opções na coluna **ações** para o backup desejado, selecione **Excluir backup**.
5. Digite a palavra "delete" para confirmar a exclusão e selecione **Yes, Delete backup**.

Resultado

O Astra Control exclui o backup.

Restaurar aplicações

O Astra Control pode restaurar sua aplicação a partir de um snapshot ou backup. A restauração a partir de um instantâneo existente será mais rápida ao restaurar o aplicativo para o mesmo cluster. Você pode usar a IU do Astra Control ou "[API Astra Control](#)" restaurar aplicações.



Se você adicionar um filtro de namespace a um gancho de execução que é executado após uma operação de restauração ou clone e a origem e destino de restauração ou clone estiverem em namespaces diferentes, o filtro de namespace será aplicado somente ao namespace de destino.

Sobre esta tarefa

- *** Proteja seus aplicativos primeiro *:** É altamente recomendável que você tire um instantâneo ou backup de seu aplicativo antes de restaurá-lo. Isso permitirá clonar a partir do instantâneo ou backup, caso a restauração não seja bem-sucedida.
- **Verificar volumes de destino:** Se você restaurar para uma classe de armazenamento diferente, verifique se a classe de armazenamento usa o mesmo modo de acesso de volume persistente (por exemplo, ReadWriteMany). A operação de restauração falhará se o modo de acesso ao volume persistente de destino for diferente. Por exemplo, se o volume persistente de origem usar o modo de acesso RWX, selecionar uma classe de armazenamento de destino que não seja capaz de fornecer RWX, como discos gerenciados do Azure, AWS EBS, Google Persistent Disk ou `ontap-san`, fará com que a operação de restauração falhe. Para obter mais informações sobre os modos de acesso de volume persistente, consulte "[Kubernetes](#)" a documentação.
- **Planejar necessidades de espaço:** Quando você executa uma restauração no local de um aplicativo que usa armazenamento NetApp ONTAP, o espaço usado pelo aplicativo restaurado pode dobrar. Depois de executar uma restauração no local, remova todos os snapshots indesejados do aplicativo restaurado para liberar espaço de armazenamento.
- **(somente clusters OpenShift) Adicionar políticas:** Quando você cria um projeto para hospedar um aplicativo em um cluster OpenShift, o projeto (ou namespace Kubernetes) recebe um UID SecurityContext. Para ativar o Astra Control Center para proteger seu aplicativo e mover o aplicativo para outro cluster ou projeto no OpenShift, você precisa adicionar políticas que permitam que o aplicativo seja executado como qualquer UID. Como exemplo, os seguintes comandos OpenShift CLI concedem as políticas apropriadas a um aplicativo WordPress.

```
oc new-project wordpress
oc adm policy add-scc-to-group anyuid system:serviceaccounts:wordpress
oc adm policy add-scc-to-user privileged -z default -n wordpress
```

- **Aplicativos implantados pelo Helm:** Os aplicativos implantados com o Helm 3 (ou atualizados do Helm 2 para o Helm 3) são totalmente suportados. As aplicações implementadas com o Helm 2 não são suportadas.



Executar uma operação de restauração no local em um aplicativo que compartilhe recursos com outro aplicativo pode ter resultados não desejados. Todos os recursos compartilhados entre os aplicativos são substituídos quando uma restauração no local é executada em um dos aplicativos. Para obter mais informações, [este exemplo](#) consulte .

Passos

1. Selecione **aplicativos** e, em seguida, selecione o nome de um aplicativo.
2. No menu Opções na coluna ações, selecione **Restaurar**.
3. Escolha o tipo de restauração:
 - **Restaurar para namespaces originais:** Use este procedimento para restaurar o aplicativo no local para o cluster original.



Se o aplicativo usar uma classe de armazenamento apoiada pelo `ontap-nas-economy` driver, você deverá restaurar o aplicativo usando as classes de armazenamento originais. Você não pode especificar uma classe de armazenamento diferente se estiver restaurando o aplicativo para o mesmo namespace.

- i. Selecione o instantâneo ou o backup a ser usado para restaurar o aplicativo no local, o que reverte o aplicativo para uma versão anterior de si mesmo.
- ii. Selecione **seguinte**.



Se você restaurar para um namespace que foi excluído anteriormente, um novo namespace com o mesmo nome será criado como parte do processo de restauração. Todos os usuários que tinham direitos para gerenciar aplicativos no namespace excluído anteriormente precisam restaurar manualmente os direitos para o namespace recém-criado.

- * Restaurar para novos namespaces*: Use este procedimento para restaurar o aplicativo para outro cluster ou com namespaces diferentes da origem.



Você pode usar este procedimento para uma classe de armazenamento suportada pelo `ontap-nas` mesmo cluster **OU** copiar o aplicativo para outro cluster com uma classe de armazenamento suportada pelo `ontap-nas-economy` driver.

- i. Especifique o nome do aplicativo restaurado.
- ii. Escolha o cluster de destino para o aplicativo que você pretende restaurar.
- iii. Insira um namespace de destino para cada namespace de origem associado ao aplicativo.



O Astra Control cria novos namespaces de destino como parte dessa opção de restauração. Namespaces de destino que você especificar não devem estar presentes no cluster de destino.

- iv. Selecione **seguinte**.
- v. Selecione o instantâneo ou a cópia de segurança a utilizar para restaurar a aplicação.

vi. Selecione **seguinte**.

vii. Escolha uma das seguintes opções:

- **Restaurar usando classes de armazenamento originais:** O aplicativo usa a classe de armazenamento originalmente associada, a menos que não exista no cluster de destino. Neste caso, a classe de armazenamento padrão para o cluster será usada.
- **Restaurar usando uma classe de armazenamento diferente:** Selecione uma classe de armazenamento existente no cluster de destino. Todos os volumes de aplicativos, independentemente de suas classes de armazenamento originalmente associadas, serão migrados para essa classe de armazenamento diferente como parte da restauração.

viii. Selecione **seguinte**.

4. Escolha quaisquer recursos para filtrar:

- **Restaurar todos os recursos:** Restaure todos os recursos associados ao aplicativo original.
- **Filtrar recursos:** Especifique regras para restaurar um sub-conjunto dos recursos originais do aplicativo:
 - i. Escolha incluir ou excluir recursos do aplicativo restaurado.
 - ii. Selecione **Adicionar regra de inclusão** ou **Adicionar regra de exclusão** e configure a regra para filtrar os recursos corretos durante a restauração do aplicativo. Você pode editar uma regra ou removê-la e criar uma regra novamente até que a configuração esteja correta.



Para saber mais sobre como configurar regras de inclusão e exclusão, [Filtre recursos durante uma restauração de aplicativos](#) consulte .

5. Selecione **seguinte**.

6. Revise os detalhes sobre a ação de restauração cuidadosamente, digite "restaurar" (se solicitado) e selecione **Restaurar**.

Resultado

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



Após uma operação de proteção de dados (clone, backup ou restauração) e subsequente redimensionamento persistente de volume, há um atraso de até vinte minutos antes que o novo tamanho de volume seja exibido na IU da Web. A operação de proteção de dados é bem-sucedida em minutos. Você pode usar o software de gerenciamento do back-end de storage para confirmar a alteração no tamanho do volume.



Qualquer usuário membro com restrições de namespace por nome/ID de namespace ou por rótulos de namespace pode clonar ou restaurar um aplicativo para um novo namespace no mesmo cluster ou para qualquer outro cluster na conta da organização. No entanto, o mesmo usuário não pode acessar o aplicativo clonado ou restaurado no novo namespace. Depois que um novo namespace é criado por uma operação de clone ou restauração, o administrador/proprietário da conta pode editar a conta de usuário membro e atualizar as restrições de função para o usuário afetado conceder acesso ao novo namespace.

Filtre recursos durante uma restauração de aplicativos

Você pode adicionar uma regra de filtro a uma "restaurar" operação que especificará os recursos existentes do aplicativo a serem incluídos ou excluídos do aplicativo restaurado. Você pode incluir ou excluir recursos com base em um namespace, rótulo ou GVK (GroupVersionKind) especificado.

Leia mais sobre incluir e excluir cenários

- **Você seleciona uma regra include com namespaces originais (in-place restore):** Os recursos de aplicativo existentes que você definir na regra serão excluídos e substituídos por aqueles do snapshot selecionado ou backup que você está usando para a restauração. Quaisquer recursos que você não especificar na regra incluir permanecerão inalterados.
- **Você seleciona uma regra de inclusão com novos namespaces:** Use a regra para selecionar os recursos específicos desejados no aplicativo restaurado. Quaisquer recursos que você não especificar na regra incluir não serão incluídos no aplicativo restaurado.
- **Você seleciona uma regra de exclusão com namespaces originais (in-loc restore):** Os recursos que você especificar para serem excluídos não serão restaurados e permanecerão inalterados. Os recursos que você não especificar para excluir serão restaurados do snapshot ou backup. Todos os dados em volumes persistentes serão excluídos e recriados se o StatefulSet correspondente fizer parte dos recursos filtrados.
- **Você seleciona uma regra de exclusão com novos namespaces:** Use a regra para selecionar os recursos específicos que deseja remover do aplicativo restaurado. Os recursos que você não especificar para excluir serão restaurados do snapshot ou backup.

As regras são incluir ou excluir tipos. Regras que combinem inclusão e exclusão de recursos não estão disponíveis.

Passos

1. Depois de escolher filtrar recursos e selecionar uma opção incluir ou excluir no assistente Restaurar aplicativo, selecione **Adicionar regra de inclusão** ou **Adicionar regra de exclusão**.



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

2. Configure a regra de filtro:



Você deve especificar pelo menos um namespace, rótulo ou GVK. Certifique-se de que todos os recursos que você mantém após as regras de filtro são suficientes para manter o aplicativo restaurado em um estado saudável.

- a. Selecione um namespace específico para a regra. Se você não fizer uma seleção, todos os namespaces serão usados no filtro.



Se o seu aplicativo originalmente continha vários namespaces e você o restaura para novos namespaces, todos os namespaces serão criados mesmo que eles não contenham recursos.

- b. (Opcional) Digite um nome de recurso.
- c. (Opcional) **Seletor de etiquetas:** Inclua a "seletor de etiquetas" para adicionar à regra. O seletor de etiquetas é utilizado para filtrar apenas os recursos que correspondem à etiqueta selecionada.

- d. (Opcional) Selecione **Use GVK (GroupVersionKind) definido para filtrar recursos** para opções de filtragem adicionais.



Se você usar um filtro GVK, você deve especificar versão e tipo.

- i. (Opcional) **Group**: Na lista suspensa, selecione o grupo da API do Kubernetes.
- ii. **Kind**: Na lista suspensa, selecione o esquema de objeto para o tipo de recurso do Kubernetes a ser usado no filtro.
- iii. **Versão**: Selecione a versão da API do Kubernetes.

3. Revise a regra criada com base em suas entradas.

4. Selecione **Adicionar**.



Você pode criar quantos recursos incluir e excluir regras quiser. As regras aparecem no resumo do aplicativo de restauração antes de iniciar a operação.

Migre do storage econômico do ONTAP nas para o storage ONTAP-nas

Você pode usar um Astra Control "[restauração de aplicativo](#)" ou "[clone de aplicativo](#)" uma operação para migrar volumes de aplicações de uma classe de storage com o suporte `ontap-nas-economy` do , que permite opções de proteção limitada de aplicações, para uma classe de storage com o respaldo `ontap-nas` de sua ampla gama de opções de proteção Astra Control. A operação clone ou restauração migra volumes baseados em Qtree que usam um `ontap-nas-economy` back-end para volumes padrão suportados `ontap-nas` pelo . Os volumes, independentemente de serem `ontap-nas-economy` apenas suportados ou mistos, serão migrados para a classe de storage de destino. Após a conclusão da migração, as opções de proteção não são mais limitadas.

Complicações de restauração no local para um aplicativo que compartilha recursos com outro aplicativo

Você pode executar uma operação de restauração no local em um aplicativo que compartilhe recursos com outro aplicativo e produza resultados não intencionais. Todos os recursos compartilhados entre os aplicativos são substituídos quando uma restauração no local é executada em um dos aplicativos.

O seguinte é um cenário de exemplo que cria uma situação indesejável ao usar a replicação do NetApp SnapMirror para uma restauração:

1. Você define o aplicativo `app1` usando o namespace `ns1`.
2. Você configura uma relação de replicação para ``app1`o` .
3. Você define o `app2` aplicativo (no mesmo cluster) usando os namespaces `ns1 ns2`.
4. Você configura uma relação de replicação para ``app2`o` .
5. Inverte a replicação para `app2`o` . Isso faz com que o ``app1` aplicativo no cluster de origem seja desativado.

Replique aplicativos para um sistema remoto usando a tecnologia SnapMirror

Com o Astra Control, você pode criar continuidade dos negócios para suas aplicações com RPO baixo (objetivo do ponto de recuperação) e rto baixo (objetivo do tempo de recuperação) usando funcionalidades de replicação assíncrona da tecnologia NetApp

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

Para obter uma comparação entre backups/restaurações e replicação, "[Conceitos de proteção de dados](#)" consulte .

Você pode replicar aplicativos em diferentes cenários, como os seguintes cenários somente no local, híbridos e multicloud:

- Local A no local B para local B
- No local para a nuvem com o Cloud Volumes ONTAP
- Nuvem com Cloud Volumes ONTAP no local
- Nuvem com Cloud Volumes ONTAP para nuvem (entre diferentes regiões no mesmo fornecedor de nuvem ou para diferentes fornecedores de nuvem)

O Astra Control pode replicar aplicações entre clusters no local, no local para a nuvem (usando o Cloud Volumes ONTAP) ou entre nuvens (Cloud Volumes ONTAP para Cloud Volumes ONTAP).



Você pode replicar simultaneamente um aplicativo diferente (em execução no outro cluster ou site) na direção oposta. Por exemplo, os aplicativos A, B, C podem ser replicados do Datacenter 1 para o Datacenter 2; e os aplicativos X, Y, Z podem ser replicados do Datacenter 2 para o Datacenter 1.

Com o Astra Control, você pode fazer as seguintes tarefas relacionadas a replicação de aplicações:

- [Configure uma relação de replicação](#)
- [Colocar um aplicativo replicado on-line no cluster de destino \(failover\)](#)
- [Ressincronizar uma falha na replicação](#)
- [Replicação reversa da aplicação](#)
- [Falha de aplicativos para o cluster de origem original](#)
- [Excluir uma relação de replicação de aplicativos](#)

Pré-requisitos de replicação

A replicação de aplicações Astra Control requer que os seguintes pré-requisitos sejam atendidos antes de começar:

- **Clusters ONTAP:**
 - **Trident:** O Astra Trident versão 22,07 ou posterior deve existir nos clusters do Kubernetes de origem e destino que utilizam o ONTAP como back-end.
 - **Licenças:** As licenças assíncronas do ONTAP SnapMirror usando o pacote proteção de dados devem estar ativadas nos clusters ONTAP de origem e destino. "[Visão geral do licenciamento do SnapMirror no ONTAP](#)" Consulte para obter mais informações.
- **Emparelhamento:**
 - **Cluster e SVM:** Clusters do ONTAP e o SVM do host precisam estar emparelhados. "[Visão geral do peering de cluster e SVM](#)" Consulte para obter mais informações.
 - **Trident e SVM:** O SVM remoto emparelhado deve estar disponível no Astra Trident no cluster de destino.

- **Astra Control Center:**



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

- **Clusters gerenciados:** Os seguintes clusters precisam ser adicionados e gerenciados pelo Astra Control, de preferência em diferentes domínios ou locais de falha:
 - Fonte do cluster do Kubernetes
 - Cluster de destino Kubernetes
 - Clusters associados do ONTAP
- **Contas de usuário:** Quando você adiciona um back-end de storage do ONTAP ao Centro de Controle Astra, aplique credenciais de usuário com a função "admin". Essa função tem métodos de acesso `http` e `ontapi` é habilitada nos clusters de origem e destino do ONTAP. "[Gerenciar contas de usuário na documentação do ONTAP](#)" Consulte para obter mais informações.
- **Configuração Astra Trident / ONTAP:** O Astra Control Center requer que você configure pelo menos uma classe de storage compatível com replicação para clusters de origem e destino.



A replicação do Astra Control é compatível com aplicações que usam uma única classe de storage. Ao adicionar um aplicativo a um namespace, verifique se o aplicativo tem a mesma classe de armazenamento que outros aplicativos no namespace. Ao adicionar um PVC a um aplicativo replicado, verifique se o novo PVC tem a mesma classe de armazenamento que outros PVCs no namespace.

Configure uma relação de replicação

A configuração de uma relação de replicação envolve o seguinte:

- Escolhendo com que frequência você deseja que o Astra Control faça Snapshot de uma aplicação (que inclui os recursos do Kubernetes da aplicação, bem como os snapshots de volume para cada um dos volumes da aplicação)
- Escolha do cronograma de replicação (incluindo recursos do Kubernetes e dados de volume persistente)
- Definir o tempo para a captura instantânea

Passos

1. Na navegação à esquerda do Astra Control, selecione **Applications**.
2. Na página da aplicação, selecione a guia **proteção de dados > replicação**.
3. Na guia proteção de dados > replicação, selecione **Configurar política de replicação**. Ou, na caixa proteção do aplicativo, selecione a opção ações e selecione **Configurar política de replicação**.
4. Introduza ou selecione as seguintes informações:
 - **Cluster de destino:** Insira um cluster de destino diferente da origem.
 - **Classe de armazenamento de destino:** Selecione ou insira a classe de armazenamento que usa o SVM emparelhado no cluster ONTAP de destino.
 - **Replication type:** "Asynchronous" é atualmente o único tipo de replicação disponível.
 - * Namespace de destino*: Insira namespaces de destino novos ou existentes para o cluster de destino.
 - (Opcional) Adicione namespaces adicionais selecionando **Add namespace** e escolhendo o

namespace na lista suspensa.

- **Frequência de replicação:** Defina com que frequência você deseja que o Astra Control tire um Snapshot e o replique para seu destino.
- **Offset:** Defina o número de minutos a partir do topo da hora em que deseja que o Astra Control tire uma Snapshot. Você pode querer usar um deslocamento para que ele não coincida com outras operações agendadas.



Offset programações de backup e replicação para evitar sobreposições de agendamento. Por exemplo, execute backups no topo da hora a cada hora e programe a replicação para começar com um deslocamento de 5 minutos e um intervalo de 10 minutos.

5. Selecione **seguinte**, reveja o resumo e selecione **Guardar**.



No início, o status exibe "APP-mirror" antes que a primeira programação ocorra.

O Astra Control cria um Snapshot de aplicação usado para replicação.

6. Para ver o status do instantâneo do aplicativo, selecione a guia **aplicativos > instantâneos**.

O nome do instantâneo usa o formato `replication-schedule-<string>` do . O Astra Control retém o último Snapshot usado para replicação. Quaisquer snapshots de replicação mais antigos são excluídos após a conclusão bem-sucedida da replicação.

Resultado

Isso cria a relação de replicação.

O Astra Control conclui as seguintes ações como resultado do estabelecimento do relacionamento:

- Cria um namespace no destino (se ele não existir)
- Cria um PVC no namespace de destino correspondente aos PVCs do aplicativo de origem.
- Obtém um Snapshot inicial consistente com o aplicativo.
- Estabelece a relação do SnapMirror para volumes persistentes usando o Snapshot inicial.

A página proteção de dados mostra o estado e o estado da relação de replicação: `<Health status> | estado do ciclo de vida da relação`

Por exemplo: Normal | estabelecido

Saiba mais sobre os estados de replicação e o status no final deste tópico.

Colocar um aplicativo replicado on-line no cluster de destino (failover)

Com o Astra Control, você pode fazer failover de aplicações replicadas para um cluster de destino. Este procedimento interrompe a relação de replicação e coloca a aplicação online no cluster de destino. Este procedimento não pára a aplicação no cluster de origem se estiver operacional.

Passos

1. Na navegação à esquerda do Astra Control, selecione **Applications**.
2. Na página da aplicação, selecione a guia **proteção de dados > replicação**.

3. Na guia proteção de dados > replicação, no menu ações, selecione **failover**.
4. Na página failover, revise as informações e selecione **failover**.

Resultado

As seguintes ações ocorrem como resultado do procedimento de failover:

- No cluster de destino, o aplicativo é iniciado com base no snapshot replicado mais recente.
- O cluster de origem e a aplicação (se operacional) não são interrompidos e continuarão a ser executados.
- O estado de replicação muda para "failover" e, em seguida, para "failover" quando ele for concluído.
- A política de proteção do aplicativo de origem é copiada para o aplicativo de destino com base nas programações presentes no aplicativo de origem no momento do failover.
- Se o aplicativo de origem tiver um ou mais ganchos de execução pós-restauração ativados, esses ganchos de execução serão executados para o aplicativo de destino.
- O Astra Control mostra a aplicação nos clusters de origem e destino e sua respectiva integridade.

Ressincronizar uma falha na replicação

A operação ressincronizada restabelece a relação de replicação. Você pode escolher a origem da relação para reter os dados no cluster de origem ou destino. Esta operação restabelece as relações SnapMirror para iniciar a replicação de volume na direção da escolha.

O processo pára o aplicativo no novo cluster de destino antes de restabelecer a replicação.



Durante o processo de ressincronização, o estado do ciclo de vida mostra como "estabelecendo".

Passos

1. Na navegação à esquerda do Astra Control, selecione **Applications**.
2. Na página da aplicação, selecione a guia **proteção de dados > replicação**.
3. Na guia proteção de dados > replicação, no menu ações, selecione **Resync**.
4. Na página Resync, selecione a instância do aplicativo de origem ou destino que contém os dados que você deseja preservar.



Escolha a fonte ressincronizada cuidadosamente, pois os dados no destino serão sobrescritos.

5. Selecione **Resync** para continuar.
6. Digite "ressync" para confirmar.
7. Selecione **Sim, ressincronizar** para concluir.

Resultado

- A página replicação mostra "estabelecer" como o status da replicação.
- O Astra Control interrompe a aplicação no novo cluster de destino.
- O Astra Control restabelece a replicação de volume persistente na direção selecionada usando o SnapMirror Resync.
- A página replicação mostra a relação atualizada.

Replicação reversa da aplicação

Esta é a operação planejada para mover o aplicativo para o cluster de destino e continuar replicando de volta para o cluster de origem original. O Astra Control interrompe a aplicação no cluster de origem e replica os dados para o destino antes de fazer failover da aplicação para o cluster de destino.

Nesta situação, você está trocando a origem e o destino. O cluster de origem original torna-se o novo cluster de destino e o cluster de destino original torna-se o novo cluster de origem.

Passos

1. Na navegação à esquerda do Astra Control, selecione **Applications**.
2. Na página da aplicação, selecione a guia **proteção de dados > replicação**.
3. Na guia proteção de dados > replicação, no menu ações, selecione **Reverse replication**.
4. Na página Reverse Replication (Reverse Replication), reveja as informações e selecione **Reverse replication** (Reverse replication) para continuar.

Resultado

As seguintes ações ocorrem como resultado da replicação reversa:

- Um Snapshot é tirado dos recursos do Kubernetes do aplicativo de origem original.
- Os pods do aplicativo de origem original são interrompidos graciosamente ao excluir os recursos do Kubernetes do aplicativo (deixando PVCs e PVS no lugar).
- Depois que os pods são desativados, os snapshots dos volumes do aplicativo são feitos e replicados.
- As relações do SnapMirror são quebradas, tornando os volumes de destino prontos para leitura/gravação.
- Os recursos do Kubernetes do aplicativo são restaurados a partir do Snapshot pré-encerramento, usando os dados de volume replicados após o desligamento do aplicativo de origem original.
- A replicação é restabelecida na direção inversa.

Falha de aplicativos para o cluster de origem original

Com o Astra Control, você pode obter "failback" após uma operação de failover usando a seguinte sequência de operações. Nesse fluxo de trabalho para restaurar a direção de replicação original, o Astra Control replica (ressincroniza) qualquer aplicação muda de volta para o cluster de origem original antes de reverter a direção de replicação.

Esse processo começa a partir de um relacionamento que concluiu um failover para um destino e envolve as seguintes etapas:

- Comece com um estado com falha em excesso.
- Ressincronizar o relacionamento.
- Inverta a replicação.

Passos

1. Na navegação à esquerda do Astra Control, selecione **Applications**.
2. Na página da aplicação, selecione a guia **proteção de dados > replicação**.
3. Na guia proteção de dados > replicação, no menu ações, selecione **Resync**.
4. Para uma operação de failback, escolha o aplicativo failover com falha como a origem da operação ressincronizada (preservando qualquer failover pós-escrito de dados).

5. Digite "ressync" para confirmar.
6. Selecione **Sim, ressincronizar** para concluir.
7. Após a conclusão da ressincronização, na guia proteção de dados > replicação, no menu ações, selecione **Reverse replication**.
8. Na página Reverse Replication (Reverse Replication), reveja as informações e selecione **Reverse replication**.

Resultado

Isso combina os resultados das operações "ressincronização" e "relação reversa" para colocar o aplicativo on-line no cluster de origem original com replicação retomada para o cluster de destino original.

Excluir uma relação de replicação de aplicativos

A exclusão do relacionamento resulta em dois aplicativos separados sem relação entre eles.

Passos

1. Na navegação à esquerda do Astra Control, selecione **Applications**.
2. Na página da aplicação, selecione a guia **proteção de dados > replicação**.
3. Na guia proteção de dados > replicação, na caixa proteção do aplicativo ou no diagrama de relacionamento, selecione **Excluir relação de replicação**.

Resultado

As seguintes ações ocorrem como resultado da exclusão de uma relação de replicação:

- Se o relacionamento for estabelecido, mas o aplicativo ainda não tiver sido colocado on-line no cluster de destino (failover), o Astra Control manterá os PVCs criados durante a inicialização, deixará um aplicativo gerenciado "vazio" no cluster de destino e manterá o aplicativo de destino para manter todos os backups que possam ter sido criados.
- Se o aplicativo for colocado on-line no cluster de destino (failover), o Astra Control manterá PVCs e aplicativos de destino. Os aplicativos de origem e destino agora são tratados como aplicativos independentes. As programações de backup permanecem em ambos os aplicativos, mas não estão associadas umas às outras.

Estado de integridade da relação de replicação e estados do ciclo de vida da relação

Astra Control exibe a integridade do relacionamento e os estados do ciclo de vida da relação de replicação.

Estados de integridade da relação de replicação

Os seguintes Estados indicam a integridade da relação de replicação:

- **Normal:** O relacionamento está estabelecendo ou estabeleceu, e o instantâneo mais recente foi transferido com sucesso.
- **Aviso:** O relacionamento está falhando ou falhou (e, portanto, não está mais protegendo o aplicativo de origem).
- **Crítica**
 - A relação está estabelecendo ou falhou e a última tentativa de reconciliar falhou.
 - A relação é estabelecida, e a última tentativa de reconciliar a adição de um novo PVC está falhando.
 - A relação é estabelecida (assim, um Snapshot bem-sucedido replicou e é possível fazer failover), mas

o Snapshot mais recente falhou ou falhou em replicar.

estados do ciclo de vida da replicação

Os seguintes estados refletem as diferentes fases do ciclo de vida de replicação:

- *** Estabelecimento***: Uma nova relação de replicação está sendo criada. O Astra Control cria um namespace, se necessário, cria declarações de volume persistentes (PVCs) em novos volumes no cluster de destino e cria relações SnapMirror. Esse status também pode indicar que a replicação está ressinchronizando ou invertendo a replicação.
- **Estabelecido**: Existe uma relação de replicação. O Astra Control verifica periodicamente se os PVCs estão disponíveis, verifica o relacionamento de replicação, cria periodicamente snapshots do aplicativo e identifica quaisquer novos PVCs de origem no aplicativo. Nesse caso, o Astra Control cria os recursos para incluí-los na replicação.
- *** Com falha***: O Astra Control quebra os relacionamentos do SnapMirror e restaura os recursos do Kubernetes do aplicativo a partir do último Snapshot do aplicativo replicado com sucesso.
- *** Failover***: O Astra Control pára de replicar a partir do cluster de origem, usa o Snapshot da aplicação mais recente (bem-sucedido) replicado no destino e restaura os recursos do Kubernetes.
- **Ressinchronização**: O Astra Control ressinchroniza os novos dados na origem ressinchronizada para o destino ressinchronizado usando o SnapMirror Resync. Esta operação pode substituir alguns dos dados no destino com base na direção da sincronização. O Astra Control interrompe a execução da aplicação no namespace de destino e remove a aplicação Kubernetes. Durante o processo de ressinchronização, o status mostra como "estabelecendo".
- **Reversing**: A é a operação planejada para mover o aplicativo para o cluster de destino, continuando a replicar de volta para o cluster de origem original. O Astra Control interrompe a aplicação no cluster de origem, replica os dados para o destino antes de fazer failover da aplicação para o cluster de destino. Durante a replicação reversa, o status é exibido como "estabelecendo".
- **Excluindo**:
 - Se a relação de replicação tiver sido estabelecida, mas ainda não tiver falha, o Astra Control removerá PVCs criados durante a replicação e excluirá o aplicativo gerenciado de destino.
 - Se a replicação já tiver falhado, o Astra Control manterá os PVCs e a aplicação de destino.

Clonar e migrar aplicações

Você pode clonar um aplicativo existente para criar um aplicativo duplicado no mesmo cluster do Kubernetes ou em outro cluster. Quando o Astra Control clona uma aplicação, ele cria um clone de sua configuração de aplicação e storage persistente.

A clonagem pode ajudar se você precisar mover aplicações e storage de um cluster Kubernetes para outro. Por exemplo, você pode querer mover workloads por meio de um pipeline de CI/CD e entre namespaces do Kubernetes. Você pode usar a IU do Astra Control Center ou "[API Astra Control](#)" clonar e migrar aplicações.



Se você adicionar um filtro de namespace a um gancho de execução que é executado após uma operação de restauração ou clone e a origem e destino de restauração ou clone estiverem em namespaces diferentes, o filtro de namespace será aplicado somente ao namespace de destino.

Antes de começar

- **Verificar volumes de destino**: Se você clonar para uma classe de armazenamento diferente, verifique se

a classe de armazenamento usa o mesmo modo de acesso de volume persistente (por exemplo, ReadWriteMany). A operação de clone falhará se o modo de acesso ao volume persistente de destino for diferente. Por exemplo, se o volume persistente de origem usar o modo de acesso RWX, selecionar uma classe de armazenamento de destino que não seja capaz de fornecer RWX, como discos gerenciados do Azure, AWS EBS, Google Persistent Disk ou `ontap-san`, fará com que a operação de clone falhe. Para obter mais informações sobre os modos de acesso de volume persistente, consulte "[Kubernetes](#)" a documentação.

- Para clonar aplicativos para um cluster diferente, você precisa garantir que as instâncias de nuvem que contêm os clusters de origem e destino (se não forem os mesmos) tenham um bucket padrão. Você precisará atribuir um bucket padrão para cada instância da nuvem.
- Durante as operações de clone, os aplicativos que precisam de um recurso do IngressClass ou webhooks para funcionar corretamente não devem ter esses recursos já definidos no cluster de destino.

Durante a clonagem de aplicativos em ambientes OpenShift, o Astra Control Center precisa permitir que o OpenShift monte volumes e altere a propriedade dos arquivos. Por causa disso, você precisa configurar uma política de exportação de volume ONTAP para permitir essas operações. Você pode fazer isso com os seguintes comandos:



1. `export-policy rule modify -vserver <storage virtual machine name> -policyname <policy name> -ruleindex 1 -superuser sys`
2. `export-policy rule modify -vserver <storage virtual machine name> -policyname <policy name> -ruleindex 1 -anon 65534`

Limitações de clone

- **Classes de armazenamento explícitas:** Se você implantar um aplicativo com uma classe de armazenamento explicitamente definida e precisar clonar o aplicativo, o cluster de destino deverá ter a classe de armazenamento especificada originalmente. Clonar um aplicativo com uma classe de storage definida explicitamente para um cluster que não tenha a mesma classe de storage falhará.
- *** Classe de armazenamento com suporte de economia de ONTAP-nas*:** Se o seu aplicativo usar uma classe de armazenamento apoiada pelo `ontap-nas-economy` driver, a parte de backup de uma operação de clone será disruptiva. O aplicativo de origem não estará disponível até que o backup esteja concluído. A parte de restauração da operação de clone não causa interrupções.
- **Clones e restrições de usuário:** Qualquer usuário membro com restrições de namespace por nome/ID de namespace ou por rótulos de namespace pode clonar ou restaurar um aplicativo para um novo namespace no mesmo cluster ou para qualquer outro cluster na conta de sua organização. No entanto, o mesmo usuário não pode acessar o aplicativo clonado ou restaurado no novo namespace. Depois que um novo namespace é criado por uma operação de clone ou restauração, o administrador/proprietário da conta pode editar a conta de usuário membro e atualizar as restrições de função para o usuário afetado conceder acesso ao novo namespace.
- **Os clones usam buckets padrão:** Durante um backup do aplicativo ou restauração do aplicativo, você pode especificar opcionalmente um ID de bucket. Uma operação de clone de aplicativo, no entanto, sempre usa o bucket padrão que foi definido. Não há opção de alterar buckets para um clone. Se você quiser controlar qual balde é usado, você pode "[altere o intervalo padrão](#)" ou fazer um "[backup](#)" seguido por um "[restaurar](#)" separadamente.
- **Com o Jenkins CI:** Se você clonar uma instância implantada pelo operador do Jenkins CI, precisará restaurar manualmente os dados persistentes. Esta é uma limitação do modelo de implantação do aplicativo.
- **Com buckets do S3:** Os buckets do S3 no Astra Control Center não relatam a capacidade disponível. Antes de fazer backup ou clonar aplicativos gerenciados pelo Astra Control Center, verifique as informações do bucket no sistema de gerenciamento ONTAP ou StorageGRID.

Considerações sobre OpenShift

- * Clusters e versões OpenShift*: Se você clonar um aplicativo entre clusters, os clusters de origem e destino devem ser a mesma distribuição do OpenShift. Por exemplo, se você clonar um aplicativo de um cluster OpenShift 4,7, use um cluster de destino que também é OpenShift 4,7.
- * Projetos e UIDs*: Quando você cria um projeto para hospedar um aplicativo em um cluster OpenShift, o projeto (ou namespace Kubernetes) recebe um UID SecurityContext. Para ativar o Astra Control Center para proteger seu aplicativo e mover o aplicativo para outro cluster ou projeto no OpenShift, você precisa adicionar políticas que permitam que o aplicativo seja executado como qualquer UID. Como exemplo, os seguintes comandos OpenShift CLI concedem as políticas apropriadas a um aplicativo WordPress.

```
oc new-project wordpress
oc adm policy add-scc-to-group anyuid system:serviceaccounts:wordpress
oc adm policy add-scc-to-user privileged -z default -n wordpress
```

Passos

1. Selecione **aplicações**.
2. Execute um dos seguintes procedimentos:
 - Selecione o menu Opções na coluna **ações** para o aplicativo desejado.
 - Selecione o nome da aplicação pretendida e selecione a lista pendente de estado no canto superior direito da página.
3. Selecione **Clone**.
4. Especifique detalhes para o clone:
 - Introduza um nome.
 - Escolha um cluster de destino para o clone.
 - Insira namespaces de destino para o clone. Cada namespace de origem associado ao aplicativo mapeia para o namespace de destino que você define.



O Astra Control cria novos namespaces de destino como parte da operação clone. Namespaces de destino que você especificar não devem estar presentes no cluster de destino.

- Selecione **seguinte**.
- Escolha 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.
 - Se você optar por clonar de um instantâneo ou backup existente, escolha o instantâneo ou o backup que deseja usar.
- Selecione **seguinte**.
- Escolha manter a classe de armazenamento original associada ao aplicativo ou selecionar uma classe de armazenamento diferente.



Você pode migrar a classe de armazenamento de um aplicativo para uma classe de armazenamento de provedor de nuvem nativa ou outra classe de armazenamento suportada, para uma classe de armazenamento suportada pelo `ontap-nas` mesmo cluster ou copiar o aplicativo para outro cluster com uma classe de armazenamento suportada pelo `ontap-nas-economy` driver.



Se você selecionar uma classe de armazenamento diferente e essa classe de armazenamento não existir no momento da restauração, um erro será retornado.

5. Selecione **seguinte**.
6. Reveja as informações sobre o clone e selecione **Clone**.

Resultado

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

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



Após uma operação de proteção de dados (clone, backup ou restauração) e subsequente redimensionamento persistente de volume, há até vinte minutos de atraso antes que o novo tamanho de volume seja exibido na IU. A operação de proteção de dados é bem-sucedida em minutos. Você pode usar o software de gerenciamento do back-end de storage para confirmar a alteração no tamanho do volume.

Gerenciar ganchos de execução de aplicativos

Um gancho de execução é uma ação personalizada que você pode configurar para ser executada em conjunto com uma operação de proteção de dados de um aplicativo gerenciado. Por exemplo, se você tiver um aplicativo de banco de dados, poderá usar um gancho de execução para pausar todas as transações de banco de dados antes de um snapshot e retomar as transações após a conclusão do snapshot. Isso garante snapshots consistentes com aplicativos.

Tipos de ganchos de execução

O Astra Control é compatível com os seguintes tipos de ganchos de execução, com base em quando eles podem ser executados:

- Pré-instantâneo
- Pós-snapshot
- Pré-backup
- Pós-backup
- Pós-restauração

Filtros de gancho de execução

Quando você adiciona ou edita um gancho de execução a um aplicativo, você pode adicionar filtros a um gancho de execução para controlar quais contentores o gancho corresponderá. Os filtros são úteis para aplicativos que usam a mesma imagem de contentor em todos os contentores, mas podem usar cada imagem para um propósito diferente (como o Elasticsearch). Os filtros permitem criar cenários onde os ganchos de execução serão executados em alguns desses contentores idênticos, mas não necessariamente todos eles. Se você criar vários filtros para um único gancho de execução, eles serão combinados com um operador LÓGICO E. Você pode ter até 10 filtros ativos por gancho de execução.

Cada filtro que você adicionar a um gancho de execução usa uma expressão regular para corresponder a containers em seu cluster. Quando um gancho corresponde a um recipiente, o gancho executará o script associado nesse recipiente.



As expressões regulares para filtros usam a sintaxe da expressão regular 2 (RE2), que não suporta a criação de um filtro que exclui contentores da lista de correspondências.

Para obter informações sobre a sintaxe que o Astra Control suporta para expressões regulares em filtros de gancho de execução, "[Suporte à sintaxe da expressão regular 2 \(RE2\)](#)" consulte .

Notas importantes sobre ganchos de execução personalizados

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



Como os ganchos de execução geralmente reduzem ou desativam completamente a funcionalidade do aplicativo em que estão sendo executados, você deve sempre tentar minimizar o tempo que seus ganchos de execução personalizados levam para serem executados. Se você iniciar uma operação de backup ou snapshot com ganchos de execução associados, mas depois cancelá-la, os ganchos ainda poderão ser executados se a operação de backup ou snapshot já tiver começado. Isso significa que a lógica usada em um gancho de execução pós-backup não pode assumir que o backup foi concluído.

- Um gancho de execução deve usar um script para executar ações. Muitos ganchos de execução podem referenciar o mesmo script.
- O Astra Control requer que os scripts que os ganchos de execução usam sejam escritos no formato de scripts shell executáveis.
- O tamanho do script está limitado a 96kbMB.
- O Astra Control usa configurações de gancho de execução e quaisquer critérios correspondentes para determinar quais ganchos são aplicáveis a uma operação de snapshot, backup ou restauração.
- Todas as falhas no gancho de execução são falhas suaves; outros ganchos e a operação de proteção de dados ainda são tentados, mesmo que um gancho falhe. No entanto, quando um gancho falha, um evento de aviso é registrado no log de eventos da página **atividade**.
- Para criar, editar ou excluir ganchos de execução, você deve ser um usuário com permissões de proprietário, administrador ou membro.
- Se um gancho de execução demorar mais de 25 minutos para ser executado, o gancho falhará, criando uma entrada de log de eventos com um código de retorno de "N/A". Qualquer instantâneo afetado expira e será marcado como falhou, com uma entrada de log de eventos resultante anotando o tempo limite.
- Para operações de proteção de dados ad hoc, todos os eventos de gancho são gerados e salvos no log de eventos da página **atividade**. No entanto, para operações agendadas de proteção de dados, apenas eventos de falha de gancho são registrados no log de eventos (eventos gerados pelas próprias operações de proteção de dados agendadas ainda são registrados).
- Se o Astra Control Center falhar em um aplicativo de origem replicado para o aplicativo de destino, todos os ganchos de execução pós-restauração ativados para o aplicativo de origem serão executados para o aplicativo de destino após a conclusão do failover.
- Se você adicionar um filtro de namespace a um gancho de execução que é executado após uma operação de restauração ou clone e a origem e destino de restauração ou clone estiverem em namespaces diferentes, o filtro de namespace será aplicado somente ao namespace de destino.

Ordem de execução

Quando uma operação de proteção de dados é executada, os eventos de gancho de execução ocorrem na seguinte ordem:

1. Todos os ganchos de execução personalizados de pré-operação aplicáveis são executados nos contentores apropriados. Você pode criar e executar quantos ganchos de pré-operação personalizados você precisar, mas a ordem de execução desses ganchos antes da operação não é garantida nem configurável.
2. A operação de proteção de dados é realizada.
3. Todos os ganchos de execução pós-operação personalizados aplicáveis são executados nos contentores apropriados. Você pode criar e executar quantos ganchos de pós-operação personalizados você precisar, mas a ordem de execução desses ganchos após a operação não é garantida nem configurável.

Se você criar vários ganchos de execução do mesmo tipo (por exemplo, pré-snapshot), a ordem de execução desses ganchos não será garantida. No entanto, a ordem de execução de ganchos de diferentes tipos é garantida. Por exemplo, a ordem de execução de uma configuração que tenha todos os cinco tipos diferentes de ganchos seria assim:

1. Ganchos pré-backup executados
2. Ganchos pré-instantâneos executados
3. Ganchos pós-snapshot executados
4. Ganchos pós-backup executados
5. Ganchos pós-restauração executados

Você pode ver um exemplo dessa configuração no cenário número 2 da tabela em [Determine se um gancho vai funcionar](#).



Você deve sempre testar seus scripts de gancho de execução antes de habilitá-los em um ambiente de produção. Você pode usar o comando 'kubectl exec' para testar convenientemente os scripts. Depois de habilitar os ganchos de execução em um ambiente de produção, teste os snapshots e backups resultantes para garantir que eles sejam consistentes. Você pode fazer isso clonando o aplicativo para um namespace temporário, restaurando o snapshot ou o backup e testando o aplicativo.

Determine se um gancho vai funcionar

Use a tabela a seguir para ajudar a determinar se um gancho de execução personalizado será executado para seu aplicativo.

Observe que todas as operações de aplicativos de alto nível consistem em executar uma das operações básicas de snapshot, backup ou restauração. Dependendo do cenário, uma operação de clone pode consistir em várias combinações dessas operações, portanto, o que os ganchos de execução executados por uma operação de clone variará.

As operações de restauração no local exigem um snapshot ou backup existente, portanto, essas operações não executam snapshots ou ganchos de backup.

Se você iniciar, mas cancelar um backup que inclua um snapshot e houver ganchos de execução associados, alguns ganchos podem ser executados e outros podem não. Isso significa que um gancho de execução pós-backup não pode assumir que o backup foi concluído. Tenha em mente os seguintes pontos para backups cancelados com ganchos de execução associados:



- Os ganchos de pré-backup e pós-backup são sempre executados.
- Se o backup incluir um novo snapshot e o snapshot tiver iniciado, os ganchos pré-snapshot e pós-snapshot serão executados.
- Se o backup for cancelado antes do início do snapshot, os ganchos pré-snapshot e pós-snapshot não serão executados.

Cenário	Operação	Snapshot existente	Backup existente	Namespa ce	Cluster	Os ganchos instantâneos funcionam	Ganchos de segurança executados	Restaurar os ganchos de funcionamento
1	Clone	N	N	Novo	O mesmo	Y	N	Y
2	Clone	N	N	Novo	Diferente	Y	Y	Y
3	Clone ou restauração	Y	N	Novo	O mesmo	N	N	Y
4	Clone ou restauração	N	Y	Novo	O mesmo	N	N	Y
5	Clone ou restauração	Y	N	Novo	Diferente	N	N	Y
6	Clone ou restauração	N	Y	Novo	Diferente	N	N	Y
7	Restaurar	Y	N	Existente	O mesmo	N	N	Y
8	Restaurar	N	Y	Existente	O mesmo	N	N	Y
9	Snapshot	N/A.	N/A.	N/A.	N/A.	Y	N/A.	N/A.
10	Backup	N	N/A.	N/A.	N/A.	Y	Y	N/A.
11	Backup	Y	N/A.	N/A.	N/A.	N	N	N/A.

Exemplos de gancho de execução

Visite o "[Projeto NetApp Verda GitHub](#)" para baixar ganchos de execução reais para aplicativos populares, como Apache Cassandra e Elasticsearch. Você também pode ver exemplos e obter ideias para estruturar seus próprios ganchos de execução personalizados.

Ver ganchos de execução existentes

Você pode exibir ganchos de execução personalizados existentes para um aplicativo.

Passos

1. Vá para **aplicativos** e selecione o nome de um aplicativo gerenciado.
2. Selecione a guia **ganchos de execução**.

Pode visualizar todos os ganchos de execução ativados ou desativados na lista resultante. Você pode ver o status de um gancho, quantos contentores ele corresponde, o tempo de criação e quando ele é executado (pré ou pós-operação). Você pode selecionar o + ícone ao lado do nome do gancho para expandir a lista de contentores em que ele será executado. Para ver os logs de eventos ao redor dos ganchos de execução para este aplicativo, vá para a guia **atividade**.

Exibir scripts existentes

Você pode visualizar os scripts carregados existentes. Você também pode ver quais scripts estão em uso, e quais ganchos estão usando, nesta página.

Passos

1. Vá para **conta**.
2. Selecione a guia **Scripts**.

Você pode ver uma lista de scripts carregados existentes nesta página. A coluna **usada por** mostra quais ganchos de execução estão usando cada script.

Adicione um script

Cada gancho de execução deve usar um script para executar ações. Você pode adicionar um ou mais scripts que os ganchos de execução podem referenciar. Muitos ganchos de execução podem referenciar o mesmo script; isso permite que você atualize muitos ganchos de execução alterando apenas um script.

Passos

1. Vá para **conta**.
2. Selecione a guia **Scripts**.
3. Selecione **Adicionar**.
4. Execute um dos seguintes procedimentos:
 - Carregue um script personalizado.
 - i. Selecione a opção **Upload file**.
 - ii. Navegue até um arquivo e carregue-o.
 - iii. Dê ao script um nome exclusivo.
 - iv. (Opcional) Digite quaisquer notas que outros administradores devem saber sobre o script.
 - v. Selecione **Salvar script**.
 - Cole em um script personalizado da área de transferência.
 - i. Selecione a opção **Colar ou tipo**.
 - ii. Selecione o campo de texto e cole o texto do script no campo.

- iii. Dê ao script um nome exclusivo.
 - iv. (Opcional) Digite quaisquer notas que outros administradores devem saber sobre o script.
5. Selecione **Salvar script**.

Resultado

O novo script aparece na lista na guia **Scripts**.

Excluir um script

Você pode remover um script do sistema se ele não for mais necessário e não for usado por nenhum hooks de execução.

Passos

1. Vá para **conta**.
2. Selecione a guia **Scripts**.
3. Escolha um script que você deseja remover e selecione o menu na coluna **ações**.
4. Selecione **Eliminar**.



Se o script estiver associado a um ou mais ganchos de execução, a ação **Delete** não estará disponível. Para excluir o script, primeiro edite os ganchos de execução associados e associe-os a um script diferente.

Crie um gancho de execução personalizado

Você pode criar um gancho de execução personalizado para um aplicativo. [Exemplos de gancho de execução](#) Consulte para obter exemplos de gancho. Você precisa ter permissões de proprietário, administrador ou membro para criar ganchos de execução.



Quando você cria um script shell personalizado para usar como um gancho de execução, lembre-se de especificar o shell apropriado no início do arquivo, a menos que você esteja executando comandos específicos ou fornecendo o caminho completo para um executável.

Passos

1. Selecione **aplicativos** e, em seguida, selecione o nome de um aplicativo gerenciado.
2. Selecione a guia **ganchos de execução**.
3. Selecione **Adicionar**.
4. Na área **Detalhes do gancho**:
 - a. Determine quando o gancho deve funcionar selecionando um tipo de operação no menu suspenso **operação**.
 - b. Introduza um nome exclusivo para o gancho.
 - c. (Opcional) Digite quaisquer argumentos para passar para o gancho durante a execução, pressionando a tecla Enter após cada argumento que você inserir para gravar cada um.
5. (Opcional) na área **Hook Filter Details** (Detalhes do filtro do gancho), você pode adicionar filtros para controlar em quais contentores o gancho de execução é executado:
 - a. Selecione **Adicionar filtro**.
 - b. Na coluna **tipo de filtro gancho**, escolha um atributo no qual filtrar no menu suspenso.

- c. Na coluna **Regex**, insira uma expressão regular para usar como filtro. O Astra Control usa o "[Sintaxe regular expressão 2 \(RE2\) regex](#)".



Se você filtrar o nome exato de um atributo (como um nome do pod) sem nenhum outro texto no campo de expressão regular, uma correspondência de subcadeia será executada. Para corresponder a um nome exato e apenas a esse nome, use a sintaxe exata de correspondência de cadeia de caracteres (por exemplo, `^exact_podname$`).

- d. Para adicionar mais filtros, selecione **Adicionar filtro**.



Vários filtros para um gancho de execução são combinados com um operador LÓGICO E. Você pode ter até 10 filtros ativos por gancho de execução.

6. Quando terminar, selecione **seguinte**.

7. Na área **Script**, execute um dos seguintes procedimentos:

- Adicione um novo script.
 - i. Selecione **Adicionar**.
 - ii. Execute um dos seguintes procedimentos:
 - Carregue um script personalizado.
 - I. Selecione a opção **Upload file**.
 - II. Navegue até um arquivo e carregue-o.
 - III. Dê ao script um nome exclusivo.
 - IV. (Opcional) Digite quaisquer notas que outros administradores devem saber sobre o script.
 - V. Selecione **Salvar script**.
 - Cole em um script personalizado da área de transferência.
 - I. Selecione a opção **Colar ou tipo**.
 - II. Selecione o campo de texto e cole o texto do script no campo.
 - III. Dê ao script um nome exclusivo.
 - IV. (Opcional) Digite quaisquer notas que outros administradores devem saber sobre o script.
- Selecione um script existente na lista.

Isso instrui o gancho de execução a usar este script.

8. Selecione **seguinte**.

9. Reveja a configuração do gancho de execução.

10. Selecione **Adicionar**.

Verifique o estado de um gancho de execução

Depois que uma operação de snapshot, backup ou restauração terminar de ser executada, você pode verificar o estado dos ganchos de execução executados como parte da operação. Você pode usar essas informações de status para determinar se deseja manter o gancho de execução, modificá-lo ou excluí-lo.

Passos

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

2. Selecione a guia **proteção de dados**.
3. Selecione **Snapshots** para ver os snapshots em execução ou **backups** para ver os backups em execução.

O estado **Hook** mostra o status da execução do hook run após a conclusão da operação. Você pode passar o Mouse sobre o estado para obter mais detalhes. Por exemplo, se houver falhas de gancho de execução durante um instantâneo, passar o Mouse sobre o estado de gancho para esse instantâneo fornece uma lista de ganchos de execução com falha. Para ver os motivos de cada falha, você pode verificar a página **atividade** na área de navegação do lado esquerdo.

Exibir o uso do script

Você pode ver quais ganchos de execução usam um script específico na IU da Web do Astra Control.

Passos

1. Selecione **conta**.
2. Selecione a guia **Scripts**.

A coluna **usada por** na lista de scripts contém detalhes sobre os ganchos que estão usando cada script na lista.

3. Selecione as informações na coluna **usado por** para um script em que você está interessado.

Uma lista mais detalhada é exibida, com os nomes de ganchos que estão usando o script e o tipo de operação com os quais eles estão configurados para executar.

Edite um gancho de execução

Você pode editar um gancho de execução se quiser alterar seus atributos, filtros ou o script que ele usa. Você precisa ter permissões de proprietário, administrador ou membro para editar ganchos de execução.

Passos

1. Selecione **aplicativos** e, em seguida, selecione o nome de um aplicativo gerenciado.
2. Selecione a guia **ganchos de execução**.
3. Selecione o menu Opções na coluna **ações** para um gancho que você deseja editar.
4. Selecione **Editar**.
5. Faça as alterações necessárias, selecionando **Next** após concluir cada seção.
6. Selecione **Guardar**.

Desativar um gancho de execução

Você pode desativar um gancho de execução se quiser impedir temporariamente que ele seja executado antes ou depois de um instantâneo de um aplicativo. Você precisa ter permissões de proprietário, Administrador ou Membro para desativar os ganchos de execução.

Passos

1. Selecione **aplicativos** e, em seguida, selecione o nome de um aplicativo gerenciado.
2. Selecione a guia **ganchos de execução**.
3. Selecione o menu Opções na coluna **ações** para um gancho que você deseja desativar.

4. Selecione **Desativar**.

Excluir um gancho de execução

Você pode remover um gancho de execução inteiramente se você não precisar mais dele. Você precisa ter permissões de proprietário, administrador ou membro para excluir ganchos de execução.

Passos

1. Selecione **aplicativos** e, em seguida, selecione o nome de um aplicativo gerenciado.
2. Selecione a guia **ganchos de execução**.
3. Selecione o menu Opções na coluna **ações** para um gancho que você deseja excluir.
4. Selecione **Eliminar**.
5. Na caixa de diálogo resultante, digite "delete" para confirmar.
6. Selecione **Sim, excluir o gancho de execução**.

Para mais informações

- ["Projeto NetApp Verda GitHub"](#)

Monitorar a integridade do aplicativo e do cluster

Exibir um resumo da integridade do aplicativo e do cluster

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

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

Mosaico de aplicações

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

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

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

Blocos de clusters

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

Azulejo dos backends de armazenamento

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

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

Visualize a integridade do cluster e gerencie classes de armazenamento

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

Exibir integridade e detalhes do cluster

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

Passos

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



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

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



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

Altere a classe de armazenamento padrão

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



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

Passos

1. Na IU da Web do Astra Control Center, selecione **clusters**.
2. Na página **clusters**, selecione o cluster que deseja alterar.
3. Selecione a guia **armazenamento**.
4. Selecione a categoria **Storage classes**.
5. Selecione o menu **ações** para a classe de armazenamento que você deseja definir como padrão.
6. Selecione **Definir como padrão**.

Veja a saúde e os detalhes de um aplicativo

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

Passos

1. Na IU do Astra Control Center, selecione **Applications** e, em seguida, selecione o nome de um aplicativo.
2. Reveja as informações.
 - **Status do aplicativo:** 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.
 - **Status da proteção do aplicativo:** Fornece um status de quão bem o aplicativo está protegido:
 - **Totalmente protegido:** O aplicativo tem um agendamento de backup ativo e um backup bem-sucedido com menos de uma semana de idade
 - **Parcialmente protegido:** O aplicativo tem um agendamento de backup ativo, um agendamento de snapshot ativo ou um backup ou snapshot bem-sucedido
 - **Desprotegido:** Aplicativos que não estão totalmente protegidos ou parcialmente protegidos.

Você não pode estar totalmente protegido até ter um backup recente. Isso é importante porque os backups são armazenados em um armazenamento de objetos longe dos volumes persistentes. Se uma falha ou acidente apagar o cluster e seu armazenamento persistente, então você precisa de um backup para recuperar. Um instantâneo não permitiria que você se recuperasse.

- **Visão geral:** Informações sobre o estado dos pods associados ao aplicativo.
- **Proteção de dados:** Permite configurar uma política de proteção de dados e visualizar os instantâneos e backups existentes.
- **Storage:** Mostra os volumes persistentes no nível do aplicativo. O estado de um volume persistente é da perspectiva do cluster do Kubernetes.
- **Recursos:** Permite verificar quais recursos estão sendo copiados e gerenciados.
- **Atividade:** Mostra as atividades relacionadas com a aplicação.



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

Gerencie sua conta

Gerencie usuários e funções locais

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

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

Utilize LDAP

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

- "[Use a API Astra Control para gerenciar usuários e autenticação remota](#)"
- "[Use a IU do Astra Control para gerenciar usuários e grupos remotos](#)"
- "[Use a IU do Astra Control para gerenciar a autenticação remota](#)"

Adicionar utilizadores

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

Passos

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

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

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

Cada função fornece as seguintes permissões:

- Um **Viewer** pode visualizar recursos.
- Um **Membro** tem permissões de função Visualizador e pode gerenciar aplicativos e clusters, desgerenciar aplicativos e excluir snapshots e backups.

- Um **Admin** tem permissões de função de Membro e pode adicionar e remover quaisquer outros usuários, exceto o proprietário.
 - Um **proprietário** tem permissões de função Admin e pode adicionar e remover quaisquer contas de usuário.
6. Para adicionar restrições a um utilizador com uma função Membro ou Visualizador, ative a caixa de verificação **restringir função a restrições**.

Para obter mais informações sobre como adicionar restrições, "[Gerencie usuários e funções locais](#)" consulte .

7. Selecione **Adicionar**.

Gerenciar senhas

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

Altere a sua palavra-passe

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

Passos

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

Repor a palavra-passe de outro utilizador

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

Passos

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



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

6. Selecione **Redefinir senha**.

Remover usuários

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

Passos

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

Resultado

O Astra Control Center remove o usuário da conta.

Gerenciar funções

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

Adicione uma restrição de namespace a uma função

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

Passos

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

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

6. Selecione **Adicionar restrição**.

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

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

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

10. Selecione **Confirm**.

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



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

Remova uma restrição de namespace de uma função

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

Passos

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

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

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

Para mais informações

- ["Funções de usuário e namespaces"](#)

Gerenciar a autenticação remota

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

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



O Astra Control Center usa o endereço de e-mail no atributo LDAP "mail" para pesquisar e acompanhar usuários remotos. Este atributo pode ser um campo opcional ou vazio no seu diretório. Um endereço de e-mail deve existir neste campo para todos os usuários remotos que você deseja aparecer no Astra Control Center. Este endereço de e-mail é usado como nome de usuário no Astra Control Center para autenticação.

Adicione um certificado para autenticação LDAPS

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

Passos

1. Vá para **conta**.

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

Ativar autenticação remota

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

Antes de começar

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

Passos

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



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

5. Insira as credenciais da conta de serviço no formato de e-mail (administrator@example.com). O Astra Control usará essas credenciais ao se conectar ao servidor LDAP.
6. Na seção **User Match**, insira o DN base e um filtro de pesquisa de usuário apropriado para usar ao recuperar informações do usuário do servidor LDAP.
7. Na seção **correspondência de grupo**, insira o DN da base de pesquisa de grupo e um filtro de pesquisa de grupo personalizado apropriado.



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

8. Selecione **Enviar**.

Resultado

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

Desativar a autenticação remota

Pode desativar temporariamente uma ligação ativa ao servidor LDAP.



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

Passos

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

Resultado

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

Editar definições de autenticação remota

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



Não é possível editar o URL ou o endereço IP do servidor LDAP quando o painel **Autenticação remota** estiver no estado "Desativado". Você precisa [Desconecte a autenticação remota](#) primeiro.

Passos

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

Desconecte a autenticação remota

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



Quando você se desconecta do servidor LDAP, todas as configurações desse servidor LDAP são removidas do Astra Control, bem como quaisquer usuários e grupos remotos que foram adicionados desse servidor LDAP.

Passos

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

Resultado

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

Gerenciar usuários e grupos remotos

Se você ativou a autenticação LDAP no sistema Astra Control, poderá pesquisar

usuários e grupos LDAP e incluí-los nos usuários aprovados do sistema.

Adicionar um utilizador remoto

Proprietários e administradores de contas podem adicionar usuários remotos ao Astra Control.



Não é possível adicionar um utilizador remoto se já existir um utilizador local com o mesmo endereço de correio eletrónico no sistema. Para adicionar o utilizador como utilizador remoto, primeiro elimine o utilizador local do sistema.



O Astra Control Center usa o endereço de e-mail no atributo LDAP "mail" para pesquisar e acompanhar usuários remotos. Este atributo pode ser um campo opcional ou vazio no seu diretório. Um endereço de e-mail deve existir neste campo para todos os usuários remotos que você deseja aparecer no Astra Control Center. Este endereço de e-mail é usado como nome de usuário no Astra Control Center para autenticação.

Passos

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



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

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



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

9. Selecione **Adicionar**.

Resultado

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

Adicionar um grupo remoto

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

remotos nesse grupo são adicionados ao Astra Control e herdam a mesma função.

Passos

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

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

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



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

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



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

9. Selecione **Adicionar**.

Resultado

O novo grupo aparece na lista de grupos remotos e todos os usuários remotos deste grupo aparecem na lista de usuários remotos. Nesta lista, você pode ver detalhes sobre o grupo, bem como gerenciar o grupo no menu **ações**.

Ver e gerir notificações

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

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



Passos

1. Selecione o número de notificações não lidas no canto superior direito.

2. Reveja as notificações e selecione **Marcar como lidas** ou **Mostrar todas as notificações**.

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

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

Adicione e remova credenciais

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

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

Adicionar credenciais

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



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

Remover credenciais

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



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

Passos

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

Resultado

O Astra Control Center remove as credenciais da conta.

Monitorar a atividade da conta

Você pode ver detalhes sobre as atividades na sua conta do Astra Control. Por exemplo, quando novos usuários foram convidados, quando um cluster foi adicionado ou quando

um snapshot foi tirado. Você também pode exportar a atividade da sua conta para um arquivo CSV.



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

Ver todas as atividades da conta no Astra Control

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

Exibir atividade da conta para um aplicativo específico

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

Ver atividade da conta dos clusters

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

Tome medidas para resolver eventos que exigem atenção

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

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

Atualizar uma licença existente

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

Passos

1. Inicie sessão no "[Site de suporte da NetApp](#)".
2. Acesse a página de download do Centro de Controle Astra, insira o número de série e baixe o arquivo de licença NetApp completo (NLF).
3. Faça login na IU do Astra Control Center.
4. Na navegação à esquerda, selecione **conta > Licença**.
5. Na página **conta > Licença**, selecione o menu suspenso status da licença existente e selecione

Substituir.

6. Navegue até o arquivo de licença que você baixou.
7. Selecione **Adicionar**.

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

Para mais informações

- ["Licenciamento do Astra Control Center"](#)

Gerenciar buckets

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

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

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

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



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



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

Um balde pode estar em um destes estados:

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

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

Você pode executar estas tarefas relacionadas ao gerenciamento de buckets:

- ["Adicione um balde"](#)
- ["Edite um balde"](#)

- [Defina o intervalo predefinido](#)
- [Gire ou remova as credenciais do bucket](#)
- [Retire um balde](#)



Os buckets do S3 no Astra Control Center não relatam a capacidade disponível. Antes de fazer backup ou clonar aplicativos gerenciados pelo Astra Control Center, verifique as informações do bucket no sistema de gerenciamento ONTAP ou StorageGRID.

Edite um balde

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



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

Passos

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



Não é possível modificar o tipo de bucket.

4. Selecione **Atualizar**.

Defina o intervalo predefinido

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

Passos

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

Gire ou remova as credenciais do bucket

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

Gire as credenciais do bucket

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

Etapas para editar e girar credenciais

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

Remova as credenciais do bucket

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



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



Se você remover credenciais de bucket ativas, ["solução de problemas na remoção de credenciais do balde"](#) consulte .

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

Retire um balde

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



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

Antes de começar

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

Se houver, você não será capaz de continuar.

Passos

1. Na navegação à esquerda, selecione **baldes**.
2. No menu **ações**, selecione **Remover**.



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

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

Encontre mais informações

- ["Use a API Astra Control"](#)

Gerenciar o back-end de storage

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

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

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

- ["Adicionar um back-end de storage"](#)
- [Veja os detalhes do back-end de armazenamento](#)
- [Editar detalhes de autenticação de back-end de armazenamento](#)
- [Gerenciar um back-end de storage descoberto](#)
- [Desgerenciar um back-end de storage](#)
- [Remover um back-end de storage](#)

Veja os detalhes do back-end de armazenamento

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

Veja os detalhes do back-end do storage no Dashboard

Passos

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

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

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

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

Passos

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



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

Umeng-Aff300-05-06 Available

Storage backend status: Healthy

Capacity (Physical): 37.3% 7.93/21.28 TiB

Performance (Last 24 hrs): Throughput, MB/s

BASIC INFORMATION

Type: ONTAP 9.7.0 Cloud private Credentials: Updated 2021/07/28 21:44 UTC

NETWORK

Cluster management IP address: [redacted]

Persistent volumes

Name	Persistent volume	Capacity	App/s	Cluster/s	Cloud
trident_pvc_...	pvc_...	0.04/46.57 GiB: 0.1%	netapp-acc	openshift-cluster010	private
trident_pvc_...	pvc_...	0.34/23.28 GiB: 1.44%	netapp-acc	openshift-cluster010	private
trident_pvc_...	pvc_...	0.02/0.93 GiB: 2.33%	netapp-acc	openshift-cluster010	private
trident_pvc_...	pvc_...	3.02/50.00 GiB: 6.04%	netapp-acc polaris-mongodb-mongodb	openshift-cluster010	private
trident_pvc_...	pvc_...	0.19/8.00 GiB: 2.39%	apps-mysql mysql-mysql	openshift-cluster010	private
trident_pvc_...	pvc_...	0.41/50.00 GiB: 0.81%	netapp-acc polaris-influxdb2-polaris-influxdb2	openshift-cluster010	private
trident_pvc_...	pvc_...	2.93/50.00 GiB: 5.87%	netapp-acc polaris-mongodb-mongodb	openshift-cluster010	private
trident_pvc_...	pvc_...	0.03/10.00 GiB: 0.26%	netapp-acc polaris-consul-consul	openshift-cluster010	private

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

Editar detalhes de autenticação de back-end de armazenamento

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

- **Autenticação baseada em credenciais:** O nome de usuário e senha para um usuário do ONTAP com as permissões necessárias. Você deve usar uma função de login de segurança predefinida, como admin, para garantir a máxima compatibilidade com versões do ONTAP.
- **Autenticação baseada em certificado:** O Astra Control Center também pode se comunicar com um cluster ONTAP usando um certificado instalado no back-end. Você deve usar o certificado de cliente, a chave e o certificado de CA confiável, se usado (recomendado).

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

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

Passos

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



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

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

5. Selecione **Guardar**.

Gerenciar um back-end de storage descoberto

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

Passos

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

Desgerenciar um back-end de storage

Você pode desgerenciar o backend.

Passos

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

Remover um back-end de storage

Você pode remover um back-end de storage que não está mais em uso. Você pode querer fazer isso para

manter sua configuração simples e atualizada.

Antes de começar

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

Passos

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

Encontre mais informações

- ["Use a API Astra Control"](#)

Monitorar tarefas em execução

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

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



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

Para ver mais informações sobre tarefas com falha, ["Monitorar a atividade da conta"](#) consulte .

Passos

1. Enquanto uma tarefa estiver em execução, vá para **aplicativos**.
2. Selecione o nome de uma aplicação na lista.

3. Nos detalhes do aplicativo, selecione a guia **tarefas**.

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



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

Monitore a infraestrutura com conexões Cloud Insights, Prometheus ou Fluentd

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

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

- [Conecte-se ao Cloud Insights](#)
- [Conecte-se ao Prometheus](#)
- [Ligar ao Fluentd](#)

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

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



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

Passos

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



HTTP PROXY

Configure Astra Control to send traffic through a proxy server.

Disconnected

Connect

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 conectada e exibe o nome do servidor.



Connected



HTTP PROXY ?

Server: proxy.example.com:8888

Authentication: Enabled

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.

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



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



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

Antes de começar

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



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

Passos

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



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

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

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

- a. Para obter o ["Token de API"](#), faça login no URL de locatário do Cloud Insights.
- b. No Cloud Insights, gere um token de acesso à API **Read/Write** e **Read Only** clicando em **Admin > API Access**.

Cloud Insights (Trial) Tutorial 0% Complete Getting Started

MONITOR & OPTIMIZE

nmm95sx / Admin / API Access

API Access Tokens (4)

<input type="checkbox"/>	Name ↑	Description	Token	API Type	Permission
<input type="checkbox"/>	astra_...		...zBskB1	All Categories	Read/Write
<input type="checkbox"/>	astra_...		...xKOel_	All Categories	Read/Write
<input type="checkbox"/>	astra_...		...2_AGHP	All Categories	Read Only
<input type="checkbox"/>	astra_...		...8BTKYY	All Categories	Read/Write

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



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

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

5. Selecione **Connect**.



Depois de selecionar **conectar**, 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 conectado 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 conectada e exibe o URL do localitário. Você pode visitar o Cloud Insights para ver os dados sendo recebidos e exibidos com êxito.

EXTERNAL ?

The screenshot shows two connection cards. The first is for 'HTTP PROXY' with a server address 'proxy.example.com:8888' and 'Authentication: Enabled'. The second is for 'CLOUD INSIGHTS' with a tenant 'Cloud Insights'. Both cards have a 'Connected' status and a dropdown arrow.

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.

The notification message reads: 'Unable to connect to Cloud Insights an hour ago. The Cloud Insights API token is invalid. Create a new API token in Cloud Insights and update Astra Control connection settings with the new token.'

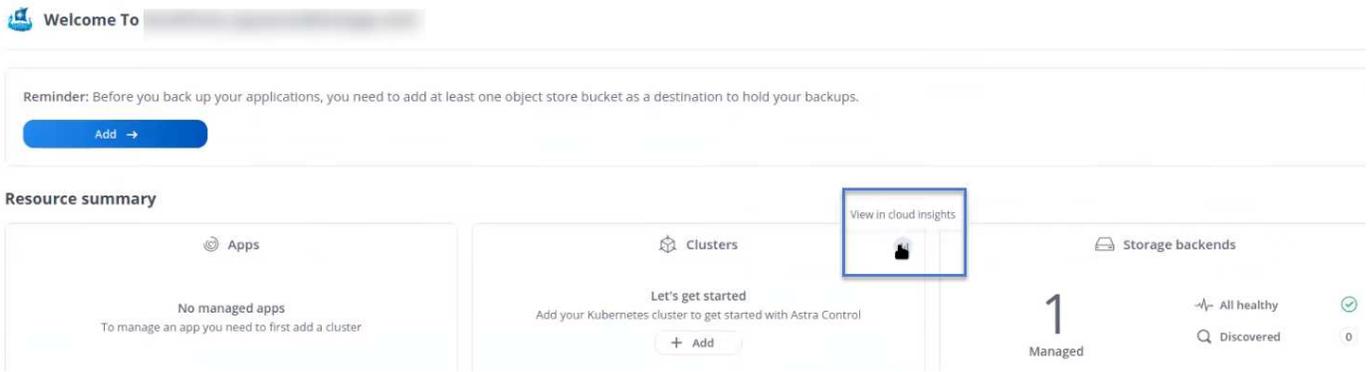
Você também pode encontrar as mesmas informações em **conta > notificações**.

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

The screenshot shows a table with columns: Name, Status, Capacity, Throughput, Type, and Actions. A tooltip for the 'Throughput' column shows a line graph and statistics: 'Throughput Last 24 hrs', '5m ago: 8.00 MB/s', 'Min: 4.00 MB/s', 'Max: 11.00 MB/s', and a link to 'View in Cloud Insights'.

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

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



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

Editar ligação à Cloud Insights

Pode editar a ligação Cloud Insights.



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

Passos

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

Desativar a ligação Cloud Insights

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

Passos

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

Conete-se ao Prometheus

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

Para obter detalhes sobre como usar Prometheus, consulte sua documentação em "[Começando com](#)"

Prometheus".

O que você vai precisar

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

Siga as instruções na documentação oficial para "[Instale Prometheus](#)".

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

Configure Prometheus

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

Passos

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

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



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

3. Reinicie o serviço Prometheus:

```
sudo systemctl restart prometheus
```

Acesse Prometheus

Acesse a URL Prometheus.

Passos

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

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

Ver dados em Prometheus

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

Passos

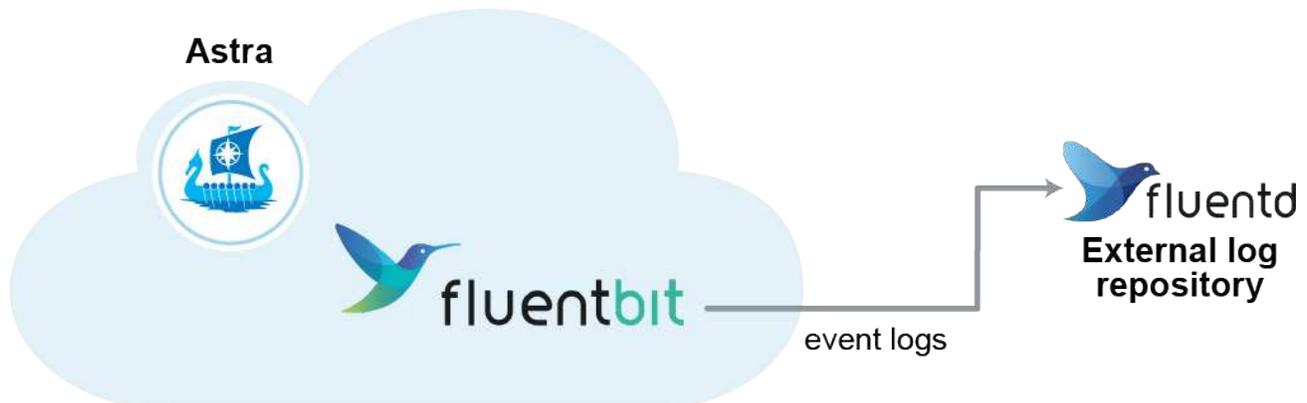
1. Em um navegador, insira o URL Prometheus.
2. No menu Prometheus, selecione **Graph**.
3. Para usar o Metrics Explorer, selecione o ícone ao lado de **execute**.
4. `scrape_samples_scraped` Selecione e selecione **Executar**.
5. Para ver a raspagem de amostra ao longo do tempo, selecione **Gráfico**.



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

Ligar ao Fluentd

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



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

Antes de começar

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

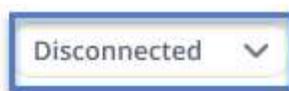


O Astra Control Center não valida os detalhes inseridos para o seu servidor Fluentd. Certifique-se de que introduz os valores corretos.

Passos

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

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



FLUENTD

Connect Astra Control logs to Fluentd for use by your log analysis software.

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 conectado. Agora você pode visitar o servidor Fluentd conectado e visualizar os logs de eventos.

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

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



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

Edite a ligação Fluentd

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

Passos

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

Desative a conexão Fluentd

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

Passos

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

Desgerenciar aplicativos e clusters

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

Desgerenciar um aplicativo

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

Quando você desgerencia um aplicativo:

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

Passos

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

Resultado

O Astra Control Center deixa de gerenciar a aplicação.

Desgerenciar um cluster

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



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

Quando você desgerencia um cluster:

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

Passos

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

Resultado

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



Se o Centro de Controle Astra e o Cloud Insights não estiverem conectados, 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 conectados**, o desgerenciamento do cluster excluirá somente os `fluentbit` pods e `event-exporter`

Atualizar o Astra Control Center

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

Antes de começar

- Antes de atualizar, "[requisitos do ambiente operacional](#)" consulte para garantir que seu ambiente ainda atenda aos requisitos mínimos para a implantação do Astra Control Center. Seu ambiente deve ter o seguinte:
 - Para determinar a versão que você está executando, execute o seguinte comando em relação ao seu Astra Control Center existente Trident:

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

```
https://docs.netapp.com/us-en/trident/trident-managing-k8s/upgrade-trident.html#determine-the-version-to-upgrade-to["Documentação do Astra Trident"]Consulte para atualizar a partir de uma versão mais antiga.
```



É necessário fazer upgrade para o Astra Trident 22,10 **ANTERIOR** para fazer upgrade para o Kubernetes 1,25.

- Para determinar a versão que você está executando, execute o seguinte comando em relação ao Astra Control Center existente: `kubectl get nodes -o wide`
- Recursos de cluster suficientes para determinar os recursos do cluster, execute o seguinte comando no cluster existente do Astra Control Center: `kubectl describe node <node name>`
- Um Registro que você pode usar para enviar e carregar imagens do Astra Control Center
- Para determinar sua classe de storage padrão, execute o seguinte comando em relação ao Astra Control Center existente: `kubectl get storageclass`
- (Apenas OpenShift) Certifique-se de que todos os operadores de cluster estão em um estado saudável e disponíveis.

```
kubectl get clusteroperators
```

- Certifique-se de que todos os serviços de API estejam em um estado saudável e disponíveis.

```
kubectl get apiservices
```

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

Sobre esta tarefa

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

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



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



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

Faça download e extraia Astra Control Center

1. Vá para o "[Página de downloads do produto Astra Control Center](#)" no site de suporte da NetApp. Pode selecionar a versão mais recente ou outra versão pretendida no menu pendente.
2. Faça o download do pacote que contém o Astra Control Center (`astra-control-center-[version].tar.gz`).
3. (Recomendado, mas opcional) Faça o download do pacote certificados e assinaturas para o Astra Control Center (`astra-control-center-certs-[version].tar.gz`) para verificar a assinatura do pacote:

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

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

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

4. Extraia as imagens do pacote Astra Control Center:

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

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

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

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

```
kubectl astra
```

2. Execute uma destas ações:

- Se o plugin estiver instalado, o comando deve retornar a ajuda do plugin kubectl. Para remover uma versão existente do kubectl-astra, execute este comando: `delete /usr/local/bin/kubectl-astra`.
- Se o comando retornar um erro, o plugin não está instalado e você pode prosseguir para a próxima etapa para instalá-lo.

3. Instale o plugin:

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



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

```
ls kubectl-astra/
```

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

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

Adicione as imagens ao seu registro local

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

Docker

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

```
acc.manifest.bundle.yaml
acc/
```

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

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

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

Podman

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

```
acc.manifest.bundle.yaml
acc/
```

2. Inicie sessão no seu registro:

```
podman login <YOUR_REGISTRY>
```

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

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

```

export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=23.04.2-7
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //'')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*://:')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done

```

Podman 3

```

export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=23.04.2-7
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //'')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*://:')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done

```



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

```

https://netappdownloads.jfrog.io/docker-astra-control-
prod/netapp/astra/acc/23.04.2-7/image:version

```

Instale o operador Astra Control Center atualizado

1. Altere o diretório:

```
cd manifests
```

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

```
vim astra_control_center_operator_deploy.yaml
```

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

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

- b. Altere `[your_registry_path]` para a `kube-rbac-proxy` imagem para o caminho do registro onde as imagens foram empurradas para um [passo anterior](#).
- c. Altere `[your_registry_path]` para a `acc-operator` imagem para o caminho do registro onde as imagens foram empurradas para um [passo anterior](#).
- d. Adicione os seguintes valores à `env` seção:

```
- name: ACCOP_HELM_UPGRADE_TIMEOUT  
  value: 300m
```

```
apiVersion: apps/v1  
kind: Deployment  
metadata:  
  labels:  
    control-plane: controller-manager  
    name: acc-operator-controller-manager  
    namespace: netapp-acc-operator  
spec:  
  replicas: 1  
  selector:  
    matchLabels:  
      control-plane: controller-manager  
  strategy:  
    type: Recreate  
  template:  
    metadata:  
      labels:  
        control-plane: controller-manager  
    spec:  
      containers:
```

```

- args:
  - --secure-listen-address=0.0.0.0:8443
  - --upstream=http://127.0.0.1:8080/
  - --logtostderr=true
  - --v=10
  image: [your_registry_path]/kube-rbac-proxy:v4.8.0
  name: kube-rbac-proxy
  ports:
    - containerPort: 8443
      name: https
- args:
  - --health-probe-bind-address=:8081
  - --metrics-bind-address=127.0.0.1:8080
  - --leader-elect
  env:
    - name: ACCOP_LOG_LEVEL
      value: "2"
    - name: ACCOP_HELM_UPGRADE_TIMEOUT
      value: 300m
  image: [your_registry_path]/acc-operator:23.04.36
  imagePullPolicy: IfNotPresent
  livenessProbe:
    httpGet:
      path: /healthz
      port: 8081
      initialDelaySeconds: 15
      periodSeconds: 20
  name: manager
  readinessProbe:
    httpGet:
      path: /readyz
      port: 8081
      initialDelaySeconds: 5
      periodSeconds: 10
  resources:
    limits:
      cpu: 300m
      memory: 750Mi
    requests:
      cpu: 100m
      memory: 75Mi
  securityContext:
    allowPrivilegeEscalation: false
  imagePullSecrets: []
  securityContext:
    runAsUser: 65532

```

```
terminationGracePeriodSeconds: 10
```

3. Instale o operador Astra Control Center atualizado:

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

Resposta da amostra:

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

4. Verifique se os pods estão em execução:

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

Atualizar o Astra Control Center

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

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

2. Altere o número da versão do Astra (astraVersion dentro do spec) para a versão para a qual você está atualizando:

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

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

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

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

```
crds:
  shouldUpgrade: true
```

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

```
additionalValues:
  nautilus:
    startupProbe:
      periodSeconds: 30
      failureThreshold: 600
```

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

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

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

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

Resposta:

NAME	UUID	VERSION	ADDRESS
READY			
astra	9aa5fdae-4214-4cb7-9976-5d8b4c0ce27f	23.04.2-7	
10.111.111.111	True		



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



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

Verifique o status do sistema

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

Desinstale o Astra Control Center

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

Se tiver algum problema com a desinstalação, [Solução de problemas de desinstalação](#) consulte .

Antes de começar

1. "[Desgerenciar todos os aplicativos](#)" nos clusters.
2. "[Desgerenciar todos os clusters](#)".

Passos

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

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

Resultado:

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

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

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

Resultado de exemplo:

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

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

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

Resultado:

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

Solução de problemas de desinstalação

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

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

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

Passos

1. Eliminar acc-monitoring agente:

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

Resultado:

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

2. Excluir o namespace:

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

Resultado:

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

3. Confirmar recursos removidos:

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

Resultado:

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

4. Confirmar o agente de monitoramento removido:

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

Resultado da amostra:

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

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

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

Resultado:

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

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

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

Passos

1. Listar CRDs Traefik instalados no cluster:

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

Resposta

```
ingressroutes.traefik.containo.us          2021-06-23T23:29:11Z
ingressroutetcps.traefik.containo.us      2021-06-23T23:29:11Z
ingressrouteudps.traefik.containo.us      2021-06-23T23:29:12Z
middlewares.traefik.containo.us           2021-06-23T23:29:12Z
middlewareetcps.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
middlewareetcps.traefik.containo.us
```

Encontre mais informações

- ["Problemas conhecidos para desinstalar"](#)

Automatize com a API REST do Astra Control

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 Control Center ou a API Astra Control.

Para saber mais, acesse "[Documentação de automação do Astra](#)".

Conhecimento e apoio

Solução de problemas

Aprenda a contornar alguns problemas comuns que você pode encontrar.

["Base de Conhecimento da NetApp para Astra"](#)

Encontre mais informações

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

Obtenha ajuda

O NetApp é compatível com o Astra Control de várias maneiras. Amplas opções gratuitas de suporte autônomo estão disponíveis 24 horas por dia, 7 dias por semana, como artigos da base de conhecimento (KB) e um canal discord. 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 através da opção de feedback ou usar o canal discord para autoatendimento.

Você deve primeiro ["Ative o suporte para o seu número de série NetApp"](#) para usar essas opções de suporte que não são de autoatendimento. É necessária uma conta SSO do site de suporte da NetApp (NSS) para chat e emissão de bilhetes na Web, juntamente com o gerenciamento de casos.

Opções de auto-suporte

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

Estas opções estão disponíveis gratuitamente, 24x7:

- **"Base de conhecimento (login necessário)":** Procure artigos, perguntas frequentes ou informações sobre Break Fix relacionadas ao Astra Control.
- **Centro de documentação:** Este é o site de documentação que você está vendo atualmente.
- **"Obter ajuda via discord":** Vá para Astra na categoria Pub para se conectar com colegas e especialistas.
- *** Criar um caso de suporte*:** Gere pacotes de suporte para fornecer ao suporte NetApp para solução de problemas.
- **Dê feedback sobre o Astra Control:** Envie um e-mail para NetApp.com para nos informar seus pensamentos, ideias ou preocupações.

Habilite o upload diário do pacote de suporte programado para o suporte da NetApp

Durante a instalação do Astra Control Center, se você especificar `enrolled: true` para o `autoSupport` arquivo de recurso personalizado (CR) do Astra Control Center (`astra_control_center.yaml`), os pacotes de suporte diários serão automaticamente carregados para o ["Site de suporte da NetApp"](#).

Gerar pacote de suporte para fornecer ao suporte da NetApp

O Astra Control Center permite que o usuário administrativo gere pacotes, que incluem informações úteis para o suporte da NetApp, incluindo logs, eventos para todos os componentes da implantação do Astra, métricas e informações de topologia sobre clusters e aplicações em gerenciamento. Se você estiver conectado à Internet, poderá fazer o upload de pacotes de suporte para o site de suporte da NetApp (NSS) diretamente a partir da IU do Centro de Controle Astra.



O tempo gasto pelo Astra Control Center para gerar o pacote depende do tamanho da instalação do Astra Control Center, bem como dos parâmetros do pacote de suporte solicitado. O tempo de duração especificado ao solicitar um pacote de suporte determina o tempo necessário para que o pacote seja gerado (por exemplo, um período de tempo mais curto resulta em geração de pacotes mais rápida).

Antes de começar

Determine se uma conexão proxy será necessária para carregar pacotes para o NSS. Se for necessária uma conexão proxy, verifique se o Astra Control Center foi configurado para usar um servidor proxy.

1. Selecione **Contas > conexões**.
2. Verifique as configurações de proxy em **Configurações de conexão**.

Passos

1. Crie um caso no portal do NSS usando o número de série da licença listado na página **suporte** da IU do Astra Control Center.
2. Execute as etapas a seguir para gerar o pacote de suporte usando a IU do Astra Control Center:
 - a. Na página **suporte**, no bloco Pacote suporte, selecione **gerar**.
 - b. Na janela **Generate a Support Bundle** (gerar um pacote de suporte), selecione o período de tempo.

Você pode escolher entre prazos rápidos ou personalizados.



Você pode escolher um intervalo de datas personalizado, bem como especificar um período de tempo personalizado durante o intervalo de datas.

- c. Depois de fazer as seleções, selecione **Confirm**.
- d. Marque a caixa de seleção **carregar o pacote para o site de suporte da NetApp quando gerado**.
- e. Selecione **Generate Bundle**.

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

Se a geração falhar, um ícone será exibido na página gerar pacote. Selecione o ícone para ver a mensagem.



O ícone de notificações no canto superior direito da interface do usuário fornece informações sobre eventos relacionados ao pacote de suporte, como quando o pacote é criado com êxito, quando a criação do pacote falha, quando o pacote não pôde ser carregado, quando o pacote não pôde ser baixado, e assim por diante.

Se você tiver uma instalação com ar-gapped

Se você tiver uma instalação com conexão via rede, execute as seguintes etapas após a geração do pacote suporte. Quando o pacote está disponível para download, o ícone Download aparece ao lado de **Generate** na seção **Support Bundles** da página **Support**.

Passos

1. Selecione o ícone Transferir para transferir o pacote localmente.
2. Carregue manualmente o pacote para o NSS.

Você pode usar um dos seguintes métodos para fazer isso:

- ["Carregamento de arquivo autenticado NetApp \(necessário iniciar sessão\)"](#) Use .
- Fixe o pacote ao estojão diretamente no NSS.
- Use o NetApp Active IQ.

Encontre mais informações

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

Versões anteriores da documentação do Astra Control Center

A documentação para versões anteriores está disponível.

- ["Documentação do Astra Control Center 22,11"](#)
- ["Documentação do Astra Control Center 22,08"](#)
- ["Documentação do Astra Control Center 22,04"](#)
- ["Documentação do Astra Control Center 21,12"](#)
- ["Documentação do Astra Control Center 21,08"](#)

Avisos legais

Avisos legais fornecem acesso a declarações de direitos autorais, marcas registradas, patentes e muito mais.

Direitos de autor

["https://www.netapp.com/company/legal/copyright/"](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 respectivos proprietários.

["https://www.netapp.com/company/legal/trademarks/"](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/"](https://www.netapp.com/company/legal/privacy-policy/)

Código aberto

Os arquivos de aviso fornecem informações sobre direitos autorais de terceiros e licenças usadas no software NetApp.

- ["Aviso para Astra Control Center 23.04.2"](#)
- ["Aviso para Astra Control Center 23.04.0"](#)

Licença de API Astra Control

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

Informações sobre direitos autorais

Copyright © 2024 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.