



Documentação do Astra Control Service

Astra Control Service

NetApp
October 21, 2024

Índice

Documentação do Astra Control Service	1
Notas de lançamento	2
Novidades do Astra Control Service	2
Problemas conhecidos	11
Limitações conhecidas	13
Comece agora	16
Saiba mais sobre o Astra Control	16
Implantações de Kubernetes compatíveis	20
Início rápido para Astra Control Service	20
Configure seu provedor de nuvem	22
Registre-se para ter uma conta do Astra Control Service	42
Adicionar um cluster ao Astra Control Service	44
O que se segue?	86
Vídeos do Astra Control Service	86
Conceitos	88
Arquitetura e componentes	88
Proteção de dados	93
Classes de armazenamento e desempenho para clusters da AWS	94
Classes de armazenamento e tamanho PV para clusters AKS	95
Tipo de serviço, classes de armazenamento e tamanho PV para clusters GKE	96
Gerenciamento de aplicativos	99
Funções de usuário e namespaces	101
Use o Astra Control Service	102
Faça login no Astra Control Service	102
Gerenciar e proteger aplicativos	102
Ver a integridade da aplicação e da computação	142
Gerenciar buckets	144
Monitorar tarefas em execução	148
Gerencie sua conta	149
Gerenciar instâncias de nuvem	158
Habilite o Astra Control Provisioner	159
Desgerenciar aplicativos e clusters	168
Implantar uma instância autogerenciada do Astra Control	170
Use o Astra Control Provisioner	171
Configurar a criptografia de back-end de storage	171
Recuperar dados de volume usando um snapshot	178
Replique volumes usando o SnapMirror	180
Automação com a API REST do Astra Control	187
Conhecimento e apoio	188
Registre-se para obter suporte	188
Solução de problemas	190
Obtenha ajuda	190
Perguntas frequentes	192

Visão geral	192
Acesso ao Astra Control	192
Registrando clusters do Kubernetes	192
Registrando clusters do Elastic Kubernetes Service (EKS)	193
Registrando clusters do Azure Kubernetes Service (AKS)	193
Registrando clusters do Google Kubernetes Engine (GKE)	193
Remoção de clusters	194
Gerenciamento de aplicações	194
Operações de gerenciamento de dados	195
Previsão do Astra Control	195
Avisos legais	198
Direitos de autor	198
Marcas comerciais	198
Patentes	198
Política de privacidade	198
Código aberto	198
Licença de API Astra Control	198

Documentação do Astra Control Service

Notas de lançamento

Novidades do Astra Control Service

A NetApp atualiza periodicamente o Serviço de Controle Astra para oferecer novos recursos, aprimoramentos e correções de bugs.

14 de março de 2024

(Visualização técnica) workflows declarativos do Kubernetes

Esta versão do Astra Control Service contém funcionalidade declarativa do Kubernetes que permite executar gerenciamento de dados a partir de um recurso personalizado nativo do Kubernetes (CR).

Essa funcionalidade só está disponível na instância do Astra Control Service Early Adopter Program (EAP). Contacte o seu representante de vendas da NetApp para obter informações sobre como aderir ao EAP.

Depois de instalar o ["Conetor Astra"](#) no cluster que deseja gerenciar, você poderá executar as seguintes operações de cluster baseadas em CR na IU ou em um CR:

- ["Definir uma aplicação utilizando um recurso personalizado"](#)
- ["Defina o balde"](#)
- ["Proteger um cluster inteiro"](#)
- ["Faça backup da sua aplicação"](#)
- ["Criar um instantâneo"](#)
- ["Crie agendas para instantâneos ou backups"](#)
- ["Restaurar uma aplicação a partir de um instantâneo ou cópia de segurança"](#)

7 de novembro de 2023

Novos recursos e suporte

- * Recursos de backup e restauração para aplicativos com backends de armazenamento com driver ONTAP-nas-Economy*: Ative operações de backup e restauração para `ontap-nas-economy` alguns ["passos simples"](#).
- **Suporte ao Astra Control Service para clusters locais do Red Hat OpenShift Container Platform**
["Adicione um cluster"](#)
- * Backups imutáveis*: O Astra Control agora é compatível ["backups inalteráveis e somente leitura"](#) como uma camada de segurança adicional contra malware e outras ameaças.
- **Apresentamos o Astra Control Provisioner**

Com a versão 23,10, o Astra Control apresenta um novo componente de software chamado Astra Control Provisioner, que estará disponível para todos os usuários licenciados do Astra Control. O Astra Control Provisioner fornece acesso a um superconjunto de recursos avançados de gerenciamento e provisionamento de storage além daqueles fornecidos pelo Astra Trident. Esses recursos estão disponíveis para todos os clientes do Astra Control sem custo adicional.

- **Comece a usar o Astra Control Provisioner** você pode ["Habilite o Astra Control Provisioner"](#) se tiver

instalado e configurado seu ambiente para usar o Astra Trident 23,10.

- **Funcionalidade do Astra Control Provisioner**

Os seguintes recursos estão disponíveis com o lançamento do Astra Control Provisioner 23,10:

- * Segurança de back-end de armazenamento aprimorada com criptografia Kerberos 5*: Você pode melhorar a segurança de armazenamento ["ativação da encriptação"](#) para o tráfego entre o cluster gerenciado e o back-end de armazenamento. O Astra Control Provisioner oferece suporte à criptografia Kerberos 5 em mais de NFSv4,1 conexões de clusters Red Hat OpenShift para volumes Azure NetApp Files e ONTAP locais.
- **Recuperar dados usando um snapshot:** O Astra Control Provisioner fornece restauração rápida de volume no local a partir de um snapshot usando o `TridentActionSnapshotRestore` (TASR) CR.
- **Recursos de backup e restauração para aplicativos com `ontap-nas-economy` backends de armazenamento com backup de driver:** Como descrito [acima](#).

- **Suporte ao Astra Control Service para Red Hat OpenShift Service nos clusters AWS (ROSA)**

["Adicione um cluster"](#)

- **Suporte ao gerenciamento de aplicações que usam storage NVMe/TCP** o Astra Control agora pode gerenciar aplicações com suporte de volumes persistentes conectados por meio de NVMe/TCP.
- **Ganchos de execução desativados por padrão:** Começando com esta versão, a funcionalidade de ganchos de execução pode ser ["ativado"](#) ou desativada para segurança adicional (ela está desativada por padrão). Se você ainda não criou ganchos de execução para uso com o Astra Control, você precisa ["ative o recurso ganchos de execução"](#) começar a criar ganchos. Se você criou ganchos de execução antes desta versão, a funcionalidade ganchos de execução permanece ativada e você pode usar ganchos como faria normalmente.

2 de outubro de 2023

Novos recursos e suporte

Esta é uma versão menor de correção de bugs.

27 de julho de 2023

Novos recursos e suporte

- As operações de clone agora são compatíveis apenas com clones ativos (estado atual da aplicação gerenciada). Para clonar de um snapshot ou backup, use o fluxo de trabalho de restauração.

["Restaurar aplicações"](#)

26 de junho de 2023

Novos recursos e suporte

- As assinaturas do Azure Marketplace agora são cobradas por hora em vez de por minuto

["Configure a faturação"](#)

30 de maio de 2023

Novos recursos e suporte

- Suporte para clusters privados do Amazon EKS

["Gerenciar clusters privados do Astra Control Service"](#)

- Suporte para selecionar a classe de storage de destino durante operações de restauração ou clone

["Restaurar aplicações"](#)

15 de maio de 2023

Novos recursos e suporte

Esta é uma versão menor de correção de bugs.

25 de abril de 2023

Novos recursos e suporte

- Suporte para clusters privados do Red Hat OpenShift

["Gerenciar clusters privados do Astra Control Service"](#)

- Suporte para incluir ou excluir recursos de aplicativos durante operações de restauração

["Restaurar aplicações"](#)

- Suporte para gerenciamento de aplicações somente de dados

["Comece a gerenciar aplicativos"](#)

17 de janeiro de 2023

Novos recursos e suporte

- Funcionalidade aprimorada de ganchos de execução com opções de filtragem adicionais

["Gerenciar ganchos de execução de aplicativos"](#)

- Suporte para NetApp Cloud Volumes ONTAP como back-end de storage

["Saiba mais sobre o Astra Control"](#)

22 de novembro de 2022

Novos recursos e suporte

- Suporte para aplicações que abrangem vários namespaces

["Definir aplicações"](#)

- Suporte para incluir recursos de cluster em uma definição de aplicativo

["Definir aplicações"](#)

- Relatórios de progresso aprimorados para suas operações de backup, restauração e clone
["Monitorar tarefas em execução"](#)
- Suporte para gerenciamento de clusters que já tenham uma versão compatível do Astra Trident instalada
["Comece a gerenciar clusters de Kubernetes a partir do Astra Control Service"](#)
- Suporte para gerenciamento de várias subscrições de fornecedor de nuvem em uma única conta do Astra Control Service
["Gerenciar instâncias de nuvem"](#)
- Suporte para adicionar clusters Kubernetes autogerenciados que são hospedados em ambientes de nuvem pública ao Astra Control Service
["Comece a gerenciar clusters de Kubernetes a partir do Astra Control Service"](#)
- A cobrança do Astra Control Service agora é mensurada por namespace em vez de por aplicação
["Configure a faturação"](#)
- Suporte para subscrição a ofertas baseadas em termos do Astra Control Service por meio do AWS Marketplace
["Configure a faturação"](#)

Problemas e limitações conhecidos

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

7 de setembro de 2022

Esta versão inclui melhorias de estabilidade e resiliência para a infraestrutura do Astra Control Service.

10 de agosto de 2022

Esta versão inclui os seguintes novos recursos e aprimoramentos.

- Fluxos de trabalho de gerenciamento de aplicações aprimorados fornecem maior flexibilidade ao definir aplicações gerenciadas pelo Astra Control.

["Gerir aplicações"](#)

- Suporte para clusters da Amazon Web Services o Astra Control Service agora pode gerenciar aplicações executadas em clusters hospedados no Amazon Elastic Kubernetes Service. Você pode configurar os clusters para usar o Amazon Elastic Block Store ou o Amazon FSX for NetApp ONTAP como o back-end de armazenamento.

["Configurar o Amazon Web Services"](#)

- Além dos hooks de execução pré e pós-snapshot, agora você pode configurar os seguintes tipos de hooks de execução:

- Pré-backup
- Pós-backup
- Pós-restauração

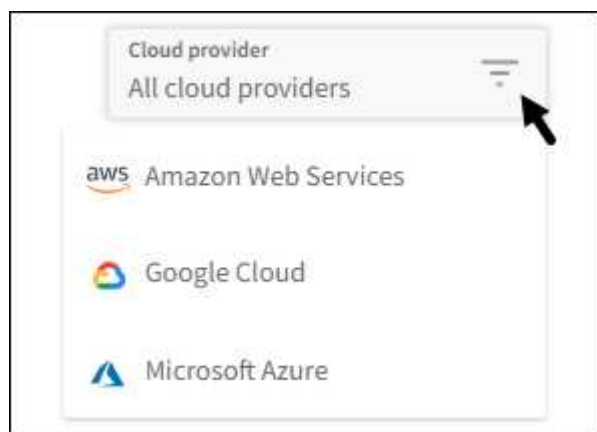
Entre outras melhorias, o Astra Control agora oferece suporte ao uso do mesmo script para vários ganchos de execução.



Os ganchos de execução pré e pós-snapshot padrão fornecidos pelo NetApp para aplicativos específicos foram removidos nesta versão. Se você não fornecer seus próprios ganchos de execução para snapshots, o Astra Control Service tirará snapshots consistentes com falhas apenas a partir de 4 de agosto de 2022. Visite o "[Repositório do NetApp Verda GitHub](#)" para scripts de gancho de execução de exemplo que podem ser modificados para se ajustarem ao seu ambiente.

"Gerenciar ganchos de execução de aplicativos"

- Suporte ao Azure Marketplace agora você pode se inscrever no Astra Control Service por meio do Azure Marketplace.
- Ao ler a documentação do Astra Control Service, você pode selecionar seu provedor de nuvem no canto superior direito da página. Você verá a documentação relevante apenas para o provedor de nuvem selecionado.



26 de abril de 2022

Esta versão inclui os seguintes novos recursos e aprimoramentos.

- O Astra Control Service agora dá suporte à atribuição de restrições de namespace aos usuários do Member ou Viewer.

"Controles de acesso baseados em função do namespace (RBAC)"

- O Azure active Directory oferece suporte ao Astra Control Service para clusters AKS que usam o Azure active Directory para autenticação e gerenciamento de identidade.

"Comece a gerenciar clusters de Kubernetes a partir do Astra Control Service"

- Suporte para clusters AKS privados agora você pode gerenciar clusters AKS que usam endereços IP privados.

"Comece a gerenciar clusters de Kubernetes a partir do Astra Control Service"

- Remoção do balde do Astra Control agora você pode remover um balde do Astra Control Service.

"Retire um balde"

14 de dezembro de 2021

Esta versão inclui os seguintes novos recursos e aprimoramentos.

- Novas opções de back-end de storage
- Agora, é possível restaurar um instantâneo, clone ou backup de um aplicativo no local, restaurando para o mesmo cluster e namespace.

"Restaurar aplicações"

- O Astra Control é compatível com scripts personalizados que podem ser executados antes ou depois de tirar um snapshot de uma aplicação. Isso permite que você execute tarefas como suspender transações de banco de dados para que o snapshot do seu aplicativo de banco de dados seja consistente.

"Gerenciar ganchos de execução de aplicativos"

- O Astra Control é compatível com alguns aplicativos quando eles são implantados com operadores.

"Comece a gerenciar aplicativos"

- Os princípios de serviço com escopo de grupo de recursos o Astra Control Service agora oferece suporte aos princípios de serviço que usam um escopo de grupo de recursos.

"Crie um diretor de serviço do Azure"

5 de agosto de 2021

Esta versão inclui os seguintes novos recursos e aprimoramentos.

- Astra Control Center Astra Control agora está disponível em um novo modelo de implantação. O *Astra Control Center* é um software autogerenciado que você instala e opera no data center para gerenciar o gerenciamento do ciclo de vida da aplicação Kubernetes para clusters do Kubernetes no local.

Para saber mais, ["Vá para a documentação do Astra Control Center"](#).

- Com seu próprio bucket, você pode gerenciar os buckets que o Astra usa para backups e clones, adicionando buckets adicionais e alterando o bucket padrão dos clusters do Kubernetes em seu fornecedor de nuvem.

"Gerenciar buckets"

2 de junho de 2021

Esta versão inclui correções de bugs e os seguintes aprimoramentos ao suporte do Google Cloud.

- Suporte para VPCs compartilhados agora você pode gerenciar clusters GKE em projetos do GCP com uma configuração de rede VPC compartilhada.

- Tamanho de volume persistente para o tipo de serviço CVS, o Astra Control Service agora cria volumes persistentes com um tamanho mínimo de 300 GiB ao usar o tipo de serviço CVS.

["Saiba como o Astra Control Service usa o Cloud Volumes Service para Google Cloud como o back-end de storage para volumes persistentes"](#).

- O suporte para SO otimizado para contentor é agora compatível com os nós de trabalho GKE. Isso é além do suporte para Ubuntu.

["Saiba mais sobre os requisitos do cluster GKE"](#).

15 de abril de 2021

Esta versão inclui os seguintes novos recursos e aprimoramentos.

- Suporte para clusters AKS o Astra Control Service agora pode gerenciar aplicativos que estão sendo executados em um cluster gerenciado do Kubernetes no Azure Kubernetes Service (AKS).

["Saiba como começar"](#).

- API REST a API REST do Astra Control agora está disponível para uso. A API é baseada em tecnologias modernas e melhores práticas atuais.

["Saiba como automatizar o gerenciamento do ciclo de vida dos dados de aplicativos usando a API REST"](#).

- Subscrição anual Astra Control Service agora oferece uma *Premium Subscription*.

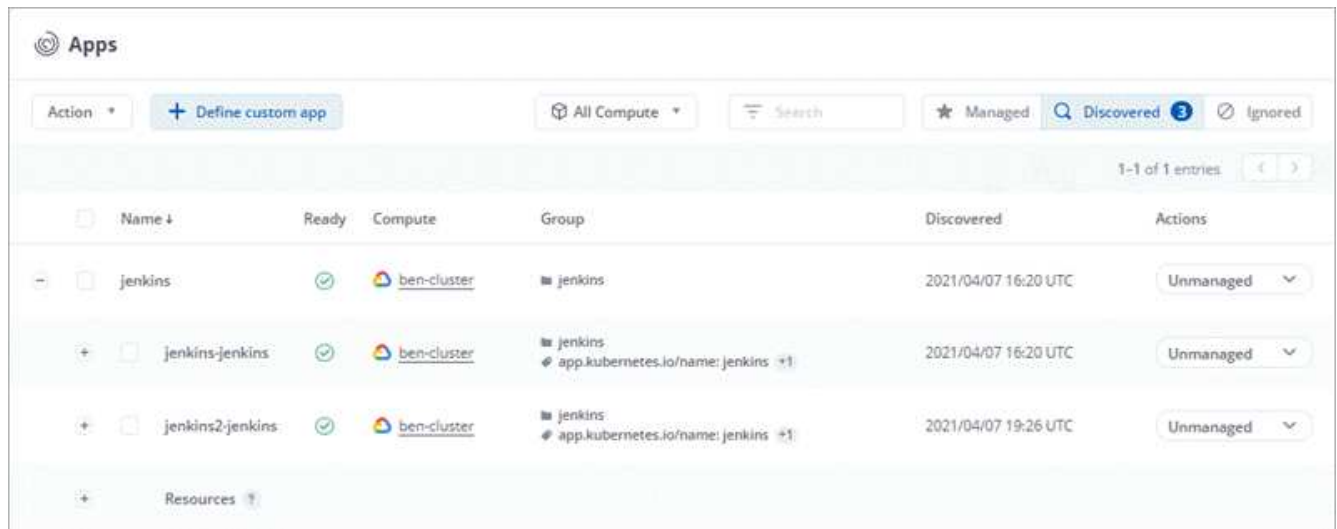
Pré-pague a uma taxa com desconto com uma assinatura anual que permite gerenciar até 10 aplicativos por *Application Pack*. Entre em Contato com a NetApp Sales para comprar quantos pacotes forem necessários para sua organização. Por exemplo, compre 3 pacotes para gerenciar aplicativos 30 do Serviço de Controle Astra.

Se você gerenciar mais aplicativos do que o permitido pela assinatura anual, será cobrado à taxa de excesso de \$0,005 USD por minuto, por aplicativo (o mesmo que o Premium PayGo).

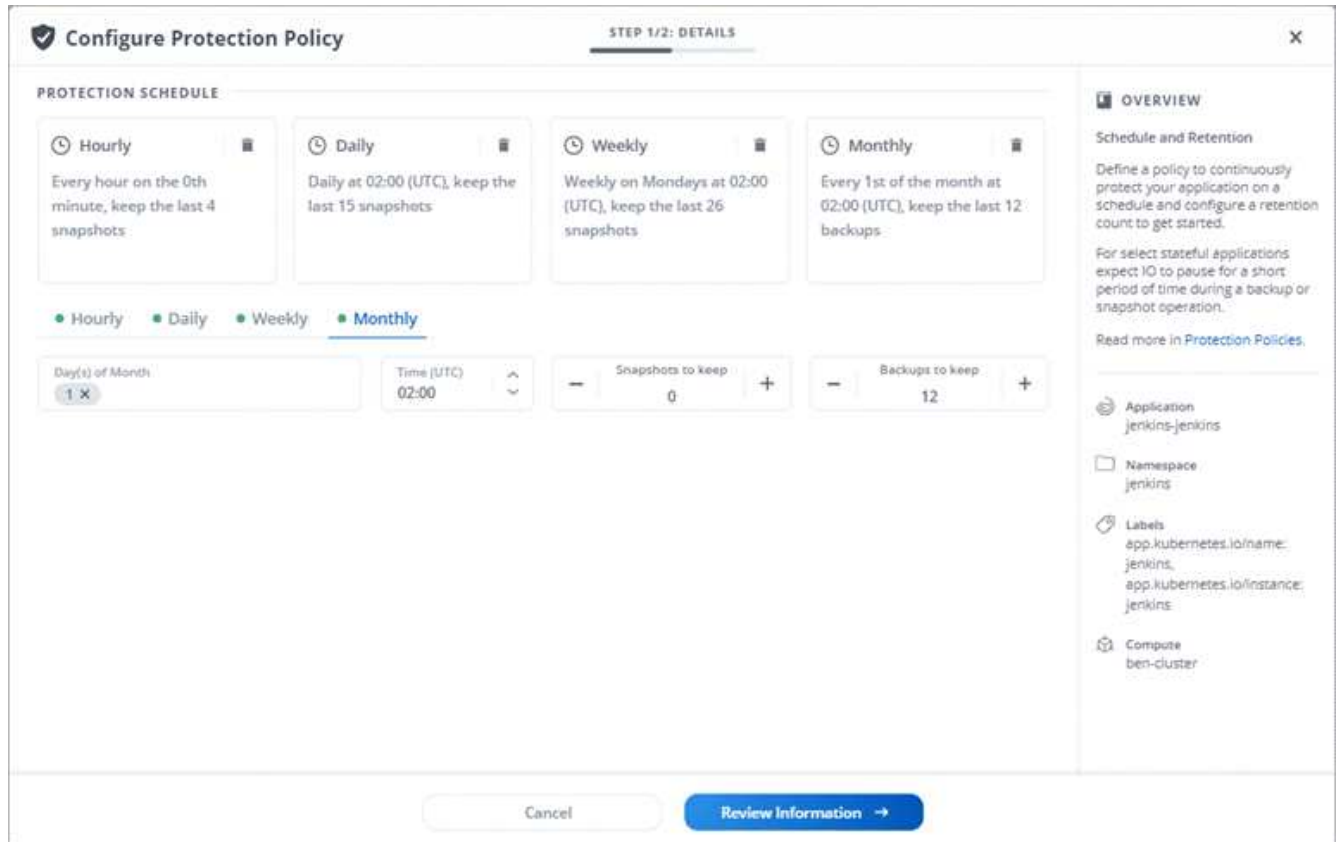
["Saiba mais sobre os preços do Astra Control Service"](#).

- Nós aprimoramos a página de aplicativos descobertos para mostrar melhor a hierarquia entre namespaces e aplicativos. Basta expandir um namespace para ver os aplicativos contidos nesse namespace.

["Saiba mais sobre como gerenciar aplicativos"](#).



- Os assistentes de proteção de dados foram aprimorados para facilitar o uso. Por exemplo, refinamos o assistente de Política de proteção para visualizar mais facilmente o cronograma de proteção conforme você o define.



- Tornamos mais fácil visualizar detalhes sobre as atividades em sua conta do Astra Control.
 - Filtre a lista de atividades por aplicativo gerenciado, nível de gravidade, usuário e intervalo de tempo.
 - Faça o download da atividade da conta do Astra Control para um arquivo CSV.
 - Visualize atividades diretamente a partir da página clusters ou da página Apps depois de selecionar um cluster ou um aplicativo.

["Saiba mais sobre como visualizar a atividade da sua conta".](#)

1 de março de 2021

O Astra Control Service agora é compatível com "[CVS tipo de serviço](#)" o Cloud Volumes Service para Google Cloud. Isso é além de já suportar o tipo de serviço *CVS-Performance*. Como lembrete, o Astra Control Service usa o Cloud Volumes Service para Google Cloud como o back-end de storage para seus volumes persistentes.

Esse aprimoramento significa que agora o Astra Control Service pode gerenciar dados de aplicações para clusters do Kubernetes executados em *qualquer* "[Região do Google Cloud onde o Cloud Volumes Service é compatível](#)".

Se você tiver flexibilidade para escolher entre as regiões do Google Cloud, escolha CVS ou CVS-Performance, dependendo dos requisitos de performance. "[Saiba mais sobre como escolher um tipo de serviço](#)".

25 de janeiro de 2021

Temos o prazer de anunciar que o Astra Control Service agora está disponível em geral. Incorporamos muito do feedback que recebemos da versão Beta e fizemos algumas outras melhorias notáveis.

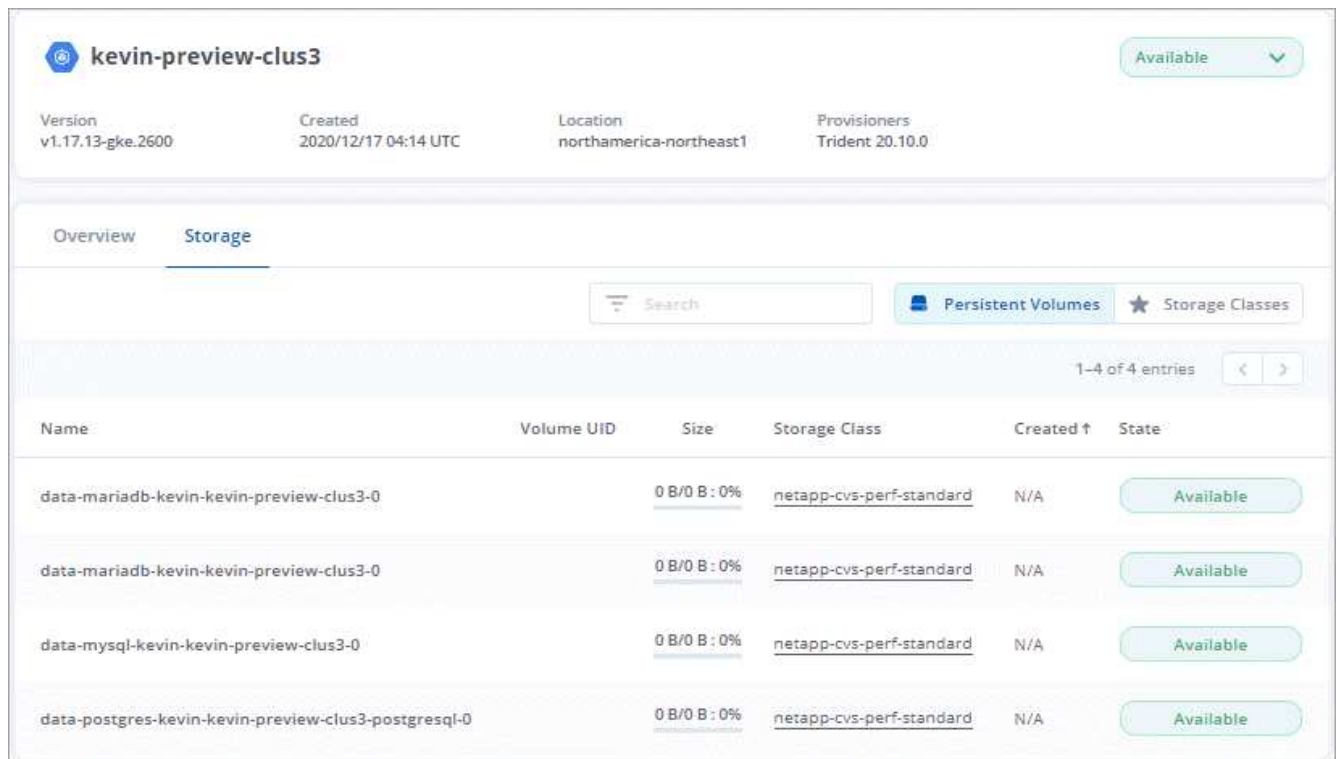
- O faturamento está agora disponível, o que permite que você passe do Plano Gratuito para o Plano Premium. "[Saiba mais sobre faturamento](#)".
- Agora, o Astra Control Service cria volumes persistentes com um tamanho mínimo de 100 GiB ao usar o tipo de serviço CVS-Performance.
- Agora, o Astra Control Service pode descobrir aplicações mais rapidamente.
- Agora você pode criar e excluir contas por conta própria.
- Aprimoramos as notificações quando o Astra Control Service não puder mais acessar um cluster Kubernetes.

Essas notificações são importantes porque o Astra Control Service não consegue gerenciar aplicações para clusters desconetados.

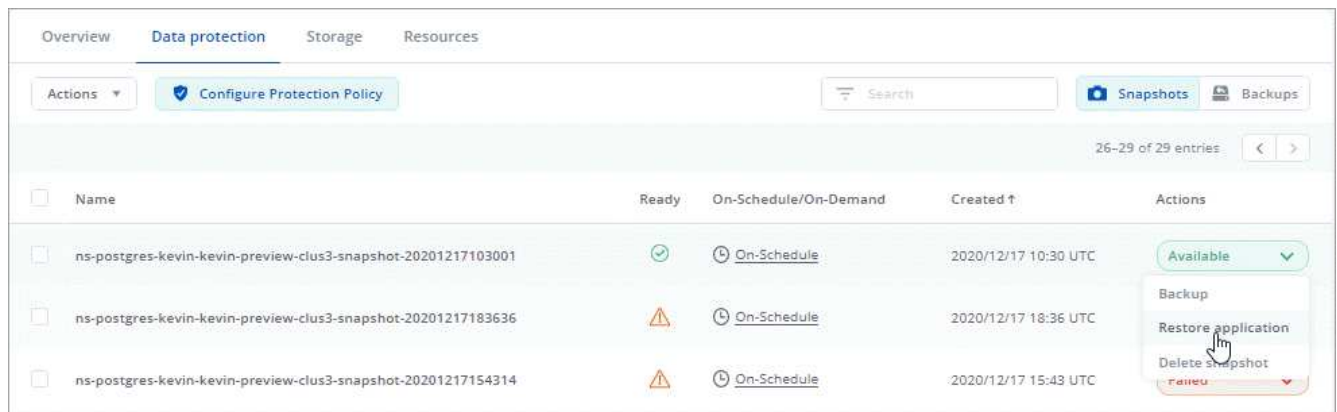
17 de dezembro de 2020 (atualização Beta)

Nós nos concentramos principalmente em correções de bugs para melhorar sua experiência, mas fizemos algumas outras melhorias notáveis:

- Quando você adiciona sua primeira computação do Kubernetes ao Astra Control Service, o armazenamento de objetos agora é criado na região geográfica em que o cluster reside.
- Detalhes sobre volumes persistentes agora estão disponíveis quando você visualiza os detalhes do storage no nível de computação.



- Adicionamos uma opção para restaurar um aplicativo a partir de um snapshot ou backup existente.



- Se você excluir um cluster do Kubernetes que o Astra Control Service está gerenciando, o cluster agora será exibido em um estado **removido**. Em seguida, é possível remover o cluster do Astra Control Service.
- Os proprietários de contas agora podem modificar as funções atribuídas para outros usuários.
- Adicionamos uma seção para faturamento, que será ativada quando o Serviço Astra Control for lançado para disponibilidade Geral (GA).

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

- Não é possível definir um aplicativo em um namespace que foi excluído e recriado

Backup, restauração e clone

- Os clones de aplicativos falham usando uma versão específica do PostgreSQL
- Backups e snapshots de aplicativos falharão se a `volumesnapshotclass` for adicionada após o gerenciamento de um cluster
- A restauração a partir de um backup ao usar a criptografia em trânsito Kerberos pode falhar
- Os dados de backup permanecem no intervalo após a exclusão para buckets com política de retenção expirada

Outras questões

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

Não é possível definir um aplicativo em um namespace que foi excluído e recriado

Se você definir um aplicativo com um namespace, excluir o namespace e reinstalar o aplicativo no mesmo namespace, a operação falhará com um código de erro 409. Para definir o aplicativo usando o namespace recriado, exclua a instância antiga primeiro.

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.

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

Backups e snapshots falham com um erro UI 500 nesse cenário. Como solução alternativa, atualize a lista de aplicativos.

A restauração a partir de um backup ao usar a criptografia em trânsito Kerberos pode falhar

Quando você restaura um aplicativo de um backup para um back-end de armazenamento que esteja usando a criptografia em trânsito Kerberos, a operação de restauração pode falhar. Esse problema não afeta a restauração de um snapshot ou a replicação dos dados do aplicativo usando o NetApp SnapMirror.



Ao usar a criptografia em trânsito Kerberos com volumes NFSv4, verifique se os volumes NFSv4 estão usando as configurações corretas. Consulte a seção Configuração de domínio do NetApp NFSv4 (página 13) do ["Guia de práticas recomendadas e aprimoramentos do NetApp NFSv4"](#).

Os dados de backup permanecem no intervalo após a exclusão para buckets com política de retenção expirada

Se você excluir o backup imutável de um aplicativo após a política de retenção do bucket expirar, o backup será excluído do Astra Control, mas não do bucket. Esse problema será corrigido em um lançamento futuro.

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.

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 gerais

As limitações a seguir afetam o gerenciamento de clusters do Kubernetes do Astra Control Service em qualquer implantação do Kubernetes compatível.

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 Service 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.

A página atividade exibe até 100.000 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](#)".

Limitações para o gerenciamento de clusters GKE

As limitações a seguir se aplicam ao gerenciamento de clusters do Kubernetes no Google Kubernetes Engine (GKE).

Limitações de gerenciamento de aplicativos

As limitações a seguir afetam o gerenciamento de aplicações do Astra Control Service.

As operações de restauração no local para as classes de storage de economia ONTAP nas falham

Se você executar uma restauração no local de um aplicativo (restaurar o aplicativo para seu namespace original) e a classe de armazenamento do aplicativo usar o `ontap-nas-economy` driver, a operação de restauração poderá falhar se o diretório instantâneo não estiver oculto. Antes de restaurar no local, siga as instruções em "[Habilite o backup e a restauração de operações de economia de ONTAP nas](#)" para ocultar o diretório de instantâneos.

Vários aplicativos que usam o mesmo namespace não podem ser restaurados coletivamente para um namespace diferente

Se você gerenciar várias aplicações que usam o mesmo 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 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.

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

Esta versão do Astra Control Service 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.

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.

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

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

- ["Apache K8ssandra"](#)



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

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

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



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.

Limitações de controle de acesso baseado em função (RBAC)

As limitações a seguir se aplicam à maneira como o Astra Control limita o acesso do usuário a recursos ou funcionalidades.

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 usuário membro com restrições de namespace não pode acessar aplicativos clonados ou restaurados até que um usuário Admin 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. Após uma operação de clone ou restauração criar um novo namespace, o administrador/proprietário da conta pode editar a `member` conta de usuário e atualizar as restrições de função para o usuário afetado conceder acesso ao novo namespace.

Os 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"](#).

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 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 as distribuições compatíveis do Kubernetes?	<ul style="list-style-type: none"> • Provedores de nuvem <ul style="list-style-type: none"> ◦ Amazon Web Services <ul style="list-style-type: none"> ▪ Amazon Elastic Kubernetes Service (EKS) ◦ Google Cloud <ul style="list-style-type: none"> ▪ Google Kubernetes Engine (GKE) ◦ Microsoft Azure <ul style="list-style-type: none"> ▪ Serviço Kubernetes do Azure (AKS) • Clusters autogeridos <ul style="list-style-type: none"> ◦ Kubernetes (upstream) ◦ Rancher Kubernetes Engine (RKE) ◦ Red Hat OpenShift Container Platform • Clusters locais <ul style="list-style-type: none"> ◦ Red Hat OpenShift Container Platform no local 	<ul style="list-style-type: none"> • Serviço Kubernetes do Azure no Azure Stack HCI • Google Anthos • Kubernetes (upstream) • Rancher Kubernetes Engine (RKE) • Red Hat OpenShift Container Platform

	Astra Control Service	Astra Control Center
Quais são os backends de armazenamento suportados?	<ul style="list-style-type: none"> • Provedores de nuvem <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 autogeridos <ul style="list-style-type: none"> ◦ Amazon EBS ◦ Discos gerenciados do Azure ◦ Persistent Disk do Google ◦ "Cloud Volumes ONTAP" ◦ NetApp MetroCluster ◦ "Longhorn" • Clusters locais <ul style="list-style-type: none"> ◦ NetApp MetroCluster ◦ Sistemas NetApp ONTAP AFF e FAS ◦ NetApp ONTAP Select ◦ "Cloud Volumes ONTAP" ◦ "Longhorn" 	<ul style="list-style-type: none"> • Sistemas NetApp ONTAP AFF e FAS • NetApp ONTAP Select • "Cloud Volumes ONTAP" • "Longhorn"

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 os discos persistentes do Google como o back-end de storage para seus 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 o link `./conceitos/arquitetura` no cluster e para criar uma ou mais classes de storage.
- Se você usa uma oferta de storage de serviço de nuvem da NetApp como back-end de storage, o Astra Control Service usa o Astra Control Provisioner 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 definir aplicativos do cluster. Volumes persistentes serão provisionados no back-end de storage por meio da 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 namespaces, então você 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 de Kubernetes com uma classe de storage configurada para Provisioner Astra Control com um back-end de storage ONTAP.

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

Você pode experimentar o Astra Control Center usando uma licença de avaliação de 90 dias. A versão de avaliação é suportada por 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 da família de produtos NetApp Astra"](#)
- ["Documentação do Astra Control Center"](#)
- ["Documentação da API Astra Control"](#)
- ["Documentação do Astra Trident"](#)
- ["Documentação do ONTAP"](#)

Implantações de Kubernetes compatíveis

O Astra Control Service pode gerenciar aplicações executadas em um cluster gerenciado do Kubernetes no Amazon Elastic Kubernetes Service (EKS), bem como clusters que você gerencia por conta própria.

O Astra Control Service pode gerenciar aplicações executadas em um cluster gerenciado do Kubernetes no Google Kubernetes Engine (GKE), bem como clusters que você gerencia por conta própria.

O Astra Control Service pode gerenciar aplicações executadas em um cluster gerenciado do Kubernetes no Azure Kubernetes Service (AKS), bem como clusters que você gerencia por conta própria.

- ["Saiba como configurar o Amazon Web Services para o Astra Control Service"](#).
- ["Saiba como configurar o Google Cloud para Astra Control Service"](#).
- ["Saiba como configurar o Microsoft Azure com o Azure NetApp Files para o Serviço Astra Control"](#).
- ["Saiba como configurar o Microsoft Azure com discos gerenciados do Azure para o Astra Control Service"](#).
- ["Saiba como preparar clusters autogerenciados antes de adicioná-los ao Astra Control Service"](#).

Início rápido para Astra Control Service

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

[Um] Configure seu provedor de nuvem

1. Google Cloud:

- Analisar os requisitos do cluster do Google Kubernetes Engine.
- Compre o Cloud Volumes Service no Google Cloud Marketplace.
- Ative as APIs necessárias.
- Crie uma conta de serviço e uma chave de conta de serviço.
- Configure o peering de rede da VPC para o Cloud Volumes Service para o Google Cloud.

["Saiba mais sobre os requisitos do Google Cloud"](#).

2. Amazon Web Services:

- Revise os requisitos de cluster do Amazon Web Services.
- Crie uma conta Amazon.
- Instale a CLI do Amazon Web Services.
- Crie um usuário do IAM.
- Crie e anexe uma política de permissões.
- Salve as credenciais para o usuário do IAM.

["Saiba mais sobre os requisitos do Amazon Web Services"](#).

3. Microsoft Azure:

- Analise os requisitos do cluster do Azure Kubernetes Service para o back-end de storage que você planeja usar.

["Saiba mais sobre os requisitos do Microsoft Azure e do Azure NetApp Files"](#).

["Saiba mais sobre os requisitos de disco gerenciado do Microsoft Azure e do Azure"](#).

Se você estiver gerenciando seu próprio cluster e não estiver hospedado por um fornecedor de nuvem, revise os requisitos para clusters autogerenciados. ["Saiba mais sobre os requisitos de cluster autogeridos"](#).

[Dois] Concluir o Registro do Astra Control

1. Crie ["NetApp BlueXP"](#) uma conta.
2. Especifique seu ID de e-mail do NetApp BlueXP ao criar sua conta do Astra Control ["Na página do produto Astra Control"](#).

["Saiba mais sobre o processo de Registro"](#).

[Três] Adicione clusters ao Astra Control

Depois de fazer login, selecione **Adicionar cluster** para começar a gerenciar seu cluster com o Astra Control.

["Saiba mais sobre como adicionar clusters"](#).

Configure seu provedor de nuvem

Configurar o Amazon Web Services

Algumas etapas são necessárias para preparar seu projeto Amazon Web Services antes de gerenciar clusters do Amazon Elastic Kubernetes Service (EKS) com o Astra Control Service.

Início rápido para configurar o Amazon Web Services

Comece rapidamente seguindo estas etapas ou role para baixo até as seções restantes para obter detalhes completos.

[Um] Analisar os requisitos do Astra Control Service para Amazon Web Services

Garantir que os clusters estejam íntegros e executando uma versão compatível do Kubernetes, que os nós de trabalho estejam on-line e executando Linux ou Windows e muito mais. [Saiba mais sobre este passo.](#)

[Dois] Crie uma conta Amazon

Se você ainda não tiver uma conta da Amazon, será necessário criar uma para que você possa usar o EKS. [Saiba mais sobre este passo.](#)

[Três] Instale a CLI do Amazon Web Services

Instale a AWS CLI para que você possa gerenciar a AWS a partir da linha de comando. [Siga as instruções passo a passo.](#)

[Quatro] Opcional: Crie um usuário do IAM

Crie um usuário do Amazon Identity and Access Management (IAM). Você também pode ignorar esta etapa e usar um usuário IAM existente com o Astra Control Service.

[Leia as instruções passo a passo.](#)

[Cinco] Crie e anexe uma política de permissões

Crie uma política com as permissões necessárias para que o Astra Control Service interaja com sua conta da AWS.

[Leia as instruções passo a passo.](#)

[Seis] Salve as credenciais para o usuário do IAM

Salve as credenciais do usuário do IAM para que você possa importar as credenciais para o Astra Control Service.

[Leia as instruções passo a passo.](#)

Requisitos do cluster do EKS

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

Versão do Kubernetes

Um cluster precisa estar executando uma versão do Kubernetes na faixa de 1,25 a 1,28.

Tipo de imagem

O tipo de imagem para cada nó de trabalho deve ser Linux.

Estado do cluster

Os clusters devem estar em execução em um estado saudável e ter pelo menos um nó de trabalho on-line sem nós de trabalho em um estado com falha.

Previsão do Astra Control

Astra Control Provisioner e uma controladora de snapshot externa são necessários para operações com back-end de storage. Para ativar essas operações, faça o seguinte:

1. ["Instale as CRDs de snapshot e o controlador de snapshot"](#).
2. ["Habilite o Astra Control Provisioner"](#).
3. ["Crie um VolumeSnapshotClass"](#).

Drivers CSI para Amazon Elastic Block Store (EBS)

Se você usar o back-end de armazenamento do Amazon EBS, precisará instalar o driver de Container Storage Interface (CSI) para EBS (ele não é instalado automaticamente).

Consulte os passos para obter instruções sobre a instalação do controlador CSI.

Instale um snapshoter externo

Se você ainda não o fez, ["Instale as CRDs de snapshot e o controlador de snapshot"](#).

Instale o driver CSI como um complemento do Amazon EKS

1. Crie a função IAM do driver do Amazon EBS CSI para contas de serviço. Siga as instruções ["Na documentação da Amazon"](#), usando os comandos da AWS CLI nas instruções.
2. Adicione o complemento Amazon EBS CSI usando o seguinte comando AWS CLI, substituindo informações entre parênteses por valores específicos para o seu ambiente. Substitua o <DRIVER_ROLE> pelo nome da função de driver do EBS CSI que você criou na etapa anterior:

```
aws eks create-addon \  
  --cluster-name <CLUSTER_NAME> \  
  --addon-name aws-ebs-csi-driver \  
  --service-account-role-arn  
arn:aws:iam::<ACCOUNT_ID>:role/<DRIVER_ROLE>
```

Configure a classe de armazenamento EBS

1. Clone o repositório GitHub do driver do Amazon EBS para o seu sistema.

```
git clone https://github.com/kubernetes-sigs/aws-ebs-csi-  
driver.git
```

2. Navegue até o diretório de exemplo de provisionamento dinâmico.

```
cd aws-ebs-csi-driver/examples/kubernetes/dynamic-provisioning/
```

3. Implemente a classe de armazenamento ebs-SC e a reclamação de volume persistente do ebs a partir do diretório manifestos.

```
kubectl apply -f manifests/storageclass.yaml  
kubectl apply -f manifests/claim.yaml
```

4. Descrever a classe de armazenamento ebs-SC.

```
kubectl describe storageclass ebs-sc
```

Você deve ver a saída descrevendo os atributos da classe de armazenamento.

Crie uma conta Amazon

Se você ainda não tiver uma conta da Amazon, será necessário criar uma para ativar o faturamento do Amazon EKS.

Passos

1. Vá para o "[Amazon homepage](#)", selecione **entrar** no canto superior direito e selecione **Iniciar aqui**.
2. Siga as instruções para criar uma conta.

Instale a CLI do Amazon Web Services

Instale a AWS CLI para que você possa gerenciar recursos da AWS a partir da linha de comando.

Passo

1. Vá para "[Primeiros passos com a AWS CLI](#)" e siga as instruções para instalar a CLI.

Opcional: Crie um usuário do IAM

Crie um usuário do IAM para que você possa usar e gerenciar serviços e recursos da AWS com maior segurança. Você também pode ignorar esta etapa e usar um usuário IAM existente com o Astra Control Service.

Passo

1. Vá para "[Criando usuários do IAM](#)" e siga as instruções para criar um usuário do IAM.

Crie e anexe uma política de permissões

Crie uma política com as permissões necessárias para que o Astra Control Service interaja com sua conta da AWS.

Passos

1. Crie um novo arquivo chamado `policy.json`.
2. Copie o seguinte conteúdo JSON para o arquivo:

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "cloudwatch:GetMetricData",
        "fsx:DescribeVolumes",
        "ec2:DescribeRegions",
        "s3:CreateBucket",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:GetObject",
        "iam:SimulatePrincipalPolicy",
        "s3:ListAllMyBuckets",
        "eks:DescribeCluster",
        "eks:ListNodegroups",
        "eks:DescribeNodegroup",
        "eks:ListClusters",
        "iam:GetUser",
        "s3:DeleteObject",
        "s3:DeleteBucket",
        "autoscaling:DescribeAutoScalingGroups"
      ],
      "Resource": "*"
    }
  ]
}

```

3. Crie a política:

```

POLICY_ARN=$(aws iam create-policy --policy-name <policy-name> --policy
-document file://policy.json --query='Policy.Arn' --output=text)

```

4. Anexe a política ao usuário do IAM. Substitua <IAM-USER-NAME> pelo nome de usuário do usuário do IAM que você criou ou por um usuário do IAM existente:

```

aws iam attach-user-policy --user-name <IAM-USER-NAME> --policy-arn
=$POLICY_ARN

```

Salve as credenciais para o usuário do IAM

Salve as credenciais do usuário do IAM para que você possa informar o Astra Control Service sobre o usuário.

Passos

1. Faça o download das credenciais. Substitua <IAM-USER-NAME> pelo nome de usuário do usuário do IAM que você deseja usar:

```
aws iam create-access-key --user-name <IAM-USER-NAME> --output json > credential.json
```

Resultado

O `credential.json` arquivo é criado e você pode importar as credenciais para o Astra Control Service.

Configure o Google Cloud

Algumas etapas são necessárias para preparar seu projeto do Google Cloud antes de gerenciar clusters do Google Kubernetes Engine com o Astra Control Service.



Se você não começar a usar o Google Cloud Volumes Service para Google Cloud como um back-end de armazenamento, mas planeja usá-lo em uma data posterior, siga as etapas necessárias para configurar o Google Cloud Volumes Service agora. Criar uma conta de serviço posteriormente significa que você pode perder o acesso aos buckets de storage existentes.

Início rápido para configurar o Google Cloud

Comece rapidamente seguindo estas etapas ou role para baixo até as seções restantes para obter detalhes completos.

[Um] Analisar os requisitos do Astra Control Service para Google Kubernetes Engine

Garantir que os clusters estejam íntegros e executando uma versão compatível do Kubernetes, que os nós de trabalho estejam on-line, executando um tipo de imagem compatível e muito mais. [Saiba mais sobre este passo.](#)

[Dois] (Opcional): Compre o Cloud Volumes Service para o Google Cloud

Se você planeja usar o Cloud Volumes Service para Google Cloud como um back-end de armazenamento, vá para a página NetApp Cloud Volumes Service no Google Cloud Marketplace e selecione Comprar. [Saiba mais sobre este passo.](#)

[Três] Habilite APIs em seu projeto do Google Cloud

Ative as seguintes APIs do Google Cloud:

- Google Kubernetes Engine
- Storage de nuvem
- API JSON do Cloud Storage
- Utilização do serviço

- API do Cloud Resource Manager
- NetApp Cloud Volumes Service
 - Necessário para o Cloud Volumes Service para o Google Cloud
 - Opcional (mas recomendado) para o Google Persistent Disk
- API de gerenciamento de clientes de serviços
- API de rede de serviço
- API de gerenciamento de serviços

[Siga as instruções passo a passo.](#)

[Quatro] Crie uma conta de serviço que tenha as permissões necessárias

Crie uma conta de serviço do Google Cloud que tenha as seguintes permissões:

- Administrador do Kubernetes Engine
- Administrador do NetApp Cloud volumes
 - Necessário para o Cloud Volumes Service para o Google Cloud
 - Opcional (mas recomendado) para o Google Persistent Disk
- Administrador de storage
- Visualizador de utilização do serviço
- Visualizador de rede de computação

[Leia as instruções passo a passo.](#)

[Cinco] Crie uma chave de conta de serviço

Crie uma chave para a conta de serviço e salve o arquivo de chave em um local seguro. [Siga as instruções passo a passo.](#)

[Seis] (Opcional): Configurar o peering de rede para sua VPC

Se você planeja usar o Cloud Volumes Service para o Google Cloud como um back-end de armazenamento, configure o peering de rede da VPC para o Cloud Volumes Service. [Siga as instruções passo a passo.](#)

Requisitos do cluster GKE

Um cluster de Kubernetes precisa atender aos requisitos a seguir para que você possa descobri-lo e gerenciá-lo no Astra Control Service. Observe que alguns desses requisitos só se aplicam se você planeja usar o Cloud Volumes Service para Google Cloud como um back-end de storage.

Versão do Kubernetes

Um cluster precisa estar executando uma versão do Kubernetes na faixa de 1,26 a 1,28.

Tipo de imagem

O tipo de imagem para cada nó de trabalho deve ser `COS_CONTAINERD`.

Estado do cluster

Os clusters devem estar em execução em um estado saudável e ter pelo menos um nó de trabalho on-line sem nós de trabalho em um estado com falha.

Região do Google Cloud

Se você planeja usar o Cloud Volumes Service para Google Cloud como um back-end de storage, os clusters precisam estar em execução em uma ["Região em que o Cloud Volumes Service para Google Cloud é compatível."](#) observação de que o Astra Control Service é compatível com ambos os tipos de serviço: CVS e CVS-Performance. Como prática recomendada, você deve escolher uma região compatível com o Cloud Volumes Service para o Google Cloud, mesmo que não a use como back-end de storage. Isso facilita o uso futuro do Cloud Volumes Service para Google Cloud como back-end de storage, se os requisitos de performance mudarem.

Rede

Se você pretende usar o Cloud Volumes Service para Google Cloud como um back-end de storage, o cluster precisa residir em uma VPC com o Cloud Volumes Service. [Este passo é descrito abaixo.](#)

Clusters privados

Se o cluster for privado, o deve permitir o endereço IP do ["redes autorizadas"](#) Astra Control Service:

52.188.218.166/32

Modo de operação para um cluster GKE

Você deve usar o modo de operação padrão. O modo piloto automático não foi testado neste momento. ["Saiba mais sobre os modos de operação"](#).

Pools de armazenamento

Se você usar o NetApp Cloud Volumes Service como um back-end de storage com o tipo de serviço CVS, precisará configurar pools de storage antes de provisionar volumes. ["Tipo de serviço, classes de armazenamento e tamanho PV para clusters GKE"](#)Consulte para obter mais informações.

Opcional: Adquira o Cloud Volumes Service para o Google Cloud

O Astra Control Service usa o Cloud Volumes Service para Google Cloud como o back-end de storage para volumes persistentes. Se você planeja usar esse serviço, precisa comprar o Cloud Volumes Service para Google Cloud no Google Cloud Marketplace para habilitar a cobrança de volumes persistentes.

Passo

1. Vá para o ["Página NetApp Cloud Volumes Service"](#) no Google Cloud Marketplace, selecione **Comprar** e siga as instruções.

["Siga as instruções passo a passo na documentação do Google Cloud para comprar e ativar o serviço"](#).

Habilite APIs em seu projeto

Seu projeto precisa de permissões para acessar APIs específicas do Google Cloud. As APIs são usadas para interagir com os recursos do Google Cloud, como clusters do Google Kubernetes Engine (GKE) e armazenamento do NetApp Cloud Volumes Service.

Passo

1. ["Use o console do Google Cloud ou a CLI gcloud para habilitar as seguintes APIs"](#):
 - Google Kubernetes Engine
 - Storage de nuvem
 - API JSON do Cloud Storage
 - Utilização do serviço

- API do Cloud Resource Manager
- NetApp Cloud Volumes Service (necessário para o Cloud Volumes Service para o Google Cloud)
- API de gerenciamento de clientes de serviços
- API de rede de serviço
- API de gerenciamento de serviços

O vídeo a seguir mostra como ativar as APIs do console do Google Cloud.

► <https://docs.netapp.com/pt-br/astra-control-service/media/get-started/video-enable-gcp-apis.mp4> (video)

Crie uma conta de serviço

O Astra Control Service usa uma conta de serviço do Google Cloud para facilitar o gerenciamento de dados da aplicação Kubernetes em seu nome.

Passos

1. Vá para Google Cloud e "[crie uma conta de serviço usando o console, o comando gcloud ou outro método preferido](#)".
2. Conceda à conta de serviço as seguintes funções:
 - * **Kubernetes Engine Admin*** - usado para listar clusters e criar acesso de administrador para gerenciar aplicativos.
 - **Admin do NetApp volumes** - usado para gerenciar o armazenamento persistente de aplicativos.
 - **Admin de armazenamento** - usado para gerenciar buckets e objetos para backups de aplicativos.
 - **Visualizador de uso do serviço** - usado para verificar se o Cloud Volumes Service necessário para APIs do Google Cloud está ativado.
 - **Visualizador de rede de computação** - usado para verificar se a VPC do Kubernetes está autorizada a acessar o Cloud Volumes Service para o Google Cloud.

Se quiser usar o gcloud, siga as etapas na interface do Astra Control. Selecione **conta > credenciais > Adicionar credenciais** e, em seguida, selecione **instruções**.

Se você quiser usar o console do Google Cloud, o vídeo a seguir mostra como criar a conta de serviço a partir do console.

► <https://docs.netapp.com/pt-br/astra-control-service/media/get-started/video-create-gcp-service-account.mp4>

(video)

Configure a conta de serviço para uma VPC compartilhada

Para gerenciar clusters do GKE que residem em um projeto, mas usar uma VPC de um projeto diferente (uma VPC compartilhada), você precisa especificar a conta de serviço Astra como membro do projeto host com a função **Compute Network Viewer**.

Passos

1. No console do Google Cloud, vá para **IAM e Admin** e selecione **Contas de serviço**.
2. Encontre a conta de serviço Astra que tenha "[as permissões necessárias](#)" e copie o endereço de e-mail.
3. Acesse ao seu projeto anfitrião e selecione **IAM & Admin > IAM**.
4. Selecione **Adicionar** e adicione uma entrada para a conta de serviço.
 - a. **Novos membros:** Insira o endereço de e-mail da conta de serviço.
 - b. **Role:** Selecione **Compute Network Viewer**.
 - c. Selecione **Guardar**.

Resultado

Adicionar um cluster GKE usando uma VPC compartilhada funcionará totalmente com o Astra.

Crie uma chave de conta de serviço

Em vez de fornecer um nome de usuário e senha ao Astra Control Service, você fornecerá uma chave de conta de serviço ao adicionar seu primeiro cluster. O Astra Control Service usa a chave da conta de serviço para estabelecer a identidade da conta de serviço que você acabou de configurar.

A chave de conta de serviço é armazenada em texto simples no formato JavaScript Object Notation (JSON). Ele contém informações sobre os recursos do GCP aos quais você tem permissão para acessar.

Você só pode visualizar ou baixar o arquivo JSON quando você criar a chave. No entanto, você pode criar uma nova chave a qualquer momento.

Passos

1. Vá para Google Cloud e "[crie uma chave de conta de serviço usando o console, o comando gcloud ou outro método preferido](#)".
2. Quando solicitado, salve o arquivo de chave da conta de serviço em um local seguro.

O vídeo a seguir mostra como criar a chave da conta de serviço no console do Google Cloud.

► <https://docs.netapp.com/pt-br/astra-control-service/media/get-started/video-create-gcp-service-account->

[key.mp4](#) (video)

Opcional: Configure o peering de rede para a VPC

Se você planeja usar o Cloud Volumes Service para Google Cloud como um serviço de back-end de armazenamento, a etapa final é configurar o peering de rede da VPC para o Cloud Volumes Service.

A maneira mais fácil de configurar o peering de rede é obtendo os comandos gcloud diretamente do Cloud Volumes Service. Os comandos estão disponíveis no Cloud Volumes Service ao criar um novo sistema de arquivos.

Passos

1. "[Vá para Mapas de Regiões globais da NetApp BlueXP](#) " E identifique o tipo de serviço que você usará na região do Google Cloud onde reside o cluster.

O Cloud Volumes Service fornece dois tipos de serviço: CVS e CVS-Performance. "[Saiba mais sobre esses tipos de serviço](#)".

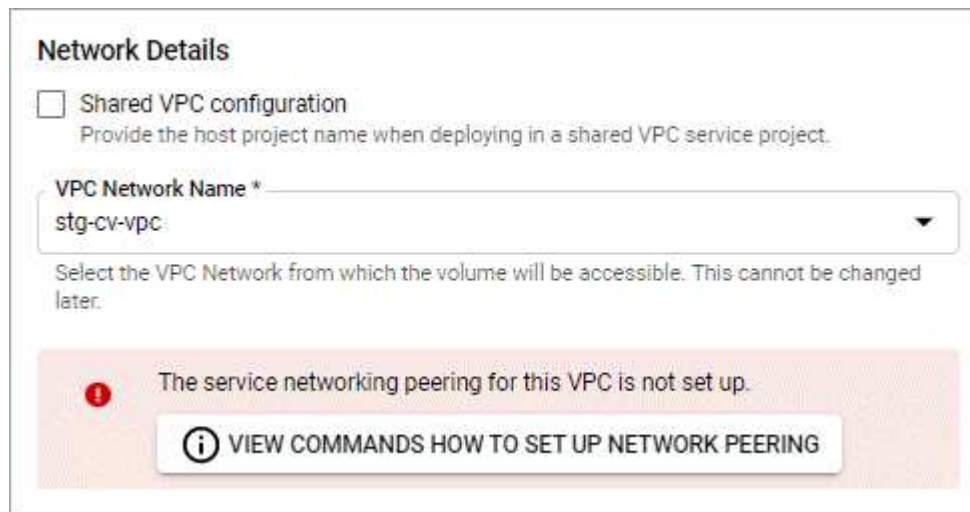
2. "[Acesse o Cloud volumes no Google Cloud Platform](#)".
3. Na página **volumes**, selecione **criar**.
4. Em **tipo de serviço**, selecione **CVS** ou **CVS-Performance**.

Você precisa escolher o tipo de serviço correto para sua região do Google Cloud. Este é o tipo de serviço identificado na etapa 1. Depois de selecionar um tipo de serviço, a lista de regiões na página é atualizada com as regiões em que esse tipo de serviço é suportado.

Após esta etapa, você só precisará inserir suas informações de rede para obter os comandos.

5. Em **região**, selecione sua região e zona.
6. Em **Detalhes da rede**, selecione sua VPC.

Se você não tiver configurado o peering de rede, verá a seguinte notificação:



7. Selecione o botão para visualizar os comandos de configuração do peering de rede.
8. Copie os comandos e execute-os no Cloud Shell.

Para obter mais detalhes sobre como usar esses comandos, consulte o "[Início rápido para Cloud Volumes](#)"

[Service para GCP](#)".

"[Saiba mais sobre como configurar o acesso a serviços privados e configurar o peering de rede](#)".

9. Depois de terminar, você pode selecionar cancelar na página **criar sistema de arquivos**.

Começamos a criar esse volume apenas para obter os comandos para peering de rede.

Configure o Microsoft Azure com o Azure NetApp Files

Algumas etapas são necessárias para preparar sua assinatura do Microsoft Azure antes que você possa gerenciar os clusters do Azure Kubernetes Service com o Astra Control Service. Siga estas instruções se você planeja usar o Azure NetApp Files como um back-end de storage.

Início rápido para configurar o Azure

Comece rapidamente seguindo estas etapas ou role para baixo até as seções restantes para obter detalhes completos.

[Um] Analisar os requisitos do Astra Control Service para Azure Kubernetes Service

Garantir que os clusters estejam íntegros e executando uma versão compatível do Kubernetes, que os pools de nós estejam online, executando Linux e muito mais. [Saiba mais sobre este passo](#).

[Dois] Inscreva-se no Microsoft Azure

Crie uma conta do Microsoft Azure. [Saiba mais sobre este passo](#).

[Três] Inscreva-se no Azure NetApp Files

Registre o Fornecedor de recursos do NetApp. [Saiba mais sobre este passo](#).

[Quatro] Crie uma conta do NetApp

Vá para o Azure NetApp Files no portal do Azure e crie uma conta do NetApp. [Saiba mais sobre este passo](#).

[Cinco] Configurar pools de capacidade

Configure um ou mais pools de capacidade para seus volumes persistentes. [Saiba mais sobre este passo](#).

[Seis] Delegar uma sub-rede ao Azure NetApp Files

Delegar uma sub-rede ao Azure NetApp Files para que o Astra Control Service possa criar volumes persistentes nessa sub-rede. [Saiba mais sobre este passo](#).

[Sete] Crie um diretor de serviço do Azure

Crie um diretor de serviço do Azure que tenha a função Colaborador. [Saiba mais sobre este passo](#).

[Oito] Opcional: Configurar redundância para buckets de backup do Azure

Por padrão, os buckets que o Astra Control Service usa para armazenar backups do Serviço Kubernetes do Azure usam a opção de redundância LRS (armazenamento redundante local). Como etapa opcional, você

pode configurar um nível mais durável de redundância para buckets do Azure. [Saiba mais sobre este passo.](#)

Requisitos de cluster do Azure Kubernetes Service

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

Versão do Kubernetes

Os clusters precisam estar executando o Kubernetes das versões 1,26 a 1,28.

Tipo de imagem

O tipo de imagem para todos os pools de nós deve ser Linux.

Estado do cluster

Os clusters devem estar em execução em um estado saudável e ter pelo menos um nó de trabalho on-line sem nós de trabalho em um estado com falha.

Região do Azure

Os clusters precisam residir em uma região onde o Azure NetApp Files esteja disponível. "[Veja os produtos Azure por região](#)".

Subscrição

Os clusters precisam residir em uma subscrição na qual o Azure NetApp Files esteja ativado. Você escolherá uma assinatura quando [Inscreva-se no Azure NetApp Files](#) .

VNet

Considere os seguintes requisitos do VNet:

- Os clusters devem residir em um VNet que tenha acesso direto a uma sub-rede delegada pelo Azure NetApp Files. [Saiba como configurar uma sub-rede delegada.](#)
- Se os clusters do Kubernetes estiverem em um VNet que seja direcionado para a sub-rede delegada do Azure NetApp Files que está em outro VNet, ambos os lados da conexão de peering devem estar online.
- Esteja ciente de que o limite padrão para o número de IPs usados em uma VNet (incluindo VNets de acesso imediato) com Azure NetApp Files é 1.000. "[Ver limites de recursos do Azure NetApp Files](#)".

Se você estiver perto do limite, você tem duas opções:

- Você pode "[envie uma solicitação para um aumento de limite](#)". Contacte o seu representante da NetApp se precisar de ajuda.
- Ao criar um novo cluster do Amazon Kubernetes Service (AKS), especifique uma nova rede para o cluster. Uma vez criada a nova rede, provisione uma nova sub-rede e delegue a sub-rede ao Azure NetApp Files.

Inscreva-se no Microsoft Azure

Se você não tiver uma conta do Microsoft Azure, comece por se inscrever no Microsoft Azure.

Passos

1. Acesse a "[Página de subscrição do Azure](#)" para subscrever o serviço Azure.
2. Selecione um plano e siga as instruções para concluir a assinatura.

Inscreva-se no Azure NetApp Files

Obtenha acesso ao Azure NetApp Files registrando o Fornecedor de recursos do NetApp.

Passos

1. Faça login no portal do Azure.
2. ["Siga a documentação do Azure NetApp Files para registrar o Fornecedor de recursos do NetApp"](#).

Crie uma conta do NetApp

Crie uma conta NetApp no Azure NetApp Files.

Passo

1. ["Siga a documentação do Azure NetApp Files para criar uma conta do NetApp a partir do portal do Azure"](#).

Configure um pool de capacidade

Um ou mais pools de capacidade são necessários para que o Astra Control Service possa provisionar volumes persistentes em um pool de capacidade. O Astra Control Service não cria pools de capacidade para você.

Leve o seguinte em consideração ao configurar pools de capacidade para suas aplicações Kubernetes:

- Os pools de capacidade precisam ser criados na mesma região do Azure, onde os clusters AKS serão gerenciados com o Astra Control Service.
- Um pool de capacidade pode ter um nível de serviço Ultra, Premium ou Standard. Cada um desses níveis de serviço foi projetado para diferentes necessidades de performance. O Astra Control Service é compatível com todos os três.

Você precisa configurar um pool de capacidade para cada nível de serviço que deseja usar com os clusters do Kubernetes.

["Saiba mais sobre os níveis de serviço do Azure NetApp Files"](#).

- Antes de criar um pool de capacidade para as aplicações que pretende proteger com o Astra Control Service, escolha a performance e a capacidade necessárias para essas aplicações.

O provisionamento da quantidade certa de capacidade garante que os usuários possam criar volumes persistentes conforme necessário. Se a capacidade não estiver disponível, os volumes persistentes não poderão ser provisionados.

- Um pool de capacidade do Azure NetApp Files pode usar o tipo de QoS manual ou automático. O Astra Control Service é compatível com pools de capacidade de QoS automática. Pools de capacidade de QoS manual não são compatíveis.

Passo

1. ["Siga a documentação do Azure NetApp Files para configurar um pool de capacidade de QoS automática"](#).

Delegar uma sub-rede ao Azure NetApp Files

Você precisa delegar uma sub-rede ao Azure NetApp Files para que o Serviço de Controle Astra possa criar volumes persistentes nessa sub-rede. Observe que o Azure NetApp Files permite que você tenha apenas uma sub-rede delegada em um VNet.

Se você estiver usando VNets peered, ambos os lados da conexão de peering devem estar on-line: O VNet onde seus clusters Kubernetes residem e o VNet que tem a sub-rede delegada pelo Azure NetApp Files.

Passo

1. ["Siga a documentação do Azure NetApp Files para delegar uma sub-rede no Azure NetApp Files"](#).

Depois de terminar

Aguarde cerca de 10 minutos antes de descobrir o cluster em execução na sub-rede delegada.

Crie um diretor de serviço do Azure

O Astra Control Service requer um diretor de serviço do Azure que é atribuído à função Colaborador. O Astra Control Service usa este princípio de serviço para facilitar o gerenciamento de dados da aplicação Kubernetes em seu nome.

Um responsável de serviço é uma identidade criada especificamente para uso com aplicativos, serviços e ferramentas. A atribuição de uma função ao responsável do serviço restringe o acesso a recursos específicos do Azure.

Siga as etapas abaixo para criar um princípio de serviço usando a CLI do Azure. Você precisará salvar a saída em um arquivo JSON e fornecê-la ao Astra Control Service mais tarde. ["Consulte a documentação do Azure para obter mais detalhes sobre como usar a CLI"](#).

As etapas a seguir assumem que você tem permissão para criar um responsável de serviço e que você tem o Microsoft Azure SDK (comando az) instalado em sua máquina.

Requisitos

- O responsável pelo serviço deve usar autenticação regular. Os certificados não são suportados.
- O responsável do serviço deve ter acesso ao Colaborador ou proprietário à sua subscrição do Azure.
- A subscrição ou o grupo de recursos que escolher para o âmbito tem de conter os clusters AKS e a sua conta Azure NetApp Files.

Passos

1. Identificar a ID da subscrição e do locatário em que residem os clusters do AKS (estes são os clusters que pretende gerir no Astra Control Service).

```
az configure --list-defaults
az account list --output table
```

2. Siga um destes procedimentos, dependendo se você usar uma assinatura inteira ou um grupo de recursos:

- Crie o responsável do serviço, atribua a função Colaborador e especifique o escopo para toda a assinatura onde os clusters residem.

```
az ad sp create-for-rbac --name service-principal-name --role
contributor --scopes /subscriptions/SUBSCRIPTION-ID
```

- Crie o principal de serviço, atribua a função Colaborador e especifique o grupo de recursos onde os clusters residem.

```
az ad sp create-for-rbac --name service-principal-name --role
contributor --scopes /subscriptions/SUBSCRIPTION-
ID/resourceGroups/RESOURCE-GROUP-ID
```

3. Armazene a saída resultante da CLI do Azure como um arquivo JSON.

Você precisará fornecer esse arquivo para que o Astra Control Service possa descobrir seus clusters AKS e gerenciar operações de gerenciamento de dados do Kubernetes. ["Saiba mais sobre como gerenciar credenciais no Astra Control Service"](#).

4. Opcional: Adicione o ID da assinatura ao arquivo JSON para que o Astra Control Service preencha automaticamente o ID quando você selecionar o arquivo.

Caso contrário, você precisará inserir o ID da assinatura no Astra Control Service quando solicitado.

Exemplo

```
{
  "appId": "0db3929a-bfb0-4c93-baee-aaf8",
  "displayName": "sp-example-dev-sandbox",
  "name": "http://sp-example-dev-sandbox",
  "password": "mypassword",
  "tenant": "011cdf6c-7512-4805-aaf8-7721afd8ca37",
  "subscriptionId": "99ce999a-8c99-99d9-a9d9-99cce99f99ad"
}
```

5. Opcional: Teste seu principal de serviço. Escolha entre os seguintes comandos de exemplo, dependendo do escopo que o seu responsável de serviço usa.

Escopo da assinatura

```
az login --service-principal --username APP-ID-SERVICEPRINCIPAL
--password PASSWORD --tenant TENANT-ID
az group list --subscription SUBSCRIPTION-ID
az aks list --subscription SUBSCRIPTION-ID
az storage container list --account-name STORAGE-ACCOUNT-NAME
```

Escopo do grupo de recursos

```
az login --service-principal --username APP-ID-SERVICEPRINCIPAL
--password PASSWORD --tenant TENANT-ID
az aks list --subscription SUBSCRIPTION-ID --resource-group RESOURCE-
GROUP-ID
```


Opcional: Configurar redundância para buckets de backup do Azure

Você pode configurar um nível de redundância mais durável para buckets de backup do Azure. Por padrão, os buckets que o Astra Control Service usa para armazenar backups do Serviço Kubernetes do Azure usam a opção de redundância LRS (armazenamento redundante local). Para usar uma opção de redundância mais durável para buckets do Azure, você precisa fazer o seguinte:

Passos

1. Crie uma conta de armazenamento do Azure que use o nível de redundância necessário usando ["estas instruções"](#)o .
2. Crie um contentor do Azure na nova conta de armazenamento usando ["estas instruções"](#)o .
3. Adicione o contêiner como um bucket ao Astra Control Service. ["Adicione um balde adicional"](#)Consulte a .
4. (Opcional) para usar o bucket recém-criado como o bucket padrão para backups do Azure, defina-o como o bucket padrão para o Azure. ["Altere o intervalo predefinido"](#)Consulte a .

Configurar o Microsoft Azure com discos gerenciados do Azure

Algumas etapas são necessárias para preparar sua assinatura do Microsoft Azure antes que você possa gerenciar os clusters do Azure Kubernetes Service com o Astra Control Service. Siga estas instruções se você planeja usar os discos gerenciados do Azure como um back-end de storage.

Início rápido para configurar o Azure

Comece rapidamente seguindo estas etapas ou role para baixo até as seções restantes para obter detalhes completos.

[Um] Analisar os requisitos do Astra Control Service para Azure Kubernetes Service

Garantir que os clusters estejam íntegros e executando uma versão compatível do Kubernetes, que os pools de nós estejam online, executando Linux e muito mais. [Saiba mais sobre este passo.](#)

[Dois] Inscreva-se no Microsoft Azure

Crie uma conta do Microsoft Azure. [Saiba mais sobre este passo.](#)

[Três] Crie um diretor de serviço do Azure

Crie um diretor de serviço do Azure que tenha a função Colaborador. [Saiba mais sobre este passo.](#)

[Quatro] Configure os detalhes do driver da Container Storage Interface (CSI)

Você precisa configurar sua assinatura do Azure e o cluster para trabalhar com os drivers CSI. [Saiba mais sobre este passo.](#)

[Cinco] Opcional: Configurar redundância para buckets de backup do Azure

Por padrão, os buckets que o Astra Control Service usa para armazenar backups do Serviço Kubernetes do Azure usam a opção de redundância LRS (armazenamento redundante local). Como etapa opcional, você pode configurar um nível mais durável de redundância para buckets do Azure. [Saiba mais sobre este passo.](#)

Requisitos de cluster do Azure Kubernetes Service

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

Versão do Kubernetes

Os clusters precisam estar executando o Kubernetes das versões 1,26 a 1,28.

Tipo de imagem

O tipo de imagem para todos os pools de nós deve ser Linux.

Estado do cluster

Os clusters devem estar em execução em um estado saudável e ter pelo menos um nó de trabalho on-line sem nós de trabalho em um estado com falha.

Região do Azure

Como prática recomendada, você deve escolher uma região compatível com Azure NetApp Files, mesmo que não a use como back-end de storage. Isso facilita o uso do Azure NetApp Files como um back-end de storage no futuro, se os requisitos de performance mudarem. ["Veja os produtos Azure por região"](#).

Controladores CSI

Os clusters devem ter os drivers CSI apropriados instalados.

Inscreva-se no Microsoft Azure

Se você não tiver uma conta do Microsoft Azure, comece por se inscrever no Microsoft Azure.

Passos

1. Acesse a ["Página de subscrição do Azure"](#) para inscrever o serviço Azure.
2. Selecione um plano e siga as instruções para concluir a assinatura.

Crie um diretor de serviço do Azure

O Astra Control Service requer um diretor de serviço do Azure que é atribuído à função Colaborador. O Astra Control Service usa este princípio de serviço para facilitar o gerenciamento de dados da aplicação Kubernetes em seu nome.

Um responsável de serviço é uma identidade criada especificamente para uso com aplicativos, serviços e ferramentas. A atribuição de uma função ao responsável do serviço restringe o acesso a recursos específicos do Azure.

Siga as etapas abaixo para criar um princípio de serviço usando a CLI do Azure. Você precisará salvar a saída em um arquivo JSON e fornecê-la ao Astra Control Service mais tarde. ["Consulte a documentação do Azure para obter mais detalhes sobre como usar a CLI"](#).

As etapas a seguir assumem que você tem permissão para criar um responsável de serviço e que você tem o Microsoft Azure SDK (comando az) instalado em sua máquina.

Requisitos

- O responsável pelo serviço deve usar autenticação regular. Os certificados não são suportados.
- O responsável do serviço deve ter acesso ao Colaborador ou proprietário à sua subscrição do Azure.
- A subscrição ou o grupo de recursos que escolher para o âmbito tem de conter os clusters AKS e a sua

conta Azure NetApp Files.

Passos

1. Identificar a ID da subscrição e do locatário em que residem os clusters do AKS (estes são os clusters que pretende gerir no Astra Control Service).

```
az configure --list-defaults
az account list --output table
```

2. Siga um destes procedimentos, dependendo se você usar uma assinatura inteira ou um grupo de recursos:

- Crie o responsável do serviço, atribua a função Colaborador e especifique o escopo para toda a assinatura onde os clusters residem.

```
az ad sp create-for-rbac --name service-principal-name --role
contributor --scopes /subscriptions/SUBSCRIPTION-ID
```

- Crie o principal de serviço, atribua a função Colaborador e especifique o grupo de recursos onde os clusters residem.

```
az ad sp create-for-rbac --name service-principal-name --role
contributor --scopes /subscriptions/SUBSCRIPTION-
ID/resourceGroups/RESOURCE-GROUP-ID
```

3. Armazene a saída resultante da CLI do Azure como um arquivo JSON.

Você precisará fornecer esse arquivo para que o Astra Control Service possa descobrir seus clusters AKS e gerenciar operações de gerenciamento de dados do Kubernetes. ["Saiba mais sobre como gerenciar credenciais no Astra Control Service"](#).

4. Opcional: Adicione o ID da assinatura ao arquivo JSON para que o Astra Control Service preencha automaticamente o ID quando você selecionar o arquivo.

Caso contrário, você precisará inserir o ID da assinatura no Astra Control Service quando solicitado.

Exemplo

```
{
  "appId": "0db3929a-bfb0-4c93-baee-aaf8",
  "displayName": "sp-example-dev-sandbox",
  "name": "http://sp-example-dev-sandbox",
  "password": "mypassword",
  "tenant": "011cdf6c-7512-4805-aaf8-7721afd8ca37",
  "subscriptionId": "99ce999a-8c99-99d9-a9d9-99cce99f99ad"
}
```

5. Opcional: Teste seu principal de serviço. Escolha entre os seguintes comandos de exemplo, dependendo do escopo que o seu responsável de serviço usa.

Escopo da assinatura

```
az login --service-principal --username APP-ID-SERVICEPRINCIPAL
--password PASSWORD --tenant TENANT-ID
az group list --subscription SUBSCRIPTION-ID
az aks list --subscription SUBSCRIPTION-ID
az storage container list --account-name STORAGE-ACCOUNT-NAME
```

Escopo do grupo de recursos

```
az login --service-principal --username APP-ID-SERVICEPRINCIPAL
--password PASSWORD --tenant TENANT-ID
az aks list --subscription SUBSCRIPTION-ID --resource-group RESOURCE-
GROUP-ID
```

Configure os detalhes do driver da Container Storage Interface (CSI)

Para usar discos gerenciados do Azure com o Astra Control Service, você precisará instalar os drivers CSI necessários.

Ative o recurso de driver CSI na sua assinatura do Azure

Antes de instalar os drivers CSI, você precisa ativar o recurso de driver CSI na sua assinatura do Azure.

Passos

1. Abra a interface da linha de comando do Azure.
2. Execute o seguinte comando para Registrar o driver:

```
az feature register --namespace "Microsoft.ContainerService" --name
"EnableAzureDiskFileCSIDriver"
```

3. Execute o seguinte comando para garantir que a alteração seja propagada:

```
az provider register -n Microsoft.ContainerService
```

Você deve ver saída semelhante ao seguinte:

```
{
  "id": "/subscriptions/b200155f-001a-43be-87be-3edde83acef4/providers/Microsoft.Features/providers/Microsoft.ContainerService/features/EnableAzureDiskFileCSIDriver",
  "name": "Microsoft.ContainerService/EnableAzureDiskFileCSIDriver",
  "properties": {
    "state": "Registering"
  },
  "type": "Microsoft.Features/providers/features"
}
```

Instale os drivers de CSI de disco gerenciado do Azure no cluster do Azure Kubernetes Service

Você pode instalar os drivers do Azure CSI para concluir sua preparação.

Passo

1. Vá para ["A documentação do driver do Microsoft CSI"](#).
2. Siga as instruções para instalar os drivers CSI necessários.

Opcional: Configurar redundância para buckets de backup do Azure

Você pode configurar um nível de redundância mais durável para buckets de backup do Azure. Por padrão, os buckets que o Astra Control Service usa para armazenar backups do Serviço Kubernetes do Azure usam a opção de redundância LRS (armazenamento redundante local). Para usar uma opção de redundância mais durável para buckets do Azure, você precisa fazer o seguinte:

Passos

1. Crie uma conta de armazenamento do Azure que use o nível de redundância necessário usando ["estas instruções"](#)o .
2. Crie um contentor do Azure na nova conta de armazenamento usando ["estas instruções"](#)o .
3. Adicione o contêiner como um bucket ao Astra Control Service. ["Adicione um balde adicional"](#)Consulte a .
4. (Opcional) para usar o bucket recém-criado como o bucket padrão para backups do Azure, defina-o como o bucket padrão para o Azure. ["Altere o intervalo predefinido"](#)Consulte a .

Registre-se para ter uma conta do Astra Control Service

Para usar o serviço Astra Control, você precisa de uma conta do serviço Astra Control que esteja associada à sua conta do NetApp BlueXP . Conclua o processo de Registro do Serviço de Controle Astra e, se você ainda não tiver uma conta do BlueXP , inscreva-se no BlueXP para acessar o Serviço de Controle Astra.

Registre-se para ter uma conta Astra Control

Antes de fazer login no Astra Control Service, você precisa concluir um processo de Registro para obter uma conta do Astra Control Service.

Ao usar o Astra Control Service, você gerenciará seus aplicativos de uma conta. Uma conta inclui usuários

que podem visualizar e gerenciar os aplicativos dentro da conta, bem como seus detalhes de cobrança.

Passos

1. ["Vá para a página Astra Control no BlueXP "](#).
2. Selecione **Inscriver-se para o plano gratuito**.
3. Forneça as informações necessárias no formulário.

Algumas coisas importantes a serem observadas ao preencher o formulário:

- O nome e o endereço da sua empresa devem ser precisos porque os verificamos para atender aos requisitos da conformidade de Comércio Global.
- O **Nome da conta Astra** é o nome da conta do Serviço Astra Control da sua empresa. Você verá esse nome na interface de usuário do Astra Control Service. Observe que você pode criar contas adicionais (até 5), se necessário.
- No campo **Endereço de e-mail comercial**, se você tiver uma conta do NetApp BlueXP , digite o e-mail usado para essa conta aqui. Se você ainda não tiver uma conta do NetApp BlueXP , use o endereço de e-mail digitado aqui quando você se inscrever no BlueXP .

4. Selecione **criar conta**.

Inscriva-se no BlueXP

O Astra Control Service está integrado ao serviço de autenticação da NetApp BlueXP . Você pode fazer login no NetApp BlueXP usando suas credenciais do site de suporte da BlueXP ou da NetApp. Se você ainda não tiver uma conta do site de suporte da NetApp BlueXP ou da NetApp, inscreva-se no BlueXP para acessar o Serviço Astra Control e os outros serviços de nuvem da NetApp. Se você já tiver uma conta do site de suporte da BlueXP ou da NetApp e tiver concluído o Registro, poderá acessar ["Astra Control Service"](#) diretamente usando suas credenciais do site de suporte da BlueXP ou da NetApp.



Você também pode usar o logon único para fazer login no BlueXP usando credenciais do diretório corporativo (identidade federada). Para saber mais, vá para o ["Centro de Ajuda"](#) e selecione **Opções de início de sessão na Cloud Central**.

Passos

1. Vá para ["NetApp BlueXP "](#).
2. No canto superior direito, selecione **Introdução**.
3. Selecione **Inscriver-se**.
4. Preencha o formulário.

Certifique-se de que o número de telefone e o endereço de e-mail inseridos aqui são os mesmos que você usou no formulário de Registro anterior do Astra Control.

5. Selecione **Inscriver-se**.



O endereço de e-mail inserido nesses formulários é para sua ID de usuário do NetApp BlueXP . Use essa ID de usuário do BlueXP ao se inscrever em uma nova conta do Astra Control ou quando um administrador do Astra Control convidar você para uma conta existente.

6. Aguarde um e-mail do NetApp BlueXP . O e-mail vem do endereço saas.support@netapp.com, e pode

levar alguns minutos para chegar. Certifique-se de verificar sua pasta de spam.

7. Quando o e-mail chegar, selecione o link no e-mail para verificar seu endereço de e-mail.

Resultado

Agora você tem um login de usuário ativo do BlueXP .

Agora que você está registrado, pode acessar o Astra Control diretamente usando suas credenciais BlueXP do <https://astra.netapp.io>.

Adicionar um cluster ao Astra Control Service

Depois de configurar o ambiente, você estará pronto para criar um cluster Kubernetes e adicioná-lo ao Astra Control Service. Isso permite que você use o Astra Control Service para proteger suas aplicações no cluster.

Dependendo do tipo de cluster que você precisa adicionar ao Astra Control Service, você precisa usar etapas diferentes para adicionar o cluster.

- "[Adicionar um cluster gerenciado por fornecedor público ao Astra Control Service](#)": Siga estas etapas para adicionar um cluster que tenha um endereço IP público e seja gerenciado por um provedor de nuvem. Você precisará da conta principal do Serviço, da conta de serviço ou da conta de usuário do provedor de nuvem.
- "[Adicionar um cluster gerenciado por fornecedor privado ao Astra Control Service](#)": Siga estas etapas para adicionar um cluster que tenha um endereço IP privado e seja gerenciado por um provedor de nuvem. Você precisará da conta principal do Serviço, da conta de serviço ou da conta de usuário do provedor de nuvem.
- "[Adicionar um cluster público autogerenciado ao Astra Control Service](#)": Siga estas etapas para adicionar um cluster que tenha um endereço IP público e seja gerenciado pela sua organização. Você precisará criar um arquivo kubeconfig para o cluster que deseja adicionar.
- "[Adicionar um cluster privado e autogerenciado ao Astra Control Service](#)": Siga estas etapas para adicionar um cluster que tenha um endereço IP privado e seja gerenciado pela sua organização. Você precisará criar um arquivo kubeconfig para o cluster que deseja adicionar.

Instalar o Astra Connector para gerenciar clusters

O Astra Connector é um software que reside nos clusters gerenciados e facilita a comunicação entre o cluster gerenciado e o Astra Control. Para clusters gerenciados usando o Astra Control Service, há duas versões disponíveis do Astra Connector:

- **Versão anterior do Astra Connector:** "[Instale a versão anterior do conetor Astra](#)" No cluster se você planeja gerenciar o cluster com fluxos de trabalho não nativos do Kubernetes.
- [Visualização técnica] **Comunicado Kubernetes Astra Connector:** "[Instalar o Astra Connector para clusters gerenciados com workflows declarativos do Kubernetes](#)" No cluster se você planeja gerenciar o cluster usando fluxos de trabalho declarativos do Kubernetes. Depois de instalar o Astra Connector no cluster, o cluster é adicionado automaticamente ao Astra Control.



O conetor declarativo Kubernetes Astra está disponível apenas como parte do Programa de Adopter antecipado (EAP) Astra Control. Contacte o seu representante de vendas da NetApp para obter informações sobre como aderir ao EAP.

Instale a versão anterior do conector Astra

O Astra Control Service usa a versão anterior do Astra Connector para permitir a comunicação entre o Astra Control Service e clusters privados gerenciados com workflows não nativos em Kubernetes. É necessário instalar o Astra Connector em clusters privados que você deseja gerenciar com workflows que não sejam nativos em Kubernetes.

A versão anterior do Astra Connector é compatível com os seguintes tipos de clusters privados gerenciados com workflows não nativos em Kubernetes:

- Amazon Elastic Kubernetes Service (EKS)
- Serviço Kubernetes do Azure (AKS)
- Google Kubernetes Engine (GKE)
- Red Hat OpenShift Service na AWS (ROSA)
- ROSA com AWS PrivateLink
- Red Hat OpenShift Container Platform on-premise

Sobre esta tarefa

- Ao executar essas etapas, execute esses comandos no cluster privado que você deseja gerenciar com o Astra Control Service.
- Se você estiver usando um host de bastião, emita esses comandos a partir da linha de comando do host de bastião.

Antes de começar

- Você precisa ter acesso ao cluster privado que deseja gerenciar com o Astra Control Service.
- Você precisa de permissões de administrador do Kubernetes para instalar o operador Astra Connector no cluster.

Passos

1. Instale o operador Astra Connector anterior no cluster privado que você deseja gerenciar com workflows que não sejam nativos em Kubernetes. Quando você executa esse comando, o namespace `astra-connector-operator` é criado e a configuração é aplicada ao namespace:

```
kubectl apply -f https://github.com/NetApp/astra-connector-operator/releases/download/23.07.0-202310251519/astraconnector_operator.yaml
```

2. Verifique se o operador está instalado e pronto:

```
kubectl get all -n astra-connector-operator
```

3. Obtenha um token de API do Astra Control. Consulte o "[Documentação do Astra Automation](#)" para obter instruções.
4. Crie o namespace `astra-Connector`:


```
kubectl create ns astra-connector
```

5. Crie o arquivo CR do Astra Connector e nomeie-o `astra-connector-cr.yaml`. Atualize os valores entre parêntesis> para corresponder ao seu ambiente Astra Control e à configuração de cluster:

- **<ASTRA_CONTROL_SERVICE_URL>**: O URL da IU da Web do serviço Astra Control. Por exemplo:

```
https://astra.netapp.io
```

- **<ASTRA_CONTROL_SERVICE_API_TOKEN>**: O token da API Astra Control que você obteve na etapa anterior.
- **<PRIVATE_AKS_CLUSTER_NAME>**: (Somente clusters AKS) - o nome do cluster do cluster privado do Azure Kubernetes Service. Descomente e preencha esta linha apenas se estiver a adicionar um cluster AKS privado.
- **<ASTRA_CONTROL_ACCOUNT_ID>**: Obtido a partir da IU da Web do Astra Control. Selecione o ícone de figura no canto superior direito da página e selecione **Acesso à API**.

```
apiVersion: netapp.astraconnector.com/v1
kind: AstraConnector
metadata:
  name: astra-connector
  namespace: astra-connector
spec:
  natssync-client:
    cloud-bridge-url: <ASTRA_CONTROL_SERVICE_URL>
  imageRegistry:
    name: theotw
    secret: ""
  astra:
    token: <ASTRA_CONTROL_SERVICE_API_TOKEN>
    #clusterName: <PRIVATE_AKS_CLUSTER_NAME>
    accountId: <ASTRA_CONTROL_ACCOUNT_ID>
    acceptEULA: yes
```

6. Depois de preencher o `astra-connector-cr.yaml` arquivo com os valores corretos, aplique o CR:

```
kubectl apply -f astra-connector-cr.yaml
```

7. Verifique se o conetor Astra está totalmente implantado:

```
kubectl get all -n astra-connector
```

8. Verifique se o cluster está registrado no Astra Control:

```
kubectl get astrconnector -n astra-connector
```

Você deve ver saída semelhante ao seguinte:

```
NAME                REGISTERED  ASTRACONNECTORID
STATUS
astra-connector    true        be475ae5-1511-4eaa-9b9e-712f09b0d065
Registered with Astra
```



Anote o ASTRACONNECTORID; você precisará dele quando adicionar o cluster ao Astra Control.

O que se segue?

Agora que você instalou o Astra Connector, está pronto para adicionar seu cluster privado ao Astra Control Service.

- ["Adicionar um cluster gerenciado por fornecedor privado ao Astra Control Service"](#): Siga estas etapas para adicionar um cluster que tenha um endereço IP privado e seja gerenciado por um provedor de nuvem. Você precisará da conta principal do Serviço, da conta de serviço ou da conta de usuário do provedor de nuvem.
- ["Adicionar um cluster privado e autogerenciado ao Astra Control Service"](#): Siga estas etapas para adicionar um cluster que tenha um endereço IP privado e seja gerenciado pela sua organização. Você precisará criar um arquivo kubeconfig para o cluster que deseja adicionar.

Para mais informações

- ["Adicione um cluster"](#)

(Visualização técnica) instale o conetor declarativo Kubernetes Astra

Os clusters gerenciados usando workflows declarativos do Kubernetes usam o Astra Connector para permitir a comunicação entre o cluster gerenciado e o Astra Control. É necessário instalar o Astra Connector em todos os clusters que você gerenciará com workflows declarativos do Kubernetes.

Você instala o conetor declarativo Kubernetes Astra usando comandos Kubernetes e arquivos de recursos personalizados (CR).

Sobre esta tarefa

- Ao executar essas etapas, execute esses comandos no cluster que deseja gerenciar com o Astra Control.
- Se você estiver usando um host de bastião, emita esses comandos a partir da linha de comando do host de bastião.

Antes de começar

- Você precisa ter acesso ao cluster que deseja gerenciar com o Astra Control.
- Você precisa de permissões de administrador do Kubernetes para instalar o operador Astra Connector no cluster.



Se o cluster estiver configurado com imposição de admissão de segurança de pod, que é o padrão para clusters Kubernetes 1,25 e posteriores, será necessário habilitar restrições PSA nos namespaces apropriados. ["Prepare seu ambiente para gerenciamento de clusters com o Astra Control"](#) Consulte para obter instruções.

Passos

1. Instale o operador Astra Connector no cluster que você deseja gerenciar com workflows declarativos do Kubernetes. Quando você executa esse comando, o namespace `astra-connector-operator` é criado e a configuração é aplicada ao namespace:

```
kubectl apply -f https://github.com/NetApp/astra-connector-operator/releases/download/24.02.0-202403151353/astraconnector_operator.yaml
```

2. Verifique se o operador está instalado e pronto:

```
kubectl get all -n astra-connector-operator
```

3. Obtenha um token de API do Astra Control. Consulte o ["Documentação do Astra Automation"](#) para obter instruções.
4. Crie um segredo usando o token. Substitua o `<API_TOKEN>` pelo token recebido do Astra Control:

```
kubectl create secret generic astra-token \
--from-literal=apiToken=<API_TOKEN> \
-n astra-connector
```

5. Crie um segredo do Docker para usar para puxar a imagem do conector Astra. Substitua os valores entre parêntesis por informações do seu ambiente:



Você pode encontrar o `<ASTRA_CONTROL_ACCOUNT_ID>` na IU da Web do Astra Control. Na IU da Web, selecione o ícone de figura no canto superior direito da página e selecione **Acesso à API**.

```
kubectl create secret docker-registry regcred \
--docker-username=<ASTRA_CONTROL_ACCOUNT_ID> \
--docker-password=<API_TOKEN> \
-n astra-connector \
--docker-server=cr.astra.netapp.io
```

6. Crie o arquivo CR do Astra Connector e nomeie-o `astra-connector-cr.yaml`. Atualize os valores entre parêntesis> para corresponder ao seu ambiente Astra Control e à configuração de cluster:
- `<ASTRA_CONTROL_ACCOUNT_ID>`: Obtido na IU da Web do Astra Control durante a etapa anterior.
 - `<CLUSTER_NAME>`: O nome que esse cluster deve ser atribuído no Astra Control.
 - `<ASTRA_CONTROL_URL>`: O URL da IU da Web do Astra Control. Por exemplo:

```
https://astra.control.url
```

```
apiVersion: astra.netapp.io/v1
kind: AstraConnector
metadata:
  name: astra-connector
  namespace: astra-connector
spec:
  astra:
    accountId: <ASTRA_CONTROL_ACCOUNT_ID>
    clusterName: <CLUSTER_NAME>
    #Only set `skipTLSValidation` to `true` when using the default
    self-signed
    #certificate in a proof-of-concept environment.
    skipTLSValidation: false #Should be set to false in production
    environments
    tokenRef: astra-token
  natsSyncClient:
    cloudBridgeURL: <ASTRA_CONTROL_HOST_URL>
  imageRegistry:
    name: cr.astra.netapp.io
    secret: regcred
```

7. Depois de preencher o `astra-connector-cr.yaml` ficheiro com os valores corretos, aplique o CR:

```
kubectl apply -n astra-connector -f astra-connector-cr.yaml
```

8. Verifique se o conector Astra está totalmente implantado:

```
kubectl get all -n astra-connector
```

9. Verifique se o cluster está registrado no Astra Control:

```
kubectl get astraconnectors.astra.netapp.io -A
```

Você deve ver saída semelhante ao seguinte:

```
NAMESPACE          NAME          REGISTERED  ASTRACONNECTORID
STATUS
astra-connector    astra-connector  true        00ac8-2cef-41ac-8777-
ed0583e    Registered with Astra
```

10. Verifique se o cluster aparece na lista de clusters gerenciados na página **clusters** da IU da Web Astra Control.

Adicionar um cluster gerenciado por provedor

Adicionar um cluster gerenciado por fornecedor público ao Astra Control Service

Depois de configurar seu ambiente de nuvem, você estará pronto para criar um cluster Kubernetes e adicioná-lo ao Astra Control Service.

- [Criar um cluster do Kubernetes](#)
- [Adicione o cluster ao Astra Control Service](#)
- [Altere a classe de armazenamento padrão](#)

Criar um cluster do Kubernetes

Se você ainda não tiver um cluster, poderá criar um que atenda "[Requisitos do Astra Control Service para Amazon Elastic Kubernetes Service \(EKS\)](#)" ao . Se você ainda não tiver um cluster, poderá criar um que atenda "[Requisitos de serviço do Astra Control para Google Kubernetes Engine \(GKE\)](#)" ao . Se você ainda não tiver um cluster, poderá criar um que atenda "[Requisitos de Serviço de Controle do Astra para Azure Kubernetes Service \(AKS\) com Azure NetApp Files](#)" ou "[Requisitos do Serviço de Controle Astra para Azure Kubernetes Service \(AKS\) com discos gerenciados do Azure](#)".



O Astra Control Service oferece suporte a clusters AKS que usam o Azure Active Directory (Azure AD) para autenticação e gerenciamento de identidade. Ao criar o cluster, siga as instruções na "[documentação oficial](#)" para configurar o cluster para utilizar o Azure AD. Você precisará garantir que seus clusters atendam aos requisitos de integração do Azure AD gerenciada pelo AKS.

Adicione o cluster ao Astra Control Service

Depois de fazer login no Astra Control Service, sua primeira etapa é começar a gerenciar os clusters. Antes de adicionar um cluster ao Astra Control Service, você precisará executar tarefas específicas e garantir que o cluster atenda a certos requisitos.

Ao gerenciar os clusters do Azure Kubernetes Service e do Google Kubernetes Engine, observe que você tem duas opções para instalação e gerenciamento de ciclo de vida do Astra Control Provisioner:

- Você pode usar o Astra Control Service para gerenciar automaticamente o ciclo de vida do Astra Control Provisioner. Para fazer isso, verifique se o Astra Trident não está instalado e se o Astra Control Provisioner não está ativado no cluster que você deseja gerenciar com o Astra Control Service. Nesse caso, o Astra Control Service habilita automaticamente o Astra Control Provisioner quando você começar a gerenciar o cluster, e as atualizações do Astra Control Provisioner são tratadas automaticamente.

- Você mesmo pode gerenciar o ciclo de vida do Astra Control Provisioner. Para fazer isso, ative o Astra Control Provisioner no cluster antes de gerenciar o cluster com o Astra Control Service. Nesse caso, o Astra Control Service detecta que o Astra Control Provisioner já está ativado e não o reinstala nem gerencia atualizações do Astra Control Provisioner. ["Habilite o Astra Control Provisioner"](#) Consulte para obter os passos Ativar Astra Control Provisioner.

Ao gerenciar clusters do Amazon Web Services com Astra Control Service, se você precisar de back-ends de storage que só podem ser usados com o Astra Control Provisioner, será necessário habilitar o Astra Control Provisioner manualmente no cluster antes de gerenciá-lo com o Astra Control Service. ["Habilite o Astra Control Provisioner"](#) Consulte para obter informações sobre os passos para ativar o Astra Control Provisioner.

Antes de começar

Amazon Web Services

- Você deve ter o arquivo JSON contendo as credenciais do usuário do IAM que criou o cluster. ["Saiba como criar um usuário do IAM"](#).
- O parceiro é necessário para o Amazon FSX for NetApp ONTAP. Se você planeja usar o Amazon FSX for NetApp ONTAP como um back-end de armazenamento para seu cluster EKS, consulte as informações do Supervisor de Controle Astra no ["Requisitos do cluster do EKS"](#).
- (Opcional) se você precisar fornecer `kubectl` acesso a comandos para um cluster a outros usuários do IAM que não sejam o criador do cluster, consulte as instruções no ["Como posso fornecer acesso a outros usuários e funções do IAM após a criação do cluster no Amazon EKS?"](#).
- Se você planeja usar o NetApp Cloud Volumes ONTAP como um back-end de storage, precisa configurar o Cloud Volumes ONTAP para trabalhar com o Amazon Web Services. Consulte o Cloud Volumes ONTAP ["documentação de configuração"](#) .

Microsoft Azure

- Você deve ter o arquivo JSON que contém a saída da CLI do Azure quando você criou o principal de serviço. ["Saiba como configurar um diretor de serviço"](#).

Você também precisará do ID de assinatura do Azure, se não o tiver adicionado ao arquivo JSON.

- Se você planeja usar o NetApp Cloud Volumes ONTAP como um back-end de storage, precisa configurar o Cloud Volumes ONTAP para trabalhar com o Microsoft Azure. Consulte o Cloud Volumes ONTAP ["documentação de configuração"](#) .

Google Cloud

- Você deve ter o arquivo de chave da conta de serviço para uma conta de serviço que tenha as permissões necessárias. ["Saiba como configurar uma conta de serviço"](#).
- Se você planeja usar o NetApp Cloud Volumes ONTAP como um back-end de storage, precisa configurar o Cloud Volumes ONTAP para trabalhar com o Google Cloud. Consulte o Cloud Volumes ONTAP ["documentação de configuração"](#) .

Passos

1. (Opcional) se você estiver adicionando um cluster do Amazon EKS ou quiser gerenciar a instalação e atualizações do Astra Control Provisioner você mesmo, ative o Astra Control Provisioner no cluster. ["Habilite o Astra Control Provisioner"](#) Consulte para obter os passos de capacitação.
2. Abra a IU da Web do Astra Control Service em um navegador.
3. No Painel, selecione **Gerenciar cluster do Kubernetes**.

Siga as instruções para adicionar o cluster.

4. **Provedor:** Selecione seu provedor de nuvem e forneça as credenciais necessárias para criar uma nova instância de nuvem ou selecione uma instância de nuvem existente para usar.
5. **Amazon Web Services:** Forneça detalhes sobre sua conta de usuário do Amazon Web Services IAM ao carregar um arquivo JSON ou colando o conteúdo desse arquivo JSON da área de transferência.

O arquivo JSON deve conter as credenciais do usuário do IAM que criou o cluster.

6. **Microsoft Azure:** Forneça detalhes sobre o seu principal de serviço do Azure carregando um arquivo JSON ou colando o conteúdo desse arquivo JSON da sua área de transferência.

O arquivo JSON deve conter a saída da CLI do Azure quando você criou o principal do serviço. Ele também pode incluir seu ID de assinatura para que ele seja adicionado automaticamente ao Astra. Caso contrário, você precisa inserir manualmente o ID após fornecer o JSON.

7. **Google Cloud Platform:** Forneça o arquivo chave da conta de serviço, seja carregando o arquivo ou colando o conteúdo da área de transferência.

O Astra Control Service usa a conta de serviço para descobrir clusters executados no Google Kubernetes Engine.

8. **Other:** Esta guia é para uso somente com clusters autogerenciados.

- a. **Nome da instância da nuvem:** Forneça um nome para a nova instância da nuvem que será criada quando você adicionar esse cluster. Saiba mais "[instâncias da nuvem](#)" sobre o .

- b. Selecione **seguinte**.

O Astra Control Service exibe uma lista de clusters que você pode escolher.

- c. **Cluster:** Selecione um cluster na lista para adicionar ao Astra Control Service.



Quando estiver selecionando a partir da lista de clusters, preste atenção à coluna **eligibility**. Se um cluster for "inelegível" ou "parcialmente elegível", passe o Mouse sobre o status para determinar se há um problema com o cluster. Por exemplo, pode identificar que o cluster não tem um nó de trabalho.

- d. Selecione **seguinte**.

- e. (Opcional) **Storage:** Opcionalmente, selecione a classe de armazenamento que você deseja que os aplicativos do Kubernetes implantados nesse cluster usem por padrão.

9. Para selecionar uma nova classe de armazenamento padrão para o cluster, ative a caixa de seleção **Assign a new default storage class** (atribuir uma nova classe de armazenamento padrão).

10. Selecione uma nova classe de armazenamento padrão na lista.

Cada serviço de storage de fornecedor de nuvem exibe as seguintes informações de preço, performance e resiliência:



- Cloud Volumes Service para Google Cloud: Informações de preço, performance e resiliência
- Persistent Disk do Google: Nenhuma informação de preço, performance ou resiliência disponível
- Azure NetApp Files: Informações de performance e resiliência
- Discos gerenciados do Azure: Nenhuma informação de preço, desempenho ou resiliência disponível
- Amazon Elastic Block Store: Sem informações de preço, desempenho ou resiliência disponíveis
- Amazon FSX for NetApp ONTAP: Sem informações de preço, desempenho ou resiliência disponíveis
- NetApp Cloud Volumes ONTAP: Sem informações de preço, performance ou resiliência disponíveis

Cada classe de storage pode utilizar um dos seguintes serviços:

- ["Cloud Volumes Service para Google Cloud"](#)
- ["Persistent Disk do Google"](#)
 - ["Azure NetApp Files"](#)
 - ["Discos gerenciados do Azure"](#)
 - ["Amazon Elastic Block Store"](#)
 - ["Amazon FSX para NetApp ONTAP"](#)
 - ["NetApp Cloud Volumes ONTAP"](#)

Saiba mais ["Classes de armazenamento para clusters do Amazon Web Services"](#)sobre o . Saiba mais ["Classes de armazenamento para clusters AKS"](#)sobre o . Saiba mais ["Classes de armazenamento para clusters GKE"](#)sobre o .

- a. Selecione **seguinte**.
- b. **Review & Approve**: Reveja os detalhes de configuração.
- c. Selecione **Adicionar** para adicionar o cluster ao Astra Control Service.

Resultado

Se este for o primeiro cluster adicionado a esse fornecedor de nuvem, o Astra Control Service criará um armazenamento de objetos para o fornecedor de nuvem para backups de aplicações executadas em clusters qualificados. (Quando você adiciona clusters subsequentes para esse fornecedor de nuvem, não são criados armazenamentos de objetos adicionais.) Se você especificou uma classe de storage padrão, o Astra Control Service define a classe de storage padrão especificada. Para clusters gerenciados na Amazon Web Services ou no Google Cloud Platform, o Astra Control Service também cria uma conta de administrador no cluster. Essas ações podem levar vários minutos.

Altere a classe de armazenamento padrão

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

Altere a classe de storage padrão usando o Astra Control

Você pode alterar a classe de storage padrão de um cluster a partir do Astra Control. Se o cluster usar um serviço de back-end de armazenamento instalado anteriormente, talvez você não consiga usar esse método para alterar a classe de armazenamento padrão (a ação **Definir como padrão** não é selecionável). Neste caso, você pode [Altere a classe de armazenamento padrão usando a linha de comando](#).

Passos

1. Na IU do Astra Control Service, 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**.

Altere a classe de armazenamento padrão usando a linha de comando

Você pode alterar a classe de storage padrão de um cluster usando comandos do Kubernetes. Esse método funciona independentemente da configuração do cluster.

Passos

1. Faça login no cluster do Kubernetes.
2. Liste as classes de armazenamento no cluster:

```
kubectl get storageclass
```

3. Remova a designação padrão da classe de armazenamento padrão. Substitua o <SC_NAME> pelo nome da classe de armazenamento:

```
kubectl patch storageclass <SC_NAME> -p '{"metadata": {"annotations":{"storageclass.kubernetes.io/is-default-class":"false"}}}'
```

4. Marque uma classe de armazenamento diferente como padrão. Substitua o <SC_NAME> pelo nome da classe de armazenamento:

```
kubectl patch storageclass <SC_NAME> -p '{"metadata": {"annotations":{"storageclass.kubernetes.io/is-default-class":"true"}}}'
```

5. Confirme a nova classe de armazenamento padrão:

```
kubectl get storageclass
```

Adicionar um cluster gerenciado por fornecedor privado ao Astra Control Service

Você pode usar o Astra Control Service para gerenciar clusters privados do Google Kubernetes Engine (GKE). Estas instruções presumem que você já criou um cluster privado AKS ou OpenShift e preparou um método seguro para acessá-lo remotamente; para obter mais informações sobre como criar e acessar clusters privados AKS ou OpenShift, consulte a seguinte documentação:

- ["Documentação do Azure para clusters AKS privados"](#)
- ["Documentação do Azure para clusters privados do OpenShift"](#)

Você pode usar o Astra Control Service para gerenciar clusters privados do Azure Kubernetes Service (AKS), bem como clusters privados do Red Hat OpenShift no AKS. Estas instruções presumem que você já criou um cluster privado AKS ou OpenShift e preparou um método seguro para acessá-lo remotamente; para obter mais informações sobre como criar e acessar clusters privados AKS ou OpenShift, consulte a seguinte documentação:

- ["Documentação do Azure para clusters AKS privados"](#)
- ["Documentação do Azure para clusters privados do OpenShift"](#)

Você pode usar o Astra Control Service para gerenciar clusters privados do Amazon Elastic Kubernetes Service (EKS). Essas instruções presumem que você já criou um cluster EKS privado e preparou um método seguro para acessá-lo remotamente; para obter mais informações sobre como criar e acessar clusters EKS privados, consulte o ["Documentação do Amazon EKS"](#).

Você precisa executar as seguintes tarefas para adicionar seu cluster privado ao Astra Control Service:

1. [Instale o conector Astra](#)
2. [Configurar o armazenamento persistente](#)
3. [Adicione o cluster gerenciado por fornecedor privado ao Astra Control Service](#)

Instale o conector Astra

Antes de adicionar um cluster privado, é necessário instalar o Astra Connector no cluster para que o Astra Control possa se comunicar com ele. ["Instalar a versão anterior do Astra Connector para clusters privados gerenciados com workflows não nativos em Kubernetes"](#) Consulte para obter instruções.

Configurar o armazenamento persistente

Configurar o armazenamento persistente para o cluster. Consulte a documentação [Introdução](#) para obter mais informações sobre como configurar o armazenamento persistente:

- ["Configure o Microsoft Azure com o Azure NetApp Files"](#)
- ["Configurar o Microsoft Azure com discos gerenciados do Azure"](#)
- ["Configurar o Amazon Web Services"](#)
- ["Configure o Google Cloud"](#)

Adicione o cluster gerenciado por fornecedor privado ao Astra Control Service

Agora você pode adicionar o cluster privado ao Astra Control Service.

Ao gerenciar os clusters do Azure Kubernetes Service e do Google Kubernetes Engine, observe que você tem duas opções para instalação e gerenciamento de ciclo de vida do Astra Control Provisioner:

- Você pode usar o Astra Control Service para gerenciar automaticamente o ciclo de vida do Astra Control Provisioner. Para fazer isso, verifique se o Astra Trident não está instalado e se o Astra Control Provisioner não está ativado no cluster que você deseja gerenciar com o Astra Control Service. Nesse caso, o Astra Control Service habilita automaticamente o Astra Control Provisioner quando você começar a gerenciar o cluster, e as atualizações do Astra Control Provisioner são tratadas automaticamente.
- Você mesmo pode gerenciar o ciclo de vida do Astra Control Provisioner. Para fazer isso, ative o Astra Control Provisioner no cluster antes de gerenciar o cluster com o Astra Control Service. Nesse caso, o Astra Control Service detecta que o Astra Control Provisioner já está ativado e não o reinstala nem gerencia atualizações do Astra Control Provisioner. "[Habilite o Astra Control Provisioner](#)" Consulte para obter os passos Ativar Astra Control Provisioner.

Ao gerenciar clusters do Amazon Web Services com Astra Control Service, se você precisar de back-ends de storage que só podem ser usados com o Astra Control Provisioner, será necessário habilitar o Astra Control Provisioner manualmente no cluster antes de gerenciá-lo com o Astra Control Service. "[Habilite o Astra Control Provisioner](#)" Consulte para obter informações sobre os passos para ativar o Astra Control Provisioner.

Antes de começar

Amazon Web Services

- Você deve ter o arquivo JSON contendo as credenciais do usuário do IAM que criou o cluster. ["Saiba como criar um usuário do IAM"](#).
- O parceiro é necessário para o Amazon FSX for NetApp ONTAP. Se você planeja usar o Amazon FSX for NetApp ONTAP como um back-end de armazenamento para seu cluster EKS, consulte as informações do Supervisor de Controle Astra no ["Requisitos do cluster do EKS"](#).
- (Opcional) se você precisar fornecer `kubectl` acesso a comandos para um cluster a outros usuários do IAM que não sejam o criador do cluster, consulte as instruções no ["Como posso fornecer acesso a outros usuários e funções do IAM após a criação do cluster no Amazon EKS?"](#).
- Se você planeja usar o NetApp Cloud Volumes ONTAP como um back-end de storage, precisa configurar o Cloud Volumes ONTAP para trabalhar com o Amazon Web Services. Consulte o Cloud Volumes ONTAP ["documentação de configuração"](#) .

Microsoft Azure

- Você deve ter o arquivo JSON que contém a saída da CLI do Azure quando você criou o principal de serviço. ["Saiba como configurar um diretor de serviço"](#).

Você também precisará do ID de assinatura do Azure, se não o tiver adicionado ao arquivo JSON.

- Se você planeja usar o NetApp Cloud Volumes ONTAP como um back-end de storage, precisa configurar o Cloud Volumes ONTAP para trabalhar com o Microsoft Azure. Consulte o Cloud Volumes ONTAP ["documentação de configuração"](#) .

Google Cloud

- Você deve ter o arquivo de chave da conta de serviço para uma conta de serviço que tenha as permissões necessárias. ["Saiba como configurar uma conta de serviço"](#).
- Se o cluster for privado, o deve permitir o endereço IP do ["redes autorizadas"](#) Astra Control Service:

52.188.218.166/32
- Se você planeja usar o NetApp Cloud Volumes ONTAP como um back-end de storage, precisa configurar o Cloud Volumes ONTAP para trabalhar com o Google Cloud. Consulte o Cloud Volumes ONTAP ["documentação de configuração"](#) .

Passos

1. (Opcional) se você estiver adicionando um cluster do Amazon EKS ou quiser gerenciar a instalação e atualizações do Astra Control Provisioner você mesmo, ative o Astra Control Provisioner no cluster. ["Habilite o Astra Control Provisioner"](#)Consulte para obter os passos de capacitação.
2. Abra a IU da Web do Astra Control Service em um navegador.
3. No Painel, selecione **Gerenciar cluster do Kubernetes**.

Siga as instruções para adicionar o cluster.
4. **Provedor:** Selecione seu provedor de nuvem e forneça as credenciais necessárias para criar uma nova instância de nuvem ou selecione uma instância de nuvem existente para usar.
5. **Amazon Web Services:** Forneça detalhes sobre sua conta de usuário do Amazon Web Services IAM ao carregar um arquivo JSON ou colando o conteúdo desse arquivo JSON da área de transferência.

O arquivo JSON deve conter as credenciais do usuário do IAM que criou o cluster.

6. **Microsoft Azure:** Forneça detalhes sobre o seu principal de serviço do Azure carregando um arquivo JSON ou colando o conteúdo desse arquivo JSON da sua área de transferência.

O arquivo JSON deve conter a saída da CLI do Azure quando você criou o principal do serviço. Ele também pode incluir seu ID de assinatura para que ele seja adicionado automaticamente ao Astra. Caso contrário, você precisa inserir manualmente o ID após fornecer o JSON.

7. **Google Cloud Platform:** Forneça o arquivo chave da conta de serviço, seja carregando o arquivo ou colando o conteúdo da área de transferência.

O Astra Control Service usa a conta de serviço para descobrir clusters executados no Google Kubernetes Engine.

8. **Other:** Esta guia é para uso somente com clusters autogerenciados.

- a. **Nome da instância da nuvem:** Forneça um nome para a nova instância da nuvem que será criada quando você adicionar esse cluster. Saiba mais "[instâncias da nuvem](#)" sobre o .

- b. Selecione **seguinte**.

O Astra Control Service exibe uma lista de clusters que você pode escolher.

- c. **Cluster:** Selecione um cluster na lista para adicionar ao Astra Control Service.



Quando estiver selecionando a partir da lista de clusters, preste atenção à coluna **eligibility**. Se um cluster for "inelegível" ou "parcialmente elegível", passe o Mouse sobre o status para determinar se há um problema com o cluster. Por exemplo, pode identificar que o cluster não tem um nó de trabalho.

9. Selecione **seguinte**.

10. (Opcional) **Storage:** Opcionalmente, selecione a classe de armazenamento que você deseja que os aplicativos do Kubernetes implantados nesse cluster usem por padrão.

- a. Para selecionar uma nova classe de armazenamento padrão para o cluster, ative a caixa de seleção **Assign a new default storage class** (atribuir uma nova classe de armazenamento padrão).

- b. Selecione uma nova classe de armazenamento padrão na lista.

Cada serviço de storage de fornecedor de nuvem exibe as seguintes informações de preço, performance e resiliência:



- Cloud Volumes Service para Google Cloud: Informações de preço, performance e resiliência
- Persistent Disk do Google: Nenhuma informação de preço, performance ou resiliência disponível
- Azure NetApp Files: Informações de performance e resiliência
- Discos gerenciados do Azure: Nenhuma informação de preço, desempenho ou resiliência disponível
- Amazon Elastic Block Store: Sem informações de preço, desempenho ou resiliência disponíveis
- Amazon FSX for NetApp ONTAP: Sem informações de preço, desempenho ou resiliência disponíveis
- NetApp Cloud Volumes ONTAP: Sem informações de preço, performance ou resiliência disponíveis

Cada classe de storage pode utilizar um dos seguintes serviços:

- ["Cloud Volumes Service para Google Cloud"](#)
- ["Persistent Disk do Google"](#)
- ["Azure NetApp Files"](#)
- ["Discos gerenciados do Azure"](#)
- ["Amazon Elastic Block Store"](#)
- ["Amazon FSX para NetApp ONTAP"](#)
- ["NetApp Cloud Volumes ONTAP"](#)

Saiba mais ["Classes de armazenamento para clusters do Amazon Web Services"](#)sobre o . Saiba mais ["Classes de armazenamento para clusters AKS"](#)sobre o . Saiba mais ["Classes de armazenamento para clusters GKE"](#)sobre o .

c. Selecione **seguinte**.

d. **Review & Approve**: Reveja os detalhes de configuração.

e. Selecione **Adicionar** para adicionar o cluster ao Astra Control Service.

Resultado

Se este for o primeiro cluster adicionado a esse fornecedor de nuvem, o Astra Control Service criará um armazenamento de objetos para o fornecedor de nuvem para backups de aplicações executadas em clusters qualificados. (Quando você adiciona clusters subsequentes para esse fornecedor de nuvem, não são criados armazenamentos de objetos adicionais.) Se você especificou uma classe de storage padrão, o Astra Control Service define a classe de storage padrão especificada. Para clusters gerenciados na Amazon Web Services ou no Google Cloud Platform, o Astra Control Service também cria uma conta de administrador no cluster. Essas ações podem levar vários minutos.

Altere a classe de armazenamento padrão

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

Altere a classe de storage padrão usando o Astra Control

Você pode alterar a classe de storage padrão de um cluster a partir do Astra Control. Se o cluster usar um serviço de back-end de armazenamento instalado anteriormente, talvez você não consiga usar esse método para alterar a classe de armazenamento padrão (a ação **Definir como padrão** não é selecionável). Neste caso, você pode [Altere a classe de armazenamento padrão usando a linha de comando](#).

Passos

1. Na IU do Astra Control Service, 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**.

Altere a classe de armazenamento padrão usando a linha de comando

Você pode alterar a classe de storage padrão de um cluster usando comandos do Kubernetes. Esse método funciona independentemente da configuração do cluster.

Passos

1. Faça login no cluster do Kubernetes.
2. Liste as classes de armazenamento no cluster:

```
kubectl get storageclass
```

3. Remova a designação padrão da classe de armazenamento padrão. Substitua o <SC_NAME> pelo nome da classe de armazenamento:

```
kubectl patch storageclass <SC_NAME> -p '{"metadata": {"annotations":{"storageclass.kubernetes.io/is-default-class":"false"}}}'
```

4. Marque uma classe de armazenamento diferente como padrão. Substitua o <SC_NAME> pelo nome da classe de armazenamento:

```
kubectl patch storageclass <SC_NAME> -p '{"metadata": {"annotations":{"storageclass.kubernetes.io/is-default-class":"true"}}}'
```

5. Confirme a nova classe de armazenamento padrão:

```
kubectl get storageclass
```

Adicione um cluster autogerenciado

Adicionar um cluster público autogerenciado ao Astra Control Service

Depois de configurar o ambiente, você estará pronto para criar um cluster Kubernetes e adicioná-lo ao Astra Control Service.

Um cluster autogerenciado é um cluster que você provisiona e gerencia diretamente. O Astra Control Service é compatível com clusters autogerenciados que são executados em um ambiente de nuvem pública. Você pode adicionar um cluster autogerenciado ao Astra Control Service carregando um `kubeconfig.yaml` arquivo. Você precisará garantir que o cluster atenda aos requisitos descritos aqui.

Distribuições compatíveis do Kubernetes

Você pode usar o Astra Control Service para gerenciar os seguintes tipos de clusters públicos autogerenciados:

Distribuição do Kubernetes	Versões suportadas
Kubernetes (upstream)	1,27 a 1,29
Rancher Kubernetes Engine (RKE)	RKE 1: Versões 1.24.17, 1.25.13, 1.26.8 com Rancher Manager 2.7.9 RKE 2: Versões 1.23.16 e 1.24.13 com Rancher Manager 2.6.13 RKE 2: Versões 1.24.17, 1.25.14, 1.26.9 com Rancher Manager 2.7.9
Red Hat OpenShift Container Platform	4,12 a 4,14

Essas instruções presumem que você já criou um cluster autogerenciado.

- [Adicione o cluster ao Astra Control Service](#)
- [Altere a classe de armazenamento padrão](#)

Adicione o cluster ao Astra Control Service

Depois de fazer login no Astra Control Service, sua primeira etapa é começar a gerenciar os clusters. Antes de adicionar um cluster ao Astra Control Service, você precisará executar tarefas específicas e garantir que o cluster atenda a certos requisitos.

Antes de começar

Um cluster autogerenciado é um cluster que você provisiona e gerencia diretamente. O Astra Control Service é compatível com clusters autogerenciados que são executados em um ambiente de nuvem pública. Seus clusters autogerenciados podem usar o Astra Control Provisioner para fazer a interface com os serviços de storage da NetApp ou usar drivers da Container Storage Interface (CSI) para fazer a interface com o Amazon Elastic Block Store (EBS), discos gerenciados do Azure e disco persistente do Google.

O Astra Control Service é compatível com clusters autogerenciados que usam as seguintes distribuições do Kubernetes:

- Red Hat OpenShift Container Platform
- Rancher Kubernetes Engine
- Kubernetes upstream

Seu cluster autogerenciado precisa atender aos seguintes requisitos:

- O cluster deve ser acessível através da Internet.
- Se você estiver usando ou planeja usar o armazenamento habilitado com drivers CSI, os drivers CSI apropriados devem ser instalados no cluster. Para obter mais informações sobre como usar drivers CSI para integrar armazenamento, consulte a documentação do seu serviço de armazenamento.
- Você tem acesso ao arquivo kubeconfig cluster que inclui apenas um elemento de contexto. Siga ["estas instruções"](#) para gerar um arquivo kubeconfig.
- Se você estiver adicionando o cluster usando um arquivo kubeconfig que faça referência a uma Autoridade de certificação privada (CA), adicione a seguinte linha à `cluster` seção do arquivo kubeconfig. Isso permite que o Astra Control adicione o cluster:

```
insecure-skip-tls-verify: true
```

- **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.
- **Requisitos da previsão do Astra Control:** Você deve ter um programa de controle Astra Control configurado corretamente, incluindo seus componentes do Astra Trident, para gerenciar clusters.
 - * Rever os requisitos de ambiente do Astra Trident*: Antes de instalar ou atualizar o Astra Control Provisioner, revise o ["interfaces suportadas, backends e configurações de host"](#).
 - **Ativar a funcionalidade do programa Astra Control:** É altamente recomendável instalar o Astra Trident 23,10 ou posterior e ativar ["Funcionalidade de storage avançada do Astra Control Provisioner"](#). Nos próximos lançamentos, o Astra Control não será compatível com o Astra Trident se o programa Astra Control também não estiver habilitado.
 - **Configurar um back-end de armazenamento:** Pelo menos um back-end de armazenamento deve estar ["Configurado no Astra Trident"](#) no cluster.
 - **Configurar uma classe de armazenamento:** Pelo menos uma classe de armazenamento deve estar ["Configurado no Astra Trident"](#) no cluster. Se uma classe de armazenamento padrão estiver configurada, certifique-se de que é a classe de armazenamento **only** que tem a anotação padrão.

- **Configure um controlador de snapshot de volume e instale uma classe de snapshot de volume:** "Instale um controlador instantâneo de volume" Para que os snapshots possam ser criados no Astra Control. "Criar" Pelo menos um `VolumeSnapshotClass` usando Astra Trident.

Passos

1. No Painel, selecione **Gerenciar cluster do Kubernetes**.

Siga as instruções para adicionar o cluster.

2. **Provider:** Selecione a guia **Other** para adicionar detalhes sobre seu cluster autogerenciado.

- a. * Outro*: Forneça detalhes sobre seu cluster autogerenciado carregando um `kubeconfig.yaml` arquivo ou colando o conteúdo do `kubeconfig.yaml` arquivo da área de transferência.



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.

3. **Nome da credencial:** Forneça um nome para a credencial de cluster autogerenciada que você está enviando para o Astra Control. Por padrão, o nome da credencial é preenchido automaticamente como o nome do cluster.
4. **Identificador de rota privada:** Este campo é para uso somente com clusters privados.
5. Selecione **seguinte**.
6. (Opcional) **Storage:** Opcionalmente, selecione a classe de armazenamento que você deseja que os aplicativos do Kubernetes implantados nesse cluster usem por padrão.
 - a. Para selecionar uma nova classe de armazenamento padrão para o cluster, ative a caixa de seleção **Assign a new default storage class** (atribuir uma nova classe de armazenamento padrão).
 - b. Selecione uma nova classe de armazenamento padrão na lista.



Cada serviço de storage de fornecedor de nuvem exibe as seguintes informações de preço, performance e resiliência:

- Cloud Volumes Service para Google Cloud: Informações de preço, performance e resiliência
- Persistent Disk do Google: Nenhuma informação de preço, performance ou resiliência disponível
- Azure NetApp Files: Informações de performance e resiliência
- Discos gerenciados do Azure: Nenhuma informação de preço, desempenho ou resiliência disponível
- Amazon Elastic Block Store: Sem informações de preço, desempenho ou resiliência disponíveis
- Amazon FSX for NetApp ONTAP: Sem informações de preço, desempenho ou resiliência disponíveis
- NetApp Cloud Volumes ONTAP: Sem informações de preço, performance ou resiliência disponíveis

Cada classe de storage pode utilizar um dos seguintes serviços:

- ["Cloud Volumes Service para Google Cloud"](#)
- ["Persistent Disk do Google"](#)
 - ["Azure NetApp Files"](#)
 - ["Discos gerenciados do Azure"](#)
 - ["Amazon Elastic Block Store"](#)
 - ["Amazon FSX para NetApp ONTAP"](#)
 - ["NetApp Cloud Volumes ONTAP"](#)

Saiba mais ["Classes de armazenamento para clusters do Amazon Web Services"](#) sobre o .
 Saiba mais ["Classes de armazenamento para clusters AKS"](#) sobre o . Saiba mais ["Classes de armazenamento para clusters GKE"](#) sobre o .

- c. Selecione **seguinte**.
- d. **Review & Approve**: Reveja os detalhes de configuração.
- e. Selecione **Adicionar** para adicionar o cluster ao Astra Control Service.

Altere a classe de armazenamento padrão

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

Altere a classe de storage padrão usando o Astra Control

Você pode alterar a classe de storage padrão de um cluster a partir do Astra Control. Se o cluster usar um serviço de back-end de armazenamento instalado anteriormente, talvez você não consiga usar esse método para alterar a classe de armazenamento padrão (a ação **Definir como padrão** não é selecionável). Neste caso, você pode [Altere a classe de armazenamento padrão usando a linha de comando](#).

Passos

1. Na IU do Astra Control Service, 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**.

Altere a classe de armazenamento padrão usando a linha de comando

Você pode alterar a classe de storage padrão de um cluster usando comandos do Kubernetes. Esse método funciona independentemente da configuração do cluster.

Passos

1. Faça login no cluster do Kubernetes.
2. Liste as classes de armazenamento no cluster:

```
kubectl get storageclass
```

3. Remova a designação padrão da classe de armazenamento padrão. Substitua o <SC_NAME> pelo nome da classe de armazenamento:

```
kubectl patch storageclass <SC_NAME> -p '{"metadata": {"annotations":{"storageclass.kubernetes.io/is-default-class":"false"}}}'
```

4. Marque uma classe de armazenamento diferente como padrão. Substitua o <SC_NAME> pelo nome da classe de armazenamento:

```
kubectl patch storageclass <SC_NAME> -p '{"metadata": {"annotations":{"storageclass.kubernetes.io/is-default-class":"true"}}}'
```

5. Confirme a nova classe de armazenamento padrão:

```
kubectl get storageclass
```

Adicionar um cluster privado e autogerenciado ao Astra Control Service

Depois de configurar o ambiente, você estará pronto para criar um cluster Kubernetes e adicioná-lo ao Astra Control Service.

Um cluster autogerenciado é um cluster que você provisiona e gerencia diretamente. O Astra Control Service é compatível com clusters autogerenciados que são executados em um ambiente de nuvem pública. Você pode adicionar um cluster autogerenciado ao Astra Control Service carregando um `kubeconfig.yaml` arquivo. Você precisará garantir que o cluster atenda aos requisitos descritos aqui.

Distribuições compatíveis do Kubernetes

Você pode usar o Astra Control Service para gerenciar os seguintes tipos de clusters privados autogerenciados:

Distribuição do Kubernetes	Versões suportadas
Kubernetes (upstream)	1,27 a 1,29
Rancher Kubernetes Engine (RKE)	RKE 1: Versões 1.24.17, 1.25.13, 1.26.8 com Rancher Manager 2.7.9 RKE 2: Versões 1.23.16 e 1.24.13 com Rancher Manager 2.6.13 RKE 2: Versões 1.24.17, 1.25.14, 1.26.9 com Rancher Manager 2.7.9
Red Hat OpenShift Container Platform	4,12 a 4,14

Essas instruções presumem que você já criou um cluster privado e preparou um método seguro para acessá-lo remotamente.

Você precisa executar as seguintes tarefas para adicionar seu cluster privado ao Astra Control Service:

1. [Instale o conector Astra](#)
2. [Configurar o armazenamento persistente](#)
3. [Adicionar o cluster privado autogerenciado ao Astra Control Service](#)

Instale o conector Astra

Antes de adicionar um cluster privado, é necessário instalar o Astra Connector no cluster para que o Astra Control possa se comunicar com ele. ["Instalar a versão anterior do Astra Connector para clusters privados gerenciados com workflows não nativos em Kubernetes"](#) Consulte para obter instruções.

Configurar o armazenamento persistente

Configurar o armazenamento persistente para o cluster. Consulte a documentação [Introdução](#) para obter mais informações sobre como configurar o armazenamento persistente:

- ["Configure o Microsoft Azure com o Azure NetApp Files"](#)
- ["Configurar o Microsoft Azure com discos gerenciados do Azure"](#)
- ["Configurar o Amazon Web Services"](#)
- ["Configure o Google Cloud"](#)

Adicionar o cluster privado autogerenciado ao Astra Control Service

Agora você pode adicionar o cluster privado ao Astra Control Service.

Antes de começar

Um cluster autogerenciado é um cluster que você provisiona e gerencia diretamente. O Astra Control Service é compatível com clusters autogerenciados que são executados em um ambiente de nuvem pública. Seus clusters autogerenciados podem usar o Astra Control Provisioner para fazer a interface com os serviços de storage da NetApp ou usar drivers da Container Storage Interface (CSI) para fazer a interface com o Amazon Elastic Block Store (EBS), discos gerenciados do Azure e disco persistente do Google.

O Astra Control Service é compatível com clusters autogerenciados que usam as seguintes distribuições do Kubernetes:

- Red Hat OpenShift Container Platform
- Rancher Kubernetes Engine
- Kubernetes upstream

Seu cluster autogerenciado precisa atender aos seguintes requisitos:

- O cluster deve ser acessível através da Internet.
- Se você estiver usando ou planeja usar o armazenamento habilitado com drivers CSI, os drivers CSI apropriados devem ser instalados no cluster. Para obter mais informações sobre como usar drivers CSI para integrar armazenamento, consulte a documentação do seu serviço de armazenamento.
- Você tem acesso ao arquivo kubeconfig cluster que inclui apenas um elemento de contexto. Siga ["estas instruções"](#) para gerar um arquivo kubeconfig.
- Se você estiver adicionando o cluster usando um arquivo kubeconfig que faça referência a uma Autoridade de certificação privada (CA), adicione a seguinte linha à `cluster` seção do arquivo kubeconfig. Isso permite que o Astra Control adicione o cluster:

```
insecure-skip-tls-verify: true
```

- **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.
- **Requisitos da previsão do Astra Control:** Você deve ter um programa de controle Astra Control configurado corretamente, incluindo seus componentes do Astra Trident, para gerenciar clusters.
 - * Rever os requisitos de ambiente do Astra Trident*: Antes de instalar ou atualizar o Astra Control Provisioner, revise o ["interfaces suportadas, backends e configurações de host"](#).
 - **Ativar a funcionalidade do programa Astra Control:** É altamente recomendável instalar o Astra Trident 23,10 ou posterior e ativar ["Funcionalidade de storage avançada do Astra Control Provisioner"](#). Nos próximos lançamentos, o Astra Control não será compatível com o Astra Trident se o programa Astra Control também não estiver habilitado.
 - **Configurar um back-end de armazenamento:** Pelo menos um back-end de armazenamento deve estar ["Configurado no Astra Trident"](#) no cluster.
 - **Configurar uma classe de armazenamento:** Pelo menos uma classe de armazenamento deve estar ["Configurado no Astra Trident"](#) no cluster. Se uma classe de armazenamento padrão estiver configurada, certifique-se de que é a classe de armazenamento **only** que tem a anotação padrão.

- **Configure um controlador de snapshot de volume e instale uma classe de snapshot de volume:** "Instale um controlador instantâneo de volume" Para que os snapshots possam ser criados no Astra Control. "Criar" Pelo menos um `VolumeSnapshotClass` usando Astra Trident.

Passos

1. No Painel, selecione **Gerenciar cluster do Kubernetes**.

Siga as instruções para adicionar o cluster.

2. **Provider:** Selecione a guia **Other** para adicionar detalhes sobre seu cluster autogerenciado.
3. * Outro*: Forneça detalhes sobre seu cluster autogerenciado carregando um `kubeconfig.yaml` arquivo ou colando o conteúdo do `kubeconfig.yaml` arquivo da área de transferência.



Se você criar seu próprio `kubeconfig` arquivo, você deve definir apenas **um** elemento de contexto nele. "estas instruções" Consulte para obter informações sobre a criação `kubeconfig` de ficheiros.

4. **Nome da credencial:** Forneça um nome para a credencial de cluster autogerenciada que você está enviando para o Astra Control. Por padrão, o nome da credencial é preenchido automaticamente como o nome do cluster.
5. **Identificador de rota privada:** Introduza o identificador de rota privada, que pode obter a partir do conector Astra. Se você consultar o conector Astra através do `kubectl get astrconnector -n astrconnector` comando, o identificador de rota privada é chamado de `ASTRACONNECTORID`.



O identificador de rota privada é o nome associado ao Astra Connector que permite que um cluster privado Kubernetes seja gerenciado pelo Astra. Nesse contexto, um cluster privado é um cluster do Kubernetes que não exponha seu servidor de API à Internet.

6. Selecione **seguinte**.
7. (Opcional) **Storage:** Opcionalmente, selecione a classe de armazenamento que você deseja que os aplicativos do Kubernetes implantados nesse cluster usem por padrão.
 - a. Para selecionar uma nova classe de armazenamento padrão para o cluster, ative a caixa de seleção **Assign a new default storage class** (atribuir uma nova classe de armazenamento padrão).
 - b. Selecione uma nova classe de armazenamento padrão na lista.

Cada serviço de storage de fornecedor de nuvem exibe as seguintes informações de preço, performance e resiliência:



- Cloud Volumes Service para Google Cloud: Informações de preço, performance e resiliência
- Persistent Disk do Google: Nenhuma informação de preço, performance ou resiliência disponível
- Azure NetApp Files: Informações de performance e resiliência
- Discos gerenciados do Azure: Nenhuma informação de preço, desempenho ou resiliência disponível
- Amazon Elastic Block Store: Sem informações de preço, desempenho ou resiliência disponíveis
- Amazon FSX for NetApp ONTAP: Sem informações de preço, desempenho ou resiliência disponíveis
- NetApp Cloud Volumes ONTAP: Sem informações de preço, performance ou resiliência disponíveis

Cada classe de storage pode utilizar um dos seguintes serviços:

- ["Cloud Volumes Service para Google Cloud"](#)
- ["Persistent Disk do Google"](#)
- ["Azure NetApp Files"](#)
- ["Discos gerenciados do Azure"](#)
- ["Amazon Elastic Block Store"](#)
- ["Amazon FSX para NetApp ONTAP"](#)
- ["NetApp Cloud Volumes ONTAP"](#)

Saiba mais ["Classes de armazenamento para clusters do Amazon Web Services"](#)sobre o . Saiba mais ["Classes de armazenamento para clusters AKS"](#)sobre o . Saiba mais ["Classes de armazenamento para clusters GKE"](#)sobre o .

- c. Selecione **seguinte**.
- d. **Review & Approve**: Reveja os detalhes de configuração.
- e. Selecione **Adicionar** para adicionar o cluster ao Astra Control Service.

Altere a classe de armazenamento padrão

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

Altere a classe de storage padrão usando o Astra Control

Você pode alterar a classe de storage padrão de um cluster a partir do Astra Control. Se o cluster usar um serviço de back-end de armazenamento instalado anteriormente, talvez você não consiga usar esse método para alterar a classe de armazenamento padrão (a ação **Definir como padrão** não é selecionável). Neste caso, você pode [Altere a classe de armazenamento padrão usando a linha de comando](#).

Passos

1. Na IU do Astra Control Service, 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**.

Altere a classe de armazenamento padrão usando a linha de comando

Você pode alterar a classe de storage padrão de um cluster usando comandos do Kubernetes. Esse método funciona independentemente da configuração do cluster.

Passos

1. Faça login no cluster do Kubernetes.
2. Liste as classes de armazenamento no cluster:

```
kubectl get storageclass
```

3. Remova a designação padrão da classe de armazenamento padrão. Substitua o <SC_NAME> pelo nome da classe de armazenamento:

```
kubectl patch storageclass <SC_NAME> -p '{"metadata": {"annotations":{"storageclass.kubernetes.io/is-default-class":"false"}}}'
```

4. Marque uma classe de armazenamento diferente como padrão. Substitua o <SC_NAME> pelo nome da classe de armazenamento:

```
kubectl patch storageclass <SC_NAME> -p '{"metadata": {"annotations":{"storageclass.kubernetes.io/is-default-class":"true"}}}'
```

5. Confirme a nova classe de armazenamento padrão:

```
kubectl get storageclass
```

Verifique a versão Astra Trident

Para adicionar um cluster autogerenciado que utilize o Astra Control Provisioner ou o Astra Trident para serviços de storage, certifique-se de que a versão instalada do Astra Trident seja a 23,10 ou a mais recente.

Passos

1. Determine a versão do Astra Trident que você está executando:

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

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

```
NAME          VERSION
trident       24.02.0
```

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

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

2. Execute um dos seguintes procedimentos:

- Se você estiver executando o Astra Trident 23,01 ou anterior, use-os ["instruções"](#) para atualizar para uma versão mais recente do Astra Trident antes de atualizar para o Astra Control Provisioner. Você pode ["faça uma atualização direta"](#) usar o Astra Control Provisioner 24,02 se o seu Astra Trident estiver dentro de uma janela de quatro versões da versão 24,02. Por exemplo, você pode fazer o upgrade diretamente do Astra Trident 23,04 para o Astra Control Provisioner 24,02.
- Se você estiver executando o Astra Trident 23,10 ou posterior, verifique se o Astra Control Provisioner foi ["ativado"](#). O Astra Control Provisioner não funcionará com versões do Astra Control Center anteriores a 23,10. ["Atualize seu Astra Control Provisioner"](#) Para que ele tenha a mesma versão do Astra Control Center que você está atualizando para acessar as funcionalidades mais recentes.

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

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

4. Verifique se as classes de storage estão usando os drivers Astra Trident compatíveis. O nome do provisionador deve ser `csi.trident.netapp.io`. Consulte o seguinte exemplo:

```
kubectl get sc
```

Resposta da amostra:

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

Crie um arquivo kubeconfig

Você pode adicionar um cluster ao Astra Control Service usando um arquivo kubeconfig. Dependendo do tipo de cluster que você deseja adicionar, talvez seja necessário criar manualmente um arquivo kubeconfig para o cluster usando etapas específicas.

- [Crie um arquivo kubeconfig para clusters do Amazon EKS](#)
- [Crie um arquivo kubeconfig para clusters do Red Hat OpenShift Service no AWS \(Rosa\)](#)
- [Crie um arquivo kubeconfig para outros tipos de clusters](#)

Crie um arquivo kubeconfig para clusters do Amazon EKS

Siga estas instruções para criar um arquivo kubeconfig e um segredo de token permanente para clusters do Amazon EKS. Um segredo de token permanente é necessário para clusters hospedados no EKS.

Passos

1. Siga as instruções na documentação da Amazon para gerar um arquivo kubeconfig:

["Criando ou atualizando um arquivo kubeconfig para um cluster do Amazon EKS"](#)

2. Crie uma conta de serviço da seguinte forma:

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

Ajuste o nome da conta de serviço conforme necessário. O namespace `kube-system` é necessário para estas etapas. Se você alterar o nome da conta de serviço aqui, você deve aplicar as mesmas alterações nas etapas a seguir.

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

+

```
apiVersion: v1
kind: ServiceAccount
metadata:
  name: astra-admin-account
  namespace: kube-system
```

3. Aplique a conta de serviço:

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

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

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

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: astra-admin-binding
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: cluster-admin
subjects:
- kind: ServiceAccount
  name: astra-admin-account
  namespace: kube-system
```

5. Aplicar a vinculação de funções do cluster:

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

6. Crie um arquivo secreto de token de conta de serviço `astracontrol-secret.yaml` chamado .

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

```
apiVersion: v1
kind: Secret
metadata:
  annotations:
    kubernetes.io/service-account.name: astra-admin-account
  name: astra-admin-account
  namespace: kube-system
type: kubernetes.io/service-account-token
```

7. Aplique o segredo do token:

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

8. Recuperar o segredo do token:

```
kubectl get secret astra-admin-account -n kube-system -o
jsonpath='{.data.token}' | base64 -d
```

9. Substitua a `user` seção do arquivo AWS EKS kubeconfig pelo token, como mostrado no exemplo a seguir:

```
user:
  token: k8s-aws-
v1.aHR0cHM6Ly9zdHMudXMtd2Vzdc0yLmFtYXpvbmF3cy5jb20vP0FjdGlvbj1HZXRDYWxsZ
XJJZGVudG10eSZWZlJ3aW9uPTIwMTUyMDYtMTUwMmE1MmE1MmE1MmE1MmE1MmE1MmE1MmE1
y1TSEEyNTYmWC1BbXotQ3JlZGVudG1hbnD1BS01MmE1MmE1MmE1MmE1MmE1MmE1MmE1MmE1
DAzJTJGdXMtd2Vzdc0yJTJGc3RzJTJGYXdzNF9yZXF1ZlZlbnR5cXp0Yw16LURhdGU9MjAy
MjA1MmE1MmE1MmE1MmE1MmE1MmE1MmE1MmE1MmE1MmE1MmE1MmE1MmE1MmE1MmE1MmE1
ngtazhzLWF3cy1pZCZlUUFteil1FeHBpcml1TaWduYXR1cmU5YjU4ZWM0NzdiM2NkZGYxNGRlbnZU
WQ2zY2NzI2YWIwM2UyNTYmWC1BbXotQ3JlZGVudG1hbnR5cXp0Yw16LURhdGU9MjAyMjA1MmE1
```

Crie um arquivo kubeconfig para clusters do Red Hat OpenShift Service no AWS (Rosa)

Siga estas instruções para criar um arquivo kubeconfig para o Red Hat OpenShift Service nos clusters AWS (Rosa).

Passos

1. Faça login no cluster ROSA.
2. Criar uma conta de serviço:

```
oc create sa astracontrol-service-account
```

3. Adicionar uma função de cluster:

```
oc adm policy add-cluster-role-to-user cluster-admin -z astracontrol-
service-account
```

4. Usando o exemplo a seguir, crie um arquivo de configuração secreta de conta de serviço:

```
<strong>secret-astra-sa.yaml</strong>
```

```
apiVersion: v1
kind: Secret
metadata:
  name: secret-astracontrol-service-account
  annotations:
    kubernetes.io/service-account.name: "astracontrol-service-account"
type: kubernetes.io/service-account-token
```

5. Crie o segredo:

```
oc create -f secret-astra-sa.yaml
```

6. Edite a conta de serviço que você criou e adicione o nome secreto da conta de serviço Astra Control à `secrets` seção:

```
oc edit sa astracontrol-service-account
```

```
apiVersion: v1
imagePullSecrets:
- name: astracontrol-service-account-dockercfg-dvfcd
kind: ServiceAccount
metadata:
  creationTimestamp: "2023-08-04T04:18:30Z"
  name: astracontrol-service-account
  namespace: default
  resourceVersion: "169770"
  uid: 965fa151-923f-4fbd-9289-30cad15998ac
secrets:
- name: astracontrol-service-account-dockercfg-dvfcd
- name: secret-astracontrol-service-account ####ADD THIS ONLY####
```

7. 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-dvfcd" },
  { "name": "secret-astracontrol-service-account" }
]
```

Os índices para cada elemento no `secrets` array começam com 0. No exemplo acima, o índice para `astracontrol-service-account-dockercfg-dvfcd` seria 0 e o índice para `secret-astracontrol-service-account` seria 1. Na sua saída, anote o número do índice para o segredo da conta de serviço. Você precisará deste número de índice na próxima etapa.

8. 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
```

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

```
mv kubeconfig-sa YOUR_CLUSTER_NAME_kubeconfig
```

Crie um arquivo kubeconfig para outros tipos de clusters

Siga estas instruções para criar um arquivo kubeconfig limitado ou expandido para clusters Rancher, Upstream Kubernetes e Red Hat OpenShift.

Para clusters gerenciados usando o kubeconfig, você pode, opcionalmente, criar uma função de administrador de permissão limitada ou expandida para o Astra Control Service.

Este procedimento ajuda você a criar um kubeconfig separado se qualquer um dos seguintes cenários se aplicar ao seu ambiente:

- Você deseja limitar as permissões do Astra Control nos clusters que ele gerencia
- Você usa vários contextos e não pode usar o kubeconfig padrão do Astra Control configurado durante a instalação ou uma função limitada com um único contexto não funcionará em seu ambiente

Antes de começar

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

- Um "versão suportada" de kubectl está instalado.
- Acesso kubectl ao cluster que você pretende adicionar e gerenciar com o Astra Control Service



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

- 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 .

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

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

- b. Aplique a conta de serviço:

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

2. Crie uma das seguintes funções de cluster com permissões suficientes para que um cluster seja gerenciado pelo Astra Control:

Função limitada do cluster

Essa função contém as permissões mínimas necessárias para que um cluster seja gerenciado pelo Astra Control:

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

```
<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
- 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
```

- b. (Somente para clusters OpenShift) Append o seguinte no final `astra-admin-account.yaml` do arquivo:

```
# OpenShift security
- apiGroups:
  - security.openshift.io
  resources:
  - securitycontextconstraints
  verbs:
  - use
  - update
```

- c. Aplique a função de cluster:

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

Função expandida do cluster

Essa função contém permissões expandidas para um cluster a ser gerenciado pelo Astra Control. Você pode usar essa função se você usar vários contextos e não puder usar o kubeconfig padrão do Astra Control configurado durante a instalação ou uma função limitada com um único contexto não funcionará em seu ambiente:



As etapas a seguir `ClusterRole` são um exemplo geral do Kubernetes. Consulte a documentação da distribuição do Kubernetes para obter instruções específicas para o seu ambiente.

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

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

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: astra-admin-account
rules:
- apiGroups:
  - '*'
  resources:
  - '*'
  verbs:
  - '*'
- nonResourceURLs:
  - '*'
  verbs:
  - '*'
```

b. 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.

```
<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
```

b. Aplicar a vinculação de funções do cluster:

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

4. Crie e aplique o segredo do token:

- a. Crie um arquivo secreto de token `secret-astracontrol-service-account.yaml` chamado .

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

```
apiVersion: v1
kind: Secret
metadata:
  name: secret-astracontrol-service-account
  namespace: default
  annotations:
    kubernetes.io/service-account.name: "astracontrol-service-
account"
type: kubernetes.io/service-account-token
```

- b. Aplique o segredo do token:

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

5. Adicione o segredo do token à conta de serviço adicionando seu nome ao `secrets` array (a última linha no exemplo a seguir):

```
kubectl edit sa astracontrol-service-account
```

```

apiVersion: v1
imagePullSecrets:
- name: astracontrol-service-account-dockercfg-48xhx
kind: ServiceAccount
metadata:
  annotations:
    kubectl.kubernetes.io/last-applied-configuration: |

{"apiVersion":"v1","kind":"ServiceAccount","metadata":{"annotations":{},"name":"astracontrol-service-account","namespace":"default"},"creationTimestamp":"2023-06-14T15:25:45Z","name":"astracontrol-service-account","namespace":"default","resourceVersion":"2767069","uid":"2ce068c4-810e-4a96-ada3-49cbf9ec3f89"}
secrets:
- name: astracontrol-service-account-dockercfg-48xhx
<strong>- name: secret-astracontrol-service-account</strong>

```

6. 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-48xhx" },
  { "name": "secret-astracontrol-service-account" }
]

```

Os índices para cada elemento no `secrets` array começam com 0. No exemplo acima, o índice para `astracontrol-service-account-dockercfg-48xhx` seria 0 e o índice para `secret-astracontrol-service-account` seria 1. Na sua saída, anote o número do índice para o segredo da conta de serviço. Você precisará desse número de índice na próxima etapa.

7. Gere o kubeconfig da seguinte forma:

- a. Crie um `create-kubeconfig.sh` arquivo.
- b. 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
```

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

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

8. (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 fez login e adicionou um cluster ao Astra Control, está pronto para começar a usar os recursos de gerenciamento de dados de aplicações do Astra Control.

- ["Comece a gerenciar aplicativos"](#)
- ["Proteja aplicativos"](#)
- ["Clonar aplicações"](#)
- ["Configure a faturação"](#)
- ["Convide e gerencie usuários"](#)
- ["Gerenciar credenciais do fornecedor de nuvem"](#)
- ["Gerenciar notificações"](#)
- ["Implantar uma instância autogerenciada do Astra Control"](#)

Vídeos do Astra Control Service

Não percas a NetApp TV para obteres o conteúdo de vídeo mais recente com o Serviço Astra Control. O NetApp TV inclui vídeos que demonstram certos recursos do Serviço de Controle Astra ou mostram como concluir certas tarefas comuns.

"Vídeos do Astra Control Service"

Conceitos

Arquitetura e componentes

O Astra Control é uma solução de gerenciamento de ciclo de vida de dados da aplicação Kubernetes que simplifica as operações de aplicações com monitoramento de estado e ajuda você a armazenar, proteger e mover seus workloads Kubernetes em ambientes híbridos e multicloud.

Recursos

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

Loja:

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

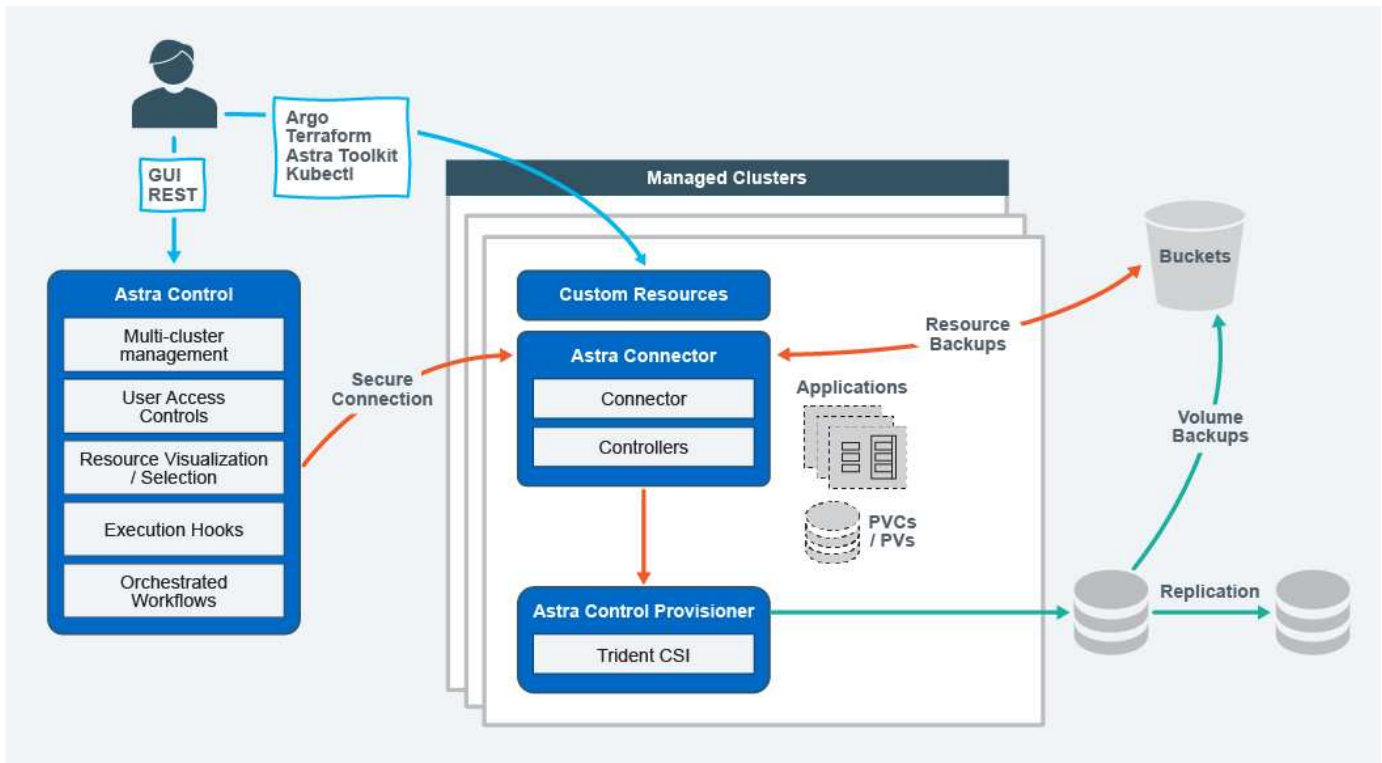
Mover:

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

Arquitetura

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

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



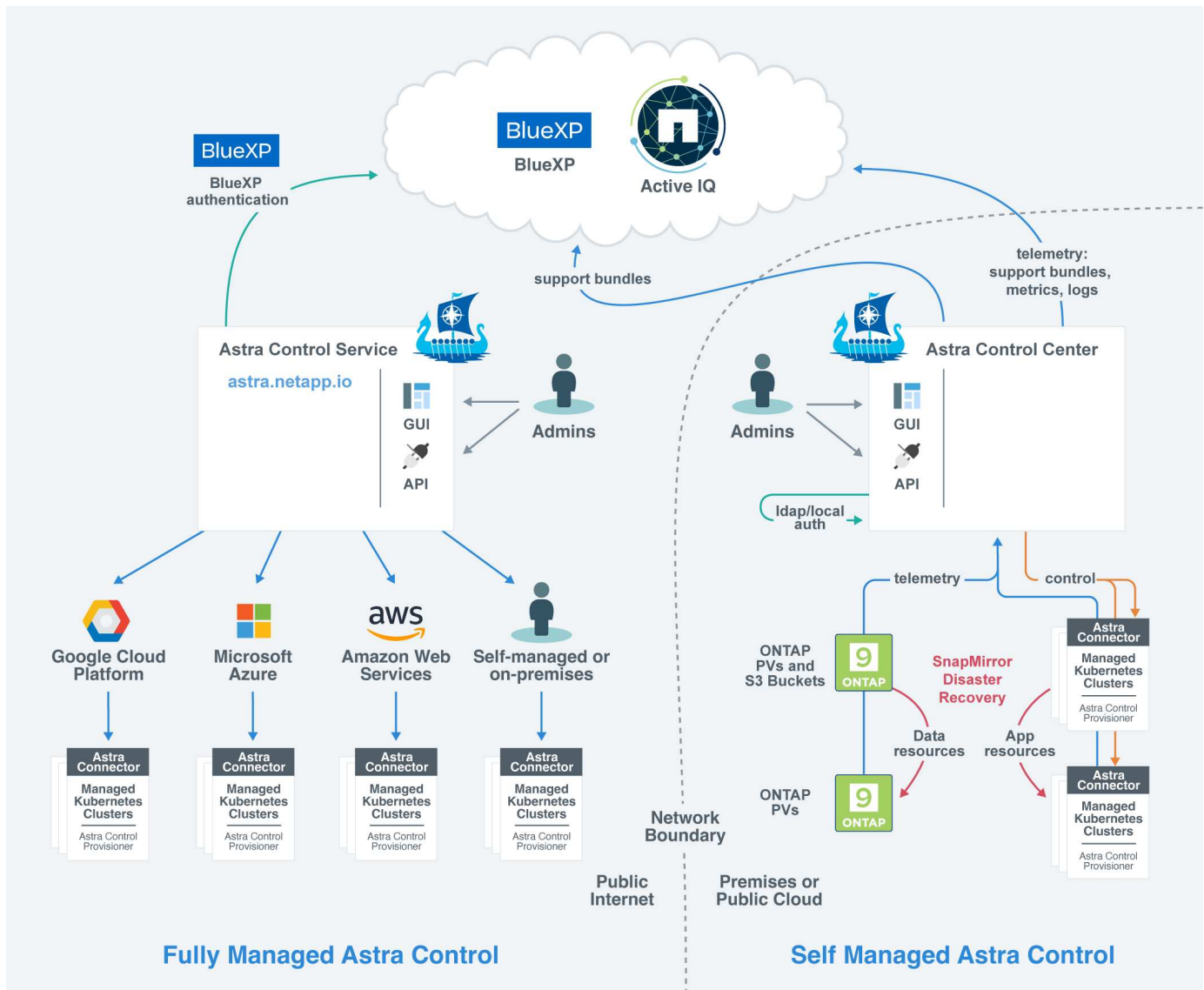
O Astra Control foi desenvolvido com base em quatro componentes complementares:

- **Astra Control:** O Astra Control é o serviço de gerenciamento centralizado para todos os clusters gerenciados, fornecendo workloads orquestrados para proteção e mobilidade de aplicações na nuvem e no local, bem como os seguintes recursos:
 - Visualização combinada de vários clusters e nuvens
 - Proteção de fluxos de trabalho orquestrados
 - Visualização e seleção granular de recursos
- **Astra Connector:** O Astra Connector combina com o Astra Control para fornecer uma conexão segura a cada cluster gerenciado, oferecendo execução local de operações agendadas independentemente do status da conexão, bem como as seguintes funcionalidades:
 - Execução local de operações agendadas independentemente do status da conexão
 - Operações locais que distribuem e otimizam o uso de recursos do sistema do Astra entre clusters
 - Instalação local que permite o menor acesso de privilégios ao cluster para maior segurança
- **Astra Control Provisioner:** O Astra Control Provisioner oferece a funcionalidade de provisionamento de CSI básico e recursos avançados de gerenciamento de storage para configuração adicional de segurança e recuperação de desastres, bem como os seguintes recursos:
 - Provisionamento de storage dinâmico para workloads em contêineres
 - Gerenciamento avançado de storage:
 - Criptografia em trânsito de dados do contêiner para o PV
 - Funcionalidade de nuvem SnapMirror com replicação entre regiões e entre zonas
- **Recursos personalizados do Astra:** Os recursos personalizados usados em cada cluster fornecem uma abordagem nativa do Kubernetes para executar operações localmente, simplificando a integração com outras ferramentas e automação compatíveis com o Kubernetes, além de fornecer os seguintes recursos:
 - Workflows de automação e integração direta de ferramentas de ecossistema

- Primitivas de nível inferior que permitem fluxos de trabalho personalizados

Modelos de implantação

O Astra Control está disponível em 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.

["Documentação do Astra Control Service"](#)

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

["Documentação do Astra Control Center"](#)

	Astra Control 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
Quais são as distribuições compatíveis do Kubernetes?	<ul style="list-style-type: none"> • Provedores de nuvem <ul style="list-style-type: none"> ◦ Amazon Web Services <ul style="list-style-type: none"> ▪ Amazon Elastic Kubernetes Service (EKS) ◦ Google Cloud <ul style="list-style-type: none"> ▪ Google Kubernetes Engine (GKE) ◦ Microsoft Azure <ul style="list-style-type: none"> ▪ Serviço Kubernetes do Azure (AKS) • Clusters autogeridos <ul style="list-style-type: none"> ◦ Kubernetes (upstream) ◦ Rancher Kubernetes Engine (RKE) ◦ Red Hat OpenShift Container Platform • Clusters locais <ul style="list-style-type: none"> ◦ Red Hat OpenShift Container Platform no local 	<ul style="list-style-type: none"> • Serviço Kubernetes do Azure no Azure Stack HCI • Google Anthos • Kubernetes (upstream) • Rancher Kubernetes Engine (RKE) • Red Hat OpenShift Container Platform

	Astra Control Service	Astra Control Center
Quais são os backends de armazenamento suportados?	<ul style="list-style-type: none"> • Provedores de nuvem <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 autogeridos <ul style="list-style-type: none"> ◦ Amazon EBS ◦ Discos gerenciados do Azure ◦ Persistent Disk do Google ◦ "Cloud Volumes ONTAP" ◦ NetApp MetroCluster ◦ "Longhorn" • Clusters locais <ul style="list-style-type: none"> ◦ NetApp MetroCluster ◦ Sistemas NetApp ONTAP AFF e FAS ◦ NetApp ONTAP Select ◦ "Cloud Volumes ONTAP" ◦ "Longhorn" 	<ul style="list-style-type: none"> • Sistemas NetApp ONTAP AFF e FAS • NetApp ONTAP Select • "Cloud Volumes ONTAP" • "Longhorn"

Para mais informações

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

- ["Documentação do ONTAP"](#)

Proteção de dados

Saiba mais sobre os tipos de proteção de dados disponíveis no Astra Control Service 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.



Se você executar um snapshot ou backup, mas a operação falhar com o erro "o recurso não foi criado por causa de um problema de servidor interno", verifique se o back-end de armazenamento que você está usando tem os drivers corretos instalados. Alguns backends de armazenamento precisam de drivers de Container Storage Interface (CSI), enquanto outros precisam de um controlador de snapshot externo.

Backups imutáveis

Um backup imutável é um backup que não pode ser alterado ou excluído durante um período especificado. Quando você cria um backup imutável, o Astra Control verifica para garantir que o bucket que você está

usando seja um bucket do WORM (write once read many) e, nesse caso, garante que o backup seja imutável a partir do Astra Control. O Astra Control Service dá suporte à criação de backups imutáveis com as seguintes plataformas e tipos de bucket:

- Amazon Web Services usando um bucket do Amazon S3 com o bloqueio de objetos S3 configurado
- Microsoft Azure usando um bucket do Azure com uma política de retenção configurada
- Google Kubernetes Engine (GKE) usando um bucket do Google Cloud Storage com uma política de retenção configurada
- NetApp StorageGRID usando um bucket S3 com bloqueio de objeto S3 configurado

Observe o seguinte ao trabalhar com backups imutáveis:

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

Clones

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

Classes de armazenamento e desempenho para clusters da AWS

O Astra Control Service pode usar o Amazon Elastic Block Store (EBS), o Amazon FSX for NetApp ONTAP ou o NetApp Cloud Volumes ONTAP como back-end de armazenamento para clusters do Amazon Elastic Kubernetes Service (EKS).

Amazon Elastic Block Store (EBS)

Seus clusters podem usar drivers de Container Storage Interface (CSI) para fazer interface com o EBS. Quando você usa o EBS como o back-end de armazenamento para clusters EKS, você pode configurar alguns parâmetros de classe de armazenamento. Para obter mais informações sobre o significado dos parâmetros e como configurá-los, ["A documentação do Kubernetes"](#) consulte .

Você pode usar vários tipos diferentes de volumes com o EBS:

- Unidades de estado sólido (SSD)
- Unidades de disco rígido (HDD)
- Geração anterior

Para obter mais informações sobre cada tipo de volume e seu desempenho, ["A documentação do Amazon EBS"](#) consulte . Para obter informações sobre preços, ["Definição de preço do Amazon EBS"](#) consulte .

Amazon FSX para NetApp ONTAP

Quando você usa o FSX for NetApp ONTAP como o back-end de armazenamento para clusters da AWS, o desempenho de e/S depende da configuração do sistema de arquivos e das características das suas cargas de trabalho. Para obter informações específicas sobre o desempenho do FSX for NetApp ONTAP, "[Desempenho do Amazon FSX para NetApp ONTAP](#)" consulte . Para obter informações sobre preços, "[Definição de preço do Amazon FSX for NetApp ONTAP](#)" consulte .

NetApp Cloud Volumes ONTAP

Para obter informações específicas sobre a configuração do NetApp Cloud Volumes ONTAP, incluindo recomendações de desempenho, visite o "[Documentação do NetApp Cloud Volumes ONTAP](#)".

Classes de armazenamento e tamanho PV para clusters AKS

O Astra Control Service é compatível com Azure NetApp Files, discos gerenciados do Azure ou NetApp Cloud Volumes ONTAP como o back-end de storage para clusters do Azure Kubernetes Service (AKS).

Azure NetApp Files

O Astra Control Service é compatível com o Azure NetApp Files como o back-end de storage para clusters do Azure Kubernetes Service (AKS). Você deve entender como escolher uma classe de storage e um tamanho de volume persistente pode ajudar você a atingir seus objetivos de performance.

Níveis de serviço e classes de armazenamento

O Azure NetApp Files dá suporte a três níveis de serviço: Armazenamento ultra-sônico, armazenamento premium e armazenamento padrão. Cada um desses níveis de serviço foi projetado para diferentes necessidades de performance:

Armazenamento ultra

Fornece até 128 MIB/s de taxa de transferência por 1 TIB.

Armazenamento premium

Fornece até 64 MIB/s de taxa de transferência por 1 TIB.

Armazenamento padrão

Fornece até 16 MIB/s de taxa de transferência por 1 TIB.

Esses níveis de serviço são um atributo de um pool de capacidade. Você precisa configurar um pool de capacidade para cada nível de serviço que deseja usar com os clusters do Kubernetes. "[Saiba como configurar pools de capacidade](#)".

O Astra Control Service usa esses níveis de serviço como classes de storage para seus volumes persistentes. Quando você adiciona clusters de Kubernetes ao Astra Control Service, será solicitado que você escolha Ultra, Premium ou Standard como a classe de storage padrão. Os nomes das classes de armazenamento são *NetApp-anf-perf-ultra*, *NetApp-anf-perf-premium* e *NetApp-anf-perf-standard*.

"[Saiba mais sobre esses níveis de serviço nos documentos do Azure NetApp Files](#)".

Tamanho do volume persistente e performance

Como descrito acima, a taxa de transferência para cada nível de serviço é por 1 TiB de capacidade provisionada. Isso significa que volumes maiores fornecem melhor desempenho. Portanto, você deve levar em consideração as necessidades de capacidade e performance ao provisionar volumes.

Tamanho mínimo do volume

O Astra Control Service provisiona volumes persistentes usando um volume mínimo de 100 GiB, mesmo que o PVC solicite um tamanho de volume menor. Por exemplo, se o PVC em um gráfico Helm solicitar 6 GiB, o Astra Control Service provisiona automaticamente um volume de 100 GiB.

Backups de aplicativos

Se você fizer backup de uma aplicação que reside no storage Azure NetApp Files, o Astra Control Service expandirá automaticamente o pool de capacidade. Após a conclusão do backup, o Astra Control Service diminuirá o pool de capacidade para seu tamanho anterior. Dependendo da sua assinatura do Azure, você pode incorrer em cobranças de armazenamento quando isso acontecer. Você pode ver um histórico de eventos de redimensionamento do pool de capacidade no log de eventos da página **atividade**.

Se o pool de capacidade exceder o tamanho máximo permitido pela assinatura do Azure durante a operação de redimensionamento, a operação de backup falhará e um aviso será acionado a partir da API do Azure.

Discos gerenciados do Azure

O Astra Control Service pode usar drivers da Container Storage Interface (CSI) para fazer interface com discos gerenciados do Azure como um back-end de storage. Esse serviço fornece storage em nível de bloco gerenciado pelo Azure.

["Saiba mais sobre discos gerenciados do Azure"](#).

NetApp Cloud Volumes ONTAP

Para obter informações específicas sobre a configuração do NetApp Cloud Volumes ONTAP, incluindo recomendações de desempenho, visite o ["Documentação do NetApp Cloud Volumes ONTAP"](#).

Tipo de serviço, classes de armazenamento e tamanho PV para clusters GKE

O Astra Control Service é compatível com o NetApp Cloud Volumes Service para Google Cloud, Google Persistent Disk ou NetApp Cloud Volumes ONTAP como opções de back-end de storage para volumes persistentes.

Cloud Volumes Service para Google Cloud

O Astra Control Service usa o Cloud Volumes Service para Google Cloud como o back-end de storage para volumes persistentes. Você deve entender como escolher um tipo de serviço, uma classe de storage e um tamanho de volume persistente pode ajudar você a atingir seus objetivos de performance.

Visão geral

O Cloud Volumes Service fornece dois tipos de serviço: *CVS* e *CVS-Performance*. Esses tipos de serviço são

compatíveis em regiões específicas do Google Cloud. ["Vá para Mapas de Regiões globais da NetApp BlueXP"](#) Para identificar o tipo de serviço compatível na região do Google Cloud onde seus clusters residem.

Se os clusters do Kubernetes precisarem residir em uma região específica, você usará o tipo de serviço compatível nessa região.

Mas se você tiver flexibilidade para escolher entre as regiões do Google Cloud, recomendamos o seguinte com base em seus requisitos de desempenho:

- Para aplicações K8s com necessidades de storage de performance média a alta, escolha uma região do Google Cloud compatível com CVS-Performance e use a classe de storage Premium ou Extreme. Tais workloads incluem pipelines de AI/ML, pipelines de CI/CD, processamento de Mídia e bancos de dados, incluindo bancos de dados relacionais, NoSQL, séries temporais etc.
- Para aplicativos K8s com necessidades de desempenho de armazenamento de baixo a médio porte (aplicações da Web, armazenamento de arquivos de uso geral, etc.), escolha uma região do Google Cloud que suporte CVS ou CVS-Performance, com a classe de armazenamento padrão.



Se você usar o tipo de serviço CVS com Astra Control Provisioner, precisará configurar pools de storage antes de provisionar volumes. Se você provisionar volumes sem pools de storage configurados, o provisionamento de volume falhará. Consulte a ["Documentação do Cloud Volumes Service"](#) para obter mais informações sobre a criação de volumes.

A tabela a seguir fornece uma comparação rápida das informações descritas nesta página.

Tipo de serviço	Caso de uso	Regiões suportadas	Classes de armazenamento	Tamanho mín. Do volume
CVS-performance	Aplicativos com necessidades de desempenho de armazenamento médio a alto	"Veja regiões compatíveis do Google Cloud"	<ul style="list-style-type: none">• NetApp-cvs-perf-standard• NetApp-cvs-perf-premium• NetApp-cvs-perf-extreme	100 GiB
CVS	Aplicativos com necessidades de desempenho de armazenamento de baixo a médio porte	"Veja regiões compatíveis do Google Cloud"	NetApp-cvs-padrão	300 GiB

Tipo de serviço CVS-Performance

Saiba mais sobre o tipo de serviço CVS-Performance antes de escolher uma classe de armazenamento e criar volumes persistentes.

Classes de armazenamento

Três níveis de serviço são compatíveis com o tipo de serviço CVS-Performance: Standard, Premium e Extreme. Quando você adiciona um cluster ao Astra Control Service, será solicitado que você escolha Standard, Premium ou Extreme como a classe de storage padrão para volumes persistentes. Cada um desses níveis de serviço é projetado para diferentes necessidades de capacidade e largura de banda.

Os nomes das classes de armazenamento são *NetApp-cvs-perf-standard*, *NetApp-cvs-perf-premium* e

NetApp-cvs-perf-extreme.

["Saiba mais sobre esses níveis de serviço nos documentos do Cloud Volumes Service para Google Cloud"](#).

Tamanho do volume persistente e performance

"[Como explica os documentos do Google Cloud](#)", A largura de banda permitida para cada nível de serviço é por GiB de capacidade provisionada. Isso significa que volumes maiores proporcionarão melhor desempenho.

Certifique-se de ler a página do Google Cloud vinculada acima. Ele inclui comparações de custos e exemplos que podem ajudá-lo a entender melhor como acoplar um nível de serviço com tamanho de volume para atender aos seus objetivos de desempenho.

Tamanho mínimo do volume

O Astra Control Service provisiona volumes persistentes usando um tamanho de volume mínimo de 100 GiB com o tipo de serviço CVS-Performance, mesmo que o PVC solicite um tamanho de volume menor. Por exemplo, se o PVC em um gráfico Helm solicitar 6 GiB, o Astra Control Service provisiona automaticamente um volume de 100 GiB.

Tipo de serviço CVS

Saiba mais sobre o tipo de serviço CVS antes de escolher uma classe de armazenamento e criar volumes persistentes.

Classe de armazenamento

Um nível de serviço é suportado com o tipo de serviço CVS: Standard. Quando você gerencia clusters em regiões onde o tipo de serviço CVS é compatível, o Astra Control Service usa o nível de serviço padrão como a classe de storage padrão para volumes persistentes. A classe de armazenamento é chamada *NetApp-cvs-standard*.

["Saiba mais sobre o nível de serviço padrão nos documentos do Cloud Volumes Service para Google Cloud"](#).

Tamanho do volume persistente e performance

A largura de banda permitida para o tipo de serviço CVS é por GiB de capacidade provisionada. Isso significa que volumes maiores proporcionarão melhor desempenho.

Tamanho mínimo do volume

O Astra Control Service provisiona volumes persistentes usando um volume mínimo de 300 GiB com o tipo de serviço CVS, mesmo que o PVC solicite um tamanho de volume menor. Por exemplo, se 20 GiB for solicitado, o Astra Control Service provisiona automaticamente um volume de 300 GiB.

Devido a uma limitação, se um PVC solicitar um volume entre 700-999 GiB, o Astra Control Service provisiona automaticamente um volume de 1000 GiB.

Persistent Disk do Google

O Astra Control Service pode usar drivers da Container Storage Interface (CSI) para fazer a interface com o Google persistent Disk como um back-end de storage. Esse serviço fornece storage em nível de bloco gerenciado pelo Google.

["Saiba mais sobre o Google Persistent Disk"](#).

"Saiba mais sobre os diferentes níveis de desempenho dos discos persistentes do Google".

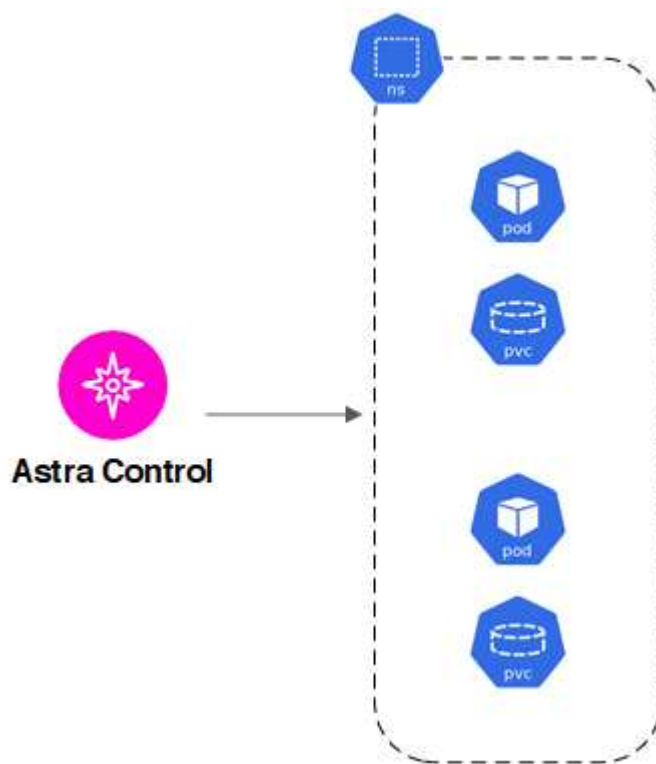
NetApp Cloud Volumes ONTAP

Para obter informações específicas sobre a configuração do NetApp Cloud Volumes ONTAP, incluindo recomendações de desempenho, visite o ["Documentação do NetApp Cloud Volumes ONTAP"](#).

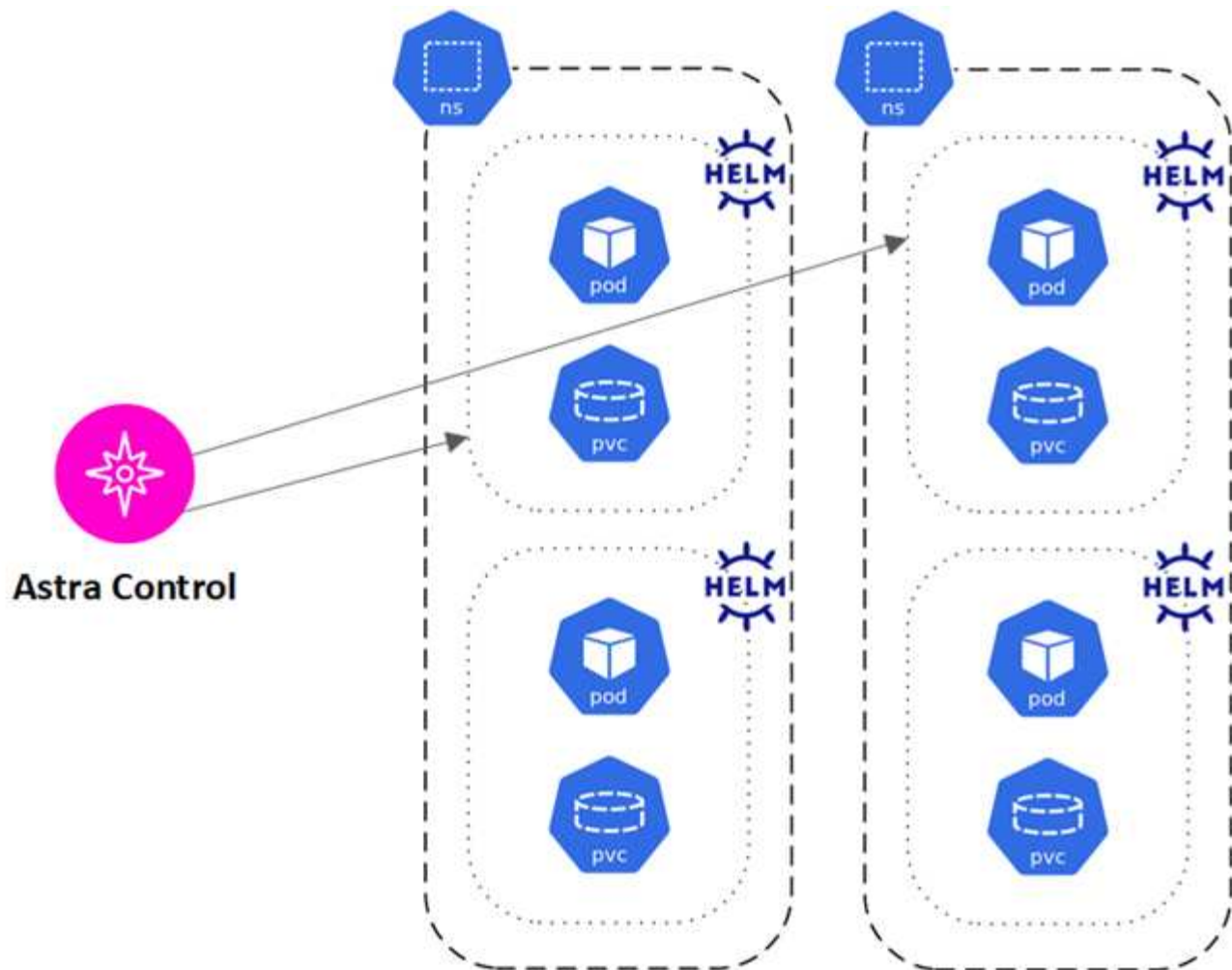
Gerenciamento de aplicativos

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:

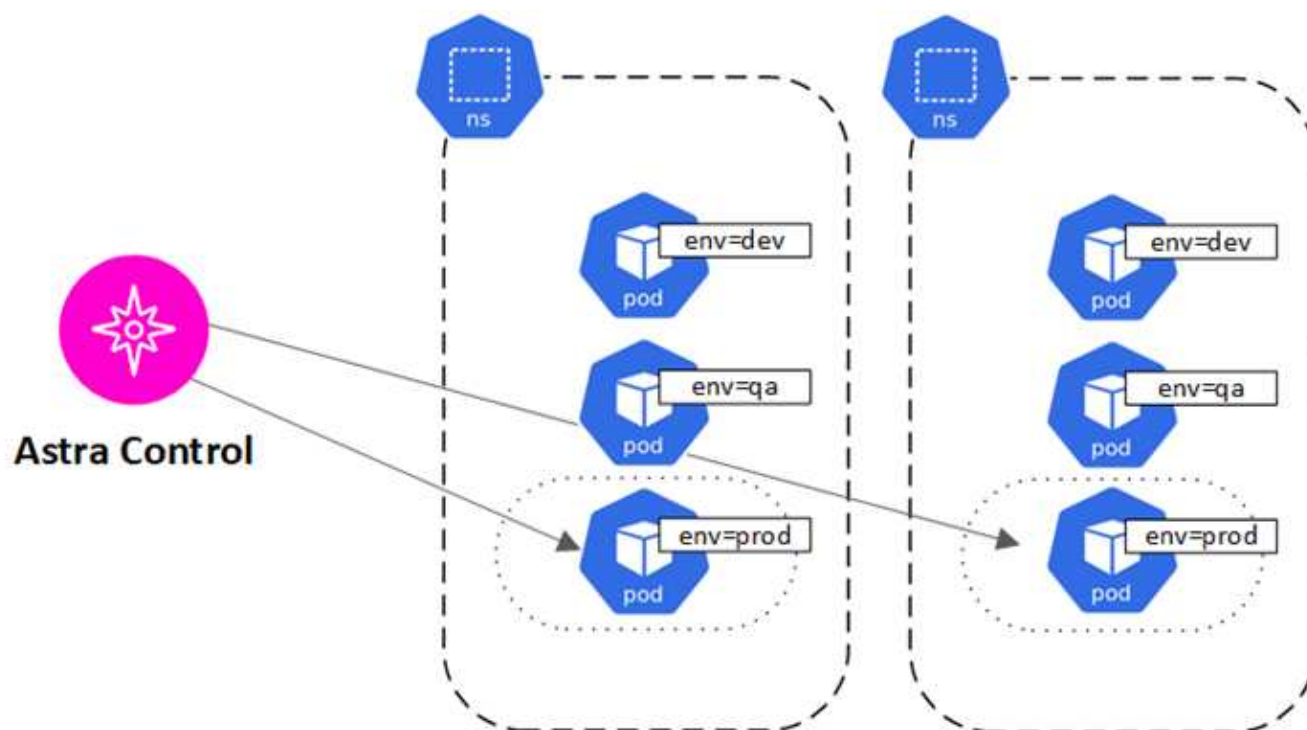
- Namespace, incluindo todos os recursos nesse namespace



- Um aplicativo individual implantado em um ou mais namespaces (Helm 3 é usado neste exemplo)



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



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 **proprietário** tem permissões de administrador e pode excluir contas.
- Um **Admin** tem permissões de Membro e pode convidar outros usuários.
- Um **Membro** pode gerenciar totalmente aplicativos e clusters.
- Um **Viewer** pode visualizar recursos.

Pode adicionar restrições a um utilizador Membro ou Visualizador para restringir o utilizador a um ou mais [Namespaces](#).

Namespaces

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

Encontre mais informações

- ["Gerenciar funções"](#)

Use o Astra Control Service

Faça login no Astra Control Service

O Astra Control Service pode ser acessado por meio de uma interface de usuário baseada em SaaS acessando <https://astra.netapp.io> o .



Você pode usar o logon único para fazer login usando credenciais de seu diretório corporativo (identidade federada). Para saber mais, vá para o "[Centro de Ajuda](#)" e selecione **Opções de início de sessão na Cloud Central**.

Antes de começar

- "[Um ID de usuário do BlueXP](#)".
- "[Uma nova conta do Astra Control](#)" ou "[um convite para uma conta existente](#)".
- Um navegador da Web compatível.

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

Passos

1. Abra um navegador da Web e vá para <https://astra.netapp.io>.
2. Faça login usando suas credenciais NetApp BlueXP .

Gerenciar e proteger aplicativos

Comece a gerenciar aplicativos

Depois do "[Adicionar um cluster de Kubernetes ao Astra Control](#)", você poderá instalar aplicações no cluster (fora do Astra Control) e, em seguida, ir para a página aplicações no Astra Control para definir as aplicações.

Você pode definir e gerenciar aplicativos que incluem recursos de storage com pods em execução ou aplicativos que incluem recursos de storage sem pods em execução. Os aplicativos que não têm pods em execução são conhecidos como aplicativos somente de dados.

Requisitos de gerenciamento de aplicativos

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

- **Licenciamento:** Para gerenciar mais de 10 namespaces, você precisa de uma assinatura Astra Control.
- **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:** Os aplicativos 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) são totalmente compatíveis. O gerenciamento de aplicativos instalados com o Helm 2 não é suportado.
- **Aplicativos implantados pelo operador:** O Astra Control suporta aplicativos instalados com operadores com escopo de namespace 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 que o operador garanta 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.

O Astra Control só gerenciará aplicações com estado monitorado se o storage estiver em uma classe de storage suportada pelo Astra Control. O Astra Control Service dá suporte a qualquer classe de storage compatível com o Astra Control Provisioner ou um driver CSI genérico.

- ["Saiba mais sobre as classes de armazenamento para clusters GKE"](#)
- ["Saiba mais sobre as classes de armazenamento para clusters AKS"](#)
- ["Saiba mais sobre as classes de armazenamento para clusters da AWS"](#)

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 seus aplicativos no Astra Control, considere "[modificação de funções de usuário com restrições de namespace](#)" antes de definir aplicativos.
- 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 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 em 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 nomes de nomes, [Definir recursos para gerenciar como um aplicativo](#) consulte a .



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.

[Visualização técnica] defina uma aplicação usando um recurso personalizado do Kubernetes

Você pode especificar os recursos do Kubernetes que deseja gerenciar com o Astra Control definindo-os como uma aplicação usando um recurso personalizado (CR). Você pode adicionar recursos com escopo de cluster se quiser gerenciar esses recursos individualmente ou todos os recursos do Kubernetes em um namespace se, por exemplo, você pretende gerenciar e proteger todos os recursos em um namespace específico de maneira semelhante e em intervalos comuns.

Passos

1. Crie o arquivo de recurso personalizado (CR) e nomeie-o (por exemplo, `astra_mysql_app.yaml`).
2. Nomeie o aplicativo em `metadata.name`.
3. Definir recursos de aplicativos a serem gerenciados:

spec.includedClusterScopedResources

Incluir tipos de recursos com escopo de cluster além daqueles que o Astra Control inclui automaticamente:

- **spec.includedClusterScopedResources:** *(Opcional)* Uma lista de tipos de recursos com escopo de cluster a serem incluídos.
 - **GroupVersionKind:** *(Opcional)* identifica inequivocamente um tipo.
 - **Group:** *(obrigatório se groupVersionKind for usado)* grupo API do recurso a incluir.
 - **Version:** *(obrigatório se groupVersionKind for usado)* versão da API do recurso a incluir.
 - **Kind:** *(obrigatório se groupVersionKind for usado)* tipo do recurso a incluir.
 - **LabelSelector:** *(Opcional)* Uma consulta de rótulo para um conjunto de recursos. Ele é usado para recuperar apenas os recursos correspondentes ao rótulo. Se você não fornecer um rótulo, o Astra Control coletará todas as instâncias do tipo de recurso especificado para esse cluster. O resultado de matchLabels e matchExpressions são ANDed.
 - **MatchLabels:** *(Opcional)* Um mapa de pares chave,valor. Uma única chave no mapa MatchLabels é equivalente a um elemento de matchExpressions que tem um campo chave de "key", operador como "in", e array de valores contendo apenas "value". Os requisitos são ANDed.
 - **MatchExpressions:** *(Opcional)* Uma lista de requisitos de seleção de etiquetas. Os requisitos são ANDed.
 - **Key:** *(obrigatório se matchExpressions for usado)* a chave de etiqueta associada ao seletor de etiquetas.
 - **Operator:** *(obrigatório se matchExpressions for usado)* representa a relação de uma chave com um conjunto de valores. Os operadores válidos são In, NotIn, Exists e DoesNotExist.
 - **Values:** *(obrigatório se matchExpressions for usado)* uma matriz de valores de string. Se o operador for In ou NotIn, a matriz de valores deve não estar vazia. Se o operador for Exists ou DoesNotExist, a matriz de valores deve estar vazia.

spec.includedNamespaces

Inclua namespaces e recursos dentro desses recursos no aplicativo:

- **spec.includedNamespaces:** *_(required)_* define o namespace e os filtros opcionais para seleção de recursos.
 - *** Namespace*:** *(obrigatório)* o namespace que contém os recursos do aplicativo que você deseja gerenciar com o Astra Control.
 - **LabelSelector:** *(Opcional)* Uma consulta de rótulo para um conjunto de recursos. Ele é usado para recuperar apenas os recursos correspondentes ao rótulo. Se você não fornecer um rótulo, o Astra Control coletará todas as instâncias do tipo de recurso especificado para esse cluster. O resultado de matchLabels e matchExpressions são ANDed.
 - **MatchLabels:** *(Opcional)* Um mapa de pares chave,valor. Uma única chave no mapa MatchLabels é equivalente a um elemento de matchExpressions que tem um campo chave de "key", operador como "in", e array de valores contendo apenas "value". Os requisitos são ANDed.
 - **MatchExpressions:** *(Opcional)* Uma lista de requisitos de seleção de etiquetas. `key` e `operator` são necessários. Os requisitos são ANDed.

- **Key:** (*obrigatório se matchExpressions for usado*) a chave de etiqueta associada ao seletor de etiquetas.
- **Operator:** (*obrigatório se matchExpressions for usado*) representa a relação de uma chave com um conjunto de valores. Os operadores válidos são In, NotIn, Exists e DoesNotExist.
- **Values:** (*obrigatório se matchExpressions for usado*) uma matriz de valores de string. Se o operador for In ou NotIn, a matriz de valores deve *não* estar vazia. Se o operador for Exists ou DoesNotExist, a matriz de valores deve estar vazia.

Exemplo YAML:

```
apiVersion: astra.netapp.io/v1
kind: Application
metadata:
  name: astra_mysql_app
spec:
  includedNamespaces:
    - namespace: astra_mysql_app
  labelSelector:
    matchLabels:
      app: nginx
      env: production
    matchExpressions:
      - key: tier
        operator: In
        values:
          - frontend
          - backend
```

4. Depois de preencher o `astra_mysql_app.yaml` ficheiro com os valores corretos, aplique o CR:

```
kubectl apply -f astra_mysql_app.yaml -n astra-connector
```

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.

Proteja aplicativos com snapshots e backups

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

Saiba mais ["Proteção de dados no Astra Control"](#)sobre o .

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](#)
- [Habilite o backup e a restauração de operações de economia de ONTAP nas](#)
- [Crie um backup imutável](#)
- [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. Você pode definir uma política de proteção usando a IU da Web do Astra Control ou um arquivo de recurso personalizado (CR).

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"](#).



Se você estiver definindo uma política de proteção que crie backups imutáveis para gravar buckets WORM (uma vez leitura muitas), verifique se o tempo de retenção dos backups não é menor do que o período de retenção configurado para o bucket.



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.

Configurar uma política de proteção usando a IU da Web

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 a serem mantidos para as programações horárias, diárias, semanais e mensais.

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.

[Uma captura de tela de uma política de configuração de exemplo, na qual você pode optar por fazer snapshots e backups por hora, diariamente, semanalmente ou mensalmente.]

5. **[Tech Preview]** escolha um intervalo de destino para os backups ou snapshots da lista de buckets de armazenamento.
6. Selecione **Revisão**.
7. Selecione **Definir política de proteção**.

[Tech Preview] Configure uma política de proteção usando um CR

Passos

1. Crie o arquivo de recurso personalizado (CR) e nomeie-o `astra-control-schedule-cr.yaml`. Atualize os valores entre parêntesis > para atender às necessidades de proteção de dados, configuração de cluster e ambiente Astra Control:
 - `<CR_NAME>`: O nome deste recurso personalizado; escolha um nome único e sensato para o seu ambiente.
 - `<APPLICATION_NAME>`: O nome do Kubernetes da aplicação para fazer backup.
 - `<APPVAULT_NAME>`: O nome do AppVault onde o conteúdo de backup deve ser armazenado.
 - `<BACKUPS_RETAINED>`: O número de backups a reter. Zero indica que nenhum backup deve ser criado.
 - `<SNAPSHOTS_RETAINED>`: O número de instantâneos a reter. Zero indica que nenhum instantâneo deve ser criado.
 - `<GRANULARITY>`: A frequência em que o horário deve ser executado. Valores possíveis, juntamente com campos associados obrigatórios:
 - `hourly` (requer que você especifique `spec.minute`)
 - `daily` (requer que você especifique `spec.minute` e `spec.hour`)
 - `weekly` (requer que você especifique `spec.minute`, `spec.hour` e `spec.dayOfWeek`)
 - `monthly` (requer que você especifique `spec.minute`, `spec.hour` e `spec.dayOfMonth`)

- <DAY_OF_MONTH>: (Opcional) o dia do mês (1 - 31) que o cronograma deve ser executado. Este campo é necessário se a granularidade estiver definida como `monthly`.
- <DAY_OF_WEEK>: (Opcional) o dia da semana (0 - 7) que o cronograma deve ser executado. Os valores de 0 ou 7 indicam domingo. Este campo é necessário se a granularidade estiver definida como `weekly`.
- <HOUR_OF_DAY>: (Opcional) a hora do dia (0 - 23) em que o horário deve ser executado. Este campo é necessário se a granularidade estiver definida como `daily`, `weekly` `monthly` ou `.`
- <MINUTE_OF_HOUR>: (Opcional) o minuto da hora (0 - 59) que o cronograma deve ser executado. Este campo é necessário se a granularidade estiver definida como `hourly`, `daily` `weekly`, ou `monthly`.

```

apiVersion: astra.netapp.io/v1
kind: Schedule
metadata:
  namespace: astra-connector
  name: <CR_NAME>
spec:
  applicationRef: <APPLICATION_NAME>
  appVaultRef: <APPVAULT_NAME>
  backupRetention: "<BACKUPS_RETAINED>"
  snapshotRetention: "<SNAPSHOTS_RETAINED>"
  granularity: <GRANULARITY>
  dayOfMonth: "<DAY_OF_MONTH>"
  dayOfWeek: "<DAY_OF_WEEK>"
  hour: "<HOUR_OF_DAY>"
  minute: "<MINUTE_OF_HOUR>"

```

2. Depois de preencher o `astra-control-schedule-cr.yaml` ficheiro com os valores corretos, aplique o CR:

```
kubectl apply -f astra-control-schedule-cr.yaml
```

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.

Sobre esta tarefa

O Astra Control é compatível com a criação de snapshot usando classes de storage com o respaldo dos seguintes drivers:

- `ontap-nas`
- `ontap-san`
- `ontap-san-economy`



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.

Crie um instantâneo usando a IU da Web

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. **[Tech Preview]** escolha um intervalo de destino para o instantâneo na lista de intervalos de armazenamento.
5. Reveja o resumo do instantâneo e selecione **Snapshot**.

[Tech preview] Crie um instantâneo usando um CR

Passos

1. Crie o arquivo de recurso personalizado (CR) e nomeie-o `astra-control-snapshot-cr.yaml`. Atualize os valores entre parêntesis > para corresponder ao seu ambiente Astra Control e à configuração de cluster:
 - `<CR_NAME>`: O nome deste recurso personalizado; escolha um nome único e sensato para o seu ambiente.
 - `<APPLICATION_NAME>`: O nome do Kubernetes da aplicação para snapshot.
 - `<APPVAULT_NAME>`: O nome do AppVault onde o conteúdo do snapshot deve ser armazenado.
 - `<RECLAIM_POLICY>`: (*Opcional*) define o que acontece com um snapshot quando o snapshot CR é excluído. Opções válidas:
 - Retain
 - Delete (predefinição)

```
apiVersion: astra.netapp.io/v1
kind: Snapshot
metadata:
  namespace: astra-connector
  name: <CR_NAME>
spec:
  applicationRef: <APPLICATION_NAME>
  appVaultRef: <APPVAULT_NAME>
  reclaimPolicy: <RECLAIM_POLICY>
```

2. Depois de preencher o `astra-control-snapshot-cr.yaml` ficheiro com os valores corretos, aplique o CR:

```
kubectl apply -f astra-control-snapshot-cr.yaml
```

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.



Esteja ciente de como o espaço de armazenamento é manipulado quando você faz backup de um aplicativo hospedado no storage Azure NetApp Files. "[Backups de aplicativos](#)" Consulte para obter mais informações.

O Astra Control é compatível com a criação de backup usando classes de storage com o respaldo dos seguintes drivers:



- `ontap-nas`
- `ontap-nas-economy`
- `ontap-san`
- `ontap-san-economy`

Sobre esta tarefa

Buckets no Astra Control não relatam a capacidade disponível. Antes de fazer backup ou clonar aplicativos gerenciados pelo Astra Control, verifique as informações do bucket no sistema de gerenciamento de storage apropriado.

Se o seu aplicativo usa uma classe de armazenamento suportada pelo `ontap-nas-economy` driver, você precisa [ativar cópia de segurança e restauro](#) de funcionalidade. Certifique-se de que definiu um `backendType` parâmetro no "[Objeto de storage do Kubernetes](#)" com um valor de `ontap-nas-economy` antes de executar quaisquer operações de proteção.

Crie um backup usando a IU da Web

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. **[Tech Preview]** 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**.

[Tech Preview] Crie uma cópia de segurança utilizando um CR

Passos

1. Crie o arquivo de recurso personalizado (CR) e nomeie-o `astra-control-backup-cr.yaml`. Atualize os valores entre parêntesis para corresponder ao seu ambiente Astra Control e à configuração de cluster:
 - `<CR_NAME>`: O nome deste recurso personalizado; escolha um nome único e sensato para o seu ambiente.
 - `<APPLICATION_NAME>`: O nome do Kubernetes da aplicação para fazer backup.
 - `<APPVAULT_NAME>`: O nome do AppVault onde o conteúdo de backup deve ser armazenado.

```
apiVersion: astra.netapp.io/v1
kind: Backup
metadata:
  namespace: astra-connector
  name: <CR_NAME>
spec:
  applicationRef: <APPLICATION_NAME>
  appVaultRef: <APPVAULT_NAME>
```

2. Depois de preencher o `astra-control-backup-cr.yaml` ficheiro com os valores corretos, aplique o CR:

```
kubectl apply -f astra-control-backup-cr.yaml
```

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.

Habilite o backup e a restauração de operações de economia de ONTAP nas

O Astra Control Provisioner oferece funcionalidade de backup e restauração que pode ser habilitada para back-ends de storage que usam a `ontap-nas-economy` classe de storage.

Antes de começar

- Você ativou o Astra Control Provisioner ou o Astra Trident.
- Você definiu uma aplicação no Astra Control. Esta aplicação terá uma funcionalidade de proteção limitada até concluir este procedimento.
- Você `ontap-nas-economy` selecionou como a classe de armazenamento padrão para o back-end de armazenamento.

Expanda para obter as etapas de configuração

1. Faça o seguinte no back-end de storage do ONTAP:

- a. Encontre o SVM que hospeda os `ontap-nas-economy` volumes baseados na aplicação.
- b. Faça login em um terminal conectado ao ONTAP onde os volumes são criados.
- c. Ocultar o diretório de snapshot para o SVM:



Essa alteração afeta todo o SVM. O diretório oculto continuará acessível.

```
nfs modify -vserver <svm name> -v3-hide-snapshot enabled
```

+



Verifique se o diretório de snapshot no back-end de storage do ONTAP está oculto. A falha em ocultar esse diretório pode levar à perda de acesso ao aplicativo, especialmente se estiver usando NFSv3.

2. Faça o seguinte no Astra Control Provisioner ou Astra Trident:

- a. Ative o diretório de snapshot para cada PV baseado em ONTAP-nas-Economy e associado ao aplicativo:

```
tridentctl update volume <pv name> --snapshot-dir=true --pool  
-level=true -n trident
```

- b. Confirme se o diretório instantâneo foi ativado para cada PV associado:

```
tridentctl get volume <pv name> -n trident -o yaml | grep  
snapshotDir
```

Resposta:

```
snapshotDirectory: "true"
```

3. No Astra Control, atualize a aplicação depois de ativar todos os diretórios snapshot associados para que o Astra Control reconheça o valor alterado.

Resultado

A aplicação está pronta para fazer backup e restauração com o Astra Control. Cada PVC também está disponível para ser usado por outras aplicações para backups e restaurações.

Crie um backup imutável

Um backup imutável não pode ser modificado, excluído ou substituído, desde que a política de retenção no bucket que armazena o backup o proíba. Você pode criar backups imutáveis fazendo backup de aplicativos em buckets que tenham uma política de retenção configurada. ["Proteção de dados"](#) Consulte para obter informações importantes sobre como trabalhar com backups imutáveis.

Antes de começar

Você precisa configurar o intervalo de destino com uma política de retenção. A forma como você faz isso será diferente dependendo do provedor de armazenamento que você usa. Consulte a documentação do fornecedor de armazenamento para obter mais informações:

- **Amazon Web Services:** ["Ative o bloqueio de objetos S3D ao criar o bucket e defina um modo de retenção padrão de "governança" com um período de retenção padrão"](#).
- **Google Cloud:** ["Configure um bucket com uma política de retenção e especifique um período de retenção"](#).
- **Microsoft Azure:** ["Configure um bucket de armazenamento de blob com uma política de retenção baseada no tempo no escopo do nível do contêiner"](#).
- **NetApp StorageGRID:** ["Ative o bloqueio de objetos S3D ao criar o bucket e defina um modo de retenção padrão de "conformidade" com um período de retenção padrão"](#).



Buckets no Astra Control não relatam a capacidade disponível. Antes de fazer backup ou clonar aplicativos gerenciados pelo Astra Control, verifique as informações do bucket no sistema de gerenciamento de storage apropriado.



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.

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. Um bucket WORM (write once read many) é indicado com um status de "bloqueado" ao lado do nome do bucket.



Se o balde for um tipo não suportado, isso é indicado quando você passa o Mouse sobre ou seleciona o balde.

6. Selecione **seguinte**.
7. Reveja o resumo da cópia de segurança e selecione **cópia de segurança**.

Resultado

O Astra Control cria um backup imutável do aplicativo.



- 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 você tentar criar dois backups imutáveis do mesmo aplicativo no mesmo bucket ao mesmo tempo, o Astra Control impede que o segundo backup seja iniciado. Aguarde até que o primeiro backup esteja concluído antes de iniciar outro.
- Não é possível cancelar um backup imutável em execução.
- 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.



Um backup imutável é indicado com um status de "bloqueado" ao lado do intervalo que está usando.

Passos

1. Selecione **aplicativos** e, em seguida, selecione o nome de um aplicativo gerenciado.
2. Selecione **proteção de dados**.

Os instantâneos são apresentados por predefinição.

3. Selecione **backups** para consultar a lista de backups.

Eliminar instantâneos

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

Passos

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



Não é possível cancelar um backup imutável em execução.

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.



Você não pode excluir um backup imutável antes que o período de retenção expire.

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.

[Tech Preview] Proteja um cluster inteiro

Você pode criar um backup automático e agendado de qualquer um ou todos os namespaces não gerenciados em um cluster. Esses fluxos de trabalho são fornecidos pelo NetApp como uma conta de serviço do Kubernetes, vinculações de função e um trabalho cron, orquestrado com um script Python.

Como funciona

Quando você configura e instala o fluxo de trabalho de backup de cluster completo, uma tarefa cron é executada periodicamente e protege qualquer namespace que ainda não seja gerenciado, criando automaticamente políticas de proteção com base nos horários escolhidos durante a instalação.

Se você não quiser proteger todos os namespace não gerenciados no cluster com o fluxo de trabalho completo de backup do cluster, pode utilizar o fluxo de trabalho de backup baseado em rótulos. O fluxo de trabalho de backup baseado em rótulos também usa uma tarefa cron, mas em vez de proteger todos os namespaces não gerenciados, ele identifica namespaces por rótulos que você fornece para proteger opcionalmente os namespaces com base em políticas de backup bronze, prata ou ouro.

Quando um novo namespace é criado que se enquadra no escopo do fluxo de trabalho escolhido, ele é protegido automaticamente, sem qualquer ação do administrador. Esses fluxos de trabalho são

implementados por cluster para que diferentes clusters possam usar qualquer fluxo de trabalho com níveis de proteção exclusivos, dependendo da importância do cluster.

Exemplo: Proteção total do cluster

Por exemplo, quando você configura e instala o fluxo de trabalho completo de backup do cluster, todos os aplicativos em qualquer namespace são gerenciados e protegidos periodicamente, sem mais esforço do administrador. O namespace não precisa existir no momento em que você instala o fluxo de trabalho; se um namespace for adicionado no futuro, ele será protegido.

Exemplo: Proteção baseada em etiquetas

Para obter mais granularidade, você pode usar o fluxo de trabalho baseado em rótulos. Por exemplo, você pode instalar esse fluxo de trabalho e dizer aos usuários para aplicar um dos vários rótulos a qualquer namespaces que eles querem proteger, dependendo do nível de proteção que eles precisam. Isso permite que os usuários criem o namespace com um desses rótulos, e eles não precisam notificar um administrador. Seu novo namespace e todos os aplicativos dentro dele são protegidos automaticamente.

Crie um backup programado de todos os namespaces

Você pode criar um backup agendado de todos os namespaces em um cluster usando o fluxo de trabalho completo de backup do cluster.

Passos

1. Transfira os seguintes ficheiros para uma máquina que tenha acesso à rede ao cluster:
 - ["Arquivo CRD Components.yaml"](#)
 - ["protectCluster.py Python script"](#)
2. Para configurar e instalar o kit de ferramentas, ["siga as instruções incluídas"](#).

Crie um backup programado de namespaces específicos

Você pode criar um backup agendado de namespaces específicos por seus rótulos usando o fluxo de trabalho de backup baseado em rótulos.

Passos

1. Transfira os seguintes ficheiros para uma máquina que tenha acesso à rede ao cluster:
 - ["Arquivo CRD Components.yaml"](#)
 - ["protectCluster.py Python script"](#)
2. Para configurar e instalar o kit de ferramentas, ["siga as instruções incluídas"](#).

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.

Antes de começar

- * 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 snapshot ou backup se a restauração não for 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.
- **Drivers de classe de armazenamento suportados:** O Astra Control suporta a restauração de backups usando classes de armazenamento suportadas pelos seguintes drivers:
 - `ontap-nas`
 - `ontap-nas-economy`
 - `ontap-san`
 - `ontap-san-economy`
- * (Somente driver ONTAP-nas-Economy) backups e restaurações*: Antes de fazer backup ou restaurar um aplicativo que usa uma classe de armazenamento apoiada pelo `ontap-nas-economy` driver, verifique se o "[O diretório snapshot no back-end de storage do ONTAP está oculto](#)". A falha em ocultar esse diretório pode levar à perda de acesso ao aplicativo, especialmente se estiver usando NFSv3.



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.

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.
 - 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 também pode usar este procedimento para migrar um aplicativo para uma classe de armazenamento diferente.
 - 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**.

[Visualização técnica] Restaurar a partir da cópia de segurança utilizando um recurso personalizado (CR)

Você pode restaurar dados de um backup usando um arquivo de recurso personalizado (CR) para um namespace diferente ou para o namespace de origem original.

Restaurar a partir de uma cópia de segurança utilizando um CR

Passos

1. Crie o arquivo de recurso personalizado (CR) e nomeie-o `astra-control-backup-restore-cr.yaml`. Atualize os valores entre parêntesis> para corresponder ao seu ambiente Astra Control e à configuração de cluster:

- <CR_NAME>: O nome desta operação de CR; escolha um nome sensato para o seu ambiente.
- <APPVAULT_NAME>: O nome do AppVault onde o conteúdo de backup é armazenado.
- <BACKUP_PATH>: O caminho dentro do AppVault onde o conteúdo do backup é armazenado. Por exemplo:

```
ONTAP-S3_1343ff5e-4c41-46b5-af00/backups/schedule-20231213023800_94347756-9d9b-401d-a0c3
```

- <SOURCE_NAMESPACE>: O namespace de origem da operação de restauração.
- <DESTINATION_NAMESPACE>: O namespace de destino da operação de restauração.

```
apiVersion: astra.netapp.io/v1
kind: BackupRestore
metadata:
  name: <CR_NAME>
  namespace: astra-connector
spec:
  appVaultRef: <APPVAULT_NAME>
  appArchivePath: <BACKUP_PATH>
  namespaceMapping: [{"source": "<SOURCE_NAMESPACE>",
"destination": "<DESTINATION_NAMESPACE>"}]
```

Diretiva não resolvida no <stdin> - include:../_include/selective-restore-CR.adoc[]

1. Depois de preencher o `astra-control-backup-restore-cr.yaml` ficheiro com os valores corretos, aplique o CR:

```
kubectl apply -f astra-control-backup-restore-cr.yaml
```

Restaure do backup para o namespace original usando um CR

Passos

1. Crie o arquivo de recurso personalizado (CR) e nomeie-o `astra-control-backup-ipr-cr.yaml`. Atualize os valores entre parêntesis> para corresponder ao seu ambiente Astra Control e à configuração de cluster:
 - <CR_NAME>: O nome desta operação de CR; escolha um nome sensato para o seu ambiente.
 - <APPVAULT_NAME>: O nome do AppVault onde o conteúdo de backup é armazenado.

- <BACKUP_PATH>: O caminho dentro do AppVault onde o conteúdo do backup é armazenado. Por exemplo:

```
ONTAP-S3_1343ff5e-4c41-46b5-af00/backups/schedule-20231213023800_94347756-9d9b-401d-a0c3
```

```
apiVersion: astra.netapp.io/v1
kind: BackupInplaceRestore
metadata:
  name: <CR_NAME>
  namespace: astra-connector
spec:
  appVaultRef: <APPVAULT_NAME>
  appArchivePath: <BACKUP_PATH>
```

Diretiva não resolvida no <stdin> - include:../_include/selective-restore-CR.adoc[]

1. Depois de preencher o `astra-control-backup-ipr-cr.yaml` ficheiro com os valores corretos, aplique o CR:

```
kubectl apply -f astra-control-backup-ipr-cr.yaml
```

[Visualização técnica] Restaurar a partir de instantâneos utilizando um recurso personalizado (CR)

É possível restaurar dados de um snapshot usando um arquivo de recurso personalizado (CR) para um namespace diferente ou namespace de origem original.

Restaurar a partir de instantâneos usando um CR

Passos

1. Crie o arquivo de recurso personalizado (CR) e nomeie-o `astra-control-snapshot-restore-cr.yaml`. Atualize os valores entre parêntesis> para corresponder ao seu ambiente Astra Control e à configuração de cluster:

- `<CR_NAME>`: O nome desta operação de CR; escolha um nome sensato para o seu ambiente.
- `<APPVAULT_NAME>`: O nome do AppVault onde o conteúdo de backup é armazenado.
- `<BACKUP_PATH>`: O caminho dentro do AppVault onde o conteúdo do backup é armazenado. Por exemplo:

```
ONTAP-S3_1343ff5e-4c41-46b5-af00/backups/schedule-20231213023800_94347756-9d9b-401d-a0c3
```

- `<SOURCE_NAMESPACE>`: O namespace de origem da operação de restauração.
- `<DESTINATION_NAMESPACE>`: O namespace de destino da operação de restauração.

```
apiVersion: astra.netapp.io/v1
kind: SnapshotRestore
metadata:
  name: <CR_NAME>
  namespace: astra-connector
spec:
  appArchivePath: <BACKUP_PATH>
  appVaultRef: <APPVAULT_NAME>
  namespaceMapping: [{"source": "<SOURCE_NAMESPACE>",
"destination": "<DESTINATION_NAMESPACE>"}]
```

Diretiva não resolvida no <stdin> - include:../_include/selective-restore-CR.adoc[]

1. Depois de preencher o `astra-control-snapshot-restore-cr.yaml` ficheiro com os valores corretos, aplique o CR:

```
kubectl apply -f astra-control-snapshot-restore-cr.yaml
```

Restaure do instantâneo para o namespace original usando um CR

Passos

1. Crie o arquivo de recurso personalizado (CR) e nomeie-o `astra-control-snapshot-ipr-cr.yaml`. Atualize os valores entre parêntesis> para corresponder ao seu ambiente Astra Control e à configuração de cluster:
 - `<CR_NAME>`: O nome desta operação de CR; escolha um nome sensato para o seu ambiente.
 - `<APPVAULT_NAME>`: O nome do AppVault onde o conteúdo de backup é armazenado.

- <BACKUP_PATH>: O caminho dentro do AppVault onde o conteúdo do backup é armazenado. Por exemplo:

```
ONTAP-S3_1343ff5e-4c41-46b5-af00/backups/schedule-20231213023800_94347756-9d9b-401d-a0c3
```

```
apiVersion: astra.netapp.io/v1
kind: SnapshotInplaceRestore
metadata:
  name: <CR_NAME>
  namespace: astra-connector
spec:
  appArchivePath: <BACKUP_PATH>
  appVaultRef: <APPVAULT_NAME>
```

Diretiva não resolvida no <stdin> - include:../_include/selective-restore-CR.adoc[]

1. Depois de preencher o `astra-control-snapshot-ipr-cr.yaml` ficheiro com os valores corretos, aplique o CR:

```
kubectl apply -f astra-control-snapshot-ipr-cr.yaml
```

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. Após uma operação de clone ou restauração criar um novo namespace, 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.

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.



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 ter certeza de que atribuiu um intervalo padrão para a instância de nuvem que contém o cluster de origem. Se a instância da nuvem de origem não tiver um bucket padrão definido, a operação de clone entre clusters falhará.
- 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.

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.

- **Aplicativos suportados pelo ONTAP-nas-Economy:** Você não pode usar operações de clonagem se a classe de armazenamento do aplicativo for apoiada pelo `ontap-nas-economy` driver. Você pode, no entanto "[habilitar o backup e a restauração de operações de economia de ONTAP nas](#)", .
- **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. Após uma operação de clone ou restauração criar um novo namespace, 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.
- **Clones usam buckets padrão:**
 - Durante um backup de aplicativo ou restauração de aplicativo, você pode especificar um intervalo para usar. É necessário especificar um bucket padrão ao clonar entre clusters, mas especificar um bucket é opcional ao clonar no mesmo cluster.
 - Ao clonar entre clusters, a instância de nuvem que contém o cluster de origem da operação do clone precisa ter um conjunto de buckets padrão.
 - Não há opção de alterar buckets para um clone. Se você quiser controlar qual balde é usado, você pode "[alterar 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.

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 um namespace de destino.
- 

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 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, migrar um aplicativo de uma classe de armazenamento suportada por `ontap-nas-economy` para uma classe de armazenamento suportada pelo `ontap-nas` mesmo cluster ou copiar o aplicativo para outro cluster com uma classe de armazenamento suportada `ontap-nas-economy` pelo 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**.

Após uma operação de clone ou restauração criar um novo namespace, 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.

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 Service dá suporte aos seguintes tipos de ganchos de execução, com base nos momentos em que 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 gerenciar 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 são executados em alguns, mas não necessariamente em todos os contentores idênticos. 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 .



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.

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 demoram 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.

- O recurso ganchos de execução é desativado por padrão para novas implantações do Astra Control.
 - Você precisa ativar o recurso de ganchos de execução antes de usar ganchos de execução.
 - Os usuários proprietários ou administradores podem ativar ou desativar o recurso ganchos de execução para todos os usuários definidos na conta atual do Astra Control. [Ative o recurso ganchos de execução](#) Consulte e [Desative o recurso ganchos de execução](#) para obter instruções.
 - O status de capacitação do recurso é preservado durante as atualizações do Astra Control.
- 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).

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 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.

Ative o recurso ganchos de execução

Se você é um usuário proprietário ou administrador, você pode ativar o recurso ganchos de execução. Quando você ativa o recurso, todos os usuários definidos nesta conta do Astra Control podem usar ganchos de execução e exibir ganchos de execução e scripts de gancho existentes.

Passos

1. Vá para **aplicativos** e selecione o nome de um aplicativo gerenciado.
2. Selecione a guia **ganchos de execução**.
3. Selecione **Ativar ganchos de execução**.

A guia **Account > Feature settings** é exibida.

4. No painel **ganchos de execução**, selecione o menu de configurações.
5. Selecione **Ativar**.
6. Observe o aviso de segurança exibido.
7. Selecione **Sim, ative os ganchos de execução**.

Desative o recurso ganchos de execução

Se você é um usuário proprietário ou administrador, você pode desativar o recurso ganchos de execução para todos os usuários definidos nesta conta Astra Control. Você deve excluir todos os ganchos de execução existentes antes de desativar o recurso ganchos de execução. [Excluir um gancho de execução](#) Consulte para obter instruções sobre como excluir um gancho de execução existente.

Passos

1. Vá para **Account** e selecione a guia **Feature settings**.
2. Selecione a guia **ganchos de execução**.
3. No painel **ganchos de execução**, selecione o menu de configurações.
4. Selecione **Desativar**.
5. Observe o aviso que aparece.
6. Digite `disable` para confirmar que deseja desativar o recurso para todos os usuários.
7. Selecione **Sim, desativar**.

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. Certifique-se de que o recurso de ganchos de execução é **ativado**.
2. Vá para **conta**.
3. Selecione a guia **Scripts**.
4. Selecione **Adicionar**.
5. 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.
6. 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 e adicioná-lo ao Astra Control. [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. Certifique-se de que o recurso de ganchos de execução é [ativado](#).
2. Selecione **aplicativos** e, em seguida, selecione o nome de um aplicativo gerenciado.
3. Selecione a guia **ganchos de execução**.
4. Selecione **Adicionar**.
5. 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.
6. (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.

7. Quando terminar, selecione **seguinte**.
8. 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.

9. Selecione **seguinte**.

10. Reveja a configuração do gancho de execução.

11. 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"](#)

Ver a integridade da aplicação e da computação

Exibir um resumo da integridade do aplicativo e do cluster

Clique no **Dashboard** para ver uma visualização de alto nível dos seus aplicativos, clusters e sua integridade.

O mosaico Apps ajuda a identificar o seguinte:

- Quantos aplicativos você está gerenciando atualmente.
- Se esses aplicativos gerenciados estão saudáveis.
- Se os aplicativos estão totalmente protegidos (eles são protegidos se os backups recentes estiverem disponíveis).

Note que estes não são apenas números ou status - você pode detalhar cada um deles. Por exemplo, se os aplicativos não estiverem totalmente protegidos, você pode passar o Mouse sobre o ícone para identificar quais aplicativos não estão totalmente protegidos, o que inclui um motivo.

O bloco clusters fornece detalhes semelhantes sobre a integridade do cluster e você pode detalhar para obter mais detalhes como você pode com um aplicativo.

Ver a integridade e os detalhes dos clusters

Depois de adicionar clusters do Kubernetes ao Astra Control, você poderá ver detalhes sobre o cluster, como localização, nós de trabalho, volumes persistentes e classes de storage.

Passos

1. Na IU do Astra Control Service, 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:** As atividades relacionadas com o cluster.



Você também pode exibir informações de cluster a partir do Astra Control Service **Dashboard**. Na guia **clusters** em **Resumo de recursos**, você pode selecionar os clusters gerenciados, que o levam à página **clusters**. Depois de acessar a página **clusters**, siga as etapas descritas acima.

Veja a saúde e os detalhes de um aplicativo

Depois de começar a gerenciar uma aplicação, o Astra Control fornece detalhes sobre a aplicação que permite identificar seu status de comunicação (se o Astra Control pode se comunicar com a aplicação), seu status de proteção (se ele está totalmente protegido em caso de falha), os pods, storage persistente e muito mais.

Passos

1. Selecione **aplicativos** e, em seguida, selecione o nome de um aplicativo.
2. Encontre as informações que você está procurando:

Estado da aplicação

Fornecer um status que reflete se o Astra Control pode se comunicar com a aplicação.

Estado de proteção da aplicação

Fornecer um status de quão bem o aplicativo está protegido:

- **Totalmente protegido:** O aplicativo tem um agendamento de backup ativo e um backup bem-sucedido com menos de uma semana de idade
- **Parcialmente protegido:** O aplicativo tem um agendamento de backup ativo, um agendamento de snapshot ativo ou um backup ou snapshot bem-sucedido
- **Desprotegido:** Aplicativos que não estão totalmente protegidos ou parcialmente protegidos.

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

Visão geral

Informações sobre o estado dos pods associados ao aplicativo.

Proteção de dados

Permite configurar uma política de proteção de dados e exibir os snapshots e backups existentes.

Armazenamento

Mostra os volumes persistentes no nível do aplicativo. O estado de um volume persistente é da perspectiva do cluster do Kubernetes.

Recursos

Permite verificar quais recursos estão sendo armazenados em backup e gerenciados.

Atividade

As atividades do Astra Control relacionadas ao aplicativo.

Gerenciar buckets

É possível gerenciar os buckets que o Astra usa para backups e clones. Você pode adicionar buckets adicionais, remover buckets existentes e alterar o bucket padrão dos clusters do Kubernetes em uma instância de nuvem.

Somente proprietários e administradores podem gerenciar buckets.

Como o Astra Control usa buckets

Quando você começa a gerenciar o primeiro cluster de Kubernetes para uma instância de nuvem, o Astra Control Service cria o bucket inicial para isso "[instância de nuvem](#)".

Você pode designar manualmente um bucket como o bucket padrão para uma instância de nuvem. Se você fizer isso, o Astra Control Service usará esse bucket por padrão para backups e clones criados em qualquer cluster gerenciado nessa instância de nuvem (você pode selecionar um bucket diferente para backups). Se você executar um clone ativo de uma aplicação de qualquer um dos clusters gerenciados em uma instância de nuvem para outro cluster, o Astra Control Service usará o bucket padrão da instância de nuvem de origem para executar a operação de clone.

Você pode definir o mesmo intervalo que o bucket padrão para várias instâncias da nuvem.

Você pode selecionar de qualquer bucket ao criar uma política de proteção ou iniciar um backup ad-hoc.



O Astra Control Service verifica se um intervalo de destino está acessível antes de iniciar um backup ou um clone.

Ver buckets existentes

Veja a lista de buckets disponíveis no Astra Control Service para determinar seu status e identificar o bucket padrão (se definido) para sua instância de nuvem.

Um balde pode ter qualquer um dos seguintes estados:

Pendente

Depois de adicionar um bucket, ele começa no estado pendente enquanto o Astra Control o descobre.

Disponível

O balde está disponível para uso pelo Astra Control.

Removido

O balde não está operacional no momento. Passe o Mouse sobre o ícone de status para identificar qual é o problema.

Se um bucket estiver no estado removido, você ainda poderá defini-lo como o bucket padrão e atribuí-lo a

um cronograma de proteção. Mas se o intervalo não estiver no estado disponível no momento em que uma operação de proteção de dados for iniciada, essa operação falhará.

Passo

1. Vá para **Buckets**.

A lista de buckets disponíveis para o Astra Control Service é exibida.

Adicione um balde adicional

Você pode adicionar buckets adicionais a qualquer momento. Isso permite que você escolha entre buckets ao criar uma política de proteção ou iniciar um backup ad-hoc e permite alterar o bucket padrão usado por uma instância de nuvem.

Você pode adicionar os seguintes tipos de buckets:

- Amazon Web Services
- Genérico S3
- Google Cloud Platform
- Microsoft Azure
- NetApp ONTAP S3
- NetApp StorageGRID S3

Antes de começar

- Certifique-se de que sabe o nome de um balde existente.
- Garanta que você tenha credenciais para o bucket que fornecem ao Astra Control as permissões de que ele precisa para gerenciar o bucket.
- Se o seu bucket estiver no Microsoft Azure:
 - O bucket deve pertencer ao grupo de recursos chamado *astra-backup-rg*.
 - Se a configuração de desempenho da instância da conta de armazenamento do Azure estiver definida como "Premium", a configuração "tipo de conta Premium" deve ser definida como "Bloquear blobs".

Passos

1. Vá para **Buckets**.
2. Selecione **Adicionar** e siga as instruções para adicionar o intervalo.
 - **Tipo:** Escolha seu provedor de nuvem.
 - **Nome do bucket existente:** Insira o nome do bucket.
 - **Descrição:** Opcionalmente, insira uma descrição do balde.
 - **Conta de armazenamento** (somente Azure): Insira o nome da sua conta de armazenamento Azure. Esse bucket deve pertencer ao grupo de recursos chamado *astra-backup-rg*.
 - **Nome do servidor S3 ou endereço IP** (apenas tipos de bucket AWS e S3): Insira o nome de domínio totalmente qualificado do endpoint S3 que corresponde à sua região, sem `https://`. "[A documentação da Amazon](#)" Consulte para obter mais informações.
 - **Selecionar credenciais:** Insira as credenciais que fornecem ao Astra Control Service as permissões necessárias para gerenciar o bucket. As informações que você precisa fornecer variam de acordo com o tipo de balde.

- a. Selecione **Adicionar** para adicionar o intervalo.

Resultado

O Astra Control Service adiciona o balde. Agora você pode escolher esse intervalo ao criar uma política de proteção ou executar um backup ad-hoc. Você também pode definir esse bucket como o bucket padrão para uma instância da nuvem.

Altere o intervalo predefinido

Você pode alterar o intervalo padrão de uma instância da nuvem. O Astra Control Service usará esse bucket por padrão para backups e clones. Cada instância da nuvem tem seu próprio bucket padrão.



O Astra Control não atribui automaticamente um bucket padrão a nenhuma instância de nuvem. Você precisa definir manualmente um bucket padrão para uma instância de nuvem antes de executar operações de clone de aplicativo entre dois clusters.

Passos

1. Vá para **instâncias da nuvem**.
2. Selecione o menu de configuração na coluna **ações** para a instância de nuvem que você deseja editar.
3. Selecione **Editar**.
4. Na lista de buckets, selecione o bucket que você deseja criar o bucket padrão para essa instância da nuvem.
5. Selecione **Atualizar**.

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.
- Não é possível remover um bucket do WORM (write once read many) antes do período de retenção do fornecedor de nuvem do bucket expirar. Os baldes SEM-FIM são indicados com "bloqueado" junto ao nome do balde.

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 bucket não está sendo usado em nenhum backup agendado.

Se houver, você não será capaz de continuar.

Passos

1. Vá para **Buckets**.
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**.

[Tech Preview] Gerencie um bucket usando um recurso personalizado

Você pode adicionar um bucket usando um recurso personalizado Astra Control (CR) no cluster de aplicações. 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. Se você estiver usando o método de recurso personalizado, a funcionalidade de snapshots de aplicativo requer um intervalo.

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

O recurso personalizado do bucket do Astra Control é conhecido como AppVault. Este CR contém as configurações necessárias para que um balde seja usado em operações de proteção.

Antes de começar

- Garanta que você tenha um bucket acessível a partir dos clusters gerenciados pelo Astra Control Center.
- Certifique-se de que tem credenciais para o bucket.
- Certifique-se de que o balde é um 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. Crie o arquivo de recurso personalizado (CR) e nomeie-o (por exemplo, `astra-appvault.yaml`).
2. Configure os seguintes atributos:
 - **metadata.name:** (*obrigatório*) o nome do recurso personalizado do AppVault.
 - **Spec.prefix:** (*Opcional*) Um caminho que é prefixado aos nomes de todas as entidades armazenadas no AppVault.
 - **spec.providerConfig:** (*required*) armazena a configuração necessária para acessar o AppVault usando o provedor especificado.
 - **spec.providerCredentials:** (*obrigatório*) armazena referências a qualquer credencial necessária para acessar o AppVault usando o provedor especificado.
 - **spec.providerCredentials.valueFromSecret:** (*Opcional*) indica que o valor da credencial deve vir de um segredo.

- **Key:** *(obrigatório se valueFromSecret for usado)* a chave válida do segredo para selecionar.
 - **Name:** *(obrigatório se valueFromSecret for usado)* Nome do segredo contendo o valor para este campo. Deve estar no mesmo namespace.
- **spec.providerType:** *(obrigatório)* determina o que fornece o backup; por exemplo, o NetApp ONTAP S3 ou o Microsoft Azure.

Exemplo YAML:

```
apiVersion: astra.netapp.io/v1
kind: AppVault
metadata:
  name: astra-appvault
spec:
  providerType: generic-s3
  providerConfig:
    path: testpath
    endpoint: 192.168.1.100:80
    bucketName: bucket1
    secure: "false"
  providerCredentials:
    accessKeyID:
      valueFromSecret:
        name: s3-creds
        key: accessKeyID
    secretAccessKey:
      valueFromSecret:
        name: s3-creds
        key: secretAccessKey
```

3. Depois de preencher o `astra-appvault.yaml` ficheiro com os valores corretos, aplique o CR:

```
kubectl apply -f astra-appvault.yaml -n astra-connector
```



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](#)".

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 consultar 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](#)".

Gerencie sua conta

Configure a faturação

Você pode usar mais de um método para gerenciar a cobrança da conta do Astra Control Service. Se você estiver usando o Azure ou o Amazon AWS, poderá se inscrever em um plano do Astra Control Service por meio do Microsoft Azure Marketplace ou do AWS Marketplace. Quando você faz isso, você pode gerenciar seus detalhes de faturamento através do Marketplace. Ou, você pode se inscrever diretamente no NetApp. Se você se inscrever diretamente no NetApp, poderá gerenciar seus detalhes de cobrança por meio do Serviço Astra Control. Se você usar o Serviço Astra Control sem uma assinatura, você será automaticamente inscrito no Plano Gratuito.

O Plano Astra Control Service Free permite gerenciar até 10 namespaces em sua conta. Se você quiser gerenciar mais de 10 namespaces, precisará configurar o faturamento atualizando do Plano Gratuito para o Plano Premium ou inscreva-se no Azure Marketplace ou no AWS Marketplace.

Visão geral de faturamento

Há dois tipos de custos associados ao uso do serviço Astra Control: Cobranças da NetApp pelo serviço Astra Control e cobranças do seu fornecedor de nuvem por volumes persistentes e storage de objetos.

Cobrança do Astra Control Service

O Astra Control Service oferece três planos:

Plano grátis

Gerencie até 10 namespaces gratuitamente.

PayGo Premium

Gerencie uma quantidade ilimitada de namespaces em uma taxa específica, por namespace.

Subscrição Premium

Pré-pague a uma taxa com desconto com uma assinatura anual que permite gerenciar até 20 namespaces por pacote *namespace*. Entre em Contato com as vendas da NetApp para comprar quantos pacotes forem necessários para sua organização. Por exemplo, compre 3 pacotes para gerenciar 60 namespaces do Astra Control Service. Se você gerenciar mais namespaces do que o permitido pela sua assinatura anual, então você será cobrado pela taxa de sobrecarga dependente da assinatura por namespace extra. Se você ainda não tem uma conta Astra Control, comprar a assinatura Premium cria automaticamente uma conta Astra Control para você. Se você tiver um Plano Gratuito existente, então você será convertido automaticamente para a assinatura Premium.

Quando você cria uma conta Astra Control, você é automaticamente inscrito no Plano Gratuito. O Dashboard do Astra Control mostra quantos namespaces você está gerenciando atualmente dos 10 namespaces gratuitos que você tem permissão. O faturamento começa para um namespace quando o primeiro aplicativo que contém o namespace é gerenciado e pára para esse namespace quando o último aplicativo que contém o namespace não é gerenciado.

Se você tentar gerenciar um namespace 11th, o Astra Control notifica você de que você atingiu o limite do Plano livre. Em seguida, ele solicita que você atualize do Plano Gratuito para um Plano Premium. Você será cobrado de acordo com a taxa de sobrecarga dependente da assinatura por namespace extra.

Você pode fazer upgrade para um Plano Premium a qualquer momento. Depois de atualizar, o Astra Control começa a cobrar por *todos* namespaces na conta. Os primeiros 10 namespaces não ficam no Plano livre.

Cobrança do Google Cloud

Os volumes persistentes são suportados pelo NetApp Cloud Volumes Service e os backups de suas aplicações são armazenados em um bucket do Google Cloud Storage.

- ["Ver detalhes de preços para Cloud Volumes Service"](#).

Observe que o Astra Control Service é compatível com todos os tipos de serviço e níveis de serviço. O tipo de serviço que você usa depende do ["Região do Google Cloud"](#).

- ["Ver detalhes de preços dos buckets de storage do Google Cloud"](#).

Faturamento do Microsoft Azure

Volumes persistentes são suportados pelo Azure NetApp Files e os backups de suas aplicações são armazenados em um contêiner de Blob do Azure.

- ["Ver detalhes de preços para Azure NetApp Files"](#).
- ["Ver detalhes de preços para o armazenamento de Blobs do Microsoft Azure"](#).
- ["Veja os planos e preços do Astra Control Service no Azure Marketplace"](#)



A taxa de faturamento do Azure para o Serviço Astra Control é por hora e uma nova hora de faturamento começa após 29 minutos da hora de uso.

Cobrança do Amazon Web Services

Volumes persistentes são suportados pelo EBS ou FSX for NetApp ONTAP e os backups de seus aplicativos são armazenados em um bucket da AWS.

- ["Exibir detalhes de preços do Amazon Web Services"](#).

Inscreva-se no Astra Control Service no Azure Marketplace

Você pode se inscrever no Astra Control Service usando o Azure Marketplace. Sua conta e detalhes de faturamento são gerenciados pelo Marketplace.



Para ver um passo a passo em vídeo do processo de subscrição do Azure Marketplace, visite ["NetApp TV"](#).

Passos

1. Vá para ["Azure Marketplace"](#).
2. Selecione **Obtenha-o agora**.
3. Siga as instruções para assinar um plano.

Inscreva-se no Astra Control Service no AWS Marketplace

Você pode se inscrever no Astra Control Service usando o AWS Marketplace. Sua conta e detalhes de faturamento são gerenciados pelo Marketplace.

Passos

1. Vá para ["AWS Marketplace"](#).
2. Selecione **Ver opções de compra**.
3. Se for solicitado, faça login na sua conta da AWS ou crie uma nova conta.
4. Siga as instruções para assinar um plano.

Inscreva-se no Astra Control Service diretamente com NetApp

Você pode se inscrever no serviço Astra Control na IU do serviço Astra Control ou entrar em Contato com a NetApp Sales.

Faça upgrade do Plano Gratuito para o Plano Premium PayGo

Atualize seu plano de cobrança a qualquer momento para começar a gerenciar mais de 10 namespaces do Astra Control pagando conforme o uso. Tudo o que você precisa é de um cartão de crédito válido.

Passos

1. Selecione **conta** e, em seguida, selecione **faturamento**.
2. Em **Plans**, vá para **Premium PayGo** e selecione **Upgrade now**.
3. Forneça detalhes de pagamento para um cartão de crédito válido e selecione **Upgrade to Premium Plan**.



O Astra Control enviará um e-mail para você se o cartão de crédito estiver prestes a expirar.

Resultado

Agora você pode gerenciar mais de 10 namespaces. O Astra Control começa a cobrar por *todos* namespaces que você está gerenciando atualmente.

Faça upgrade do Plano Gratuito para a assinatura Premium

Entre em Contato com as vendas da NetApp para pagar antecipadamente com uma taxa com desconto com uma assinatura anual.

Passos

1. Selecione **conta** e, em seguida, selecione **faturamento**.
2. Em **Plans**, vá para **Premium Subscription** e selecione **Contact Sales**.
3. Forneça detalhes à equipe de vendas para iniciar o processo.

Resultado

Um representante de vendas da NetApp entrará em Contato com você para processar seu pedido de compra. Após a conclusão do pedido, o Astra Control refletirá seu plano atual na guia **faturamento**.

Veja seus custos atuais e histórico de faturamento

O Astra Control mostra seus custos mensais atuais, bem como um histórico detalhado de cobrança por namespace. Se você se inscreveu em um plano por meio de um Marketplace, o histórico de faturamento não estará visível (mas você poderá visualizá-lo fazendo login no Marketplace).

Passos

1. Selecione **conta** e, em seguida, selecione **faturamento**.

Seus custos atuais aparecem sob a visão geral de faturamento.

2. Para ver o histórico de faturação por namespace, selecione **Histórico de faturação**.

O Astra Control mostra os minutos de uso e o custo de cada namespace. Um minuto de uso é de quantos minutos o Astra Control gerenciou seu namespace durante um período de faturamento.

3. Selecione a lista pendente para selecionar um mês anterior.

Altere o cartão de crédito para Premium PayGo

Se necessário, você pode alterar o cartão de crédito que o Astra Control tem registrado para cobrança.

Passos

1. Selecione **conta > faturamento > método de pagamento**.
2. Selecione o ícone de configuração.
3. Modificar o cartão de crédito.

Notas importantes

- Seu plano de cobrança é por conta Astra Control.

Se você tiver várias contas, cada uma tem seu próprio plano de faturamento.

- Sua fatura do Astra Control inclui cobranças pelo gerenciamento de namespaces. Você será cobrado separadamente pelo seu fornecedor de nuvem pelo back-end de storage para volumes persistentes.

["Saiba mais sobre os preços do Astra Control"](#).

- Cada período de faturamento termina no último dia do mês.
- Você não pode fazer o downgrade de um Plano Premium para o Plano Gratuito.

Convide e remova usuários

Convide os usuários a ingressar na sua conta Astra Control e remova os usuários que não deveriam mais ter acesso à conta.

Convide usuários

Os proprietários e administradores de contas podem convidar outros usuários para ingressar na conta Astra Control.

Passos

1. Certifique-se de que o utilizador tem um ["Login BlueXP"](#).
2. Selecione **conta**.
3. Na guia **usuários**, selecione **convidar**.
4. Introduza o nome do utilizador, o endereço de correio eletrônico e a respetiva função.

Observe o seguinte:

- O endereço de e-mail deve corresponder ao endereço de e-mail que o usuário usou para se inscrever no BlueXP .
 - Cada função fornece as seguintes permissões:
 - Um **proprietário** tem permissões de administrador e pode excluir contas.
 - Um **Admin** tem permissões de Membro e pode convidar outros usuários.
 - Um **Membro** pode gerenciar totalmente aplicativos e clusters.
 - Um **Viewer** pode visualizar recursos.
5. Para adicionar restrições a um utilizador com uma função Membro ou Visualizador, ative a caixa de verificação **restringir função a restrições**.

Para obter mais informações sobre como adicionar restrições, ["Gerenciar funções"](#) consulte .

6. Para convidar outro usuário, selecione **Adicionar outro usuário** e insira informações para o novo usuário.

Você pode convidar até 10 usuários de cada vez. Você pode navegar entre os usuários que está convidando no lado esquerdo da caixa de diálogo **convidar usuários**.

7. Selecione **convidar utilizadores**.

Resultado

O usuário ou os usuários receberão um e-mail que os convida a ingressar na sua conta.

Altere a função de um usuário

Um proprietário de conta pode alterar a função de todos os usuários, enquanto um Administrador de conta pode alterar a função de usuários que têm a função de Administrador, Membro ou Visualizador.

Passos

1. Selecione **conta**.
2. Na guia **usuários**, selecione o menu na coluna **ações** para o usuário.
3. Selecione **Editar função**.
4. Selecione uma nova função.
5. Para adicionar restrições a um utilizador com uma função Membro ou Visualizador, ative a caixa de verificação **restringir função a restrições**.

Para obter mais informações sobre como adicionar restrições, "[Gerenciar funções](#)" consulte .

6. Selecione **Confirm**.

Resultado

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

Remover usuários

Um usuário com a função proprietário pode remover outros usuários da conta a qualquer momento.

Passos

1. Selecione **conta**.
2. Na guia **usuários**, selecione os usuários que você deseja remover.
3. Selecione o menu na coluna **ações** e selecione **Remover usuário**.
4. Quando for solicitado, confirme a exclusão digitando "remove" e selecione **Yes, Remove User**.

Resultado

O Astra Control remove o usuário da conta.

Gerenciar funções

Você pode gerenciar funções adicionando restrições de namespace e restringindo funções de usuário a essas restrições. Isso permite que você controle o acesso a recursos dentro de sua organização. Você pode usar a IU do Astra Control ou "[API Astra Control](#)" gerenciar funções.

Adicione uma restrição de namespace a uma função

Um usuário Admin ou proprietário pode adicionar restrições de namespace.

Passos

1. Na área de navegação **Gerenciar sua conta**, selecione **conta**.
2. Selecione a guia **usuários**.
3. Na coluna **ações**, selecione o botão de menu para um usuário com a função Membro ou Visualizador.

4. Selecione **Editar função**.
5. Ative a caixa de verificação **restringir função a restrições**.

A caixa de verificação só está disponível para funções Membro ou Visualizador. Você pode selecionar uma função diferente na lista suspensa **Role**.

6. Selecione **Adicionar restrição**.

Você pode ver a lista de restrições disponíveis por namespace ou por rótulo de namespace.

7. Na lista suspensa **tipo de restrição**, selecione **namespace do Kubernetes** ou **rótulo do namespace do Kubernetes** dependendo de como seus namespaces são configurados.
8. Selecione um ou mais namespaces ou rótulos da lista para compor uma restrição que restrinja funções a esses namespaces.
9. Selecione **Confirm**.

A página **Editar função** exibe a lista de restrições que você escolheu para essa função.

10. Selecione **Confirm**.

Na página **conta**, você pode visualizar as restrições para qualquer função de Membro ou Visualizador na coluna **função**.



Se você habilitar restrições para uma função e selecionar **Confirm** sem adicionar nenhuma restrição, a função será considerada como tendo restrições completas (a função é negada acesso a quaisquer recursos atribuídos a namespaces).

Remova uma restrição de namespace de uma função

Um usuário Admin ou proprietário pode remover uma restrição de namespace de uma função.

Passos

1. Na área de navegação **Gerenciar sua conta**, selecione **conta**.
2. Selecione a guia **usuários**.
3. Na coluna **ações**, selecione o botão de menu para um usuário com a função Membro ou Visualizador que tem restrições ativas.
4. Selecione **Editar função**.

A caixa de diálogo **Editar função** exibe as restrições ativas para a função.

5. Selecione **X** à direita da restrição que você precisa remover.
6. Selecione **Confirm**.

Para mais informações

- ["Funções de usuário e namespaces"](#)

Adicione e remova credenciais

Adicione e remova as credenciais do provedor de nuvem da sua conta a qualquer

momento. O Astra Control usa essas credenciais para descobrir um cluster Kubernetes e as aplicações no cluster e provisionar recursos em seu nome.

Observe que todos os usuários do Astra Control compartilham os mesmos conjuntos de credenciais.

Adicionar credenciais

A maneira mais comum de adicionar credenciais ao Astra Control é quando você gerencia clusters, mas também pode adicionar credenciais a partir da página da conta. As credenciais estarão disponíveis para você escolher quando você gerenciar clusters adicionais do Kubernetes.

Antes de começar

- Para o Amazon Web Services, você deve ter a saída JSON das credenciais para a conta do IAM usada para criar o cluster. "[Saiba como configurar um usuário do IAM](#)".
- Para o GKE, você deve ter o arquivo de chave de conta de serviço para uma conta de serviço que tenha as permissões necessárias. "[Saiba como configurar uma conta de serviço](#)".
- Para AKS, você deve ter o arquivo JSON que contém a saída da CLI do Azure quando você criou o responsável pelo serviço. "[Saiba como configurar um diretor de serviço](#)".

Você também precisará do ID de assinatura do Azure, se não o tiver adicionado ao arquivo JSON.

Passos

1. Selecione **conta > credenciais**.
2. Selecione **Adicionar credenciais**.
3. Selecione **Microsoft Azure**.
4. Selecione **Google Cloud Platform**.
5. Selecione **Amazon Web Services**.
6. Insira um nome para as credenciais que as distingue de outras credenciais no Astra Control.
7. Forneça as credenciais necessárias.
8. **Microsoft Azure**: Forneça ao Astra Control detalhes sobre o seu principal de serviço do Azure, carregando um arquivo JSON ou colando o conteúdo desse arquivo JSON da sua área de transferência.

O arquivo JSON deve conter a saída da CLI do Azure quando você criou o principal do serviço. Ele também pode incluir seu ID de assinatura para que ele seja adicionado automaticamente ao Astra Control. Caso contrário, você precisa inserir manualmente o ID após fornecer o JSON.

9. **Google Cloud Platform**: Forneça o arquivo de chave da conta de serviço do Google Cloud carregando o arquivo ou colando o conteúdo da área de transferência.
10. **Amazon Web Services**: Forneça as credenciais de usuário do Amazon Web Services IAM ao carregar o arquivo ou colando o conteúdo da área de transferência.
11. Selecione **Adicionar credenciais**.

Resultado

As credenciais agora estão disponíveis para seleção quando você adiciona um cluster ao Astra Control.

Remover credenciais

Remova as credenciais de uma conta a qualquer momento. Só deve remover credenciais após "[desgerenciar](#)".

todos os clusters", a menos que esteja a rodar credenciais ([Gire as credenciais](#) consulte a).



O primeiro conjunto de credenciais que você adiciona ao Astra Control está sempre em uso porque o Astra Control usa as credenciais para autenticar no bucket do backup. É melhor não remover essas credenciais.

Passos

1. Selecione **conta > credenciais**.
2. Selecione a lista suspensa na coluna **Estado** para obter as credenciais que deseja remover.
3. Selecione **Remover**.
4. Digite o nome das credenciais para confirmar a exclusão e selecione **Sim, Remover credenciais**.

Resultado

O Astra Control remove as credenciais da conta.

Gire as credenciais

Você pode girar credenciais em sua conta. Se você girar credenciais, gire-as durante uma janela de manutenção quando nenhum backup estiver em andamento (agendado ou sob demanda).

Passos

1. Remova as credenciais existentes seguindo as etapas em [Remover credenciais](#).
2. Adicione as novas credenciais seguindo as etapas em [Adicionar credenciais](#).
3. Atualize todos os buckets para usar as novas credenciais:
 - a. Na navegação à esquerda, selecione **Buckets**.
 - b. Selecione a lista suspensa na coluna **ações** para o intervalo que você deseja editar.
 - c. Selecione **Editar**.
 - d. Na seção **Selecionar credenciais**, escolha as novas credenciais adicionadas ao Astra Control.
 - e. Selecione **Atualizar**.
 - f. Repita os passos **b** a **e** para quaisquer baldes restantes no seu sistema.

Resultado

O Astra Control começa a usar as novas credenciais do fornecedor de nuvem.

Monitorar a atividade da conta

Você pode ver detalhes sobre as atividades na sua conta do Astra Control. Por exemplo, quando novos usuários foram convidados, quando um cluster foi adicionado ou quando um snapshot foi tirado. Você também pode exportar a atividade da sua conta para um arquivo CSV.

Ver todas as atividades da conta no Astra Control

1. Selecione **atividade**.
2. Use os filtros para restringir a lista de atividades ou use a caixa de pesquisa para encontrar exatamente o que você está procurando.
3. Selecione **Exportar para CSV** para fazer o download da atividade da sua conta para um arquivo CSV.

Exibir atividade da conta para um aplicativo específico

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

Ver atividade da conta dos clusters

1. Selecione **clusters** e, em seguida, selecione o nome do cluster.
2. Selecione **atividade**.

Ver e gerir notificações

O Astra Control notifica você quando as ações forem concluídas ou falhadas. Por exemplo, você verá uma notificação se um backup de um aplicativo for concluído com êxito.

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

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

Passos

1. 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**.

Feche a sua conta

Se você não precisar mais de sua conta Astra Control, poderá fechá-la a qualquer momento.



Os buckets que o Astra Control criou automaticamente serão excluídos automaticamente quando você fechar sua conta.

Passos

1. "[Desgerencie todas as aplicações e clusters](#)".
2. "[Remover credenciais do Astra Control](#)".
3. Selecione **conta > faturamento > método de pagamento**.
4. Selecione **Fechar conta**.
5. Introduza o nome da sua conta e confirme para fechar a conta.

Gerenciar instâncias de nuvem

Uma instância de nuvem é um domínio exclusivo dentro de um provedor de nuvem. Você pode criar várias instâncias de nuvem para cada fornecedor de nuvem e cada instância

de nuvem tem seu próprio nome, credenciais e clusters associados.

Você cria uma instância de nuvem quando adiciona um novo cluster ao Astra Control. Você pode editar uma instância da nuvem para alterar seu nome ou bucket padrão usando a IU do Astra Control e executar outras ações com a instância de nuvem usando a API Astra Control.

Adicione uma instância de nuvem

Você pode adicionar uma nova instância de nuvem ao adicionar um novo cluster ao Astra Control. "[Comece a gerenciar clusters de Kubernetes a partir do Astra Control Service](#)" Consulte para obter mais informações.

Edite uma instância de nuvem

Você pode modificar uma instância de nuvem existente para um provedor de nuvem.

Passos

1. Vá para **instâncias da nuvem**.
2. Na lista de instâncias de nuvem, selecione o menu **ações** para a instância de nuvem que deseja editar.
3. Selecione **Editar**.

Nesta página, você pode atualizar o nome e o bucket padrão da instância da nuvem.



Cada instância de nuvem no Astra Control precisa ter um nome exclusivo.

Gire as credenciais para uma instância de nuvem

Você pode usar a API Astra Control para girar as credenciais para uma instância de nuvem. Para saber mais, "[Vá para a documentação de automação do Astra](#)".

Remover uma instância da nuvem

Você pode usar a API Astra Control para remover uma instância de nuvem de um fornecedor de nuvem. Para saber mais, "[Vá para a documentação de automação do Astra](#)".

Habilite o Astra Control Provisioner

O Astra Trident versões 23,10 e posteriores incluem a opção de usar o Astra Control Provisioner, que permite que usuários licenciados do Astra Control acessem o recurso avançado de provisionamento de storage. O Astra Control Provisioner fornece essa funcionalidade estendida, além da funcionalidade padrão baseada em CSI Astra Trident. Você pode usar este procedimento para ativar e instalar o Astra Control Provisioner.

Sua assinatura do Astra Control Service inclui automaticamente a licença para uso do Astra Control Provisioner.

Nas próximas atualizações do Astra Control, o parceiro Astra Control substituirá o Astra Trident como provisionador de storage e orquestrador e será obrigatório para uso do Astra Control. Por causa disso, é altamente recomendável que os usuários do Astra Control ativem o Astra Control Provisioner. O Astra Trident continuará a ser de código aberto e será lançado, mantido, suportado e atualizado com o novo CSI e outros recursos do NetApp.

Como sei se preciso habilitar o Astra Control Provisioner?

Se você adicionar um cluster ao Astra Control Service que não tenha o Astra Trident instalado anteriormente, o cluster será marcado como `Eligible`. Depois de "[Adicione o cluster ao Astra Control](#)" você , o Astra Control Provisioner será ativado automaticamente.

Se o cluster não estiver marcado `Eligible`, ele será marcado `Partially eligible` por uma das seguintes opções:

- Ele está usando uma versão mais antiga do Astra Trident
- Ele está usando um Astra Trident 23,10 que ainda não tem a opção de provisionador habilitada
- É um tipo de cluster que não permite a ativação automática

Para `Partially eligible` casos, use estas instruções para ativar manualmente o Astra Control Provisioner para seu cluster.

The screenshot shows the 'Add cluster' wizard in the Astra Control console. The wizard is at 'STEP 2/4: CLUSTER'. It shows a list of clusters with columns for 'Cluster', 'Location', and 'Eligibility'. One cluster, 'sandbox-ragnarok-aks-03', is marked as 'Partially eligible' with a tooltip that says 'Configuration required Failed to detect Astra Control Provisioner on cluster'. Other clusters are marked as 'Eligible'. A warning banner at the top indicates 'Some Kubernetes cluster(s) below have private networking.' Navigation buttons for 'Back' and 'Next' are at the bottom.

Antes de ativar o Astra Control Provisioner

Se você já tiver um Astra Trident sem o parceiro Astra Control e quiser habilitar o parceiro Astra Control, faça o seguinte primeiro:

- **Se você tiver o Astra Trident instalado, confirme que sua versão está dentro de uma janela de quatro versões:** Você pode fazer uma atualização direta para o Astra Trident 24,02 com o Astra Control Provisioner se o seu Astra Trident estiver dentro de uma janela de quatro versões da versão 24,02. Por exemplo, você pode fazer o upgrade diretamente do Astra Trident 23,04 para o 24,02.
- **Confirme que seu cluster tem uma arquitetura de sistema AMD64:** A imagem Astra Control Provisioner é fornecida em arquiteturas de CPU AMD64 e ARM64, mas apenas AMD64 é compatível com Astra Control.

Passos

1. Acesse o Registro de imagem do NetApp Astra Control:
 - a. Faça login na IU do Astra Control Service e Registre sua ID de conta do Astra Control.
 - i. Selecione o ícone de figura no canto superior direito da página.
 - ii. Selecione **Acesso à API**.
 - iii. Anote o seu ID de conta.
 - b. Na mesma página, selecione **Generate API token** e copie a cadeia de token da API para a área de transferência e salve-a no seu editor.
 - c. Faça login no Registro Astra Control usando seu método preferido:

```
docker login cr.astra.netapp.io -u <account-id> -p <api-token>
```

```
crane auth login cr.astra.netapp.io -u <account-id> -p <api-token>
```

2. (Apenas registros personalizados) siga estes passos para mover a imagem para o seu registro personalizado. Se você não estiver usando um Registro, siga as etapas do operador Trident no [próxima seção](#).



Você pode usar Podman em vez de Docker para os seguintes comandos. Se você estiver usando um ambiente Windows, o PowerShell é recomendado.

Docker

- a. Extraia a imagem Astra Control Provisioner do Registro:



A imagem puxada não suportará múltiplas plataformas e só suportará a mesma plataforma que o host que puxou a imagem, como o Linux AMD64.

```
docker pull cr.astra.netapp.io/astra/trident-acp:24.02.0
--platform <cluster platform>
```

Exemplo:

```
docker pull cr.astra.netapp.io/astra/trident-acp:24.02.0
--platform linux/amd64
```

- b. Marque a imagem:

```
docker tag cr.astra.netapp.io/astra/trident-acp:24.02.0
<my_custom_registry>/trident-acp:24.02.0
```

- c. Envie a imagem para o seu registro personalizado:

```
docker push <my_custom_registry>/trident-acp:24.02.0
```

Grua

- a. Copie o manifesto Astra Control Provisioner para o seu Registro personalizado:

```
crane copy cr.astra.netapp.io/astra/trident-acp:24.02.0
<my_custom_registry>/trident-acp:24.02.0
```

3. Determine se o método de instalação original do Astra Trident usou um.
4. Ative o Astra Control Provisioner no Astra Trident usando o método de instalação que você usou originalmente:

Operador do Astra Trident

- a. "Baixe o instalador do Astra Trident e extraia-o."
- b. Siga estas etapas se você ainda não tiver instalado o Astra Trident ou se tiver removido o operador da sua implantação original do Astra Trident:
 - i. Crie o CRD:

```
kubectl create -f
deploy/crds/trident.netapp.io_tridentorchestrators_crd_post1.1
6.yaml
```

- ii. Crie o namespace Trident (`kubectl create namespace trident`) ou confirme se o namespace Trident ainda existe (`kubectl get all -n trident`). Se o namespace tiver sido removido, crie-o novamente.
- c. Atualize o Astra Trident para 24.02.0:



Para clusters que executam o Kubernetes 1,24 ou anterior, `bundle_pre_1_25.yaml` use o `.`. Para clusters que executam o Kubernetes 1,25 ou posterior, `bundle_post_1_25.yaml` use o `.`.

```
kubectl -n trident apply -f trident-installer/deploy/<bundle-
name.yaml>
```

- d. Verifique se o Astra Trident está em execução:

```
kubectl get torc -n trident
```

Resposta:

```
NAME          AGE
trident       21m
```

- e. se você tem um Registro que usa segredos, crie um segredo para usar para puxar a imagem Astra Control Provisioner:

```
kubectl create secret docker-registry <secret_name> -n trident
--docker-server=<my_custom_registry> --docker-username=<username>
--docker-password=<token>
```

- f. Edite o TridentOrchestrator CR e faça as seguintes edições:

```
kubectl edit torc trident -n trident
```

- i. Defina um local de Registro personalizado para a imagem Astra Trident ou extraia-a do Registro Astra Control (`tridentImage: <my_custom_registry>/trident:24.02.0`ou `tridentImage: netapp/trident:24.02.0`).
- ii. Ative o Astra Control Provisioner (`enableACP: true`).
- iii. Defina o local de Registro personalizado para a imagem Astra Control Provisioner ou extraia-a do Registro Astra Control (`acpImage: <my_custom_registry>/trident-acp:24.02.0`ou `acpImage: cr.astra.netapp.io/astra/trident-acp:24.02.0`).
- iv. Se tiver estabelecido [a imagem puxa segredos](#) anteriormente neste procedimento, pode defini-los aqui (`imagePullSecrets: - <secret_name>`). Use o mesmo nome secreto que você estabeleceu nas etapas anteriores.

```
apiVersion: trident.netapp.io/v1
kind: TridentOrchestrator
metadata:
  name: trident
spec:
  debug: true
  namespace: trident
  tridentImage: <registry>/trident:24.02.0
  enableACP: true
  acpImage: <registry>/trident-acp:24.02.0
  imagePullSecrets:
    - <secret_name>
```

- g. Salve e saia do arquivo. O processo de implantação começará automaticamente.
- h. Verifique se o operador, a implantação e as replicaset são criados.

```
kubectl get all -n trident
```



Deve haver apenas **uma instância** do operador em um cluster do Kubernetes. Não crie várias implantações do operador Astra Trident.

- i. Verifique se o `trident-acp` contentor está em execução e se `acpVersion` está `24.02.0` com um status de `Installed`:

```
kubectl get torc -o yaml
```

Resposta:

```
status:
  acpVersion: 24.02.0
  currentInstallationParams:
    ...
    acpImage: <registry>/trident-acp:24.02.0
    enableACP: "true"
    ...
  ...
  status: Installed
```

tridentctl

- "Baixe o instalador do Astra Trident e extraia-o".
- "Se você tiver um Astra Trident existente, desinstale-o do cluster que o hospeda".
- Instalar o Astra Trident com a previsão de controle Astra ativada (`--enable-acp=true`):

```
./tridentctl -n trident install --enable-acp=true --acp
-image=mycustomregistry/trident-acp:24.02
```

- Confirme se o Astra Control Provisioner foi ativado:

```
./tridentctl -n trident version
```

Resposta:

```
+-----+-----+-----+ | SERVER
VERSION | CLIENT VERSION | ACP VERSION | +-----+
+-----+-----+-----+ | 24.02.0 | 24.02.0 | 24.02.0. |
+-----+-----+-----+
```

Leme

- Se tiver o Astra Trident 23.07.1 ou anterior instalado, "**desinstalar**" o operador e outros componentes.
- Se o cluster do Kubernetes estiver executando o 1,24 ou anterior, exclua a psp:

```
kubectl delete psp tridentoperatorpod
```

- Adicione o repositório Astra Trident Helm:


```
helm repo add netapp-trident https://netapp.github.io/trident-helm-chart
```

d. Atualize o gráfico Helm:

```
helm repo update netapp-trident
```

Resposta:

```
Hang tight while we grab the latest from your chart
repositories...
...Successfully got an update from the "netapp-trident" chart
repository
Update Complete. ☐Happy Helming!☐
```

e. Liste as imagens:

```
./tridentctl images -n trident
```

Resposta:

```
| v1.28.0           | netapp/trident:24.02.0|
|                  | docker.io/netapp/trident-
autosupport:24.02 |
|                  | registry.k8s.io/sig-storage/csi-
provisioner:v4.0.0|
|                  | registry.k8s.io/sig-storage/csi-
attacher:v4.5.0 |
|                  | registry.k8s.io/sig-storage/csi-
resizer:v1.9.3 |
|                  | registry.k8s.io/sig-storage/csi-
snapshotter:v6.3.3|
|                  | registry.k8s.io/sig-storage/csi-node-
driver-registrar:v2.10.0 |
|                  | netapp/trident-operator:24.02.0 (optional)
```

f. Certifique-se de que o Trident-Operator 24.02.0 está disponível:

```
helm search repo netapp-trident/trident-operator --versions
```

Resposta:

NAME	CHART VERSION	APP VERSION	
DESCRIPTION			
netapp-trident/trident-operator	100.2402.0	24.02.0	A

g. Utilize `helm install` e execute uma das seguintes opções que incluem estas definições:

- Um nome para o local de implantação
- A versão Astra Trident
- O nome da imagem Astra Control Provisioner
- A bandeira para habilitar o provisionador
- (Opcional) Um caminho de Registro local. Se você estiver usando um Registro local, o ["Imagens de Trident"](#) pode estar localizado em um Registro ou Registros diferentes, mas todas as imagens CSI devem estar localizadas no mesmo Registro.
- O namespace Trident

Opções

- Imagens sem registo

```
helm install trident netapp-trident/trident-operator --version
100.2402.0 --set acpImage=cr.astra.netapp.io/astra/trident-
acp:24.02.0 --set enableACP=true --set operatorImage=netapp/trident-
operator:24.02.0 --set
tridentAutosupportImage=docker.io/netapp/trident-autosupport:24.02
--set tridentImage=netapp/trident:24.02.0 --namespace trident
```

- Imagens em um ou mais Registros

```
helm install trident netapp-trident/trident-operator --version
100.2402.0 --set acpImage=<your-registry>:<acp image> --set
enableACP=true --set imageRegistry=<your-registry>/sig-storage --set
operatorImage=netapp/trident-operator:24.02.0 --set
tridentAutosupportImage=docker.io/netapp/trident-autosupport:24.02
--set tridentImage=netapp/trident:24.02.0 --namespace trident
```

Você pode usar `helm list` para revisar detalhes de instalação, como nome, namespace, gráfico, status, versão do aplicativo e número de revisão.

Se você tiver algum problema na implantação do Trident usando o Helm, execute este comando para desinstalar completamente o Astra Trident:

```
./tridentctl uninstall -n trident
```

Não ["Remova completamente CRDS Astra Trident"](#) como parte da sua desinstalação antes de tentar ativar o Astra Control Provisioner novamente.

Resultado

A funcionalidade Astra Control Provisioner está ativada e você pode usar todos os recursos disponíveis para a versão em execução.

Depois que o Astra Control Provisioner for instalado, o cluster que hospeda o provisionador na IU do Astra Control mostrará um `ACP version` número de versão instalado em vez `Trident version` de campo e atual.

-📶- CLUSTER STATUS

✔️ Available

Version v1.24.9+rke2r2	Managed 2024/03/15 17:32 UTC	Kube-system namespace UID ██████████████████████████████████████	ACP Version ██████████
Private route identifier ██████████████████████... #	Cloud instance private ✎	Default bucket astra-bucket1 (inherited) ✎	

[Overview](#) [Namespaces](#) [Storage](#) [Activity](#)

Para mais informações

- ["O Astra Trident atualiza a documentação"](#)

Desgerenciar aplicativos e clusters

Remova do Astra Control todas as aplicações ou clusters que você não quiser mais gerenciar.

Pare de gerenciar um aplicativo

Pare de gerenciar aplicações que não deseja mais fazer backup, snapshot ou clonar a partir do Astra Control.

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 aplicativo**.

Resultado

O Astra Control deixa de gerenciar a aplicação.

Pare de gerenciar um cluster

Pare de gerenciar o cluster que não deseja mais gerenciar a partir do Astra Control.



Antes de desgerenciar o cluster, você deve desgerenciar os aplicativos associados ao cluster.

Como prática recomendada, recomendamos que você remova o cluster do Astra Control antes de excluí-lo pelo GCP.

Quando você desgerencia um cluster:

- Essa ação impede que o cluster seja gerenciado pelo Astra Control. Ele não faz alterações na configuração do cluster e não exclui o cluster.
- O Astra Control Provisioner ou o Astra Trident não serão desinstalados do cluster. ["Saiba como desinstalar o Astra Trident"](#).

Passos

1. Selecione **clusters**.
2. Marque a caixa de seleção do cluster que você não deseja mais gerenciar.
3. No menu de opções na coluna **ações**, selecione **Desgerenciar**.
4. Confirme se deseja desgerenciar o cluster e selecione **Sim, desgerenciar**.

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.

Exclusão de clusters do seu provedor de nuvem

Antes de excluir um cluster do Kubernetes que tenha volumes persistentes (PV) residentes em classes de storage do NetApp, primeiro exclua as declarações de volume persistente (PVC) seguindo um dos métodos abaixo. Excluir o PVC e o PV antes de excluir o cluster garante que você não receba contas inesperadas do seu provedor de nuvem.

- **Método nº 1:** Exclua os namespaces da carga de trabalho do aplicativo do cluster. *Não* exclua o namespace Trident.
- **Método nº 2:** Exclua os PVCs e os pods, ou a implantação onde os PVS são montados.

Quando você gerencia um cluster de Kubernetes a partir do Astra Control, as aplicações nesse cluster usam seu provedor de nuvem como back-end de storage para volumes persistentes. Se você excluir o cluster do seu provedor de nuvem sem primeiro remover os PVS, os volumes de back-end serão *não* excluídos junto com o cluster.

Usar um dos métodos acima excluirá os PVS correspondentes do cluster. Certifique-se de que não existem PVS residentes nas classes de armazenamento do NetApp no cluster antes de excluí-lo.

Se você não excluiu os volumes persistentes antes de excluir o cluster, precisará excluir manualmente os

volumes de back-end do seu provedor de nuvem.

Implantar uma instância autogerenciada do Astra Control

Se você quiser uma instância autogerenciada do Astra Control que resida na sua rede, é possível implantar o Astra Control Center diretamente do Astra Control Service.

Passos

1. Na área primeiros passos do Dashboard, selecione **Deploy a self-managed instance of Astra Control**.
2. Execute um dos seguintes procedimentos:
 - Gere um novo token de API selecionando **Generate**.
 - Cole em um token de API REST do Astra Control existente. Consulte o "[Documentação do Astra Automation](#)" para obter orientação sobre como gerar um token de API.
3. Siga as instruções na janela **Deploy Astra Control Center**.

Use o Astra Control Provisioner

Configurar a criptografia de back-end de storage

Com o Astra Control Provisioner, você pode melhorar a segurança de acesso aos dados habilitando a criptografia para o tráfego entre o cluster gerenciado e o back-end de storage.

O Astra Control Provisioner oferece suporte à criptografia Kerberos para dois tipos de backends de armazenamento:

- **On-Premises ONTAP** - o Astra Control Provisioner oferece suporte à criptografia Kerberos em conexões NFSv3 e NFSv4 de clusters do Red Hat OpenShift e upstream do Kubernetes para volumes ONTAP locais.
- **Azure NetApp Files** - o Provisioner oferece suporte à criptografia Kerberos em mais de NFSv4,1 conexões de clusters do Kubernetes upstream para volumes do Azure NetApp Files.

Você pode criar, excluir, redimensionar, snapshot, clone, clone somente leitura e importar volumes que usam criptografia NFS.

Configurar a criptografia Kerberos em trânsito com volumes ONTAP locais

Você pode ativar a criptografia Kerberos no tráfego de armazenamento entre o cluster gerenciado e um back-end de armazenamento ONTAP local.



A criptografia Kerberos para tráfego NFS com backends de armazenamento ONTAP no local é suportada apenas usando o `ontap-nas` driver de armazenamento.

Antes de começar

- Certifique-se de que você está "[Ativou o Astra Control Provisioner](#)" no cluster gerenciado.
- Certifique-se de que tem acesso ao `tridentctl` utilitário.
- Verifique se você tem acesso de administrador ao back-end de storage do ONTAP.
- Certifique-se de saber o nome do volume ou volumes que você compartilhará no back-end de storage do ONTAP.
- Certifique-se de que você preparou a VM de armazenamento ONTAP para oferecer suporte à criptografia Kerberos para volumes NFS. "[Ative o Kerberos em um LIF de dados](#)" Consulte para obter instruções.
- Certifique-se de que todos os volumes NFSv4 usados com criptografia Kerberos estejam configurados corretamente. Consulte a seção Configuração de domínio do NetApp NFSv4 (página 13) do "[Guia de práticas recomendadas e aprimoramentos do NetApp NFSv4](#)".

Adicionar ou modificar políticas de exportação do ONTAP

Você precisa adicionar regras às políticas de exportação existentes do ONTAP ou criar novas políticas de exportação que suportem a criptografia Kerberos para o volume raiz da VM de armazenamento do ONTAP, bem como quaisquer volumes do ONTAP compartilhados com o cluster do Kubernetes upstream. As regras de política de exportação que você adicionar ou as novas políticas de exportação que você criar precisam oferecer suporte aos seguintes protocolos de acesso e permissões de acesso:

Protocolos de acesso

Configurar a política de exportação com protocolos de acesso NFS, NFSv3 e NFSv4.

Aceder aos detalhes

Você pode configurar uma das três versões diferentes da criptografia Kerberos, dependendo de suas necessidades para o volume:

- **Kerberos 5** - (autenticação e criptografia)
- **Kerberos 5i** - (autenticação e criptografia com proteção de identidade)
- **Kerberos 5P** - (autenticação e criptografia com proteção de identidade e privacidade)

Configure a regra de política de exportação do ONTAP com as permissões de acesso apropriadas. Por exemplo, se os clusters estiverem montando os volumes NFS com uma mistura de criptografia Kerberos 5i e kerberos 5P, use as seguintes configurações de acesso:

Tipo	Acesso somente leitura	Acesso de leitura/escrita	Acesso ao superusuário
UNIX	Ativado	Ativado	Ativado
Kerberos 5i	Ativado	Ativado	Ativado
Kerberos 5P	Ativado	Ativado	Ativado

Consulte a documentação a seguir para saber como criar políticas de exportação e regras de política de exportação do ONTAP:

- ["Crie uma política de exportação"](#)
- ["Adicione uma regra a uma política de exportação"](#)

Crie um back-end de storage

Você pode criar uma configuração de back-end de storage do Astra Control Provisioner que inclua o recurso de criptografia Kerberos.

Sobre esta tarefa

Quando você cria um arquivo de configuração de back-end de armazenamento que configura a criptografia Kerberos, você pode especificar uma das três versões diferentes da criptografia Kerberos usando o `spec.nfsMountOptions` parâmetro:

- `spec.nfsMountOptions: sec=krb5` (autenticação e criptografia)
- `spec.nfsMountOptions: sec=krb5i` (autenticação e criptografia com proteção de identidade)
- `spec.nfsMountOptions: sec=krb5p` (autenticação e criptografia com proteção de identidade e privacidade)

Especifique apenas um nível Kerberos. Se você especificar mais de um nível de criptografia Kerberos na lista de parâmetros, somente a primeira opção será usada.

Passos

1. No cluster gerenciado, crie um arquivo de configuração de back-end de storage usando o exemplo a seguir. Substitua os valores entre parêntesis> por informações do seu ambiente:

```

apiVersion: v1
kind: Secret
metadata:
  name: backend-ontap-nas-secret
type: Opaque
stringData:
  clientID: <CLIENT_ID>
  clientSecret: <CLIENT_SECRET>
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-ontap-nas
spec:
  version: 1
  storageDriverName: "ontap-nas"
  managementLIF: <STORAGE_VM_MGMT_LIF_IP_ADDRESS>
  dataLIF: <PROTOCOL_LIF_FQDN_OR_IP_ADDRESS>
  svm: <STORAGE_VM_NAME>
  username: <STORAGE_VM_USERNAME_CREDENTIAL>
  password: <STORAGE_VM_PASSWORD_CREDENTIAL>
  nasType: nfs
  nfsMountOptions: ["sec=krb5i"] #can be krb5, krb5i, or krb5p
  qtreesPerFlexvol:
  credentials:
    name: backend-ontap-nas-secret

```

2. Use o arquivo de configuração que você criou na etapa anterior para criar o backend:

```
tridentctl create backend -f <backend-configuration-file>
```

Se a criação do backend falhar, algo está errado com a configuração do backend. Você pode exibir os logs para determinar a causa executando o seguinte comando:

```
tridentctl logs
```

Depois de identificar e corrigir o problema com o arquivo de configuração, você pode executar o comando create novamente.

Crie uma classe de armazenamento

Você pode criar uma classe de armazenamento para provisionar volumes com criptografia Kerberos.

Sobre esta tarefa

Ao criar um objeto de classe de armazenamento, você pode especificar uma das três versões diferentes da criptografia Kerberos usando o `mountOptions` parâmetro:

- `mountOptions: sec=krb5` (autenticação e criptografia)
- `mountOptions: sec=krb5i` (autenticação e criptografia com proteção de identidade)
- `mountOptions: sec=krb5p` (autenticação e criptografia com proteção de identidade e privacidade)

Especifique apenas um nível Kerberos. Se você especificar mais de um nível de criptografia Kerberos na lista de parâmetros, somente a primeira opção será usada. Se o nível de criptografia especificado na configuração de back-end de armazenamento for diferente do nível especificado no objeto de classe de armazenamento, o objeto de classe de armazenamento terá precedência.

Passos

1. Crie um objeto Kubernetes StorageClass, usando o exemplo a seguir:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-nas-sc
provisioner: csi.trident.netapp.io
mountOptions: ["sec=krb5i"] #can be krb5, krb5i, or krb5p
parameters:
  backendType: "ontap-nas"
  storagePools: "ontapnas_pool"
  trident.netapp.io/nasType: "nfs"
allowVolumeExpansion: True
```

2. Crie a classe de armazenamento:

```
kubectl create -f sample-input/storage-class-ontap-nas-sc.yaml
```

3. Certifique-se de que a classe de armazenamento foi criada:

```
kubectl get sc ontap-nas-sc
```

Você deve ver saída semelhante ao seguinte:

NAME	PROVISIONER	AGE
ontap-nas-sc	csi.trident.netapp.io	15h

Volumes de provisionamento

Depois de criar um back-end de storage e uma classe de storage, agora é possível provisionar um volume.

Consulte estas instruções para ["provisionamento de um volume"](#).

Configurar a criptografia Kerberos em trânsito com volumes Azure NetApp Files

Você pode ativar a criptografia Kerberos no tráfego de armazenamento entre o cluster gerenciado e um único back-end de armazenamento Azure NetApp Files ou um pool virtual de backends de armazenamento Azure NetApp Files.

Antes de começar

- Certifique-se de que você ativou o Astra Control Provisioner no cluster gerenciado do Red Hat OpenShift. ["Habilite o Astra Control Provisioner"](#) Consulte para obter instruções.
- Certifique-se de que tem acesso ao `tridentctl` utilitário.
- Certifique-se de que preparou o back-end de armazenamento Azure NetApp Files para criptografia Kerberos, observando os requisitos e seguindo as instruções em ["Documentação do Azure NetApp Files"](#).
- Certifique-se de que todos os volumes NFSv4 usados com criptografia Kerberos estejam configurados corretamente. Consulte a seção Configuração de domínio do NetApp NFSv4 (página 13) do ["Guia de práticas recomendadas e aprimoramentos do NetApp NFSv4"](#).

Crie um back-end de storage

Você pode criar uma configuração de back-end de armazenamento Azure NetApp Files que inclua o recurso de criptografia Kerberos.

Sobre esta tarefa

Quando você cria um arquivo de configuração de back-end de armazenamento que configura a criptografia Kerberos, você pode defini-lo para que ele seja aplicado em um dos dois níveis possíveis:

- O **nível de back-end de armazenamento** usando o `spec.kerberos` campo
- O **nível de pool virtual** usando o `spec.storage.kerberos` campo

Quando você define a configuração no nível do pool virtual, o pool é selecionado usando o rótulo na classe de armazenamento.

Em ambos os níveis, você pode especificar uma das três versões diferentes da criptografia Kerberos:

- `kerberos: sec=krb5` (autenticação e criptografia)
- `kerberos: sec=krb5i` (autenticação e criptografia com proteção de identidade)
- `kerberos: sec=krb5p` (autenticação e criptografia com proteção de identidade e privacidade)

Passos

1. No cluster gerenciado, crie um arquivo de configuração de back-end de storage usando um dos exemplos a seguir, dependendo de onde você precisa definir o back-end de storage (nível de back-end de armazenamento ou nível de pool virtual). Substitua os valores entre parêntesis > por informações do seu ambiente:

Exemplo de nível de back-end de storage

```
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-anf-secret
type: Opaque
stringData:
  clientID: <CLIENT_ID>
  clientSecret: <CLIENT_SECRET>
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-anf
spec:
  version: 1
  storageDriverName: azure-netapp-files
  subscriptionID: <SUBSCRIPTION_ID>
  tenantID: <TENANT_ID>
  location: <AZURE_REGION_LOCATION>
  serviceLevel: Standard
  networkFeatures: Standard
  capacityPools: <CAPACITY_POOL>
  resourceGroups: <RESOURCE_GROUP>
  netappAccounts: <NETAPP_ACCOUNT>
  virtualNetwork: <VIRTUAL_NETWORK>
  subnet: <SUBNET>
  nasType: nfs
  kerberos: sec=krb5i #can be krb5, krb5i, or krb5p
  credentials:
    name: backend-tbc-anf-secret
```

Exemplo de nível de pool virtual

```

apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-anf-secret
type: Opaque
stringData:
  clientID: <CLIENT_ID>
  clientSecret: <CLIENT_SECRET>
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-anf
spec:
  version: 1
  storageDriverName: azure-netapp-files
  subscriptionID: <SUBSCRIPTION_ID>
  tenantID: <TENANT_ID>
  location: <AZURE_REGION_LOCATION>
  serviceLevel: Standard
  networkFeatures: Standard
  capacityPools: <CAPACITY_POOL>
  resourceGroups: <RESOURCE_GROUP>
  netappAccounts: <NETAPP_ACCOUNT>
  virtualNetwork: <VIRTUAL_NETWORK>
  subnet: <SUBNET>
  nasType: nfs
  storage:
    - labels:
      type: encryption
      kerberos: sec=krb5i #can be krb5, krb5i, or krb5p
  credentials:
    name: backend-tbc-anf-secret

```

2. Use o arquivo de configuração que você criou na etapa anterior para criar o backend:

```
tridentctl create backend -f <backend-configuration-file>
```

Se a criação do backend falhar, algo está errado com a configuração do backend. Você pode exibir os logs para determinar a causa executando o seguinte comando:

```
tridentctl logs
```

Depois de identificar e corrigir o problema com o arquivo de configuração, você pode executar o comando `create` novamente.

Crie uma classe de armazenamento

Você pode criar uma classe de armazenamento para provisionar volumes com criptografia Kerberos.

Passos

1. Crie um objeto Kubernetes StorageClass, usando o exemplo a seguir:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: anf-sc-nfs
provisioner: csi.trident.netapp.io
parameters:
  backendType: "azure-netapp-files"
  trident.netapp.io/nasType: "nfs"
  selector: "type=encryption"
```

2. Crie a classe de armazenamento:

```
kubectl create -f sample-input/storage-class-anf-sc-nfs.yaml
```

3. Certifique-se de que a classe de armazenamento foi criada:

```
kubectl get sc anf-sc-nfs
```

Você deve ver saída semelhante ao seguinte:

NAME	PROVISIONER	AGE
anf-sc-nfs	csi.trident.netapp.io	15h

Volumes de provisionamento

Depois de criar um back-end de storage e uma classe de storage, agora é possível provisionar um volume. Consulte estas instruções para ["provisionamento de um volume"](#).

Recuperar dados de volume usando um snapshot

O Astra Control Provisioner fornece restauração rápida de volume no local a partir de um snapshot usando o `TridentActionSnapshotRestore` (TASR) CR. Esse CR funciona como uma ação imperativa do Kubernetes e não persiste após a conclusão da operação.

O Astra Control Provisioner oferece suporte à restauração de snapshot no `ontap-san`, `ontap-san-economy`, `ontap-nas`, `ontap-nas-flexgroup`, `azure-netapp-files`, `gcp-cvs`, e `solidfire-san` drivers.

Antes de começar

Você deve ter um PVC vinculado e instantâneo de volume disponível.

- Verifique se o status do PVC está vinculado.

```
kubectl get pvc
```

- Verifique se o instantâneo do volume está pronto para ser usado.

```
kubectl get vs
```

Passos

1. Crie o TASR CR. Este exemplo cria um CR para instantâneo de PVC `pvc1` e volume `pvc1-snapshot`.

```
cat tasr-pvc1-snapshot.yaml

apiVersion: v1
kind: TridentActionSnapshotRestore
metadata:
  name: this-doesnt-matter
  namespace: trident
spec:
  pvcName: pvc1
  volumeSnapshotName: pvc1-snapshot
```

2. Aplique o CR para restaurar a partir do instantâneo. Este exemplo restaura do instantâneo `pvc1`.

```
kubectl create -f tasr-pvc1-snapshot.yaml

tridentactionsnapshotrestore.trident.netapp.io/this-doesnt-matter
created
```

Resultados

O Astra Control Provisioner restaura os dados do snapshot. Você pode verificar o status de restauração de snapshot.

```
kubectl get tasr -o yaml

apiVersion: v1
items:
- apiVersion: trident.netapp.io/v1
  kind: TridentActionSnapshotRestore
  metadata:
    creationTimestamp: "2023-04-14T00:20:33Z"
    generation: 3
    name: this-doesnt-matter
    namespace: trident
    resourceVersion: "3453847"
    uid: <uid>
  spec:
    pvcName: pvcl
    volumeSnapshotName: pvcl-snapshot
  status:
    startTime: "2023-04-14T00:20:34Z"
    completionTime: "2023-04-14T00:20:37Z"
    state: Succeeded
kind: List
metadata:
  resourceVersion: ""
```



- Na maioria dos casos, o Astra Control Provisioner não tentará automaticamente a operação em caso de falha. Terá de efetuar novamente a operação.
- Os usuários do Kubernetes sem acesso de administrador podem ter permissão para que o administrador crie um TASR CR em seu namespace de aplicativo.

Replique volumes usando o SnapMirror

Com o Astra Control Provisioner, você pode criar relacionamentos de espelhamento entre um volume de origem em um cluster e o volume de destino no cluster peered para replicação de dados para recuperação de desastres. Você pode usar uma Definição de recursos personalizados (CRD) para executar as seguintes operações:

- Criar relações de espelhamento entre volumes (PVCs)
- Remova as relações de espelho entre volumes
- Quebre as relações do espelho
- Promover o volume secundário durante as condições de desastre (failovers)
- Realizar a transição sem perda de aplicativos do cluster para o cluster (durante failovers planejados ou migrações)

Pré-requisitos de replicação

Certifique-se de que os seguintes pré-requisitos sejam atendidos antes de começar:

Clusters de ONTAP

- **Provisioner:** O Astra Control Provisioner versão 23,10 ou posterior deve existir nos clusters do Kubernetes de origem e destino que utilizam o ONTAP como um 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.

Peering

- **Cluster e SVM:** Os backends de storage do ONTAP devem ser colocados em Contato. ["Visão geral do peering de cluster e SVM"](#) Consulte para obter mais informações.



Certifique-se de que os nomes do SVM usados na relação de replicação entre dois clusters ONTAP sejam exclusivos.

- **Astra Control Provisioner e SVM:** Os SVMs remotas com peering devem estar disponíveis para o Astra Control Provisioner no cluster de destino.

Drivers suportados

- A replicação de volume é compatível com os drivers ONTAP-nas e ONTAP-san.

Crie um PVC espelhado

Siga estas etapas e use os exemplos CRD para criar relação de espelhamento entre volumes primário e secundário.

Passos

1. Execute as etapas a seguir no cluster primário do Kubernetes:
 - a. Crie um objeto StorageClass com o `trident.netapp.io/replication: true` parâmetro.

Exemplo

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: csi-nas
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-nas"
  fsType: "nfs"
  trident.netapp.io/replication: "true"
```

- b. Crie um PVC com StorageClass criado anteriormente.

Exemplo

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: csi-nas
spec:
  accessModes:
  - ReadWriteMany
  resources:
    requests:
      storage: 1Gi
  storageClassName: csi-nas
```

- c. Crie um MirrorRelationship CR com informações locais.

Exemplo

```
kind: TridentMirrorRelationship
apiVersion: trident.netapp.io/v1
metadata:
  name: csi-nas
spec:
  state: promoted
  volumeMappings:
  - localPVCName: csi-nas
```

O Astra Control Provisioner obtém as informações internas do volume e do estado atual de proteção de dados (DP) do volume e, em seguida, preenche o campo de status do MirrorRelationship.

- d. Obtenha o tridentMirrorRelationship CR para obter o nome interno e SVM do PVC.

```
kubectl get tmr csi-nas
```

```

kind: TridentMirrorRelationship
apiVersion: trident.netapp.io/v1
metadata:
  name: csi-nas
  generation: 1
spec:
  state: promoted
  volumeMappings:
    - localPVCName: csi-nas
status:
  conditions:
    - state: promoted
      localVolumeHandle:
"datavserver:trident_pvc_3bedd23c_46a8_4384_b12b_3c38b313c1e1"
      localPVCName: csi-nas
      observedGeneration: 1

```

2. Execute as etapas a seguir no cluster secundário do Kubernetes:

- a. Crie um StorageClass com o parâmetro Trident.NetApp.io/replicação: True.

Exemplo

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: csi-nas
provisioner: csi.trident.netapp.io
parameters:
  trident.netapp.io/replication: true

```

- b. Crie um MirrorRelationship CR com informações de destino e origem.

Exemplo

```

kind: TridentMirrorRelationship
apiVersion: trident.netapp.io/v1
metadata:
  name: csi-nas
spec:
  state: established
  volumeMappings:
    - localPVCName: csi-nas
      remoteVolumeHandle:
"datavserver:trident_pvc_3bedd23c_46a8_4384_b12b_3c38b313c1e1"

```

O Provisioner criará um relacionamento SnapMirror com o nome da política de relacionamento configurado (ou padrão para ONTAP) e inicializará-o.

- c. Crie um PVC com StorageClass criado anteriormente para atuar como secundário (destino SnapMirror).

Exemplo

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: csi-nas
  annotations:
    trident.netapp.io/mirrorRelationship: csi-nas
spec:
  accessModes:
    - ReadWriteMany
resources:
  requests:
    storage: 1Gi
storageClassName: csi-nas
```

O Astra Control Provisioner verificará o CRD de relacionamento do tridentMirrorRelationship e falhará em criar o volume se o relacionamento não existir. Se o relacionamento existir, o Supervisor de Controle Astra garantirá que o novo FlexVol volume seja colocado em um SVM que seja emparelhado com o SVM remoto definido no espelhamento.

Estados de replicação de volume

Um relacionamento de espelhamento do Trident (TMR) é um CRD que representa um fim de uma relação de replicação entre PVCs. O TMR de destino tem um estado, que diz ao Astra Control Provisioner qual é o estado desejado. O TMR de destino tem os seguintes estados:

- *** Estabelecido***: O PVC local é o volume de destino de uma relação de espelho, e esta é uma nova relação.
- **Promovido**: O PVC local é ReadWrite e montável, sem relação de espelho atualmente em vigor.
- *** Restabelecido***: O PVC local é o volume de destino de uma relação de espelho e também estava anteriormente nessa relação de espelho.
 - O estado restabelecido deve ser usado se o volume de destino estiver em uma relação com o volume de origem, porque ele sobrescreve o conteúdo do volume de destino.
 - O estado restabelecido falhará se o volume não estiver previamente em uma relação com a fonte.

Promover PVC secundário durante um failover não planejado

Execute a seguinte etapa no cluster secundário do Kubernetes:

- Atualize o campo `spec.State` do `TridentMirrorRelationship` para `promoted`.

Promover PVC secundário durante um failover planejado

Durante um failover planejado (migração), execute as seguintes etapas para promover o PVC secundário:

Passos

1. No cluster primário do Kubernetes, crie um snapshot do PVC e aguarde até que o snapshot seja criado.
2. No cluster principal do Kubernetes, crie o SnapshotInfo CR para obter detalhes internos.

Exemplo

```
kind: SnapshotInfo
apiVersion: trident.netapp.io/v1
metadata:
  name: csi-nas
spec:
  snapshot-name: csi-nas-snapshot
```

3. No cluster secundário do Kubernetes, atualize o campo *spec.State* do *tridentMirrorRelationship* CR para *promoted* e *spec.promotedSnapshotHandle* para ser o *internalName* do snapshot.
4. No cluster secundário do Kubernetes, confirme o status (campo *status.State*) do *TridentMirrorRelationship* para promovido.

Restaurar uma relação de espelhamento após um failover

Antes de restaurar uma relação de espelho, escolha o lado que você deseja fazer como o novo primário.

Passos

1. No cluster secundário do Kubernetes, certifique-se de que os valores do campo *spec.remoteVolumeHandle* no *TridentMirrorRelationship* sejam atualizados.
2. No cluster secundário do Kubernetes, atualize o campo *spec.mirror* do *TridentMirrorRelationship* para *reestablished*.

Operações adicionais

O Astra Control Provisioner dá suporte às seguintes operações nos volumes primário e secundário:

Replique PVC primário para um novo PVC secundário

Certifique-se de que você já tem um PVC primário e um PVC secundário.

Passos

1. Exclua as CRDs *PersistentVolumeClaim* e *TridentMirrorRelationship* do cluster secundário (destino) estabelecido.
2. Exclua o CRD do *tridentMirrorRelationship* do cluster primário (de origem).
3. Crie um novo CRD de *TridentMirrorRelationship* no cluster primário (de origem) para o novo PVC secundário (de destino) que você deseja estabelecer.

Redimensione um PVC espelhado, primário ou secundário

O PVC pode ser redimensionado como normal, o ONTAP irá expandir automaticamente qualquer destino flexvols se a quantidade de dados exceder o tamanho atual.

Remova a replicação de um PVC

Para remover a replicação, execute uma das seguintes operações no volume secundário atual:

- Exclua o MirrorRelationship no PVC secundário. Isso quebra a relação de replicação.
- Ou atualize o campo spec.State para *promovido*.

Excluir um PVC (que foi anteriormente espelhado)

O Astra Control Provisioner verifica se há PVCs replicados e libera a relação de replicação antes de tentar excluir o volume.

Eliminar um TMR

A exclusão de um TMR em um lado de um relacionamento espelhado faz com que o TMR restante passe para o estado *promovido* antes que o Astra Control Provisioner conclua a exclusão. Se o TMR selecionado para exclusão já estiver no estado *promovido*, não há relacionamento de espelhamento existente e o TMR será removido e o Astra Control Provisioner promoverá o PVC local para *ReadWrite*. Essa exclusão libera os metadados do SnapMirror para o volume local no ONTAP. Se este volume for usado em uma relação de espelho no futuro, ele deve usar um novo TMR com um estado de replicação de volume *established* ao criar a nova relação de espelho.

Atualizar relações de espelho quando o ONTAP estiver online

As relações de espelho podem ser atualizadas a qualquer momento depois que são estabelecidas. Pode utilizar os `state: promoted` campos ou `state: reestablished` para atualizar as relações. Ao promover um volume de destino para um volume ReadWrite regular, você pode usar *promotedSnapshotHandle* para especificar um snapshot específico para restaurar o volume atual.

Atualizar relações de espelho quando o ONTAP estiver offline

Você pode usar um CRD para executar uma atualização do SnapMirror sem que o Astra Control tenha conectividade direta com o cluster do ONTAP. Consulte o seguinte formato de exemplo do TrigentActionMirrorUpdate:

Exemplo

```
apiVersion: trident.netapp.io/v1
kind: TridentActionMirrorUpdate
metadata:
  name: update-mirror-b
spec:
  snapshotHandle: "pvc-1234/snapshot-1234"
  tridentMirrorRelationshipName: mirror-b
```

`status.state` Reflete o estado do CRD do TrigentActionMirrorUpdate. Ele pode tomar um valor de *successful*, *in progress* ou *Failed*.

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 saber mais, ["Vá para a documentação de automação do Astra"](#).

Conhecimento e apoio

Registre-se para obter suporte

O Astra Control tenta Registrar automaticamente sua conta para suporte quando você configura sua conta. Se não puder, então você pode se Registrar manualmente para obter suporte. O Registro do suporte é necessário para obter ajuda do suporte técnico da NetApp.

Verifique o seu registo de suporte

O Astra Control inclui um campo Status do suporte que permite confirmar seu Registro de suporte.

Passos

1. Selecione **suporte**.
2. Dê uma olhada no campo Status do suporte.

O Status do suporte começa como "não registrado", mas depois passa para "em andamento" e, finalmente, para "registrado" quando concluído.

Este status de Registro de suporte é polled a cada 15 minutos. Os novos clientes da NetApp podem levar até o próximo dia útil para concluir o Registro de integração e suporte. Se o número de série não mostrar "registrado" dentro de 48 horas, você pode entrar em Contato com a NetApp usando o NetApp.com ou Registrar manualmente em <https://register.netapp.com>.

Obtenha o seu número de série

Quando você se Registra em uma conta, o Astra Control usa as informações fornecidas sobre sua empresa para gerar um número de série NetApp de 20 dígitos que começa com "941".

O número de série do NetApp representa a sua conta do Astra Control. Você precisará usar esse número de série ao abrir um ticket da Web.

Você pode encontrar seu número de série na interface do Astra Control na página **Support**.

Ativar direitos de suporte

Se o Astra Control não conseguir Registrar automaticamente sua conta para suporte, Registre o número de série do NetApp associado ao Astra Control para ativar os direitos de suporte. Oferecemos 2 opções para Registro de suporte:

1. Cliente NetApp atual com conta SSO do site de suporte da NetApp (NSS) existente
2. Novo cliente da NetApp sem conta SSO do site de suporte da NetApp (NSS) existente

Opção 1: Cliente NetApp atual com uma conta existente do site de suporte da NetApp (NSS)

Passos

1. Navegue até a "[Registro de suporte de serviços de dados em nuvem](#)" página.
2. Selecione **já estou registado como cliente NetApp**.

3. Introduza as credenciais do site de suporte da NetApp para iniciar sessão.

É apresentada a página Registo de cliente existente.

4. Preencha as informações necessárias no formulário:
 - a. Digite seu nome, empresa e endereço de e-mail.
 - b. Selecione **Astra Control Service** como a linha de produtos.
 - c. Selecione um fornecedor de faturação.
 - d. Introduza o seu número de série.
 - e. Selecione **Enviar**.

Resultado

Você deve ser redirecionado para uma página "Registro enviado com sucesso". O endereço de e-mail associado ao seu Registro receberá um e-mail dentro de alguns minutos informando que "seu produto agora é elegível para suporte".

Este é um registo de suporte único para o número de série aplicável.

Opção 2: Novo cliente NetApp sem conta do site de suporte da NetApp (NSS) existente

Passos

1. Navegue até a "[Registro de suporte de serviços de dados em nuvem](#)" página.
2. Selecione **não sou um Cliente NetApp registrado**.

É apresentada a página New Customer Registration (Registo de novo cliente).

3. Preencha as informações necessárias no formulário:
 - a. Insira seu nome, informações da empresa e detalhes de Contato.
 - b. Selecione **Astra Control Service** como linha de Produtos.
 - c. Selecione um fornecedor de faturação.
 - d. Introduza o seu número de série.
 - e. Introduza o valor captcha.
 - f. Marque a caixa de seleção para confirmar que leu a Política de Privacidade da NetApp.
 - g. Selecione **Enviar**.

Você receberá um e-mail de confirmação do seu Registro enviado. Se não ocorrerem erros, você será redirecionado para uma página "Registro enviado com sucesso". Você também receberá um e-mail dentro de uma hora informando que "seu produto agora é elegível para suporte".

Este é um registo de suporte único para o número de série aplicável.

4. Como um novo cliente da NetApp, você também precisa criar uma conta de usuário do site de suporte da NetApp (NSS) para futuras ativações de suporte e para acesso ao portal de suporte para bate-papo de suporte técnico e tíquetes na Web.

Aceda a "[Site de Registro de suporte da NetApp](#)" para executar esta tarefa. Você pode fornecer seu número de série Astra Control recém-registrado para acelerar o processo.

Solução de problemas

Aprenda a contornar alguns problemas comuns que você pode encontrar.

<https://kb.netapp.com/Cloud/Astra/Control>

Para mais informações

- ["Solução de problemas"](#)

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.

Você deve primeiro ["Ative o suporte para o seu número de série NetApp"](#) para usar essas opções de suporte que não são de autoatendimento. É necessária uma conta SSO do site de suporte da NetApp (NSS) para chat e emissão de bilhetes na Web, juntamente com o gerenciamento de casos.

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

Auto-suporte

Estas opções estão disponíveis gratuitamente 24x7:

- ["Base de conhecimento"](#)

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

- Documentação

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

- ["Obter ajuda via discord"](#)

Vá para Astra na categoria Pub para se conectar com colegas e especialistas.

- E-mail de feedback

Envie um e-mail para NetApp.com para nos informar sobre seus pensamentos, ideias ou preocupações.

Suporte por assinatura

Além das opções de suporte autônomo acima, você pode trabalhar com um engenheiro de suporte da NetApp para resolver quaisquer problemas depois de ["Ative o suporte para o seu número de série NetApp"](#) você .

Depois que o número de série do Astra Control estiver ativado, você poderá acessar os recursos de suporte técnico da NetApp criando um ["Ticket de suporte"](#).

Perguntas frequentes

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

Visão geral

O Astra Control simplifica as operações de gerenciamento de ciclo de vida dos dados da aplicação para aplicações nativas em Kubernetes. O Astra Control Service é compatível com clusters Kubernetes executados em vários ambientes de fornecedor de nuvem.

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

Acesso ao Astra Control

Por que eu preciso fornecer tantos detalhes ao me Registrar no Astra Control?

O Astra Control requer informações precisas do cliente ao se Registrar. Esta informação é necessária para passar por uma verificação de conformidade de comércio global (GTC).

Por que estou recebendo um erro "Falha no Registro" ao me Registrar para o Astra Control?

O Astra Control requer que você forneça informações precisas dos clientes na seção de integração. Você receberá um erro "Falha no Registro" se você forneceu informações incorretas. Outras contas das quais você é membro também ficam bloqueadas.

Qual é a URL do Astra Control Service?

Você pode acessar o Astra Control Service em <https://astra.netapp.io>.

Enviei um convite por e-mail para um colega, mas eles não o receberam. O que devo fazer?

Peça a eles para verificar a pasta de spam para um e-mail do NetApp.com, ou procurar na caixa de entrada para "convite". Você também pode remover o usuário e tentar adicioná-lo novamente.

Eu atualizei para o Plano Premium PayGO do Plano Gratuito. Serei cobrado pelos primeiros 10 namespaces?

Sim. Depois de atualizar para o Plano Premium, o Astra Control começa a cobrar por todos os namespaces gerenciados em sua conta.

Eu atualizei para o Premium PayGO Plan no meio de um mês. Vou ser cobrado pelo mês inteiro?

Não. O faturamento começa a partir do momento em que você fez o upgrade para o Plano Premium.

Estou a utilizar o plano gratuito, serei cobrado pelas declarações de volume persistentes?

Sim, você cobrará pelos volumes persistentes usados pelos clusters do seu fornecedor de nuvem.

Registrando clusters do Kubernetes

Preciso instalar drivers CSI no meu cluster antes de adicioná-lo ao Astra Control Service?

Não. Quando seu cluster for adicionado ao Astra Control, o serviço instalará automaticamente o driver da Interface de armazenamento de contêiner (CSI) Astra Trident no cluster Kubernetes. Esse driver de CSI é usado para provisionar volumes persistentes para clusters com o seu fornecedor de nuvem.

Eu preciso adicionar nós de trabalho ao meu cluster depois de adicioná-lo ao Astra Control Service. O que devo fazer?

Novos nós de trabalho podem ser adicionados a pools existentes ou novos pools podem ser criados desde que sejam o `COS_CONTAINERD` tipo de imagem. 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.

Registrando clusters do Elastic Kubernetes Service (EKS)

Posso adicionar um cluster EKS privado ao Astra Control Service?

Sim, você pode adicionar clusters EKS privados ao Astra Control Service. Para adicionar um cluster EKS privado, "[Comece a gerenciar clusters de Kubernetes a partir do Astra Control Service](#)" consulte .

Registrando clusters do Azure Kubernetes Service (AKS)

Posso adicionar um cluster AKS privado ao Astra Control Service?

Sim, você pode adicionar clusters AKS privados ao Astra Control Service. Para adicionar um cluster AKS privado, "[Comece a gerenciar clusters de Kubernetes a partir do Astra Control Service](#)" consulte .

Posso usar o Azure Active Directory para gerenciar a autenticação para meus clusters AKS?

Sim, você pode configurar seus clusters AKS para usar o Azure Active Directory (Azure AD) para autenticação e gerenciamento de identidade. Ao criar o cluster, siga as instruções na "[documentação oficial](#)" para configurar o cluster para utilizar o Azure AD. Você precisará garantir que seus clusters atendam aos requisitos de integração do Azure AD gerenciada pelo AKS.

Registrando clusters do Google Kubernetes Engine (GKE)

Posso adicionar um cluster GKE privado ao Astra Control Service?

Sim, você pode adicionar clusters GKE privados ao Astra Control Service. Para adicionar um cluster GKE privado, "[Comece a gerenciar clusters de Kubernetes a partir do Astra Control Service](#)" consulte .

Os clusters privados do GKE devem ter o "[redes autorizadas](#)" conjunto para permitir o endereço IP do Astra Control:

52.188.218.166/32

Meu cluster GKE pode residir em uma VPC compartilhada?

Sim. O Astra Control pode gerenciar clusters que residem em uma VPC compartilhada. "[Saiba como configurar a conta de serviço Astra para uma configuração VPC compartilhada](#)".

Onde posso encontrar as credenciais da minha conta de serviço no GCP?

Depois de iniciar sessão "[Google Cloud Console](#)" no , os detalhes da sua conta de serviço estarão na seção **IAM e Admin**. Para obter mais detalhes, "[Como configurar o Google Cloud para Astra Control](#)" consulte .

Gostaria de adicionar diferentes clusters GKE de diferentes projetos do GCP. Isso é compatível com Astra Control?

Não, esta não é uma configuração suportada. Apenas um único projeto do GCP é compatível.

Remoção de clusters

Como faço para cancelar o Registro corretamente, reduzir um cluster e excluir os volumes associados?

1. ["Desgerenciar as aplicações do Astra Control"](#).
2. ["Desmarque o cluster do Astra Control"](#).
3. ["Exclua as reivindicações de volume persistente"](#).
4. Eliminar o cluster.

O que acontece com minhas aplicações e dados após a remoção do cluster 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 dados instantâneos de volume armazenados no back-end de armazenamento não serão removidos. Os backups de storage persistente criados pelo Astra Control permanecerão no armazenamento de objetos do seu fornecedor de nuvem, mas não poderão ser restaurados.



Sempre remova um cluster do Astra Control antes de excluí-lo pelo GCP. Excluir um cluster do GCP enquanto ele ainda está sendo gerenciado pelo Astra Control pode causar problemas para sua conta Astra Control.

O Astra Control Provisioner é desinstalado automaticamente de um cluster quando eu o desgerencio?

Quando você desgerencia um cluster do Astra Control Center, o Astra Control Provisioner ou o Astra Trident não é desinstalado automaticamente do cluster. Para desinstalar o Astra Control Provisioner e seus componentes ou o Astra Trident, você precisará ["Siga estas etapas para desinstalar a instância do Astra Trident que contém o serviço Provisioner do Astra Control"](#).

Gerenciamento de aplicações

O Astra Control pode implantar uma aplicação?

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

Não vejo nenhum dos PVCs do meu aplicativo vinculado ao CVS do GCP. O que há de errado?

O operador Astra Trident define a classe de storage padrão para `netapp-cvs-perf-premium` depois que ela é adicionada com sucesso ao Astra Control. Quando os PVCs de um aplicativo não estão vinculados ao Cloud Volumes Service para Google Cloud, há algumas etapas que você pode seguir:

- Execute `kubectl get sc` e verifique a classe de armazenamento padrão.
- Verifique o arquivo yaml ou o gráfico Helm que foi usado para implantar o aplicativo e veja se uma classe de armazenamento diferente está definida.
- O GKE versão 1,24 e posterior não suporta imagens de nó baseadas em Docker. Verifique se o tipo de imagem do nó de trabalho no GKE é `COS_CONTAINERD` e se a montagem NFS foi bem-sucedida.

O que acontece com as aplicações depois que eu paro 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.

Operações de gerenciamento de dados

Onde o Astra Control cria o bucket do armazenamento de objetos?

A geografia do primeiro cluster gerenciado determina o local do armazenamento de objetos. Por exemplo, se o primeiro cluster adicionado estiver em uma zona europeia, o intervalo será criado na mesma região geográfica. Se necessário, você pode ["adicione baldes adicionais"](#).

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

Em algumas situações, o Astra Control criará automaticamente um snapshot como parte da execução de outro processo. Se esses snapshots tiverem mais de alguns minutos, você poderá excluí-los com segurança.

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

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 tirados pelo Astra Control diretamente pelo meu fornecedor de nuvem?

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

Previsão do Astra Control

Como os recursos de provisionamento de storage do Astra Control Provisioner são diferentes dos do Astra Trident?

Como parte do Astra Control, o Astra Control Provisioner é compatível com um superconjunto de recursos de provisionamento de storage que não estão disponíveis em código aberto Astra Trident. Esses recursos são além de todos os recursos que estão disponíveis para o Trident de código aberto.

O Astra Control está substituindo o Astra Trident?

O Astra Control Provisioner substituiu o Astra Trident como provisionador de storage e orquestrador na arquitetura Astra Control. Os usuários do Astra Control devem ["Habilite o Astra Control Provisioner"](#) usar o Astra Control. O Astra Trident continuará a ser suportado neste lançamento, mas não será suportado em versões futuras. O Astra Trident permanecerá de código aberto e será lançado, mantido, com suporte e atualizado com o novo CSI e outros recursos do NetApp. No entanto, somente o Astra Control Provisioner que contém a funcionalidade Astra Trident CSI e funcionalidades de gerenciamento de storage estendido podem ser usados com os próximos lançamentos do Astra Control.

Tenho que pagar pelo Astra Trident?

Não. O Astra Trident continuará a ser de código aberto e gratuito para download. O uso de recursos do Astra Control Provisioner agora requer uma licença do Astra Control.

Posso usar o gerenciamento de storage e recursos de provisionamento no Astra Control sem instalar e usar todo o Astra Control?

Sim, você pode fazer upgrade para o Astra Control Provisioner e usar suas funcionalidades mesmo que não queira consumir o conjunto completo de recursos do recurso de gerenciamento de dados Astra Control.

Como saber se o Astra Control Provisioner substituiu o Astra Trident no meu cluster?

Depois que o Astra Control Provisioner for instalado, o cluster de host na IU do Astra Control mostrará um `ACP version` número de versão instalada em vez `Trident version` de campo e atual.


 **CLUSTER STATUS**

 Available

Version
v1.24.9+rke2r2


Managed
2024/03/15 17:32 UTC

Kube-system namespace UID


ACP Version


Private route identifier


Cloud instance
private 

Default bucket
astra-bucket1 (inherited) 

[Overview](#)

[Namespaces](#)

[Storage](#)

[Activity](#)

Se você não tiver acesso à interface do usuário, poderá confirmar a instalação bem-sucedida usando os seguintes métodos:

Operador do Astra Trident

Verifique se o `trident-acp` contentor está em execução e que `acpVersion` está `23.10.0` ou mais tarde com um status de `Installed`:

```
kubectl get torc -o yaml
```

Resposta:

```
status:
  acpVersion: 23.10.0
  currentInstallationParams:
    ...
  acpImage: <my_custom_registry>/trident-acp:v23.10.0
  enableACP: "true"
  ...
  ...
  status: Installed
```

tridentctl

Confirme se o Astra Control Provisioner foi ativado:

```
./tridentctl -n trident version
```

Resposta:

```
+-----+-----+-----+ | SERVER VERSION |
CLIENT VERSION | ACP VERSION | +-----+-----
+-----+ | 23.10.0 | 23.10.0 | 23.10.0. | +-----
+-----+-----+
```


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"](#)

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 INTERRUPTÃO 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.