



Documentação do Astra Control Automation 21,08

Astra Automation

NetApp
October 23, 2024

Índice

Documentação do Astra Control Automation 21,08	1
Notas de lançamento	2
Sobre esta versão	2
Novidades da API REST do Astra Control	2
Introdução à API REST do Astra Control	4
Comece agora	5
Antes de começar	5
Obtenha um token de API	5
Olá mundo	6
Prepare-se para usar os fluxos de trabalho	6
Implementação principal do REST	9
Serviços web REST	9
Recursos e coleções	10
Detalhes HTTP	11
Formato de URL	14
Considerações adicionais DE DESCANSO	16
Segurança	16
Trabalhando com coleções	17
Diagnóstico e suporte	17
Recursos e endpoints	19
Recursos REST e pontos de extremidade do Astra Control	19
Recursos e endpoints adicionais	21
Workflows de infraestrutura	22
Antes de começar	22
Identidade e acesso	22
Balões	23
Armazenamento	24
Clusters	25
Fluxos de trabalho de gerenciamento	27
Antes de começar	27
Controlo de aplicações	28
Proteção da aplicação	34
Clonar e restaurar um aplicativo	41
Suporte	46
Usando Python	49
Antes de começar	49
Liste os aplicativos gerenciados	50
Referência da API	54
Recursos adicionais	55
Astra	55
Recursos de nuvem da NetApp	55
Conceitos REST e tecnologia de nuvem	55
Avisos legais	56

Direitos de autor	56
Marcas comerciais	56
Patentes	56
Política de privacidade	56
Licença de API Astra Control	56

Documentação do Astra Control Automation 21,08

Notas de lançamento

Sobre esta versão

A documentação neste local descreve a API REST do Astra Control e as tecnologias de automação relacionadas disponíveis nas versões de 2021 de agosto (21,08) e 2021 de abril (21,04) do Astra Control. Em particular, esta versão da API REST é usada com a versão 21,08 correspondente do Astra Control Center.

Consulte as páginas e sites a seguir para obter mais informações sobre esta versão, bem como versões anteriores:

- ["Novidades da API REST do Astra Control"](#)
- ["Recursos e endpoints"](#)
- ["Documentação do Astra Control Center 2108"](#)

Novidades da API REST do Astra Control

O NetApp atualiza periodicamente a API REST do Astra Control para oferecer novos recursos, melhorias e correções de bugs.

5 de agosto de 2021 (21,08)

Esta versão inclui a introdução de um novo modelo de implantação Astra e uma grande expansão da API REST.

Modelo de implantação do Astra Control Center

Além da oferta existente do Astra Control Service fornecida como serviço de nuvem pública, esta versão também inclui o modelo de implantação no local do Astra Control Center. Você pode instalar o Astra Control Center no seu local para gerenciar seu ambiente Kubernetes local. Os dois modelos de implantação do Astra Control compartilham a mesma API REST, com pequenas diferenças observadas conforme necessário na documentação.

Expansão dos tipos de recursos REST

O número de recursos acessíveis por meio da API REST Astra Control foi muito ampliado, com muitos dos novos recursos fornecendo a base para a oferta do Astra Control Center no local. Os novos recursos incluem: ASUP, direito, recurso, licença, configuração, assinatura, bucket, nuvem, cluster, cluster gerenciado, back-end de storage e classe de storage. Consulte ["Recursos"](#) para obter mais informações.

Pontos de extremidade adicionais compatíveis com a implantação do Astra

Além dos recursos REST expandidos, há vários outros pontos de extremidade de API novos disponíveis para dar suporte à implantação do Astra Control.

Suporte ao OpenAPI

Os endpoints OpenAPI fornecem acesso ao documento JSON OpenAPI atual e a outros recursos relacionados.

Suporte ao OpenMetrics

Os endpoints OpenMetrics fornecem acesso às métricas da conta por meio do recurso OpenMetrics.

15 de abril de 2021 (21,04)

Esta versão inclui os seguintes novos recursos e aprimoramentos.

Introdução da API REST

A API REST do Astra Control está disponível para uso com a oferta do Astra Control Service. Ele foi criado com base em TECNOLOGIAS REST e nas melhores práticas atuais. A API fornece uma base para a automação das implantações do Astra e inclui os recursos e benefícios a seguir.

Recursos

Existem quatorze tipos de recursos REST disponíveis.

Acesso ao token de API

O acesso à API REST é fornecido por meio de um token de acesso à API que você pode gerar na interface de usuário da Web Astra. O token de API fornece acesso seguro à API.

Suporte para coleções

Há um conjunto rico de parâmetros de consulta que podem ser usados para acessar as coleções de recursos. Algumas das operações suportadas incluem filtragem, classificação e paginação.

Introdução à API REST do Astra Control

O Astra Control Center e o Astra Control Service fornecem uma API REST comum que você pode acessar diretamente por meio de uma linguagem de programação ou utilitário, como o Curl. Os principais destaques e benefícios da API são apresentados abaixo.



Para acessar a API REST, você precisa primeiro fazer login na interface de usuário da Web Astra e gerar um token de API. Você deve incluir o token em cada solicitação de API.

Desenvolvido com base na TECNOLOGIA REST

A API Astra Control foi criada usando a TECNOLOGIA REST e as práticas recomendadas atuais. A tecnologia principal inclui HTTP, JSON e RBAC.

Suporte para os dois modelos de implantação do Astra Control

O Astra Control Service é usado no ambiente de nuvem pública enquanto o Astra Control Center é para suas implantações locais. Há uma API REST compatível com ambos os modelos de implantação.

Limpar o mapeamento entre os recursos de endpoint REST e o modelo de objeto

Os pontos de extremidade REST externos usados para acessar o mapa de recursos a um modelo de objeto consistente mantido internamente pelo serviço Astra. O modelo de objeto é projetado usando modelagem de relacionamento de entidade (ER) que ajuda a definir claramente as ações e respostas da API.

Conjunto rico de parâmetros de consulta

A API REST fornece um conjunto rico de parâmetros de consulta que você pode usar para acessar as coleções de recursos. Algumas das operações suportadas incluem filtragem, classificação e paginação.

Alinhamento com a IU da Web Astra Control

O design da interface de usuário da Web Astra está alinhado com a API REST e, portanto, há consistência entre os dois caminhos de acesso e a experiência do usuário.

Depuração robusta e dados de determinação de problemas

A API REST do Astra Control fornece um recurso robusto de depuração e determinação de problemas, incluindo eventos do sistema e notificações do usuário.

Processos de fluxo de trabalho

Um conjunto de fluxos de trabalho é fornecido para ajudar no desenvolvimento de seu código de automação. Os fluxos de trabalho são organizados em duas categorias principais: Infraestrutura e gerenciamento.

Base para tecnologias avançadas de automação

Além de acessar a API REST diretamente, você pode usar outras tecnologias de automação baseadas na API REST.

Comece agora

Antes de começar

Você pode se preparar rapidamente para começar a usar a API REST do Astra Control revisando as etapas descritas abaixo.

Rever conceitos REST e implementação

Certifique-se de consultar "[Implementação principal do REST](#)" informações sobre conceitos REST e detalhes sobre como a API REST do Astra Control foi projetada.

Ter credenciais de conta Astra

Você precisará de credenciais Astra para fazer login na interface de usuário da Web Astra e gerar um token de API. Com o Astra Control Center, você gerencia essas credenciais localmente. Com o Astra Control Service, as credenciais da conta são mantidas pelo serviço **Auth0**.

Obtenha mais informações

Você deve estar ciente dos recursos de informações adicionais, conforme sugerido no "[Recursos adicionais](#)".

Obtenha um token de API

Você precisa ter um token de acesso à API para usar a API REST do Astra Control.



Os tokens da API Astra nunca expiram, no entanto, você pode revogar um token quando ele não for mais necessário.

Antes de começar

Você precisa de credenciais para uma conta Astra.

Sobre esta tarefa

Essa tarefa gera um token de API na interface Web do Astra. Você também deve recuperar o ID da conta, que também é necessário para fazer uma chamada à API.

Passos

1. Faça login no Astra usando suas credenciais de conta.

Acesse o seguinte site do Astra Control Service: "<https://astra.netapp.io>"

2. Clique no ícone de figura no canto superior direito da página e selecione **Acesso à API**.
3. Clique em **Generate API token** na página e na janela pop-up clique em **Generate API token**.
4. Clique no ícone para copiar a string de token para a área de transferência e salvá-la no editor.
5. Copie e salve o ID da conta que está disponível na mesma página.

Depois de terminar

Ao acessar a API REST do Astra Control por meio do Curl ou de uma linguagem de programação, você deve incluir o token portador da API no `Authorization` cabeçalho da solicitação. Para revogar o token, "[Segurança](#)" consulte .

Olá mundo

Você pode emitir um simples comando Curl na CLI da sua estação de trabalho para começar a usar a API REST do Astra Control e confirmar sua disponibilidade.

Antes de começar

O utilitário Curl deve estar disponível na estação de trabalho local. Você também deve ter um token de API e o identificador de conta associado. Consulte ["Obtenha um token de API"](#) para obter mais informações.

Curl exemplo

O seguinte comando Curl recupera uma lista de usuários Astra. Forneça o <ACCOUNT_ID> e o <API_TOKEN> apropriados, conforme indicado.

```
curl --location --request GET
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/core/v1/users' --header
'Content-Type: application/json' --header 'Authorization: Bearer
<API_TOKEN>'
```

Exemplo de saída JSON

```
{
  "items": [
    [
      "David",
      "Peterson",
      "844ec6234-11e0-49ea-8434-a992a6270ec1"
    ],
    [
      "Scott",
      "Morris",
      "2a3e227c-fda7-4145-a86c-ed9aa0183a6c"
    ]
  ],
  "metadata": {}
}
```

Prepare-se para usar os fluxos de trabalho

Você deve estar familiarizado com a organização e o formato dos workflows do Astra antes de usá-los em uma implantação ao vivo.

Introdução

Um *workflow* é uma sequência de uma ou mais etapas necessárias para realizar uma tarefa ou objetivo administrativo específico. Cada etapa em um fluxo de trabalho do Astra Control é uma das seguintes:

- Chamada de API REST (com detalhes como exemplos curl e JSON)
- Invocação de outro fluxo de trabalho Astra
- Tarefa relacionada diversos (como tomar uma decisão de projeto necessária)

Os fluxos de trabalho incluem as etapas principais e os parâmetros necessários para realizar cada tarefa. Eles fornecem um ponto de partida para personalizar seu ambiente de automação.

Parâmetros de entrada comuns

Os parâmetros de entrada descritos abaixo são comuns a todas as amostras curl usadas para ilustrar uma chamada de API REST.



Como esses parâmetros de entrada são universalmente necessários, eles não são descritos mais detalhadamente nos fluxos de trabalho individuais. Se forem utilizados parâmetros de entrada adicionais para um exemplo de curl específico, estes são descritos na seção **parâmetros de entrada adicionais**.

Parâmetros do caminho

O caminho do endpoint usado com cada chamada de API REST inclui os seguintes parâmetros. Consulte também "[Formato de URL](#)" para obter mais informações.

ID da conta

Esse é o valor UUIDv4 que identifica a conta Astra onde a operação da API é executada. "[Obtenha um token de API](#)" Consulte para obter mais informações sobre como localizar o ID da sua conta.

Cabeçalhos de solicitação

Existem vários cabeçalhos de solicitação que você pode precisar incluir dependendo da chamada da API REST.

Autorização

Todas as chamadas de API nos fluxos de trabalho precisam de um token de API para identificar o usuário. Você deve incluir o token no `Authorization` cabeçalho da solicitação. Consulte "[Obtenha um token de API](#)" para obter mais informações sobre como gerar um token de API.

Tipo de conteúdo

Com as solicitações HTTP POST e PUT em que JSON é incluído no corpo da solicitação, você deve declarar o tipo de Mídia com base no recurso Astra. Por exemplo, você pode incluir o cabeçalho `Content-Type: application/astra-appSnap+json` ao criar um snapshot para um aplicativo gerenciado.

Aceitar

Você pode declarar o tipo de Mídia específico do conteúdo esperado na resposta com base no recurso Astra. Por exemplo, você pode incluir o cabeçalho `Accept: application/astra-appBackup+json` ao listar os backups de um aplicativo gerenciado. No entanto, para simplificar, as amostras curl nos fluxos de trabalho aceitam todos os tipos de Mídia.

Apresentação de tokens e identificadores

O token API e outros valores de ID usados com os exemplos curl são opacos sem significado discernível. E assim, para melhorar a legibilidade das amostras, os valores reais de token e ID não são usados. Em vez disso, palavras-chave reservadas menores são usadas que tem vários benefícios:

- As amostras curl e JSON são mais claras e fáceis de entender.
- Como todas as palavras-chave usam o mesmo formato com colchetes e letras maiúsculas, você pode identificar rapidamente o local e o conteúdo a ser inserido ou extraído.
- Nenhum valor é perdido porque os parâmetros originais não podem ser copiados e usados com uma implantação real.

Aqui estão algumas das palavras-chave reservadas comuns usadas nos exemplos curl. Esta lista não é exaustiva e palavras-chave adicionais são usadas conforme necessário. Seu significado deve ser óbvio com base no contexto.

Palavra-chave	Tipo	Descrição
<ACCOUNT_ID>	Caminho	O valor UUIDv4 identificando a conta onde a operação da API é executada.
<API_TOKEN>	Colhedor	O token do portador identificando e autorizando o chamador.
<MANAGED_APP_ID>	Caminho	O valor UUIDv4 identificando o aplicativo gerenciado para a chamada API.

Categorias de fluxo de trabalho

Há duas grandes categorias de workflows do Astra disponíveis com base no seu modelo de implantação. Se você estiver usando o Astra Control Center, comece com os workflows de infraestrutura e prossiga para os workflows de gerenciamento. Ao usar o Astra Control Service, você costuma ir diretamente aos workflows de gerenciamento.



As amostras curl nos fluxos de trabalho usam o URL do Astra Control Service. Você precisa alterar o URL ao usar o Astra Control Center no local, conforme apropriado para seu ambiente.

Workflows de infraestrutura

Esses workflows lidam com a infraestrutura Astra, incluindo credenciais, buckets e back-ends de storage. Elas são necessárias com o Astra Control Center, mas na maioria dos casos também podem ser usadas com o Astra Control Service. Os fluxos de trabalho concentram-se nas tarefas necessárias para estabelecer e manter um cluster gerenciado do Astra.

Fluxos de trabalho de gerenciamento

Você pode usar esses fluxos de trabalho depois de ter um cluster gerenciado. Os workflows se concentram em operações de suporte e proteção de aplicativos, como backup, restauração e clonagem de um aplicativo gerenciado.

Implementação principal do REST

Serviços web REST

Representational State Transfer (REST) é um estilo para a criação de aplicações web distribuídas. Quando aplicado ao design de uma API de serviços da Web, ele estabelece um conjunto de tecnologias e práticas recomendadas principais para expor recursos baseados em servidor e gerenciar seus estados. Embora O REST forneça uma base consistente para o desenvolvimento de aplicativos, os detalhes de cada API podem variar com base nas escolhas específicas de design. Você deve estar ciente das características da API REST do Astra Control antes de usá-la com uma implantação ativa.

Recursos e representação do Estado

Os recursos são os componentes básicos de um sistema baseado na Web. Ao criar um aplicativo REST de serviços da Web, as tarefas iniciais de design incluem:

- Identificação de recursos baseados em sistema ou servidor

Cada sistema usa e mantém recursos. Um recurso pode ser um arquivo, transação comercial, processo ou entidade administrativa. Uma das primeiras tarefas no projeto de um aplicativo baseado em serviços web REST é identificar os recursos.

- Definição de estados de recursos e operações de estado associadas

Os recursos estão sempre em um de um número finito de estados. Os estados, bem como as operações associadas usadas para afetar as mudanças de estado, devem ser claramente definidos.

Pontos de extremidade URI

Todos os recursos REST devem ser definidos e disponibilizados usando um esquema de endereçamento bem definido. Os endpoints onde os recursos estão localizados e identificados usam um URI (Uniform Resource Identifier). O URI fornece uma estrutura geral para criar um nome exclusivo para cada recurso na rede. O Uniform Resource Locator (URL) é um tipo de URI usado com serviços da Web para identificar e acessar recursos. Os recursos são normalmente expostos em uma estrutura hierárquica semelhante a um diretório de arquivos.

Mensagens HTTP

O Hypertext Transfer Protocol (HTTP) é o protocolo usado pelo cliente e servidor de serviços da Web para trocar mensagens de solicitação e resposta sobre os recursos. Como parte do projeto de um aplicativo de serviços da Web, os métodos HTTP são mapeados para os recursos e as ações de gerenciamento de estado correspondentes. HTTP está sem estado. Portanto, para associar um conjunto de solicitações e respostas relacionadas como parte de uma transação, informações adicionais devem ser incluídas nos cabeçalhos HTTP carregados com os fluxos de dados de solicitação e resposta.

Formatação JSON

Embora as informações possam ser estruturadas e transferidas entre um cliente e um servidor de serviços da Web de várias maneiras, a opção mais popular é JavaScript Object Notation (JSON). JSON é um padrão da indústria para representar estruturas de dados simples em texto simples e é usado para transferir informações de estado descrevendo os recursos. A API REST DO Astra Control usa JSON para formatar os dados transportados no corpo de cada solicitação e resposta HTTP.

Recursos e coleções

A API REST do Astra Control fornece acesso a instâncias de recursos e coleções de instâncias de recursos.



Conceitualmente um resource * REST é semelhante a um objeto * conforme definido com as linguagens e sistemas de programação orientada a objetos (OOP). Às vezes, esses termos são usados de forma intercambiável. Mas, em geral, "recurso" é preferível quando usado no contexto da API REST externa enquanto "objeto" é usado para os dados de instância com estado correspondente armazenados no servidor.

Atributos dos recursos do Astra

A API REST do Astra Control está em conformidade com os princípios de design RESTful. Cada instância de recurso Astra é criada com base em um tipo de recurso bem definido. Um conjunto de instâncias de recursos do mesmo tipo é chamado de **Collection**. As chamadas API atuam sobre recursos individuais ou coleções de recursos.

Tipos de recursos

Os tipos de recursos incluídos na API REST do Astra Control têm as seguintes características:

- Cada tipo de recurso é definido usando um esquema (normalmente em JSON)
- Cada esquema de recursos inclui o tipo de recurso e a versão
- Os tipos de recursos são globalmente únicos

Instâncias de recursos

As instâncias de recursos disponíveis pela API REST do Astra Control têm as seguintes características:

- As instâncias de recurso são criadas com base em um único tipo de recurso
- O tipo de recurso é indicado utilizando o valor tipo de material
- As instâncias são compostas por dados com estado que são mantidos pelo serviço Astra
- Cada instância é acessível através de uma URL única e de longa duração
- Nos casos em que uma instância de recurso pode ter mais de uma representação, diferentes tipos de Mídia podem ser usados para solicitar a representação desejada

Coleções de recursos

As coleções de recursos disponíveis pela API REST do Astra Control têm as seguintes características:

- O conjunto de instâncias de recursos de um único tipo de recurso é conhecido como uma coleção
- Coleções de recursos têm uma URL única e de longa duração

Identificadores de instância

Cada instância de recurso recebe um identificador quando é criada. Este identificador é um valor UUIDv4 de 128 bits. Os valores UUIDv4 atribuídos são globalmente únicos e imutáveis. Depois de emitir uma chamada de API que cria uma nova instância, um URL com o ID associado é retornado ao chamador em um `Location` cabeçalho da resposta HTTP. Você pode extrair o identificador e usá-lo em chamadas subsequentes quando se refere à instância de recurso.



O identificador de recurso é a chave primária usada para coleções.

Estrutura comum para recursos do Astra

Todos os recursos do Astra Control são definidos usando uma estrutura comum.

Dados comuns

Cada recurso Astra contém os valores-chave mostrados na tabela a seguir.

Chave	Descrição
tipo	Um tipo de recurso globalmente único que é conhecido como tipo de recurso .
versão	Um identificador de versão que é conhecido como a versão resource .
id	Um identificador global único que é conhecido como resource identifier .
metadados	Um objeto JSON contendo várias informações, incluindo rótulos de usuário e sistema.

Objeto de metadados

O objeto JSON de metadados incluído com cada recurso Astra contém os valores-chave mostrados na tabela a seguir.

Chave	Descrição
etiquetas	Matriz JSON de rótulos especificados pelo cliente associados ao recurso.
CriaçãoTimestamp	String JSON contendo um carimbo de data/hora indicando quando o recurso foi criado.
Alteração do Timestamp	String JSON contendo um carimbo de data/hora formatado ISO-8601 indicando quando o recurso foi alterado pela última vez.
CreatedBy	String JSON contendo o identificador UUIDv4 do ID do usuário que criou o recurso. Se o recurso foi criado por um componente interno do sistema e não houver UUID associado à entidade criadora, o UUID null é usado.

Estado do recurso

Recursos selecionados um `state` valor que é usado para orquestrar transições de ciclo de vida e controlar o acesso.

Detalhes HTTP

A API REST do Astra Control usa HTTP e parâmetros relacionados para agir sobre os recursos e coleções. Detalhes da implementação HTTP são apresentados abaixo.

Transações de API e o modelo CRUD

A API REST do Astra Control implementa um modelo transacional com operações bem definidas e transições de estado.

Transação de API de solicitação e resposta

Cada chamada de API REST é executada como uma solicitação HTTP para o serviço Astra. Cada solicitação gera uma resposta associada de volta ao cliente. Esse par de solicitação-resposta pode ser considerado uma transação de API.

Suporte para o modelo operacional CRUD

Cada uma das instâncias e coleções de recursos disponíveis por meio da API REST do Astra Control é acessada com base no modelo **CRUD**. Existem quatro operações, cada uma delas mapeia para um único método HTTP. As operações incluem:

- Criar
- Leia
- Atualização
- Eliminar

Para alguns recursos do Astra, apenas um subconjunto dessas operações é suportado. Você deve revisar o ["Referência da API"](#) para obter mais informações sobre uma chamada de API específica.

Métodos HTTP

Os métodos HTTP ou verbos suportados pela API são apresentados na tabela abaixo.

Método	CRUD	Descrição
OBTER	Leia	Recupera propriedades de objeto para uma instância ou coleção de recursos. Isso é considerado uma operação list quando usado com uma coleção.
POST	Criar	Cria uma nova instância de recurso com base nos parâmetros de entrada. O URL de longo prazo é retornado em um <code>Location</code> cabeçalho de resposta.
COLOQUE	Atualização	Atualiza uma instância de recurso inteira com o corpo de solicitação JSON fornecido. Os valores-chave que não são modificáveis pelo usuário são preservados.
ELIMINAR	Eliminar	Exclui uma instância de recurso existente.

Cabeçalhos de solicitação e resposta

A tabela a seguir resume os cabeçalhos HTTP usados com a API REST do Astra Control.



"RFC 7232" Consulte e "RFC 7233" para obter mais informações.

Colhedor	Tipo	Notas de utilização
Aceitar	Pedido	Se o valor for "/" ou não for fornecido, <code>application/json</code> será retornado no cabeçalho de resposta <code>Content-Type</code> . Se o valor estiver definido para o tipo de Mídia de recurso Astra, o mesmo tipo de Mídia será retornado no cabeçalho <code>Content-Type</code> .
Autorização	Pedido	Token de portador com a chave API para o usuário.
Tipo de conteúdo	Resposta	Devolvido com base no <code>Accept</code> cabeçalho da solicitação.
ETAG	Resposta	Incluído com um sucesso como definido com RFC 7232. O valor é uma representação hexadecimal do valor MD5 para todo o recurso JSON.
If-Match	Pedido	Um cabeçalho de solicitação de pré-condição implementado conforme descrito na seção 3,1 RFC 7232 e suporte para solicitações PUT .
Se-modificado-desde	Pedido	Um cabeçalho de solicitação de pré-condição implementado conforme descrito na seção 3,4 RFC 7232 e suporte para solicitações PUT .
If-Unmodified-since	Pedido	Um cabeçalho de solicitação de pré-condição implementado conforme descrito na seção 3,4 RFC 7232 e suporte para solicitações PUT .
Localização	Resposta	Contém a URL completa do recurso recém-criado.

Parâmetros de consulta

Os seguintes parâmetros de consulta estão disponíveis para uso com coleções de recursos. Consulte "[Trabalhando com coleções](#)" para obter mais informações.

Parâmetro de consulta	Descrição
incluir	Contém os campos que devem ser retornados ao ler uma coleção.
filtro	Indica os campos que devem corresponder para que um recurso seja retornado ao ler uma coleção.
Ordenar	Determina a ordem de classificação dos recursos retornados ao ler uma coleção.
limite	Limita o número máximo de recursos retornados ao ler uma coleção.
ignorar	Define o número de recursos para passar e pular ao ler uma coleção.
contar	Indica se o número total de recursos deve ser retornado no objeto metadados.

Códigos de status HTTP

Os códigos de status HTTP usados pela API REST do Astra Control são descritos abaixo.



A API REST do Astra Control também usa o padrão **Detalhes do problema para APIs HTTP**. Consulte "[Diagnóstico e suporte](#)" para obter mais informações.

Código	Significado	Descrição
200	OK	Indica sucesso para chamadas que não criam uma nova instância de recurso.
201	Criado	Um objeto é criado com sucesso e o cabeçalho de resposta de localização inclui o identificador exclusivo para o objeto.
204	Nenhum conteúdo	A solicitação foi bem-sucedida, embora nenhum conteúdo tenha sido retornado.
400	Pedido incorreto	A entrada de solicitação não é reconhecida ou é inadequada.
401	Não autorizado	O usuário não está autorizado e deve autorizar.
403	Proibido	O acesso é negado devido a um erro de autorização.
404	Não encontrado	O recurso referido na solicitação não existe.
409	Conflito	Uma tentativa de criar um objeto falhou porque o objeto já existe.
500	Erro interno	Ocorreu um erro interno geral no servidor.
503	Serviço indisponível	O serviço não está pronto para lidar com a solicitação por algum motivo.

Formato de URL

A estrutura geral da URL usada para acessar uma instância ou coleção de recursos através da API REST é composta por vários valores. Esta estrutura reflete o modelo de objeto subjacente e o design do sistema.

Conta como raiz

A raiz do caminho do recurso para cada endpoint REST é a conta Astra. E assim todos os caminhos no URL começam com `/account/{account_id}` onde `account_id` é o valor UUIDv4 exclusivo para a conta. Estrutura interna isso reflete um design em que todo o acesso a recursos é baseado em uma conta específica.

Categoria de recurso de endpoint

Os pontos de extremidade de recursos do Astra se enquadram em três categorias diferentes:

- (`/core`Núcleo`)
- Aplicativo gerenciado (`/k8s`)
- Topologia (`/topology`)

Consulte "[Recursos](#)" para obter mais informações.

Versão da categoria

Cada uma das três categorias de recursos tem uma versão global que controla a versão dos recursos acessados. Por convenção e definição, mover para uma nova versão principal de uma categoria de recurso (como, de `/v1` para `/v2`) introduzirá alterações de quebra na API.

Instância ou coleção de recursos

Uma combinação de tipos de recursos e identificadores pode ser usada no caminho, com base no acesso a uma instância ou coleção de recursos.

Exemplo

- Caminho do recurso

Com base na estrutura apresentada acima, um caminho típico para um endpoint é:

`/accounts/{account_id}/core/v1/users.`

- URL completo

O URL completo para o endpoint correspondente é: [https://astra.netapp.io/accounts/{account_id}/core/v1/users.](https://astra.netapp.io/accounts/{account_id}/core/v1/users)

Considerações adicionais DE DESCANSO

Segurança

A API REST do Astra Control fornece várias camadas de segurança.



Todo o tráfego de rede HTTP é protegido usando o padrão de segurança da camada de transporte (TLS).

Tokens de API Astra

Para usar a API REST do Astra Control, você deve fornecer um token de API em todas as solicitações `Authorization` no cabeçalho da solicitação. Observe o seguinte:

- Você pode gerar um token de API na interface de usuário da Web Astra.
- Um token nunca expira depois que ele é criado.
- Você pode revogar um token a qualquer momento na interface de usuário da Web Astra.

Consulte "[Obtenha um token de API](#)" para obter mais informações.

Revogando um token de acesso à API

Você pode revogar um token de API na interface da Web Astra quando não for mais necessário.

Antes de começar

Você precisa de uma conta para o serviço Astra. Você também deve identificar os tokens que deseja revogar.

Sobre esta tarefa

Depois que um token é revogado, ele é imediatamente e permanentemente inutilizável.

Passos

1. Faça login no Astra usando suas credenciais de conta.

Acesse o seguinte site do Astra Control Service: "<https://astra.netapp.io>"

2. Clique no ícone de figura no canto superior direito da página e selecione **Acesso à API**.
3. Selecione o token ou tokens que você deseja revogar.
4. Na caixa suspensa **ações**, clique em **revogar tokens**.

Funções e controle de acesso

Cada usuário do Astra é atribuído a uma única função que determina as ações que podem ser executadas. As funções são organizadas em uma hierarquia conforme descrito na tabela abaixo.

Função	Descrição
Proprietário	Tem todas as permissões da função Admin e também pode excluir contas Astra.

Função	Descrição
Administrador	Tem todas as permissões da função Membro e também pode convidar os usuários para participar de uma conta.
Membro	Pode gerenciar totalmente a aplicação Astra e os recursos de computação.
Visualizador	Restrito à visualização apenas de recursos.

Trabalhando com coleções

A API REST do Astra Control fornece várias maneiras diferentes de acessar coleções de recursos por meio dos parâmetros de consulta definidos.

Selecionar valores

Você pode especificar quais pares de chave-valor devem ser retornados para cada instância de recurso usando o `include` parâmetro. Todas as instâncias são retornadas no corpo de resposta.

Filtragem

A filtragem de recursos de coleta permite que um usuário da API especifique condições que determinam se um recurso é retornado no corpo da resposta. O `filter` parâmetro é usado para indicar a condição de filtragem.

Ordenação

A classificação de recursos de coleta permite que um usuário da API especifique a ordem em que os recursos são retornados no corpo de resposta. O `orderBy` parâmetro é usado para indicar a condição de filtragem.

Paginação

Você pode impor a paginação restringindo o número de instâncias de recursos retornadas em uma solicitação usando o `limit` parâmetro.

Contar

Se você incluir o parâmetro booleano `count` definido como `true`, o número de recursos na matriz retornada para uma determinada resposta será fornecido na seção metadados.

Diagnóstico e suporte

Há vários recursos de suporte disponíveis com a API REST do Astra Control que podem ser usados para diagnósticos e depuração.

Recursos de API

Há vários recursos do Astra expostos por meio de recursos de API que fornecem informações de diagnóstico e suporte.

Tipo	Descrição
Evento	Atividades do sistema registradas como parte do processamento do Astra.
Notificação	Um subconjunto dos Eventos que são considerados importantes o suficiente para ser apresentado ao usuário.

Tipo	Descrição
Notificação não lida	As notificações que ainda não foram lidas ou recuperadas pelo usuário.

Recursos e endpoints

Você pode usar os recursos fornecidos pela API REST do Astra Control para automatizar uma implantação Astra. Cada recurso é acessado por meio de um ou mais endpoints. Esta seção fornece uma introdução aos RECURSOS REST que você pode usar como parte do Planejamento de uma implantação de automação.



O formato do caminho e URL completo usados para acessar os recursos do Astra Control é baseado em vários valores. Consulte "[Formato de URL](#)" para obter mais informações. Consulte também "[Referência da API](#)" para obter detalhes sobre como usar os recursos e pontos de extremidade do Astra.

Recursos REST e pontos de extremidade do Astra Control

Os principais pontos de extremidade de recurso fornecidos na API REST do Astra Control são organizados em três categorias. Cada recurso pode ser acessado com o conjunto completo de operações CRUD (criar, ler, atualizar, excluir), exceto onde indicado.

A coluna **Release** indica a versão Astra quando o recurso foi introduzido pela primeira vez. Este campo está em negrito para recursos recém-adicionados com a versão atual.

Recursos básicos

Os principais pontos de extremidade dos recursos fornecem os serviços básicos necessários para estabelecer e manter o ambiente de tempo de execução do Astra.

Recurso	Solte	Descrição
ASUP	21,08	Os recursos do ASUP representam os pacotes do AutoSupport encaminhados para o suporte do NetApp.
Credencial	21,04	Os recursos de credenciais contêm informações relacionadas à segurança que podem ser usadas com usuários, clusters, buckets e back-ends de storage do Astra.
Direitos	21,08	Os recursos de direito representam os recursos e capacidades disponíveis para uma conta com base nas licenças e assinaturas ativas.
Evento	21,04	Os recursos do evento representam todos os eventos que ocorrem no sistema, incluindo o subconjunto classificado como notificações.
Recurso	21,08	Os recursos do recurso representam os recursos selecionados do Astra que você pode consultar para determinar se eles estão ativados ou desativados no sistema. O acesso é limitado a somente leitura.
Licença	21,08	Os recursos de licença representam as licenças disponíveis para uma conta Astra.
Notificação	21,04	Os recursos de notificação representam eventos Astra que têm um destino de notificação. O acesso é fornecido por usuário.

Recurso	Solte	Descrição
Vinculação de função	21,04	Os recursos de vinculação de função representam as relações entre pares específicos de usuários e contas. Além da ligação entre os dois, um conjunto de permissões é especificado para cada um através de uma função específica.
Definição	21,08	A configuração de recursos representa um conjunto de pares de valor-chave que descrevem um recurso para uma conta Astra específica.
Subscrição	21,08	Os recursos de subscrição representam as subscrições ativas de uma conta Astra.
Token	21,04	Os recursos do token representam os tokens disponíveis para acessar programaticamente a API REST DO Astra Control.
Notificação não lida	21,04	Os recursos de notificação não lidos representam notificações atribuídas a um usuário específico, mas ainda não lidas.
Utilizador	21,04	Os recursos de usuário representam usuários do Astra capazes de acessar o sistema com base em sua função definida.

Recursos de aplicativos gerenciados

Os pontos de extremidade de recursos de aplicação gerenciados fornecem acesso às aplicações Kubernetes gerenciadas.

Recurso	Solte	Descrição
Ativo da aplicação	21,04	Os recursos de ativos da aplicação representam coleções internas de informações de estado necessárias para gerenciar as aplicações Astra.
Backup de aplicativos	21,04	Os recursos de backup de aplicativos representam backups dos aplicativos gerenciados.
Snapshot da aplicação	21,04	Os recursos de snapshot do aplicativo representam snapshots dos aplicativos gerenciados.
Aplicação gerenciada	21,04	Os recursos gerenciados da aplicação representam as aplicações Kubernetes gerenciadas pelo Astra.
Programação	21,04	Os recursos do cronograma representam operações de proteção de dados agendadas para os aplicativos gerenciados como parte de uma política de proteção de dados.

Recursos de topologia

Os pontos de extremidade dos recursos de topologia fornecem acesso aos aplicativos não gerenciados e aos recursos de storage.

Recurso	Solte	Descrição
Aplicação	21,04	Os recursos da aplicação representam todas as aplicações Kubernetes, incluindo as não gerenciadas pelo Astra.
Balde	21,08	Os recursos de bucket representam os buckets em nuvem do S3 usados para armazenar backups das aplicações gerenciadas pelo Astra.

Recurso	Solte	Descrição
Nuvem	21,08	Os recursos de nuvem representam nuvens às quais os clientes Astra podem se conectar para gerenciar clusters e aplicações.
Cluster	21,08	Os recursos do cluster representam os clusters do Kubernetes não gerenciados pelo Kubernetes.
Cluster gerenciado	21,08	Os recursos do cluster gerenciado representam os clusters do Kubernetes atualmente gerenciados pelo Kubernetes.
Back-end de storage	21,08	Os recursos de back-end de storage representam fornecedores de serviços de storage que podem ser usados pelos clusters e aplicações gerenciados do Astra.
Classe de armazenamento	21,08	Os recursos da classe de armazenamento representam diferentes classes ou tipos de armazenamento descobertos e disponíveis para um cluster gerenciado específico.
Volume	21,04	Os recursos de volume representam os volumes de storage do Kubernetes associados às aplicações gerenciadas.

Recursos e endpoints adicionais

Há vários recursos e pontos de extremidade adicionais que você pode usar para dar suporte a uma implantação do Astra.



Esses recursos e pontos de extremidade não estão incluídos atualmente na documentação de referência da API REST do Astra Control.

OpenAPI

Os endpoints OpenAPI fornecem acesso ao documento JSON OpenAPI atual e a outros recursos relacionados.

OpenMetrics

Os endpoints OpenMetrics fornecem acesso às métricas da conta por meio do recurso OpenMetrics. O suporte está disponível com o modelo de implantação do Astra Control Center.

Workflows de infraestrutura

Antes de começar

Use esses workflows para criar e manter a infraestrutura usada com o modelo de implantação do Astra Control Center. Na maioria dos casos, os workflows também podem ser usados com o Astra Control Service.



Esses fluxos de trabalho podem ser expandidos e aprimorados pelo NetApp a qualquer momento, portanto, você deve revisá-los periodicamente.

Preparação geral

Antes de usar qualquer um dos workflows do Astra, revise "[Prepare-se para usar os fluxos de trabalho](#)".

Categorias de fluxo de trabalho

Os fluxos de trabalho de infraestrutura são organizados em diferentes categorias para facilitar a localização do que você deseja.

Categoria	Descrição
Identidade e acesso	Esses fluxos de trabalho permitem gerenciar identidade e como o Astra é acessado. Os recursos incluem usuários, credenciais e tokens.
Baldes	Você pode usar esses fluxos de trabalho para criar e gerenciar os buckets do S3 usados para armazenar backups.
Armazenamento	Esses fluxos de trabalho permitem adicionar e manter backends e volumes de armazenamento.
Clusters	É possível adicionar clusters gerenciados do Kubernetes que permitem proteger e dar suporte às aplicações que eles contêm.

Identidade e acesso

Listar usuários

Você pode listar os usuários que estão definidos para uma conta Astra específica.

1. Liste os usuários

Execute a seguinte chamada de API REST.

Método HTTP	Caminho
OBTER	/Conta/core/v1/users

Parâmetros de entrada adicionais

Além dos parâmetros comuns com todas as chamadas de API REST, os seguintes parâmetros também são

usados nos exemplos curl para esta etapa.

Parâmetro	Tipo	Obrigatório	Descrição
incluir	Consulta	Não	Opcionalmente, selecione os valores que você deseja retornar na resposta.

Curl exemplo: Retorna todos os dados para todos os usuários

```
curl --location -i --request GET
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/core/v1/users' --header
'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

Curl exemplo: Retorna o primeiro nome, sobrenome e id para todos os usuários

```
curl --location -i --request GET
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/core/v1/users?include=first
Name,lastName,id' --header 'Accept: */*' --header 'Authorization: Bearer
<API_TOKEN>'
```

Exemplo de saída JSON

```
{
  "items": [
    [
      "David",
      "Peterson",
      "844ec6234-11e0-49ea-8434-a992a6270ec1"
    ],
    [
      "Scott",
      "Morris",
      "2a3e227c-fda7-4145-a86c-ed9aa0183a6c"
    ]
  ],
  "metadata": {}
}
```

Baldes

Listar buckets

Você pode listar os buckets do S3 definidos para uma conta específica do Astra.

1. Liste os buckets

Execute a seguinte chamada de API REST.

Método HTTP	Caminho
OBTER	/Account/v1/buckets

Curl exemplo: Retorna todos os dados para todos os buckets

```
curl --location -i --request GET
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/topology/v1/buckets'
--header 'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

Armazenamento

Listar backends de armazenamento

Você pode listar os backends de armazenamento disponíveis.

1. Liste os buckets

Execute a seguinte chamada de API REST.

Método HTTP	Caminho
OBTER	/Account/topology/v1/storageBackends

Curl exemplo: Retorna todos os dados para todos os backends de armazenamento

```
curl --location -i --request GET
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/topology/v1/storageBackends'
--header 'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

Exemplo de saída JSON

```

{
  "items": [
    {
      "backendCredentialsName": "10.191.77.177",
      "backendName": "myinchunhcluster-1",
      "backendType": "ONTAP",
      "backendVersion": "9.8.0",
      "configVersion": "Not applicable",
      "health": "Not applicable",
      "id": "46467c16-1585-4b71-8e7f-f0bc5ff9da15",
      "location": "nalab2",
      "metadata": {
        "createdBy": "4c483a7e-207b-4f9a-87b7-799a4629d7c8",
        "creationTimestamp": "2021-07-30T14:26:19Z",
        "modificationTimestamp": "2021-07-30T14:26:19Z"
      },
      "ontap": {
        "backendManagementIP": "10.191.77.177",
        "managementIPs": [
          "10.191.77.177",
          "10.191.77.179"
        ]
      },
      "protectionPolicy": "Not applicable",
      "region": "Not applicable",
      "state": "Running",
      "stateUnready": [],
      "type": "application/astra-storageBackend",
      "version": "1.0",
      "zone": "Not applicable"
    }
  ]
}

```

Clusters

Listar clusters gerenciados

É possível listar os clusters de Kubernetes gerenciados atualmente pelo Astra.

1. Liste os clusters

Execute a seguinte chamada de API REST.

Método HTTP	Caminho
OBTER	/Account//topoly/v1/managedclusters

Exemplo de curl: Retorna todos os dados de todos os clusters

```
curl --location -i --request GET
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/topology/v1/managedClusters
' --header 'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

Fluxos de trabalho de gerenciamento

Antes de começar

Use esses workflows como parte da administração das aplicações em um cluster gerenciado do Astra.



Esses fluxos de trabalho podem ser expandidos e aprimorados pelo NetApp a qualquer momento, portanto, você deve revisá-los periodicamente.

Preparação geral

Antes de usar qualquer um dos workflows do Astra, revise ["Prepare-se para usar os fluxos de trabalho"](#).

Categorias de fluxo de trabalho

Os fluxos de trabalho de gerenciamento são organizados em diferentes categorias para facilitar a localização do que você deseja.

Categoria	Descrição
Controle de aplicação	Esses fluxos de trabalho permitem que você controle os aplicativos gerenciados e não gerenciados. Você pode listar os aplicativos, bem como criar e remover um aplicativo gerenciado.
Proteção de aplicação	Use esses fluxos de trabalho para proteger suas aplicações gerenciadas por meio de snapshots e backups.
Clonagem e restauração de aplicações	Esse fluxo de trabalho descreve como clonar e restaurar aplicativos gerenciados.
Suporte	Há vários fluxos de trabalho disponíveis para depurar e dar suporte às suas aplicações, bem como o ambiente geral do Kubernetes.

Considerações adicionais

Há várias considerações adicionais ao usar os fluxos de trabalho de gerenciamento.

Clonar uma aplicação

Há algumas coisas a considerar ao clonar um aplicativo. Os parâmetros descritos abaixo fazem parte da entrada JSON.

Identificador do cluster de origem

O valor de `sourceClusterID` sempre identifica o cluster onde o aplicativo original está instalado.

Identificador de cluster

O valor de `clusterID` identifica o cluster onde o novo aplicativo será instalado.

- Ao clonar dentro do mesmo cluster `clusterID` e `sourceClusterID` ter o mesmo valor.
- Ao clonar entre clusters, os dois valores são diferentes e `clusterID` devem ser a ID do cluster de

destino.

Namespaces

O `namespace` valor deve ser diferente do aplicativo de origem original. Além disso, o namespace para o clone não pode existir e o Astra o criará.

Backups e snapshots

Opcionalmente, você pode clonar um aplicativo a partir de um backup ou snapshot existente usando os `backupID` parâmetros ou `snapshotID`. Se você não fornecer um backup ou snapshot, o Astra criará primeiro um backup da aplicação e, em seguida, clonará a partir do backup.

Restaurar uma aplicação

Aqui estão algumas coisas a considerar ao restaurar um aplicativo.

- Restaurar um aplicativo é muito semelhante à operação clone.
- Ao restaurar um aplicativo, você deve fornecer um backup ou um snapshot.

Controlo de aplicações

Liste os aplicativos não gerenciados

Você pode listar as aplicações que não são gerenciadas pelo Astra no momento. Você pode fazer isso como parte da seleção de um aplicativo a ser gerenciado.



Este fluxo de trabalho lista todas as aplicações Astra. Você pode olhar para a saída para determinar quais aplicativos não são gerenciados examinando o `managedState` campo.

1. Liste os aplicativos

Execute a seguinte chamada de API REST.

Método HTTP	Caminho
OBTER	/Account/topology/v1/apps

Parâmetros de entrada adicionais

Além dos parâmetros comuns com todas as chamadas de API REST, os seguintes parâmetros também são usados nos exemplos curl para esta etapa.

Parâmetro	Tipo	Obrigatório	Descrição
incluir	Consulta	Não	Opcionalmente, selecione os valores que você deseja retornar na resposta.

Curl exemplo: Retorna todos os dados para todos os aplicativos

```
curl --location -i --request GET
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/topology/v1/apps' --header
'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

Curl exemplo: Retorna o nome, id e managedState para todos os aplicativos

```
curl --location -i --request GET
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/topology/v1/apps?include=na
me,id,managedState' --header 'Accept: */*' --header 'Authorization: Bearer
<API_TOKEN>'
```

Exemplo de saída JSON

```
{
  "items": [
    [
      "maria",
      "eed19f78-0884-4792-bb7a-313258c6b0b1",
      "unmanaged"
    ],
    [
      "mariadb-mariadb",
      "8da20fff-c69c-4170-bb0d-e4f91c5a1333",
      "managed"
    ],
    [
      "test-postgres-app",
      "1ee6235b-cda1-45cb-8d4c-630bdb8b41a5",
      "unmanaged"
    ],
    [
      "postgres1-postgresql",
      "e591ee59-ea90-4a9f-8e6c-d2b6e8647096",
      "unmanaged"
    ],
    [
      "kube-system",
      "077a2f73-4b51-4d04-8c6c-f63b3b069755",
      "unmanaged"
    ],
    [
      "trident",
      "5b6fc28f-e308-4653-b9d2-6d66a764d2e1",
      "unmanaged"
    ],
    [
      "postgres1-postgresql-clone",
      "06be05c5-763e-4d73-bd06-1f27f5f2e130",
      "unmanaged"
    ],
    [
      "davidns-postgres-app",
      "11e046b7-ec64-4184-85b3-debcc3b1da4d",
      "managed"
    ]
  ],
  "metadata": {}
}
```

Liste os aplicativos gerenciados

Você pode listar as aplicações que atualmente são gerenciadas pelo Astra. Você pode fazer isso como parte de encontrar os snapshots ou backups de um aplicativo específico.

1. Liste os aplicativos

Execute a seguinte chamada de API REST.

Método HTTP	Caminho
OBTER	/Conta//k8s/v1/managedApps

Parâmetros de entrada adicionais

Além dos parâmetros comuns com todas as chamadas de API REST, os seguintes parâmetros também são usados nos exemplos curl para esta etapa.

Parâmetro	Tipo	Obrigatório	Descrição
incluir	Consulta	Não	Opcionalmente, selecione os valores que você deseja retornar na resposta.

Curl exemplo: Retorna todos os dados para todos os aplicativos

```
curl --location -i --request GET
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/k8s/v1/managedApps'
--header 'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

Curl exemplo: Retorna o nome, id e estado de todos os aplicativos

```
curl --location -i --request GET
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/k8s/v1/managedApps?include=
name,id,state' --header 'Accept: */*' --header 'Authorization: Bearer
<API_TOKEN>'
```

Exemplo de saída JSON

```

{
  "items": [
    [
      "test-postgres-app",
      "1ee6235b-cda1-45cb-8d4c-630bdb8b41a5",
      "running"
    ]
  ],
  "metadata": {}
}

```

Obtenha um aplicativo gerenciado

Você pode recuperar todas as variáveis de recurso descrevendo um único aplicativo gerenciado.

Antes de começar

Você deve ter o ID do aplicativo gerenciado que deseja recuperar. Se necessário, você pode usar o fluxo de trabalho ["Liste os aplicativos gerenciados"](#) para localizar o aplicativo.

1. Obtenha o aplicativo

Execute a seguinte chamada de API REST.

Método HTTP	Caminho
OBTER	/Accounts/_id/k8s/v1/managedApps/_id

Parâmetros de entrada adicionais

Além dos parâmetros comuns com todas as chamadas de API REST, os seguintes parâmetros também são usados nos exemplos curl para esta etapa.

Parâmetro	Tipo	Obrigatório	Descrição
id da aplicação gerida	Caminho	Sim	Valor de ID do aplicativo gerenciado a ser recuperado.

Curl exemplo: Retorna todos os dados para o aplicativo

```

curl --location -i --request GET
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/k8s/v1/managedApps/<MANAGED_APP_ID>' --header 'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'

```

Gerenciar um aplicativo

Você pode criar uma aplicação gerenciada com base em uma aplicação já conhecida pelo Astra. Quando um aplicativo é gerenciado, você pode protegê-lo fazendo backups e snapshots regulares.

Antes de começar

Você deve ter o ID do aplicativo descoberto que deseja gerenciar. Se necessário, você pode usar o fluxo de trabalho "[Liste os aplicativos não gerenciados](#)" para localizar o aplicativo.

1. Gerencie o aplicativo

Execute a seguinte chamada de API REST.

Método HTTP	Caminho
POST	/Conta//k8s/v1/managedApps

Parâmetros de entrada adicionais

Além dos parâmetros comuns com todas as chamadas de API REST, os seguintes parâmetros também são usados nos exemplos curl para esta etapa.

Parâmetro	Tipo	Obrigatório	Descrição
JSON	Corpo	Sim	Fornecer os parâmetros necessários para identificar o aplicativo a ser gerenciado. Veja o exemplo abaixo.

Exemplo de entrada JSON

```
{
  "type": "application/astra-managedApp",
  "version": "1.1",
  "id": "7da20fff-c69d-4270-bb0d-a4f91c5a1333"
}
```

Curl exemplo: Gerencie um aplicativo

```
curl --location -i --request POST
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/k8s/v1/managedApps'
--header 'Content-Type: application/astra-managedApp+json' --header
'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>' --d @JSONinput
```

Desgerenciar um aplicativo

Você pode remover um aplicativo gerenciado quando não for mais necessário. A

remoção de um aplicativo gerenciado também exclui as programações associadas.

Antes de começar

Você deve ter o ID do aplicativo gerenciado que deseja desgerenciar. Se necessário, você pode usar o fluxo de trabalho "[Liste os aplicativos gerenciados](#)" para localizar o aplicativo.

Os backups e snapshots do aplicativo não são removidos automaticamente quando são excluídos. Se você não precisar mais dos backups e snapshots, exclua-os antes de remover o aplicativo.

1. Não gerido a aplicação

Execute a seguinte chamada de API REST.

Método HTTP	Caminho
ELIMINAR	/Accounts/_id/k8s/v1/managedApps/_id

Parâmetros de entrada adicionais

Além dos parâmetros comuns com todas as chamadas de API REST, os seguintes parâmetros também são usados nos exemplos curl para esta etapa.

Parâmetro	Tipo	Obrigatório	Descrição
id da aplicação gerida	Caminho	Sim	Identifica o aplicativo gerenciado a ser removido.

Curl exemplo: Remover um aplicativo gerenciado

```
curl --location -i --request DELETE
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/k8s/v1/managedApps/<MANAGED_APP_ID>' --header 'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

Proteção da aplicação

Liste os instantâneos

Você pode listar os snapshots que foram obtidos para um aplicativo gerenciado específico.

Antes de começar

Você deve ter o ID do aplicativo gerenciado para o qual deseja listar os snapshots. Se necessário, você pode usar o fluxo de trabalho "[Liste os aplicativos gerenciados](#)" para localizar o aplicativo.

1. Liste os instantâneos

Execute a seguinte chamada de API REST.

Método HTTP	Caminho
OBTER	/Accounts/_id/k8s/v1/managedApps//appSnaps

Parâmetros de entrada adicionais

Além dos parâmetros comuns com todas as chamadas de API REST, os seguintes parâmetros também são usados nos exemplos curl para esta etapa.

Parâmetro	Tipo	Obrigatório	Descrição
id da aplicação gerida	Caminho	Sim	Identifica o aplicativo gerenciado que possui os snapshots listados.
contar	Consulta	Não	Se <code>count=true</code> o número de instantâneos estiver incluído na seção metadados da resposta.

Curl exemplo: Retornar todos os snapshots para o aplicativo

```
curl --location -i --request GET
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/k8s/v1/managedApps/<MANAGED_APP_ID>/appSnaps' --header 'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

Curl exemplo: Retorna todos os instantâneos para o aplicativo e a contagem

```
curl --location -i --request GET
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/k8s/v1/managedApps/<MANAGED_APP_ID>/appSnaps?count=true' --header 'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

Exemplo de saída JSON

```

{
  "items": [
    {
      "id": "dc2974ae-f71d-4c81-91b5-f96cf72dc3ba",
      "metadata": {
        "createdBy": "fb093413-b6fc-4a64-a48a-afc32ada8537",
        "creationTimestamp": "2021-06-04T21:23:14Z",
        "modificationTimestamp": "2021-06-04T21:23:14Z",
        "labels": []
      },
      "snapshotAppAsset": "4547658d-cc06-4c1d-ad8a-4a05274d0db0",
      "snapshotCreationTimestamp": "2021-06-04T21:23:47Z",
      "name": "test-postgres-app-snapshot-20210604212213",
      "state": "completed",
      "stateUnready": [],
      "type": "application/astra-appSnap",
      "version": "1.0"
    }
  ],
  "metadata": {
    "count": 1
  }
}

```

Liste os backups

Você pode listar os backups que foram criados para um aplicativo gerenciado específico.

Antes de começar

Você deve ter o ID do aplicativo gerenciado para o qual deseja listar os backups. Se necessário, você pode usar o fluxo de trabalho ["Liste os aplicativos gerenciados"](#) para localizar o aplicativo.

1. Liste os backups

Execute a seguinte chamada de API REST.

Método HTTP	Caminho
OBTER	/Accounts/_id/k8s/v1/managedApps/_id/appBackups

Parâmetros de entrada adicionais

Além dos parâmetros comuns com todas as chamadas de API REST, os seguintes parâmetros também são usados nos exemplos curl para esta etapa.

Parâmetro	Tipo	Obrigatório	Descrição
id da aplicação gerida	Caminho	Sim	Identifica o aplicativo gerenciado que possui os backups listados.

Curl exemplo: Retornar todos os backups para o aplicativo

```
curl --location -i --request GET
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/k8s/v1/managedApps/<MANAGED_APP_ID>/appBackups' --header 'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

Exemplo de saída JSON

```
{
  "items": [
    {
      "type": "application/astra-appBackup",
      "version": "1.0",
      "id": "ed39fdb0-12db-497b-9e46-20036c1fb0d2",
      "name": "mariadb-mariadb-backup-20210617175900",
      "state": "completed",
      "stateUnready": [],
      "bytesDone": 0,
      "percentDone": 100,
      "metadata": {
        "labels": [],
        "creationTimestamp": "2021-06-17T17:59:09Z",
        "modificationTimestamp": "2021-06-17T17:59:09Z",
        "createdBy": "fb093413-b6fc-4a64-a48a-afc32ada8537"
      }
    }
  ],
  "metadata": {}
}
```

Crie um instantâneo para um aplicativo gerenciado

Você pode criar um snapshot para um aplicativo gerenciado específico.

Antes de começar

Você deve ter o ID do aplicativo gerenciado para o qual deseja criar um snapshot. Se necessário, você pode usar o fluxo de trabalho ["Liste os aplicativos gerenciados"](#) para localizar o aplicativo.

1. Criar um instantâneo

Execute a seguinte chamada de API REST.

Método HTTP	Caminho
POST	/Accounts/_id/k8s/v1/managedApps//appSnaps

Parâmetros de entrada adicionais

Além dos parâmetros comuns com todas as chamadas de API REST, os seguintes parâmetros também são usados nos exemplos curl para esta etapa.

Parâmetro	Tipo	Obrigatório	Descrição
id da aplicação gerida	Caminho	Sim	Identifica o aplicativo gerenciado onde o snapshot será criado.
JSON	Corpo	Sim	Fornecer os parâmetros para o instantâneo. Veja o exemplo abaixo.

Exemplo de entrada JSON

```
{
  "type": "application/astra-appSnap",
  "version": "1.0",
  "name": "snapshot-david-1"
}
```

Curl exemplo: Crie um instantâneo para o aplicativo

```
curl --location -i --request POST
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/k8s/v1/managedApps/<MANAGED_APP_ID>/appSnaps' --header 'Content-Type: application/astra-appSnap+json'
--header 'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>' --d
@JSONinput
```

Crie um backup para um aplicativo gerenciado

Você pode criar um backup para um aplicativo gerenciado específico. Você pode usar o backup para restaurar ou clonar o aplicativo.

Antes de começar

Você deve ter o ID do aplicativo gerenciado para o qual deseja criar um backup. Se necessário, você pode usar o fluxo de trabalho "[Liste os aplicativos gerenciados](#)" para localizar o aplicativo.

1. Crie uma cópia de segurança

Execute a seguinte chamada de API REST.

Método HTTP	Caminho
POST	/Accounts/_id/k8s/v1/managedApps/_id/appBackups

Parâmetros de entrada adicionais

Além dos parâmetros comuns com todas as chamadas de API REST, os seguintes parâmetros também são usados nos exemplos curl para esta etapa.

Parâmetro	Tipo	Obrigatório	Descrição
id da aplicação gerida	Caminho	Sim	Identifica o aplicativo gerenciado onde o backup será criado.
JSON	Corpo	Sim	Fornecer os parâmetros para o backup. Veja o exemplo abaixo.

Exemplo de entrada JSON

```
{
  "type": "application/astra-appBackup",
  "version": "1.0",
  "name": "backup-david-1"
}
```

Curl exemplo: Crie um backup para o aplicativo

```
curl --location -i --request POST
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/k8s/v1/managedApps/<MANAGED_APP_ID>/appBackups' --header 'Content-Type: application/astra-appBackup+json' --header 'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>' --d @JSONinput
```

Eliminar um instantâneo

Você pode excluir um snapshot associado a um aplicativo gerenciado.

Antes de começar

Você deve ter o seguinte:

- ID do aplicativo gerenciado que possui o snapshot. Se necessário, você pode usar o fluxo de trabalho ["Liste os aplicativos gerenciados"](#) para localizar o aplicativo.
- ID do instantâneo que pretende eliminar. Se necessário, você pode usar o fluxo de trabalho ["Liste os](#)

[instantâneos](#)" para localizar o instantâneo.

1. Eliminar o instantâneo

Execute a seguinte chamada de API REST.

Método HTTP	Caminho
ELIMINAR	/Accounts/_id/k8s/v1/managedApps/_id/appSnaps/.appSnap_id

Parâmetros de entrada adicionais

Além dos parâmetros comuns com todas as chamadas de API REST, os seguintes parâmetros também são usados nos exemplos curl para esta etapa.

Parâmetro	Tipo	Obrigatório	Descrição
id da aplicação gerida	Caminho	Sim	Identifica o aplicativo gerenciado que possui o snapshot.
id do instantâneo	Caminho	Sim	Identifica o instantâneo a ser eliminado.

Curl exemplo: Exclua um único snapshot para o aplicativo

```
curl --location -i --request DELETE
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/k8s/v1/managedApps/<MANAGED_APP_ID>/appSnaps/<SNAPSHOT_ID>' --header 'Accept: */*' --header
'Authorization: Bearer <API_TOKEN>'
```

Eliminar uma cópia de segurança

Você pode excluir um backup associado a um aplicativo gerenciado.

Antes de começar

Você deve ter o seguinte:

- ID do aplicativo gerenciado que possui o backup. Se necessário, você pode usar o fluxo de trabalho ["Liste os aplicativos gerenciados"](#) para localizar o aplicativo.
- ID da cópia de segurança que pretende eliminar. Se necessário, você pode usar o fluxo de trabalho ["Liste os backups"](#) para localizar o instantâneo.

1. Eliminar a cópia de segurança

Execute a seguinte chamada de API REST.



Você pode forçar a exclusão de um backup com falha usando o cabeçalho de solicitação opcional, conforme descrito abaixo.

Método HTTP	Caminho
ELIMINAR	/Accounts/_id/k8s/v1/managedApps/_id/appBackups/_id

Parâmetros de entrada adicionais

Além dos parâmetros comuns com todas as chamadas de API REST, os seguintes parâmetros também são usados nos exemplos curl para esta etapa.

Parâmetro	Tipo	Obrigatório	Descrição
id da aplicação gerida	Caminho	Sim	Identifica o aplicativo gerenciado que possui o backup.
id de cópia de segurança	Caminho	Sim	Identifica o backup a ser excluído.
forçar a eliminação	Colhedor	Não	Usado para forçar a exclusão de um backup com falha.

Curl exemplo: Exclua um único backup para o aplicativo

```
curl --location -i --request DELETE
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/k8s/v1/managedApps/<MANAGED_APP_ID>/appBackups/<BACKUP_ID>' --header 'Accept: */*' --header
'Authorization: Bearer <API_TOKEN>'
```

Curl exemplo: Exclua um único backup para o aplicativo com a opção forçar

```
curl --location -i --request DELETE
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/k8s/v1/managedApps/<MANAGED_APP_ID>/appBackups/<BACKUP_ID>' --header 'Accept: */*' --header
'Authorization: Bearer <API_TOKEN>' --header 'Force-Delete: true'
```

Clonar e restaurar um aplicativo

Clonar um aplicativo gerenciado

É possível criar uma nova aplicação clonando uma aplicação gerenciada existente.

Antes de começar

Observe o seguinte sobre este fluxo de trabalho:

- Não é utilizado um backup ou instantâneo da aplicação
- A operação de clone é executada no mesmo cluster



Para clonar um aplicativo para um cluster diferente, você precisa atualizar o `clusterId` parâmetro na entrada JSON conforme apropriado para o seu ambiente.

1. Selecione o aplicativo gerenciado para clonar

Execute o fluxo de trabalho "[Liste os aplicativos gerenciados](#)" e selecione a aplicação que deseja clonar. Vários dos valores de recursos são necessários para a chamada REST usada para clonar o aplicativo.

2. Clonar a aplicação

Execute a seguinte chamada de API REST.

Método HTTP	Caminho
POST	/Conta//k8s/v1/managedApps

Parâmetros de entrada adicionais

Além dos parâmetros comuns com todas as chamadas de API REST, os seguintes parâmetros também são usados nos exemplos curl para esta etapa.

Parâmetro	Tipo	Obrigatório	Descrição
JSON	Corpo	Sim	Fornecer os parâmetros para o aplicativo clonado. Veja o exemplo abaixo.

Exemplo de entrada JSON

```
{
  "type": "application/astra-managedApp",
  "version": "1.0",
  "name": "postgres1-postgresql-clone",
  "clusterID": "30880586-d579-4d27-930f-a9633e59173b",
  "sourceClusterID": "30880586-d579-4d27-930f-a9633e59173b",
  "namespace": "davidns-postgres-app",
  "sourceAppID": "e591ee59-ea90-4a9f-8e6c-d2b6e8647096"
}
```

Curl exemplo: Clonar um aplicativo

```
curl --location -i --request POST
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/k8s/v1/managedApps'
--header 'Content-Type: application/astra-managedApp+json' --header '*/*'
--header 'Authorization: Bearer <API_TOKEN>' --d @JSONinput
```

Clonar um aplicativo gerenciado a partir de um snapshot

Você pode criar uma nova aplicação clonando-a a partir de um snapshot do aplicativo.

Antes de começar

Observe o seguinte sobre este fluxo de trabalho:

- É utilizado um instantâneo da aplicação
- A operação de clone é executada no mesmo cluster



Para clonar um aplicativo para um cluster diferente, você precisa atualizar o `clusterId` parâmetro na entrada JSON conforme apropriado para o seu ambiente.

1. Selecione o aplicativo gerenciado para clonar

Execute o fluxo de trabalho "[Liste os aplicativos gerenciados](#)" e selecione a aplicação que deseja clonar. Vários dos valores de recursos são necessários para a chamada REST usada para clonar o aplicativo.

2. Selecione o instantâneo a utilizar

Execute o fluxo de trabalho "[Liste os instantâneos](#)" e selecione instantâneo que deseja usar.

3. Clonar a aplicação

Execute a seguinte chamada de API REST.

Método HTTP	Caminho
POST	/Conta//k8s/v1/managedApps

Parâmetros de entrada adicionais

Além dos parâmetros comuns com todas as chamadas de API REST, os seguintes parâmetros também são usados nos exemplos curl para esta etapa.

Parâmetro	Tipo	Obrigatório	Descrição
JSON	Corpo	Sim	Fornecer os parâmetros para o aplicativo clonado. Veja o exemplo abaixo.

Exemplo de entrada JSON

```
{
  "type": "application/astra-managedApp",
  "version": "1.0",
  "name": "postgres1-postgresql-clone",
  "clusterID": "30880586-d579-4d27-930f-a9633e59173b",
  "sourceClusterID": "30880586-d579-4d27-930f-a9633e59173b",
  "namespace": "davidns-postgres-app",
  "snapshotID": "e24515bd-a28e-4b28-b832-f3c74dbf32fb",
  "sourceAppID": "e591ee59-ea90-4a9f-8e6c-d2b6e8647096"
}
```

Curl exemplo: Clonar um aplicativo a partir de um snapshot

```
curl --location -i --request POST
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/k8s/v1/managedApps'
--header 'Content-Type: application/astra-managedApp+json' --header '*/*'
--header 'Authorization: Bearer <API_TOKEN>' --d @JSONinput
```

Clonar um aplicativo gerenciado a partir de um backup

É possível criar uma nova aplicação gerenciada clonando-a a partir de um backup de aplicativo.

Antes de começar

Observe o seguinte sobre este fluxo de trabalho:

- Um backup de aplicativo é usado
- A operação de clone é executada no mesmo cluster



Para clonar um aplicativo para um cluster diferente, você precisa atualizar o `clusterId` parâmetro na entrada JSON conforme apropriado para o seu ambiente.

1. Selecione o aplicativo gerenciado para clonar

Execute o fluxo de trabalho "[Liste os aplicativos gerenciados](#)" e selecione a aplicação que deseja clonar. Vários dos valores de recursos são necessários para a chamada REST usada para clonar o aplicativo.

2. Selecione a cópia de segurança a utilizar

Execute o fluxo de trabalho "[Liste os backups](#)" e selecione cópia de segurança que pretende utilizar.

3. Clonar a aplicação

Execute a seguinte chamada de API REST.

Método HTTP	Caminho
POST	/Conta//k8s/v1/managedApps

Parâmetros de entrada adicionais

Além dos parâmetros comuns com todas as chamadas de API REST, os seguintes parâmetros também são usados nos exemplos curl para esta etapa.

Parâmetro	Tipo	Obrigatório	Descrição
JSON	Corpo	Sim	Fornecer os parâmetros para o aplicativo clonado. Veja o exemplo abaixo.

Exemplo de entrada JSON

```
{
  "type": "application/astra-managedApp",
  "version": "1.0",
  "name": "postgres1-postgresql-clone",
  "clusterID": "30880586-d579-4d27-930f-a9633e59173b",
  "sourceClusterID": "30880586-d579-4d27-930f-a9633e59173b",
  "namespace": "davidns-postgres-app",
  "backupID": "e24515bd-a28e-4b28-b832-f3c74dbf32fb",
  "sourceAppID": "e591ee59-ea90-4a9f-8e6c-d2b6e8647096"
}
```

Curl exemplo: Clonar um aplicativo a partir de um backup

```
curl --location -i --request POST
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/k8s/v1/managedApps'
--header 'Content-Type: application/astra-managedApp+json' --header '*/*'
--header 'Authorization: Bearer <API_TOKEN>' --d @JSONinput
```

Restaurar um aplicativo gerenciado a partir de um backup

Você pode restaurar um aplicativo gerenciado criando um novo aplicativo a partir de um backup.

1. Selecione a aplicação gerida para restaurar

Execute o fluxo de trabalho "[Liste os aplicativos gerenciados](#)" e selecione a aplicação que deseja clonar. Vários dos valores de recursos são necessários para a chamada REST usada para clonar o aplicativo.

2. Selecione a cópia de segurança a utilizar

Execute o fluxo de trabalho "[Liste os backups](#)" e selecione cópia de segurança que pretende utilizar.

3. Restaure a aplicação

Execute a seguinte chamada de API REST.

Método HTTP	Caminho
POST	/Conta//k8s/v1/managedApps

Parâmetros de entrada adicionais

Além dos parâmetros comuns com todas as chamadas de API REST, os seguintes parâmetros também são usados nos exemplos curl para esta etapa.

Parâmetro	Tipo	Obrigatório	Descrição
JSON	Corpo	Sim	Fornecer os parâmetros para o aplicativo clonado. Veja o exemplo abaixo.

Exemplo de entrada JSON

```
{
  "type": "application/astra-managedApp",
  "version": "1.0",
  "name": "postgres1-postgresql-clone",
  "clusterID": "30880586-d579-4d27-930f-a9633e59173b",
  "sourceClusterID": "30880586-d579-4d27-930f-a9633e59173b",
  "namespace": "davidns-postgres-app",
  "backupID": "e24515bd-a28e-4b28-b832-f3c74dbf32fb",
  "sourceAppID": "e591ee59-ea90-4a9f-8e6c-d2b6e8647096"
}
```

Curl exemplo: Clonar um aplicativo a partir de um backup

```
curl --location -i --request POST
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/k8s/v1/managedApps'
--header 'Content-Type: application/astra-managedApp+json' --header '*/*'
--header 'Authorization: Bearer <API_TOKEN>' --d @JSONinput
```

Suporte

Liste as notificações

Você pode listar as notificações de uma conta Astra específica. Você pode fazer isso como parte do monitoramento da atividade do sistema ou depuração de um problema.

1. Liste as notificações

Execute a seguinte chamada de API REST.

Método HTTP	Caminho
OBTER	/Conta//core/v1/notificações

Parâmetros de entrada adicionais

Além dos parâmetros comuns com todas as chamadas de API REST, os seguintes parâmetros também são usados nos exemplos curl para esta etapa.

Parâmetro	Tipo	Obrigatório	Descrição
filtro	Consulta	Não	Opcionalmente, filtre as notificações que você deseja retornar na resposta.
incluir	Consulta	Não	Opcionalmente, selecione os valores que você deseja retornar na resposta.

Curl exemplo: Retornar todas as notificações

```
curl --location -i --request GET
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/core/v1/notifications'
--header 'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

Curl exemplo: Retorne a descrição para notificações com gravidade de aviso

```
curl --location -i --request GET
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/core/v1/notifications?filter=severity%20eq%20'warning'&include=description' --header 'Accept: */*'
--header 'Authorization: Bearer <API_TOKEN>'
```

Exemplo de saída JSON

```
{
  "items": [
    [
      "Trident on cluster david-ie-00 has failed or timed out;
installation of the Trident operator failed or is not yet complete;
operator failed to reach an installed state within 300.00 seconds;
container trident-operator not found in operator deployment"
    ],
    [
      "Trident on cluster david-ie-00 has failed or timed out;
installation of the Trident operator failed or is not yet complete;
operator failed to reach an installed state within 300.00 seconds;
container trident-operator not found in operator deployment"
    ]
  ],
  "metadata": {}
}
```

Eliminar uma aplicação com falha

Talvez você não consiga remover um aplicativo gerenciado se ele tiver um backup ou snapshot em um estado com falha. Neste caso, você pode remover manualmente o aplicativo usando o fluxo de trabalho descrito abaixo.

1. Selecione a aplicação gerida a eliminar

Execute o fluxo de trabalho "[Liste os aplicativos gerenciados](#)" e selecione a aplicação que pretende remover.

2. Liste os backups existentes para o aplicativo

Execute o fluxo de "[Liste os backups](#)"trabalho .

3. Exclua todos os backups

Exclua todos os backups de aplicativos executando o fluxo de trabalho "[Eliminar uma cópia de segurança](#)" para cada backup na lista.

4. Liste os instantâneos existentes para o aplicativo

Execute o fluxo de "[Liste os instantâneos](#)"trabalho .

5. Eliminar todos os instantâneos

Execute o fluxo de trabalho "[Eliminar um instantâneo](#)"de cada instantâneo na lista.

6. Remova a aplicação

Execute o fluxo de trabalho "[Desgerenciar um aplicativo](#)" para remover a aplicação.

Usando Python

Antes de começar

Python é uma linguagem de desenvolvimento popular, especialmente para automação de data center. Antes de usar os recursos nativos do Python juntamente com vários pacotes comuns, você precisa preparar o ambiente e os arquivos de entrada necessários.

Prepare o ambiente

Os requisitos básicos de configuração para executar os scripts Python são descritos abaixo.

Python 3

Você precisa ter a versão mais recente do Python 3 instalada.

Bibliotecas adicionais

As bibliotecas **requests** e **urllib3** devem ser instaladas. Você pode usar o pip ou outra ferramenta de gerenciamento Python conforme apropriado para o seu ambiente.

Acesso à rede

A estação de trabalho onde os scripts são executados deve ter acesso à rede e ser capaz de alcançar o Astra Control. Ao usar o Astra Control Service, você deve estar conectado à Internet e ser capaz de se conectar ao serviço em <https://astra.netapp.io>.

Informações de identidade

Você precisa de uma conta Astra válida com o identificador de conta e token de API. Consulte "[Obtenha um token de API](#)" para obter mais informações.

Crie os arquivos de entrada JSON

Os scripts Python dependem de informações de configuração contidas em arquivos de entrada JSON. Os arquivos de amostra são fornecidos abaixo.



Você precisa atualizar as amostras conforme apropriado para o seu ambiente.

Informações de identidade

O arquivo a seguir contém o token de API e a conta Astra. Você precisa passar esse arquivo para scripts Python usando o `-i` parâmetro CLI (ou `--identity`).

```
{
  "api_token": "kH4CA_uVIa8q9UuPzhJaAHaGlaR7-no901DkkrVjIXk=",
  "account_id": "5131dfdf-03a4-5218-ad4b-fe84442b9786"
}
```

Liste os aplicativos gerenciados

Você pode usar o script a seguir para listar os aplicativos gerenciados da sua conta Astra.

```
#!/usr/bin/env python3
##-----
-----
#
# Usage: python3 list_man_apps.py -i identity_file.json
#
# (C) Copyright 2021 NetApp, Inc.
#
# This sample code is provided AS IS, with no support or warranties of
# any kind, including but not limited for warranties of merchantability
# or fitness of any kind, expressed or implied. Permission to use,
# reproduce, modify and create derivatives of the sample code is granted
# solely for the purpose of researching, designing, developing and
# testing a software application product for use with NetApp products,
# provided that the above copyright notice appears in all copies and
# that the software application product is distributed pursuant to terms
# no less restrictive than those set forth herein.
#
##-----
-----

import argparse
import json
import requests
import urllib3
import sys

# Global variables
api_token = ""
account_id = ""

def get_managed_apps():
    ''' Get and print the list of managed apps '''

    # Global variables
    global api_token
    global account_id

    # Create an HTTP session
    sess1 = requests.Session()
```

```

# Suppress SSL unsigned certificate warning
urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)

# Create URL
url1 = "https://astra.netapp.io/accounts/" + account_id +
"/k8s/v1/managedApps"

# Headers and response output
req_headers = {}
resp_headers = {}
resp_data = {}

# Prepare the request headers
req_headers.clear
req_headers['Authorization'] = "Bearer " + api_token
req_headers['Content-Type'] = "application/astra-managedApp+json"
req_headers['Accept'] = "application/astra-managedApp+json"

# Make the REST call
try:
    resp1 = sess1.request('get', url1, headers=req_headers,
allow_redirects=True, verify=False)

except requests.exceptions.ConnectionError:
    print("Connection failed")
    sys.exit(1)

# Retrieve the output
http_code = resp1.status_code
resp_headers = resp1.headers

# Print the list of managed apps
if http_code == 200:
    resp_data = json.loads(resp1.text)
    items = resp_data['items']
    for i in items:
        print(" ")
        print("Name: " + i['name'])
        print("ID: " + i['id'])
        print("State: " + i['state'])
    else:
        print("Failed with HTTP status code: " + str(http_code))

print(" ")

# Close the session

```

```

sess1.close()

return

def read_id_file(idf):
    ''' Read the identity file and save values '''

    # Global variables
    global api_token
    global account_id

    with open(idf) as f:
        data = json.load(f)

    api_token = data['api_token']
    account_id = data['account_id']

    return

def main(args):
    ''' Main top level function '''

    # Global variables
    global api_token
    global account_id

    # Retrieve name of JSON input file
    identity_file = args.id_file

    # Get token and account
    read_id_file(identity_file)

    # Issue REST call
    get_managed_apps()

    return

def parseArgs():
    ''' Parse the CLI input parameters '''

    parser = argparse.ArgumentParser(description='Astra REST API -
List the managed apps',
                                   add_help = True)
    parser.add_argument("-i", "--identity", action="store", dest
="id_file", default=None,
                        help='(Req) Name of the identity input file',
                        required=True)

```

```
        return parser.parse_args()

if __name__ == '__main__':
    ''' Begin here '''

    # Parse input parameters
    args = parseArgs()

    # Call main function
    main(args)
```

Referência da API

Você pode acessar os detalhes de todas as chamadas da API REST do Astra Control, incluindo os métodos HTTP, parâmetros de entrada e respostas. Essa referência completa é útil ao desenvolver aplicativos de automação usando a API REST.



A documentação de referência da API REST é fornecida atualmente com o Astra Control e está disponível on-line.

Antes de começar

Você precisa de uma conta para Astra Control Center ou Astra Control Service.

Passos

1. Faça login no Astra usando suas credenciais de conta.

Acesse o seguinte site do Astra Control Service: "<https://astra.netapp.io>"

2. Clique no ícone de figura no canto superior direito da página e selecione **Acesso à API**.
3. Na parte superior da página, clique no URL exibido em **Documentação da API**.
4. Forneça as credenciais da sua conta novamente, se solicitado.

Recursos adicionais

Há recursos adicionais que você pode acessar para obter ajuda e encontrar mais informações sobre os serviços e suporte em nuvem da NetApp, bem como conceitos GERAIS DE REST e nuvem.

Astra

- ["Documentação do Astra Control Center 2108"](#)

Documentação do software Astra Control Center implantado nas instalações do cliente.

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

Documentação do software Astra Control Service disponível na nuvem pública.

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

Documentação do orquestrador de storage de código aberto Astra Trident mantida pelo NetApp.

Recursos de nuvem da NetApp

- ["Soluções de nuvem da NetApp"](#)

Local central para as soluções de nuvem da NetApp.

- ["Console central da nuvem NetApp"](#)

Console de serviço NetApp Cloud Central com login.

- ["Suporte à NetApp"](#)

Acesse ferramentas de solução de problemas, documentação e assistência técnica.

Conceitos REST e tecnologia de nuvem

- PhD ["dissertação"](#) por Roy Fielding

Esta publicação introduziu e estabeleceu o modelo de desenvolvimento de aplicações REST.

- ["Auth0"](#)

Este é o serviço de plataforma de autenticação e autorização usado pelo serviço Astra para acesso à Web.

- ["Editor RFC"](#)

Fonte autorizada para padrões da Web e da Internet mantida como uma coleção de documentos RFC numerados de forma única.

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/)

Licença de API Astra Control

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

Informações sobre direitos autorais

Copyright © 2024 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.