



Comece agora

Astra Automation

NetApp
January 31, 2025

Índice

Comece agora	1
Antes de começar	1
Obtenha um token de API	1
Sua primeira chamada de API	2
Conceitos básicos do Kubernetes	3
Prepare-se para usar os fluxos de trabalho	3
Referência de API online	6

Comece agora

Antes de começar

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

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 acessadas pelo serviço **Auth0**.

Familiarize-se com os conceitos básicos do Kubernetes

Você deve estar familiarizado com vários conceitos básicos do Kubernetes. Consulte "[Conceitos básicos do Kubernetes](#)" para obter mais informações.

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.

Obtenha mais informações

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

Obtenha um token de API

Você precisa obter um token da API Astra para usar a API REST do Astra Control.

Visão geral

Um token de API identifica o chamador para o Astra e deve ser incluído em todas as chamadas da API REST.

- Você precisa gerar um token de API usando a interface de usuário da Web Astra.
- O procedimento para gerar um token é o mesmo para ambos os modelos de implantação do Astra. Somente o URL usado para acessar o Astra é diferente.
- A identidade do usuário carregada com o token e as permissões associadas são determinadas pelo usuário que criou o token.
- O token deve ser incluído no `Authorization` cabeçalho de solicitação HTTP.
- Um token nunca expira depois que ele é criado.
- Você pode revogar um token na interface de usuário da Web Astra.

Informações relacionadas

- "[Revogar um token de API](#)"

Crie um token da API Astra

As etapas a seguir descrevem como criar um token da API Astra.

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 ao fazer chamadas de API.

Passos

1. Faça login no Astra usando suas credenciais de conta da seguinte maneira:
 - Astra Control Service: "<https://astra.netapp.io>"
 - Astra Control Center: Use o URL do seu ambiente local, conforme estabelecido durante a instalação
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, em seguida, clique em **Generate API token** na janela pop-up.
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

Quando você acessa a API REST do Astra Control por meio de curl ou uma linguagem de programação, você deve incluir o token portador da API no cabeçalho da solicitação HTTP `Authorization`.

Sua primeira chamada de API

Você pode emitir um comando curl simples na CLI da estação de trabalho para começar a usar a API REST 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 a `CONTA_ID` apropriada e `API_TOKEN` conforme indicado.

```
curl --request GET \
--location "https://astra.netapp.io/accounts/$ACCOUNT_ID/core/v1/users" \
--include \
--header "Content-Type: application/json" \
--header "Accept: */*" \
--header "Authorization: Bearer $API_TOKEN"
```

Exemplo de saída JSON

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

Conceitos básicos do Kubernetes

Há vários conceitos do Kubernetes que são relevantes ao usar a API REST do Astra.

Objetos

Os objetos mantidos em um ambiente Kubernetes são entidades persistentes que representam a configuração do cluster. Esses objetos descrevem coletivamente o estado do sistema, incluindo a carga de trabalho do cluster.

Namespaces

Namespaces fornecem uma técnica para isolar recursos em um único cluster. Essa estrutura organizacional é útil ao dividir os tipos de trabalho, usuários e recursos. Objetos com um escopo *namespace* precisam ser exclusivos dentro do namespace, enquanto aqueles com um escopo *cluster* devem ser exclusivos em todo o cluster.

Etiquetas

Os rótulos podem ser associados aos objetos Kubernetes. Eles descrevem atributos usando pares de chave-valor e podem impor uma organização arbitrária no cluster que pode ser útil para uma organização, mas estão fora da operação principal do Kubernetes.

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.



Um fluxo de trabalho pode conter apenas uma etapa. Esses fluxos de trabalho de etapa única são formatados de forma ligeiramente diferente dos fluxos de trabalho que contêm várias etapas. Por exemplo, o nome explícito da etapa é removido. A ação ou operação deve ser clara com base no título do fluxo de trabalho.

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 para 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 configurar um cluster gerenciado. Os workflows de gerenciamento se concentram em operações de suporte e proteção de aplicativos, como backup, restauração e clonagem de um aplicativo.

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.

As variáveis são formatadas para uso em um ambiente de shell Bash. Cada variável começa com um sinal de dólar e é incluída em aspas duplas, conforme necessário. Isso os torna reconhecíveis ao Bash. Maiúsculas são usadas consistentemente para os nomes.

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

Palavra-chave	Tipo	Descrição
CONTA_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.
APP_ID	Caminho	O valor UUIDv4 identificando o aplicativo para a chamada API.

Usando os exemplos com Bash

Se você usar os exemplos de cURL de fluxo de trabalho diretamente, você deve atualizar as variáveis que eles contêm com os valores apropriados para o seu ambiente. Você pode editar manualmente os exemplos ou confiar no shell Bash para fazer a substituição por você, como descrito abaixo.



Uma vantagem de usar o Bash é que você pode definir os valores da variável uma vez em uma sessão de shell em vez de uma vez por comando curl.

Passos

1. Abra o shell Bash fornecido com Linux ou sistema operacional semelhante.
2. Defina os valores da variável incluídos no exemplo curl que você deseja executar. Por exemplo:

```
$API_TOKEN=SGgpXHeco6M8PLxzIlgbzA4k3_eX4UCa842hOXHBFA=
```

3. Copie o exemplo curl da página de fluxo de trabalho e cole-o no terminal shell.
4. Pressione **ENTER** para executar as seguintes tarefas:
 - a. Substitua os valores da variável que você definir.
 - b. Execute o comando curl.

Referência de API online

Acesse a documentação de referência da API Astra

Você pode acessar os detalhes das 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.

Antes de começar

Você precisa de credenciais para fazer login na interface de usuário da Web Astra para sua implantação. O procedimento para acessar a documentação de referência é o mesmo para o Astra Control Service e o Astra Control Center. Apenas o URL é diferente. Não é necessário um token de API para acessar e visualizar o documento de referência

Passos

1. Faça login no Astra usando suas credenciais de conta da seguinte maneira:
 - Astra Control Service: "<https://astra.netapp.io>"
 - Astra Control Center: Use o URL do seu ambiente local, conforme estabelecido durante a instalação
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**.

Resultado

A página Swagger é iniciada em uma nova janela ou guia. Aviso o URL inclui o ID da conta para a conta com a qual você entrou.

O que se segue?

Você pode opcionalmente executar uma chamada de API a partir da página Swagger. Consulte "[Emitir uma chamada de API REST do Astra](#)" para obter mais informações.

Emitir uma chamada de API REST do Astra

Você pode emitir uma chamada da API REST do Astra Control na página de documentação de referência da API.

Antes de começar

Você precisa fazer login no Astra e acessar a página de referência da API. Consulte "[Acesse a documentação de referência da API Astra](#)" para obter mais informações. Você também precisa de um token para usar a API REST. "[Obtenha um token de API](#)" Consulte para obter detalhes sobre como gerar um token de API.

Passos

1. Na parte superior da página de referência da API, clique em **autorizar**.
2. Copie e cole o valor do token da API no campo na janela pop-up e clique em **autorizar** e, em seguida, clique em **Fechar**.
3. Role a página para baixo e abra a chamada de API desejada.
4. Clique com o botão direito em **Experimente**.
5. Role para baixo dentro da mesma chamada de API. Forneça os valores de parâmetros necessários e clique em **execute** para emitir a chamada.

Resultado

A chamada API é executada e o código de status HTTP é exibido.

Informações sobre direitos autorais

Copyright © 2025 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.