Manos a la obra

Astra Automation

NetApp
April 02, 2025

This PDF was generated from https://docs.netapp.com/es-es/astra-automation-2307/get-started/before_get_started.html on April 02, 2025. Always check docs.netapp.com for the latest.

Tabla de contenidos

Manos a la obra . . . 1
- Antes de empezar . . . 1
- Obtenga un token de API . . . 1
  - Descripción general . . . 1
  - Cree un token de API Astra . . . 1
- Su primera llamada API . . . 2
- Conceptos básicos de Kubernetes . . . 3
  - Objetos . . . 3
  - Espacios de nombres . . . 3
  - Etiquetas . . . 3
- Prepárese para usar los flujos de trabajo . . . 3
  - Introducción . . . 4
  - Parámetros de entrada comunes . . . 4
  - Presentación de tokens e identificadores . . . 5
  - Categorías de flujo de trabajo . . . 5
- Referencia de API en línea . . . 5
  - Accede a la documentación de referencia de la API de Astra . . . 6
  - Emitir una llamada a la API de REST DE Astra . . . 6

Manos a la obra

Antes de empezar

Puede prepararse rápidamente para empezar con la API REST de Astra Control revisando los siguientes pasos.

Tener credenciales de cuenta de Astra

Necesitará credenciales de Astra para iniciar sesión en la interfaz de usuario web de Astra y generar un token de API. Con Astra Control Center, puede gestionar estas credenciales localmente. Con Astra Control Service, se accede a las credenciales de la cuenta a través del servicio **Auth0**.

Familiarícese con los conceptos básicos de Kubernetes

Debería estar familiarizado con varios conceptos básicos de Kubernetes. Consulte "Conceptos básicos de Kubernetes" si quiere más información.

Revisar los conceptos e implementación de REST

Asegúrese de revisarlo "Implementación básica de REST" Para obtener información sobre conceptos DE REST y detalles sobre cómo se diseña la API ASTRA Control REST.

Obtenga más información

Debe conocer los recursos de información adicionales que se sugieren en la "Recursos adicionales".

Obtenga un token de API

Necesita obtener un token de API Astra para utilizar la API REST de Astra Control.

Descripción general

Un identificador de API identifica a la persona que llama a Astra y debe incluirse con cada llamada de API DE REST.

- Debe generar un token de API mediante la interfaz de usuario web de Astra.
- El procedimiento para generar un token es el mismo para ambos modelos de puesta en marcha de Astra. Solo la URL que se utiliza para acceder a Astra es diferente.
- La identidad de usuario que lleva el token y los permisos asociados son determinados por el usuario que creó el token.
- El token debe incluirse en el `Authorization` Encabezado de solicitud HTTP.
- Un token nunca caduca después de que se crea.
- Puede revocar un token en la interfaz de usuario web de Astra.

Información relacionada

- "Revocar un token de API"

Cree un token de API Astra

En los siguientes pasos se describe cómo crear un token de API de Astra.

Antes de empezar

Necesita credenciales para una cuenta Astra.

Acerca de esta tarea

Esta tarea genera un token de API en la interfaz web de Astra. También debe recuperar el ID de cuenta que también se necesita al realizar llamadas API.

Pasos

1. Inicia sesión en Astra con las credenciales de tu cuenta de la siguiente manera:
   - Servicio Astra Control: "https://astra.netapp.io"
   - Astra Control Center: Utilice la URL de su entorno local tal y como se establece durante la instalación
2. Haga clic en el icono de figura situado en la parte superior derecha de la página y seleccione **acceso API**.
3. Haga clic en **Generar token de API** en la página y luego haga clic en **Generar token de API** en la ventana emergente.
4. Haga clic en el icono para copiar la cadena de token al portapapeles y guardarla en el editor.
5. Copie y guarde el ID de cuenta que está disponible en la misma página.

Después de terminar

Cuando accedes a la API de REST DE Astra Control mediante curl o un lenguaje de programación, debes incluir el token del portador de la API en HTTP `Authorization` solicite el encabezado.

Su primera llamada API

Puede emitir un sencillo comando curl en la interfaz de línea de comandos de su estación de trabajo para empezar a utilizar la API ASTRA Control REST y confirmar su disponibilidad.

Antes de empezar

La utilidad Curl debe estar disponible en la estación de trabajo local. También debe tener un token de API y el identificador de cuenta asociado. Consulte "Obtenga un token de API" si quiere más información.

Ejemplo de curl

El siguiente comando Curl recupera una lista de usuarios de Astra. Proporcione el <ACCOUNT_ID> y el <API_TOKEN> adecuados según se indica.

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

Ejemplo de resultado JSON

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

Conceptos básicos de Kubernetes

Hay varios conceptos de Kubernetes que son relevantes cuando se usa la API REST de Astra.

Objetos

Los objetos que se mantienen en un entorno de Kubernetes son entidades persistentes que representan la configuración del clúster. Estos objetos describen de manera colectiva el estado del sistema, incluida la carga de trabajo del clúster.

Espacios de nombres

Los espacios de nombres proporcionan una técnica para aislar recursos dentro de un único clúster. Esta estructura organizativa es útil cuando se dividen los tipos de trabajo, los usuarios y los recursos. Los objetos con un *Namespace Scope* deben ser únicos dentro del espacio de nombres, mientras que los que tienen un *cluster scope* deben ser únicos en todo el clúster.

Etiquetas

Las etiquetas pueden asociarse con los objetos de Kubernetes. Describen los atributos mediante pares de clave-valor y pueden aplicar una organización arbitraria en el clúster que puede ser útil para una organización pero que se encuentra fuera del funcionamiento de Kubernetes principal.

Prepárese para usar los flujos de trabajo

Debe estar familiarizado con la organización y el formato de los flujos de trabajo de Astra antes de utilizarlos con una implementación en directo.

Introducción

Un *Workflow* es una secuencia de uno o más pasos necesarios para llevar a cabo una tarea o un objetivo administrativos específicos. Cada paso de un flujo de trabajo de Astra Control es uno de los siguientes:

- Llamada a API REST (con detalles como ejemplos curl y JSON)
- Invocación de otro flujo de trabajo de Astra
- Tareas relacionadas varias (como tomar una decisión de diseño necesaria)

Los flujos de trabajo incluyen los pasos principales y los parámetros necesarios para realizar cada tarea. Proporcionan un punto de partida para personalizar el entorno de automatización.

Parámetros de entrada comunes

Los parámetros de entrada descritos a continuación son comunes a todas las muestras de curl utilizadas para ilustrar una llamada a la API DE REST.

> Debido a que estos parámetros de entrada son universalmente necesarios, no se describen más adelante en los flujos de trabajo individuales. Si se utilizan parámetros de entrada adicionales para un ejemplo de rizo específico, se describen en la sección **parámetros de entrada adicionales**.

Parámetros de ruta

La ruta de extremo utilizada con cada llamada de API DE REST incluye los siguientes parámetros. Consulte también "Formato de URL" si quiere más información.

ID de cuenta

Este es el valor UUIDv4 que identifica la cuenta Astra en la que se ejecuta la operación API. Consulte "Obtenga un token de API" Para obtener más información acerca de cómo localizar su ID de cuenta.

Solicitar encabezados

Existen varios encabezados de solicitud que puede necesitar incluir en función de la llamada a la API DE REST.

Autorización

Todas las llamadas API de los flujos de trabajo necesitan un token de API para identificar al usuario. Debe incluir el token en el `Authorization` solicite el encabezado. Consulte "Obtenga un token de API" Para obtener más información acerca de la generación de un token de API.

Tipo de contenido

Con LA POST HTTP y LAS peticiones DE PONER donde JSON está incluido en el cuerpo de la solicitud, debe declarar el tipo de medio basado en el recurso Astra. Por ejemplo, puede incluir el encabezado `Content-Type: application/astra-appSnap+json` al crear una instantánea para una aplicación administrada.

Acepte

Puede declarar el tipo de medio específico del contenido que espera en la respuesta en función del recurso Astra. Por ejemplo, puede incluir el encabezado `Accept: application/astra-appBackup+json` al enumerar los backups de una aplicación gestionada. Sin embargo, para mayor simplicidad, las muestras curl de los flujos de trabajo aceptan todos los tipos de medios.

Presentación de tokens e identificadores

El token de la API y otros valores de ID utilizados con los ejemplos curl son opacos sin significado discernible. Para mejorar la legibilidad de las muestras, no se utilizan los valores de identificador y token reales. Más bien, se utilizan palabras clave reservadas más pequeñas que tiene varias ventajas:

- Las muestras curl y JSON son más claras y fáciles de entender.
- Puesto que todas las palabras clave utilizan el mismo formato con corchetes y letras mayúsculas, puede identificar rápidamente la ubicación y el contenido que se debe insertar o extraer.
- No se pierde ningún valor porque los parámetros originales no se pueden copiar y utilizar con una implementación real.

Aquí están algunas de las palabras clave reservadas comunes usadas en los ejemplos curl. Esta lista no es exhaustiva y se utilizan palabras clave adicionales según sea necesario. Su significado debe ser obvio basado en el contexto.

Palabra clave	Tipo	Descripción
<ACCOUNT_ID>	Ruta	El valor UUIDv4 que identifica la cuenta en la que se ejecuta la operación API.
<API_TOKEN>	Encabezado	El token del portador identifica y autoriza al llamante.
<APP_ID>	Ruta	El valor UUIDv4 que identifica la aplicación para la llamada API.

Categorías de flujo de trabajo

Existen dos amplias categorías de flujos de trabajo de Astra disponibles en función de su modelo de puesta en marcha. Si utiliza Astra Control Center, debería empezar con los flujos de trabajo de la infraestructura y, a continuación, proceder a los flujos de trabajo de gestión. Cuando utilice Astra Control Service, normalmente puede dirigirse directamente a los flujos de trabajo de gestión.

Los ejemplos de curl de los flujos de trabajo utilizan la dirección URL del servicio de control Astra. Debe cambiar la dirección URL cuando utilice el Centro de control Astra de las instalaciones según sea necesario para su entorno.

Flujos de trabajo de infraestructura

Estos flujos de trabajo hacen frente a la infraestructura Astra, que incluye credenciales, bloques y back-ends. Se necesitan con Astra Control Center, pero en la mayoría de los casos también se pueden utilizar con Astra Control Service. Los flujos de trabajo se centran en las tareas necesarias para establecer y mantener un clúster gestionado por Astra.

Flujos de trabajo de gestión

Puede utilizar estos flujos de trabajo después de tener un clúster gestionado. Los flujos de trabajo centran su atención en la protección de las aplicaciones y en operaciones de soporte como backup, restauración y clonado de una aplicación.

Referencia de API en línea

Accede a la documentación de referencia de la API de Astra

Puede acceder a los detalles de las llamadas API REST de Astra Control, incluidos los métodos HTTP, los parámetros de entrada y las respuestas. Esta referencia completa es útil cuando se desarrollan aplicaciones de automatización mediante la API DE REST.

Antes de empezar

Necesitará credenciales para iniciar sesión en la interfaz de usuario web de Astra para su puesta en marcha. El procedimiento para acceder a la documentación de referencia es el mismo para Astra Control Service y Astra Control Center. Solo la URL es diferente. No se necesita un token de API para acceder al documento de referencia y verlo

Pasos

1. Inicia sesión en Astra con las credenciales de tu cuenta de la siguiente manera:
   - Servicio Astra Control: "https://astra.netapp.io"
   - Astra Control Center: Utilice la URL de su entorno local tal y como se establece durante la instalación
2. Haga clic en el icono de figura situado en la parte superior derecha de la página y seleccione **acceso API**.
3. En la parte superior de la página, haga clic en la dirección URL que aparece en **Documentación de API**.

Resultado

La página de Swagger se inicia en una nueva ventana o pestaña. Observe que la URL incluye el ID de cuenta de la cuenta con la que inició sesión.

El futuro

Opcionalmente, puede ejecutar una llamada API desde la página de Swagger. Consulte "Emitir una llamada a la API de REST DE Astra" si quiere más información.

Emitir una llamada a la API de REST DE Astra

Puedes emitir una llamada a la API de REST DE Astra Control desde la página de documentación de referencia de la API.

Antes de empezar

Debes iniciar sesión en Astra y acceder a la página de referencia de la API. Consulte "Accede a la documentación de referencia de la API de Astra" si quiere más información. También se necesita un token para usar la API de REST. Consulte "Obtenga un token de API" Para obtener detalles sobre la generación de un token de API.

Pasos

1. En la parte superior de la página de referencia de la API, haga clic en **Autorizar**.
2. Copia y pega el valor de tu token API en el campo de la ventana emergente y haz clic en **Autorizar** y luego en **Cerrar**.
3. Desplácese hacia abajo por la página y abra la llamada API deseada.
4. En el clic derecho **Pruébalo**.
5. Desplácese hacia abajo dentro de la misma llamada API. Proporcione los valores de parámetros requeridos y haga clic en **Ejecutar** para emitir la llamada.

Resultado

Se ejecuta la llamada API y se muestra el código de estado HTTP.

Información de copyright

Copyright © 2025 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en http://www.netapp.com/TM son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.