# Los geht's

## Astra Automation

NetApp
January 31, 2025

This PDF was generated from https://docs.netapp.com/de-de/astra-automation-2307/get-started/before_get_started.html on January 31, 2025. Always check docs.netapp.com for the latest.

# Inhalt

Los geht’s . . . . . 1
Bevor Sie beginnen . . . . . 1
Holen Sie sich ein API-Token . . . . . 1
Ihr erster API-Aufruf . . . . . 2
Grundlegende Kubernetes-Konzepte . . . . . 3
Die Nutzung der Workflows wird vorbereitet . . . . . 3
Online-API-Referenz . . . . . 6

# Los geht's

## Bevor Sie beginnen

Sie können sich schnell auf den Einstieg in die Astra Control REST API vorbereiten, indem Sie die unten aufgeführten Schritte überprüfen.

**Astra-Konto besitzen Anmeldedaten**

Sie benötigen Astra-Anmeldeinformationen, um sich bei der Astra Web-Benutzeroberfläche anzumelden und ein API-Token zu generieren. Mit Astra Control Center verwalten Sie diese Anmeldedaten lokal. Mit dem Astra Control Service können Sie über den **Auth0**-Dienst auf die Anmeldeinformationen zugreifen.

**Lernen Sie die grundlegenden Kubernetes-Konzepte kennen**

Sie sollten mit verschiedenen grundlegenden Kubernetes-Konzepten vertraut sein. Siehe "Grundlegende Kubernetes-Konzepte" Finden Sie weitere Informationen.

**ÜBERPRÜFUNG DER REST-Konzepte und der Implementierung**

Prüfen Sie die Daten "Core-REST-Implementierung" Für Informationen über REST-Konzepte und die Details zur Entwicklung der Astra Control REST API.

**Weitere Informationen**

Beachten Sie die zusätzlichen Informationsressourcen, wie in vorgeschlagen "Weitere Ressourcen".

## Holen Sie sich ein API-Token

Sie müssen ein Astra API Token erhalten, um die Astra Control REST API zu verwenden.

### Überblick

Ein API-Token identifiziert den Anrufer an Astra und muss bei jedem REST-API-Aufruf enthalten sein.

- Sie müssen über die Astra Web-Benutzeroberfläche ein API-Token generieren.
- Das Verfahren zum Generieren eines Tokens ist für beide Astra-Implementierungsmodelle gleich. Nur die URL, die für den Zugriff auf Astra verwendet wird, ist anders.
- Die mit dem Token übermittelte Benutzeridentität und die zugehörigen Berechtigungen werden vom Benutzer bestimmt, der das Token erstellt hat.
- Das Token muss in das enthalten sein `Authorization` HTTP-Anfragekopf.
- Ein Token läuft nie ab, nachdem es erstellt wurde.
- Sie können ein Token über die Astra Web-Benutzeroberfläche widerrufen.

**Verwandte Informationen**

- "Ein API-Token widerrufen"

### Erstellen Sie ein Astra API-Token

In den folgenden Schritten wird beschrieben, wie ein Astra API Token erstellt wird.

**Bevor Sie beginnen**

Sie benötigen die Zugangsdaten für ein Astra-Konto.

### Über diese Aufgabe

Diese Aufgabe erzeugt ein API-Token in der Astra-Webschnittstelle. Sie sollten auch die Account-ID abrufen, die auch bei API-Aufrufen benötigt wird.

### Schritte

1. Melden Sie sich mit Ihren Account-Anmeldedaten für Astra wie folgt an:
   - Astra Control Service: "https://astra.netapp.io"
   - Astra Control Center: Verwenden Sie die bei der Installation festgelegte URL für Ihre lokale Umgebung
2. Klicken Sie auf das Figurensymbol oben rechts auf der Seite und wählen Sie **API Access**.
3. Klicken Sie auf der Seite auf **API-Token generieren** und klicken Sie dann im Popup-Fenster auf **API-Token generieren**.
4. Klicken Sie auf das Symbol, um die Token-Zeichenfolge in die Zwischenablage zu kopieren und im Editor zu speichern.
5. Kopieren Sie die Konto-id, die auf derselben Seite verfügbar ist, und speichern Sie sie.

### Nachdem Sie fertig sind

Wenn Sie über Curl oder eine Programmiersprache auf die Astra Control REST-API zugreifen, müssen Sie das API-Trägertoken in das HTTP einschließen `Authorization` Kopfzeile der Anfrage.

# Ihr erster API-Aufruf

Sie können einen einfachen curl Befehl an Ihrer Workstation CLI ausgeben, um mit dem Astra Control REST API zu beginnen und seine Verfügbarkeit zu bestätigen.

### Bevor Sie beginnen

Das Dienstprogramm Curl muss auf Ihrer lokalen Workstation verfügbar sein. Sie müssen außerdem über ein API-Token und die zugehörige Account-ID verfügen. Siehe "Holen Sie sich ein API-Token" Finden Sie weitere Informationen.

### Beispiel für die Wellung

Der folgende Curl Befehl ruft eine Liste der Astra-Benutzer ab. Geben Sie die entsprechenden <ACCOUNT_ID> und <API_TOKEN> wie angegeben an.

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

**Beispiel für eine JSON-Ausgabe**

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

# Grundlegende Kubernetes-Konzepte

Es gibt verschiedene Kubernetes-Konzepte, die für die Verwendung der Astra REST API relevant sind.

## Objekte

Die in einer Kubernetes-Umgebung gepflegten Objekte sind persistente Einheiten, die die Konfiguration des Clusters repräsentieren. Diese Objekte beschreiben zusammen den Status des Systems einschließlich des Cluster-Workloads.

## Namespaces

Namespaces bieten eine Technik zum Isolation von Ressourcen in einem einzigen Cluster. Diese Organisationsstruktur ist nützlich, wenn die Arten von Arbeit, Nutzer und Ressourcen aufgeteilt werden. Objekte mit einem Umfang „*Namespace“* müssen innerhalb des Namespace eindeutig sein, während Objekte mit einem „*Cluster Scope*“ im gesamten Cluster eindeutig sein müssen.

## Etiketten

Labels können den Kubernetes-Objekten zugeordnet werden. Sie beschreiben Attribute mit Schlüsselwert-Paaren und können eine beliebige Organisation auf dem Cluster durchsetzen. Diese können sich für ein Unternehmen nützlich sein, liegen aber nicht in der zentralen Handhabung von Kubernetes.

# Die Nutzung der Workflows wird vorbereitet

Vor der Live-Implementierung sollten Sie sich mit der Organisation und dem Format der Astra-Workflows vertraut machen.

## Einführung

Ein *Workflow* ist eine Sequenz aus einem oder mehreren Schritten, die zum Erreichen einer bestimmten administrativen Aufgabe oder eines bestimmten Ziels erforderlich sind. Jeder Schritt in einem Astra Control Workflow ist einer der folgenden:

- REST-API-Aufruf (mit Details wie Curl- und JSON-Beispiele)
- Aufruf eines weiteren Astra-Workflows
- Sonstige verwandte Aufgaben (z. B. die Entscheidung für eine erforderliche Designentscheidung)

Workflows umfassen die wichtigsten Schritte und Parameter, die zur Durchführung jeder Aufgabe erforderlich sind. Sie bieten als Ausgangspunkt für die Anpassung Ihrer Automatisierungsumgebung.

## Allgemeine Eingabeparameter

Die unten beschriebenen Eingabeparameter sind für alle Curl-Proben, die zur Veranschaulichung eines REST-API-Aufrufs verwendet werden, üblich.

> Da diese Eingabeparameter universell erforderlich sind, werden sie in den einzelnen Arbeitsabläufen nicht weiter beschrieben. Wenn für ein bestimmtes Curl-Beispiel zusätzliche Eingabeparameter verwendet werden, werden sie im Abschnitt **zusätzliche Eingabeparameter** beschrieben.

### Pfadparameter

Der bei jedem REST-API-Aufruf verwendete Endpunkt-Pfad umfasst die folgenden Parameter. Siehe auch "URL-Format" Finden Sie weitere Informationen.

**Konto-ID**

Dies ist der UUIDv4-Wert, der das Astra-Konto identifiziert, auf dem der API-Vorgang ausgeführt wird. Siehe "Holen Sie sich ein API-Token" Weitere Informationen zur Suche nach Ihrer Konto-ID.

### Anfragekopfzeilen

Je nach REST-API-Aufruf müssen Sie möglicherweise mehrere Anforderungsheader einbeziehen.

**Autorisierung**

Für alle API-Aufrufe in den Workflows wird ein API-Token zur Identifizierung des Benutzers benötigt. Sie müssen das Token in das aufnehmen `Authorization` Kopfzeile der Anfrage. Siehe "Holen Sie sich ein API-Token" Weitere Informationen zum Generieren eines API-Tokens finden Sie unter.

**Content-Typ**

Mit dem HTTP-POST und PUT-Anfragen, bei denen JSON im Anforderungstext enthalten ist, sollten Sie den Medientyp basierend auf der Astra-Ressource deklarieren. Beispielsweise können Sie die Kopfzeile einschließen `Content-Type: application/astra-appSnap+json` Beim Erstellen eines Snapshots für eine verwaltete Anwendung.

**Akzeptieren**

Sie können den spezifischen Medientyp des Inhalts, den Sie in der Antwort erwarten, basierend auf der Astra-Ressource erklären. Beispielsweise können Sie die Kopfzeile einschließen `Accept: application/astra-appBackup+json` Wenn Sie die Backups für eine gemanagte Applikation auflisten. Zur Vereinfachung akzeptieren die Wellproben in den Workflows jedoch alle Medientypen.

## Darstellung von Token und Identifikatoren

Das API-Token und andere ID-Werte, die mit den Curl-Beispielen verwendet werden, sind undurchsichtig und haben keine erkennbare Bedeutung. Um die Lesbarkeit der Proben zu verbessern, werden die tatsächlichen Token- und ID-Werte nicht verwendet. Stattdessen werden kleinere reservierte Schlüsselwörter verwendet, die mehrere Vorteile haben:

- Die Curl- und JSON-Proben sind klarer und leichter zu verstehen.
- Da alle Schlüsselwörter dasselbe Format mit Klammern und Großbuchstaben verwenden, können Sie schnell den Ort und den Inhalt identifizieren, der eingefügt oder extrahiert werden soll.
- Kein Wert geht verloren, da die ursprünglichen Parameter nicht kopiert und bei einer tatsächlichen Implementierung verwendet werden können.

Hier sind einige der in den Curl-Beispielen verwendeten allgemein reservierten Schlüsselwörter. Diese Liste ist nicht vollständig und weitere Schlüsselwörter werden bei Bedarf verwendet. Ihre Bedeutung sollte auf der Grundlage des Kontexts offensichtlich sein.

| Stichwort | Typ | Beschreibung |
|---|---|---|
| <ACCOUNT_ID> | Pfad | Der UUIDv4-Wert identifiziert das Konto, auf dem der API-Vorgang ausgeführt wird. |
| <API_TOKEN> | Kopfzeile | Das Inhaberzeichen, das den Anrufer identifiziert und autorisiert. |
| <APP_ID> | Pfad | Der UUIDv4-Wert, der die Anwendung für den API-Aufruf identifiziert. |

## Workflow-Kategorien

Je nach Ihrem Implementierungsmodell stehen Ihnen zwei weit gefassten Kategorien von Astra-Workflows zur Verfügung. Wenn Sie Astra Control Center nutzen, sollten Sie mit den Infrastruktur-Workflows beginnen und anschließend mit den Management-Workflows fortfahren. Mit dem Astra Control Service können Sie in der Regel direkt zu den Management-Workflows wechseln.

Die Curl-Beispiele in den Workflows verwenden die URL für den Astra Control Service. Sie müssen die URL ändern, wenn Sie das On-Premise Astra Control Center entsprechend Ihrer Umgebung verwenden.

### Infrastruktur-Workflows

Diese Workflows befassen sich mit der Astra-Infrastruktur, einschließlich Referenzen, Buckets und Storage-Back-Ends. Sie werden mit dem Astra Control Center benötigt, können aber in den meisten Fällen auch mit dem Astra Control Service verwendet werden. Die Workflows konzentrieren sich auf die Aufgaben, die für die Einrichtung und Wartung eines von Astra gemanagten Clusters erforderlich sind.

### Management-Workflows

Diese Workflows können nach einem verwalteten Cluster verwendet werden. Die Workflows konzentrieren sich auf die Applikationssicherung und unterstützen Abläufe wie das Backup, Restore und Klonen einer Applikation.

# Online-API-Referenz

## Zugriff auf die Referenzdokumentation zur Astra API

Sie können auf die Details der Astra Control REST-API-Aufrufe zugreifen, einschließlich HTTP-Methoden, Eingabeparameter und Antworten. Diese vollständige Referenz ist hilfreich, wenn Automatisierungsapplikationen mithilfe der REST API entwickelt werden.

### Bevor Sie beginnen

Sie benötigen die Zugangsdaten, um sich für Ihre Implementierung in der Astra Web-Benutzeroberfläche anzumelden. Für Astra Control Service und Astra Control Center gilt die gleiche Vorgehensweise für den Zugriff auf die Referenzdokumentation. Nur die URL ist anders. Ein API-Token ist nicht erforderlich, um auf das Referenzdok zuzugreifen und es anzuzeigen.

### Schritte

1. Melden Sie sich mit Ihren Account-Anmeldedaten für Astra wie folgt an:
   - Astra Control Service: "https://astra.netapp.io"
   - Astra Control Center: Verwenden Sie die bei der Installation festgelegte URL für Ihre lokale Umgebung
2. Klicken Sie auf das Figurensymbol oben rechts auf der Seite und wählen Sie **API Access**.
3. Klicken Sie oben auf der Seite auf die URL, die unter **API Documentation** angezeigt wird.

### Ergebnis

Die Seite Swagger wird in einem neuen Fenster oder Tab geöffnet. Hinweis: Die URL enthält die Konto-ID für das Konto, bei dem Sie sich angemeldet haben.

### Was kommt als Nächstes?

Sie können optional einen API-Aufruf von der Seite Swagger ausführen. Siehe "Einen Astra-REST-API-Aufruf ausgeben" Finden Sie weitere Informationen.

## Einen Astra-REST-API-Aufruf ausgeben

Sie können einen Astra Control REST API-Aufruf über die API-Referenzdokumentations-Seite ausgeben.

### Bevor Sie beginnen

Sie müssen sich bei Astra anmelden und auf die API-Referenzseite zugreifen. Siehe "Zugriff auf die Referenzdokumentation zur Astra API" Finden Sie weitere Informationen. Sie benötigen außerdem ein Token, um die REST-API zu verwenden. Siehe "Holen Sie sich ein API-Token" Für Details zum Generieren eines API-Tokens.

### Schritte

1. Klicken Sie oben auf der API-Referenzseite auf **Autorisieren**.
2. Kopieren Sie Ihren API-Token-Wert in das Feld im Popup-Fenster, klicken Sie auf **autorisieren** und klicken Sie dann auf **Schließen**.
3. Blättern Sie auf der Seite nach unten, und öffnen Sie den gewünschten API-Aufruf.
4. Klicken Sie auf der rechten Seite auf **Probieren Sie es aus**.
5. Scrollen Sie innerhalb desselben API-Anrufs nach unten. Geben Sie alle erforderlichen Parameterwerte

ein, und klicken Sie auf **Ausführen**, um den Aufruf auszustellen.

**Ergebnis**

Der API-Aufruf wird ausgeführt und der HTTP-Statuscode wird angezeigt.

**Copyright-Informationen**

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

**Markeninformationen**

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.