# Commencez

## Astra Automation

NetApp
August 11, 2025

This PDF was generated from https://docs.netapp.com/fr-fr/astra-automation-2304/get-started/before_get_started.html on August 11, 2025. Always check docs.netapp.com for the latest.

# Sommaire


Commencez . . . 1
- Avant de commencer . . . 1
- Obtenir un jeton API . . . 1
  - Introduction . . . 1
  - Créez un jeton API Astra . . . 2
- Votre premier appel API . . . 2
- Préparez l'utilisation des workflows . . . 3
  - Introduction . . . 3
  - Paramètres d'entrée communs . . . 3
  - Présentation des jetons et des identificateurs . . . 4
  - Catégories de flux de travail . . . 5
- Concepts de base de Kubernetes . . . 5
  - Objets . . . 5
  - Espaces de noms . . . 5
  - Étiquettes . . . 5
- Référence d'API en ligne . . . 6
  - Accédez à la documentation de référence d'Astra API . . . 6
  - Émettez un appel d'API REST Astra . . . 6

# Commencez

## Avant de commencer

Vous pouvez vous préparer rapidement à vous lancer avec l'API REST Astra Control en passant en revue les étapes ci-dessous.

**Possèdent des identifiants de compte Astra**

Vous aurez besoin d'informations d'identification Astra pour vous connecter à l'interface utilisateur Web Astra et générer un jeton API. Avec Astra Control Center, vous gérez ces informations d'identification localement. Avec le service de contrôle Astra, les informations d'identification du compte sont accessibles via le service **Auth0**.

**Concepts de base de Kubernetes**

Vous devez maîtriser plusieurs concepts Kubernetes de base. Voir "Concepts de base de Kubernetes" pour en savoir plus.

**Examiner les concepts DE REPOS et la mise en œuvre**

Assurez-vous de passer en revue "Implémentation DE l'APPLICATION REST de cœur" Pour plus d'informations sur les concepts DE REPOS et les détails concernant la conception de l'API REST Astra Control.

**En savoir plus**

Vous devez connaître les ressources d'information supplémentaires, comme le suggère le "Ressources supplémentaires".

## Obtenir un jeton API

Vous devez obtenir un jeton API Astra pour utiliser l'API REST Astra Control.

### Introduction

Un jeton API identifie l'appelant auprès d'Astra et doit être inclus avec chaque appel d'API REST.

- Vous devez générer un jeton d'API à l'aide de l'interface utilisateur web d'Astra.
- La procédure de génération d'un jeton est la même pour les deux modèles de déploiement Astra. Seule l'URL utilisée pour accéder à Astra est différente.
- L'identité de l'utilisateur avec le token et les autorisations associées sont déterminées par l'utilisateur qui a créé le token.
- Le jeton doit être inclus dans le `Authorization` En-tête de requête HTTP.
- Un jeton n'expire jamais après sa création.
- Vous pouvez révoquer un jeton dans l'interface utilisateur Web Astra.

**Informations associées**

- "Révoquer un jeton API"

## Créez un jeton API Astra

Les étapes suivantes décrivent comment créer un jeton API Astra.

### Avant de commencer

Vous avez besoin d'informations d'identification pour un compte Astra.

### Description de la tâche

Cette tâche génère un jeton API sur l'interface Web Astra. Vous devez également récupérer l'ID de compte qui est également nécessaire lors de la réalisation d'appels API.

### Étapes

1. Connectez-vous à Astra en utilisant les identifiants de votre compte comme suit :
   - ASTRA Control Service : "https://astra.netapp.io"
   - ASTRA Control Center : utilisez l'URL de votre environnement local tel qu'établi lors de l'installation
2. Cliquez sur l'icône figure en haut à droite de la page et sélectionnez **API Access**.
3. Cliquez sur **générer jeton API** sur la page, puis cliquez sur **générer jeton API** dans la fenêtre contextuelle.
4. Cliquez sur l'icône pour copier la chaîne de token dans le presse-papiers et l'enregistrer dans votre éditeur.
5. Copiez et enregistrez l'ID de compte disponible sur la même page.

### Une fois que vous avez terminé

Lorsque vous accédez à l'API REST d'Astra Control via curl ou un langage de programmation, vous devez inclure le jeton de support d'API dans le protocole HTTP `Authorization` en-tête de demande.

# Votre premier appel API

Vous pouvez lancer une commande curl simple sur la CLI de votre station de travail pour commencer à utiliser l'API REST Astra Control et confirmer sa disponibilité.

### Avant de commencer

L'utilitaire Curl doit être disponible sur votre poste de travail local. Vous devez également disposer d'un jeton API et de l'identifiant de compte associé. Voir "Obtenir un jeton API" pour en savoir plus.

### Exemple de boucle

La commande Curl suivante récupère la liste des utilisateurs Astra. Fournissez les <ACCOUNT_ID> et <API_TOKEN> appropriés comme indiqué.

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

**Exemple de sortie JSON**

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

# Préparez l'utilisation des workflows

Vous devez aussi connaître l'entreprise et le format des workflows Astra avant de les utiliser avec un déploiement en direct.

## Introduction

Un *workflow* est une séquence d'une ou de plusieurs étapes nécessaires à la réalisation d'une tâche ou d'un objectif administratif spécifique. Chaque étape d'un workflow de contrôle Astra est l'une des suivantes :

- Appel d'API REST (avec des détails tels que des exemples Curl et JSON)
- Appel d'un autre flux de travail Astra
- Tâche associée divers (par exemple, prise d'une décision de conception requise)

Ces flux de travail incluent les étapes clés et les paramètres nécessaires à l'exécution de chaque tâche. Ils constituent un point de départ pour la personnalisation de votre environnement d'automatisation.

## Paramètres d'entrée communs

Les paramètres d'entrée décrits ci-dessous sont communs à tous les échantillons curl utilisés pour illustrer un appel API REST.

> Comme ces paramètres d'entrée sont universellement requis, ils ne sont pas décrits plus en détail dans les flux de travail individuels. Si des paramètres d'entrée supplémentaires sont utilisés pour un exemple de boucle spécifique, ils sont décrits dans la section **Paramètres d'entrée supplémentaires**.

### Paramètres de chemin

Le chemin du noeud final utilisé avec chaque appel d'API REST inclut les paramètres suivants. Voir aussi "Format d'URL" pour en savoir plus.

#### ID de compte

Il s'agit de la valeur UUIDv4 identifiant le compte Astra sur lequel l'opération API s'exécute. Voir "Obtenir un jeton API" Pour plus d'informations sur la localisation de votre identifiant de compte.

### En-têtes de demande

En fonction de l'appel d'API REST, vous devrez peut-être inclure plusieurs en-têtes de requête.

#### Autorisation

Tous les appels d'API dans les workflows requièrent un jeton d'API pour identifier l'utilisateur. Vous devez inclure le token dans le `Authorization` en-tête de demande. Voir "Obtenir un jeton API" Pour plus d'informations sur la génération d'un jeton API.

#### Types de contenu

Avec LA PUBLICATION HTTP et LES requêtes PUT où JSON est inclus dans le corps de la demande, vous devez déclarer le type de support en fonction de la ressource Astra. Par exemple, vous pouvez inclure l'en-tête `Content-Type: application/astra-appSnap+json` lors de la création d'un snapshot pour une application gérée.

#### Accepter

Vous pouvez déclarer le type de support spécifique du contenu que vous attendez dans la réponse en fonction de la ressource Astra. Par exemple, vous pouvez inclure l'en-tête `Accept: application/astra-appBackup+json` lors de la liste des sauvegardes pour une application gérée. Cependant, pour plus de simplicité, les échantillons curl dans les flux de production acceptent tous les types de support.

## Présentation des jetons et des identificateurs

Le jeton API et les autres valeurs d'ID utilisées avec les exemples de boucles sont opaques sans signification perceptible. Afin d'améliorer la lisibilité des échantillons, les valeurs réelles de jeton et d'ID ne sont pas utilisées. Des mots-clés réservés plus petits sont utilisés, ce qui présente plusieurs avantages :

- Les échantillons curl et JSON sont plus clairs et plus faciles à comprendre.
- Comme tous les mots-clés utilisent le même format avec des crochets et des lettres majuscules, vous pouvez rapidement identifier l'emplacement et le contenu à insérer ou extraire.
- Aucune valeur n'est perdue car les paramètres d'origine ne peuvent pas être copiés et utilisés avec un déploiement réel.

Voici quelques-uns des mots-clés réservés communs utilisés dans les exemples curl. Cette liste n'est pas exhaustive et des mots-clés supplémentaires sont utilisés au besoin. Leur signification devrait être évidente sur la base du contexte.

| Mot-clé | Type | Description |
|---|---|---|
| <ID_COMPTE> | Chemin | Valeur UUIDv4 identifiant le compte sur lequel l'opération API s'exécute. |
| <API_TOKEN> | En-tête | Le jeton porteur identifiant et autorise l'appelant. |

| Mot-clé | Type | Description |
| --- | --- | --- |
| <ID_APP> | Chemin | Valeur UUIDv4 identifiant l'application pour l'appel d'API. |

## Catégories de flux de travail

Selon votre modèle de déploiement, vous pouvez consulter deux catégories de workflows Astra, Si vous utilisez Astra Control Center, vous devez d'abord les workflows d'infrastructure, puis passer aux workflows de gestion. Avec Astra Control Service, vous pouvez généralement accéder directement aux workflows de gestion.

Les exemples de boucles des flux de travail utilisent l'URL du service de contrôle Astra. Vous devez modifier l'URL lorsque vous utilisez le centre de contrôle Astra sur site en fonction de votre environnement.

### Workflows d'infrastructure

Ces workflows sont associés à l'infrastructure Astra, notamment les identifiants, les compartiments et les systèmes de stockage back-end. Elles sont nécessaires avec le centre de contrôle Astra, mais dans la plupart des cas peuvent également être utilisées avec le service de contrôle Astra. Les flux de travail se concentrent sur les tâches requises pour établir et gérer un cluster géré par Astra.

### Flux de travail de gestion

Vous pouvez utiliser ces flux de travail une fois que vous avez un cluster géré. Les workflows sont axés sur la protection des applications, ainsi que sur les opérations de prise en charge, comme la sauvegarde, la restauration et le clonage d'une application.

# Concepts de base de Kubernetes

Plusieurs concepts Kubernetes sont pertinents pour l'utilisation de l'API REST d'Astra.

## Objets

Les objets gérés dans un environnement Kubernetes sont des entités permanentes qui représentent la configuration du cluster. Ces objets décrivent collectivement l'état du système, y compris la charge de travail du cluster.

## Espaces de noms

Les espaces de noms fournissent une technique d'isolement des ressources au sein d'un même cluster. Cette structure organisationnelle est utile pour répartir les types de travail, d'utilisateurs et de ressources. Les objets avec un *namespace scope* doivent être uniques dans le namespace, tandis que ceux avec un *cluster scope* doivent être uniques dans tout le cluster.

## Étiquettes

Des étiquettes peuvent être associées aux objets Kubernetes. Ils décrivent les attributs à l'aide de paires de valeurs clés et peuvent appliquer une organisation arbitraire sur le cluster, ce qui peut être utile à une entreprise, mais ne fonctionne pas dans le système Kubernetes de base.

# Référence d’API en ligne

## Accédez à la documentation de référence d’Astra API

Vous pouvez accéder aux détails des appels de l’API REST Astra Control, y compris les méthodes HTTP, les paramètres d’entrée et les réponses. Cette référence complète est utile lors du développement d’applications d’automatisation à l’aide de l’API REST.

### Avant de commencer

Vous avez besoin de identifiants pour vous connecter à l’interface utilisateur web d’Astra pour votre déploiement. La procédure d’accès à la documentation de référence est la même pour Astra Control Service et Astra Control Center. Seule l’URL est différente. Un jeton API n’est pas nécessaire pour accéder au document de référence et l’afficher

### Étapes

1. Connectez-vous à Astra en utilisant les identifiants de votre compte comme suit :
   - ASTRA Control Service : "https://astra.netapp.io"
   - ASTRA Control Center : utilisez l’URL de votre environnement local tel qu’établi lors de l’installation
2. Cliquez sur l’icône figure en haut à droite de la page et sélectionnez **API Access**.
3. En haut de la page, cliquez sur l’URL affichée sous **Documentation API**.

### Résultat

La page swagger est lancée dans une nouvelle fenêtre ou un nouvel onglet. Notez que l’URL inclut l’ID de compte du compte avec lequel vous vous êtes connecté.

### Et la suite ?

Vous pouvez éventuellement exécuter un appel d’API à partir de la page swagger. Voir "Émettez un appel d’API REST Astra" pour en savoir plus.

## Émettez un appel d’API REST Astra

Vous pouvez émettre un appel d’API REST Astra Control à partir de la page de documentation de référence de l’API.

### Avant de commencer

Vous devez vous connecter à Astra et accéder à la page de référence de l’API. Voir "Accédez à la documentation de référence d’Astra API" pour en savoir plus. Vous avez également besoin d’un jeton pour utiliser l’API REST. Voir "Obtenir un jeton API" Pour plus d’informations sur la génération d’un jeton d’API.

### Étapes

1. En haut de la page de référence de l’API, cliquez sur **Autoriser**.
2. Copiez et collez votre valeur de jeton d’API dans le champ de la fenêtre contextuelle, cliquez sur **Autoriser**, puis cliquez sur **Fermer**.
3. Faites défiler la page vers le bas et ouvrez l’appel d’API souhaité.
4. Cliquez avec le bouton droit de la souris sur **essayez-le**.
5. Faites défiler vers le bas dans le même appel d’API. Indiquez les valeurs de paramètres requises et cliquez sur **Execute** pour émettre l’appel.

**Résultat**

L’appel API est exécuté et le code d’état HTTP s’affiche.

## Informations sur le copyright

Copyright © 2025 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

## Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site http://www.netapp.com/TM sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.