# Inizia subito

## Astra Automation

NetApp
January 31, 2025

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

# Sommario

Inizia subito . . . . . 1
Prima di iniziare . . . . . 1
Ottieni un token API . . . . . 1
La prima chiamata API . . . . . 2
Concetti di base di Kubernetes . . . . . 3
Preparati a utilizzare i flussi di lavoro . . . . . 3
Riferimento API online . . . . . 5

# Inizia subito

## Prima di iniziare

Puoi prepararti rapidamente a iniziare a utilizzare l'API REST di Astra Control seguendo i passaggi riportati di seguito.

**Disporre delle credenziali dell'account Astra**

Per accedere all'interfaccia utente web Astra e generare un token API, sono necessarie le credenziali Astra. Con Astra Control Center, queste credenziali vengono gestite in locale. Con Astra Control Service è possibile accedere alle credenziali dell'account tramite il servizio **Auth0**.

**Acquisire familiarità con i concetti di base di Kubernetes**

Dovresti avere familiarità con diversi concetti di base di Kubernetes. Vedere "Concetti di base di Kubernetes" per ulteriori informazioni.

**Esaminare i concetti DI REST e l'implementazione**

Assicurarsi di rivedere "Implementazione core REST" Per informazioni sui concetti REST e sui dettagli relativi alla progettazione dell'API REST di Astra Control.

**Ulteriori informazioni**

È necessario conoscere le risorse informative aggiuntive come suggerito in "Risorse aggiuntive".

## Ottieni un token API

Per utilizzare l'API REST di Astra Control è necessario ottenere un token API Astra.

### Panoramica

Un token API identifica il chiamante di Astra e deve essere incluso in ogni chiamata API REST.

- È necessario generare un token API utilizzando l'interfaccia utente web Astra.
- La procedura per generare un token è la stessa per entrambi i modelli di implementazione Astra. Solo l'URL utilizzato per accedere ad Astra è diverso.
- L'identità dell'utente con il token e le autorizzazioni associate sono determinate dall'utente che ha creato il token.
- Il token deve essere incluso in `Authorization` Intestazione della richiesta HTTP.
- Un token non scade mai dopo la sua creazione.
- È possibile revocare un token nell'interfaccia utente web Astra.

**Informazioni correlate**

- "Revocare un token API"

### Creare un token API Astra

La seguente procedura descrive come creare un token API Astra.

**Prima di iniziare**

Hai bisogno di credenziali per un account Astra.

**A proposito di questa attività**

Questa attività genera un token API nell'interfaccia web Astra. È inoltre necessario recuperare l'ID dell'account necessario anche per effettuare chiamate API.

**Fasi**

1. Accedi ad Astra utilizzando le credenziali del tuo account come segue:
   - Servizio di controllo Astra: "https://astra.netapp.io"
   - Astra Control Center (Centro di controllo Astra): Utilizzare l'URL dell'ambiente locale stabilito durante l'installazione
2. Fare clic sull'icona a forma di figura nella parte superiore destra della pagina e selezionare **API access**.
3. Fare clic su **generate API token** nella pagina, quindi fare clic su **generate API token** nella finestra popup.
4. Fare clic sull'icona per copiare la stringa del token negli Appunti e salvarla nell'editor.
5. Copiare e salvare l'id account disponibile nella stessa pagina.

**Al termine**

Quando si accede all'API REST di Astra Control tramite curl o un linguaggio di programmazione, è necessario includere il token del bearer API nell'HTTP `Authorization` intestazione della richiesta.

# La prima chiamata API

È possibile eseguire un semplice comando curl sulla CLI della workstation per iniziare a utilizzare l'API REST di Astra Control e verificarne la disponibilità.

**Prima di iniziare**

L'utility Curl deve essere disponibile sulla workstation locale. È inoltre necessario disporre di un token API e dell'identificativo account associato. Vedere "Ottieni un token API" per ulteriori informazioni.

**Esempio di arricciamento**

Il seguente comando Curl recupera un elenco di utenti Astra. Fornire il <ACCOUNT_ID> e il <API_TOKEN> appropriati, come indicato.

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

**Esempio di output JSON**

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

# Concetti di base di Kubernetes

Esistono diversi concetti di Kubernetes rilevanti quando si utilizza l'API ASTRA REST.

## Oggetti

Gli oggetti mantenuti in un ambiente Kubernetes sono entità persistenti che rappresentano la configurazione del cluster. Questi oggetti descrivono collettivamente lo stato del sistema, incluso il carico di lavoro del cluster.

## Spazi dei nomi

Gli spazi dei nomi forniscono una tecnica per isolare le risorse all'interno di un singolo cluster. Questa struttura organizzativa è utile quando si dividono i tipi di lavoro, gli utenti e le risorse. Gli oggetti con un *ambito dello spazio dei nomi* devono essere univoci all'interno dello spazio dei nomi, mentre quelli con un *ambito del cluster* devono essere univoci nell'intero cluster.

## Etichette

Le etichette possono essere associate agli oggetti Kubernetes. Descrivono gli attributi che utilizzano coppie chiave-valore e possono imporre un'organizzazione arbitraria sul cluster, che può essere utile a un'organizzazione ma non è al di fuori dell'operazione Kubernetes principale.

# Preparati a utilizzare i flussi di lavoro

Prima di utilizzarli con un'implementazione live, è necessario conoscere l'organizzazione e il formato dei flussi di lavoro Astra.

## Introduzione

Un *workflow* è una sequenza di uno o più passaggi necessari per eseguire un'attività o un obiettivo amministrativo specifico. Ogni fase del flusso di lavoro di Astra Control è una delle seguenti:

- REST API Call (con dettagli come ad esempio CURL e JSON)
- Invocazione di un altro workflow Astra
- Attività correlate a varie attività (come prendere una decisione di progettazione richiesta)

I flussi di lavoro includono i passaggi principali e i parametri necessari per eseguire ogni attività. Forniscono un punto di partenza per personalizzare il tuo ambiente di automazione.

## Parametri di input comuni

I parametri di input descritti di seguito sono comuni a tutti gli esempi di curl utilizzati per illustrare una chiamata API REST.

> Poiché questi parametri di input sono universalmente richiesti, non vengono descritti ulteriormente nei singoli flussi di lavoro. Se si utilizzano parametri di input aggiuntivi per un esempio specifico di curl, questi sono descritti nella sezione **parametri di input aggiuntivi**.

### Parametri del percorso

Il percorso dell'endpoint utilizzato con ogni chiamata API REST include i seguenti parametri. Vedere anche "Formato URL" per ulteriori informazioni.

**ID account**
: Questo è il valore UUIDv4 che identifica l'account Astra in cui viene eseguita l'operazione API. Vedere "Ottieni un token API" Per ulteriori informazioni su come individuare l'ID account.

### Intestazioni delle richieste

A seconda della chiamata API REST, potrebbe essere necessario includere diverse intestazioni di richiesta.

**Autorizzazione**
: Tutte le chiamate API nei flussi di lavoro richiedono un token API per identificare l'utente. È necessario includere il token in `Authorization` intestazione della richiesta. Vedere "Ottieni un token API" Per ulteriori informazioni sulla generazione di un token API.

**Tipo di contenuto**
: Con le richieste HTTP POST e PUT in cui JSON è incluso nel corpo della richiesta, è necessario dichiarare il tipo di supporto in base alla risorsa Astra. Ad esempio, è possibile includere l'intestazione `Content-Type: application/astra-appSnap+json` quando si crea uno snapshot per un'applicazione gestita.

**Accettare**
: È possibile dichiarare il tipo di supporto specifico del contenuto previsto nella risposta in base alla risorsa Astra. Ad esempio, è possibile includere l'intestazione `Accept: application/astra-appBackup+json` quando si elencano i backup per un'applicazione gestita. Tuttavia, per semplicità, i campioni di arricciatura nei flussi di lavoro accettano tutti i tipi di supporto.

## Presentazione di token e identificatori

Il token API e gli altri valori ID utilizzati con gli esempi di curl sono opachi e non sono comprensibili. Per migliorare la leggibilità dei campioni, non vengono utilizzati i valori token e ID effettivi. Piuttosto, vengono utilizzate parole chiave riservate più piccole che hanno diversi benefici:

- I campioni Curl e JSON sono più chiari e comprensibili.
- Poiché tutte le parole chiave utilizzano lo stesso formato con parentesi quadre e lettere maiuscole, è possibile identificare rapidamente la posizione e il contenuto da inserire o estrarre.
- Nessun valore viene perso perché i parametri originali non possono essere copiati e utilizzati con un'implementazione effettiva.

Ecco alcune delle parole chiave riservate più comuni utilizzate negli esempi di curl. Questo elenco non è esaustivo e vengono utilizzate parole chiave aggiuntive in base alle necessità. Il loro significato dovrebbe essere ovvio in base al contesto.

| Parola chiave | Tipo | Descrizione |
|---|---|---|
| <ACCOUNT_ID> | Percorso | Il valore UUIDv4 che identifica l'account in cui viene eseguita l'operazione API. |
| <API_TOKEN> | Intestazione | Il token del bearer che identifica e autorizza il chiamante. |
| <APP_ID> | Percorso | Il valore UUIDv4 che identifica l'applicazione per la chiamata API. |

## Categorie di workflow

Sono disponibili due ampie categorie di flussi di lavoro Astra in base al modello di implementazione. Se si utilizza Astra Control Center, è necessario iniziare con i flussi di lavoro dell'infrastruttura e passare ai flussi di lavoro di gestione. Quando si utilizza Astra Control Service, in genere è possibile accedere direttamente ai flussi di lavoro di gestione.

Gli esempi di arricciatura nei flussi di lavoro utilizzano l'URL per Astra Control Service. È necessario modificare l'URL quando si utilizza l'Astra Control Center on-premise in base all'ambiente in uso.

### Flussi di lavoro dell'infrastruttura

Questi flussi di lavoro si occupano dell'infrastruttura Astra, inclusi credenziali, bucket e backend dello storage. Sono necessari con Astra Control Center, ma nella maggior parte dei casi possono essere utilizzati anche con Astra Control Service. I flussi di lavoro si concentrano sulle attività necessarie per stabilire e gestire un cluster gestito da Astra.

### Workflow di gestione

È possibile utilizzare questi flussi di lavoro dopo aver gestito un cluster. I flussi di lavoro si concentrano sulla protezione delle applicazioni e supportano operazioni come il backup, il ripristino e la clonazione di un'applicazione.

# Riferimento API online

## Accedere alla documentazione di riferimento API Astra

È possibile accedere ai dettagli delle chiamate REST API di Astra Control, inclusi i metodi HTTP, i parametri di input e le risposte. Questo riferimento completo è utile quando si sviluppano applicazioni di automazione utilizzando l'API REST.

### Prima di iniziare

Sono necessarie le credenziali per accedere all'interfaccia utente Web Astra per la distribuzione. La procedura per accedere alla documentazione di riferimento è la stessa per Astra Control Service e Astra Control Center. Solo l'URL è diverso. Non è necessario un token API per accedere e visualizzare il documento di riferimento.

### Fasi

1. Accedi ad Astra utilizzando le credenziali del tuo account come segue:
   - Servizio di controllo Astra: "https://astra.netapp.io"
   - Astra Control Center (Centro di controllo Astra): Utilizzare l'URL dell'ambiente locale stabilito durante l'installazione
2. Fare clic sull'icona a forma di figura nella parte superiore destra della pagina e selezionare **API access**.
3. Nella parte superiore della pagina, fare clic sull'URL visualizzato sotto **API Documentation** (documentazione API).

### Risultato

La pagina Swagger viene avviata in una nuova finestra o scheda. L'URL include l'ID dell'account con cui hai effettuato l'accesso.

### Quali sono le prossime novità?

Facoltativamente, è possibile eseguire una chiamata API dalla pagina Swagger. Vedere "Eseguire una chiamata API Astra REST" per ulteriori informazioni.

## Eseguire una chiamata API Astra REST

È possibile eseguire una chiamata all'API REST di Astra Control dalla pagina di documentazione di riferimento API.

### Prima di iniziare

Devi accedere ad Astra e alla pagina di riferimento API. Vedere "Accedere alla documentazione di riferimento API Astra" per ulteriori informazioni. È inoltre necessario un token per utilizzare l'API REST. Vedere "Ottieni un token API" Per informazioni dettagliate sulla generazione di un token API.

### Fasi

1. Nella parte superiore della pagina di riferimento API, fare clic su **autorizzare**.
2. Copiare e incollare il valore del token API nel campo della finestra popup, fare clic su **autorizzare**, quindi fare clic su **Chiudi**.
3. Scorrere la pagina verso il basso e aprire la chiamata API desiderata.
4. Fare clic con il pulsante destro del mouse su **Provalo**.
5. Scorrere verso il basso all'interno della stessa chiamata API. Fornire i valori dei parametri richiesti e fare clic su **Execute** (Esegui) per effettuare la chiamata.

### Risultato

La chiamata API viene eseguita e viene visualizzato il codice di stato HTTP.

## Informazioni sul copyright

Copyright © 2025 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEQUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

## Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina http://www.netapp.com/TM sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.