Astra Control Automation 22.08 - Dokumentation

Astra Automation 22.08

NetApp
June 28, 2024

Inhalt

Astra Control Automation 22.08 - Dokumentation

Versionshinweise

Informationen zu diesem Release

Die Dokumentation auf dieser Seite beschreibt die Astra Control REST API und die damit verbundenen Automatisierungstechnologien, die mit der August 2022 (22.08) Version von Astra Control verfügbar sind. Diese Version der REST-API ist insbesondere mit den entsprechenden 22.08 Versionen von Astra Control Center und Astra Control Service enthalten.

Weitere Informationen zu diesem Release sowie zu vorherigen Versionen finden Sie auf den folgenden Seiten und den folgenden Websites:

- "Neuerungen bei der Astra Control REST-API"
- "REST-Ressourcen und -Endpunkte"
- "Astra Control Center 22.08-Dokumentation"
- "Dokumentation des Astra Control Service"
- "Frühere Versionen der Dokumentation von Astra Automation"

Bleiben Sie mit Twitter am Ball. @NetAppDoc. Senden Sie Feedback zu Dokumentation, indem Sie ein "GitHub-Autor" Oder senden Sie eine E-Mail an doccomments@netapp.com.

Was ist neu mit der Astra Control REST API

NetApp aktualisiert regelmäßig die Astra Control REST API und bietet Ihnen neue Funktionen, Verbesserungen und Fehlerbehebungen.

August 10 2022 (22.08)

Diese Version umfasst eine Erweiterung und Aktualisierung der REST-API sowie erweiterte Sicherheits- und Administrationsfunktionen.

Neue und verbesserte Astra-Ressourcen

Es wurden drei neue Ressourcen-Typen hinzugefügt: **Zertifikat**, **Gruppe** und **AppMirror**. Darüber hinaus wurden die Versionen verschiedener vorhandener Ressourcen aktualisiert.

LDAP-Authentifizierung

Optional können Sie Astra Control Center so konfigurieren, dass sie sich in einen LDAP-Server integrieren lassen, um ausgewählte Astra-Benutzer zu authentifizieren. Siehe "LDAP-Konfiguration" Finden Sie weitere Informationen.

Verbesserter Execution Hook

Die Astra Control 21.12 Version bietet zusätzliche Unterstützung für die Testdurchführung. Zusätzlich zu den vorhandenen Hooks für die vor- und NachSnapshot-Ausführung können Sie nun mit der Version 22.08 die folgenden Testausführungshaken konfigurieren:

- Vor dem Backup
- Nach dem Backup
- Nach dem Wiederherstellen

Astra Control ermöglicht jetzt auch die Verwendung desselben Skripts für mehrere Testausführungshaken.

Applikationsreplizierung mit SnapMirror

Daten und Applikationsänderungen lassen sich nun mithilfe der NetApp SnapMirror Technologie auf Clustern replizieren. Diese Verbesserung kann auch zur Verbesserung Ihrer Business Continuity- und Recovery-Funktionen eingesetzt werden.

Verwandte Informationen

- "Astra Control Center: Was ist neu"
- "Astra Control Service: Was ist neu"

26. April 2022 (22.04)

Diese Version umfasst eine Erweiterung und Aktualisierung der REST-API sowie erweiterte Sicherheits- und Administrationsfunktionen.

Neue und verbesserte Astra-Ressourcen

Es wurden zwei neue Ressourcen-Typen hinzugefügt: **Paket** und **Upgrade**. Außerdem wurden die Versionen verschiedener vorhandener Ressourcen aktualisiert.

Erweiterte RBAC mit Namespace-Granularität

Wenn Sie eine Rolle einem zugeordneten Benutzer zuweisen, können Sie die Namespaces beschränken, auf die der Benutzer Zugriff hat. Siehe * Role Binding API* Referenz und "RBAC-Sicherheit" Finden Sie weitere Informationen.

Entfernen des Buckets

Sie können einen Eimer entfernen, wenn er nicht mehr benötigt wird oder nicht ordnungsgemäß funktioniert.

Unterstützung von Cloud Volumes ONTAP

Cloud Volumes ONTAP wird nun als Storage Back-End unterstützt.

Zusätzliche Produktverbesserungen

Die beiden Astra Control-Produktimplementierungen sind mit einigen zusätzlichen Verbesserungen vertraut:

- Generischer Eingang für Astra Control Center
- Privates Cluster in AKS
- Unterstützung für Kubernetes 1.22
- Unterstützung des VMware Tanzu Portfolios

Sehen Sie sich die Seite **Was ist neu** auf den Dokumentationsseite des Astra Control Centers und des Astra Control Service an.

Verwandte Informationen

- "Astra Control Center: Was ist neu"
- "Astra Control Service: Was ist neu"

Bis 14. Dezember 2021 (21.12)

Dieses Release enthält eine Erweiterung der REST API sowie eine Änderung der Dokumentationsstruktur, um die Entwicklung von Astra Control durch zukünftige Release-Updates besser zu unterstützen.

Separate Dokumentation für Astra Automation für jede Version von Astra Control

Jede Version von Astra Control verfügt über eine eigene REST-API, die auf die Funktionen der spezifischen Version zugeschnitten wurde. Die Dokumentation für jede Version der Astra Control REST API ist jetzt auf einer eigenen dedizierten Website zusammen mit dem zugehörigen GitHub Content Repository verfügbar. Die Hauptdoktorandseite "Astra Control Automation" Enthält immer die Dokumentation für die aktuellste Version. Siehe "Frühere Versionen der Dokumentation Astra Control Automation" Weitere Informationen zu vorherigen Releases.

Erweiterung der REST-Ressourcentypen

Die Anzahl DER REST-Ressourcentypen hat sich mit Schwerpunkt auf Ausführungs-Hooks und Storage-Back-Ends weiter erweitert. Die neuen Ressourcen umfassen: Konto, Testsuite, Hook Source, Execution Hook Override, Cluster Node, Managed Storage Back-End, Namespace, Storage-Gerät und Storage-Node. Siehe "Ressourcen" Finden Sie weitere Informationen.

NetApp Astra Control Python SDK

NetApp Astra Control Python SDK ist ein Open-Source-Paket, mit dem sich der Automatisierungscode für Ihre Astra Control Umgebung leichter entwickeln lässt. Der Kern ist das Astra SDK, das eine Reihe von Klassen umfasst, um die Komplexität der REST API Aufrufe zu abstrahieren. Es gibt auch ein Toolkit-Skript zur Ausführung spezifischer administrativer Aufgaben durch Zusammenfassung und Abstrahierung der Python-Klassen. Siehe "NetApp Astra Control Python SDK" Finden Sie weitere Informationen.

August 5 2021 (21.08)

Diese Version umfasst die Einführung eines neuen Astra Implementierungsmodells und eine wesentliche Erweiterung der REST-API.

Astra Control Center-Implementierungsmodell

Neben dem vorhandenen Astra Control Service, der als Public Cloud-Service bereitgestellt wird, umfasst diese Version auch das On-Premises-Implementierungsmodell von Astra Control Center. Sie können Astra Control Center an Ihrem Standort installieren und so Ihre lokale Kubernetes-Umgebung managen. Die beiden Astra Control Implementierungsmodelle nutzen dieselbe REST-API, wobei in der Dokumentation nur geringfügige Unterschiede zu berücksichtigen sind.

Erweiterung der REST-Ressourcentypen

Die Zahl der Ressourcen, auf die über die Astra Control REST-API zugegriffen werden kann, ist enorm erweitert. Viele der neuen Ressourcen bilden die Grundlage für das On-Premises Astra Control Center-Angebot. Die neuen Ressourcen umfassen: ASUP, Berechtigung, Funktion, Lizenz, Einstellung, Abonnement, Bucket, Cloud, Cluster, gemanagtes Cluster, Back-End-Storage und Storage-Klasse. Siehe "Ressourcen" Finden Sie weitere Informationen.

Zusätzliche Endpunkte unterstützen eine Astra Implementierung

Neben den erweiterten REST-Ressourcen stehen noch mehrere weitere neue API-Endpunkte zur Unterstützung einer Astra Control Implementierung zur Verfügung.

OpenAPI-Unterstützung
: Die OpenAPI-Endpunkte bieten Zugriff auf das aktuelle OpenAPI JSON-Dokument und andere zugehörige Ressourcen.

Unterstützung von OpenMetrics
: Die OpenMetrics-Endpunkte bieten über die OpenMetrics-Ressource Zugriff auf Kontokennzahlen.

15. April 2021 (21.04)

Diese Version umfasst die folgenden neuen Funktionen und Verbesserungen.

Einführung DER REST API

Die Astra Control REST API ist für den Astra Control Service verfügbar. Das System wurde auf Basis VON REST-Technologien und aktuellen Best Practices erstellt. Die API ist die Grundlage für die Automatisierung Ihrer Astra-Implementierungen und umfasst die folgenden Funktionen und Vorteile.

Ressourcen
: Es sind vierzehn REST-Ressourcen verfügbar.

Zugriff auf API-Token
: Der Zugriff auf DIE REST-API wird über ein API-Zugriffstoken bereitgestellt, das Sie über die Astra Web-Benutzeroberfläche generieren können. Das API-Token bietet sicheren Zugriff auf die API.

Unterstützung für Sammlungen
: Es gibt eine umfangreiche Reihe von Abfrageparametern, die für den Zugriff auf die Ressourcen-Sammlungen verwendet werden können. Einige der unterstützten Vorgänge umfassen Filtern, Sortieren und Paginieren.

Bekannte Probleme

Sie sollten alle bekannten Probleme für die aktuelle Version im Zusammenhang mit der Astra Control REST API überprüfen. Die bekannten Probleme identifizieren Probleme, die die erfolgreiche Verwendung des Produkts verhindern könnten.

> Es gibt keine neuen Probleme, die mit der Version 22.08 der Astra Control REST API bekannt sind. Die unten beschriebenen Probleme wurden in vorherigen Versionen entdeckt und gelten noch für die aktuelle Version.

Es werden nicht alle Speichergeräte in einem Back-End-Speicher-Node erkannt

Wenn ein REST-API-Aufruf zum Abrufen der in einem Storage-Node definierten Speichergeräte ausruft, werden nur die Astra Data Store-Geräte erkannt. Es werden nicht alle Geräte zurückgegeben.

Überblick über die Merkmale und Vorteile

Astra Control Center und Astra Control Service bieten eine gemeinsame REST-API, auf die Sie direkt über eine Programmiersprache oder ein Dienstprogramm wie Curl zugreifen können. Die wichtigsten Highlights und Vorteile der API sind nachfolgend aufgeführt.

Um auf DIE REST-API zuzugreifen, müssen Sie sich zunächst bei der Astra Web-Benutzeroberfläche anmelden und ein API-Token generieren. Sie müssen das Token bei jeder API-Anforderung einschließen.

Basiert auf REST-Technologie

Die Astra Control API wurde mit REST-Technologie und aktuellen Best Practices erstellt. Die Kerntechnologie umfasst HTTP, JSON und RBAC.

Unterstützung der beiden Astra Control Implementierungsmodelle

Astra Control Service wird in der Public Cloud-Umgebung eingesetzt und Astra Control Center ist Ihre lokale Implementierung. Beide Implementierungsmodelle werden über eine REST-API unterstützt.

Klare Zuordnung zwischen REST-Endpunkt-Ressourcen und Objektmodell

Die externen REST-Endpunkte, mit denen auf die Ressourcenzuordnung auf ein konsistentes Objektmodell zugegriffen wird, das vom Astra-Service intern gewartet wird. Das Objektmodell basiert auf er-Modellierung (Entity-Relationship), mit der API-Aktionen und -Antworten klar definiert werden können.

Umfangreiche Reihe von Abfrageparametern

Die REST-API bietet eine umfangreiche Reihe von Abfrageparametern, mit denen Sie auf die Ressourcensammlungen zugreifen können. Einige der unterstützten Vorgänge umfassen Filtern, Sortieren und Paginieren.

Ausrichtung auf die Web-UI von Astra Control

Das Design der Astra Web-Benutzeroberfläche ist auf DIE REST-API abgestimmt, so dass es Konsistenz zwischen den beiden Zugriffspfaden und der Benutzererfahrung gibt.

Robuste Debugging- und Problemermittlung

Die Astra Control REST API bietet eine robuste Debugging- und Problembestimmung, einschließlich Systemereignissen und Benutzerbenachrichtigungen.

Workflow-Prozesse

Sie erhalten eine Reihe von Workflows, die Sie bei der Entwicklung Ihres Automatisierungscodes unterstützen. Die Workflows sind in zwei Kategorien unterteilt: Infrastruktur und Management.

Grundlage für erweiterte Automatisierungstechnologien

Neben dem direkten Zugriff auf DIE REST API können weitere Automatisierungstechnologien verwendet werden, die auf der REST-API basieren.

Teil der Dokumentation der Astra-Familie

Die Dokumentation der Astra Control Automation ist Teil der größeren Dokumentation der Astra-Familie. Siehe "Astra-Dokumentation" Finden Sie weitere Informationen.

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.

Einführung

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

- Sie können über die Astra Web-Benutzeroberfläche ein API-Token generieren.
- Die mit dem Token getragene Benutzeridentität wird vom Benutzer bestimmt, der das Token erstellt.
- 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 Anmeldedaten im Astra an.

   Rufen Sie die folgende Website für den Astra Control Service auf: "https://astra.netapp.io"

2. Klicken Sie auf das Figurensymbol oben rechts auf der Seite und wählen Sie **API Access**.
3. Klicken Sie auf **API-Token generieren** auf der Seite und klicken Sie 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-Träger-Token in das HTTP einbeziehen `Authorization` Kopfzeile der Anfrage.

Hallo Welt

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": {}
}
```


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.

Stichwort	Typ	Beschreibung
<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.

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.

Core-REST-Implementierung

REST-Web-Services

Representational State Transfer (REST) ist ein Stil für die Erstellung von verteilten Web-Anwendungen. Bei der Anwendung auf das Design einer Web-Services-API, stellt sie eine Reihe von Mainstream-Technologien und Best Practices für die Offenlegung serverbasierter Ressourcen und die Verwaltung ihrer Status. REST bietet eine konsistente Grundlage für die Applikationsentwicklung, doch je nach den jeweiligen Designoptionen können die Details jeder API variieren. Vor dem Einsatz in einer Live-Implementierung sollten Sie sich der Merkmale der Astra Control REST API bewusst sein.

Ressourcen- und Zustandsdarstellung

Ressourcen sind die Grundkomponenten eines webbasierten Systems. Beim Erstellen einer ANWENDUNG FÜR REST-Webservices umfassen die frühen Designaufgaben Folgendes:

- Identifizierung von System- oder serverbasierten Ressourcen

  Jedes System nutzt und verwaltet Ressourcen. Eine Ressource kann eine Datei-, Geschäftstransaktion-, Prozess- oder Verwaltungseinheit sein. Eine der ersten Aufgaben bei der Entwicklung einer auf REST-Webservices basierenden Applikation ist die Identifizierung der Ressourcen.

- Definition von Ressourcenstatus und zugehörigen Statusoperationen

  Die Ressourcen befinden sich immer in einer endlichen Anzahl von Staaten. Die Zustände sowie die damit verbundenen Operationen, die zur Auswirkung der Statusänderungen verwendet werden, müssen klar definiert werden.

URI-Endpunkte

Jede REST-Ressource muss definiert und über ein gut definiertes Adressierungssystem verfügbar gemacht werden. Die Endpunkte, in denen die Ressourcen gefunden und identifiziert werden, verwenden einen einheitlichen Resource Identifier (URI). Der URI bietet ein allgemeines Framework zum Erstellen eines eindeutigen Namens für jede Ressource im Netzwerk. Der Uniform Resource Locator (URL) ist ein URI-Typ, der mit Webservices zur Identifizierung und zum Zugriff von Ressourcen verwendet wird. Ressourcen werden in der Regel in einer hierarchischen Struktur ausgesetzt, die einem Dateiverzeichnis ähnelt.

HTTP-Meldungen

Hypertext Transfer Protocol (HTTP) ist das Protokoll, das vom Webservice-Client und -Server zum Austausch von Anforderungs- und Antwortmeldungen zu den Ressourcen verwendet wird. Im Rahmen der Entwicklung einer Web-Services-Anwendung werden HTTP-Methoden den Ressourcen und entsprechenden Statusmanagement-Aktionen zugeordnet. HTTP ist statusfrei. Um im Rahmen einer Transaktion eine Reihe verwandter Anforderungen und Antworten zuzuordnen, müssen daher zusätzliche Informationen in die HTTP-Header enthalten sein, die mit den Anforderungs- und Antwortdatenströmen verwendet werden.

JSON-Formatierung

Während Informationen auf verschiedene Weise zwischen einem Web-Services-Client und Server strukturiert und übertragen werden können, ist die beliebteste Option JavaScript Object Notation (JSON). JSON ist ein Branchenstandard für die Darstellung einfacher Datenstrukturen im Klartext und wird zur Übertragung von Zustandsdaten zur Beschreibung der Ressourcen verwendet. Die Astra Control REST API verwendet JSON, um die Daten zu formatieren, die im Körper von jeder HTTP-Anfrage und Antwort.

Ressourcen und Sammlungen

DIE Rest-API von Astra Control bietet Zugriff auf Ressourceninstanzen und Ressourcensammlungen.

Konzeptionell ist eine REST **Ressource** ähnlich wie ein **Objekt** wie mit den objektorientierten Programmiersprachen und -Systemen definiert. Manchmal werden diese Begriffe synonym verwendet. Aber im Allgemeinen wird „Ressource“ bevorzugt, wenn sie im Kontext der externen REST API verwendet wird, während „Objekt“ für die entsprechenden zustandsorientierte Instanz Daten verwendet wird, die auf dem Server gespeichert sind.

Eigenschaften der Astra-Ressourcen

Die Astra Control REST API entspricht den Prinzipien des RESTful Designs. Jede Astra-Ressourceninstanz wird auf Basis eines klar definierten Ressourcentyps erstellt. Eine Reihe von Ressourceninstanzen desselben Typs wird als **Sammlung** bezeichnet. Die API-Aufrufe wirken sich auf einzelne Ressourcen oder Ressourcensammlungen aus.

Ressourcentypen

Die in der Astra Control REST API enthaltenen Ressourcentypen weisen folgende Merkmale auf:

- Jeder Ressourcentyp wird mit einem Schema definiert (in der Regel in JSON)
- Jedes Ressourcenschema enthält den Ressourcentyp und die -Version
- Ressourcentypen sind global eindeutig

Ressourceninstanzen

Die über die Astra Control REST-API verfügbaren Ressourceinstanzen weisen folgende Merkmale auf:

- Ressourceninstanzen werden auf Basis eines einzelnen Ressourcentyps erstellt
- Der Ressourcentyp wird mit dem Wert Medientyp angezeigt
- Instanzen bestehen aus statusorientierten Daten, die vom Astra-Service gewartet werden
- Auf jede Instanz kann über eine eindeutige und langlebige URL zugegriffen werden
- In Fällen, in denen eine Ressourceninstanz mehr als eine Darstellung haben kann, können verschiedene Medientypen verwendet werden, um die gewünschte Darstellung anzufordern

Ressourcensammlungen

Die Ressourcensammlungen, die über die ASTRA Control REST-API verfügbar sind, weisen folgende Merkmale auf:

- Der Satz von Ressourceninstanzen eines einzelnen Ressourcentyps wird als Sammlung bezeichnet
- Ressourcensammlungen haben eine einzigartige und langlebige URL

Instanz-IDs

Jeder Ressourceninstanz wird bei der Erstellung eine Kennung zugewiesen. Diese Kennung ist ein 128-Bit UUIDv4-Wert. Die zugewiesenen UUUIDv4-Werte sind global eindeutig und unveränderbar. Nachdem ein API-Aufruf ausgegeben wurde, der eine neue Instanz erstellt, wird eine URL mit der zugehörigen id an den Anrufer in A zurückgegeben `Location` Kopfzeile der HTTP-Antwort. Sie können die Kennung extrahieren und bei nachfolgenden Anrufen verwenden, wenn Sie sich auf die Ressourceninstanz beziehen.

Die Ressourcen-ID ist der primäre Schlüssel, der für Sammlungen verwendet wird.

Gemeinsame Struktur für Astra-Ressourcen

Jede Astra Control-Ressource ist mit einer gemeinsamen Struktur definiert.

Einheitliche Daten

Jede Astra-Ressource enthält die in der folgenden Tabelle aufgeführten Schlüsselwerte.

Taste	Beschreibung
Typ	Ein global eindeutiger Ressourcentyp, der als **Ressourcentyp** bezeichnet wird.
Version	Eine Version-ID, die als **Resource-Version** bezeichnet wird.
id	Ein global eindeutiger Bezeichner, der als **Resource Identifier** bezeichnet wird.
Metadaten	Ein JSON-Objekt mit verschiedenen Informationen, einschließlich Benutzer- und Systemetiketten.

Metadatenobjekt

Das JSON-Metadatenobjekt, das in jeder Astra-Ressource enthalten ist, enthält die in der folgenden Tabelle aufgeführten Schlüsselwerte.

Taste	Beschreibung
Etiketten	JSON-Array mit Client-angegebenen Beschriftungen, die der Ressource zugeordnet sind.
CreationZeitstempel	JSON-Zeichenfolge mit einem Zeitstempel, der angibt, wann die Ressource erstellt wurde.
Änderungszeitstempel	JSON-Zeichenfolge mit einem ISO-8601-formatierten Zeitstempel, der angibt, wann die Ressource zuletzt geändert wurde.
Erstellt von	JSON-Zeichenfolge mit der UUUIDv4-Kennung der Benutzer-id, die die Ressource erstellt hat. Wenn die Ressource von einer internen Systemkomponente erstellt wurde und der Erstellungseinheit keine UUID zugeordnet ist, wird die **Null** UUID verwendet.

Ressourcenstatus

Ausgewählte Ressourcen A `state` Wert, der zur Orchestrierung von Lifecycle-Übergängen und zur Steuerung des Zugriffs eingesetzt wird.

HTTP-Details

Die Astra Control REST-API verwendet HTTP und zugehörige Parameter, um auf die Ressourceinstanzen und -Sammlungen zu reagieren. Einzelheiten zur HTTP-Implementierung finden Sie unten.

API-Transaktionen und das CRUD-Modell

Die Astra Control REST API implementiert ein transaktionsorientiertes Modell mit klar definierten Abläufen und Zustandsübergängen.

API-Transaktion bei Anfrage und Reaktion

Jeder REST-API-Aufruf erfolgt als HTTP-Anfrage an den Astra-Service. Jede Anforderung generiert eine entsprechende Antwort zurück an den Client. Dieses Request-Response-Paar kann als API-Transaktion betrachtet werden.

Unterstützung für CRUD-Betriebsmodell

Auf Grundlage des **CRUD**-Modells kann auf alle über die Astra Control REST API verfügbaren Ressourcen und Sammlungen zugegriffen werden. Es gibt vier Vorgänge, von denen jede einer einzigen HTTP-Methode zugeordnet wird. Dazu gehören:

- Erstellen
- Lesen
- Aktualisierung
- Löschen

Bei einigen der Astra-Ressourcen wird nur ein Teil dieser Vorgänge unterstützt. Sie sollten die überprüfen "API-Referenz" Weitere Informationen zu einem bestimmten API-Aufruf.

HTTP-Methoden

Die von der API unterstützten HTTP-Methoden oder Verben werden in der folgenden Tabelle dargestellt.

Methode	CRUD	Beschreibung
GET	Lesen	Ruft Objekteigenschaften für eine Ressourceninstanz oder -Sammlung ab. Dies wird als **list**-Operation bei Verwendung mit einer Sammlung betrachtet.
POST	Erstellen	Erstellt eine neue Ressourceninstanz basierend auf den Eingabeparametern. Die langfristige URL wird in A zurückgegeben `Location` Kopfzeile der Antwort.
PUT	Aktualisierung	Aktualisiert eine gesamte Ressourceninstanz mit dem mitgelieferten JSON Request Body. Wichtige Werte, die nicht vom Benutzer änderbar sind, bleiben erhalten.
Löschen	Löschen	Löscht eine vorhandene Ressourceninstanz.

Header für Anfragen und Antworten

Die folgende Tabelle fasst die HTTP-Header zusammen, die mit der Astra Control REST API verwendet werden.

Siehe "RFC 7232" Und "RFC 7233" Finden Sie weitere Informationen.

Kopfzeile	Typ	Nutzungshinweise
Akzeptieren	Anfrage	Wenn der Wert „/“ ist oder nicht angegeben wird, `application/json` Wird in der Kopfzeile der Inhaltstyp-Antwort zurückgegeben. Wenn der Wert auf den Astra Resource Media Type gesetzt ist, wird derselbe Medientyp in der Kopfzeile des Inhaltstyps zurückgegeben.
Autorisierung	Anfrage	Träger-Token mit dem API-Schlüssel für den Benutzer.
Inhaltstyp	Antwort	Wird basierend auf dem zurückgegeben `Accept` Kopfzeile der Anfrage.
Etag	Antwort	Im Lieferumfang eines erfolgreichen RFC 7232-Standards enthalten. Der Wert ist eine hexadezimale Darstellung des MD5-Werts für die gesamte JSON-Ressource.
If-Match	Anfrage	Ein Precondition Request Header, wie in Abschnitt 3.1 RFC 7232 beschrieben und unterstützt **PUT** Anforderungen.
Wenn-Geändert-Seit	Anfrage	Ein Precondition Request Header, wie in Abschnitt 3.4 RFC 7232 beschrieben und unterstützt **PUT** Anforderungen.
Wenn-Unmodified-Since	Anfrage	Ein Precondition Request Header, wie in Abschnitt 3.4 RFC 7232 beschrieben und unterstützt **PUT** Anforderungen.
Standort	Antwort	Enthält die vollständige URL der neu erstellten Ressource.

Abfrageparameter

Die folgenden Abfrageparameter stehen zur Verwendung mit Ressourcensammlungen zur Verfügung. Siehe "Arbeiten mit Sammlungen" Finden Sie weitere Informationen.

Abfrageparameter	Beschreibung
Einschließlich	Enthält die Felder, die beim Lesen einer Sammlung zurückgegeben werden sollen.
Filtern	Gibt die Felder an, die für die Rückgabe einer Ressource beim Lesen einer Sammlung übereinstimmen müssen.
Orderby	Bestimmt die Reihenfolge der beim Lesen einer Sammlung zurückgegebenen Ressourcen.
Grenze	Begrenzt die maximale Anzahl an Ressourcen, die beim Lesen einer Sammlung zurückgegeben werden.
überspringen	Legt fest, wie viele Ressourcen beim Lesen einer Sammlung weitergehen und überspringen sollen.
Zählen	Gibt an, ob die Gesamtzahl der Ressourcen im Metadatenobjekt zurückgegeben werden soll.

HTTP-Statuscodes

Im Folgenden werden die HTTP-Statuscodes beschrieben, die von der REST-API von Astra Control verwendet werden.

Die Astra Control REST API nutzt auch den **Problemdetails für HTTP APIs** Standard. Siehe "Diagnose und Support" Finden Sie weitere Informationen.

Codieren	Bedeutung	Beschreibung
200	OK	Zeigt Erfolg für Anrufe an, die keine neue Ressourceninstanz erstellen.
201	Erstellt	Ein Objekt wurde erfolgreich erstellt, und die Kopfzeile für die Standortantwort enthält die eindeutige Kennung für das Objekt.
204	Kein Inhalt	Die Anfrage war erfolgreich, obwohl kein Inhalt zurückgegeben wurde.
400	Schlechte Anfrage	Die Eingabe der Anfrage ist nicht erkannt oder nicht angemessen.
401	Nicht Autorisiert	Der Benutzer ist nicht autorisiert und muss authentieren.
403	Verboten	Der Zugriff wird aufgrund eines Autorisierungsfehlers verweigert.
404	Nicht gefunden	Die Ressource, auf die in diesem Antrag verwiesen wird, ist nicht vorhanden.
409	Konflikt	Der Versuch, ein Objekt zu erstellen, ist fehlgeschlagen, weil das Objekt bereits vorhanden ist.
500	Interner Fehler	Ein allgemeiner interner Fehler ist auf dem Server aufgetreten.
503	Service nicht verfügbar	Der Dienst ist aus irgendeinem Grund nicht bereit, die Anfrage zu bearbeiten.

URL-Format

Die allgemeine Struktur der URL, die für den Zugriff auf eine Ressourceninstanz oder -Sammlung über DIE REST-API verwendet wird, besteht aus mehreren Werten. Diese Struktur spiegelt das zugrunde liegende Objektmodell und das Systemdesign wider.

Konto als Root

Die Wurzel des Ressourcenpfads zu jedem REST-Endpunkt ist das Astra-Konto. Daher beginnen alle Pfade in der URL mit `/account/{account_id}` Wo `account_id` Ist der eindeutige UUUIDv4-Wert für das Konto. Interne Struktur Dies ist ein Design, in dem der gesamte Ressourcenzugriff auf einem bestimmten Konto basiert.

Kategorie der Endpoint-Ressourcen

Die Astra-Ressourcenendpunkte lassen sich in drei verschiedene Kategorien einteilen:

- Kern (`/core`)
- Gemanagte Applikation (`/k8s`)
- Topologie (`/topology`)

Siehe "Ressourcen" Finden Sie weitere Informationen.

Kategorienversion

Jede der drei Ressourcenkategorien verfügt über eine globale Version, die die Version der Ressourcen steuert, auf die zugegriffen wird. Nach Konventionen und Definition zu einer neuen Hauptversion einer Ressourcenkategorie wechseln (z. B. von) `/v1` Bis `/v2`) Wird Bruchänderungen in der API einführen.

Ressourceinstanz oder -Sammlung

Eine Kombination von Ressourcentypen und Identifikatoren kann im Pfad verwendet werden, basierend darauf, ob auf eine Ressourceninstanz oder -Sammlung zugegriffen wird.

Beispiel

- Ressourcenpfad

  Basierend auf der oben dargestellten Struktur ist ein typischer Pfad zu einem Endpunkt: `/accounts/{account_id}/core/v1/users`.

- Vollständige URL

  Die vollständige URL für den entsprechenden Endpunkt lautet: `https://astra.netapp.io/accounts/{account_id}/core/v1/users`.

Ressourcen und Endpunkte

Zur Automatisierung einer Astra Implementierung können Sie auf die Ressourcen zugreifen, die über die ASTRA Control REST-API bereitgestellt werden. Jede Ressource ist über einen oder mehrere Endpunkte verfügbar. Nachfolgend finden Sie eine Einführung zu DEN REST-Ressourcen, die Sie im Rahmen einer Automatisierungsimplementierung nutzen können.

Das Format des Pfads und der vollständigen URL für den Zugriff auf die Astra Control-Ressourcen basiert auf mehreren Werten. Siehe "URL-Format" Finden Sie weitere Informationen. Siehe auch "API-Referenz" Weitere Informationen zur Verwendung der Astra-Ressourcen und -Endpunkte.

Zusammenfassung der Astra Control REST-Ressourcen

Die primären Ressourcenendpunkte in der Astra Control REST API sind in drei Kategorien unterteilt. Auf jede Ressource kann mit allen CRUD-Vorgängen (Erstellen, Lesen, Aktualisieren, Löschen) zugegriffen werden, sofern nicht anders angegeben.

Die Spalte **Release** zeigt den Astra-Release an, als die Ressource zum ersten Mal eingeführt wurde. Dieses Feld ist für Ressourcen verfügbar, die mit der aktuellen Version neu hinzugefügt wurden.

Kernressourcen

Die Kernressourcenendpunkte bieten die grundlegenden Services, die zum Aufbau und zur Wartung der Astra-Laufzeitumgebung erforderlich sind.

Ressource	Freigabe	Beschreibung
Konto	21.12	Mithilfe der Account-Ressourcen können Sie die isolierten Mandanten innerhalb der mandantenfähigen Astra Control Implementierungsumgebung managen.
ASUP	21.08	Die ASUP Ressourcen stellen die AutoSupport Bundles dar, die an den NetApp Support weitergeleitet werden.
Zertifikat	**22.08**	Die Zertifikatressourcen stellen die installierten Zertifikate dar, die für eine starke Authentifizierung für ausgehende Verbindungen verwendet werden.
Anmeldedaten	21.04	Die Ressourcen für Zugangsdaten enthalten sicherheitsbezogene Informationen, die mit Astra-Benutzern, Clustern, Buckets und Storage-Back-Ends verwendet werden können.
Berechtigung	21.08	Die Berechtigungsressourcen stellen die Funktionen und Kapazitäten dar, die für ein Konto auf Basis der aktiven Lizenzen und Abonnements verfügbar sind.
Ereignis	21.04	Die Event-Ressourcen repräsentieren alle Ereignisse, die im System auftreten, einschließlich der Untergruppe, die als Benachrichtigungen klassifiziert ist.

Ressource	Freigabe	Beschreibung
Execution Hook	21.12	Die Hook-Ressourcen für die Ausführung stellen benutzerdefinierte Skripts dar, die Sie entweder vor oder nach einem Snapshot einer verwalteten App ausführen können.
Merkmal	21.08	Die Funktionsressourcen stellen ausgewählte Astra-Funktionen dar, die Sie abfragen können, um festzustellen, ob diese im System aktiviert oder deaktiviert sind. Der Zugriff ist auf schreibgeschützt beschränkt.
Gruppieren	**22.08**	Die Gruppenressourcen sind die Astra-Gruppen und die damit verbundenen Ressourcen. In der aktuellen Version werden nur LDAP-Gruppen unterstützt.
Hook-Quelle	21.12	Die Hakenquellenressourcen stellen den aktuellen Quellcode dar, der mit einem Testsuite verwendet wird. Die Trennung des Quellcodes von der Ausführungskontrolle hat mehrere Vorteile, wie z. B. die Freigabe der Skripte.
Lizenz	21.08	Die Lizenzressourcen stellen die für ein Astra-Konto verfügbaren Lizenzen dar.
Benachrichtigung	21.04	Die Benachrichtigungsressourcen sind Astra-Ereignisse mit einem Benachrichtigungsziel. Der Zugriff erfolgt auf Benutzerbasis.
Paket	22.04	Die Paketressourcen ermöglichen die Registrierung und den Zugriff auf Paketdefinitionen. Softwarepakete bestehen aus verschiedenen Komponenten, einschließlich Dateien, Bildern und anderen Artefakten.
Rollenbindung	21.04	Die Role Binding Ressourcen stellen die Beziehungen zwischen bestimmten Paaren von Benutzern und Konten dar. Zusätzlich zur Verknüpfung zwischen den beiden wird für jede über eine bestimmte Rolle ein Satz von Berechtigungen festgelegt.
Einstellung	21.08	Die Einstellungsressourcen stellen eine Sammlung von Schlüsselwert-Paaren dar, die ein Feature für ein bestimmtes Astra-Konto beschreiben.
Abonnement	21.08	Die Abonnementressourcen stellen die aktiven Abonnements für ein Astra-Konto dar.
Token	21.04	Die Token-Ressourcen stellen die Token dar, die für den programmatischen Zugriff auf die Astra Control REST API verfügbar sind.
Ungelesene Benachrichtigung	21.04	Die nicht gelesenen Benachrichtigungsressourcen stellen Benachrichtigungen dar, die einem bestimmten Benutzer zugewiesen, aber noch nicht gelesen wurden.
Upgrade	22.04	Die Upgrade-Ressourcen bieten Zugriff auf Softwarekomponenten und können Upgrades initiieren.
Benutzer	21.04	Die Benutzerressourcen sind Astra-Benutzer, die auf das System basierend auf ihrer definierten Rolle zugreifen können.

Gemanagte Applikationsressourcen

Die Endpunkte der gemanagten Applikationsressourcen bieten Zugriff auf die gemanagten Kubernetes-Applikationen.

Ressource	Freigabe	Beschreibung
Anwendungsressource	21.04	Die Anwendungsressourcen stellen interne Sammlungen von staatlichen Informationen dar, die für das Management der Astra-Anwendungen erforderlich sind.
Applikations-Backup	21.04	Die Backup-Ressourcen der Applikation stellen Backups der gemanagten Applikationen dar.
Anwendungs-Snapshot	21.04	Die Snapshot-Ressourcen der Anwendung stellen Snapshots der verwalteten Anwendungen dar.
Überschreiben des Testablaufanhängehaken	21.12	Über die Ressourcen zum Überschreiben der Execution Hooks können Sie die vorab geladenen NetApp Standard-Testausführungshaken für bestimmte Applikationen nach Bedarf deaktivieren.
Zeitplan	21.04	Die Zeitplanressourcen sind Datensicherungsvorgänge, die im Rahmen einer Datenschutzrichtlinie für die gemanagten Applikationen geplant sind.

Topologieressourcen

Die Endpunkte der Topologieressourcen bieten Zugriff auf nicht verwaltete Applikationen und Storage-Ressourcen.

Ressource	Freigabe	Beschreibung
App.	21.04	Die App-Ressourcen umfassen alle Kubernetes-Applikationen, auch die, die nicht von Astra gemanagt werden.
AppMirror	**22.08**	Die AppMirror-Ressourcen stellen die AppMirror-Ressourcen dar, die für das Management von Applikationsspiegelungsbeziehungen bereitgestellt werden.
Eimer	21.08	Die Bucket-Ressourcen sind die S3-Cloud-Buckets, die für die Speicherung von Backups der vom Astra gemanagten Applikationen verwendet werden.
Cloud	21.08	Die Cloud-Ressourcen stellen Clouds dar, mit denen Astra-Clients verbunden werden können, um Cluster und Applikationen zu managen.
Cluster	21.08	Die Cluster-Ressourcen stellen die Kubernetes-Cluster dar, die nicht von Kubernetes gemanagt werden.
Cluster-Node	21.12	Die Cluster-Node-Ressourcen bieten eine zusätzliche Auflösung, durch die Sie auf die einzelnen Nodes innerhalb eines Kubernetes-Clusters zugreifen können.
Verwalteter Cluster	21.08	Die gemanagten Cluster-Ressourcen stellen die Kubernetes-Cluster dar, die derzeit von Kubernetes gemanagt werden.
Gemanagtes Storage-Back-End	21.12	Die gemanagten Storage-Backend-Ressourcen ermöglichen Ihnen den Zugriff auf abstrahierte Darstellungen der Back-End-Storage-Anbieter. Diese Storage-Back-Ends können von den gemanagten Clustern und Applikationen verwendet werden.
Namespace	21.12	Die Namespace-Ressourcen bieten Zugriff auf die innerhalb eines Kubernetes-Clusters verwendeten Namespaces.

Ressource	Freigabe	Beschreibung
Storage-Back-End	21.08	Die Storage-Back-End-Ressourcen stellen Anbieter von Storage-Services dar, die von den von Astra gemanagten Clustern und Applikationen verwendet werden können.
Storage-Klasse	21.08	Ressourcen der Storage-Klasse stellen unterschiedliche Storage-Klassen oder -Typen dar, die für ein bestimmtes gemanagtes Cluster erkannt und verfügbar sind.
Datenmenge	21.04	Die Volume-Ressourcen stellen die Kubernetes Storage Volumes dar, die mit den gemanagten Applikationen verknüpft sind.

Zusätzliche Ressourcen und Endpunkte

Zur Unterstützung einer Astra-Implementierung stehen mehrere zusätzliche Ressourcen und Endpunkte zur Verfügung.

Diese Ressourcen und Endpunkte sind derzeit nicht in der Astra Control REST API-Referenzdokumentation enthalten.

OpenAPI

Die OpenAPI-Endpunkte bieten Zugriff auf das aktuelle OpenAPI JSON-Dokument und andere zugehörige Ressourcen.

OpenMetrics

Die OpenMetrics-Endpunkte bieten über die OpenMetrics-Ressource Zugriff auf die Kontokennzahlen. Support ist mit dem Astra Control Center Implementierungsmodell verfügbar.

Weitere Nutzungsüberlegungen

RBAC-Sicherheit

Die Astra REST API unterstützt die rollenbasierte Zugriffssteuerung (RBAC), um den Zugriff auf Systemfunktionen zu gewähren und einzuschränken.

Astra Rollen

Jeder Astra-Benutzer wird einer einzigen Rolle zugewiesen, die die Aktionen bestimmt, die durchgeführt werden können. Die Rollen sind in einer Hierarchie angeordnet, wie in der folgenden Tabelle beschrieben.

Rolle	Beschreibung
Eigentümer	Hat alle Berechtigungen der Admin-Rolle und kann auch Astra-Konten löschen.
Admin	Verfügt über alle Berechtigungen der Mitgliedsrolle und kann Benutzer auch dazu einladen, einem Konto beizutreten.
Mitglied	Kunden können ihre Astra-Applikations- und Computing-Ressourcen vollständig managen.
Prüfer	Beschränkt auf die Anzeige von Ressourcen.

Erweiterte RBAC mit Namespace-Granularität

Diese Funktion wurde mit Version 22.04 des Astra REST API eingeführt.

Wenn eine Rollenbindung für einen bestimmten Benutzer festgelegt wird, kann eine Einschränkung angewendet werden, um die Namespaces zu begrenzen, auf die der Benutzer Zugriff hat. Diese Bedingung kann auf verschiedene Weise definiert werden, wie in der nachstehenden Tabelle beschrieben. Siehe Parameter `roleContraints` In der Role Binding API für weitere Informationen.

Namespaces	Beschreibung
Alle	Der Benutzer kann über den Platzhalterparameter „*“ auf alle Namespaces zugreifen. Dies ist der Standardwert, um die Abwärtskompatibilität beizubehalten.
Keine	Die Bedingungsliste wird angegeben, obwohl sie leer ist. Dies bedeutet, dass der Benutzer keinen Zugriff auf einen Namespace hat.
Namespace-Liste	Die UUID eines Namespace enthält, die den Benutzer auf den Single Namespace beschränkt. Eine kommagetrennte Liste kann auch verwendet werden, um den Zugriff auf mehrere Namespaces zu ermöglichen.
Etikett	Ein Etikett wird angegeben und der Zugriff ist allen übereinstimmenden Namespaces erlaubt.

Arbeit mit Sammlungen

Die Astra Control REST API bietet verschiedene Möglichkeiten, über die definierten Abfrageparameter auf Ressourcensammlungen zuzugreifen.

Wählen Sie Werte aus

Sie können angeben, welche Schlüsselwertpaare für jede Ressourceninstanz mit dem zurückgegeben werden sollen `include` Parameter. Alle Fälle werden im Antwortkörper zurückgegeben.

Filtern

Mithilfe der Filterung von Sammlungsressourcen kann ein API-Benutzer Bedingungen festlegen, die bestimmen, ob eine Ressource im Antwortkörper zurückgegeben wird. Der `filter` Parameter wird verwendet, um die Filterbedingung anzuzeigen.

Sortieren

Die Sammelressource-Sortierung ermöglicht einem API-Benutzer, die Reihenfolge anzugeben, in der Ressourcen im Antwortkörper zurückgegeben werden. Der `orderBy` Parameter wird verwendet, um die Filterbedingung anzuzeigen.

Paginierung

Sie können Paginierung erzwingen, indem Sie die Anzahl der Ressourceninstanzen beschränken, die für eine Anforderung über die zurückgegeben werden `limit` Parameter.

Zählen

Wenn Sie den Booleschen Parameter angeben `count` Auf einstellen `true`, Die Anzahl der Ressourcen im zurückgegebenen Array für eine bestimmte Antwort ist im Abschnitt Metadaten angegeben.

Diagnose und Support

Mit der Astra Control REST API stehen verschiedene Supportfunktionen zur Verfügung, die für Diagnose und Debugging genutzt werden können.

API-Ressourcen

Verschiedene Astra-Funktionen sind über API-Ressourcen zugänglich und bieten diagnostische Informationen und Support.

Typ	Beschreibung
Ereignis	Systemaktivitäten, die im Rahmen der Astra-Verarbeitung erfasst werden.
Benachrichtigung	Eine Untergruppe der Ereignisse, die als wichtig genug betrachtet werden, um dem Benutzer präsentiert zu werden.
Ungelesene Benachrichtigung	Die Benachrichtigungen, die noch vom Benutzer gelesen oder abgerufen werden müssen.

Ein API-Token widerrufen

Sie können ein API-Token an der Astra-Webschnittstelle widerrufen, wenn es nicht mehr benötigt wird.

Bevor Sie beginnen

Sie benötigen ein Astra-Konto. Sie sollten auch die Token identifizieren, die Sie widerrufen möchten.

Über diese Aufgabe

Nachdem ein Token entzogen wurde, ist es sofort und dauerhaft unbrauchbar.

Schritte

1. Melden Sie sich mit Ihren Anmeldedaten im Astra an.

   Rufen Sie die folgende Website für den Astra Control Service auf: "https://astra.netapp.io"

2. Klicken Sie auf das Figurensymbol oben rechts auf der Seite und wählen Sie **API Access**.
3. Wählen Sie das Token oder die Token aus, die Sie widerrufen möchten.
4. Klicken Sie im Dropdown-Feld **Aktionen** auf **Token aufheben**.

Infrastruktur-Workflows

Bevor Sie beginnen

Mithilfe dieser Workflows können Sie die Infrastruktur erstellen und warten, die bei einer Implementierung von Astra Control Center verwendet wird. In vielen Fällen können die Workflows auch mit dem Astra Control Service genutzt werden.

Diese Workflows können jederzeit von NetApp erweitert und ergänzt werden, sodass Sie sie in regelmäßigen Abständen prüfen sollten.

Allgemeine Vorbereitung

Bevor Sie einen Astra-Workflow verwenden, sollten Sie unbedingt lesen "Die Nutzung der Workflows wird vorbereitet".

Workflow-Kategorien

Die Infrastruktur-Workflows sind in verschiedene Kategorien unterteilt, um den gewünschten Workflow leichter finden zu können.

Kategorie	Beschreibung
Identität und Zugriff	Mit diesen Workflows können Sie die Identität und den Zugriff auf Astra verwalten. Zu den Ressourcen zählen Benutzer, Anmeldedaten und Token.
LDAP-Konfiguration	Optional können Sie Astra Control Center so konfigurieren, dass Sie LDAP zur Authentifizierung ausgewählter Benutzer verwenden.
Buckets	Sie können diese Workflows zum Erstellen und Managen der S3-Buckets verwenden, die zum Speichern von Backups verwendet werden.
Storage	Durch diese Workflows können Sie Storage-Back-Ends und -Volumes hinzufügen und verwalten.
Cluster	Sie können Managed Kubernetes Cluster hinzufügen, damit Sie die enthaltenen Applikationen schützen und unterstützen können.

Identität und Zugriff

Benutzer auflisten

Sie können die Benutzer auflisten, die für ein bestimmtes Astra-Konto definiert sind.

1. Listen Sie die Benutzer auf

Führen Sie den folgenden REST-API-Aufruf aus.

HTTP-Methode	Pfad
GET	/Account/{Account_id}/Core/v1/users

Zusätzliche Eingabeparameter

Zusätzlich zu den Parametern, die bei allen REST-API-Aufrufen üblich sind, werden die folgenden Parameter auch in den Curl-Beispielen für diesen Schritt verwendet.

Parameter	Typ	Erforderlich	Beschreibung
Einschließlich	Abfrage	Nein	Wählen Sie optional die Werte aus, die in der Antwort zurückgegeben werden sollen.

Curl-Beispiel: Alle Daten für alle Benutzer zurückgeben

```
curl --location -i --request GET
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/core/v1/users' --header
'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

Curl Beispiel: Gibt den vor-, Nachnamen und die id für alle Benutzer zurück

```
curl --location -i --request GET
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/core/v1/users?include=first
Name,lastName,id' --header 'Accept: */*' --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": {}
}
```

LDAP-Konfiguration

Vorbereiten der LDAP-Konfiguration

Optional können Sie Astra Control Center mit einem LDAP-Server (Lightweight Directory Access Protocol) integrieren, um die Authentifizierung für ausgewählte Astra-Benutzer durchzuführen. LDAP ist ein branchenübliches Protokoll für den Zugriff auf verteilte Verzeichnisinformationen und eine beliebte Wahl für die Unternehmensauthentifizierung.

Verwandte Informationen

- "LDAP - Technische Spezifikation - Road Map"
- "LDAP-Version 3"

Überblick über den Implementierungsprozess

Auf hohem Niveau müssen Sie mehrere Schritte durchführen, um einen LDAP-Server für die Authentifizierung von Astra-Benutzern zu konfigurieren.

> Während sich die unten aufgeführten Schritte nacheinander befinden, können Sie sie in einer anderen Reihenfolge ausführen. Sie können beispielsweise die Astra-Benutzer und -Gruppen festlegen, bevor Sie den LDAP-Server konfigurieren.

1. Prüfen "Anforderungen und Einschränkungen zu erfüllen" Um Optionen, Anforderungen und Einschränkungen zu verstehen.
2. Wählen Sie einen LDAP-Server und die gewünschten Konfigurationsoptionen (einschließlich Sicherheit) aus.
3. Führen Sie den Workflow aus "Konfigurieren Sie Astra für die Verwendung eines LDAP-Servers" Um Astra mit dem LDAP-Server zu integrieren.
4. Überprüfen Sie die Benutzer und Gruppen auf dem LDAP-Server, um sicherzustellen, dass sie ordnungsgemäß definiert sind.
5. Führen Sie den entsprechenden Workflow in aus "Fügen Sie LDAP-Einträge zum Astra hinzu" So identifizieren Sie die Benutzer, die mit LDAP authentifiziert werden sollen.

Anforderungen und Einschränkungen zu erfüllen

Vor der Konfiguration von Astra zur Verwendung von LDAP zur Authentifizierung sollten Sie sich die unten aufgeführten Konfigurationsmöglichkeiten, einschließlich Einschränkungen und Konfigurationsoptionen, ansehen.

Nur unterstützt durch Astra Control Center

Die Astra Control-Plattform verfügt über zwei Implementierungsmodelle. Die LDAP-Authentifizierung wird nur bei Astra Control Center-Implementierungen unterstützt.

Nur DIE REST-API-Konfiguration

Die aktuelle Version von Astra Control Center unterstützt nur die Konfiguration der LDAP-Authentifizierung mithilfe der Astra Control REST API. Ein wichtiger Aspekt dieser Einschränkung ist, dass die LDAP-Benutzer nicht auf der Registerkarte Benutzer des Astra Web-Interface angezeigt werden. Sie sind über DIE REST-API am Endpunkt verfügbar `../core/v1/users`.

LDAP-Server erforderlich

Sie müssen über einen LDAP-Server verfügen, um die Astra-Authentifizierungsanforderungen zu akzeptieren und zu bearbeiten. Das Active Directory von Microsoft wird mit der aktuellen Version von Astra Control Center unterstützt.

Sichere Verbindung zum LDAP-Server

Bei der Konfiguration des LDAP-Servers in Astra können Sie optional eine sichere Verbindung festlegen. In diesem Fall wird ein Zertifikat für das LDAPS-Protokoll benötigt.

Konfigurieren von Benutzern oder Gruppen

Sie müssen die Benutzer auswählen, die mit LDAP authentifiziert werden sollen. Dazu können Sie entweder die einzelnen Benutzer oder eine Gruppe von Benutzern identifizieren. Die Konten müssen auf dem LDAP-Server definiert werden. Sie müssen auch im Astra (Typ LDAP) identifiziert werden, wodurch die Authentifizierungsanforderungen an LDAP weitergeleitet werden können.

Rollenbedingung beim Binden eines Benutzers oder einer Gruppe

Mit der aktuellen Version von Astra Control Center ist der einzige unterstützte Wert für `roleConstraint` Ist „*“. Dies bedeutet, dass der Benutzer nicht auf eine begrenzte Anzahl von Namespaces beschränkt ist und auf alle zugreifen kann. Siehe "Fügen Sie LDAP-Einträge zum Astra hinzu" Finden Sie weitere Informationen.

LDAP-Anmeldedaten

Zu den von LDAP verwendeten Anmeldeinformationen gehören der Benutzername (E-Mail-Adresse) und das zugehörige Passwort.

Eindeutige E-Mail-Adressen

Alle E-Mail-Adressen, die in einer Astra Control Center-Implementierung als Benutzernamen fungieren, müssen eindeutig sein. Sie können keinen LDAP-Benutzer mit einer E-Mail-Adresse hinzufügen, die bereits in Astra definiert ist. Wenn eine doppelte E-Mail vorhanden ist, müssen Sie sie zuerst aus Astra löschen. Siehe "Benutzer entfernen" Auf der Astra Control Center Dokumentationswebsite finden Sie weitere Informationen.

Definieren Sie optional zuerst LDAP-Benutzer und -Gruppen

Sie können die LDAP-Benutzer und -Gruppen zum Astra Control Center hinzufügen, auch wenn sie noch nicht in LDAP vorhanden sind oder der LDAP-Server nicht konfiguriert ist. Auf diese Weise können Sie vor der Konfiguration des LDAP-Servers Benutzer und Gruppen konfigurieren.

Ein in mehreren LDAP-Gruppen definierter Benutzer

Wenn ein LDAP-Benutzer zu mehreren LDAP-Gruppen gehört und den Gruppen verschiedene Rollen in Astra zugewiesen wurden, ist die effektive Rolle des Benutzers bei der Authentifizierung die bevorzugte. Wenn einem Benutzer beispielsweise das zugewiesen ist `viewer` Rolle mit Gruppe1, aber hat die `member` Rolle in Groupp2, die Rolle des Benutzers wäre `member`. Dies basiert auf der Hierarchie des Astra (höchste bis niedrigste):

- Eigentümer
- Admin
- Mitglied
- Prüfer

Regelmäßige Kontosynchronisation

Astra synchronisiert seine Benutzer und Gruppen etwa alle 60 Sekunden mit dem LDAP-Server. Wenn also ein Benutzer oder eine Gruppe zu LDAP hinzugefügt oder aus dieser entfernt wird, kann es bis zu einer Minute dauern, bis er in Astra verfügbar ist.

Deaktivieren und Zurücksetzen der LDAP-Konfiguration

Bevor Sie versuchen, die LDAP-Konfiguration zurückzusetzen, müssen Sie zunächst die LDAP-Authentifizierung deaktivieren. Außerdem zum Ändern des LDAP-Servers (`connectionHost`), Sie müssen beide Operationen ausführen. Siehe "Deaktivieren und Zurücksetzen von LDAP" Finden Sie weitere Informationen.

REST-API-Parameter

Die LDAP-Konfigurations-Workflows führen REST-API-Aufrufe zur Ausführung der spezifischen Aufgaben durch. Jeder API-Aufruf kann Eingabeparameter enthalten, wie in den angegebenen Beispielen dargestellt. Siehe "API-Referenz" Weitere Informationen zum Auffinden der Referenzdokumentation.

Konfigurieren Sie Astra für die Verwendung eines LDAP-Servers

Sie müssen einen LDAP-Server auswählen und Astra so konfigurieren, dass der Server als Authentifizierungsanbieter verwendet wird. Die Konfigurationsaufgabe besteht aus den unten beschriebenen Schritten. Jeder Schritt umfasst einen einzelnen REST-API-Aufruf.

1. Fügen Sie ein CA-Zertifikat hinzu

Führen Sie den folgenden REST-API-Aufruf durch, um ein CA-Zertifikat zu Astra hinzuzufügen.

> Dieser Schritt ist optional und nur erforderlich, wenn Astra und LDAP über einen sicheren Kanal über LDAPS kommunizieren möchten.

HTTP-Methode	Pfad
POST	/Account/{Account_id}/Core/v1/certificates

JSON-Eingabebeispiel

```
{
  "type": "application/astra-certificate",
  "version": "1.0",
  "certUse": "rootCA",
  "cert": "LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUMyVEN",
  "isSelfSigned": "true"
}
```

Beachten Sie folgende Informationen zu den Eingabeparametern:

- `cert` Ist ein JSON-String mit einem base64-kodierten PKCS-11-Zertifikat (PEM-codiert).
- `isSelfSigned` Sollte auf eingestellt sein `true` Wenn das Zertifikat selbst signiert ist. Die Standardeinstellung lautet `false`.

Beispiel für die Wellung

```
curl --location -i --request POST --data @JSONinput
'https://astra.example.com/accounts/<ACCOUNT_ID>/core/v1/certificates'
--header 'Content-Type: application/astra-certificate+json' --header
'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

Beispiel für JSON-Antwort

```
{
  "type": "application/astra-certificate",
  "version": "1.0",
  "id": "a5212e7e-402b-4cff-bba0-63f3c6505199",
  "certUse": "rootCA",
  "cert": "LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUMyVEN",
  "cn": "adldap.example.com",
  "expiryTimestamp": "2023-07-08T20:22:07Z",
  "isSelfSigned": "true",
  "trustState": "trusted",
  "trustStateTransitions": [
  {
    "from": "untrusted",
    "to": [
      "trusted",
      "expired"
    ]
  },
  {
    "from": "trusted",
    "to": [
      "untrusted",
      "expired"
    ]
  },
  {
    "from": "expired",
    "to": [
     "untrusted",
     "trusted"
    ]
  }
  ],
  "trustStateDesired": "trusted",
  "trustStateDetails": [],
  "metadata": {
    "creationTimestamp": "2022-07-21T04:16:06Z",
    "modificationTimestamp": "2022-07-21T04:16:06Z",
    "createdBy": "8a02d2b8-a69d-4064-827f-36851b3e1e6e",
    "modifiedBy": "8a02d2b8-a69d-4064-827f-36851b3e1e6e",
    "labels": []
    }
}
```

2. Fügen Sie die Bindungsanmeldeinformationen hinzu

Führen Sie den folgenden REST-API-Aufruf durch, um die Bindungsanmeldeinformationen hinzuzufügen.

HTTP-Methode	Pfad
POST	/Account/{Account_id}/Core/v1/Credentials

JSON-Eingabebeispiel

```
{
  "name": "ldapBindCredential",
  "type": "application/astra-credential",
  "version": "1.1",
  "keyStore": {
    "bindDn": "dWlkPWFkbWluLG91PXN5c3RlbQ==",
    "password": "cGFzc3dvcmQ="
  }
}
```

Beachten Sie folgende Informationen zu den Eingabeparametern:

- `bindDn` Und `password` Sind die base64-kodierten Bindungsanmeldeinformationen des LDAP-Admin-Benutzers, der eine Verbindung herstellen und das LDAP-Verzeichnis durchsuchen kann. `bindDn` Ist die E-Mail-Adresse des LDAP-Benutzers.

Beispiel für die Wellung

```
curl --location -i --request POST --data @JSONinput
'https://astra.example.com/accounts/<ACCOUNT_ID>/core/v1/credentials'
--header 'Content-Type: application/astra-credential+json' --header
'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

Beispiel für JSON-Antwort

```
{
    "type": "application/astra-credential",
    "version": "1.1",
    "id": "3bd9c8a7-f5a4-4c44-b778-90a85fc7d154",
    "name": "ldapBindCredential",
    "metadata": {
        "creationTimestamp": "2022-07-21T06:53:11Z",
        "modificationTimestamp": "2022-07-21T06:53:11Z",
        "createdBy": "527329f2-662c-41c0-ada9-2f428f14c137"
    }
}
```


Beachten Sie die folgenden Antwortparameter:

- Der `id` Der Anmeldedaten werden in nachfolgenden Workflow-Schritten verwendet.

3. Abrufen der UUID der LDAP-Einstellung

Führen Sie den folgenden REST-API-Aufruf aus, um die UUID von abzurufen `astra.account.ldap` Die Einstellung ist im Astra Control Center enthalten.

> Das folgende Curl-Beispiel verwendet einen Abfrageparameter, um die Einstellensammlung zu filtern. Sie können stattdessen den Filter entfernen, um alle Einstellungen zu erhalten und dann nach zu suchen `astra.account.ldap`.

HTTP-Methode	Pfad
GET	/Account/{Account_id}/Core/v1/settings

Beispiel für die Wellung

```
curl --location -i --request GET
'https://astra.example.com/accounts/<ACCOUNT_ID>/core/v1/settings?filter=n
ame%20eq%20'astra.account.ldap'&include=name,id' --header 'Accept: */*'
--header 'Authorization: Bearer <API_TOKEN>'
```

Beispiel für JSON-Antwort

```
{
  "items": [
    ["astra.account.ldap",
    "12072b56-e939-45ec-974d-2dd83b7815df"
    ]
  ],
  "metadata": {}
}
```

4. Aktualisieren Sie die LDAP-Einstellung

Führen Sie den folgenden REST-API-Aufruf durch, um die LDAP-Einstellung zu aktualisieren und die Konfiguration abzuschließen. Verwenden Sie die `id` Wert aus dem vorherigen API-Aufruf für das `<SETTING_ID>` Wert im URL-Pfad unten.

Sie können zuerst eine ANFRAGE FÜR DIE spezifische Einstellung ausstellen, um das configSchema zu sehen. Hier erhalten Sie weitere Informationen zu den erforderlichen Feldern in der Konfiguration.

HTTP-Methode	Pfad
PUT	/Account/{Account_id}/Core/v1/settings/{setting_id}

JSON-Eingabebeispiel

```
{
  "type": "application/astra-setting",
  "version": "1.0",
  "desiredConfig": {
    "connectionHost": "myldap.example.com",
    "credentialId": "3bd9c8a7-f5a4-4c44-b778-90a85fc7d154",
    "groupBaseDN": "OU=groups,OU=astra,DC=example,DC=com",
    "isEnabled": "true",
    "port": 686,
    "secureMode": "LDAPS",
    "userBaseDN": "OU=users,OU=astra,DC=example,dc=com",
    "userSearchFilter": "((objectClass=User))",
    "vendor": "Active Directory"
    }
}
```

Beachten Sie folgende Informationen zu den Eingabeparametern:

- `isEnabled` Sollte auf eingestellt sein `true` Oder es kann ein Fehler auftreten.

- `credentialId` Ist die id der zuvor erstellten Bindungsanmeldeinformationen.
- `secureMode` Sollte auf eingestellt sein `LDAP` Oder `LDAPS` Basierend auf Ihrer Konfiguration im vorherigen Schritt.
- Als Anbieter wird nur „Active Directory“ unterstützt.

Beispiel für die Wellung

```
curl --location -i --request PUT --data @JSONinput
'https://astra.example.com/accounts/<ACCOUNT_ID>/core/v1/settings/<SETTING
_ID>' --header 'Content-Type: application/astra-setting+json' --header
'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

Wenn der Anruf erfolgreich ist, wird die HTTP 204-Antwort zurückgegeben.

5. Abrufen der LDAP-Einstellung

Sie können optional den folgenden REST-API-Aufruf durchführen, um die LDAP-Einstellungen abzurufen und die Aktualisierung zu bestätigen.

HTTP-Methode	Pfad
GET	/Account/{Account_id}/Core/v1/settings/{setting_id}

Beispiel für die Wellung

```
curl --location -i --request GET
'https://astra.example.com/accounts/<ACCOUNT_ID>/core/v1/settings/<SETTING
_ID>' --header 'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

Beispiel für JSON-Antwort


```
{
  "items": [
  {
    "type": "application/astra-setting",
    "version": "1.0",
    "metadata": {
      "creationTimestamp": "2022-06-17T21:16:31Z",
      "modificationTimestamp": "2022-07-21T07:12:20Z",
      "labels": [],
      "createdBy": "system",
      "modifiedBy": "00000000-0000-0000-0000-000000000000"
    },
    "id": "12072b56-e939-45ec-974d-2dd83b7815df",
```

```
    "name": "astra.account.ldap",
    "desiredConfig": {
      "connectionHost": "10.193.61.88",
      "credentialId": "3bd9c8a7-f5a4-4c44-b778-90a85fc7d154",
      "groupBaseDN": "ou=groups,ou=astra,dc=example,dc=com",
      "isEnabled": "true",
      "port": 686,
      "secureMode": "LDAPS",
      "userBaseDN": "ou=users,ou=astra,dc=example,dc=com",
      "userSearchFilter": "((objectClass=User))",
      "vendor": "Active Directory"
    },
    "currentConfig": {
      "connectionHost": "10.193.160.209",
      "credentialId": "3bd9c8a7-f5a4-4c44-b778-90a85fc7d154",
      "groupBaseDN": "ou=groups,ou=astra,dc=example,dc=com",
      "isEnabled": "true",
      "port": 686,
      "secureMode": "LDAPS",
      "userBaseDN": "ou=users,ou=astra,dc=example,dc=com",
      "userSearchFilter": "((objectClass=User))",
      "vendor": "Active Directory"
    },
    "configSchema": {
      "$schema": "http://json-schema.org/draft-07/schema#",
      "title": "astra.account.ldap",
      "type": "object",
      "properties": {
        "connectionHost": {
          "type": "string",
          "description": "The hostname or IP address of your LDAP server."
        },
        "credentialId": {
          "type": "string",
          "description": "The credential ID for LDAP account."
        },
        "groupBaseDN": {
          "type": "string",
          "description": "The base DN of the tree used to start the group
search. The system searches the subtree from the specified location."
        },
        "groupSearchCustomFilter": {
          "type": "string",
          "description": "Type of search that controls the default group
search filter used."
        },
```

```
        "isEnabled": {
          "type": "string",
          "description": "This property determines if this setting is
enabled or not."
        },
        "port": {
          "type": "integer",
          "description": "The port on which the LDAP server is running."
        },
        "secureMode": {
          "type": "string",
          "description": "The secure mode LDAPS or LDAP."
        },
        "userBaseDN": {
          "type": "string",
          "description": "The base DN of the tree used to start the user
search. The system searches the subtree from the specified location."
        },
        "userSearchFilter": {
          "type": "string",
          "description": "The filter used to search for users according a
search criteria."
        },
        "vendor": {
          "type": "string",
          "description": "The LDAP provider you are using.",
          "enum": ["Active Directory"]
        }
      },
      "additionalProperties": false,
      "required": [
        "connectionHost",
        "secureMode",
        "credentialId",
        "userBaseDN",
        "userSearchFilter",
        "groupBaseDN",
        "vendor",
        "isEnabled"
      ]
      },
      "state": "valid",
    }
  ],
  "metadata": {}
}
```

Suchen Sie das `state` Feld in der Antwort, die einen der Werte in der unten stehenden Tabelle enthält.

Bundesland	Beschreibung
Ausstehend	Die Konfiguration ist noch aktiv und noch nicht abgeschlossen.
Gültig	Die Konfiguration wurde erfolgreich abgeschlossen und `currentConfig` In der Antwort Matches `desiredConfig`.
Fehler	Die LDAP-Konfiguration ist fehlgeschlagen.

Fügen Sie LDAP-Einträge zum Astra hinzu

Nachdem LDAP als Authentifizierungsanbieter für Astra Control Center konfiguriert wurde, können Sie die LDAP-Benutzer auswählen, die Astra mit den LDAP-Anmeldedaten authentifizieren soll. Jeder Benutzer muss eine Rolle im Astra haben, bevor er über die Astra Control REST API auf den Astra zugreifen kann.

Es gibt zwei Möglichkeiten, Astra für die Zuweisung von Rollen zu konfigurieren. Wählen Sie den für Ihre Umgebung geeigneten aus.

- "Hinzufügen und Binden eines einzelnen Benutzers"
- "Fügen Sie eine Gruppe hinzu und binden Sie sie"

Die LDAP-Anmeldedaten bestehen in Form eines Benutzernamens als E-Mail-Adresse und des zugehörigen LDAP-Passworts.

Hinzufügen und Binden eines einzelnen Benutzers

Sie können jedem Astra-Benutzer eine Rolle zuweisen, die nach der LDAP-Authentifizierung verwendet wird. Dies ist angemessen, wenn es eine kleine Anzahl von Benutzern gibt und jeder über unterschiedliche administrative Merkmale verfügt.

1. Fügen Sie einen Benutzer hinzu

Führen Sie den folgenden REST-API-Aufruf durch, um einen Benutzer zu Astra hinzuzufügen und anzugeben, dass LDAP der Authentifizierungsanbieter ist.

HTTP-Methode	Pfad
POST	/Account/{Account_id}/Core/v1/users

JSON-Eingabebeispiel

```
{
  "type" :  "application/astra-user",
  "version" : "1.1",
  "authID" : "cn=JohnDoe,ou=users,ou=astra,dc=example,dc=com",
  "authProvider" : "ldap",
  "firstName" : "John",
  "lastName" : "Doe",
  "email" : "john.doe@example.com"
}
```

Beachten Sie folgende Informationen zu den Eingabeparametern:

- Die folgenden Parameter sind erforderlich:
  - `authProvider`
  - `authID`
  - `email`
- `authID` Ist der Distinguished Name (DN) des Benutzers in LDAP
- `email` Muss für alle in Astra definierten Benutzer eindeutig sein

Wenn der `email` Der Wert ist nicht eindeutig, es tritt ein Fehler auf und ein HTTP-Statuscode 409 wird in der Antwort zurückgegeben.

Beispiel für die Wellung

```
curl --location -i --request POST --data @JSONinput
'https://astra.example.com/accounts/<ACCOUNT_ID>/core/v1/users' --header
'Content-Type: application/astra-user+json' --header 'Accept: */*'
--header 'Authorization: Bearer <API_TOKEN>'
```

Beispiel für JSON-Antwort

```
{
  "metadata": {
    "creationTimestamp": "2022-07-21T17:44:18Z",
    "modificationTimestamp": "2022-07-21T17:44:18Z",
    "createdBy": "8a02d2b8-a69d-4064-827f-36851b3e1e6e",
    "labels": []
  },
  "type": "application/astra-user",
  "version": "1.2",
  "id": "a7b5e674-a1b1-48f6-9729-6a571426d49f",
  "authProvider": "ldap",
  "authID": "cn=JohnDoe,ou=users,ou=astra,dc=example,dc=com",
  "firstName": "John",
  "lastName": "Doe",
  "companyName": "",
  "email": "john.doe@example.com",
  "postalAddress": {
    "addressCountry": "",
    "addressLocality": "",
    "addressRegion": "",
    "streetAddress1": "",
    "streetAddress2": "",
    "postalCode": ""
  },
  "state": "active",
  "sendWelcomeEmail": "false",
  "isEnabled": "true",
  "isInviteAccepted": "true",
  "enableTimestamp": "2022-07-21T17:44:18Z",
  "lastActTimestamp": ""
}
```


2. Fügen Sie eine Rollenbindung für den Benutzer hinzu

Führen Sie den folgenden REST-API-Aufruf durch, um den Benutzer an eine bestimmte Rolle zu binden. Sie müssen die UUID des Benutzers im vorherigen Schritt erstellen lassen.

HTTP-Methode	Pfad
POST	/Account/{Account_id}/Core/v1/roleBindungen

JSON-Eingabebeispiel

```
{
  "type": "application/astra-roleBinding",
  "version": "1.1",
  "accountID": "{account_id}",
  "userID": "a7b5e674-a1b1-48f6-9729-6a571426d49f",
  "role": "member",
  "roleConstraints": ["*"]
}
```

Beachten Sie folgende Informationen zu den Eingabeparametern:

- Der oben verwendete Wert für `roleConstraint` Ist die einzige Option, die für die aktuelle Version von Astra verfügbar ist. Er zeigt an, dass der Benutzer nicht auf eine begrenzte Anzahl von Namespaces beschränkt ist und alle darauf zugreifen können.

Beispiel für die Wellung

```
curl --location -i --request POST --data @JSONinput
'https://astra.example.com/accounts/<ACCOUNT_ID>/core/v1/roleBindings'
--header 'Content-Type: application/astra-roleBinding+json' --header
'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

Beispiel für JSON-Antwort

```
{
  "metadata": {
    "creationTimestamp": "2022-07-21T18:08:24Z",
    "modificationTimestamp": "2022-07-21T18:08:24Z",
    "createdBy": "8a02d2b8-a69d-4064-827f-36851b3e1e6e",
    "labels": []
  },
  "type": "application/astra-roleBinding",
  "principalType": "user",
  "version": "1.1",
  "id": "b02c7e4d-d483-40d1-aaff-e1f900312114",
  "userID": "a7b5e674-a1b1-48f6-9729-6a571426d49f",
  "groupID": "00000000-0000-0000-0000-000000000000",
  "accountID": "d0fdbfa7-be32-4a71-b59d-13d95b42329a",
  "role": "member",
  "roleConstraints": ["*"]
}
```

Beachten Sie folgende Hinweise zu den Antwortparametern:

- Der Wert `user` Für das `principalType` Feld gibt an, dass die Rollenbindung für einen Benutzer hinzugefügt wurde (keine Gruppe).

Fügen Sie eine Gruppe hinzu und binden Sie sie

Sie können einer Astra-Gruppe eine Rolle zuweisen, die nach der LDAP-Authentifizierung verwendet wird. Dies ist angemessen, wenn es eine große Anzahl von Benutzern gibt und jeder über ähnliche administrative Merkmale verfügt.

1. Fügen Sie eine Gruppe hinzu

Führen Sie den folgenden REST-API-Aufruf durch, um eine Gruppe zu Astra hinzuzufügen und anzugeben, dass LDAP der Authentifizierungsanbieter ist.

HTTP-Methode	Pfad
POST	/Account/{Account_id}/Core/v1/groups

JSON-Eingabebeispiel

```
{
  "type": "application/astra-group",
  "version": "1.0",
  "name": "Engineering",
  "authProvider": "ldap",
  "authID": "CN=Engineering,OU=groups,OU=astra,DC=example,DC=com"
}
```

Beachten Sie folgende Informationen zu den Eingabeparametern:

- Die folgenden Parameter sind erforderlich:
  - `authProvider`
  - `authID`

Beispiel für die Wellung

```
curl --location -i --request POST --data @JSONinput
'https://astra.example.com/accounts/<ACCOUNT_ID>/core/v1/groups' --header
'Content-Type: application/astra-group+json' --header 'Accept: */*'
--header 'Authorization: Bearer <API_TOKEN>'
```

Beispiel für JSON-Antwort

```
{
  "type": "application/astra-group",
  "version": "1.0",
  "id": "8b5b54da-ae53-497a-963d-1fc89990525b",
  "name": "Engineering",
  "authProvider": "ldap",
  "authID": "CN=Engineering,OU=groups,OU=astra,DC=example,DC=com",
  "metadata": {
    "creationTimestamp": "2022-07-21T18:42:52Z",
    "modificationTimestamp": "2022-07-21T18:42:52Z",
    "createdBy": "8a02d2b8-a69d-4064-827f-36851b3e1e6e",
    "labels": []
  }
}
```

2. Fügen Sie eine Rollenbindung für die Gruppe hinzu

Führen Sie den folgenden REST-API-Aufruf durch, um die Gruppe an eine bestimmte Rolle zu binden. Sie müssen die UUID der Gruppe im vorherigen Schritt erstellen lassen. Benutzer, die Mitglieder der Gruppe sind, können sich bei Astra anmelden, nachdem LDAP die Authentifizierung durchgeführt hat.

HTTP-Methode	Pfad
POST	/Account/{Account_id}/Core/v1/roleBindungen

JSON-Eingabebeispiel

```
{
  "type": "application/astra-roleBinding",
  "version": "1.1",
  "accountID": "{account_id}",
  "groupID": "8b5b54da-ae53-497a-963d-1fc89990525b",
  "role": "viewer",
  "roleConstraints": ["*"]
}
```

Beachten Sie folgende Informationen zu den Eingabeparametern:

- Der oben verwendete Wert für `roleConstraint` Ist die einzige Option, die für die aktuelle Version von Astra verfügbar ist. Er gibt an, dass der Benutzer nicht auf bestimmte Namespaces beschränkt ist und alle darauf zugreifen können.

Beispiel für die Wellung

```
curl --location -i --request POST --data @JSONinput
'https://astra.example.com/accounts/<ACCOUNT_ID>/core/v1/roleBindings'
--header 'Content-Type: application/astra-roleBinding+json' --header
'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

Beispiel für JSON-Antwort

```
{
  "metadata": {
    "creationTimestamp": "2022-07-21T18:59:43Z",
    "modificationTimestamp": "2022-07-21T18:59:43Z",
    "createdBy": "527329f2-662c-41c0-ada9-2f428f14c137",
    "labels": []
  },
  "type": "application/astra-roleBinding",
  "principalType": "group",
  "version": "1.1",
  "id": "2f91b06d-315e-41d8-ae18-7df7c08fbb77",
  "userID": "00000000-0000-0000-0000-000000000000",
  "groupID": "8b5b54da-ae53-497a-963d-1fc89990525b",
  "accountID": "d0fdbfa7-be32-4a71-b59d-13d95b42329a",
  "role": "viewer",
  "roleConstraints": ["*"]
}
```

Beachten Sie folgende Hinweise zu den Antwortparametern:

- Der Wert `group` Für das `principalType` Feld gibt an, dass die Rollenbindung für eine Gruppe hinzugefügt wurde (kein Benutzer).

Deaktivieren und Zurücksetzen von LDAP

Für eine Astra Control Center-Implementierung können Sie zwei optionale administrative Aufgaben durchführen. Sie können die LDAP-Authentifizierung global deaktivieren und die LDAP-Konfiguration zurücksetzen.

Beide Workflow-Aufgaben erfordern die id für den `astra.account.ldap` Astra-Einstellung: Details zum Abrufen der Einstellungen-id finden Sie in **Konfigurieren des LDAP-Servers**. Siehe "Abrufen der UUID der LDAP-Einstellung" Finden Sie weitere Informationen.

- "Deaktivieren Sie die LDAP-Authentifizierung"
- "LDAP-Authentifizierungskonfiguration zurücksetzen"

Deaktivieren Sie die LDAP-Authentifizierung

Sie können den folgenden REST-API-Aufruf durchführen, um die LDAP-Authentifizierung für eine bestimmte Astra-Implementierung global zu deaktivieren. Der Anruf aktualisiert den `astra.account.ldap` Einstellung und das `isEnabled` Wert ist gesetzt auf `false`.

HTTP-Methode	Pfad
PUT	/Account/{Account_id}/Core/v1/settings/{setting_id}

JSON-Eingabebeispiel

```
{
  "type": "application/astra-setting",
  "version": "1.0",
  "desiredConfig": {
    "connectionHost": "myldap.example.com",
    "credentialId": "3bd9c8a7-f5a4-4c44-b778-90a85fc7d154",
    "groupBaseDN": "OU=groups,OU=astra,DC=example,DC=com",
    "isEnabled": "false",
    "port": 686,
    "secureMode": "LDAPS",
    "userBaseDN": "OU=users,OU=astra,DC=example,dc=com",
    "userSearchFilter": "((objectClass=User))",
    "vendor": "Active Directory"
    }
}
```

```
curl --location -i --request PUT --data @JSONinput
'https://astra.example.com/accounts/<ACCOUNT_ID>/core/v1/settings/<SETTING
_ID>' --header 'Content-Type: application/astra-setting+json' --header
'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

Wenn der Anruf erfolgreich ist, wird der angezeigt `HTTP 204` Die Antwort wird zurückgegeben. Sie können optional die Konfigurationseinstellungen erneut abrufen, um die Änderung zu bestätigen.

LDAP-Authentifizierungskonfiguration zurücksetzen

Sie können den folgenden REST-API-Aufruf ausführen, um Astra vom LDAP-Server zu trennen und die LDAP-Konfiguration in Astra zurückzusetzen. Der Anruf aktualisiert den `astra.account.ldap` Einstellung und der Wert von `connectionHost` Wird gelöscht.

Der Wert von `isEnabled` Muss auch auf festgelegt sein `false`. Sie können diesen Wert entweder vor dem Rücksetzen oder als Teil des Rückrufs festlegen. Im zweiten Fall `connectionHost` Sollte gelöscht werden und `isEnabled` Bei demselben Reset-Anruf auf false gesetzt.

Dies ist ein disruptiver Betrieb, und Sie sollten mit Vorsicht vorgehen. Alle importierten LDAP-Benutzer und -Gruppen werden gelöscht. Außerdem werden alle zugehörigen Astra-Benutzer, Gruppen und RoleBindings (LDAP-Typ) gelöscht, die Sie im Astra Control Center erstellt haben.

HTTP-Methode	Pfad
PUT	/Account/{Account_id}/Core/v1/settings/{setting_id}

JSON-Eingabebeispiel

```
{
  "type": "application/astra-setting",
  "version": "1.0",
  "desiredConfig": {
    "connectionHost": "",
    "credentialId": "3bd9c8a7-f5a4-4c44-b778-90a85fc7d154",
    "groupBaseDN": "OU=groups,OU=astra,DC=example,DC=com",
    "isEnabled": "false",
    "port": 686,
    "secureMode": "LDAPS",
    "userBaseDN": "OU=users,OU=astra,DC=example,dc=com",
    "userSearchFilter": "((objectClass=User))",
    "vendor": "Active Directory"
    }
}
```

Beachten Sie Folgendes:

- Um den LDAP-Server zu ändern, müssen Sie die LDAP-Änderung deaktivieren und zurücksetzen `connectHost` Bis zu einem Null-Wert, wie im Beispiel oben gezeigt.

```
curl --location -i --request PUT --data @JSONinput
'https://astra.example.com/accounts/<ACCOUNT_ID>/core/v1/settings/<SETTING
_ID>' --header 'Content-Type: application/astra-setting+json' --header
'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

Wenn der Anruf erfolgreich ist, wird der angezeigt `HTTP 204` Die Antwort wird zurückgegeben. Sie können optional die Konfiguration erneut abrufen, um die Änderung zu bestätigen.

Cluster

Listen Sie die Cluster auf

Sie können die verfügbaren Cluster in einer bestimmten Cloud auflisten.

1. Wählen Sie die Cloud

Führen Sie den Workflow aus "Clouds auflisten" Wählen Sie dann die Cloud mit den Clustern aus.

2. Listen Sie die Cluster auf

Führen Sie den folgenden REST-API-Aufruf durch, um die Cluster in einer bestimmten Cloud aufzulisten.

HTTP-Methode	Pfad
GET	/Account/{Account_id}/Topology/v1/Clouds/{Cloud_id}/Cluster

Curl-Beispiel: Gibt alle Daten für alle Cluster zurück

```
curl --location -i --request GET
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/topology/v1/clouds/<CLOUD_I
D>/clusters' --header 'Accept: */*' --header 'Authorization: Bearer
<API_TOKEN>'
```

Beispiel für eine JSON-Ausgabe


```
{
    "items": [
        {
            "type": "application/astra-cluster",
            "version": "1.1",
            "id": "7ce83fba-6aa1-4e0c-a194-26e714f5eb46",
            "name": "openshift-clstr-ol-07",
            "state": "running",
            "stateUnready": [],
            "managedState": "managed",
            "protectionState": "full",
            "protectionStateDetails": [],
            "restoreTargetSupported": "true",
            "snapshotSupported": "true",
            "managedStateUnready": [],
            "managedTimestamp": "2022-11-03T15:50:59Z",
            "inUse": "true",
            "clusterType": "openshift",
            "accHost": "true",
            "clusterVersion": "1.23",
            "clusterVersionString": "v1.23.12+6b34f32",
            "namespaces": [
                "default",
                "kube-node-lease",
                "kube-public",
```

```
                "kube-system",
                "metallb-system",
                "mysql",
                "mysql-clone1",
                "mysql-clone2",
                "mysql-clone3",
                "mysql-clone4",
                "netapp-acc-operator",
                "netapp-monitoring",
                "openshift",
                "openshift-apiserver",
                "openshift-apiserver-operator",
                "openshift-authentication",
                "openshift-authentication-operator",
                "openshift-cloud-controller-manager",
                "openshift-cloud-controller-manager-operator",
                "openshift-cloud-credential-operator",
                "openshift-cloud-network-config-controller",
                "openshift-cluster-csi-drivers",
                "openshift-cluster-machine-approver",
                "openshift-cluster-node-tuning-operator",
                "openshift-cluster-samples-operator",
                "openshift-cluster-storage-operator",
                "openshift-cluster-version",
                "openshift-config",
                "openshift-config-managed",
                "openshift-config-operator",
                "openshift-console",
                "openshift-console-operator",
                "openshift-console-user-settings",
                "openshift-controller-manager",
                "openshift-controller-manager-operator",
                "openshift-dns",
                "openshift-dns-operator",
                "openshift-etcd",
                "openshift-etcd-operator",
                "openshift-host-network",
                "openshift-image-registry",
                "openshift-infra",
                "openshift-ingress",
                "openshift-ingress-canary",
                "openshift-ingress-operator",
                "openshift-insights",
                "openshift-kni-infra",
                "openshift-kube-apiserver",
                "openshift-kube-apiserver-operator",
```

```
                "openshift-kube-controller-manager",
                "openshift-kube-controller-manager-operator",
                "openshift-kube-scheduler",
                "openshift-kube-scheduler-operator",
                "openshift-kube-storage-version-migrator",
                "openshift-kube-storage-version-migrator-operator",
                "openshift-machine-api",
                "openshift-machine-config-operator",
                "openshift-marketplace",
                "openshift-monitoring",
                "openshift-multus",
                "openshift-network-diagnostics",
                "openshift-network-operator",
                "openshift-node",
                "openshift-oauth-apiserver",
                "openshift-openstack-infra",
                "openshift-operator-lifecycle-manager",
                "openshift-operators",
                "openshift-ovirt-infra",
                "openshift-sdn",
                "openshift-service-ca",
                "openshift-service-ca-operator",
                "openshift-user-workload-monitoring",
                "openshift-vsphere-infra",
                "pcloud",
                "postgreql",
                "trident"
            ],
            "defaultStorageClass": "4bacbb3c-0727-4f58-b13c-3a2a069baf89",
            "cloudID": "4f1e1086-f415-4451-a051-c7299cd672ff",
            "credentialID": "7ffd7354-b6c2-4efa-8e7b-cf64d5598463",
            "isMultizonal": "false",
            "tridentManagedStateAllowed": [
                "unmanaged"
            ],
            "tridentVersion": "22.10.0",
            "apiServiceID": "98df44dc-2baf-40d5-8826-e198b1b40909",
            "metadata": {
                "labels": [
                    {
                        "name": "astra.netapp.io/labels/read-
only/cloudName",
                        "value": "private"
                    }
                ],
                "creationTimestamp": "2022-11-03T15:50:59Z",
```

```
                "modificationTimestamp": "2022-11-04T14:42:32Z",
                "createdBy": "00000000-0000-0000-0000-000000000000"
            }
        }
    ]
}
```


Auflistung gemanagter Cluster

Sie können die Kubernetes-Cluster auflisten, die derzeit vom Astra gemanagt werden.

1. Listen Sie die verwalteten Cluster auf

Führen Sie den folgenden REST-API-Aufruf aus.

HTTP-Methode	Pfad
GET	/Account/{Account_id}/Topology/v1/manageClusters

Curl-Beispiel: Gibt alle Daten für alle Cluster zurück

```
curl --location -i --request GET
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/topology/v1/managedClusters
' --header 'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

Clouds

Clouds auflisten

Sie können die definierten Clouds mit einem spezifischen Astra Konto auflisten.

1. Die Wolken auflisten

Führen Sie den folgenden REST-API-Aufruf durch, um die Clouds aufzulisten.

HTTP-Methode	Pfad
GET	/Account/{Account_id}/Topology/v1/Clouds

Curl-Beispiel: Alle Daten aus allen Clouds zurückgeben

```
curl --location -i --request GET
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/topology/v1/clouds'
--header 'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

Buckets

Listen Sie die Buckets auf

Sie können die S3-Buckets für ein bestimmtes Astra-Konto auflisten.

1. Listen Sie die Eimer auf

Führen Sie den folgenden REST-API-Aufruf durch, um die Buckets aufzulisten.

HTTP-Methode	Pfad
GET	/Account/{Account_id}/Topology/v1/Buckets

Curl-Beispiel: Gibt alle Daten für alle Buckets zurück

```
curl --location -i --request GET
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/topology/v1/buckets'
--header 'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

Storage

Auflisten von Speicherklassen

Sie können die verfügbaren Speicherklassen auflisten.

1. Wählen Sie die Cloud

Führen Sie den Workflow aus "Clouds auflisten" Und wählen Sie die Cloud aus, in der Sie arbeiten werden.

2. Wählen Sie den Cluster

Führen Sie den Workflow aus "Listen Sie die Cluster auf" Und wählen Sie den Cluster aus.

3. Liste der Speicherklassen für einen bestimmten Cluster

Führen Sie den folgenden REST-API-Aufruf durch, um die Storage-Klassen für einen bestimmten Cluster und die Cloud aufzulisten.

HTTP-Methode	Pfad
GET	/Account/{Account_id}/Topology/v1/Clouds/<CLOUD_ID>/Cluster/<CLUSTER_ID>/storageClasses

Curl Beispiel: Gibt alle Daten für alle Speicherklassen zurück

```
curl --location -i --request GET
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/topology/v1/clouds/<CLOUD_I
D>/clusters/<CLUSTER_ID>/storageClasses' --header 'Accept: */*' --header
'Authorization: Bearer <API_TOKEN>'
```

Beispiel für eine JSON-Ausgabe


```
{
    "items": [
        {
            "type": "application/astra-storageClass",
            "version": "1.1",
            "id": "4bacbb3c-0727-4f58-b13c-3a2a069baf89",
            "name": "ontap-basic",
            "provisioner": "csi.trident.netapp.io",
            "available": "eligible",
            "allowVolumeExpansion": "true",
            "reclaimPolicy": "Delete",
            "volumeBindingMode": "Immediate",
            "isDefault": "true",
            "metadata": {
                "createdBy": "system",
                "creationTimestamp": "2022-10-26T05:16:19Z",
                "modificationTimestamp": "2022-10-26T05:16:19Z",
                "labels": []
            }
        },
        {
            "type": "application/astra-storageClass",
            "version": "1.1",
            "id": "150fe657-4a42-47a3-abc6-5dafba3de8bf",
            "name": "thin",
            "provisioner": "kubernetes.io/vsphere-volume",
            "available": "ineligible",
            "reclaimPolicy": "Delete",
            "volumeBindingMode": "Immediate",
            "metadata": {
                "createdBy": "system",
                "creationTimestamp": "2022-10-26T04:46:08Z",
                "modificationTimestamp": "2022-11-04T14:58:19Z",
                "labels": []
            }
        },
        {
```

```
            "type": "application/astra-storageClass",
            "version": "1.1",
            "id": "7c6a5c58-6a0d-4cb6-98a0-8202ad2de74a",
            "name": "thin-csi",
            "provisioner": "csi.vsphere.vmware.com",
            "available": "ineligible",
            "allowVolumeExpansion": "true",
            "reclaimPolicy": "Delete",
            "volumeBindingMode": "WaitForFirstConsumer",
            "metadata": {
                "createdBy": "system",
                "creationTimestamp": "2022-10-26T04:46:17Z",
                "modificationTimestamp": "2022-10-26T04:46:17Z",
                "labels": []
            }
        },
        {
            "type": "application/astra-storageClass",
            "version": "1.1",
            "id": "7010ef09-92a5-4c90-a5e5-3118e02dc9a7",
            "name": "vsim-san",
            "provisioner": "csi.trident.netapp.io",
            "available": "eligible",
            "allowVolumeExpansion": "true",
            "reclaimPolicy": "Delete",
            "volumeBindingMode": "Immediate",
            "metadata": {
                "createdBy": "system",
                "creationTimestamp": "2022-11-03T18:40:03Z",
                "modificationTimestamp": "2022-11-03T18:40:03Z",
                "labels": []
            }
        }
    ]
}
```


Auflisten von Storage-Back-Ends

Sie können die verfügbaren Storage-Back-Ends auflisten.

1. Listen Sie die Back-Ends auf

Führen Sie den folgenden REST-API-Aufruf aus.

HTTP-Methode	Pfad
GET	/Account/{Account_id}/Topology/v1/storageBackends

Curl-Beispiel: Gibt alle Daten für alle Storage-Back-Ends zurück

```
curl --location -i --request GET
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/topology/v1/storageBackends
' --header 'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

Beispiel für eine JSON-Ausgabe

```
{
  "items": [
    {
      "backendCredentialsName": "10.191.77.177",
      "backendName": "myinchunhcluster-1",
      "backendType": "ONTAP",
      "backendVersion": "9.8.0",
      "configVersion": "Not applicable",
      "health": "Not applicable",
      "id": "46467c16-1585-4b71-8e7f-f0bc5ff9da15",
      "location": "nalab2",
      "metadata": {
        "createdBy": "4c483a7e-207b-4f9a-87b7-799a4629d7c8",
        "creationTimestamp": "2021-07-30T14:26:19Z",
        "modificationTimestamp": "2021-07-30T14:26:19Z"
      },
      "ontap": {
        "backendManagementIP": "10.191.77.177",
        "managementIPs": [
          "10.191.77.177",
          "10.191.77.179"
        ]
      },
      "protectionPolicy": "Not applicable",
      "region": "Not applicable",
      "state": "Running",
      "stateUnready": [],
      "type": "application/astra-storageBackend",
      "version": "1.0",
      "zone": "Not applicable"
    }
  ]
}
```

Management-Workflows

Bevor Sie beginnen

Diese Workflows können als Teil der Verwaltung der Applikationen in einem von Astra gemanagten Cluster verwendet werden.

Diese Workflows können jederzeit von NetApp erweitert und ergänzt werden, sodass Sie sie in regelmäßigen Abständen prüfen sollten.

Allgemeine Vorbereitung

Bevor Sie einen Astra-Workflow verwenden, sollten Sie unbedingt lesen "Die Nutzung der Workflows wird vorbereitet".

Workflow-Kategorien

Die Management-Workflows sind in verschiedene Kategorien unterteilt, um die Suche nach den gewünschten zu erleichtern.

Kategorie	Beschreibung
Applikationskontrolle	Mithilfe dieser Workflows können Sie verwaltete und nicht gemanagte Applikationen steuern. Sie können die Apps auflisten sowie eine verwaltete App erstellen und entfernen.
Applikationssicherung	Mithilfe dieser Workflows können gemanagte Applikationen durch Snapshots und Backups gesichert werden.
Klonen und Wiederherstellen von Applikationen	In diesen Workflows wird beschrieben, wie Sie gemanagte Applikationen klonen und wiederherstellen.
Unterstützung	Es stehen mehrere Workflows zur Verfügung, um Ihre Applikationen zu debuggen und zu unterstützen sowie die allgemeine Kubernetes-Umgebung.

Weitere Überlegungen

Bei der Verwendung der Management-Workflows müssen einige zusätzliche Aspekte berücksichtigt werden.

Klonen einer Applikation

Beim Klonen einer Applikation müssen einige Aspekte berücksichtigt werden. Die unten beschriebenen Parameter sind Teil des JSON-Eingangs.

Quell-Cluster-ID

Der Wert von `sourceClusterID` Identifiziert immer das Cluster, auf dem die ursprüngliche App installiert ist.

Cluster-ID

Der Wert von `clusterID` Identifiziert das Cluster, auf dem die neue App installiert werden soll.

- Beim Klonen innerhalb desselben Clusters `clusterID` Und `sourceClusterID` Gleicher Wert.
- Beim Klonen über Cluster unterscheiden sich die beiden Werte und `clusterID` Sollte die ID des Ziel-Clusters sein.

Namespaces

Der `namespace` Der Wert muss sich von der ursprünglichen Quell-App unterscheiden. Außerdem kann der Namespace für den Klon nicht vorhanden sein und Astra wird ihn erstellen.

Backups und Snapshots

Optional können Sie eine Applikation aus einem vorhandenen Backup oder Snapshot mit der klonen `backupID` Oder `snapshotID` Parameter. Wenn Sie keine Backup oder Momentaufnahme zur Verfügung stellen, wird Astra zuerst eine Sicherung der Anwendung erstellen und dann aus dem Backup klonen.

Wiederherstellen einer Anwendung

Folgende Punkte sind bei der Wiederherstellung einer Applikation zu beachten.

- Das Wiederherstellen einer Applikation ähnelt dem Klonvorgang.
- Beim Wiederherstellen einer Anwendung müssen Sie entweder ein Backup oder einen Snapshot bereitstellen.

Applikationskontrolle

Listen Sie die Apps auf

Sie können die Applikationen auflisten, die aktuell vom Astra verwaltet werden. Dies könnten Sie tun, um die Snapshots oder Backups für eine bestimmte Anwendung zu finden.

1. Listen Sie die Anwendungen auf

Führen Sie den folgenden REST-API-Aufruf aus.

HTTP-Methode	Pfad
GET	/Account/{Account_id}/k8s/v2/Apps

Zusätzliche Eingabeparameter

Zusätzlich zu den Parametern, die bei allen REST-API-Aufrufen üblich sind, werden die folgenden Parameter auch in den Curl-Beispielen für diesen Schritt verwendet.

Parameter	Typ	Erforderlich	Beschreibung
Einschließlich	Abfrage	Nein	Wählen Sie optional die Werte aus, die in der Antwort zurückgegeben werden sollen.

Curl Beispiel: Gibt alle Daten für alle Apps zurück

```
curl --location -i --request GET
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/k8s/v2/apps' --header
'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

Curl-Beispiel: Gibt den Namen, die id und den Status aller Apps zurück

```
curl --location -i --request GET
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/k8s/v2/apps?include=name,id
,state' --header 'Accept: */*' --header 'Authorization: Bearer
<API_TOKEN>'
```

Beispiel für eine JSON-Ausgabe


```
{
    "items": [
        [
            "mysql",
            "4ee2b8fa-3696-4f32-8879-399792f477c3",
            "ready"
        ],
        [
            "postgresql",
            "3b984474-e5c9-4b64-97ee-cdeb9bcd212e",
            "ready"
        ],
    ],
    "metadata": {}
}
```


Holen Sie sich eine App

Sie können alle Ressourcenvariablen abrufen, die eine einzelne Anwendung beschreiben.

Bevor Sie beginnen

Sie müssen die ID der App haben, die Sie abrufen möchten. Bei Bedarf können Sie den Workflow verwenden "Listen Sie die Apps auf" Zum Auffinden der Anwendung.

1. Holen Sie sich die Anwendung

Führen Sie den folgenden REST-API-Aufruf aus.

HTTP-Methode	Pfad
GET	/Accounts/{Account_id}/k8s/v2/Apps/{App_id}

Zusätzliche Eingabeparameter

Zusätzlich zu den Parametern, die bei allen REST-API-Aufrufen üblich sind, werden die folgenden Parameter auch in den Curl-Beispielen für diesen Schritt verwendet.

Parameter	Typ	Erforderlich	Beschreibung
App-id	Pfad	Ja.	ID-Wert der abzurufenden Anwendung.

Curl Beispiel: Alle Daten für die Anwendung zurückgeben

```
curl --location -i --request GET
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/k8s/v2/apps/<APP_ID>'
--header 'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

Eine App verwalten

Sie können eine gemanagte Applikation auf Basis einer Applikation erstellen, die Astra in einem bestimmten Namespace bereits bekannt ist. Wenn eine Applikation mit Astra verwaltet oder definiert wird, können Sie sie durch Backups und Snapshots schützen.

1. Wählen Sie den Namespace

Führen Sie den Workflow aus "Listen Sie die Namespaces auf" Und wählen Sie den Namespace aus.

2. Wählen Sie den Cluster

Führen Sie den Workflow aus "Listen Sie die Cluster auf" Und wählen Sie den Cluster aus.

3. Die Anwendung verwalten

Führen Sie den folgenden REST-API-Aufruf durch, um die Anwendung zu verwalten.

HTTP-Methode	Pfad
POST	/Account/{Account_id}/k8s/v2/Apps

Zusätzliche Eingabeparameter

Zusätzlich zu den Parametern, die bei allen REST-API-Aufrufen üblich sind, werden die folgenden Parameter auch in den Curl-Beispielen für diesen Schritt verwendet.

Parameter	Typ	Erforderlich	Beschreibung
JSON	Text	Ja.	Stellt die Parameter bereit, die zur Identifizierung der zu verwaltenden Anwendung erforderlich sind. Siehe das folgende Beispiel.

JSON-Eingabebeispiel

```
{
  "clusterID": "7ce83fba-6aa1-4e0c-a194-26e714f5eb46",
  "name": "subtext",
  "namespaceScopedResources": [{"namespace": "kube-matrix"}],
  "type": "application/astra-app",
  "version": "2.0"
}
```

Curl Beispiel: Eine App verwalten

```
curl --location -i --request POST
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/k8s/v2/apps' --header
'Content-Type: application/astra-app+json' --header 'Accept: */*' --header
'Authorization: Bearer <API_TOKEN>'  --data @JSONinput
```

Verwaltung einer Anwendung aufheben

Sie können eine verwaltete Anwendung entfernen, wenn sie nicht mehr benötigt wird. Durch Entfernen einer verwalteten Anwendung werden auch die zugeordneten Zeitpläne gelöscht.

Bevor Sie beginnen

Sie müssen über die ID der App verfügen, die Sie verwalten möchten. Bei Bedarf können Sie den Workflow verwenden "Listen Sie die Apps auf" Zum Auffinden der Anwendung.

Backups und Snapshots der Applikation werden nicht automatisch entfernt, wenn sie gelöscht wird. Wenn Sie die Backups und Snapshots nicht mehr benötigen, sollten Sie sie löschen, bevor Sie die Anwendung entfernen.

1. Die App wurde nicht verwaltet

Führen Sie den folgenden REST-API-Aufruf durch, um die App zu entfernen.

HTTP-Methode	Pfad
Löschen	/Accounts/{Account_id}/k8s/v2/Apps/{App_id}

Zusätzliche Eingabeparameter

Zusätzlich zu den Parametern, die bei allen REST-API-Aufrufen üblich sind, werden die folgenden Parameter auch in den Curl-Beispielen für diesen Schritt verwendet.

Parameter	Typ	Erforderlich	Beschreibung
App-id	Pfad	Ja.	Identifiziert die zu entfernende Anwendung.

Curl Beispiel: Eine verwaltete App entfernen

```
curl --location -i --request DELETE
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/k8s/v2/apps/<APP_ID>'
--header 'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

App-Schutz

Listen Sie die Snapshots auf

Sie können die Snapshots auflisten, die für eine bestimmte Anwendung erstellt wurden.

Bevor Sie beginnen

Sie müssen über die ID der App verfügen, für die Sie die Snapshots auflisten möchten. Bei Bedarf können Sie den Workflow verwenden "Listen Sie die Apps auf" Zum Auffinden der Anwendung.

1. Listen Sie die Snapshots auf

Führen Sie den folgenden REST-API-Aufruf durch, um die Snapshots aufzulisten.

HTTP-Methode	Pfad
GET	/Accounts/{Account_id}/k8s/v1/Apps/{App_id}/appSnaps

Zusätzliche Eingabeparameter

Zusätzlich zu den Parametern, die bei allen REST-API-Aufrufen üblich sind, werden die folgenden Parameter auch in den Curl-Beispielen für diesen Schritt verwendet.

Parameter	Typ	Erforderlich	Beschreibung
App-id	Pfad	Ja.	Identifiziert die Anwendung, die die aufgeführten Snapshots besitzt.
Zählen	Abfrage	Nein	Wenn `count=true` Die Anzahl der Snapshots wird im Metadatenabschnitt der Antwort berücksichtigt.

Curl Beispiel: Gibt alle Schnappschüsse für die App zurück

```
curl --location -i --request GET
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/k8s/v1/apps/<APP_ID>/appSna
ps' --header 'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

Curl Beispiel: Gibt alle Snapshots für die App und die Zählung zurück

```
curl --location -i --request GET
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/k8s/v1/apps/<APP_ID>/appSna
ps?count=true' --header 'Accept: */*' --header 'Authorization: Bearer
<API_TOKEN>'
```

Beispiel für eine JSON-Ausgabe


```
{
    "items": [
        {
            "type": "application/astra-appSnap",
            "version": "1.1",
            "id": "1ce34da4-bb0a-4926-b925-4a5d85dda8c2",
            "hookState": "success",
            "metadata": {
                "createdBy": "a530e865-23e8-4e2e-8020-e92c419a3867",
                "creationTimestamp": "2022-10-30T22:44:20Z",
                "modificationTimestamp": "2022-10-30T22:44:20Z",
                "labels": []
            },
            "snapshotAppAsset": "0ebfe3f8-40ed-4bdc-88c4-2144fbda85a0",
            "snapshotCreationTimestamp": "2022-10-30T22:44:33Z",
            "name": "snapshot-david-1",
            "state": "completed",
            "stateUnready": []
        }
    ],
    "metadata": {}
}
```


Listen Sie die Backups auf

Sie können die für eine bestimmte Anwendung erstellten Backups auflisten.

Bevor Sie beginnen

Sie müssen über die ID der App verfügen, für die Sie die Backups auflisten möchten. Bei Bedarf können Sie den Workflow verwenden "Listen Sie die Apps auf" Zum Auffinden der Anwendung.

1. Listen Sie die Backups auf

Führen Sie den folgenden REST-API-Aufruf aus.

HTTP-Methode	Pfad
GET	/Accounts/{Account_id}/k8s/v1/Apps/{App_id}/appBackups

Zusätzliche Eingabeparameter

Zusätzlich zu den Parametern, die bei allen REST-API-Aufrufen üblich sind, werden die folgenden Parameter auch in den Curl-Beispielen für diesen Schritt verwendet.

Parameter	Typ	Erforderlich	Beschreibung
App-id	Pfad	Ja.	Gibt die verwaltete Anwendung an, die die aufgeführten Backups besitzt.

Curl Beispiel: Alle Backups für die App zurückgeben

```
curl --location -i --request GET
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/k8s/v1/apps/<APP_ID>/appBac
kups' --header 'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

Beispiel für eine JSON-Ausgabe

```
{
    "items": [
        {
            "type": "application/astra-appBackup",
            "version": "1.1",
            "id": "8edeb4a4-fd8b-4222-a559-1013145b28fc",
            "name": "backup-david-oct28-1",
            "bucketID": "a443e58f-59bd-4d45-835a-1bc7813f659a",
            "snapshotID": "dfe237cb-57b7-4576-af4d-00ba3a8f2828",
            "state": "completed",
            "stateUnready": [],
            "hookState": "success",
            "totalBytes": 205219132,
            "bytesDone": 205219132,
            "percentDone": 100,
            "metadata": {
                "labels": [
                    {
                        "name": "astra.netapp.io/labels/read-
only/triggerType",
                        "value": "backup"
                    }
                ],
                "creationTimestamp": "2022-10-28T21:58:37Z",
                "modificationTimestamp": "2022-10-28T21:58:55Z",
                "createdBy": "a530e865-23e8-4e2e-8020-e92c419a3867"
            }
        }
    ],
    "metadata": {}
}
```


Erstellen Sie einen Snapshot für eine Anwendung

Sie können einen Snapshot für eine bestimmte Anwendung erstellen.

Bevor Sie beginnen

Sie müssen über die ID der App verfügen, für die Sie einen Snapshot erstellen möchten. Bei Bedarf können Sie den Workflow verwenden "Listen Sie die Apps auf" Zum Auffinden der Anwendung.

1. Erstellen Sie einen Snapshot

Führen Sie den folgenden REST-API-Aufruf aus.

HTTP-Methode	Pfad
POST	/Accounts/{Account_id}/k8s/v1/Apps/{App_id}/appSnaps

Zusätzliche Eingabeparameter

Zusätzlich zu den Parametern, die bei allen REST-API-Aufrufen üblich sind, werden die folgenden Parameter auch in den Curl-Beispielen für diesen Schritt verwendet.

Parameter	Typ	Erforderlich	Beschreibung
App-id	Pfad	Ja.	Gibt die verwaltete Anwendung an, in der der Snapshot erstellt werden soll.
JSON	Text	Ja.	Stellt die Parameter für den Snapshot bereit. Siehe das folgende Beispiel.

JSON-Eingabebeispiel

```
{
  "type": "application/astra-appSnap",
  "version": "1.1",
  "name": "snapshot-david-1"
}
```

Curl Beispiel: Erstellen Sie einen Snapshot für die App

```
curl --location -i --request POST
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/k8s/v1/apps/<APP_ID>/appSna
ps' --header 'Content-Type: application/astra-appSnap+json' --header
'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>' --data
@JSONinput
```

Backup für eine Anwendung erstellen

Sie können ein Backup für eine bestimmte Applikation erstellen und dann das Backup zum Wiederherstellen oder Klonen der App verwenden.

Bevor Sie beginnen

Sie müssen über die ID der App verfügen, die Sie sichern möchten. Bei Bedarf können Sie den Workflow verwenden "Listen Sie die Apps auf" Zum Auffinden der Anwendung.

1. Erstellen Sie ein Backup

Führen Sie den folgenden REST-API-Aufruf aus.

HTTP-Methode	Pfad
POST	/Accounts/{Account_id}/k8s/v1/Apps/{App_id}/appBackups

Zusätzliche Eingabeparameter

Zusätzlich zu den Parametern, die bei allen REST-API-Aufrufen üblich sind, werden die folgenden Parameter auch in den Curl-Beispielen für diesen Schritt verwendet.

Parameter	Typ	Erforderlich	Beschreibung
App-id	Pfad	Ja.	Gibt die Applikation an, in der das Backup erstellt werden soll.
JSON	Text	Ja.	Stellt die Parameter für die Sicherung bereit. Siehe das folgende Beispiel.

JSON-Eingabebeispiel

```
{
  "type": "application/astra-appBackup",
  "version": "1.1",
  "name": "backup-david-1"
}
```

Curl Beispiel: Erstellen Sie ein Backup für die App

```
curl --location -i --request POST
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/k8s/v1/apps/<APP_ID>/appBac
kups' --header 'Content-Type: application/astra-appBackup+json' --header
'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>' --data
@JSONinput
```

Löschen Sie einen Snapshot

Sie können einen Snapshot löschen, der einer Anwendung zugeordnet ist.

Bevor Sie beginnen

Sie müssen Folgendes haben:

- ID der Anwendung, die den Snapshot besitzt. Bei Bedarf können Sie den Workflow verwenden "Listen Sie die Apps auf" Zum Auffinden der Anwendung.
- ID des Snapshots, den Sie löschen möchten. Bei Bedarf können Sie den Workflow verwenden "Listen Sie die Snapshots auf" Um den Snapshot zu finden.

1. Löschen Sie den Snapshot

Führen Sie den folgenden REST-API-Aufruf aus.

HTTP-Methode	Pfad
Löschen	/Accounts/{Account_id}/k8s/v1/Apps/{App_id}/appSnaps/{appSnap_id}

Zusätzliche Eingabeparameter

Zusätzlich zu den Parametern, die bei allen REST-API-Aufrufen üblich sind, werden die folgenden Parameter auch in den Curl-Beispielen für diesen Schritt verwendet.

Parameter	Typ	Erforderlich	Beschreibung
App-id	Pfad	Ja.	Identifiziert die verwaltete Anwendung, die den Snapshot besitzt.
snapshot-id	Pfad	Ja.	Identifiziert den zu löschenden Snapshot.

Curl Beispiel: Löschen Sie einen einzelnen Snapshot für die App

```
curl --location -i --request DELETE
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/k8s/v1/apps/<APP_ID>/appSna
ps/<SNAPSHOT_ID>' --header 'Accept: */*' --header 'Authorization: Bearer
<API_TOKEN>'
```

Löschen Sie ein Backup

Sie können ein Backup einer Anwendung löschen.

Bevor Sie beginnen

Sie müssen Folgendes haben:

- ID der Applikation, für die das Backup zuständig ist. Bei Bedarf können Sie den Workflow verwenden "Listen Sie die Apps auf" Zum Auffinden der Anwendung.
- ID des zu löschenden Backups. Bei Bedarf können Sie den Workflow verwenden "Listen Sie die Backups auf" Um den Snapshot zu finden.

1. Löschen Sie die Sicherung

Führen Sie den folgenden REST-API-Aufruf aus.

> Sie können das Löschen einer fehlgeschlagenen Sicherung wie unten beschrieben mit der optionalen Anforderungs-Kopfzeile erzwingen.

HTTP-Methode	Pfad
Löschen	/Accounts/{Account_id}/k8s/v1/Apps/{App_id}/appBackups/{appBackup_id}

Zusätzliche Eingabeparameter

Zusätzlich zu den Parametern, die bei allen REST-API-Aufrufen üblich sind, werden die folgenden Parameter auch in den Curl-Beispielen für diesen Schritt verwendet.

Parameter	Typ	Erforderlich	Beschreibung
App-id	Pfad	Ja.	Gibt die verwaltete Anwendung an, die das Backup besitzt.
Backup-id	Pfad	Ja.	Identifiziert das zu löschende Backup.
Löschen erzwingen	Kopfzeile	Nein	Wird verwendet, um das Löschen eines fehlgeschlagenen Backups zu erzwingen.

Curl Beispiel: Löschen Sie ein einzelnes Backup für die App

```
curl --location -i --request DELETE
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/k8s/v1/apps/<APP_ID>/appBac
kups/<BACKUP_ID>' --header 'Accept: */*' --header 'Authorization: Bearer
<API_TOKEN>'
```

Curl Beispiel: Löschen Sie eine einzelne Sicherung für die App mit der Force-Option

```
curl --location -i --request DELETE
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/k8s/v1/apps/<APP_ID>/appBac
kups/<BACKUP_ID>' --header 'Accept: */*' --header 'Authorization: Bearer
<API_TOKEN>' --header 'Force-Delete: true'
```

Klonen und Wiederherstellen einer Applikation

Klonen einer Anwendung

Sie können eine neue Applikation erstellen, indem Sie eine vorhandene Applikation klonen.

Bevor Sie beginnen

Beachten Sie Folgendes zu diesem Workflow:

- Ein Anwendungsbackup oder -Snapshot wird nicht verwendet
- Der Klonvorgang wird im selben Cluster durchgeführt
- Die neue App wird in einem anderen Namespace platziert

> Zum Klonen einer App auf einem anderen Cluster müssen Sie den aktualisieren `clusterId` Parameter in den JSON-Input, wie es für Ihre Umgebung geeignet ist.

1. Wählen Sie die zu klonenden App aus

Führen Sie den Workflow aus "Listen Sie die Apps auf" Und wählen Sie die Anwendung aus, die Sie klonen möchten. Für DEN REST-Aufruf, der zum Klonen der App verwendet wird, sind mehrere Ressourcenwerte erforderlich.

2. Die App klonen

Führen Sie den folgenden REST-API-Aufruf durch, um die App zu klonen.

HTTP-Methode	Pfad
POST	/Account/{Account_id}/k8s/v2/Apps

Zusätzliche Eingabeparameter

Zusätzlich zu den Parametern, die bei allen REST-API-Aufrufen üblich sind, werden die folgenden Parameter auch in den Curl-Beispielen für diesen Schritt verwendet.

Parameter	Typ	Erforderlich	Beschreibung
JSON	Text	Ja.	Stellt die Parameter für die geklonte App bereit. Siehe das folgende Beispiel.

JSON-Eingabebeispiel

```
{
  "type": "application/astra-app",
  "version": "2.0",
  "name": "mysql-clone",
  "clusterID": "30880586-d579-4d27-930f-a9633e59173b",
  "sourceClusterID": "30880586-d579-4d27-930f-a9633e59173b",
  "namespace": "mysql-ns",
  "sourceAppID": "e591ee59-ea90-4a9f-8e6c-d2b6e8647096"
}
```

Curl Beispiel: Klonen einer App

```
curl --location -i --request POST
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/k8s/v2/apps' --header
'Content-Type: application/astra-app+json' --header '*/*' --header
'Authorization: Bearer <API_TOKEN>' --data @JSONinput
```

Eine Anwendung aus einem Snapshot klonen

Sie können eine neue Applikation erstellen, indem Sie sie aus einem Snapshot klonen.

Bevor Sie beginnen

Beachten Sie Folgendes zu diesem Workflow:

- Ein App-Snapshot wird verwendet
- Der Klonvorgang wird im selben Cluster durchgeführt

> Zum Klonen einer App auf einem anderen Cluster müssen Sie den aktualisieren `clusterId` Parameter in den JSON-Input, wie es für Ihre Umgebung geeignet ist.

1. Wählen Sie die zu klonenden App aus

Führen Sie den Workflow aus "Listen Sie die Apps auf" Und wählen Sie die Anwendung aus, die Sie klonen möchten. Für DEN REST-Aufruf, der zum Klonen der App verwendet wird, sind mehrere Ressourcenwerte erforderlich.

2. Wählen Sie den zu verwendenden Snapshot aus

Führen Sie den Workflow aus "Listen Sie die Snapshots auf" Und wählen Sie den gewünschten Snapshot aus.

3. Die App klonen

Führen Sie den folgenden REST-API-Aufruf aus.

HTTP-Methode	Pfad
POST	/Account/{Account_id}/k8s/v2/Apps

Zusätzliche Eingabeparameter

Zusätzlich zu den Parametern, die bei allen REST-API-Aufrufen üblich sind, werden die folgenden Parameter auch in den Curl-Beispielen für diesen Schritt verwendet.

Parameter	Typ	Erforderlich	Beschreibung
JSON	Text	Ja.	Stellt die Parameter für die geklonte App bereit. Siehe das folgende Beispiel.

JSON-Eingabebeispiel

```
{
  "type": "application/astra-app",
  "version": "2.0",
  "name": "mysql-clone2",
  "clusterID": "30880586-d579-4d27-930f-a9633e59173b",
  "sourceClusterID": "30880586-d579-4d27-930f-a9633e59173b",
  "namespace": "mysql",
  "snapshotID": "e24515bd-a28e-4b28-b832-f3c74dbf32fb"
}
```

Curl Beispiel: Klonen einer App aus einem Snapshot

```
curl --location -i --request POST
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/k8s/v2/apps' --header
'Content-Type: application/astra-app+json' --header '*/*' --header
'Authorization: Bearer <API_TOKEN>' --data @JSONinput
```

Klonen einer Applikation aus einem Backup

Sie können eine neue Applikation erstellen, indem Sie sie aus einem Backup klonen.

Bevor Sie beginnen

Beachten Sie Folgendes zu diesem Workflow:

- Es wird ein App-Backup verwendet
- Der Klonvorgang wird im selben Cluster durchgeführt

> Zum Klonen einer App auf einem anderen Cluster müssen Sie den aktualisieren `clusterId` Parameter in den JSON-Input, wie es für Ihre Umgebung geeignet ist.

1. Wählen Sie die zu klonenden App aus

Führen Sie den Workflow aus "Listen Sie die Apps auf" Und wählen Sie die Anwendung aus, die Sie klonen möchten. Für DEN REST-Aufruf, der zum Klonen der App verwendet wird, sind mehrere Ressourcenwerte erforderlich.

2. Wählen Sie das zu verwendende Backup aus

Führen Sie den Workflow aus "Listen Sie die Backups auf" Und wählen Sie das gewünschte Backup aus.

3. Die App klonen

Führen Sie den folgenden REST-API-Aufruf aus.

HTTP-Methode	Pfad
POST	/Account/{Account_id}/k8s/v2/qpps

Zusätzliche Eingabeparameter

Zusätzlich zu den Parametern, die bei allen REST-API-Aufrufen üblich sind, werden die folgenden Parameter auch in den Curl-Beispielen für diesen Schritt verwendet.

Parameter	Typ	Erforderlich	Beschreibung
JSON	Text	Ja.	Stellt die Parameter für die geklonte App bereit. Siehe das folgende Beispiel.

JSON-Eingabebeispiel

```
{
  "type": "application/astra-app",
  "version": "2.0",
  "name": "mysql-clone3",
  "clusterID": "30880586-d579-4d27-930f-a9633e59173b",
  "sourceClusterID": "30880586-d579-4d27-930f-a9633e59173b",
  "namespace": "mysql",
  "backupID": "e24515bd-a28e-4b28-b832-f3c74dbf32fb"
}
```

Curl Beispiel: Klonen einer Applikation aus einem Backup

```
curl --location -i --request POST
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/k8s/v2/apps' --header
'Content-Type: application/astra-app+json' --header '*/*' --header
'Authorization: Bearer <API_TOKEN>' --data @JSONinput
```

Wiederherstellung einer Anwendung aus einem Backup

Sie können eine Applikation wiederherstellen, indem Sie eine neue Applikation aus einem Backup erstellen.

1. Wählen Sie die Anwendung, die wiederhergestellt werden soll

Führen Sie den Workflow aus "Listen Sie die Apps auf" Und wählen Sie die Anwendung aus, die Sie klonen möchten. Für DEN REST-Aufruf, der zur Wiederherstellung der App verwendet wird, sind mehrere Ressourcenwerte erforderlich.

2. Wählen Sie das zu verwendende Backup aus

Führen Sie den Workflow aus "Listen Sie die Backups auf" Und wählen Sie das gewünschte Backup aus.

3. Stellen Sie die App wieder her

Führen Sie den folgenden REST-API-Aufruf aus. Sie müssen die ID für ein Backup (wie unten gezeigt) oder einen Snapshot angeben.

HTTP-Methode	Pfad
PUT	/Account/{Account_id}/k8s/v2/Apps/{App_id}

Zusätzliche Eingabeparameter

Zusätzlich zu den Parametern, die bei allen REST-API-Aufrufen üblich sind, werden die folgenden Parameter auch in den Curl-Beispielen für diesen Schritt verwendet.

Parameter	Typ	Erforderlich	Beschreibung
JSON	Text	Ja.	Stellt die Parameter für die geklonte App bereit. Siehe das folgende Beispiel.

JSON-Eingabebeispiel

```
{
  "type": "application/astra-app",
  "version": "2.0",
  "backupID": "e24515bd-a28e-4b28-b832-f3c74dbf32fb"
}
```

Curl Beispiel: Wiederherstellen einer vorhandenen Applikation aus einem Backup

```
curl --location -i --request PUT
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/k8s/v2/apps/<APP_ID>'
--header 'Content-Type: application/astra-app+json' --header '*/*'
--header 'ForceUpdate: true' --header 'Authorization: Bearer <API_TOKEN>'
--data @JSONinput
```

Namespaces

Listen Sie die Namespaces auf

Sie können die verfügbaren Namespaces auflisten.

1. Listen Sie die Namespaces auf

Führen Sie den folgenden REST-API-Aufruf durch, um die Namespaces aufzulisten.

HTTP-Methode	Pfad
GET	/Account/{Account_id}/Topology/v1/Namespaces

Curl Beispiel: Gibt alle Daten für alle Namespaces zurück

```
curl --location -i --request GET
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/topology/v1/namespaces'
--header 'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

Curl-Beispiel: Rückgabename, Status und Cluster-ID für alle Namespaces

```
curl --location -i --request GET
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/topology/v1/namespaces?incl
ude=name,namespaceState,clusterID' --header 'Accept: */*' --header
'Authorization: Bearer <API_TOKEN>'
```

Beispiel für eine JSON-Ausgabe


```
{
    "items": [
        [
            "default",
            "discovered",
            "922f924a-a476-4a79-97f6-472571698154"
        ],
        [
            "kube-node-lease",
            "discovered",
            "922f924a-a476-4a79-97f6-472571698154"
        ],
        [
            "kube-public",
            "discovered",
            "922f924a-a476-4a79-97f6-472571698154"
        ],
        [
            "kube-system",
            "discovered",
            "922f924a-a476-4a79-97f6-472571698154"
        ],
        [
            "mysql",
            "discovered",
            "922f924a-a476-4a79-97f6-472571698154"
        ],
        [
            "mysql-clone1",
            "discovered",
            "922f924a-a476-4a79-97f6-472571698154"
        ],
        [
            "netapp-acc-operator",
            "discovered",
            "922f924a-a476-4a79-97f6-472571698154"
```

```
        ],
        [
            "openshift",
            "discovered",
            "922f924a-a476-4a79-97f6-472571698154"
        ],
        [
            "trident",
            "discovered",
            "922f924a-a476-4a79-97f6-472571698154"
        ]
    ],
    "metadata": {}
}
```

Unterstützung

Listen Sie die Benachrichtigungen auf

Sie können die Benachrichtigungen für ein bestimmtes Astra-Konto auflisten. Dies können Sie im Rahmen der Überwachung der Systemaktivität oder des Debugging eines Problems tun.

1. Listen Sie die Benachrichtigungen auf

Führen Sie den folgenden REST-API-Aufruf aus.

HTTP-Methode	Pfad
GET	/Account/{Account_id}/Core/v1/notifications

Zusätzliche Eingabeparameter

Zusätzlich zu den Parametern, die bei allen REST-API-Aufrufen üblich sind, werden die folgenden Parameter auch in den Curl-Beispielen für diesen Schritt verwendet.

Parameter	Typ	Erforderlich	Beschreibung
Filtern	Abfrage	Nein	Filtern Sie optional die Benachrichtigungen, die in der Antwort zurückgegeben werden sollen.
Einschließlich	Abfrage	Nein	Wählen Sie optional die Werte aus, die in der Antwort zurückgegeben werden sollen.

Curl Beispiel: Alle Benachrichtigungen zurückgeben

```
curl --location -i --request GET
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/core/v1/notifications'
--header 'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

Curl Beispiel: Gibt die Beschreibung für Benachrichtigungen mit Schweregrad der Warnung zurück

```
curl --location -i --request GET
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/core/v1/notifications?filte
r=severity%20eq%20'warning'&include=description' --header 'Accept: */*'
--header 'Authorization: Bearer <API_TOKEN>'
```

Beispiel für eine JSON-Ausgabe


```
{
  "items": [
    [
      "Trident on cluster david-ie-00 has failed or timed out;
installation of the Trident operator failed or is not yet complete;
operator failed to reach an installed state within 300.00 seconds;
container trident-operator not found in operator deployment"
    ],
    [
      "Trident on cluster david-ie-00 has failed or timed out;
installation of the Trident operator failed or is not yet complete;
operator failed to reach an installed state within 300.00 seconds;
container trident-operator not found in operator deployment"
    ]
  ],
  "metadata": {}
}
```


Löschen einer fehlgeschlagenen Anwendung

Sie können eine verwaltete Anwendung möglicherweise nicht entfernen, wenn eine Sicherung oder ein Snapshot in einem fehlgeschlagenen Zustand vorhanden ist. In diesem Fall können Sie die App mithilfe des unten beschriebenen Workflows manuell entfernen.

1. Wählen Sie die zu löschende App

Führen Sie den Workflow aus "Listen Sie die Apps auf" Und wählen Sie die Anwendung aus, die Sie entfernen möchten.

2. Listen Sie die bestehenden Backups für die App auf

Führen Sie den Workflow aus "Listen Sie die Backups auf".

3. Löschen Sie alle Backups

Löschen Sie alle App-Backups durch Ausführen des Workflows "Löschen Sie ein Backup" Für jedes Backup in der Liste.

4. Listen Sie die vorhandenen Snapshots für die App auf

Führen Sie den Workflow aus "Listen Sie die Snapshots auf".

5. Löschen Sie alle Snapshots

Führen Sie den Workflow aus "Löschen Sie einen Snapshot" Von jedem Snapshot in der Liste.

6. Entfernen Sie die Anwendung

Führen Sie den Workflow aus "Verwaltung einer Anwendung aufheben" Um die Anwendung zu entfernen.

Verwendung Von Python

NetApp Astra Control Python SDK

NetApp Astra Control Python SDK ist ein Open-Source-Paket, mit dem Sie eine Astra Control Implementierung automatisieren können. Das Paket ist auch eine wertvolle Ressource, um sich über die Astra Control REST API zu informieren, vielleicht im Rahmen der Erstellung Ihrer eigenen Automatisierungsplattform.

Zur Einfachheit wird das NetApp Astra Control Python SDK durchgehend auf dieser Seite als **SDK** bezeichnet.

Zwei verwandte Softwaretools

Das SDK enthält zwei verschiedene, wenn auch verwandte Tools, die auf verschiedenen Ebenen der Abstraktion beim Zugriff auf die Astra Control REST API arbeiten.

Astra SDK

Das Astra SDK bietet die Kernfunktionen der Plattform. Es enthält eine Reihe von Python-Klassen, in denen die zugrunde liegenden REST-API-Aufrufe abstrahiert werden. Die Klassen unterstützen administrative Aktionen auf verschiedenen Astra Control Ressourcen, einschließlich Apps, Backups, Snapshots und Cluster.

Das Astra SDK ist ein Teil des Pakets und wird in der Single bereitgestellt `astraSDK.py` Datei: Sie können diese Datei in Ihre Umgebung importieren und die Klassen direkt verwenden.

Das **NetApp Astra Control Python SDK** (oder nur SDK) ist der Name des gesamten Pakets. Das **Astra SDK** bezieht sich auf die Core Python Klassen in der einzelnen Datei `astraSDK.py`.

Toolkit-Skript

Neben der Astra SDK-Datei, die `toolkit.py` Skript ist ebenfalls verfügbar. Dieses Skript wird auf einer höheren Abstraktionsebene ausgeführt und bietet Zugriff auf diskrete, intern als Python-Funktionen definierte administrative Aktionen. Das Skript importiert das Astra SDK und ruft nach Bedarf die Klassen an.

Zugang zu

Sie haben folgende Möglichkeiten, auf das SDK zuzugreifen:

Python-Paket

Das SDK ist unter verfügbar "Python-Paketindex" Unter dem Namen **acToolkit**. Dem Paket wird eine Versionsnummer zugewiesen und bei Bedarf auch weiterhin aktualisiert. Sie müssen das Paketverwaltungsprogramm * PIP* verwenden, um das Paket in Ihrer Umgebung zu installieren.

Nach der Installation können die astraSDK.py Klassen durch Platzieren genutzt werden `import astraSDK` In Ihren Skripten. Darüber Hinaus `actoolkit` Kann direkt an Ihrer Eingabeaufforderung aufgerufen werden und entspricht `toolkit.py` (`actoolkit list clusters` Ist das gleiche wie `./toolkit.py list clusters`).

Siehe "PyPI: NetApp Astra Control Python SDK" Finden Sie weitere Informationen.

GitHub-Quellcode

Der SDK-Quellcode ist auch bei GitHub erhältlich. Das Repository umfasst Folgendes:

- `astraSDK.py` (Astra SDK mit Python-Klassen)
- `toolkit.py` (Auf höherer Ebene funktionbasiertes Skript)
- Detaillierte Installationsanforderungen und Anweisungen
- Installationsskripte
- Zusätzliche Dokumentation

Sie können die klonen "GitHub: NetApp/netapp-astra-Toolkits" Repository in Ihre lokale Umgebung einbinden

Installation und grundlegende Anforderungen

Es gibt verschiedene Optionen und Anforderungen, die bei der Installation des Pakets und bei der Vorbereitung der Verwendung berücksichtigt werden müssen.

Zusammenfassung der Installationsoptionen

Sie können das SDK auf eine der folgenden Arten installieren:

- Verwenden Sie das vorbereitete "Docker: NetApp/astra-Toolkits" Image, das alle erforderlichen Abhängigkeiten installiert hat, einschließlich `actoolkit`
- Verwenden Sie Pip, um den zu installieren `actoolkit` Paket von PyPI in Ihre Python-Umgebung
- Klonen Sie das GitHub Repository und kopieren/ändern Sie die beiden Core Python-Dateien, damit sie für Ihren Python-Client-Code zugänglich sind

Weitere Informationen finden Sie auf den Seiten PyPI und GitHub.

Anforderungen für die Astra Control-Umgebung

Ob direkt die Python-Klassen im Astra SDK oder die Funktionen im `toolkit.py` Skript, schließlich sind Sie bei einer Implementierung von Astra Control auf DIE REST-API zugreifen. Aus diesem Grund benötigen Sie ein Astra-Konto zusammen mit einem API-Token. Siehe "Bevor Sie beginnen" Und die anderen Seiten im Abschnitt **Get Started** dieser Dokumentation für weitere Informationen.

Anforderungen für das NetApp Astra Control Python SDK

Das SDK verfügt über mehrere Voraussetzungen für die lokale Python-Umgebung. Beispiel: Sie müssen Python 3.8 oder höher verwenden. Darüber hinaus sind mehrere Python-Pakete erforderlich. Weitere Informationen finden Sie auf der GitHub Repository-Seite oder auf der Seite des PyPI-Pakets.

Zusammenfassung hilfreicher Ressourcen

Im Folgenden finden Sie einige Ressourcen, die Sie für den Einstieg benötigen.

- "PyPI: NetApp Astra Control Python SDK"
- "GitHub: NetApp/netapp-astra-Toolkits"
- "Docker: NetApp/astra-Toolkits"

Native Python

Bevor Sie beginnen

Python ist eine beliebte Entwicklungssprache bei der Datacenter-Automatisierung. Bevor Sie die nativen Funktionen von Python zusammen mit mehreren gängigen Paketen nutzen, müssen Sie die Umgebung und die erforderlichen Eingabedateien vorbereiten.

NetApp hat nicht nur direkt mit Python auf die Astra Control REST API zugegriffen, sondern bietet auch ein Toolkit-Paket, das die API abstrahiert und einige der Komplexität beseitigt. Siehe "NetApp Astra Control Python SDK" Finden Sie weitere Informationen.

Bereiten Sie die Umgebung vor

Im Folgenden werden die grundlegenden Konfigurationsanforderungen für die Ausführung der Python-Skripte beschrieben.

Python 3

Sie müssen die neueste Version von Python 3 installiert haben.

Weitere Bibliotheken

Die Bibliotheken **Requests** und **urllib3** müssen installiert sein. Sie können je nach Ihrer Umgebung Pip oder ein anderes Python Management Tool verwenden.

Netzwerkzugriff

Die Arbeitsstation, auf der die Skripte ausgeführt werden, muss Netzwerkzugriff haben und Astra Control erreichen können. Bei der Verwendung des Astra Control Service müssen Sie mit dem Internet verbunden sein und eine Verbindung zum Dienst unter herstellen können `https://astra.netapp.io`.

Identitätsinformationen

Sie benötigen ein gültiges Astra-Konto mit der Account-ID und dem API-Token. Siehe "Holen Sie sich ein API-Token" Finden Sie weitere Informationen.

Erstellen Sie die JSON-Eingabedateien

Die Python-Skripte basieren auf Konfigurationsinformationen in JSON-Eingabedateien. Im Folgenden finden Sie Beispieldateien.

Sie müssen die Proben entsprechend Ihrer Umgebung aktualisieren.

Identitätsinformationen

Die folgende Datei enthält das API-Token und das Astra-Konto. Sie müssen diese Datei mit der an Python-Skripte übergeben `-i` (Oder `--identity`) CLI-Parameter.

```
{
  "api_token": "kH4CA_uVIa8q9UuPzhJaAHaGlaR7-no901DkkrVjIXk=",
  "account_id": "5131dfdf-03a4-5218-ad4b-fe84442b9786"
}
```

Listen Sie die Apps auf

Mit dem folgenden Skript können Sie die Anwendungen für Ihr Astra-Konto auflisten.

Siehe "Bevor Sie beginnen" Beispiel für die erforderliche JSON-Eingabedatei.

```
#!/usr/bin/env python3
##-----------------------------------------------------------------------------
------
#
# Usage: python3 list_man_apps.py -i identity_file.json
#
# (C) Copyright 2022 NetApp, Inc.
#
# This sample code is provided AS IS, with no support or warranties of
# any kind, including but not limited for warranties of merchantability
# or fitness of any kind, expressed or implied. Permission to use,
# reproduce, modify and create derivatives of the sample code is granted
# solely for the purpose of researching, designing, developing and
# testing a software application product for use with NetApp products,
# provided that the above copyright notice appears in all copies and
# that the software application product is distributed pursuant to terms
# no less restrictive than those set forth herein.
#
##-----------------------------------------------------------------------------
------

import argparse
import json
import requests
import urllib3
import sys

# Global variables
api_token = ""
account_id = ""

def get_managed_apps():
    ''' Get and print the list of apps '''

    # Global variables
    global api_token
    global account_id

    # Create an HTTP session
    sess1 = requests.Session()
```

```
    # Suppress SSL unsigned certificate warning
    urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)

    # Create URL
    url1 = "https://astra.netapp.io/accounts/" + account_id +
"/k8s/v2/apps"

    # Headers and response output
    req_headers  = {}
    resp_headers = {}
    resp_data    = {}

    # Prepare the request headers
    req_headers.clear
    req_headers['Authorization'] = "Bearer " + api_token
    req_headers['Content-Type'] = "application/astra-app+json"
    req_headers['Accept'] = "application/astra-app+json"

    # Make the REST call
    try:
        resp1 = sess1.request('get', url1, headers=req_headers,
allow_redirects=True, verify=False)

    except requests.exceptions.ConnectionError:
        print("Connection failed")
        sys.exit(1)

    # Retrieve the output
    http_code = resp1.status_code
    resp_headers = resp1.headers

    # Print the list of apps
    if resp1.ok:
        resp_data = json.loads(resp1.text)
        items = resp_data['items']
        for i in items:
            print(" ")
            print("Name: " + i['name'])
            print("ID: " + i['id'])
            print("State: " + i['state'])
    else:
        print("Failed with HTTP status code: " + str(http_code))

    print(" ")
```

```
    # Close the session
    sess1.close()

    return

def read_id_file(idf):
    ''' Read the identity file and save values '''

    # Global variables
    global api_token
    global account_id

    with open(idf) as f:
        data = json.load(f)

    api_token = data['api_token']
    account_id = data['account_id']

    return

def main(args):
    ''' Main top level function '''

    # Global variables
    global api_token
    global account_id

    # Retrieve name of JSON input file
    identity_file = args.id_file

    # Get token and account
    read_id_file(identity_file)

    # Issue REST call
    get_managed_apps()

    return

def parseArgs():
        ''' Parse the CLI input parameters '''

        parser = argparse.ArgumentParser(description='Astra REST API -
List the apps',
                                add_help = True)
        parser.add_argument("-i", "--identity", action="store", dest
="id_file", default=None,
                                help='(Req) Name of the identity input file',
```

```
required=True)

        return parser.parse_args()

if __name__ == '__main__':
    ''' Begin here '''

    # Parse input parameters
    args = parseArgs()

    # Call main function
    main(args)
```

API-Referenz

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.

Die REST-API-Referenzdokumentation wird derzeit mit Astra Control bereitgestellt und ist online verfügbar.

Bevor Sie beginnen

Sie benötigen ein Konto für Astra Control Center oder Astra Control Service.

Schritte

1. Melden Sie sich mit Ihren Anmeldedaten im Astra an.

   Rufen Sie die folgende Website für den Astra Control Service auf: "https://astra.netapp.io"

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.
4. Geben Sie bei Aufforderung erneut Ihre Anmeldeinformationen für das Konto an.

Weitere Ressourcen

Auf weitere Ressourcen erhalten Sie Zugriff. Dort erhalten Sie weitere Informationen zu NetApp Cloud Services und Support sowie ZU allgemeinen REST- und Cloud-Konzepten.

Astra

- "Astra Control Center 22.08-Dokumentation"

  Dokumentation für die aktuelle Version der Astra Control Center-Software, die beim Kunden vor Ort eingesetzt wird.

- "Dokumentation des Astra Control Service"

  Dokumentation für die aktuelle Version der Astra Control Service-Software, die in der Public Cloud verfügbar ist.

- "Astra Trident-Dokumentation"

  Dokumentation für die aktuelle Version der Astra Trident Software, einem Open-Source-Storage-Orchestrator von NetApp.

- "Dokumentation der Astra-Familie"

  Zentraler Standort für den Zugriff auf die gesamte Astra Dokumentation für On-Premises- und Public-Cloud-Implementierungen.

NetApp Cloud-Ressourcen

- "NetApp BlueXP"

  Zentraler Standort für NetApp Cloud Lösungen.

- "NetApp Cloud Central Konsole"

  NetApp Cloud Central Service-Konsole mit Anmeldung.

- "NetApp Support"

  Sie erhalten Zugriff auf Tools für die Fehlerbehebung, Dokumentation und technische Support-Unterstützung.

REST- und Cloud-Konzepte

- PhD "Dissertation" Von Roy Fielding

  In dieser Publikation wurde das MODELL DER REST-Anwendungsentwicklung eingeführt und etabliert.

- "Auth0"

  Dies ist der Authentifizierungs- und Autorisierungsplattform-Service, der vom Astra-Service für den

Webzugriff genutzt wird.

- "RFC-Editor"

  Maßgebliche Quelle für Web- und Internet-Standards wird als Sammlung von eindeutig nummerierten RFC-Dokumenten gepflegt.

Frühere Versionen der Dokumentation Astra Control Automation

Die Dokumentation zur Automatisierung früherer Astra Control Versionen finden Sie unter den nachfolgenden Links.

- "Astra Control Automation 22.04 - Dokumentation"
- "Astra Control Automation 21.12 - Dokumentation"
- "Astra Control Automation 21.08 - Dokumentation"

Rechtliche Hinweise

Rechtliche Hinweise ermöglichen den Zugriff auf Copyright-Erklärungen, Marken, Patente und mehr.

Urheberrecht

"https://www.netapp.com/company/legal/copyright/"

Marken

NetApp, das NETAPP Logo und die auf der NetApp Markenseite aufgeführten Marken sind Marken von NetApp Inc. Andere Firmen- und Produktnamen können Marken der jeweiligen Eigentümer sein.

"https://www.netapp.com/company/legal/trademarks/"

Patente

Eine aktuelle Liste der NetApp Patente finden Sie unter:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Datenschutzrichtlinie

"https://www.netapp.com/company/legal/privacy-policy/"

Astra Control API-Lizenz

https://docs.netapp.com/us-en/astra-automation/media/astra-api-license.pdf