Infrastruktur-Workflows

Astra Automation

NetApp
March 07, 2024

Inhalt

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.
Cluster	Sie können Managed Kubernetes Cluster hinzufügen, damit Sie die enthaltenen Applikationen schützen und unterstützen können.
Clouds	Diese Workflows ermöglichen den Zugriff auf die Clouds, die über die Astra Control REST-API verfügbar sind.
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.

Identität und Zugriff

Listen Sie die Benutzer auf

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	/Accounts/{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": {}
}
```

Erstellen Sie einen Benutzer

Sie können einen Benutzer mit spezifischen Anmeldedaten und einer vordefinierten Rolle erstellen. Sie können optional auch den Zugriff des Benutzers auf bestimmte Namespaces beschränken.

1. Wählen Sie einen Benutzernamen

Führen Sie den Workflow aus "Benutzer auflisten" Und wählen Sie einen verfügbaren Namen aus, der derzeit nicht verwendet wird.

2. Erstellen Sie den Benutzer

Führen Sie den folgenden REST-API-Aufruf aus, um einen Benutzer zu erstellen. Nach erfolgreichem Abschluss des Anrufs ist der neue Benutzer noch nicht nutzbar.

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

JSON-Eingabebeispiel

```
{
  "type" :  "application/astra-user",
  "version" : "1.1",
  "firstName" : "John",
  "lastName" : "West",
  "email" : "jwest@example.com"
}
```

Beispiel für die Wellung

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

Beispiel für eine JSON-Ausgabe

```
{
    "metadata": {
        "creationTimestamp": "2022-11-20T17:23:15Z",
        "modificationTimestamp": "2022-11-20T17:23:15Z",
        "createdBy": "a20e91f3-2c49-443b-b240-615d940ec5f3",
        "labels": []
    },
    "type": "application/astra-user",
    "version": "1.2",
    "id": "d07dac0a-a328-4840-a216-12de16bbd484",
    "authProvider": "local",
    "authID": "jwest@example.com",
    "firstName": "John",
    "lastName": "West",
    "companyName": "",
    "email": "jwest@example.com",
    "postalAddress": {
        "addressCountry": "",
        "addressLocality": "",
        "addressRegion": "",
        "streetAddress1": "",
        "streetAddress2": "",
        "postalCode": ""
    },
    "state": "active",
    "sendWelcomeEmail": "false",
    "isEnabled": "true",
    "isInviteAccepted": "true",
    "enableTimestamp": "2022-11-20T17:23:15Z",
    "lastActTimestamp": ""
}
```


3. Wählen Sie optional die zulässigen Namespaces

Führen Sie den Workflow aus "Listen Sie die Namespaces auf" Und wählen Sie die Namespaces aus, auf die Sie den Zugriff beschränken möchten.

4. Binden Sie den Benutzer an eine Rolle

Führen Sie den folgenden REST-API-Aufruf durch, um den Benutzer an eine Rolle zu binden. Das Beispiel unten beschränkt den Namespace-Zugriff nicht. Siehe "Erweiterte RBAC mit Namespace-Granularität" Finden Sie weitere Informationen.

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

JSON-Eingabebeispiel

```
{
  "type" :  "application/astra-roleBinding",
  "version" : "1.1",
  "userID" : "d07dac0a-a328-4840-a216-12de16bbd484",
  "accountID" : "29e1f39f-2bf4-44ba-a191-5b84ef414c95",
  "role" : "viewer",
  "roleConstraints": [ "*" ]
}
```

Beispiel für die Wellung

```
curl --location -i --request POST
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/core/v1/roleBindings'
--header 'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>' --data
@JSONinput
```

5. Erstellen Sie eine Anmeldeinformation

Führen Sie den folgenden REST-API-Aufruf durch, um eine Berechtigung zu erstellen und sie dem Benutzer zuzuordnen. Dieses Beispiel verwendet ein Passwort, das als base64-Wert angegeben wird. Der `name` Eigenschaft sollte die ID des im vorherigen Schritt zurückgegebenen Benutzers enthalten. Die Eingabeeigenschaft `change` Muss auch in base64 kodiert werden und bestimmt, ob der Benutzer bei der ersten Anmeldung sein Passwort ändern muss (`true` Oder `false`).

> Dieser Schritt ist nur bei Astra Control Center-Implementierungen mit lokaler Authentifizierung erforderlich. Bei Implementierungen des Astra Control Center mit LDAP oder mit Astra Control Service sind dies nicht erforderlich.

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

JSON-Eingabebeispiel

```
{
  "type" :  "application/astra-credential",
  "version" : "1.1",
  "name" : "d07dac0a-a328-4840-a216-12de16bbd484",
  "keyType" : "passwordHash",
  "keyStore" : {
      "cleartext" : "TmV0QXBwMTIz",
      "change" : "ZmFsc2U="
  },
  "valid" : "true"
}
```

Beispiel für die Wellung

```
curl --location -i --request POST
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/core/v1/credentials'
--header 'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>' --data
@JSONinput
```

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.

Konfiguration über REST-API oder Web-Benutzeroberfläche

Die aktuelle Version von Astra Control Center unterstützt die Konfiguration der LDAP-Authentifizierung sowohl mit der Astra Control REST API als auch mit der Astra Web-Benutzeroberfläche.

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 "Online-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	/Accounts/{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	/Accounts/{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	/Accounts/{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	/Accounts/{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	/Accounts/{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.

Status	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	/Accounts/{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	/Accounts/{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	/Accounts/{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	/Accounts/{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	/Accounts/{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	/Accounts/{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	/Accounts/{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"
            }
        }
    ]
}
```

Fügen Sie mithilfe der Anmeldedaten einen Cluster hinzu

Sie können einen Cluster hinzufügen, sodass er vom Astra gemanagt werden kann. Ab dem Astra 22.11 können Sie ein Cluster sowohl mit dem Astra Control Center als auch mit dem Astra Control Service hinzufügen.

Das Hinzufügen eines Clusters ist nicht erforderlich, wenn ein Kubernetes-Service von einem der wichtigsten Cloud-Provider verwendet wird (AKS, EKS, GKE).

1. Holen Sie sich die kubeconfig-Datei

Sie benötigen eine Kopie der **kubconfig**-Datei von Ihrem Kubernetes-Administrator oder -Dienst.

2. Bereiten Sie die kubeconfig Datei

Vor der Verwendung der Datei **kubeconfig** sollten Sie die folgenden Vorgänge durchführen:

Konvertieren Sie die Datei aus dem YAML-Format in JSON

Wenn Sie die kubeconfg-Datei erhalten, die als YAML formatiert ist, müssen Sie sie in JSON konvertieren.

JSON in base64 kodieren

Sie müssen die JSON-Datei in base64 kodieren.

Beispiel

Hier ist ein Beispiel dafür, wie die Datei kubeconfig von YAML nach JSON konvertiert und dann in base64 verschlüsselt wird:

```
yq -o=json ~/.kube/config | base64
```

3. Wählen Sie die Wolke

Führen Sie den Workflow aus "Clouds auflisten" Und wählen Sie die Cloud aus, der der Cluster hinzugefügt werden soll.

Die einzige Cloud, die Sie auswählen können, ist die **private** Cloud.

4. Erstellen Sie eine Anmeldedaten

Führen Sie den folgenden REST-API-Aufruf durch, um mithilfe der kubeconfig-Datei eine Anmeldedaten zu erstellen.

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

JSON-Eingabebeispiel

```
{
  "type" :  "application/astra-credential",
  "version" : "1.1",
  "name" : "Cloud One",
  "keyType" : "kubeconfig",
  "keyStore" : {
    "base64": encoded_kubeconfig
  },
  "valid" : "true"
}
```

Beispiel für die Wellung

```
curl --location -i --request POST
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/core/v1/credentials'
--header 'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>' --data
@JSONinput
```

5. Fügen Sie den Cluster hinzu

Führen Sie den folgenden REST-API-Aufruf durch, um das Cluster zur Cloud hinzuzufügen. Der Wert des `credentialID` Das Eingabefeld wird vom REST-API-Aufruf im vorherigen Schritt abgerufen.

HTTP-Methode	Pfad
POST	/Accounts/{Account_id}/Topology/v1/Clouds/{Cloud_id}/Cluster

JSON-Eingabebeispiel

```
{
  "type" :  "application/astra-cluster",
  "version" : "1.1",
  "credentialID": credential_id
}
```

Beispiel für die Wellung

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

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	/Accounts/{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>'
```

Verwalten eines Clusters

Sie können ein Kubernetes-Cluster so managen, dass die Datensicherung durchgeführt werden kann.

1. Wählen Sie den zu verwaltenden Cluster aus

Führen Sie den Workflow aus "Listen Sie Cluster auf" Und wählen Sie das gewünschte Cluster aus. Das Hotel `managedState` Des Clusters muss sein `unmanaged`.

2. Wählen Sie optional die Speicherklasse aus

Führen Sie optional den Workflow aus "Auflisten von Speicherklassen" Und wählen Sie die gewünschte Storage-Klasse aus.

> Wenn Sie beim Aufruf zum Verwalten des Clusters keine Storage-Klasse anbieten, wird die standardmäßige Storage-Klasse verwendet.

3. Verwalten Sie den Cluster

Führen Sie den folgenden REST-API-Aufruf durch, um das Cluster zu verwalten.

HTTP-Methode	Pfad
POST	/Accounts/{Account_id}/Topology/v1/manageClusters

JSON-Eingabebeispiel

```
{
  "type": "application/astra-managedCluster",
  "version": "1.0",
  "id": "d0fdf455-4330-476d-bb5d-4d109714e07d"
}
```

Beispiel für die Wellung

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

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	/Accounts/{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	/Accounts/{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	/Accounts/{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	/Accounts/{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"
    }
  ]
}
```


Aktivieren Sie dynamische ANF-Pools für selbst gemanagte Cluster

Wenn Sie eine gemanagte App in einem privaten On-Premises-Cluster mit einem ANF-Storage-Back-End sichern, müssen Sie die Funktion Dynamic ANF Pools aktivieren. Dazu wird eine Abonnement-ID zur Verfügung gestellt, die beim erweitern und Verkleinern der Kapazitäts-Pools verwendet wird.

Dynamic ANF Pools ist eine Funktion der von Astra gemanagten Applikationen, die ein Azure NetApp Files (ANF) Storage-Back-End verwenden. Beim Backup dieser Applikationen erweitert und schließt Astra automatisch die Kapazitätspools, zu denen die persistenten Volumes gehören, um den Faktor 1.5. Dadurch wird sichergestellt, dass genügend Speicherplatz für das Backup zur Verfügung steht, ohne dass eine zusätzliche permanente Gebühr entsteht. Siehe "Backups von Azure-Applikationen" Finden Sie weitere Informationen.

1. Fügen Sie die Azure-Abonnement-ID hinzu

Führen Sie den folgenden REST-API-Aufruf aus.

Sie müssen das JSON-Eingabebeispiel entsprechend Ihrer Umgebung aktualisieren, einschließlich der Abonnement-ID und dem base64-Wert für den Service-Prinzipal.

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

JSON-Eingabebeispiel

```
{
  "keyStore": {
    "privKey": "SGkh",
    "pubKey": "UGhpcyCpcyBhbiBleGFtcGxlLg==",
    "base64":
"fwogICAgJmFwcElkIjogIjY4ZmSiODFiLTY0YWYtNDdjNC04ZjUzLWE2NDdlZTUzMGZkZCIsC
iAgICAiZGlzcGxheU5hbWUiOiAic3AtYXN0cmEtZGV2LXFhIiwKICAgICJuYW1lIjogImh0dHA
6Ly9zcC1hc3RyYS1kZXYtcWEiLAogICAgInBhc3N3b3JkIjogIllLQThRfk9IVVJkZWZYM0pST
WJlLnpUeFBleVE0UnNwTG9DcUJjazAiLAogICAgInRlbmFudCI6ICIwMTFjZGY2Yy03NTEyLTQ
3MDUtYjI0ZS03NzIxYWZkOGNhMzciLAogICAgInN1YnNjcmlwdGlvbklkIjogImIyMDAxNTVmL
TAwMWEtNDNiZS04N2JlLTNlZGRlODNhY2VmNCIKfQ=="
  },
  "name": "myCert",
  "type": "application/astra-credential",
  "version": "1.1",
  "metadata": {
    "labels": [
      {
        "name": "astra.netapp.io/labels/read-only/credType",
        "value": "service-account"
      },
      {
        "name": "astra.netapp.io/labels/read-only/cloudName",
        "value": "OCP"
      },
      {
        "name": "astra.netapp.io/labels/read-only/azure/subscriptionID",
        "value": "b212156f-001a-43be-87be-3edde83acef5"
      }
    ]
  }
}
```

Beispiel für die Wellung

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

2. Fügen Sie bei Bedarf einen Eimer hinzu

Sie sollten bei Bedarf der verwalteten Anwendung einen Bucket hinzufügen.

3. Nehmen Sie ein Backup der verwalteten App

Führen Sie den Workflow aus "Backup für eine Anwendung erstellen". Der Kapazitäts-Pool, in dem das ursprüngliche persistente Volume vorhanden ist, wird automatisch erweitert oder verkleinert.

4. Überprüfen Sie das Ereignisprotokoll

Aktivitätsereignisse werden während des Backups protokolliert. Führen Sie den Workflow aus "Listen Sie die Benachrichtigungen auf" Um die Nachrichten anzuzeigen.