



LDAP-Konfiguration

Astra Automation

NetApp
December 01, 2023

Inhalt

- LDAP-Konfiguration 1
 - Vorbereiten der LDAP-Konfiguration 1
 - Konfigurieren Sie Astra für die Verwendung eines LDAP-Servers 3
 - Fügen Sie LDAP-Einträge zum Astra hinzu 12
 - Deaktivieren und Zurücksetzen von LDAP 18

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 Konfigurationsoptionen, 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 Group2, 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 Konfigurationaufgabe 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": "LS0tLS1CRUdJTlBDRVJUSUZJQ0FURS0tLS0tCk1JSUMyVEN",
  "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": "dWlkPWFkbWluLG91PXM5c3RlbQ==",
    "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=name%20eq%20'astra.account.ldap'&include=name,id' --header 'Accept: */*'
--header 'Authorization: Bearer <API_TOKEN>'

```

Beispiel für JSON-Antwort

```

{
  "items": [
    ["astra.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 <code>currentConfig</code> in der Antwort Matches <code>desiredConfig</code> .
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.

Copyright-Informationen

Copyright © 2023 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

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

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

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

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

Markeninformationen

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