Configuration LDAP

Astra Automation 22.08

NetApp
February 20, 2023

Table des matières

Configuration LDAP

Préparation à la configuration LDAP

Vous pouvez intégrer Astra Control Center avec un serveur LDAP (Lightweight Directory Access Protocol) pour effectuer l'authentification pour certains utilisateurs Astra. LDAP est un protocole standard de l'industrie pour l'accès aux informations d'annuaires distribués et un choix populaire pour l'authentification d'entreprise.

Informations associées

- "Spécification technique LDAP feuille de route"
- "LDAP version 3"

Aperçu du processus de mise en œuvre

À un niveau élevé, il existe plusieurs étapes à suivre pour configurer un serveur LDAP afin de fournir une authentification aux utilisateurs d'Astra.

> Bien que les étapes présentées ci-dessous se trouvent dans une séquence, vous pouvez dans certains cas les exécuter dans un ordre différent. Par exemple, vous pouvez définir les utilisateurs et les groupes Astra avant de configurer le serveur LDAP.

1. Révision "Exigences et restrictions" connaître les options, les exigences et les limites.
2. Sélectionnez un serveur LDAP et les options de configuration souhaitées (y compris la sécurité).
3. Exécutez le flux de travail "Configurez Astra pour qu'il utilise un serveur LDAP" Pour intégrer Astra avec le serveur LDAP.
4. Vérifiez les utilisateurs et les groupes du serveur LDAP pour vous assurer qu'ils sont correctement définis.
5. Exécutez le flux de travail approprié dans "Ajoutez des entrées LDAP à Astra" Identifier les utilisateurs à authentifier à l'aide de LDAP.

Exigences et restrictions

Nous vous recommandons de consulter les éléments essentiels de configuration Astra présentés ci-dessous, y compris les limites et les options de configuration, avant de configurer Astra pour utiliser LDAP pour l'authentification.

Uniquement pris en charge avec Astra Control Center

La plateforme Astra Control propose deux modèles de déploiement. L'authentification LDAP est prise en charge uniquement avec les déploiements d'Astra Control Center.

Configuration de l'API REST uniquement

La version actuelle d'Astra Control Center prend uniquement en charge la configuration de l'authentification LDAP à l'aide de l'API REST Astra Control. Un aspect important de cette limitation est que les utilisateurs LDAP ne sont pas affichés dans l'onglet utilisateurs de l'interface Web Astra. Ils sont disponibles via l'API REST au niveau du terminal `../core/v1/users`.

Serveur LDAP requis

Vous devez disposer d'un serveur LDAP pour accepter et traiter les demandes d'authentification Astra.

Microsoft Active Directory est pris en charge avec la version actuelle d'Astra Control Center.

Connexion sécurisée au serveur LDAP

Lors de la configuration du serveur LDAP dans Astra, vous pouvez éventuellement définir une connexion sécurisée. Dans ce cas, un certificat est nécessaire pour le protocole LDAPS.

Configurer des utilisateurs ou des groupes

Vous devez sélectionner les utilisateurs à authentifier à l'aide de LDAP. Pour ce faire, vous pouvez identifier les utilisateurs individuels ou un groupe d'utilisateurs. Les comptes doivent être définis au niveau du serveur LDAP. Elles doivent également être identifiées dans Astra (type LDAP) qui permet de transférer les demandes d'authentification vers LDAP.

Contrainte de rôle lors de la liaison d'un utilisateur ou d'un groupe

Avec la version actuelle d'Astra Control Center, la seule valeur prise en charge pour `roleConstraint` est "*". Cela indique que l'utilisateur n'est pas limité à un ensemble limité d'espaces de noms et qu'il peut y accéder tous. Voir "Ajoutez des entrées LDAP à Astra" pour en savoir plus.

Informations d'identification LDAP

Les informations d'identification utilisées par LDAP incluent le nom d'utilisateur (adresse e-mail) et le mot de passe associé.

Adresses e-mail uniques

Toutes les adresses e-mail agissant comme noms d'utilisateur dans un déploiement Astra Control Center doivent être uniques. Vous ne pouvez pas ajouter un utilisateur LDAP avec une adresse e-mail déjà définie pour Astra. Si un e-mail en double existe, vous devez d'abord le supprimer d'Astra. Voir "Supprimer des utilisateurs" Sur le site de documentation Astra Control Center pour plus d'informations.

Vous pouvez éventuellement définir d'abord les utilisateurs et les groupes LDAP

Vous pouvez ajouter les utilisateurs et groupes LDAP au Centre de contrôle Astra même s'ils n'existent pas encore dans LDAP ou si le serveur LDAP n'est pas configuré. Cela vous permet de préconfigurer les utilisateurs et les groupes avant de configurer le serveur LDAP.

Utilisateur défini dans plusieurs groupes LDAP

Si un utilisateur LDAP appartient à plusieurs groupes LDAP et que des rôles différents ont été attribués aux groupes dans Astra, le rôle effectif de l'utilisateur lors de l'authentification sera le plus privilégié. Par exemple, si un utilisateur est affecté à l' `viewer` rôle avec groupe1 mais a le `member` rôle dans le groupe 2, le rôle de l'utilisateur serait `member`. Ceci est basé sur la hiérarchie utilisée par Astra (la plus haute à la plus basse) :

- Propriétaire
- Admin
- Membre
- Visualiseur

Synchronisation périodique du compte

Astra synchronise ses utilisateurs et groupes avec le serveur LDAP environ toutes les 60 secondes. Par conséquent, si un utilisateur ou un groupe est ajouté à LDAP ou supprimé, il peut prendre jusqu'à une minute avant qu'il soit disponible dans Astra.

Désactivation et réinitialisation de la configuration LDAP

Avant de tenter de réinitialiser la configuration LDAP, vous devez d'abord désactiver l'authentification LDAP. De même, pour modifier le serveur LDAP (`connectionHost`), vous devez effectuer les deux opérations. Voir

"Désactivez et réinitialisez LDAP" pour en savoir plus.

Paramètres de l'API REST

Les workflows de configuration LDAP appellent l'API REST pour accomplir des tâches spécifiques. Chaque appel API peut inclure des paramètres d'entrée comme indiqué dans les échantillons fournis. Voir "Référence API" pour plus d'informations sur la localisation de la documentation de référence.

Configurez Astra pour qu'il utilise un serveur LDAP

Vous devez sélectionner un serveur LDAP et configurer Astra pour qu'il utilise le serveur en tant que fournisseur d'authentification. La tâche de configuration comprend les étapes décrites ci-dessous. Chaque étape inclut un appel d'API REST unique.

1. Ajoutez un certificat CA

Effectuez l'appel d'API REST suivant pour ajouter un certificat d'autorité de certification à Astra.

Cette étape est facultative et requise uniquement si vous voulez qu'Astra et le LDAP communiquent via un canal sécurisé à l'aide de LDAPS.

Méthode HTTP	Chemin
POST	/account/{account_id}/core/v1/certificats

Exemple d'entrée JSON

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

Notez les informations suivantes concernant les paramètres d'entrée :

- `cert` Est une chaîne JSON contenant un certificat au format PKCS-11 codé en base64 (codé PEM).
- `isSelfSigned` doit être réglé sur `true` si le certificat est auto-signé. La valeur par défaut est `false`.

Exemple de boucle

```
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>'
```

Exemple de réponse JSON


```
{
  "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. Ajoutez les informations d'identification de liaison

Effectuez l'appel d'API REST suivant pour ajouter les informations d'identification de liaison.

Méthode HTTP	Chemin
POST	/account/{account_id}/core/v1/credentials

Exemple d'entrée JSON

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

Notez les informations suivantes concernant les paramètres d'entrée :

- `bindDn` et `password` Sont les informations d'identification de liaison codées en base64 de l'utilisateur admin LDAP qui peut se connecter et rechercher dans le répertoire LDAP. `bindDn` Est l'adresse e-mail de l'utilisateur LDAP.

Exemple de boucle

```
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>'
```

Exemple de réponse JSON

```
{
    "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"
    }
}
```


Noter les paramètres de réponse suivants :

- Le `id` des informations d'identification sont utilisées dans les étapes suivantes du flux de travail.

3. Récupérez l'UUID du paramètre LDAP

Exécutez l'appel de l'API REST suivant pour récupérer l'UUID du `astra.account.ldap` Réglage inclus avec le centre de contrôle Astra.

> L'exemple curl ci-dessous utilise un paramètre de requête pour filtrer la collection de paramètres. Vous pouvez à la place supprimer le filtre pour obtenir tous les paramètres, puis rechercher `astra.account.ldap`.

Méthode HTTP	Chemin
OBTENEZ	/account/{account_id}/core/v1/settings

Exemple de boucle

```
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>'
```

Exemple de réponse JSON

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

4. Mettez à jour le paramètre LDAP

Effectuez l'appel d'API REST suivant pour mettre à jour le paramètre LDAP et terminer la configuration. Utilisez le `id` Valeur de l'appel API précédent pour le `<SETTING_ID>` Valeur dans le chemin d'accès à l'URL ci-dessous.

Vous pouvez d'abord lancer une demande GET pour le paramètre spécifique afin de voir le schéma de configuration. Ceci fournira plus d'informations sur les champs requis dans la configuration.

Méthode HTTP	Chemin
EN	/account/{account_id}/core/v1/settings/{setting_id}

Exemple d'entrée JSON

```
{
  "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"
    }
}
```

Notez les informations suivantes concernant les paramètres d'entrée :

- `isEnabled` doit être réglé sur `true` ou une erreur peut se produire.

- `credentialId` est l'id des informations d'identification de liaison créées précédemment.
- `secureMode` doit être réglé sur `LDAP` ou `LDAPS` en fonction de votre configuration à l'étape précédente.
- Seul Active Directory est pris en charge en tant que fournisseur.

Exemple de boucle

```
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>'
```

Si l'appel a réussi, la réponse HTTP 204 est renvoyée.

5. Récupérez le paramètre LDAP

Vous pouvez éventuellement effectuer l'appel d'API REST suivant pour récupérer les paramètres LDAP et confirmer la mise à jour.

Méthode HTTP	Chemin
OBTENEZ	/account/{account_id}/core/v1/settings/{setting_id}

Exemple de boucle

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

Exemple de réponse JSON


```
{
  "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": {}
}
```

Localisez le `state` champ de la réponse qui contient l'une des valeurs du tableau ci-dessous.

État	Description
en attente	Le processus de configuration est toujours actif et n'est pas encore terminé.
valide	La configuration a été effectuée avec succès et `currentConfig` la réponse correspond `desiredConfig`.
erreur	Le processus de configuration LDAP a échoué.

Ajoutez des entrées LDAP à Astra

Après avoir configuré LDAP en tant que fournisseur d'authentification pour Astra Control Center, vous pouvez sélectionner les utilisateurs LDAP qu'Astra authentifie à l'aide des informations d'identification LDAP. Chaque utilisateur doit avoir un rôle dans Astra avant d'avoir accès à Astra via l'API REST Astra Control.

Il existe deux façons de configurer Astra pour affecter des rôles. Choisissez celle qui convient le mieux à votre environnement.

- "Ajouter et lier un utilisateur individuel"
- "Ajouter et lier un groupe"

Les informations d'identification LDAP se présentent sous la forme d'un nom d'utilisateur sous la forme d'une adresse e-mail et du mot de passe LDAP associé.

Ajouter et lier un utilisateur individuel

Vous pouvez attribuer un rôle à chaque utilisateur Astra qui est utilisé après l'authentification LDAP. Ceci est approprié lorsqu'il y a un petit nombre d'utilisateurs et que chacun peut avoir des caractéristiques administratives différentes.

1. Ajoutez un utilisateur

Effectuez l'appel d'API REST suivant pour ajouter un utilisateur à Astra et indiquer que LDAP est le fournisseur d'authentification.

Méthode HTTP	Chemin
POST	/account/{account_id}/core/v1/users

Exemple d'entrée JSON

```
{
  "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"
}
```

Notez les informations suivantes concernant les paramètres d'entrée :

- Les paramètres suivants sont requis :
  - `authProvider`
  - `authID`
  - `email`
- `authID` Est le nom distinctif (DN) de l'utilisateur dans LDAP
- `email` Doit être unique pour tous les utilisateurs définis dans Astra

Si le `email` La valeur n'est pas unique, une erreur se produit et un code d'état HTTP 409 est renvoyé dans la réponse.

Exemple de boucle

```
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>'
```

Exemple de réponse JSON

```
{
  "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. Ajoutez une liaison de rôle pour l'utilisateur

Effectuez l'appel de l'API REST suivant pour lier l'utilisateur à un rôle spécifique. Vous devez créer l'UUID de l'utilisateur à l'étape précédente.

Méthode HTTP	Chemin
POST	/Account/{account_ID}/core/v1/roleliaisons

Exemple d'entrée JSON

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

Notez les informations suivantes concernant les paramètres d'entrée :

- Valeur utilisée ci-dessus pour `roleConstraint` Est la seule option disponible pour la version actuelle d'Astra. Il indique que l'utilisateur n'est pas limité à un ensemble limité d'espaces de noms et peut y accéder tous.

Exemple de boucle

```
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>'
```

Exemple de réponse JSON

```
{
  "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": ["*"]
}
```

Noter les éléments suivants concernant les paramètres de réponse :

- La valeur `user` pour le `principalType` champ indique que la liaison du rôle a été ajoutée pour un utilisateur (et non pour un groupe).

Ajouter et lier un groupe

Vous pouvez affecter un rôle à un groupe Astra qui est utilisé après l'authentification LDAP. Ceci est approprié lorsqu'il y a un grand nombre d'utilisateurs et que chacun peut avoir des caractéristiques administratives similaires.

1. Ajoutez un groupe

Effectuez l'appel d'API REST suivant pour ajouter un groupe à Astra et indiquer que LDAP est le fournisseur d'authentification.

Méthode HTTP	Chemin
POST	/account/{account_id}/core/v1/groupes

Exemple d'entrée JSON

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

Notez les informations suivantes concernant les paramètres d'entrée :

- Les paramètres suivants sont requis :
  - `authProvider`
  - `authID`

Exemple de boucle

```
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>'
```

Exemple de réponse JSON

```
{
  "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. Ajoutez une liaison de rôle pour le groupe

Effectuez l'appel d'API REST suivant pour lier le groupe à un rôle spécifique. Vous devez créer l'UUID du groupe à l'étape précédente. Les utilisateurs qui sont membres du groupe pourront se connecter à Astra une fois que LDAP aura effectué l'authentification.

Méthode HTTP	Chemin
POST	/Account/{account_ID}/core/v1/roleliaisons

Exemple d'entrée JSON

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

Notez les informations suivantes concernant les paramètres d'entrée :

- Valeur utilisée ci-dessus pour `roleConstraint` Est la seule option disponible pour la version actuelle d'Astra. Il indique que l'utilisateur n'est pas limité à certains espaces de noms et peut y accéder tous.

Exemple de boucle

```
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>'
```

Exemple de réponse JSON

```
{
  "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": ["*"]
}
```

Noter les éléments suivants concernant les paramètres de réponse :

- La valeur `group` pour le `principalType` champ indique que la liaison de rôle a été ajoutée pour un groupe (et non pour un utilisateur).

Désactivez et réinitialisez LDAP

Il existe deux tâches administratives facultatives, bien que liées, que vous pouvez effectuer selon vos besoins pour un déploiement de centre de contrôle Astra. Vous pouvez désactiver globalement l'authentification LDAP et réinitialiser la configuration LDAP.

Les deux tâches de flux de travail requièrent l'ID pour le `astra.account.ldap` Réglage Astra. Les détails sur la récupération de l'ID de paramètre sont inclus dans **configurer le serveur LDAP**. Voir "Récupère l'UUID du paramètre LDAP" pour en savoir plus.

- "Désactivez l'authentification LDAP"
- "Réinitialisez la configuration de l'authentification LDAP"

Désactivez l'authentification LDAP

Vous pouvez effectuer l'appel d'API REST suivant pour désactiver globalement l'authentification LDAP pour un déploiement Astra spécifique. L'appel met à jour le `astra.account.ldap` réglage et `isEnabled` la valeur est définie sur `false`.

Méthode HTTP	Chemin
EN	/account/{account_id}/core/v1/settings/{setting_id}

Exemple d'entrée JSON

```
{
  "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>'
```

Si l'appel a réussi, le `HTTP 204` la réponse est renvoyée. Vous pouvez éventuellement récupérer à nouveau les paramètres de configuration pour confirmer la modification.

Réinitialisez la configuration de l'authentification LDAP

Vous pouvez effectuer l'appel d'API REST suivant pour déconnecter Astra du serveur LDAP et réinitialiser la configuration LDAP dans Astra. L'appel met à jour le `astra.account.ldap` réglage et valeur de `connectionHost` est effacé.

La valeur de `isEnabled` doit également être défini sur `false`. Vous pouvez soit définir cette valeur avant d'effectuer l'appel de réinitialisation, soit dans le cadre de l'appel de réinitialisation. Dans le deuxième cas, `connectionHost` doit être effacé et `isEnabled` défini sur false lors du même appel de réinitialisation.

Il s'agit d'une opération perturbatrice et vous devez procéder avec précaution. Elle supprime tous les utilisateurs et groupes LDAP importés. Il supprime également tous les utilisateurs, groupes et liaisons Astra (type LDAP) associés que vous avez créés dans Astra Control Center.

Méthode HTTP	Chemin
EN	/account/{account_id}/core/v1/settings/{setting_id}

Exemple d'entrée JSON

```
{
  "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"
    }
}
```

Notez ce qui suit :

- Pour modifier le serveur LDAP, vous devez à la fois désactiver et réinitialiser la modification LDAP `connectHost` à une valeur nulle comme indiqué dans l'exemple ci-dessus.

```
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>'
```

Si l'appel a réussi, le `HTTP 204` la réponse est renvoyée. Vous pouvez éventuellement récupérer à nouveau la configuration pour confirmer la modification.

Informations sur le copyright

Informations sur les marques commerciales