Configuración de LDAP

Astra Automation

NetApp
December 01, 2023

Tabla de contenidos

Configuración de LDAP 1
Prepare la configuración de LDAP 1
Configure Astra para que utilice un servidor LDAP 3
Agregue entradas LDAP a Astra 11
Deshabilite y restablezca LDAP 17

Configuración de LDAP

Prepare la configuración de LDAP

Opcionalmente, puede integrar Astra Control Center con un servidor Lightweight Directory Access Protocol (LDAP) para realizar la autenticación de determinados usuarios de Astra. LDAP es un protocolo estándar del sector para acceder a información de directorio distribuida y una opción muy popular para la autenticación empresarial.

Información relacionada

- "Hoja de ruta de especificación técnica de LDAP"
- "LDAP, versión 3"

Descripción general del proceso de implementación

En un nivel superior, hay varios pasos que debe realizar para configurar un servidor LDAP con el fin de proporcionar autenticación a los usuarios de Astra.

> Aunque los pasos que se muestran a continuación están en una secuencia, en algunos casos puede realizarlos en un orden diferente. Por ejemplo, puede definir los usuarios y grupos de Astra antes de configurar el servidor LDAP.

1. Revisar "Requisitos y limitaciones" para comprender las opciones, requisitos y limitaciones.
2. Seleccione un servidor LDAP y las opciones de configuración deseadas (incluida la seguridad).
3. Realice el flujo de trabajo "Configure Astra para que utilice un servidor LDAP" Integrar Astra con el servidor LDAP.
4. Revise los usuarios y grupos del servidor LDAP para asegurarse de que están definidos correctamente.
5. Ejecute el flujo de trabajo adecuado en "Agregue entradas LDAP a Astra" Identificar los usuarios que se autenticarán mediante LDAP.

Requisitos y limitaciones

Antes de configurar Astra para utilizar LDAP para la autenticación, debe revisar los aspectos básicos de configuración de Astra que se presentan a continuación, incluidas las limitaciones y las opciones de configuración.

Sólo compatible con Astra Control Center

La plataforma Astra Control proporciona dos modelos de puesta en marcha. La autenticación LDAP solo es compatible con las implementaciones de Astra Control Center.

Configuración mediante la API DE REST o la interfaz de usuario web

La versión actual de Astra Control Center admite la configuración de la autenticación LDAP mediante la API REST de Astra Control y la interfaz de usuario web de Astra.

Se requiere servidor LDAP

Debe tener un servidor LDAP para aceptar y procesar las solicitudes de autenticación Astra. Active Directory de Microsoft es compatible con la versión actual de Astra Control Center.

Conexión segura con el servidor LDAP

Al configurar el servidor LDAP en Astra, puede definir opcionalmente una conexión segura. En este caso, se necesita un certificado para el protocolo LDAPS.

Configurar usuarios o grupos

Debe seleccionar los usuarios para autenticarse con el LDAP. Puede hacerlo identificando los usuarios individuales o un grupo de usuarios. Las cuentas se deben definir en el servidor LDAP. También deben identificarse en Astra (tipo LDAP) que permite que las solicitudes de autenticación se reenvíen a LDAP.

Restricción de función al enlazar un usuario o un grupo

Con la versión actual de Astra Control Center, el único valor admitido para `roleConstraint` es "*". Esto indica que el usuario no está restringido a un conjunto limitado de espacios de nombres y que puede acceder a todos ellos. Consulte "Agregue entradas LDAP a Astra" si quiere más información.

Credenciales de LDAP

Entre las credenciales que utiliza LDAP, se incluyen el nombre de usuario (dirección de correo electrónico) y la contraseña asociada.

Direcciones de correo electrónico exclusivas

Todas las direcciones de correo electrónico que actúen como nombres de usuario en una implementación de Astra Control Center deben ser únicas. No puede agregar un usuario LDAP con una dirección de correo electrónico que ya esté definida en Astra. Si existe un correo electrónico duplicado, primero debe eliminarlo de Astra. Consulte "Quitar usuarios" En el sitio de documentación de Astra Control Center para obtener más información.

Opcionalmente, defina primero los grupos y usuarios LDAP

Puede agregar los usuarios y grupos LDAP a Astra Control Center aunque aún no existan en LDAP o si no se ha configurado el servidor LDAP. Esto permite preconfigurar los usuarios y grupos antes de configurar el servidor LDAP.

Un usuario definido en varios grupos LDAP

Si un usuario LDAP pertenece a varios grupos LDAP y se han asignado roles diferentes en Astra a los grupos, el rol efectivo del usuario al autenticarse será el más privilegiado. Por ejemplo, si se asigna un usuario el `viewer` rol con group1 pero tiene la `member` función en grupo2, el rol del usuario sería `member`. Esto se basa en la jerarquía utilizada por Astra (de la más alta a la más baja):

- Propietario
- Admin
- Miembro
- Visionador

Sincronización periódica de cuentas

Astra sincroniza los usuarios y grupos de TI con el servidor LDAP aproximadamente cada 60 segundos. Por lo tanto, si se agrega o elimina un usuario o grupo de LDAP, puede tardar hasta un minuto en estar disponible en Astra.

Deshabilitar y restablecer la configuración de LDAP

Antes de intentar restablecer la configuración de LDAP, primero debe deshabilitar la autenticación LDAP. Además, para cambiar el servidor LDAP (`connectionHost`), debe realizar ambas operaciones. Consulte "Deshabilite y restablezca LDAP" si quiere más información.

Parámetros de la API de REST

Los flujos de trabajo de configuración LDAP realizan llamadas a la API DE REST para realizar las tareas específicas. Cada llamada API puede incluir parámetros de entrada, como se muestra en las muestras proporcionadas. Consulte "Referencia de API en línea" para obtener información sobre cómo localizar la documentación de referencia.

Configure Astra para que utilice un servidor LDAP

Debe seleccionar un servidor LDAP y configurar Astra para utilizar el servidor como proveedor de autenticación. La tarea de configuración consta de los pasos descritos a continuación. Cada paso incluye una única llamada API DE REST.

1. Añadir un certificado de CA

Realice la siguiente llamada a la API DE REST para añadir un certificado de CA a Astra.

Este paso es opcional y solo es necesario si desea que Astra y LDAP se comuniquen a través de un canal seguro mediante LDAPS.

Método HTTP	Ruta
PUBLICAR	/accounts/{account_id}/core/v1/certificates

Ejemplo de entrada JSON

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

Tenga en cuenta lo siguiente acerca de los parámetros de entrada:

- `cert` Es una cadena JSON que contiene un certificado con formato PKCS-11 codificado en base64 (codificado en PEM).
- `isSelfSigned` se debe establecer en `true` si el certificado está autofirmado. El valor predeterminado es `false`.

Ejemplo de curl

```
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>'
```

Ejemplo de respuesta 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. Añada las credenciales de enlace

Ejecute la siguiente llamada API de REST para añadir las credenciales de enlace.

Método HTTP	Ruta
PUBLICAR	/accounts/{account_id}/core/v1/credenciales

Ejemplo de entrada JSON

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

Tenga en cuenta lo siguiente acerca de los parámetros de entrada:

- `bindDn` y.. `password` Son las credenciales de enlace codificadas base64 del usuario administrador LDAP que puede conectarse y buscar en el directorio LDAP. `bindDn` Es la dirección de correo electrónico del usuario LDAP.

Ejemplo de curl

```
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>'
```

Ejemplo de respuesta 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"
    }
}
```

Tenga en cuenta los siguientes parámetros de respuesta:

- La `id` de la credencial se utiliza en los pasos posteriores del flujo de trabajo.

3. Recupere el UUID de la configuración LDAP

Realice la siguiente llamada API DE REST para recuperar el UUID del `astra.account.ldap` Ajuste que se incluye con Astra Control Center.

> ⓘ El ejemplo curl que se muestra a continuación utiliza un parámetro de consulta para filtrar la colección de ajustes. En su lugar, puede quitar el filtro para obtener todos los ajustes y, a continuación, buscar `astra.account.ldap`.

Método HTTP	Ruta
OBTENGA	/accounts/{account_id}/core/v1/settings

Ejemplo de curl

```
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>'
```

Ejemplo de respuesta JSON

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

4. Actualice la configuración de LDAP

Realice la siguiente llamada a la API DE REST para actualizar la configuración de LDAP y completar la configuración. Utilice la `id` Valor de la llamada de API anterior para `<SETTING_ID>` Valor en la ruta de dirección URL a continuación.

> Puede emitir primero una solicitud GET para la configuración específica para ver el esquema configSchema. Esto proporcionará más información acerca de los campos requeridos en la configuración.

Método HTTP	Ruta
PUESTO	/accounts/{account_id}/core/v1/settings/{setting_id}

Ejemplo de entrada 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"
    }
}
```

Tenga en cuenta lo siguiente acerca de los parámetros de entrada:

- `isEnabled` se debe establecer en `true` o se puede producir un error.
- `credentialId` es el id de la credencial de enlace creada anteriormente.

- `secureMode` se debe establecer en `LDAP` o. `LDAPS` según la configuración del paso anterior.
- Sólo se admite "Active Directory" como proveedor.

Ejemplo de curl

```
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 la llamada se realiza correctamente, se devuelve la respuesta HTTP 204.

5. Recupere el ajuste LDAP

De forma opcional, puede realizar la siguiente llamada API DE REST para recuperar la configuración de LDAP y confirmar la actualización.

Método HTTP	Ruta
OBTENGA	/accounts/{account_id}/core/v1/settings/{setting_id}

Ejemplo de curl

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

Ejemplo de respuesta 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": {}
}
```

Localice el `state` en el campo de respuesta que tendrá uno de los valores de la tabla siguiente.

Estado	Descripción
pendiente	El proceso de configuración sigue activo y aún no se ha completado.
válido	La configuración se ha completado correctamente y. `currentConfig` en la respuesta coincide `desiredConfig`.
error	Error en el proceso de configuración de LDAP.

Agregue entradas LDAP a Astra

Después de configurar LDAP como proveedor de autenticación para Astra Control Center, puede seleccionar los usuarios LDAP que Astra autenticará mediante las credenciales LDAP. Cada usuario debe tener una función en Astra para poder acceder a Astra a través de la API ASTRA Control REST.

Hay dos formas de configurar Astra para asignar funciones. Elija el que mejor se adapte a su entorno.

- "Agregar y enlazar un usuario individual"
- "Agregar y enlazar un grupo"

Las credenciales LDAP tienen el formato de nombre de usuario como dirección de correo electrónico y contraseña LDAP asociada.

Agregar y enlazar un usuario individual

Puede asignar una función a cada usuario Astra que se utilice después de la autenticación LDAP. Esto resulta apropiado cuando hay un número reducido de usuarios y cada uno puede tener características administrativas diferentes.

1. Agregar un usuario

Realice la siguiente llamada a la API DE REST para añadir un usuario a Astra e indicar que LDAP es el proveedor de autenticación.

Método HTTP	Ruta
PUBLICAR	/accounts/{account_id}/core/v1/users

Ejemplo de entrada 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"
}
```

Tenga en cuenta lo siguiente acerca de los parámetros de entrada:

- Se requieren los siguientes parámetros:
  - `authProvider`
  - `authID`
  - `email`
- `authID` Es el nombre distintivo (DN) del usuario en LDAP
- `email` Debe ser único para todos los usuarios definidos en Astra

Si la `email` El valor no es único, se produce un error y se devuelve un código de estado HTTP 409 en la respuesta.

Ejemplo de curl

```
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>'
```

Ejemplo de respuesta 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. Agregue un enlace de rol para el usuario

Ejecute la siguiente llamada API de REST para enlazar el usuario con un rol específico. Debe tener creado el UUID del usuario en el paso anterior.

Método HTTP	Ruta
PUBLICAR	/Accounts/{account_id}/core/v1/roleBindings

Ejemplo de entrada JSON

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

Tenga en cuenta lo siguiente acerca de los parámetros de entrada:

- El valor utilizado anteriormente para `roleConstraint` Es la única opción disponible para la versión actual de Astra. Indica que el usuario no está restringido a un conjunto limitado de espacios de nombres y puede acceder a todos ellos.

Ejemplo de curl

```
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>'
```

Ejemplo de respuesta 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": ["*"]
}
```

Tenga en cuenta lo siguiente sobre los parámetros de respuesta:

- El valor `user` para la `principalType` el campo indica que se ha agregado el enlace de función a un usuario (no a un grupo).

Agregar y enlazar un grupo

Puede asignar una función a un grupo Astra que se utilice después de la autenticación LDAP. Resulta apropiado cuando hay un gran número de usuarios y cada uno puede tener características administrativas similares.

1. Agregar un grupo

Realice la siguiente llamada a la API DE REST para agregar un grupo a Astra e indicar que LDAP es el proveedor de autenticación.

Método HTTP	Ruta
PUBLICAR	/accounts/{account_id}/core/v1/groups

Ejemplo de entrada JSON

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

Tenga en cuenta lo siguiente acerca de los parámetros de entrada:

- Se requieren los siguientes parámetros:
  - `authProvider`
  - `authID`

Ejemplo de curl

```
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>'
```

Ejemplo de respuesta 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. Agregue un enlace de rol para el grupo

Realice la siguiente llamada de API de REST para enlazar el grupo con un rol específico. Debe haber creado el UUID del grupo en el paso anterior. Los usuarios que sean miembros del grupo podrán iniciar sesión en Astra después de que LDAP realice la autenticación.

Método HTTP	Ruta
PUBLICAR	/Accounts/{account_id}/core/v1/roleBindings

Ejemplo de entrada JSON

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

Tenga en cuenta lo siguiente acerca de los parámetros de entrada:

- El valor utilizado anteriormente para `roleConstraint` Es la única opción disponible para la versión actual de Astra. Indica que el usuario no está restringido a determinados espacios de nombres y puede acceder a todos ellos.

Ejemplo de curl

```
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>'
```

Ejemplo de respuesta 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": ["*"]
}
```

Tenga en cuenta lo siguiente sobre los parámetros de respuesta:

- El valor `group` para la `principalType` el campo indica que se ha agregado el enlace de función para un grupo (no un usuario).

Deshabilite y restablezca LDAP

Hay dos tareas administrativas opcionales a través de las relacionadas que puede realizar según sea necesario para una implementación de Astra Control Center. Es posible deshabilitar la autenticación LDAP de forma global y restablecer la configuración de LDAP.

Ambas tareas de flujo de trabajo requieren el id para `astra.account.ldap` Ajuste Astra. En **Configurar el servidor LDAP** se incluyen detalles sobre cómo recuperar el identificador de configuración. Consulte "Recupere el UUID de la configuración LDAP" si quiere más información.

- "Deshabilitar la autenticación LDAP"
- "Restablece la configuración de autenticación de LDAP"

Deshabilitar la autenticación LDAP

Puede realizar la siguiente llamada a la API DE REST para deshabilitar globalmente la autenticación LDAP para una implementación específica de Astra. La llamada actualiza la `astra.account.ldap` y la `isEnabled` el valor se establece en `false`.

Método HTTP	Ruta
PUESTO	/accounts/{account_id}/core/v1/settings/{setting_id}

Ejemplo de entrada 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 la llamada se realiza correctamente, el `HTTP 204` se devuelve la respuesta. Opcionalmente, puede recuperar de nuevo los ajustes de configuración para confirmar el cambio.

Restablece la configuración de autenticación de LDAP

Puede realizar la siguiente llamada a la API DE REST para desconectar Astra del servidor LDAP y restablecer la configuración de LDAP en Astra. La llamada actualiza la `astra.account.ldap` y el valor de `connectionHost` se borra.

Valor de `isEnabled` también se debe establecer en `false`. Puede establecer este valor antes de realizar la llamada de restablecimiento o como parte de realizar la llamada de restablecimiento. En el segundo caso, `connectionHost` debe ser despejado y. `isEnabled` establezca como falso en la misma llamada de restablecimiento.

Esto es una operación disruptiva y debe continuar con precaución. Elimina todos los grupos y usuarios LDAP importados. También elimina todos los usuarios, grupos y enlaces (tipo LDAP) de Astra relacionados que creó en Astra Control Center.

Método HTTP	Ruta
PUESTO	/accounts/{account_id}/core/v1/settings/{setting_id}

Ejemplo de entrada 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"
    }
}
```

Tenga en cuenta lo siguiente:

- Para cambiar el servidor LDAP, debe deshabilitar y restablecer el cambio LDAP `connectHost` a un valor nulo como se muestra en el ejemplo anterior.

```
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 la llamada se realiza correctamente, el `HTTP 204` se devuelve la respuesta. De manera opcional, puede recuperar la configuración de nuevo para confirmar el cambio.

Información de copyright

Información de la marca comercial