Configurazione LDAP

Astra Automation

NetApp
March 17, 2024

Sommario

Configurazione LDAP

Preparazione per la configurazione LDAP

È possibile integrare Astra Control Center con un server LDAP (Lightweight Directory Access Protocol) per eseguire l'autenticazione per gli utenti Astra selezionati. LDAP è un protocollo standard di settore per l'accesso alle informazioni di directory distribuite e una scelta popolare per l'autenticazione aziendale.

Informazioni correlate

- "Roadmap delle specifiche tecniche LDAP"
- "LDAP versione 3"

Panoramica del processo di implementazione

Ad alto livello, è necessario eseguire diversi passaggi per configurare un server LDAP in modo da fornire l'autenticazione agli utenti Astra.

> Sebbene i passaggi presentati di seguito siano in sequenza, in alcuni casi è possibile eseguirli in un ordine diverso. Ad esempio, è possibile definire gli utenti e i gruppi Astra prima di configurare il server LDAP.

1. Revisione "Requisiti e limitazioni" per comprendere le opzioni, i requisiti e le limitazioni.
2. Selezionare un server LDAP e le opzioni di configurazione desiderate (inclusa la protezione).
3. Eseguire il flusso di lavoro "Configurare Astra per l'utilizzo di un server LDAP" Per integrare Astra con il server LDAP.
4. Esaminare gli utenti e i gruppi sul server LDAP per assicurarsi che siano definiti correttamente.
5. Eseguire il flusso di lavoro appropriato in "Aggiungere voci LDAP ad Astra" Identificare gli utenti da autenticare utilizzando LDAP.

Requisiti e limitazioni

Prima di configurare Astra per l'utilizzo di LDAP per l'autenticazione, è necessario esaminare gli elementi essenziali della configurazione di Astra presentati di seguito, incluse le limitazioni e le opzioni di configurazione.

Supportato solo con Astra Control Center

La piattaforma Astra Control offre due modelli di implementazione. L'autenticazione LDAP è supportata solo con le implementazioni di Astra Control Center.

Configurazione mediante API REST o interfaccia utente Web

L'attuale release di Astra Control Center supporta la configurazione dell'autenticazione LDAP utilizzando sia l'API REST di Astra Control che l'interfaccia utente web Astra.

Server LDAP richiesto

Per accettare ed elaborare le richieste di autenticazione Astra, è necessario disporre di un server LDAP. Active Directory di Microsoft è supportata con la release corrente di Astra Control Center.

Connessione sicura al server LDAP

Quando si configura il server LDAP in Astra, è possibile definire una connessione sicura. In questo caso è necessario un certificato per il protocollo LDAPS.

Configurare utenti o gruppi

Selezionare gli utenti da autenticare utilizzando LDAP. È possibile eseguire questa operazione identificando i singoli utenti o un gruppo di utenti. Gli account devono essere definiti sul server LDAP. Inoltre, devono essere identificati in Astra (tipo LDAP), che consente di inoltrare le richieste di autenticazione a LDAP.

Vincolo di ruolo quando si lega un utente o un gruppo

Con l'attuale release di Astra Control Center, l'unico valore supportato per `roleConstraint` è "*". Questo indica che l'utente non è limitato a un set limitato di spazi dei nomi e può accedervi tutti. Vedere "Aggiungere voci LDAP ad Astra" per ulteriori informazioni.

Credenziali LDAP

Le credenziali utilizzate da LDAP includono il nome utente (indirizzo e-mail) e la password associata.

Indirizzi e-mail univoci

Tutti gli indirizzi e-mail che fungono da nomi utente in un'implementazione di Astra Control Center devono essere univoci. Non è possibile aggiungere un utente LDAP con un indirizzo e-mail già definito in Astra. Se esiste un'email duplicata, devi prima eliminarla da Astra. Vedere "Rimuovere gli utenti" Per ulteriori informazioni, visitare il sito di documentazione di Astra Control Center.

È possibile definire prima utenti e gruppi LDAP

È possibile aggiungere utenti e gruppi LDAP a Astra Control Center anche se non esistono ancora in LDAP o se il server LDAP non è configurato. Ciò consente di preconfigurare gli utenti e i gruppi prima di configurare il server LDAP.

Un utente definito in più gruppi LDAP

Se un utente LDAP appartiene a più gruppi LDAP e ai gruppi sono stati assegnati ruoli diversi in Astra, il ruolo effettivo dell'utente al momento dell'autenticazione sarà il più privilegiato. Ad esempio, se a un utente è assegnato il `viewer` con il group1, ma ha il `member` ruolo nel group2, il ruolo dell'utente sarebbe `member`. Si basa sulla gerarchia utilizzata da Astra (dal più alto al più basso):

- Proprietario
- Amministratore
- Membro
- Visualizzatore

Sincronizzazione periodica dell'account

Astra sincronizza gli utenti e i gruppi IT con il server LDAP circa ogni 60 secondi. Quindi, se un utente o un gruppo viene aggiunto o rimosso da LDAP, può essere necessario fino a un minuto prima che sia disponibile in Astra.

Disattivazione e ripristino della configurazione LDAP

Prima di tentare di ripristinare la configurazione LDAP, è necessario disattivare l'autenticazione LDAP. Inoltre, per modificare il server LDAP (`connectionHost`), è necessario eseguire entrambe le operazioni. Vedere "Disattivare e ripristinare LDAP" per ulteriori informazioni.

Parametri API REST

I flussi di lavoro di configurazione LDAP effettuano chiamate API REST per eseguire le attività specifiche. Ogni

chiamata API può includere parametri di input come mostrato negli esempi forniti. Vedere "Riferimento API online" per informazioni su come individuare la documentazione di riferimento.

Configurare Astra per l'utilizzo di un server LDAP

Selezionare un server LDAP e configurare Astra per utilizzare il server come provider di autenticazione. L'attività di configurazione consiste nei passaggi descritti di seguito. Ogni passaggio include una singola chiamata API REST.

1. Aggiungere un certificato CA

Eseguire la seguente chiamata API REST per aggiungere un certificato CA ad Astra.

> Questo passaggio è facoltativo e necessario solo se si desidera che Astra e LDAP comunichino su un canale sicuro utilizzando LDAPS.

Metodo HTTP	Percorso
POST	/accounts/{account_id}/core/v1/certificates

Esempio di input JSON

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

Tenere presente quanto segue sui parametri di input:

- `cert` È una stringa JSON contenente un certificato con codifica base64 e formato PKCS-11 (con codifica PEM).
- `isSelfSigned` deve essere impostato su `true` se il certificato è autofirmato. L'impostazione predefinita è `false`.

Esempio di arricciamento

```
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>'
```

Esempio di risposta 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. Aggiungere le credenziali di binding

Eseguire la seguente chiamata API REST per aggiungere le credenziali BIND.

Metodo HTTP	Percorso
POST	/accounts/{account_id}/core/v1/credentials

Esempio di input JSON

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

Tenere presente quanto segue sui parametri di input:

- `bindDn` e. `password` Sono le credenziali bind codificate base64 dell'utente amministratore LDAP in grado di connettersi e cercare nella directory LDAP. `bindDn` È l'indirizzo e-mail dell'utente LDAP.

Esempio di arricciamento

```
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>'
```

Esempio di risposta 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"
    }
}
```

Osservare i seguenti parametri di risposta:

- Il `id` della credenziale viene utilizzata nelle fasi successive del flusso di lavoro.

3. Recuperare l'UUID dell'impostazione LDAP

Eseguire la seguente chiamata API REST per recuperare l'UUID di `astra.account.ldap` Impostazione inclusa in Astra Control Center.

> Nell'esempio riportato di seguito viene utilizzato un parametro di query per filtrare la raccolta delle impostazioni. È invece possibile rimuovere il filtro per ottenere tutte le impostazioni e quindi cercare `astra.account.ldap`.

Metodo HTTP	Percorso
OTTIENI	/accounts/{account_id}/core/v1/settings

Esempio di arricciamento

```
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>'
```

Esempio di risposta JSON

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

4. Aggiornare l'impostazione LDAP

Eseguire la seguente chiamata API REST per aggiornare l'impostazione LDAP e completare la configurazione. Utilizzare `id` Valore della chiamata API precedente per `<SETTING_ID>` Valore nel percorso URL riportato di seguito.

> È possibile inviare una richiesta GET per l'impostazione specifica prima di visualizzare configSchema. In questo modo verranno fornite ulteriori informazioni sui campi obbligatori della configurazione.

Metodo HTTP	Percorso
IN PRIMO PIANO	/accounts/{account_id}/core/v1/settings/{setting_id}

Esempio di input 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"
    }
}
```

Tenere presente quanto segue sui parametri di input:

- `isEnabled` deve essere impostato su `true` oppure si potrebbe verificare un errore.
- `credentialId` è l'id della credenziale bind creata in precedenza.
- `secureMode` deve essere impostato su `LDAP` oppure `LDAPS` in base alla configurazione del passaggio precedente.
- Solo "Active Directory" è supportato come vendor.

Esempio di arricciamento

```
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>'
```

Se la chiamata ha esito positivo, viene restituita la risposta HTTP 204.

5. Recuperare l'impostazione LDAP

È possibile eseguire la seguente chiamata API REST per recuperare le impostazioni LDAP e confermare l'aggiornamento.

Metodo HTTP	Percorso
OTTIENI	/accounts/{account_id}/core/v1/settings/{setting_id}

Esempio di arricciamento

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

Esempio di risposta 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": {}
}
```


Individuare il `state` nella risposta che avrà uno dei valori nella tabella seguente.

Stato	Descrizione
in sospeso	Il processo di configurazione è ancora attivo e non ancora completato.
valido	La configurazione è stata completata correttamente e. `currentConfig` nella risposta corrisponde `desiredConfig`.
errore	Il processo di configurazione LDAP non è riuscito.

Aggiungere voci LDAP ad Astra

Una volta configurato LDAP come provider di autenticazione per Astra Control Center, è possibile selezionare gli utenti LDAP che Astra eseguirà l'autenticazione utilizzando le credenziali LDAP. Ogni utente deve avere un ruolo in Astra prima di poter accedere ad Astra attraverso l'API REST di Astra Control.

Esistono due modi per configurare Astra per assegnare i ruoli. Scegliere quello più adatto al proprio ambiente.

- "Aggiungere e associare un singolo utente"

- "Aggiungere e associare un gruppo"

> Le credenziali LDAP sono sotto forma di nome utente come indirizzo e-mail e password LDAP associata.

Aggiungere e associare un singolo utente

È possibile assegnare un ruolo a ciascun utente Astra utilizzato dopo l'autenticazione LDAP. Ciò è appropriato quando vi è un numero limitato di utenti e ciascuno potrebbe avere caratteristiche amministrative diverse.

1. Aggiungere un utente

Eseguire la seguente chiamata API REST per aggiungere un utente ad Astra e indicare che LDAP è il provider di autenticazione.

Metodo HTTP	Percorso
POST	/accounts/{account_id}/core/v1/users

Esempio di input 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"
}
```

Tenere presente quanto segue sui parametri di input:

- Sono necessari i seguenti parametri:
  - `authProvider`
  - `authID`
  - `email`
- `authID` È il nome distinto (DN) dell'utente in LDAP
- `email` Deve essere univoco per tutti gli utenti definiti in Astra

Se il `email` Il valore non è univoco, si verifica un errore e nella risposta viene restituito un codice di stato 409 HTTP.

Esempio di arricciamento

```
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>'
```

Esempio di risposta 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. Aggiungere un’associazione di ruolo per l’utente

Eseguire la seguente chiamata API REST per associare l’utente a un ruolo specifico. È necessario creare l’UUID dell’utente nel passaggio precedente.

Metodo HTTP	Percorso
POST	/Accounts/{account_id}/core/v1/roleBindings

Esempio di input JSON

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

Tenere presente quanto segue sui parametri di input:

- Il valore utilizzato in precedenza per `roleConstraint` È l'unica opzione disponibile per la release corrente di Astra. Indica che l'utente non è limitato a un set limitato di spazi dei nomi e può accedervi tutti.

Esempio di arricciamento

```
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>'
```

Esempio di risposta 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": ["*"]
}
```

Tenere presente quanto segue in merito ai parametri di risposta:

- Il valore `user` per `principalType` il campo indica l'aggiunta dell'associazione di ruoli per un utente (non un gruppo).

Aggiungere e associare un gruppo

È possibile assegnare un ruolo a un gruppo Astra che viene utilizzato dopo l'autenticazione LDAP. Ciò è appropriato quando vi è un numero elevato di utenti e ciascuno potrebbe avere caratteristiche amministrative simili.

1. Aggiungere un gruppo

Eseguire la seguente chiamata API REST per aggiungere un gruppo ad Astra e indicare che LDAP è il provider di autenticazione.

Metodo HTTP	Percorso
POST	/accounts/{account_id}/core/v1/groups

Esempio di input JSON

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

Tenere presente quanto segue sui parametri di input:

- Sono necessari i seguenti parametri:
  - `authProvider`
  - `authID`

Esempio di arricciamento

```
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>'
```

Esempio di risposta 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. Aggiungere un’associazione di ruolo per il gruppo

Eseguire la seguente chiamata API REST per associare il gruppo a un ruolo specifico. È necessario creare l’UUID del gruppo nel passaggio precedente. Gli utenti che sono membri del gruppo potranno accedere ad Astra dopo che LDAP ha eseguito l’autenticazione.

Metodo HTTP	Percorso
POST	/Accounts/{account_id}/core/v1/roleBindings

Esempio di input JSON

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

Tenere presente quanto segue sui parametri di input:

- Il valore utilizzato in precedenza per `roleConstraint` È l'unica opzione disponibile per la release corrente di Astra. Indica che l'utente non è limitato a determinati spazi dei nomi e può accedervi tutti.

Esempio di arricciamento

```
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>'
```

Esempio di risposta 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": ["*"]
}
```

Tenere presente quanto segue in merito ai parametri di risposta:

- Il valore `group` per `principalType` il campo indica l'aggiunta dell'associazione di ruoli per un gruppo (non per un utente).

Disattivare e ripristinare LDAP

Sono disponibili due attività amministrative opzionali, sebbene correlate, che è possibile eseguire in base alle necessità per un'implementazione di Astra Control Center. È possibile disattivare globalmente l'autenticazione LDAP e ripristinare la configurazione LDAP.

Entrambe le attività del flusso di lavoro richiedono l'id per `astra.account.ldap` Impostazione Astra. I dettagli su come recuperare l'id impostazione sono inclusi in **Configurazione del server LDAP**. Vedere "Recuperare l'UUID dell'impostazione LDAP" per ulteriori informazioni.

- "Disattiva autenticazione LDAP"
- "Ripristinare la configurazione di autenticazione LDAP"

Disattiva autenticazione LDAP

È possibile eseguire la seguente chiamata REST API per disattivare globalmente l'autenticazione LDAP per una specifica implementazione Astra. La chiamata aggiorna `astra.account.ldap` e il `isEnabled` il valore è impostato su `false`.

Metodo HTTP	Percorso
IN PRIMO PIANO	/accounts/{account_id}/core/v1/settings/{setting_id}

Esempio di input 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>'
```

Se la chiamata ha esito positivo, il `HTTP 204` la risposta viene restituita. È possibile recuperare di nuovo le impostazioni di configurazione per confermare la modifica.

Ripristinare la configurazione di autenticazione LDAP

È possibile eseguire la seguente chiamata REST API per disconnettere Astra dal server LDAP e reimpostare la configurazione LDAP in Astra. La chiamata aggiorna `astra.account.ldap` e il valore di `connectionHost` è deselezionato.

Il valore di `isEnabled` deve anche essere impostato su `false`. È possibile impostare questo valore prima di effettuare la chiamata di ripristino o come parte della chiamata di ripristino. Nel secondo caso, `connectionHost` devono essere cancellati e. `isEnabled` impostare su false per la stessa chiamata di ripristino.

> Si tratta di un'operazione di interruzione e si consiglia di procedere con cautela. Elimina tutti gli utenti e i gruppi LDAP importati. Inoltre, elimina tutti gli utenti, i gruppi e le associazioni di roleBinding Astra (tipo LDAP) creati in Astra Control Center.

Metodo HTTP	Percorso
IN PRIMO PIANO	/accounts/{account_id}/core/v1/settings/{setting_id}

Esempio di input 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"
    }
}
```

Tenere presente quanto segue:

- Per modificare il server LDAP, è necessario disattivare e reimpostare LDAP Changing `connectHost` su un valore nullo come mostrato nell'esempio precedente.

```
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>'
```

Se la chiamata ha esito positivo, il `HTTP 204` la risposta viene restituita. È possibile recuperare nuovamente la configurazione per confermare la modifica.