



Configuração LDAP

Astra Automation

NetApp
January 31, 2025

Índice

- Configuração LDAP 1
 - Prepare-se para a configuração LDAP 1
 - Configure o Astra para usar um servidor LDAP 3
 - Adicionar entradas LDAP ao Astra 12
 - Desativar e repor LDAP 19

Configuração LDAP

Prepare-se para a configuração LDAP

Opcionalmente, é possível integrar o Astra Control Center a um servidor LDAP (Lightweight Directory Access Protocol) para executar a autenticação para usuários selecionados do Astra. O LDAP é um protocolo padrão do setor para acessar informações de diretórios distribuídos e uma escolha popular para autenticação empresarial.

Informações relacionadas

- ["Mapa rodoviário da especificação técnica LDAP"](#)
- ["LDAP versão 3"](#)

Visão geral do processo de implementação

Em um alto nível, há várias etapas que você precisa executar para configurar um servidor LDAP para fornecer autenticação para usuários Astra.



Enquanto as etapas apresentadas abaixo estão em uma sequência, em alguns casos você pode executá-las em uma ordem diferente. Por exemplo, você pode definir os usuários e grupos Astra antes de configurar o servidor LDAP.

1. Revise ["Requisitos e limitações"](#) para entender as opções, os requisitos e as limitações.
2. Selecione um servidor LDAP e as opções de configuração desejadas (incluindo segurança).
3. Execute o fluxo de trabalho ["Configure o Astra para usar um servidor LDAP"](#) para integrar o Astra ao servidor LDAP.
4. Reveja os utilizadores e grupos no servidor LDAP para se certificar de que estão definidos corretamente.
5. Execute o fluxo de trabalho apropriado em ["Adicionar entradas LDAP ao Astra"](#) para identificar os usuários a serem autenticados usando LDAP.

Requisitos e limitações

Antes de configurar o Astra para usar LDAP para autenticação, você deve consultar os fundamentos de configuração do Astra apresentados abaixo, incluindo limitações e opções de configuração.

Compatível apenas com Astra Control Center

A plataforma Astra Control oferece dois modelos de implantação. A autenticação LDAP só é compatível com implantações do Astra Control Center.

Configuração usando API REST ou interface de usuário da Web

A versão atual do Astra Control Center é compatível com a configuração de autenticação LDAP usando a API REST Astra Control e a interface de usuário web Astra.

Servidor LDAP necessário

É necessário ter um servidor LDAP para aceitar e processar as solicitações de autenticação Astra. O ativo Directory da Microsoft é compatível com a versão atual do Astra Control Center.

Ligação segura ao servidor LDAP

Ao configurar o servidor LDAP no Astra, você pode definir opcionalmente uma conexão segura. Neste caso, é necessário um certificado para o protocolo LDAPS.

Configurar usuários ou grupos

Você precisa selecionar os usuários a serem autenticados usando LDAP. Você pode fazer isso identificando os usuários individuais ou um grupo de usuários. As contas devem ser definidas no servidor LDAP. Eles também precisam ser identificados no Astra (tipo LDAP), o que permite que as solicitações de autenticação sejam encaminhadas para LDAP.

Restrição de função ao vincular um usuário ou grupo

Com a versão atual do Astra Control Center, o único valor suportado para `roleConstraint` é `""`. Isso indica que o usuário não está restrito a um conjunto limitado de namespaces e pode acessar todos eles. Consulte ["Adicionar entradas LDAP ao Astra"](#) para obter mais informações.

Credenciais LDAP

As credenciais usadas pelo LDAP incluem o nome de usuário (endereço de e-mail) e a senha associada.

Endereços de e-mail exclusivos

Todos os endereços de e-mail atuando como nomes de usuário em uma implantação do Astra Control Center devem ser exclusivos. Não é possível adicionar um usuário LDAP com um endereço de e-mail que já esteja definido para Astra. Se houver um e-mail duplicado, você precisará primeiro excluí-lo do Astra. Consulte ["Remover usuários"](#) o site de documentação do Astra Control Center para obter mais informações.

Opcionalmente, defina primeiro os usuários e grupos LDAP

Você pode adicionar os usuários e grupos LDAP ao Astra Control Center mesmo que eles ainda não existam no LDAP ou se o servidor LDAP não estiver configurado. Isto permite pré-configurar os utilizadores e grupos antes de configurar o servidor LDAP.

Um usuário definido em vários grupos LDAP

Se um usuário LDAP pertencer a vários grupos LDAP e os grupos tiverem sido atribuídos diferentes funções no Astra, a função efetiva do usuário ao autenticar será a mais privilegiada. Por exemplo, se um usuário for atribuído a `viewer` função com `group1`, mas tiver a `member` função em `group2`, a função do usuário será `member`. Isso é baseado na hierarquia usada pelo Astra (mais alto a mais baixo):

- Proprietário
- Administrador
- Membro
- Visualizador

Sincronização periódica de contas

O Astra sincroniza os usuários e grupos de TI com o servidor LDAP aproximadamente a cada 60 segundo. Portanto, se um usuário ou grupo for adicionado ou removido do LDAP, pode levar até um minuto antes de estar disponível no Astra.

Desativar e repor a configuração LDAP

Antes de tentar repor a configuração LDAP, tem de desativar primeiro a autenticação LDAP. Além disso, para alterar o servidor LDAP (`connectionHost`), é necessário executar ambas as operações. Consulte ["Desativar e repor LDAP"](#) para obter mais informações.

Parâmetros da API REST

Os fluxos de trabalho de configuração LDAP fazem chamadas de API REST para realizar as tarefas específicas. Cada chamada de API pode incluir parâmetros de entrada como mostrado nas amostras fornecidas. Consulte ["Referência de API online"](#) para obter informações sobre como localizar a documentação de referência.

Configure o Astra para usar um servidor LDAP

Você precisa selecionar um servidor LDAP e configurar o Astra para usar o servidor como um provedor de autenticação. A tarefa de configuração consiste nos passos descritos abaixo. Cada etapa inclui uma única chamada de API REST.

Etapa 1: Adicione um certificado de CA

Execute a seguinte chamada de API REST para adicionar um certificado de CA ao Astra.



Esta etapa é opcional e somente necessária se você quiser que o Astra e o LDAP se comuniquem em um canal seguro usando o LDAPS.

Método HTTP e endpoint

Essa chamada de API REST usa o método e o endpoint a seguir.

Método HTTP	Caminho
POST	/accounts//core/v1/certificates

Curl exemplo

```
curl --request POST \  
--location \  
"https://astra.example.com/accounts/$ACCOUNT_ID/core/v1/certificates" \  
--include \  
--header "Content-Type: application/astra-certificate+json" \  
--header "Accept: */*" \  
--header "Authorization: Bearer $API_TOKEN" \  
--data @JSONinput
```

Exemplo de entrada JSON

```
{  
  "type": "application/astra-certificate",  
  "version": "1.0",  
  "certUse": "rootCA",  
  "cert": "LS0tLS1CRUdJTtIBDRVJUSUZJQ0FURS0tLS0tCk1JSUMyVEN",  
  "isSelfSigned": "true"  
}
```

Observe o seguinte sobre os parâmetros de entrada:

- `cert` É uma string JSON contendo um certificado formatado PKCS-11 codificado base64 (codificado PEM).
- `isSelfSigned` deve ser definido como `true` se o certificado for auto-assinado. A predefinição é `false`.

Exemplo de saída JSON

```
{
  "type": "application/astra-certificate",
  "version": "1.0",
  "id": "a5212e7e-402b-4cff-bba0-63f3c6505199",
  "certUse": "rootCA",
  "cert": "LS0tLS1CRUdJTlBDRVJUSUZJQ0FURS0tLS0tCk1JSUMyVEN",
  "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": []
  }
}
```

Etapa 2: Adicione as credenciais de vinculação

Execute a seguinte chamada de API REST para adicionar as credenciais de vinculação.

Método HTTP e endpoint

Essa chamada de API REST usa o método e o endpoint a seguir.

Método HTTP	Caminho
POST	/accounts/_id/core/v1/credentials

Curl exemplo

```
curl --request POST \  
--location \  
"https://astra.example.com/accounts/$ACCOUNT_ID/core/v1/credentials" \  
--include \  
--header "Content-Type: application/astra-certificate+json" \  
--header "Accept: */*" \  
--header "Authorization: Bearer $API_TOKEN" \  
--data @JSONinput
```

Exemplo de entrada JSON

```
{  
  "name": "ldapBindCredential",  
  "type": "application/astra-credential",  
  "version": "1.1",  
  "keyStore": {  
    "bindDn": "dWlkPWFkbWluLG91PXM5c3RlbQ==",  
    "password": "cGFzc3dvcmQ="
```

Observe o seguinte sobre os parâmetros de entrada:

- `bindDn` E `password` são as credenciais de vinculação codificadas base64 do usuário de administrador LDAP que é capaz de conectar e pesquisar o diretório LDAP. `bindDn` É o endereço de e-mail do usuário LDAP.

Exemplo de saída 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"
  }
}
```

Observe os seguintes parâmetros de resposta:

- `id` da credencial é utilizado em etapas subsequentes do fluxo de trabalho.

Etapa 3: Recupere o UUID da configuração LDAP

Execute a seguinte chamada de API REST para recuperar o UUID da `astra.account.ldap` configuração incluída no Astra Control Center.



O exemplo curl abaixo usa um parâmetro de consulta para filtrar a coleção de configurações. Em vez disso, você pode remover o filtro para obter todas as configurações e, em seguida, procurar `astra.account.ldap`.

Método HTTP e endpoint

Essa chamada de API REST usa o método e o endpoint a seguir.

Método HTTP	Caminho
OBTER	<code>/accounts/_id/core/v1/settings</code>

Curl exemplo

```
curl --request GET \
--location
"https://astra.example.com/accounts/$ACCOUNT_ID/core/v1/settings?filter=na
me%20eq%20'astra.account.ldap'&include=name,id" \
--include \
--header "Accept: */*" \
--header "Authorization: Bearer $API_TOKEN" \
```

Exemplo de saída JSON

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

Etapa 4: Atualize a configuração LDAP

Execute a seguinte chamada de API REST para atualizar a configuração LDAP e concluir a configuração. Use o `id` valor da chamada de API anterior para o `<SETTING_ID>` valor no caminho de URL abaixo.



Você pode emitir uma SOLICITAÇÃO GET para a configuração específica primeiro para ver o `configSchema`. Isso fornecerá mais informações sobre os campos obrigatórios na configuração.

Método HTTP e endpoint

Essa chamada de API REST usa o método e o endpoint a seguir.

Método HTTP	Caminho
COLOQUE	/accounts/_id/core/v1/settings//setting_id

Curl exemplo

```
curl --request PUT \
--location
"https://astra.example.com/accounts/$ACCOUNT_ID/core/v1/settings/<SETTING_ID>" \
--include \
--header "Content-Type: application/astra-setting+json" \
--header "Accept: */*" \
--header "Authorization: Bearer $API_TOKEN" \
--data @JSONinput
```

Exemplo 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"
  }
}
```

Observe o seguinte sobre os parâmetros de entrada:

- `isEnabled` deve ser definido como `true` ou pode ocorrer um erro.
- `credentialId` é o id da credencial de ligação criada anteriormente.
- `secureMode` deve ser definido como `LDAP` ou `LDAPS` com base na sua configuração na etapa anterior.
- Apenas o 'Active Directory' é suportado como fornecedor.

Se a chamada for bem-sucedida, a resposta HTTP 204 será retornada.

Etapa 5: Recupere a configuração LDAP

Opcionalmente, você pode executar a seguinte chamada de API REST para recuperar as configurações LDAP e confirmar a atualização.

Método HTTP e endpoint

Essa chamada de API REST usa o método e o endpoint a seguir.

Método HTTP	Caminho
OBTER	/accounts/_id/core/v1/settings//setting_id

Curl exemplo

```
curl --request GET \  
--location \  
"https://astra.example.com/accounts/$ACCOUNT_ID/core/v1/settings/<SETTING_ID>" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Bearer $API_TOKEN"
```

Exemplo de saída 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": {}
}

```

Localize o `state` campo na resposta que terá um dos valores na tabela abaixo.

Estado	Descrição
pendente	O processo de configuração ainda está ativo e ainda não foi concluído.
válido	A configuração foi concluída com sucesso e <code>currentConfig</code> na resposta corresponde <code>desiredConfig</code> .
erro	O processo de configuração LDAP falhou.

Adicionar entradas LDAP ao Astra

Depois que o LDAP é configurado como um provedor de autenticação para o Astra Control Center, você pode selecionar os usuários LDAP que o Astra autenticará usando as credenciais LDAP. Cada usuário precisa ter uma função no Astra antes de poder acessar o Astra por meio da API REST Astra Control.

Há duas maneiras de configurar o Astra para atribuir funções. Escolha o que é apropriado para o seu ambiente.

- ["Adicione e vincule um usuário individual"](#)

- "Adicione e vincule um grupo"



As credenciais LDAP estão na forma de um nome de usuário como endereço de e-mail e a senha LDAP associada.

Adicione e vincule um usuário individual

Você pode atribuir uma função a cada usuário Astra que é usado após a autenticação LDAP. Isso é apropriado quando há um pequeno número de usuários e cada um pode ter características administrativas diferentes.

Passo 1: Adicione um usuário

Execute a seguinte chamada de API REST para adicionar um usuário ao Astra e indicar que o LDAP é o provedor de autenticação.

Método HTTP e endpoint

Essa chamada de API REST usa o método e o endpoint a seguir.

Método HTTP	Caminho
POST	/accounts/_id/core/v1/users

Curl exemplo

```
curl --request POST \  
--location "https://astra.example.com/accounts/$ACCOUNT_ID/core/v1/users" \  
\  
--include \  
--header "Content-Type: application/astra-user+json" \  
--header "Accept: */*" \  
--header "Authorization: Bearer $API_TOKEN" \  
--data @JSONinput
```

Exemplo 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"  
}
```

Observe o seguinte sobre os parâmetros de entrada:

- São necessários os seguintes parâmetros:

- authProvider
- authID
- email
- authID É o nome distinto (DN) do usuário no LDAP
- email Deve ser exclusivo para todos os usuários definidos no Astra

Se o email valor não for exclusivo, ocorrerá um erro e um código de status HTTP 409 será retornado na resposta.

Exemplo de saída 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": ""
}
```


Etapa 2: Adicione uma vinculação de função para o usuário

Execute a seguinte chamada de API REST para vincular o usuário a uma função específica. Você precisa ter o UUID do usuário criado na etapa anterior.

Método HTTP e endpoint

Essa chamada de API REST usa o método e o endpoint a seguir.

Método HTTP	Caminho
POST	/Accounts/_id/core/v1/roleBindings

Curl exemplo

```
curl --request POST \  
--location \  
"https://astra.example.com/accounts/$ACCOUNT_ID/core/v1/roleBindings" \  
--include \  
--header "Content-Type: application/astra-roleBinding+json" \  
--header "Accept: */*" \  
--header "Authorization: Bearer $API_TOKEN" \  
--data @JSONinput
```

Exemplo de entrada JSON

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

Observe o seguinte sobre os parâmetros de entrada:

- O valor utilizado acima para `roleConstraint` é a única opção disponível para a versão atual do Astra. Ele indica que o usuário não está restrito a um conjunto limitado de namespaces e pode acessá-los todos.

Exemplo de resposta 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": ["*"]
}
```

Observe o seguinte sobre os parâmetros de resposta:

- O valor `user` para o `principalType` campo indica que a vinculação de função foi adicionada para um usuário (não para um grupo).

Adicione e vincule um grupo

Você pode atribuir uma função a um grupo Astra que é usado após a autenticação LDAP. Isso é apropriado quando há um grande número de usuários e cada um pode ter características administrativas semelhantes.

Passo 1: Adicione um grupo

Execute a seguinte chamada de API REST para adicionar um grupo ao Astra e indicar que o LDAP é o provedor de autenticação.

Método HTTP e endpoint

Essa chamada de API REST usa o método e o endpoint a seguir.

Método HTTP	Caminho
POST	/accounts//core/v1/groups

Curl exemplo

```
curl --request POST \  
--location "https://astra.example.com/accounts/$ACCOUNT_ID/core/v1/groups" \  
\  
--include \  
--header "Content-Type: application/astra-group+json" \  
--header "Accept: */*" \  
--header "Authorization: Bearer $API_TOKEN" \  
--data @JSONinput
```

Exemplo 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"  
}
```

Observe o seguinte sobre os parâmetros de entrada:

- São necessários os seguintes parâmetros:
 - authProvider
 - authID

Exemplo de resposta 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": []  
  }  
}
```

Etapa 2: Adicione uma vinculação de função para o grupo

Execute a seguinte chamada de API REST para vincular o grupo a uma função específica. Você precisa ter o UUID do grupo criado na etapa anterior. Os usuários que são membros do grupo poderão fazer login no Astra após o LDAP executar a autenticação.

Método HTTP e endpoint

Essa chamada de API REST usa o método e o endpoint a seguir.

Método HTTP	Caminho
POST	/Accounts/_id/core/v1/roleBindings

Curl exemplo

```
curl --request POST \  
--location \  
"https://astra.example.com/accounts/$ACCOUNT_ID/core/v1/roleBindings" \  
--include \  
--header "Content-Type: application/astra-roleBinding+json" \  
--header "Accept: */*" \  
--header "Authorization: Bearer $API_TOKEN" \  
--data @JSONinput
```

Exemplo de entrada JSON

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

Observe o seguinte sobre os parâmetros de entrada:

- O valor utilizado acima para `roleConstraint` é a única opção disponível para a versão atual do Astra. Ele indica que o usuário não está restrito a certos namespaces e pode acessá-los todos.

Exemplo de resposta 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": ["*"]
}
```

Observe o seguinte sobre os parâmetros de resposta:

- O valor `group` para o `principalType` campo indica que a vinculação de função foi adicionada para um grupo (não para um usuário).

Desativar e repor LDAP

Há duas tarefas administrativas opcionais relacionadas que você pode executar conforme necessário para uma implantação do Astra Control Center. Pode desativar globalmente a autenticação LDAP e repor a configuração LDAP.

Ambas as tarefas de fluxo de trabalho exigem o `id` para a `astra.account.ldap` configuração Astra. Detalhes sobre como recuperar o ID de configuração estão incluídos em **Configurar o servidor LDAP**. Consulte ["Recupere o UUID da configuração LDAP"](#) para obter mais informações.

- ["Desativar a autenticação LDAP"](#)
- ["Redefina a configuração de autenticação LDAP"](#)

Desativar a autenticação LDAP

Você pode executar a seguinte chamada de API REST para desativar globalmente a autenticação LDAP para uma implantação específica do Astra. A chamada atualiza a `astra.account.ldap` configuração e o `isEnabled` valor é definido como `false`.

Método HTTP e endpoint

Essa chamada de API REST usa o método e o endpoint a seguir.

Método HTTP	Caminho
COLOQUE	/accounts/_id/core/v1/settings//setting_id

```
curl --request PUT \  
--location \  
"https://astra.example.com/accounts/$ACCOUNT_ID/core/v1/settings/<SETTING_ID>" \  
--include \  
--header "Content-Type: application/astra-setting+json" \  
--header "Accept: */*" \  
--header "Authorization: Bearer $API_TOKEN" \  
--data @JSONinput
```

Exemplo 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"  
  }  
}
```

Se a chamada for bem-sucedida, a HTTP 204 resposta será retornada. Opcionalmente, você pode recuperar as configurações novamente para confirmar a alteração.

Redefina a configuração de autenticação LDAP

Você pode executar a seguinte chamada de API REST para desconectar o Astra do servidor LDAP e redefinir a configuração LDAP no Astra. A chamada atualiza a `astra.account.ldap` configuração e o valor de `connectionHost` é apagado.

O valor de `isEnabled` também deve ser definido como `false`. Você pode definir esse valor antes de fazer a chamada de redefinição ou como parte de fazer a chamada de redefinição. No segundo caso, `connectionHost` deve ser limpo e `isEnabled` definido como `false` na mesma chamada de redefinição.



Esta é uma operação disruptiva e você deve prosseguir com cuidado. Elimina todos os utilizadores e grupos LDAP importados. Ele também exclui todos os usuários, grupos e roleBindings relacionados do Astra (tipo LDAP) que você criou no Astra Control Center.

Método HTTP e endpoint

Essa chamada de API REST usa o método e o endpoint a seguir.

Método HTTP	Caminho
COLOQUE	/accounts/_id/core/v1/settings//setting_id

```
curl --request PUT \  
--location \  
"https://astra.example.com/accounts/$ACCOUNT_ID/core/v1/settings/<SETTING_ID>" \  
--include \  
--header "Content-Type: application/astra-setting+json" \  
--header "Accept: */*" \  
--header "Authorization: Bearer $API_TOKEN" \  
--data @JSONinput
```

Exemplo 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"  
  }  
}
```

Observe o seguinte:

- Para alterar o servidor LDAP, você deve desabilitar e redefinir a alteração LDAP `connectHost` para um valor nulo, como mostrado no exemplo acima.
- Se a chamada for bem-sucedida, a HTTP 204 resposta será retornada. Opcionalmente, você pode recuperar a configuração novamente para confirmar a alteração.

Informações sobre direitos autorais

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.