LDAP 組態

Astra Automation

NetApp
March 07, 2024

目錄

LDAP 組態 1
準備 LDAP 組態 1
設定Astra使用LDAP伺服器 2
將LDAP項目新增至Astra 11
停用並重設LDAP 17

LDAP 組態

準備 LDAP 組態

您可以選擇性地將Astra Control Center與輕量型目錄存取傳輸協定（LDAP）伺服器整合、以便為選取的Astra使用者執行驗證。LDAP是存取分散式目錄資訊的業界標準傳輸協定、也是企業驗證的熱門選擇。

相關資訊

- "LDAP技術規格藍圖"
- "LDAP版本3"

實作程序總覽

在高層級上、您需要執行幾個步驟來設定LDAP伺服器、以便為Astra使用者提供驗證。

> 雖然下列步驟依序顯示、但在某些情況下、您可以依照不同的順序執行這些步驟。例如、您可以先定義Astra使用者和群組、再設定LDAP伺服器。

1. 檢閱 "要求與限制" 以瞭解選項、需求及限制。
2. 選取LDAP伺服器和所需的組態選項（包括安全性）。
3. 執行工作流程 "設定Astra使用LDAP伺服器" 將Astra與LDAP伺服器整合。
4. 檢閱LDAP伺服器上的使用者和群組、確定其定義正確。
5. 在中執行適當的工作流程 "將LDAP項目新增至Astra" 識別要使用LDAP驗證的使用者。

要求與限制

您應該先檢閱下列Astra組態基本要點、包括限制和組態選項、再將Astra設定為使用LDAP進行驗證。

僅**Astra**控制中心支援

Astra Control平台提供兩種部署模式。LDAP驗證僅支援Astra Control Center部署。

使用**REST API**或**Web**使用者介面進行組態設定

目前版本的Astra Control Center支援使用Astra Control REST API和Astra網路使用者介面來組態LDAP驗證。

需要**LDAP**伺服器

您必須擁有LDAP伺服器、才能接受及處理Astra驗證要求。Microsoft的Active Directory受目前Astra Control Center版本支援。

安全連線至**LDAP**伺服器

在Astra中設定LDAP伺服器時、您可以選擇性地定義安全連線。在此情況下、LDAPS傳輸協定需要憑證。

設定使用者或群組

您需要選取要使用LDAP驗證的使用者。您可以透過識別個別使用者或使用者群組來執行此作業。帳戶必須

在LDAP伺服器上定義。也需要在Astra（類型LDAP）中識別這些驗證要求、以便將驗證要求轉送到LDAP。

連結使用者或群組時的角色限制

目前推出的Astra Control Center是唯一支援的值 `roleConstraint` 為「*」。這表示使用者不受限於一組有限的命名空間、而且可以存取所有命名空間。請參閱 "將LDAP項目新增至Astra" 以取得更多資訊。

LDAP認證

LDAP使用的認證資料包括使用者名稱（電子郵件地址）和相關密碼。

獨特的電子郵件地址

Astra Control Center部署中所有以使用者名稱身分使用的電子郵件地址都必須是唯一的。您無法使用已定義為Astra的電子郵件地址新增LDAP使用者。如果存在重複的電子郵件、您必須先從Astra刪除。請參閱 "移除使用者" 如需詳細資訊、請參閱Astra Control Center文件網站。

（可選）先定義**LDAP**使用者和群組

您可以將LDAP使用者和群組新增至Astra Control Center、即使LDAP中尚未存在或LDAP伺服器尚未設定亦然。這可讓您在設定LDAP伺服器之前預先設定使用者和群組。

在多個**LDAP**群組中定義的使用者

如果LDAP使用者屬於多個LDAP群組、且已在Astra中指派不同的角色、則使用者在驗證時的有效角色將是最具權限的角色。例如、如果指派給使用者 `viewer` 角色與群組1、但具有 `member` 角色在群組2中、使用者的角色是 `member`。這是根據Astra（最高至最低）所使用的階層架構而定：

- 擁有者
- 管理
- 成員
- 檢視者

定期帳戶同步

Astra大約每60秒將IT的使用者和群組與LDAP伺服器同步一次。因此、如果將使用者或群組新增至LDAP或從LDAP移除、可能需要一分鐘的時間才能在Astra中使用。

停用及重設**LDAP**組態

在嘗試重設LDAP組態之前、您必須先停用LDAP驗證。此外、也可變更LDAP伺服器 (`connectionHost`）、您必須同時執行這兩項作業。請參閱 "停用並重設LDAP" 以取得更多資訊。

REST API參數

LDAP組態工作流程會呼叫REST API來完成特定工作。每個API呼叫都可以包含輸入參數、如所提供的範例所示。請參閱 "線上API參考" 以取得如何找到參考文件的相關資訊。

設定Astra使用LDAP伺服器

您需要選取LDAP伺服器、並設定Astra以使用伺服器做為驗證供應商。組態工作包含下列步驟。每個步驟都包含單一REST API呼叫。

1.新增CA憑證

執行下列REST API呼叫、將CA憑證新增至Astra。

此步驟為選用步驟、只有當您希望Astra和LDAP透過使用LDAPS的安全通道進行通訊時才需要執行。

HTTP方法	路徑
貼文	/Accounts / {account_id} /核心/ v1/certificates

JSONN輸入範例

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

請注意下列關於輸入參數的資訊：

- `cert` 是Json字串、其中包含一個已編碼的64位元的PKCS-11格式化憑證（PES編碼）。
- `isSelfSigned` 應設為 `true` 如果憑證是自我簽署的。預設值為 `false`。

Curl範例

```
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>'
```

JSONN回應範例

```
{
  "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.新增連結認證資料

執行下列REST API呼叫以新增繫結認證。

HTTP方法	路徑
貼文	/Accounts / {account_id} /核心/ v1 /認證

JSONN輸入範例

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

請注意下列關於輸入參數的資訊：

- `bindDn` 和 `password` 是LDAP管理使用者的基礎64編碼繫結認證、可連線及搜尋LDAP目錄。 `bindDn` 為LDAP使用者的電子郵件地址。

Curl範例

```
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>'
```

JSONN回應範例

```
{
    "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"
    }
}
```

請注意下列回應參數：

- 。 `id` 的認證資料會用於後續的工作流程步驟。

3.擷取LDAP設定的UUID

執行下列REST API呼叫、以擷取的UUID `astra.account.ldap` Astra Control Center隨附的設定。

下列Curl範例使用查詢參數來篩選設定集合。您可以移除篩選條件、以取得所有設定、然後搜尋 `astra.account.ldap`。

HTTP方法	路徑
取得	/Accounts / {account_id} /核心/ v1/settings

Curl範例

```
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>'
```

JSONN回應範例

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

4.更新**LDAP**設定

執行下列REST API呼叫、以更新LDAP設定並完成組態。使用 `id` 先前API呼叫的值 `<SETTING_ID>` URL路徑中的值。

您可以先發出特定設定的Get要求、以查看configSchema。這將提供組態中必要欄位的詳細資訊。

HTTP方法	路徑
放入	/Accounts / {account_id} /核心/ v1/settings / {setting_id}

JSONN輸入範例

```
{
  "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"
    }
}
```

請注意下列關於輸入參數的資訊：

- `isEnabled` 應設為 `true` 或可能發生錯誤。
- `credentialId` 是先前建立的連結認證資料ID。
- `secureMode` 應設為 `LDAP` 或 `LDAPS` 根據您在先前步驟中的組態。

- 廠商僅支援「Active Directory」。

Curl範例

```
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>'
```

如果通話成功、則會傳回HTTP 204回應。

5.擷取LDAP設定

您可以選擇性地執行下列REST API呼叫、以擷取LDAP設定並確認更新。

HTTP方法	路徑
取得	/Accounts / {account_id} /核心/ v1/settings / {setting_id}

Curl範例

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

JSONN回應範例

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

找到 `state` 回應中的欄位、其值如下表所示。

州/省	說明
擱置中	組態程序仍在作用中、尚未完成。
有效	組態已成功完成且 `currentConfig` 在回應中相符 `desiredConfig`。
錯誤	LDAP組態程序失敗。

將LDAP項目新增至Astra

將LDAP設定為Astra Control Center的驗證提供者之後、您可以選取Astra將使用LDAP認證進行驗證的LDAP使用者。每位使用者必須在Astra中扮演角色、才能透過Astra Control REST API存取Astra。

您可以使用兩種方式設定Astra來指派角色。選擇適合您環境的產品。

- "新增及連結個別使用者"
- "新增及繫結群組"

LDAP認證資料的形式為使用者名稱、電子郵件地址及相關的LDAP密碼。

新增及連結個別使用者

您可以指派角色給LDAP驗證後所使用的每個Astra使用者。當使用者人數不多、而且每個使用者可能具有不同的管理特性時、這是適當的做法。

1.新增使用者

執行下列REST API呼叫、將使用者新增至Astra、並指出LDAP為驗證提供者。

HTTP方法	路徑
貼文	/Accounts / {account_id} /核心/ v1 /使用者

JSONN輸入範例

```
{
  "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"
}
```

請注意下列關於輸入參數的資訊：

- 需要下列參數：
  - `authProvider`
  - `authID`
  - `email`
- `authID` 是LDAP中使用者的辨別名稱（DN）
- `email` 對於Astra中定義的所有使用者而言、必須是唯一的

如果是 `email` 值並非唯一、會發生錯誤、並傳回回應中的409 HTTP狀態代碼。

Curl範例

```
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>'
```

JSONN回應範例

```
{
  "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.新增使用者的角色繫結

執行下列REST API呼叫、將使用者繫結至特定角色。您必須擁有上一步建立的使用者UUID。

HTTP方法	路徑
貼文	/Accounts / ｛account_id｝/核心/ v1/roleBindings

JSONN輸入範例

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

請注意下列關於輸入參數的資訊：

- 上述使用的值 `roleConstraint` 是目前Astra版本唯一可用的選項。這表示使用者不受限於一組有限的命名空間、而且可以全部存取。

Curl範例

```
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>'
```

JSONN回應範例

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

請注意下列關於回應參數的資訊：

- 價值 `user` 適用於 `principalType` 欄位表示已為使用者（而非群組）新增角色繫結。

新增及繫結群組

您可以將角色指派給Astra群組、此群組在LDAP驗證之後使用。當使用者數量眾多、而且每個使用者可能具有類似的管理特性時、這是適當的做法。

1.新增群組

執行下列REST API呼叫、將群組新增至Astra、並指出LDAP為驗證提供者。

HTTP方法	路徑
貼文	/Accounts / {account_id} /核心/ v1/Groups

JSONN輸入範例

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

請注意下列關於輸入參數的資訊：

- 需要下列參數：
  - `authProvider`
  - `authID`

Curl範例

```
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>'
```

JSONN回應範例

```
{
  "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.新增群組的角色繫結

執行下列REST API呼叫、將群組繫結至特定角色。您必須擁有上一步建立的群組UUID。在LDAP執行驗證之後、屬於群組成員的使用者將能夠登入Astra。

HTTP方法	路徑
貼文	/Accounts / {account_id} /核心/ v1/roleBindings

JSONN輸入範例

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

請注意下列關於輸入參數的資訊：

- 上述使用的值 `roleConstraint` 是目前Astra版本唯一可用的選項。這表示使用者不受限於特定命名空間、而且可以全部存取。

Curl範例

```
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>'
```

JSONN回應範例

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

請注意下列關於回應參數的資訊：

- 價值 `group` 適用於 `principalType` 欄位表示已新增群組的角色繫結（非使用者）。

停用並重設LDAP

您可以視需要執行兩項選用的相關管理工作、以進行Astra Control Center部署。您可以全域停用LDAP驗證並重設LDAP組態。

這兩個工作流程工作都需要的ID `astra.account.ldap` Astra環境。有關如何擷取設定ID的詳細資訊、請參閱*設定LDAP伺服器*。請參閱 "擷取LDAP設定的UUID" 以取得更多資訊。

- "停用 LDAP 驗證"
- "重設LDAP驗證組態"

停用 LDAP 驗證

您可以執行下列REST API呼叫、以全域停用特定Astra部署的LDAP驗證。通話會更新 `astra.account.ldap` 設定和 `isEnabled` 值設為 `false`。

HTTP方法	路徑
放入	/Accounts / {account_id} /核心/ v1/settings / {setting_id}

JSONN輸入範例

```
{
  "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>'
```

如果通話成功、則為 `HTTP 204` 傳回回應。您可以選擇再次擷取組態設定以確認變更。

重設LDAP驗證組態

您可以執行下列REST API呼叫、以中斷Astra與LDAP伺服器的連線、並在Astra中重設LDAP組態。通話會更新 `astra.account.ldap` 設定和值 `connectionHost` 已清除。

的價值 `isEnabled` 也必須設定為 `false`。您可以在進行重設通話之前或在進行重設通話時設定此值。在第二種情況下、 `connectionHost` 應清除及 `isEnabled` 在相同的重設通話中設為假。

這是一項顛覆性的作業、您應該謹慎進行。它會刪除所有匯入的LDAP使用者和群組。它也會刪除您在Astra Control Center中建立的所有相關Astra使用者、群組和角色繫結（LDAP類型）。

HTTP方法	路徑
放入	/Accounts / {account_id} /核心/ v1/settings / {setting_id}

JSONN輸入範例

```
{
  "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"
    }
}
```

請注意下列事項：

- 若要變更LDAP伺服器、您必須停用並重設LDAP變更 `connectHost` 至null值、如上例所示。

```
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>'
```

如果通話成功、則為 `HTTP 204` 傳回回應。您可以選擇再次擷取組態以確認變更。