身分識別與存取

Astra Automation

NetApp
August 11, 2025

This PDF was generated from https://docs.netapp.com/zh-tw/astra-automation/workflows_infra/wf_list_users.html on August 11, 2025. Always check docs.netapp.com for the latest.

目錄

身分識別與存取 1
列出使用者 1
建立使用者 2
步驟 1 ：選取使用者名稱 2
步驟 2 ：建立使用者 2
步驟 3 ：選擇性地選取允許的命名空間 4
步驟 4 ：將使用者繫結至角色 4
步驟 5 ：建立認證 5

身分識別與存取

列出使用者

您可以列出針對特定Astra帳戶所定義的使用者。

HTTP 方法和端點

此 REST API 呼叫使用下列方法和端點。

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

其他輸入參數

除了所有REST API呼叫通用的參數之外、此步驟的Curl範例也會使用下列參數。

參數	類型	必要	說明
包括	查詢	否	選擇性地選取您要傳回回應中的值。

Curl範例：傳回所有使用者的所有資料

```
curl --request GET \
--location "https://astra.netapp.io/accounts/$ACCOUNT_ID/core/v1/users" \
--include \
--header "Accept: */*" \
--header "Authorization: Bearer $API_TOKEN"
```

捲曲範例：傳回所有使用者的名字、姓氏和 **ID**

```
curl --request GET \
--location
"https://astra.netapp.io/accounts/$ACCOUNT_ID/core/v1/users?include=firstN
ame,lastName,id" \
--include \
--header "Accept: */*" \
--header "Authorization: Bearer $API_TOKEN"
```

Json輸出範例

```
{
  "items": [
    [
    "David",
    "Anderson",
    "844ec6234-11e0-49ea-8434-a992a6270ec1"
    ],
    [
      "Jane",
      "Cohen",
      "2a3e227c-fda7-4145-a86c-ed9aa0183a6c"
    ]
  ],
  "metadata": {}
}
```

建立使用者

您可以建立具有特定認證和預先定義角色的使用者。您也可以選擇性地限制使用者對特定命名空間的存取。

步驟 1 ：選取使用者名稱

執行工作流程 "列出使用者" 並選取目前未使用的可用名稱。

步驟 2 ：建立使用者

執行下列REST API呼叫以建立使用者。成功完成通話之後、新使用者將無法使用。

HTTP 方法和端點

此 REST API 呼叫使用下列方法和端點。

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

Curl範例

```
curl --request POST \
--location "https://astra.netapp.io/accounts/$ACCOUNT_ID/core/v1/users" \
--include \
--header "Accept: */*" \
--header "Authorization: Bearer $API_TOKEN" \
--data  @JSONinput
```

JSONN輸入範例

```
{
  "type" :  "application/astra-user",
  "version" : "1.1",
  "firstName" : "John",
  "lastName" : "West",
  "email" : "jwest@example.com"
}
```

Json輸出範例

```
{
    "metadata": {
        "creationTimestamp": "2022-11-20T17:23:15Z",
        "modificationTimestamp": "2022-11-20T17:23:15Z",
        "createdBy": "a20e91f3-2c49-443b-b240-615d940ec5f3",
        "labels": []
    },
    "type": "application/astra-user",
    "version": "1.2",
    "id": "d07dac0a-a328-4840-a216-12de16bbd484",
    "authProvider": "local",
    "authID": "jwest@example.com",
    "firstName": "John",
    "lastName": "West",
    "companyName": "",
    "email": "jwest@example.com",
    "postalAddress": {
        "addressCountry": "",
        "addressLocality": "",
        "addressRegion": "",
        "streetAddress1": "",
        "streetAddress2": "",
        "postalCode": ""
    },
    "state": "active",
    "sendWelcomeEmail": "false",
    "isEnabled": "true",
    "isInviteAccepted": "true",
    "enableTimestamp": "2022-11-20T17:23:15Z",
    "lastActTimestamp": ""
}
```

步驟 3 ：選擇性地選取允許的命名空間

執行工作流程 "列出命名空間" 然後選取您要限制存取的命名空間。

步驟 4 ：將使用者繫結至角色

執行下列REST API呼叫、將使用者繫結至角色。以下範例對命名空間存取沒有任何限制。請參閱 "增強的RBAC與命名空間精細度" 以取得更多資訊。

HTTP 方法和端點

此 REST API 呼叫使用下列方法和端點。

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

Curl範例

```
curl --request POST \
--location
"https://astra.netapp.io/accounts/$ACCOUNT_ID/core/v1/roleBindings" \
--include \
--header "Accept: */*" \
--header "Authorization: Bearer $API_TOKEN" \
--data  @JSONinput
```

JSONN輸入範例

```
{
  "type" :  "application/astra-roleBinding",
  "version" : "1.1",
  "userID" : "d07dac0a-a328-4840-a216-12de16bbd484",
  "accountID" : "29e1f39f-2bf4-44ba-a191-5b84ef414c95",
  "role" : "viewer",
  "roleConstraints": [ "*" ]
}
```

步驟 5 ：建立認證

執行下列REST API呼叫、以建立認證並將其與使用者建立關聯。此範例使用以base64值提供的密碼。。 `name` 內容應包含上一步傳回的使用者ID。輸入內容 `change` 也必須以base64編碼、並決定使用者是否必須在第一次登入時變更密碼 (`true` 或 `false`) 。

> 此步驟僅適用於使用本機驗證的Astra Control Center部署。使用LDAP或Astra Control Service部署的Astra Control Center不需要此功能。

HTTP 方法和端點

此 REST API 呼叫使用下列方法和端點。

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

Curl範例

```
curl --request POST \
--location
"https://astra.netapp.io/accounts/$ACCOUNT_ID/core/v1/credentials" \
--include \
--header "Accept: */*" \
--header "Authorization: Bearer $API_TOKEN" \
--data  @JSONinput
```

JSONN輸入範例

```
{
  "type" :  "application/astra-credential",
  "version" : "1.1",
  "name" : "d07dac0a-a328-4840-a216-12de16bbd484",
  "keyType" : "passwordHash",
  "keyStore" : {
      "cleartext" : "TmV0QXBwMTIz",
      "change" : "ZmFsc2U="
  },
  "valid" : "true"
}
```

版權資訊

Copyright © 2025 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變更本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。 美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 http://www.netapp.com/TM 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。