Identité et accès

Astra Automation

NetApp
December 01, 2023

Sommaire

Identité et accès

Dressez la liste des utilisateurs

Vous pouvez lister les utilisateurs définis pour un compte Astra spécifique.

1. Dressez la liste des utilisateurs

Effectuez l'appel de l'API REST suivant.

Méthode HTTP	Chemin
OBTENEZ	/accounts/{account_id}/core/v1/users

Paramètres d'entrée supplémentaires

Outre les paramètres communs à tous les appels API REST, les paramètres suivants sont également utilisés dans les exemples de boucles pour cette étape.

Paramètre	Type	Obligatoire	Description
inclure	Requête	Non	Sélectionner éventuellement les valeurs que vous souhaitez renvoyer dans la réponse.

Exemple Curl : renvoie toutes les données pour tous les utilisateurs

```
curl --location -i --request GET
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/core/v1/users' --header
'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

Exemple Curl : renvoie le prénom, le nom et l'ID de tous les utilisateurs

```
curl --location -i --request GET
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/core/v1/users?include=first
Name,lastName,id' --header 'Accept: */*' --header 'Authorization: Bearer
<API_TOKEN>'
```

Exemple de sortie JSON

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

Créer un utilisateur

Vous pouvez créer un utilisateur avec des informations d'identification spécifiques et un rôle prédéfini. Vous pouvez également restreindre l'accès de l'utilisateur à des espaces de noms spécifiques.

1. Sélectionnez un nom d'utilisateur

Exécutez le flux de travail "Répertorier les utilisateurs" et sélectionnez un nom disponible qui n'est pas actuellement utilisé.

2. Créez l'utilisateur

Effectuez l'appel de l'API REST suivant pour créer un utilisateur. Une fois l'appel terminé, le nouvel utilisateur ne sera pas encore utilisable.

Méthode HTTP	Chemin
POST	/accounts/{account_id}/core/v1/users

Exemple d'entrée JSON

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

Exemple de boucle

```
curl --location -i --request POST
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/core/v1/users' --header
'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>' --data
@JSONinput
```

Exemple de sortie JSON


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


3. Sélectionner éventuellement les espaces de noms autorisés

Exécutez le flux de travail "Lister les espaces de noms" et sélectionnez les espaces de noms auxquels vous souhaitez limiter l'accès.

4. Lier l'utilisateur à un rôle

Exécutez l'appel d'API REST suivant pour lier l'utilisateur à un rôle. L'exemple ci-dessous n'impose aucune restriction sur l'accès à l'espace de noms. Voir "RBAC amélioré avec granularité de l'espace de noms" pour en savoir plus.

Méthode HTTP	Chemin
POST	/Accounts/{account_ID}/core/v1/roleBindings

Exemple d'entrée JSON

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

Exemple de boucle

```
curl --location -i --request POST
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/core/v1/roleBindings'
--header 'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>' --data
@JSONinput
```

5. Créez une information d'identification

Effectuez l'appel de l'API REST suivant pour créer un identifiant et l'associer à l'utilisateur. Dans cet exemple, un mot de passe est fourni sous la forme d'une valeur base64. Le `name` La propriété doit contenir l'ID de l'utilisateur renvoyé à l'étape précédente. La propriété d'entrée `change` doit également être encodé en base64 et déterminer si l'utilisateur doit modifier son mot de passe lors de la première connexion (`true` ou `false`).

> Cette étape est uniquement requise avec les déploiements Astra Control Center utilisant l'authentification locale. Il n'est pas nécessaire de déployer Astra Control Center avec LDAP ou avec Astra Control Service.

Méthode HTTP	Chemin
POST	/accounts/{account_id}/core/v1/credentials

Exemple d'entrée JSON

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

Exemple de boucle

```
curl --location -i --request POST
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/core/v1/credentials'
--header 'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>' --data
@JSONinput
```

Informations sur le copyright

Informations sur les marques commerciales