



Workflows d'infrastructure

Astra Automation

NetApp
December 01, 2023

Sommaire

- Workflows d'infrastructure 1
 - Avant de commencer 1
 - Identité et accès 1
 - Configuration LDAP 6
 - Clusters 25
 - Cloud 32
 - Seaux 32
 - Stockage 33

Workflows d'infrastructure

Avant de commencer

Vous pouvez utiliser ces workflows pour créer et entretenir l'infrastructure utilisée avec un déploiement d'Astra Control Center. Dans de nombreux cas, les flux de travail peuvent également être utilisés avec le service Astra Control.



Il est possible de développer et d'améliorer ces flux de travail par NetApp à tout moment, et nous vous recommandons de les consulter régulièrement.

Préparation générale

Avant d'utiliser l'un des flux de travail Astra, veuillez à le lire "[Préparez l'utilisation des workflows](#)".

Catégories de flux de travail

Les workflows d'infrastructure sont organisés selon différentes catégories, pour faciliter la localisation.

Catégorie	Description
Identité et accès	Ces flux de travail vous permettent de gérer les identités et d'accéder à Astra. Les ressources comprennent les utilisateurs, les informations d'identification et les jetons.
Configuration LDAP	Vous pouvez configurer Astra Control Center pour qu'il utilise LDAP pour authentifier les utilisateurs sélectionnés.
Clusters	Vous pouvez ajouter des clusters Kubernetes gérés, ce qui vous permet de protéger et de prendre en charge les applications qu'ils contiennent.
Cloud	Ces workflows permettent d'accéder aux clouds disponibles via l'API REST d'Astra Control.
Seaux	Vous pouvez utiliser ces workflows pour créer et gérer les compartiments S3 utilisés pour stocker les sauvegardes.
Stockage	Ces workflows permettent d'ajouter et de gérer des volumes et des systèmes back-end de stockage.

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
```

Configuration LDAP

Préparez la configuration LDAP

Vous pouvez intégrer Astra Control Center avec un serveur LDAP (Lightweight Directory Access Protocol) pour effectuer l'authentification pour certains utilisateurs Astra. LDAP est un protocole standard de l'industrie pour l'accès aux informations d'annuaires distribués et un choix populaire pour l'authentification d'entreprise.

Informations associées

- ["Spécification technique LDAP feuille de route"](#)
- ["LDAP version 3"](#)

Aperçu du processus de mise en œuvre

À un niveau élevé, il existe plusieurs étapes à suivre pour configurer un serveur LDAP afin de fournir une authentification aux utilisateurs d'Astra.



Bien que les étapes présentées ci-dessous se trouvent dans une séquence, vous pouvez dans certains cas les exécuter dans un ordre différent. Par exemple, vous pouvez définir les utilisateurs et les groupes Astra avant de configurer le serveur LDAP.

1. Révision ["Exigences et restrictions"](#) connaître les options, les exigences et les limites.
2. Sélectionnez un serveur LDAP et les options de configuration souhaitées (y compris la sécurité).
3. Exécutez le flux de travail ["Configurez Astra pour qu'il utilise un serveur LDAP"](#) Pour intégrer Astra avec le

serveur LDAP.

4. Vérifiez les utilisateurs et les groupes du serveur LDAP pour vous assurer qu'ils sont correctement définis.
5. Exécutez le flux de travail approprié dans "[Ajoutez des entrées LDAP à Astra](#)" Identifier les utilisateurs à authentifier à l'aide de LDAP.

Exigences et restrictions

Nous vous recommandons de consulter les éléments essentiels de configuration Astra présentés ci-dessous, y compris les limites et les options de configuration, avant de configurer Astra pour utiliser LDAP pour l'authentification.

Uniquement pris en charge avec Astra Control Center

La plateforme Astra Control propose deux modèles de déploiement. L'authentification LDAP est prise en charge uniquement avec les déploiements d'Astra Control Center.

Configuration via l'API REST ou l'interface utilisateur Web

La version actuelle d'Astra Control Center prend en charge la configuration de l'authentification LDAP à l'aide de l'API REST Astra Control et de l'interface utilisateur Web Astra.

Serveur LDAP requis

Vous devez disposer d'un serveur LDAP pour accepter et traiter les demandes d'authentification Astra. Microsoft Active Directory est pris en charge avec la version actuelle d'Astra Control Center.

Connexion sécurisée au serveur LDAP

Lors de la configuration du serveur LDAP dans Astra, vous pouvez éventuellement définir une connexion sécurisée. Dans ce cas, un certificat est nécessaire pour le protocole LDAPS.

Configurer des utilisateurs ou des groupes

Vous devez sélectionner les utilisateurs à authentifier à l'aide de LDAP. Pour ce faire, vous pouvez identifier les utilisateurs individuels ou un groupe d'utilisateurs. Les comptes doivent être définis au niveau du serveur LDAP. Elles doivent également être identifiées dans Astra (type LDAP) qui permet de transférer les demandes d'authentification vers LDAP.

Contrainte de rôle lors de la liaison d'un utilisateur ou d'un groupe

Avec la version actuelle d'Astra Control Center, la seule valeur prise en charge pour `roleConstraint` est `""`. Cela indique que l'utilisateur n'est pas limité à un ensemble limité d'espaces de noms et qu'il peut y accéder tous. Voir "[Ajoutez des entrées LDAP à Astra](#)" pour en savoir plus.

Informations d'identification LDAP

Les informations d'identification utilisées par LDAP incluent le nom d'utilisateur (adresse e-mail) et le mot de passe associé.

Adresses e-mail uniques

Toutes les adresses e-mail agissant comme noms d'utilisateur dans un déploiement Astra Control Center doivent être uniques. Vous ne pouvez pas ajouter un utilisateur LDAP avec une adresse e-mail déjà définie pour Astra. Si un e-mail en double existe, vous devez d'abord le supprimer d'Astra. Voir "[Supprimer des utilisateurs](#)" Sur le site de documentation Astra Control Center pour plus d'informations.

Vous pouvez éventuellement définir d'abord les utilisateurs et les groupes LDAP

Vous pouvez ajouter les utilisateurs et groupes LDAP au Centre de contrôle Astra même s'ils n'existent pas encore dans LDAP ou si le serveur LDAP n'est pas configuré. Cela vous permet de préconfigurer les utilisateurs et les groupes avant de configurer le serveur LDAP.

Utilisateur défini dans plusieurs groupes LDAP

Si un utilisateur LDAP appartient à plusieurs groupes LDAP et que des rôles différents ont été attribués aux groupes dans Astra, le rôle effectif de l'utilisateur lors de l'authentification sera le plus privilégié. Par exemple, si un utilisateur est affecté à l' `viewer` rôle avec `groupe1` mais a le `member` rôle dans le `groupe 2`, le rôle de l'utilisateur serait `member`. Ceci est basé sur la hiérarchie utilisée par Astra (la plus haute à la plus basse) :

- Propriétaire
- Admin
- Membre
- Visualiseur

Synchronisation périodique du compte

Astra synchronise ses utilisateurs et groupes avec le serveur LDAP environ toutes les 60 secondes. Par conséquent, si un utilisateur ou un groupe est ajouté à LDAP ou supprimé, il peut prendre jusqu'à une minute avant qu'il soit disponible dans Astra.

Désactivation et réinitialisation de la configuration LDAP

Avant de tenter de réinitialiser la configuration LDAP, vous devez d'abord désactiver l'authentification LDAP. De même, pour modifier le serveur LDAP (`connectionHost`), vous devez effectuer les deux opérations. Voir "[Désactivez et réinitialisez LDAP](#)" pour en savoir plus.

Paramètres de l'API REST

Les workflows de configuration LDAP appellent l'API REST pour accomplir des tâches spécifiques. Chaque appel API peut inclure des paramètres d'entrée comme indiqué dans les échantillons fournis. Voir "[Référence d'API en ligne](#)" pour plus d'informations sur la localisation de la documentation de référence.

Configurez Astra pour qu'il utilise un serveur LDAP

Vous devez sélectionner un serveur LDAP et configurer Astra pour qu'il utilise le serveur en tant que fournisseur d'authentification. La tâche de configuration comprend les étapes décrites ci-dessous. Chaque étape inclut un appel d'API REST unique.

1. Ajoutez un certificat CA

Effectuez l'appel d'API REST suivant pour ajouter un certificat d'autorité de certification à Astra.



Cette étape est facultative et requise uniquement si vous voulez qu'Astra et le LDAP communiquent via un canal sécurisé à l'aide de LDAPS.

Méthode HTTP	Chemin
POST	<code>/accounts/{account_id}/core/v1/certificats</code>

Exemple d'entrée JSON

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

Notez les informations suivantes concernant les paramètres d'entrée :

- `cert` Est une chaîne JSON contenant un certificat au format PKCS-11 codé en base64 (codé PEM).
- `isSelfSigned` doit être réglé sur `true` si le certificat est auto-signé. La valeur par défaut est `false`.

Exemple de boucle

```
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>'
```

Exemple de réponse JSON

```

{
  "type": "application/astra-certificate",
  "version": "1.0",
  "id": "a5212e7e-402b-4cff-bba0-63f3c6505199",
  "certUse": "rootCA",
  "cert": "LS0tLS1CRUdJTtiBDRVJUSUZJQ0FURS0tLS0tCk1JSUMyVEN",
  "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. Ajoutez les informations d'identification de liaison

Effectuez l'appel d'API REST suivant pour ajouter les informations d'identification de liaison.

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

Exemple d'entrée JSON

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

Notez les informations suivantes concernant les paramètres d'entrée :

- `bindDn` et `password` Sont les informations d'identification de liaison codées en base64 de l'utilisateur admin LDAP qui peut se connecter et rechercher dans le répertoire LDAP. `bindDn` Est l'adresse e-mail de l'utilisateur LDAP.

Exemple de boucle

```
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>'
```

Exemple de réponse 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"
  }
}
```

Noter les paramètres de réponse suivants :

- Le `id` des informations d'identification sont utilisées dans les étapes suivantes du flux de travail.

3. Récupérez l'UUID du paramètre LDAP

Exécutez l'appel de l'API REST suivant pour récupérer l'UUID du `astra.account.ldap` Réglage inclus avec le centre de contrôle Astra.



L'exemple curl ci-dessous utilise un paramètre de requête pour filtrer la collection de paramètres. Vous pouvez à la place supprimer le filtre pour obtenir tous les paramètres, puis rechercher `astra.account.ldap`.

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

Exemple de boucle

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

Exemple de réponse JSON

```

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

```

4. Mettez à jour le paramètre LDAP

Effectuez l'appel d'API REST suivant pour mettre à jour le paramètre LDAP et terminer la configuration. Utilisez le id Valeur de l'appel API précédent pour le <SETTING_ID> Valeur dans le chemin d'accès à l'URL ci-dessous.



Vous pouvez d'abord lancer une demande GET pour le paramètre spécifique afin de voir le schéma de configuration. Ceci fournira plus d'informations sur les champs requis dans la configuration.

Méthode HTTP	Chemin
EN	/accounts/{account_id}/core/v1/settings/{setting_id}

Exemple d'entrée 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"
  }
}

```

Notez les informations suivantes concernant les paramètres d'entrée :

- isEnabled doit être réglé sur true ou une erreur peut se produire.

- `credentialId` est l'id des informations d'identification de liaison créées précédemment.
- `secureMode` doit être réglé sur LDAP ou LDAPS en fonction de votre configuration à l'étape précédente.
- Seul Active Directory est pris en charge en tant que fournisseur.

Exemple de boucle

```
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>'
```

Si l'appel a réussi, la réponse HTTP 204 est renvoyée.

5. Récupérez le paramètre LDAP

Vous pouvez éventuellement effectuer l'appel d'API REST suivant pour récupérer les paramètres LDAP et confirmer la mise à jour.

Méthode HTTP	Chemin
OBTENEZ	/accounts/{account_id}/core/v1/settings/{setting_id}

Exemple de boucle

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

Exemple de réponse 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": {}
}

```

Localisez le `state` champ de la réponse qui contient l'une des valeurs du tableau ci-dessous.

État	Description
en attente	Le processus de configuration est toujours actif et n'est pas encore terminé.
valide	La configuration a été effectuée avec succès et <code>currentConfig</code> la réponse correspond <code>desiredConfig</code> .
erreur	Le processus de configuration LDAP a échoué.

Ajoutez des entrées LDAP à Astra

Après avoir configuré LDAP en tant que fournisseur d'authentification pour Astra Control Center, vous pouvez sélectionner les utilisateurs LDAP qu'Astra authentifie à l'aide des informations d'identification LDAP. Chaque utilisateur doit avoir un rôle dans Astra avant d'avoir accès à Astra via l'API REST Astra Control.

Il existe deux façons de configurer Astra pour affecter des rôles. Choisissez celle qui convient le mieux à votre environnement.

- ["Ajouter et lier un utilisateur individuel"](#)
- ["Ajouter et lier un groupe"](#)



Les informations d'identification LDAP se présentent sous la forme d'un nom d'utilisateur sous la forme d'une adresse e-mail et du mot de passe LDAP associé.

Ajouter et lier un utilisateur individuel

Vous pouvez attribuer un rôle à chaque utilisateur Astra qui est utilisé après l'authentification LDAP. Ceci est approprié lorsqu'il y a un petit nombre d'utilisateurs et que chacun peut avoir des caractéristiques administratives différentes.

1. Ajoutez un utilisateur

Effectuez l'appel d'API REST suivant pour ajouter un utilisateur à Astra et indiquer que LDAP est le fournisseur d'authentification.

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

Exemple d'entrée 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"
}
```

Notez les informations suivantes concernant les paramètres d'entrée :

- Les paramètres suivants sont requis :
 - authProvider
 - authID
 - email
- authID Est le nom distinctif (DN) de l'utilisateur dans LDAP
- email Doit être unique pour tous les utilisateurs définis dans Astra

Si le email La valeur n'est pas unique, une erreur se produit et un code d'état HTTP 409 est renvoyé dans la réponse.

Exemple de boucle

```
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>'
```

Exemple de réponse 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. Ajoutez une liaison de rôle pour l'utilisateur

Effectuez l'appel de l'API REST suivant pour lier l'utilisateur à un rôle spécifique. Vous devez créer l'UUID de l'utilisateur à l'étape précédente.

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

Exemple d'entrée JSON

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

Notez les informations suivantes concernant les paramètres d'entrée :

- Valeur utilisée ci-dessus pour `roleConstraint` Est la seule option disponible pour la version actuelle d'Astra. Il indique que l'utilisateur n'est pas limité à un ensemble limité d'espaces de noms et peut y accéder tous.

Exemple de boucle

```
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>'
```

Exemple de réponse 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": ["*"]
}
```

Notez les éléments suivants concernant les paramètres de réponse :

- La valeur `user` pour le `principalType` champ indique que la liaison du rôle a été ajoutée pour un utilisateur (et non pour un groupe).

Ajouter et lier un groupe

Vous pouvez affecter un rôle à un groupe Astra qui est utilisé après l'authentification LDAP. Ceci est approprié lorsqu'il y a un grand nombre d'utilisateurs et que chacun peut avoir des caractéristiques administratives similaires.

1. Ajoutez un groupe

Effectuez l'appel d'API REST suivant pour ajouter un groupe à Astra et indiquer que LDAP est le fournisseur d'authentification.

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

Exemple d'entrée JSON

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

Notez les informations suivantes concernant les paramètres d'entrée :

- Les paramètres suivants sont requis :
 - `authProvider`
 - `authID`

Exemple de boucle

```
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>'
```

Exemple de réponse 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. Ajoutez une liaison de rôle pour le groupe

Effectuez l'appel d'API REST suivant pour lier le groupe à un rôle spécifique. Vous devez créer l'UUID du groupe à l'étape précédente. Les utilisateurs qui sont membres du groupe pourront se connecter à Astra une fois que LDAP aura effectué l'authentification.

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

Exemple d'entrée JSON

```

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

```

Notez les informations suivantes concernant les paramètres d'entrée :

- Valeur utilisée ci-dessus pour `roleConstraint` Est la seule option disponible pour la version actuelle d'Astra. Il indique que l'utilisateur n'est pas limité à certains espaces de noms et peut y accéder tous.

Exemple de boucle


```
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>'
```

Exemple de réponse 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": ["*"]
}
```

Noter les éléments suivants concernant les paramètres de réponse :

- La valeur `group` pour le `principalType` champ indique que la liaison de rôle a été ajoutée pour un groupe (et non pour un utilisateur).

Désactivez et réinitialisez LDAP

Il existe deux tâches administratives facultatives, bien que liées, que vous pouvez effectuer selon vos besoins pour un déploiement de centre de contrôle Astra. Vous pouvez désactiver globalement l'authentification LDAP et réinitialiser la configuration LDAP.

Les deux tâches de flux de travail requièrent l'ID pour le `astra.account.ldap` Réglage Astra. Les détails sur la récupération de l'ID de paramètre sont inclus dans **configurer le serveur LDAP**. Voir ["Récupère l'UUID du paramètre LDAP"](#) pour en savoir plus.

- ["Désactivez l'authentification LDAP"](#)
- ["Réinitialisez la configuration de l'authentification LDAP"](#)

Désactivez l'authentification LDAP

Vous pouvez effectuer l'appel d'API REST suivant pour désactiver globalement l'authentification LDAP pour un déploiement Astra spécifique. L'appel met à jour le `astra.account.ldap` réglage et `isEnabled` la valeur est définie sur `false`.

Méthode HTTP	Chemin
EN	/accounts/{account_id}/core/v1/settings/{setting_id}

Exemple d'entrée 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>'
```

Si l'appel a réussi, le HTTP 204 la réponse est renvoyée. Vous pouvez éventuellement récupérer à nouveau les paramètres de configuration pour confirmer la modification.

Réinitialisez la configuration de l'authentification LDAP

Vous pouvez effectuer l'appel d'API REST suivant pour déconnecter Astra du serveur LDAP et réinitialiser la configuration LDAP dans Astra. L'appel met à jour le `astra.account.ldap` réglage et valeur de `connectionHost` est effacé.

La valeur de `isEnabled` doit également être défini sur `false`. Vous pouvez soit définir cette valeur avant d'effectuer l'appel de réinitialisation, soit dans le cadre de l'appel de réinitialisation. Dans le deuxième cas, `connectionHost` doit être effacé et `isEnabled` défini sur `false` lors du même appel de réinitialisation.



Il s'agit d'une opération perturbatrice et vous devez procéder avec précaution. Elle supprime tous les utilisateurs et groupes LDAP importés. Il supprime également tous les utilisateurs, groupes et liaisons Astra (type LDAP) associés que vous avez créés dans Astra Control Center.

Méthode HTTP	Chemin
EN	/accounts/{account_id}/core/v1/settings/{setting_id}

Exemple d'entrée 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"
  }
}
```

Notez ce qui suit :

- Pour modifier le serveur LDAP, vous devez à la fois désactiver et réinitialiser la modification LDAP connectHost à une valeur nulle comme indiqué dans l'exemple ci-dessus.

```
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>'
```

Si l'appel a réussi, le HTTP 204 la réponse est renvoyée. Vous pouvez éventuellement récupérer à nouveau la configuration pour confirmer la modification.

Clusters

Lister les clusters

Vous pouvez afficher la liste des clusters disponibles dans un cloud spécifique.

1. Sélectionnez le nuage

Exécutez le flux de travail "Lister les clouds" et sélectionnez le cloud contenant les clusters.

2. Dresser la liste des clusters

Effectuez l'appel d'API REST suivant pour répertorier les clusters dans un cloud spécifique.

Méthode HTTP	Chemin
OBTENEZ	/accounts/{account_id}/topologique/v1/nuages/{cloud_id}/clusters

Exemple Curl : renvoie toutes les données de tous les clusters

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

Exemple de sortie JSON

```
{
  "items": [
    {
      "type": "application/astra-cluster",
      "version": "1.1",
      "id": "7ce83fba-6aa1-4e0c-a194-26e714f5eb46",
      "name": "openshift-clstr-ol-07",
      "state": "running",
      "stateUnready": [],
      "managedState": "managed",
      "protectionState": "full",
      "protectionStateDetails": [],
      "restoreTargetSupported": "true",
      "snapshotSupported": "true",
      "managedStateUnready": [],
      "managedTimestamp": "2022-11-03T15:50:59Z",
      "inUse": "true",
      "clusterType": "openshift",
      "accHost": "true",
      "clusterVersion": "1.23",
      "clusterVersionString": "v1.23.12+6b34f32",
      "namespaces": [
        "default",
        "kube-node-lease",
        "kube-public",
```

```
"kube-system",
"metallb-system",
"mysql",
"mysql-clone1",
"mysql-clone2",
"mysql-clone3",
"mysql-clone4",
"netapp-acc-operator",
"netapp-monitoring",
"openshift",
"openshift-apiserver",
"openshift-apiserver-operator",
"openshift-authentication",
"openshift-authentication-operator",
"openshift-cloud-controller-manager",
"openshift-cloud-controller-manager-operator",
"openshift-cloud-credential-operator",
"openshift-cloud-network-config-controller",
"openshift-cluster-csi-drivers",
"openshift-cluster-machine-approver",
"openshift-cluster-node-tuning-operator",
"openshift-cluster-samples-operator",
"openshift-cluster-storage-operator",
"openshift-cluster-version",
"openshift-config",
"openshift-config-managed",
"openshift-config-operator",
"openshift-console",
"openshift-console-operator",
"openshift-console-user-settings",
"openshift-controller-manager",
"openshift-controller-manager-operator",
"openshift-dns",
"openshift-dns-operator",
"openshift-etcd",
"openshift-etcd-operator",
"openshift-host-network",
"openshift-image-registry",
"openshift-infra",
"openshift-ingress",
"openshift-ingress-canary",
"openshift-ingress-operator",
"openshift-insights",
"openshift-kni-infra",
"openshift-kube-apiserver",
"openshift-kube-apiserver-operator",
```

```

    "openshift-kube-controller-manager",
    "openshift-kube-controller-manager-operator",
    "openshift-kube-scheduler",
    "openshift-kube-scheduler-operator",
    "openshift-kube-storage-version-migrator",
    "openshift-kube-storage-version-migrator-operator",
    "openshift-machine-api",
    "openshift-machine-config-operator",
    "openshift-marketplace",
    "openshift-monitoring",
    "openshift-multus",
    "openshift-network-diagnostics",
    "openshift-network-operator",
    "openshift-node",
    "openshift-oauth-apiserver",
    "openshift-openstack-infra",
    "openshift-operator-lifecycle-manager",
    "openshift-operators",
    "openshift-ovirt-infra",
    "openshift-sdn",
    "openshift-service-ca",
    "openshift-service-ca-operator",
    "openshift-user-workload-monitoring",
    "openshift-vsphere-infra",
    "pcloud",
    "postgresql",
    "trident"
  ],
  "defaultStorageClass": "4bacbb3c-0727-4f58-b13c-3a2a069baf89",
  "cloudID": "4f1e1086-f415-4451-a051-c7299cd672ff",
  "credentialID": "7ffd7354-b6c2-4efa-8e7b-cf64d5598463",
  "isMultizonal": "false",
  "tridentManagedStateAllowed": [
    "unmanaged"
  ],
  "tridentVersion": "22.10.0",
  "apiServiceID": "98df44dc-2baf-40d5-8826-e198b1b40909",
  "metadata": {
    "labels": [
      {
        "name": "astra.netapp.io/labels/read-
only/cloudName",
        "value": "private"
      }
    ]
  },
  "creationTimestamp": "2022-11-03T15:50:59Z",

```

```
        "modificationTimestamp": "2022-11-04T14:42:32Z",
        "createdBy": "00000000-0000-0000-0000-000000000000"
    }
}
]
```

Ajouter un cluster à l'aide des informations d'identification

Vous pouvez ajouter un cluster pour qu'il soit géré par Astra. À compter de la version 22.11 de l'Astra, vous pouvez ajouter un groupe d'instruments avec le centre de contrôle Astra et le service de contrôle Astra.



L'ajout d'un cluster n'est pas nécessaire lors de l'utilisation d'un service Kubernetes depuis l'un des principaux fournisseurs cloud (AKS, EKS, GKE).

1. Procurez-vous le fichier kubeconfig

Vous devez obtenir une copie du fichier **kubeconfig** auprès de votre administrateur ou service Kubernetes.

2. Préparez le fichier kubeconfig

Avant d'utiliser le fichier **kubeconfig**, vous devez effectuer les opérations suivantes :

Convertir le fichier du format YAML au format JSON

Si vous recevez le fichier kubeconfig formaté en YAML, vous devez le convertir au format JSON.

Codage JSON en base64

Vous devez coder le fichier JSON en base64.

Exemple

Voici un exemple de conversion du fichier kubeconfig de YAML au JSON, puis de codage dans base64 :

```
yq -o=json ~/.kube/config | base64
```

3. Sélectionnez le Cloud

Exécutez le flux de travail "[Lister les clouds](#)" et sélectionnez le cloud dans lequel le cluster sera ajouté.



Le seul cloud que vous pouvez sélectionner est le **cloud privé**.

4. Créez une information d'identification

Effectuez l'appel de l'API REST suivant pour créer des informations d'identification à l'aide du fichier kubeconfig.

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

Exemple d'entrée JSON

```
{
  "type" : "application/astra-credential",
  "version" : "1.1",
  "name" : "Cloud One",
  "keyType" : "kubeconfig",
  "keyStore" : {
    "base64": encoded_kubeconfig
  },
  "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
```

5. Ajoutez le cluster

Effectuez l'appel d'API REST suivant pour ajouter le cluster au cloud. La valeur du `credentialID` Le champ de saisie est obtenu à partir de l'appel d'API REST à l'étape précédente.

Méthode HTTP	Chemin
POST	/accounts/{account_id}/topologique/v1/nuages/{cloud_id}/clusters

Exemple d'entrée JSON

```
{
  "type" : "application/astra-cluster",
  "version" : "1.1",
  "credentialID": credential_id
}
```

Exemple de boucle

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


Répertoire des clusters gérés

Vous pouvez lister les clusters Kubernetes actuellement gérés par Astra.

1. Dressez la liste des clusters gérés

Effectuez l'appel de l'API REST suivant.

Méthode HTTP	Chemin
OBTENEZ	/Accounts/{account_ID}/topologique/v1/managedclusters

Exemple Curl : renvoie toutes les données de tous les clusters

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

Gérer un cluster

Vous pouvez gérer un cluster Kubernetes afin d'assurer la protection des données.

1. Sélectionnez le cluster à gérer

Exécutez le flux de travail "[Lister les clusters](#)" et sélectionnez le cluster souhaité. La propriété `managedState` du cluster doit être `unmanaged`.

2. Sélectionnez éventuellement la classe de stockage

Éventuellement, exécutez le flux de travail "[Répertoire des classes de stockage](#)" et sélectionnez la classe de stockage souhaitée.



Si vous ne fournissez pas de classe de stockage à l'appel pour gérer le cluster, votre classe de stockage par défaut sera utilisée.

3. Gérez le cluster

Effectuez l'appel d'API REST suivant pour gérer le cluster.

Méthode HTTP	Chemin
POST	/Accounts/{account_ID}/topologique/v1/managedclusters

Exemple d'entrée JSON

```
{
  "type": "application/astra-managedCluster",
  "version": "1.0",
  "id": "d0fdf455-4330-476d-bb5d-4d109714e07d"
}
```

Exemple de boucle

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

Cloud

Lister les clouds

Vous pouvez répertorier les nuages définis et disponibles un compte Astra spécifique.

1. Dresser la liste des clouds

Effectuez l'appel d'API REST suivant pour répertorier les clouds.

Méthode HTTP	Chemin
OBTENEZ	/accounts/{account_id}/topologique/v1/clouds

Exemple de curl : retournez toutes les données de tous les clouds

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

Seaux

Répertorier les rubriques

Vous pouvez afficher la liste des compartiments S3 définis pour un compte Astra spécifique.

1. Dressez la liste des compartiments

Effectuez l'appel suivant de l'API REST pour afficher la liste des compartiments.

Méthode HTTP	Chemin
OBTENEZ	/accounts/{account_id}/topologique/v1/seaux

Exemple de gondolage : renvoie toutes les données de tous les compartiments

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

Stockage

Répertorier les classes de stockage

Vous pouvez afficher la liste des classes de stockage disponibles.

1. Sélectionnez le nuage

Exécutez le flux de travail "[Lister les clouds](#)" et choisissez le cloud dans lequel vous travaillez.

2. Sélectionnez le cluster

Exécutez le flux de travail "[Lister les clusters](#)" et sélectionnez le cluster.

3. Énumérez les classes de stockage d'un cluster spécifique

Effectuez l'appel d'API REST suivant pour répertorier les classes de stockage d'un cluster et d'un cloud spécifiques.

Méthode HTTP	Chemin
OBTENEZ	/Accounts/{account_ID}/topologique/v1/nuages/<CLOUD_ID>/clusters/<CLUSTER_ID>/storageclasses

Exemple Curl : renvoie toutes les données de toutes les classes de stockage

```
curl --location -i --request GET
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/topology/v1/clouds/<CLOUD_ID>/clusters/<CLUSTER_ID>/storageClasses' --header 'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

Exemple de sortie JSON

```
{
  "items": [
    {
```

```

    "type": "application/astra-storageClass",
    "version": "1.1",
    "id": "4bacbb3c-0727-4f58-b13c-3a2a069baf89",
    "name": "ontap-basic",
    "provisioner": "csi.trident.netapp.io",
    "available": "eligible",
    "allowVolumeExpansion": "true",
    "reclaimPolicy": "Delete",
    "volumeBindingMode": "Immediate",
    "isDefault": "true",
    "metadata": {
      "createdBy": "system",
      "creationTimestamp": "2022-10-26T05:16:19Z",
      "modificationTimestamp": "2022-10-26T05:16:19Z",
      "labels": []
    }
  },
  {
    "type": "application/astra-storageClass",
    "version": "1.1",
    "id": "150fe657-4a42-47a3-abc6-5dafba3de8bf",
    "name": "thin",
    "provisioner": "kubernetes.io/vsphere-volume",
    "available": "ineligible",
    "reclaimPolicy": "Delete",
    "volumeBindingMode": "Immediate",
    "metadata": {
      "createdBy": "system",
      "creationTimestamp": "2022-10-26T04:46:08Z",
      "modificationTimestamp": "2022-11-04T14:58:19Z",
      "labels": []
    }
  },
  {
    "type": "application/astra-storageClass",
    "version": "1.1",
    "id": "7c6a5c58-6a0d-4cb6-98a0-8202ad2de74a",
    "name": "thin-csi",
    "provisioner": "csi.vsphere.vmware.com",
    "available": "ineligible",
    "allowVolumeExpansion": "true",
    "reclaimPolicy": "Delete",
    "volumeBindingMode": "WaitForFirstConsumer",
    "metadata": {
      "createdBy": "system",
      "creationTimestamp": "2022-10-26T04:46:17Z",

```

```

        "modificationTimestamp": "2022-10-26T04:46:17Z",
        "labels": []
    }
},
{
    "type": "application/astra-storageClass",
    "version": "1.1",
    "id": "7010ef09-92a5-4c90-a5e5-3118e02dc9a7",
    "name": "vsim-san",
    "provisioner": "csi.trident.netapp.io",
    "available": "eligible",
    "allowVolumeExpansion": "true",
    "reclaimPolicy": "Delete",
    "volumeBindingMode": "Immediate",
    "metadata": {
        "createdBy": "system",
        "creationTimestamp": "2022-11-03T18:40:03Z",
        "modificationTimestamp": "2022-11-03T18:40:03Z",
        "labels": []
    }
}
]
}

```

Liste des systèmes back-end

Vous pouvez lister les systèmes back-end disponibles.

1. Dressez la liste des systèmes back-end

Effectuez l'appel de l'API REST suivant.

Méthode HTTP	Chemin
OBTENEZ	/Accounts/{account_ID}/topologique/v1/storageBackends

Exemple de curl : renvoie toutes les données pour tous les systèmes back-end

```

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

```

Exemple de sortie JSON

```

{
  "items": [
    {
      "backendCredentialsName": "10.191.77.177",
      "backendName": "myinchunhcluster-1",
      "backendType": "ONTAP",
      "backendVersion": "9.8.0",
      "configVersion": "Not applicable",
      "health": "Not applicable",
      "id": "46467c16-1585-4b71-8e7f-f0bc5ff9da15",
      "location": "nalab2",
      "metadata": {
        "createdBy": "4c483a7e-207b-4f9a-87b7-799a4629d7c8",
        "creationTimestamp": "2021-07-30T14:26:19Z",
        "modificationTimestamp": "2021-07-30T14:26:19Z"
      },
      "ontap": {
        "backendManagementIP": "10.191.77.177",
        "managementIPs": [
          "10.191.77.177",
          "10.191.77.179"
        ]
      },
      "protectionPolicy": "Not applicable",
      "region": "Not applicable",
      "state": "Running",
      "stateUnready": [],
      "type": "application/astra-storageBackend",
      "version": "1.0",
      "zone": "Not applicable"
    }
  ]
}

```

Activez des pools ANF dynamiques pour les clusters autogérés

Lors de la sauvegarde d'une application gérée dans un cluster privé sur site doté d'un système back-end de stockage ANF, vous devez activer la fonctionnalité de pools ANF dynamiques. Pour ce faire, il faut fournir un ID d'abonnement à utiliser lors de l'extension et de la réduction des pools de capacité.



Les pools ANF dynamiques sont une fonctionnalité des applications gérées par Astra qui utilisent un système back-end de stockage Azure NetApp Files (ANF). Lors de la sauvegarde de ces applications, Astra multiplie et réduit automatiquement les pools de capacité auxquels les volumes persistants appartiennent par 1.5. Cela permet de s'assurer que l'espace disponible pour la sauvegarde est suffisant sans frais permanents supplémentaires. Voir "[Sauvegardes d'applications Azure](#)" pour en savoir plus.

1. Ajoutez l'identifiant d'abonnement Azure

Effectuez l'appel de l'API REST suivant.



Vous devez mettre à jour l'exemple d'entrée JSON en fonction de votre environnement, y compris l'ID d'abonnement et la valeur base64 du principal de service.

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

Exemple d'entrée JSON

```
{
  "keyStore": {
    "privKey": "SGkh",
    "pubKey": "UGhpcyCpcyBhbiBleGFtcGxlLg==",
    "base64":
    "fwogICAgJmFwcElkIjogIjY4ZmSiODFiLTU0YWYtNDdjNC04ZjUzLWE2NDdlZTUzMGZkZCIsc
    iAgICAiZGlzcGxheU5hbWUiOiAic3AtYXN0cmEtZGV2LXFhIiwKICAgICJuYW11IjogImh0dHA
    6Ly9zcC1hc3RyYS1kZXYtcWEiLAogICAgInBhc3N3b3JkIjogIlllLQThRfk9IVVJkZWZYM0pST
    WJlLnUeFBleVE0UnNwTG9DcUJjazAiLAogICAgInRlbnFudCI6ICIwMTFjZGY2Yy03NTEyLTQ
    3MDUtYjI0ZS03NzIxYWZkOGNhMzciLAogICAgInN1YnNjcmlwdGlvbklkIjogImIyMDAxNTVmL
    TAwMWEtNDNiZS04N2JlLTNlZGRlODNhY2VmNCIKfQ=="
  },
  "name": "myCert",
  "type": "application/astra-credential",
  "version": "1.1",
  "metadata": {
    "labels": [
      {
        "name": "astra.netapp.io/labels/read-only/credType",
        "value": "service-account"
      },
      {
        "name": "astra.netapp.io/labels/read-only/cloudName",
        "value": "OCP"
      },
      {
        "name": "astra.netapp.io/labels/read-only/azure/subscriptionID",
        "value": "b212156f-001a-43be-87be-3edde83acef5"
      }
    ]
  }
}
```

Exemple de boucle

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

2. Ajouter un seuil si nécessaire

Si nécessaire, vous devez ajouter un compartiment à l'application gérée.

3. Sauvegardez l'application gérée

Exécutez le flux de travail "[Créez une sauvegarde pour une application](#)". Le pool de capacité sur lequel se trouve le volume persistant d'origine se développe et diminue automatiquement.

4. Consultez le journal des événements

Les événements d'activité sont consignés pendant la sauvegarde. Exécutez le flux de travail "[Dressez la liste des notifications](#)" pour afficher les messages.

Informations sur le copyright

Copyright © 2023 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.