Flujos de trabajo de infraestructura

Astra Automation

NetApp
August 11, 2025

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

Tabla de contenidos

Flujos de trabajo de infraestructura . . . 1
- Prepárese para usar los flujos de trabajo de infraestructura . . . 1
  - Preparación general . . . 1
  - Categorías de flujo de trabajo . . . 1
- Identidad y acceso . . . 1
  - Enumere los usuarios . . . 1
  - Cree un usuario . . . 3
- Configuración de LDAP . . . 7
  - Prepare la configuración de LDAP . . . 7
  - Configure Astra para que utilice un servidor LDAP . . . 9
  - Agregue entradas LDAP a Astra . . . 18
  - Deshabilite y restablezca LDAP . . . 25
- De clúster . . . 28
  - Enumere los clústeres . . . 28
  - Añada un clúster mediante credenciales . . . 31
  - Enumere los clústeres gestionados . . . 33
  - Gestione un clúster . . . 33
- Nubes . . . 34
  - Enumerar las nubes . . . 34
- Cucharones . . . 35
  - Enumere los cucharones . . . 35
- Reducida . . . 35
  - Enumerar las clases de almacenamiento . . . 35
  - Enumerar los back-ends de almacenamiento . . . 38
  - Habilite ANF Pools dinámicos para clústeres autogestionados . . . 39

Flujos de trabajo de infraestructura

Prepárese para usar los flujos de trabajo de infraestructura

Puede utilizar estos flujos de trabajo para crear y mantener la infraestructura utilizada con una implementación de Astra Control Center. En muchos casos, los flujos de trabajo también se pueden utilizar con Astra Control Service.

Estos flujos de trabajo pueden ampliarse y mejorarse mediante NetApp en cualquier momento, por lo que debe revisarlos periódicamente.

Preparación general

Antes de utilizar cualquiera de los flujos de trabajo de Astra, asegúrese de revisarlos "Prepárese para usar los flujos de trabajo".

Categorías de flujo de trabajo

Los flujos de trabajo de infraestructuras están organizados en diferentes categorías para facilitar la localización del que desee.

Categoría	Descripción
Identidad y acceso	Estos flujos de trabajo le permiten gestionar la identidad y cómo se accede a Astra. Los recursos incluyen usuarios, credenciales y tokens.
Configuración de LDAP	Opcionalmente, puede configurar Astra Control Center para que utilice LDAP para autenticar a los usuarios seleccionados.
De clúster	Es posible añadir clústeres de Kubernetes gestionados, que permiten proteger y admitir las aplicaciones que contienen.
Nubes	Estos flujos de trabajo proporcionan acceso a las nubes disponibles a través de la API REST de Astra Control.
Cucharones	Se pueden usar estos flujos de trabajo para crear y gestionar los bloques S3 que se utilizan para almacenar backups.
Reducida	Estos flujos de trabajo permiten añadir y mantener volúmenes y back-ends de almacenamiento.

Identidad y acceso

Enumere los usuarios

Puede enumerar los usuarios definidos para una cuenta Astra específica.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
OBTENGA	/accounts/{account_id}/core/v1/users

Parámetros de entrada adicionales

Además de los parámetros comunes con todas las llamadas API DE REST, en los ejemplos curl de este paso se incluyen los siguientes parámetros.

Parámetro	Tipo	Obligatorio	Descripción
incluya	Consulta	No	Opcionalmente, seleccione los valores que desea devolver en la respuesta.

Ejemplo curl: Devuelve todos los datos de todos los usuarios

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

Ejemplo de Curl: Devuelve el nombre, el apellido y el identificador de todos los usuarios

```
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"
```

Ejemplo de resultado JSON


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


Cree un usuario

Se puede crear un usuario con credenciales específicas y un rol predefinido. También puede restringir de manera opcional el acceso del usuario a espacios de nombres específicos.

Paso 1: Seleccione un nombre de usuario

Realice el flujo de trabajo "Enumere usuarios" y seleccione un nombre disponible que no esté en uso actualmente.

Paso 2: Crear el usuario

Realice la siguiente llamada de API de REST para crear un usuario. Una vez finalizada correctamente la llamada, el nuevo usuario aún no será utilizable.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
PUBLICAR	/accounts/{account_id}/core/v1/users

Ejemplo de curl

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

Ejemplo de entrada JSON

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

Ejemplo de resultado 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": ""
}
```


Paso 3: Opcionalmente, seleccione los espacios de nombres permitidos

Realice el flujo de trabajo "Enumere los espacios de nombres" y seleccione los espacios de nombres a los que desea restringir el acceso.

Paso 4: Vincular al usuario a un rol

Ejecute la siguiente llamada API de REST para enlazar el usuario con un rol. En el ejemplo siguiente no se establece ninguna restricción en el acceso al espacio de nombres. Consulte "RBAC mejorado con granularidad de espacio de nombres" si quiere más información.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
PUBLICAR	/Accounts/{account_id}/core/v1/roleBindings

Ejemplo de curl

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

Ejemplo de entrada JSON

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

Paso 5: Crear una credencial

Realice la siguiente llamada a la API DE REST para crear una credencial y asociarla con el usuario. En este ejemplo se utiliza una contraseña que se proporciona como valor base64. La `name` La propiedad debe contener el ID del usuario devuelto en el paso anterior. La propiedad de entrada `change` también se debe codificar en base64 y determinar si el usuario debe cambiar su contraseña al iniciar sesión (`true` o. `false`).

> Este paso solo es necesario con las implementaciones de Astra Control Center mediante autenticación local. No es necesario con las puestas en marcha de Astra Control Center con LDAP o con las puestas en marcha de Astra Control Service.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
PUBLICAR	/accounts/{account_id}/core/v1/credenciales

Ejemplo de curl

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

Ejemplo de entrada JSON

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

Configuración de LDAP

Prepare la configuración de LDAP

Opcionalmente, puede integrar Astra Control Center con un servidor Lightweight Directory Access Protocol (LDAP) para realizar la autenticación de determinados usuarios de Astra. LDAP es un protocolo estándar del sector para acceder a información de directorio distribuida y una opción muy popular para la autenticación empresarial.

Información relacionada

- "Hoja de ruta de especificación técnica de LDAP"
- "LDAP, versión 3"

Descripción general del proceso de implementación

En un nivel superior, hay varios pasos que debe realizar para configurar un servidor LDAP con el fin de proporcionar autenticación a los usuarios de Astra.

> Aunque los pasos que se muestran a continuación están en una secuencia, en algunos casos puede realizarlos en un orden diferente. Por ejemplo, puede definir los usuarios y grupos de Astra antes de configurar el servidor LDAP.

1. Revisar "Requisitos y limitaciones" para comprender las opciones, requisitos y limitaciones.
2. Seleccione un servidor LDAP y las opciones de configuración deseadas (incluida la seguridad).
3. Realice el flujo de trabajo "Configure Astra para que utilice un servidor LDAP" Integrar Astra con el servidor LDAP.
4. Revise los usuarios y grupos del servidor LDAP para asegurarse de que están definidos correctamente.
5. Ejecute el flujo de trabajo adecuado en "Agregue entradas LDAP a Astra" Identificar los usuarios que se autenticarán mediante LDAP.

Requisitos y limitaciones

Antes de configurar Astra para utilizar LDAP para la autenticación, debe revisar los aspectos básicos de configuración de Astra que se presentan a continuación, incluidas las limitaciones y las opciones de configuración.

Sólo compatible con Astra Control Center

La plataforma Astra Control proporciona dos modelos de puesta en marcha. La autenticación LDAP solo es compatible con las implementaciones de Astra Control Center.

Configuración mediante la API DE REST o la interfaz de usuario web

La versión actual de Astra Control Center admite la configuración de la autenticación LDAP mediante la API REST de Astra Control y la interfaz de usuario web de Astra.

Se requiere servidor LDAP

Debe tener un servidor LDAP para aceptar y procesar las solicitudes de autenticación Astra. Active Directory de Microsoft es compatible con la versión actual de Astra Control Center.

Conexión segura con el servidor LDAP

Al configurar el servidor LDAP en Astra, puede definir opcionalmente una conexión segura. En este caso, se necesita un certificado para el protocolo LDAPS.

Configurar usuarios o grupos

Debe seleccionar los usuarios para autenticarse con el LDAP. Puede hacerlo identificando los usuarios individuales o un grupo de usuarios. Las cuentas se deben definir en el servidor LDAP. También deben identificarse en Astra (tipo LDAP) que permite que las solicitudes de autenticación se reenvíen a LDAP.

Restricción de función al enlazar un usuario o un grupo

Con la versión actual de Astra Control Center, el único valor admitido para `roleConstraint` es "*". Esto indica que el usuario no está restringido a un conjunto limitado de espacios de nombres y que puede acceder a todos ellos. Consulte "Agregue entradas LDAP a Astra" si quiere más información.

Credenciales de LDAP

Entre las credenciales que utiliza LDAP, se incluyen el nombre de usuario (dirección de correo electrónico) y la contraseña asociada.

Direcciones de correo electrónico exclusivas

Todas las direcciones de correo electrónico que actúen como nombres de usuario en una implementación de Astra Control Center deben ser únicas. No puede agregar un usuario LDAP con una dirección de correo electrónico que ya esté definida en Astra. Si existe un correo electrónico duplicado, primero debe eliminarlo de Astra. Consulte "Quitar usuarios" En el sitio de documentación de Astra Control Center para obtener más información.

Opcionalmente, defina primero los grupos y usuarios LDAP

Puede agregar los usuarios y grupos LDAP a Astra Control Center aunque aún no existan en LDAP o si no se ha configurado el servidor LDAP. Esto permite preconfigurar los usuarios y grupos antes de configurar el servidor LDAP.

Un usuario definido en varios grupos LDAP

Si un usuario LDAP pertenece a varios grupos LDAP y se han asignado roles diferentes en Astra a los grupos, el rol efectivo del usuario al autenticarse será el más privilegiado. Por ejemplo, si se asigna un usuario el `viewer` rol con group1 pero tiene la `member` función en grupo2, el rol del usuario sería `member`. Esto se basa en la jerarquía utilizada por Astra (de la más alta a la más baja):

- Propietario
- Admin
- Miembro
- Visionador

Sincronización periódica de cuentas

Astra sincroniza los usuarios y grupos de TI con el servidor LDAP aproximadamente cada 60 segundos. Por lo tanto, si se agrega o elimina un usuario o grupo de LDAP, puede tardar hasta un minuto en estar disponible en Astra.

Deshabilitar y restablecer la configuración de LDAP

Antes de intentar restablecer la configuración de LDAP, primero debe deshabilitar la autenticación LDAP. Además, para cambiar el servidor LDAP (`connectionHost`), debe realizar ambas operaciones. Consulte "Deshabilite y restablezca LDAP" si quiere más información.

Parámetros de la API de REST

Los flujos de trabajo de configuración LDAP realizan llamadas a la API DE REST para realizar las tareas específicas. Cada llamada API puede incluir parámetros de entrada, como se muestra en las muestras proporcionadas. Consulte "Referencia de API en línea" para obtener información sobre cómo localizar la documentación de referencia.

Configure Astra para que utilice un servidor LDAP

Debe seleccionar un servidor LDAP y configurar Astra para utilizar el servidor como proveedor de autenticación. La tarea de configuración consta de los pasos descritos a continuación. Cada paso incluye una única llamada API DE REST.

Paso 1: Agregue un certificado de CA

Realice la siguiente llamada a la API DE REST para añadir un certificado de CA a Astra.

> Este paso es opcional y solo es necesario si desea que Astra y LDAP se comuniquen a través de un canal seguro mediante LDAPS.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
PUBLICAR	/accounts/{account_id}/core/v1/certificates

Ejemplo de curl

```
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
```

Ejemplo de entrada JSON

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

Tenga en cuenta lo siguiente acerca de los parámetros de entrada:

- `cert` Es una cadena JSON que contiene un certificado con formato PKCS-11 codificado en base64 (codificado en PEM).
- `isSelfSigned` se debe establecer en `true` si el certificado está autofirmado. El valor predeterminado es `false`.

Ejemplo de resultado JSON


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

Paso 2: Agregue las credenciales de enlace

Ejecute la siguiente llamada API de REST para añadir las credenciales de enlace.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
PUBLICAR	/accounts/{account_id}/core/v1/credenciales

Ejemplo de curl

```
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
```

Ejemplo de entrada JSON

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

Tenga en cuenta lo siguiente acerca de los parámetros de entrada:

- `bindDn` y.. `password` Son las credenciales de enlace codificadas base64 del usuario administrador LDAP que puede conectarse y buscar en el directorio LDAP. `bindDn` Es la dirección de correo electrónico del usuario LDAP.

Ejemplo de resultado 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"
    }
}
```

Tenga en cuenta los siguientes parámetros de respuesta:

- La `id` de la credencial se utiliza en los pasos posteriores del flujo de trabajo.

Paso 3: Recupere el UUID de la configuración LDAP

Realice la siguiente llamada API DE REST para recuperar el UUID del `astra.account.ldap` Ajuste que se incluye con Astra Control Center.

> El ejemplo curl que se muestra a continuación utiliza un parámetro de consulta para filtrar la colección de ajustes. En su lugar, puede quitar el filtro para obtener todos los ajustes y, a continuación, buscar `astra.account.ldap`.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
OBTENGA	/accounts/{account_id}/core/v1/settings

Ejemplo de curl

```
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" \
```

Ejemplo de resultado JSON

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

Paso 4: Actualice la configuración de LDAP

Realice la siguiente llamada a la API DE REST para actualizar la configuración de LDAP y completar la configuración. Utilice la `id` Valor de la llamada de API anterior para `<SETTING_ID>` Valor en la ruta de dirección URL a continuación.

> Puede emitir primero una solicitud GET para la configuración específica para ver el esquema configSchema. Esto proporcionará más información acerca de los campos requeridos en la configuración.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
PUESTO	/accounts/{account_id}/core/v1/settings/{setting_id}

Ejemplo de curl

```
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
```

Ejemplo 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"
    }
}
```

Tenga en cuenta lo siguiente acerca de los parámetros de entrada:

- `isEnabled` se debe establecer en `true` o se puede producir un error.
- `credentialId` es el id de la credencial de enlace creada anteriormente.
- `secureMode` se debe establecer en `LDAP` o. `LDAPS` según la configuración del paso anterior.
- Sólo se admite "Active Directory" como proveedor.

Si la llamada se realiza correctamente, se devuelve la respuesta HTTP 204.

Paso 5: Recupere la configuración LDAP

De forma opcional, puede realizar la siguiente llamada API DE REST para recuperar la configuración de LDAP y confirmar la actualización.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
OBTENGA	/accounts/{account_id}/core/v1/settings/{setting_id}

Ejemplo de curl

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

Ejemplo de resultado 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": {}
}
```


Localice el `state` en el campo de respuesta que tendrá uno de los valores de la tabla siguiente.

Estado	Descripción
pendiente	El proceso de configuración sigue activo y aún no se ha completado.
válido	La configuración se ha completado correctamente y. `currentConfig` en la respuesta coincide `desiredConfig`.
error	Error en el proceso de configuración de LDAP.

Agregue entradas LDAP a Astra

Después de configurar LDAP como proveedor de autenticación para Astra Control Center, puede seleccionar los usuarios LDAP que Astra autenticará mediante las credenciales LDAP. Cada usuario debe tener una función en Astra para poder acceder a Astra a través de la API ASTRA Control REST.

Hay dos formas de configurar Astra para asignar funciones. Elija el que mejor se adapte a su entorno.

- "Agregar y enlazar un usuario individual"
- "Agregar y enlazar un grupo"

Las credenciales LDAP tienen el formato de nombre de usuario como dirección de correo electrónico y contraseña LDAP asociada.

Agregar y enlazar un usuario individual

Puede asignar una función a cada usuario Astra que se utilice después de la autenticación LDAP. Esto resulta apropiado cuando hay un número reducido de usuarios y cada uno puede tener características administrativas diferentes.

Paso 1: Agregar un usuario

Realice la siguiente llamada a la API DE REST para añadir un usuario a Astra e indicar que LDAP es el proveedor de autenticación.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
PUBLICAR	/accounts/{account_id}/core/v1/users

Ejemplo de curl

```
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
```

Ejemplo 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"
}
```

Tenga en cuenta lo siguiente acerca de los parámetros de entrada:

- Se requieren los siguientes parámetros:
  - `authProvider`

    - authID
    - email

- `authID` Es el nombre distintivo (DN) del usuario en LDAP
- `email` Debe ser único para todos los usuarios definidos en Astra

Si la `email` El valor no es único, se produce un error y se devuelve un código de estado HTTP 409 en la respuesta.

Ejemplo de resultado 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": ""
}
```

Paso 2: Agregue un enlace de rol para el usuario

Ejecute la siguiente llamada API de REST para enlazar el usuario con un rol específico. Debe tener creado el UUID del usuario en el paso anterior.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
PUBLICAR	/Accounts/{account_id}/core/v1/roleBindings

Ejemplo de curl

```
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
```

Ejemplo de entrada JSON

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

Tenga en cuenta lo siguiente acerca de los parámetros de entrada:

- El valor utilizado anteriormente para `roleConstraint` Es la única opción disponible para la versión actual de Astra. Indica que el usuario no está restringido a un conjunto limitado de espacios de nombres y puede acceder a todos ellos.

Ejemplo de respuesta 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": ["*"]
}
```


Tenga en cuenta lo siguiente sobre los parámetros de respuesta:

- El valor `user` para la `principalType` el campo indica que se ha agregado el enlace de función a un usuario (no a un grupo).

Agregar y enlazar un grupo

Puede asignar una función a un grupo Astra que se utilice después de la autenticación LDAP. Resulta apropiado cuando hay un gran número de usuarios y cada uno puede tener características administrativas similares.

Paso 1: Agregar un grupo

Realice la siguiente llamada a la API DE REST para agregar un grupo a Astra e indicar que LDAP es el proveedor de autenticación.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
PUBLICAR	/accounts/{account_id}/core/v1/groups

Ejemplo de curl

```
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
```

Ejemplo 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"
}
```

Tenga en cuenta lo siguiente acerca de los parámetros de entrada:

- Se requieren los siguientes parámetros:
  - `authProvider`
  - `authID`

Ejemplo de respuesta 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": []
  }
}
```

Paso 2: Agregue un enlace de rol para el grupo

Realice la siguiente llamada de API de REST para enlazar el grupo con un rol específico. Debe haber creado el UUID del grupo en el paso anterior. Los usuarios que sean miembros del grupo podrán iniciar sesión en Astra después de que LDAP realice la autenticación.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
PUBLICAR	/Accounts/{account_id}/core/v1/roleBindings

Ejemplo de curl

```
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
```

Ejemplo de entrada JSON

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

Tenga en cuenta lo siguiente acerca de los parámetros de entrada:

- El valor utilizado anteriormente para `roleConstraint` Es la única opción disponible para la versión actual de Astra. Indica que el usuario no está restringido a determinados espacios de nombres y puede acceder a todos ellos.

Ejemplo de respuesta 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": ["*"]
}
```

Tenga en cuenta lo siguiente sobre los parámetros de respuesta:

- El valor `group` para la `principalType` el campo indica que se ha agregado el enlace de función para un grupo (no un usuario).

Deshabilite y restablezca LDAP

Hay dos tareas administrativas opcionales a través de las relacionadas que puede realizar según sea necesario para una implementación de Astra Control Center. Es posible deshabilitar la autenticación LDAP de forma global y restablecer la configuración de LDAP.

Ambas tareas de flujo de trabajo requieren el id para `astra.account.ldap` Ajuste Astra. En **Configurar el servidor LDAP** se incluyen detalles sobre cómo recuperar el identificador de configuración. Consulte "Recupere el UUID de la configuración LDAP" si quiere más información.

- "Deshabilitar la autenticación LDAP"
- "Restablece la configuración de autenticación de LDAP"

Deshabilitar la autenticación LDAP

Puede realizar la siguiente llamada a la API DE REST para deshabilitar globalmente la autenticación LDAP para una implementación específica de Astra. La llamada actualiza la `astra.account.ldap` y la `isEnabled` el valor se establece en `false`.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
PUESTO	/accounts/{account_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
```

Ejemplo 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"
    }
}
```

Si la llamada se realiza correctamente, el `HTTP 204` se devuelve la respuesta. Opcionalmente, puede recuperar de nuevo los ajustes de configuración para confirmar el cambio.

Restablece la configuración de autenticación de LDAP

Puede realizar la siguiente llamada a la API DE REST para desconectar Astra del servidor LDAP y restablecer la configuración de LDAP en Astra. La llamada actualiza la `astra.account.ldap` y el valor de `connectionHost` se borra.

Valor de `isEnabled` también se debe establecer en `false`. Puede establecer este valor antes de realizar la llamada de restablecimiento o como parte de realizar la llamada de restablecimiento. En el segundo caso, `connectionHost` debe ser despejado y. `isEnabled` establezca como falso en la misma llamada de restablecimiento.

Esto es una operación disruptiva y debe continuar con precaución. Elimina todos los grupos y usuarios LDAP importados. También elimina todos los usuarios, grupos y enlaces (tipo LDAP) de Astra relacionados que creó en Astra Control Center.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
PUESTO	/accounts/{account_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
```

Ejemplo 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"
    }
}
```

Tenga en cuenta lo siguiente:

- Para cambiar el servidor LDAP, debe deshabilitar y restablecer el cambio LDAP `connectHost` a un valor nulo como se muestra en el ejemplo anterior.
- Si la llamada se realiza correctamente, el `HTTP 204` se devuelve la respuesta. De manera opcional, puede recuperar la configuración de nuevo para confirmar el cambio.

De clúster

Enumere los clústeres

Puede mostrar los clústeres disponibles en un cloud específico.

Paso 1: Seleccione la nube

Realice el flujo de trabajo "Enumerar las nubes" y seleccione el cloud que contiene los clústeres.

Paso 2: Enumere los clústeres

Realice la siguiente llamada de API DE REST para enumerar los clústeres en un cloud específico.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
OBTENGA	/accounts/{account_id}/topolog/v1/cloud/{cloud_id}/clusters

Ejemplo curl: Devuelve todos los datos de todos los clústeres

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

Ejemplo de resultado 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",
            "postgreql",
            "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"
            }
        }
    ]
}
```

Añada un clúster mediante credenciales

Puede añadir un clúster para que Astra lo gestione. A partir de la versión Astra 22.11, puede añadir un clúster con Astra Control Center y Astra Control Service.

No es necesario añadir un clúster cuando se usa un servicio de Kubernetes de uno de los principales proveedores de cloud (AKS, EKS, GKE).

Paso 1: Obtenga el archivo kubeconfig

Necesita obtener una copia del archivo **kubconfig** de su administrador o servicio de Kubernetes.

Paso 2: Preparar el archivo kubeconfig

Antes de utilizar el archivo **kubeconfig**, debe realizar las siguientes operaciones:

1. Convertir archivo de formato YAML a JSON:

   Si recibe el archivo kubeconfig con formato YAML, debe convertirlo a JSON.

2. Codificar JSON en base64:

   Debe codificar el archivo JSON en base64.

Ejemplo

Aquí hay un ejemplo de la conversión del archivo kubeconfig de YAML a JSON y luego codificarlo en base64:

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

Paso 3: Seleccione la nube

Realice el flujo de trabajo "Enumerar las nubes" y seleccione el cloud donde se añadirá el clúster.

La única nube que puede seleccionar es la **nube privada**.

Paso 4: Crear una credencial

Realice la siguiente llamada a la API DE REST para crear una credencial mediante el archivo kubeconfig.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
PUBLICAR	/accounts/{account_id}/core/v1/credenciales

Ejemplo de curl

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

Ejemplo de entrada JSON

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

Paso 5: Añada el clúster

Realice la siguiente llamada de API REST para añadir el clúster al cloud. El valor de `credentialID` El campo de entrada se obtiene de la llamada a la API DE REST en el paso anterior.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
PUBLICAR	/accounts/{account_id}/topolog/v1/cloud/{cloud_id}/clusters

Ejemplo de curl

```
curl --request POST \
--location
"https://astra.netapp.io/accounts/$ACCOUNT_ID/topology/v1/clouds/<CLOUD_ID
>/clusters" \
--include \
--header "Accept: */*" \
--header "Authorization: Bearer $API_TOKEN" \
--data  @JSONinput
```

Ejemplo de entrada JSON

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

Enumere los clústeres gestionados

Puede enumerar los clústeres de Kubernetes que gestiona actualmente Astra.

Realice la siguiente llamada de API de REST.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
OBTENGA	/Accounts/{account_id}/topolog/v1/managedClusters

Ejemplo curl: Devuelve todos los datos de todos los clústeres

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

Gestione un clúster

Es posible gestionar un clúster de Kubernetes para poder llevar a cabo la protección de datos.

Paso 1: Seleccione el clúster que desea administrar

Realice el flujo de trabajo "Enumere los clústeres" y seleccione el clúster que desee. La propiedad `managedState` del clúster debe ser `unmanaged`.

Paso 2: De manera opcional, seleccione la clase de almacenamiento

Si lo desea, puede ejecutar el flujo de trabajo "Enumerar las clases de almacenamiento" y seleccione la clase de almacenamiento que desee.

> Si no proporciona una clase de almacenamiento a la llamada para gestionar el clúster, se usará la clase de almacenamiento predeterminada.

Paso 3: Administre el clúster

Realice la siguiente llamada API REST para gestionar el clúster.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
PUBLICAR	/Accounts/{account_id}/topolog/v1/managedClusters

Ejemplo de curl

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

Ejemplo de entrada JSON

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

Nubes

Enumerar las nubes

Puede enumerar las nubes definidas y disponibles una cuenta de Astra específica.

Realice las siguientes llamadas a la API DE REST para enumerar las nubes.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
OBTENGA	/accounts/{account_id}/topolog/v1/nubes

Ejemplo curl: Devuelve todos los datos de todos los clouds

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

Cucharones

Enumere los cucharones

Puede enumerar los bloques de S3 definidos para una cuenta de Astra específica.

Realice la siguiente llamada a la API de REST para enumerar los bloques.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
OBTENGA	/accounts/{account_id}/topolog/v1/buckets

Ejemplo de curl: Devuelve todos los datos de todos los bloques

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

Reducida

Enumerar las clases de almacenamiento

Puede enumerar las clases de almacenamiento disponibles.

Paso 1: Seleccione la nube

Realice el flujo de trabajo "Enumerar las nubes" y seleccione el cloud en el que trabajará.

Paso 2: Seleccione el clúster

Realice el flujo de trabajo "Enumere los clústeres" y seleccione el clúster.

Paso 3: Enumere las clases de almacenamiento para un clúster específico

Realice la siguiente llamada a la API DE REST para enumerar las clases de almacenamiento para un clúster y un cloud específicos.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
OBTENGA	/Accounts/{account_id}/topolog/v1/cloud/<CLOUD_ID>/Clusters/<CLUSTER_ID>/storageClasses

Ejemplo curl: Devuelve todos los datos de todas las clases de almacenamiento

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

Ejemplo de resultado 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": []
            }
        }
    ]
}
```

Enumerar los back-ends de almacenamiento

Es posible enumerar los back-ends de almacenamiento disponibles.

Realice la siguiente llamada de API de REST.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
OBTENGA	/Accounts/{account_id}/topolog/v1/storageBackends

Ejemplo de curl: Devuelve todos los datos de todos los back-ends de almacenamiento

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

Ejemplo de resultado 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"
    }
  ]
}
```


Habilite ANF Pools dinámicos para clústeres autogestionados

Cuando se realiza un backup de una aplicación gestionada en un clúster privado de las instalaciones que tiene un back-end de almacenamiento de ANF, debe habilitar la función dinámica ANF Pools. Esto se realiza proporcionando un identificador de suscripción para utilizarlo al expandir y contraer los pools de capacidad.

Los pools de ANF dinámicos son una característica de las aplicaciones gestionadas por Astra que utilizan un entorno de administración de almacenamiento Azure NetApp Files (ANF). Cuando se realiza un backup de estas aplicaciones, Astra amplía automáticamente y reduce 1,5 veces los pools de capacidad a los volúmenes persistentes. Esto garantiza que haya espacio suficiente para la copia de seguridad sin incurrir en un cargo permanente adicional. Consulte "Backups de aplicaciones Azure" si quiere más información.

Paso 1: Agregue el identificador de suscripción de Azure

Realice la siguiente llamada de API de REST.

Debe actualizar el ejemplo de entrada JSON según corresponda para su entorno, incluido el ID de suscripción y el valor base64 para el principal de servicio.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo.

Método HTTP	Ruta
PUBLICAR	/accounts/{account_id}/core/v1/credenciales

Ejemplo de curl

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

Ejemplo de entrada JSON


```
{
  "keyStore": {
    "privKey": "SGkh",
    "pubKey": "UGhpcyCpcyBhbiBleGFtcGxlLg==",
    "base64":
"fwogICAgJmFwcElkIjogIjY4ZmSiODFiLTY0YWYtNDdjNC04ZjUzLWE2NDdlZTUzMGZkZCIsC
iAgICAiZGlzcGxheU5hbWUiOiAic3AtYXN0cmEtZGV2LXFhIiwKICAgICJuYW1lIjogImh0dHA
6Ly9zcC1hc3RyYS1kZXYtcWEiLAogICAgInBhc3N3b3JkIjogIllLQThRfk9IVVJkZWZYM0pST
WJlLnpUeFBleVE0UnNwTG9DcUJjazAiLAogICAgInRlbmFudCI6ICIwMTFjZGY2Yy03NTEyLTQ
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"
      }
    ]
  }
}
```


Paso 2: Agregue un cubo si es necesario

Si es necesario, debe agregar un depósito a la aplicación gestionada.

Paso 3: Realice una copia de seguridad de la aplicación administrada

Realice el flujo de trabajo "Cree una copia de seguridad para una aplicación". El pool de capacidad donde está presente el volumen persistente original se expandirá y se reducirá automáticamente.

Paso 4: Revise el registro de eventos

Los eventos de actividad se registran durante la copia de seguridad. Realice el flujo de trabajo "Enumere las notificaciones" para ver los mensajes.

Información de copyright

Copyright © 2025 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en http://www.netapp.com/TM son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.