Tot plugin AWS IAM

Control de versiones **2**
Introducción **3**
Servicios disponibles en el plugin 3
Modelo de integración **3**
Gobierno activo 3
Credenciales requeridas **3**
Gobierno activo 3
Restricciones **4**
Configuración necesaria **4**

Control de versiones

Versión	Fecha de modificación	Responsable	Aprobador	Resumen de cambios
1.0	04/03/2024	Anjana Producto	Anjana Producto	Creación del documento

Introducción

Este plugin se usa en coordinación con los plugins de tecnologías de almacenamiento conectadas al IAM de AWS para provisionar los grupos que representan a los DSA y adicionalmente gestiona las membresías que representan la aceptación de los DSA por parte de los usuarios.

Servicios disponibles en el plugin

- Crear y asociar permisos a grupos: Crear grupos con usuarios, asociar permisos al grupo de acceso al bucket y a partes del mismo.
- Añadir usuario a grupos: Añadir usuarios a grupos existentes.
- Quitar usuarios de grupos: Quitar usuarios de grupos.
- Eliminar acceso: Modificar las políticas del grupo para retirar el acceso a un recurso en particular.
- Eliminar grupos: Eliminar grupos previamente creados y eliminando la política creada para el mismo.

Modelo de integración

Gobierno activo

De forma general los DSA de Anjana Data se representan como grupos en el IAM de AWS y los firmantes de dichos DSA son miembros de dichos grupos.

Anjana Data crea y elimina los grupos de forma automática, al igual que incluye y excluye a usuarios de cada grupo con el objetivo de materializar la adhesión o desadherencia de un usuario a un DSA.

Para la provisión de grupos de usuarios a los que posteriormente se asignan permisos de acceso a recursos de datos gobernados por el producto se explota la interfaz del sdk de AWS.

Credenciales requeridas

Gobierno activo

Para el gobierno activo se necesita una credencial de servicio con los siguientes permisos:

- AddUserToGroup: Incluir usuarios a los grupos.
- AttachGroupPolicy: Asociar políticas de acceso a los grupos.
- CreateGroup: Crear grupos.
- CreatePolicy: Crear políticas de acceso.
- CreatePolicyVersion: Crea una nueva versión en una política.

- DeleteGroup: Borrar grupos.
- DeletePolicy: Borra una política.
- DeletePolicyVersion: Borra una versión de una política.
- DeleteGroupPolicy: Borra las políticas de un grupo.
- DetachGroupPolicy: Desasociar las managed policy de un grupo.
- GetGroup: Recuperar grupos
- GetPolicy: Recuperar políticas.
- GetPolicyVersion: Recupera una versión de una política.
- GetUser: Listar y recuperar usuarios.
- ListAttachedGroupPolicies: Lista y recupera las managed policy de un grupo.
- ListGroupPolicies: Lista y recupera las políticas de un grupo.
- ListPolicyVersions: Lista las versiones de una política.
- RemoveUserFromGroup: Eliminar usuarios de los grupos.

Los servicios disponibles usan los siguientes permisos:

- Crear y asociar permisos a grupos: AddUserToGroup, AttachGroupPolicy, CreateGroup, CreatePolicy, GetGroup y GetUser.
- Añadir usuario a grupos: AddUserToGroup, GetGroup y GetUser.
- Quitar usuarios de grupos: GetGroup, GetUser y RemoveUserFromGroup.
- Eliminar acceso: CreatePolicyVersion, DeletePolicyVersion, GetGroup, GetPolicyVersion y ListPolicyVersions.
- Eliminar grupos: DeleteGroup, DeleteGroupPolicy, DeletePolicy, DetachGroupPolicy, GetGroup, ListAttachedGroupPolicies, ListGroupPolicies y RemoveUserFromGroup.

Restricciones

El prefijo para los grupos (y el propio nombre del DSA) no puede contener espacios y los únicos caracteres permitidos son alfanuméricos y _=,.@- ; si el prefijo tiene valor y no es válido el plugin no se levantara y generara un log con el error.

Dada la longitud máxima de las políticas no se recomienda gobernar más de 100 datasets en un mismo DSA.

Por limitaciones de AWS, un usuario no puede estar adherido y/o ser owner's (la suma de ambos) de más de 10 DSAs.

Configuración necesaria

Aquí se incluye el detalle de la configuración específica del plugin.
En la Guía de Configuración técnica se explica la configuración común.

```yaml
server:
  port: 15008

totplugin:
  server:
    urls:
      - http://totserver:15000/tot/
  connection:
    pathSeparator: "/"
    proxy: ""
    accessKey: <accessKey>
    secretKey: <secretKey>
    bucket: <bucket>
    region: <region>
    idAccount: <idAccount>
  groupPrefix: Dsa_
  bucketPolicy: "anjana_ListAllMyBuckets"
  policyPrefix: "DsaPolicy_"
  aris:
    - ari: "anja:totplugin:im:/AWS/awsIam/devQA/"
eureka:
  client:
    serviceUrl:
      defaultZone: http://totserver:15000/tot/eureka
```

Server:

- port: El puerto en el que se va a desplegar el plugin.

TotPlugin:

- groupPrefix: Parámetro opcional para indicar un prefijo en el nombre de todos los grupos generados por el plugin.
- bucketPolicy: Parámetro opcional para indicar el nombre de la política general de acceso a buckets generada y usada por los grupos creados por el plugin.
- policyPrefix: Parámetro opcional para indicar el prefijo en el nombre de la política única de acceso a recursos generada y usada por los grupos creados por el plugin.

Connection:

- pathSeparator: Indica cuál es el separador en los path recuperados de los objetos gobernados.
- proxy: Parámetro opcional si se quiere realizar la conexión a AWS mediante un proxy.
- accessKey: Clave de acceso de la cuenta de Anjana generada para el plugin.
- secretKey: La contraseña de acceso de la cuenta de Anjana generada para el plugin.
- bucket: Nombre del bucket que se gobierna.
- región: La región donde se encuentra registrada la cuenta.