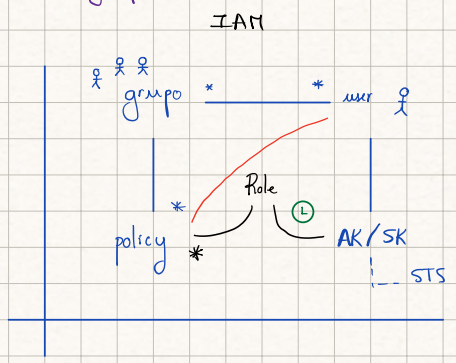
AWS

- root account (primera cuenta creada)

  usuario targeta (root user)

- crear usuario admin → IAM

  IAM dasboard → User groups → Create group → administradores (nom) → permissions policies → AdministratorAccess → Create group



permitimos todas las acciones posibles

- por defecto un usuario no puede hacer nada
- si lo añadimos al grupo podrá hacer de todo

(L) Temporales

Users → Add users → nom (judit) - Console access - custom password (manual) - Next → add user to group → administradores

Ahora este usuario podrá crear permisos y policies.

Boundary →

¿no permitir crear vm (no podría escalar privilegios)

Tag → project - upctalent → Next → Create User - Darle al link - acceder

Sesiones distintas en el mismo navegador → causa problemas de confusion

Borrar MFA del root user del telefono → nadie podrá usarlo. (fuera gestión de permisos, no debería usarse nunca)

Organizations → Activar

Organizations

Las cuentas son un mecanismo de aislamiento, no tienen acceso entre ellas. (pug)

Cuenta inicial

Cuenta creada

Cuenta escribir blogs

(barreras de aislamiento, algo mal configurado dificilmente puede afectar otra cuenta)

Asociada a varias cosas, como por ejemplo, la tarjeta de credito. Que tiene dentro su propio IAM y su propio root user.

AWS accounts → Create an AWS account → upctalentaccount

Mail → nuevo usuario - forgot password - new password (mail)

El root account no tiene poder sobre las otras cuentas creadas. (suelen ser la misma persona) y no puede siquiera cortar el grifo. (ni borrarlos)

Precio tener cuentas AWS - 0€

Pasos

S3 - Servicio de almacenamiento
- Crear bucket
- Nombre unico
- tag (Project upctalent)
- cifrado (activar)
- upload (fichero)

Dar acceso a recursos.

Invocar api servicio s3 listar

(aws s3 ls --region eu-west-1)

Quien se autentica es la app aws a la que estoy accediendo.

Access Key - nombre id de la app.

Secret Key - password (no se transmite, solo sirve para firmar)

Encontrar AK y SK asociada a una policy

STS - security token service. Quien asegura las credenciales.

AK y SK generadas tiene policy asignadas al usuario.

Cualquier deny sobrescribe cualquier allow.

IAM - usuario - Security credentials (MFA) - Access Keys - Create - Se genera (ID, Key) - Guardar

Se especifica a que región le envías la llamada.

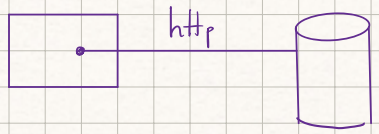
Listar buckets - este en todas las regiones

Listar ficheros, descargar - solo en la region asignada (Irlanda)

ls -a

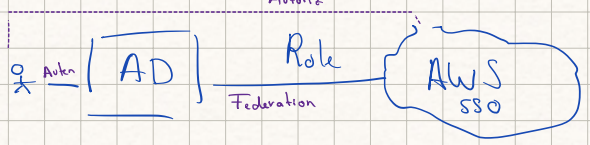
ls .aws

cat .aws/* - dentro access Key y secret Key



Metadata (contiene AK y SK)

curl - devuelve metadata



AD - active directory. Enlazamos cuenta amazon con AD, asumiendo X role

Federacion - relación confianza entre AD y AWS.

AD = recuerda si has puesto bien tu pass y user

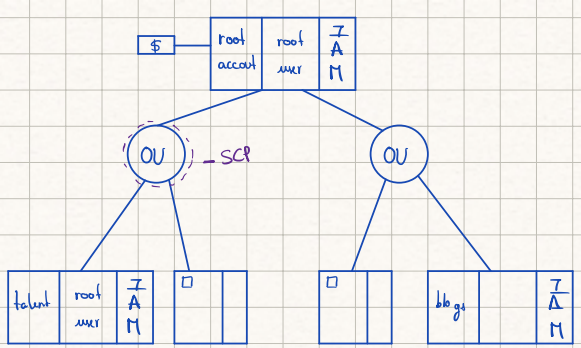
SSO - sign in sign on

Role = forma de darle a alguien poder para acceder a las cuentas.

integracion → root account

role - en cadauna de las cuentas.

OU = organization unit = organizar cuentas



Jerarquia de cuentas

Limitacion (checkeo) de permisos - SCP
ej. denyanythingoutsidevirginia - policy