LABORATORIO DE AWS WAF Y AWS ORGANIZATIONS

AWS ORGANIZATIONS (Gobierno Empresarial)

Lo que vamos a realizar

- Crear estructura multi-cuenta
- Aplicar Service Control Policies (SCP)
- Centralizar seguridad

Paso 1: Crear estructura organizacional

Desde la cuenta management la principal:

Ir a:
AWS Organizations

Crear la distribución de unidades organizacionales

OU: Organizational Unit

Root

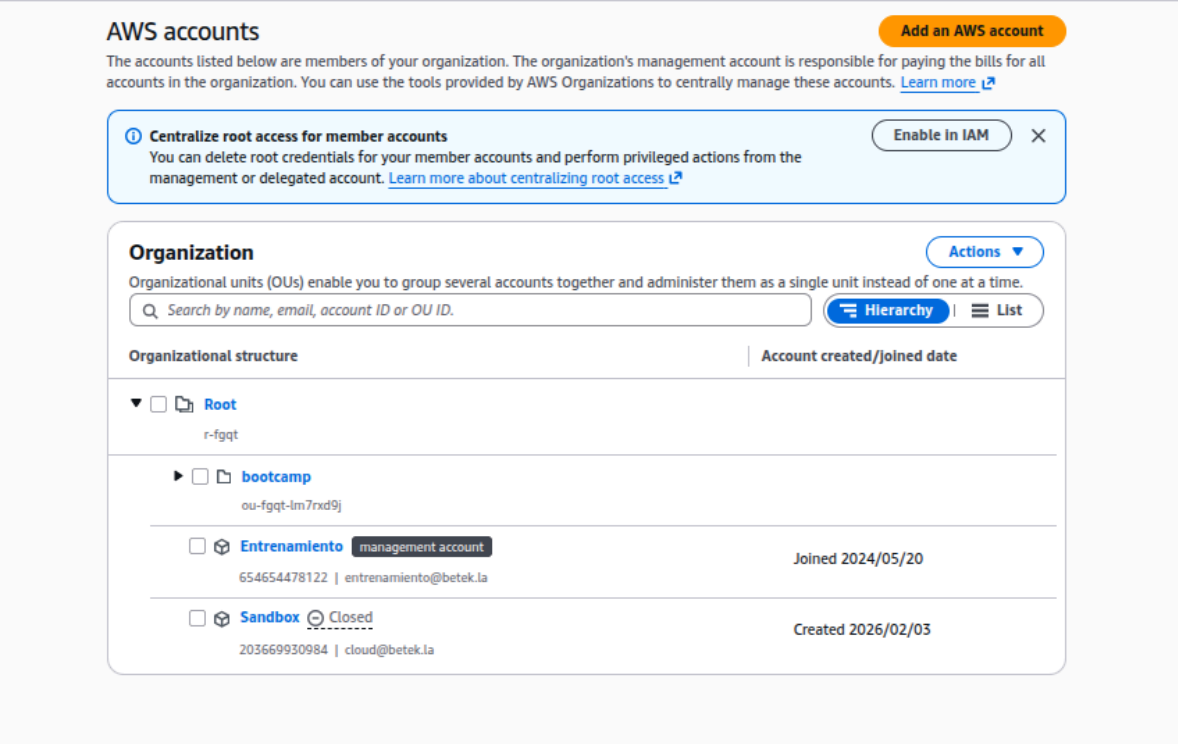
├── OU-Workloads

│ ├── DEV

│ ├── PROD

└── OU-Security

└── SECURITY



Paso 2: Crear un SCP

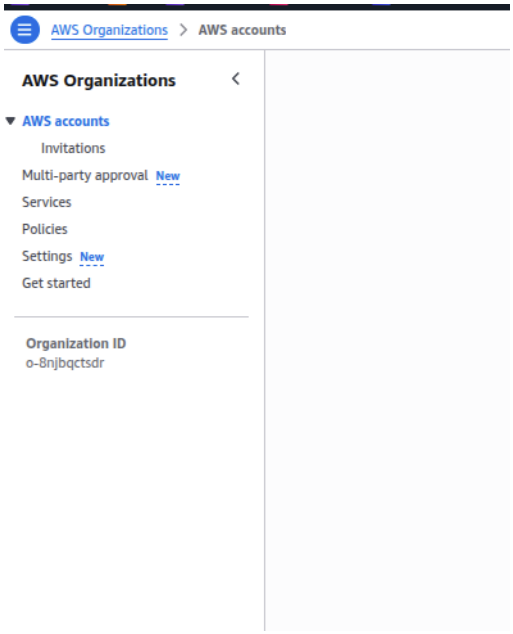
¿Qué es una SCP explicado en palabras cotidianas?

- AWS Organization: Es el centro comercial completo.
- Cuentas de AWS: Son los locales individuales (una tienda de ropa, un cine, un restaurante).
- IAM Policies: Son las llaves que el dueño del local le da a sus empleados. El empleado puede abrir la caja fuerte porque tiene la "llave" (permiso).
- SCP (Service Control Policies): Es el reglamento del centro comercial. Si el reglamento dice "Prohibido usar gas", por más que el dueño del restaurante le dé la llave de la cocina a su chef, el chef no podrá encender la estufa de gas. El reglamento manda sobre la llave.

Una SCP no da permisos, solo pone una "barrera". Si la SCP lo prohíbe, IAM no puede permitirlo.

Una vez se genere la cuenta, generamos una SCP (Service control policy)

- Ingresamos a policies
- Despues Service control policies
- Cada uno deberá escoger una SCP (La de control de instancias y la aplicaremos en otra cuenta).
- La Regla: Las SCP sólo se aplican a las Member Accounts (cuentas miembro).
- La Razón: AWS hace esto para evitar que el administrador se bloquee a sí mismo "por fuera" de la organización. Si aplicaras una SCP que bloquea todo en la cuenta principal, podrías perder el acceso para siempre a la gestión de pagos y de otras cuentas.



Ejemplo de SCP que bloquean acciones en cualquier región que no sea Ohio y Virginia.

Bloquea cualquier operación que no ocurra en las dos regiones de EE.UU. especificadas, pero deja pasar los servicios globales

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAllOutsideVirginiaAndOhio",
      "Effect": "Deny",
      "NotAction": [
        "iam:*",
        "organizations:*",
        "route53:*",
        "cloudfront:*",
        "support:*"
      ],
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": [
            "us-east-1",
            "us-east-2"
          ]
        }
      }
    }
  ]
```

```
}
```

SCP de Control de Costos: EC2 (Capa Gratuita)

Esta se enfoca exclusivamente en las máquinas virtuales. Si intenta lanzar algo que no sea t2.micro o t3.micro

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RestrictEC2ToFreeTier",
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": "arn:aws:ec2:*:*:instance/*",
      "Condition": {
        "StringNotLike": {
          "ec2:InstanceType": ["t2.micro", "t3.micro"]
        }
      }
    }
  ]
}
```

SCP de Control de Costos: RDS (Bases de Datos)

Esta se enfoca exclusivamente en las máquinas virtuales. Si intenta lanzar algo que no sea db.t2.micro o db.t3.micro

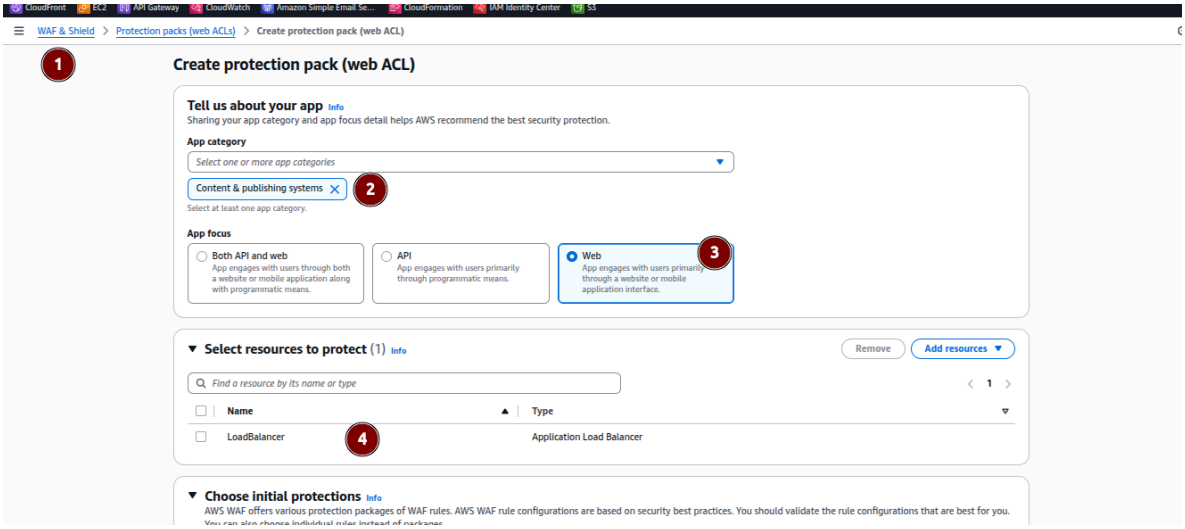
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RestrictRDSToFreeTier",
      "Effect": "Deny",
      "Action": "rds:CreateDBInstance",
      "Resource": "arn:aws:rds:*:*:db/*",
      "Condition": {
        "StringNotLike": {
          "rds:DatabaseClass": ["db.t2.micro", "db.t3.micro"]
        }
      }
    }
  ]
}
```

Paso 3: Probar la SCP

- Se otorgarán 3 usuarios de IAM con permisos.
- Validamos el comportamiento intentando lanzar uno de los recursos no permitidos.
- Después levantaremos una restricción y procederemos a volver a probar.

AWS WAF (Seguridad contra ataques)

- Iniciamos al servicio de WAF
- Después en ACLs
- Create protección packweb ACL
- Seleccionamos la categoría de la APP
- Selección el foco del APP si es consumo de api o aplicación Web
- Selecciona las reglas En este caso seleccionaremos Essential rules, que por defecto ya tiene algunas reglas (También se pueden hacer personalizadas .
- entre las cuales
    - 1000 requests per IP per 5-minute period Si una IP hace más de 1000 requests en 5 minutos ⟶ se bloquea.
    - Bloquear IP específicas manualmente
    - Permitir IP específicas aunque otras reglas las bloqueen
    - country bloqueo por ubicación geográfica
    - Destino de los logs



RECUERDA: Siempre eliminar todos los recursos desplegados en esta práctica