Platzi

Curso Práctico de

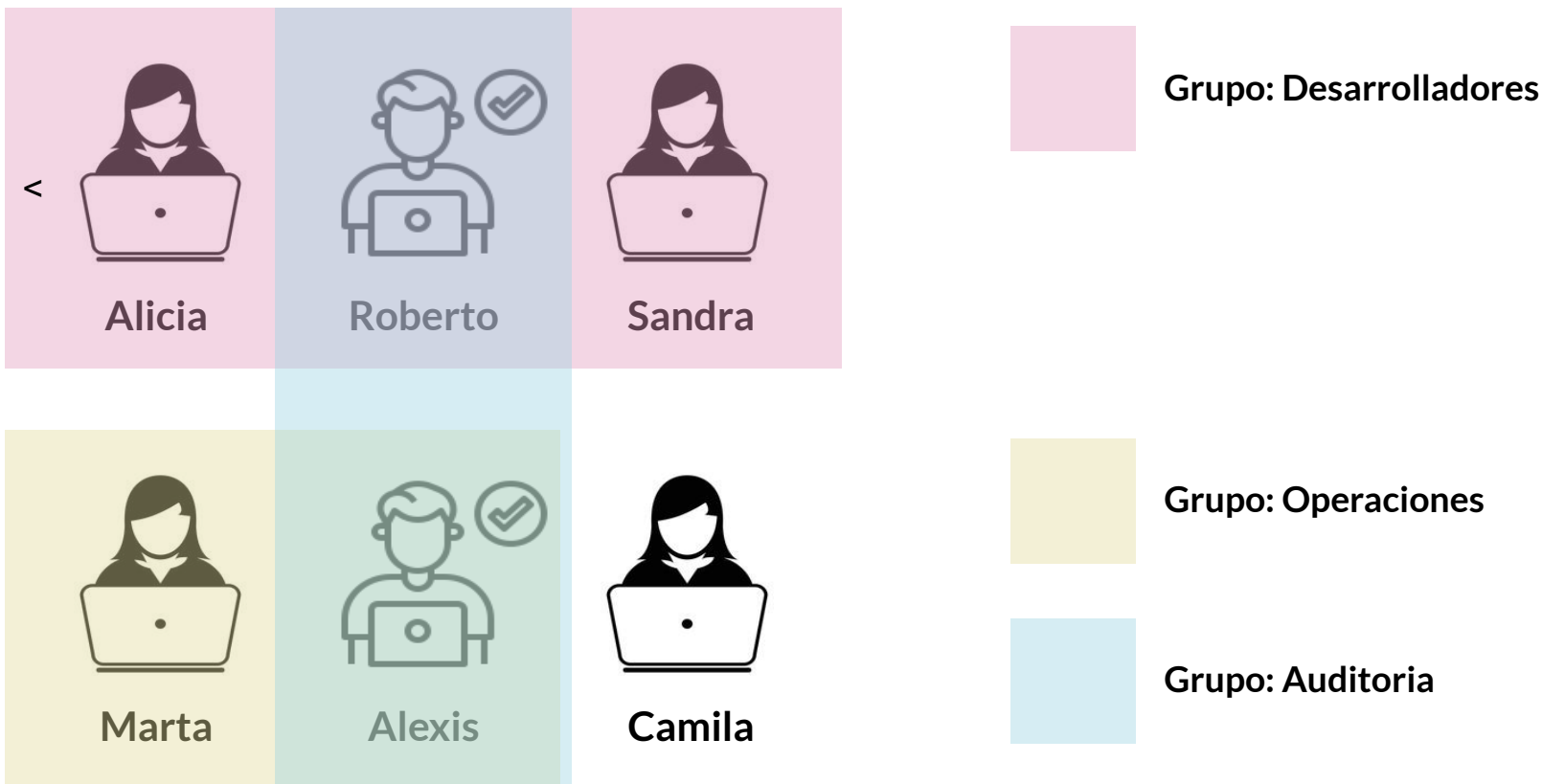
AWS: IAM

Usuarios, grupos y políticas.

IAM: Usuarios y grupos

- **IAM**: Gestión de acceso e identidad, servicio global.
- **Root Account**: creada de manera predeterminada, no debe usarse ni compartirse.
- **Usuarios:** son personas dentro de su organización y se pueden agrupar.
- **Grupos:** solo contienen usuarios, no otros grupos.
- Los usuarios no tienen que pertenecer a un grupo, y el usuario puede pertenecer a varios grupos

Usuarios y grupos



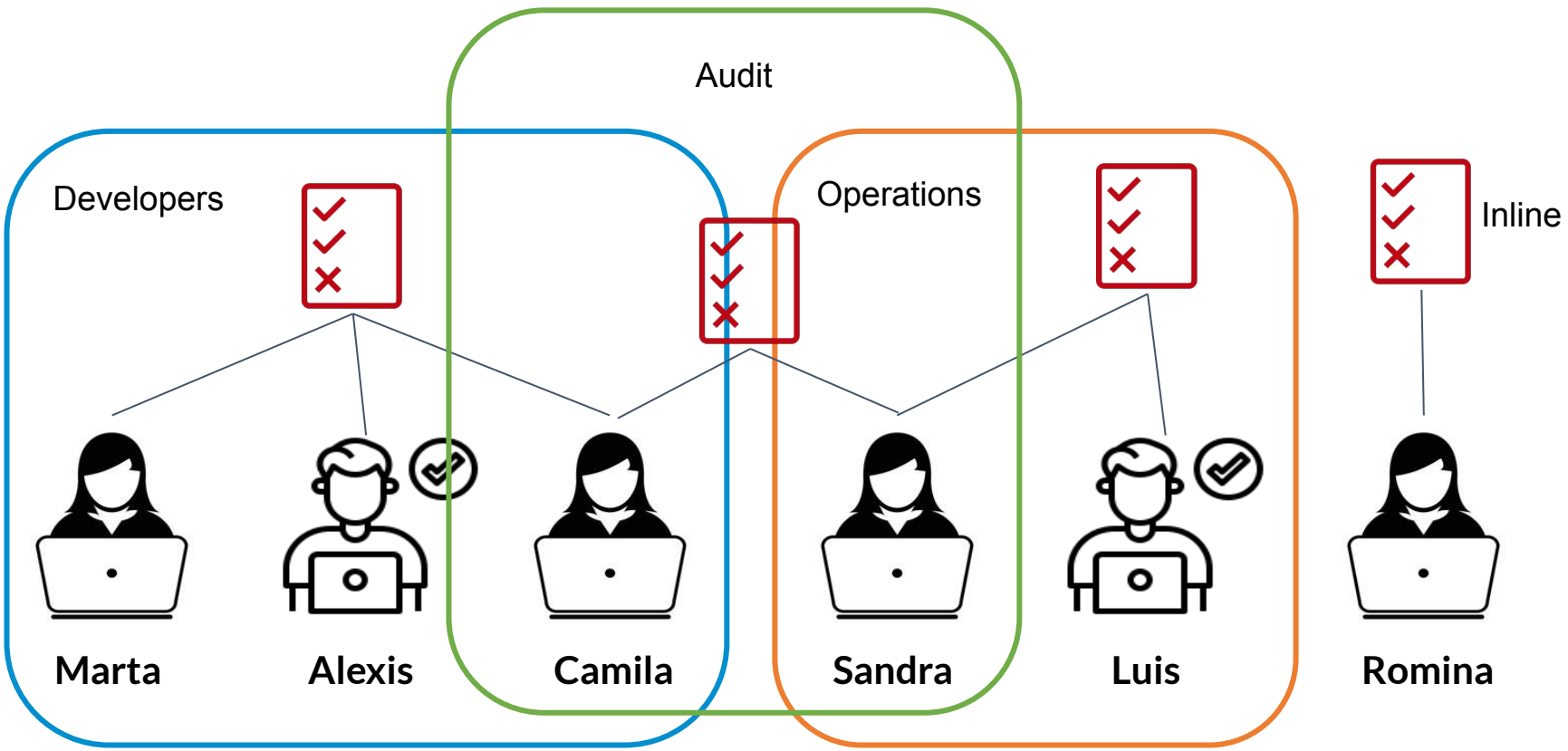
IAM: Politicas

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "elasticloadbalancing:Describe*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:Describe*"
      ],
      "Resource": "*"
    }
  ]
}
```

- A los usuarios o grupos se les pueden asignar documentos JSON llamados políticas.
- Estas políticas definen los permisos de los usuarios.
- En AWS se aplica el principio de privilegios mínimos: no otorgar más permisos de los que necesita un usuario

Politicas IAM

Herencia de Políticas de IAM



Estructura en las Políticas

- Consiste de:
  - Versión
  - Id: Un identificador para la política
  - Declaracion: una o más.

- Declaracion consiste de:
  - Sid: Un identificador.
  - Efecto: permite o deniega el acceso.
  - Principal: cuenta/usuario/rol al que se aplica esta política.
  - Acción: lista de acciones.
  - Recurso: lista de recursos.
  - Condición: condiciones (opcional)

```
{
  "Version": "2012-10-17",
  "Id": "S3-Account-Permissions",
  "Statement": [
    {
      "Sid": "1",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:root"
      },
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource": [
        "arn:aws:s3:::my-bucket/*"
      ]
    }
  ]
}
```

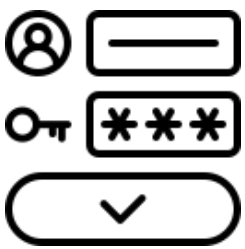
Vision general IAM MFA

Política de Contraseñas

Contraseñas seguras

Longitud mínima de contraseña

Tipos de caracteres específicos



Cambien sus propias contraseñas

Caducidad de contraseña

Reutilizar contraseñas

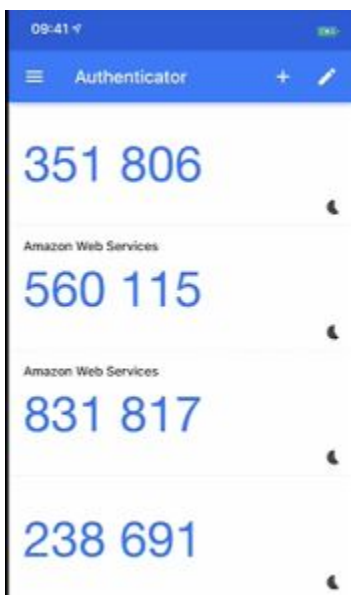
Autenticacion multifactor o MFA

- Los usuarios tienen acceso a su cuenta y posiblemente pueden cambiar configuraciones o eliminar recursos en su cuenta de AWS.
- Quiere proteger sus cuentas raíz y usuarios de IAM
- MFA = contraseña que conoce + dispositivo de seguridad que posee.

Si una contraseña es robada o pirateada, la cuenta no se ve comprometida

Opciones de dispositivos MFA en AWS

Dispositivo Virtual



Google Authenticator (unico dispositivo)

Authy (Multidispositivo)

2º Factor Universal (Universal 2nd Factor)

YubiKey by Yubico (3rd party)

Otros dispositivos MFA en AWS

Dispositivo MFA de llavero de hardware

Provided by Gemalto (3rd party)

MFA de llavero para AWS GovCloud en US

Provided by SurePassID (3rd party)

AWS Access Keys, CLI y SDK

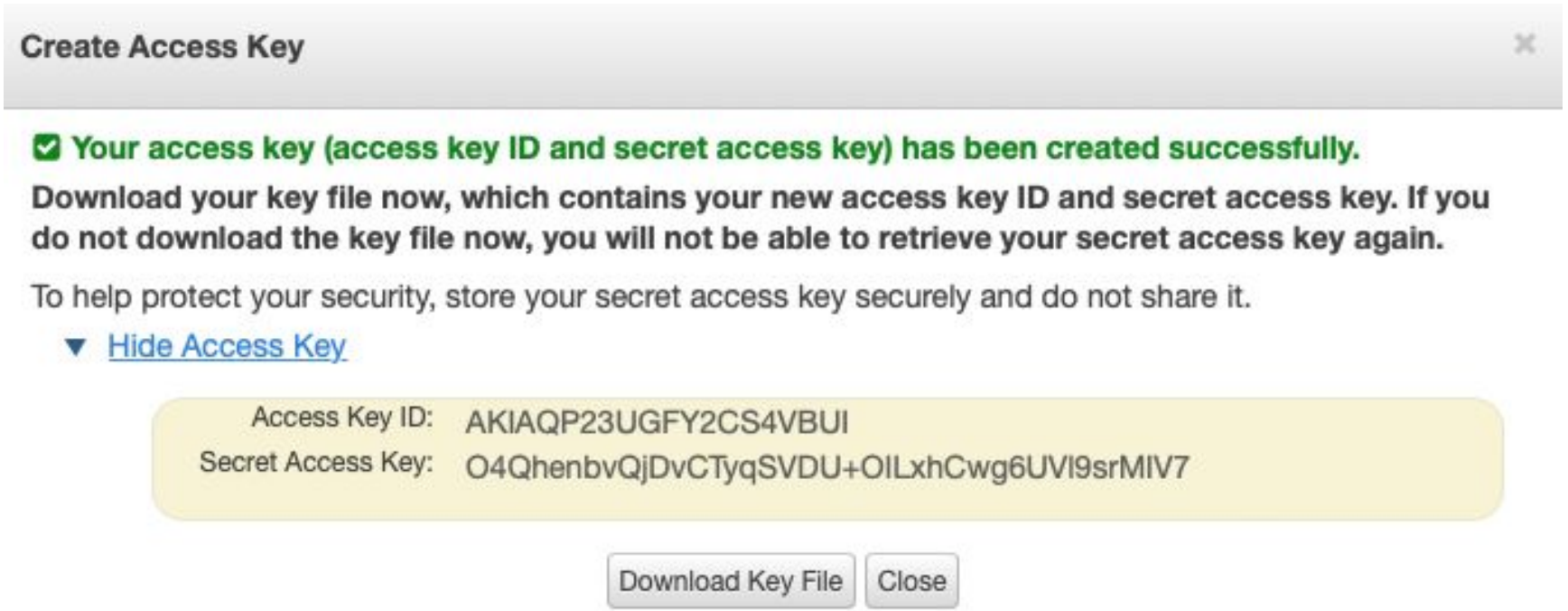
¿Cómo pueden los usuarios acceder a AWS?

AWS CLI

AWS SDK

AWS Management Console

Ejemplo de claves de acceso (falsas)

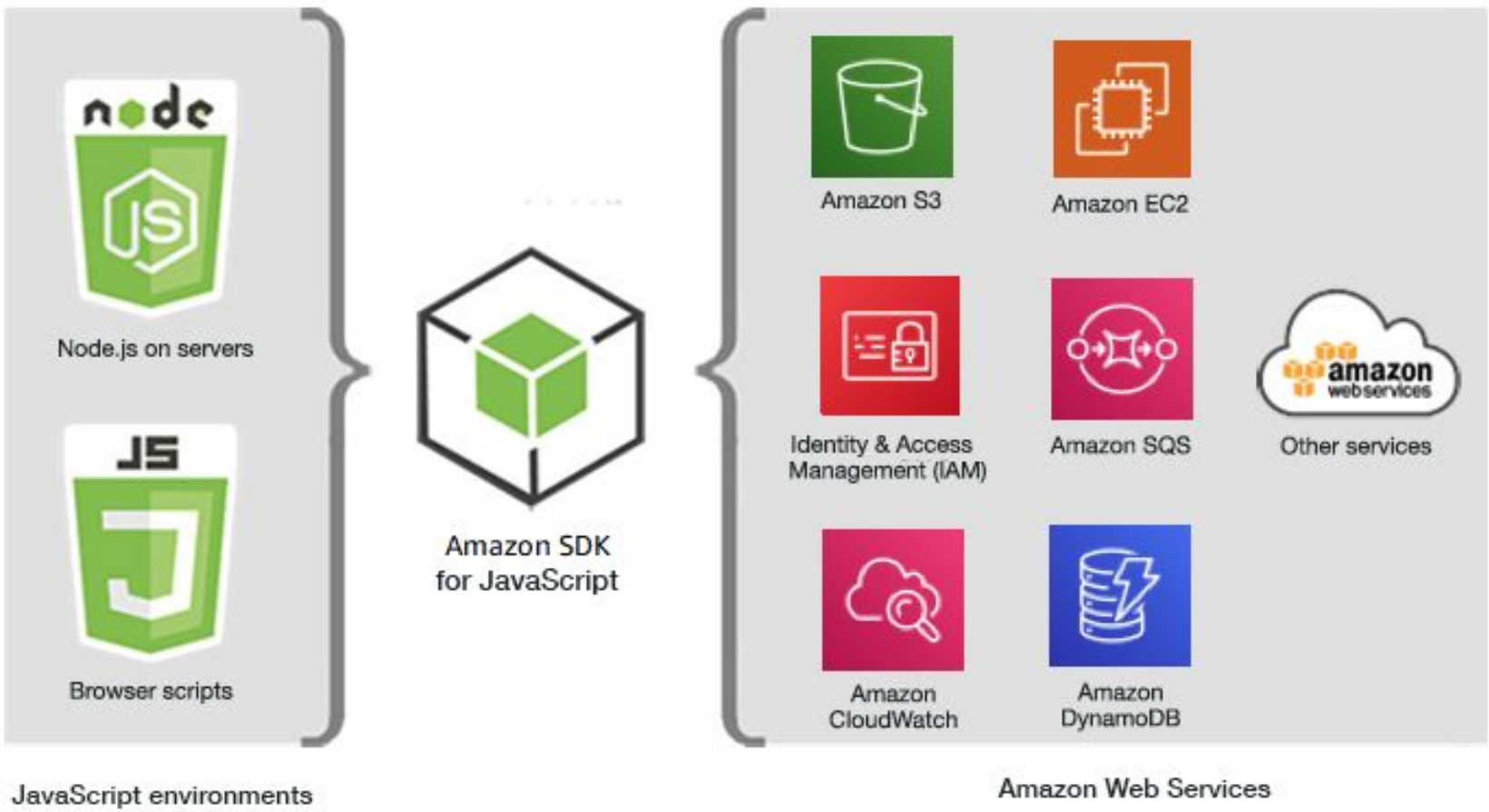


- Access Key ID
- Secret Access Key
- **Recuerda: no compartir tus llaves de acceso**

¿Qué es la CLI de AWS?

- Herramienta que le permite interactuar con los servicios de AWS mediante comandos en su shell de línea de comandos.
- Acceso directo a las API públicas de los servicios de AWS.
- Puede desarrollar scripts para administrar sus recursos
- Es de código abierto https://github.com/aws/aws-cli

¿Qué es el SDK de AWS?

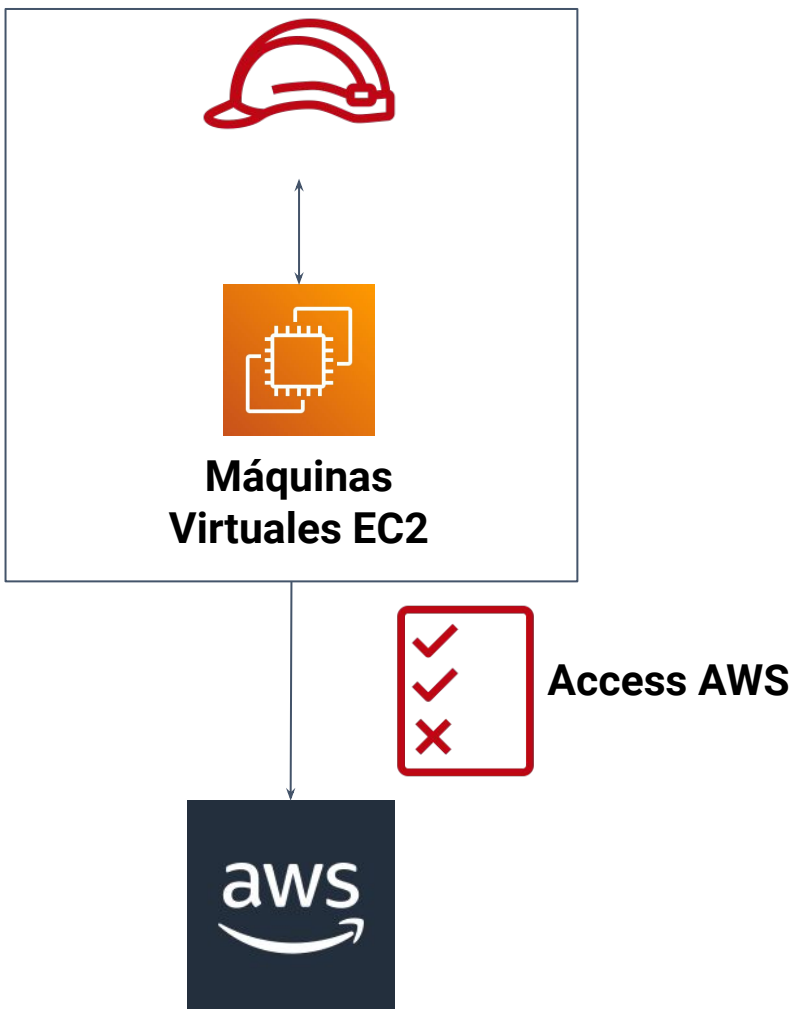


¿Qué es el SDK de AWS?

Software Development Kit

Roles en IAM

Roles IAM para servicios



- Algunos servicios de AWS deberán realizar acciones en su nombre.
- Para ello, asignaremos permisos a los servicios de AWS con Roles de IAM.
- Roles comunes:
  - Roles de la instancia EC2
  - Roles de la función Lambda
  - Roles para CloudFormation

Herramientas de Seguridad en IAM

Herramientas de seguridad

Reporte de Credenciales

Herramientas de seguridad

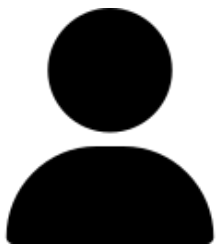
Reporte de Credenciales

Asesor de Acceso

Mejores prácticas en IAM

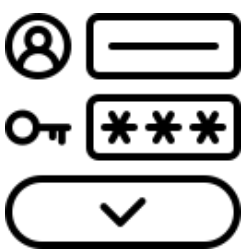
Mejores Prácticas

No usar la cuenta ROOT



Un usuario físico = Un usuario AWS

Asignar Usuarios a Grupos

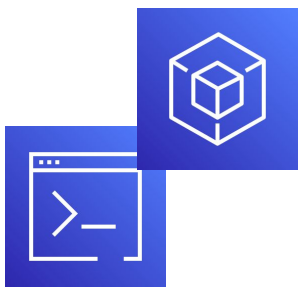


Crear política para contraseñas

Multi Factor Authentication

Crear y usar roles

Mejores Prácticas



Usar Access Keys para accesos programáticos

Nunca Compartir usuarios y access keys

Informe de credenciales de IAM

Modelo de responsabilidad compartida

Modelo de responsabilidad compartida en IAM

- Infraestructura (seguridad de red global).
- Análisis de configuración y vulnerabilidad.
- Validación de cumplimiento.

- Gestión y seguimiento de Usuarios, Grupos, Roles, Políticas.
- Habilitar MFA en todas las cuentas.
- Rotar todas sus llaves con frecuencia
- Usar herramientas de IAM para aplicar los permisos apropiados
- Analizar patrones de acceso y revisar permisos

Resumen IAM

Resumen

Usuarios

Grupos

Politicas

Roles

MFA

CLI

Resumen

AWS SDK

Auditoria

Access Keys