Cloudshine
Enjoy the journey to the cloud

Cloud Essentials

Practico N° 4
Seguridad en la nube de AWS

Repaso

- Modelo de responsabilidad compartida de AWS
- AWS Identity and Access Management (IAM)
- Protección de una cuenta nueva de AWS
- Protección de cuentas
- Protección de datos en AWS
- Trabajo para garantizar la conformidad

Modelo de responsabilidad

Cloudshine
Enjoy the journey to the cloud

Modelo de responsabilidad

CLIENTE

RESPONSABLE DE LA SEGURIDAD "DENTRO" DE LA NUBE

Datos del cliente

Aplicaciones, IAM

Configuración de firewall, red y sistema operativo

Cifrado de datos del lado del cliente y autenticación de integridad de los datos

Cifrado del lado del servidor (datos o sistema de archivos)

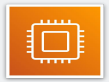
Protección del tráfico en la red (cifrado, integridad, identidad)

Configurable por el cliente

AWS

RESPONSABLE DE LA SEGURIDAD "DE" LA NUBE

Servicios de AWS



Informática

Almacenamiento

Base de datos

Redes

Infraestructura global de AWS

Regiones

Zonas de disponibilidad

Ubicaciones de borde

Cloudshine

Enjoy the journey to the cloud

Servicios y responsabilidad en seguridad

Infraestructura como servicio (IaaS)

- El cliente tiene más flexibilidad en lo que respecta a la configuración de redes y almacenamiento.
- El cliente es responsable de administrar más aspectos de la seguridad.
- El cliente configura los controles de acceso.

Plataforma como servicio (PaaS)

- El cliente no necesita administrar la infraestructura subyacente.
- AWS gestiona el sistema operativo, la implementación de parches a la base de datos, la configuración del firewall y la recuperación de desastres.
- El cliente puede centrarse en la administración de código o datos.

Software como servicio (SaaS)

- El software está alojado de forma centralizada.
- Cuenta con licencia según un modelo de suscripción o de pago por uso.
- Normalmente, el acceso a los servicios se realiza a través de un navegador web, una aplicación móvil o una interfaz de programación de aplicaciones (API).
- Los clientes no necesitan administrar la infraestructura que respalda el servicio.

Servicios administrados por el cliente

Amazon EC2

Amazon Elastic Block Store (Amazon EBS)

Amazon Virtual Private Cloud (Amazon VPC)

Servicios administrados por AWS

Amazon Relational Database Service (Amazon RDS)

AWS Elastic Beanstalk

Ejemplos de SaaS

AWS Trusted Advisor

AWS Shield

Amazon Chime

Cloudshine
Enjoy the journey to the cloud

AWS Identity and Access Management (IAM)

Características

- Administración del acceso a los recursos de AWS (Instancias EC2, Lambda function, bucket s3,etc)
- Define los derechos de acceso de manera detallada
  - **Quién** puede obtener acceso al recurso
  - **A qué** recursos se puede obtener acceso y qué puede hacer el usuario con el recurso
  - **Cómo** se puede obtener acceso a los recursos
- Servicio gratuito de AWS

Componentes esenciales

- **User:** Persona o aplicación que se puede autenticar con una cuenta de AWS
- **Group:** Colección de usuarios
- **Policy:** documento que define a qué recursos se puede obtener acceso y el nivel de acceso a cada recurso
- **Role:** Herramienta para conceder permisos o acceso temporal a recursos de AWS específicos de una cuenta de AWS

Formas de autenticación

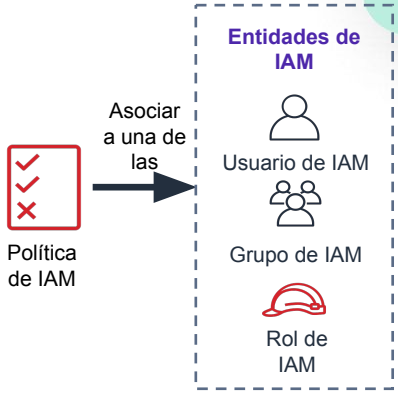
- Acceso mediante programación
  - AWS CLI
  - AWS SDK
- Acceso mediante consola de administración de AWS

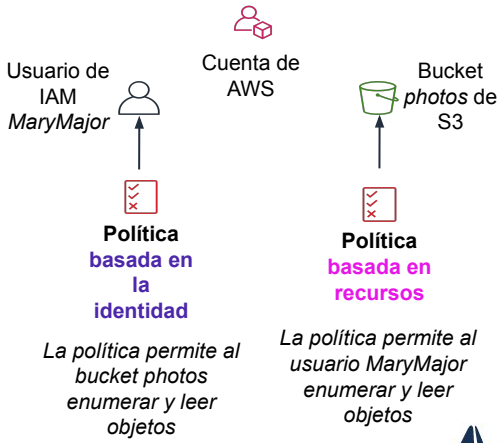
Cloudshine
Enjoy the journey to the cloud

IAM Policies

Características

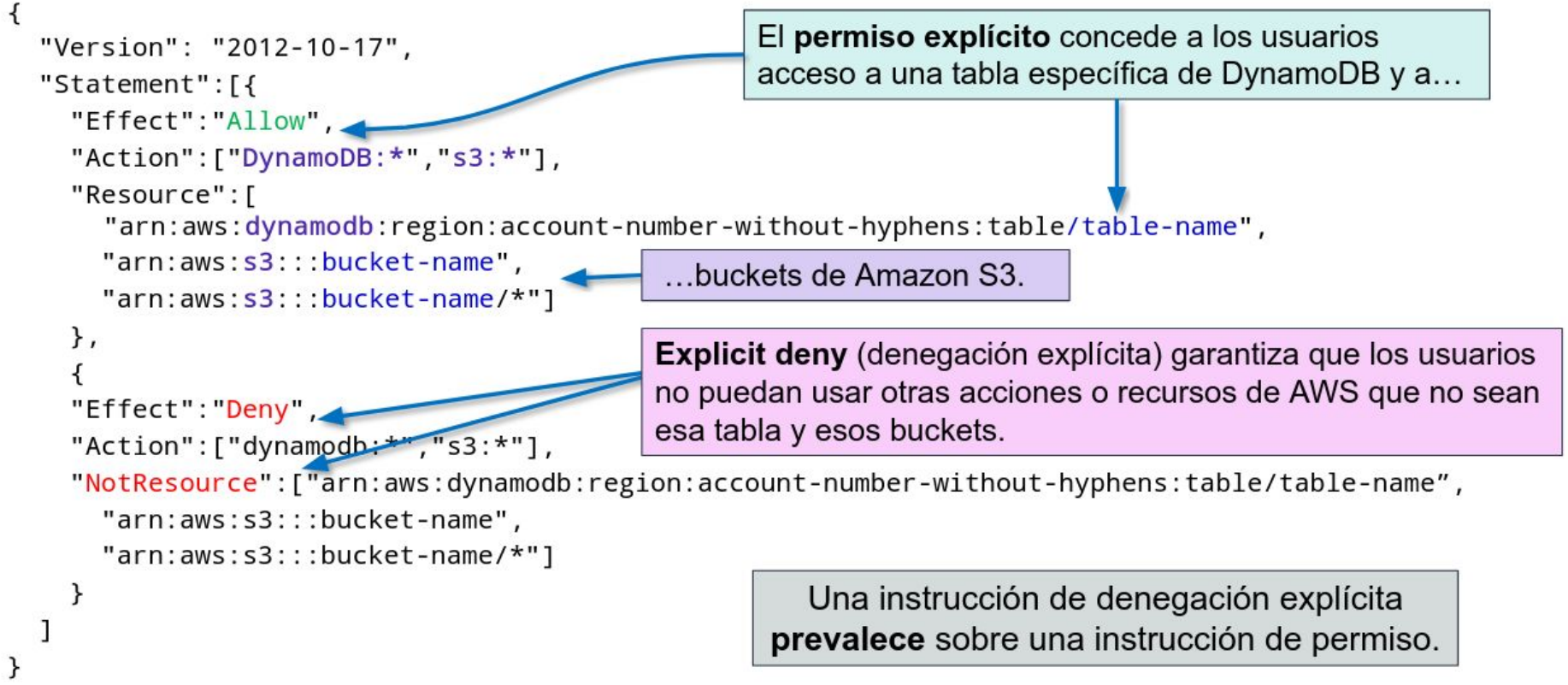
- Una política es un documento que define permisos
- Tipos:
  - **Basada en identidad**
    - Asociada a cualquier **entidad IAM** (user, group, role)
    - **Acciones** que pueden o no hacer las entidades
    - Una policy se puede **asociar a varias entidades**
    - Una entidad puede tener **varias policies asociadas**
      - Tipos:
        - Políticas **administradas**
        - Políticas **insertadas**
  - **Basada en recursos**
    - Asociadas a un **recurso** (bucket s3)
    - Solo son insertadas, **no se administran**





Cloudshine
Enjoy the journey to the cloud

IAM Policies



IAM Groups

Cuenta de AWS

Grupo de IAM: **Administradores**	Grupo de IAM: **Desarrolladores**	Grupo de IAM: **Evaluadores**
Carlos Salazar	Li Juan	Zhang Wei
Márcia Oliveira	Mary Major	John Stiles
	Richard Roe	Li Juan

Cloudshine
Enjoy the journey to the cloud

IAM Roles

Características

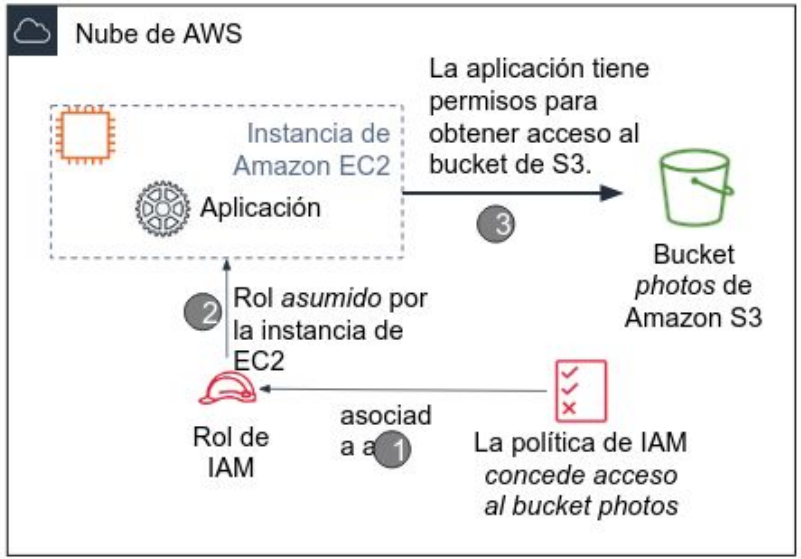
- Un rol de IAM es una **identidad de IAM** con **permisos específicos**.
- **Se asocian políticas** a un rol
- Puede ser asumido por una persona, aplicación o servicio
- Proporciona credenciales temporales
- Ejemplo:

Situación:

- Una aplicación que se ejecuta en una instancia EC2 necesita acceso a un bucket de S3

Solución:

- Definir una política de IAM que conceda acceso al bucket de S3
- Asociar la política a un rol
- Permitir que la instancia EC2 asuma el rol



Cloudshine
Enjoy the journey to the cloud

Protección de una cuenta nueva de AWS

Acceso de usuario raíz de la cuenta de AWS frente al acceso de IAM

- Usuario **root** tiene **permisos de administrador**
- Puede hacer:
  - Actualizar la **contraseña del usuario raíz** de la cuenta
  - Cambiar el plan de **AWS Support**
  - **Restaurar los permisos** de un usuario de IAM
  - Cambiar la **configuración de la cuenta** (por ejemplo, la información de contacto o las regiones permitidas)
- **Acciones de protección:**
  - Dejar de usar el usuario root apenas se pueda
    - **Crear usuarios de IAM** con permisos específicos
    - **Deshabilitar y eliminar** claves de acceso de usuario root
    - **Política de contraseñas** para usuarios
    - Guardar credenciales de usuario root en un lugar seguro
  - Habilitar **MFA**
  - Usar **AWS Cloudtrail**
  - Habilitar **informe de facturación**

Cloudshine
Enjoy the journey to the cloud

Protección de cuentas

AWS Organizations

- Agrupa cuentas en **unidades organizativas** y se asocian **politicas de acceso** a cada una
- **Integración con IAM**
- Usa **Service Control Policy (SCP)** para controlar **acciones de API** y **servicios de AWS** a los que cada cuenta puede tener acceso
    - Son similares a políticas de premisos de IAM, pero no conceden permisos **solo limita**

AWS Key Management Service (AWS KMS)

- Crear y administrar claves de cifrado
- Se integra con AWS Cloudtrail

Amazon Cognito

- Incorpora **control de acceso, inicio de sesión y registro de usuarios** a sus aplicaciones web y móviles
- Admite inicio de sesion con **otros proveedores de identidad** (Google, Facebook, etc)

AWS Shield

- Servicio de proteccion contra **ataques DDoS**
- Detección permanente
- 2 niveles:
    - AWS Shield Standard (sin costo)(OSI capa 3 y 4)
    - AWS Shield Advanced (pago adicional)(OSI capa 3 a 7)

Cloudshine
Enjoy the journey to the cloud

Protección de datos en AWS

Cifrado de datos en reposo

- Codifica los datos de manera que solo se puedan **leer con una clave secreta**, administrada por AWS KMS
- Se admite el cifrado de datos en reposo de cualquier servicio
  - S3
  - EBS
  - EFS
  - RDS

Cifrado de datos en tránsito

- Datos que circulan en una red
- Con AWS Certificate Manager se pueden administrar, implementar y renovar certificados TLS o SSL
- Los servicios de AWS admiten el cifrado en tránsito

Protección de buckets y objetos de Amazon S3

- Por defecto los **buckets son privados**
- Si es necesario se pueden administrar **permisos de acceso**
- Herramientas:
  - S3 Block Public Access
  - Bucket policies
  - Access Control List

Programas de conformidad en AWS

- AWS colabora con **organismos de certificación y auditores independientes** para ofrecer a los clientes información detallada sobre las políticas, los procesos y los controles que establece y aplica AWS.
- Programas de conformidad
    - **Certificaciones y acreditaciones**
    - Leyes, regulaciones y privacidad
    - Alineaciones y marcos de trabajo

AWS Config

- **Evalúe, audite y analice** las **configuraciones** de sus recursos de AWS.
- Monitoreo continuo de las configuraciones.
- Consulta historiales de configuración detallados.
- Simplificar la auditoría de conformidad y el análisis de seguridad.

AWS Artifact

- Es un recurso destinado a la información relacionada con la **conformidad**.
- Proporciona acceso a **informes de seguridad y conformidad,** así como también a acuerdos en línea seleccionados.
- Puede obtener acceso a descargas de ejemplo:
    - Certificaciones **ISO** de AWS
    - Informes del sector de tarjetas de pago (**PCI**) y del control de organizaciones de servicios (**SOC**)

Servicios y recursos de seguridad adicionales

Amazon Macie

- Es un servicio de seguridad de datos que **detecta datos confidenciales** mediante el machine learning y la concordancia de patrones, proporciona visibilidad de los riesgos de seguridad de los datos y permite automatizar la protección contra esos riesgos.

Amazon Inspector

- Es un servicio de administración automatizada de vulnerabilidades que analiza continuamente las cargas de trabajo de AWS en **busca de vulnerabilidades de software y exposición involuntaria a la red**.

Amazon GuardDuty

- Brinda **detección de amenazas inteligente** y monitoreo continuo para proteger sus cargas de trabajo y cuentas de AWS.

Gracias

Cloudshine
Enjoy the journey to the cloud