Laboratorio #1

Introducción a AWS y Creación de Cuenta

Proyecto:
Laboratorios Virtuales de Redes en AWS para el
Fortalecimiento de Competencias en Redes de Nueva Generación

Estudiantes:
Nicolás Carreño Tascón
Juan Manuel Canchala Jiménez

Director:
Carlos Olarte

Asignatura:
Redes de Nueva Generación

Duración Estimada: 60-90 minutos
Costo: \$0.00 (100 % Gratuito)

Septiembre 2025
Elaborado: 22 de septiembre de 2025

Índice

Resumen

Este laboratorio introduce los conceptos fundamentales de Amazon Web Services (AWS) y guía paso a paso en la creación y configuración de una cuenta AWS. Los estudiantes aprenderán a navegar por la consola de AWS, configurar Identity and Access Management (IAM) para gestionar usuarios y permisos, habilitar la autenticación multifactor (MFA) para mejorar la seguridad, y configurar alertas de facturación para monitorear el uso de servicios.

El laboratorio está diseñado para ser completado utilizando exclusivamente el nivel gratuito (Free Tier) de AWS, lo que permite a los estudiantes adquirir experiencia práctica sin incurrir en costos. Al finalizar, los participantes comprenderán la arquitectura global de AWS, incluyendo regiones y zonas de disponibilidad, y estarán preparados para trabajar de manera segura con servicios en la nube.

Palabras clave: AWS, Cloud Computing, IAM, MFA, Free Tier, Seguridad en la Nube, Consola AWS

1 Objetivos

1.1 Objetivo General

Proporcionar a los estudiantes una comprensión práctica de Amazon Web Services y desarrollar las habilidades necesarias para crear, configurar y gestionar de manera segura una cuenta AWS utilizando las mejores prácticas de la industria.

1.2 Objetivos Específicos

- Comprender los conceptos fundamentales de cloud computing y el modelo de servicios de AWS
- Crear y configurar correctamente una cuenta de AWS aprovechando el nivel gratuito (Free Tier)
- Implementar medidas de seguridad básicas utilizando AWS IAM (Identity and Access Management)
- Configurar autenticación multifactor (MFA) para proteger el acceso a la cuenta
- Establecer alertas de facturación para monitorear y controlar costos
- Navegar eficientemente por la consola de AWS y comprender su estructura
- Identificar las diferentes regiones y zonas de disponibilidad de AWS
- Aplicar el principio de mínimo privilegio en la gestión de permisos

1.3 Competencias a Desarrollar

- **Gestión de Identidad y Acceso:** Capacidad para crear y administrar usuarios, grupos y políticas de seguridad en entornos de nube
- **Seguridad en la Nube:** Implementación de controles de seguridad y mejores prácticas para proteger recursos en AWS
- **Administración de Costos:** Monitoreo y control del gasto en servicios de nube mediante alertas y herramientas de facturación
- **Navegación de Consolas:** Destreza en el uso de interfaces web para la gestión de infraestructura en la nube
- **Toma de Decisiones Técnicas:** Selección apropiada de regiones y servicios según requisitos de latencia, cumplimiento y disponibilidad

2 Marco Teórico

2.1 ¿Qué es Cloud Computing?

El Cloud Computing o computación en la nube es un modelo que permite el acceso bajo demanda a un conjunto compartido de recursos computacionales configurables (redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente aprovisionados y liberados con un mínimo esfuerzo de gestión.

2.1.1. Características Esenciales del Cloud Computing

1. **Autoservicio bajo demanda:** Los usuarios pueden aprovisionar recursos automáticamente sin interacción humana con el proveedor
2. **Amplio acceso a la red:** Los servicios están disponibles a través de la red mediante mecanismos estándar
3. **Agrupación de recursos:** Los recursos del proveedor se agrupan para servir a múltiples clientes usando un modelo multi-tenant
4. **Rápida elasticidad:** Los recursos pueden ser aprovisionados y liberados de forma elástica, en algunos casos automáticamente
5. **Servicio medido:** Los sistemas en la nube controlan y optimizan automáticamente el uso de recursos mediante capacidades de medición

2.1.2. Modelos de Servicio

Infrastructure as a Service (IaaS): Proporciona recursos computacionales fundamentales como procesamiento, almacenamiento y redes. El usuario controla sistemas operativos, almacenamiento y aplicaciones, pero no la infraestructura subyacente. AWS EC2 y VPC son ejemplos de IaaS.

Platform as a Service (PaaS): Proporciona una plataforma que permite a los clientes desarrollar, ejecutar y gestionar aplicaciones sin la complejidad de construir y mantener la infraestructura. AWS Elastic Beanstalk es un ejemplo.

Software as a Service (SaaS): Proporciona aplicaciones completas que se ejecutan en la infraestructura del proveedor. Los usuarios acceden a las aplicaciones desde diversos dispositivos cliente. Amazon WorkMail es un ejemplo.

2.2 Introducción a Amazon Web Services (AWS)

Amazon Web Services es la plataforma de servicios en la nube más completa y ampliamente adoptada del mundo. Lanzada en 2006, AWS ofrece más de 200 servicios completamente funcionales desde centros de datos distribuidos globalmente. Millones de clientes, incluyendo startups, grandes empresas y agencias gubernamentales, utilizan AWS para reducir costos, ser más ágiles e innovar más rápido.

2.2.1. Ventajas de AWS

- **Elasticidad y Escalabilidad:** Capacidad de aumentar o reducir recursos según la demanda
- **Pago por uso:** Solo pagas por los recursos que consumes, sin contratos a largo plazo
- **Alcance Global:** Presencia en múltiples regiones geográficas para baja latencia
- **Seguridad:** Cumplimiento de estándares internacionales y herramientas de seguridad robustas
- **Innovación Continua:** Lanzamiento constante de nuevos servicios y funcionalidades
- **Experiencia y Madurez:** Más de 15 años de experiencia en servicios en la nube

2.3 Infraestructura Global de AWS

2.3.1. Regiones (Regions)

Una región de AWS es una ubicación geográfica física en el mundo donde AWS tiene múltiples centros de datos. Cada región es completamente independiente y está aislada de las demás para lograr la máxima tolerancia a fallos y estabilidad.

Características de las Regiones:

- Cada región tiene múltiples zonas de disponibilidad aisladas
- Los datos no se replican automáticamente entre regiones (cumplimiento normativo)
- Puedes elegir la región según latencia, costos y requisitos regulatorios
- A partir de 2025, AWS cuenta con más de 30 regiones en todo el mundo

Ejemplos de Regiones:

- `us-east-1` - Virginia del Norte (EE.UU.) - Región más antigua y con más servicios
- `us-west-2` - Oregón (EE.UU.)
- `eu-west-1` - Irlanda (Europa)
- `ap-southeast-1` - Singapur (Asia Pacífico)
- `sa-east-1` - São Paulo (Sudamérica)

2.3.2. Zonas de Disponibilidad (Availability Zones - AZs)

Una Zona de Disponibilidad es uno o más centros de datos discretos, cada uno con energía, redes y conectividad redundantes, ubicados dentro de una región de AWS. Las AZs están diseñadas para el aislamiento de fallos.

Características de las AZs:

- Cada región tiene múltiples AZs (típicamente 3 o más)
- Las AZs están separadas físicamente (kilómetros de distancia)
- Conectadas entre sí con redes de baja latencia (menos de 1ms)
- Permiten diseñar aplicaciones de alta disponibilidad
- Identificadas con letras: us-east-1a, us-east-1b, us-east-1c

Ejemplo de Arquitectura Multi-AZ:
Si una aplicación se despliega en dos AZs diferentes, si una AZ falla (por desastre natural, corte de energía, etc.), la aplicación continúa funcionando en la otra AZ, garantizando alta disponibilidad.

2.3.3. Edge Locations y CloudFront

Las Edge Locations son puntos de presencia que AWS utiliza para entregar contenido con baja latencia a los usuarios finales. Hay más de 400 edge locations distribuidas globalmente, muchas más que regiones. Se utilizan principalmente para Amazon CloudFront (CDN) y Route 53 (DNS).

2.4 AWS Free Tier (Nivel Gratuito)

AWS ofrece un nivel gratuito que permite a los usuarios explorar y probar servicios de AWS sin costo. Existen tres tipos de ofertas de Free Tier:

2.4.1. Prueba Gratuita de 12 Meses

Disponible para nuevos clientes de AWS, comienza desde la fecha de registro inicial. Incluye:

- **Amazon EC2:** 750 horas por mes de instancias t2.micro (o t3.micro en algunas regiones)
- **Amazon S3:** 5 GB de almacenamiento estándar
- **Amazon RDS:** 750 horas por mes de instancias db.t2.micro
- **Amazon CloudFront:** 50 GB de transferencia de datos salientes
- **Amazon VPC:** Sin costo adicional (incluido en Free Tier)

2.4.2. Siempre Gratuito

Ofertas que no expiran y están disponibles para todos los clientes de AWS:

- **AWS Lambda:** 1 millón de solicitudes gratuitas por mes
- **Amazon DynamoDB:** 25 GB de almacenamiento
- **Amazon SNS:** 1 millón de publicaciones
- **Amazon CloudWatch:** 10 métricas personalizadas y 10 alarmas

2.4.3. Pruebas a Corto Plazo

Ofertas de prueba que comienzan desde la primera vez que activas un servicio particular.

IMPORTANTE: Para este laboratorio, utilizaremos exclusivamente servicios incluidos en el Free Tier. Es fundamental seguir las instrucciones de limpieza al final para evitar cargos no deseados.

2.5 AWS Identity and Access Management (IAM)

IAM es el servicio de AWS que permite gestionar de forma segura el acceso a los recursos de AWS. Con IAM, puedes controlar quién está autenticado (ha iniciado sesión) y autorizado (tiene permisos) para usar recursos.

2.5.1. Componentes Principales de IAM

1. Usuarios (Users):

- Representan a una persona o aplicación que interactúa con AWS
- Cada usuario tiene credenciales únicas (contraseña y/o access keys)
- Pueden tener permisos asignados directamente o a través de grupos
- Buena práctica: NO usar la cuenta root para tareas diarias

2. Grupos (Groups):

- Colección de usuarios IAM
- Los permisos asignados al grupo se aplican a todos sus miembros
- Un usuario puede pertenecer a múltiples grupos
- Facilita la gestión de permisos a escala

3. Roles (Roles):

- Identidad IAM con permisos específicos
- Pueden ser asumidos temporalmente por usuarios, aplicaciones o servicios

- No tienen credenciales permanentes (se generan temporalmente)
- Útiles para servicios de AWS que necesitan acceder a otros servicios

4. Políticas (Policies):

- Documentos JSON que definen permisos
- Especifican qué acciones se permiten o deniegan sobre qué recursos
- Pueden ser administradas por AWS o creadas por el usuario
- Se adjuntan a usuarios, grupos o roles

2.5.2. Ejemplo de Política IAM

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::mi-bucket/*",
        "arn:aws:s3:::mi-bucket"
      ]
    }
  ]
}
```

Listing 1: Política que permite solo lectura en S3

2.5.3. Principio de Mínimo Privilegio

Es una mejor práctica de seguridad que consiste en otorgar únicamente los permisos necesarios para realizar una tarea específica. Esto limita el impacto de compromisos de seguridad y reduce el riesgo de cambios accidentales.

Aplicación práctica:

- No usar la cuenta root para operaciones diarias
- Crear usuarios IAM con permisos específicos
- Revisar y auditar permisos regularmente
- Eliminar permisos no utilizados

2.6 Autenticación Multifactor (MFA)

MFA añade una capa adicional de seguridad al requerir dos o más métodos de verificación:

1. **Algo que sabes:** Contraseña o PIN
2. **Algo que tienes:** Dispositivo físico o aplicación móvil
3. **Algo que eres:** Huella digital o reconocimiento facial

Tipos de MFA en AWS:

- **MFA Virtual:** Aplicaciones como Google Authenticator, Microsoft Authenticator, Authy
- **U2F Security Key:** Dispositivos físicos como YubiKey
- **MFA por Hardware:** Token físico dedicado

Para este laboratorio, utilizaremos MFA Virtual (gratuito y fácil de configurar).

3 Requisitos Previos

3.1 Conocimientos Necesarios

- Conocimientos básicos de navegación web
- Comprensión general de conceptos de redes e internet
- Capacidad para seguir instrucciones técnicas detalladas
- Familiaridad con correo electrónico y aplicaciones móviles

3.2 Recursos Técnicos Requeridos

- **Computadora:** PC, Mac o Linux con navegador web moderno
- **Navegador:** Chrome, Firefox, Safari o Edge (actualizado)
- **Conexión a Internet:** Estable, mínimo 1 Mbps
- **Correo Electrónico:** Cuenta de email válida y activa
- **Teléfono Móvil:** Para instalar aplicación MFA (Google Authenticator o similar)
- **Tarjeta de Crédito/Débito:** Para verificación de identidad (NO se realizarán cargos)

3.3 Costos Estimados

Concepto	Costo
Creación de cuenta AWS	$0.00
Servicios IAM	$0.00 (siempre gratuito)
MFA Virtual	$0.00 (aplicación gratuita)
Alertas de facturación	$0.00 (Free Tier)
TOTAL	**$0.00**

Cuadro 1: Costos del Laboratorio 1

NOTA IMPORTANTE: AWS requiere una tarjeta de crédito/débito para verificar tu identidad, pero NO se realizarán cargos si sigues las instrucciones correctamente y permaneces dentro de los límites del Free Tier.

3.4 Tiempo Estimado

- Lectura del marco teórico: 15-20 minutos
- Creación de cuenta AWS: 15-20 minutos
- Configuración de IAM y MFA: 20-30 minutos
- Configuración de alertas: 10-15 minutos

- Exploración de la consola: 10-15 minutos
- **TOTAL ESTIMADO:** 60-90 minutos

4 Procedimiento Paso a Paso

4.1 Paso 1: Creación de Cuenta AWS

Objetivo: Crear una nueva cuenta de Amazon Web Services aprovechando el nivel gratuito.

4.1.1. 1.1 Acceder al Sitio Web de AWS

Instrucciones detalladas:

1. Abrir tu navegador web preferido (Chrome, Firefox, Safari o Edge)
2. En la barra de direcciones, escribir: `https://aws.amazon.com`
3. Presionar Enter para cargar la página
4. Esperar a que la página principal de AWS se cargue completamente
5. Verificar que estés en el sitio oficial (debe aparecer el candado de seguridad en la barra de direcciones)

Descripción visual de la página: La página principal de AWS muestra un banner grande con opciones de servicios, un botón naranja que dice Çrear una cuenta de AWS.en la esquina superior derecha, y varios menús desplegables incluyendo "Productos", "Solucionesz Recursos".

4.1.2. 1.2 Iniciar el Proceso de Registro

Instrucciones:

1. Localizar el botón naranja Çrear una cuenta de AWS.en la esquina superior derecha
2. Si no lo ves, busca "Sign Up.o Registrarse"
3. Hacer clic en el botón
4. Serás redirigido a la página de registro

Alternativa: Puedes ir directamente a: `https://portal.aws.amazon.com/billing/signup`

4.1.3. 1.3 Proporcionar Información de la Cuenta Root

Formulario a completar:
Instrucciones paso a paso:

1. En el campo Root user email address", escribir tu correo electrónico
2. IMPORTANTE: Usa un correo que revises frecuentemente
3. El correo debe ser válido y accesible (recibirás un código de verificación)

Campo	Descripción / Qué ingresar
Root user email address	Tu dirección de correo electrónico personal (ej: tunombre@gmail.com)
AWS account name	Un nombre descriptivo para tu cuenta (ej: ÇuentaEstudiantil-NombreApellido")

Cuadro 2: Información de Cuenta Root

4. En .ªWS account name", ingresar un nombre descriptivo
5. Ejemplos de nombres: .ªWS-Estudiante-2025", "Proyecto-Redes-AWS", "MiCuenta-Practica"
6. Hacer clic en "Verify email address"(Verificar dirección de correo)

Verificación de correo electrónico:

1. AWS enviará un código de verificación de 6 dígitos a tu correo
2. Abrir tu bandeja de entrada (puede tardar 1-2 minutos)
3. Buscar un correo de .ªmazon Web Servicesçon asunto "Your AWS verification code"
4. Copiar el código de 6 dígitos
5. Volver a la página de AWS
6. Pegar el código en el campo "Verification code"
7. Hacer clic en "Verify"(Verificar)

¿Qué pasa si no recibo el correo?

- Revisar la carpeta de spam/correo no deseado
- Esperar 3-5 minutos (a veces hay retraso)
- Verificar que escribiste correctamente el correo
- Hacer clic en Resend code"si es necesario

4.1.4. 1.4 Crear Contraseña para la Cuenta Root

Requisitos de la contraseña:

- Mínimo 8 caracteres
- Al menos una letra mayúscula
- Al menos una letra minúscula
- Al menos un número

- Se recomienda incluir caracteres especiales (!@#$%^&*)

Instrucciones:

1. En Root user password", crear una contraseña segura
2. Ejemplo de contraseña segura: `MiAWS2025!Segura`
3. En Çonfirm root user password", escribir exactamente la misma contraseña
4. IMPORTANTE: Guardar esta contraseña en un lugar seguro (administrador de contraseñas)
5. NO compartir esta contraseña con nadie
6. Hacer clic en Çontinue"(Continuar)

Recomendación de seguridad: Utiliza un administrador de contraseñas como LastPass, 1Password, Bitwarden o el integrado en tu navegador para generar y almacenar contraseñas seguras.

4.1.5. 1.5 Proporcionar Información de Contacto

Tipo de cuenta a seleccionar:

- AWS ofrece dos tipos: "Personal"(Personal) y "Business"(Empresarial)
- Para este laboratorio, seleccionar **"Personal"**
- La diferencia principal es administrativa, los servicios son los mismos

Formulario de información personal:

Campo	**Qué ingresar**
Full Name	Tu nombre completo (ej: Nicolás Carreño Tascón)
Phone Number	Número de teléfono con código de país (ej: +57 300 123 4567)
Country/Region	Seleccionar tu país de la lista desplegable
Address	Dirección física completa (calle y número)
City	Ciudad de residencia
State/Province/Region	Departamento o estado
Postal Code	Código postal

Cuadro 3: Información de Contacto Requerida

Instrucciones paso a paso:

1. Hacer clic en el círculo "Personal.$^{\text{en}}$.$^{\text{A}}$ccount type"
2. Completar "Full Nameçon tu nombre completo legal
3. En "Phone Number":

- Seleccionar el código de tu país del menú desplegable (ej: +57 para Colombia)
- Escribir tu número de celular sin espacios ni guiones
- Ejemplo: +57 3001234567

4. Seleccionar tu país en Çountry or Region"
5. Completar tu dirección física exacta en .ªddress"
6. Escribir tu ciudad en Çity"
7. Seleccionar o escribir tu estado/departamento en "State/Province/Region"
8. Ingresar el código postal en "Postal Code"
9. Leer el .ªWS Customer Agreement"(Acuerdo de Cliente de AWS)
10. Marcar la casilla Ï have read and agree to the terms of the AWS Customer Agreement"
11. Hacer clic en Çontinue"(Continuar)

Nota importante: AWS utiliza esta información para cumplir con regulaciones fiscales y geográficas. Los datos deben ser verídicos y precisos.

4.1.6. 1.6 Agregar Información de Pago

¿Por qué AWS requiere una tarjeta?

- Para verificar tu identidad y prevenir fraude
- Para tener un método de pago en caso de que excedas los límites del Free Tier
- La tarjeta NO será cargada si te mantienes dentro del Free Tier
- Se realizará una autorización temporal de $1 USD que será revertida

Tipos de tarjeta aceptadas:

- Tarjetas de crédito (Visa, Mastercard, American Express)
- Tarjetas de débito con logo Visa o Mastercard
- NO se aceptan tarjetas prepagadas en la mayoría de casos

Formulario de pago:

Campo	**Descripción**
Credit or debit card number	Número de la tarjeta (16 dígitos típicamente)
Expiration date	Fecha de vencimiento (MM/YY)
Cardholder's name	Nombre exacto como aparece en la tarjeta
Security code (CVV)	Código de 3 o 4 dígitos al reverso
Billing address	Usar la misma dirección del paso anterior

Cuadro 4: Información de Pago

Instrucciones:

1. En Çredit or debit card number", ingresar los 16 dígitos de tu tarjeta
2. No incluir espacios ni guiones, solo números
3. En .Expiration date", seleccionar mes y año de vencimiento
4. En Çardholder's name", escribir el nombre EXACTO que aparece en la tarjeta
5. Incluir todos los nombres y apellidos como están impresos
6. En "Security code", ingresar el CVV (3 dígitos en Visa/MC, 4 en Amex)
7. Para "Billing address", puedes:
   - Seleccionar Üse contact address"si es la misma
   - O completar una dirección diferente si es necesario
8. Hacer clic en "Verify and Add"(Verificar y Agregar)

Verificación de la tarjeta:

1. AWS realizará una autorización temporal de $1 USD
2. Este cargo aparecerá como "pendiente.en tu estado de cuenta
3. Será cancelado automáticamente en 3-5 días hábiles
4. Es solo para verificar que la tarjeta es válida y activa
5. NO es un cobro real

Si la verificación falla:

- Verificar que los datos estén correctos (número, fecha, CVV, nombre)
- Asegurarse de que la tarjeta tenga fondos disponibles para la autorización
- Contactar a tu banco si persiste el problema
- Intentar con otra tarjeta si es posible

4.1.7. 1.7 Confirmar Identidad (Verificación Telefónica)

Proceso de verificación:

1. Serás redirigido a la página Çonfirm your identity"
2. AWS te contactará por teléfono o SMS para verificar tu identidad
3. Seleccionar método de verificación:
   - "Text message (SMS) Recibirás un código por mensaje de texto
   - "Voice call Recibirás una llamada automática
4. Se recomienda seleccionar "Text message (SMS)"(más rápido y fácil)

Verificación por SMS (recomendado):

1. Seleccionar "Text message (SMS)"
2. Confirmar que el número de teléfono mostrado es correcto
3. Si no es correcto, hacer clic en .Edit"para modificarlo
4. En el campo "Security check", completar el CAPTCHA

- Escribir los caracteres que aparecen en la imagen distorsionada
- Si no puedes leerlos, hacer clic en el ícono de refrescar

5. Hacer clic en "Send SMS"(Enviar SMS)
6. Esperar 30-60 segundos a recibir el mensaje
7. El mensaje contendrá un código de 4 dígitos
8. Ingresar el código en el campo "Verification code"
9. Hacer clic en "Verify Code"(Verificar Código)

Verificación por Llamada (alternativa):

1. Seleccionar "Voice call"
2. Completar el CAPTCHA
3. Hacer clic en Çall me now"
4. Responder la llamada (puede tardar 1-2 minutos)
5. Escucharás un mensaje automático en inglés
6. El mensaje te dirá un código de 4 dígitos
7. Ingresar el código en el sitio web
8. Hacer clic en "Verify Code"

Solución de problemas:

- Si no recibes el SMS en 2 minutos, hacer clic en Resend SMS"
- Verificar que tu teléfono tenga señal y pueda recibir mensajes internacionales
- Algunos operadores bloquean SMS automáticos - contacta a tu operador
- Si SMS no funciona, intentar con llamada telefónica

4.1.8. 1.8 Seleccionar Plan de Soporte

Planes disponibles:

Plan	Costo	Descripción
Basic Support	$0/mes	Acceso a foros, documentación y AWS Trusted Advisor básico
Developer	$29/mes	Soporte técnico durante horario laboral
Business	$100/mes	Soporte 24/7, tiempo de respuesta más rápido
Enterprise	$15,000/mes	Account manager dedicado, soporte premium

Cuadro 5: Planes de Soporte AWS

Instrucciones:

1. En la página "Select a support plan", verás los 4 planes disponibles

2. Para este laboratorio y uso educativo, seleccionar **"Basic Support - Free"**
3. Este plan es completamente gratuito y suficiente para aprendizaje
4. Incluye:
   - Acceso a documentación y whitepapers
   - Acceso a AWS Forums
   - AWS Personal Health Dashboard
   - 7 comprobaciones básicas de AWS Trusted Advisor
5. Hacer clic en el botón Çomplete sign up"(Completar registro) debajo de "Basic Support"

¿Qué pasa después?

- Verás una página de confirmación: Çongratulations! Your AWS account is ready"
- AWS procesará tu cuenta (puede tomar 5-10 minutos)
- Recibirás un correo de confirmación cuando esté lista
- El correo tendrá el asunto: "Welcome to Amazon Web Services"

Tiempo de espera:

- Normalmente la cuenta se activa en 5-10 minutos
- En algunos casos puede tomar hasta 24 horas
- Durante este tiempo, puedes explorar la documentación de AWS
- Recibirás un correo cuando tu cuenta esté completamente activa

4.2 Paso 2: Primer Inicio de Sesión y Exploración de la Consola

Objetivo: Iniciar sesión en la consola de AWS y familiarizarse con la interfaz.

4.2.1. 2.1 Acceder a la Consola de AWS

Instrucciones:

1. Una vez que recibas el correo de confirmación de cuenta activa
2. Abrir el navegador e ir a: `https://console.aws.amazon.com`
3. Alternativamente, ir a `https://aws.amazon.com` y hacer clic en "Sign In to the Console"
4. Verás la página de inicio de sesión de AWS

4.2.2. 2.2 Iniciar Sesión como Usuario Root

Proceso de inicio de sesión:

1. En la página de inicio de sesión, seleccionar Root user"
2. En el campo Root user email address", ingresar el correo con el que creaste la cuenta
3. Hacer clic en "Next"(Siguiente)

4. En la siguiente pantalla, ingresar tu contraseña en "Password"
5. Resolver el CAPTCHA de seguridad si aparece
6. Hacer clic en "Sign in"(Iniciar sesión)
7. Serás redirigido a la consola de administración de AWS

Primera vista de la consola: La consola de AWS se divide en varias secciones:

- **Barra superior:** Servicios, información de cuenta, región, notificaciones
- **Barra de búsqueda:** Para buscar servicios rápidamente
- **Panel central:** Widgets personalizables con información
- **Recently visited:** Servicios usados recientemente
- **Favorites:** Servicios marcados como favoritos

4.2.3. 2.3 Familiarizarse con la Navegación

Menú "Services"(Servicios):

1. En la esquina superior izquierda, hacer clic en "Services"
2. Verás una lista desplegable con todos los servicios de AWS
3. Los servicios están organizados por categorías:
   - Compute (Cómputo): EC2, Lambda, Elastic Beanstalk
   - Storage (Almacenamiento): S3, EBS, Glacier
   - Database (Bases de datos): RDS, DynamoDB, Aurora
   - Networking & Content Delivery (Redes): VPC, CloudFront, Route 53
   - Security, Identity & Compliance: IAM, Cognito, WAF
   - Y muchas más categorías...
4. Explorar brevemente cada categoría para familiarizarte

Selector de Región:

1. En la barra superior derecha, junto al nombre de tu cuenta
2. Verás el nombre de una región (ej: "N. Virginia", .ºhio", .ºregon")
3. Hacer clic en el nombre de la región
4. Se desplegará una lista con todas las regiones disponibles
5. Cada región está identificada con:
   - Nombre descriptivo (ej: ÜS East (N. Virginia)")
   - Código de región (ej: üs-east-1")
6. Para este laboratorio, seleccionar una región cercana a tu ubicación
7. Recomendaciones por ubicación:
   - Sudamérica: "South America (São Paulo) sa-east-1
   - Norte América: ÜS East (N. Virginia) us-east-1
   - Europa: .ºrope (Ireland) eu-west-1

8. Hacer clic en la región deseada para seleccionarla

Importante sobre regiones:

- La mayoría de recursos son específicos de región
- Si creas un recurso en us-east-1, no lo verás si cambias a eu-west-1
- Algunos servicios son globales (IAM, CloudFront, Route 53)
- Siempre verifica en qué región estás trabajando

4.2.4. 2.4 Explorar el Panel de Control (Dashboard)

AWS Management Console Home:

1. Hacer clic en el logo de AWS (esquina superior izquierda) para volver al inicio
2. El dashboard muestra:
   - **Build a solution:** Tutoriales para empezar
   - **Recently visited services:** Servicios que has usado
   - **Explore AWS:** Recursos de aprendizaje
   - **Cost and usage:** Vista rápida de costos (debe estar en $0.00)
3. Puedes personalizar este dashboard agregando/removiendo widgets

Búsqueda rápida de servicios:

1. En la barra superior, hay un campo de búsqueda
2. Escribir el nombre de un servicio (ej: ÏAM", .[EC]2", "S3")
3. Aparecerán sugerencias mientras escribes
4. Hacer clic en el servicio deseado para acceder directamente
5. Esto es más rápido que navegar por menús

4.3 Paso 3: Configuración de Seguridad con IAM

Objetivo: Crear usuarios IAM, grupos y configurar políticas de seguridad siguiendo mejores prácticas.

4.3.1. 3.1 Acceder al Servicio IAM

Instrucciones:

1. En la consola de AWS, hacer clic en "Services"(esquina superior izquierda)
2. Desplazarse hasta la categoría "Security, Identity, & Compliance"
3. Hacer clic en ÏAM"
4. Alternativamente, usar la búsqueda rápida: escribir ÏAMz hacer clic
5. Serás redirigido al dashboard de IAM

Dashboard de IAM: El dashboard muestra:

- **IAM Resources:** Número de usuarios, grupos, roles, políticas

- **Security Status:** Recomendaciones de seguridad (5 inicialmente)
- **Sign-in URL for IAM users:** URL personalizada para que usuarios IAM inicien sesión

4.3.2. 3.2 Eliminar Claves de Acceso de Root (Seguridad)

Recomendación de seguridad AWS: La cuenta root no debe tener claves de acceso activas para prevenir uso indebido.

Verificar claves de acceso:

1. En el dashboard de IAM, buscar "Security recommendations"
2. Debería aparecer: .Add MFA for root user"(esto lo haremos después)
3. Si aparece "Delete your root user access keys", seguir estos pasos:
   - Hacer clic en el menú de cuenta (esquina superior derecha)
   - Seleccionar "Security credentials"
   - Desplazarse hasta .Access keys"
   - Si hay alguna clave listada, hacer clic en "Delete"
   - Confirmar la eliminación
4. Si no hay claves, ¡perfecto! Continuar al siguiente paso

4.3.3. 3.3 Crear un Alias de Cuenta (Opcional pero Recomendado)

¿Qué es un alias de cuenta? Un nombre personalizado para tu cuenta AWS que hace más fácil recordar la URL de inicio de sesión para usuarios IAM.

Crear alias:

1. En el dashboard de IAM, buscar .AWS Account.en el panel derecho
2. Verás .Account Aliasçon un enlace Çreate.o .Editçon un enlace Çreate.o .Edit"
3. Hacer clic en Çreate.o .Edit"
4. Ingresar un alias único (solo letras minúsculas, números y guiones)
5. Ejemplo: .aws-estudiante-2025.o "proyecto-redes-aws"
6. Hacer clic en "Save changes"
7. El alias debe ser único globalmente en AWS
8. Si el alias ya existe, intentar con otro nombre

URL de inicio de sesión: Después de crear el alias, tu URL personalizada será: `https://tu-alias.signin.aws.amazon.com/console`

Por ejemplo: `https://aws-estudiante-2025.signin.aws.amazon.com/console`

4.3.4. 3.4 Crear un Grupo de Administradores

¿Por qué crear grupos? Los grupos facilitan la gestión de permisos para múltiples usuarios. En lugar de asignar permisos individualmente, asignas permisos al grupo.

Crear grupo:

1. En el panel izquierdo del dashboard de IAM, hacer clic en Üser groups"
2. Hacer clic en el botón Çreate group"(Crear grupo)
3. En Üser group name", ingresar: `Administradores`
4. En la sección .Attach permissions policies", buscar políticas:
   - En el campo de búsqueda, escribir: .AdministratorAccess"
   - Marcar la casilla junto a .AdministratorAccess"
   - Esta política otorga acceso completo a todos los servicios de AWS
5. Hacer clic en Çreate group"(Crear grupo) en la parte inferior
6. El grupo .Administradores.ahora aparecerá en la lista

Descripción de la política AdministratorAccess:

- Proporciona acceso completo a todos los servicios y recursos de AWS
- Equivalente a permisos de cuenta root (excepto tareas específicas de root)
- Solo debe asignarse a usuarios que necesitan acceso administrativo completo

4.3.5. 3.5 Crear un Usuario IAM Administrador

¿Por qué crear un usuario IAM?

- La cuenta root solo debe usarse para tareas administrativas críticas
- Los usuarios IAM son más seguros para el trabajo diario
- Cada persona debe tener su propio usuario (no compartir credenciales)
- Permite auditoría y control de acceso granular

Crear usuario:

1. En el panel izquierdo de IAM, hacer clic en Üsers"(Usuarios)
2. Hacer clic en Çreate user"(Crear usuario)
3. En Üser name", ingresar un nombre descriptivo
   - Ejemplo: tu nombre (ej: "nicolas-admin.º "juan-admin")
   - O un nombre genérico: .admin-usuario"
   - Sin espacios, solo letras, números, guiones y guiones bajos
4. En "Provide user access to the AWS Management Console", marcar la casilla
5. Esto permite al usuario iniciar sesión en la consola web
6. Aparecerán más opciones:

Opciones de acceso a la consola:

1. Seleccionar Ï want to create an IAM user"(default)
2. En Çonsole password", elegir una opción:
   - **Autogenerated password:** AWS genera una contraseña aleatoria
   - **Custom password:** Tú defines la contraseña
3. Recomendación: Seleccionar Çustom passwordz crear una contraseña segura

4. Ejemplo de contraseña: `AdminAWS2025!Segura`
5. En Üsers must create a new password at next sign-in":
   - Marcar si quieres forzar cambio de contraseña en primer inicio
   - Para este laboratorio, puedes dejarla desmarcada
6. Hacer clic en "Next"(Siguiente)

Asignar permisos:

1. En la página "Set permissions", seleccionar .ªdd user to group"
2. Marcar la casilla junto al grupo .ªdministradores"que creaste anteriormente
3. El usuario heredará todos los permisos del grupo
4. Hacer clic en "Next"(Siguiente)

Revisar y crear:

1. Revisar la información del usuario:
   - Nombre de usuario
   - Acceso a la consola: Habilitado
   - Grupos: Administradores
   - Políticas: AdministratorAccess (heredada del grupo)
2. Si todo es correcto, hacer clic en Çreate user"(Crear usuario)
3. Verás una página de confirmación con las credenciales del usuario

Guardar credenciales de forma segura:

1. En la página de confirmación, verás:
   - Console sign-in URL (URL para iniciar sesión)
   - User name (nombre de usuario)
   - Console password (contraseña, si fue autogenerada)
2. Hacer clic en "Download .csv file"para descargar las credenciales
3. IMPORTANTE: Guardar este archivo en un lugar seguro
4. También puedes copiar y pegar la información en un documento
5. Hacer clic en Return to users listçuando hayas guardado todo

URL de inicio de sesión para usuarios IAM: La URL será algo como:

- Si creaste un alias: `https://tu-alias.signin.aws.amazon.com/console`
- Sin alias: `https://123456789012.signin.aws.amazon.com/console`

4.4 Paso 4: Habilitar Autenticación Multifactor (MFA)

Objetivo: Configurar MFA para la cuenta root y el usuario IAM para mejorar significativamente la seguridad.

4.4.1. 4.1 Instalar Aplicación MFA en tu Teléfono

Aplicaciones MFA recomendadas (todas gratuitas):

- **Google Authenticator:** Disponible para iOS y Android
- **Microsoft Authenticator:** Disponible para iOS y Android
- **Authy:** Disponible para iOS, Android y escritorio
- **LastPass Authenticator:** Si ya usas LastPass

Instalar la aplicación:

1. Abrir la tienda de aplicaciones en tu teléfono
   - iOS: App Store
   - Android: Google Play Store
2. Buscar "Google Authenticator"(o la aplicación que prefieras)
3. Descargar e instalar la aplicación
4. Abrir la aplicación después de instalarla
5. Si es la primera vez, puede pedir permisos de cámara (para escanear códigos QR)
6. Conceder los permisos necesarios
7. Mantener la aplicación abierta para el siguiente paso

4.4.2. 4.2 Habilitar MFA para la Cuenta Root

¿Por qué MFA en la cuenta root? La cuenta root tiene acceso ilimitado a todos los recursos. MFA agrega una capa crítica de protección en caso de que la contraseña sea comprometida.

Configurar MFA para root:

1. Asegurarte de estar iniciado sesión como usuario root (no usuario IAM)
2. Hacer clic en tu nombre de cuenta (esquina superior derecha)
3. Seleccionar "Security credentials"del menú desplegable
4. Serás llevado a la página de credenciales de seguridad
5. Desplazarse hasta la sección "Multi-factor authentication (MFA)"
6. Hacer clic en .ªssign MFA device"(Asignar dispositivo MFA)

Seleccionar tipo de dispositivo MFA:

1. En "Device name", ingresar un nombre descriptivo
   - Ejemplo: "MiTelefono-MFA.º "GoogleAuth-Root"
2. En "Select MFA device", elegir .ªuthenticator app"(Aplicación autenticadora)
3. Hacer clic en "Next"(Siguiente)

Escanear código QR:

1. AWS mostrará un código QR en la pantalla
2. En tu aplicación MFA del teléfono:

- Hacer clic en -.º .ªdd account"(Agregar cuenta)
- Seleccionar "Scan a QR code"(Escanear código QR)
- Apuntar la cámara al código QR en la pantalla del computador
- La aplicación automáticamente agregará la cuenta .ªWS.º .ªmazon Web Services"

3. La aplicación comenzará a generar códigos de 6 dígitos cada 30 segundos

Alternativa si no puedes escanear el QR:

1. En la pantalla de AWS, hacer clic en "Show secret key"(Mostrar clave secreta)
2. Copiar el código largo que aparece
3. En la aplicación MFA, seleccionar .Ena setup key"(Ingresar clave de configuración)
4. Pegar el código copiado
5. Ingresar un nombre para la cuenta (ej: .ªWS Root")
6. La aplicación comenzará a generar códigos

Verificar configuración:

1. En la pantalla de AWS, verás dos campos: "MFA code 1z "MFA code 2"
2. En tu aplicación MFA, verás un código de 6 dígitos junto a .ªWS"
3. Ingresar ese código en "MFA code 1"
4. ESPERAR a que el código cambie (aproximadamente 30 segundos)
5. Ingresar el NUEVO código en "MFA code 2"
6. Hacer clic en .ªdd MFA"(Agregar MFA)
7. Si todo es correcto, verás un mensaje de confirmación
8. El dispositivo MFA ahora aparecerá en tu lista de dispositivos

¿Qué pasa si el código es rechazado?

- Verificar que la hora del teléfono esté sincronizada correctamente
- Asegurarse de ingresar el código antes de que expire (30 segundos)
- No reutilizar el mismo código dos veces
- Si persiste el problema, eliminar la cuenta de la app y volver a escanear el QR

4.4.3. 4.3 Cerrar Sesión y Probar MFA

Probar el inicio de sesión con MFA:

1. Cerrar sesión de la consola de AWS:
   - Hacer clic en tu nombre (esquina superior derecha)
   - Seleccionar "Sign out"(Cerrar sesión)
2. Ir nuevamente a `https://console.aws.amazon.com`
3. Seleccionar Root user"
4. Ingresar tu correo electrónico
5. Hacer clic en "Next"

6. Ingresar tu contraseña
7. Hacer clic en "Sign in"
8. NUEVO: Aparecerá una pantalla pidiendo el código MFA
9. Abrir la aplicación MFA en tu teléfono
10. Ingresar el código de 6 dígitos que aparece junto a .ªWS"
11. Hacer clic en "Submit"(Enviar)
12. Serás dirigido a la consola de AWS

¡Felicidades! Ahora tu cuenta root está protegida con MFA. Incluso si alguien obtiene tu contraseña, no podrá acceder sin el código de tu teléfono.

4.5 Paso 5: Configurar Alertas de Facturación

Objetivo: Configurar alertas para ser notificado si el uso de AWS genera costos, previniendo cargos inesperados.

4.5.1. 5.1 Habilitar Alertas de Facturación

Acceder a la configuración de facturación:

1. Hacer clic en tu nombre de cuenta (esquina superior derecha)
2. Seleccionar "Billing and Cost Management"del menú desplegable
3. Si aparece un mensaje sobre permisos, ignorarlo (estás usando root)
4. Serás dirigido al dashboard de facturación

Habilitar preferencias de facturación:

1. En el panel izquierdo, hacer clic en "Billing preferences"
2. Desplazarse hasta .ªlert preferences"
3. Marcar las siguientes casillas:
   - Receive Free Tier Usage Alerts Te avisa si estás cerca de exceder Free Tier
   - Receive CloudWatch Billing Alerts Permite crear alarmas personalizadas
4. En .ºmail"bajo Free Tier alerts, ingresar tu correo electrónico
5. Verificar que sea el correo que revisas frecuentemente
6. Hacer clic en "Save preferences"(Guardar preferencias)

4.5.2. 5.2 Crear Alarma de Facturación en CloudWatch

Acceder a CloudWatch:

1. IMPORTANTE: Cambiar a la región ÜS East (N. Virginia) us-east-1
2. Las métricas de facturación solo están disponibles en esta región
3. En la barra superior derecha, verificar que dice "N. Virginia"
4. Si no, hacer clic y seleccionar ÜS East (N. Virginia)"

Navegar a CloudWatch:

1. En el menú "Services", buscar ÇloudWatch"
2. O usar la búsqueda rápida: escribir ÇloudWatch"
3. Hacer clic en ÇloudWatch"para abrir el servicio
4. Serás dirigido al dashboard de CloudWatch

Crear alarma de costos:

1. En el panel izquierdo, hacer clic en .Alarms"(Alarmas)
2. Hacer clic en Çreate alarm"(Crear alarma)
3. Hacer clic en "Select metric"(Seleccionar métrica)
4. En la lista de namespaces, hacer clic en "Billing"
5. Hacer clic en "Total Estimated Charge"(Cargo total estimado)
6. Verás una métrica con Çurrency: USD"
7. Marcar la casilla junto a esta métrica
8. Hacer clic en "Select metric"(parte inferior)

Configurar condiciones de la alarma:

1. En "Metric name", deberías ver .EstimatedCharges"
2. En "Statistic", dejar "Maximum"(Máximo)
3. En "Period", dejar "6 hours"(6 horas)
4. En Çonditions", seleccionar "Static"(Estático)
5. En "Whenever EstimatedCharges is...", seleccionar "Greater"(Mayor que)
6. En "than...", ingresar un valor umbral
   - Para estar muy seguro: `1` (te alertará con $1 USD)
   - Para un poco más de margen: `5` (te alertará con $5 USD)
   - Recomendación: usar `1` para máxima seguridad
7. Hacer clic en "Next"(Siguiente)

Configurar notificación:

1. En "Notification", dejar Ïn alarm"seleccionado
2. En "Select an SNS topic":
   - Seleccionar Çreate new topic"(Crear nuevo tema)
   - En Çreate a new topic", dejar el nombre sugerido o cambiarlo
   - Ejemplo: "Billing-Alarm-Topic"
3. En .Email endpoints that will receive the notification":
   - Ingresar tu correo electrónico
   - Puedes agregar múltiples correos separados por comas
4. Hacer clic en Çreate topic"(Crear tema)
5. Hacer clic en "Next"(Siguiente)

Nombrar la alarma:

1. En .Alarm name", ingresar un nombre descriptivo
2. Ejemplo: .Alerta-Costo-Mayor-1USD"
3. En .Alarm description"(opcional), agregar descripción
4. Ejemplo: "Me notifica si los costos de AWS superan $1 USD"
5. Hacer clic en "Next"(Siguiente)
6. Revisar toda la configuración
7. Hacer clic en Çreate alarm"(Crear alarma)

Confirmar suscripción por correo:

1. Revisar tu bandeja de entrada
2. Buscar un correo de .AWS Notifications"
3. Asunto: .AWS Notification - Subscription Confirmation"
4. Hacer clic en Çonfirm subscription.en el correo
5. Verás una página de confirmación
6. La alarma ahora está activa y funcional

Importante:

- Recibirás un correo si tu factura supera el umbral definido
- La métrica de facturación se actualiza cada 6 horas aproximadamente
- No es en tiempo real, puede haber un retraso
- Si recibes la alerta, revisa inmediatamente qué servicios están generando costos

4.6 Paso 6: Verificación de Configuración

Objetivo: Verificar que todas las configuraciones se realizaron correctamente.

4.6.1. 6.1 Verificar Configuración de IAM

Checklist de verificación:

1. Ir al dashboard de IAM (Services → IAM)
2. Verificar "Security Status"(debe estar en verde mayormente):
   - Delete your root access keys - Completado
   - Activate MFA on your root account - Completado
   - Create individual IAM users - Completado (al menos 1 usuario)
   - Use groups to assign permissions - Completado (grupo Administradores)
   - Apply an IAM password policy - Opcional (puedes configurarlo después)
3. En ÏAM Resources", deberías ver:
   - Users: 1 (tu usuario administrador)
   - User groups: 1 (Administradores)
   - Roles: números variables (algunos creados por defecto)
   - Policies: números altos (políticas de AWS + las tuyas)

4.6.2. 6.2 Verificar MFA

Para cuenta root:

1. Click en tu nombre (esquina superior derecha)
2. Seleccionar "Security credentials"
3. Desplazarse a "Multi-factor authentication (MFA)"
4. Deberías ver un dispositivo MFA listado con estado .ªctive"

4.6.3. 6.3 Verificar Alarmas de Facturación

Verificar alarma en CloudWatch:

1. Asegurarse de estar en región ÜS East (N. Virginia)"
2. Ir a CloudWatch (Services → CloudWatch)
3. Click en .ªlarms.en el panel izquierdo
4. Deberías ver tu alarma listada
5. Estado debería ser .ºK"(verde) si los costos son $0
6. Si está en Ïnsufficient data", esperar unas horas

Verificar costo actual:

1. Click en tu nombre (esquina superior derecha)
2. Seleccionar "Billing and Cost Management"
3. En el dashboard, verás "Month-to-date costs"
4. Debe decir "$0.00.º un valor muy pequeño
5. Si hay costos, investigar qué servicios los están generando

4.6.4. 6.4 Probar Inicio de Sesión con Usuario IAM

Cerrar sesión de root:

1. Click en tu nombre (esquina superior derecha)
2. Seleccionar "Sign out"

Iniciar sesión como usuario IAM:

1. Ir a la URL de inicio de sesión de IAM que guardaste anteriormente
2. Ejemplo: `https://tu-alias.signin.aws.amazon.com/console`
3. O: `https://123456789012.signin.aws.amazon.com/console`
4. En ÏAM user name", ingresar el nombre del usuario que creaste
5. Ingresar la contraseña del usuario IAM
6. Si configuraste MFA para el usuario, ingresar el código MFA
7. Hacer clic en "Sign in"
8. Deberías acceder a la consola de AWS normalmente

9. Verificar que puedes navegar por los servicios

Diferencia entre root e IAM user:

- En la esquina superior derecha, verás tu nombre de usuario IAM (no el correo)
- Ejemplo: "nicolas-admin @ tu-alias.º .ªdmin-usuario @ 123456789012"
- Esto confirma que estás usando el usuario IAM, no root

4.7 Paso 7: Limpieza y Consideraciones Finales

Objetivo: Asegurar que no quedan recursos que puedan generar costos.

4.7.1. 7.1 Verificación de Recursos

¿Qué limpiamos en este laboratorio? En este laboratorio solo configuramos servicios que son completamente gratuitos:

- IAM - Siempre gratuito
- CloudWatch (Alarmas básicas) - 10 alarmas gratis incluidas en Free Tier
- SNS (Notificaciones) - 1,000 notificaciones gratis al mes

NO hay nada que limpiar, pero es buena práctica verificar:

1. Ir a "Billing and Cost Management"
2. Verificar que "Month-to-date costs"sea $0.00
3. Si hay algún costo, revisar en "Bill details"qué lo generó

4.7.2. 7.2 Mejores Prácticas Aprendidas

Resumen de mejores prácticas de seguridad:

1. NO usar la cuenta root para tareas diarias
2. Crear usuarios IAM individuales para cada persona
3. Habilitar MFA en cuenta root (obligatorio)
4. Habilitar MFA en usuarios IAM (muy recomendado)
5. No crear access keys para root (a menos que sea absolutamente necesario)
6. Usar grupos para asignar permisos (no directamente a usuarios)
7. Aplicar principio de mínimo privilegio
8. Configurar alertas de facturación
9. Revisar costos regularmente
10. Eliminar recursos no utilizados

4.7.3. 7.3 Próximos Pasos Recomendados

Después de completar este laboratorio, puedes:

- Explorar otros servicios de AWS (EC2, S3, VPC) en laboratorios siguientes
- Configurar AWS CLI en tu computadora local
- Leer documentación oficial de AWS
- Tomar cursos gratuitos en AWS Skill Builder
- Practicar con tutoriales de AWS Hands-On

5 Cuestionario de Evaluación

Instrucciones: Selecciona la respuesta correcta para cada pregunta. Las respuestas están al final.

5.1 Preguntas de Selección Múltiple

1. **¿Cuál es la principal diferencia entre IaaS, PaaS y SaaS?**
   a) IaaS proporciona aplicaciones completas, PaaS infraestructura, y SaaS plataformas
   b) IaaS ofrece infraestructura virtualizada, PaaS plataforma de desarrollo, SaaS aplicaciones listas para usar
   c) IaaS es para empresas grandes, PaaS para medianas, SaaS para pequeñas
   d) Todos son lo mismo, solo cambia el nombre
2. **¿Qué modelo de despliegue de nube describe una infraestructura dedicada exclusivamente a una organización?**
   a) Nube pública
   b) Nube privada
   c) Nube híbrida
   d) Nube comunitaria
3. **¿Cuántas regiones tiene AWS aproximadamente a nivel mundial?**
   a) 10 regiones
   b) 20 regiones
   c) Más de 30 regiones
   d) 5 regiones
4. **¿Cuántas Zonas de Disponibilidad (AZs) mínimo tiene cada región de AWS?**
   a) 1 AZ
   b) 2 AZs
   c) 3 AZs o más
   d) 10 AZs
5. **¿Cuál de los siguientes servicios de AWS es SIEMPRE gratuito (no solo 12 meses)?**
   a) Amazon EC2 t2.micro con 750 horas al mes
   b) Amazon S3 con 5 GB de almacenamiento
   c) AWS IAM (Identity and Access Management)
   d) Amazon RDS con 750 horas de db.t2.micro
6. **¿Por cuánto tiempo están disponibles los beneficios del nivel gratuito de AWS Free Tier para servicios como EC2 y RDS?**
   a) 6 meses desde el registro

b) 12 meses desde el registro
c) 24 meses desde el registro
d) Son permanentemente gratuitos

7. **¿Qué es IAM en AWS?**
   a) Un servicio de almacenamiento de archivos
   b) Un servicio de gestión de identidades y accesos
   c) Un servicio de bases de datos
   d) Un servicio de máquinas virtuales
8. **¿Por qué NO se recomienda usar la cuenta root de AWS para tareas diarias?**
   a) Porque es más lenta que los usuarios IAM
   b) Porque tiene acceso ilimitado y comprometerla sería catastrófico
   c) Porque no puede acceder a todos los servicios
   d) Porque AWS cobra por usarla
9. **¿Qué significa MFA?**
   a) Multi-Factor Authentication (Autenticación de Múltiples Factores)
   b) Multiple File Access
   c) Managed Firewall Application
   d) Master Function Administrator
10. **¿Cuántos códigos de verificación consecutivos debes ingresar al configurar MFA en AWS?**
    a) 1 código
    b) 2 códigos consecutivos (esperando que cambie entre el primero y el segundo)
    c) 3 códigos
    d) No se requieren códigos
11. **¿Qué tipo de MFA es más común y económico para proteger cuentas de AWS?**
    a) Hardware MFA (llave física)
    b) SMS al teléfono
    c) Aplicación de autenticación virtual (Google Authenticator, Microsoft Authenticator, etc.)
    d) Llamada telefónica automatizada
12. **¿En qué región deben configurarse las alarmas de facturación de CloudWatch?**
    a) En cualquier región que elijas
    b) En la región más cercana a tu ubicación
    c) Solo en US East (N. Virginia) us-east-1
    d) En todas las regiones simultáneamente

13. **Si configuras una alarma de facturación con umbral de $1 USD, ¿cuándo recibirás la notificación?**
    a) Inmediatamente cuando gastes exactamente $1.00
    b) Cuando el cargo estimado supere $1.00
    c) Antes de que llegues a $1.00 (predicción)
    d) Solo al final del mes si superaste $1.00
14. **¿Qué política de AWS otorga acceso administrativo completo a todos los servicios?**
    a) PowerUserAccess
    b) ReadOnlyAccess
    c) AdministratorAccess
    d) FullAccess
15. **¿Cuál es la mejor práctica para asignar permisos a usuarios IAM?**
    a) Adjuntar políticas directamente a cada usuario individual
    b) Crear grupos con políticas y agregar usuarios a esos grupos
    c) Dar acceso root a todos los usuarios
    d) No usar políticas, solo roles

5.2 Respuestas del Cuestionario

1. **Respuesta correcta: b)** IaaS ofrece infraestructura virtualizada (servidores, almacenamiento, redes), PaaS ofrece plataformas de desarrollo (donde despliegas aplicaciones sin gestionar infraestructura), y SaaS ofrece aplicaciones completas listas para usar (como Gmail, Office 365).
2. **Respuesta correcta: b)** Una nube privada es una infraestructura de nube dedicada exclusivamente a una organización, proporcionando mayor control y seguridad. La nube pública es compartida entre múltiples clientes, la híbrida combina ambas, y la comunitaria es compartida por varias organizaciones con intereses comunes.
3. **Respuesta correcta: c)** AWS tiene más de 30 regiones distribuidas globalmente (el número exacto aumenta constantemente). Cada región es un área geográfica separada que contiene múltiples Zonas de Disponibilidad.
4. **Respuesta correcta: c)** Cada región de AWS tiene al menos 3 Zonas de Disponibilidad, aunque algunas regiones tienen más. Esto garantiza alta disponibilidad y tolerancia a fallos.
5. **Respuesta correcta: c)** AWS IAM es siempre gratuito, sin límite de tiempo. Los demás servicios mencionados son gratuitos solo durante 12 meses como parte del Free Tier, después comienzan a generar cargos.
6. **Respuesta correcta: b)** Los servicios del nivel gratuito como EC2 t2.micro (750 horas/mes) y RDS db.t2.micro están disponibles durante 12 meses desde la fecha de registro de la cuenta AWS.

7. **Respuesta correcta: b)** IAM (Identity and Access Management) es el servicio de AWS para gestionar identidades (usuarios, grupos, roles) y controlar el acceso a recursos de AWS mediante políticas de permisos.
8. **Respuesta correcta: b)** La cuenta root tiene acceso completo e ilimitado a todos los recursos y servicios de AWS. Si esta cuenta es comprometida, un atacante tendría control total. Por eso se recomienda usarla solo para tareas administrativas críticas y usar usuarios IAM para operaciones diarias.
9. **Respuesta correcta: a)** MFA significa Multi-Factor Authentication (Autenticación de Múltiples Factores). Es un método de seguridad que requiere dos o más factores de verificación: algo que sabes (contraseña) y algo que tienes (código de teléfono).
10. **Respuesta correcta: b)** AWS requiere que ingreses 2 códigos consecutivos al configurar MFA. Debes esperar a que el primer código cambie (aproximadamente 30 segundos) y luego ingresar el nuevo código. Esto verifica que el dispositivo MFA esté correctamente sincronizado.
11. **Respuesta correcta: c)** Las aplicaciones de autenticación virtual como Google Authenticator, Microsoft Authenticator, o Authy son la opción más común y económica. Son gratuitas, funcionan sin conexión a internet, y son más seguras que SMS.
12. **Respuesta correcta: c)** Las métricas de facturación de AWS solo están disponibles en la región US East (N. Virginia) us-east-1. Debes cambiar a esta región antes de crear alarmas de facturación en CloudWatch.
13. **Respuesta correcta: b)** Recibirás una notificación cuando el cargo estimado total supere el umbral configurado ($1.00 en este caso). La métrica se actualiza cada 6 horas aproximadamente, por lo que puede haber un pequeño retraso.
14. **Respuesta correcta: c)** AdministratorAccess es la política administrada de AWS que otorga acceso completo a todos los servicios y recursos. PowerUserAccess da acceso amplio pero sin permisos de gestión de usuarios/grupos IAM.
15. **Respuesta correcta: b)** La mejor práctica es crear grupos de IAM con las políticas necesarias y luego agregar usuarios a esos grupos. Esto facilita la gestión de permisos a escala y sigue el principio de privilegio mínimo.

6 Conclusiones

Al finalizar este laboratorio, has dado los primeros pasos fundamentales en el ecosistema de Amazon Web Services, estableciendo una base sólida de seguridad y gestión que te acompañará en todos tus proyectos futuros en la nube. Las competencias adquiridas no solo son aplicables a AWS, sino que representan mejores prácticas universales en computación en nube.

6.1 Logros Principales

1. Comprensión de Fundamentos de Cloud Computing

Has desarrollado una comprensión conceptual de los modelos de servicio en la nube (IaaS, PaaS, SaaS) y los modelos de despliegue (público, privado, híbrido). Comprendes cómo AWS se posiciona como proveedor líder de infraestructura en la nube y conoces su arquitectura global basada en regiones y zonas de disponibilidad.

2. Creación y Configuración de Cuenta AWS

Has creado exitosamente una cuenta de AWS, completando el proceso de registro que incluye verificación de correo electrónico, configuración de información de pago (sin cargos en Free Tier), y verificación de identidad por teléfono. Conoces las diferentes opciones de soporte y has seleccionado el plan Basic gratuito adecuado para aprendizaje.

3. Implementación de Seguridad con IAM

Has aplicado el principio de mínimo privilegio creando usuarios IAM separados en lugar de usar la cuenta root para tareas diarias. Comprendes la estructura de IAM (usuarios, grupos, roles, políticas) y has configurado un grupo de administradores con permisos completos, demostrando que entiendes cómo delegar acceso de manera controlada.

4. Protección con Autenticación Multifactor (MFA)

Has implementado una capa adicional de seguridad configurando MFA tanto en la cuenta root como en tu usuario IAM administrador. Esta habilidad es crítica en entornos de producción y demuestra tu comprensión de que la seguridad en capas es esencial para proteger recursos en la nube.

5. Gestión Financiera y Control de Costos

Has configurado alertas de facturación en CloudWatch, estableciendo un sistema de monitoreo proactivo que te notificará si se generan costos inesperados. Esta competencia es fundamental para cualquier profesional de nube, ya que la gestión de costos es una responsabilidad crítica en proyectos reales.

6.2 Habilidades Técnicas Desarrolladas

- Navegación eficiente en la Consola de Administración de AWS
- Gestión de identidades y accesos (IAM)
- Configuración de autenticación multifactor (MFA)
- Creación de grupos y asignación de políticas
- Configuración de servicios de monitoreo (CloudWatch)
- Configuración de notificaciones (SNS)

- Gestión de facturación y costos
- Aplicación de mejores prácticas de seguridad

6.3 Competencias Profesionales

Más allá de las habilidades técnicas, has desarrollado competencias profesionales valiosas:

- **Pensamiento en seguridad:** Comprendes que la seguridad no es un agregado posterior, sino una consideración desde el primer momento
- **Responsabilidad financiera:** Entiendes que en la nube, cada recurso tiene un costo y debe ser monitoreado
- **Mejores prácticas:** Has aprendido que seguir estándares de la industria (como no usar root, habilitar MFA) es fundamental
- **Documentación y verificación:** Has practicado el seguimiento de pasos documentados y la verificación sistemática de configuraciones

6.4 Preparación para Siguientes Laboratorios

Este laboratorio es la piedra angular sobre la que construirás conocimientos más avanzados:

- **Laboratorio 2 - VPC:** Crearás redes virtuales privadas, aplicando los conceptos de IAM para controlar quién puede gestionar recursos de red
- **Laboratorio 3 - Internet Gateway:** Conectarás redes privadas a internet, entendiendo flujos de tráfico
- **Laboratorio 4 - EC2 y Security Groups:** Lanzarás máquinas virtuales protegidas con reglas de firewall
- **Laboratorios 5-8:** Integrarás seguridad avanzada, monitoreo, y arquitecturas completas

En cada laboratorio futuro, las credenciales IAM que configuraste hoy te permitirán trabajar de manera segura, y las alarmas de facturación te protegerán de costos inesperados.

6.5 Reflexión Final

La computación en nube ha transformado la manera en que se diseñan, despliegan y operan sistemas de información. AWS, como líder en este espacio, ofrece un ecosistema completo de servicios que potencian la innovación. Sin embargo, con gran poder viene gran responsabilidad: la seguridad y el control de costos deben ser prioridades constantes.

Has demostrado que comprendes estos principios fundamentales. La configuración que realizaste hoy - cuenta protegida con MFA, usuario IAM con permisos adecuados, alertas de facturación activas - es el sello distintivo de un profesional responsable que entiende que la excelencia técnica debe ir acompañada de rigurosidad en seguridad y gestión.

Continúa aplicando estos principios en todos tus proyectos en AWS, y estarás preparado para diseñar e implementar soluciones en la nube que sean no solo funcionales, sino también seguras, eficientes y sostenibles económicamente.

¡Felicidades por completar exitosamente este primer laboratorio!

7 Referencias

7.1 Documentación Oficial de AWS

1. **AWS General**
   - AWS Documentation - Página principal de documentación
     https://docs.aws.amazon.com/
   - AWS Getting Started Resource Center
     https://aws.amazon.com/getting-started/
   - AWS Global Infrastructure - Regiones y Zonas de Disponibilidad
     https://aws.amazon.com/about-aws/global-infrastructure/
2. **AWS Free Tier**
   - AWS Free Tier - Información completa sobre servicios gratuitos
     https://aws.amazon.com/free/
   - AWS Free Tier FAQs
     https://aws.amazon.com/free/free-tier-faqs/
3. **AWS Identity and Access Management (IAM)**
   - AWS IAM Documentation
     https://docs.aws.amazon.com/IAM/latest/UserGuide/
   - IAM Best Practices
     https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html
   - IAM Users Guide
     https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users.html
   - IAM Groups Guide
     https://docs.aws.amazon.com/IAM/latest/UserGuide/id_groups.html
   - IAM Policies and Permissions
     https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html
4. **Multi-Factor Authentication (MFA)**
   - Using Multi-Factor Authentication (MFA) in AWS
     https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa.html
   - Enable a Virtual MFA Device for Your AWS Account Root User
     https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_enable_virtual.html
   - Enable a Virtual MFA Device for an IAM User
     https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_enable_virtual.html
5. **AWS Billing and Cost Management**
   - AWS Billing and Cost Management Documentation
     https://docs.aws.amazon.com/account-billing/
   - Creating a Billing Alarm to Monitor Your Estimated AWS Charges
     https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/monitor_estimated_charges_with_cloudwatch.html

- Avoiding Unexpected Charges
  https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/checklistforunwanted
  html

6. **Amazon CloudWatch**
   - Amazon CloudWatch Documentation
     https://docs.aws.amazon.com/cloudwatch/
   - Using Amazon CloudWatch Alarms
     https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/AlarmThatSendsEmai
     html
7. **Amazon SNS (Simple Notification Service)**
   - Amazon SNS Documentation
     https://docs.aws.amazon.com/sns/
   - Getting Started with Amazon SNS
     https://docs.aws.amazon.com/sns/latest/dg/sns-getting-started.html

7.2 Recursos de Aprendizaje AWS

1. **AWS Training and Certification**
   - AWS Skill Builder - Cursos gratuitos y de pago
     https://skillbuilder.aws/
   - AWS Cloud Practitioner Essentials (curso gratuito)
     https://aws.amazon.com/training/digital/aws-cloud-practitioner-essentials/
2. **AWS Whitepapers y Guías**
   - AWS Well-Architected Framework
     https://aws.amazon.com/architecture/well-architected/
   - Security Pillar - AWS Well-Architected Framework
     https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/welcome.
     html
   - Overview of Amazon Web Services (Whitepaper)
     https://docs.aws.amazon.com/whitepapers/latest/aws-overview/introduction.
     html

7.3 Libros y Publicaciones Académicas

1. Velte, A. T., Velte, T. J., & Elsenpeter, R. (2010). *Cloud Computing: A Practical Approach*. McGraw-Hill.
   Proporciona una introducción práctica a los conceptos fundamentales de computación en nube.
2. Erl, T., Mahmood, Z., & Puttini, R. (2013). *Cloud Computing: Concepts, Technology & Architecture*. Prentice Hall.
   Explica en detalle los modelos de servicio (IaaS, PaaS, SaaS) y patrones de arquitectura en la nube.

3. Wittig, A., & Wittig, M. (2018). *Amazon Web Services in Action* (2nd ed.). Manning Publications.
   Guía práctica completa de AWS con ejemplos paso a paso.
4. NIST Special Publication 800-145. (2011). *The NIST Definition of Cloud Computing*. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
   Definición estándar de computación en nube del National Institute of Standards and Technology.

7.4 Aplicaciones de Autenticación MFA

1. **Google Authenticator**
   - iOS: https://apps.apple.com/app/google-authenticator/id388497605
   - Android: https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2
2. **Microsoft Authenticator**
   - iOS: https://apps.apple.com/app/microsoft-authenticator/id983156458
   - Android: https://play.google.com/store/apps/details?id=com.azure.authenticator
3. **Authy**
   - Multiplataforma: https://authy.com/download/

7.5 Herramientas y Recursos Adicionales

1. **AWS CLI (Command Line Interface)**
   - Documentación: https://docs.aws.amazon.com/cli/
   - Instalación: https://aws.amazon.com/cli/
2. **AWS SDKs** (Software Development Kits)
   - Página principal de SDKs: https://aws.amazon.com/tools/
3. **AWS Architecture Center**
   - Diagramas de referencia y mejores prácticas: https://aws.amazon.com/architecture/

Nota: Todas las URLs fueron verificadas y están activas al momento de la creación de este documento. AWS actualiza constantemente su documentación, por lo que se recomienda buscar en https://docs.aws.amazon.com/ si algún enlace cambia en el futuro.