Introducción a Amazon AWS y su ecosistema

Contenido

[Configuración Inicial de AWS y CLI 3](#_Toc198387886)

[Paso 1: Crear una cuenta en AWS 3](#_Toc198387887)

[Paso 2: Crear un Usuario IAM con Acceso Administrativo 3](#_Toc198387888)

[Paso 3: Instalar y Configurar AWS CLI 3](#_Toc198387889)

[Paso 4: Validar conexión con AWS CLI 3](#_Toc198387890)

[Gestión de IAM y Política Personalizada 4](#_Toc198387891)

[Paso 1: Crear un Grupo IAM 4](#_Toc198387892)

[Paso 2: Crear una Política Personalizada 4](#_Toc198387893)

[Paso 3: Crear un Usuario con la Política 4](#_Toc198387894)

[Paso 4: Validar con AWS CLI 5](#_Toc198387895)

[VPC y EC2: Redes Personalizadas y Máquinas Virtuales 5](#_Toc198387896)

[Paso 1: Crear una VPC 5](#_Toc198387897)

[Paso 2: Crear un Grupo de Seguridad (Firewall) 5](#_Toc198387898)

[Paso 3: Crear una Instancia EC2 5](#_Toc198387899)

[Paso 4: Conectarte vía SSH desde Ubuntu (WSL) 6](#_Toc198387900)

[S3: Almacenamiento de Objetos en la Nube 6](#_Toc198387901)

[Paso 1: Crear un Bucket S3 6](#_Toc198387902)

[Paso 2: Subir un Archivo desde la Consola Web 6](#_Toc198387903)

[Paso 3: Instalar AWS CLI en Ubuntu (WSL) 6](#_Toc198387904)

[Paso 4: Subir y Descargar Archivos con CLI 6](#_Toc198387905)

[Paso 5: Opcional - Hacer Público un Archivo 7](#_Toc198387906)

[Despliegue de Kubernetes con Elastic Kubernetes Service (EKS) 7](#_Toc198387907)

[Paso 1: Crear un Rol IAM para EKS 7](#_Toc198387908)

[Paso 2: Crear un Clúster EKS 7](#_Toc198387909)

[Paso 3: Configurar kubectl y AWS CLI 7](#_Toc198387910)

[Paso 4: Crear un Grupo de Nodos Gestionados 8](#_Toc198387911)

[Paso 5: Desplegar una Aplicación de Prueba 8](#_Toc198387912)

# Configuración Inicial de AWS y CLI

Este módulo te guiará en la configuración inicial de tu entorno de AWS para comenzar a trabajar con servicios como IAM, EC2, S3, VPC y EKS. Está diseñado para ejecutarse desde Windows 11 utilizando CMD, PowerShell o Ubuntu (WSL). Todo dentro del Free Tier de AWS.

## Paso 1: Crear una cuenta en AWS

1. Accede a https://aws.amazon.com y selecciona 'Crear una cuenta gratuita'.  
2. Completa el formulario con tu correo electrónico, contraseña y nombre de la cuenta.  
3. Proporciona los datos de tu tarjeta de crédito/débito (no se cobrará si usas el Free Tier).  
4. Verifica tu identidad mediante SMS o llamada telefónica.  
5. Selecciona el plan Básico (Free).  
6. Accede al portal de administración en https://console.aws.amazon.com

## Paso 2: Crear un Usuario IAM con Acceso Administrativo

1. Desde la consola, busca 'IAM' y entra al servicio.  
2. Ve a 'Usuarios' > 'Agregar usuario'.  
3. Nombre de usuario: admin-user  
4. Selecciona 'Acceso mediante consola de administración de AWS' y crea una contraseña.  
5. Asigna permisos: elige 'Adjuntar políticas existentes directamente' y selecciona 'AdministratorAccess'.  
6. Finaliza la creación del usuario.

## Paso 3: Instalar y Configurar AWS CLI

1. Descargar AWS CLI para Windows desde: https://aws.amazon.com/cli/  
2. Instalar y luego verificar con:  
 CMD o PowerShell:  
 aws --version  
  
3. Configurar las credenciales con el siguiente comando (usa las credenciales del usuario IAM creado):  
 aws configure  
 - AWS Access Key ID: [tu clave]  
 - AWS Secret Access Key: [tu secreto]  
 - Región por defecto: us-east-1  
 - Formato de salida: json

## Paso 4: Validar conexión con AWS CLI

Ejecuta el siguiente comando para validar que estás conectado correctamente:  
 aws sts get-caller-identity

Debe devolver tu ID de cuenta, usuario y ARN.

aws s3 ls  
devuelve la lista de bucket de mi cuenta

# Gestión de IAM y Política Personalizada

En este módulo aprenderás a crear roles, grupos y políticas personalizadas en IAM (Identity and Access Management). También configurarás permisos mínimos para un usuario con acceso limitado a S3.

## Paso 1: Crear un Grupo IAM

1. Accede a IAM desde la consola.  
2. Ve a 'Grupos de usuarios' > 'Crear grupo'.  
3. Nombre del grupo: s3-readonly-group  
4. Adjunta la política 'AmazonS3ReadOnlyAccess'.  
5. Crea el grupo.

## Paso 2: Crear una Política Personalizada

1. En IAM, ve a 'Políticas' > 'Crear política'.  
2. Selecciona 'Editor JSON' y pega el siguiente contenido:

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

3. Haz clic en 'Siguiente', agrega un nombre como 'S3BucketReadOnlyPolicy', luego crea la política.

## Paso 3: Crear un Usuario con la Política

1. Ve a 'Usuarios' > 'Agregar usuario'.  
2. Nombre del usuario: s3-user  
3. Habilita acceso por consola o acceso programático (según necesidad).  
4. Asigna el usuario al grupo 's3-readonly-group' y adjunta la política personalizada adicionalmente.  
5. Crea el usuario y guarda sus credenciales.

## Paso 4: Validar con AWS CLI

1. Ejecuta el comando `aws s3 ls s3://tu-bucket-ejemplo --profile s3-user` (si configuraste múltiples perfiles).  
2. Si todo está correcto, verás la lista de objetos. Si no, revisa permisos y políticas.

# VPC y EC2: Redes Personalizadas y Máquinas Virtuales

Este módulo te guía en la creación de una red personalizada (VPC) y una instancia EC2 básica dentro del Free Tier. Aprenderás a configurar subredes, tablas de rutas, un grupo de seguridad y una instancia EC2 con acceso SSH.

## Paso 1: Crear una VPC

1. Desde la consola de AWS, busca y selecciona el servicio 'VPC'.  
2. Haz clic en 'Crear VPC'.  
3. Selecciona 'VPC solo con subred pública'.  
4. Asigna un nombre: VPC-Ejemplo  
5. Rango CIDR: 10.0.0.0/16  
6. Zona de disponibilidad: us-east-1a (o la que prefieras)  
7. Subred pública: 10.0.1.0/24  
8. Habilita la asignación automática de IP pública.  
9. Finaliza la creación.

## Paso 2: Crear un Grupo de Seguridad (Firewall)

1. En el servicio 'EC2', selecciona 'Grupos de seguridad' y haz clic en 'Crear'.  
2. Nombre: sg-acceso-ssh  
3. Descripción: Permite acceso SSH desde tu IP  
4. En 'Reglas de entrada', añade:  
 - Tipo: SSH  
 - Puerto: 22  
 - Origen: Tu dirección IP (usa opción 'Mi IP')  
5. Crea el grupo.

## Paso 3: Crear una Instancia EC2

1. Desde EC2, selecciona 'Instancias' > 'Lanzar instancia'.  
2. Nombre: EC2-Ejemplo  
3. AMI: Amazon Linux 2023 (Free Tier elegible)  
4. Tipo: t2.micro  
5. Par de claves: crea una nueva o usa una existente (descarga el archivo .pem)  
6. Red: VPC-Ejemplo  
7. Subred: 10.0.1.0/24  
8. Habilita IP pública autoasignada  
9. Grupo de seguridad: selecciona 'sg-acceso-ssh'  
10. Lanza la instancia.

## Paso 4: Conectarte vía SSH desde Ubuntu (WSL)

1. Abre Ubuntu (WSL) en Windows 11  
2. Da permisos a tu archivo .pem:  
 chmod 400 clave.pem  
3. Conéctate a la instancia (usa la IP pública):  
 ssh -i clave.pem ec2-user@IP\_PUBLICA  
4. Una vez conectado, puedes usar comandos como `uptime`, `top`, `free -m`, etc.

# S3: Almacenamiento de Objetos en la Nube

En este módulo aprenderás a crear un bucket en Amazon S3, subir y descargar archivos, configurar permisos básicos y usar la CLI para interactuar con el servicio.

## Paso 1: Crear un Bucket S3

1. Ve a la consola de AWS y busca 'S3'.  
2. Haz clic en 'Crear bucket'.  
3. Nombre: bucket-ejemplo-[tu-nombre-unico]  
4. Región: us-east-1  
5. Desactiva el bloqueo de acceso público solo si vas a hacer pruebas públicas (se recomienda dejarlo activado para este ejercicio).  
6. Deja las opciones por defecto y haz clic en 'Crear bucket'.

## Paso 2: Subir un Archivo desde la Consola Web

1. Entra al bucket creado.  
2. Haz clic en 'Cargar'.  
3. Selecciona un archivo desde tu PC (por ejemplo, un .txt o una imagen).  
4. Haz clic en 'Cargar' para subirlo.

## Paso 3: Instalar AWS CLI en Ubuntu (WSL)

1. Ejecuta los siguientes comandos:  
 sudo apt update  
 sudo apt install awscli -y  
2. Verifica con:  
 aws --version  
3. Configura si no lo has hecho:  
 aws configure

## Paso 4: Subir y Descargar Archivos con CLI

1. Subir un archivo:  
 aws s3 cp archivo.txt s3://bucket-ejemplo-[tu-nombre-unico]/archivo.txt  
  
2. Listar archivos:  
 aws s3 ls s3://bucket-ejemplo-[tu-nombre-unico]/  
  
3. Descargar archivo:  
 aws s3 cp s3://bucket-ejemplo-[tu-nombre-unico]/archivo.txt archivo-descargado.txt

## Paso 5: Opcional - Hacer Público un Archivo

1. En la consola S3, entra al bucket y selecciona el archivo.  
2. Ve a 'Permisos' > 'Editar' > 'Hacer público'.  
3. También puedes usar este comando:  
 aws s3api put-object-acl --bucket bucket-ejemplo-[tu-nombre-unico] --key archivo.txt --acl public-read  
  
4. Accede al archivo desde:  
 https://bucket-ejemplo-[tu-nombre-unico].s3.amazonaws.com/archivo.txt

# Despliegue de Kubernetes con Elastic Kubernetes Service (EKS)

En este módulo aprenderás a desplegar un clúster de Kubernetes utilizando Amazon EKS (Elastic Kubernetes Service). El enfoque será usar recursos elegibles dentro del Free Tier, utilizando t3.micro y configuraciones básicas desde consola y CLI.

## Paso 1: Crear un Rol IAM para EKS

1. Accede al servicio IAM desde la consola.  
2. Ve a 'Roles' > 'Crear rol'.  
3. Tipo de entidad confiable: AWS Service > EKS.  
4. Adjunta la política: AmazonEKSClusterPolicy.  
5. Nombre del rol: eksClusterRole.  
6. Crea el rol.

## Paso 2: Crear un Clúster EKS

1. Ve a EKS en la consola y selecciona 'Add Cluster > Create'.  
2. Nombre del clúster: eks-demo  
3. Rol IAM: selecciona eksClusterRole creado previamente.  
4. Red: usa una VPC existente o crea una nueva (con subredes públicas y privadas).  
5. Versión de Kubernetes: usa la más reciente disponible.  
6. Avanza con la configuración por defecto y crea el clúster.

## Paso 3: Configurar kubectl y AWS CLI

1. Instala kubectl: https://docs.aws.amazon.com/eks/latest/userguide/install-kubectl.html  
2. Configura las credenciales:  
 aws eks update-kubeconfig --region us-east-1 --name eks-demo  
3. Verifica el acceso:  
 kubectl get svc

## Paso 4: Crear un Grupo de Nodos Gestionados

1. Ve al clúster EKS > Compute > Add Node Group.  
2. Nombre: nodegroup-demo  
3. Rol IAM del nodo: crear uno con políticas AmazonEKSWorkerNodePolicy, AmazonEC2ContainerRegistryReadOnly y AmazonEKS\_CNI\_Policy.  
4. Tipo de instancia: t3.micro (Free Tier)  
5. Número de nodos: 1  
6. Crea el grupo y espera que los nodos estén en estado activo.

## Paso 5: Desplegar una Aplicación de Prueba

1. Despliega NGINX con los siguientes comandos:  
 kubectl create deployment nginx --image=nginx  
 kubectl expose deployment nginx --port=80 --type=LoadBalancer  
  
2. Obtén la IP pública:  
 kubectl get service  
  
3. Accede a la app desde el navegador usando la IP del LoadBalancer.