TEMARIO: ARQUITECTURA EN LA NUBE - ADMINISTRACIÓN REMOTA DE SERVIDORES WEB EN AWS A TRAVÉS DE SSH

CONCEPTOS BÁSICOS PARA LA CLASE

¿Qué es AWS?

AWS (*Amazon Web Services*) es como el alquiler de ordenadores en Internet. En lugar de comprar un ordenador físico que tengas en tu habitación, AWS te permite tener un ordenador virtual en los servidores de Amazon, en el que tú tienes control total.

Comparación real

- Comprar un ordenador = Comprar un servidor físico en tu oficina
- Alquilar en AWS = Alquilar un apartamento. Tú no eres dueño del edificio, pero puedes usarlo como si fuera tuyo. Pagas mensualmente y cuando no lo necesites, dejas de pagar.

Con AWS, creas una instancia **EC2,** que es básicamente un **ordenador Linux** o **Windows virtual en la nube** donde puedes instalar lo que quieras, configurarlo como prefieras, y usarlo como si fuera un ordenador real.

¿Qué es SSH?

SSH (*Secure Shell*) es como un teléfono seguro que te permite hablar con tu ordenador remoto.

Comparación real:

- Llamada telefónica normal = SSH sin cifrado (*alguien podría escuchar*)
- Llamada por WhatsApp = SSH (*nadie puede escuchar excepto tú y la otra persona*)

Con SSH, te conectas desde tu máquina (*WSL en Windows*) al ordenador en la nube (*AWS*) y puedes escribir comandos exactamente como si estuvieras sentado frente a ese ordenador. Todo lo que escribes viaja cifrado, así que es seguro.

Cómo funciona:

- **Tu máquina (*WSL*):** Escribes aquí, el ordenador en la nube responde
- **SSH cifrado**
- **Servidor AWS (*EC2*):** Se ejecuta aquí, ves el resultado aquí

¿Qué son los archivos PEM?

Un **archivo .pem** es como una llave de casa muy especial. Es un archivo de texto que contiene una clave privada.

Comparación real:

Imagina que tienes una casa y has hecho dos llaves idénticas:

- **Clave privada (.pem):** La llave que guardas en tu bolsillo (*en tu máquina*). NUNCA debes perderla ni dársela a nadie.
- **Clave pública:** Una copia de la llave que le das a Amazon. Amazon guarda esta "*copia*" en el servidor.

Cuando quieres entrar en la casa (*conectarte al servidor*):

1. Tú tienes tu llave privada (*.pem*)
2. El servidor tiene la clave pública
3. Encajas una con la otra y... ¡acceso permitido!

Si alguien roba tu archivo .pem, puede acceder a tu servidor. Por eso es tan importante guardarlo en un lugar seguro y con permisos limitados.

¿Cómo funciona todo junto?

Cuando haces una conexión SSH desde WSL a AWS:

1. Descargas el archivo .pem (*tu llave privada*) desde AWS
2. Lo guardas en ~/.ssh/labsuser.pem en tu máquina
3. Escribes: ssh -i ~/.ssh/labsuser.pem ubuntu@54.123.45.67
4. Tu máquina dice: "*Tengo la llave privada*"
5. AWS dice: "*Verifiquemos que tienes la clave privada correcta*"
6. Se verifica criptográficamente que tu clave coincida
7. ¡Conexión establecida! Ahora puedes escribir comandos

Es como meterse en un edificio:

- AWS = Edificio con seguridad
- Tu archivo .pem = Tu carnet de identificación
- Comandos SSH = Lo que haces adentro (*encender luces, usar la cocina, etc.*)

Security Groups: El Guardaespaldas del Servidor

Los **Security Groups** son como un guardaespaldas que controla quién puede hablar con tu servidor y por dónde.

Comparación real:

Imagina que tu servidor es una discoteca:

- **Puerto 22 (*SSH*) =** La puerta trasera por donde entran los administradores
- **Puerto 8080 (*Apache*) =** Una ventana por donde sale música
- **Puerto 8081 (*Nginx*) =** Otra ventana por donde sale música
- **Puerto 8082 (*Caddy*) =** Otra ventana más
- **Puerto 8443 (*HTTPS*) =** Una ventana especial con cristal de seguridad

El Security Group decide:

- "*Puedo dejar entrar por la puerta trasera (SSH) a cualquiera*"
- "*La música sale por las ventanas 8080, 8081, 8082 y 8443*"
- "*Nadie puede entrar por otros lados*"

Sin un Security Group correcto, tu servidor estaría cerrado (*abierto a nadie*) y nadie podría conectarse.

Lo que vas a hacer

1. Descargarás el archivo .pem desde AWS (*tu llave privada*)
2. Lo guardarás en WSL con permisos seguros
3. Configurarás el Security Group (*el guardaespaldas*)
4. Crearás una instancia EC2 (*tu ordenador virtual*)
5. Te conectarás por SSH (*con la llave privada*)

6. Ejecutarás todos los comandos de la Segunda Práctica de forma remota
7. Accederás desde tu navegador local a los servicios web en los puertos 8080, 8081, 8082 y 8443

COMANDOS Y PROCEDIMIENTOS

PARTE 0: PREPARACIÓN DEL ENTORNO LOCAL (*WSL/VM*)

1. Verificar WSL2

```
wsl --version
```

Descripción: Verifica que WSL2 esté instalado y funcionando correctamente.

---

2. Crear directorio para las claves SSH

```
mkdir -p ~/.ssh
```

```
chmod 700 ~/.ssh
```

Descripción: Crea el directorio .ssh con permisos correctos para almacenar claves.

PARTE 1: CONFIGURACIÓN EN AWS (*Interfaz Visual*)

1. Descargar la clave PEM desde la página del laboratorio

1. Localiza el botón o enlace **"Download key"** o **"Download .pem"**
2. Se descargará un archivo con extensión .pem (*por ejemplo: labsuser.pem*)
3. **Importante:** Guarda este archivo en una ubicación segura, preferiblemente en WSL

Pasos para mover la clave a WSL:

Si descargaste el archivo en Windows:

```
cp /mnt/c/Users/TU-USUARIO/Downloads/labsuser.pem ~/.ssh/
```

O si prefieres descargarlo directamente en WSL:

```
cp ~/Downloads/labsuser.pem ~/.ssh/
```

---

2. Configurar permisos de la clave PEM

chmod 400 ~/.ssh/labsuser.pem

Verifica los permisos:

ls -la ~/.ssh/labsuser.pem

 # Deberías ver: -r--------

---

3. Crear instancia EC2

1. **Nombre:** servidor-web-practica
2. **AMI:** Ubuntu 22.04 LTS o Ubuntu 24.04 LTS
3. **Tipo:** t2/3.micro (*Free Tier*)
4. **Red:** VPC y Subred por defecto
5. **IP pública:** Habilitada
6. **Almacenamiento:** 8 GiB, tipo gp2
7. **Etiquetas (*opcional*):** Curso → ArquitecturaNube
8. **Grupo de Seguridad:** sg-servidores-web

---

4. Configurar Security Group (*Reglas de entrada*)

Puerto	Protocolo	Tipo	Descripción
22	TCP	SSH	Acceso SSH remoto
8080	TCP	HTTP personalizado	Apache HTTP
8081	TCP	HTTP personalizado	Nginx
8082	TCP	HTTP personalizado	Caddy
8443	TCP	HTTPS personalizado	Apache HTTPS (SSL)

---

5. Especificar la clave PEM al lanzar la instancia

Selecciona **Use existing key pair** y elige la clave labsuser.pem.

Si la instancia fue creada sin clave, termina la instancia y crea una nueva seleccionando la clave correcta.

PARTE 2: CONEXIÓN SSH DESDE WSL A AWS

1. Obtener la IP pública de la instancia

En AWS Console:

EC2 → Instances → Public IPv4 address

---

2. Conectar por SSH

ssh -i ~/.ssh/labsuser.pem ubuntu@TU-IP-PUBLICA

Ejemplo:

ssh -i ~/.ssh/labsuser.pem ubuntu@54.123.45.67

PARTE 3: EJECUTAR LA SEGUNDA PRÁCTICA ORIGINAL

A partir de aquí lo tienes todo configurado

Ejecuta **todos los comandos de la Segunda Práctica** directamente en la instancia EC2 conectada por SSH.

Accede desde tu navegador local:

http://TU-IP-PUBLICA:PUERTO

PROPUESTA DE EJERCICIO PRÁCTICO

Laboratorio: Administración Remota de Servidores Web en AWS mediante SSH desde WSL

Objetivos

- Obtener y gestionar la clave PEM desde AWS
- Establecer conexión SSH segura desde WSL hacia una instancia EC2 de AWS
- Configurar Security Groups en AWS con reglas de entrada apropiadas
- Acceder remotamente a la instancia para ejecutar los procedimientos de la Segunda Práctica original
- Documentar todo el proceso de administración remota

Tareas a realizar:

Los estudiantes trabajarán desde su máquina local con WSL2 (*Windows Subsystem for Linux*) para conectarse de forma remota a una instancia EC2 de AWS usando la clave PEM descargada directamente desde la página inicial del laboratorio. Esta aproximación simula un entorno de trabajo real donde los administradores gestionan servidores remotos desde sus estaciones de trabajo, ejecutando exactamente los mismos comandos y configuraciones descritos en el documento original.

Entregables:

1. Capturas de Clave PEM:
    - Descarga del archivo .pem desde el laboratorio
    - Contenido del directorio ~/.ssh/ mostrando la clave
    - Permisos correctos del archivo PEM (*chmod 400*)
    - Conexión SSH exitosa desde WSL
2. Capturas de Configuración AWS:
    - Instancia EC2 creada y ejecutándose
    - IP pública visible
    - Security Group con sus 5 reglas de entrada
    - Información de la clave PEM utilizada

3. Verificación de Conectividad:
    - Terminal mostrando conexión SSH exitosa
4. Documentación:
    - Documento de texto con todos los pasos seguidos
    - Explicación de qué es una clave PEM y por qué es segura
    - Descripción de cada regla del Security Group
    - Troubleshooting: qué hacer si no conecta

CRITERIOS DE EVALUACIÓN

1. Descarga y Gestión de Clave PEM (*25%*)

- Descarga correctamente la clave PEM desde el laboratorio
- Coloca la clave en la ubicación correcta (*~/.ssh/*)
- Implementa permisos correctos (*400 o 600*)
- Verifica integridad de la clave

2. Configuración de Instancia EC2 (*20%*)

- Crea instancia con especificaciones correctas (*t2/3.micro, Ubuntu 22.04/ Ubuntu 24.04*)
- IP pública habilitada
- Almacenamiento y red configurados adecuadamente

3. Configuración de Security Groups (*30%*)

- Configura todas las 5 reglas de entrada correctamente
- Comprende el propósito de cada puerto
- Entiende principios básicos de seguridad en AWS

4. Conexión SSH y Acceso Remoto (*15%*)

- Conecta exitosamente por SSH usando la clave PEM
- Ejecuta comandos remotos correctamente
- Verifica estado del sistema remoto

5. Documentación y Capturas (*10%*)

- Capturas claras de descarga y configuración de clave PEM
- Capturas de configuración AWS (*EC2, Security Groups*)
- Capturas de conexión exitosa y comandos remotos ejecutados

SOLUCIÓN DE PROBLEMAS COMUNES

- **Permission denied (publickey)**
    - chmod 400 ~/.ssh/labsuser.pem
- **Connection refused**
    - Verifica que la instancia esté activa
    - Asegúrate de usar la IP correcta
    - Prueba con ssh -v para depuración
- **Usuario incorrecto**
    - ssh -i ~/.ssh/labsuser.pem ec2-user@IP