

Hoja01_Herramientas_02

En este ejercicio vamos a crear Amazon Virtual Private Cloud (VPC) Además, en el grupo de seguridad vamos a crear la instancia EC2 (Máquina virtual) y finalmente configuraremos y personalizamos la instancia EC2 para ejecutar un servidor web

Crear una VPC

Crea una VPC con los siguientes datos:

Nombre: lab

CIDR: 10.0.0.0/16

En La zona: us-east-1a

Con una subred pública en el 10.0.0.0/24 y una subred privada 10.0.1.0/24

NO poner el gateways de NAT

Y la resolución de DNS estará activa

El resultado será:

VPC: lab-vpc

- **Subnets:**

- us-east-1a

- **Public subnet name:** lab-subnet-public1-us-east-1a

- **Private subnet name:** lab-subnet-private1-us-east-1a

- **Route tables**

- lab-rtb-public

- lab-rtb-private1-us-east-1a

- **Network connections**

- lab-igw

Una *puerta de enlace de Internet* es un recurso de VPC que permite la comunicación entre instancias EC2 en su VPC e Internet.

La subred pública lab-subnet-public1-us-east-1a tiene un CIDR de **10.0.0.0/24**, lo que significa que contiene todas las direcciones IP que comienzan con **10.0.0.x**. El hecho de que la tabla de rutas asociada con esta subred pública enrute el tráfico de red 0.0.0.0/0 a la puerta de enlace de Internet es lo que la convierte en una subred pública.

La subred privada lab-subnet-private1-us-east-1a tiene un CIDR de **10.0.1.0/24**, lo que significa que contiene todas las direcciones IP que comienzan con **10.0.1.x**.

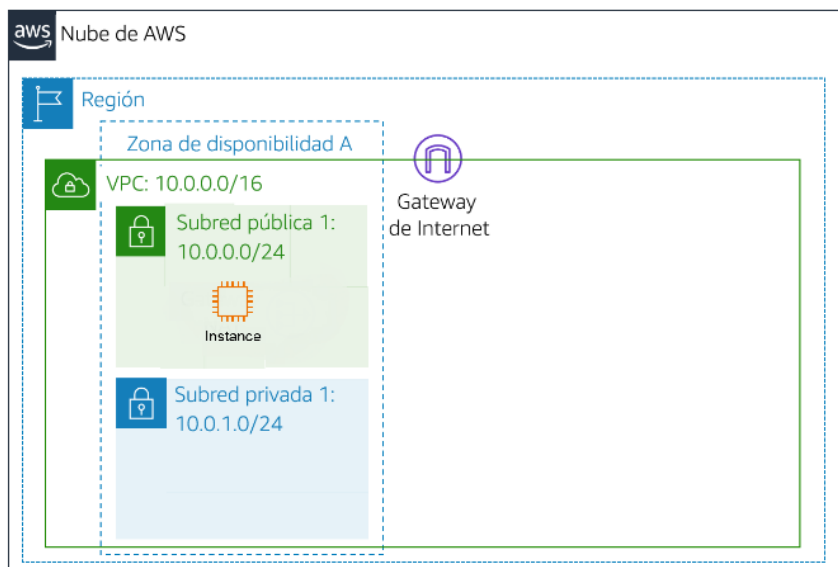


Tabla de enrutamiento pública

Destino	Objetivo
10.0.0.0/16	Local
0.0.0.0/0	Gateway de Internet

Crear un grupo de seguridad

Creamos un grupo de seguridad de nombre grupo-seguridad-web que permita abrir el puerto 80

Nombre: grupo-seguridad-web

Descripción: habilitar los puertos de web

VPC que pertenezca al grupo Lab

Abrir el puerto 80

Crear una Máquina Virtual

Crear una instancia EC2 en la subred pública creada con anterioridad

Nombre: miServidorWeb

Crearemos una máquina Ubuntu server 22.04 con disco SSD

Con un T2 medium

Selecciona el par de claves **vockey** (siempre para los laboratorios elijeremos estas claves)

Crearla en la subred pública **lab-subnet-public1-us-east-1a** y activar la ip pública

Que tenga el grupo de seguridad **grupo-seguridad-web**

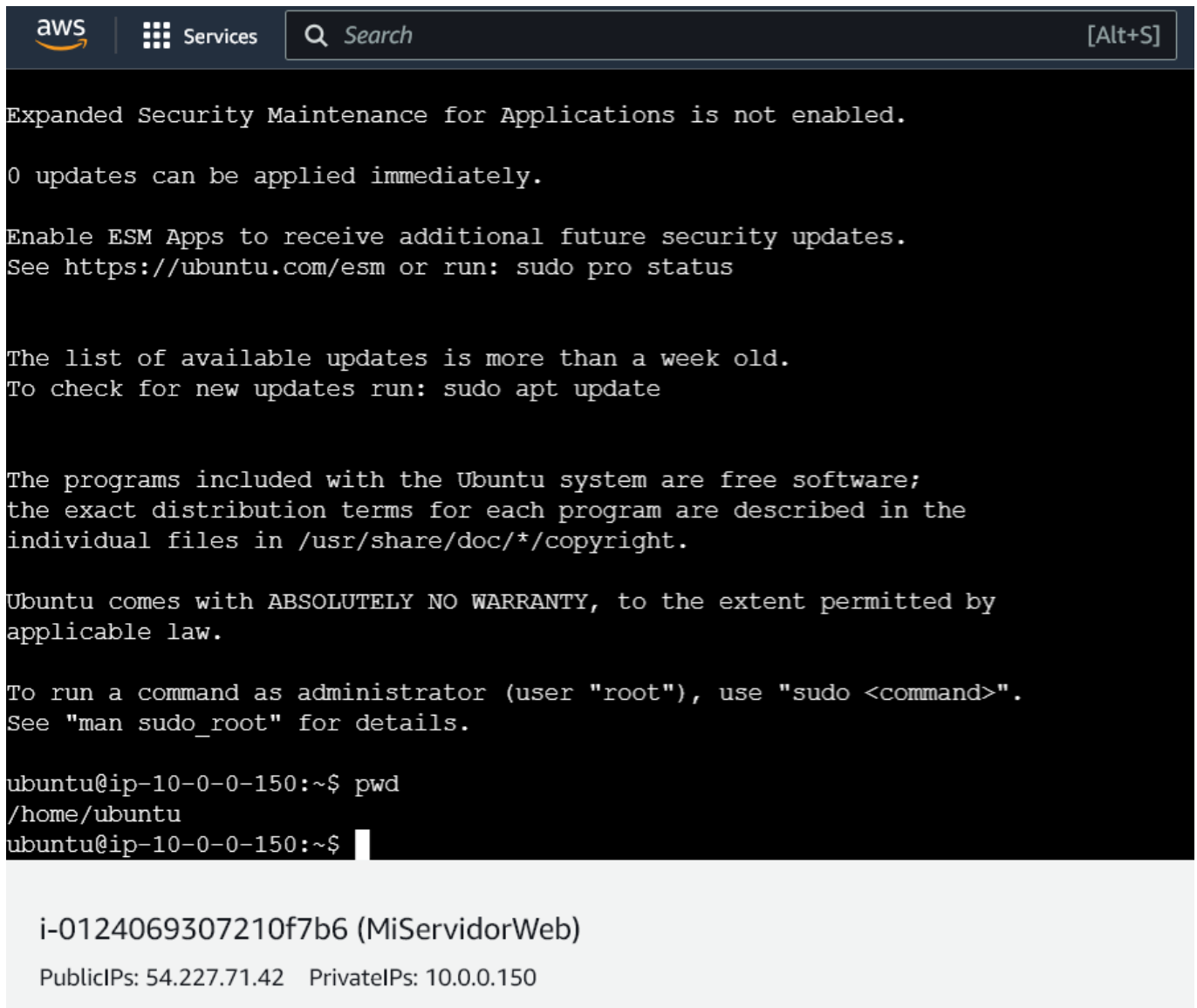
Con 20 gigas de disco

conectarnos a la máquina

En la instancia desde la opción **Connect** seleccionamos **EC2 instance Connect**, como no hemos cambiado el usuario será ubuntu.

Para ello utiliza el par de claves vockey, lo acaba de inyectar para conectarnos

Podemos trabajar directamente conectados a esta consola



The screenshot shows the AWS Management Console interface at the top with the AWS logo, a 'Services' menu, a search bar, and an '[Alt+S]' button. Below this is a terminal window with a black background and white text. The terminal output consists of several informational messages from the Ubuntu system, including a warning about 'Expanded Security Maintenance for Applications' not being enabled, instructions on how to enable it, and a notice about the age of available updates. It also includes the standard Ubuntu disclaimer about warranty and the use of 'sudo'. At the bottom of the terminal, a user prompt shows the command 'pwd' being executed, resulting in the output '/home/ubuntu'. Below the terminal window, a light gray box contains the instance ID 'i-0124069307210f7b6 (MiServidorWeb)' and its IP addresses: 'PublicIPs: 54.227.71.42' and 'PrivateIPs: 10.0.0.150'.

```

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-0-0-150:~$ pwd
/home/ubuntu
ubuntu@ip-10-0-0-150:~$

```

i-0124069307210f7b6 (MiServidorWeb)
PublicIPs: 54.227.71.42 PrivateIPs: 10.0.0.150

O tenemos la opción de conectarnos desde el terminal utilizando bien WindowsPowerShell o Putty ambos utilizan el protocolo SSH por lo que debemos modificar el grupo de seguridad e incorporar el puerto 22 para permitir la conexión

La conexión a utilizar en Windows PowerShell es **SSH cliente**

Para ver donde se encuentran las credenciales vockey, nos vamos al panel del laboratorio y vamos a la opción AWS Detalles

► Start Lab ■ End Lab ⓘ AWS Details ⓘ Readme ↺ Reset ✕

Clo

Cloud Access

AWS CLI: Show

Cloud Labs

Remaining session time: 03:13:08(194 minutes)

Session started at: 2023-10-19T09:39:10-0700

Session to end at: 2023-10-19T13:39:10-0700

Accumulated lab time: 12:01:00 (721 minutes)

No running instance

SSH key Show Download PEM Download PPK

AWS SSO Download URL

AWSAccountId	911833685022
Region	us-east-1

y podemos descargar el archivo.pem para utilizar WindowsPowerShell o el archivo.PPK para Putty

Al descargar el archivo en vez de denominarlo vockey se denomina **labuser**.

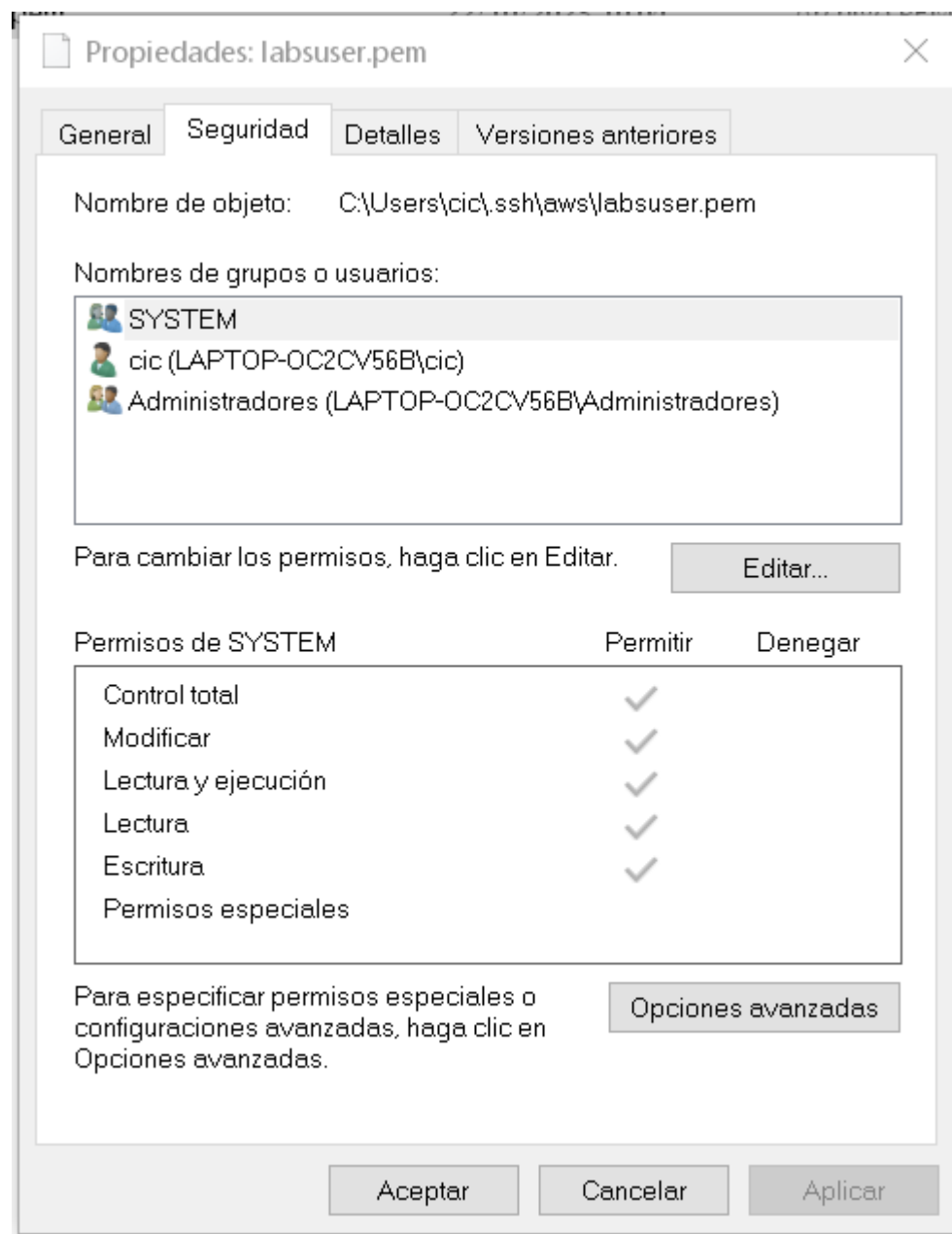
```
ssh -i <ruta_archivo_labuser.pem> ubuntu@<IP_pública>
```

Nos muestra el siguiente error

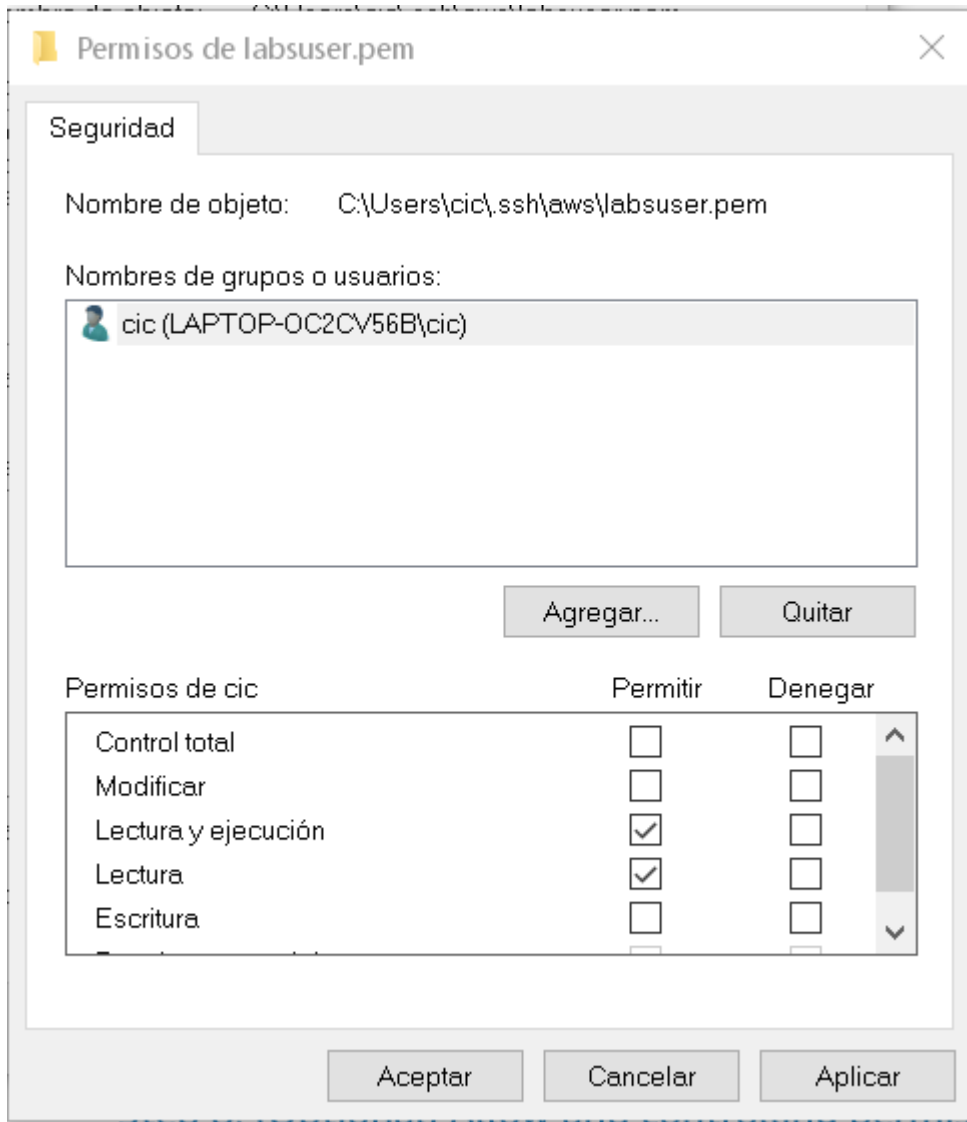
```
PS C:\Users\cic\.ssh\aws> ssh -i labuser.pem ubuntu@ec2-54-227-71-42.compute-1.amazonaws.com
Warning: Identity file labuser.pem not accessible: llo such file or directory.
The authenticity of host 'ec2-54-227-71-42.compute-1.amazonaws.com (54.227.71.42)' can't be established.
ECDSA key fingerprint is SHA256:P1HnbXn0vXAkIzRunb79dB4Jwbzxf6dgrcbrZxJAx4.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-54-227-71-42.compute-1.amazonaws.com,54.227.71.42' (ECDSA) to the list of known hosts.
ubuntu@ec2-54-227-71-42.compute-1.amazonaws.com: Permission denied (publickey).
PS C:\Users\cic\.ssh\aws>
```

Como la conexión la estamos realizando desde una máquina windows tenemos que quitar permisos al fichero labuser.pem y solo dejar como usuario solo a nuestro usuario. Si es linux cambiamos los permisos cono indica

en la pantalla de conexión SSH cliente. En Windows primero tenemos:



Para quedar, solo dejar permisos con el usuario que estoy:



Abrimos de nuevo una consola de Windows PowerShell y ahora nos dejará conectarnos

```

PS C:\Users\cic\.ssh\aws> ssh -i "labuser.pem" ubuntu@ec2-54-205-151-168.compute-1.amazonaws.com
The authenticity of host 'ec2-54-205-151-168.compute-1.amazonaws.com (54.205.151.168)' can't be established.
ECDSA key fingerprint is SHA256:P1HnbXn0vXAkIzRunb79dB4Jwbzxzf6dgrcbrZxJAx4.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-54-205-151-168.compute-1.amazonaws.com,54.205.151.168' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-1012-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Sun Oct 22 11:14:34 UTC 2023

System load:  0.0          Processes:    110
Usage of /:   9.6% of 19.2GB Users logged in: 1
Memory usage: 6%          IPv4 address for eth0: 10.0.0.150
Swap usage:   0%

 * Ubuntu Pro delivers the most comprehensive open source security and
   compliance features.

https://ubuntu.com/aws/pro

Expanded Security Maintenance for Applications is not enabled.

35 updates can be applied immediately.
25 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Sun Oct 22 10:39:04 2023 from 18.206.107.27
ubuntu@ip-10-0-0-150:~$

```

Si quieres conectarte utilizando Putty sigue el manual de ayuda que figura en la consola de AWS [Usuarios de Windows: Uso de SSH para conectarse](#)

Crear una ip pública fija

Para que cada vez que arranquemos la máquina no nos cambie la IP pública deberemos crear una **Elastic IP** que dependa de la zona **us-east-1** y luego asociar a esa ip a la máquina creada así tendremos siempre la misma ip

Nos queda:

<input type="checkbox"/>	Name	Allocated IPv4 addr...	Type	Allocation ID	Reverse DNS record
<input checked="" type="checkbox"/>	ip pública maquina	54.205.151.168	Public IP	eipalloc-001968a36685b8c37	–
<input type="checkbox"/>	Laboratorio-eip-us-east-1a	54.209.212.245	Public IP	eipalloc-0b24c883b1b171776	–

54.205.151.168 Association ID eipassoc-014ed942f441fbb34 Network interface ID eni-03dda5086c8dba614	Public IP Scope VPC Network interface owner account ID 911833685022	eipalloc-001968a36685b8c37 Associated instance ID i-0124069307210f7b6 Public DNS ec2-54-205-151-168.compute-1.amazonaws.com	Private IP address 10.0.0.150 NAT Gateway ID –
--	--	--	---

Crear un Servidor Web

Con alguna de las conexiones anteriores vamos a instalar el servidor web de apache y el php, seguir los pasos indicados en la práctica **hoja01_Herramientas_01**.

