



## **UNIVERSIDAD DON BOSCO**

**Administración de Servicios en la Nube ASN901 G01T**

**DOCENTE: Ing. Napoleón López**

**Proyecto fase 1**

**Link de video: <https://youtu.be/DVH1iLBAhMs>**

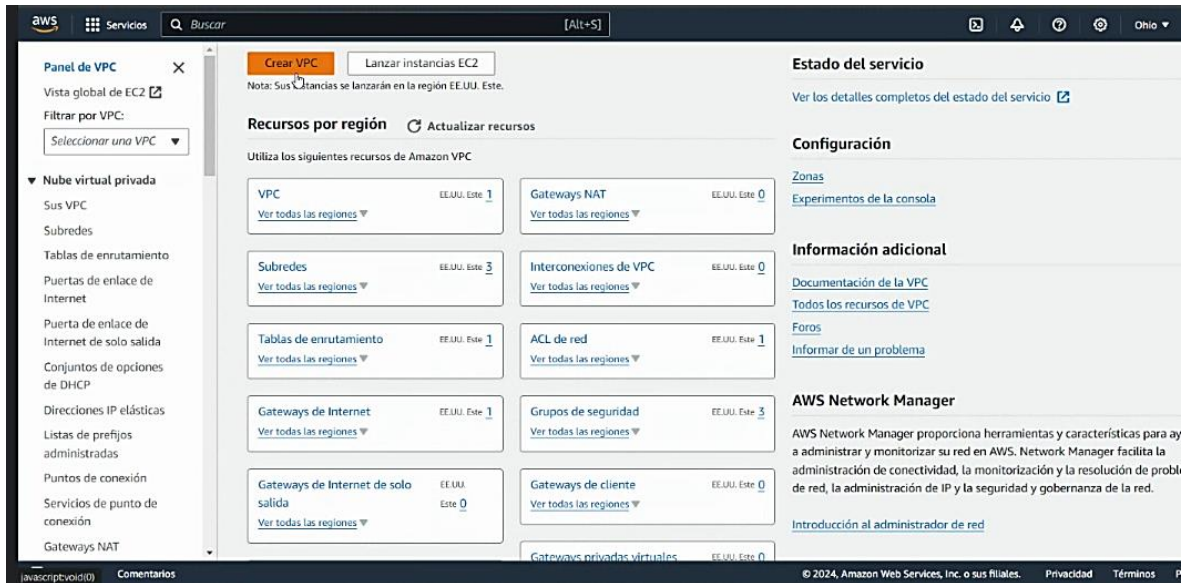
### **Alumnos:**

Jordan Ismael Zelaya Ramírez	ZR170168
Henry Vladimir Nájera Guerra	NG110680

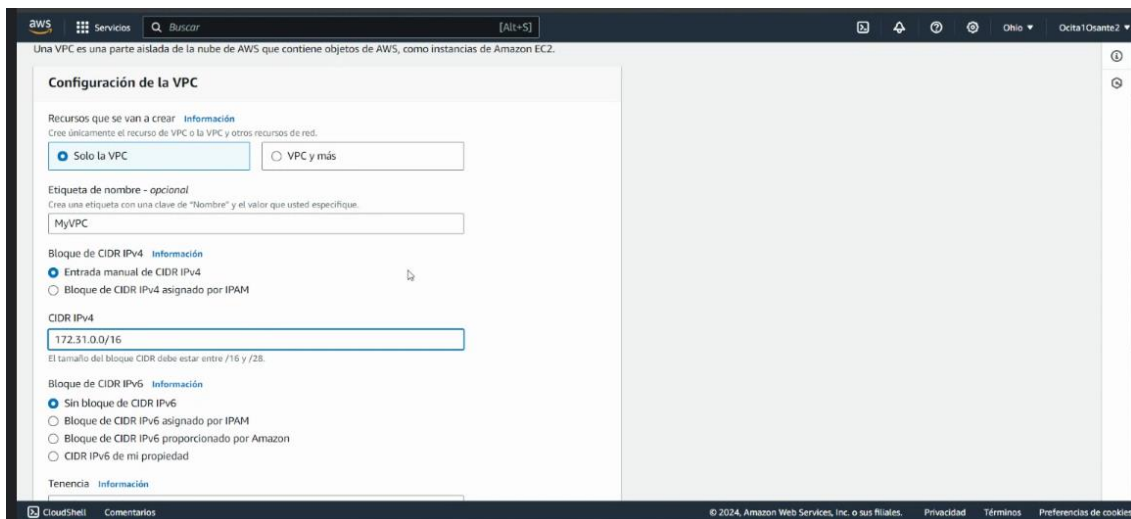
**Ciudadela Don Bosco, 9 de abril del 2024**

## CREACION DE VPC PARA PROPORCIONAR CONECTIVIDAD

Damos clic en CREAR VPC del panel de VPC.

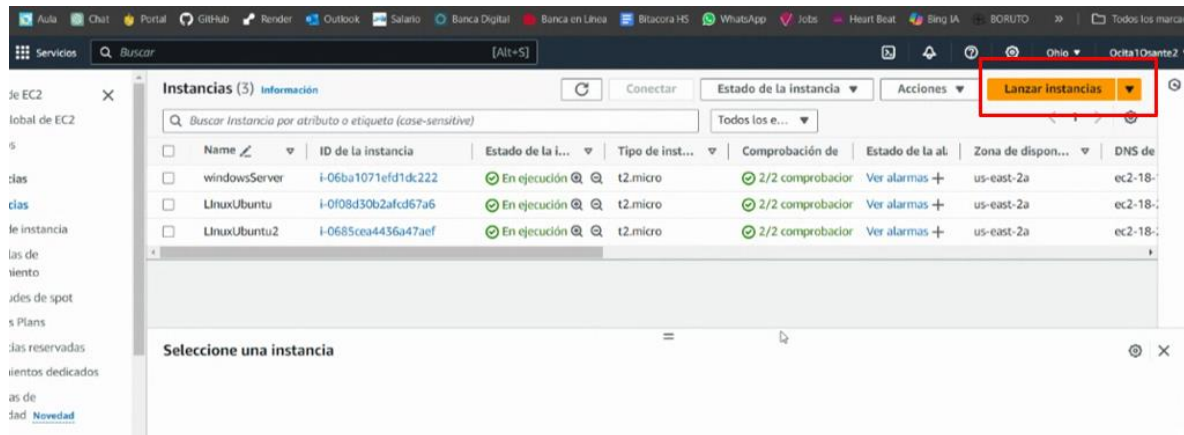


Damos clic en solo VPC, luego seleccionamos entrada manual, colocamos la IP con su respectivo sufijo y luego en CREAR VPC

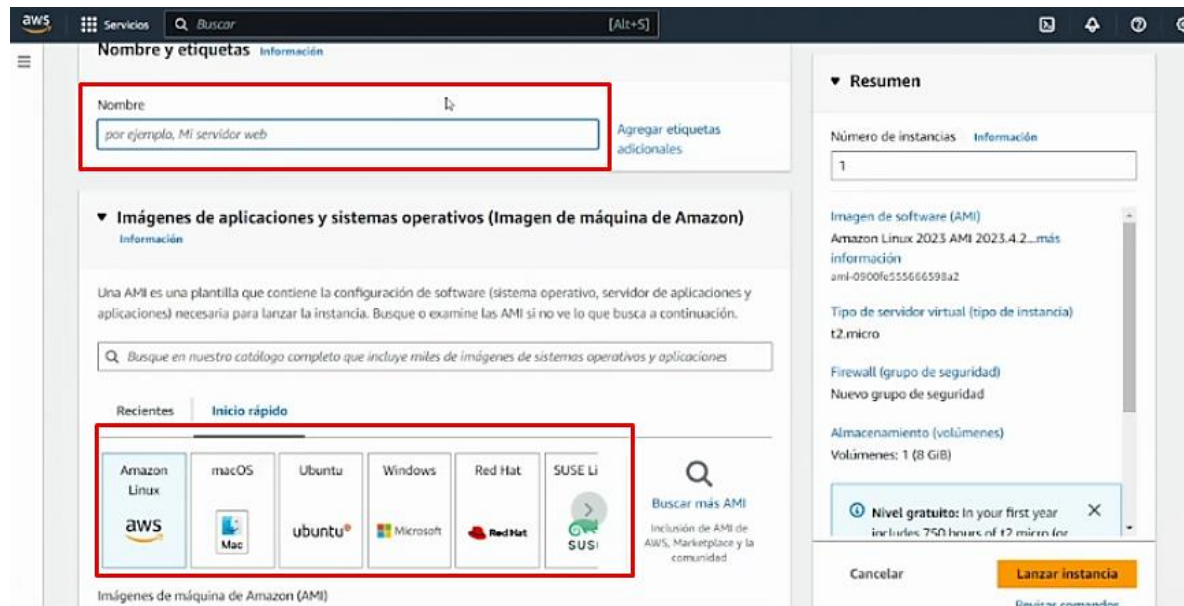


## CREACION DE INSTANCIAS

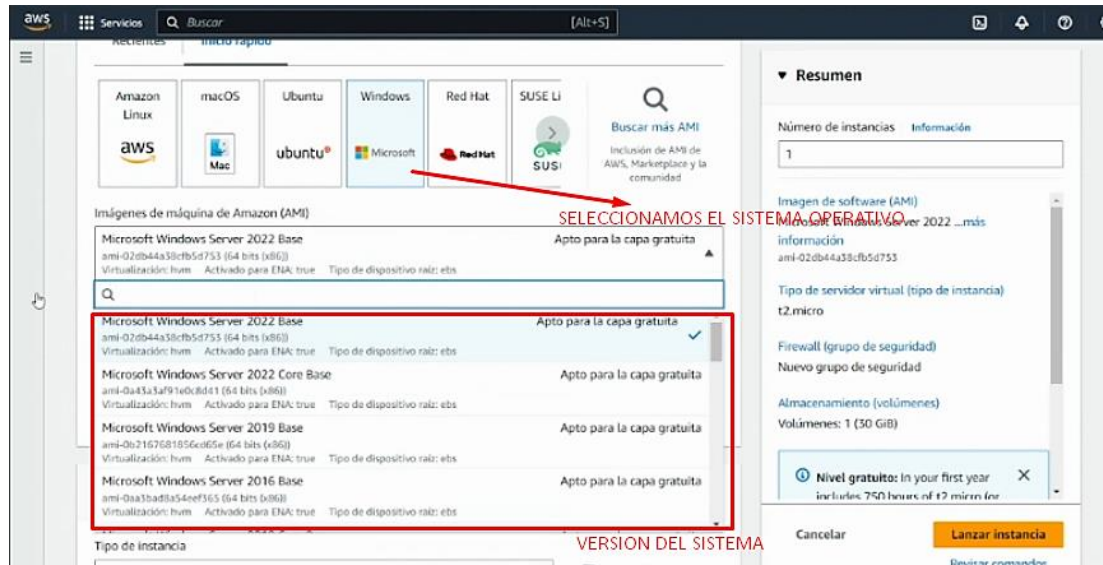
Creamos las instancias o maquinas virtuales seleccionando la opcion LANZAR INSTANCIAS en el menú



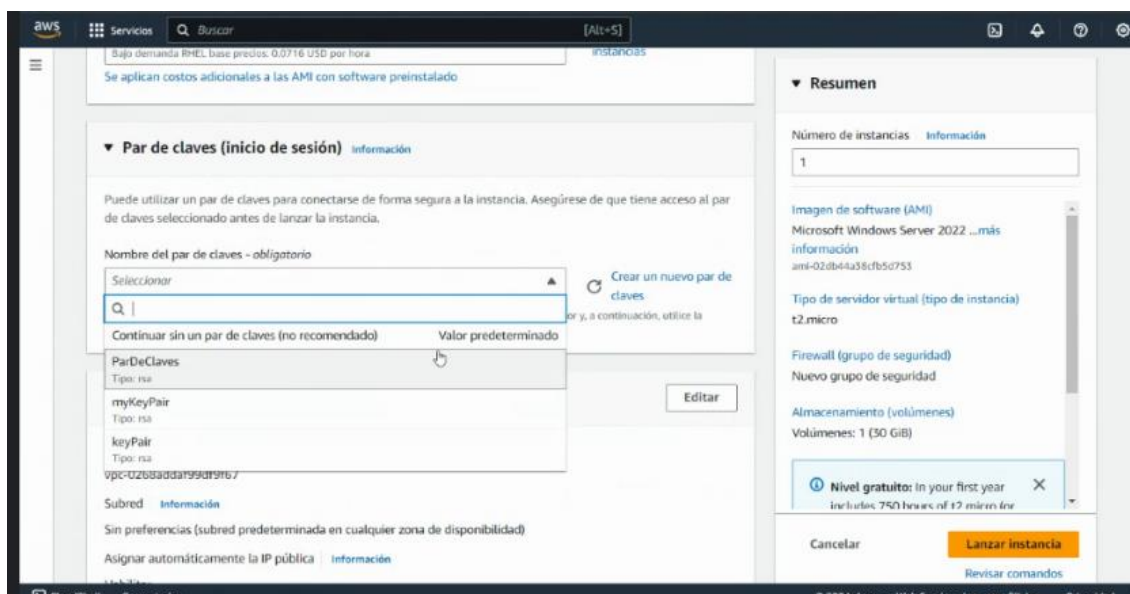
Nombramos cada una de las instancias a crear y seleccionamos el sistema operativo para cada una de ellas.



Luego de seleccionar el Sistema Operativo, debemos elegir la version del mismo según nuestra conveniencia.



Luego, crearemos un par de claves, las cuales son las credenciales de seguridad necesarias para validar nuestra identidad.



Luego haremos las configuraciones de vpc para nuestra red virtual.

Una vez creada la red, tambien debemos crear subredes y habilitamos el asignar la IP publica.

Configuraciones de red

VPC: obligatorio [Información](#)

vpc-0268adda199d9f967 (predeterminado)

Subred [Información](#)

Sin preferencias [Crear nueva subred](#)

Asignar automáticamente la IP pública [Información](#)

Habilitar

Additional charges apply when outside of free tier allowance

Firewall (grupos de seguridad) [Información](#)

Un grupo de seguridad es un conjunto de reglas de firewall que controlan el tráfico de la instancia. Agregue reglas para permitir que un tráfico específico llegue a la instancia.

☒ Crear grupo de seguridad ☐ Seleccionar un grupo de seguridad existente

Nombre del grupo de seguridad - obligatorio

launch-wizard-2

Este grupo de seguridad se agregará a todas las interfaces de red. El nombre no se puede editar después de crear el grupo de seguridad. La longitud máxima es de 255 caracteres. Caracteres válidos: a-z, A-Z, 0-9, espacios y \_- / [ ] \* = & . ! \$ % ^ & #

Descripción - obligatorio [Información](#)

launch-wizard-2 created 2024-04-04T03:06:37.732Z

Resumen

Número de instancias [Información](#)

1

Imagen de software (AMI) [Información](#)

Canonical, Ubuntu, 22.04 LTS, ... más información

ami-0b844ec9a8f90422

Tipo de servidor virtual (tipo de instancia)

t2.micro

Firewall (grupo de seguridad)

Nuevo grupo de seguridad

Almacenamiento (volumenes)

Volumenes: 1 (8 GiB)

Nivel gratuito: In your first year includes 750 hours of t2.micro (or t3.micro in the Review in which

Cancelar [Lanzar instancia](#)

Revisar comandos

El siguiente paso es crear un grupo de seguridad, el cual controla el trafico de entrada y salida de nuestra VPC, seleccionamos el tipo de protocolo y el rango de puertos.

Firewall (grupos de seguridad) [Información](#)

Un grupo de seguridad es un conjunto de reglas de firewall que controlan el tráfico de la instancia. Agregue reglas para permitir que un tráfico específico llegue a la instancia.

☒ Crear grupo de seguridad ☐ Seleccionar un grupo de seguridad existente

Nombre del grupo de seguridad - obligatorio

launch-wizard-2

Este grupo de seguridad se agregará a todas las interfaces de red. El nombre no se puede editar después de crear el grupo de seguridad. La longitud máxima es de 255 caracteres. Caracteres válidos: a-z, A-Z, 0-9, espacios y \_- / [ ] \* = & . ! \$ % ^ & #

Descripción - obligatorio [Información](#)

launch-wizard-2 created 2024-04-04T03:06:37.732Z

Reglas de grupos de seguridad de entrada

▼ Regla del grupo de seguridad 1 (TCP, 3389, 0.0.0.0/0) [Eliminar](#)

Tipo <a href="#">Información</a>	Protocolo <a href="#">Información</a>	Intervalo de puertos <a href="#">Información</a>
rdp	TCP	3389

Tipo de origen <a href="#">Información</a>	Origen <a href="#">Información</a>	Descripción - opcional <a href="#">Información</a>
Cualquier lugar	0.0.0.0/0	por ejemplo, SSH para Admin Desk

Resumen

Número de instancias [Información](#)

1

Imagen de software (AMI) [Información](#)

Microsoft Windows Server 2022 ... más información

ami-020b44a38cfb5d753

Tipo de servidor virtual (tipo de instancia)

t2.micro

Firewall (grupo de seguridad)

Nuevo grupo de seguridad

Almacenamiento (volumenes)

Volumenes: 1 (30 GiB)

Nivel gratuito: In your first year includes 750 hours of t2.micro (or t3.micro in the Review in which

Cancelar [Lanzar instancia](#)

Revisar comandos

Para crear la instancia damos clic en LANZAR INSTANCIA

Reglas de grupos de seguridad de entrada

▼ Regla del grupo de seguridad 1 (TCP, 3389, 0.0.0.0/0)

Eliminar

Tipo: Información  
Protocolo: Información  
Intervalo de puertos: Información

rdp  
TCP  
3389

Tipo de origen: Información  
Origen: Información  
Descripción - opcional: Información

Cualquier lugar  
Add CIDR, prefix list or security  
por ejemplo, SSH para Admin Desk

0.0.0.0/0

Firewall (grupo de seguridad)  
Nuevo grupo de seguridad

Almacenamiento (volúmenes)  
Volúmenes: 1 (30 GiB)

Nivel gratuito: In your first year includes 750 hours of t2.micro for

Cancelar Lanzar instancia

Procedemos con la creación de otra instancia solo que, en esta ocasión con Sistema Operativo Linux, seleccionamos Ubuntu y también la versión.

aws Servicios Q. Buscar [Alt+S] Ohio Ocita1Osanta2

Recientes Inicio rápido

Amazon Linux macOS Ubuntu Windows Red Hat SUSE Linux

Buscar más AMI

Inclusión de AMI de AWS, Marketplace y la comunidad

Imágenes de máquina de Amazon (AMI)

Ubuntu Server 22.04 LTS (HVM), SSD Volume Type  
ami-0b8b44ec9a8f90422 (64 bits x86) / ami-0000425a99b7b6a9d (64 bits (Arm))  
Virtualización: hvm Activado para ENA: true Tipo de dispositivo raíz: ebs

Apto para la capa gratuita

Descripción  
Canonical, Ubuntu, 22.04 LTS, amd64 jammy image build on 2024-03-01

Arquitectura ID de AMI

64 bits (x86) ami-0b8b44ec9a8f90422

Proveedor verificado

▼ Tipo de instancia Información | Obtener asesoramiento

Resumen

Número de instancias Información

1

Imagen de software (AMI)  
Canonical, Ubuntu, 22.04 LTS, ... más información  
ami-0b8b44ec9a8f90422

Tipo de servidor virtual (tipo de instancia)  
t2.micro

Firewall (grupo de seguridad)  
Nuevo grupo de seguridad

Almacenamiento (volúmenes)  
Volúmenes: 1 (8 GiB)

Nivel gratuito: In your first year includes 750 hours of t2.micro (or 750 hours in the Region in which

Cancelar Lanzar instancia

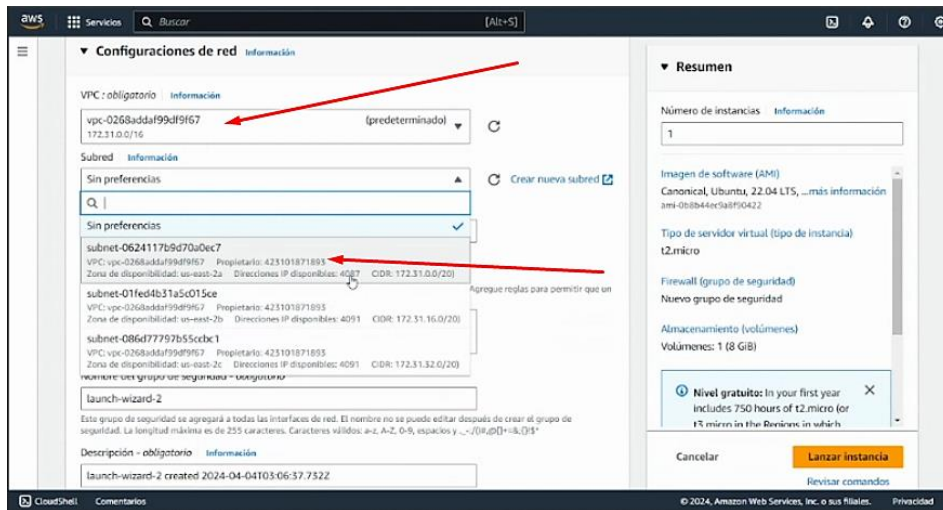
Revisar comandos

CloudShell Comentarios

© 2024, Amazon Web Services, Inc. o sus filiales. Privacidad Términos Preferencias de cookies

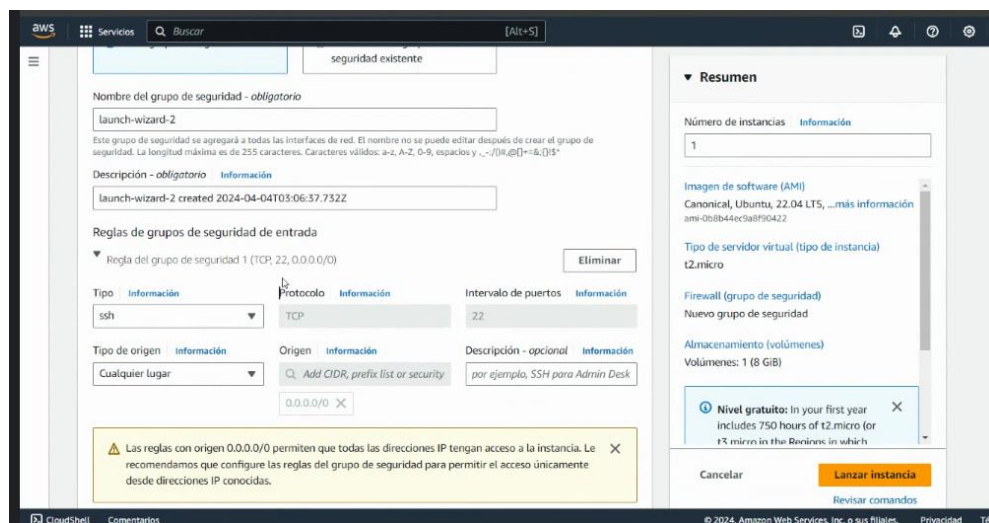


Para que exista comunicación entre las maquinas virtuales, incluimos la nueva instancia a la VPC con su respectiva subred que en este caso es sufijo 20. Es importante recalcar que las 3 maquinas virtuales deben estar configuradas en la misma VPC.



Para la configuración del grupo de seguridad en Linux, el tipo a seleccionar es ssh y el puerto 22.

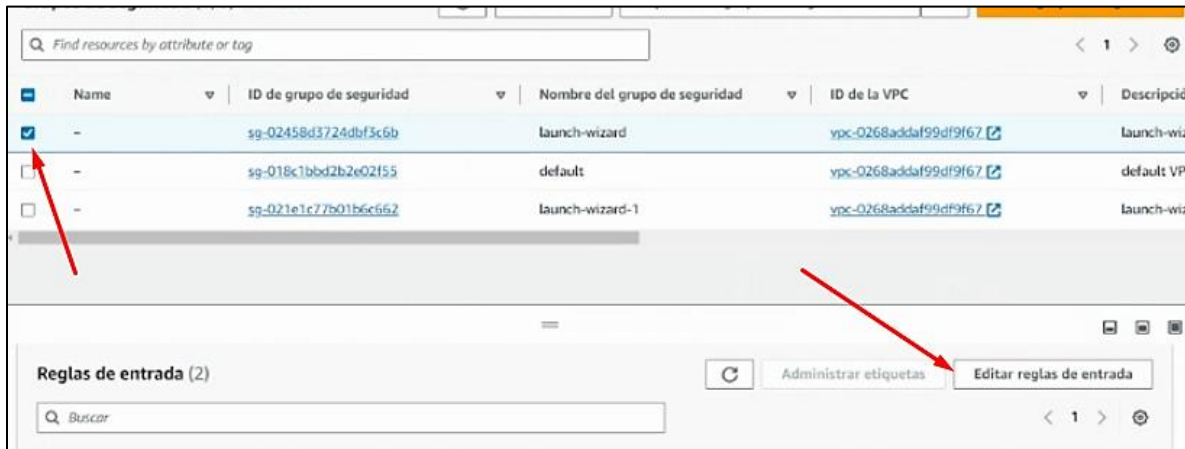
Creamos la instancia dando clic en LANZAR INSTANCIA.



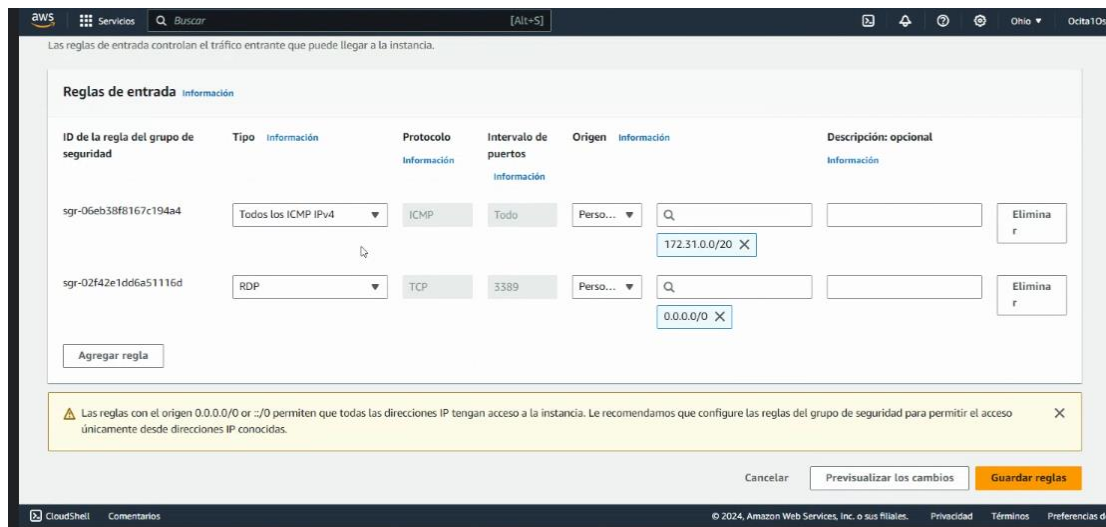
## EDITAR REGLAS DE ENTRADA PARA LOS GRUPOS DE SEGURIDAD

Habilitamos el protocolo ICMP para poder hacer PING entre instancias

Seleccionamos la instancia, luego damos clic en EDITAR REGLAS DE ENTRADA



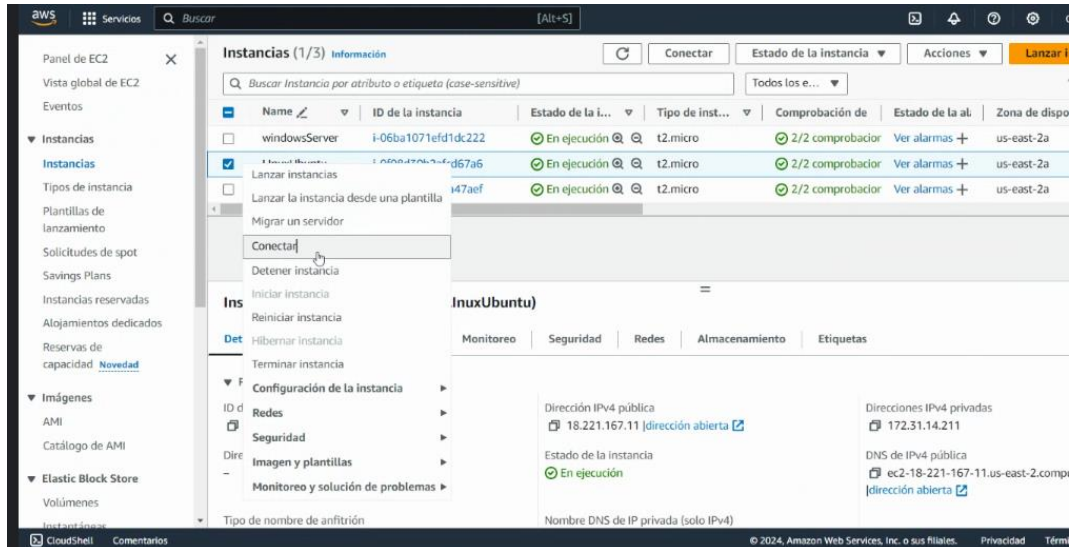
Seleccionamos el protocolo ICMP, también seleccionamos la subred con sufijo 20 y luego en GUARDAR





## EJECUCIÓN DE INSTANCIAS

Seleccionamos la instancia a ejecutar y luego en conectar.



Luego seleccionamos la conexión de estancia EC2 la cual contiene nuestras configuraciones de red



Seleccionamos el punto de conexión, el cual varia dependiendo el sistema que posea nuestra instancia.

ID de la instancia  
i-0f08d30b2afcd67a6 (LinuxUbuntu)

Tipo de conexión

☐ Conectarse mediante la Conexión de la Instancia EC2  
Conéctese mediante el cliente basado en navegador de EC2 Instance Connect, con una dirección IPv4 pública.

☒ Conectarse mediante punto de conexión de EC2 Instance Connect  
Conéctese mediante el cliente basado en navegador de EC2 Instance Connect, con una dirección IPv4 privada y un punto de conexión de VPC.

Dirección IP privada  
172.31.14.211

Punto de conexión de EC2 Instance Connect  
Only endpoints that have completed the creation process can be selected. The process can take up to 15 minutes. If you create an endpoint, refresh this list to check if its in the available state.

Q eice-0661215541e194762 X

Utilizar: \*eice-0661215541e194762\*

eice-0661215541e194762  
State: create-complete | AZ: us-east-2a

Q ubuntu X

Duración máxima de túnel (segundos)  
La duración máxima permitida de la conexión SSH. Debe cumplir la condición maxTunnelDuration (si se especificó) en la política de IAM.

3600

1 segundo mínimo. 3600 segundos (1 hora) máximo.

Damos clic en CONECTAR

el nombre de usuario predeterminado, ubuntu.

Q ubuntu X

Duración máxima de túnel (segundos)  
La duración máxima permitida de la conexión SSH. Debe cumplir la condición maxTunnelDuration (si se especificó) en la política de IAM.

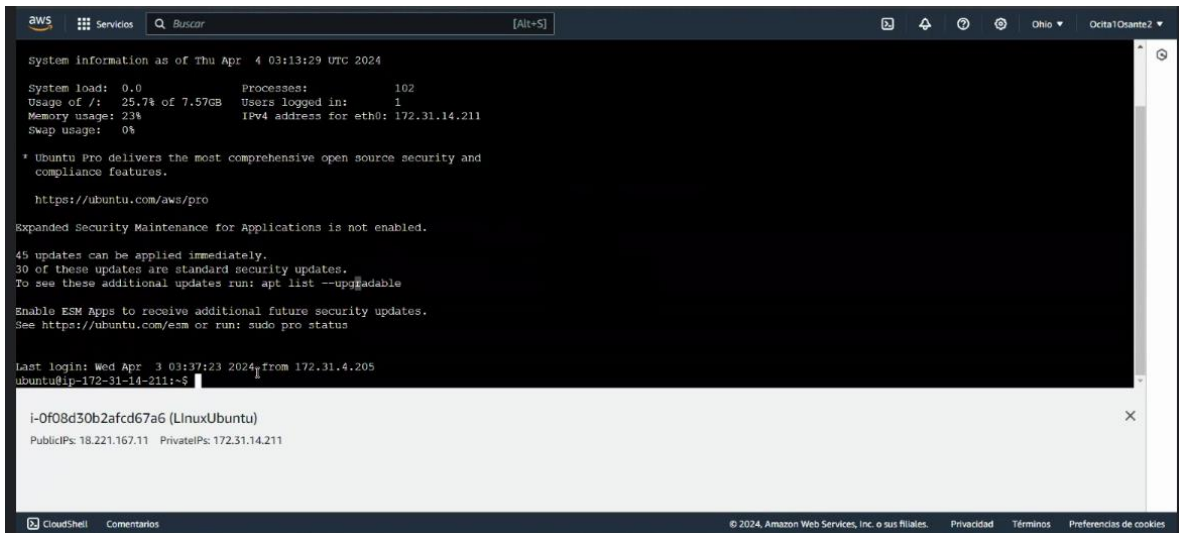
3600

1 segundo mínimo. 3600 segundos (1 hora) máximo.

**Nota:** En la mayoría de los casos, el nombre de usuario predeterminado, ubuntu, es correcto. Sin embargo, lea las instrucciones de uso de la AMI para comprobar si el propietario de la AMI ha cambiado el nombre de usuario predeterminado.

Cancelar Conectar

Se nos mostrará en pantalla nuestra máquina virtual en línea.



The screenshot shows the AWS CloudShell interface. The terminal displays system information for a Linux Ubuntu instance. The system load is 0.0, with 102 processes. Memory usage is 25.7% of 7.57GB, and swap usage is 0%. The terminal also shows that 45 updates can be applied immediately, with 30 being standard security updates. A message indicates that Expanded Security Maintenance for Applications is not enabled. The terminal prompt is 'ubuntu@ip-172-31-14-211:~\$'. Below the terminal, a metadata box shows the instance ID 'i-0f08d30b2afcd67a6 (LinuxUbuntu)' and its public and private IP addresses.

```
System information as of Thu Apr  4 03:13:29 UTC 2024

System load:  0.0                Processes:    102
Usage of /:   25.7% of 7.57GB    Users logged in:  1
Memory usage: 23%              IPv4 address for eth0: 172.31.14.211
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.

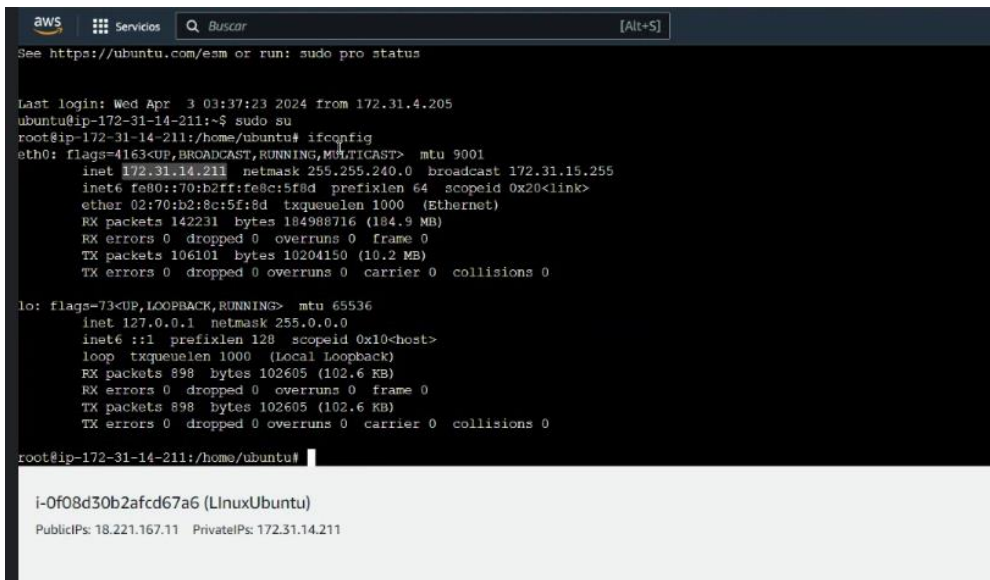
45 updates can be applied immediately.
30 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

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

Last login: Wed Apr  3 03:37:23 2024 from 172.31.4.205
ubuntu@ip-172-31-14-211:~$
```

i-0f08d30b2afcd67a6 (LinuxUbuntu)  
PublicIPs: 18.221.167.11 PrivateIPs: 172.31.14.211

Mediante el comando ifconfig podemos ver la IP



The screenshot shows the AWS CloudShell interface. The terminal displays the output of the 'ifconfig' command. It shows the configuration for the 'eth0' interface, including its IP address (172.31.14.211), netmask (255.255.240.0), broadcast address (172.31.15.255), and other details like MTU, RX/TX packets, and errors. It also shows the configuration for the 'lo' (loopback) interface with IP address 127.0.0.1. The terminal prompt is 'root@ip-172-31-14-211:/home/ubuntu#'. Below the terminal, the same metadata box as in the previous screenshot is visible.

```
See https://ubuntu.com/esm or run: sudo pro status

Last login: Wed Apr  3 03:37:23 2024 from 172.31.4.205
ubuntu@ip-172-31-14-211:~$ sudo su
root@ip-172-31-14-211:/home/ubuntu# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 9001
    inet 172.31.14.211  netmask 255.255.240.0  broadcast 172.31.15.255
    inet6 fe80::70:b2ff:fe8c:5f8d  prefixlen 64  scopeid 0x20<link>
    ether 02:70:b2:8c:5f:8d  txqueuelen 1000  (Ethernet)
    RX packets 142231  bytes 184988716 (184.9 MB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 106101  bytes 10204150 (10.2 MB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    inet6 ::1  prefixlen 128  scopeid 0x10<host>
    loop txqueuelen 1000  (Local Loopback)
    RX packets 898  bytes 102605 (102.6 KB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 898  bytes 102605 (102.6 KB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

root@ip-172-31-14-211:/home/ubuntu#
```

i-0f08d30b2afcd67a6 (LinuxUbuntu)  
PublicIPs: 18.221.167.11 PrivateIPs: 172.31.14.211

Verificamos su conexión a internet mediante el comando PING + DIRECCION WEB

```
aws
Servicios
Buscar
[Alt+S]

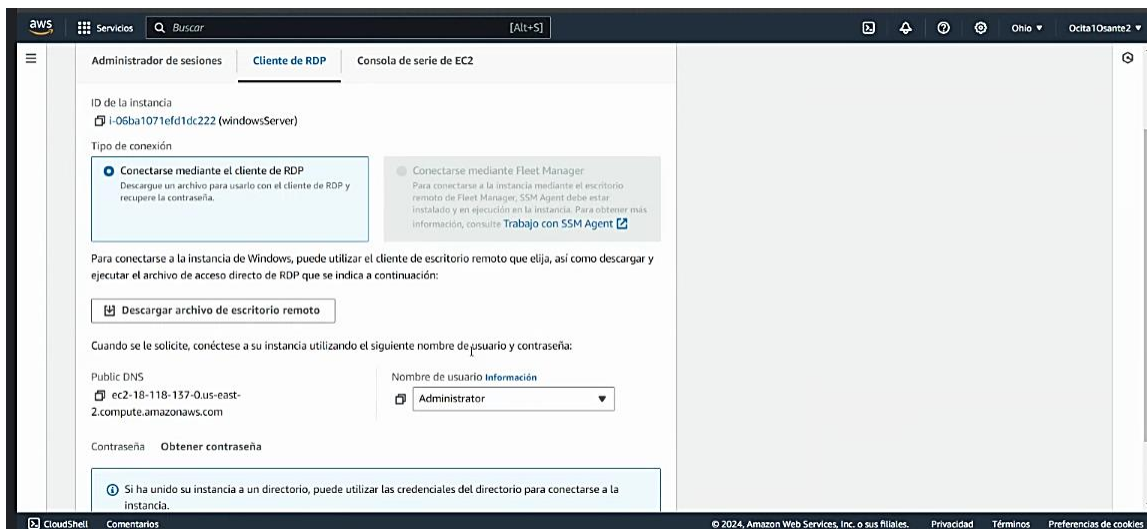
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 9001
    inet 172.31.14.211 netmask 255.255.240.0 broadcast 172.31.15.255
    inet6 fe80::70:b2ff:fe8c:5f8d prefixlen 64 scopeid 0x20<link>
    ether 02:70:b2:8c:5f:8d txqueuelen 1000 (Ethernet)
    RX packets 142231 bytes 184988716 (184.9 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 106101 bytes 10204150 (10.2 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 898 bytes 102605 (102.6 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 898 bytes 102605 (102.6 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

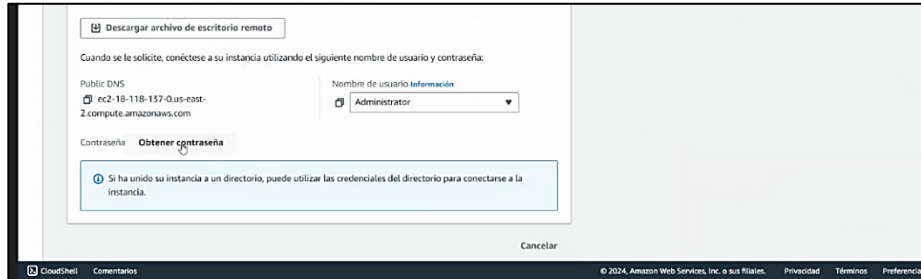
root@ip-172-31-14-211:/home/ubuntu# ping www.google.com
PING www.google.com (142.250.191.164) 56(84) bytes of data:
64 bytes from ord38s30-in-f4.1e100.net (142.250.191.164): icmp_seq=1 ttl=112 time=16.8 ms
64 bytes from ord38s30-in-f4.1e100.net (142.250.191.164): icmp_seq=2 ttl=112 time=16.9 ms
64 bytes from ord38s30-in-f4.1e100.net (142.250.191.164): icmp_seq=3 ttl=112 time=16.9 ms
64 bytes from ord38s30-in-f4.1e100.net (142.250.191.164): icmp_seq=4 ttl=112 time=16.9 ms

i-0f08d30b2afcd67a6 (LinuxUbuntu)
PublicIPs: 18.221.167.11 PrivateIPs: 172.31.14.211
```

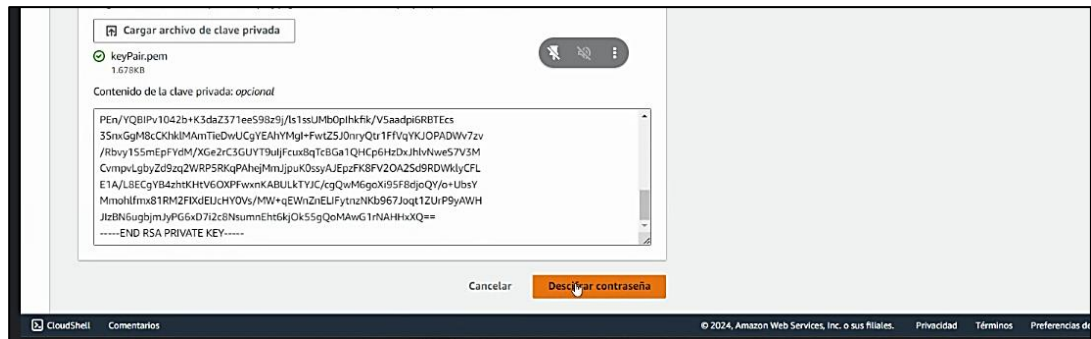
Ejecutamos la instancia de Windows, seleccionamos la pestaña CLIENTE DE RDP y luego en la opcion DESCARGAR ARCHIVO DE ESCRITORIO REMOTO



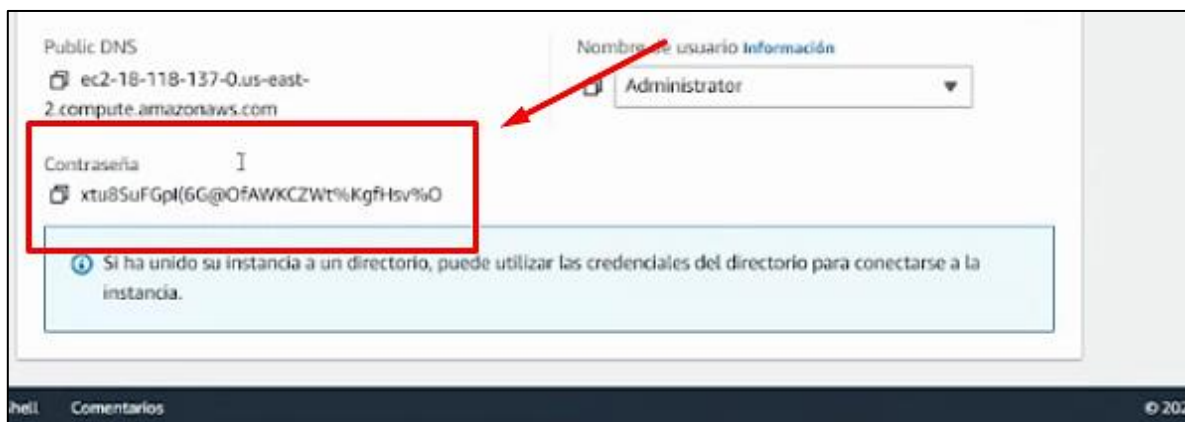
Seleccionamos OBTENER CONTRASEÑA



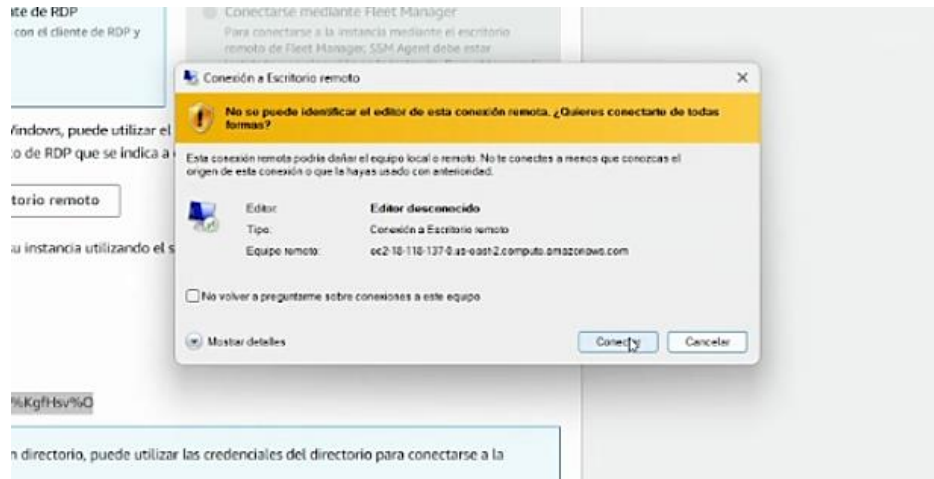
Damos clic en la opción de CARGAR ARCHIVO DE CLAVE PRIVADA, seleccionamos el archivo que descargamos anteriormente y luego en la opción DESCIFRAR CONTRASEÑA.



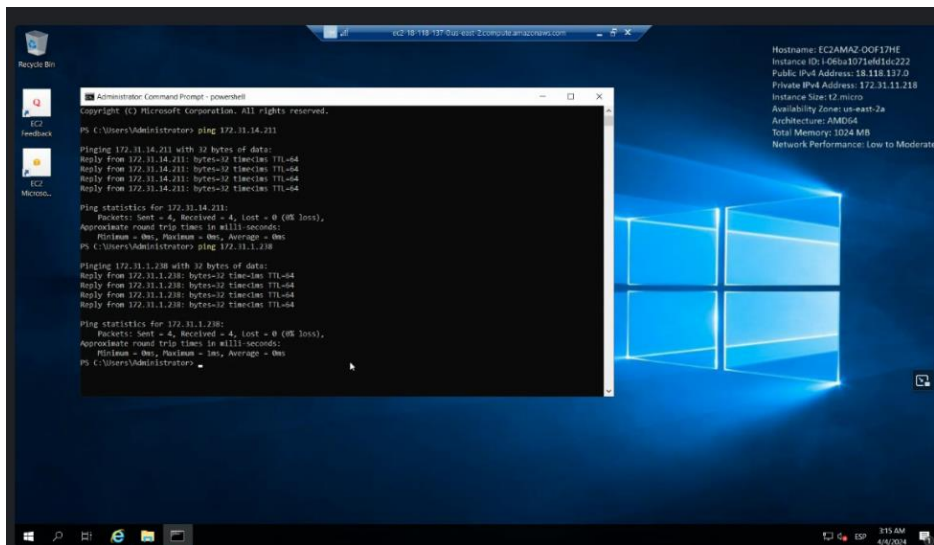
La contraseña generada nos servirá para entrar al servidor de Windows



Seleccionamos Windows Server, damos clic en CONECTAR e ingresamos la contraseña.

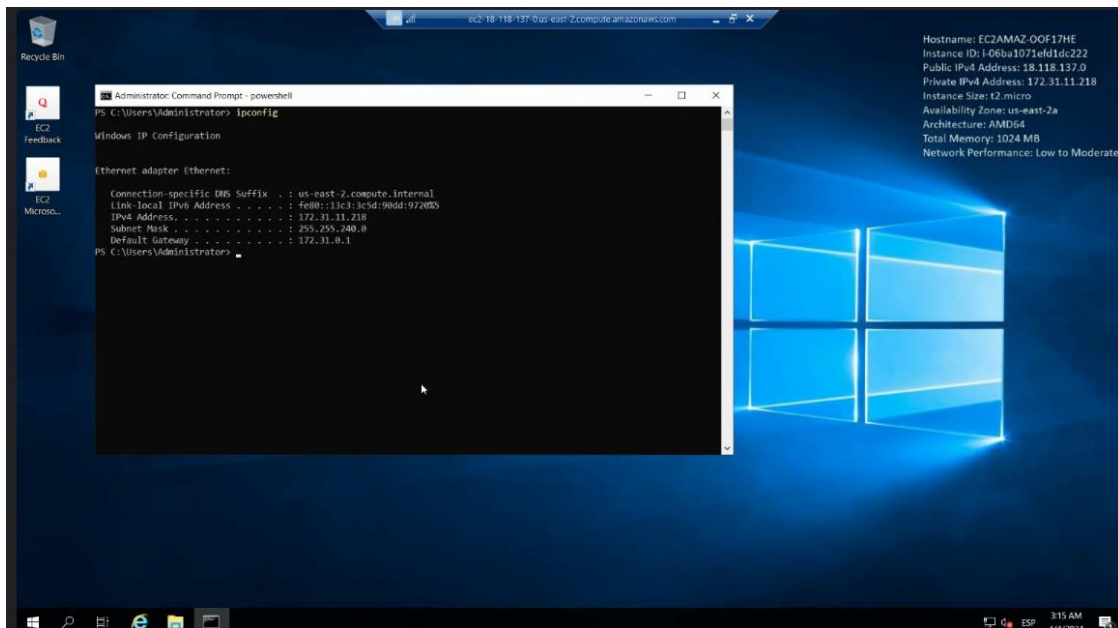


Nos mostrará la siguiente pantalla





Mediante el comando IPCONFIG podremos observar su configuración de IP



Comprobamos conexión entre máquinas mediante el comando PING + IP de la otra máquina.

