

PRÁCTICA 6

INSTALACIÓN Y CONFIGURACIÓN BÁSICA DE TECNOLOGÍAS DE VIRTUALIZACIÓN DE SERVIDORES EN LA NUBE

FECHA DE INICIO: 5/12/2024

FECHA DE FINALIZACIÓN ESPERADA: 12/12/2024

RAs ASOCIADOS: RA1. Implanta arquitecturas web analizando y aplicando criterios de funcionalidad.
RA2. Implanta aplicaciones web en servidores web, evaluando y aplicando criterios de configuración para su funcionamiento seguro.

CEs ASOCIADOS: RA1: e y f; RA2: i.

INDICE

Contenido

INDICE.....	1
OBJETIVOS	2
ENUNCIADO.....	2
DOCUMENTACIÓN	2
Acceso al curso y activación del laboratorio	2
Obtención de claves PEM.....	4
Creación y configuración de la VPC y Configuración de la red.....	5
Instancia EC2 de Windows (pública)	8
Instancia EC2 de Ubuntu (pública)	13
Conexión a la Instancia de Windows.....	18
Web de Apache y personalizada	22
Acceso desde el cliente a el servidor privado + pruebas	31
Pruebas.....	32
RÚBRICA DE CORRECCIÓN.....	33

OBJETIVOS

- Aprender a probar un laboratorio de pruebas en la nube para el despliegue web con Linux, Apache y MariaDb en distintos servidores.
- Comprobar el funcionamiento de la instalación mediante el acceso mediante escritorio remoto
- Documentar el proceso de instalación.

ENUNCIADO

En este ejercicio vamos a crear Amazon Virtual Private Cloud (VPC) con una subred pública y otra privada

Además, vamos a crear instancias EC2 (Máquinas virtuales) en dichas subredes.

Para ello deberás seguir las instrucciones detalladas en el video adjunto a la tarea:

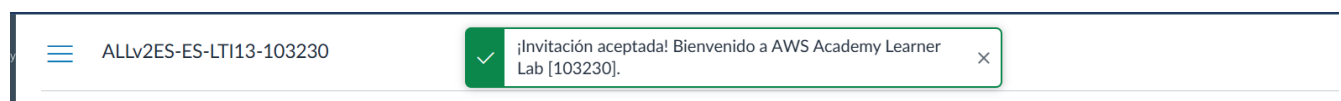
https://educantabria.sharepoint.com/:v:/s/agl_informatica_dpto/EQsDb76zkWRBnacDKl0ZqqEBsDqrHokntFHv2lyM8Y8-mQ?e=Uq9LrV

DOCUMENTACIÓN

Documenta el proceso de creación e instalación. Realiza las capturas de pantalla que consideres necesarias.

Acceso al curso y activación del laboratorio


Accedemos al link que nos facilitó el profesor, y, al entrar, nos debería decir que hemos aceptado la invitación:




Nos dirigimos a **Contenidos** y accedemos a **Lanzamiento del Laboratorio para el alumnado de AWS Academy**, para iniciar la configuración del entorno:


[Página de inicio](#)
[Contenidos](#)
[Foros de discusión](#)
[Notas](#)
[Lucid \(pizarra\)](#)


▼ Bienvenida e información general sobre el curso

 Encuesta previa al curso [Pre-Course Survey ES-ES]


 Guía del alumno del Laboratorio para el alumnado de AWS Academy

▼ Conformidad y seguridad del Laboratorio para el alumnado de AWS Academy


 Aprende a utilizar eficazmente el Laboratorio para el alumnado de Academy






 **Módulo Prueba de conocimientos**
100 puntos Puntuación mínima 70.0

▼ Laboratorio para el alumnado de AWS Academy

 **Lanzamiento del Laboratorio para el alumnado de AWS Academy**

Una vez dentro nos aparecerá sin activar. En cuanto pulsemos en Start Lab debería ponerse en amarillo, lo cual indica que se está encendiendo el laboratorio:

AWS 

 **Start Lab**  End Lab  AWS Details  Readme  Reset

Como indicador de que está encendido, nos aparecerá en color verde, y tendremos el dinero disponible (el saldo consumido y el disponible para gastar):

AWS ● Used \$0 of \$50 03:57 ▶ Start Lab ■ End Lab ⓘ AWS Details ⓘ Readme ⌂ Reset ✕

eee_k_3896689@runweb150755:~\$ ⌵ ⌶

Cloud Access Close

Obtención de claves PEM

Para obtener las claves PEM, nos dirigimos a los detalles del laboratorio (**AWS Details**) y seleccionamos la opción **Download PEM**:

▶ Start Lab ■ End Lab ⓘ AWS Details ⓘ Readme ⌂ Reset ✕

⌵ ⌶ Cloud Access Close

Cloud Access

AWS CLI: Show

Cloud Labs

Remaining session time: 03:59:54(240 minutes)

Session started at: 2024-12-04T23:35:03-0800

Session to end at: 2024-12-05T03:35:03-0800

Accumulated lab time: 00:00:00 (0 minutes)

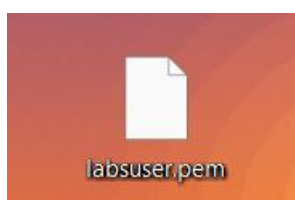
No running instance

SSH key Show Download PEM

Download PPK

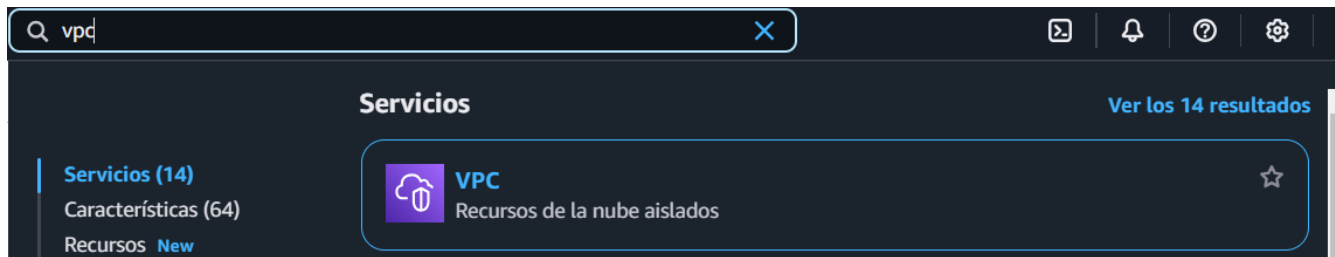
AWS SSO Download URL

En mi caso, lo he guardado en el escritorio, para tener más facilidad a la hora de encontrarlo:

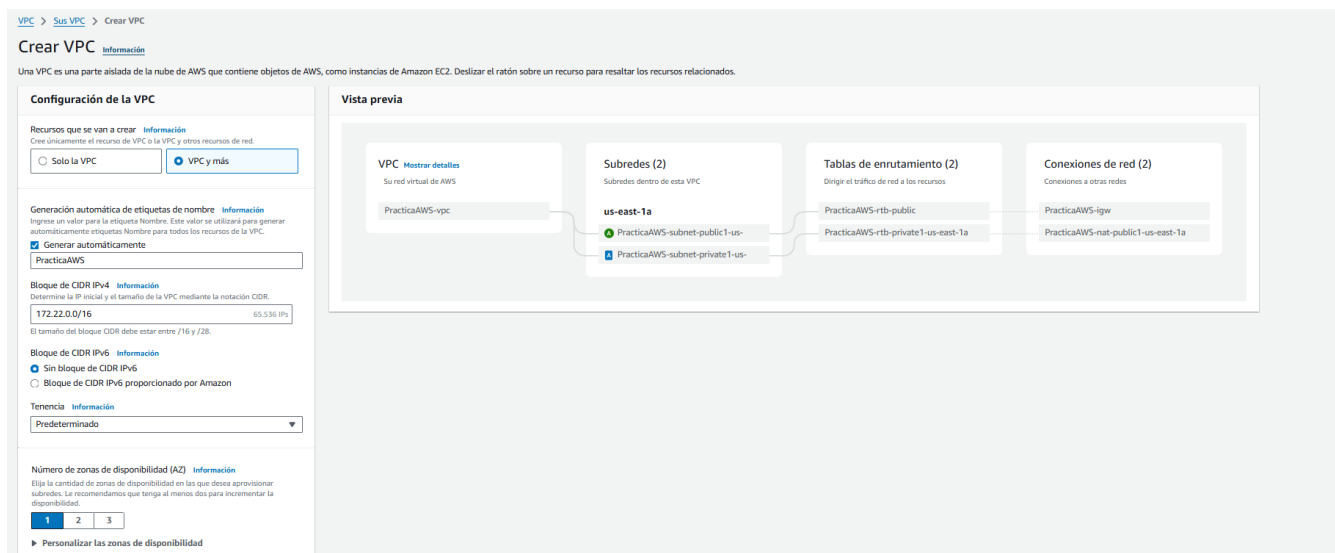
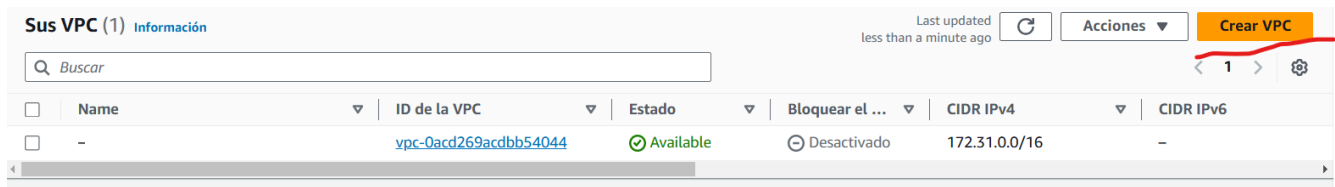


Creación y configuración de la VPC y Configuración de la red

Buscamos VPC en el configurador y le damos al servicio:



Una vez dentro, vamos a configurar el VPC con la configuración que se nos indica en el vídeo, y pulsamos en **Crear VPC**:



En este punto le indicamos la configuración de red:

► Personalizar las zonas de disponibilidad

Cantidad de subredes públicas [Información](#)
La cantidad de subredes públicas que se van a agregar a la VPC. Utilice subredes públicas para las aplicaciones web que deban ser accesibles públicamente a través de Internet.

☐ 0 ☒ 1

Cantidad de subredes privadas [Información](#)
La cantidad de subredes privadas que se van a agregar a la VPC. Utilice subredes privadas para proteger los recursos del backend que no necesitan acceso público.

☐ 0 ☒ 1 ☐ 2

▼ Personalizar bloques de CIDR de subredes

Bloque de CIDR de la subred pública en us-east-1a
 256 IPs

Bloque de CIDR de la subred privada en us-east-1a
 256 IPs

Gateways NAT (\$) [Información](#)
Elija el número de zonas de disponibilidad (AZ) en las que crear gateway NAT. Tenga en cuenta que hay un cargo por cada puertan de enlace NAT.


☐ Ninguna ☒ En 1 AZ ☐ 1 por zona de disponibilidad

Puntos de enlace de la VPC [Información](#)
Los puntos de enlace pueden ayudar a reducir los cargos de gateway NAT y mejorar la seguridad gracias a la posibilidad de acceder a S3 directamente desde la VPC. De forma predeterminada, se utiliza una política de acceso completo. Puede personalizar esta política en cualquier momento.

☒ Ninguna ☐ Gateway de S3

Opciones de DNS [Información](#)
☒ Habilitar nombres de host DNS
☒ Habilitar la resolución de DNS

► Etiquetas adicionales

Cancelar  Vista previa del código

Cuando lo tengamos revisado y configurado, lo lanzamos, y nos mostrará que todo se ha completado con éxito:

Flujo de trabajo de creación de VPC

✓ Correcto

▼ Detalles

✓ Crear VPC: [vpc-0da9a171465e19fe4](#)

✓ Habilitar nombres de host DNS

✓ Habilitar la resolución de DNS

✓ Verificar la creación de una VPC: [vpc-0da9a171465e19fe4](#)

✓ Crear subred: [subnet-053c0b0d6eaeef8329](#)

✓ Crear subred: [subnet-027907de0317a8426](#)

✓ Crear una gateway de Internet: [igw-078ca7186c5282bf3](#)

✓ Adjuntar gateway de Internet a la VPC

✓ Crear tabla de enrutamiento: [rtb-000d9b5bc8a1268b9](#)

✓ Crear ruta

✓ Asociar tabla de enrutamiento

✓ Asignar IP elástica: [eipalloc-00783ed726c4b22bf](#)

✓ Crear gateway NAT: [nat-01bfb61fdd636b99f](#)

✓ Espere a que se activen las gateways NAT

✓ Crear tabla de enrutamiento: [rtb-0f0081f5ad6cbb092](#)

✓ Crear ruta

✓ Asociar tabla de enrutamiento

✓ Verificando la creación de la tabla de enrutamiento

Ver VPC

Si le damos a ver VPC, veremos lo siguiente:

VPC > [Sus VPC](#) > [vpc-0da9a171465e19fe4](#)

vpc-0da9a171465e19fe4 / PracticaAWS-vpc

Acciones ▼

Detalles

Información

ID de la VPC

[vpc-0da9a171465e19fe4](#)

Resolución de DNS

Habilitado

ACL de red principal

[acl-0c45cb5d76043edec](#)

CIDR IPv6 (grupo de bordes de red)

-

Estado

✓ Available

Tenencia

Default

VPC predeterminada

No

Métricas de uso de direcciones de red

Desactivado

Bloquear el acceso público

☐ Desactivado

Conjunto de opciones de DHCP

[dopt-025d2c9d25560e328](#)

CIDR IPv4

172.22.0.0/16

Grupos de reglas del firewall de DNS de Route 53 Resolver

No se pudieron cargar los grupos de reglas

Nombres de host de DNS

Habilitado

Tabla de enrutamiento principal

[rtb-0c516cf617454272c](#)

Grupo IPv6

-

ID de propietario

[851725188508](#)

Mapa de recursos

CIDR

Registros de flujo

Etiquetas

Integraciones

Mapa de recursos

Información

VPC

Mostrar detalles

Su red virtual de AWS

PracticaAWS-vpc

Subredes (2)

Subredes dentro de esta VPC

us-east-1a

✓ PracticaAWS-subnet-public1-us-ea...

PracticaAWS-subnet-private1-us-e...

Tablas de enrutamiento (3)

Dirigir el tráfico de red a los recursos

rtb-0c516cf617454272c

PracticaAWS-rtb-public

PracticaAWS-rtb-private1-us-east-1a

Conexiones de red (2)

Conexiones a otras redes

PracticaAWS-igw

PracticaAWS-nat-public1-us-east-1a

Instancia EC2 de Windows (pública)

Vamos a crear la primera instancia, que es una máquina cliente de Windows:

aws

Cloud9

EC2

Buscar

[Alt+S]

Panel

Vista global de EC2

Eventos

▼ Instancias

Instancias

Tipos de instancia

Plantillas de lanzamiento

Solicitudes de spot

Savings Plans

Instancias reservadas

Alojamientos dedicados

Reservas de capacidad

▼ Imágenes

AMI

Catálogo de AMI

▼ Elastic Block Store

Volúmenes

Instantáneas

Administrador del ciclo de vida

▼ Red y seguridad

Security Groups

Direcciones IP elásticas

Grupos de ubicación

Pares de claves

Interfases de red

▼ Equilibrio de carga

Balanceadores de carga

Grupos de destino

Trust Stores

Nuevo

Recursos

EC2 Global View

Actualmente, utiliza los siguientes recursos de Amazon EC2 en la región EE.UU. Este (Norte de Virginia):

Instancias (en ejecución)	0	Balanceadores de carga	0	Capacity Reservations	0
Direcciones IP elásticas	1	Grupos de escalamiento automático	0	Grupos de seguridad	2
Grupos de ubicación	0	Hosts dedicados	0	Instancias	0
Instantáneas	0	Pares de claves	1	Volúmenes	0

Lanzar la instancia

Para comenzar, lance una instancia de Amazon EC2, que es un servidor virtual en la nube.

Lanzar la instancia

Migrar un servidor

Nota: Sus instancias se lanzarán en la región EE.UU. Este (Norte de Virginia)

Alarmas de instancia

Ver en CloudWatch

0 en alarma

0 Aceptar

0 datos insuficientes

Instancias en alarma

Eventos programados

EE.UU. Este (Norte de Virginia)

No hay eventos programados

Migrar un servidor

Utilice AWS Application Migration Service para simplificar y acelerar la migración desde una

Estado del servicio

Panel de AWS Health

Región

EE.UU. Este (Norte de Virginia)

Estado

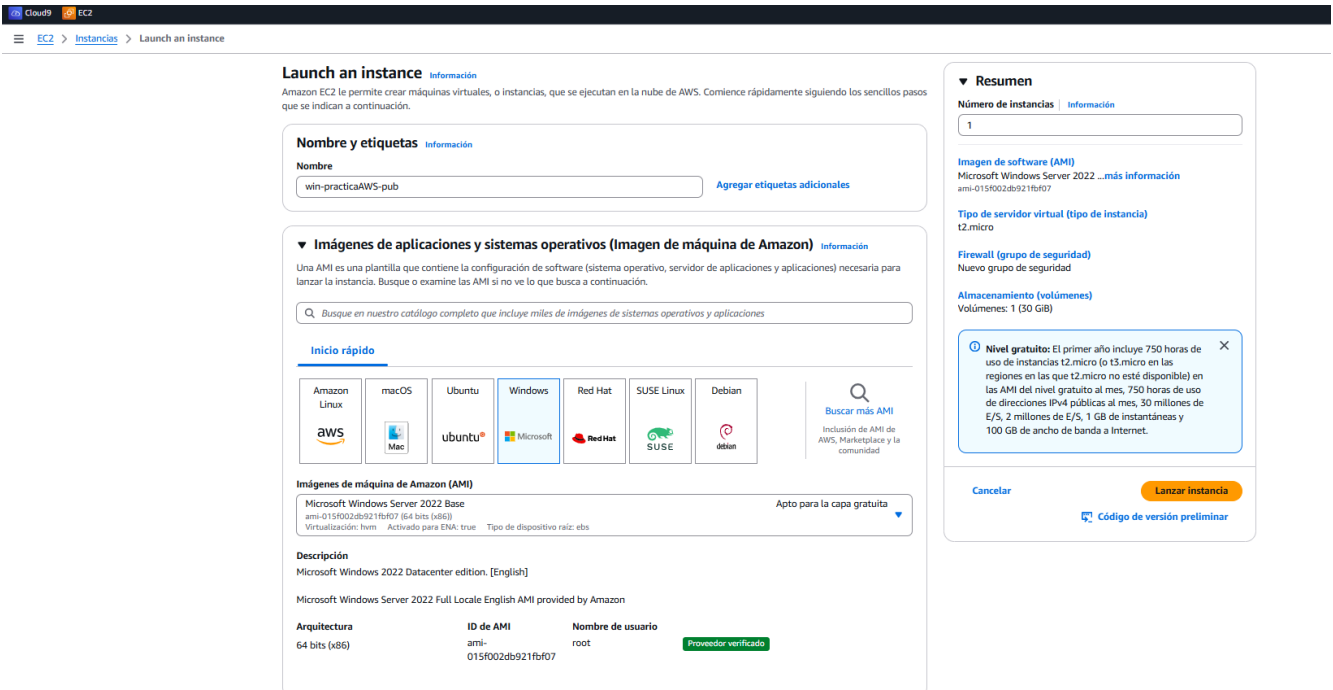
Este servicio funciona con normalidad.

Zonas

Nombre de la zona	ID de la zona
us-east-1a	use1-az2
us-east-1b	use1-az4
us-east-1c	use1-az6
us-east-1d	use1-az1
us-east-1e	use1-az3
us-east-1f	use1-az5

Habilitar zonas adicionales

Seleccionamos la máquina que queremos configurar. En nuestro caso, sería un Windows Server de 2022, ya que esta más probado:



Le indicamos el tamaño, las claves y la configuración de red que va a tener, asociándola al VPC que hemos creado previamente:

Tipo de instancia

Información | Obtener asesoramiento

Tipo de instancia

t2.micro

Familia: t2 1 vCPU 1 GiB Memoria Generación actual: true

Bajo demanda Windows base precios: 0.0162 USD por hora

Bajo demanda Ubuntu Pro base precios: 0.0134 USD por hora

Bajo demanda SUSE base precios: 0.0116 USD por hora

Bajo demanda RHEL base precios: 0.026 USD por hora

Bajo demanda Linux base precios: 0.0116 USD por hora

Apto para la capa gratuita

Todas las generaciones

Comparar tipos de instancias

Se aplican costos adicionales a las AMI con software preinstalado

Par de claves (inicio de sesión)

Información

Puede utilizar un par de claves para conectarse de forma segura a la instancia. Asegúrese de que tiene acceso al par de claves seleccionado antes de lanzar la instancia.

Nombre del par de claves - obligatorio

vockey

Crear un nuevo par de claves

Para las instancias de Windows, utilice un par de claves para descifrar la contraseña del administrador y, a continuación, utilice la contraseña descifrada para conectarse a la instancia.

Configuraciones de red

Información

VPC : obligatorio

Información

vpc-0da9a171465e19fe4 (PracticaAWS-vpc)

172.22.0.0/16

Subred

Información

subnet-053c0b0d6eaeef8329

PracticaAWS-subnet-public1-us-east-1a

VPC: vpc-0da9a171465e19fe4 Propietario: 851725188508

Zona de disponibilidad: us-east-1a Tipo de zona: Zona de disponibilidad

Direcciones IP disponibles: 250 CIDR: 172.22.1.0/24

Asignar automáticamente la IP pública

Información

Habilitar

Se aplican cargos adicionales cuando no se cumplen los límites del nivel gratuito

Creamos el grupo de seguridad, dejando todos los campos por defecto:

Se aplican cargos adicionales cuando no se cumplen los límites del nivel gratuito

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-1

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-1 created 2024-12-05T08:07:05.278Z

Reglas de grupos de seguridad de entrada

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

Eliminar

Tipo

Información

rdp

Protocolo

Información

TCP

Intervalo de puertos

Información

3389

Tipo de origen

Información

Cualquier lugar

Origen

Información

Agregue CIDR, lista de prefijos o grupo

0.0.0.0/0

Descripción - opcional

Información

por ejemplo, SSH para Admin Desktop

Las reglas con origen 0.0.0.0/0 permiten que todas las direcciones IP tengan acceso a la instancia. Le recomendamos que configure las reglas del grupo de seguridad para permitir el acceso únicamente desde direcciones IP conocidas.

X

Agregar regla del grupo de seguridad

10

El único cambio que añadiremos es la ip que va a tener:

▼ Configuración de red avanzada

Interfaz de red 1

Índice de dispositivos | [Información](#)

0

Subred | [Información](#)

subnet-053c0b0d6eaeef8329

Direcciones IP disponibles: 250

IP secundaria | [Información](#)

Seleccionar ▼

Prefijos IPv6 | [Información](#)

Seleccionar ▼

El tipo de instancia seleccionado no admite prefijos IPv6.

Tipo de interfaz | [Información](#)

Seleccionar ▼

ENA Express UDP | [Información](#)

Seleccionar ▼

El tipo de instancia seleccionado no admite ENA Express.

Agregue interfaz de red

Interfaz de red | [Información](#)

Nueva interfaz ▼

Grupos de seguridad | [Información](#)

Nuevo grupo de seguridad

Direcciones IP IPv6 | [Información](#)

Seleccionar ▼

La subred seleccionada no soporta IP de IPv6.

Asignar IP IPv6 principal | [Información](#)

Seleccionar ▼

Una dirección IPv6 principal solo es compatible con subredes compatibles con IPv6.

Índice de tarjeta de red | [Información](#)

Seleccionar ▼

El tipo de instancia seleccionado no admite varias tarjetas de red.

Tiempo de espera de seguimiento de conexiones inactivas | [Información](#)

☐ Habilitar

El tiempo de espera de seguimiento de conexión inactiva solo es compatible con las instancias de Nitro.

Descripción | [Información](#)

IP principal | [Información](#)

172.22.1.100

Prefijos IPv4 | [Información](#)

Seleccionar ▼

El tipo de instancia seleccionado no admite prefijos IPv4.

Eliminar cuando termine | [Información](#)

Seleccionar ▼

ENA Express | [Información](#)

Seleccionar ▼

El tipo de instancia seleccionado no admite ENA Express.

Aquí, podemos visualizar el resumen de lo que queremos instanciar:

▼ Resumen

Número de instancias | [Información](#)


1


Imagen de software (AMI)
Microsoft Windows Server 2022 ...[más información](#)
ami-015f002db921fbf07

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


Firewall (grupo de seguridad)
Nuevo grupo de seguridad

Almacenamiento (volúmenes)
Volúmenes: 1 (30 GiB)


 **Nivel gratuito:** El primer año incluye 750 horas de uso de instancias t2.micro (o t3.micro en las regiones en las que t2.micro no esté disponible) en las AMI del nivel gratuito al mes, 750 horas de uso de direcciones IPv4 públicas al mes, 30 millones de E/S, 2 millones de E/S, 1 GB de instantáneas y 100 GB de ancho de banda a Internet.



[Cancelar](#) [Lanzar instancia](#)





 Código de versión preliminar

En este punto, con todo correcto, ya tendremos la instancia de EC2 creada y lista:

 **Correcto**

El lanzamiento de la instancia se inició correctamente ([i-06089c7690c3ea453](#))

▼ Registro de lanzamiento

Inicialización de solicitudes	 Se realizó correctamente
Creación de grupos de seguridad	 Se realizó correctamente
Creación de reglas de grupo de seguridad	 Se realizó correctamente
Inicio del lanzamiento	 Se realizó correctamente

En este punto podemos ver que se ha configurado correctamente:

Instancias (1) Información										
<input type="text" value="Buscar instancia por atributo o etiqueta (case-sensitive)"/>				Todos los ...		<div> <div>Última actualización</div> <div>Hace less than a minute</div> </div> <div> Conectar Estado de la instancia Acciones Lanzar instancias </div>				
Name	ID de la instancia	Estado de la I...	Tipo de inst...	Comprobación de	Estado de la al	Zona de dispon...	DNS de IPv4 pública	Dirección IP...	IP elástica	Direcciones I...
win-practicaA...	i-06089c7690c3ea453	En ejecución	t2.micro	Iniciando	Ver alarmas +	us-east-1a	ec2-34-207-85-69.com...	34.207.85.69	-	-
										Monitoreo
										laun

Instancia EC2 de Ubuntu (pública)

Vamos a crear la segunda instancia. En este caso, será un Ubuntu con la siguiente configuración:

Launch an instance Información

Amazon EC2 le permite crear máquinas virtuales, o instancias, que se ejecutan en la nube de AWS. Comience rápidamente siguiendo los sencillos pasos que se indican a continuación.

Nombre y etiquetas Información

Nombre

[Agregar etiquetas adicionales](#)

▼ Imágenes de aplicaciones y sistemas operativos (Imagen de máquina de Amazon) Información

Una AMI es una plantilla que contiene la configuración de software (sistema operativo, servidor de aplicaciones y aplicaciones) necesaria para lanzar la instancia. Busque o examine las AMI si no ve lo que busca a continuación.

Recientes

Inicio rápido



Buscar más AMI

Inclusión de AMI de AWS, Marketplace y la comunidad

Imágenes de máquina de Amazon (AMI)

Ubuntu Server 22.04 LTS (HVM) with SQL Server 2022 Standard
ami-051027b61544b3d11 (64 bits (x86))
Virtualización: hvm Activado para ENA: true Tipo de dispositivo raíz: ebs

Descripción

Microsoft SQL Server 2022 Standard edition on Ubuntu Server 22.04 LTS.

Canonical, Ubuntu, 24.04, amd64 noble image

Arquitectura

64 bits (x86)

ID de AMI

ami-0866a3c8686eaeaba

Nombre de usuario

ubuntu



Proveedor verificado

La configuración básica es la misma que la realizada anteriormente, dado que las dos instancias son públicas y usan las mismas claves para el acceso:

▼ Tipo de instancia [Información](#) | [Obtener asesoramiento](#)

Tipo de instancia

t2.micro

Familia: t2 1 vCPU 1 GiB Memoria Generación actual: true

Bajo demanda Windows base precios: 0.0162 USD por hora

Bajo demanda Ubuntu Pro base precios: 0.0134 USD por hora

Bajo demanda SUSE base precios: 0.0116 USD por hora

Bajo demanda RHEL base precios: 0.026 USD por hora Bajo demanda Linux base precios: 0.0116 USD por hora

Apto para la capa gratuita

☐ Todas las generaciones

[Comparar tipos de instancias](#)

Se aplican costos adicionales a las AMI con software preinstalado

▼ Par de claves (inicio de sesión) [Información](#)

Puede utilizar un par de claves para conectarse de forma segura a la instancia. Asegúrese de que tiene acceso al par de claves seleccionado antes de lanzar la instancia.

Nombre del par de claves - obligatorio

vockey

↕

↻

[Crear un nuevo par de claves](#)

▼ Configuraciones de red [Información](#)

VPC : obligatorio | [Información](#)

vpc-0da9a171465e19fe4 (PracticaAWS-vpc)

172.22.0.0/16

↻

Subred | [Información](#)

subnet-053c0b0d6eaeef8329

PracticaAWS-subnet-public1-us-east-1a

VPC: vpc-0da9a171465e19fe4 Propietario: 851725188508

Zona de disponibilidad: us-east-1a Tipo de zona: Zona de disponibilidad

Direcciones IP disponibles: 249 CIDR: 172.22.1.0/24

↻ [Crear nueva subred](#)

Asignar automáticamente la IP pública | [Información](#)

Habilitar

Se aplican cargos adicionales cuando no se cumplen los límites del [nivel gratuito](#)

Crearemos un grupo de seguridad y añadiremos la regla de entrada de ssh (puerto 22) para el acceso a dicha máquina:

☒ Crear grupo de seguridad

☐ Seleccionar un grupo de seguridad existente

Nombre del grupo de seguridad - *obligatorio*

sg_ubuntu_pub

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 2024-12-05T08:18:59.231Z

Reglas de grupos de seguridad de entrada

▼ Regla del grupo de seguridad 1 (TCP, 22, 0.0.0.0/0)

Eliminar

Tipo | [Información](#)

ssh ▼

Protocolo | [Información](#)

TCP

Intervalo de puertos | [Información](#)

22

Tipo de origen | [Información](#)

Cualquier lugar ▼

Origen | [Información](#)

Q Agregar CIDR, lista de prefijos o grupo

0.0.0.0/0 ✕

Descripción - *opcional* | [Información](#)

por ejemplo, SSH para Admin Desktop

⚠ Las reglas con origen 0.0.0.0/0 permiten que todas las direcciones IP tengan acceso a la instancia. Le recomendamos que configure las reglas del grupo de seguridad para permitir el acceso únicamente desde direcciones IP conocidas. ✕

Agregar regla del grupo de seguridad

► Configuración de red avanzada

▼ Configurar almacenamiento | [Información](#) [Avanzado](#)

1x 8 GiB gp3 ▼ Volumen raíz (Sin cifrar)


i Los clientes que cumplan los requisitos de la capa gratuita pueden obtener hasta 30 GB de almacenamiento magnético o de uso general (SSD) de EBS ✕

15

Le añadiremos los comandos que queramos que se ejecuten al crearla, para preparar la máquina. En mi caso, he añadido los siguientes:

Datos de usuario - *opcional* | [Información](#)

Cargue un archivo con los datos de usuario o escríbalos en el campo.

 **Elegir archivo**

```
#!/bin/bash
sudo apt update -y
sudo apt upgrade -y
sudo apt install -y apache2
# sudo apt install -y mariadb-server
#sudo apt install -y php php-mysql
sudo systemctl restart apache2
```

☐ Los datos de usuario ya han sido codificados en base64

De nuevo, nos aparece el resumen de la máquina que vamos a instanciar:

▼ Resumen

Número de instancias

Información

1

Imagen de software (AMI)

Canonical, Ubuntu, 24.04, amd64...más información

ami-0866a3c8686eaeeba

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: El primer año incluye 750 horas de uso de instancias t2.micro (o t3.micro en las regiones en las que t2.micro no esté disponible) en las AMI del nivel gratuito al mes, 750 horas de uso de direcciones IPv4 públicas al mes, 30 millones de E/S, 2 millones de E/S, 1 GB de instantáneas y 100 GB de ancho de banda a Internet.

Cancelar

Lanzar instancia

🔗 Código de versión preliminar

Como podemos ver, se ha lanzado correctamente:

✔ Correcto

El lanzamiento de la instancia se inició correctamente (i-087b16f40285c5da1)

▼ Registro de lanzamiento

Inicialización de solicitudes

Creación de grupos de seguridad

Creación de reglas de grupo de seguridad

Inicio del lanzamiento

✔ Se realizó correctamente

✔ Se realizó correctamente

✔ Se realizó correctamente

✔ Se realizó correctamente

Aquí podemos ver las dos instancias creadas correctamente:

Instancias (2) Información

Última actualización
Hace less than a minute

Conectar

Estado de la in

🔍 Buscar instancia por atributo o etiqueta (case-sensitive)

Todos los ... ▼

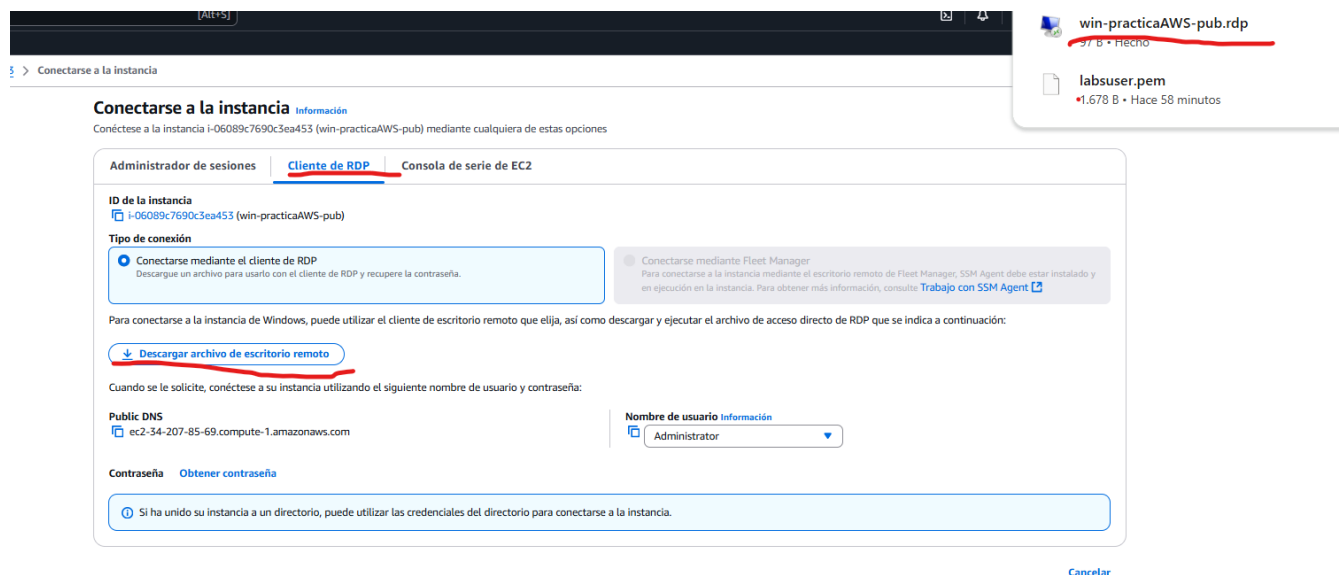
<input type="checkbox"/>	Name	ID de la instancia	Estado de la i...	Tipo de inst...	Comprobación de	Estado de la al.	Zona de dispon...	DNS de IPv4 pública	Dirección IP...	IP elástico
<input type="checkbox"/>	win-practicaA...	i-06089c7690c3ea453	✔ En ejecución	t2.micro	✔ 2/2 comprobaci...	Ver alarmas +	us-east-1a	ec2-34-207-85-69.com...	34.207.85.69	-
<input type="checkbox"/>	ubu-practicaA...	i-087b16f40285c5da1	✔ En ejecución	t2.micro	⌚ Inicializando	Ver alarmas +	us-east-1a	ec2-54-204-75-210.co...	54.204.75.210	-

Conexión a la Instancia de Windows

Primero de todo, desde el panel de la instancia EC2 en AWS, seleccionamos la opción **Conectar** para acceder a las opciones de conexión remota.



En este punto, seleccionamos **Cliente de RDP**, y pulsamos en **descargar archivo de escritorio remoto**. Como vemos, se nos descargará nuestro archivo con extensión .rdp



Seleccionamos la opción para descifrar la contraseña, introduciendo las claves .pem que descargamos previamente.

Obtener la contraseña de Windows Información

Utilice la clave privada para recuperar y descifrar la contraseña de administrador de Windows inicial correspondiente a esta instancia.

ID de la instancia
i-06089c7690c3ea453 (win-practicaAWS-pub)

Par de claves asociado a esta instancia
vockey

Clave privada
Cargue el archivo de la clave privada o copie y pegue su contenido en el campo que aparece a continuación.

[Cargar archivo de clave privada](#)

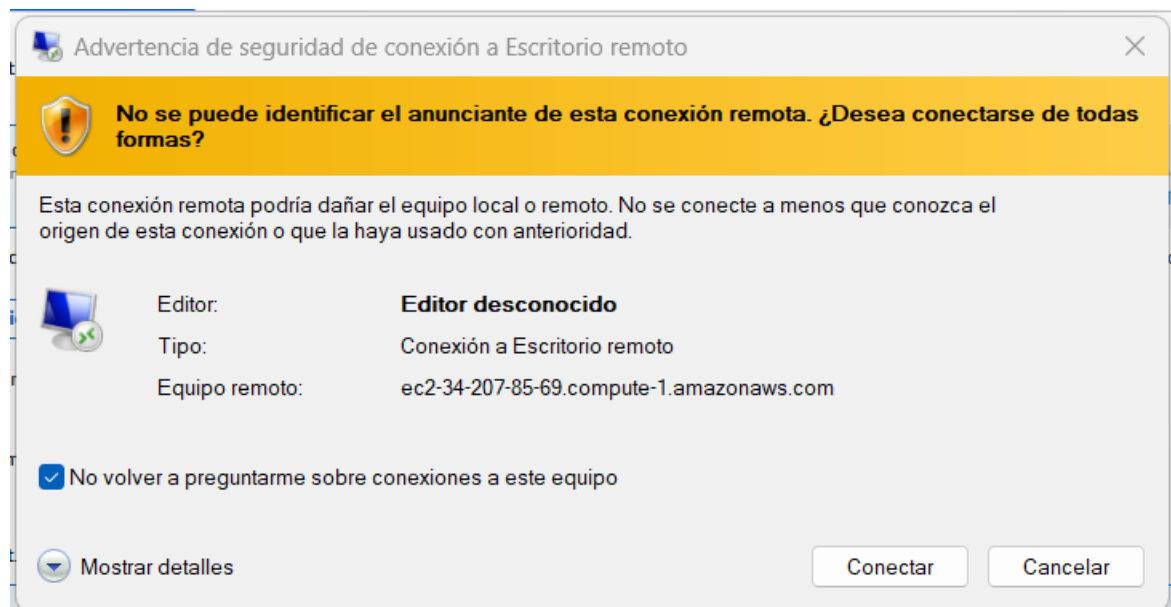
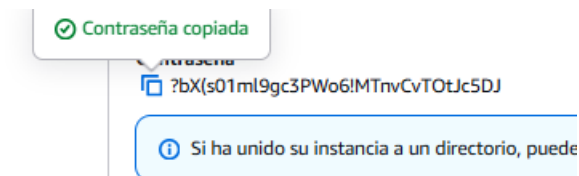
labsuser.pem
1.678KB

Contenido de la clave privada: *opcional*

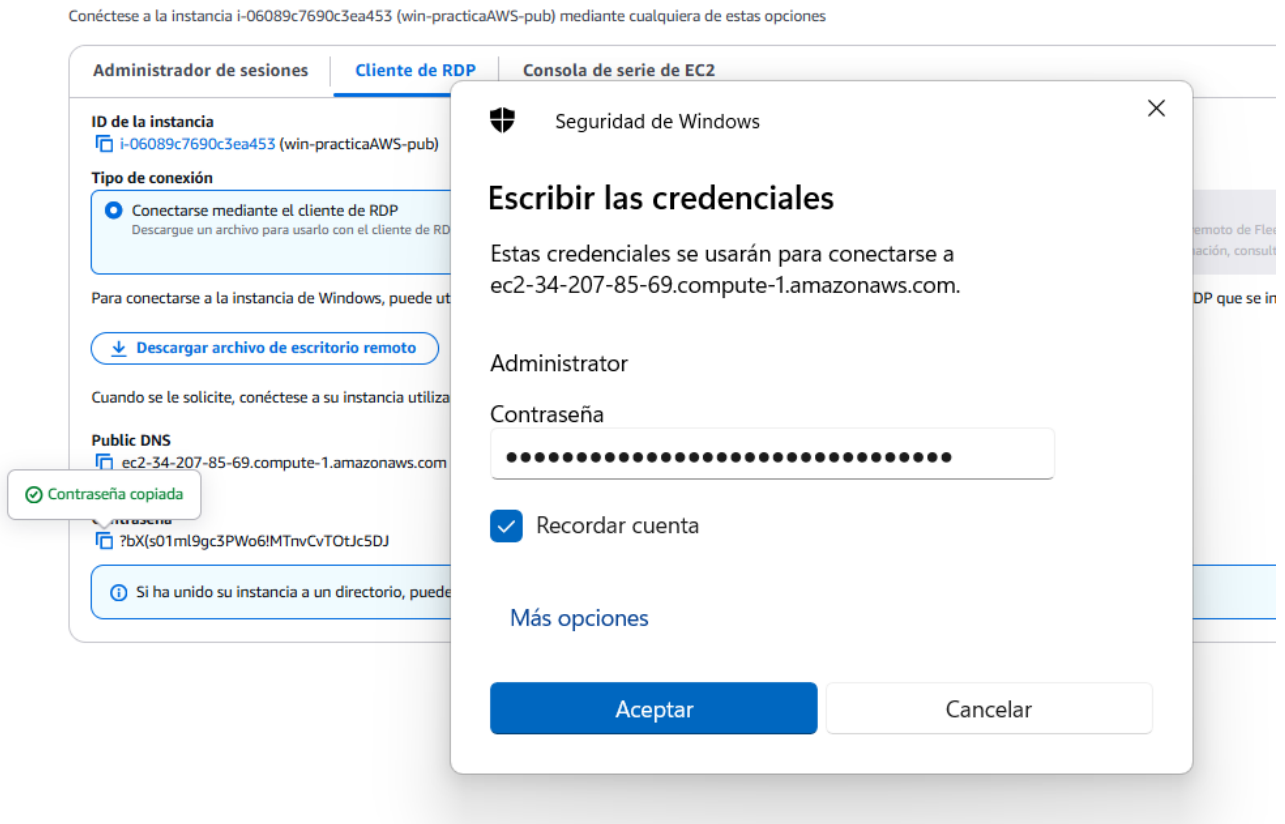
```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAxuxc+al1q4LUUvMunYIGIT/T9gu46rA6p1qKNVgpTp8BzRS
+tCCqdWl4qoSi5j9TLehlWmncZOCdEutazlNjd9rOoLylo7mBN/qQyWgSv5eA
1gVEFJaeFfMj6D97EDJCBK+kfx2TKUF6q6SsBaPCBWS13GiNgLJxhhl+8gAj
ZkgND3/82iXOhXNq3hAI24Up/Egz61HstFdrWeOwhzC8jquw3AV4EerSOB+Kwia/
Yo7F054GiziewmkHuwLk0GhG+oKwR6Burumwt97d58ef3l8Sk7dyMvhTWevsbTU
buFXN51uk0G0gNi61Z+RQvd1uevXvxj6JgGKCQIDAQABAoIBAFz5Rm9uM9BI4slu
ZRzv8/qltZf0+91vBqHhlyekq3ouYwxh+VK/OAL3Cfae9PIIJSVFQqGZ8yiqX5m
-----
```

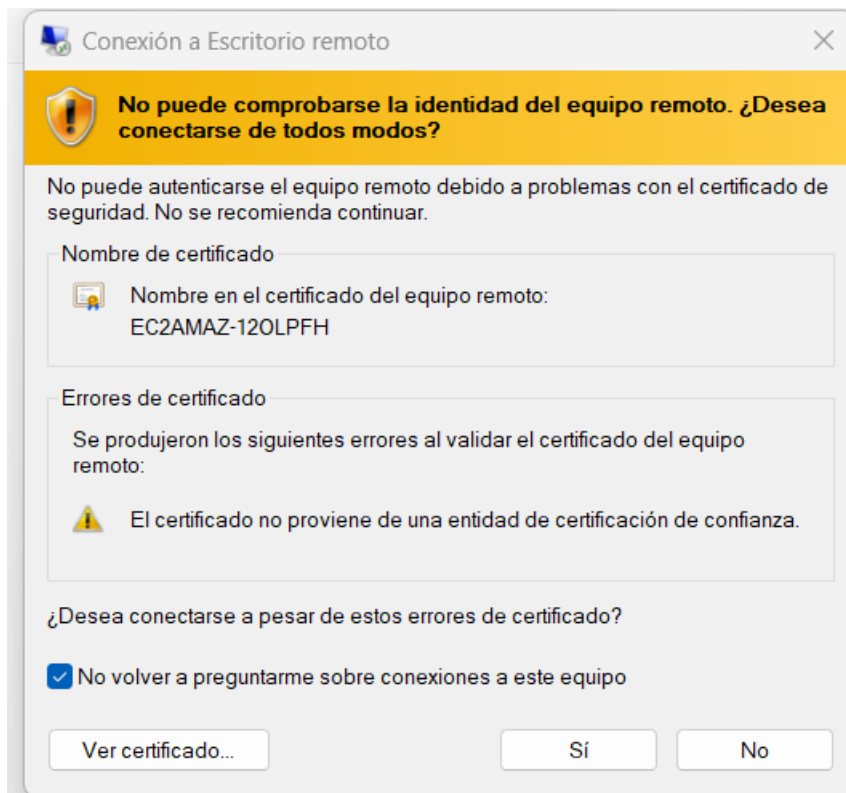
[Cancelar](#) [Descifrar contraseña](#)

Copiamos la contraseña obtenida, y la utilizamos para autenticar en la conexión de escritorio remoto.

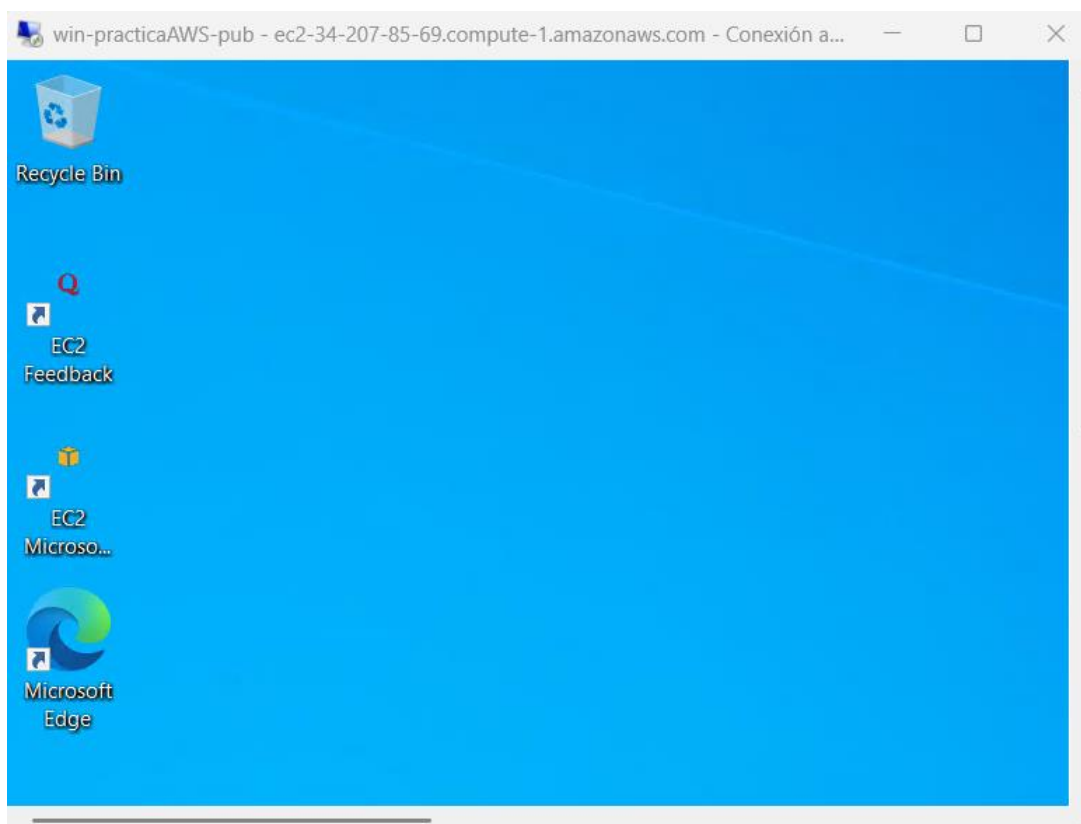


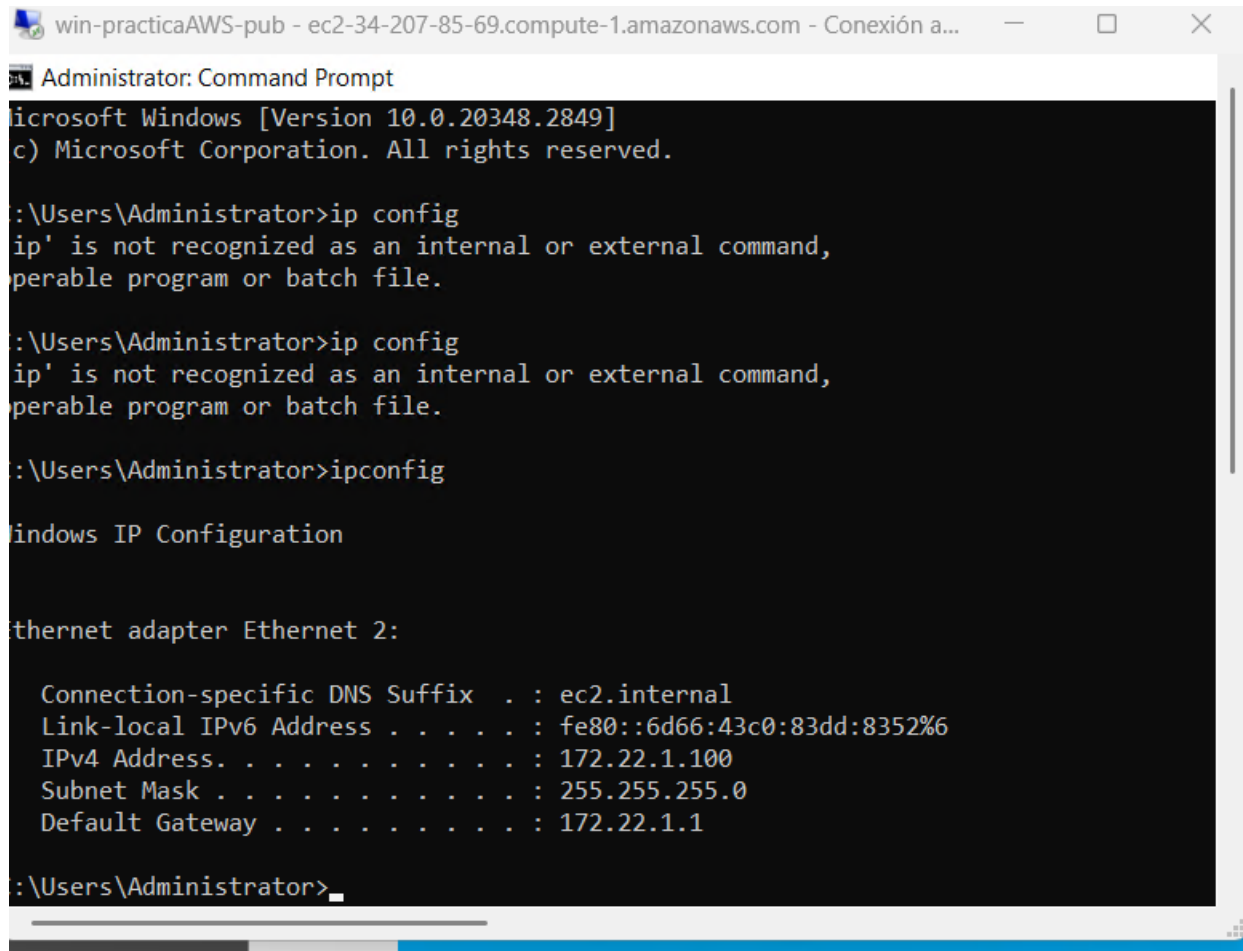
Cuando nos pida las credenciales, introducimos la contraseña que hemos copiado previamente:





Al ingresar las credenciales correctas, accedemos al escritorio del Windows Server, confirmando que la conexión fue exitosa





The screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt". The window displays the output of the 'ipconfig' command. The text is as follows:

```
Microsoft Windows [Version 10.0.20348.2849]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ip config

ip' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator>ip config

ip' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator>ipconfig

Windows IP Configuration

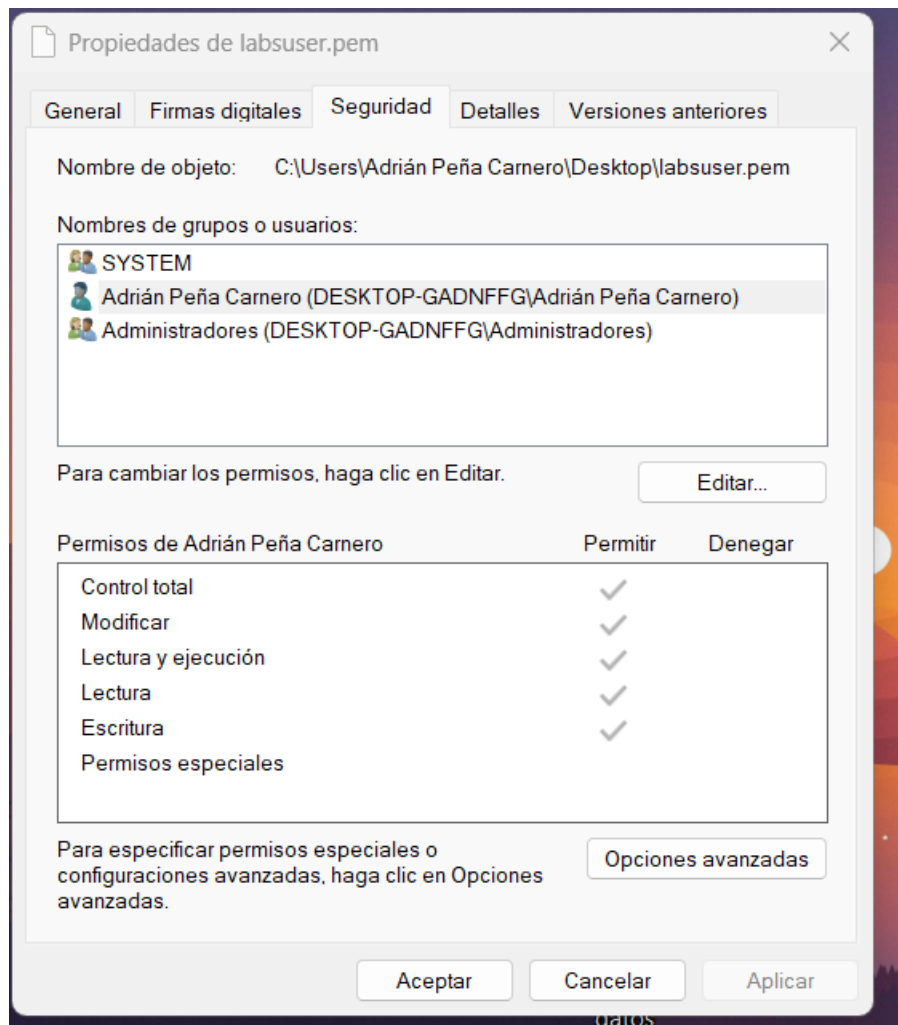
Ethernet adapter Ethernet 2:

    Connection-specific DNS Suffix  . : ec2.internal
    Link-local IPv6 Address . . . . . : fe80::6d66:43c0:83dd:8352%6
    IPv4 Address. . . . . : 172.22.1.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.22.1.1

C:\Users\Administrator>
```

Web de Apache y personalizada

¡IMPORTANTE! Si por algún motivo no os deja conectaros por tema de permisos, simplemente cambiad los permisos del archivo .PEM y solo habilitaros todos los permisos a vosotros.



Una vez no tenemos problemas nos vamos a conectar a la instancia de Ubuntu con el siguiente comando: `ssh -i "vockey.pem" ubuntu@<dirección IP o dominio de la instancia>`. En mi caso, será `ssh -i "vockey.pem" ubuntu@ec2-34-230-71-56.compute-1.amazonaws.com`

```

ubuntu@ip-172-22-1-209: ~
PS C:\Users\Usuario\OneDrive\Escritorio> ssh -i "vockey.pem" ubuntu@ec2-34-230-71-56.compute-1.amazonaws.com
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-1019-aws x86_64)

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

System information as of Thu Dec  5 13:43:57 UTC 2024

System load:  0.0          Processes:            107
Usage of /:   31.1% of 6.71GB   Users logged in:    0
Memory usage: 20%          IPv4 address for enx0: 172.22.1.209
Swap usage:   0%

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

Last login: Thu Dec  5 13:26:40 2024 from 18.206.107.27
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-22-1-209:~$ pwd
/home/ubuntu
ubuntu@ip-172-22-1-209:~$ |

```

Una vez dentro, vamos a comprobar si el servicio de apache esta activo y en ejecución con el comando **sudo systemctl status apache2**. Como vemos, mi servidor web sí está funcionando correctamente:

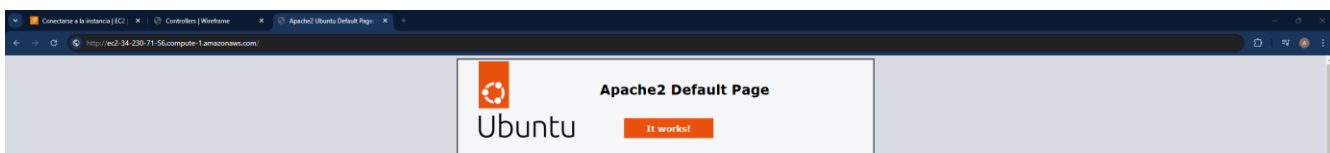
```

ubuntu@ip-172-22-1-209:~$ service apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: enabled)
   Active: active (running) since Thu 2024-12-05 13:36:21 UTC; 52min ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 498 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
  Main PID: 529 (apache2)
    Tasks: 55 (limit: 1130)
   Memory: 8.5M (peak: 8.7M)
      CPU: 210ms
   CGroup: /system.slice/apache2.service
           └─529 /usr/sbin/apache2 -k start
             └─530 /usr/sbin/apache2 -k start
               └─531 /usr/sbin/apache2 -k start

Dec 05 13:36:21 ip-172-22-1-209 systemd[1]: Starting apache2.service - The Apache HTTP Server...
Dec 05 13:36:21 ip-172-22-1-209 systemd[1]: Started apache2.service - The Apache HTTP Server.
ubuntu@ip-172-22-1-209:~$ |

```

Desde un navegador del propio ordenador vamos a introducir el nombre de dominio de AWS, lo cual nos debería mostrar la interfaz predeterminada de Apache2:

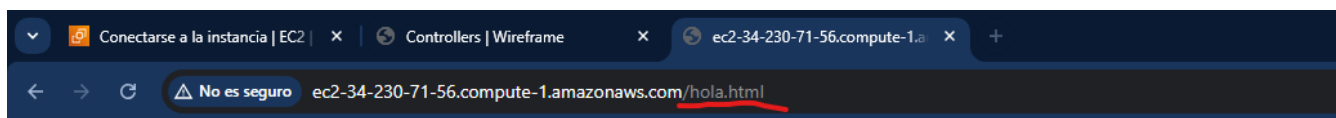


Una vez dentro, nos dirigiremos a la siguiente ruta utilizando el comando `cd`, y crearemos un fichero `html` utilizando un editor de texto (en mi caso, `nano`):

```
Dec 05 13:36:21 ip-172-22-1-209 systemd[1]: Started apache2.service
ubuntu@ip-172-22-1-209:~$ cd /var/www/html/
ubuntu@ip-172-22-1-209:/var/www/html$ sudo nano hola.html
```

```
GNU nano 7.2 hola.html
<html>
<h1>que guapos y guapas sois todos y todas </h1>
```

Cuando lo hayamos añadido, al enlazarlo a la ruta, podremos ver el `html` que acabamos de crear:



que guapos y guapas sois todos y todas

Instancia EC2 de Ubuntu (privada) y Creación de la base de datos

Vamos a crear ahora una instancia de Ubuntu privada, a la que solo tendrá acceso el cliente Windows.

Lo primero, vamos a lanzar una instancia llamada “ubu-practicaAWS-privado”, seleccionando Ubuntu Server 22.04 LTS como sistema operativo de la instancia y eligiendo la arquitectura de 64 bits (x86):

Launch an instance [Información](#)

Amazon EC2 le permite crear máquinas virtuales, o instancias, que se ejecutan en la nube de AWS. Comience rápidamente siguiendo los sencillos pasos que se indican a continuación.

Nombre y etiquetas [Información](#)

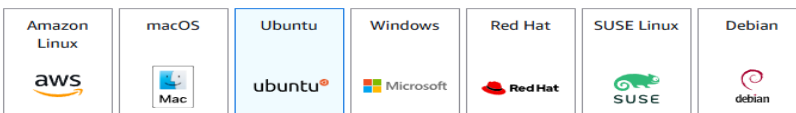
Nombre

ubu-practicaAWS-privado

[Agregar etiquetas adicionales](#)**▼ Imágenes de aplicaciones y sistemas operativos (Imagen de máquina de Amazon)** [Información](#)

Una AMI es una plantilla que contiene la configuración de software (sistema operativo, servidor de aplicaciones y aplicaciones) necesaria para lanzar la instancia. Busque o examine las AMI si no ve lo que busca a continuación.

Recientes

Inicio rápido

[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-005fc0f236362e99f (64 bits (x86)) / ami-07ee04759daf109de (64 bits (Arm))
Virtualización: hvm Activado para ENA: true Tipo de dispositivo raíz: ebs

Apto para la capa gratuita

Descripción

Ubuntu Server 22.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).

Canonical, Ubuntu, 22.04 LTS, amd64 jammy image build on 2024-09-27

Arquitectura

64 bits (x86)

ID de AMI

ami-005fc0f236362e99f

Nombre de usuario ⓘ

ubuntu

Proveedor verificado

Seleccionamos el tipo de instancia la más pequeña, ya que con **1GiB** de memoria es suficiente y consume menos, y le asignaremos el par de clave **vockey** para el acceso:

▼ Tipo de instancia [Información](#) | [Obtener asesoramiento](#)**Tipo de instancia****t2.micro**

Familia: t2 1 vCPU 1 GiB Memoria Generación actual: true

Apto para la capa gratuita

Bajo demanda Windows base precios: 0.0162 USD por hora Bajo demanda Ubuntu Pro base precios: 0.0134 USD por hora

Bajo demanda SUSE base precios: 0.0116 USD por hora Bajo demanda RHEL base precios: 0.026 USD por hora

Bajo demanda Linux base precios: 0.0116 USD por hora

☐ Todas las generaciones[Comparar tipos de instancias](#)[Se aplican costos adicionales a las AMI con software preinstalado](#)**▼ Par de claves (inicio de sesión)** [Información](#)

Puede utilizar un par de claves para conectarse de forma segura a la instancia. Asegúrese de que tiene acceso al par de claves seleccionado antes de lanzar la instancia.

Nombre del par de claves - obligatorio

vockey

[Crear un nuevo par de claves](#)

Enlazamos el VPC que habíamos creado previamente. En este caso, no habilitaremos la asignación automática de la IP pública, ya que no nos sería útil. Además, creamos un grupo de seguridad por defecto para SSH:

▼ Configuraciones de red [Información](#)

VPC : obligatorio | [Información](#)

vpc-0af3a9f91707de809 (PracticaAWS-vpc)
172.22.0.0/16

Subred | [Información](#)

subnet-07eb74099cfceafc6 PracticaAWS-subnet-private1-us-east-1a
VPC: vpc-0af3a9f91707de809 Propietario: 851725188508 Zona de disponibilidad: us-east-1a
Tipo de zona: Zona de disponibilidad Direcciones IP disponibles: 251 CIDR: 172.22.2.0/24

Asignar automáticamente la IP pública | [Información](#)

Desactivar

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 2024-12-05T14:35:13.572Z

Reglas de grupos de seguridad de entrada

▼ Regla del grupo de seguridad 1 (TCP, 22, 0.0.0.0/0) Eliminar

Tipo | [Información](#) **Protocolo** | [Información](#) **Intervalo de puertos** | [Información](#)

ssh TCP 22

Tipo de origen | [Información](#) **Origen** | [Información](#) **Descripción - opcional** | [Información](#)

Cualquier lugar

Las reglas con origen 0.0.0.0/0 permiten que todas las direcciones IP tengan acceso a la instancia. Le recomendamos que configure las reglas del grupo de seguridad para permitir el acceso únicamente desde direcciones IP conocidas.

Asignamos la IP principal que tendrá la máquina y dejamos el almacenamiento predeterminado que proporciona AWS:

▼ Configuración de red avanzada

Interfaz de red 1

Índice de dispositivos | Información

0

Subred | Información

subnet-07eb74099cfceafc6

Direcciones IP disponibles: 251

IP secundaria | Información

Seleccionar

Prefijos IPv6 | Información

Seleccionar

El tipo de instancia seleccionado no admite prefijos IPv6.

Tipo de interfaz | Información

Seleccionar

ENA Express UDP | Información

Seleccionar

El tipo de instancia seleccionado no admite ENA Express.

Agregue interfaz de red

Interfaz de red | Información

Nueva interfaz

Grupos de seguridad | Información

Nuevo grupo de seguridad

Direcciones IP IPv6 | Información

Seleccionar

La subred seleccionada no soporta IP de IPv6.

Asignar IP IPv6 principal | Información

Seleccionar

Una dirección IPv6 principal solo es compatible con subredes compatibles con IPv6.

Índice de tarjeta de red | Información

Seleccionar

El tipo de instancia seleccionado no admite varias tarjetas de red.

Tiempo de espera de seguimiento de conexiones inactivas | Información

☐ Habilitar

El tiempo de espera de seguimiento de conexión inactiva solo es compatible con las instancias de Nitro.

Descripción | Información

IP principal | Información

172.22.2.200

Prefijos IPv4 | Información

Seleccionar

El tipo de instancia seleccionado no admite prefijos IPv4.

Eliminar cuando termine | Información

Seleccionar

ENA Express | Información

Seleccionar

El tipo de instancia seleccionado no admite ENA Express.

▼ Configurar almacenamiento | Información

Avanzado

1x 8 GiB gp2 Volumen raíz (Sin cifrar)

Aquí tendríamos un resumen de la instancia que acabamos de crear:

▼ Resumen

Número de instancias | [Información](#)


1


Imagen de software (AMI)
Canonical, Ubuntu, 22.04 LTS, ...[más información](#)
ami-005fc0f236362e99f

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:** El primer año incluye 750 horas de uso de instancias t2.micro (o t3.micro en las regiones en las que t2.micro no esté disponible) en las AMI del nivel gratuito al mes, 750 horas de uso de direcciones IPv4 públicas al mes, 30 millones de E/S, 2 millones de E/S, 1 GB de instantáneas y 100 GB de ancho de banda a Internet.



[Cancelar](#)

Lanzar instancia

 [Código de versión preliminar](#)

Aquí le añadiremos los comandos que queremos que se apliquen al crear la instancia:

Datos de usuario - *opcional* | Información

Cargue un archivo con los datos de usuario o escríbalos en el campo.

⬆ Elegir archivo

```
sudo apt update -y  
sudo apt upgrade -y  
sudo apt install -y mariadb-server  
sudo systemctl restart mariadb
```

Aquí añadiremos la base de datos que queremos, especificando la IP desde la que se podrá acceder. Si queremos hacerlo de manera más profesional, sería ideal permitir el acceso únicamente a las instancias creadas o a la máquina que sabemos que necesita acceder, configurando su IP. Esto ayudará a evitar accesos no autorizados.

(Realmente, lo que estamos haciendo es habilitar una regla y abrir el puerto necesario para permitir el acceso a MySQL.)

MYSQL/Aurora

TCP

3306

Person...

Q 172.22.1.0/24

×

solo desde la red publica

Eliminar

172.22.1.0/24

×

Una vez con todo configurado lanzaremos la instancia y podremos ver que se ha creado correctamente:

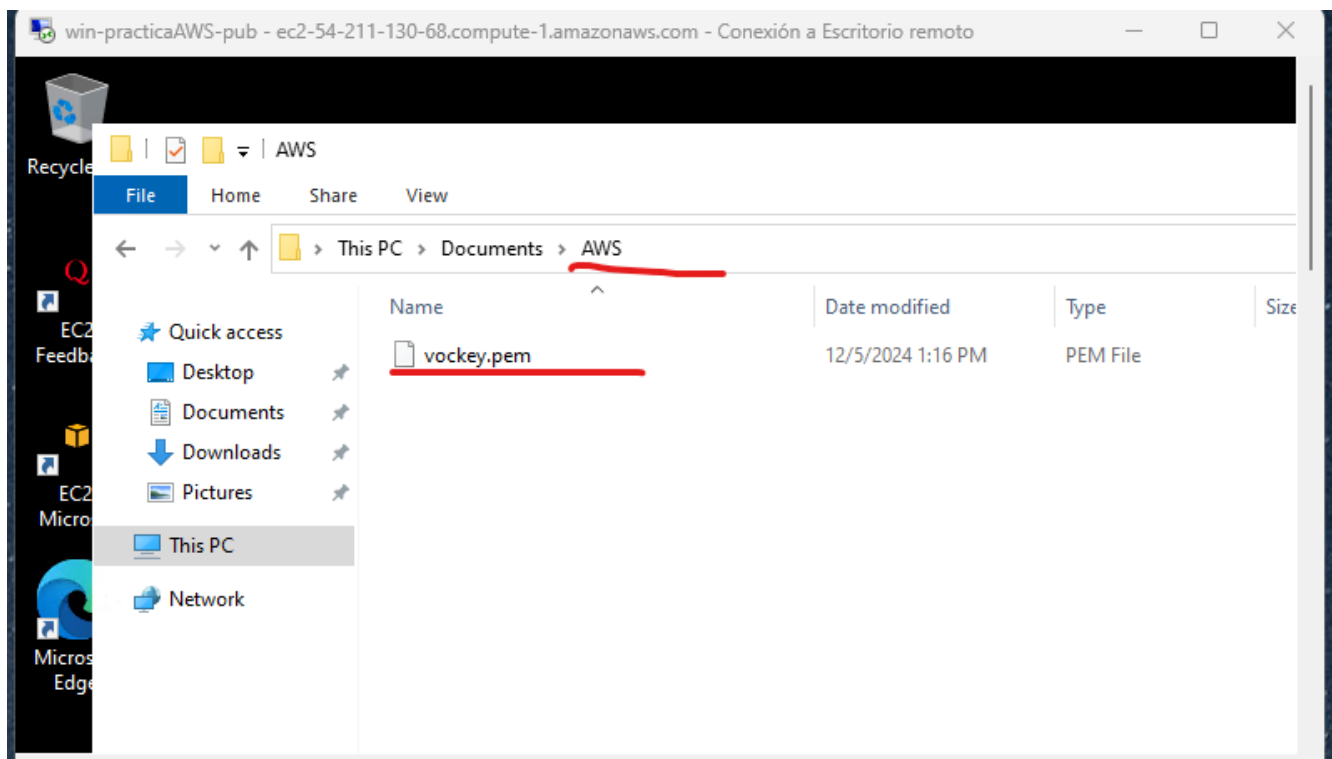
✔ **Correcto**
El lanzamiento de la instancia se inició correctamente (i-0b078fb8d73de70fe)

▼ Registro de lanzamiento

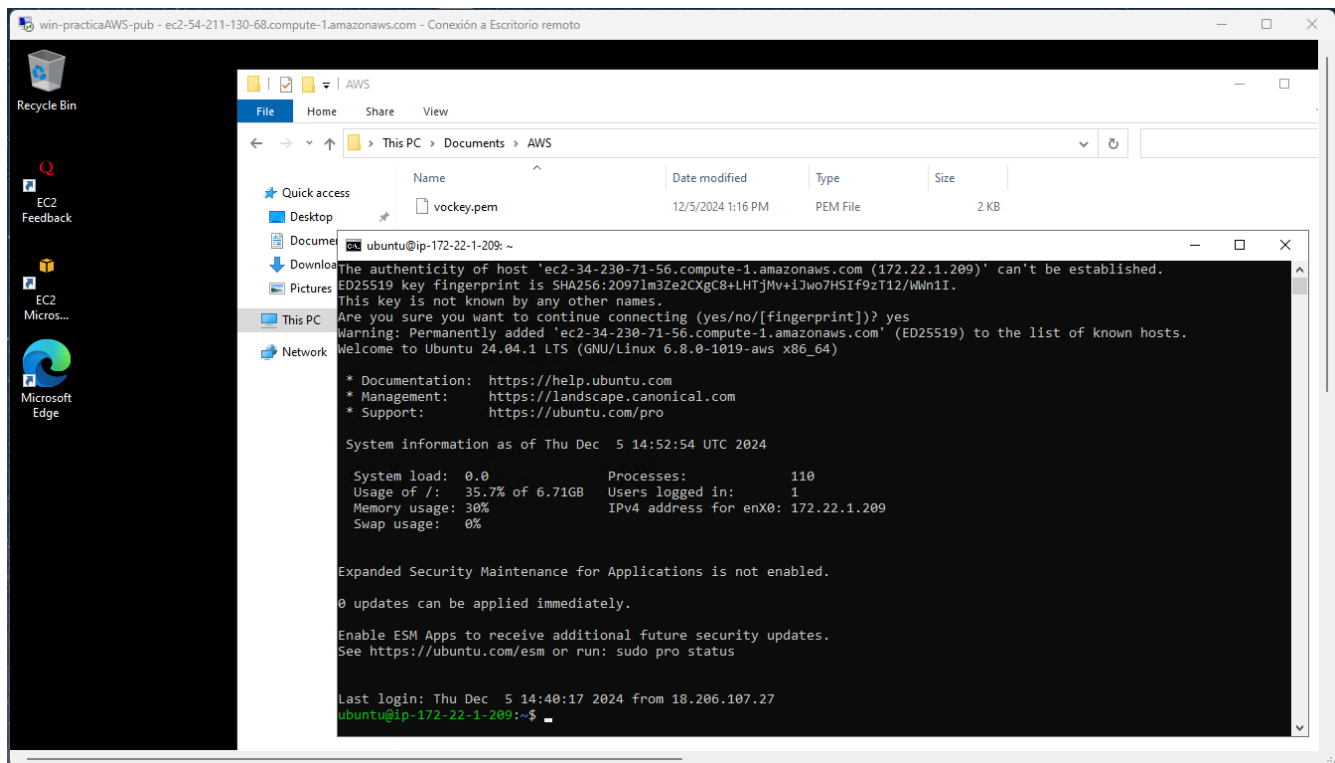
Inicialización de solicitudes	✔ Se realizó correctamente
Creación de grupos de seguridad	✔ Se realizó correctamente
Creación de reglas de grupo de seguridad	✔ Se realizó correctamente
Inicio del lanzamiento	✔ Se realizó correctamente

Acceso desde el cliente a el servidor privado + pruebas

Crearemos en documentos una carpeta AWS y le pasaremos las claves **vockey.pem** para poder acceder a el servidor:

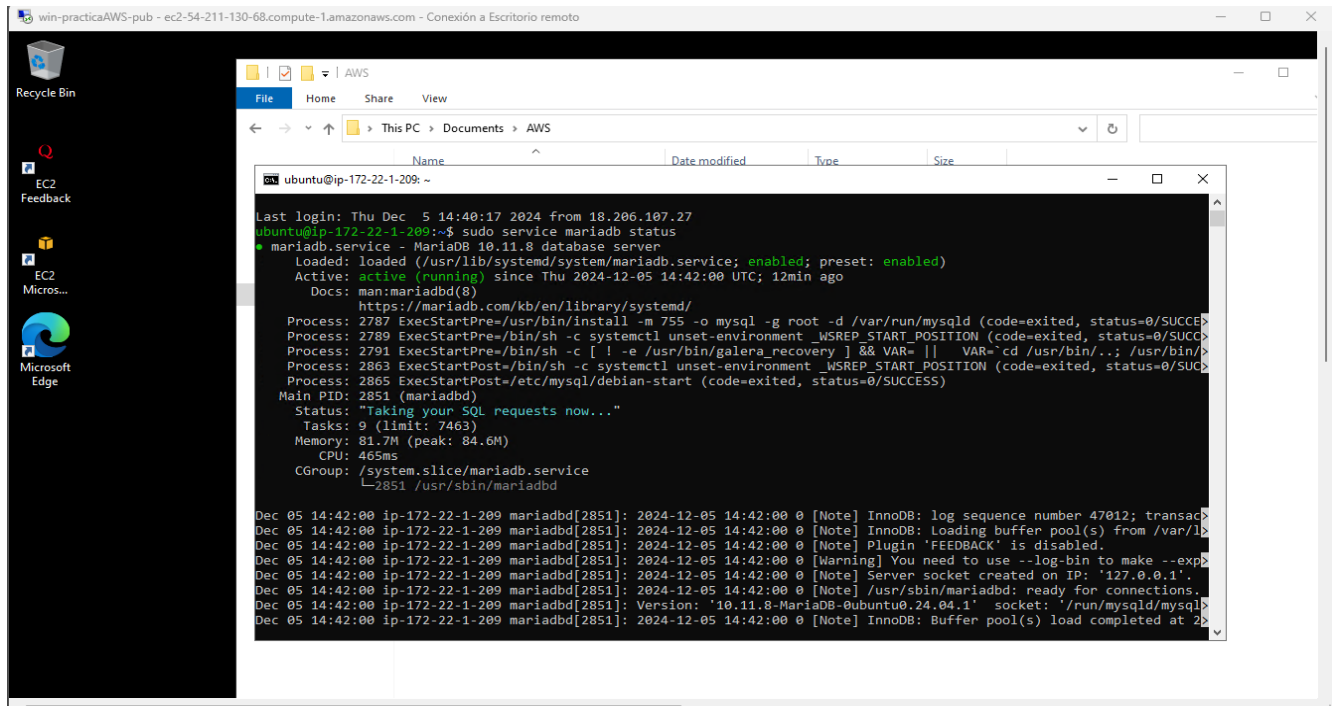


Introduciremos el comando correspondiente y, utilizando la clave **vokey**, accederemos a la máquina privada de Ubuntu desde el cliente público.



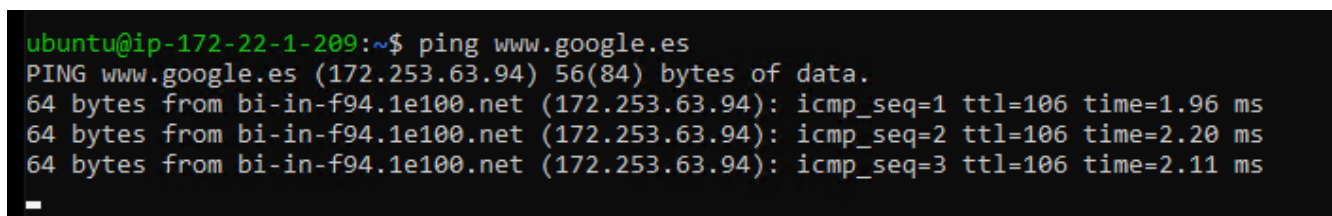
Pruebas

Una vez dentro, verificaremos si el servicio de **MariaDB** está activo. Como podemos observar, está funcionando correctamente.



Vamos a realizar un ping a Google para comprobar si tenemos acceso a Internet. Como podemos observar, tenemos conexión.

(Aunque pueda ser tentador hacer ping a las máquinas privadas, no obtendríamos respuesta, ya que no están configuradas para responder a este tipo de solicitudes).



RÚBRICA DE CORRECCIÓN

- Se ha accedido al curso y se ha activado el laboratorio (1 punto)
- Se han obtenido y guardado las claves PEM (1 punto)
- Se ha creado y configurado correctamente la VPC (2 puntos)
- Se ha configurado correctamente la red (1 puntos)
- Se ha creado y configurado correctamente la instancia EC2 de Windows (1 punto)

- Se ha creado y configurado correctamente la instancia EC2 de Ubuntu en la red pública (1 punto)
- Se ha mostrado la web de Apache y la web personalizada (1 punto)
- Se ha creado y configurado correctamente la instancia EC2 de Ubuntu en la red privada (1 puntos)
- Se ha creado la base de datos (1 punto)

En escala sobre 100:

Acceso al curso y activación del laboratorio	No se ha accedido al curso ni activado el laboratorio. 0 puntos	Acceso al curso, pero sin activar el laboratorio. 5 puntos	Se accede y activa correctamente el laboratorio. 10 puntos
Obtención de claves PEM	No se obtienen o no se guardan las claves PEM. 0 puntos	Claves obtenidas, pero no se documenta su uso o almacenamiento. 5 puntos	Claves obtenidas y almacenadas correctamente. 10 puntos
Creación y configuración de la VPC	No se crea la VPC o contiene errores críticos. 0 puntos	VPC creada con configuraciones básicas, pero incompletas. 10 puntos	VPC creada y configurada correctamente con sus subredes. 20 puntos
Configuración de la red	No se configura o configuración por defecto. 0 puntos	Configuración parcial o con errores menores. 5 puntos	Configuración correcta de red y subredes 10 puntos
Instancia EC2 de Windows (pública)	No se crea o no se configura correctamente la instancia de Windows. 0 puntos	Instancia creada con configuración parcial. 5 puntos	Instancia creada con configuración parcial. 10 puntos
Instancia EC2 de Ubuntu (pública)	No se crea o no se configura la instancia de Ubuntu en la red pública. 0 puntos	Instancia creada, pero no accesible por HTTP o SSH. 5 puntos	Instancia creada y accesible mediante HTTP y SSH. 10 puntos
Web de Apache y personalizada	No se muestra. 0 puntos	Se muestra sólo una 5 puntos	Se muestran las dos. 10 puntos
Instancia EC2 de Ubuntu (privada)	No se crea o no se configura correctamente la instancia privada. 0 puntos	Instancia creada, pero con problemas de conexión. 5 puntos	Instancia creada y conectada correctamente desde la pública y el exterior. 10 puntos
Creación de la base de datos	No se crea o no funciona la base de datos en la instancia privada. 0 puntos	Base de datos creada, pero con errores menores. 5 puntos	Base de datos creada y accesible desde la instancia pública. 10 puntos