

AMAZON EC2: LANZAMIENTO DE A UNA INSTANCIA EC2 CON MICROSOFT WINDOWS SERVER

Objetivo:

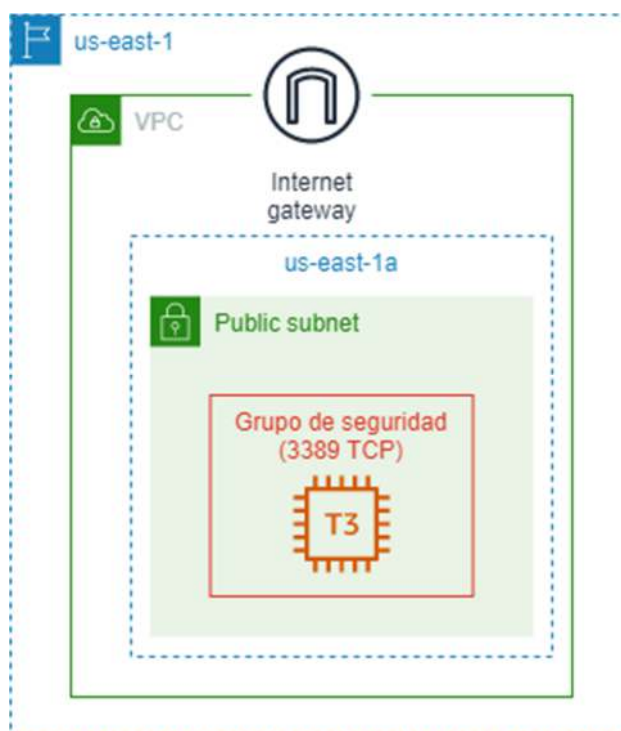
Las instancias EC2 se despliegan a partir de **Imágenes de Máquina de Amazon (AMI, Amazon Machine Image)**. Las AMIs incluyen entre otra información, una imagen del volumen de arranque (*root*) de la instancia. El sistema operativo de este volumen puede ser Amazon Linux, Ubuntu, OpenSuse, RHEL, MacOS o Microsoft Windows Server.

En esta práctica, se lanzará una instancia EC2 con sistema operativo Microsoft Windows Server en una subred pública y se lanzará una conexión por Escritorio Remoto contra dicha instancia, a través del puerto 3389 TCP (RDP, *Remote Desktop Protocol*).

Requerimientos:

- Disponer de acceso a los recursos de AWS a través de un *sandbox* de AWS Academy
- Cliente RDP (*Remote Desktop Protocol*).

Arquitectura propuesta:



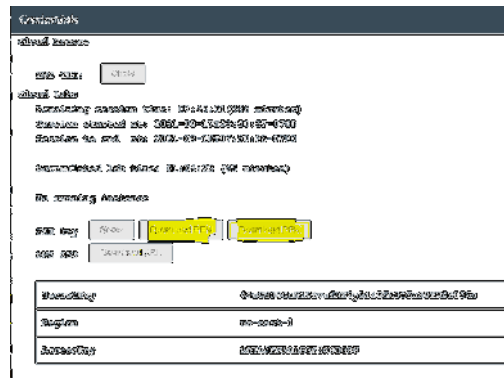
Realización:

- 1) Una vez iniciada la sesión en el laboratorio del *sandbox* del curso de AWS Academy, es necesario descargar la clave privada que nos permitirá obtener la contraseña del usuario *Administrator* del sistema operativo Windows Server de la instancia EC2 que vamos a crear. Para ello, hacemos clic

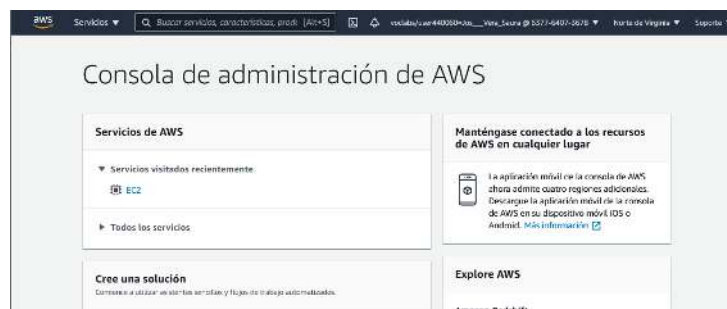
José Emilio Vera



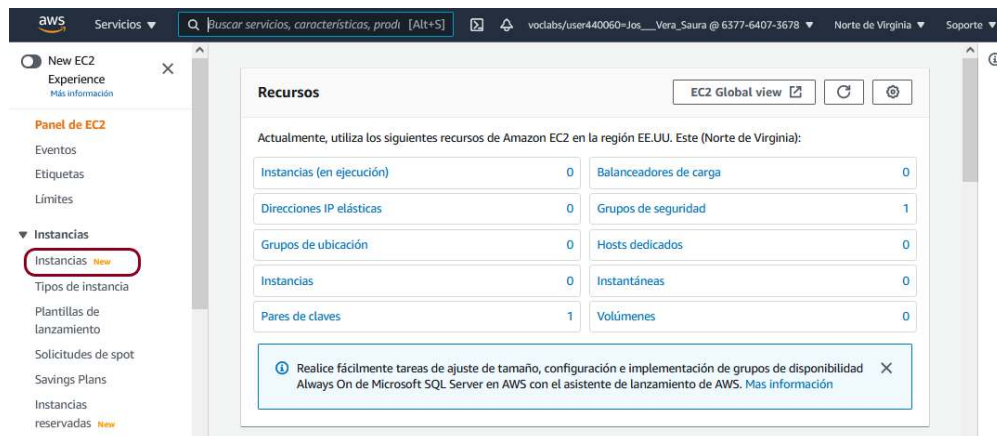
en *Detalles* y mostramos las credenciales temporales del entorno del *sandbox*. Desde esta ventana, descargamos la clave privada en formato PEM. Tras este proceso habremos descargado los archivos *labuser.pem* y *labuser.ppk*



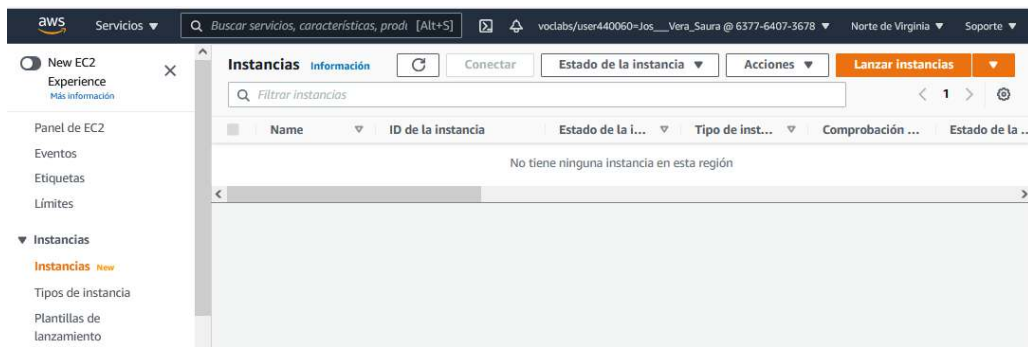
- 2) Abrimos la consola de AWS, presionando el botón AWS y nos aseguramos de que estamos trabajando en la región *us-east-1* (Norte de Virginia):



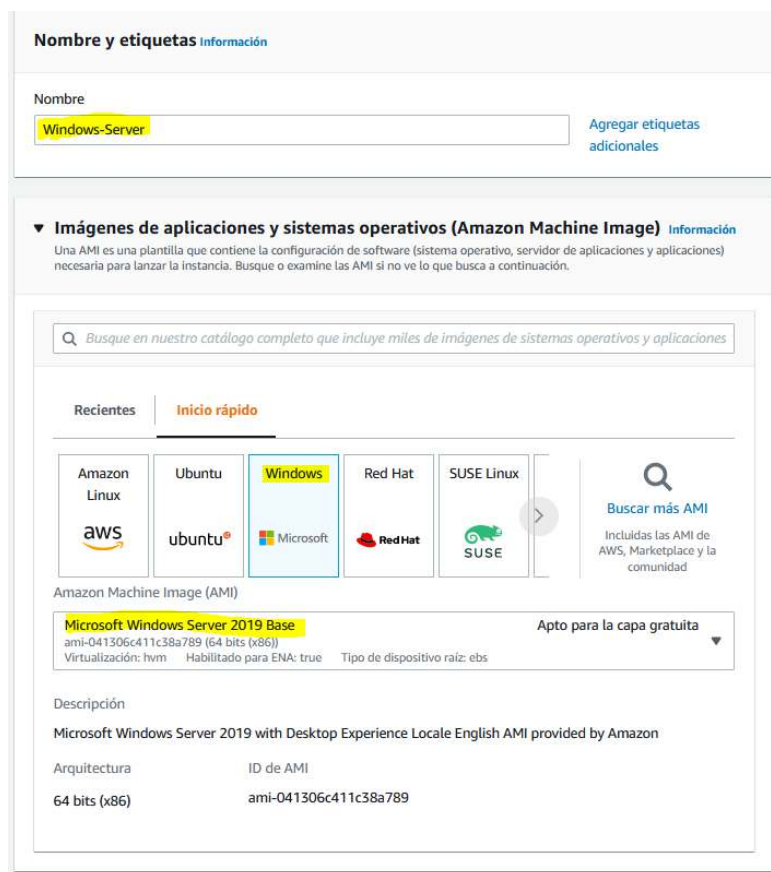
- 1) Buscamos el servicio Amazon EC2 desde el menú desplegable de *Servicios* (en la sección *Informática*) y abrimos la consola del servicio. Una vez allí, hacemos clic sobre *Instancias*:



- 2) Desde la siguiente ventana, hacemos clic en el botón *Lanzar instancias*:



- 3) A continuación, en la siguiente ventana introducimos en el apartado **Nombre y Etiquetas** en el campo **Nombre** el valor *Windows-Server*. En el apartado de **Imágenes de Aplicaciones y Sistemas Operativos (Amazon Machine Image)** debemos seleccionar en **Inicio Rápido** la opción *Microsoft Windows*, verificando que la **AMI (Amazon Machine Image)** será *Microsoft Windows Server 2019 Base* para arquitectura x86 (64 bits):



- 4) Ahora debemos elegir el **tipo de la instancia**. Debido a las restricciones del *sandbox*, podemos elegir un tipo muy limitado de instancias. En nuestro caso, elegiremos un tipo de instancia de propósito general, *t3.medium*:

▼ Tipo de instancia **Información**

Tipo de instancia

t3.medium

Familia: t3 2 vCPU 4 GiB Memoria

Bajo demanda Linux precios: 0.0416 USD por hora

Bajo demanda Windows precios: 0.06 USD por hora

Bajo demanda us-east-1-bos-1a Linux precios: 0.052 USD por hora

Bajo demanda us-east-1-bos-1a Windows precios: 0.0704 USD por hora

Bajo demanda us-east-1-chi-1a Linux precios: 0.052 USD por hora

Bajo demanda us-east-1-chi-1a Windows precios: 0.0704 USD por hora

[Comparar tipos de instancias](#)

- 5) A continuación, como **Par de claves**, seleccionamos en el campo **Nombre del par de claves** el valor **vockey**:

▼ 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.

- 6) En el apartado de **Configuraciones de red**, en el campo **VPC** seleccionamos la VPC predeterminada, y en el campo **Subred** elegimos la que se encuentra en la zona de disponibilidad **us-east-1a**. En el apartado **Firewall (grupos de seguridad)** seleccionamos la opción **Crear grupo de seguridad**, indicando en el campo **Nombre del grupo de seguridad** el valor **Windows-RDP** y en el campo **Descripción** la etiqueta **Acceso por RDP TCP 3389**:

▼ Configuraciones de red

VPC - obligatorio **Información**

vpc-0ac376f9a90b8c6bb (predeterminado)

172.31.0.0/16

Subred **Información**

subnet-02b5bdc72e68e72ad

VPC: vpc-0ac376f9a90b8c6bb Propietario: 265547453809

Zona de disponibilidad: **us-east-1a** Direcciones IP disponibles: 4091

[Crear una nueva subred](#)

Asignar automáticamente IP pública **Información**

Habilitar

Firewall (grupos de seguridad) **Información**

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☒ **Crear grupo de seguridad**

☐ Seleccionar un grupo de seguridad existente

Nombre del grupo de seguridad - obligatorio

Windows-RDP

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**

Acceso por RDP TCP 3389

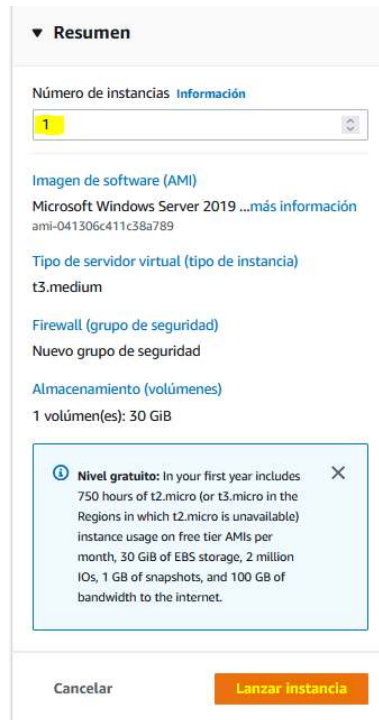
Reglas de grupos de seguridad de entrada

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

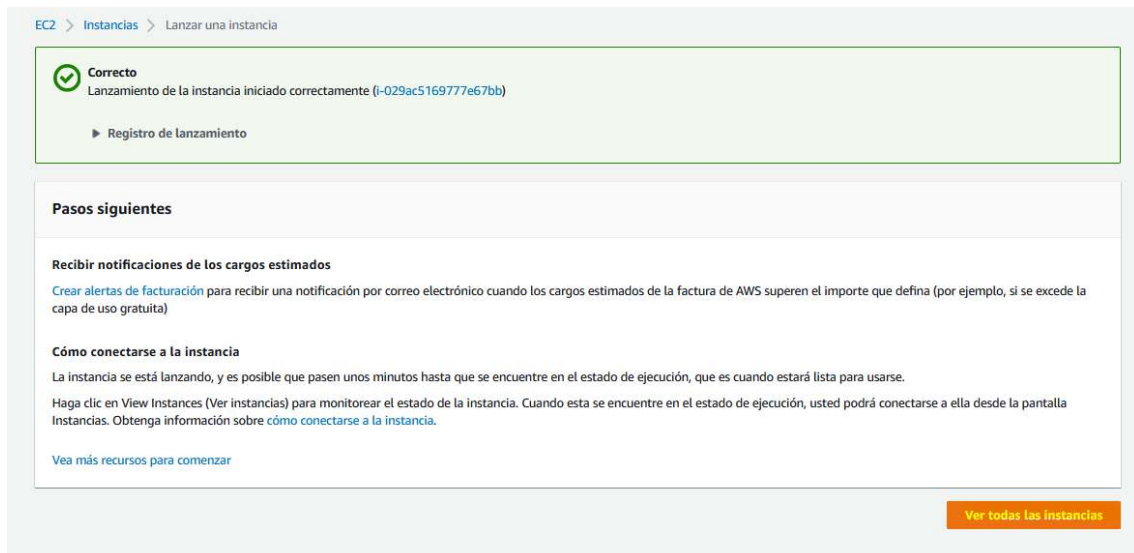
[Eliminar](#)

Tipo Información	Protocolo Información	Intervalo de puertos Información
rdp	TCP	3389
Tipo de origen Información	Origen Información	Descripción - optional Información
Cualquier lugar	Agregar CIDR, lista de prefijos	por ejemplo, SSH para Admin Desk
	0.0.0.0/0	

- 7) El resto de opciones las dejaremos con los valores por defecto, elegiremos en el campo **Número de instancias** el valor **1** y presionamos el botón **Lanzar instancia**:



- 8) Tras realizar el proceso, aparecerá una ventana como la siguiente. Presionamos el botón **Ver todas las instancias**:



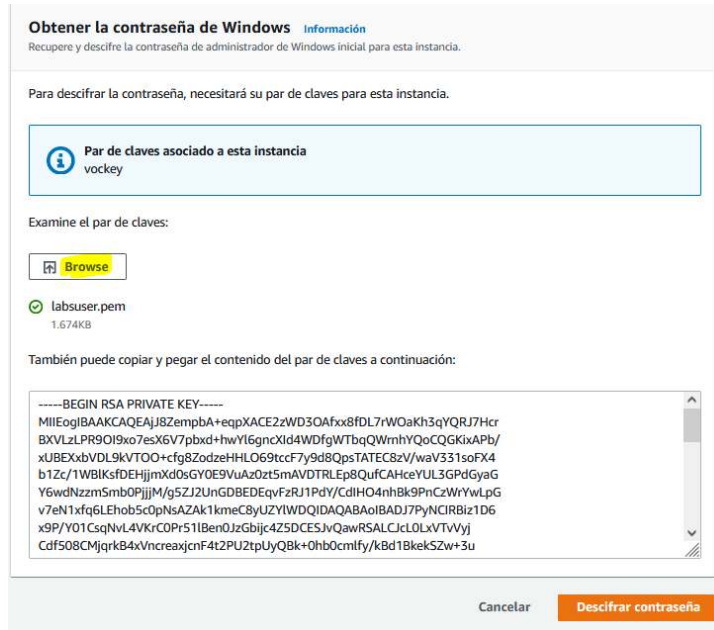
- 9) Tras ello, el servicio Amazon EC2 comenzará a aprovisionar la instancia. Las instancias EC2 con sistema operativo Microsoft Windows Server demoran más tiempo (entre 5-10 minutos) en estar operativas que las instancias EC2 con Linux. Si hacemos clic en el nombre de la instancia podemos ver sus detalles en la parte inferior de la ventana. Anotamos la IP pública o el nombre DNS público para poder acceder remotamente a la instancia.

- 10) A continuación, presionamos el botón *Conectar* y, en la siguiente ventana, hacemos clic en la pestaña *Cliente RDP*:

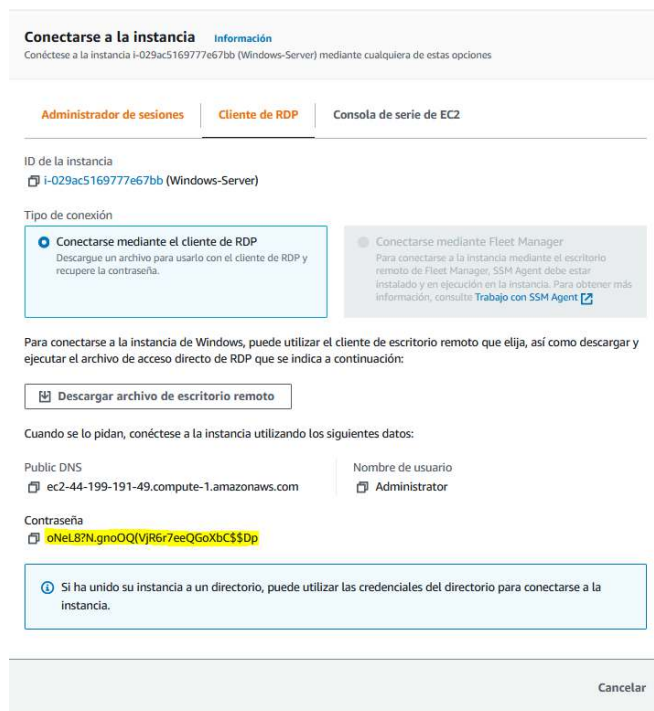
Desde esta ventana, hacemos clic en *Descargar archivo de escritorio remoto*, que nos permitirá descargar un archivo RDP con la configuración necesaria para efectuar la conexión por Escritorio Remoto a nuestra instancia EC2.

- 11) Además, haremos clic también en *Obtener contraseña* y facilitaremos, presionando en el botón *Browse*, nuestra clave privada que obtuvimos en el apartado 1) de esta práctica para poder

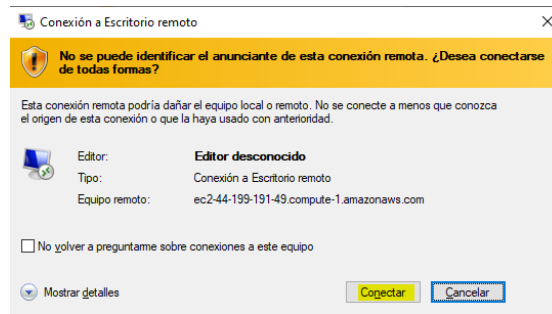
acceder a la contraseña del usuario *Administrator* de Microsoft Windows. Presionamos el botón *Descifrar Contraseña*:



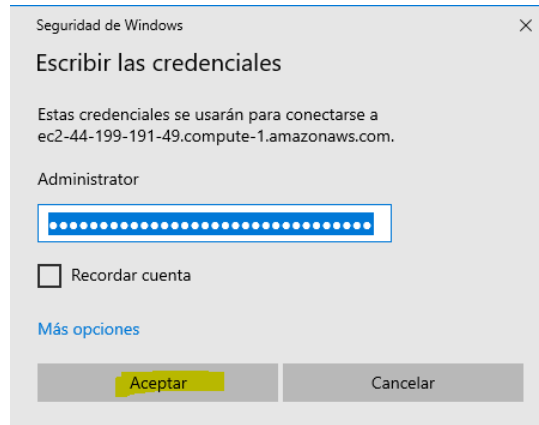
12) Tras ello, obtendremos la contraseña del usuario *Administrator*; la anotamos:



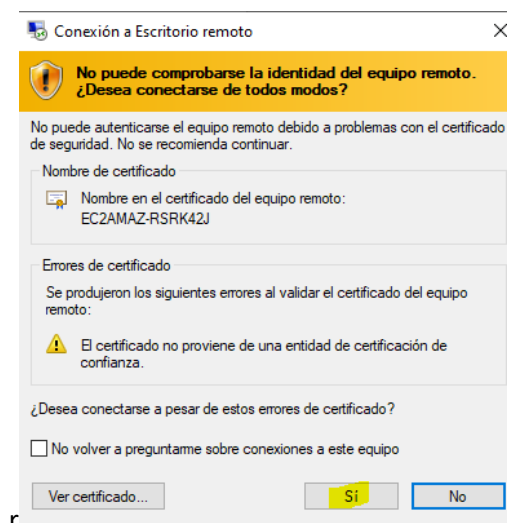
13) A continuación, hacemos doble clic sobre el archivo RDP que hemos descargado en el paso 12) y se abrirá el *cliente de Escritorio Remoto* y presionamos el botón *Conectar*:



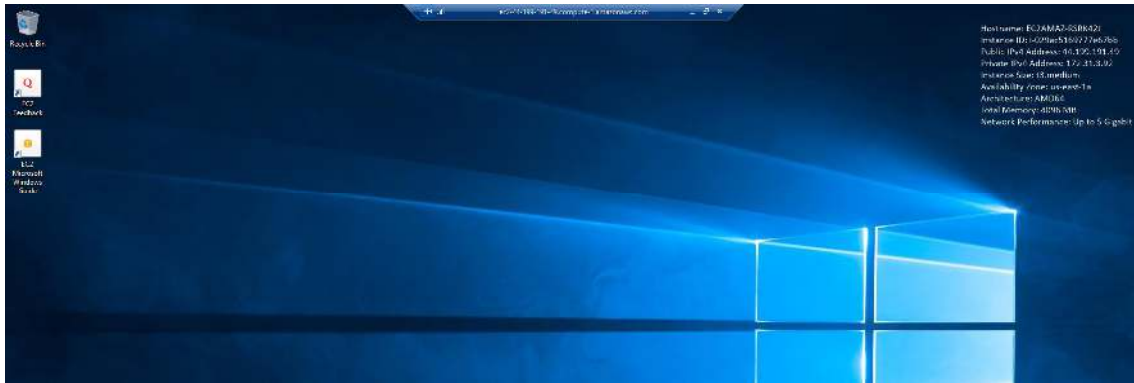
14) Introducimos la contraseña el usuario *Administrator* y presionamos *Aceptar*:



15) En la siguiente ventana, aceptamos el certificado digital como válido y presionamos *Sí*:

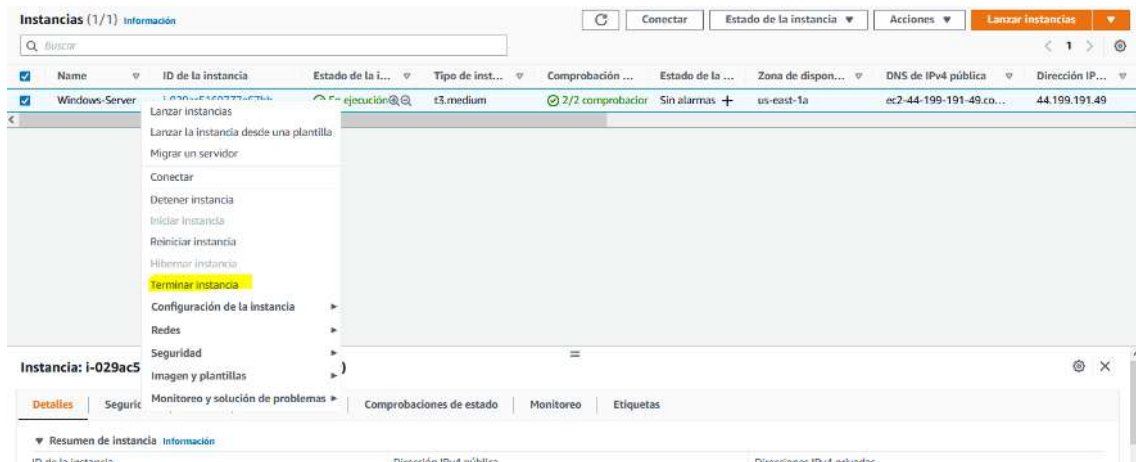


16) Tras unos instantes, habremos iniciado la sesión por Escritorio Remoto a nuestra instancia EC2 con sistema operativo Microsoft Windows Server:



Limpieza de la Práctica:

Para eliminar la práctica y que no consuma recursos de AWS, simplemente procedemos a terminar la instancia EC2 que hemos creado. Para ello, desde la consola de Amazon EC2 hacemos clic con el botón derecho del ratón sobre nuestra instancia y seleccionamos *Terminar Instancia*:



Recuerda también que, para hacer un uso responsable de los recursos en la nube, **el laboratorio de AWS Academy debe cerrarse** presionando el botón *End Lab* desde la plataforma.