



TRABAJO DE GRADO
Opción Seminario-Diplomado.

Aite delivery

Corporación Universitaria Remington.
Facultad de ingeniería
Ingeniería de Sistemas

John Alexander Rivera Rivera

Docente: Juan Pablo Berrio López – CEAD
Opción de Trabajo de grado Seminario-Diplomado.
2025.

Tabla de Contenidos

Resumen.....	4
Marco conceptual.....	4
Marco contextual	5
Documentación Técnica.....	6
Diagrama de arquitectura.....	6
Descripción de la arquitectura	7
Configuraciones realizadas	8
Procedimiento de acceso.....	9
Configuración del servidor web.....	9
Implementación y pruebas	12
Crear la infraestructura	12
VPC y subredes.....	12
Lanzar dos instancias EC2:.....	13
Configurar Grupos de Seguridad	13
RDP (puerto 3389) para Windows desde la IP pública del alumno.	13
SSH (puerto 22) para Linux desde la IP pública del alumno.....	14
Acceder a las instancias	14
Acceder vía RDP a la instancia Windows.	14
Acceder vía SSH a la instancia Linux.....	19
Instalar y configurar los servidores web	21
Windows: Instalar el rol de IIS y levantar el sitio por defecto. Se instala en la instancia con	
Windows el IIS y se habilita el total acceso por el puerto 80	21
Linux: Instalar Apache o Nginx y levantar el sitio por defecto.....	23
Pruebas de conectividad.....	24
Desde la instancia Windows hacer ping a la IP privada de la instancia Linux y viceversa..	24
Documentar si hay necesidad de habilitar ICMP en los Grupos de Seguridad para permitir	
ping.	25
Validación de acceso web.....	27
Acceder desde el navegador local al sitio web de la instancia Windows (http://ec2-3-148-236-194.us-east-2.compute.amazonaws.com/	27
Acceder desde el navegador local al sitio web de la instancia Linux (http://18.118.216.95/	27
Entrega Final.....	28
Diagrama general de la infraestructura	28
Balanceador de Carga.	28
Instancias EC2	30
Instancias con Proxy Reverso	30
Implementación Docker.....	31
Auto escalado.....	31

	3
Conclusiones	32
Referencias.....	33
(Puedes citar con normas APA o Vancouver. Se anexa ejemplo de normas APA).....	¡Error!
Marcador no definido.	

Resumen

El presente documento aborda la necesidad de la empresa Aite solutions SAS de implementar infraestructura en nube para su aplicación de domicilios para los productos de sus diferentes clientes, los cuales se enfocan en el área de venta de alimentos y consumibles.

Debido a la alta demanda de los usuarios de la aplicación, se requiere la implementación de una infraestructura en AWS que garantice la alta disponibilidad para garantizar al máximo su funcionamiento. Para esto, este documento contiene el esquema que se requiere para la nueva infraestructura junto con sus pruebas de funcionamiento en etapa de pruebas.(De la Bastida Sornoza Ginger Liliana Zhinin Gómez Alex Paúl & Quishpe Manuel William, 2022)

Palabras clave

AWS

Computación en la nube

Auto escalado

Balanceo de carga (ALB)

Docker

Servicios WEB

Marco conceptual

Computación en la nube AWS: Modelo de tecnología enfocado en la demanda de los recursos informáticos. La computación en la nube provee hardware como servidores, redes, bases de datos según las demandas de aplicaciones y servicios necesarios por los clientes sin necesidad de incurrir en sobredimensionamiento de infraestructura.(Joyanes Aguilar, 2009)

Características clave:

- Orientado a la demanda.
- Pago por uso.
- Infraestructura gestionada por el proveedor.

Administración de recursos: Capacidad de organizar, controlar y mejorar los activos tecnológicos por medios de herramientas de monitoreo continuo a la infraestructura, el cual permite tomar decisiones basado en datos reales de uso, capacidad y demanda de los servicios.

Características clave:

- Monitoreo continuo
- Cumplimiento y seguridad

Auto escalamiento: Es la capacidad de los sistemas informáticos de aumentar o disminuir basado en medidas objetivas que son monitoreadas bajo la demanda de disponibilidad de los recursos y evitando saturación de estos (Kewate, 2022)

Características clave.

- Escalamiento horizontal para añadir instancias EC2 según las políticas.

Marco contextual

La Startup Aite solutions SAS creo a finales del año pasado una plataforma innovadora que permite conectar los diferentes restaurantes con los clientes mediante pedidos en línea y entregas rápidas a domicilio. Debido a la aceptación y creciente uso de la aplicación, la cual permite el registro de restaurantes y usuarios en todo el país (Colombia), la capacidad de procesamiento y solicitudes de los usuarios demanda una actualización de la infraestructura tecnológica. Para cumplir con la demanda de la aplicación, se propone migrar toda la infraestructura tecnológica a la nube, específicamente a los servicios de AWS.

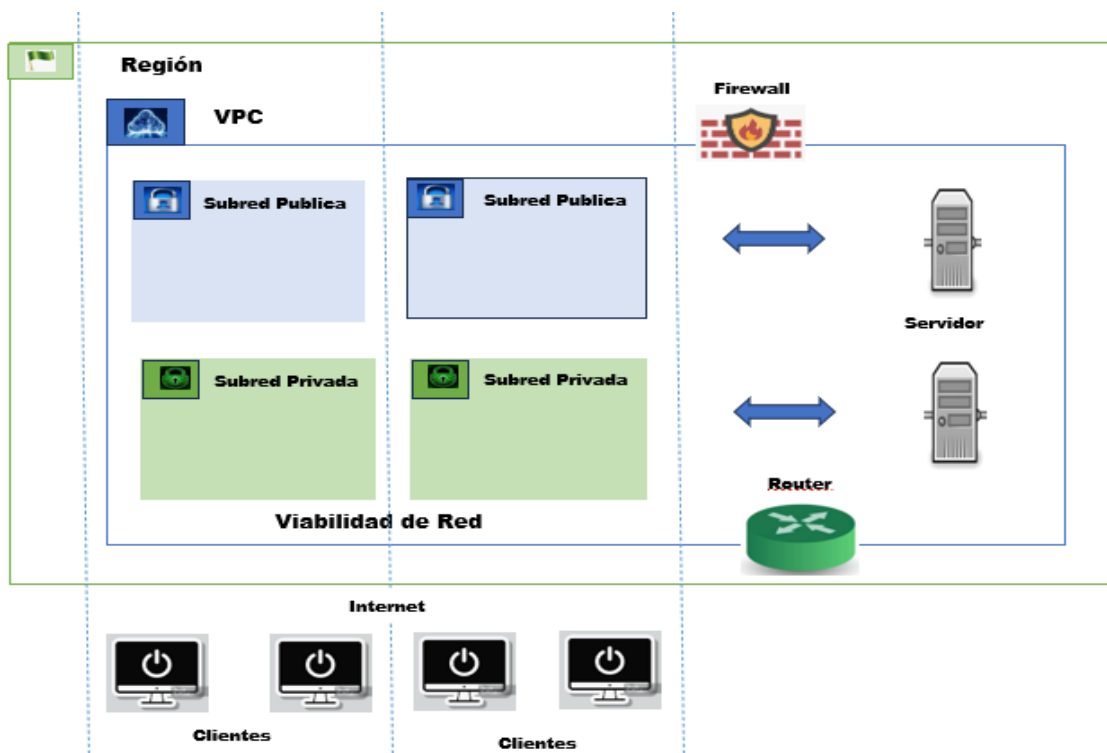
Esta migración permitirá aumentar de forma más rápida los recursos de la plataforma por medio del recurso de auto escalamiento, Aumentar la alta disponibilidad de los servicios y así brindar un constante servicio tanto a restaurantes como a los clientes. Adicional, de un aumento del nivel de seguridad de la aplicación.

A lo anterior, se suma la capacidad de reducción de costos basados en el pago único de los recursos utilizados.

Desarrollo e implementación del aprendizaje
Documentación Técnica.

Diagrama de arquitectura.

Figure 1. Representación gráfica de la red (EC2s, subredes, IPs públicas/privadas, grupos de seguridad, VPC, etc.)



Descripción de la arquitectura.

La red creada VPC (Amazon Virtual Private Cloud) consiste en una red aislada dentro de la nube de AWS, es semejante a una red tradicional, proporcionando un entorno aislado para desplegar los recursos, lo que permite internamente este VPC es definir las subredes publicadas y privadas para crear los segmentos y los recursos que actúan en el control del tráfico permitiendo la comunicación por medio del internet Gateway, este VPC se creó con el nombre de “Seminario-vpc” se encuentra compuesto por dos subredes públicas permitiendo la comunicación directa por internet y son esenciales para servicios accesibles públicamente y de igual manera se crearon dos subredes privadas en este caso no tiene acceso directo a internet y actualmente es utilizado para los recursos que no necesitan ser expuestos, esto se realizó con el fin de que las dos instancias puedan tener conexión entre sí y públicamente se pueda tener acceso a los servicios web que se configuran en cada una, teniendo en cuenta los rangos de dirección IP, Gateway y reglas de seguridad.

Las Instancias Linux (Ubuntu) se utilizan con EC2 instancias con el sistema operativo Ubuntu este permite el alojamiento de algunas aplicaciones y servicios debido a Ubuntu es la distribución más conocida de Linux por varias características como lo es su flexibilidad, seguridad, el tipo de soporte que brinda, amplia gama de herramientas y paquetes disponibles, facilitando la configuración y la gestión de servicios.

La VPC nos permite el aislamiento y control sobre el tráfico de red, teniendo muy buena capacidad de seguridad y la organización de los recursos como las subredes que en este caso segmentan la red, facilitando la separación de los recursos públicos y privados esto es en gran parte importante para la seguridad, el internet (Gateway).

Los beneficios de utilizar una VPC con instancias Windows server, principalmente permite por medio de segmentos su infraestructura en subredes, cada una maneja sus propias reglas en seguridad, protegiendo así las instancias de Windows server, se pueden elegir las instancias que se pueden comunicar entre sí por medio del internet, utilizando listas de control de acceso (ACLs) y grupo de seguridad, se puede escalar la infraestructura que se desea creando o eliminando instancias Windows Server dentro de la VPC según los requisitos. Nos permite conectar la VPC con otros servicios de la nube como almacenamiento, servicios de mensajería, para la creación de aplicaciones. Se puede alojar un servidor web IIS en la instancia Windows Server dentro de la VPC, esta te permite crear los entornos aislados para el desarrollo de pruebas de las aplicaciones que tenemos en Windows sin afectar el proceso. Se genera un acceso remoto seguro a las instancias de Windows server por medio de VPN y RDP permitiendo a los clientes acceder a los escritorios virtuales desde cualquier parte del país.

Si en algún momento se necesita la migración de datos a la nube, el VPC permite crear el entorno local en la nube de forma segura y controlada.

Configuraciones realizadas.

En la creación de instancias EC2 en AWS y la configuración de su acceso, es importante cumplir con estos requisitos selecciona una AMI, se elige un tipo de instancia, se configura la red, se asigna un grupo de seguridad con los puertos abiertos (RDP, SSH, HTTP), y gestiona IPs públicas y privadas.

Pasos para crear instancias EC2: Se debe seleccionar una AMI (Amazon Machine Image), eligiendo el sistema operativo y la configuración inicial de la instancia. Se elige un tipo de instancia seleccionando la configuración de hardware (CPU, memoria, almacenamiento, etc.) que mejor se adapte a tus necesidades. Configurando la red se define la VPC, y las subredes con el grupo de seguridad para la instancia. Se asignan una clave segura y dinámica (pública y privada) para acceder a la instancia mediante SSH o RDP. Luego se configura el almacenamiento, seleccionando el tipo y tamaño de almacenamiento para la instancia. Se define las reglas de entrada y salida para el tráfico de la red de la instancia, se lanza la instancia EC2 con nombre: "Server1jarr"(Windows SRV 20216) y "Linux1jarr" (Linux) con la configuración adecuada, los firewalls virtuales controlan el tráfico de red entrante y saliente de las instancias EC2, los puertos abiertos como: RDP (Remote Desktop Protocol) (puerto 3389) para Windows desde la IP pública del alumno, permite acceso remoto a instancias Windows, SSH (Secure Shell) (puerto 22) para Linux desde la IP pública del alumno. permite acceso remoto a instancias Linux, HTTP (80) para la futura configuración y puesta en marcha del servidor IIS y HTTPS permite acceso a sitios web.

En la entrada permite el tráfico hacia la instancia donde se configura para permitir conexiones entrantes a los puertos deseados desde las IPS o rangos permitidos.

En la salida permite el tráfico desde la instancia por defecto, permite todo el tráfico saliente, pero se restringen por seguridad. Los grupos de seguridad son stateful, esto permite una conexión entrante y la conexión de salida también está permitida. La asignación de IPS públicas permite a la instancia ser accesible desde internet y las IPS privadas permiten la comunicación entre instancias dentro de la misma VPC. El tipo de IP elástica pública se puede asignar a la instancia y liberar cuando no se necesite, evitando cambios de IP. La IP pública asignada automáticamente a la instancia se libera al detener o terminar la instancia. Al lanzar una instancia, se puede asignar una IP elástica si la necesitas de lo contrario se asignará una IP pública temporal. Puedes asignar una IP privada para la instancia al crearla o posteriormente. Se recomienda usar IPS elásticas para instancias que necesiten una IP pública fija.

Procedimiento de acceso.

El acceso en el servidor Windows y Linux en AWS, se utilizan protocolos como: RDP (Remote Desktop Protocol) para Windows y SSH (Secure Shell) para Linux. Para ambos, la dirección IP pública de la instancia y, en el caso de SSH, las credenciales de usuario. Para el acceso a instancias Windows (RDP), la dirección IP pública de la instancia de Windows esta consola de AWS, en la sección de EC2 y se busca la instancia, la dirección IP pública será visible en la pestaña, se obtiene la contraseña como administrador, en la consola de AWS, se obtiene la contraseña cifrada de la instancia de Windows, es necesario un par de claves (archivo. Pem) para descifrarlas, se utiliza cliente RDP en Windows, la "Conexión a Escritorio Remoto", en Linux, puedes usar Remmina o rdesktop, para ingresar a la dirección IP del usuario (administrador) y contraseña descifrada El acceso a las instancias Linux (SSH) se obtiene la dirección IP pública de la instancia Linux de igual manera que con Windows, busca la instancia en la consola de AWS y en la dirección IP en la pestaña.

El acceso al RDP de la instancia de Windows para acceder a la Instancia con Windows server. Se ingresa a la opción de conectar, revisamos que la conexión este activa, el submenú de "cliente RDP", se hace clic en la opción final de obtener contraseña, cargando así el archivo. PEM con la contraseña encriptada por seguridad del sistema, después se realiza la descifrado, de esta manera nos permite revisar los datos de la conexión por medio del cliente RDP ingresamos el nombre de DNS de la instancia o la IP publica, después ingresamos las credenciales para ingresar a la instancia, luego se puede acceder vía SSH a la instancia Linux. En el menú de "Conectar" de la instancia Linux, abrir el submenú "Cliente SSH" para obtener los datos de conexión, en el caso de un cliente Externo para conexión SSH, ingresamos los datos del nombre del host, nombre de usuario y la archivo. PEM para ingresar.

Configuración del servidor web.

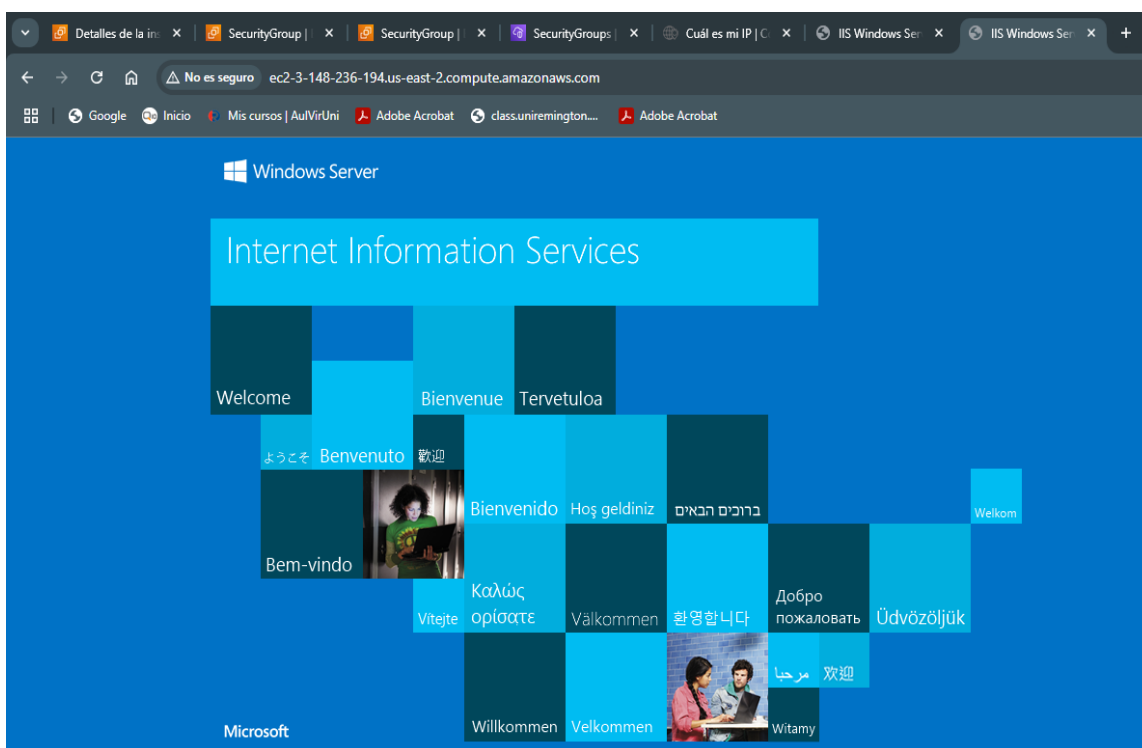
La instalación IIS (Servicios de Información de Internet) en un servidor Windows en Amazon EC2, primero necesitas acceder a la instancia, luego habilitar el rol de servidor web (IIS) y finalmente configurar los componentes necesarios. Principalmente instalar y configurar los servidores web, el siguiente paso en Windows instalar el rol de IIS y levantar el sitio por defecto. El tercer paso se instala en la instancia con Windows el IIS y se habilita el total acceso por el puerto 80, es de gran importancia validar la IP publica desde la información de la instancia en AWS por este motivo se ingresa externamente utilizando el nombre de domino de la instancia. En Linux instalar Apache Nginx y levantar el sitio por defecto, Se instala el servicio Apache y se realiza la respectiva validación del estado este debe estar activo, luego se identifica la IP publica de la instancia para ingresar desde el navegador web, las pruebas de conectividad desde la instancia Windows hacer ping a la IP privada de la instancia Linux y viceversa. Documentar si hay necesidad de habilitar ICMP

en los Grupos de Seguridad para permitir ping, para permitir el tráfico ICMP es necesario crear en el grupo de seguridad de cada instancia la regla que permita el tráfico ICMP. En la Instancia de Windows fue necesario crear una regla en el firewall de Windows permitiendo el tráfico del protocolo ICMP.

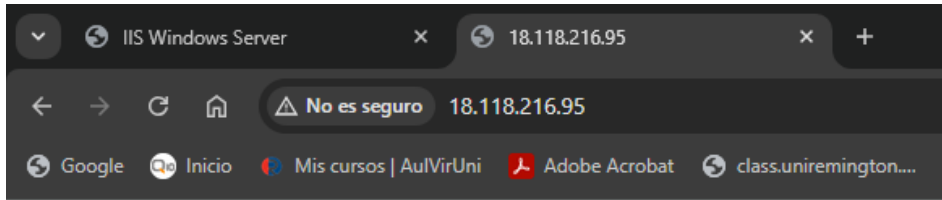
Validación de acceso web

Acceder desde el navegador local al sitio web de la instancia Windows (<http://ec2-3-148-236-194.us-east-2.compute.amazonaws.com/>)

Figure 2 Funcionamiento IIS en Windows server



*Figure 3*Funcionamiento servicio httpd en Linux



It works!

Acceder desde el navegador local al sitio web de la instancia Linux (<http://18.118.216.95/>)

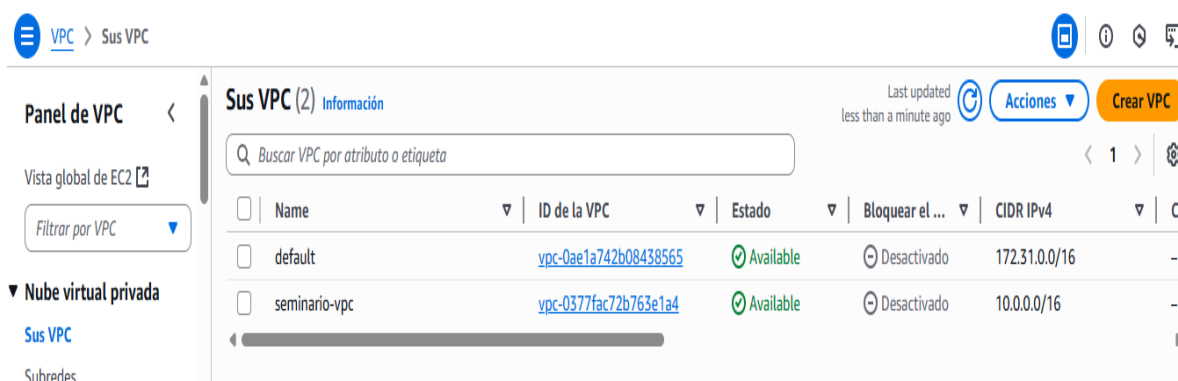
Implementación y pruebas.

Crear la infraestructura.

VPC y subredes.

Inicialmente se debe crear el VPC para la creación de la red interna, este VPC llamado “Seminario-vpc” consta de dos subredes públicas y dos subredes privadas con el propósito de que las dos instancias puedan tener conexión entre sí y públicamente se pueda tener acceso a los servicios web que se configuraran en cada una.

Figure 4 Listado de VPC



The screenshot shows the AWS Management Console interface for VPCs. On the left, there is a sidebar with 'Panel de VPC' and 'Nube virtual privada'. The main area displays 'Sus VPC (2) Información' with a search bar and a table of VPCs.

Name	ID de la VPC	Estado	Bloquear el ...	CIDR IPv4	CIDR IPv6
default	vpc-0ae1a742b08438565	Available	Desactivado	172.31.0.0/16	-
seminario-vpc	vpc-0377fac72b763e1a4	Available	Desactivado	10.0.0.0/16	-

Figure 5 Vista previa a la Subred



Instancias EC2.

Se crearon dos instancias con nombre: “Server1jarr” (Windows SRV 2016) y “Linux1jarr” (Linux)

Figure 6 Listado de instancias creadas.

✓	Name	ID de la instancia	Estado de la i...	Tipo de inst...	Comprobación de	E:
✓	Server1jarr	i-0db644bb5c96838fd	En ejecución	t2.micro	-	V
✓	Linux1jarr	i-0fcc493e4585864b9	En ejecución	t2.micro	-	V

Grupos de Seguridad.

RDP (puerto 3389).

Para el grupo de seguridad del servidor Windows, se habilito el acceso al protocolo RDP (3389) y el puerto HTTP (80) para la futura configuración y puesta en marcha del servidor IIS

Figure 7 Reglas de entrada instancia Windows

Nombre	ID de la regla del grupo d...	Intervalo de pu...	Protocolo	Origen	Grupos de seguridad	Descripción
-	sg-0f38069405a05e66	3389	TCP	190.67.63.204/32	sg-windowsServer	-
-	sg-00be2191a45adb2b	80	TCP	0.0.0.0/0	sg-windowsServer	-

SSH (puerto 22).

El grupo de seguridad de la instancia con SO Linux permite el tráfico entrante desde el puerto 22 del protocolo SSH y el puerto 80 de HTTP para la configuración futura del servidor WEB

Figure 8 Reglas de entrada instancia Linux

Instancias (1/2) Información

Última actualización: Hace less than a minute

Conectar Estado de la instancia Acciones Lanzar instancias

Buscar Instancia por atributo o etiqueta (case-sensitive) Todos los ...

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 L...
Server1jarr	i-0db644bb5c96838fd	En ejecución	t2.micro	2/2 comprobador	Ver alarmas +	us-east-2a	ec2-3-148-236-194.us...	3.148.236.194	-	-
Linux1jarr	i-0fcc493e4585864b9	En ejecución	t2.micro	2/2 comprobador	Ver alarmas +	us-east-2b	ec2-18-118-216-95.us...	18.118.216.95	-	-

i-0fcc493e4585864b9 (Linux1jarr)

Detalles Estado y alarmas Monitoreo Seguridad Redes Almacenamiento Etiquetas

▼ Detalles de seguridad

Rol de IAM: - ID del propietario: 871159689375 Hora de lanzamiento: Sun Jun 29 2025 13:18:34 GMT-0500 (hora estándar de Colombia)

Grupos de seguridad: sg-00083bb178a282262 (launch-wizard-1)

▼ Reglas de entrada

Nombre ID de la regla del grupo d... Intervalo de pu... Protocolo Origen Grupos de seguridad Descripción

-	sgr-041795fb81903f8a8	22	TCP	190.67.63.204/32	launch-wizard-1	-
-	sgr-090c69fa011ab9202	80	TCP	0.0.0.0/0	launch-wizard-1	-

▼ Reglas de salida

Nombre ID de la regla del grupo d... Intervalo de pu... Protocolo Destino Grupos de seguridad Descripción

-	sgr-08878232c23ad324e	Todo	Todo	0.0.0.0/0	launch-wizard-1	-
---	-----------------------	------	------	-----------	-----------------	---

Acceder a las instancias.

Acceso vía RDP.

Para acceder a la Instancia con Windows server. Se ingresa a la opción de conectar

Figure 9 Botón "Conectar"

Instancias (1/2) Información

Última actualización: Hace 3 minutos

Conectar

Buscar Instancia por atributo o etiqueta (case-sensitive) Todos

Name	ID de la instancia	Estado de la i...	Tipo de inst...
Server1jarr	i-0db644bb5c96838fd	En ejecución	t2.micro
Linux1jarr	i-0fcc493e4585864b9	En ejecución	t2.micro

En el submenú de “cliente RDP”, clic en la opción final de obtener contraseña

Figure 10 Submenú "Cliente RDP"

☰ [EC2](#) > [Instancias](#) > [i-0db644bb5c96838fd](#) > Conectarse a la instancia

Conéctese a una instancia a través del cliente basado en navegador.

Administrador de sesiones | **Cliente de RDP** | Consola de serie de EC2

Grabar conexiones RDP
Ahora puede registrar las conexiones RDP mediante el acceso a los nodos justo a tiempo de AWS Systems Manager. [Más información](#)

ID de la instancia
[i-0db644bb5c96838fd](#) (Server1jarr)

Tipo de conexión

Conectarse mediante el cliente de RDP
Descargue un archivo para usarlo con el cliente de RDP y recupere la contraseña.

Para conectarse a la instancia de Windows, puede utilizar el cliente de escritorio remoto que elija, así como descargar y ejecutarlo.

[Descargar archivo de escritorio remoto](#)

Cuando se le solicite, conéctese a su instancia utilizando el siguiente nombre de usuario y contraseña:

Public DNS
[ec2-3-148-236-194.us-east-2.compute.amazonaws.com](#)

Contraseña [Obtener contraseña](#)


Cargamos el archivo de extensión “. PEM” con la contraseña encriptada

Figure 11 menú para cargar el archivo. PEM

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-0db644bb5c96838fd (Server1jarr)

Par de claves asociado a esta instancia
 WinServer

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](#)


Contenido de la clave privada: *opcional*

Contenido de la clave privada

Desciframos la contraseña

Figure 12 Evidencia cifrado de contraseña

[↑ Cargar archivo de clave privada](#)

 WinServerEC2.pem
1.674KB

Contenido de la clave privada: *opcional*

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAmnqKtORQkzhtvln6x0O/EpRcNqo4lqhCcsBYuFBEOmizAL
dEF8HzOpml7Ozwouj9PdNIZV7P3d5V30HRAM08rJ99FFmwbCDTKH2/9yb/6lczd
V8lhw+nldpRWuhnkQJtCkS2Gj7cpXQsVwgULlBfnuc4sQGaOtoLLwSR78L3o
BVOMv/5draYcSMCouh047Uf1qX07YwJu/pxPF8xvLjNl8XdMnZb8lIQleDY6Ua
5ygcH7QK1r/8pphve9ZeGf603O1UofC3cPgkcnplmm3M0xglWCMOmjinIQY7BY
eDKpzWcsxbWJyIpt7+gmkv65uYg7F8DnE9upQIDAQAABAHA4Jo2ppc9tHpaKj
Ts4jf8WJ9JJPjWmh6WlQx0zfrgs+4HyJUSvmluH/8YKH9/DVt9wgnutl0KXW
-----
```

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

Obtenemos todos los datos de conexión

Figure 13 Datos de conexión

Cuando se le solicite, conectase a su instancia utilizando el siguiente nombre de usuario y contraseña.

Public DNS
ec2-3-148-236-194.us-east-2.compute.amazonaws.com

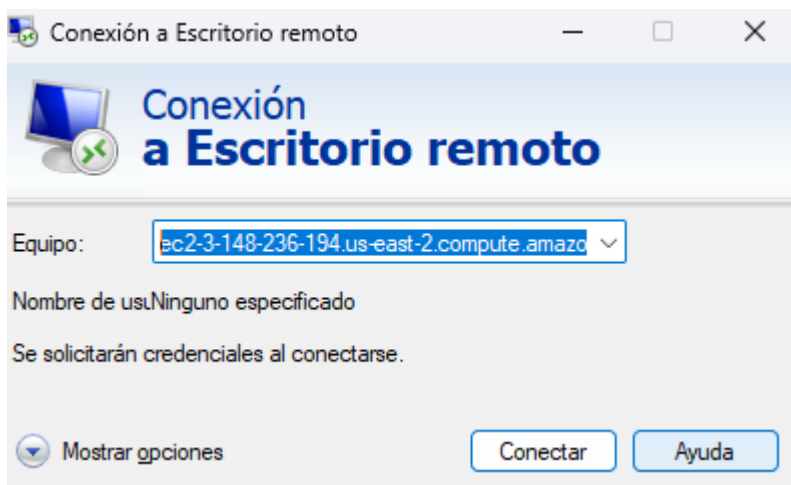
Nombre de usuario Información
Administrator

Contraseña
*zU&XlsKø%?TC;Z9ystTdKLTfN);QRy

Si ha unido su instancia a un directorio, puede utilizar las credenciales del directorio para conectarse a la instancia.

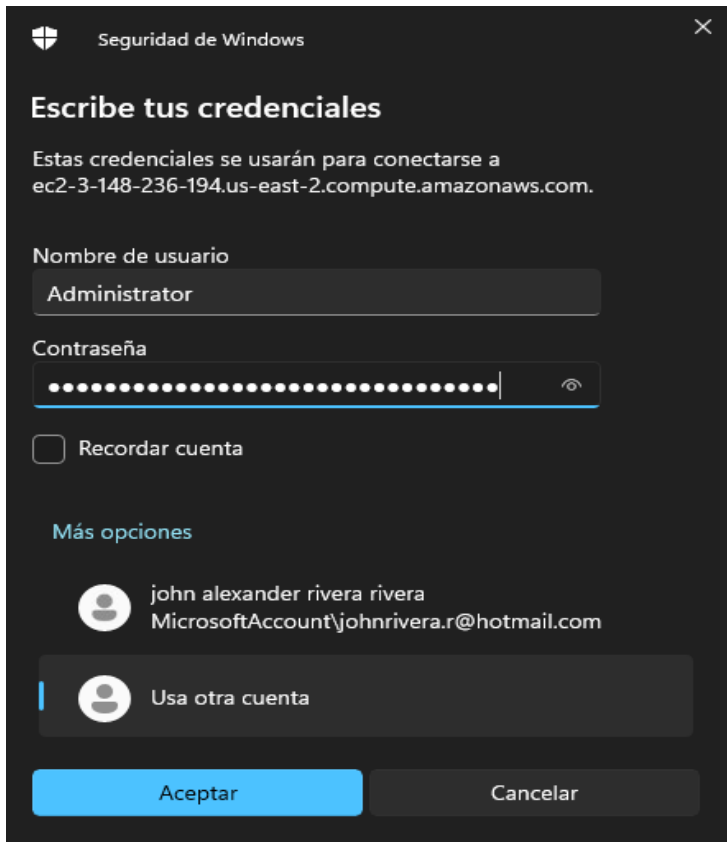
Utilizando el cliente RDP ingresamos el nombre de DNS de la instancia o la IP publica

Figure 14 Aplicación de Escritorio remoto de Windows



Ingresamos las credenciales

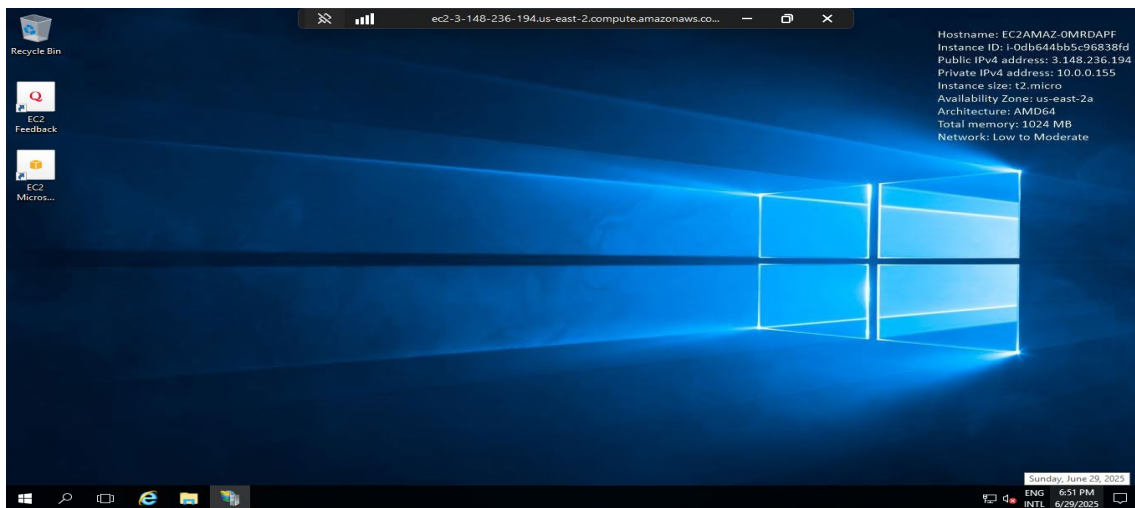
Figure 15 ventana emergente para ingreso de credenciales



The image shows a Windows Security dialog box titled "Seguridad de Windows" with a close button (X) in the top right corner. The main heading is "Escribe tus credenciales". Below this, a message states: "Estas credenciales se usarán para conectarse a ec2-3-148-236-194.us-east-2.compute.amazonaws.com." There are two input fields: "Nombre de usuario" containing "Administrator" and "Contraseña" which is currently masked with dots and has a visibility toggle icon. Below the password field is a checkbox labeled "Recordar cuenta" which is unchecked. Under the heading "Más opciones", there are two account entries: one for "john alexander rivera rivera" with email "MicrosoftAccount\johnrivera.r@hotmail.com" and another "Usa otra cuenta" which is selected with a blue vertical bar. At the bottom, there are two buttons: "Aceptar" (highlighted in blue) and "Cancelar".

Ingresamos a la instancia

Figure 16 Acceso remoto a la instancia Windows



Acceder vía SSH.

En el menú de “Conectar” de la instancia Linux, abrir el submenú “Cliente SSH” para obtener los datos de conexión

Figure 17 submenú AWS para acceso al cliente SSH

Conectar Información

Conéctese a una instancia a través del cliente basado en navegador.

Conexión de la instancia EC2 | Administrador de sesiones | **Cliente SSH** | Consola de serie de EC2

ID de la instancia
 i-0fcc493e4585864b9 (Linux1jarr)

1. Abra un cliente SSH.
2. Localice el archivo de clave privada. La clave utilizada para lanzar esta instancia es WinServer.pem
3. Ejecute este comando, si es necesario, para garantizar que la clave no se pueda ver públicamente.
`chmod 400 "WinServer.pem"`
4. Conéctese a la instancia mediante su DNS público:
`ec2-18-118-216-95.us-east-2.compute.amazonaws.com`

Ejemplo:
`ssh -i "WinServer.pem" ec2-user@ec2-18-118-216-95.us-east-2.compute.amazonaws.com`

Nota: En la mayoría de los casos, el nombre de usuario adivinado es correcto. Sin embargo, lea las instrucciones de uso de la AM

Utilizando un cliente Externo para conexión SSH, ingresamos los datos del nombre del host, nombre de usuario y la archivo. PEM para ingresar.

Figure 18 App MobaXtern, parámetros de conexión.

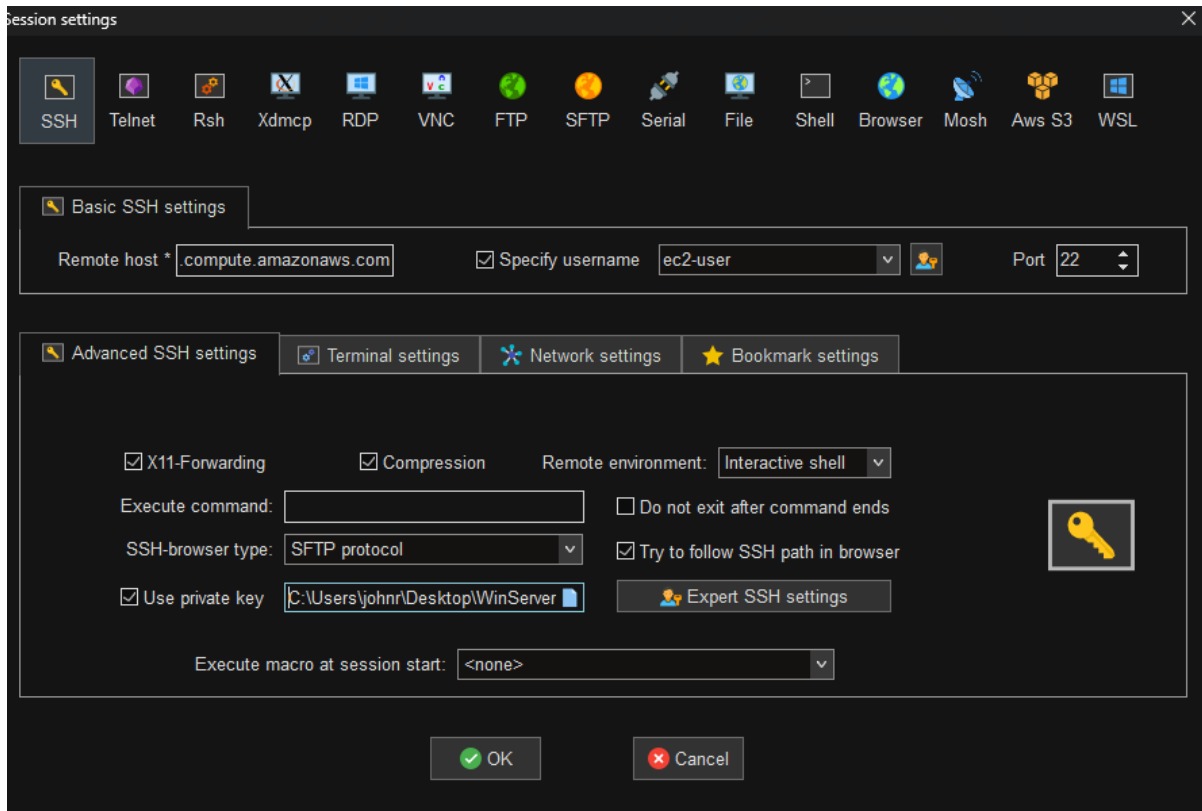
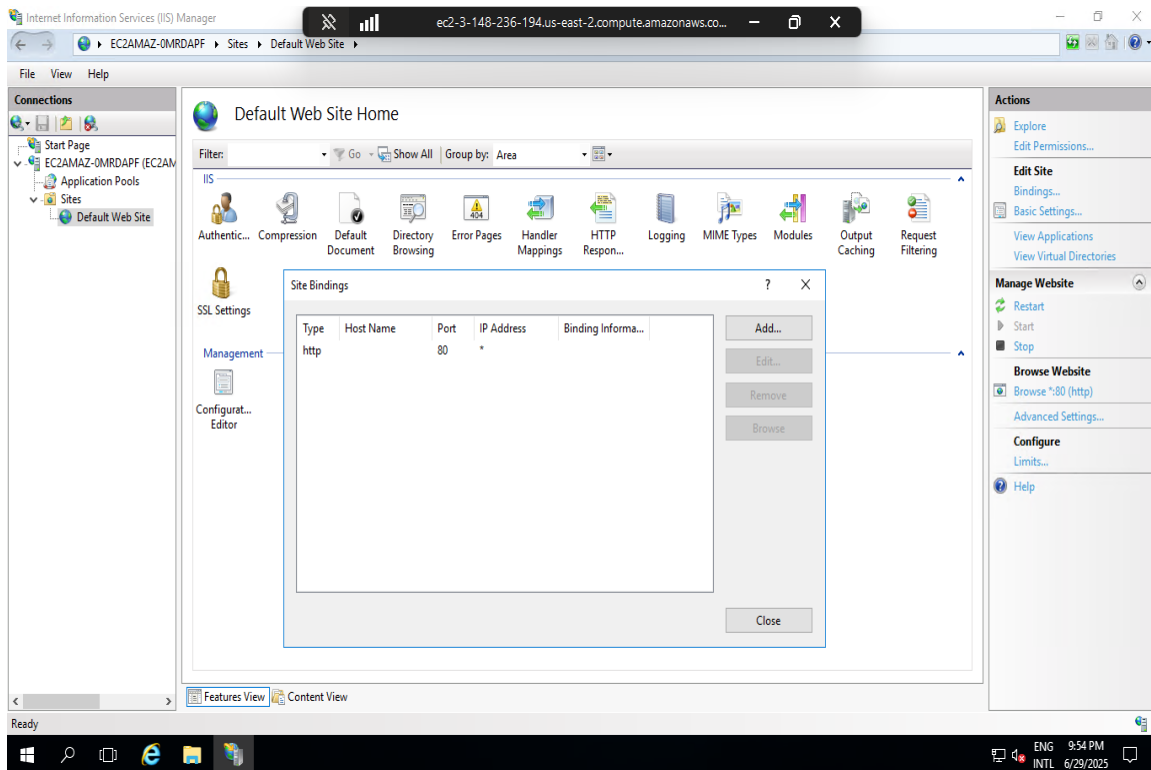
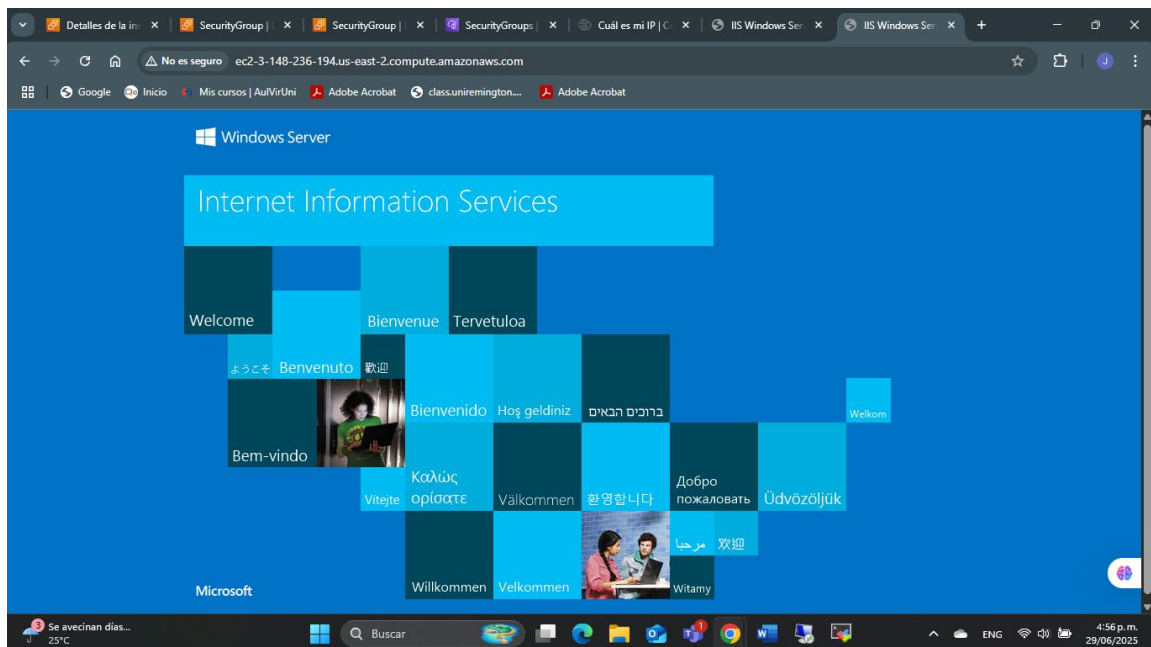


Figure 21 Parámetros de conexión IIS



Se ingresa externamente utilizando el nombre de dominio de la instancia.

Figure 22 ingreso exitoso por medio del nombre del dominio



Linux: Instalación Apache o Nginx.

Se instala el servicio Apache y se valida que su estado sea activo.

Figure 23 estado del servicio httpd

```

https://aws.amazon.com/linux/amazon-linux-2023
Last login: Sun Jun 29 18:41:20 2025 from 190.67.63.204
[ec2-user@ip-10-0-17-199 ~]$ sudo su
[root@ip-10-0-17-199 ec2-user]# dnf install httpd
Last metadata expiration check: 3:38:07 ago on Sun Jun 29 18:18:50 2025.
Package httpd-2.4.62-1.amzn2023.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[root@ip-10-0-17-199 ec2-user]# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; preset: disabled)
   Active: active (running) since Sun 2025-06-29 18:45:02 UTC; 3h 12min ago
     Docs: man:httpd.service(8)
  Main PID: 4495 (httpd)
    Status: "Total requests: 13; Idle/Busy workers 100/0; Requests/sec: 0.00113; Bytes served/sec: 0 B/sec"
      Tasks: 177 (limit: 1111)
     Memory: 18.7M
        CPU: 5.439s
   CGroup: /system.slice/httpd.service
           └─4495 /usr/sbin/httpd -DFOREGROUND
             └─4512 /usr/sbin/httpd -DFOREGROUND
               └─4513 /usr/sbin/httpd -DFOREGROUND
                 └─4514 /usr/sbin/httpd -DFOREGROUND
                   └─4515 /usr/sbin/httpd -DFOREGROUND

Jun 29 18:45:02 ip-10-0-17-199.us-east-2.compute.internal systemd[1]: Starting httpd.service - The Apache HTTP Server...
Jun 29 18:45:02 ip-10-0-17-199.us-east-2.compute.internal systemd[1]: Started httpd.service - The Apache HTTP Server.
Jun 29 18:45:02 ip-10-0-17-199.us-east-2.compute.internal httpd[4495]: Server configured, listening on: port 80
[root@ip-10-0-17-199 ec2-user]#

```

Se identifica la IP pública de la instancia para ingresar desde el navegador web

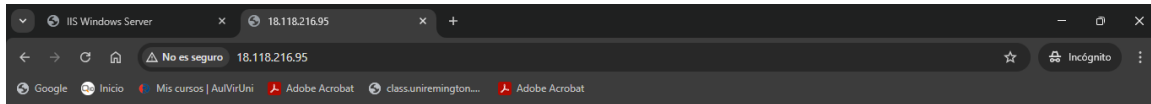
Figure 24 datos de conexión instancia Linux

Resumen de instancia de i-0fcc493e4585864b9 (Linux1jarr) Información

Se ha actualizado hace less than a minute

ID de la instancia i-0fcc493e4585864b9	Dirección IPv4 pública 18.118.216.95 dirección abierta	Direcciones IPv4 privadas 10.0.17.199
Dirección IPv6 -	Estado de la instancia En ejecución	DNS público ec2-18-118-216-95.us-east-2.compute.amazonaws.com dirección abierta

Figure 25 Funcionamiento Http



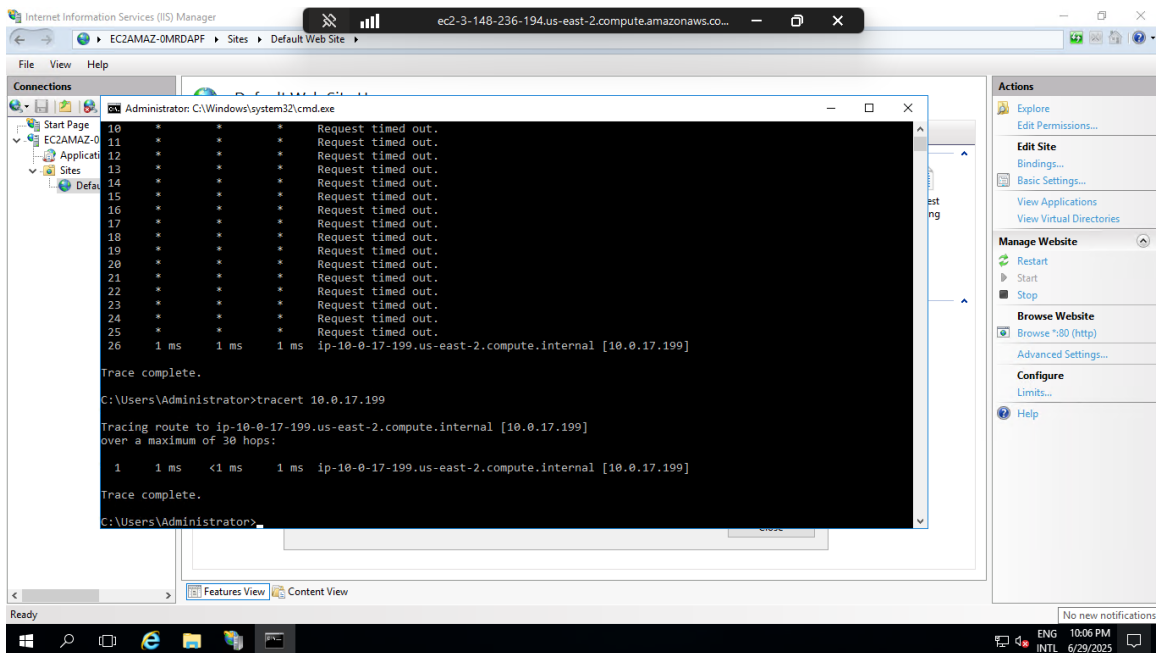
It works!



Pruebas de conectividad.

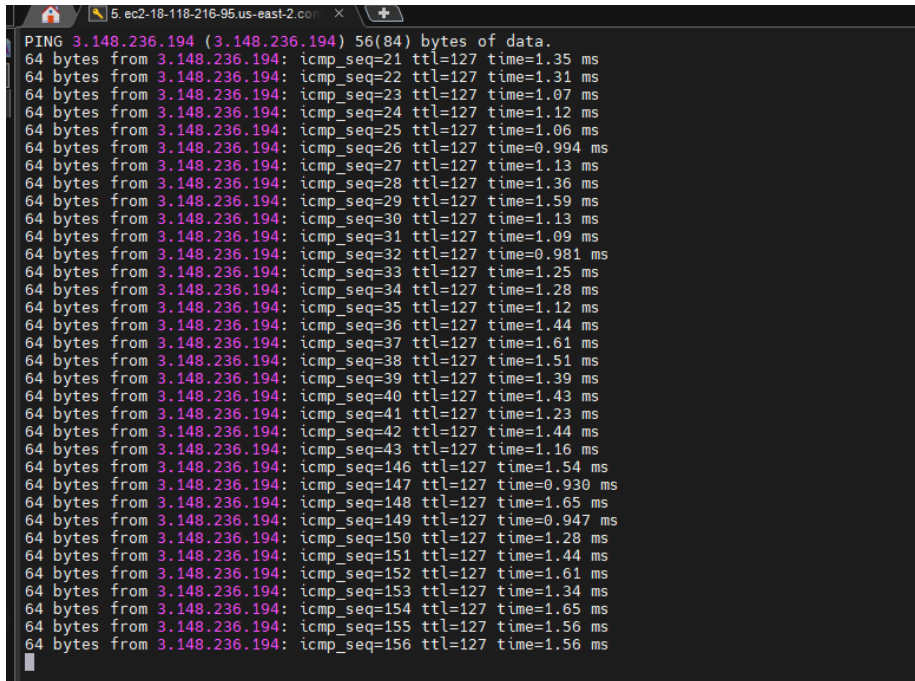
Desde la instancia Windows hacer ping a la IP privada de la instancia Linux y viceversa.
Prueba de tracer desde la instancia Windows a Linux

Figure 26 Evidencia tracer desde windows a Linux.



Prueba de ping desde Linux a Windows

Figure 27 Ping de Linux a window.



```

PING 3.148.236.194 (3.148.236.194) 56(84) bytes of data.
64 bytes from 3.148.236.194: icmp_seq=21 ttl=127 time=1.35 ms
64 bytes from 3.148.236.194: icmp_seq=22 ttl=127 time=1.31 ms
64 bytes from 3.148.236.194: icmp_seq=23 ttl=127 time=1.07 ms
64 bytes from 3.148.236.194: icmp_seq=24 ttl=127 time=1.12 ms
64 bytes from 3.148.236.194: icmp_seq=25 ttl=127 time=1.06 ms
64 bytes from 3.148.236.194: icmp_seq=26 ttl=127 time=0.994 ms
64 bytes from 3.148.236.194: icmp_seq=27 ttl=127 time=1.13 ms
64 bytes from 3.148.236.194: icmp_seq=28 ttl=127 time=1.36 ms
64 bytes from 3.148.236.194: icmp_seq=29 ttl=127 time=1.59 ms
64 bytes from 3.148.236.194: icmp_seq=30 ttl=127 time=1.13 ms
64 bytes from 3.148.236.194: icmp_seq=31 ttl=127 time=1.09 ms
64 bytes from 3.148.236.194: icmp_seq=32 ttl=127 time=0.981 ms
64 bytes from 3.148.236.194: icmp_seq=33 ttl=127 time=1.25 ms
64 bytes from 3.148.236.194: icmp_seq=34 ttl=127 time=1.28 ms
64 bytes from 3.148.236.194: icmp_seq=35 ttl=127 time=1.12 ms
64 bytes from 3.148.236.194: icmp_seq=36 ttl=127 time=1.44 ms
64 bytes from 3.148.236.194: icmp_seq=37 ttl=127 time=1.61 ms
64 bytes from 3.148.236.194: icmp_seq=38 ttl=127 time=1.51 ms
64 bytes from 3.148.236.194: icmp_seq=39 ttl=127 time=1.39 ms
64 bytes from 3.148.236.194: icmp_seq=40 ttl=127 time=1.43 ms
64 bytes from 3.148.236.194: icmp_seq=41 ttl=127 time=1.23 ms
64 bytes from 3.148.236.194: icmp_seq=42 ttl=127 time=1.44 ms
64 bytes from 3.148.236.194: icmp_seq=43 ttl=127 time=1.16 ms
64 bytes from 3.148.236.194: icmp_seq=146 ttl=127 time=1.54 ms
64 bytes from 3.148.236.194: icmp_seq=147 ttl=127 time=0.930 ms
64 bytes from 3.148.236.194: icmp_seq=148 ttl=127 time=1.65 ms
64 bytes from 3.148.236.194: icmp_seq=149 ttl=127 time=0.947 ms
64 bytes from 3.148.236.194: icmp_seq=150 ttl=127 time=1.28 ms
64 bytes from 3.148.236.194: icmp_seq=151 ttl=127 time=1.44 ms
64 bytes from 3.148.236.194: icmp_seq=152 ttl=127 time=1.61 ms
64 bytes from 3.148.236.194: icmp_seq=153 ttl=127 time=1.34 ms
64 bytes from 3.148.236.194: icmp_seq=154 ttl=127 time=1.65 ms
64 bytes from 3.148.236.194: icmp_seq=155 ttl=127 time=1.56 ms
64 bytes from 3.148.236.194: icmp_seq=156 ttl=127 time=1.56 ms
  
```

Habilitar ICMP.

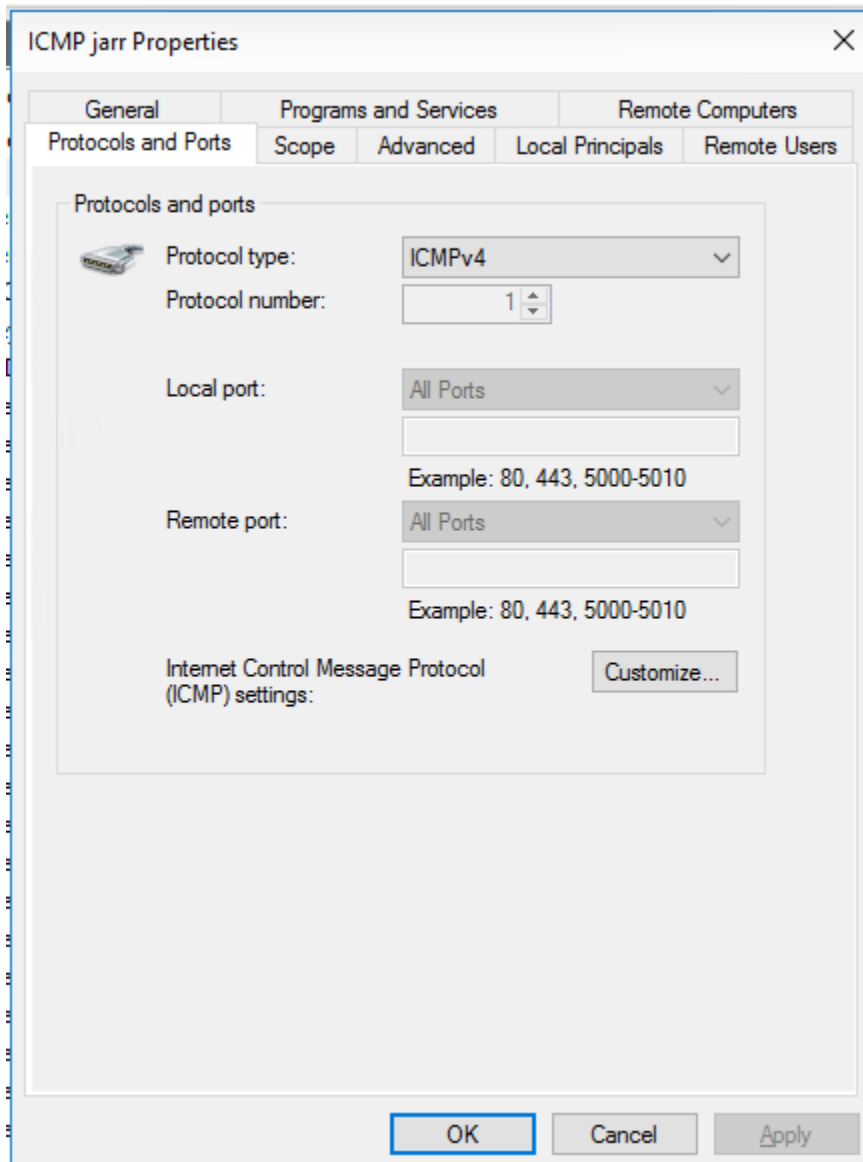
Para permitir el tráfico ICMP es necesario crear en el grupo de seguridad de cada instancia la regla que permita el tráfico ICMP

Figure 28 Configuración de red para permitir el tráfico ICMP



Adicional para la Instancia Windows fue necesario crear una regla en el firewall de Windows permitiendo el tráfico del protocolo ICMP.

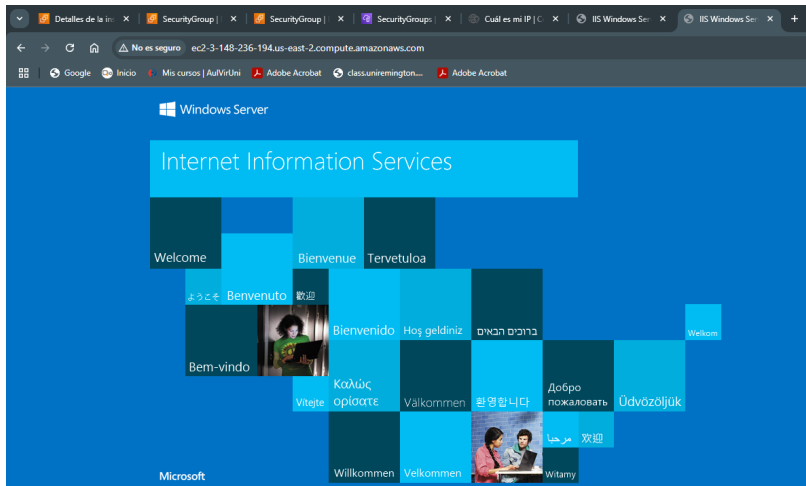
Figure 29 configuración firewall Windows



Validación de acceso web.

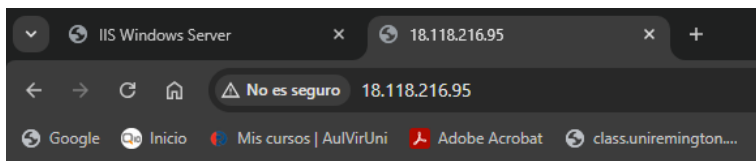
Acceder desde el navegador local al sitio web de la instancia Windows (<http://ec2-3-148-236-194.us-east-2.compute.amazonaws.com/>)

Figure 30 validación acceso servicio IIS



Acceder desde el navegador local al sitio web de la instancia Linux (<http://18.118.216.95/>)

Figure 31 Validación acceso servicio httpd

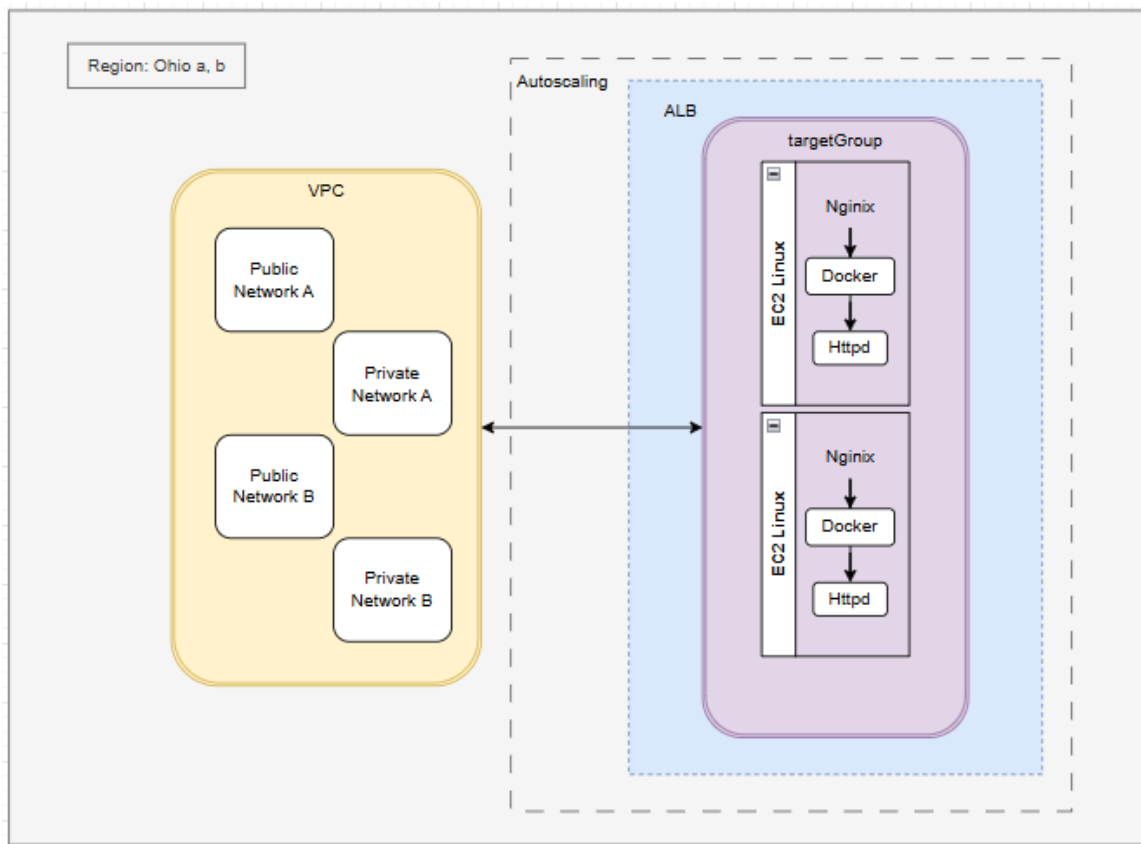


It works!

Entrega Final.

Diagrama general de la infraestructura.

Figure 32 Diagrama General de la infraestructura



Balancedador de Carga.

Configure un **Application Load Balancer (ALB)** para distribuir el tráfico entrante a múltiples instancias EC2.

Figure 33 Lista ALB

Balancedores de carga (1/1) Acciones Crear balanceador de carga

Elastic Load Balancing escala automáticamente la capacidad del equilibrador de carga en respuesta a los cambios en el tráfico entrante.

Buscar:

Nombre	Nombre de DNS	Estado	ID de VPC	Zonas de disponibi...	Tipo	Fecha creada
LoadBalancer1	LoadBalancer1-880193759...	Activo	vpc-0377fac72b763e1a4	2 Zonas de disponibilidad	application	1 de julio de 2025, 18:54 (UTC-05:00)

Equilibrador de carga: LoadBalancer1

Detalles | **Agentes de escucha y reglas** | Mapeo de red | Mapa de recursos | Seguridad | Monitorización | Integraciones | Atributos | Capacidad | Etiquetas

Agentes de escucha y reglas (1) Administrar reglas Administrar agente de escucha Agregar agente de escucha

Un agente de escucha comprueba las solicitudes de conexión en su protocolo y puerto configurados. El tráfico recibido por el agente de escucha se enruta de acuerdo con la acción predeterminada y cualquier regla adicional.

Buscar:

Protocolo/Port	Acción predeterminada	Reglas	ARN	Política de seguridad	Certificado SSL/TLS predet...	mTLS	Trust store	Estado de asociación del al...	Etiquetas
HTTP:80	Reenviar al grupo de destino <ul style="list-style-type: none"> targetGroupSeminariojarr (1 (100%)) Permanencia del grupo de destino: Desactivada 	1 regla	ARN	No aplicable	No aplicable	No aplicable	No aplicable	No aplicable	0 etiquetas

Figure 34 Parámetros del grupo del ALB

targetGroupSeminariojarr Acciones

Detalles

arn:aws:elasticloadbalancing:us-east-2:871159689375:targetgroup/targetGroupSeminariojarr/93792aa026c3ca45

Tipo de destino Instancia	Protocolo : Puerto HTTP: 80	Versión del protocolo HTTP1	VPC vpc-0377fac72b763e1a4
Tipo de dirección IP IPv4	Balancedor de carga LoadBalancer1		

2 Destinos totales	2 En buen estado	0 En mal estado	0 Sin utilizar	0 Inicial	0 Vaciado
-----------------------	---------------------	--------------------	-------------------	--------------	--------------

Distribución de destinos por zona de disponibilidad (AZ)
 Seleccione los valores de esta tabla para ver los filtros correspondientes aplicados a la tabla Destinos registrados que aparece a continuación.

Destinos | Monitorización | Comprobaciones de estado | Atributos | Etiquetas

Destinos registrados (2) Mitigación de anomalías: No aplicable Anular el registro Registrar destinos

Los grupos de destinos enrutan las solicitudes a destinos individuales registrados mediante el protocolo y el número de puerto que especifique. Las comprobaciones de estado se realizan en todos los destinos registrados de acuerdo con la configuración de comprobación de estado del grupo de destinos. La detección de anomalías se aplica automáticamente a los grupos de destinos de HTTP/HTTPS con al menos 3 destinos en buen estado.

Buscar:

ID de instancia	Nombre	Puerto	Zona	Estado	Detalles del estado	Sustitución admi...	Detalles de la sus...	Hora d...	Resultado
i-09edd8d6cc43411fe	Linuxjarr2	80	us-east-2a (us...	Healthy	-	No override	No override is curren...	14 de juli...	Normal
i-0086e47bba350ffaf	Linuxjarr	80	us-east-2b (us...	Healthy	-	No override	No override is curren...	14 de juli...	Normal

Implementación Docker.

Se implemento el servicio Docker agregando una imagen de nginx dentro del host

Figure 37 imágenes nginx del host

```
[root@ip-10-0-24-109 ec2-user]# docker images
REPOSITORY          TAG             IMAGE ID        CREATED         SIZE
nginxdemos/hello    0.4-plain-text d85cd407faf5   2 weeks ago    52.5MB
nginxdemos/hello    latest          691caebbd731   2 weeks ago    52.5MB
```

Se implementaron 3 Docker

Figure 38 Listado de Docker

```
[root@ip-10-0-24-109 ec2-user]# docker ps
CONTAINER ID   IMAGE             COMMAND                  CREATED        STATUS        PORTS                               NAMES
9f86375e174f   nginxdemos/hello "/docker-entrypoint..." 4 hours ago   Up 4 hours   0.0.0.0:83->80/tcp, :::83->80/tcp   jarr3
bd11399b37e5   nginxdemos/hello "/docker-entrypoint..." 4 hours ago   Up 4 hours   0.0.0.0:82->80/tcp, :::82->80/tcp   jarr2
107df57168ea   nginxdemos/hello "/docker-entrypoint..." 4 hours ago   Up 4 hours   0.0.0.0:81->80/tcp, :::81->80/tcp   jarr
```

Auto escalado.

Se implementaron políticas de escalado para mantener 2 instancias activas en el ALB para sustentar servicios.

Figure 39 Estado servicio de auto escalado

AutoScalingSeminariojarr

AutoScalingSeminariojarr Descripción general de la capacidad Edit

arn:aws:autoscaling:us-east-2:871159689375:autoScalingGroup:da8fa660-875e-48b7-8840-3543cf7d2bb1:autoScalingGroupName/AutoScalingSeminariojarr

Capacidad deseada	Límites de escalamiento (Min. - Máx.)	Tipo de capacidad deseado	Estado
2	1 - 2	Unidades (número de instancias)	-

Fecha de creación
Tue Jul 01 2025 19:32:52 GMT-0500 (hora estándar de Colombia)

[Detalles](#) | [Integraciones - nueva](#) | [Escalado automático](#) | [Administración de instancias](#) | [Actualización de instancias](#) | [Actividad](#) | [Monitoreo](#)

Plantilla de lanzamiento Edit

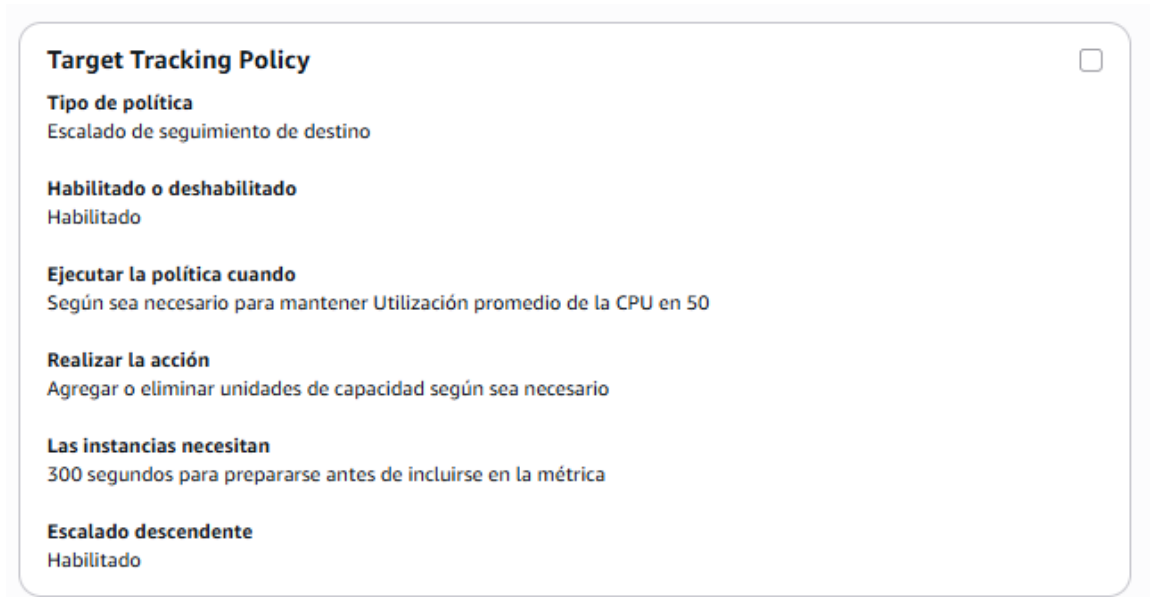
Plantilla de lanzamiento it-0360875b0b8b54455 linuxok	ID de AMI ami-05957de8b4b63d44e	Tipo de instancia t2.micro	Propietario arn:aws:iam::871159689375:root
Versión Default	Grupos de seguridad -	ID de grupos de seguridad sg-0073d089c6a7f6969	Hora de creación Mon Jul 14 2025 14:40:27 GMT-0500 (hora estándar de Colombia)
Descripción -	Almacenamiento (volumenes) -	Nombre del par de claves WinServer	Solicitar instancias de spot No

[Ver detalles en la consola de la plantilla de lanzamiento](#)

Red Edit

Zonas de disponibilidad use2-az2 (us-east-2b) use2-az1 (us-east-2a)	ID de subred subnet-0320e6f5722bc2192 subnet-0da57e8314dc8b176	Distribución de zonas de disponibilidad Mejor esfuerzo equilibrado
---	--	---

Figure 40 Política de auto escalado



Conclusiones.

Del anterior documento se puede concluir la importancia del avance de la tecnología y que la adopción de esta puede llegar a mejorar la calidad de los servicios se prestan en la actualidad. Con un aumento constante en la demanda de servicios y la alta disponibilidad de estos se vuelve indispensable implementar mejores mecanismos de control y administración con la facultad de aprovechar al máximo con los costos necesarios para la correcta operación.

Si bien, la tecnología cada día hace el mundo más fácil para los usuarios, es importante tener entendimiento de su funcionamiento para estar siempre a la vanguardia de los retos que la vida cotidiana exige.

Referencias.

- De la Bastida Sornoza Ginger Liliana Zhinin Gómez Alex Paúl, D., & Quishpe Manuel William, V. (2022). *ANÁLISIS COMPARATIVO DEL USO DE MÁQUINAS VIRTUALES Y DOCKER PARA EL DESPLIEGUE DE APLICACIONES DE SOFTWARE: CASO DE ESTUDIO APLICACIÓN DE UN GESTOR DOCUMENTAL*.
- Joyanes Aguilar, L. (2009). *La Computación en Nube (Cloud Computing): El nuevo paradigma tecnológico para empresas y organizaciones en la Sociedad del Conocimiento*.
- Kewate, N. (2022). A Review on AWS - Cloud Computing Technology. *International Journal for Research in Applied Science and Engineering Technology*, 10(1), 258–263. <https://doi.org/10.22214/ijraset.2022.39802>