# Índice

# 1. Computación en la nube.

## 1.1. Introducción a la computación en la nube.

### Definición de computación en la nube

Computación en la nube es la entrega bajo demanda de potencia de cómputo, base de datos, almacenamiento, aplicaciones y otros recursos de TI a través de Internet con precios de pago por uso.

#### Infraestructura como software

La computación en la nube le permite dejar de pensar en su infraestructura como hardware y, en cambio, pensar en ella (y usarla) como software.

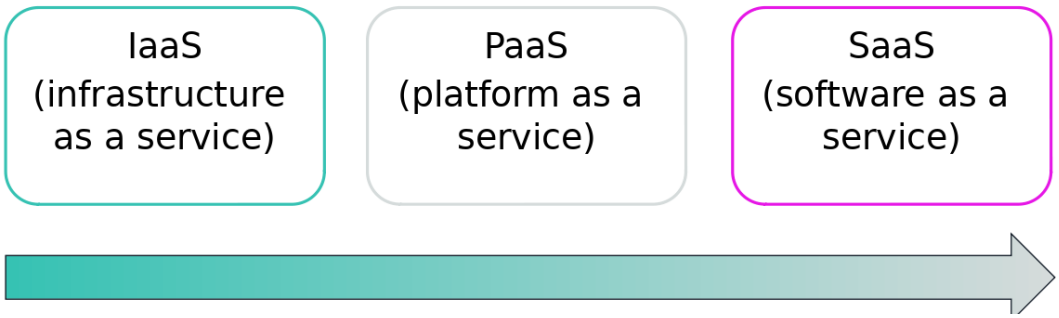
### Modelo informático tradicional

- Infraestructura como hardware
- Soluciones de hardware:
    - Requiere espacio, personal, seguridad física, planificación, gastos de capital
    - Tener un ciclo de adquisición de hardware largo
    - Requerirle que aprovisione capacidad adivinando picos máximos teóricos

## Modelo de computación en la nube

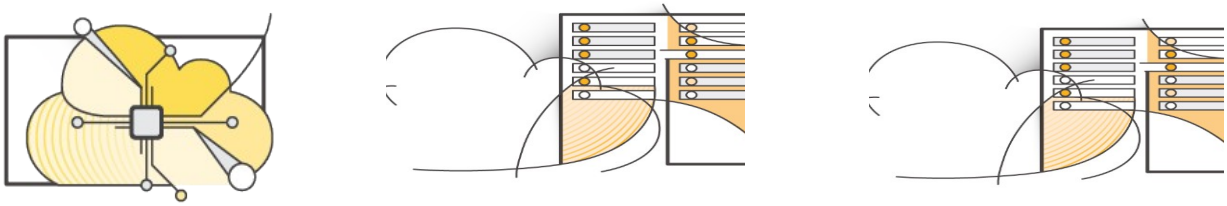
- Infraestructura como software
- Soluciones de software:
    - Son flexibles
    - Puede cambiar de forma más rápida, sencilla y rentable que las soluciones de hardware
    - Elimina las tareas pesadas indiferenciadas

## Modelos de servicios en la nube




**Más control** **Menos control**

## Modelos de implantación de la computación en nube



**Cloud** **Híbrido** **A demanda**

## Resumen

- La computación en nube es la entrega de recursos informáticos bajo demanda a través de Internet con precios de pago por uso.
- La computación en nube le permite pensar (y utilizar) su infraestructura como un software.
- Hay tres modelos de servicio en la nube: IaaS, PaaS y SaaS.
- Hay tres modelos de despliegue en la nube: nube, híbrido y en las instalaciones o nube privada.
- Casi todo lo que se puede implementar con la TI tradicional también se puede implementar como un servicio de computación en la nube de AWS.

## 1.2. Ventajas.

Pagar sólo por la cantidad que se consume.

Grandes economías de escala

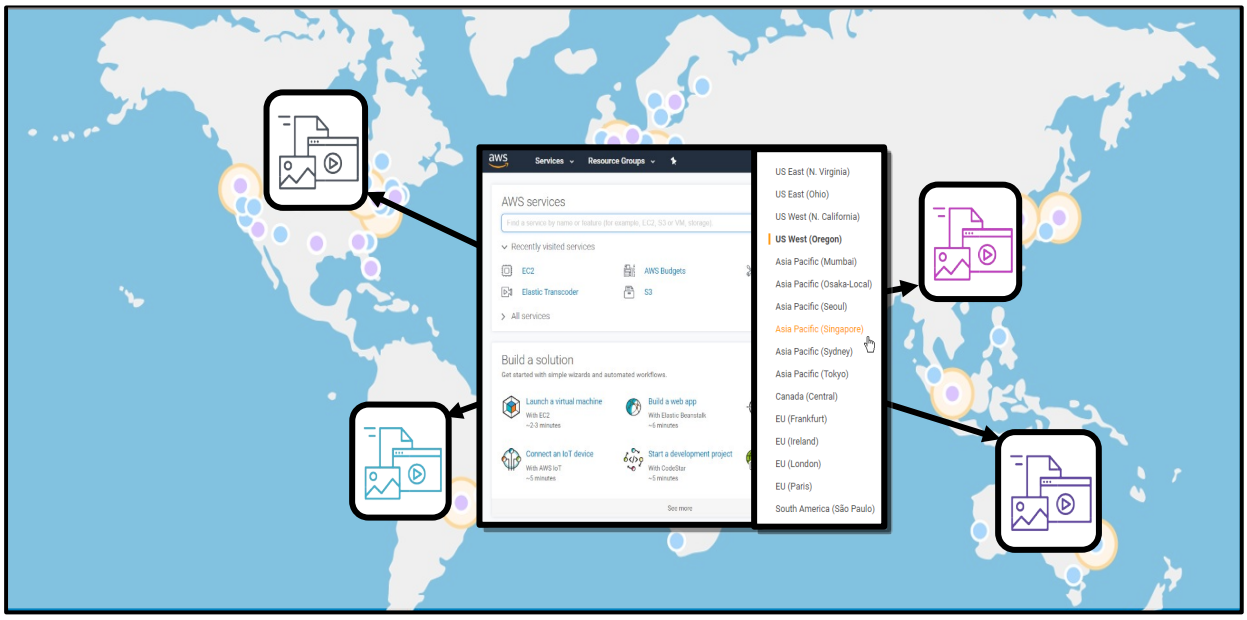
Debido al uso agregado de todos los clientes, AWS puede lograr mayores economías de escala y trasladar el ahorro a los clientes.

Aumentar la velocidad y la agilidad

Pocos minutos entre querer los recursos y obtenerlos.

Dejar de gastar dinero en el funcionamiento y el mantenimiento de los centros de datos.

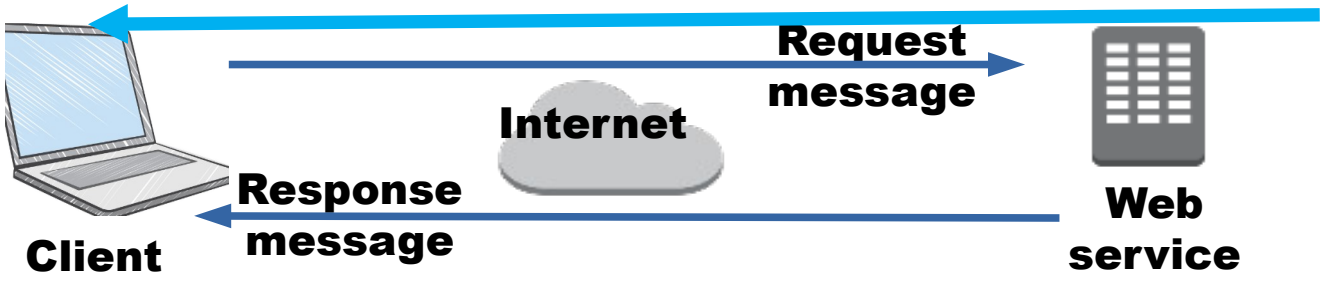
Globalizar en minutos



## 1.3. Introducción a Amazon Web Services (AWS)

### ¿Qué son los servicios web?

Un servicio web es cualquier pieza de software que se pone a disposición a través de Internet y utiliza un formato estandarizado -como el Lenguaje de Marcado Extensible (XML) o la Notación de Objetos de JavaScript (JSON)- para la solicitud y la respuesta de una interacción de interfaz de programación de aplicaciones (API).

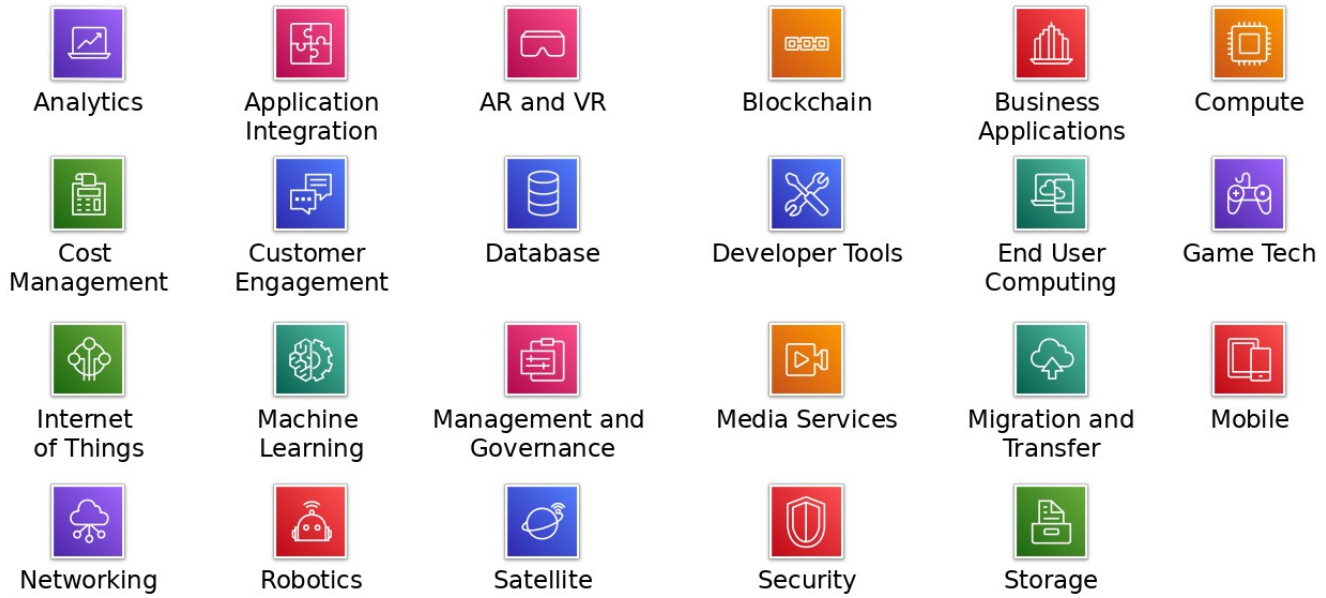



### ¿Qué es AWS?

- AWS es una plataforma de nube segura que ofrece un amplio conjunto de productos globales basados en la nube.
- AWS proporciona acceso bajo demanda a recursos informáticos, de almacenamiento, de red, de bases de datos y otros recursos de TI y herramientas de gestión.
- AWS ofrece flexibilidad.
- Pagar sólo por los servicios individuales necesarios, durante el tiempo que los utilice.
- Los servicios de AWS funcionan juntos como bloques de construcción.

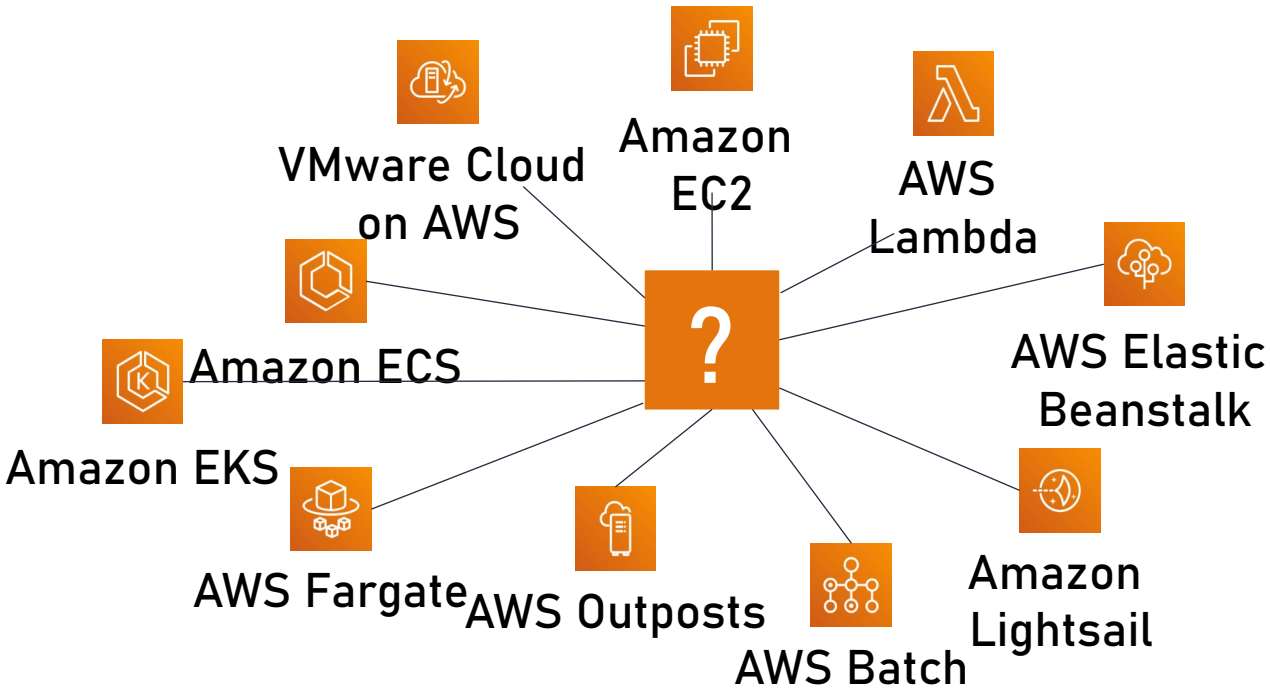
## Categorías de los servicios AWS

Los servicios de aws se dividen en diferentes categorías y cada categosría contiene uno o más servicios.




## Choosing a service

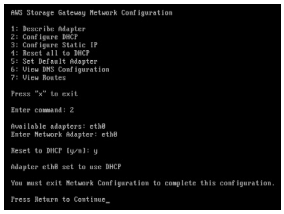
El servicio a elegir dependerá de los objetivos de la empresa y de las necesidades tecnológicas. Por ejemplo, Amazon EC2 permite el control total sobre los recursos computacionales y la infraestructura. AWS Lambda permite ejecutar código sin gestionar servidores. AWS Elastic Beantalk permite proporcionar un servicio que luego despliega, gestiona y escala las aplicaciones web de manera automática. Amazon Ligthsail es una plataforma para una aplicación web simple.



## Tres formas de interactuar con AWS

**Consola de administración de AWS**

Interfaz gráfica fácil de usar




**Interfaz de línea de comandos (AWS CLI)**

Acceso a los servicios mediante comandos o scripts discretos


**Kits de desarrollo de software (SDK)**

Acceso a servicios directamente desde código (como Java, Python..)

## Resumen

- AWS es una plataforma en la nube segura que ofrece un amplio conjunto de productos globales basados en la nube llamados servicios que están diseñados para trabajar juntos.
- Hay muchas categorías de servicios de AWS, y cada categoría tiene muchos servicios entre los que elegir.
- Elección de servicio en función de los objetivos empresariales y los requisitos tecnológicos.
- Hay tres formas de interactuar con los servicios de AWS.

## 2. Alta usuario AWS Academy.

En el buzón de entrada debes tener un correo cuyo remitente es AWS Academy.

You have been invited to participate in the course, AWS Academy Cloud Foundations [17782]. Course role: Student

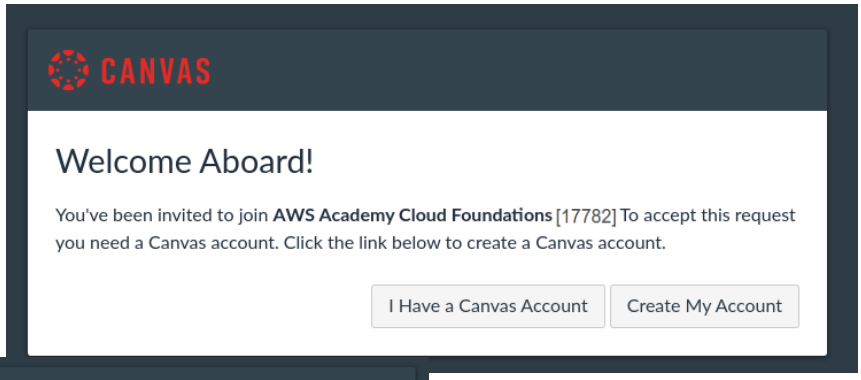
Name: **AnaAula**
Email: **anagonzalezjorge@gmail.com**

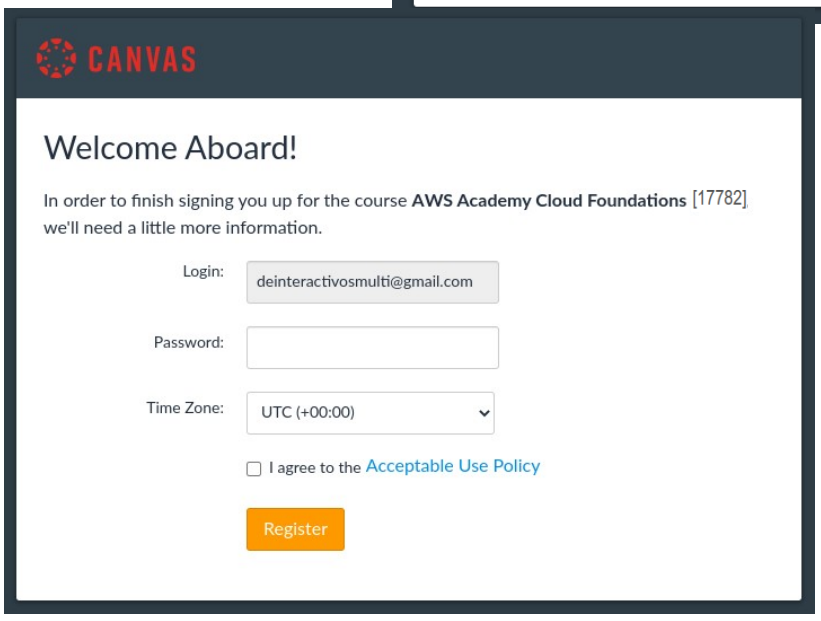
**Get started**

CANVAS

Click here to view the course page | Update your notification settings

Acceder y crear cuenta.

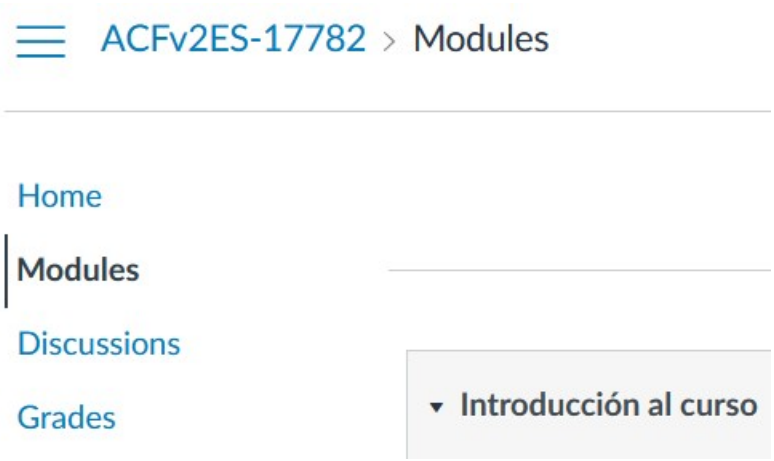


Añadir estos datos en la fila Acceso CANVAS en el documento de credenciales (Credenciales.ods).

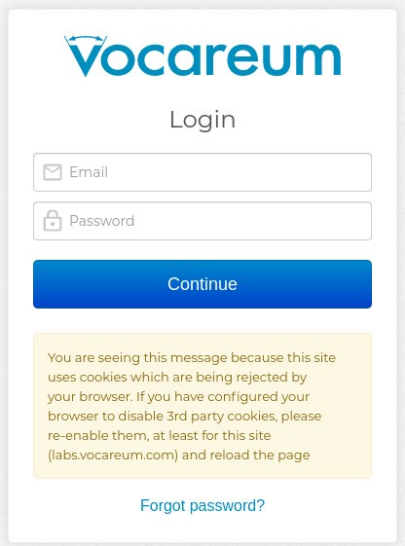
| | |
|---|---|
| Curso | ACFv2ES-17782 |
| Acceso lab | anagonzalezjorge@gmail.com / |

Acceder al curso ACFv2ES-17782, a la sección Módulos.

Acceder a la siguiente URL: **https://labs.vocareum.com/main**

Se muestra una pantalla de Login, añadir los valores indicados para la cuenta de CANVAS:




Añadir estos datos en la fila Acceso Vocarerum  en el documento de credenciales (Credenciales.ods).

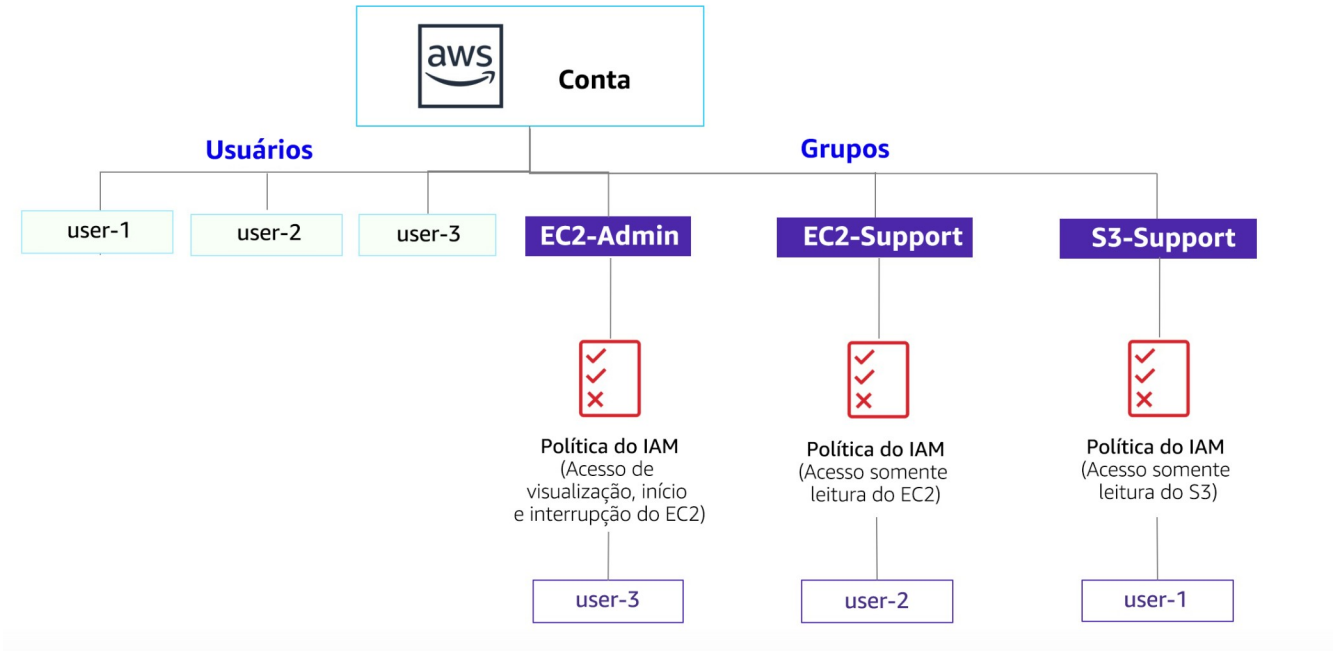
| | |
|---|---|
| **Curso** | ACFv2ES-17782 |

## Laboratorio 1: Introducción a AWS IAM (Obligatorio)

**AWS Identity and Access Management (IAM)** es un servicio web que permite a los clientes de Amazon Web Services (AWS) administrar los usuarios y los permisos de usuario en AWS. Con IAM, puede administrar de forma centralizada los usuarios, las credenciales de seguridad, como las claves de acceso y los permisos, que controlan a qué recursos de AWS pueden acceder los usuarios.

### Temas

En este laboratorio, aprenderá a completar las siguientes tareas:




•Analizar los usuarios y los grupos de IAM creados previamente

•Inspeccionar las políticas de IAM, según se apliquen a los grupos creados previamente

•Según una situación real, agregar usuarios a los grupos con capacidades específicas habilitadas

•Ubicar y usar la dirección URL de inicio de sesión de IAM

•Probar los efectos de las políticas en el acceso a los servicios

## Otros servicios de AWS

Durante el laboratorio, es posible que aparezcan mensajes de error cuando intente realizar acciones que no se ajusten a los pasos incluidos en esta guía de laboratorio. Estos mensajes no afectarán su capacidad para completar el laboratorio.

## AWS Identity and Access Management

AWS Identity and Access Management (IAM) se puede utilizar para lo siguiente:

•Administrar usuarios de IAM y su acceso: puede crear usuarios y asignarles credenciales de seguridad individuales (claves de acceso, contraseñas y dispositivos de autenticación multifactor). Puede administrar los permisos para controlar qué operaciones puede realizar cada usuario.

•Administrar roles de IAM y sus permisos: un rol de IAM es similar a un usuario, ya que es una identidad de AWS con políticas de permisos que establecen qué puede hacer o no la identidad en AWS. Sin embargo, en lugar de estar asociada únicamente a una persona, el objetivo es que pueda asignarse un rol a cualquier persona que lo necesite.

•Administrar usuarios federados y sus permisos: puede habilitar la identidad federada a fin de permitir que los usuarios existentes de su empresa puedan acceder a la consola de administración de AWS, llamar a las API de AWS y acceder a los recursos, sin necesidad de crear un usuario de IAM para cada identidad.

Duración

La duración estimada de este laboratorio es de 40 minutos aproximadamente.

## Acceso a la consola de administración de AWS

0.

**1.**En la parte superior de estas instrucciones, haga clic en Start Lab (Iniciar laboratorio) para lanzar su laboratorio.

Se abrirá el panel “Start Lab” (Iniciar laboratorio), donde se muestra el estado del laboratorio. En el cuadro de diálogo Start Lab (Iniciar laboratorio) que se abre, tenga en cuenta la región de AWS, ya que deberá consultarla más adelante en este laboratorio.

**2.**Espere hasta que aparezca el mensaje “Lab status: ready” (Estado del laboratorio: listo) y, luego, haga clic en la X para cerrar el panel “Start Lab (Iniciar laboratorio)”.

3.En la parte superior de estas instrucciones, haga clic en AWS .

La consola de administración de AWS se abrirá en una nueva pestaña del navegador. El sistema iniciará su sesión automáticamente.

Sugerencia: Si no se abre una pestaña nueva del navegador, debería aparecer un banner o un icono en la parte superior de este, el cual indique que el navegador no permite que se abran ventanas emergentes en el sitio. Haga clic en el banner o en el icono, y elija “Allow pop ups” (Permitir ventanas emergentes).

4.Ubique la pestaña de la consola de administración de AWS en un lugar donde aparezca al lado de estas instrucciones. Idealmente, debería poder ver ambas pestañas del navegador al mismo tiempo para que sea más sencillo seguir los pasos del laboratorio.

### Tarea 1: analizar los usuarios y los grupos

En esta tarea, analizará los usuarios y los grupos que ya se crearon para usted en IAM.

**5.**En la consola de administración de AWS, encontrará el menú Services (Servicios), donde debe hacer clic en IAM.
**6.**En el panel de navegación izquierdo, haga clic en Users (Usuarios).
Ya se crearon los siguientes usuarios de IAM para usted:
•user-1

•user-2

•user-3

**7.**Haga clic en user-1 (usuario-1).

Esto le mostrará la página de resumen de usuario-1. Se visualizará la pestaña Permissions (Permisos).

8.Observe que usuario-1 no tiene permisos.

**9.**Haga clic en la pestaña Groups (Grupos).

Usuario-1 tampoco es miembro de ningún grupo.
**10.**Haga clic en la pestaña Security credentials (Credenciales de seguridad).
Usuario-1 tiene asignada una contraseña de consola
**11.**En el panel de navegación izquierdo, haga clic en Groups (Grupos).
Ya se crearon los siguientes grupos para usted:
•EC2-Admin

•EC2-Support

•S3-Support

**12.**Haga clic en el grupo EC2-Support.

Esto le mostrará la página de resumen del grupo EC2-Support.

**13.**Haga clic en la pestaña Permissions (Permisos).

Este grupo está asociado a una política administrada que se llama AmazonEC2ReadOnlyAccess. Las políticas administradas son aquellas diseñadas con anterioridad (creadas por sus administradores o por AWS) que se pueden asociar a grupos y a usuarios de IAM. Cuando la política se actualiza, los cambios se implementan inmediatamente en todos los usuarios y los grupos que tiene asociados.

**14.**En Actions (Acciones), haga clic en el enlace Show Policy (Mostrar política).

Una política define qué acciones se permiten o rechazan para determinados recursos de AWS. Esta política concede permiso para describir e incluir en listas información acerca de EC2, Elastic Load Balancing, CloudWatch y Auto Scaling. Esta capacidad que permite ver recursos, pero no modificarlos, es ideal como rol de soporte.

La estructura básica de las declaraciones de una política de IAM es la siguiente:

•Effect (Efecto) determina si los permisos se conceden (Allow) o rechazan (Deny).

•Action (Acción) especifica las llamadas a la API que se pueden efectuar respecto de un servicio de AWS (p. ej., cloudwatch:ListMetrics).

•Resource (Recurso) define el alcance de las entidades cubiertas por la regla de la política (p. ej., un bucket de Amazon S3 o una instancia de Amazon EC2 específicos, o bien, * que significa cualquier recurso).

**15.**Cierre la ventana Show Policy (Mostrar política).

**16.**En el panel de navegación izquierdo, haga clic en Groups (Grupos).

**17.**Haga clic en el grupo S3-Support.

El grupo S3-Support está asociado a la política AmazonS3ReadOnlyAccess.

**18.**En el menú Actions (Acciones), haga clic en el enlace Show Policy (Mostrar política).

La política tiene permisos GET y LIST sobre los recursos en Amazon S3.

**19.**Cierre la ventana Show Policy (Mostrar política).

**20.**En el panel de navegación izquierdo, haga clic en Groups (Grupos).

**21.**Haga clic en el grupo EC2-Admin.

Este grupo difiere levemente de los otros dos. En vez de una política administrada, tiene una política insertada, la cual es una política asignada a un único usuario o grupo. Las políticas insertadas, en general, se usan para asignar permisos en caso de situaciones aisladas.

**22.**Para ver la política, vaya a Actions (Acciones) y haga clic en Show Policy (Mostrar política).

La política concede permiso para ver información descriptiva de Amazon EC2 y también de la capacidad de iniciar o detener instancias.

**23.**Para cerrar la política, vaya a la parte inferior de la pantalla y haga clic en Cancel (Cancelar).

### Situación empresarial

Durante el resto del laboratorio, trabajaremos con estos usuarios y grupos para habilitar los permisos que admiten la siguiente situación empresarial:

Su compañía aprovecha Amazon Web Services cada vez más, y utiliza muchas instancias de Amazon EC2 y un gran volumen de almacenamiento de Amazon S3. Usted desea otorgar acceso a personal nuevo según su función laboral:

| Usuario | En grupo | Permisos |
|---|---|---|
| user-1 | S3-Support | Acceso de solo lectura a Amazon S3 |
| user-2 | EC2-Support | Acceso de solo lectura a Amazon EC2 |
| user-3 | EC2-Admin | Visualizar, iniciar y detener instancias de Amazon EC2 |

### Tarea 2: agregar usuarios a los grupos

Recientemente contrató a user-1 (usuario-1) para un rol que brindará soporte a Amazon S3. Lo agregará al grupo S3-Support para que pueda heredar los permisos necesarios mediante la política AmazonS3ReadOnlyAccess asociada.

Durante esta tarea, puede ignorar cualquier error que incluya el texto “not authorized” (no autorizado). Se provocan porque su cuenta de laboratorio tiene permisos limitados, pero esto no afectará su capacidad para completar el laboratorio.

#### Agregue a “user-1” (usuario-1) al grupo S3-Support.

**24.**En el panel de navegación izquierdo, haga clic en Groups (Grupos).

**25.**Haga clic en el grupo S3-Support.

**26.**Haga clic en la pestaña Users (Usuarios).

**27.**En la pestaña Users (Usuarios), haga clic en Add Users to Group (Agregar usuarios al grupo).

**28.**En la ventana Add Users to Group (Agregar usuarios al grupo), configure los siguientes parámetros:

•Seleccione user-1.

•En la parte inferior de la pantalla, haga clic en Add Users (Agregar usuarios).

En la pestaña Users (Usuarios), verá que “user-1” (usuario-1) se agregó al grupo.

#### Agregue a “user-2” (usuario-2) al grupo EC2-Support.

Contrató a user-2 (usuario-2) para un rol que brindará soporte a Amazon EC2.

**29.**Mediante pasos similares a los anteriores, agregue a user-2 (usuario-2) al grupo EC2-Support.
Ahora, “user-2” (usuario-2) debería formar parte del grupo EC2-Support.

### Agregue a “user-3” (usuario-3) al grupo EC2-Admin.

Contrató a user-3 (usuario-3) como administrador de Amazon EC2 para que se encargue de administrar sus instancias EC2.

**30.**Mediante pasos similares a los anteriores, agregue a user-3 (usuario-3) al grupo EC2-Admin.

Ahora, “user-3” (usuario-3) debería formar parte del grupo EC2-Admin.

**31.**En el panel de navegación izquierdo, haga clic en Groups (Grupos).

Cada grupo debería tener un 1 en la columna “Users” (Usuarios) como representación de la cantidad de usuarios en cada grupo.

Si no se muestra un 1 junto a cada grupo, revise las instrucciones anteriores para asegurarse de que cada usuario esté asignado a un grupo, como se muestra en la tabla de la sección “Situación empresarial”.

### Tarea 3: iniciar sesión y probar usuarios

En esta tarea, probará los permisos de cada usuario de IAM.

**32.**En el panel de navegación izquierdo, haga clic en Dashboard (Panel).
Se muestra un enlace de inicio de sesión para usuarios de IAM. Será similar a https://123456789012.signin.aws.amazon.com/console

El enlace se puede usar para iniciar sesión en la cuenta de AWS que está usando en este momento.

**33.**Copie el enlace de inicio de sesión para usuarios de IAM en un editor de texto.

34.Abra una ventana privada.

**Mozilla Firefox**

•Haga clic en las barras de menú de la parte superior derecha de la pantalla.

•Seleccione New Private Window (Nueva ventana privada).

**Google Chrome**

•Haga clic en los puntos suspensivos de la parte superior derecha de la pantalla.

•Haga clic en New incognito window (Nueva ventana de incógnito).

**Microsoft Edge**

•Haga clic en los puntos suspensivos de la parte superior derecha de la pantalla.

•Haga clic en New InPrivate window (Ventana InPrivate nueva).

**Microsoft Internet Explorer**

•Haga clic en la opción de menú Tools (Herramientas).

•Haga clic en InPrivate Browsing (Navegación InPrivate).

**35.**Pegue el enlace de inicio de sesión para usuarios de IAM en la ventana privada y presione Enter (Intro).

Ahora iniciará sesión como user-1 (usuario-1), a quien se contrató como personal de soporte para el almacenamiento de Amazon S3.

36.Inicie sesión con los siguientes datos:

•IAM user name (Nombre de usuario de IAM): `user-1`

•Contraseña: `Lab-Password1`

**37.**En el menú Services (Servicios), haga clic en S3.

38.Haga clic en el nombre de uno de los buckets y examine el contenido.

Dado que el usuario forma parte del grupo S3-Support en IAM, tiene permiso para ver una lista de buckets de Amazon S3 y su contenido.

Ahora, pruebe si tienen acceso a Amazon EC2.

**39.**En el menú Services (Servicios), haga clic en EC2.

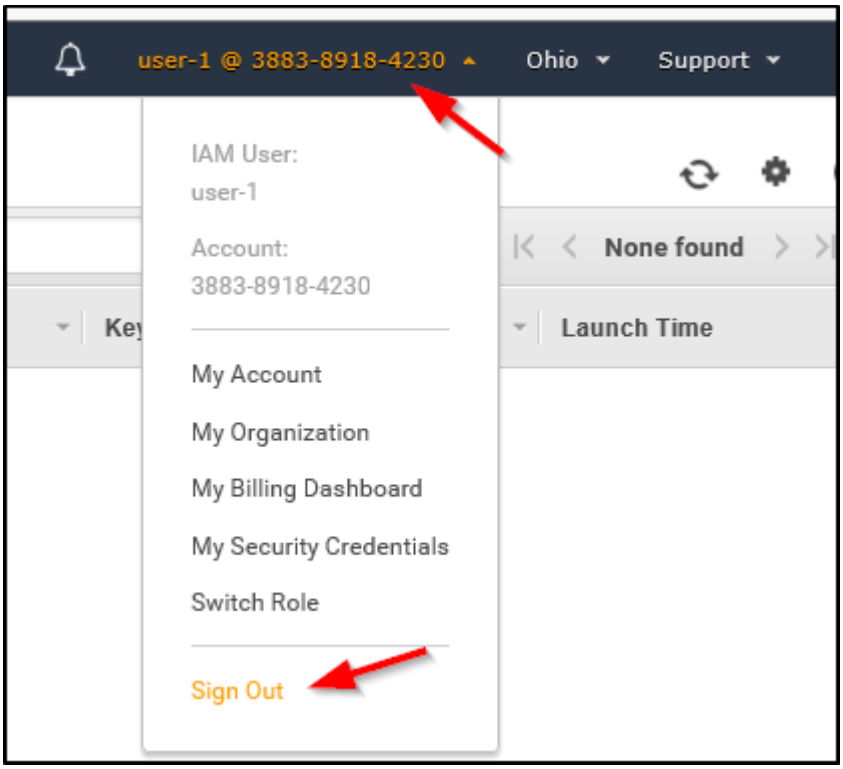
**40.**En el panel de navegación de la izquierda, haga clic en Instances (Instancias).
No puede ver ninguna instancia. En su lugar, dice que no tiene ninguna instancia en esta región. Esto se debe a que al usuario no se le otorgó ningún permiso para usar Amazon EC2.

Ahora iniciará sesión como user-2 (usuario-2), a quien se contrató como personal de soporte para Amazon EC2.

**41.**Cierre la sesión de “user-1” (usuario-1) en la consola de administración de AWS mediante la configuración de los siguientes parámetros:

•En la parte superior de la pantalla, haga clic en user-1 (usuario-1).

•Haga clic en Sign Out (Cerrar sesión).




**42.**Pegue el enlace de inicio de sesión para usuarios de IAM en la ventana privada y presione Enter (Intro).

Se debe visualizar este enlace en su editor de texto.

43.Inicie sesión con los siguientes datos:

•IAM user name (Nombre de usuario de IAM): user-2

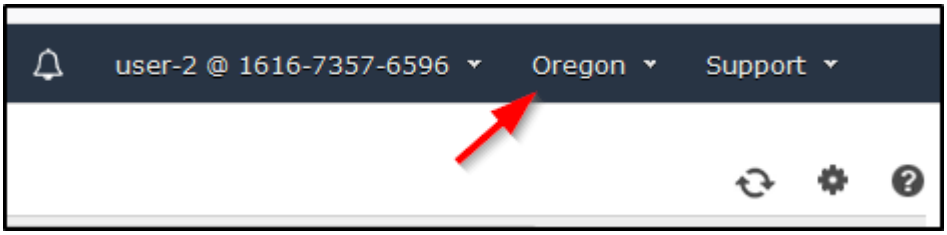
•Contraseña: Lab-Password2

**44.**En el menú Services (Servicios), haga clic en EC2.

**45.**En el panel de navegación izquierdo, haga clic en Instances (Instancias).

Ahora puede ver una instancia de Amazon EC2 porque tiene permisos de solo lectura. Sin embargo, no podrá realizar ninguna modificación en los recursos de Amazon EC2.

Si no puede ver una instancia de Amazon EC2, es posible que la región sea incorrecta. En la parte superior derecha de la pantalla, despliegue el menú “Region” (Región) y seleccione la región que anotó al principio del laboratorio (p. ej., N. Virginia [Virginia del Norte]).




Su instancia EC2 debería estar seleccionada . Si no lo está, selecciónela.

**46.**En el menú Actions (Acciones), haga clic en Instance State (Estado de la instancia) > Stop (Detener).

**47.**En la ventana Stop Instances (Detener instancias), haga clic en Yes, Stop (Sí, detener).


Verá un mensaje de error con el texto You are not authorized to perform this operation (No tiene autorización para realizar esta operación). Esto demuestra que la política solo le permite ver la información, pero no lo autoriza a realizar cambios.

**48.**En la ventana Stop Instances (Detener instancias), haga clic en Cancel (Cancelar).

Luego, verifique si “user-2” (usuario-2) puede acceder a Amazon S3.

**49.**En Services (Servicios), haga clic en S3.

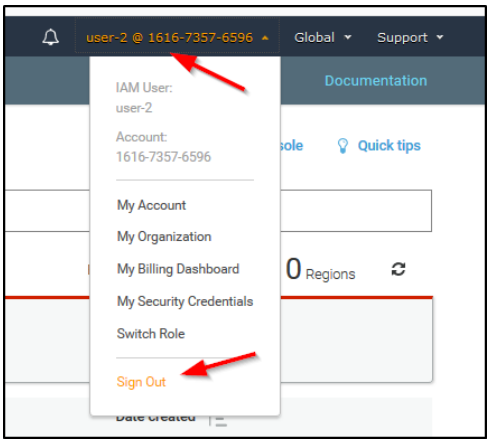
Recibirá el mensaje  Error Access Denied (Error de acceso denegado) porque el usuario-2 no tiene permiso para utilizar Amazon S3.

Ahora iniciará sesión como user-3 (usuario-3), a quien se contrató como administrador de Amazon EC2.

**50.**Cierre la sesión de “user-2” (usuario-2) en la consola de administración de AWS mediante la configuración de los siguientes parámetros:

•En la parte superior de la pantalla, haga clic en user-2 (usuario-2).

•Haga clic en Sign Out (Cerrar sesión).



**51.**Pegue el enlace de inicio de sesión para usuarios de IAM en la ventana privada y presione Enter (Intro).

52.Vuelva a pegar el enlace de inicio de sesión en la barra de direcciones del navegador web. Si no está en el portapapeles, recupérelo del editor de texto en el que lo guardó anteriormente.

53.Inicie sesión con los siguientes datos:

•IAM user name (Nombre de usuario de IAM): user-3

•Contraseña: Lab-Password3

**54.**En el menú Services (Servicios), haga clic en EC2.

**55.**En el panel de navegación izquierdo, haga clic en Instances (Instancias).

Como administrador de EC2, debería tener permisos para detener la instancia de Amazon EC2.
Su instancia EC2 debería estar seleccionada . Si no es así, selecciónela.

Si no puede ver una instancia de Amazon EC2, es posible que la región sea incorrecta. En la parte superior derecha de la pantalla, despliegue el menú “Region” (Región) y seleccione la región que anotó al principio del laboratorio (p. ej., Oregon [Oregón]).

**56.**En el menú Actions (Acciones), haga clic en Instance State (Estado de la instancia) > Stop (Detener).

**57.**En la ventana Stop Instances (Detener instancias), haga clic en Yes, Stop (Sí, detener).

La instancia ingresará al estado stopping (en proceso de detención) y se cerrará.

58.Cierre la ventana privada.

## Fin del laboratorio

¡Felicitaciones! Ha completado el laboratorio.

59.Haga clic en End Lab (Finalizar laboratorio) en la parte superior de esta página y, a continuación, en Yes (Sí) para confirmar que desea finalizar el laboratorio.

Aparecerá un panel en el que se indica: “DELETE has been initiated… You may close this message box now”. (Se ha iniciado la ELIMINACIÓN… Ya puede cerrar este cuadro de mensajes).

**60.**Haga clic en la X de la esquina superior derecha para cerrar el panel.

**Realizar una captura de pantalla de la sección de usuarios-grupos y añadir a la tarea de Moodle Lab1.**

## Laboratorio 2: Creación de una VPC y lanzamiento de un servidor web

En este laboratorio, deberá utilizar Amazon Virtual Private Cloud (VPC) para crear su propia VPC y agregarle componentes adicionales con el fin de generar una red personalizada. Además, creará grupos de seguridad para su instancia EC2. Luego, tendrá que configurar y personalizar una instancia EC2 para ejecutar un servidor web y lanzarlo en la VPC.

Amazon Virtual Private Cloud (Amazon VPC) le permite lanzar recursos de Amazon Web Services (AWS) en la red virtual que usted defina. Esta red virtual se asemeja en gran medida a una red tradicional que ejecutaría en su propio centro de datos, con los beneficios de utilizar la infraestructura escalable de AWS. Puede crear una VPC que abarque varias zonas de disponibilidad.

### Situación

En este laboratorio, creará la siguiente infraestructura:

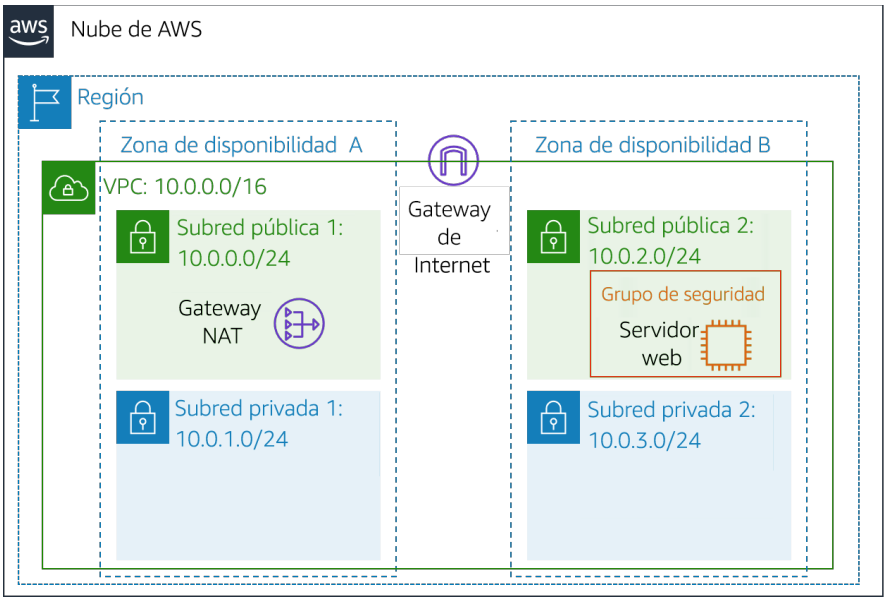



Tabla de enrutamiento pública

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

Tabla de enrutamiento pública

| Destino | Objetivo |
|---|---|
| 10.0.0.0/16 | Local |
| 0.0.0.0/0 | Gateway NAT |

### Objetivos

Después de completar este laboratorio, podrá hacer lo siguiente:

•Crear una VPC

•Crear subredes

•Configurar un grupo de seguridad

•Lanzar una instancia EC2 en una VPC

## Acceso a la consola de administración de AWS

0.En la parte superior de estas instrucciones, haga clic en Start Lab (Iniciar laboratorio) para lanzar su laboratorio.
Se abrirá el panel “Start Lab” (Iniciar laboratorio), donde se muestra el estado del laboratorio.
**1.**Espere hasta que aparezca el mensaje “Lab status: ready” (Estado del laboratorio: listo) y, luego, haga clic en la X para cerrar el panel “Start Lab (Iniciar laboratorio)”.
2.En la parte superior de estas instrucciones, haga clic en AWS.
La consola de administración de AWS se abrirá en una nueva pestaña del navegador. El sistema iniciará su sesión automáticamente.
Sugerencia: Si no se abre una pestaña nueva del navegador, debería aparecer un banner o un icono en la parte superior de este, el cual indique que el navegador no permite que se abran ventanas emergentes en el sitio. Haga clic en el banner o en el icono, y elija “Allow pop ups” (Permitir ventanas emergentes).
3.Ubique la pestaña de la consola de administración de AWS en un lugar donde aparezca al lado de estas instrucciones. Idealmente, debería poder ver ambas pestañas del navegador al mismo tiempo para que sea más sencillo seguir los pasos del laboratorio.

---

## Tarea 1: crear una VPC

En esta tarea, utilizará el asistente de VPC para crear una VPC, una gateway de Internet y dos subredes en una única zona de disponibilidad. Una gateway de Internet (IGW) es un componente de la VPC que permite la comunicación entre instancias de la VPC e Internet.

Después de crear una VPC, puede agregar subredes. Cada subred está ubicada por completo dentro de una zona de disponibilidad y no puede abarcar otras zonas. Si el tráfico de una subred se direcciona a una gateway de Internet, la subred recibe el nombre de subred pública. Si una subred no dispone de una ruta a la gateway de Internet, recibe el nombre de subred privada.

El asistente también creará una Gateway NAT, que se utiliza para proporcionar conectividad a Internet a instancias EC2 en las subredes privadas.

**5.**En la consola de administración de AWS, encontrará el menú **Services** (Servicios), donde debe hacer clic en VPC.
6.Haga clic en **Launch VPC Wizard** (Lanzar asistente de VPC).
**7.**En el panel de navegación izquierdo, haga clic en VPC with Public and Private Subnets (VPC con subredes públicas y privadas), la segunda opción.
8.Haga clic en **Select** (Seleccionar) y, luego, configure lo siguiente:

•VPC name (Nombre de la VPC): Lab VPC

•Availability Zone (Zona de disponibilidad): seleccione la primera zona de disponibilidad

•Public subnet name (Nombre de la subred pública): Public Subnet 1 (Subred pública 1)

•Availability Zone (Zona de disponibilidad): seleccione la primera zona de disponibilidad (la misma que utilizó anteriormente).

•Private subnet name (Nombre de la subred privada): Private Subnet 1 (Subred privada 1)

•Elastic IP Allocation ID (ID de asignación de IP elástica): haga clic en el cuadro y seleccione la dirección IP que se muestra.

9.Haga clic en **Create VPC** (Crear VPC)
El asistente creará la VPC.
10.Una vez que la configuración esté completa, haga clic en **OK** (Aceptar).
El asistente ha aprovisionado una VPC con una subred pública y una subred privada en la misma zona de disponibilidad, junto con tablas de enrutamiento para cada subred:

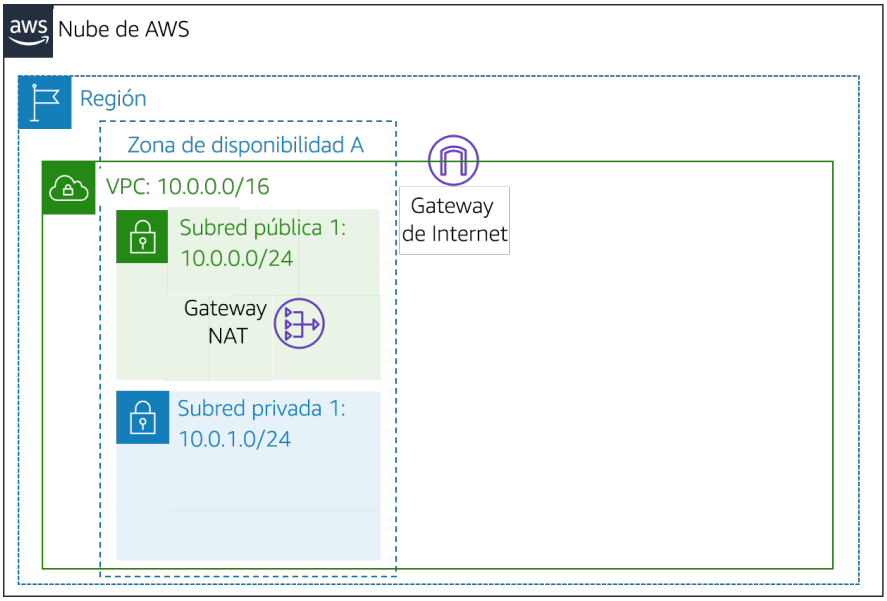



Tabla de enrutamiento pública

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

Tabla de enrutamiento pública

| Destino | Objetivo |
|---|---|
| 10.0.0.0/16 | Local |
| 0.0.0.0/0 | Gateway NAT |

La subred pública tiene un CIDR de 10.0.0.0/24, lo que significa que contiene todas las direcciones IP que comienzan con 10.0.0.x.

La subred privada tiene un CIDR de 10.0.1.0/24, lo que significa que contiene todas las direcciones IP que comienzan con 10.0.1.x.

### Tarea 2: crear subredes adicionales

En esta tarea, creará dos subredes adicionales en una segunda zona de disponibilidad. Esto resulta útil a la hora de crear recursos en varias zonas de disponibilidad para ofrecer una alta disponibilidad.

**11.**En el panel de navegación de la izquierda, haga clic en Subnets (Subredes).
Primero, creará una segunda subred pública.
12.Haga clic en **Create subnet** (Crear subred) y, luego, configure lo siguiente:
•Name tag (Etiqueta de nombre): Public Subnet 2 (Subred pública 2)

•VPC: VPC de laboratorio

•Availability Zone (Zona de disponibilidad): seleccione la segunda zona de disponibilidad

•IPv4 CIDR block (Bloque de CIDR IPv4): 10.0.2.0/24

La subred tendrá todas las direcciones IP que comiencen con 10.0.2.x.
13.Haga clic en **Create** (Crear) y, posteriormente, en **Close** (Cerrar).
Ahora creará una segunda subred privada.
14.Haga clic en **Create subnet** (Crear subred) y, luego, configure lo siguiente:
•Name tag (Etiqueta de nombre): Private Subnet 2 (Subred privada 2)

•VPC: VPC de laboratorio

•Availability Zone (Zona de disponibilidad): seleccione la segunda zona de disponibilidad

•CIDR block (Bloque de CIDR): 10.0.3.0/24

La subred tendrá todas las direcciones IP que comiencen con 10.0.3.x.
15.Haga clic en **Create** (Crear) y, posteriormente, en **Close** (Cerrar).
Ahora, configurará las subredes privadas para dirigir el tráfico orientado hacia Internet a la gateway NAT a fin de que los recursos de la subred privada puedan conectarse a Internet, a la vez que mantienen los recursos privados. Esto se realiza mediante la configuración de una tabla de enrutamiento.
Una tabla de enrutamiento contiene un conjunto de reglas llamadas rutas que se utilizan para determinar el destino del tráfico de red. Cada subred de una VPC debe estar asociada a una tabla de enrutamiento, que es la que controla el direccionamiento de la subred.
**16.**En el panel de navegación de la izquierda, haga clic en Route Tables (Tablas de enrutamiento).
**17.**Seleccione la tabla de enrutamiento con Main = Yes (Principal = Sí) y VPC = Lab VPC. (Si fuera necesario, expanda la columna _VPC ID [ID de VPC] _ para ver el nombre de la VPC).
**18.**En el panel inferior, haga clic en la pestaña Routes (Rutas).
Tenga en cuenta que Destination 0.0.0.0/0 (Destino 0.0.0.0/0) está establecido en Target nat-xxxxxxxx (Objetivo nat-xxxxxxxx). Esto significa que el tráfico destinado a Internet (0.0.0.0/0) se enviará a la gateway NAT. Luego, la Gateway NAT reenviará el tráfico a Internet.

Por lo tanto, esta tabla de enrutamiento se utiliza para direccionar el tráfico desde subredes privadas. Ahora, agregará un nombre a la tabla de enrutamiento para que sea más fácil de reconocer en el futuro.

**19.**En la columna Name (Nombre) de esta tabla de enrutamiento, haga clic en el lápiz y, a continuación, escriba Private Route Table (Tabla de enrutamiento privada) y haga clic en

**20.**En el panel inferior, haga clic en la pestaña Subnet Associations (Asociaciones de subredes).

Ahora, asociará esta tabla de enrutamiento a las subredes privadas.

21.Haga clic en **Edit subnet associations** (Editar asociaciones de subredes).

**22.**Seleccione ambas subredes: Private Subnet 1 (Subred privada 1) y Private Subnet 2 (Subred privada 2).

Puede ampliar la columna Subnet ID (ID de subred) para visualizar los nombres de las subredes.

23.Haga clic en **Save** (Guardar).

Ahora, configurará la tabla de enrutamiento que utilizan las subredes públicas.

**24.**Seleccione la tabla de enrutamiento con Main = No (Principal = No) y VPC = Lab VPC, y anule la selección de cualquier otra subred.

**25.**En la columna Name (Nombre) de esta tabla de enrutamiento, haga clic en el lápiz y, a continuación, escriba Public Route Table (Tabla de enrutamiento pública) y haga clic en

**26.**En el panel inferior, haga clic en la pestaña Routes (Rutas).

Tenga en cuenta que Destination 0.0.0.0/0 (Destino 0.0.0.0/0) está establecido en Target igw-xxxxxxxx (Objetivo igw-xxxxxxxx), que es la gateway de Internet. Esto significa que el tráfico orientado hacia Internet se enviará directamente a Internet mediante la gateway de Internet.

Ahora, asociará esta tabla de enrutamiento a las subredes públicas.

**27.**Haga clic en la pestaña Subnet Associations (Asociaciones de subredes).

28.Haga clic en **Edit subnet associations (Editar asociaciones de subredes)**.

**29.**Seleccione ambas subredes: Public Subnet 1 (Subred pública 1) y Public Subnet 2 (Subred pública 2).

30.Haga clic en **Save** (Guardar).

La VPC ahora tiene subredes públicas y privadas configuradas en dos zonas de disponibilidad:

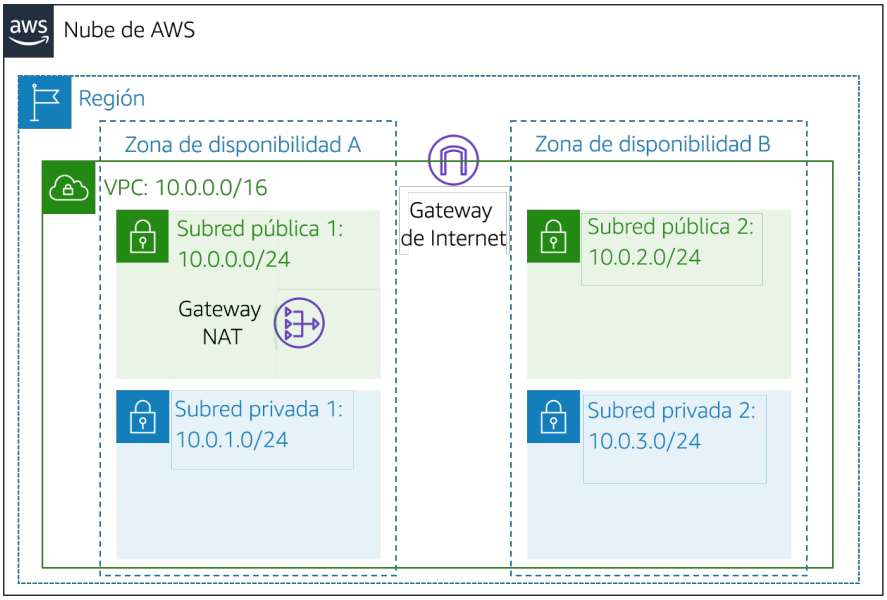



Tabla de enrutamiento pública

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

Tabla de enrutamiento pública

| Destino | Objetivo |
|---|---|
| 10.0.0.0/16 | Local |
| 0.0.0.0/0 | Gateway NAT |

---

### Tarea 3: crear un grupo de seguridad de VPC

En esta tarea, creará un grupo de seguridad de VPC, que actúa como un firewall virtual. Cuando se lanza una instancia, se asocia uno o varios grupos de seguridad a ella. Puede agregar reglas a cada grupo de seguridad que permitan el tráfico hacia las instancias asociadas o desde ellas.

**31.**En el panel de navegación izquierdo, haga clic en Security Groups (Grupos de seguridad).

32.Haga clic en **Create security group** (Crear grupo de seguridad) y, a continuación, configure lo siguiente:

•Security group name (Nombre del grupo de seguridad): Web Security Group (Grupo de seguridad web)

•Description (Descripción): Enable HTTP access (Habilitar acceso HTTP)

•VPC: VPC de laboratorio

**33.**En el panel Inbound rules (Reglas de entrada), seleccione **Add rule** (Agregar regla)

34.Configure los siguientes ajustes:

•Type (Tipo): HTTP

•Source (Origen): Anywhere (Cualquiera)

•Description (Descripción): Permit web requests (Permitir solicitudes web)

35.Desplácese hasta la parte inferior de la página y seleccione **Create security group** (Crear grupo de seguridad)

Utilizará este grupo de seguridad en la siguiente tarea a la hora de lanzar una instancia de Amazon EC2.

---

### Tarea 4: lanzar una instancia de servidor web

En esta tarea, lanzará una instancia de Amazon EC2 en la nueva VPC. Configurará la instancia para que actúe como un servidor web.

**39.**En el menú **Services (Servicios),** haga clic en EC2.

40.Haga clic en **Launch Instance** (Lanzar instancia) y, a continuación, seleccione **Launch Instance** (Lanzar instancia)

Primero, seleccionará una Imagen de Amazon Machine (AMI), la cual contiene el sistema operativo deseado.

**41.**En la fila de Amazon Linux 2 (en la parte superior), haga clic en **Select** (Seleccionar)

El tipo de instancia define los recursos de hardware asignados a la instancia.

**42.**Seleccione t2.micro, que se muestra en la columna Type (Tipo).

43.Haga clic en **Next: Configure Instance Details** (Siguiente: Configurar detalles de instancia).

Ahora, configurará la instancia para lanzarla en una subred pública de la nueva VPC.

44.Configure los siguientes ajustes:

•Network (Red): Lab VPC

•Subnet (Subred): Public Subnet 2 (Subred pública 2) (no privada)

•Auto-assign Public IP (Asignar automáticamente IP pública): Enable (Habilitar)

**45.**Expanda la sección Advanced Details (Detalles avanzados), en la parte inferior de la página.

**46.**Copie y pegue este código en el cuadro User data (Datos de usuario):

```
# Install Apache Web Server and PHP
yum install -y httpd mysql php
# Download Lab files
wget https://aws-tc-largeobjects.s3.us-west-2.amazonaws.com/CUR-TF-100-ACCLFO-2/2-lab2-vpc/s3/lab-app.zip
unzip lab-app.zip -d /var/www/html/
# Turn on web server
chkconfig httpd on
service httpd start
```

Este script se ejecutará automáticamente al lanzar la instancia por primera vez. El script carga y configura una aplicación web PHP.

47.Haga clic en **Next: Add Storage** (Siguiente: agregar almacenamiento).

Utilizará los ajustes de almacenamiento predeterminados.

48.Haga clic en **Next: Add Tags** (Siguiente: agregar etiquetas).

Las etiquetas se pueden utilizar para identificar recursos. Utilizará una etiqueta para asignar un nombre a la instancia.

49.Haga clic en **Add Tag** (Agregar etiqueta) y, luego, configure lo siguiente:

•Key (Clave): Name (Nombre)

•Value (Valor): Web Server 1 (Servidor web 1)

50.Haga clic en **Next: Configure Security Group** (Siguiente: Configurar grupo de seguridad).

Configurará la instancia para que utilice el Grupo de seguridad web que creó anteriormente.

**51.**Seleccione Select an existing security group (Seleccionar un grupo de seguridad existente)

**52.**Seleccione Web Security Group (Grupo de seguridad web).

Este es el grupo de seguridad que creó en la tarea anterior. Le dará acceso HTTP a la instancia.

53.Haga clic en **Review and Launch** (Revisar y lanzar).

**54.**Cuando se muestre un mensaje de advertencia en el que se indica que no podrá conectarse a la instancia a través del puerto 22, haga clic en **Continue** (Continuar)

55.Revise la información de la instancia y haga clic en **Launch** (Lanzar).

**56.**En el cuadro de diálogo Select an existing keypair (Seleccionar un par de claves existente), seleccione I acknowledge... (Acepto...).

57.Haga clic en **Launch Instances** (Lanzar instancias) y, a continuación, en **View Instances** (Visualizar instancias).

**58.**Espere a que Web Server 1 (Servidor web 1) muestre el mensaje 2/2 checks passed (2/2 comprobaciones aprobadas) en la columna Status Checks (Comprobaciones de estado).

Es posible que esto tarde unos minutos. Haga clic en “Refresh” (Actualizar) en la parte superior derecha cada 30 segundos para obtener actualizaciones.

Ahora se conectará al servidor web que se ejecuta en la instancia EC2.

**59.**Copie el valor Public DNS (IPv4) (DNS público [IPv4]) que aparece en la pestaña Description (Descripción), en la parte inferior de la página.

**60.**Abra una nueva pestaña en el navegador web, pegue el valor Public DNS (DNS público) y presione “Enter (Intro)”.

Verá una página web que muestra el logotipo de AWS y los valores de metadatos de instancias.

La arquitectura completa que ha implementado es la siguiente:

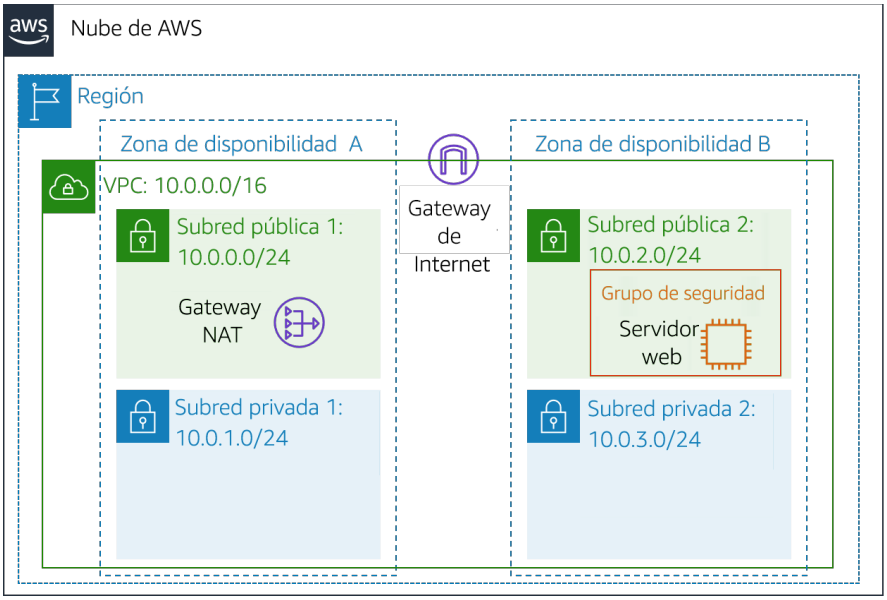



Tabla de enrutamiento pública

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

Tabla de enrutamiento pública

| Destino | Objetivo |
|---|---|
| 10.0.0.0/16 | Local |
| 0.0.0.0/0 | Gateway NAT |

## Fin del laboratorio

¡Felicitaciones! Ha completado el laboratorio.

61.Haga clic en End Lab (Finalizar laboratorio) en la parte superior de esta página y, a continuación, en Yes (Sí) para confirmar que desea finalizar el laboratorio.
Aparecerá un panel en el que se indica: “DELETE has been initiated… You may close this message box now”. (Se ha iniciado la ELIMINACIÓN… Ya puede cerrar este cuadro de mensajes).
**62.**Haga clic en la X de la esquina superior derecha para cerrar el panel.

# Laboratorio 3: Introducción a Amazon EC2

## Información general


En este laboratorio, se proporciona información general básica sobre el lanzamiento, la modificación del tamaño, la administración y el monitoreo de una instancia de Amazon EC2.

Amazon Elastic Compute Cloud (Amazon EC2) es un servicio web que proporciona capacidad informática con tamaño modificable en la nube. Está diseñado con el fin de simplificar la informática en la nube a escala web para los desarrolladores.

La sencilla interfaz de servicios web de Amazon EC2 permite obtener y configurar capacidad con una fricción mínima. Proporciona un control completo sobre los recursos informáticos y permite ejecutarse en el entorno informático acreditado de Amazon. Amazon EC2 reduce el tiempo necesario para obtener y arrancar nuevas instancias de servidor a solo minutos, lo que permite escalar rápidamente la capacidad, ya sea de forma ascendente o descendente, en función de sus necesidades.

Amazon EC2 cambia el modelo económico de la informática, y permite pagar solo por la capacidad que utiliza realmente. Amazon EC2 proporciona a los desarrolladores las herramientas necesarias para crear aplicaciones resistentes a errores y aislarse de los casos de error más comunes.

### Temas

•Lanzar un servidor web con la protección contra terminación habilitada

•Monitorear la instancia EC2

•Modificar el grupo de seguridad que utiliza el servidor web para permitir el acceso HTTP

•Modificar el tamaño de la instancia de Amazon EC2 a la escala necesaria

•Explorar los límites de EC2

•Probar la protección contra terminación

•Terminar la instancia EC2

## Acceso a la consola de administración de AWS

0.En la parte superior de estas instrucciones, haga clic en Start Lab (Iniciar laboratorio) para lanzar su laboratorio.
Se abrirá el panel “Start Lab” (Iniciar laboratorio), donde se muestra el estado del laboratorio.
**1.**Espere hasta que aparezca el mensaje “Lab status: ready” (Estado del laboratorio: listo) y, luego, haga clic en la X para cerrar el panel “Start Lab (Iniciar laboratorio)”.
2.En la parte superior de estas instrucciones, haga clic en AWS.
La consola de administración de AWS se abrirá en una nueva pestaña del navegador. El sistema iniciará su sesión automáticamente.
Sugerencia: Si no se abre una pestaña nueva del navegador, debería aparecer un banner o un icono en la parte superior de este, el cual indique que el navegador no permite que se abran ventanas emergentes en el sitio. Haga clic en el banner o en el icono, y elija “Allow pop ups” (Permitir ventanas emergentes).
3.Ubique la pestaña de la consola de administración de AWS en un lugar donde aparezca al lado de estas instrucciones. Idealmente, debería poder ver ambas pestañas del navegador al mismo tiempo para que sea más sencillo seguir los pasos del laboratorio.

## Tarea 1: Lanzar una instancia de Amazon EC2

En esta tarea, lanzará una instancia de Amazon EC2 con protección contra terminación. La protección contra terminación impide terminar una instancia EC2 por accidente. Implementará una instancia con un script de datos de usuario que le permitirá implementar un servidor web sencillo.

**5.**En el menú Services (Servicios) de la consola de administración de AWS, haga clic en EC2.

6.Elija Launch instance (Lanzar instancia) y, luego, seleccione Launch Instance (Lanzar instancia).

## Paso 1: Elegir una imagen de Amazon Machine (AMI)

Una Imagen de Amazon Machine (AMI) proporciona la información necesaria para lanzar una instancia, que es un servidor virtual en la nube. La AMI incluye lo siguiente:

•Una plantilla para el volumen raíz de la instancia (por ejemplo, un sistema operativo o un servidor de aplicaciones con aplicaciones)

•Permisos de lanzamiento que controlan qué cuentas de AWS pueden utilizar la AMI para lanzar instancias

•Una asignación de dispositivos de bloques que especifica los volúmenes que deben asociarse a la instancia cuando se lanza

En la lista de Quick Start, se incluyen las AMI más utilizadas. También puede crear su propia AMI o elegir una de AWS Marketplace, una tienda en línea donde se puede vender o comprar software que se ejecuta en AWS.

**7.**En la parte superior de la lista, haga clic en **Select** (Seleccionar), junto a **Amazon Linux 2 AMI** (AMI de Amazon Linux 2).

## Paso 2: Elegir el tipo de instancia

Amazon EC2 ofrece una amplia variedad de tipos de instancias optimizados para adaptarse a diferentes casos de uso. Los tipos de instancias abarcan distintas combinaciones de capacidad de CPU, memoria, almacenamiento y redes. Además, le proporcionan flexibilidad a la hora de elegir la combinación de recursos adecuada para sus aplicaciones. En cada tipo de instancia, se incluyen uno o más tamaños de instancia, lo que permite adaptar la escala de los recursos a los requisitos de la carga de trabajo de destino.

Utilizará una instancia t2.micro, que debería estar seleccionada de forma predeterminada. Este tipo de instancia posee 1 CPU virtual y 1 GiB de memoria. NOTA: Es posible que en este laboratorio no pueda usar otros tipos de instancia.

8.Haga clic en **Next: Configure Instance Details** (Siguiente: Configurar detalles de instancia).

## Paso 3: configurar los detalles de la instancia

Esta página se utiliza para configurar la instancia a fin de que cumpla con sus requisitos. Esto incluye la configuración de redes y de monitoreo.

En Network (Red), se define dentro de cuál nube virtual privada (VPC) se quiere lanzar la instancia. Se pueden tener varias redes diferentes para desarrollo, pruebas y producción.

**9.**En Network (Red), seleccione **Lab VPC**.

Lab VPC se creó con una plantilla de AWS CloudFormation durante el proceso de configuración del laboratorio. Esta VPC contiene dos subredes públicas en dos zonas de disponibilidad diferentes.

**10.**En **Enable termination** protection (Habilitar la protección de terminación), seleccione **Protect against accidental termination** (Proteger contra la terminación accidental).

Cuando una instancia de Amazon EC2 ya no es necesaria, se la puede terminar, lo que significa que se la detiene y se liberan sus recursos. No se puede volver a iniciar una instancia terminada. Si quiere evitar que la instancia se termine por accidente, puede habilitar la protección contra terminación para la instancia, que impide su terminación.

**11.**Desplácese hacia abajo y, a continuación, expanda **Advanced Details** (Detalles avanzados).

Aparecerá el campo **User data** (Datos de usuario).

Cuando lanza una instancia, puede transmitirle los datos de usuario, que se pueden utilizar para realizar tareas de configuración automatizadas comunes e, incluso, para ejecutar scripts después de iniciar la instancia.

Dado que la instancia ejecuta Amazon Linux, tendrá que proporcionar un script de shell que se ejecutará cuando se inicie la instancia.

**12.**Copie los siguientes comandos y péguelos en el campo User data (Datos de usuario):

```
yum -y install httpd
systemctl enable httpd
systemctl start httpd
echo '<html><h1>Hello From Your Web Server!</h1></html>' > /var/www/html/index.html
```

Este script permite hacer lo siguiente:

•Instalar un servidor web Apache (httpd)

•Configurar el servidor web para que se inicie automáticamente durante el arranque

•Activar el servidor web

•Crear una página web sencilla

13.Haga clic en **Next: Add Storage** (Siguiente: Agregar almacenamiento).

## Paso 4: Agregar almacenamiento

Amazon EC2 almacena los datos en un disco virtual asociado a la red que se denomina Elastic Block Store.

Se lanzará la instancia de Amazon EC2 con un volumen de disco predeterminado de 8 GiB. Este será el volumen raíz (también conocido como volumen “de arranque”).

14.Haga clic en **Next: Add Tags** (Siguiente: agregar etiquetas).

## Paso 5: agregar etiquetas

Las etiquetas le permiten clasificar los recursos de AWS de maneras diversas, por ejemplo, según su finalidad, propietario o entorno. Esto resulta útil cuando se tienen muchos recursos del mismo tipo; se puede identificar rápidamente un recurso específico con las etiquetas que se le han asignado. Cada etiqueta consta de una clave y un valor, los cuales usted define.

15.Haga clic en **Add Tag** (Agregar etiqueta) y, luego, configure lo siguiente:

•Key (Clave): Name (Nombre)

•Value (Valor): Web Server (Servidor web)

16.Haga clic en **Next: Configure Security Group** (Siguiente: Configurar grupo de seguridad).

## Paso 6: Configurar un grupo de seguridad

Un grupo de seguridad funciona como un firewall virtual que controla el tráfico de una o más instancias. Cuando se lanza una instancia, uno o más grupos de seguridad se asocian a ella. Se agregan reglas a cada grupo de seguridad que permiten que el tráfico fluya a sus instancias asociadas o desde ellas. Las reglas de un grupo de seguridad se pueden modificar en cualquier momento. Las nuevas reglas se aplican automáticamente a todas las instancias que estén asociadas al grupo de seguridad.

**17.**En el Paso 6: Configurar un grupo de seguridad, establezca los siguientes ajustes:

•Security group name (Nombre del grupo de seguridad): Web Server security group (Grupo de seguridad del servidor web)

•Description (Descripción): Security group for my web server (Grupo de seguridad para mi servidor web)

En este laboratorio, no iniciará sesión en la instancia mediante SSH. Al eliminar el acceso mediante SSH, se mejora la seguridad de la instancia.

18.Elimine la regla SSH existente.

19.Haga clic en **Review and Launch** (Revisar y lanzar).

## Paso 7: revisar el lanzamiento de la instancia

En la página “Review” (Revisar), se muestra la configuración de la instancia que está a punto de lanzar.

20.Haga clic en **Launch** (Lanzar).

Aparecerá la ventana **Select an existing key pair or create a new key pair** (Seleccionar un par de claves existente o crear un nuevo par de claves).

Amazon EC2 utiliza la criptografía de clave pública para cifrar y descifrar la información de inicio de sesión. Para iniciar sesión en una instancia, deberá crear un par de claves. En el lanzamiento de la instancia, tendrá que especificar el nombre del par de claves y, cuando se conecte a dicha instancia, tendrá que proporcionar la clave privada.

Debido a que en este laboratorio no iniciará sesión en la instancia, no necesita un par de claves.

**21.**Haga clic en el menú desplegable **Choose an existing key pair** (Elegir un par de claves existente) y seleccione **Proceed without a key pair** (Continuar sin un par de claves).

**22.**Seleccione **I acknowledge that...** (Acepto que...).

23.Haga clic en **Launch Instances** (Lanzar instancias).

Ahora se lanzará la instancia.

24.Haga clic en **View Instances** (Ver instancias).

La instancia aparecerá con estado pending (pendiente), lo que indica que se está lanzando. Después cambiará a running (en ejecución), lo que indica que la instancia está arrancando. Es posible que transcurran unos instantes hasta que pueda acceder a la instancia.

La instancia recibe un nombre de DNS público que puede utilizar para contactarla desde Internet.

Su Web Server debe estar seleccionado. En la pestaña Description (Descripción), se incluye información detallada sobre la instancia.

Para ver más información en la pestaña “Description” (Descripción), arrastre hacia arriba el divisor de la ventana.

Revise la información que aparece en la pestaña Description (Descripción). Esta contiene información sobre el tipo de instancia, así como configuraciones de seguridad y de red.

25.Espere a que en la instancia aparezca lo siguiente:

•Instance State (Estado de la instancia): running (en ejecución)

•Status Checks (Comprobaciones de estado): 2/2 checks passed (2/2 comprobaciones aprobadas)

¡Enhorabuena! Ha lanzado correctamente su primera instancia de Amazon EC2.

## Tarea 2: Monitorear la instancia

El monitoreo es un factor importante a la hora de mantener el rendimiento, la disponibilidad y la fiabilidad de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) y las soluciones de AWS.

**26.**Haga clic en la pestaña **Status Checks** (Comprobaciones de estado).

Con el monitoreo del estado de las instancias, puede determinar rápidamente si Amazon EC2 ha detectado algún problema que pudiera impedir que las instancias ejecuten aplicaciones. Amazon EC2 realiza comprobaciones automatizadas en cada instancia EC2 en ejecución para identificar problemas de hardware y software.

Observe que se ha aprobado tanto la comprobación de Accesibilidad del sistema como la de Accesibilidad de la instancia.

**27.**Haga clic en la pestaña **Monitoring** (Monitoreo).

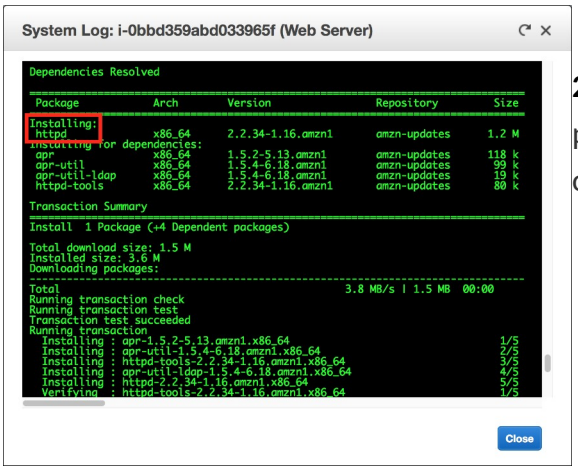
En esta pestaña, se muestran las métricas de Amazon CloudWatch sobre la instancia. En este momento, no aparecen muchas métricas debido a que la instancia se acaba de lanzar.

Puede hacer clic en un gráfico para ver una vista expandida.

Amazon EC2 envía métricas sobre sus instancias EC2 a Amazon CloudWatch. El monitoreo básico (cinco minutos) está habilitado de forma predeterminada. Se puede habilitar el monitoreo detallado (un minuto).

**28.**En el menú **Actions** (Acciones), seleccione Monitor and troubleshoot (Monitorear y solucionar problemas) Obtener registro del sistema.

En el registro del sistema, se muestra el resultado de la consola de la instancia, que constituye una herramienta valiosa para el diagnóstico de problemas. Resulta especialmente útil para solucionar problemas de kernel y de configuración de servicios que podrían causar la terminación de una instancia o hacer que esta se torne inalcanzable antes de poder iniciar su demonio de SSH. Si no ve un registro del sistema, espere unos minutos e inténtelo de nuevo.




**29.**Desplácese por el resultado. Observe que se instaló el paquete HTTP a partir de los datos de usuario que agregó cuando creó la instancia.

**30.**Elija Cancel (Cancelar).

**31.**En el menú **Actions** (Acciones), seleccione Monitor and troubleshoot (Monitorear y solucionar problemas)  Obtener captura de pantalla de la instancia.

Así se vería la consola de la instancia de Amazon EC2 si estuviera asociada a una pantalla.


Si no puede alcanzar la instancia a través de SSH o RDP, puede hacer una captura de pantalla de la instancia y verla como una imagen. Esto permite ver el estado de la instancia y solucionar los problemas más rápidamente.

**32.**Elija Cancel (Cancelar).

¡Enhorabuena! Ha analizado varias formas de monitorear la instancia.

## Tarea 3: Actualizar el grupo de seguridad y acceder al servidor web

Cuando lanzó la instancia EC2, proporcionó un script que instaló un servidor web y creó una página web sencilla. En esta tarea, accederá al contenido del servidor web.

**33.**Haga clic en la pestaña **Details** (Detalles).

**34.**Copie la I**Pv4 Public IP** (dirección IP pública IPv4) de la instancia en el portapapeles.

**35.**Abra una nueva pestaña del navegador web, pegue la dirección IP que acaba de copiar y presione Enter (Intro).

Pregunta: ¿Puede acceder al servidor web? ¿Por qué no?

En este momento, no puede acceder al servidor web porque el grupo de seguridad no permite tráfico entrante en el puerto 80, que se usa para solicitudes web HTTP. Esto es un ejemplo del uso de un grupo de seguridad como firewall para restringir el tráfico de red entrante y saliente en una instancia.

Para corregir esta situación, debe actualizar el grupo de seguridad, de manera que permita el tráfico web en el puerto 80.

**36.**Deje abierta la pestaña del navegador, pero vuelva a la pestaña de la **consola de administración de EC2**.

**37.**En el panel de navegación izquierdo, haga clic en **Security Groups** (Grupos de seguridad).

**38.**Seleccione **Web Server security group** (Grupo de seguridad del servidor web).

**39.**Haga clic en la pestaña **Inbound** (Entrante).

Actualmente, el grupo de seguridad no tiene reglas.

40.Haga clic en **Edit inbound rules** (Editar reglas de entrada) y, luego, establezca los siguientes ajustes:

•Type (Tipo): **HTTP**

•Source (Origen): **Anywhere** (Cualquiera)

•Haga clic en **Save rules** (Guardar reglas).

41.Vuelva a la pestaña del servidor web que abrió antes y actualice la página.

Debería ver este mensaje: **Hello From Your Web Server**! (¡Saludos de parte de su servidor web!)

¡Enhorabuena! Ha modificado correctamente su grupo de seguridad para permitir el tráfico HTTP en su instancia de Amazon EC2.

## Tarea 4: Modificar el tamaño de la instancia (tipo de instancia y volumen de EBS)

A medida que sus necesidades cambien, es posible que descubra que su instancia se utiliza en exceso (es demasiado pequeña) o no se utiliza lo suficiente (es demasiado grande). En ese caso, puede cambiar el tipo de instancia. Por ejemplo, si una instancia t2.micro es demasiado pequeña para su carga de trabajo, puede cambiarla a una m5.medium. Del mismo modo, puede cambiar el tamaño de un disco.

## Detener la instancia

Para poder cambiar el tamaño de una instancia, antes debe detenerla.

Cuando se detiene una instancia, se apaga. Una instancia EC2 detenida no genera cargos, pero sí se mantienen los cargos de almacenamiento por los volúmenes de Amazon EBS que están asociados a ella.

**42.**En la consola de administración de EC2, en el panel de navegación izquierdo, haga clic en Instances (Instancias).

Web Server (Servidor web) ya debería estar seleccionado.

**43.**En el menú **Instance State** (Estado de la instancia), seleccione Stop instance (Detener instancia).

44.Elija **Stop** (Detener).

La instancia se apagará de forma normal y, a continuación, dejará de ejecutarse.

**45.**Espere a que Instance State (Estado de la instancia) se muestre como stopped (detenida)

## Cambiar el tipo de instancia

**46.**En el menú **Actions** (Acciones), seleccione Instance Settings (Configuración de la instancia) Change Instance Type (Cambiar el tipo de instancia) y, a continuación, configure lo siguiente:

•Instance type (Tipo de instancia): t2.small

•Elija **Apply** (Aplicar).

Cuando la instancia se inicie de nuevo, será del tipo t2.small, que tiene el doble de memoria que una instancia t2.micro. NOTA: Es posible que en este laboratorio no pueda usar otros tipos de instancia.

## Modificar el tamaño del volumen de EBS

**47.**En el menú de navegación izquierdo, haga clic en Volumes (Volúmenes).

**48.**En el menú **Actions** (Acciones), seleccione Modify Volume (Modificar volumen).

El tamaño actual del disco es de 8 GiB. A continuación, aumentará el tamaño del disco.

**49.**Cambie el tamaño a `10`. NOTA: Es posible que en este laboratorio no se puedan crear volúmenes grandes de Amazon EBS.

50.Elija **Modify** (Modificar).

51.Elija **Yes** (Sí) para confirmar y aumentar el tamaño del volumen.

52.Elija **Close** (Cerrar).

## Iniciar la instancia con tamaño nuevo

A continuación, iniciará nuevamente la instancia, pero ahora con más memoria y más espacio en disco.

**53.**En el panel de navegación izquierdo, haga clic en Instances (Instancias).

**54.**En el menú **Instance State** (Estado de la instancia), seleccione Start instance (Iniciar instancia).

55.Elija **Start** (Iniciar).

¡Enhorabuena! Ha modificado el tamaño de su instancia de Amazon EC2 correctamente. En esta tarea, cambió el tipo de instancia de t2.micro a t2.small. También modificó el volumen del disco raíz de 8 GiB a 10 GiB.

## Tarea 5: Explorar los límites de EC2

Amazon EC2 permite utilizar diferentes recursos. Entre estos recursos, se incluyen imágenes, instancias, volúmenes e instantáneas. Cuando se crea una cuenta de AWS, estos recursos tienen límites predeterminados que dependen de la región.

**56.**En el panel de navegación izquierdo, haga clic en Limits (Límites).

**57.**En la lista desplegable, elija Running instances (Instancias en ejecución).

Observe que hay un límite sobre la cantidad de instancias que puede lanzar en esta región. Cuando se lanza una instancia, la solicitud no puede hacer que el uso supere el límite de instancias para esa región en ese momento.

Puede solicitar un aumento para muchos de estos límites.

## Tarea 6: Probar la protección de la terminación

Puede eliminar la instancia cuando ya no la necesite. Esto se denomina terminar la instancia. Una vez que se ha terminado una instancia, no es posible conectarse a ella ni reiniciarla.

En esta tarea, aprenderá a utilizar la protección de terminación.

**58.**En el panel de navegación izquierdo, haga clic en Instances (Instancias).

**59.**En el menú **Instance State** (Estado de la instancia), seleccione Terminate instance (Terminar instancia).

60.A continuación, elija **Terminate** (Terminar).

Tenga en cuenta que hay un mensaje que dice: Error al finalizar la instancia i-1234567xxx. Es posible que la instancia 'i-1234567xxx' no se termine. Modifique su atributo de instancia 'DisableApiTermination' e inténtelo de nuevo.

Esta es una protección para impedir que se termine una instancia por accidente. Si realmente quiere terminar la instancia, tendrá que deshabilitar la protección contra terminación.

**61.**En el menú **Actions** (Acciones), seleccione Instance Settings (Configuración de la instancia) Change Termination Protection (Cambiar protección de terminación).

**62.**Elimine la comprobación situada junto a Enable (Habilitar).

63.Elija Save (Guardar).

Ahora ya puede terminar la instancia.

**64.**En el menú Instance State (Estado de la instancia), seleccione Terminate (Terminar).

65.Elija Terminate (Terminar).

¡Enhorabuena! Ha probado la protección contra terminación y ha terminado la instancia correctamente.

## Fin del laboratorio

66.Haga clic en End Lab (Finalizar laboratorio) en la parte superior de esta página y, a continuación, en Yes (Sí) para confirmar que desea finalizar el laboratorio.

Aparecerá un panel en el que se indica: "DELETE has been initiated... You may close this message box now". (Se ha iniciado la ELIMINACIÓN... Ya puede cerrar este cuadro de mensajes).

**67.**Haga clic en la X de la esquina superior derecha para cerrar el panel.

## Recursos adicionales

- Lanzar la instancia
- Tipos de instancias de Amazon EC2
- Imágenes de Amazon Machine (AMI)
- Amazon EC2: datos de usuario y scripts de shell
- Volumen de dispositivo raíz de Amazon EC2
- Etiquetado de los recursos de Amazon EC2
- Grupos de seguridad
- Pares de claves de Amazon EC2
- Comprobaciones de estado para sus instancias
- Cómo conseguir el resultado de la consola y reiniciar las instancias
- Dimensiones y métricas de Amazon EC2
- Cambiar el tamaño de la instancia
- Detener e iniciar la instancia
- Service Limits de Amazon EC2
- Terminar una instancia
- Protección contra terminación de instancias

**Actividad: AWS Lambda**

**Información general**


En esta actividad práctica, creará una función de AWS Lambda. También creará un evento de Amazon CloudWatch para activar la función cada minuto. La función utiliza un rol de AWS Identity and Access Management (IAM). Este rol de IAM permite que la función detenga una instancia de Amazon Elastic Compute Cloud (Amazon EC2) que se ejecuta en la cuenta de Amazon Web Services (AWS)

## Acceso a la consola de administración de AWS

0.En la parte superior de estas instrucciones, haga clic en Start Lab (Iniciar laboratorio) para lanzar su laboratorio.

Se abrirá el panel Start Lab (Iniciar laboratorio), donde se muestra el estado del laboratorio.

**1.**Espere hasta que aparezca el mensaje Lab status: in creation (Estado del laboratorio: creándose). Para cerrar el panel Start Lab (Iniciar laboratorio), haga clic en X.

2.En la parte superior de estas instrucciones, haga clic en AWS.

La consola de administración de AWS se abrirá en una pestaña nueva del navegador. El sistema iniciará su sesión de forma automática.

Sugerencia: si no se abre una pestaña del navegador nueva, debería aparecer un banner o un icono en la parte superior de este, el cual indique que el navegador no permite que se abran ventanas emergentes en el sitio web. Haga clic en el banner o en el icono, y elija Allow pop ups (Permitir ventanas emergentes).

**3.**Ubique la pestaña de la consola de administración de AWS en un lugar donde aparezca al lado de estas instrucciones. Idealmente, debería poder ver ambas pestañas del navegador al mismo tiempo para que sea más sencillo seguir los pasos de la actividad.

## Tarea 1: crear una función de Lambda

**5.**En la consola de administración de AWS, encontrará el menú Services (Servicios), donde debe elegir **Lambda**.
Nota: Si ve un mensaje de advertencia que indica tags failed to load (no se pudieron cargar las etiquetas), puede omitirlo.
6.Haga clic en **Create function** (Crear función).
**7.**En la pantalla Create function (Crear función), configure los siguientes ajustes:
•Elija Author from scratch (Crear desde cero).

•Function name (Nombre de la función): `myStopinator`

•Runtime (Tiempo de ejecución):Python 3.8

•Haga clic en Choose or create an execution role (Seleccionar o crear un rol de ejecución).

•Execution Role (Rol de ejecución): Use an existing role (Utilizar un rol existente)

•Existing role (Rol existente): en la lista desplegable, elija myStopinatorRole.

8.Haga clic en **Create function** (Crear función).

## Tarea 2: configurar el desencadenador

En esta tarea, configurará un evento programado para activar la función de Lambda con un evento de CloudWatch como el origen de eventos (o desencadenador). La función de Lambda se puede configurar para que funcione de forma similar a un trabajo cron en un servidor de Linux o a una tarea programada en un servidor de Microsoft Windows. Sin embargo, no es necesario disponer de un servidor en ejecución para alojarlo.

9.Haga clic en **+ Add trigger** (+ Agregar desencadenador).

**10.**Haga clic en el menú desplegable Select a trigger (Seleccionar un desencadenador) y elija EventBridge (CloudWatch Events).

**11.**Para la regla, elija Create a new rule (Crear una nueva regla) y configure estos ajustes:

•Rule name (Nombre de la regla): `everyMinute`

•Rule type (Tipo de regla): Schedule expression (Expresión de programación)

•Schedule expression (Expresión de programación): `rate(1 minute)` (frecuencia [1 minuto])

Nota: Es probable que una función stopinador de Lambda basada en programación más realista se active con una expresión cron en lugar de una expresión rate. Sin embargo, para esta actividad, el uso de una expresión rate garantiza que la función de Lambda se active a tiempo como para poder ver los resultados.

12.Haga clic en Add (Agregar).

## Tarea 3: configurar la función de Lambda

En esta tarea, pegará algunas líneas de código para actualizar dos valores en el código de la función. No es necesario escribir código para completar esta tarea.

**13.**En el cuadro Diseñador, haga clic en MyStopinator (que es el nombre de su función Lambda) para mostrar y editar el código de la función Lambda.

**14.**En el cuadro Function code (Código de la función), borre el código existente. Copie el siguiente código y péguelo en el cuadro:

```
region = '<REPLACE_WITH_REGION>'
instances = ['<REPLACE_WITH_INSTANCE_ID>']
ec2 = boto3.client('ec2', region_name=region)

def lambda_handler(event, context):
    ec2.stop_instances(InstanceIds=instances)
    print('stopped your instances: ' + str(instances))
```

**15.**Sustituya el marcador de posición `<REPLACE_WITH_REGION>` (Reemplazar con región) con la región real que está utilizando. Para ello, realice lo siguiente:

Haga clic en la región de la esquina superior derecha y utilice el código de región. Por ejemplo, el código de región para EE. UU. Este (Norte de Virginia) es us-este--1.

Importante: En el código, mantenga las comillas simples ('') alrededor de la región. Por ejemplo, para el N. Virginia, sería `“us-este--1”`

**16.**Sección de desafío: compruebe que la instancia EC2 denominada instance1 se esté ejecutando en su cuenta y copie su ID de instancia.

**si necesita orientación detallada, haga clic aquí.**

**17.**Vuelva a la pestaña del navegador de la consola de AWS Lambda y sustituya `<REPLACE_WITH_INSTANCE_ID>` (Reemplazar con ID de la instancia) con el ID real de la instancia que acaba de copiar.

Importante: En el código, mantenga las comillas simples ('') alrededor del ID de la instancia.

**18.**En la esquina superior derecha del cuadro Código de función , elija Deploy (Desplegar).

La función de Lambda ya está totalmente configurada. Debería intentar detener la instancia a cada minuto.

**19.**Haga clic en Monitoring (Monitoreo), la pestaña que se encuentra cerca de la parte superior de la página.

Tenga en cuenta que uno de los gráficos muestra cuántas veces se ha invocado la función. También hay un gráfico que muestra el recuento de errores y la tasa de éxito en forma de porcentaje.

## Tarea 4: verificar que la función de Lambda funcione

**20.**Vuelva a la pestaña del navegador con la consola de Amazon EC2 y compruebe si se detuvo la instancia.

Sugerencia: puede hacer clic en el icono de actualización  o actualice la página del navegador para ver el cambio de estado más rápidamente.

21.Intente iniciar la instancia de nuevo. ¿Qué cree que va a pasar?

**aquí para revelar la respuesta.**

## Fin de la actividad

¡Felicitaciones! Ha completado la actividad.

22.Haga clic en End Lab (Finalizar laboratorio) en la parte superior de esta página y, a continuación, en Yes (Sí) para confirmar que desea finalizar la actividad.

Aparecerá un panel con un mensaje que indica: DELETE has been initiated... You may close this message box now. (Se ha iniciado la ELIMINACIÓN... Ya puede cerrar este cuadro de mensajes).

**23.**Para cerrar el panel, vaya a la esquina superior derecha y haga clic en X.

# Laboratorio 4: Uso de EBS

## Información general sobre el laboratorio


El laboratorio se enfoca en Amazon Elastic Block Store (Amazon EBS), un mecanismo de almacenamiento subyacente clave para las instancias de Amazon EC2. En este laboratorio, aprenderá a crear un volumen de Amazon EBS, asociarlo a una instancia, implementar un sistema de archivos en el volumen y, a continuación, tomar una instantánea como copia de seguridad.

## Temas

Al final de este laboratorio, podrá hacer lo siguiente:

- Crear un volumen de Amazon EBS
- Asociar el volumen a una instancia EC2 y montarlo en ella
- Crear una instantánea del volumen
- Crear un volumen nuevo a partir de la instantánea
- Asociar el volumen nuevo a la instancia EC2 y montarlo en ella

## Requisitos previos del laboratorio

Para completar este laboratorio correctamente, debe estar familiarizado con el uso básico de Amazon EC2 y con la administración de servidores básica de Linux. Debe saber usar las herramientas de línea de comandos de Linux.

**Otros servicios de AWS**

La política de IAM deshabilita otros servicios de AWS diferentes a los requeridos para este laboratorio durante su tiempo de acceso al laboratorio. Además, las capacidades de los servicios utilizados para este laboratorio están limitadas según los requisitos de este e incluso, en algunos casos, de forma deliberada como parte del diseño del laboratorio. Espere recibir mensajes de error cuando acceda a otros servicios o cuando lleve a cabo acciones que no consten en la guía de este laboratorio.

**¿Qué es Amazon Elastic Block Store?**

**Amazon Elastic Block Store (Amazon EBS)** ofrece almacenamiento persistente para las instancias de Amazon EC2. Los volúmenes de Amazon EBS están asociados a la red, y su duración es independiente a la vida de una instancia. Los volúmenes de Amazon EBS tienen un alto nivel de disponibilidad y de confianza, y pueden aprovecharse como particiones de arranque de instancias de Amazon EC2 o asociarse a una instancia de Amazon EC2 en ejecución como dispositivos de bloques estándar.

Cuando se utilizan como particiones de arranque, las instancias de Amazon EC2 pueden detenerse y, posteriormente, reiniciarse, lo que le permite pagar solo por los recursos de almacenamiento utilizados al mismo tiempo que conserva el estado de la instancia. Los volúmenes de Amazon EBS tienen durabilidad mucho mayor que los almacenes de instancias de Amazon EC2 locales porque los volúmenes de Amazon EBS se replican automáticamente en el backend (en una única zona de disponibilidad).

Sin embargo, para los que quieran aún más durabilidad, con Amazon EBS es posible crear instantáneas uniformes puntuales de los volúmenes, que luego se almacenan en Amazon Simple Storage Service (Amazon S3) y se replican automáticamente en varias zonas de disponibilidad. Estas instantáneas se pueden utilizar como punto de partida para nuevos volúmenes de Amazon EBS y permiten proteger la durabilidad de sus datos a largo plazo. También puede compartirlas fácilmente con colegas y otros desarrolladores de AWS.

En esta guía de laboratorio, se explican los conceptos básicos de Amazon EBS paso a paso. Sin embargo, solo se presenta un poco de información general sobre los conceptos de Amazon EBS. Para obtener más información, consulte la documentación de Amazon EBS.

**Características de los volúmenes de Amazon EBS**

Los volúmenes de Amazon EBS ofrecen las siguientes características:

- **Almacenamiento persistente:** el tiempo de vida de los volúmenes es independiente de cualquier instancia de Amazon EC2.
- **De uso general:** los volúmenes de Amazon EBS son dispositivos de bloques sin formato que se pueden utilizar en cualquier sistema operativo.

•**Alto rendimiento:** los volúmenes de Amazon EBS son iguales que las unidades de Amazon EC2 locales o mejores que ellas.

•**Nivel de fiabilidad alto:** los volúmenes de Amazon EBS tienen redundancia integrada dentro de una zona de disponibilidad.

•**Diseñados para ofrecer resiliencia:** la AFR (tasa anual de errores) de Amazon EBS oscila entre 0,1 % y 1 %.

•**Tamaño variable:** los tamaños de los volúmenes varían entre 1 GB y 16 TB.

•**Fáciles de usar:** los volúmenes de Amazon EBS se pueden crear, asociar, almacenar en copias de seguridad, restaurar y eliminar fácilmente.

## Acceso a la consola de administración de AWS

1.En la parte superior de estas instrucciones, haga clic en Start Lab (Iniciar laboratorio) para lanzarlo.

Se abrirá el panel “Start Lab” (Iniciar laboratorio), donde se muestra el estado del laboratorio.

**2.**Espere hasta que aparezca el mensaje “**Lab status: ready**” (Estado del laboratorio: listo) y, a continuación, haga clic en **X** para cerrar el panel “Start Lab” (Iniciar laboratorio).

3.En la parte superior de estas instrucciones, haga clic en AWS.

La consola de administración de AWS se abrirá en una nueva pestaña del navegador. El sistema iniciará su sesión automáticamente.

**Sugerencia**: si no se abre una pestaña del navegador nueva, debería aparecer un banner o un icono en la parte superior de este, el cual indique que el navegador no permite que se abran ventanas emergentes en el sitio. Haga clic en el banner o en el icono, y elija “Allow pop ups” (Permitir ventanas emergentes).

4.Ubique la pestaña de la consola de administración de AWS en un lugar donde aparezca al lado de estas instrucciones. Idealmente, debería poder ver ambas pestañas del navegador al mismo tiempo para que sea más sencillo seguir los pasos del laboratorio.

### Tarea 1: crear un volumen de EBS nuevo

En esta tarea, creará y asociará un volumen de Amazon EBS a una nueva instancia de Amazon EC2.

**5.**En la **consola de administración de AWS**, encontrará el menú **Services** (Servicios), donde debe hacer clic en **EC2**.

**6.**En el panel de navegación izquierdo, haga clic en **Instances** (Instancias).

Ya se lanzó una instancia de Amazon EC2 denominada **Lab** (Laboratorio) para el laboratorio.

**7.**Observe la **zona de disponibilidad** de la instancia. Tendrá un aspecto similar a us-west-2a.

**8.**En el panel de navegación izquierdo, haga clic en **Volumes** (Volúmenes).

Verá un volumen existente que utiliza la instancia de Amazon EC2. Dicho volumen tiene un tamaño de 8 GiB, lo que permite distinguirlo con facilidad del volumen que creará a continuación, el cual será de 1 GiB.

9.Haga clic en **Create Volume** (Crear volumen) y luego configure lo siguiente:

- **Volume Type** (Tipo de volumen): General Purpose SSD (gp2) (SSD de uso general [gp2])
- **Size (GiB)** (Tamaño [GiB]): 1. **NOTA**: Es posible que no pueda crear volúmenes grandes.
- **Availability Zone** (Zona de disponibilidad): seleccione la misma zona que la de la instancia EC2.
- Haga clic en **Add Tag** (Agregar etiqueta).
- En el editor de etiquetas, escriba lo siguiente:
  - **Key** (Clave): Name (Nombre)
  - **Value** (Valor): My Volume (Mi volumen)

10.Haga clic en **Create Volume** (Crear volumen) y, a continuación, en **Close** (Cerrar).

El volumen nuevo aparecerá en la lista, y su estado cambiará de creating (creándose) a available (disponible). Es posible que tenga que hacer clic en **refresh** (actualizar) para ver el volumen nuevo.

### Tarea 2: asociar el volumen a una instancia

Ahora puede asociar el volumen nuevo a la instancia de Amazon EC2.

**11.**Seleccione **My Volume** (Mi volumen).

**12.**En el menú **Actions** (Acciones), haga clic en **Attach Volume** (Asociar volumen).

**13.**Haga clic en el campo **Instance** (Instancia) y, a continuación, seleccione la instancia que aparece (Lab [Laboratorio]).

Observe que el campo **Device** (Dispositivo) está definido como /dev/sdf. Utilizará este identificador de dispositivo en una tarea posterior.

**14.**Haga clic en Attach (Asociar). El estado del volumen pasará a in-use (en uso).

## Tarea 3: conectarse a la instancia de Amazon EC2

### Usuarios de Windows: uso de SSH para conectarse

Estas instrucciones son solo para usuarios de Windows.

Si utiliza macOS o Linux, vaya a la siguiente sección.

15.Lea los tres puntos de este paso antes de comenzar, ya que no podrá consultar estas instrucciones cuando el panel "Details" (Detalles) esté abierto.

- Haga clic en el menú desplegable Details (Detalles) situado por encima de estas instrucciones que está leyendo actualmente y, a continuación, haga clic en Show (Mostrar). Se abrirá la ventana "Credentials" (Credenciales).
- Haga clic en **Download PPK** (Descargar PPK) y guarde el archivo **labsuser.ppk**. Por lo general, el navegador lo guarda en el directorio "Downloads" (Descargas).
- A continuación, haga clic en **X** para salir del panel "Details" (Detalles).

16.Descargue el software necesario.

- Utilizará **PuTTY** para conectarse mediante SSH a las instancias de Amazon EC2. Si no tiene instalado PuTTY en su equipo, descárguelo aquí.

**17.**Abra **putty.exe**.

18.Configure PuTTY para que no tenga tiempo de espera:

- Haga clic en **Connection** (Conexión).
- Defina el valor de **Seconds between keepalives** (Segundos entre keepalives) en 30 segundos.

Esto le permite mantener la sesión de PuTTY abierta durante un periodo más prolongado.

19.Configure la sesión de PuTTY de la siguiente manera:

- Haga clic en **Session** (Sesión).
- **Host Name (or IP address)** (Nombre del host [o dirección IP]): copie y pegue el valor de **IPv4 Public IP address** (Dirección IP pública IPv4) de la instancia. Para obtenerla, vuelva a la consola de EC2 y haga clic en **Instances** (Instancias). Marque la casilla que se

encuentra junto a la instancia y, en la pestaña Description (Descripción), copie el valor de **IPv4 Public IP** (Dirección IP pública IPv4).

- En PuTTY, en la lista **Connection** (Conexión), expanda **SSH**
- Haga clic en **Auth** (Autenticación) (no lo amplíe).
- Haga clic en **Browse** (Buscar).
- Busque y seleccione el archivo labsuser.ppk que descargó.
- Haga clic en **Open** (Abrir) para seleccionarlo.
- Haga clic en **Open** (Abrir).

**20.** Haga clic en **Yes** (Sí) para validar el host y conectarse a él.

**21.** Cuando aparezca **Login as** (Iniciar sesión como), escriba `ec2-user`.

Esto lo conectará a la instancia EC2.

**22.** Usuario de Windows: haga clic aquí para pasar a la siguiente tarea.

**Usuarios de macOS y Linux**

Estas instrucciones están dirigidas únicamente a los usuarios de Mac o Linux. Si es un usuario de Windows, pase a la anterior tarea.

23. Lea todas las instrucciones de este paso antes de comenzar, ya que no las podrá consultar cuando el panel "Details" (Detalles) esté abierto.

- Haga clic en el menú desplegable `Details` (Detalles) situado por encima de estas instrucciones que está leyendo actualmente y, a continuación, haga clic en `Show` (Mostrar). Se abrirá la ventana "Credentials" (Credenciales).
- Haga clic en **Download** (Descargar) y guarde el archivo **labsuser.pem**.
- A continuación, haga clic en **X** para salir del panel "Details" (Detalles).

**24.** Abra una ventana de terminal y cambie el `cd` del directorio a aquel donde se descargó el archivo labsuser.pem.

Por ejemplo, ejecute este comando si se guardó en el directorio "Downloads" (Descargas):

```
cd ~/Downloads
```

25. Ejecute este comando para cambiar los permisos de la clave a fin de que sean de solo lectura:

```
chmod 400 labsuser.pem
```

**26.**Vuelva a la consola de administración de AWS y, en el servicio EC2, haga clic en **Instances** (Instancias).

Debe seleccionarse la instancia **Lab** (Laboratorio).

**27.**En la pestaña Description (Descripción), copie el valor de **IPv4 Public IP** (Dirección IP pública IPv4).

**28.**Vuelva a la ventana de terminal y ejecute este comando (sustituya **<public-ip>** con la dirección IP pública real que haya copiado):

```
ssh -i labsuser.pem ec2-user@<public-ip>
```

**29.**Escriba yes (sí) cuando se le pregunte si desea permitir una primera conexión a este servidor SSH remoto.

Como está usando un par de claves para la autenticación, no se le pedirá una contraseña.

### Tarea 4: crear y configurar el sistema de archivos

En esta tarea, agregará el volumen nuevo a la instancia de Linux como un sistema de archivos ext3 en el punto de montaje /mnt/data-store.

Si utiliza PuTTY, puede pegar texto mediante un clic con el botón derecho en la ventana de PuTTY.

30.Consulte el almacenamiento disponible de la instancia:

```
df -h
```

Debería ver un resultado similar al siguiente:

```
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        488M   60K  488M   1% /dev
tmpfs           497M     0  497M   0% /dev/shm
/dev/xvda1      7.8G  982M  6.7G  13% /
```

Se muestra el volumen de disco original de 8 GB. El volumen nuevo todavía no se muestra.

31.Cree un sistema de archivos ext3 en el volumen nuevo:

```
sudo mkfs -t ext3 /dev/sdf
```

32.Cree un directorio para montar el volumen de almacenamiento nuevo:

```
sudo mkdir /mnt/data-store
```

33.Monte el volumen nuevo:

```
sudo mount /dev/sdf /mnt/data-store
```

Para configurar la instancia de Linux y poder montar este volumen siempre que se inicie la instancia, deberá agregar una línea a /etc/fstab.

```
echo "/dev/sdf   /mnt/data-store ext3 defaults,noatime 1 2" | sudo tee -a /etc/fstab
```

34.Consulte el archivo de configuración para ver el parámetro de la última línea:

```
cat /etc/fstab
```

35.Consulte nuevamente el espacio de almacenamiento disponible:

```
df -h
```

El resultado ahora incluirá una línea adicional - /dev/xvdf:

```
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        488M   60K  488M   1% /dev
tmpfs           497M     0  497M   0% /dev/shm
/dev/xvda1      7.8G  982M  6.7G  13% /
/dev/xvdf       976M  1.3M  924M   1% /mnt/data-store
```

36.Cree un archivo en el volumen montado y agréguele algo de texto.

```
sudo sh -c "echo some text has been written > /mnt/data-store/file.txt"
```

37.Compruebe que se haya escrito el texto en el volumen.

```
cat /mnt/data-store/file.txt
```

## Recursos adicionales

Características, funciones y precios de Amazon Elastic Block Store

AWS Training and Certification