



Máquinas virtuales de tecnología de datos en AWS

Versión 1.1

Guía Paso a Paso



La información que figura a continuación incluye requisitos detallados previos a la implementación, una guía detallada paso a paso para la implementación de AWS Virtual Machines v1.1 Click to Run, y los pasos posteriores a la implementación que deberán tenerse en cuenta.

[Página 2: Requisitos de infraestructura.](#)

[Página 2: Pasos previos a la implementación](#)

[Página 5: implementación DE Máquinas virtuales de AWS Click to Run](#)

[Página 9: Actividades posteriores a la implementación](#)

Pre-Requisitos de Máquinas Virtuales:

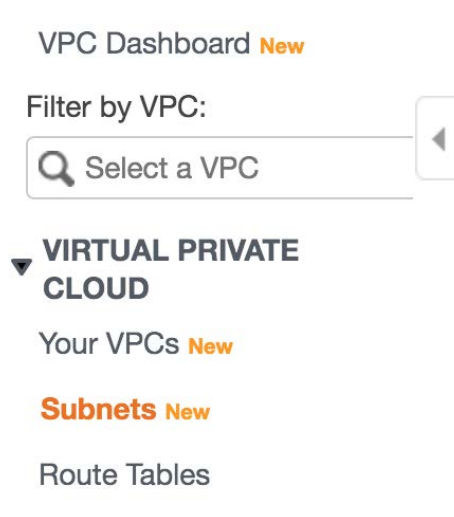
✓ Requisitos de Infraestructura

- **VPC y subredes existentes:** Para desplegar la solución click to run, debe existir ya en la región una VPC con las subredes asociadas, con las correspondientes tablas de rutas, puertas de enlace, etc. La solución no realiza ninguna configuración fuera del alcance de la máquina virtual, por lo que para garantizar el acceso a internet la VPC debe estar configurada correctamente.
- **Par de claves existentes:** Para acceder a la instancia EC2, se debe elegir un par de claves. El par de claves debe existir en la región seleccionada en el momento de la implementación.

Máquinas virtuales v1.1 Pasos previos a la implementación

1. Para buscar los ID de la VPC y la Subred donde se implementará la solución:

- a. Vaya a la consola de AWS.
- b. Una vez en la consola, seleccione la región donde implementará la solución.
- c. Busque el servicio “VPC”.
- d. Vaya a la sección “subredes”.



e. A continuación, seleccione entre las subredes y VPC disponibles. Tome nota de los nombres de VPC y subred correspondientes. Asegúrese de que la subred pertenece a la VPC seleccionada.

<input type="checkbox"/>	Name ▾	Subnet ID ▾	State ▾	VPC
<input type="checkbox"/>	-	subnet-36698f6f	✔ Available	vpc-8f53acea
<input type="checkbox"/>	-	subnet-482dee3f	✔ Available	vpc-8f53acea
<input type="checkbox"/>	-	subnet-a6c460c3	✔ Available	vpc-8f53acea

f. Si no hay VPC o subredes en la lista, proceda a crear una VPC y una subred según las instrucciones de AWS.

2. Para buscar el par de claves utilizado para acceder al host:

- a. Vaya a la consola de AWS.
- b. Una vez en la consola, seleccione la región donde implementará la solución.
- c. Busque el servicio “EC2”.
- d. Vaya a la sección “Key pairs”, en “Network & Security”.

▼ Network & Security

Security Groups **New**

Elastic IPs **New**

Placement Groups **New**

Key Pairs **New**

Network Interfaces **New**

e. Tome nota del nombre del par de claves que desea utilizar para acceder a su instancia EC2.

<input type="checkbox"/>	Name	Fingerprint	ID
<input type="checkbox"/>	aws-ec2	89:4f:7d:57:e6:b5:32:96:b5:00:6a:ae:e...	key-0e212e26f167398af

f. Si no hay pares de claves en la lista, cree uno haciendo clic en “Create key pair”.

Para implementar máquinas virtuales basadas en Centos7:

Las instancias EC2 basadas en Centos 7 no se pueden implementar sin antes reconocer el acuerdo de licencia. Esto debe hacerse desde el mercado de AWS, en la cuenta de AWS donde se implementará la solución. Para aceptar el acuerdo, suscríbese a la siguiente solución de mercado: <https://aws.amazon.com/marketplace/pp/B00O7WM7QW>

Ahora puede continuar con la implementación de la solución

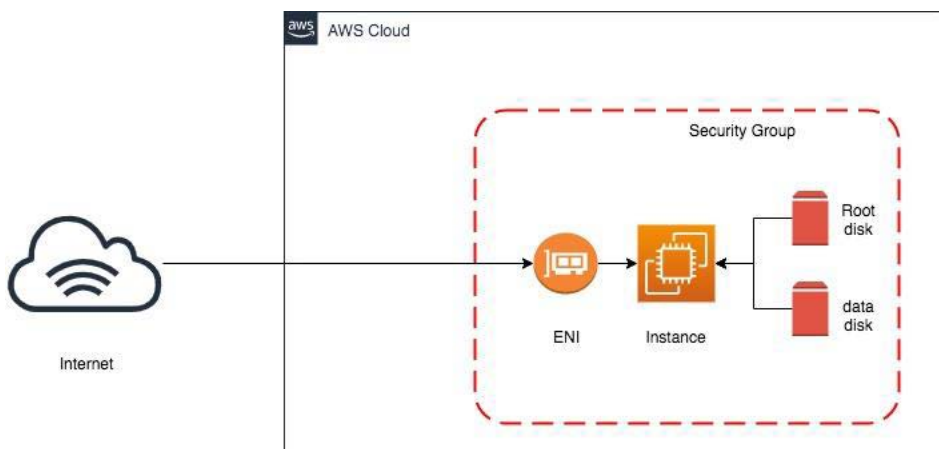
Descripción general de la solución:

“Elastic Cloud Computing, o EC2, es una solución de máquinas virtuales optimizada para ejecutarse en la nube de AWS. Estas instancias son compatibles con los sistemas operativos Linux y Windows, y todos los controladores y configuraciones necesarios son administrados por usted como parte del proceso de implementación. Hay una variedad de optimizaciones y tamaños de camisa para elegir, por lo que se puede seleccionar el tipo de instancia que mejor se adapte a su caso de uso “.

Parámetros y entradas:

- Introduzca un nombre para su instancia EC2
- Seleccione una instancia AMI (diferentes versiones de Linux disponibles)
- Seleccione una tenencia de host (predeterminado, dedicado)
- Introduzca el nombre del par de claves (como se indica en la sección anterior)
- Seleccione el tamaño del volumen raíz (mínimo 10 Gb para Linux y 40 Gb para Windows, máximo 1Tb)
- Opcionalmente, introduzca la URL de un script de arranque para ejecutarlo durante el inicio.
- Opcionalmente, introduzca una cadena de ejecución para pasar al script de arranque.
- Introduzca un bloque CIDR para permitir el acceso desde.
- Habilitar o deshabilitar el acceso HTTP al host.
- Habilitar o deshabilitar el acceso SSH al host.
- Introduzca el ID de la VPC (como se indica en la sección anterior)
- Introduzca el ID de la subred (como se indica en la sección anterior)

Arquitectura de implementación:



Implementación y consideraciones de máquinas virtuales de AWS

Adquiera la solución AWS Virtual Machines V1 Click to Run a través de StreamOne Marketplace y diríjase a Digital Locker para configurar e implementar la solución.

1. **Seleccione una región de AWS disponible:** esta es la región donde se implementará la solución. No todas las regiones están disponibles para cada solución.

Location

Select data center location

2. **Seleccione un nombre de máquina virtual:** Este será el nombre que se mostrará en la consola EC2 para identificar la instancia EC2. No se permiten espacios.

Basic Information

Virtual machine name

3. **Seleccione una instancia AMI:** Esta es la imagen del sistema operativo que se implementará con la solución. ** Nota: Para desplegar una máquina Centos, consulte las instrucciones anteriores.

Instance AMI

- Amazon Linux 2
- Amazon Linux
- Centos 7
- Ubuntu Server 18.04 LTS
- Ubuntu Server 16.04 LTS
- SuSE Enterprise Linux 15

4. **Seleccione un modo de alquiler:** el alquiler define dónde se ejecuta la instancia EC2, en términos del hipervisor subyacente. Si se selecciona “predeterminado”, la instancia EC2 se ejecutará en hardware compartido. Si se selecciona “dedicado”, la instancia EC2 se ejecutará en hardware dedicado (se aplicarán cargos adicionales)

Tenancy

- dedicated
- default

5. **Introduzca un par de claves EC2:** El par de claves se utilizará para acceder a la instancia EC2 a través de SSH. Para obtener un par de claves disponible o crear uno, siga los pasos resaltados en la sección anterior.

Key pair

6. **Seleccionar tamaños de disco:** Se provisionarán dos discos con la instancia EC2, uno para el sistema operativo (volumen raíz) y otro para datos (volumen de datos). Utilice el control deslizante para seleccionar el tamaño deseado. (Para las instancias de Windows, el volumen raíz mínimo debe ser de 40Gb).

Size of the root volume

10

Size of the data volume

10

7. **(Opcional) Introduzca la URL de un script de arranque:** El script definido en este campo se ejecutará la primera vez que se arranque la instancia EC2. Este script tiene que ser un archivo BASH. Por lo general, esto se utiliza para instalar software adicional, hacer endurecimiento o realizar pasos adicionales. Esto es solo para usuarios avanzados.

(Optional) Bootstrap script

8. **(Opcional) Introduzca una cadena de ejecución para el script:** Si define un script de arranque anterior, es posible que sea necesario pasar parámetros (es decir, "--filesystem EFS--language python"). Esto es solo para usuarios avanzados.

(Optional) Execution string

9. **Introduzca un bloque CIDR para permitir el acceso SSH:** el acceso SSH a esta instancia EC2 solo se permitirá desde el bloque CIDR especificado en este campo. Si se requiere acceso universal (no recomendado), ingrese 0.0.0.0/0 como el bloque CIDR.

Allowed access CIDR

10. **Seleccione si desea permitir el acceso HTTP:** Si necesita acceso HTTP a la instancia, marque la casilla de verificación. El acceso público en el puerto 80 se otorgará en el Grupo de Seguridad. Sin embargo, asegúrese de que la subred y VPC donde se implementa la instancia EC2 permitan el acceso a este host.

Enable HTTP access

11. **Seleccione si desea permitir el acceso SSH:** Si necesita acceso SSH a la instancia, marque la casilla de verificación. Se otorgará acceso SSH al Grupo de Seguridad, desde el rango de direcciones especificado en el “Acceso permitido CIDR”. La clave ssh especificada en el “AWS Keypair” será necesaria cuando inicie sesión.

Enable SSH access

12. **Ingrese el VPCID:** el ID del VPC donde se aprovisionará la instancia EC2. Introduzca el ID que anotó en el paso de requisitos previos.

VPCID

13. **Ingrese el ID de subred:** el ID de la subred donde se aprovisionará la instancia EC2. Esta subred debe estar en el mismo VPC que se ha introducido anteriormente. Introduzca el ID que anotó en el paso de requisitos previos.

Subnet ID

14. **Verificación final:** valide sus entradas y haga clic en “Implementar”. Esto cambiará a “Implementación...” y cerrará la ventana después de unos momentos. A continuación, debe ver la solución que aparece como “In Progress” en el casillero digital.

-- Continúe a la siguiente página para ver los pasos posteriores a la implementación --

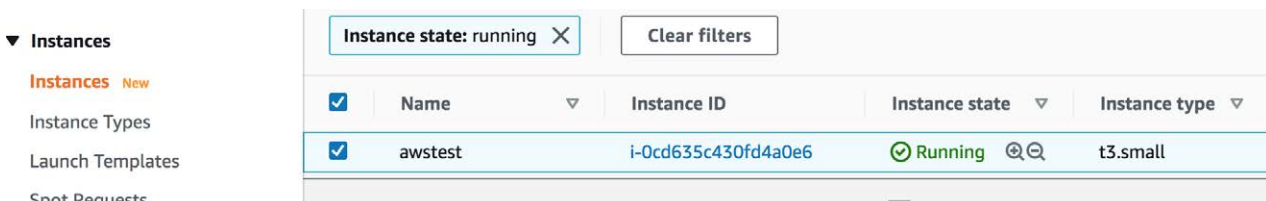
Actividades posteriores a la implementación para AWS Virtual Machines V1 (instancias EC2)

- Verificando el estado de su instancia.
- Conexión a su instancia EC2.
- Modificación de los permisos de acceso a la red.

Actividades posteriores al despliegue

Verificando el estado de su instancia.

Cuando la instancia se implementa por primera vez, su estado cambiará a “running” después de unos minutos. Si la instancia no se inicia, es posible que haya habido un problema durante el inicio, así que compruebe los registros de implementación o póngase en contacto con nuestro soporte. Para verificar el estado, vaya a su consola de AWS. Una vez que haya iniciado sesión, seleccione el servicio “EC2”. Vaya a “Instances”. Su instancia debe aparecer allí, con el nombre que seleccionó como nombre de la instancia. El estado se mostrará en la columna “estado de la instancia”.



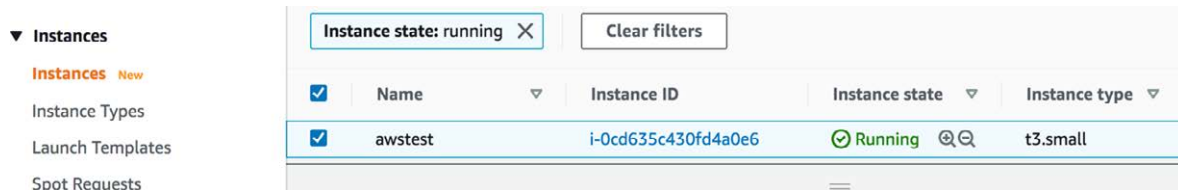
Instance state: running X					Clear filters
<input checked="" type="checkbox"/>	Name	Instance ID	Instance state	Instance type	
<input checked="" type="checkbox"/>	awstest	i-0cd635c430fd4a0e6	Running	t3.small	

Conexión a su instancia EC2.

Puede suceder que en algún momento tenga que conectarse a su instancia EC2, por ejemplo, para realizar tareas administrativas o para instalar software. Hay dos maneras posibles de lograr esto: usando la consola de AWS o conectando a través de SSH.

Para conectarse a través de la consola de AWS:

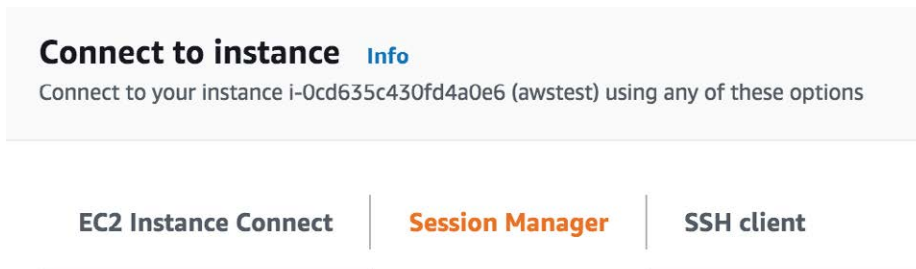
1. Vaya a su consola de AWS y, a continuación, seleccione el servicio “EC2” en el menú superior izquierdo.
2. Vaya a “Instances”.



3. En la esquina superior derecha, selecciona “conectar”:



4. Seleccione “Session Manager” como método de conexión:

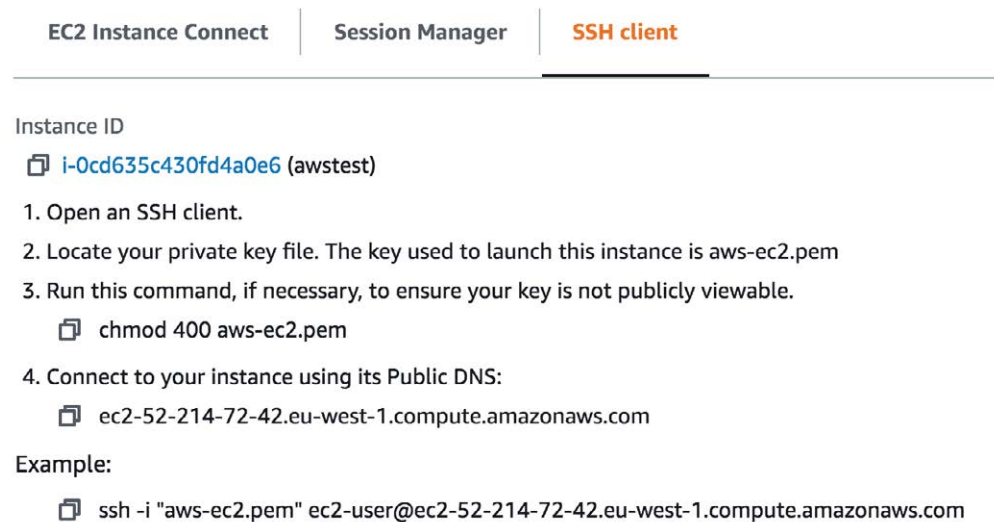


5. Haga clic en “connect” en la esquina inferior derecha.

6. Se le presentará una sesión ssh basada en web en una nueva pestaña.

Para conectarse a través del cliente SSH:

1. Siga los pasos anteriores hasta el paso 3.
2. Seleccione “SSH client” como método de conexión:



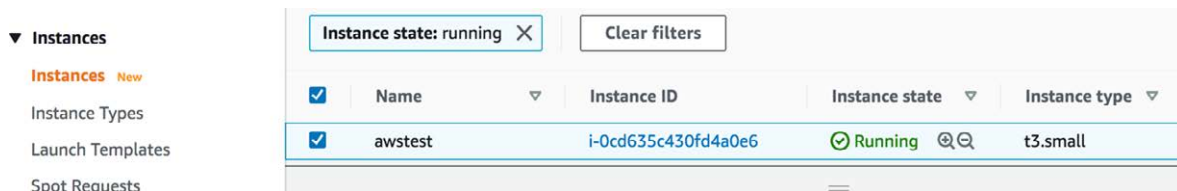
The screenshot shows the AWS console interface for connecting to an EC2 instance via SSH. At the top, there are three tabs: "EC2 Instance Connect", "Session Manager", and "SSH client", with "SSH client" being the active tab. Below the tabs, the "Instance ID" is listed as "i-0cd635c430fd4a0e6 (awstest)". A list of four steps is provided: 1. Open an SSH client. 2. Locate your private key file. The key used to launch this instance is aws-ec2.pem. 3. Run this command, if necessary, to ensure your key is not publicly viewable. Below this step is a code block: `chmod 400 aws-ec2.pem`. 4. Connect to your instance using its Public DNS: Below this step is a code block: `ec2-52-214-72-42.eu-west-1.compute.amazonaws.com`. Below the steps, there is an "Example:" section with a code block: `ssh -i "aws-ec2.pem" ec2-user@ec2-52-214-72-42.eu-west-1.compute.amazonaws.com`.

3. Siga las instrucciones detalladas para conectarse a través de SSH. Tenga en cuenta que, para conectarse a la dirección IP pública de la máquina, debe haber seleccionado el CIDR de acceso apropiado en el campo “CIDR de acceso remoto”, o se rechazará la conexión. Si no ha configurado correctamente su instancia, siga las instrucciones de la sección “Modifying network access permissions (Modificación de los permisos de acceso a la red)” en esta sección.

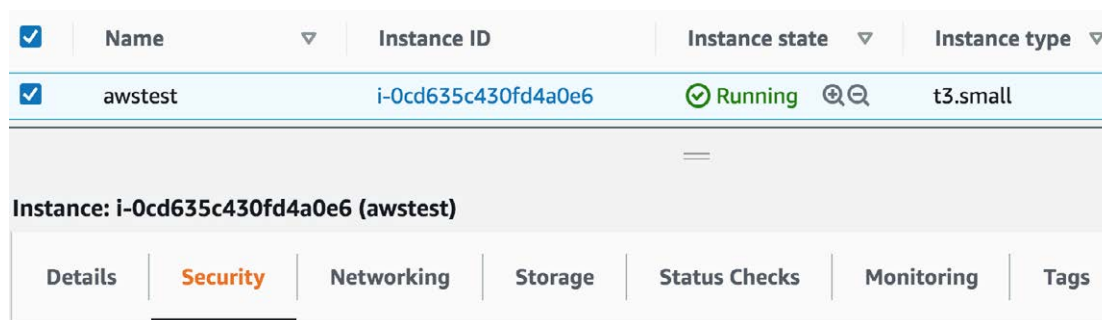
Modificación de los permisos de acceso a la red.

Es totalmente posible que los permisos básicos emitidos en la implementación de instancias deban modificarse más adelante a medida que cambien las demandas, o podría ser que se cometiera un error y no se asignara el bloque CIDR adecuado. Para modificar los permisos de acceso a la red, siga estos pasos:

1. Conéctese a su consola de AWS. Seleccione el servicio “EC2”.
2. Vaya a “instances” en la barra de navegación izquierda.
3. Seleccione su sesión:



4. En la mitad inferior, seleccione la pestaña “Seguridad”:



5. En la sección “seguridad”, busque los “Grupos de seguridad” y haga clic en el único Grupo de seguridad que se mostrará.

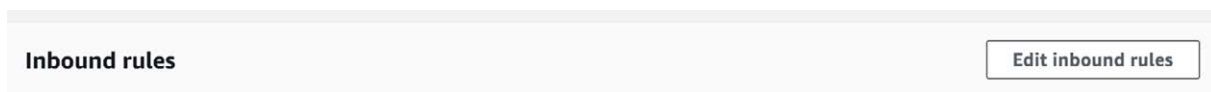
Security groups


[sg-0233415f9890d44ca \(GCI-100000000000210255-1606212152949-EC2LinuxStack-1QII4N5R5N2OO-SecurityGroup-1JKSPK0064ICZ\)](#)

6. Se le dirigirá a la interfaz de “Grupos de seguridad”. Allí, debe moverse hacia abajo hasta que vea la sección “Inbound rules”. Sus reglas de acceso deben mostrarse allí. Si seleccionó “Allow SSH access (Permitir acceso SSH)”, se mostrará una regla al puerto 22 desde la dirección CIDR que seleccionó:

Inbound rules			
Type	Protocol	Port range	Source
SSH	TCP	22	10.0.0.0/20
All ICMP - IPv4	ICMP	All	10.0.0.0/20

7. Para modificar o añadir reglas de acceso, haga clic en “Edit inbound rules (Editar reglas entrantes)”, en la esquina superior derecha de la sección “inbound rules (reglas entrantes)”.



8. Podrá modificar la “fuente” y el puerto, o añadir puertos adicionales. Recuerde que es posible que tenga que editar los Grupos de Seguridad asignados a la subred para permitir el acceso al host.

Inbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info	
SSH ▼	TCP	22	Custom ▼ <input type="text" value="10.0.0.0/20"/>	<input type="text"/>	Delete
All ICMP - IPv4 ▼	ICMP	All	Custom ▼ <input type="text" value="10.0.0.0/20"/>	<input type="text"/>	Delete