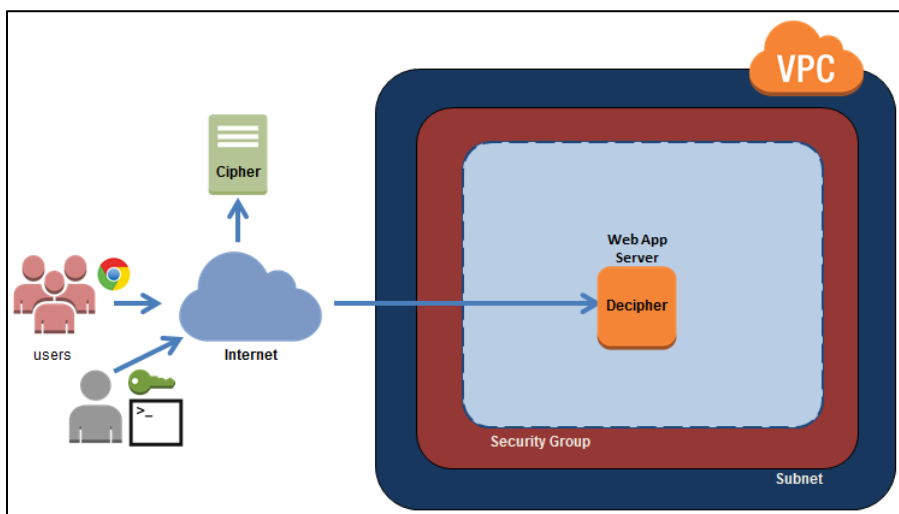


Taller de Amazon Web Services – Parte 2

Objetivo

Conocer de manera práctica algunos de los servicios ofrecidos por un proveedor Cloud Computing de Infraestructura como Servicio (IaaS), a través de un caso de uso basado en el despliegue de una aplicación Web escalable bajo demanda sobre la infraestructura de Amazon Web Services (AWS).

Arquitectura de la aplicación



Pasos del laboratorio

1. Desplegar una instancia en EC2 y acceder al servidor por medio de SSH.

Esta actividad se realiza sobre la instancia desplegada en el
Taller de Amazon Web Services – Parte 1.

- Acceder a la consola de AWS. Identifique el nombre DNS público y la dirección IPv4 pública asignadas a la instancia. Asegúrese de tener a la mano el archivo .pem con la llave privada descargado al momento de hacer el **Taller de Amazon Web Services – Parte 1**.
- Identificar la dirección IP que está usando su computador en el momento de realizar este taller.
- Modificar la regla del grupo de seguridad asociado a la instancia para que pueda acceder a través del protocolo SSH desde la dirección IP identificada en el punto anterior. Ver **Taller de Amazon Web Services – Parte 1** (página 14).
- Ingresa a través de un cliente SSH a la instancia. Recuerde que en la AMI de Amazon el nombre de usuario es **ec2-user** y no tiene password asignado.

2. Desplegar una aplicación Web en un servidor virtual.

Este taller incluye una aplicación web desarrollada en PHP. Para ejecutarla, es necesario instalar algunas dependencias, junto con el código de la aplicación. Siga cuidadosamente los pasos a continuación.

- a. Cambiar a superusuario. Escriba el siguiente comando:

```
sudo su
```

- b. Instalar Apache y PHP.

```
yum install httpd php php-mysql php-gd php-imap phpldap php-odbc php-pear php-xml php-xmlrpc
```

- c. Reiniciar el servidor Web.

```
/etc/init.d/httpd restart
```

- d. Configurar el sistema operativo para que inicie el servidor Web cuando el sistema operativo se inicia. Este último comando no debe generar ninguna salida.

```
chkconfig --levels 235 httpd on
```

- e. Copiar la aplicación al servidor virtual. Descargue el usando el comando:

```
wget https://github.com/ISIS4426-Desarrollo-Soluciones-Cloud/Talleres-AWS/raw/master/Pagina.zip
```

- f. Verificar que el archivo fue correctamente descargado. Utilice el comando `ls`.

- g. Descomprimir el archivo.

```
unzip Pagina.zip
```

- h. Identificar los archivos y directorios que quedaron almacenados en el directorio **Pagina**

```
ls Pagina
```

- i. Copiar el contenido del directorio **Pagina** al directorio **/var/www/html**.

```
cp -a Pagina/. /var/www/html
```

- j. Verificar que los archivos hayan sido copiados.

```
ls /var/www/html
```

3. Verificar que la aplicación fue instalada correctamente.

La aplicación Web para este taller permite descifrar un texto cifrado mediante el algoritmo RC4. En adelante, esta aplicación será llamada **Decipher**. Para poder utilizarla, será necesario proporcionar texto cifrado mediante el mismo protocolo con una aplicación externa, la cual se llamará **Cipher**.

- Verificar que el grupo de seguridad asociado a la instancia EC2 tenga acceso a través de los protocolos HTTP y HTTPS, tal como lo indica el **Taller de Amazon Web Services – Parte 1** (página 14).
- Acceder al servidor Web mediante un navegador usando el nombre DNS o la dirección IP de la instancia EC2.



- Probar la aplicación.

Para probar la aplicación, se requiere un texto cifrado previamente. Se va a utilizar una aplicación **Cipher** que permita cifrar texto con el algoritmo RC4. Mediante el navegador acceda a un codificador RC4 online.

Esta aplicación ofrece cifrado mediante varios algoritmos. En este taller, el algoritmo a utilizar es **RC4**, por lo que se requiere que sea este el algoritmo seleccionado.

Para cifrar, utilice el siguiente texto. Ingrésele en el área de texto **“Original data”**:

In cryptography, RC4 is the most widely used software stream cipher and is used in popular protocols such as Secure Sockets Layer (SSL) and WEP.

Para evitar errores en la codificación, asegúrese de no tener saltos de línea, los cuales pueden afectar el proceso.

En el campo de texto **“Key”** ingrese la siguiente llave

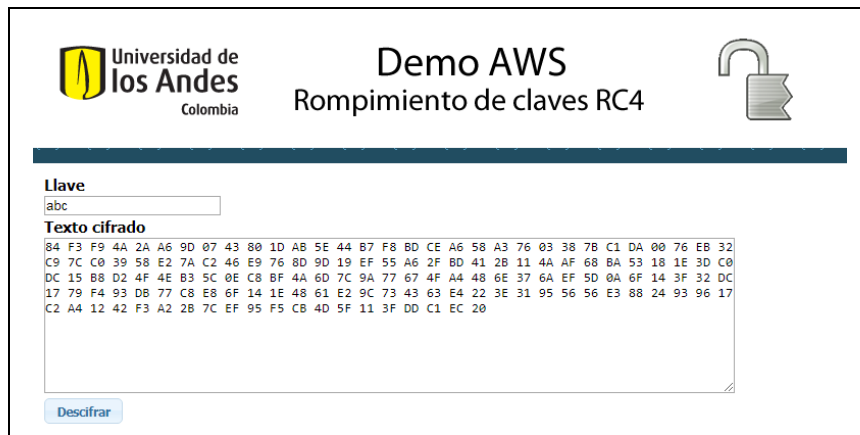
abc

La llave a emplear es sensible a mayúsculas y minúsculas. Haga clic en el botón **ENCRYPT**. Observe el texto cifrado en el área de texto **"Encrypted data"**.

El texto cifrado corresponde a:

```
84 F3 F9 4A 2A A6 9D 07 43 80 1D AB 5E 44 B7 F8 BD CE A6 58 A3 76 03 38 7B C1 DA 00 76 EB 32
C9 7C C0 39 58 E2 7A C2 46 E9 76 8D 9D 19 EF 55 A6 2F BD 41 2B 11 4A AF 68 BA 53 18 1E 3D C0
DC 15 B8 D2 4F 4E B3 5C 0E C8 BF 4A 6D 7C 9A 77 67 4F A4 48 6E 37 6A EF 5D 0A 6F 14 3F 32 DC
17 79 F4 93 DB 77 C8 E8 6F 14 1E 48 61 E2 9C 73 43 63 E4 22 3E 31 95 56 56 E3 88 24 93 96 17 C2
A4 12 42 F3 A2 2B 7C EF 95 F5 CB 4D 5F 11 3F DD C1 EC 20
```

- d. Nuevamente en el navegador, utilice la función **Copiar/Pegar** para llevar el texto cifrado y la llave, y de este modo hacer una prueba funcional de la aplicación web.



Universidad de los Andes Colombia

Demo AWS

Rompimiento de claves RC4

Llave

Texto cifrado

```
84 F3 F9 4A 2A A6 9D 07 43 80 1D AB 5E 44 B7 F8 BD CE A6 58 A3 76 03 38 7B C1 DA 00 76 EB 32
C9 7C C0 39 58 E2 7A C2 46 E9 76 8D 9D 19 EF 55 A6 2F BD 41 2B 11 4A AF 68 BA 53 18 1E 3D C0
DC 15 B8 D2 4F 4E B3 5C 0E C8 BF 4A 6D 7C 9A 77 67 4F A4 48 6E 37 6A EF 5D 0A 6F 14 3F 32 DC
17 79 F4 93 DB 77 C8 E8 6F 14 1E 48 61 E2 9C 73 43 63 E4 22 3E 31 95 56 56 E3 88 24 93 96 17 C2
A4 12 42 F3 A2 2B 7C EF 95 F5 CB 4D 5F 11 3F DD C1 EC 20
```

Descifrar

Haga clic en el botón **Descifrar** y observe el resultado obtenido.



Universidad de los Andes Colombia

Demo AWS

Rompimiento de claves RC4

Clave

Texto descifrado

In cryptography, RC4 is the most widely used software stream cipher and is used in popular protocols such as Secure Sockets Layer (SSL) and WEP.

- e. Analizar el tiempo de descifrado empleado por la aplicación **Decipher** instalada en la instancia EC2, considerando textos de diferente cantidad de caracteres.

Texto	Tiempo de cifrado
Cloud computing es un nuevo modelo de entrega de servicios computacionales que pueden ser accedidos bajo demanda y donde los usuarios deben pagar solamente por los recursos consumidos.	
Cloud computing es un nuevo modelo de entrega de servicios computacionales que pueden ser accedidos bajo demanda y donde los usuarios deben pagar solamente por los recursos consumidos. Principalmente hay tres modelos de entrega de servicios: Infraestructura como Servicio (IaaS), Plataforma como Servicio (PaaS) y Software como Servicios (SaaS).	

Deje abierta la aplicación **Cipher**. El texto cifrado será utilizado para analizar el desempeño de instancia.

4. Monitorización del desempeño de la instancia EC2.

- a. Acceder la pestaña **Monitoring** en la consola de administración de EC2.

Abra cinco pestañas en el navegador para probar el desempeño de la aplicación **Decipher**. Ingrese el texto cifrado correspondiente al siguiente texto, con la llave “abc”.

Cloud computing es un nuevo modelo de entrega de servicios computacionales que pueden ser accedidos bajo demanda y donde los usuarios deben pagar solamente por los recursos consumidos.

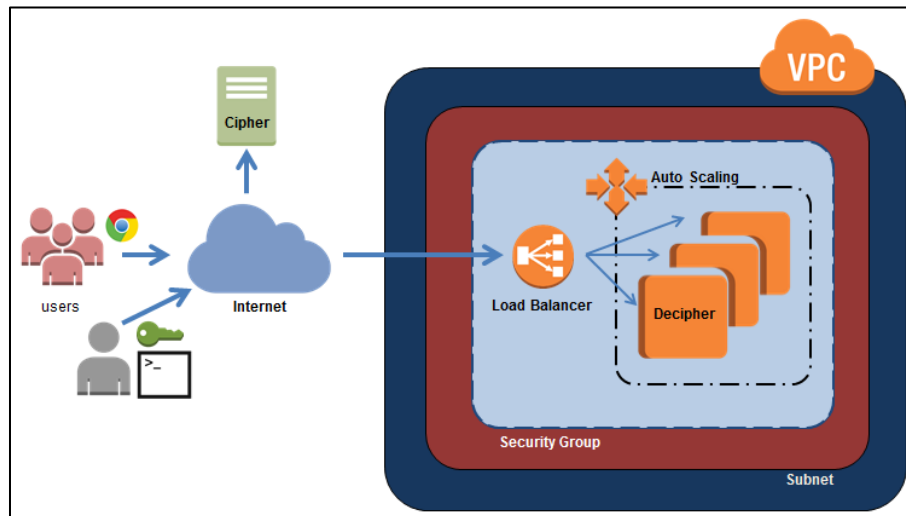
Haga clic en la pestaña “**Monitoring**” de la consola de administración de AWS EC2. Observe las gráficas de desempeño ofrecidas por este servicio y la información que aparece en las demás pestañas.

- b. Seleccionar la métrica “**CPU Utilization**” haciendo clic en la gráfica correspondiente.

La gráfica muestra los detalles de monitorización del servicio Cloud Watch para la instancia seleccionada. En la parte superior de la gráfica se pueden ver información relacionada con la gráfica como la estadística, el rango de tiempo y el período correspondiente.

- c. Identificar el comportamiento de la CPU y los picos generados al descifrar sus textos.

5. Escalar la aplicación Web.



- Crear una imagen del servidor Web. Una imagen de la instancia en la que instaló el servidor Web con la aplicación **Decipher** será utilizada para crear nuevas instancias, las cuales van a permitir que la aplicación escale automáticamente.
 - Haga clic derecho en su instancia (en la consola EC2) y seleccione **Image** y luego **Create Image**.
 - Asigne como nombre "**Decipher**". En la descripción escriba "**Decipher Web Server**".
 - Haga clic en **Create Image**.

Create Image

Instance ID

i-00526d2fcfe6430d4

Image name

Decipher

Image description

Decipher Web Server

No reboot

☐

Instance Volumes

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encrypted
Root	/dev/xvda	snap-0633c5ff821eaf489	8	General Purpose SSD (GP2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

Add New Volume

Total size of EBS Volumes: 8 GiB

When you create an EBS image, an EBS snapshot will also be created for each of the above volumes.

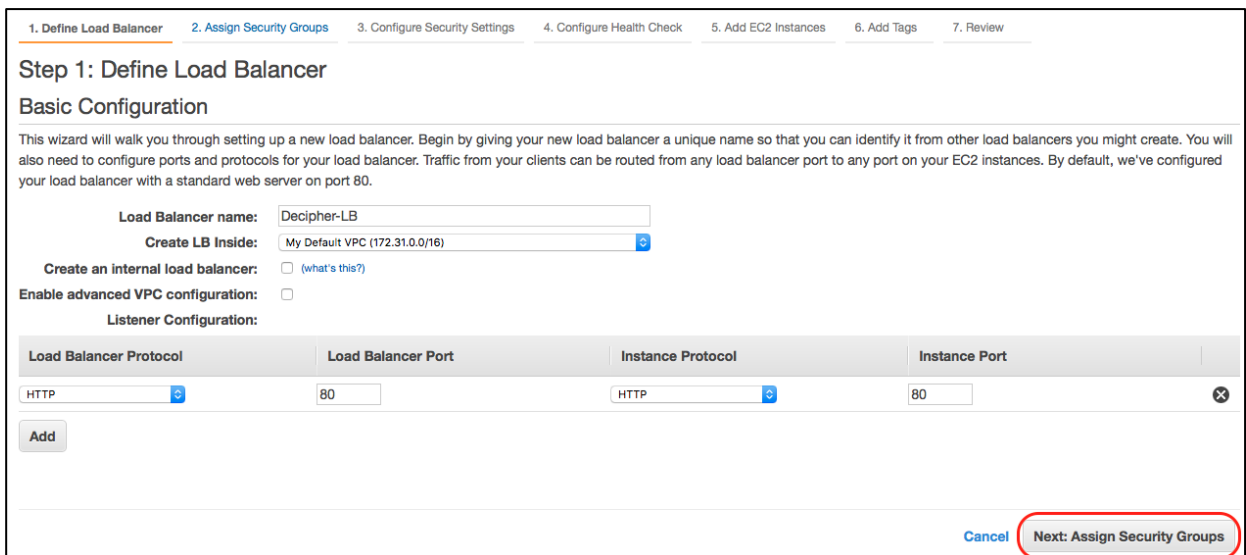
Cancel

Create Image

- Verificar que la imagen haya sido creada exitosamente. En la opción **AMI** del menú de servicios de la consola EC2 se puede ver la imagen. La creación de la imagen toma algunos minutos.

- c. Configurar un balanceador de carga para la aplicación Web **Decipher**. El servicio de AWS ELB (Elastic Load Balancer) permite incrementar la disponibilidad de las aplicaciones por medio de la distribución del tráfico entre varias instancias EC2.

- Haga clic en la opción **Load Balancers** del menú de servicios de la consola EC2.
- Haga clic en el botón **Create Load Balancer**.
- Seleccione el balanceador clásico y haga clic en el botón **Create**.
- Configure el balanceador de carga. Asigne el nombre **Decipher-LB**. Las otras opciones pueden quedar sin modificaciones.
- Haga clic en el botón **Next: Assign Security Groups**.



1. Define Load Balancer 2. Assign Security Groups 3. Configure Security Settings 4. Configure Health Check 5. Add EC2 Instances 6. Add Tags 7. Review

Step 1: Define Load Balancer

Basic Configuration

This wizard will walk you through setting up a new load balancer. Begin by giving your new load balancer a unique name so that you can identify it from other load balancers you might create. You will also need to configure ports and protocols for your load balancer. Traffic from your clients can be routed from any load balancer port to any port on your EC2 instances. By default, we've configured your load balancer with a standard web server on port 80.

Load Balancer name:

Create LB inside:

Create an internal load balancer: ☐ (what's this?)

Enable advanced VPC configuration: ☐

Listener Configuration:

Load Balancer Protocol	Load Balancer Port	Instance Protocol	Instance Port
HTTP	80	HTTP	80

[Add](#)

[Cancel](#) [Next: Assign Security Groups](#)

- Asigne el grupo de seguridad que creó en el **Taller de Amazon Web Services – Parte 1**.
- Haga clic en el botón **Next: Configure Security Settings**.
- La configuración del balanceador de carga en este taller no incluye protocolos seguros como HTTPS o SSL. Por lo tanto ignore la advertencia de seguridad y haga clic en el botón **Next: Configure Health Check**.
- Configure el Health Check. En este caso, el protocolo empleado será HTTP en el puerto 80. En el parámetro **Ping Path** escriba **/index.php**.
- Haga clic en el botón **Next: Add EC2 Instances**.

1. Define Load Balancer 2. Assign Security Groups 3. Configure Security Settings 4. Configure Health Check 5. Add EC2 Instances 6. Add Tags 7. Review

Step 4: Configure Health Check

Your load balancer will automatically perform health checks on your EC2 instances and only route traffic to instances that pass the health check. If an instance fails the health check, it is automatically removed from the load balancer. Customize the health check to meet your specific needs.

Ping Protocol: HTTP
Ping Port: 80
Ping Path: /index.php

Advanced Details

Response Timeout: 5 seconds
Interval: 30 seconds
Unhealthy threshold: 2
Healthy threshold: 10

Cancel Previous **Next: Add EC2 Instances**

- Agregue la instancia que está ejecutando la aplicación Web **Decipher**.
- Haga clic en el botón **Next: Add Tags**.

1. Define Load Balancer 2. Assign Security Groups 3. Configure Security Settings 4. Configure Health Check 5. Add EC2 Instances 6. Add Tags 7. Review

Step 5: Add EC2 Instances

The table below lists all your running EC2 Instances. Check the boxes in the Select column to add those instances to this load balancer.

VPC vpc-0dd6576a (172.31.0.0/16)

Instance	Name	State	Security groups	Zone	Subnet ID	Subnet CIDR
<input checked="" type="checkbox"/>	i-00526d2f6430d4	Taller2	running	launch-wizard-1	us-west-2b	subnet-ee18e7a7 172.31.32.0/20

Availability Zone Distribution
1 Instance in us-west-2b

☒ Enable Cross-Zone Load Balancing
☒ Enable Connection Draining 300 seconds

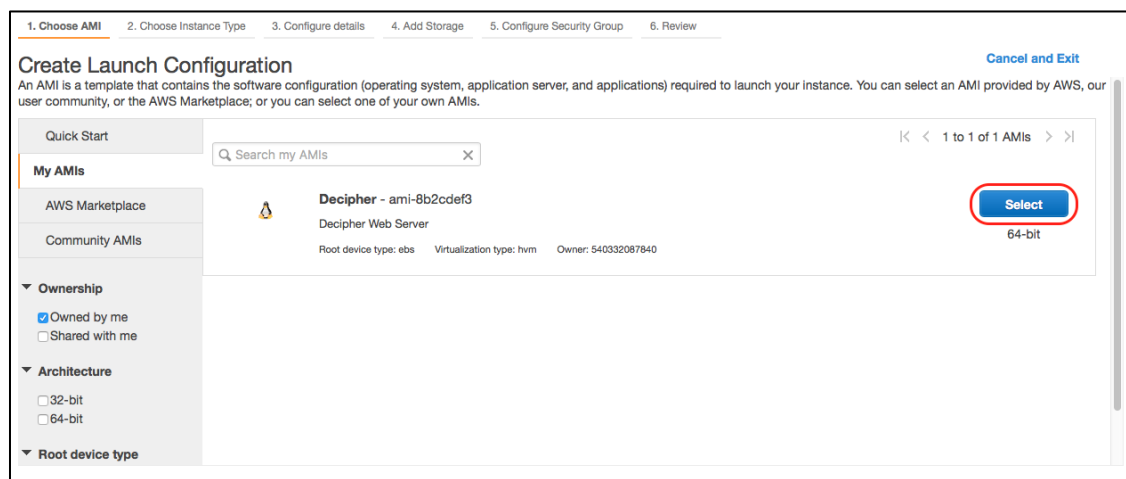
Cancel Previous **Next: Add Tags**

- Las tags son parejas llave-valor que se utilizan para organizar los recursos en AWS. Puede continuar sin crear tags y hacer clic en el botón **Review and Create**.
- Revise el resumen de cada uno de los componentes que está utilizando para crear el balanceador de carga. Si todo está listo, haga clic en el botón **Create**.
- Al terminar, aparece en la pantalla un mensaje que indica si el balanceador de carga fue creado exitosamente. Haga clic en el botón **Close**.
- Apague la instancia EC2 empleada para la creación del balanceador de carga. Haga clic derecho sobre la instancia y seleccione la opción **Instance State** y a continuación seleccione la opción **Stop**.

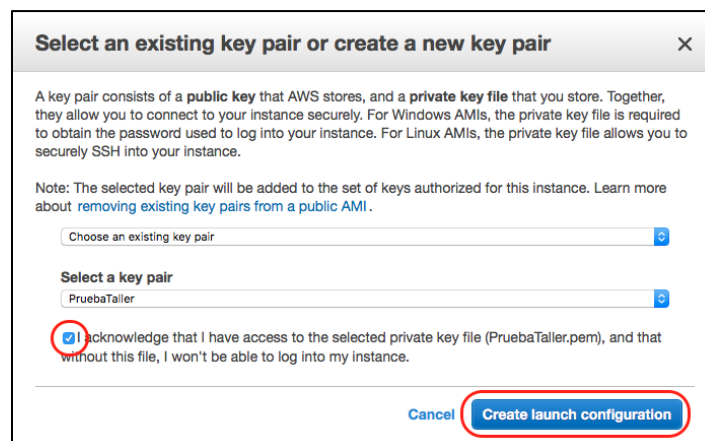
6. Crear un grupo de AutoScaling.

a. Crear una configuración de lanzamiento.

- Haga clic en la opción **Launch Configurations** del menú de servicios de la consola EC2.
- Haga clic en el botón **Create Auto Scaling group**.
- Haga clic en el botón **Create launch configuration**.
- Seleccione la AMI que va a utilizar en la configuración de lanzamiento. En este caso seleccione la creada previamente. Haga clic en la opción **My AMIs** y haga clic en el botón **Select** frente a la AMI correspondiente.



- Seleccione el tipo de instancia. Se recomienda que utilice la que hace parte del **Free tier**.
- Haga clic en el botón **Next: Configure details**.
- Asigne el nombre a la configuración de lanzamiento: **Decipher-LC**.
- Haga clic en el botón **Next: Add Storage**, luego haga clic en el botón **Next: Configure Security Group**.
- Seleccione el grupo de seguridad que creó previamente y haga clic en el botón **Review**.
- Observe los detalles. Si todo es correcto, haga clic en el botón **Create launch configuration**.
- Seleccione un conjunto de llaves existente o cree uno nuevo, haga clic en el checkbox que le indica que sin el archivo correspondiente no puede tener acceso a la instancia y haga clic en el botón **Create launch configuration**.



b. Crear un grupo de autoscaling.

- Asigne el nombre al grupo de autoscaling: **Decipher-AS**.
- Seleccione o cree una nueva subred para las nuevas instancias que se vayan creando.
- Haga clic en la opción **Advanced Details**.

1. Configure Auto Scaling group details 2. Configure scaling policies 3. Configure Notifications 4. Configure Tags 5. Review

Create Auto Scaling Group [Cancel and Exit](#)

Launch Configuration ⓘ Decipher-LC

Group name ⓘ Decipher-AS

Group size ⓘ Start with 1 instances

Network ⓘ vpc-0dd6576a (172.31.0.0/16) (default) [Create new VPC](#)

Subnet ⓘ subnet-32329755 (172.31.16.0/20) | Default in us-west-2a [Create new subnet](#)

Each instance in this Auto Scaling group will be assigned a public IP address. ⓘ

[Advanced Details](#)

- Haga clic en el checkbox que le indica que recibirá tráfico de uno o más balanceadores de carga.
- En el campo **Classic Load Balancers** seleccione el balanceador de carga creado anteriormente
- Haga clic en el botón de radio **ELB** para especificar el tipo de **Health Check**.
- Haga clic en el botón **Next: Configure scaling policies**.

Create Auto Scaling Group [Cancel and Exit](#)

▼ Advanced Details

Load Balancing ⓘ ☒ Receive traffic from one or more load balancers [Learn about Elastic Load Balancing](#)

Classic Load Balancers ⓘ Decipher-LB x

Target Groups ⓘ

Health Check Type ⓘ ☒ ELB ☐ EC2

Health Check Grace Period ⓘ 60 seconds

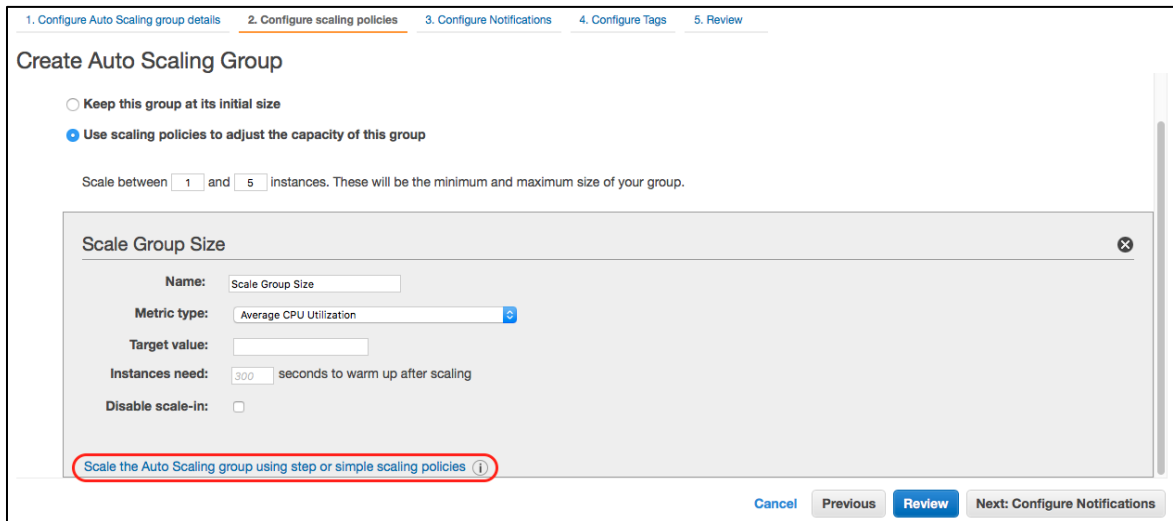
Monitoring ⓘ Amazon EC2 Detailed Monitoring metrics, which are provided at 1 minute frequency, are not enabled for the launch configuration Decipher-LC. Instances launched from it will use Basic Monitoring metrics, provided at 5 minute frequency. [Learn more](#)

Instance Protection ⓘ

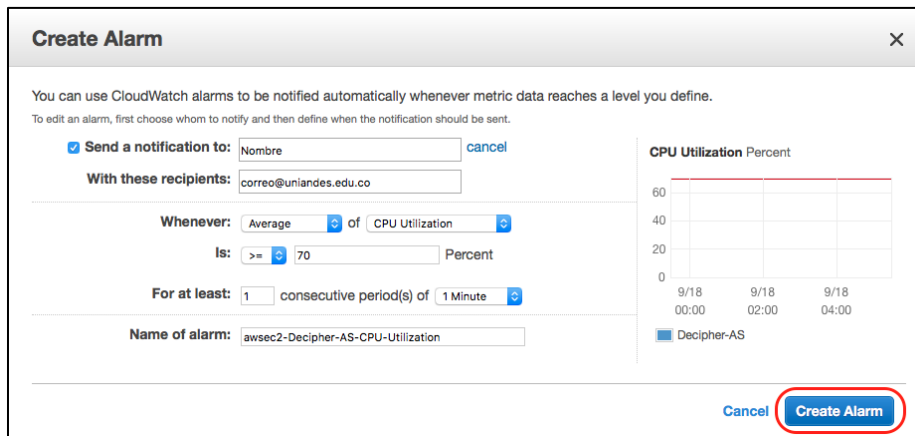
[Cancel](#) [Next: Configure scaling policies](#)

c. Configure las políticas de escalado de instancias.

- Haga clic en el botón de radio **Use scaling policies to adjust the capacity of this group.**
- Configure el rango para que escale entre 1 y 5 instancias.
- Haga clic en el enlace **Scale the Auto Scaling group using step or simple scaling policies.**



- Haga clic en **Add new alarm** en el grupo **Increase Group Size**.
- Haga clic en el checkbox situado a la izquierda del mensaje **Send notification to:**
- Haga clic en **create topic**.
- Escriba el nombre y el correo electrónico en el cual quiere recibir las notificaciones acerca del comportamiento del escalado automático. Recibirá un correo electrónico en el cual le informan que se ha creado una suscripción, la cual debe ser confirmada.
- Configure la alarma para que cuando el promedio de utilización de CPU sea igual o mayor a 70% por más de un minuto se incremente el número de instancias.
- Asigne el nombre a la alarma.
- Haga clic en el botón **Create Alarm**.



- En el campo **Take the action** del cuadro **Increase Group Size**, deberá indicar la acción a realizar cada vez que el porcentaje de CPU sea igual o mayor al 70%. En este caso, que se lancen dos instancias.



The screenshot shows the 'Increase Group Size' configuration window. The 'Name' field is 'Increase Group Size'. The 'Execute policy when' section shows the policy 'awsec2-Decipher-AS-CPU-Utilization' with a description: 'breaches the alarm threshold: CPUUtilization >= 70 for 60 seconds for the metric dimensions AutoScalingGroupName = Decipher-AS'. The 'Take the action' field is highlighted with a red circle and contains the text 'Add 2 instances when CPUUtilization >= 70%'. Below this, there is an 'Add step' button and an 'Instances need' field set to '60 seconds to warm up after each step'. At the bottom, there is a link 'Create a simple scaling policy'.

- Configure la alarma para decrecer el número de instancias. En este caso, cree una alarma que reduzca el número de instancias cuando el promedio de utilización sea menor o igual al 20% por más de un minuto.
- En el campo **Take the action** del cuadro **Decrease Group Size**, indique que se apague una instancia cuando el porcentaje de CPU sea igual o menor al 20%.
- Haga clic en el botón **Review**.
- Si toda la configuración es correcta, haga clic en el botón **Create Auto Scaling group**.
- Al terminar, aparece en la pantalla un mensaje que indica si el grupo de autoscaling fue creado exitosamente. Haga clic en el botón **Close**.

7. Probar la escalabilidad automática.

- Identifique el nombre DNS público asignado al balanceador de carga.
- Acceda al balanceador de carga mediante un navegador usando el nombre DNS o la dirección IP.
- Utilizando la aplicación **Cipher**, cifre el texto a continuación con la llave **abc**:

Cloud computing es un nuevo modelo de entrega de servicios computacionales que pueden ser accedidos bajo demanda y donde los usuarios deben pagar solamente por los recursos consumidos.

Cloud computing es un nuevo modelo de entrega de servicios computacionales que pueden ser accedidos bajo demanda y donde los usuarios deben pagar solamente por los recursos consumidos.

Principalmente hay tres modelos de entrega de servicios: Infraestructura como Servicio (IaaS), Plataforma como Servicio (PaaS) y Software como Servicios (SaaS).

- Pruebe la aplicación **Decipher** en el balanceador de carga en cinco pestañas al mismo tiempo, descifrando el mismo texto.
- Revise las instancias que se encuentran en ejecución y podrá ver como aumentan y disminuyen a medida que se van cumpliendo las condiciones asignadas en las alarmas creadas.

8. Eliminar el ambiente AWS.

Para evitar cobros por el uso de los recursos innecesarios, se recomienda eliminar el grupo de auto scaling, el balanceador de carga, las instancias y demás recursos utilizados en este taller.

9. Crear alarmas en AWS para control de costos.

Es muy importante tener control sobre los recursos que se utilizan en AWS. En ocasiones detectar el uso innecesario de recursos y el alto cobro de los mismos es prioritario. En esta sección se crea una alarma que verifique que el costo generado por el uso de recursos de AWS no supere una cantidad especificada.

- a. Haga clic sobre el nombre de usuario en el menú superior, y haga clic sobre la opción **My Billing Dashboard**.
- b. Seleccione la opción **Preferences** en el menú ubicado al lado izquierdo de la consola.
- c. Habilite la opción **Recibir alertas de facturación**.
- d. Haga clic en **Guardar Preferencias**. Haga clic sobre el enlace **Gestionar alertas de facturación**.
- e. En la nueva venta seleccionar la opción **Create Alarm**.
- f. Seleccione como tipo de alarma la opción **Total Estimated Charge** de la categoría **Billing Alarms**.
- g. Defina un nombre para la alarma como **Billing Alarm**, y defina una relación con los costos mayor o igual al valor que considere apropiado. En este caso seleccionamos un valor de **5 USD**.
- h. En la sección de acciones defina una notificación para un estado de alarma.
- i. ¿En cuántos estados se pueden encontrar las alarmas?
- j. Finalmente de clic en **Create Alarm**.

Este ha sido un ejemplo básico de cómo se puede crear una aplicación Web escalable sobre un proveedor de Infraestructura como Servicio (IaaS) como es el caso de Amazon Web Services (AWS).