

Universidad de Costa Rica
Facultad de Ingeniería
Escuela de Ciencias de la Computación e Informática
CI-0121 Redes de comunicación de datos
Grupo 02
Docente: Mag. José Antonio Brenes Carranza
Enunciado de tarea corta #2
Fecha: Jueves 5 de noviembre del 2020
Fechas máximas de entrega: Jueves 12 de noviembre del 2020 a las 13:00 horas.

Instrucciones generales

Complete los pasos que se detallan a continuación y lea cuidadosamente las instrucciones que se le brindan. Las secciones señaladas con la leyenda “*** Entregable ***” se refieren a los “productos” que deben ser entregados como parte de esta tarea corta. Al finalizar esta tarea corta, elabore un documento en el cual incluya los “productos” solicitados y la documentación asociada. A continuación, suba este documento en formato PDF al enlace que se provee en la plataforma Mediación Virtual.

Pasos para configurar e iniciar una instancia de máquina virtual en Amazon AWS

Ingresa y regístrate en la plataforma Amazon AWS Educate mediante el enlace enviado a su correo electrónico institucional. Complete los pasos requeridos para obtener acceso a la clase “Data Communication Networks” que se muestra en la siguiente Figura #1.

Course Name	Description	Educator	Course End Date	Credit Allocated Per Student	Status
Data Communication Networks	Introduction to data communication networks.	José Antonio Brenes Carranza	12/19/2020	\$50	<button>Accept Invitation</button> <button>Decline</button>

Figura # 1 Lista de clases asignadas a la cuenta. Se muestra la clase "Data Communication Networks" asociada al curso

En la pantalla mostrada en la Figura #1, acepte la invitación a la clase “Data Communication Networks” dando clic en el botón “Accept invitation” y aceptando los términos y condiciones del servicio. A continuación, diríjase al espacio de la clase dando clic en el botón “Go to classroom” resaltado en la Figura #2.

Course Name IT	Description	Educator IT	Course End Date IT	Credit Allocated Per Student IT	Status
Data Communication Networks	Introduction to data communication networks.	José Antonio Brenes Carranza	12/19/2020	\$50	Accepted

[Go to classroom](#)

Figura # 2 Botón mediante el cual se accede a la clase "Data Communication Networks"

A continuación, se le dirigirá a una pantalla correspondiente al panel de control de la máquina virtual a utilizar en la clase. En dicha pantalla, de clic en el botón "AWS Console" con lo cual ingresará a una pantalla con el acceso a todas las opciones de su cuenta.

En la sección "Build a solution" de clic en la opción "Launch a virtual machine" resaltada en la Figura #3.

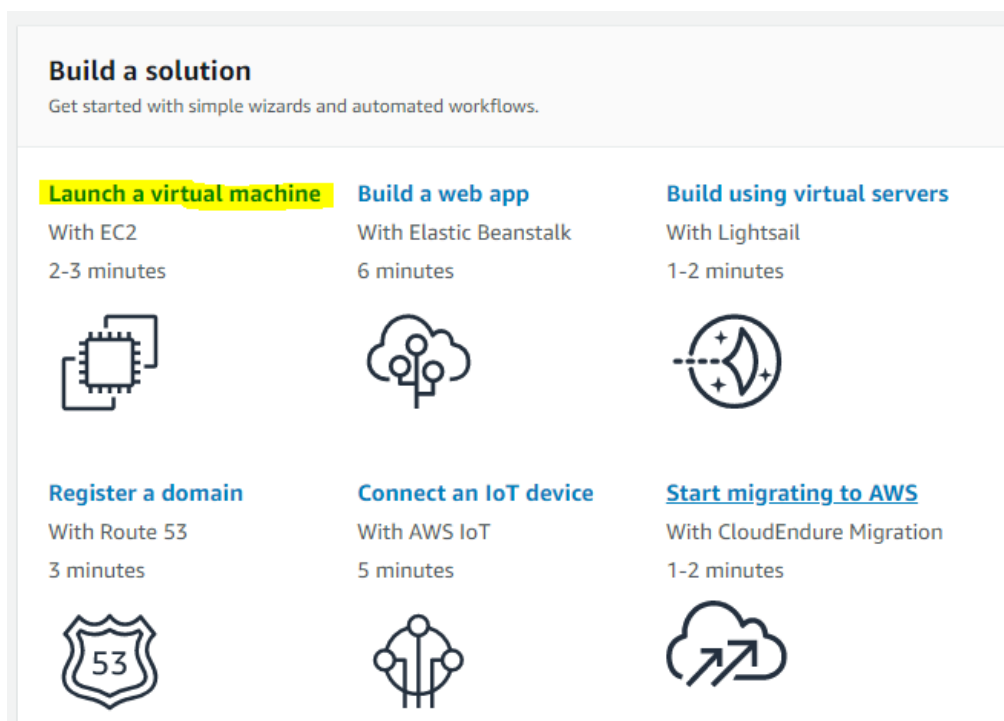


Figura # 3 Soluciones que se pueden crear en Amazon AWS

A continuación, seleccione el sistema operativo Ubuntu Server 20.04 LTS y la arquitectura x86-64, como se muestra resaltado en la Figura #4.

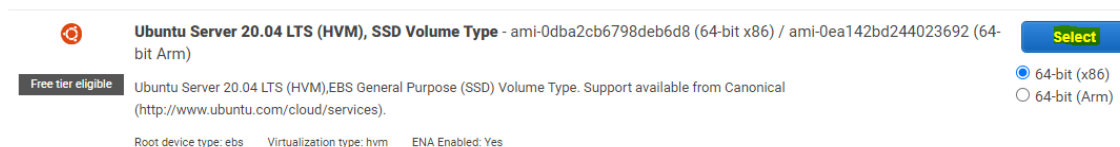


Figura # 4 Sistema operativo y arquitectura a seleccionar para la instancia virtual

Para este ejercicio, deje las opciones seleccionadas por defecto excepto las definidas en la pantalla “Step 6: Configure Security Group”. En dicha pantalla, en la tabla que se muestra, bajo la columna “Source” seleccione del desplegable la opción “My IP” resaltada en la Figura #5

Step 6: Configure Security Group
 A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: ☒ Create a new security group
☐ Select an existing security group

Security group name:
 Description:

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Custom Custom Anywhere My IP	CIDR, IP or Security Group e.g. SSH for Admin Desktop

Add Rule

Figura # 5 Configuración de grupos de seguridad de la instancia virtual

Al seleccionar dicha opción, se cargará automáticamente la dirección IP pública por la cual la red en la que usted se encuentra conectado sale a Internet. A continuación de clic en el botón “Review and Launch” y luego en el botón “Launch”

En la ventana que se muestra, siga los pasos para crear una llave de conexión y a continuación de clic en el botón “Launch instances”

Revise las guías que se ofrecen con detalles acerca de cómo conectarse a la instancia de la máquina virtual recién creada. Para ello, de clic en la opción resaltada en la Figura #6.

Launch Status

How to connect to your instances

Your instances are launching, and it may take a few minutes until they are in the **running** state, when they will be ready for you to use. Usage hours on your new instances will start immediately and continue to accrue until you stop or terminate your instances.

Click **View Instances** to monitor your instances' status. Once your instances are in the **running** state, you can **connect** to them from the Instances screen. [Find out](#) how to connect to your instances.

▼ Here are some helpful resources to get you started

- How to connect to your Linux instance
- Amazon EC2: User Guide
- Learn about AWS Free Usage Tier
- Amazon EC2: Discussion Forum

Figura # 6 Documentación acerca de cómo conectarse a la instancia virtual

Dé clic en el enlace que se muestra en la parte superior de la pantalla para acceder al panel de gestión de instancias. Dicho enlace se encuentra seguido de la leyenda “The following instance launches have been initiated: ...” En dicho panel podrá darse cuenta cuando la instancia ha sido aprovisionada y se encuentre corriendo. En la Figura #7 se muestra dicho panel. Nótese que la instancia ya fue aprovisionada y se encuentra en estado “Running”

Name	Instance ID	Instance state	Instance type	Status check	Alarm Status	Availability zone
-	i-0c3bf64ff3315c1d6	Running	t2.micro	Initializing	No alarms	us-east-1d

Figura # 7 Detalles de aprovisionamiento y estado de la instancia virtual creada

* Entregable *

Documente los detalles y especificaciones de la instancia de máquina virtual creada. Entre los aspectos a documentar incluya: recursos asignados a la máquina virtual, sistema operativo, arquitectura, direccionamiento IPv4 e IPv6 tanto público como privado, detalles de DNS.

En la pantalla que se muestra en la Figura #7, de clic en el enlace asociado al identificador de la instancia. A continuación, de clic en el botón “Connect” para acceder a los detalles de conexión a la instancia. En la pantalla que se muestra, siga las instrucciones detalladas en la pestaña SSH client para conectarse a la máquina virtual. En la Figura #8 se muestran tales instrucciones. Note que los detalles de conexión serán distintos a los mostrados en la Figura #8, pues estos son específicos a cada instancia creada en Amazon AWS.

Connect to instance Info

Connect to your instance i-0c3bf64ff3315c1d6 using any of these options

EC2 Instance Connect | Session Manager | **SSH client**

Instance ID
i-0c3bf64ff3315c1d6

1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is Antonio-AWS_Educate.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.

```
chmod 400 Antonio-AWS_Educate.pem
```
4. Connect to your instance using its Public DNS:

```
ec2-54-226-213-55.compute-1.amazonaws.com
```

Example:

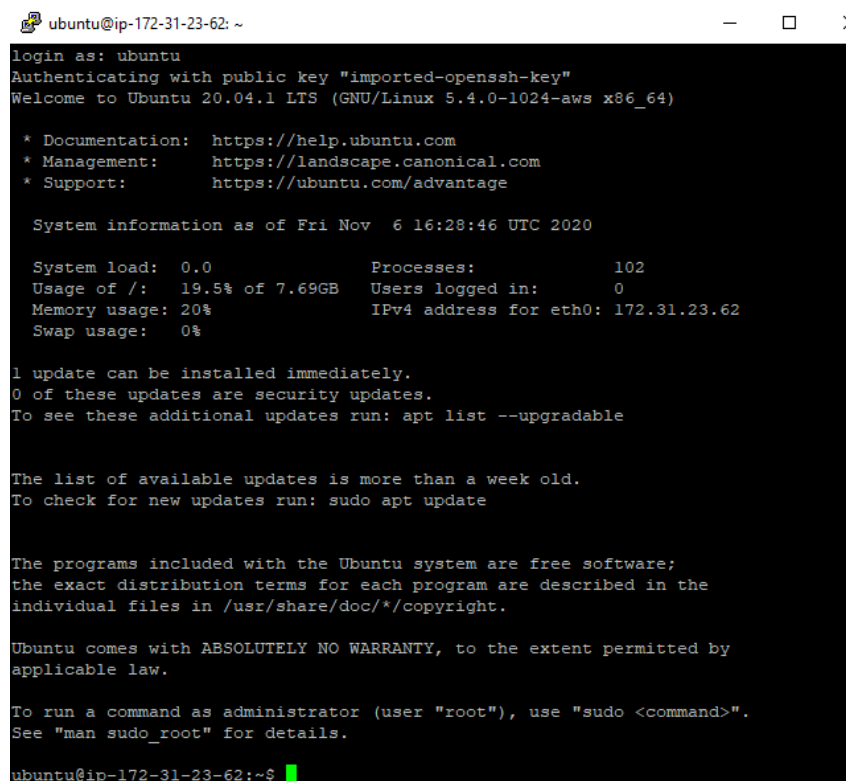
```
ssh -i "Antonio-AWS_Educate.pem" ubuntu@ec2-54-226-213-55.compute-1.amazonaws.com
```

Note: In most cases, the guessed user name is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

Figura # 8 Detalles de cómo conectarse a la instancia virtual

Nota: si utiliza el cliente Putty en Windows, puede hacer uso de esta guía para conectarse: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.html>

De conectarse correctamente, podrá visualizar la terminal de la instancia de máquina virtual, tal y como se muestra en la Figura #9.



```
ubuntu@ip-172-31-23-62: ~
login as: ubuntu
Authenticating with public key "imported-openssh-key"
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-1024-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Fri Nov  6 16:28:46 UTC 2020

System load:  0.0               Processes:    102
Usage of /:   19.5% of 7.69GB   Users logged in:  0
Memory usage: 20%              IPv4 address for eth0: 172.31.23.62
Swap usage:   0%

1 update can be installed immediately.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-23-62:~$
```

Figura # 9 Mensaje de bienvenida mostrado en la terminal de la instancia virtual

*** Entregable ***

Utilice la herramienta *nmap* para obtener los puertos abiertos en la instancia virtual. Ejecute el comando para todas las direcciones IPs asignadas a la instancia virtual. Documente los resultados.

Pasos para instalar y configurar un servidor web Apache

Una vez que haya obtenido acceso a la terminal de la instancia virtual, siga los pasos que se detallan en la siguiente guía para instalar y configurar un servidor web Apache.

Guía → <https://www.digitalocean.com/community/tutorials/how-to-install-the-apache-web-server-on-ubuntu-20-04>

*** Entregable ***

Documente los resultados de la instalación y configuración del servidor web Apache. Para ello, cree una página web simple con la sigla y el nombre del curso, así como con su número de carné y nombre completo. Muestre cada uno de estos datos en una línea de la página web.

*** Entregable ***

Utilice la herramienta wireshark o TCP-dump para filtrar los paquetes asociados a la consulta de la página web creada en el servidor. Documente mediante pantallazos, los datos enviados (HTTP request) y recibidos (HTTP response).

Pasos para instalar y configurar un certificado digital auto-firmado

Una vez que haya instalado y configurado el servidor web Apache en la instancia virtual, proceda a crear un certificado digital auto-firmado mediante el cual se habilite el acceso al servidor a través del protocolo HTTPS. Puede crear el certificado para que funcione con el dominio "<Su_Apellido>.com"

Para llevar a cabo la creación del certificado digital, siga los pasos que se detallan en la siguiente guía.

Guía → <https://www.digitalocean.com/community/tutorials/how-to-create-a-self-signed-ssl-certificate-for-apache-in-ubuntu-20-04>

*** Entregable ***

Documente los resultados de la creación e instalación del certificado digital en el servidor web Apache. Para ello, consulte la página web creada en la sección anterior y utilice la herramienta wireshark o TCP-dump para filtrar los paquetes asociados a la consulta de la página web creada en el servidor. Documente nuevamente mediante pantallazos, los datos enviados (HTTP request) y recibidos (HTTP response). ¿Son los datos enviados visibles en texto plano? ¿Por qué no puede ver los datos de la página web?

*** Entregable ***

Utilice la herramienta *nmap* para obtener los puertos abiertos en la instancia virtual, una vez instalado y configurado el servidor web Apache y el certificado digital auto-firmado. Ejecute el comando para todas las direcciones IPs asignadas a la instancia virtual. Documente los resultados.

Nota: documente toda la información que considere pertinente. Recuerde incluir en el documento de la solución su nombre completo y número de carné.

IMPORTANTE: el modelo de costos con que trabajan las instancias virtuales de Amazon AWS está basado en el tiempo de uso que se les dé a las mismas. Cada estudiante cuenta con un voucher de \$50 para hacer uso de las instancias virtuales. Recuerde apagar las instancias una vez concluido el trabajo, para evitar quedarse sin crédito.

*** ACTUALIZACIÓN ***

¡Información importante!

Si al intentar conectarse a la instancia virtual con el explorador web, reciben un *timeout* verifiquen los siguientes pasos:

Cuando se intenten conectar a la instancia virtual deben utilizar el registro de “Public IPv4 DNS” (mostrado en la Figura #10) el cual se puede encontrar en los datos de la instancia virtual en la pestaña de Networking. Esto se debe a que como ya hemos visto en el curso, no hay suficientes direcciones IPv4 públicas como para asignarle una a cada instancia virtual, por lo que de seguro las instancias virtuales que estamos utilizando están detrás de un servidor NAT, el cual como también ya vimos, impide que desde Internet se pueda acceder a un host directamente en la red privada. Al utilizar un nombre de dominio, internamente se redirecciona el tráfico hacia uno u otro host como en este caso.












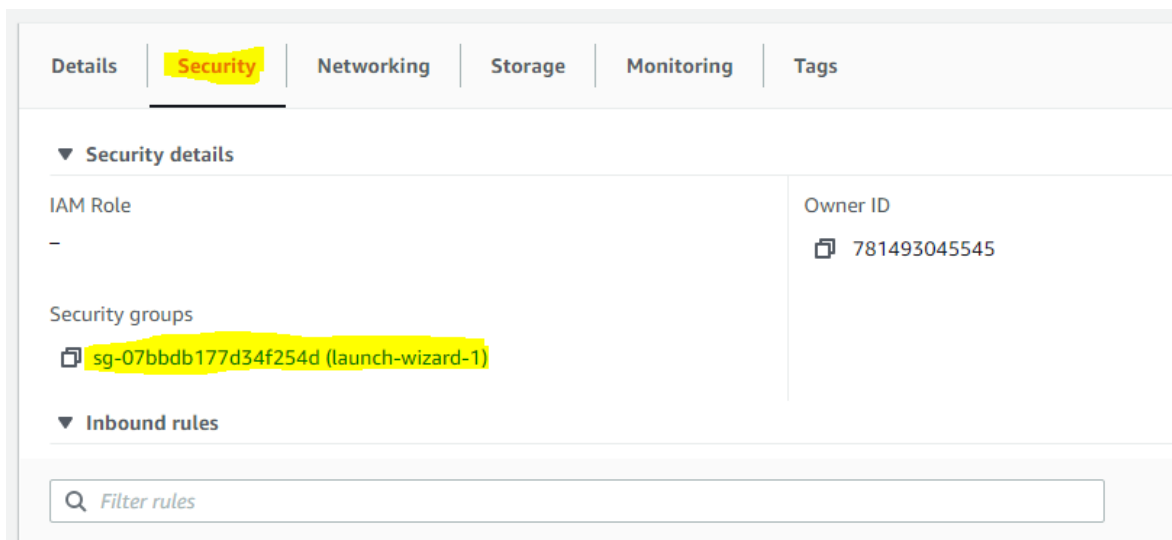
Details	Security	Networking	Storage	Monitoring	Tags
▼ Networking details Info					
Public IPv4 address  54.91.92.205 open address 		Private IPv4 addresses  172.31.23.62		VPC ID  vpc-0af53c77 	
Public IPv4 DNS  ec2-54-91-92-205.compute-1.amazonaws.com open address 		Private IPv4 DNS  ip-172-31-23-62.ec2.internal		Subnet ID  subnet-230d416e 	
IPv6 addresses -		Secondary private IPv4 addresses -		Availability zone  us-east-1d	
Carrier IP addresses (ephemeral) -		Outpost ID -			
▼ Network Interfaces Info					

Figura # 10 Registro Public IPv4 DNS

Las instancias virtuales se encuentran detrás de un firewall de Amazon (adicional al que se implementa en cada instancia virtual). Por ello, para conectarse a un servicio en un puerto en específico, se debe habilitar dicho puerto en el firewall de la plataforma. Para ello se debe ir a la configuración de la instancia virtual, pestaña “Security” y dar click en el nombre del grupo de seguridad, tal y como se resalta en la Figura #11.



A continuación, deben agregar una regla para conexiones entrantes dando clic en el botón “Edit inbound rules”. EN la pantalla que se muestra, deben dar clic en el botón “Add rule” y en la lista desplegable “Type” seleccionar el servicio para el cual desean abrir el puerto, en este caso HTTP o HTTPS. Además, en el campo “Source” deben digitar la dirección 0.0.0.0/0¹. En la Figura #12 se muestra como debe quedar la regla. Al finalizar se debe dar clic en el botón “Save rules”

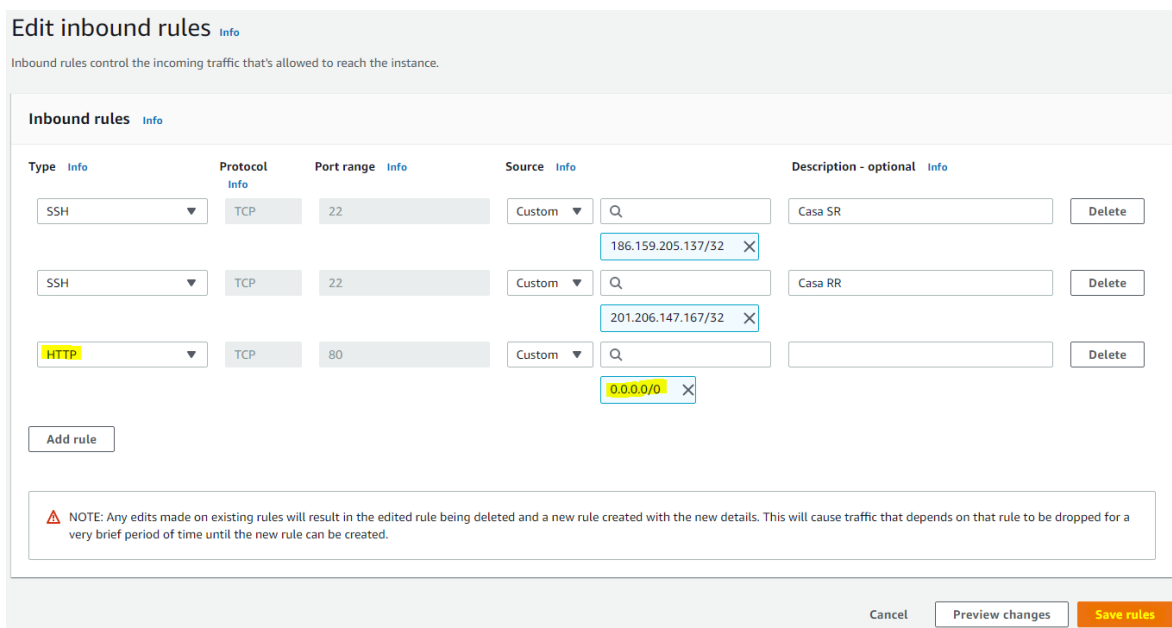


Figura # 11 Creación de ejemplo de regla para conexiones entrantes en puerto 80 (HTTP)

De esta manera ya debería poder conectarse a la instancia virtual, utilizando el “Public IPv4 DNS”

¹ En este caso la dirección 0.0.0.0/0 se utiliza para hacer referencia a todas las direcciones IPs con cualquier máscara de red. Este tipo de direcciones se utilizan con frecuencia en los firewalls y en algunos algoritmos de enrutamiento y se conocen como wildcards.