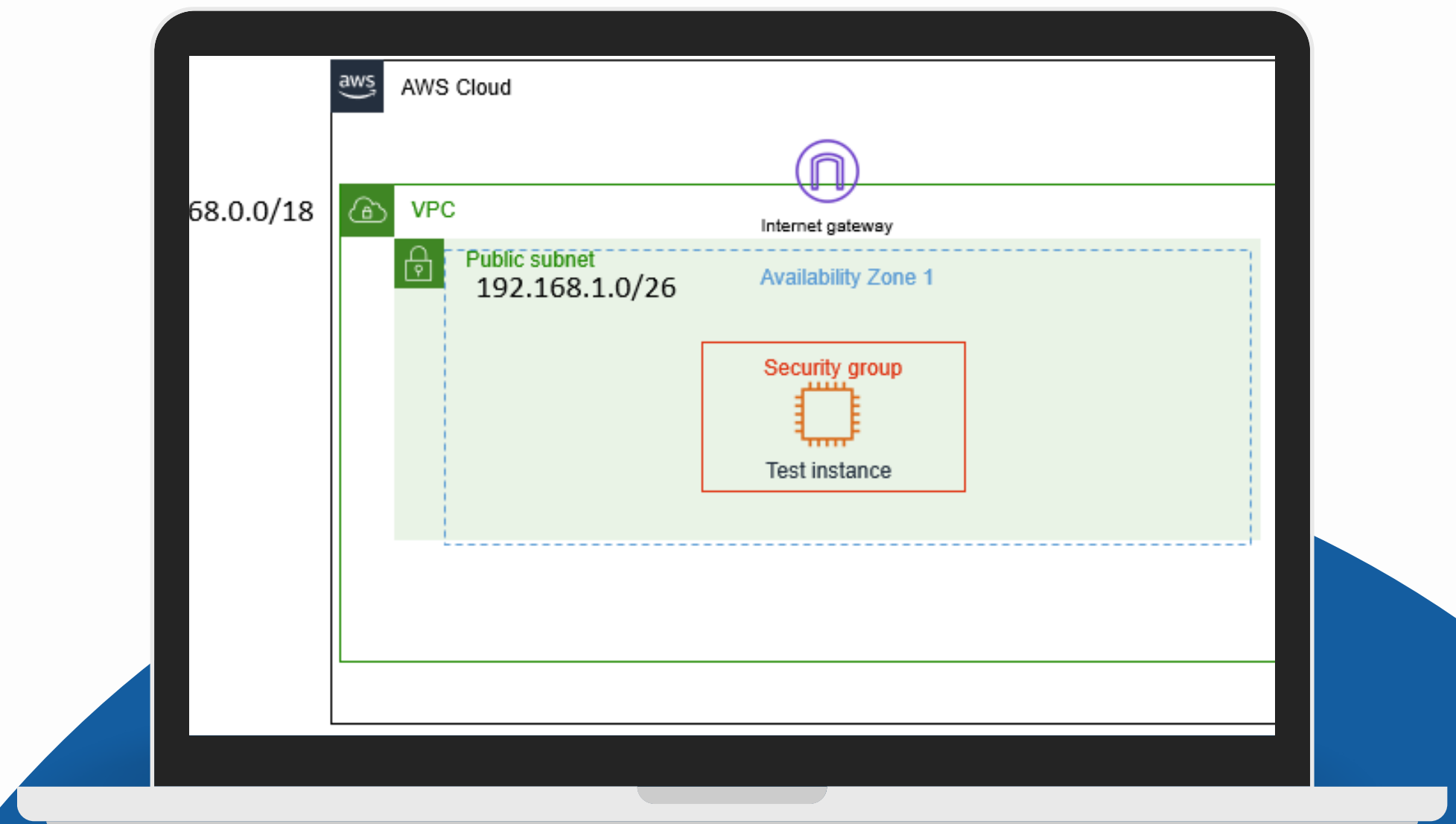




Lab - Recursos de red para una VPC

Presentación realizada por Brendon Buriol,
Paulo Sena, Ignivé Amaro y Valeria Cantoni



Objetivos

- Resumir el escenario del cliente
- Crear una VPC, una puerta de enlace de Internet, una tabla de rutas, un grupo de seguridad, una lista de acceso a la red y una instancia EC2 para crear una red enrutable dentro de la VPC.
- Familiarizarse con la consola
- Desarrollar una solución al problema de los clientes que se encuentra en esta práctica de laboratorio.

Correo electrónico del cliente

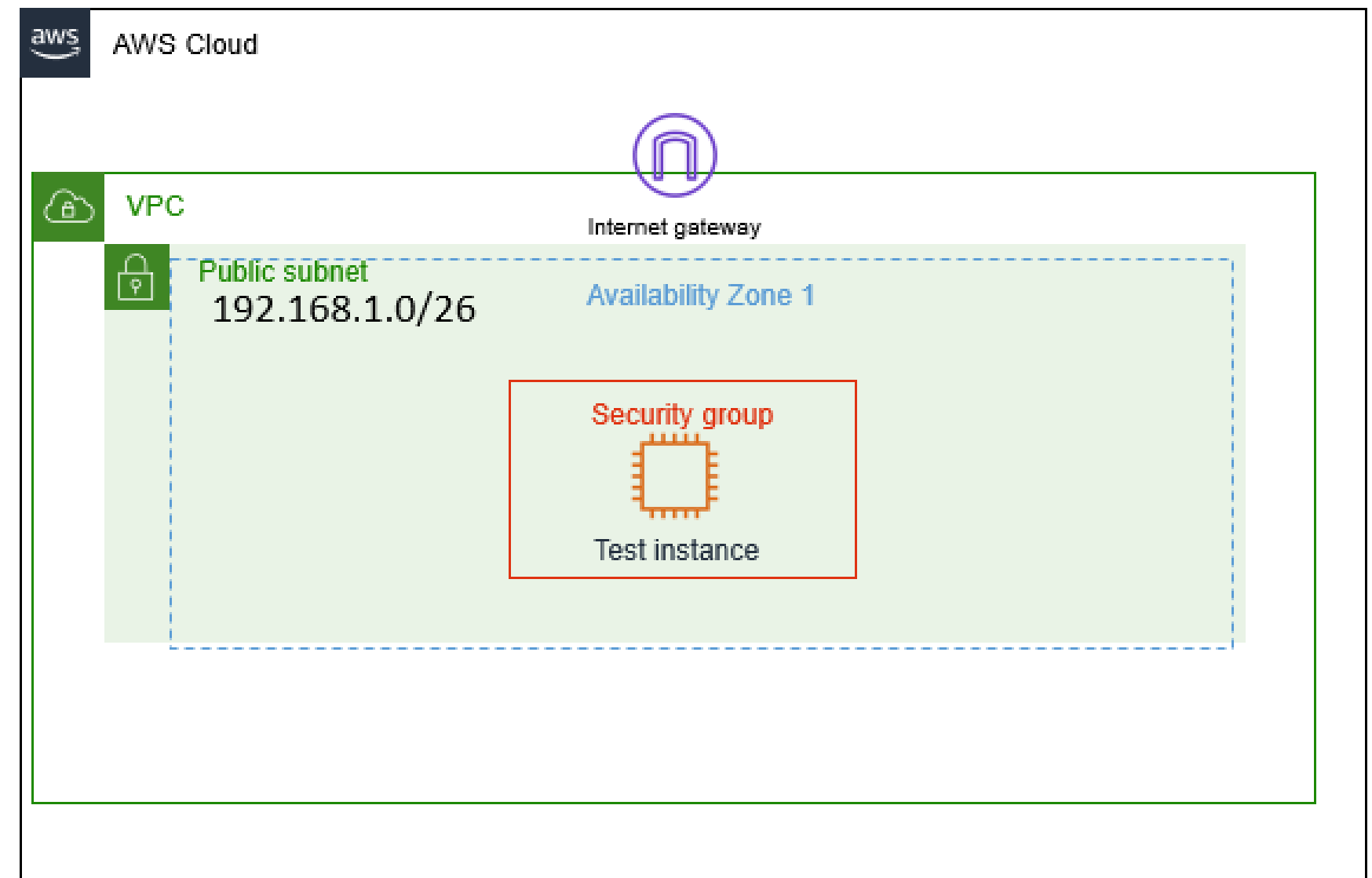
¡Hola, soporte en la nube!

Anteriormente me comuniqué con usted para solicitar ayuda para configurar mi VPC. Pensé que sabía cómo conectar todos los recursos para establecer una conexión a Internet, pero ni siquiera puedo hacer ping fuera de la VPC. ¡Todo lo que necesito hacer es hacer ping! ¿Pueden ayudarme a configurar mi VPC para que tenga conectividad de red y pueda hacer ping? La arquitectura está debajo.

¡Gracias!

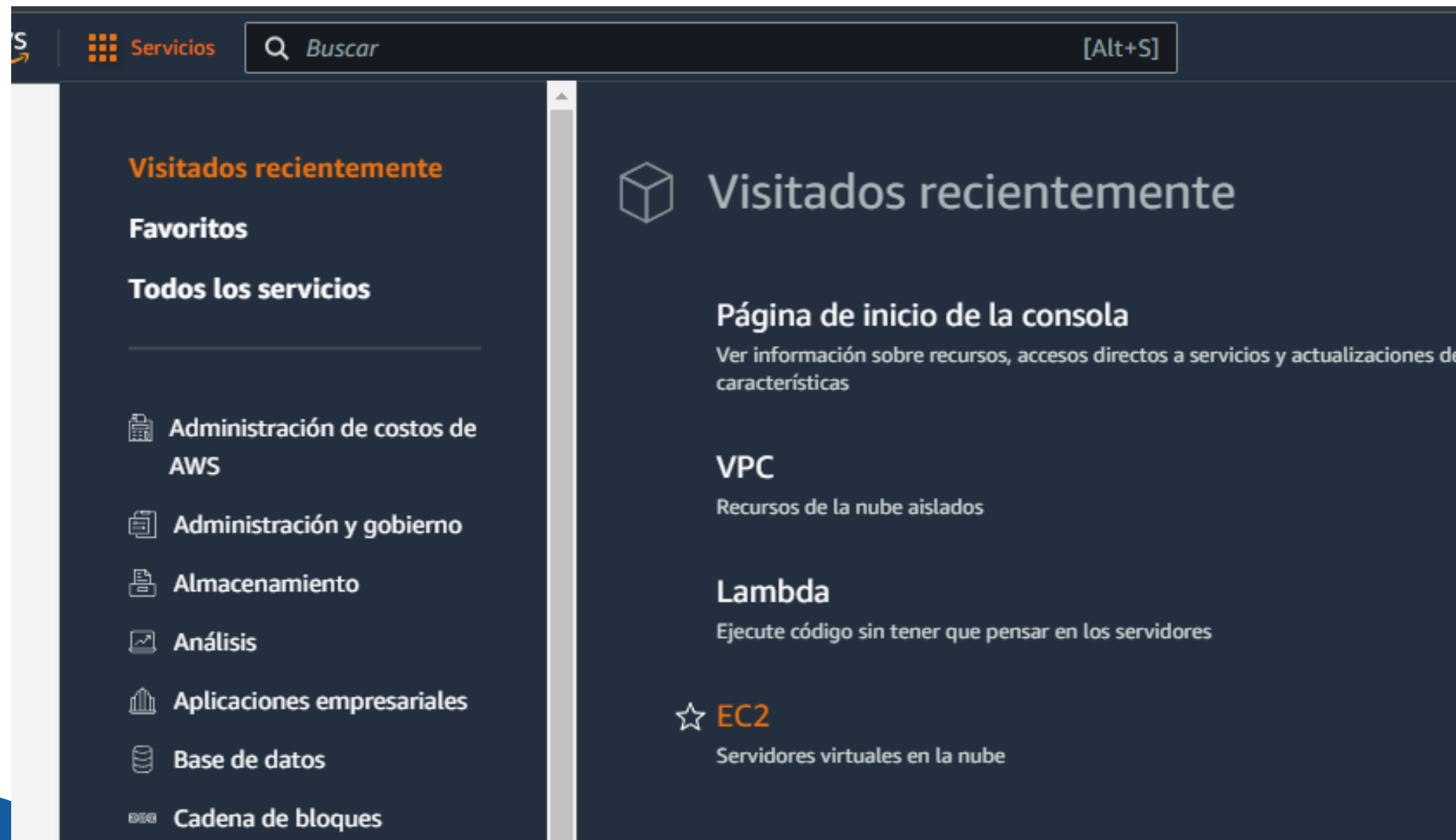
Brock, propietario de una startup

192.168.0.0/18



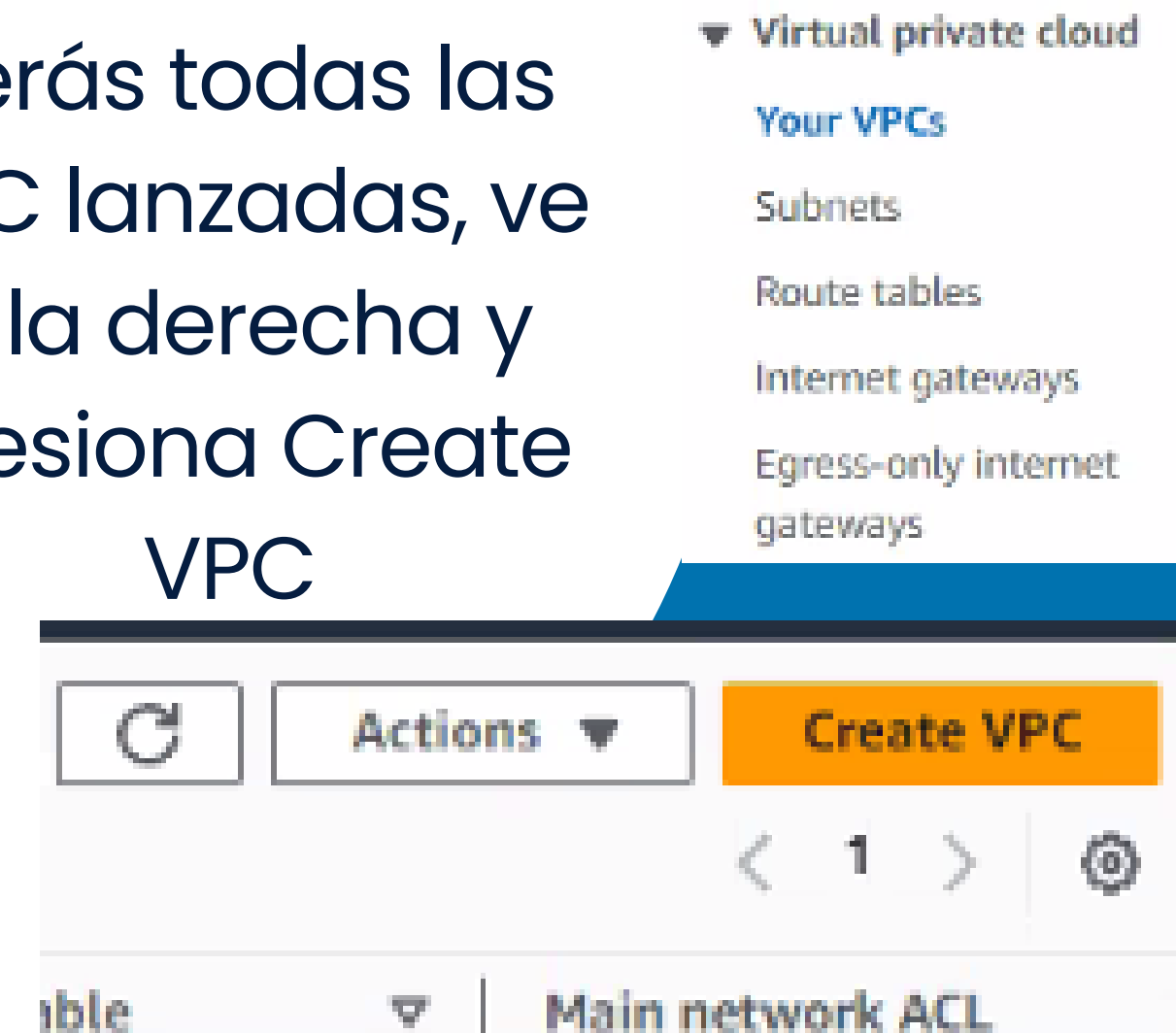
Tarea 1: Investigar las necesidades del cliente

Una vez en la AWS Management Console, ve al menu de servicios y busca el servicio VPC



En el panel izquierdo selecciona **Your VPCs**

Verás todas las VPC lanzadas, ve a la derecha y presiona **Create VPC**



VPC settings

Resources to create [Info](#)

Create only the VPC resource or the VPC and other networking resources.

☒ VPC only

☐ VPC and more

Name tag - optional

Creates a tag with a key of 'Name' and a value that you specify.

Test vpc

IPv4 CIDR block [Info](#)

☒ IPv4 CIDR manual input

☐ IPAM-allocated IPv4 CIDR block

IPv4 CIDR

192.168.0.0/18

CIDR block size must be between /16 and /28.

IPv6 CIDR block [Info](#)

☒ No IPv6 CIDR block

☐ IPAM-allocated IPv6 CIDR block

☐ Amazon-provided IPv6 CIDR block

☐ IPv6 CIDR owned by me

Tenancy [Info](#)

Default

En VPC settings utiliza
esta configuración

Name tag: Test VPC

IPv4 CIDR: 192.168.0.0/18

Luego deja todo en
predeterminado



Para el siguiente paso
ve al panel izquierdo y
clickea en Subnets



Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet
gateways

VPC

VPC ID
Create subnets in this VPC.

vpc-08288fff3895cf05f (Test vpc) ▼

Associated VPC CIDRs

IPv4 CIDRs

192.168.0.0/18

En VPC ID selecciona la que termine en
(Test vpc)
y copia esta configuración



Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.

Public subnate

The name can be up to 256 characters long.

Availability Zone [Info](#)
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

No preference ▼

IPv4 VPC CIDR block [Info](#)
Choose the IPv4 VPC CIDR block to create a subnet in.

192.168.0.0/18 ▼

IPv4 subnet CIDR block

192.168.1.0/28 16 IPs

< > ^ v

▼ **Tags - optional**

Key	Value - optional	
Q Name X	Q Public subnate X	Remove
Add new tag		
You can add 49 more tags.		
Remove		
Add new subnet		

Cancel **Create subnet**

✓ You have successfully created 1 subnet: subnet-0cb82c278f9866a3f

Subnets (1) [Info](#)

Find resources by attribute or tag

Subnet ID : subnet-0cb82c278f9866a3f ✕ Clear filters

<input type="checkbox"/>	Name	Subnet ID	State	VPC	IPv4 CIDR
<input type="checkbox"/>	Public subnate	subnet-0cb82c278f9866a3f	✓ Available	vpc-08288fff3895cf05f Test vpc	192.168.1.0/28

Una vez finalizado verifica que aparezca

Luego en el panel izquierdo selecciona
Route Tables

Filter by VPC:
Select a VPC

▼ Virtual private cloud

- Your VPCs
- Subnets
- Route tables**
- Internet gateways
- Egress-only internet gateways
- Carrier gateways

Create route table [Info](#)

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Route table settings

Name - optional

Create a tag with a key of 'Name' and a value that you specify.

VPC

The VPC to use for this route table.

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key

Value - optional

[Remove](#)[Add new tag](#)

You can add 49 more tags.

[Cancel](#)[Create route table](#)

En la pestaña de Name escribe
Public route table
En VPC selecciona la que termine
en (Test VPC)
Y en Tags copia estos valores
Key: Name
Value: Public route table

▼ Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

Carrier gateways

DHCP option sets

Elastic IPs

Managed prefix lists

Endpoints

Endpoint services

Luego en el panel izquierdo selecciona
Internet gateways

Y clickea en Create a internet gateway
y dale el nombre de IGW test VPC

Create internet gateway [Info](#)

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

Name tag

Creates a tag with a key of 'Name' and a value that you specify.

Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key

Value - optional

Remove

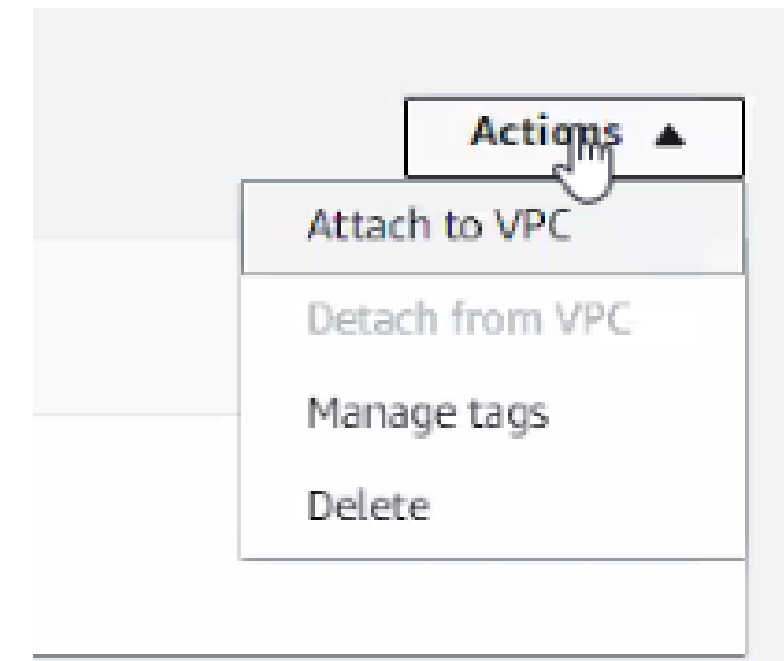
Add new tag

You can add 49 more tags.

Cancel

Create internet gateway

Luego adjuntalo a una VPC en la pestaña de Actions en la esquina superior derecha y elige la VPC creada anteriormente



Attach to VPC (igw-078a18cdb64dd9b85) [Info](#)

VPC
Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs
Attach the internet gateway to this VPC.

► AWS Command Line Interface command

Cancel **Attach internet gateway**

▼ Virtual private cloud

Your VPCs

Subnets

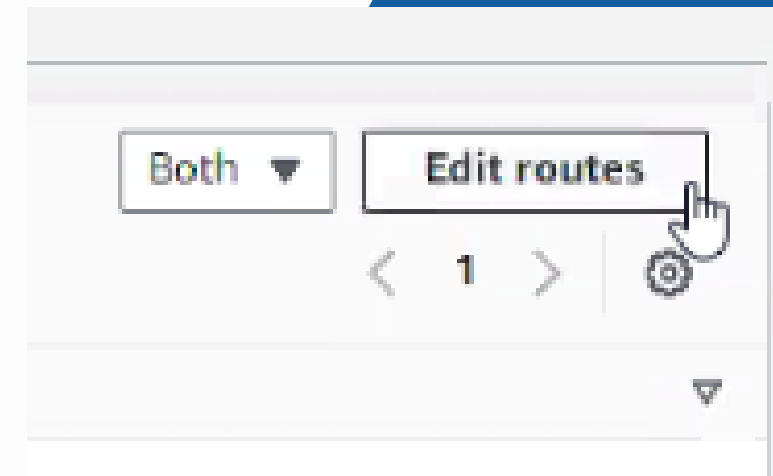
Route tables

Internet gateways

Egress-only internet gateways

Carrier gateways

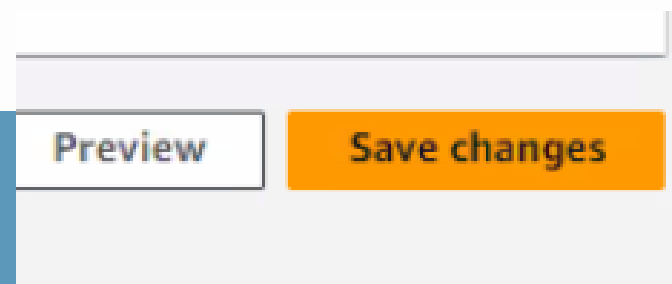
En el panel izquierdo selecciona **Route tables** y selecciona Public Route tables y clickea en Edit routes.



Luego copia esta configuración



Destination		Target	Status
192.168.0.0/18		local	✓ Active
		Q local	X
Q 0.0.0.0/0	X	Internet Gateway	-
		Q igw-078a18cdb64dd9b85	X
Add route			



Subnets without explicit associations (1)

Edit subnet associations

< 1 > ⓘ

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

Find subnet association

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
Public subnate	subnet-0cb82c278f9866a3f	192.168.1.0/28	-

Asociamos una tabla de erutamiento a una subnet.
Seleccionandola y clikeando en Save Association

Available subnets (1/1)

Filter subnet associations

< 1 > ⓘ

☒

Name

☒

Subnet ID

☒

IPv4 CIDR

☒

IPv6 CIDR

☒

Route table ID

☒

Public subnate

[subnet-0cb82c278f9866a3f](#)

192.168.1.0/28

-

[Main \(rtb-02056951ae1e03f47\)](#)

ected subnets

subnet-0cb82c278f9866a3f / Public subnate

Cancel

Save associations

▼ Security

Network ACLs

Security groups

En el panel izquierdo seleccionamos esta opción



Seleccionamos este ítem para crear la ACL



Network ACLs (1/2) [Info](#)

Find resources by attribute or tag

	Name	Network ACL ID	Associated with	Default	VPC ID	Inbound rules count	Outbound rules count	Owner
<input type="checkbox"/>	-	acl-08d075b4f87823774	4 Subnets	Yes	vpc-0b1731b243bf085ba	2 Inbound rules	2 Outbound rules	510905830354
<input checked="" type="checkbox"/>	-	acl-0a3335f096b0e6a70	subnet-0cb82c278f9866a3f / Public subnate	Yes	vpc-08288fff3895cf05f / Test vpc	2 Inbound rules	2 Outbound rules	510905830354

Después de crear la NACL, debería tener el siguiente aspecto. Esto indica que solo hay un número de regla, que es 100, que establece que todo el tráfico, todos los protocolos, todos los rangos de puertos, de cualquier fuente (0.0.0.0/0) pueden ingresar (entrante) a la subred. El asterisco * indica que se rechaza cualquier otra cosa que no coincida con esta regla.

acl-0a3335f096b0e6a70

Details | **Inbound rules** | Outbound rules | Subnet associations | Tags

Inbound rules (2)

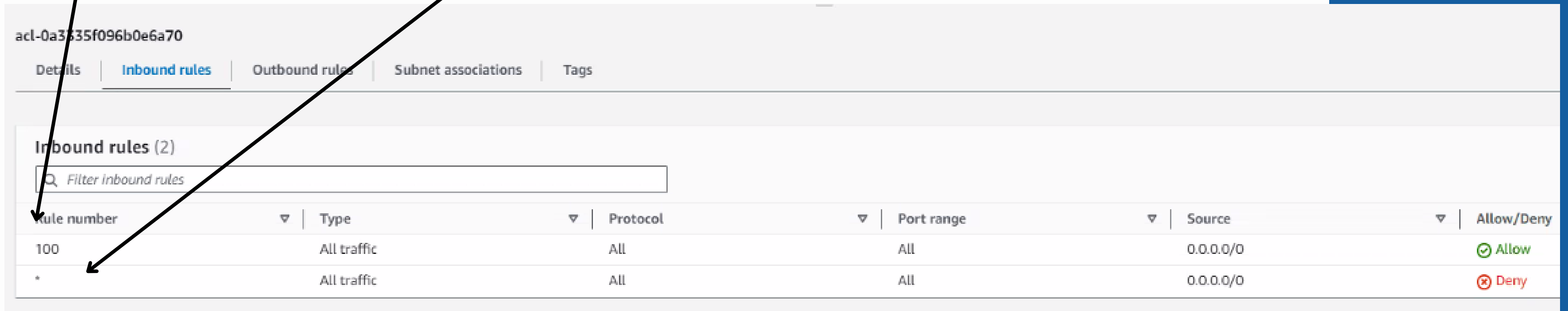
Filter inbound rules

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	✓ Allow
*	All traffic	All	All	0.0.0.0/0	✗ Deny

Después de crear la NACL, debería tener el siguiente aspecto.

Esto indica que solo hay un número de regla, que es 100, que establece que todo el tráfico, todos los protocolos, todos los rangos de puertos, de cualquier fuente (0.0.0.0/0) pueden ingresar (entrante) a la subred.

El asterisco * indica que se rechaza cualquier otra cosa que no coincida con esta regla.



acl-0a3335f096b0e6a70

Details | **Inbound rules** | Outbound rules | Subnet associations | Tags

Inbound rules (2)

Filter inbound rules

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

Create network ACL [Info](#)

A network ACL is an optional layer of security that acts as a firewall for controlling traffic in and out of a subnet.

Network ACL settings

Name - optional

Creates a tag with a key of 'Name' and a value that you specify.

VPC

VPC to use for this network ACL.

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key

Value - optional

You can add 49 more tags

Ve al panel izquierdo y selecciona Network ACL y crea una nueva con esta configuración

Después de crear la NACL, debería tener el siguiente aspecto. Esto indica que hay un solo número de regla, que es 100,

y que establece que todo el tráfico, todos los protocolos y todos los rangos de puerto desde cualquier fuente (0.0.0.0/0) pueden ingresar (entrar) a la subred.

acl-0a3335f096b0e6a70

Details



Inbound rules

Outbound rules

Subnet associations

Tags

Outbound rules (2)

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	 Allow
*	All traffic	All	All	0.0.0.0/0	 Deny

Luego, nos dirigimos a Security dentro del panel de navegación de la izquierda. Dentro de él, ingresamos a Security groups



▼ **Security**

- Network ACLs
- Security groups**



Creamos un Grupo de Seguridad

Al crear el grupo, ingresamos los siguientes datos:

Create security group [Info](#)

A security group acts as a virtual firewall for your instance to control

Basic details

Security group name [Info](#)

Public Security Group

Name cannot be edited after creation.

Description [Info](#)

allows public access

VPC [Info](#)

vpc-08288fff3895cf05f (Test vpc)

**En reglas de Inbound
agregamos SSH, HTTP y
HTTPS**

Inbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Source Info
SSH ▼	TCP	22	Anywhere-IPv4 ▼ 0.0.0.0/0 X
HTTP ▼	TCP	80	Anywhere-IPv4 ▼ 0.0.0.0/0 X
HTTPS ▼	TCP	443	Anywhere-IPv4 ▼ 0.0.0.0/0 X

[Add rule](#)

**En reglas de Outbound
permitimos All traffic**

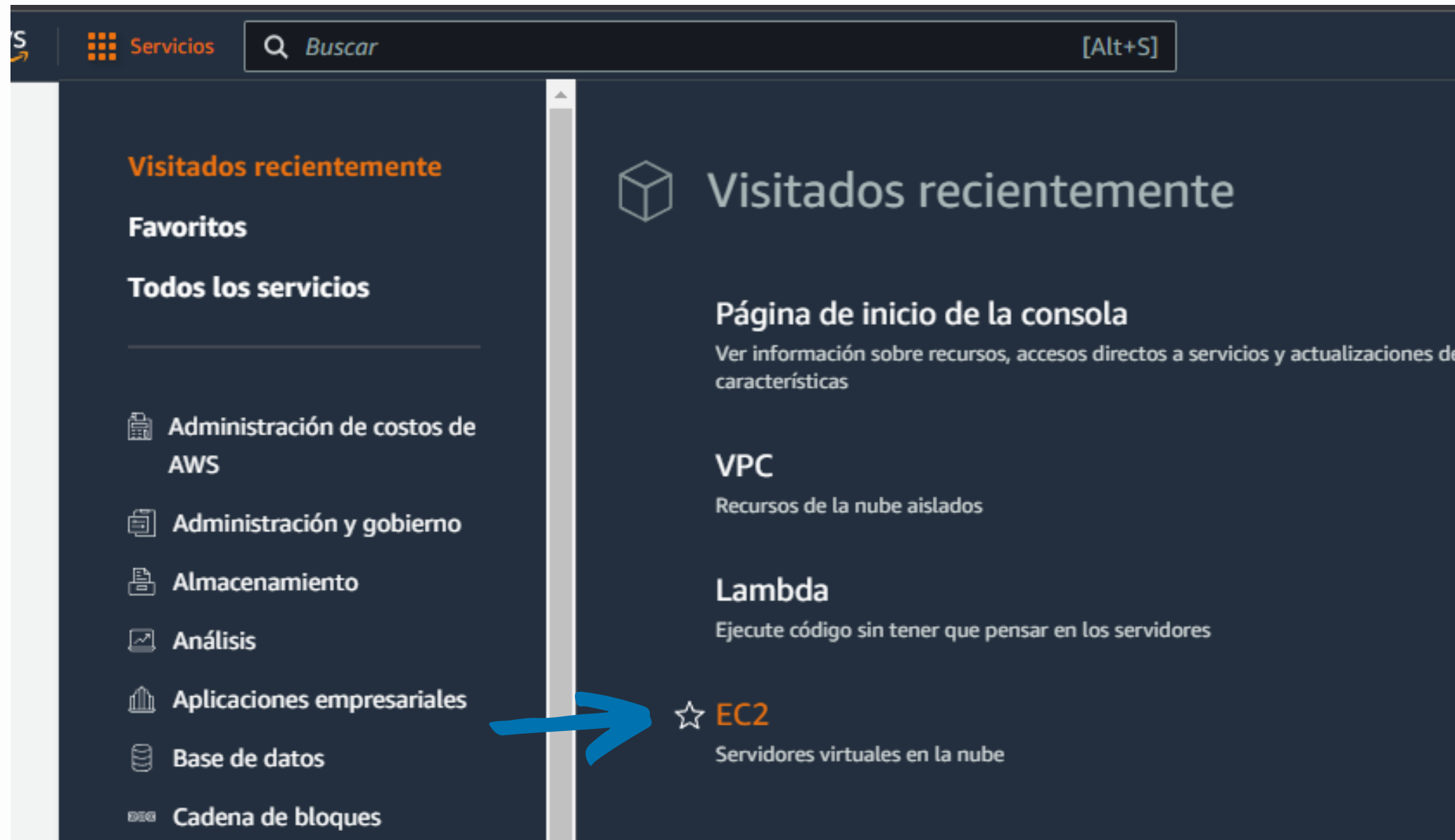
Outbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Destination Info
All traffic ▼	All	All	Custom ▼ 0.0.0.0/0 X

[Add rule](#)

Tarea 2: iniciar la instancia EC2 y SSH en la instancia

Para iniciar la instancia EC2, primero debemos dirgirnos, a partir del desplegable "Servicios", a EC2



Luego, ingresaremos a la sección Instances, desde la barra de navegación izquierda



Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans

▼ Network settings [Info](#)

VPC - required [Info](#)

vpc-08288fff3895cf05f (Test vpc)
192.168.0.0/18



Subnet [Info](#)

subnet-0cb82c278f9866a3f **Public subnate**
VPC: vpc-08288fff3895cf05f Owner: 510905830354 Availability Zone: us-west-2b
IP addresses available: 11 CIDR: 192.168.1.0/28



[Create](#)

Auto-assign public IP [Info](#)

Enable

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to

En Network settings sigue estos pasos:

- En VPC elige la que termine en (Test VPC)
- En Subnet elige la Public Subnet
- En Auto-assing selecciona la opción Enable

Name and tags [Info](#)

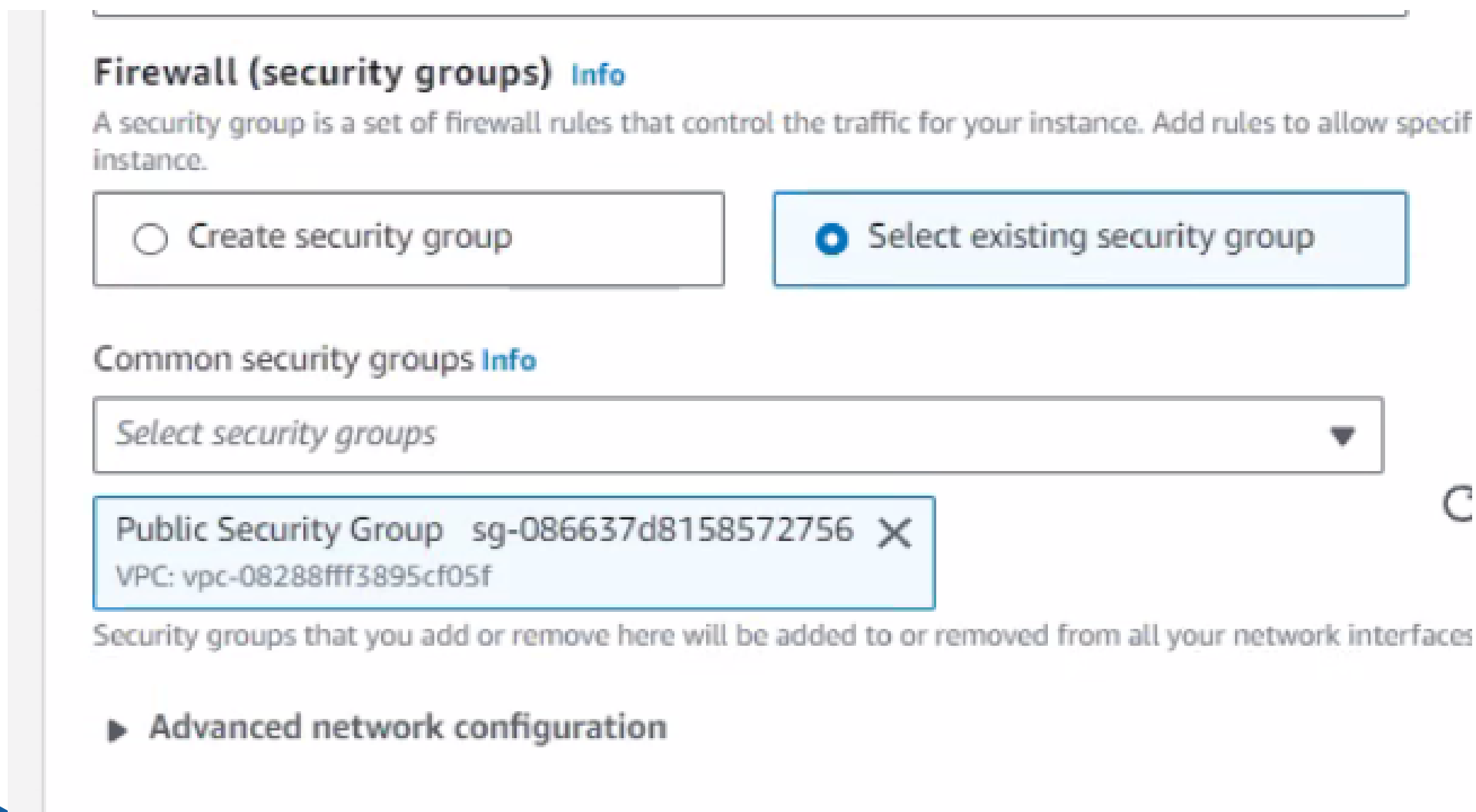
Name

Sala 3

En Name and tags,
ingresaremos el nombre de
nuestra sala

Por último en la pestaña de Firewall (security groups):

- Selecciona la opción "Select existing security group"
- Luego elige Public Security Group



Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific instance.

☐ Create security group ☒ Select existing security group

Common security groups [Info](#)

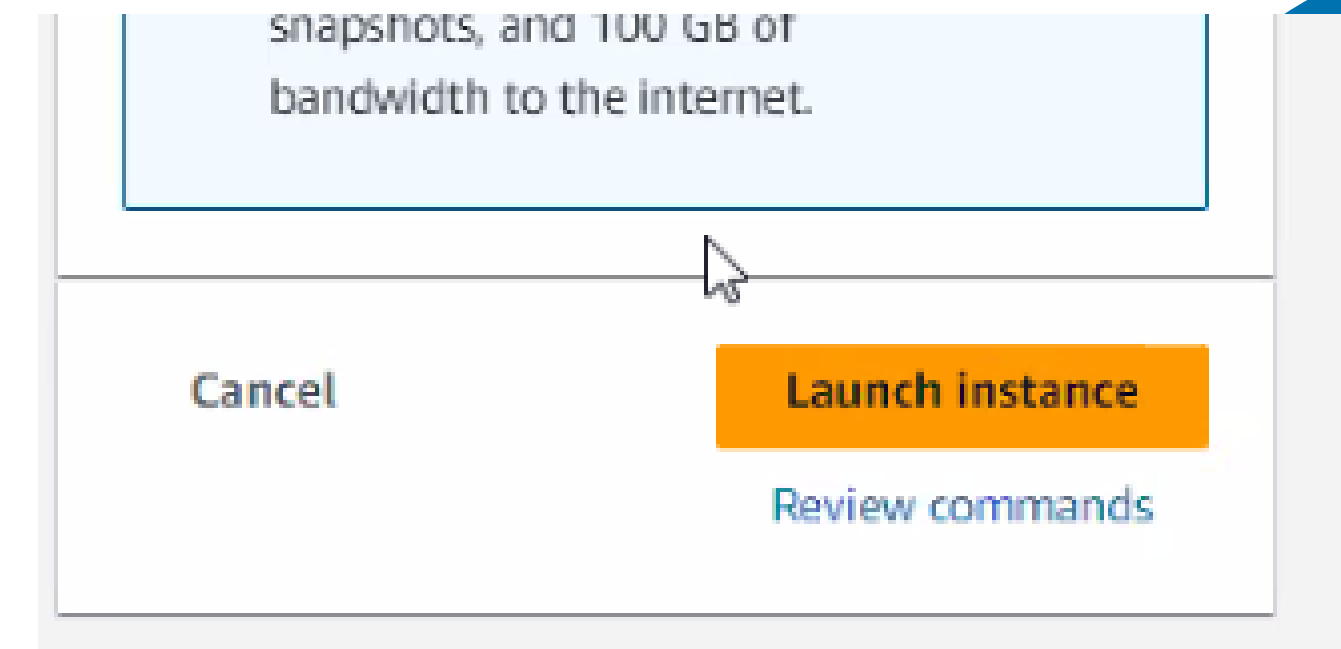
Select security groups

Public Security Group sg-086637d8158572756 ✕
VPC: vpc-08288fff3895cf05f

Security groups that you add or remove here will be added to or removed from all your network interfaces

► Advanced network configuration

El resto de campos quedarán con las opciones predeterminadas. Ahora si ya puedes Lanzar la instancia



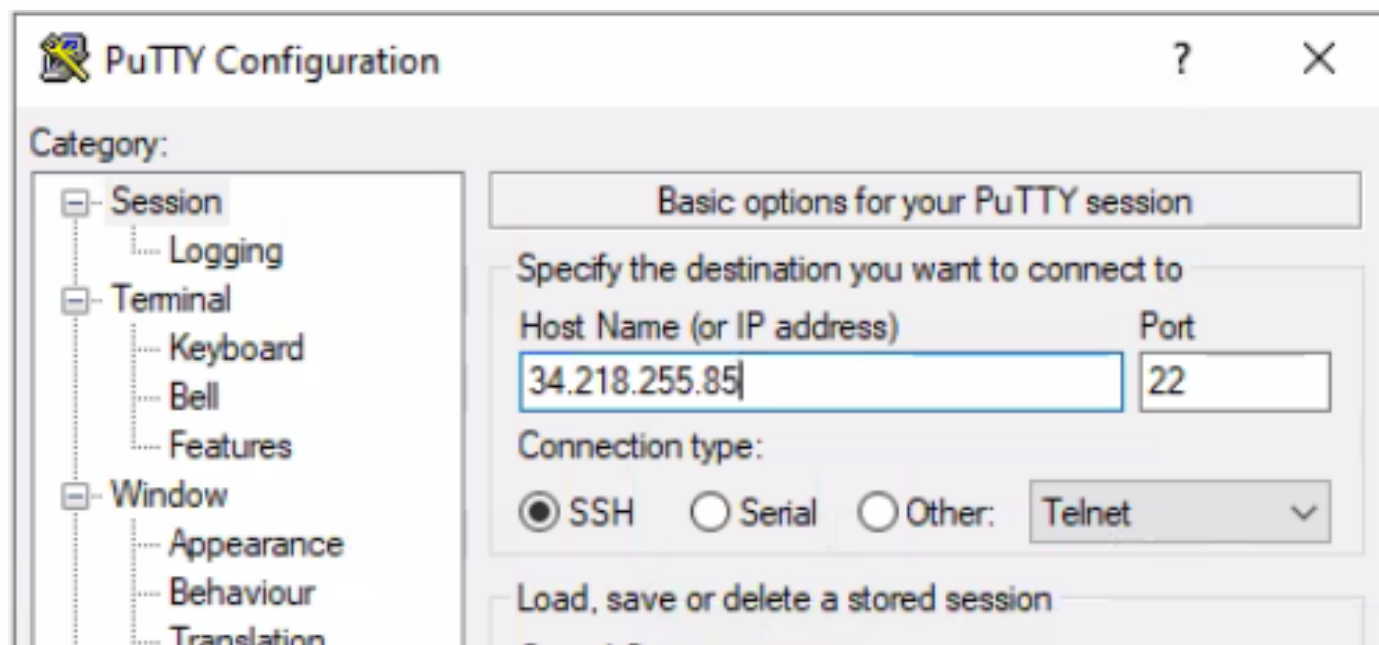
snapshots, and 100 GB of bandwidth to the internet.

Cancel **Launch instance**

[Review commands](#)

Tarea 3: utilizar ping para probar la conectividad a Internet

Luego de conectarnos a la instancia utilizando PuTTY, realizamos un ping a Google utilizando el comando ping.google.com



Como podemos ver, el ping se realiza con éxito, comprobando que se solucionó problema inicial del cliente.

FIN :)



```
login as: ec2-user
Authenticating with public key "imported-openssh-key"

#_
~\_####_      Amazon Linux 2
~~~\_#####\
~~~\_####|     AL2 End of Life is 2025-06-30.
~~~\_#/
~~~V~' '->
~~~~
~~~.~.~
~~~/_/_/_/
~~~/_m/'

A newer version of Amazon Linux is available!

Amazon Linux 2023, GA and supported until 2028-03-15.
https://aws.amazon.com/linux/amazon-linux-2023/

[ec2-user@ip-192-168-1-9 ~]$ ping google.com
PING google.com (142.251.215.238) 56(84) bytes of data.
64 bytes from sea09s35-in-fl4.1el00.net (142.251.215.238): icmp_seq=1 ttl=99 time=7.90 ms
64 bytes from sea09s35-in-fl4.1el00.net (142.251.215.238): icmp_seq=2 ttl=99 time=7.96 ms
64 bytes from sea09s35-in-fl4.1el00.net (142.251.215.238): icmp_seq=3 ttl=99 time=7.90 ms
64 bytes from sea09s35-in-fl4.1el00.net (142.251.215.238): icmp_seq=4 ttl=99 time=7.92 ms
64 bytes from sea09s35-in-fl4.1el00.net (142.251.215.238): icmp_seq=5 ttl=99 time=7.96 ms
64 bytes from sea09s35-in-fl4.1el00.net (142.251.215.238): icmp_seq=6 ttl=99 time=7.91 ms
64 bytes from sea09s35-in-fl4.1el00.net (142.251.215.238): icmp_seq=7 ttl=99 time=7.86 ms
64 bytes from sea09s35-in-fl4.1el00.net (142.251.215.238): icmp_seq=8 ttl=99 time=7.99 ms
64 bytes from sea09s35-in-fl4.1el00.net (142.251.215.238): icmp_seq=9 ttl=99 time=7.93 ms
64 bytes from sea09s35-in-fl4.1el00.net (142.251.215.238): icmp_seq=10 ttl=99 time=7.89 ms
64 bytes from sea09s35-in-fl4.1el00.net (142.251.215.238): icmp_seq=11 ttl=99 time=7.97 ms
64 bytes from sea09s35-in-fl4.1el00.net (142.251.215.238): icmp_seq=12 ttl=99 time=13.4 ms
^C
--- google.com ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 11013ms
rtt min/avg/max/mdev = 7.867/8.386/13.406/1.517 ms
[ec2-user@ip-192-168-1-9 ~]$
```