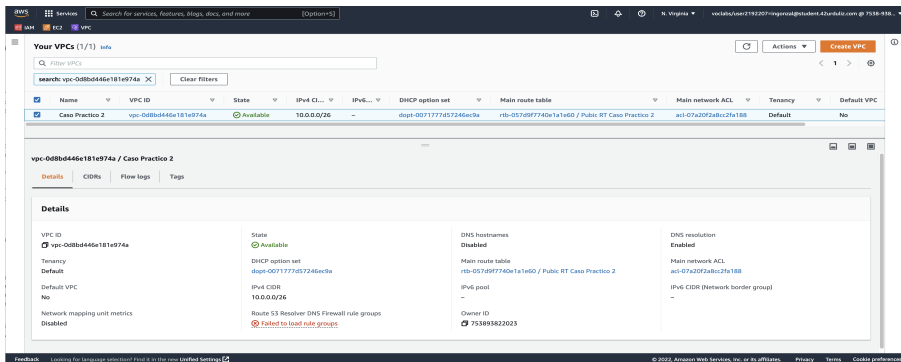


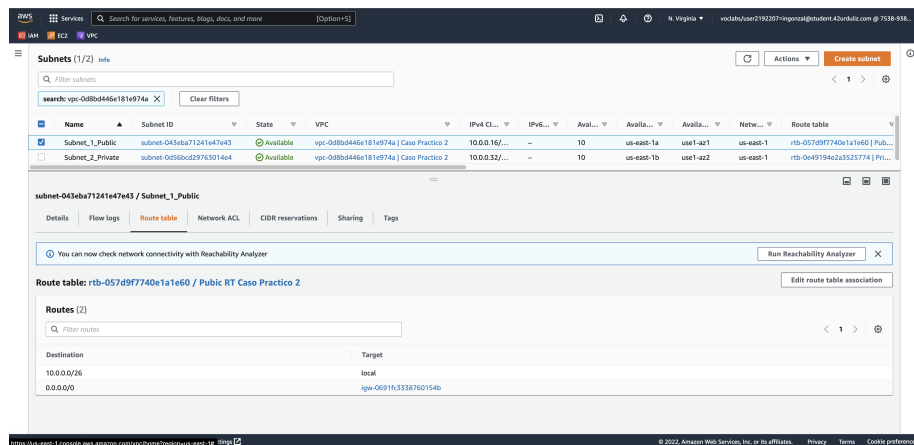
Caso Práctico 2: Redes y Computación en AWS

Tarea 1:

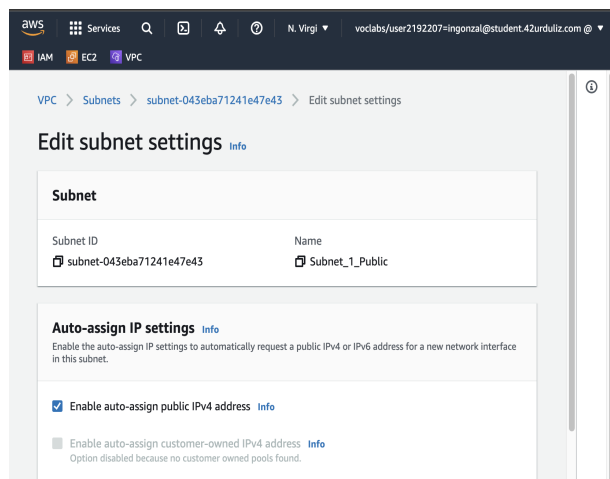
- VPC:



- Public Subnet:



- Auto Assign Ipv4:



- Private Subnet:

Subnets (1/2) Info

search: vpc-0d8bd446e181e974a X Clear filters

Name	Subnet ID	State	VPC	IPv4 Cl...	IPv6...	Avail...	Availa...	Netw...	Route table
Subnet_1_Public	subnet-043bba71241e47e43	Available	vpc-0d8bd446e181e974a Caso Practico 2	10.0.0.16/...	-	10	us-east-1a	us-east-1	rtb-0578f7740e1a1e60 Pub...
Subnet_2_Private	subnet-0d56bcd29763014e4	Available	vpc-0d8bd446e181e974a Caso Practico 2	10.0.0.32/...	-	10	us-east-1b	us-east-1	rtb-0e49194e2a3525774 Pri...

subnet-0d56bcd29763014e4 / Subnet_2_Private

Details Flow logs Route table Network ACL CIDR reservations Sharing Tags

You can now check network connectivity with Reachability Analyzer Run Reachability Analyzer X

Route table: rtb-0e49194e2a3525774 / Private RT Caso Practico 2 Edit route table association

Routes (1)

Filter routes

Destination	Target
10.0.0.0/26	local

- Internet Gateway:

Internet gateways (1/1) Info

search: vpc-0d8bd446e181e974a X Clear filters

Name	Internet gateway ID	State	VPC ID	Owner
igw_Caso_practico_2	igw-0691fc3338760154b	Attached	vpc-0d8bd446e181e974a Caso Practico 2	753893822023

igw-0691fc3338760154b / igw_Caso_practico_2

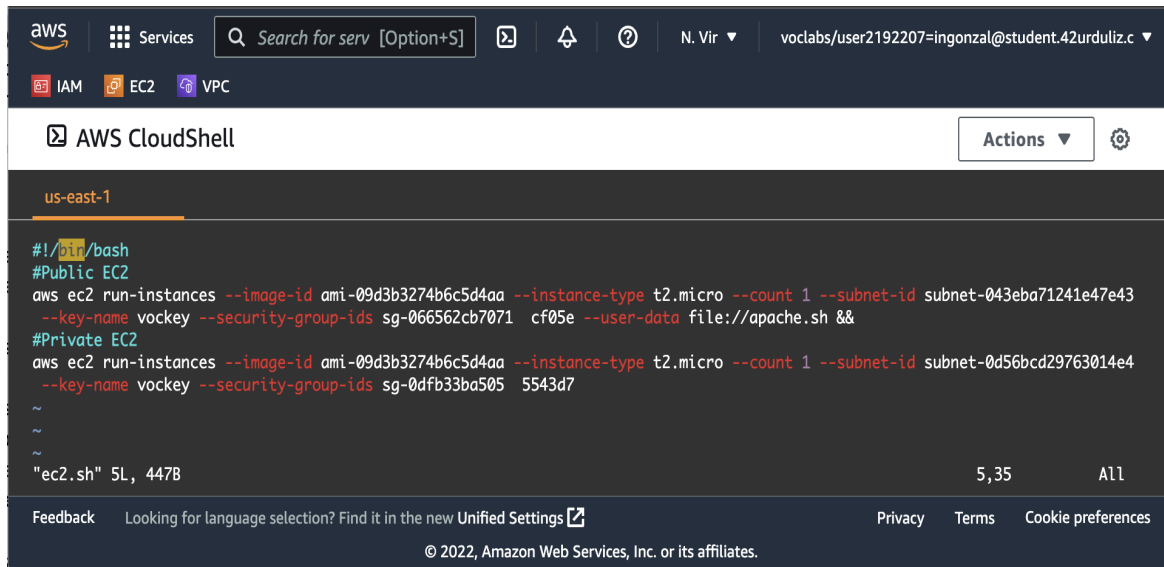
Details Tags

Details

Internet gateway ID	State	VPC ID	Owner
igw-0691fc3338760154b	Attached	vpc-0d8bd446e181e974a Caso Practico 2	753893822023

Tarea 2:

- EC2 script



```
#!/bin/bash
#Public EC2
aws ec2 run-instances --image-id ami-09d3b3274b6c5d4aa --instance-type t2.micro --count 1 --subnet-id subnet-043eba71241e47e43
--key-name vockey --security-group-ids sg-066562cb7071 cf05e --user-data file://apache.sh &&
#Private EC2
aws ec2 run-instances --image-id ami-09d3b3274b6c5d4aa --instance-type t2.micro --count 1 --subnet-id subnet-0d56bcd29763014e4
--key-name vockey --security-group-ids sg-0dfb33ba505 5543d7
~
~
~
"ec2.sh" 5L, 447B
```

- Transcript:

```
#!/bin/bash
```

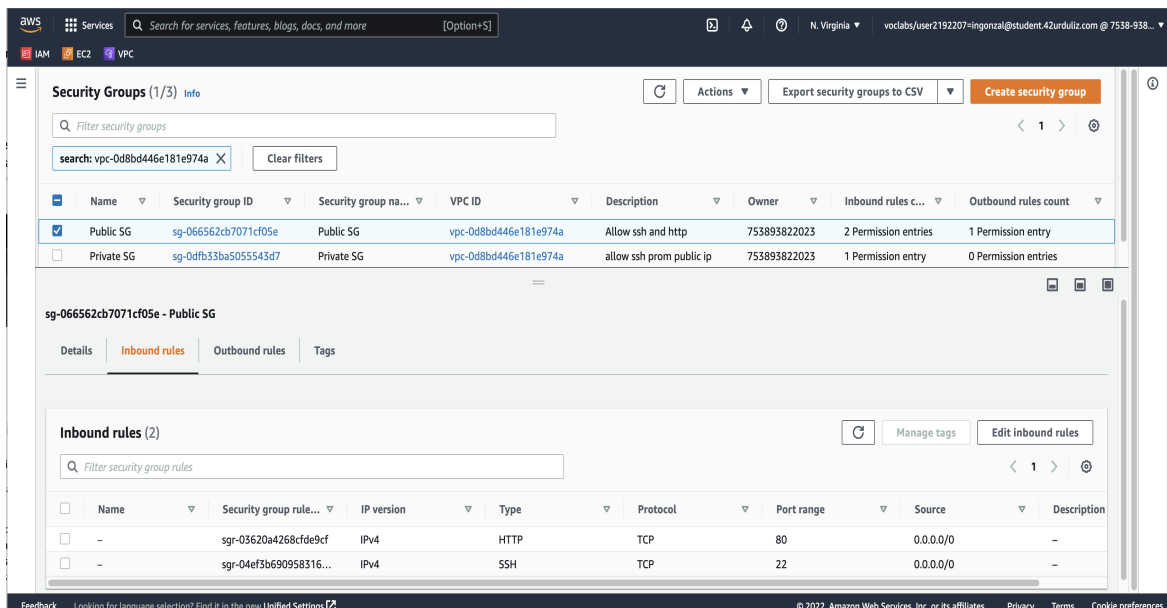
```
#Public EC2
```

```
aws ec2 run-instances --image-id ami-09d3b3274b6c5d4aa --instance-type t2.micro --count 1 --subnet-id subnet-043eba71241e47e43
--key-name vockey --security-group-ids sg-066562cb7071 cf05e --user-data file://apache.sh &&
```

```
#Private EC2
```

```
aws ec2 run-instances --image-id ami-09d3b3274b6c5d4aa --instance-type t2.micro --count 1 --subnet-id subnet-0d56bcd29763014e4
--key-name vockey --security-group-ids sg-0dfb33ba505 5543d7
```

Public Security Groups:



Security Groups (1/3)

Name	Security group ID	Security group na...	VPC ID	Description	Owner	Inbound rules c...	Outbound rules count
<input checked="" type="checkbox"/> Public SG	sg-066562cb7071cf05e	Public SG	vpc-0d8bd446e181e974a	Allow ssh and http	753893822023	2 Permission entries	1 Permission entry
<input type="checkbox"/> Private SG	sg-0dfb33ba5055543d7	Private SG	vpc-0d8bd446e181e974a	allow ssh prom public ip	753893822023	1 Permission entry	0 Permission entries

sg-066562cb7071cf05e - Public SG

Inbound rules (2)

Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
<input type="checkbox"/>	sg-03620a4268cfd9cf	IPv4	HTTP	TCP	80	0.0.0.0/0	-
<input type="checkbox"/>	sg-04ef3b690958316...	IPv4	SSH	TCP	22	0.0.0.0/0	-

- Private Security Groups:

The screenshot shows the AWS Management Console interface for Security Groups. The top navigation bar includes the AWS logo, Services menu, a search bar, and user information. The main content area is titled 'Security Groups (1/3) Info'. A search filter is applied: 'search: vpc-0d8bd446e181e974a'. A table lists two security groups: 'Public SG' and 'Private SG'. The 'Private SG' is selected, and its details are shown below. The 'Inbound rules' tab is active, displaying a single rule for SSH access from the source '10.0.0.0/24'.

Name	Security group ID	Security group name	VPC ID	Description	Owner	Inbound rules count	Outbound rules count
Public SG	sg-066562cb7071cf05e	Public SG	vpc-0d8bd446e181e974a	Allow ssh and http	753893822023	2 Permission entries	1 Permission entry
Private SG	sg-0dfb33ba505543d7	Private SG	vpc-0d8bd446e181e974a	allow ssh prom public ip	753893822023	1 Permission entry	0 Permission entries

Name	Security group rule name	IP version	Type	Protocol	Port range	Source	Description
-	sgr-0b32ebd3f8389547c	IPv4	SSH	TCP	22	10.0.0.0/24	-

- User data Script:

The screenshot shows the AWS CloudShell interface. The top navigation bar includes the AWS logo, Services menu, a search bar, and user information. The main content area is titled 'AWS CloudShell'. The terminal session shows the following commands and output:

```
#!/bin/bash
yum update -y
yum install httpd apache2 -y
systemctl start httpd
systemctl enable httpd
systemctl start apache2
systemctl enable apache2
```

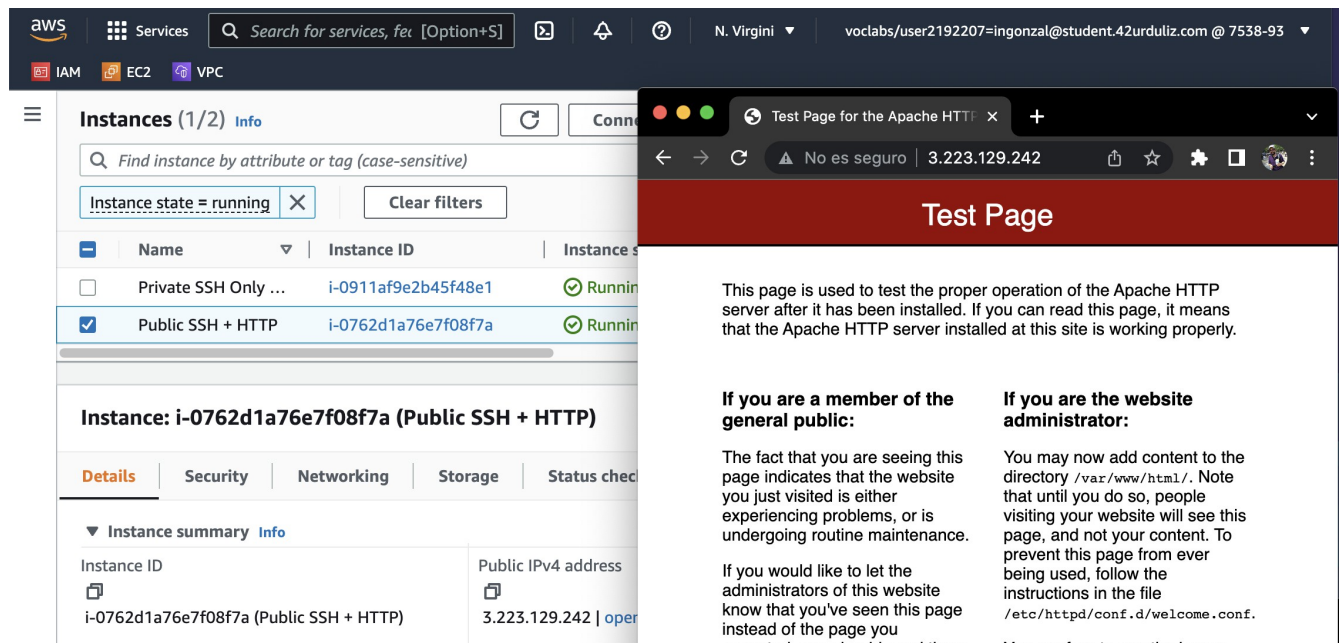
The output of the commands is displayed below the terminal session, showing the status of the services and the size of the files.

```
"apache.sh" 7L, 149B
```

- Transcript:

```
#!/bin/bash
yum update -y
yum install httpd apache2 -y
systemctl start httpd
systemctl enable httpd
systemctl start apache2
systemctl enable apache2
```

- Comprobación apache



The screenshot shows the AWS Management Console on the left and a web browser on the right. The browser displays the 'Test Page for the Apache HTTP' at IP address 3.223.129.242. The test page contains instructions for general public and website administrators.

Test Page

This page is used to test the proper operation of the Apache HTTP server after it has been installed. If you can read this page, it means that the Apache HTTP server installed at this site is working properly.

If you are a member of the general public:

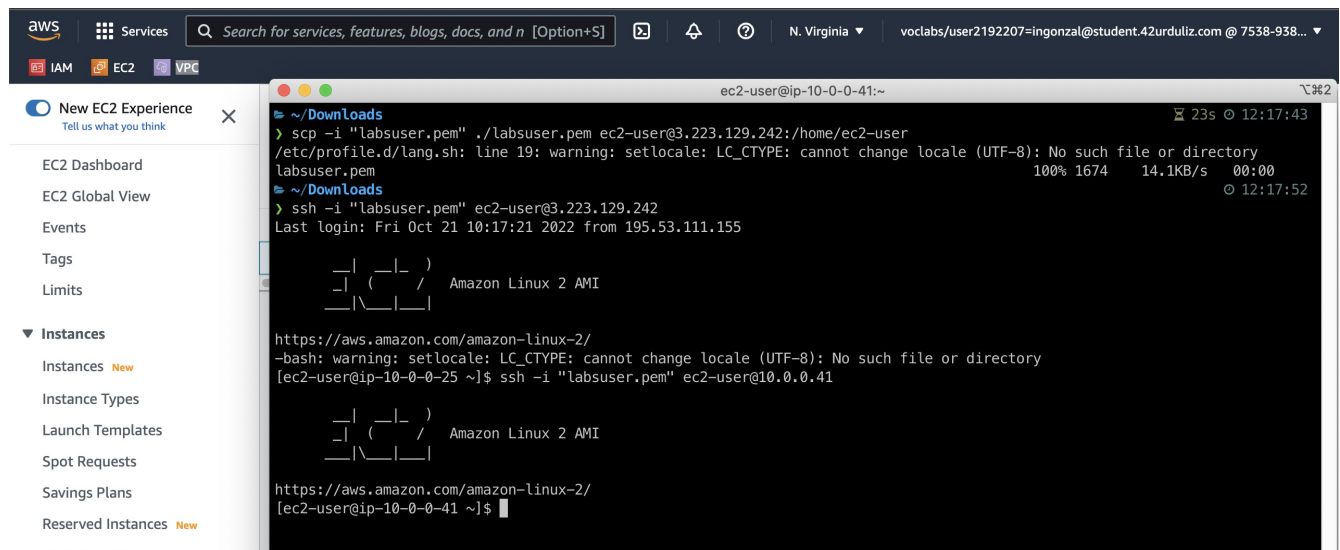
The fact that you are seeing this page indicates that the website you just visited is either experiencing problems, or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them

If you are the website administrator:

You may now add content to the directory `/var/www/html/`. Note that until you do so, people visiting your website will see this page, and not your content. To prevent this page from ever being used, follow the instructions in the file `/etc/httpd/conf.d/welcome.conf`.

- Comprobación SSH a EC2 publica y privada



The screenshot shows the AWS Management Console on the left and a terminal window on the right. The terminal window shows the process of connecting to an EC2 instance via SSH using a private key.

```
ec2-user@ip-10-0-0-41:~  
~/Downloads  
$ scp -i "labsuser.pem" ./labsuser.pem ec2-user@3.223.129.242:/home/ec2-user  
/etc/profile.d/lang.sh: line 19: warning: setlocale: LC_CTYPE: cannot change locale (UTF-8): No such file or directory  
100% 1674 14.1KB/s 00:00  
$ ssh -i "labsuser.pem" ec2-user@3.223.129.242  
Last login: Fri Oct 21 10:17:21 2022 from 195.53.111.155  
  
_ | _ | _ )  
_ | ( _ | / Amazon Linux 2 AMI  
_ | \ _ | _ |  
  
https://aws.amazon.com/amazon-linux-2/  
-bash: warning: setlocale: LC_CTYPE: cannot change locale (UTF-8): No such file or directory  
[ec2-user@ip-10-0-0-25 ~]$ ssh -i "labsuser.pem" ec2-user@10.0.0.41  
  
_ | _ | _ )  
_ | ( _ | / Amazon Linux 2 AMI  
_ | \ _ | _ |  
  
https://aws.amazon.com/amazon-linux-2/  
[ec2-user@ip-10-0-0-41 ~]$
```