

Caso Práctico 2: Redes y Computación en AWS

Tarea 1:

- VPC:

VPC ID: vpc-0d8bd446e181e974a / Caso Practico 2

Details

VPC ID	vpc-0d8bd446e181e974a	State	Available	DNS Intra-region	Disabled	DNS resolution	Enabled
Tenancy	Default	DHCP option set	dhcpc-0071777d57246ec9a	Main route table	rtb-057d9f7740e1a1e60 / Public RT Caso Practico 2	Main network ACL	act-07a20f2a8cc2fa188
Default VPC	No	IPv4 CIDR	10.0.0.0/26	IPv6 pool	-	IPv6 CIDR (Network border group)	-
Network mapping unit metrics	Disabled	Route 53 Resolver DNS Firewall rule groups	Failed to load rule groups	Owner ID	53893822023		

- Public Subnet:

Subnets (1/2) Info

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Availability zone	Availability zone	Availability zone	Network interface	Route table
Subnet_1_Public	subnet-043eba71241e47e43	Available	vpc-0d8bd446e181e974a Caso Practico 2	10.0.0.16/24	-	us-east-1a	us-east-1a1	us-east-1a2	us-east-1	rtb-057d9f7740e1a1e60 Public RT Caso Practico 2
Subnet_2_Private	subnet-0d56bc029763014ec4	Available	vpc-0d8bd446e181e974a Caso Practico 2	10.0.0.32/24	-	us-east-1b	us-east-1b1	us-east-1b2	us-east-1	rtb-0e49194e2a3535774 Private RT Caso Practico 2

subnet-043eba71241e47e43 / Subnet_1_Public

Route table: rtb-057d9f7740e1a1e60 / Public RT Caso Practico 2

Routes (2)

Destination	Target
10.0.0.0/26	local
0.0.0.0/0	igw-06911c3338760154b

- Auto Assign Ipv4:

VPC > Subnets > subnet-043eba71241e47e43 > Edit subnet settings

Edit subnet settings

Subnet

Subnet ID	Name
subnet-043eba71241e47e43	Subnet_1_Public

Auto-assign IP settings

Enable the auto-assign IP settings to automatically request a public IPv4 or IPv6 address for a new network interface in this subnet.

Enable auto-assign public IPv4 address

Enable auto-assign customer-owned IPv4 address

Option disabled because no customer owned pools found.

- Private Subnet:

The screenshot shows the AWS VPC Subnets page. It displays two subnets: Subnet_1_Public and Subnet_2_Private. Subnet_1_Public has an IPv4 CIDR of 10.0.0.16/24 and Subnet_2_Private has an IPv4 CIDR of 10.0.0.32/24. Both subnets are associated with the same VPC (vpc-0d8bd446e181e974a) and Route Table (rtb-0e49194e2a3525774). The Subnet_2_Private route table contains one route to the local target.

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Aval. IP range	Available IP range	Netw. ACL	Route table	
Subnet_1_Public	subnet-043eba71241e47e5	Available	vpc-0d8bd446e181e974a Caso Practico 2	10.0.0.16/24	-	10	us-east-1a	use1-a2	us-east-1	rtb-0579ff7740e1a1e160 Pub...
Subnet_2_Private	subnet-0d56bcd29763014e4	Available	vpc-0d8bd446e181e974a Caso Practico 2	10.0.0.32/24	-	10	us-east-1b	use1-a2	us-east-1	rtb-0e49194e2a3525774 Pri...

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

Destination	Target
10.0.0.0/26	local

- Internet Gateway:

The screenshot shows the AWS Internet Gateways page. It displays one internet gateway named igw_Caso_practico_2, which is attached to the VPC vpc-0d8bd446e181e974a. The internet gateway ID is igw-0691fc3338760154b.

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

Tarea 2:

- EC2 script

The screenshot shows the AWS CloudShell interface in the us-east-1 region. The terminal window contains a shell script for launching two EC2 instances. The first instance is labeled '#Public EC2' and the second is '#Private EC2'. Both instances use the same AMI (ami-09d3b3274b6c5d4aa), instance type (t2.micro), and subnet (subnet-043eba71241e47e43). The private instance includes a user-data file named apache.sh. The script ends with a comment (~) and the command "ec2.sh" followed by its line count (5L) and byte count (447B).

```
#!/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:

The screenshot shows the AWS Security Groups page. It lists two security groups: 'Public SG' and 'Private SG'. The 'Public SG' group has a description 'Allow ssh and http', owner '753893822023', and two inbound rules. The 'Private SG' group has a description 'allow ssh from public ip', owner '753893822023', and one inbound rule. The 'Inbound rules' section for the Public SG shows two rules: one for port 80 (HTTP) and one for port 22 (SSH).

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

Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
-	sgr-03620a4268cfde9cf	IPv4	HTTP	TCP	80	0.0.0.0/0	-
-	sgr-04ef3b690958316...	IPv4	SSH	TCP	22	0.0.0.0/0	-

- Private Security Groups:

The screenshot shows the AWS VPC Security Groups page. At the top, there are navigation links for IAM, EC2, and VPC. A search bar and a 'Create security group' button are also present. The main table lists two security groups:

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-0dfb33ba5055543d7	Private SG	vpc-0d8bd446e181e974a	allow ssh from public ip	753893822023	1 Permission entry	0 Permission entries

Below the table, a specific security group is selected: "sg-0dfb33ba5055543d7 - Private SG". The "Inbound rules" tab is active, showing one rule:

Name	Security group rule...	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 links for IAM, EC2, and VPC. The main area displays a user data script for the "us-east-1" region:

```
#!/bin/bash
yum update -y
yum install httpd apache2 -y
systemctl start httpd
systemctl enable httpd
systemctl start apache2
systemctl enable apache2
~
~
~
"apache.sh" 7L, 149B
```

At the bottom, there are feedback links, privacy terms, and cookie preferences.

- 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 with the EC2 service selected. On the left, the 'Instances' page lists two instances: 'i-0911af9e2b45f48e1' (Private SSH Only) and 'i-0762d1a76e7f08f7a' (Public SSH + HTTP). The second instance is selected. On the right, a browser window displays the 'Test Page for the Apache HTTP' page, which includes instructions for website members and administrators.

Instances (1/2) Info

Find instance by attribute or tag (case-sensitive)

Instance state = running

Name Instance ID Instance State

Private SSH Only ... i-0911af9e2b45f48e1 Running

Public SSH + HTTP i-0762d1a76e7f08f7a Running

Instance: i-0762d1a76e7f08f7a (Public SSH + HTTP)

Details Security Networking Storage Status check

Instance summary Info

Instance ID: i-0762d1a76e7f08f7a (Public SSH + HTTP)

Public IPv4 address: 3.223.129.242 | open

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

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 pública y privada

The screenshot shows the AWS Management Console with the EC2 service selected. The left sidebar shows various EC2 management options. The main area shows a terminal session titled 'ec2-user@ip-10-0-0-41:~'. The session history includes an SCP command to transfer a PEM file to the instance and an SSH command to log in, both of which fail due to locale issues.

New EC2 Experience Tell us what you think

EC2 Dashboard EC2 Global View Events Tags Limits

Instances Instances New Instance Types Launch Templates Spot Requests Savings Plans Reserved Instances New

~/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 ~]\$