

Contents

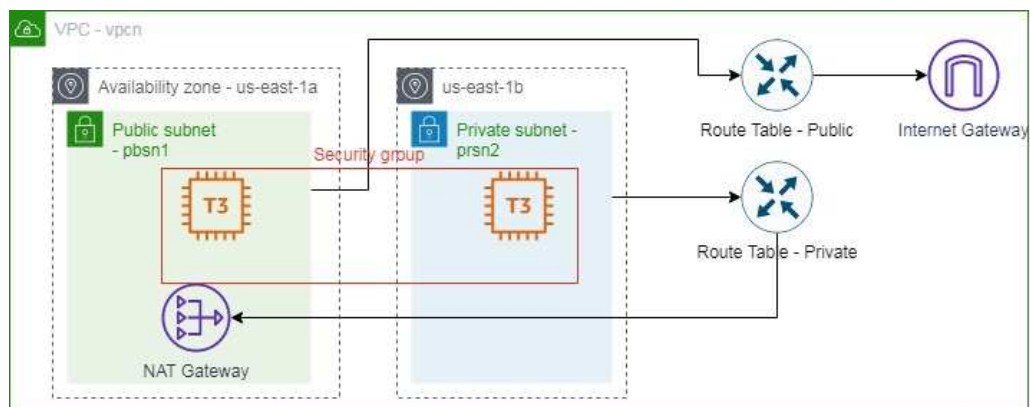
Purpose	2
General Diagram	2
Prerequisites	2
Lab 4A: VPC with IGW and NAT GW.....	3
Lab 4A using Web Management Console	3
Create VPC.....	3
Create Subnets	4
Create Routing Tables	7
Create Internet Gateway (IGW)	8
Create NAT Gateway (NAT GW).....	10
Assign IGW and NAT GW to Routing Tables.....	11
Assign Routing Tables to Subnets	14
Create Key Pair to connect to Instances	16
Create EC2 instances	17
Make the review	25
Add and Revoke Ports on Security Group	25
Lab 4A using Command Line (Windows).....	29
Create VPC, Public Subnet, IGW and Route Table	29
Create EC2 Keys, Sec Groups. Choose AMI and create EC2 Instances.	31
Create Private Subnet, EIP, NAT Gateway, Private Route Table and EC2 Instance	31
Get Information about Instances	33
Review Configurations using Putty, SFTP and Browser.....	34
Add Port to Security Group	35
Delete Port to Security Group	36
Clean resources	37
For Web Management Console	37
For Command Line (Windows).....	37
Evidences to send.....	38

Purpose

To create a common computing infrastructure in a public and private subnet, so you have to configure and connect routing tables and internet or NAT gateway.

General Diagram

One VPC with two subnets, with instances connected on each subnet. Configuration to outbound connections has to be made on Routing Tables using Internet Gateway and NAT Gateway.



Simple Web Server using
Python- SSH to Private
Instance

Check Outbound Connection
using NAT GW

Steps:

1. Create VPC and Subnets.
3. Create empty routing tables.
4. Create IGW and attached to VPC.
5. Create NAT GW.
6. Assign default route for Routing Tables (IGW and NAT GW).
7. Assign Routing Tables to Subnets.
8. Create Keypair.
9. Launch a instance on each subnet and create and assign Security Group.
10. Make the procedure using SSH and SFTP.

Prerequisites

Labs1c1 have to be done and the context for Administrative user have to activated on Command Line Session.

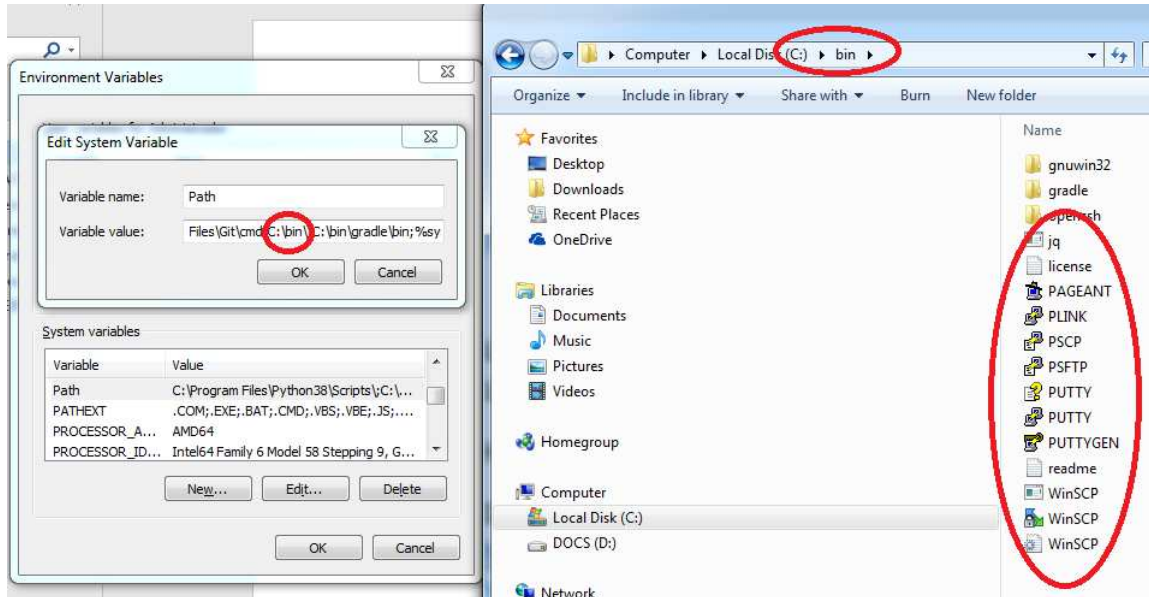
Have installed putty and winscp on Windows; and those files on a folder in the PATH environment.

Download complete and portable putty and winscp using

<https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html> and

<https://winscp.net/eng/downloads.php>

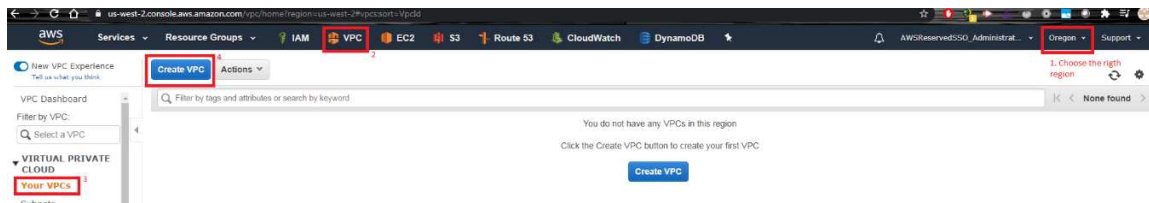
We use winscp as SFTP client (put Keypair on Public Instance) and for modifying PEM to PPK file on Windows. You can use Cyberduck as SFTP Client on MacOS.



Lab 4A: VPC with IGW and NAT GW

Lab 4A using Web Management Console

Create VPC



VPCs > Create VPC

Create VPC

A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances. You must specify an IPv4 address range for your VPC. Specify the IPv4 address range as a Classless Inter-Domain Routing (CIDR) block; for example, 10.0.0.0/16. You cannot specify an IPv4 CIDR block larger than /16. You can optionally associate an IPv6 CIDR block with the VPC.

Name tag ⓘ

IPv4 CIDR block* ⓘ

IPv6 CIDR block ☒ No IPv6 CIDR Block ⓘ
☐ Amazon provided IPv6 CIDR block

Tenancy ⓘ

* Required

Cancel

Create

VPCs > Create VPC

Create VPC

✓ The following VPC was created:

VPC ID [vpc-0a8c496e5ea60c325](#)

Close

Create Subnets

For Public Subnet,

The screenshot shows the AWS Management Console interface. At the top, there's a navigation bar with the AWS logo and 'Services' dropdown. Below it, a 'New VPC Experience' banner is visible. The main content area has a 'Create subnet' button highlighted with a red box. To the left, there's a sidebar with a search bar and a list of navigation links under the 'VIRTUAL PRIVATE CLOUD' section. The 'Subnets' link is highlighted with a red box. Other links in the sidebar include 'VPC Dashboard', 'Your VPCs', 'Route Tables', and 'Internet Gateways'.

us-west-1.console.aws.a...

aws Services Resource Groups AWSReservedSSO_Administrat... N. C

Subnets > Create subnet

Create subnet

Specify your subnet's IP address block in CIDR format; for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask, and can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag Public_Subnet

VPC* vpc-0a8c496e5ea60c325

Availability Zone us-west-1a

VPC CIDRs

CIDR	Status	Status Reason
10.0.0.0/16	associated	

IPv4 CIDR block* 10.0.0.0/24

* Required

Cancel Create

Modifying Public Subnet to assign Public IP to any instances on this subnet, you have to select the subnet and apply the feature.

aws Services Resource Groups AWSRes

New VPC Experience
Tell us what you think

VPC Dashboard

Filter by VPC:
Select a VPC

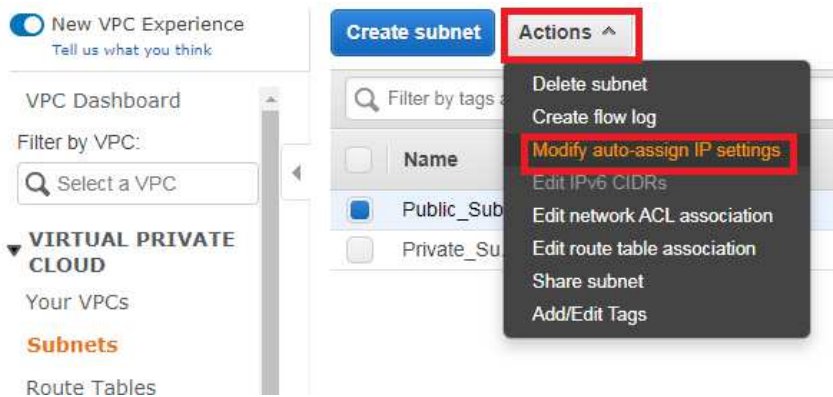
VIRTUAL PRIVATE CLOUD

- Your VPCs
- Subnets**
- Route Tables

Create subnet Actions

Filter by tags and attributes or search by keywo

	Name	Subnet ID
<input checked="" type="checkbox"/>	Public_Sub...	subnet-02fbecd6491760
<input type="checkbox"/>	Private_Su...	subnet-04bf93eaad018f



Subnets > Modify auto-assign IP settings

Modify auto-assign IP settings

Enable the auto-assign IP address setting to automatically request a public IPv4 or IPv6 address for an instance launched in this subnet. You can override the auto-assign IP settings for an instance at launch time.

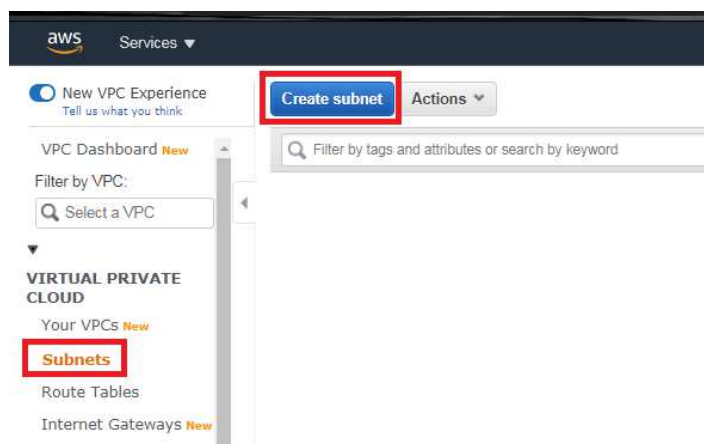
Subnet ID subnet-02fbecd6491760823

Auto-assign IPv4 ☒ Enable auto-assign public IPv4 address ?

* Required

Cancel Save

For Private Subnet,



[Subnets](#) > Create subnet

Create subnet

Specify your subnet's IP address block in CIDR format; for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask, and can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag

VPC*

Availability Zone

VPC CIDRs	CIDR	Status	Status Reason
	10.0.0.0/16	associated	

IPv4 CIDR block*

* Required

[Cancel](#) [Create](#)

[Subnets](#) > Create subnet

Create subnet

✓ The following Subnet was created:

Subnet ID [subnet-04bf93eaa018f629](#)

[Close](#)

Create Routing Tables

For this step, we create empty routing tables without attached or assign anything. First, we create the public routing table,

aws Services Resource Groups IAM **VPC** EC2

[Create route table](#) Actions

Filter by tags and attributes or search by keyword

You do not have any Route Table

Click the Create Route Table button to create a new route table

[Create route table](#)

VPC Dashboard

Filter by VPC:

Select a VPC

VIRTUAL PRIVATE CLOUD

Your VPCs

Subnets

Route Tables

Internet Gateways New

Private Only Internet

us-west-1.console.aws.amazon.com/vpc/home?region=us-...
aws Services Resource Groups AWSReservedSSO_Administrat... N. California Support

Route Tables > Create route table

Create route table

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

Name tag

VPC*

* Required Cancel Create

Route Tables > Create route table

Create route table

✓ The following Route Table was created:

Route Table ID `rtb-037bb7ab1144c6ef4`

Close

Then, we create the private routing table.

Route Tables > Create route table

Create route table

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

Name tag

VPC*

* Required Cancel Create

Create route table

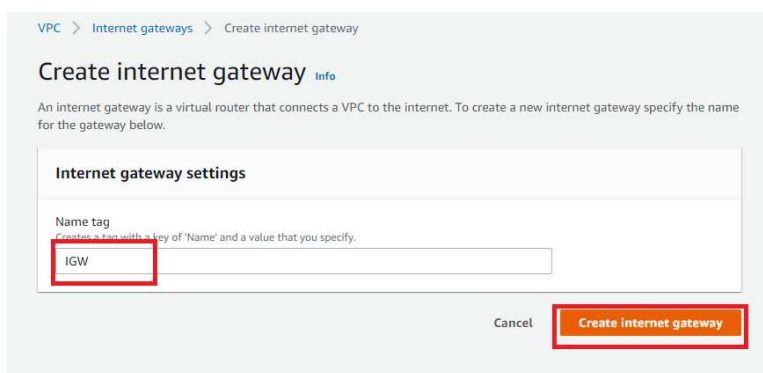
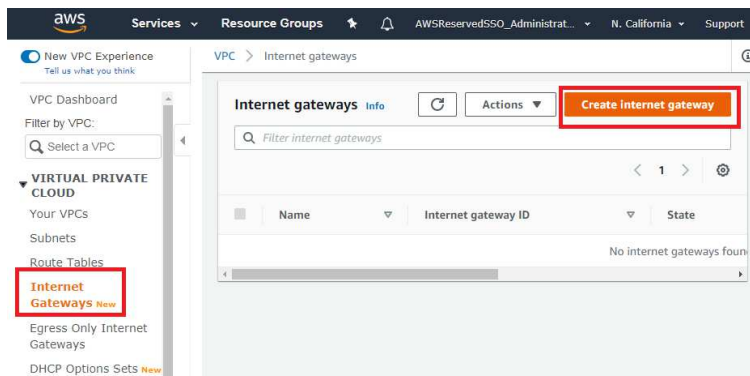
✓ The following Route Table was created:

Route Table ID `rtb-0e4ddcfe291ee0445`

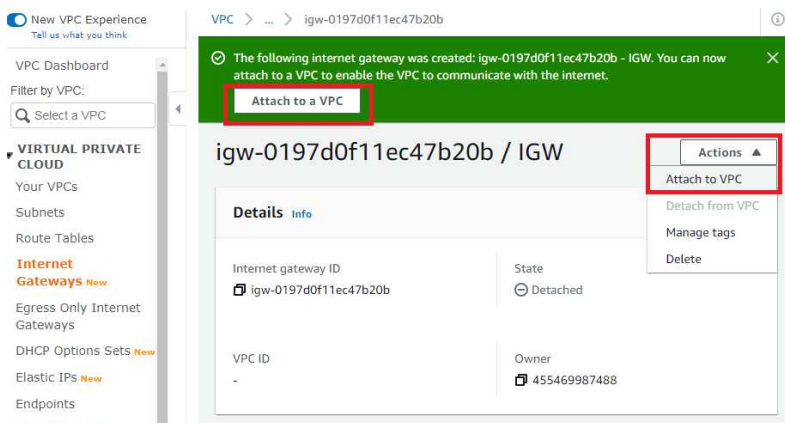
Close

Create Internet Gateway (IGW)

Create a IGW and then, attach to the VPC.



After it confirmation message, we attach to the VPC.



Select the VPC to attach the IGW,

VPC > Internet gateways > Attach to VPC (igw-0197d0f11ec47b20b)

Attach to VPC (igw-0197d0f11ec47b20b) [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

Confirmation message

New VPC Experience

VPC > Internet gateways

Internet gateway igw-0197d0f11ec47b20b successfully attached to vpc-0a8c496e5ea60c325

Internet gateways (1/1) [Info](#)

Actions **Create internet gateway**

Filter internet gateways

<input checked="" type="checkbox"/>	Name	Internet gateway ID	State
<input checked="" type="checkbox"/>	IGW	igw-0197d0f11ec47b20b	Attached

Create NAT Gateway (NAT GW)

us-west-1 console.aws.amazon.com/vpc/home?region=us-west-1#/nattogateways

Services Resource Groups IAM **VPC** EC2

New VPC Experience

Create NAT Gateway Actions

Filter by tags and attributes or search by keyword

You do not have any NAT Gateways.

Click the Create NAT Gateway button.

Create NAT Gateway

VPC Dashboard

Filter by VPC:

Select a VPC

VIRTUAL PRIVATE CLOUD

Your VPCs

Subnets

Route Tables

Internet Gateways **New**

Egress Only Internet Gateways

DHCP Options Sets **New**

Elastic IPs **New**

Endpoints

Endpoint Services **2**

NAT Gateways

Peering Connections

In this info window, you have to create an Elastic IP for assign it to the NAT Gateway, therefore you click on “Allocate Elastic IP Address” and AWS Console create and assign an EIP for this NAT GW automatically.

us-west-1.console.aws.amazon.com/v2/home?region=us-west-1

aws Services Resource Groups AWSReservedSSO_Administrat... N. California Support

NAT Gateways > Create NAT Gateway

Create NAT Gateway

Create a NAT gateway and assign it an Elastic IP address. [Learn more.](#)

1. Choose public subnet

Subnet: subnet-02f6cd6491760823

2. Create new EIP

Elastic IP Allocation ID: eipalloc-0174486bb88096475

Allocate Elastic IP address

Elastic IP address (52.9.83.5) allocated.

Key	Value
This resource currently has no tags	

Add Tag 50 remaining (Up to 50 tags maximum)

* Required Cancel **Create a NAT Gateway**

Confirmation message,

NAT Gateways > Create NAT Gateway

Create NAT Gateway

✓ Your NAT gateway has been created.

Note: In order to use your NAT gateway, ensure that you [edit your route tables](#) to include a route with the following NAT gateway. [Find out more.](#)

NAT Gateway ID nat-095234709b6bea0b1

[Edit route tables](#) [Close](#)

Assign IGW and NAT GW to Routing Tables

For Public Table, you modify routing tables to assign default route (0.0.0.0/0) to IGW.

aws Services Resource Groups AWSReservedSSO_Ad

New VPC Experience
Tell us what you think

VPC Dashboard
Filter by VPC:
Select a VPC

VIRTUAL PRIVATE CLOUD

Your VPCs

Subnets

Route Tables

Internet Gateways *New*

Egress Only Internet Gateways

DHCP Options Sets *New*

Elastic IPs *New*

Endpoints

Endpoint Services

NAT Gateways

Peering Connections

SECURITY

Network ACLs

Create route table Actions

Filter by tags and attributes or search by keyword

Name	Route Table ID	Expli
Public_RT	rtb-037bb7ab1144c6ef4	-
	rtb-0c502810afd6e620c	-
Private_RT	rtb-0e4ddcfe291ee0445	-

Route Table: rtb-037bb7ab1144c6ef4

Summary Routes Subnet Associations

Edit routes

View All routes

Destination

10.0.0.0/16

Route Tables > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
0.0.0.0/0		No	No

Add route

* Required

Egress Only Internet Gateway
Instance
Internet Gateway
NAT Gateway
Network Interface

Cancel Save routes

Route Tables > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
0.0.0.0/0	igw-0197d0f11ec47b20b	No	No

Add route

* Required

Cancel Save routes

Confirmation message

Route Tables > Edit routes

Edit routes

✓ Routes successfully edited

Close

For Private Routing Table, you modify routing tables to assign default route (0.0.0.0/0) to NAT GW.

The screenshot shows the AWS Management Console interface for editing a route table. On the left, the 'Route Tables' link is highlighted in the navigation menu. The main panel shows a list of route tables, with 'Private_RT' (ID: rtb-0e4ddcfe291ee0445) selected. Below the list, the 'Routes' tab is active for the selected route table. It displays a table with one route: destination 10.0.0.0/16, target 'local', and status 'active'. The 'Edit routes' button is highlighted with a red box.

Route Tables > Edit routes

Edit routes

This screenshot shows the 'Edit routes' page with a dropdown menu open for the 'Target' field. The dropdown menu lists several options: 'Egress Only Internet Gateway', 'Instance', 'Internet Gateway', 'NAT Gateway' (which is highlighted with a red box), and 'Network Interface'. The 'Destination' field is set to '0.0.0.0/0' (also highlighted with a red box). The 'Add route' button is visible below the table.

Route Tables > Edit routes

Edit routes

This screenshot shows the 'Edit routes' page after selecting 'NAT Gateway' from the dropdown menu. The dropdown menu now shows the specific NAT Gateway ID: 'nat-095234709b6bea0b1' (highlighted with a red box). The 'Destination' field remains '0.0.0.0/0'. The 'Add route' button is visible below the table.

Confirmation message,

Route Tables > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
0.0.0.0/0	nat-095234709b6bea0b1		No

* Required Cancel

Edit routes

✓ Routes successfully edited

Close

Assign Routing Tables to Subnets

For Public Routing Table, you select the public subnet.

☒ New VPC Experience
Tell us what you think

VPC Dashboard

Filter by VPC:

VIRTUAL PRIVATE CLOUD

- Your VPCs
- Subnets
- Route Tables**
- Internet Gateways New
- Egress Only Internet Gateways
- DHCP Options Sets New
- Elastic IPs New
- Endpoints

<input type="checkbox"/>	Name	Route Table ID	Explicit sub
<input checked="" type="checkbox"/>	Public_RT	rtb-037bb7ab1144c6ef4	-
<input type="checkbox"/>		rtb-0c502810afd6e620c	-
<input type="checkbox"/>	Private_RT	rtb-0e4ddcfe291ee0445	-

Route Table: rtb-037bb7ab1144c6ef4

Route Tables > Edit subnet associations

Edit subnet associations

Route table **rtb-037bb7ab1144c6ef4 (Public_RT)**

Associated subnets **subnet-02fbecd6491760823**

Filter by attributes or search by keyword			1 to 2 of 2	
<input type="checkbox"/>	Subnet ID	IPv4 CIDR	IPv6 CIDR	
<input checked="" type="checkbox"/>	subnet-02fbecd6491760823 Public_Subnet	10.0.0.0/24	-	1
<input type="checkbox"/>	subnet-04bf93eaaad018f629 Private_Subnet	10.0.1.0/24	-	

* Required

Cancel **Save**

For Private Routing Table, you select private subnet.

☒ New VPC Experience
Tell us what you think

VPC Dashboard

Filter by VPC:

VIRTUAL PRIVATE CLOUD

Your VPCs

Subnets

Route Tables

Internet Gateways **New**

Egress Only Internet Gateways

DHCP Options Sets **New**

Elastic IPs **New**

Endpoints

Endpoint Services

NAT Gateways

Create route table

Actions

Filter by tags and attributes or search by keyword

<input type="checkbox"/>	Name	Route Table ID	Explicit subnet a
<input type="checkbox"/>	Public_RT	rtb-037bb7ab1144c6ef4	subnet-02fbecd6491760823
<input type="checkbox"/>		rtb-0c502810afd6e620c	-
<input checked="" type="checkbox"/>	Private_RT	rtb-0e4ddcfe291ee0445	-

Route Table: rtb-0e4ddcfe291ee0445

Summary

Routes

Subnet Associations

Edge

Edit subnet associations

Subnet ID	IPv4 CIDR	IPv6 C
-----------	-----------	--------

Edit subnet associations

Route table **rtb-0e4ddcfe291ee0445 (Private_RT)**

Associated subnets **subnet-04bf93eaa018f629**

Filter by attributes or search by keyword

Subnet ID	IPv4 CIDR	IPv6 CIDR
subnet-02fbec6491760823 Public_Subnet	10.0.0.0/24	-
subnet-04bf93eaa018f629 Private_Subnet	10.0.1.0/24	-

* Required

Cancel **Save**

Create Key Pair to connect to Instances

A Keypair, it is a file to authenticate ec2-user (default user for Amazon Linux AMI). For this step, we create that file and use to connect it.

aws Services Resource Groups IAM VPC **EC2** AWSReservedSSO_Administrat... Oregon Support

New EC2 Experience Tell us what you think

Capacity Reservations

IMAGES

AMIs

Bundle Tasks

ELASTIC BLOCK STORE

Volumes

Snapshots

Lifecycle Manager

NETWORK & SECURITY

Security Groups **New**

Elastic IPs **New**

Placement Groups **New**

Key Pairs **New**

Network Interfaces

Key pairs

Filter key pairs

Actions **Create key pair**

Name	Fingerprint	ID
No key pairs to display		

EC2 > Key pairs > Create key pair

Create key pair

Key pair
A key pair, consisting of a private key and a public key, is a set of security credentials that you use to prove your identity when connecting to an instance.

Name

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

File format

☐ pem
For use with OpenSSH

☒ ppk
For use with PuTTY

Cancel

Store on the folder with the code of Command Line.

If you have Windows, we don't need to use winscp to make the transformation to ppk. You download ppk file to use putty.

If you have MacOS, you don't need to download the ppk format, you have to use pem file to use SSH in command line.

Create EC2 instances

An instance is a Virtual Machine. Those steps are straight forward because we have to make it on detail on next session.

aws Services Resource Groups IAM VPC **EC2** S3

New EC2 Experience
Tell us what you think

EC2 Dashboard New

Events New
Tags
Reports
Limits

▼ INSTANCES
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts New
Capacity Reservations

▼ IMAGES
AMIs
Bundle Tasks

▼ ELASTIC BLOCK STORE
Volumes
Snapshots
Lifecycle Manager

Welcome to the new EC2 console!
We're redesigning the EC2 console to make it easier to use and improve performance. To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

EC2

Resources

You are using the following Amazon EC2 resources in the US West (N. California) Region:

Running instances	0	Elastic IPs
Snapshots	0	Volumes
Key pairs	1	Security groups

1

2

3

4

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Launch instance

Launch instance

Launch instance from template

aws Services Resource Groups AWSReservedSSO_Administrat... N. California

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace, or you can select one of your own AMIs.

Search for an AMI by entering a search term e.g. "Windows"

Search by Systems Manager parameter

Quick Start

My AMIs

AWS Marketplace

Community AMIs

☒ Free tier only

1

2

Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-04e59c05167ea7bd5

Free tier eligible

Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras.

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

64-bit (x86)

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

Filter by: All instance types Current generation Show/Hide Columns

Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
<input type="checkbox"/>	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate
<input checked="" type="checkbox"/>	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	t2.small	1	2	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	t2.large	2	8	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	t2.xlarge	4	16	EBS only	-	Moderate
<input type="checkbox"/>	General purpose	t2.2xlarge	8	32	EBS only	-	Moderate
<input type="checkbox"/>	General purpose	t3a.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit
<input type="checkbox"/>	General purpose	t3a.micro	2	1	EBS only	Yes	Up to 5 Gigabit
<input type="checkbox"/>	General purpose	t3a.small	2	2	EBS only	Yes	Up to 5 Gigabit

Cancel Previous Review and Launch Next: Configure Instance Details

For this case, you create the public instance:

aws

Services

Resource Groups

AWSReservedSSO_Administrat...

N. California

Support

1. Choose AMI

2. Choose Instance Type

3. Configure Instance

4. Add Storage

5. Add Tags

6. Configure Security Group

7. Review

Step 3: Configure Instance Details

No default VPC found. Select another VPC, or [create a new default VPC](#).

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances

1

Launch into Auto Scaling Group

Purchasing option

☐ Request Spot instances

Network

vpc-0a8c496e5ea60c325 | Nombre_VPC

Create new VPC

No default VPC found. [Create a new default VPC](#).

Subnet

subnet-02fbecd6491760823 | Public_Subnet | us-we

Create new subnet

250 IP Addresses available

Auto-assign Public IP

Use subnet setting (Enable)

Placement group

☐ Add instance to placement group

Capacity Reservation

Open

Create new Capacity Reservation

IAM role

None

Create new IAM role

Shutdown behavior

Stop

Stop - Hibernate behavior

☐ Enable hibernation as an additional stop behavior

Enable termination protection

☐ Protect against accidental termination

Monitoring

☐ Enable CloudWatch detailed monitoring

Additional charges apply.

Cancel

Previous

Review and Launch

Next: Add Storage

You have to choose next steps until you reach, Configuring Security Group

us-west-1 console.aws.amazon.com/EC2/v2/home#res:secgroup:launch-wizard-1

Services Resource Groups AWSReservedSSO_Administrat... N. California Support

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

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: A Name

Description:

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Custom 0.0.0.0/0	SSH Access

[Add Rule](#)

Warning

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

[Cancel](#)
[Previous](#)
[Review and Launch](#)

Review page, before of launching EC2 Instance.

us-west-1 console.aws.amazon.com/EC2/v2/home#res:secgroup:launch-wizard-1

Services Resource Groups AWSReservedSSO_Administrat... N. California Support

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 7: Review Instance Launch

You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. [Edit security groups](#)

AMI Details [Edit AMI](#)

Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-04e59c08167ea7bd5

Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras.

Root Device Type: ebs Virtualization type: hvm

Instance Type [Edit instance type](#)

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	Variable	1	1	EBS only	-	Low to Moderate

Security Groups [Edit security groups](#)

Security group name: SSH Access

Description: launch-wizard-1 created 2020-06-20T17:35:12.195-05:00

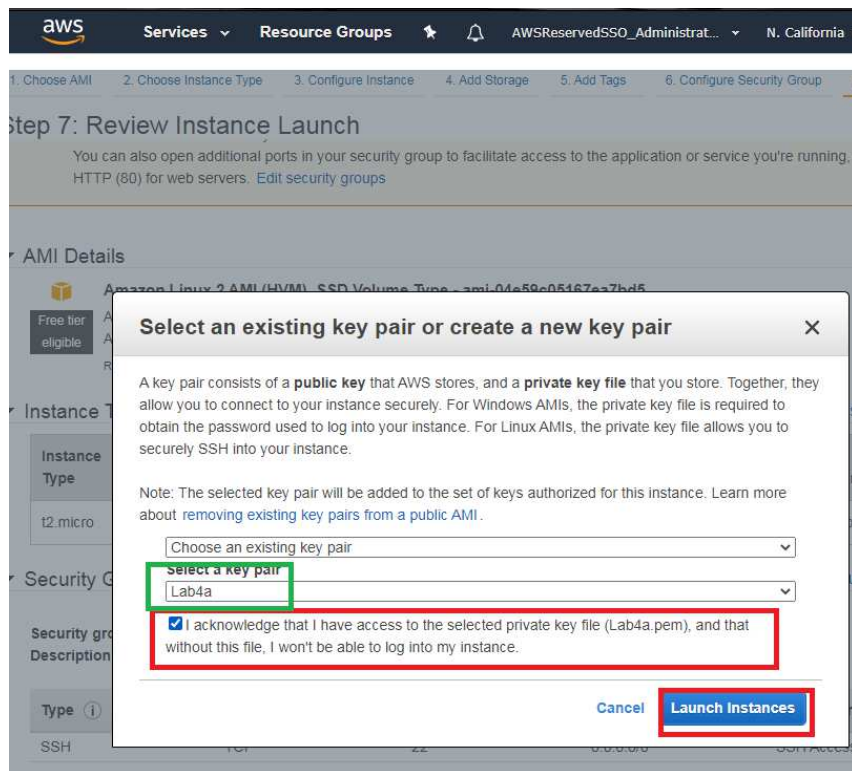
Type	Protocol	Port Range	Source	Description
SSH	TCP	22	0.0.0.0/0	SSH Access

Instance Details [Edit instance details](#)

Storage [Edit storage](#)

Tags [Edit tags](#)

[Cancel](#)
[Previous](#)
[Launch](#)



Launch Status

✓ Your instances are now launching

The following instance launches have been initiated: I-0284d26758ff5b752 [View launch log](#)

ℹ Get notified of estimated charges

Create billing alerts to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier).

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](#)

While your instances are launching you can also

- [Create status check alarms](#) to be notified when these instances fail status checks. (Additional charges may apply)
- [Create and attach additional EBS volumes](#) (Additional charges may apply)
- [Manage security groups](#)

[View Instances](#)

For Private Instances, the procedure is similar however, it changes on the subnet to create the instances and the security group is chosen from the previous step.

aws

Services

Resource Groups

AWSReservedSSO_Administrat...

N. California

Support

1. Choose AMI

2. Choose Instance Type

3. Configure Instance

4. Add Storage

5. Add Tags

6. Configure Security Group

7. Review

Step 3: Configure Instance Details

No default VPC found. Select another VPC, or create a new default VPC.

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances

1

Launch into Auto Scaling Group

Purchasing option

☐ Request Spot instances

Network

vpc-0a8c496e5ea60c325 | Nombre_VPC

Create new VPC

No default VPC found. Create a new default VPC.

Subnet

subnet-04bf93ead018f629 | Private_Subnet | us-we

Create new subnet

254 IP addresses available

Auto-assign Public IP

Use subnet setting (Disable)

Placement group

☐ Add instance to placement group

Capacity Reservation

Open

Create new Capacity Reservation

IAM role

None

Create new IAM role

Shutdown behavior

Stop

Stop - Hibernate behavior

☐ Enable hibernation as an additional stop behavior

Enable termination protection

☐ Protect against accidental termination

Monitoring

☐ Enable CloudWatch detailed monitoring

Additional charges apply.

Tags

Standard. Discontinued features instance

Cancel

Previous

Review and Launch

Next: Add Storage

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 ID	Name	Description	Actions
<input type="checkbox"/> sg-0b56ea23b6f579142	default	default VPC security group	Copy to new
<input checked="" type="checkbox"/> sg-0aa48dadd0ceaec1b	SSH Access	launch-wizard-1 created 2020-06-20T17:35:12.195-05:00	Copy to new

Inbound rules for sg-0aa48dadd0ceaec1b (Selected security groups: sg-0aa48dadd0ceaec1b)

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	0.0.0.0/0	SSH Access

[Cancel](#)

[Previous](#)

[Review and Launch](#)



Services

Resource Groups



AWSReservedSSO_Administrat...

N. California

Support

Launch Status



Your instances are now launching

The following instance launches have been initiated: [i-01c1aab2df07ce1ef](#) [View launch log](#)



Get notified of estimated charges

Create billing alerts to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier).

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](#)

While your instances are launching you can also

- [Create status check alarms](#) to be notified when these instances fail status checks. (Additional charges may apply)
- [Create and attach additional EBS volumes](#) (Additional charges may apply)
- [Manage security groups](#)

[View Instances](#)

Make the review

Use the same tools of Command Line (Windows): putty.

Check the “Review Configurations using Putty, SFTP and Browser” section, except the Add and Revoke Ports on Security Groups.

Add and Revoke Ports on Security Group

To add ports,

The screenshot displays the AWS Management Console interface for the 'Security Groups' page. The left-hand navigation pane shows the 'EC2' section expanded, with 'Security Groups' highlighted. The main content area shows a list of security groups. The first group, 'SSH Access' (ID: sg-0aa48dadd0ceaec1b), is selected. Below the list, the 'Inbound rules' tab is active, showing details for the selected rule. The details include the security group name 'SSH Access', the security group ID 'sg-0aa48dadd0ceaec1b', a description 'launch-wizard-1 created 2020-06-20T17:35:12.195-05:00', and the VPC ID 'vpc-0a8c496e5ea60c325'.

Name	Security group ID	Security group name
SSH Access	sg-0aa48dadd0ceaec1b	SSH Access
default	sg-0b56ea23b6f579142	default

Details	Inbound rules	Outbound rules	Tags
Details			
Security group name	SSH Access	Security group ID	sg-0aa48dadd0ceaec1b
Description	launch-wizard-1 created 2020-06-20T17:35:12.195-05:00	VPC ID	vpc-0a8c496e5ea60c325

aws

Services

Resource Groups

AWSReservedSSO_Administrat...

N. California

Support

New EC2 Experience

Tell us what you think

Instance types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts New

Capacity Reservations

IMAGES

AMIs

Bundle Tasks

ELASTIC BLOCK STORE

Volumes

Snapshots

Lifecycle Manager

NETWORK & SECURITY

Security Groups New

Elastic IPs New

Placement Groups New

Key Pairs New

Network Interfaces

LOAD BALANCING

Load Balancers

Target Groups

EC2 > Security Groups

Security Groups (1/2) Info

Actions

Create security group

Q

Filter security groups

<

1

>

Name

Security group ID

Security group name

☒

-

sg-0aa48dadd0ceaec1b

SSH Access

☐

-

sg-0b56ea23b6f579142

default

sg-0aa48dadd0ceaec1b - SSH Access

Details

Inbound rules

Outbound rules

Tags

Inbound rules

Edit inbound rules

Type

Protocol

Port range

Source

Description - optional

SSH

TCP

22

0.0.0.0/0

SSH Access

EC2 > Security Groups > sg-0aa48dadd0ceaec1b - SSH Access > Edit inbound rules

Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info

Type Info

Protocol Info

Port range Info

Source Info

Description - optional Info

SSH

TCP

22

Custom

Q

0.0.0.0/0

X

SSH Access

Delete

Add rule

NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.

Cancel

Preview changes

Save rules

Edit inbound rules [Info](#)

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info	
SSH	TCP	22	Custom <input type="text" value="Q"/> <input type="text" value="0.0.0.0/0"/>	SSH Access	Delete
HTTP	TCP	80	Custom <input type="text" value="Q"/>		Delete

Q

HTTP

POP3

IMAP

LDAP

HTTPS

SMB

SMTTPS

IMAPS

POP3S

MSSQL

NFS

MySQL/Aurora

RDP

Redshift

on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be f period of time until the new rule can be created.

Cancel Preview changes **Save rules**

Edit inbound rules [Info](#)

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info	
SSH	TCP	22	Custom <input type="text" value="Q"/> <input type="text" value="0.0.0.0/0"/>	SSH Access	Delete
HTTP	TCP	80	Custom <input type="text" value="Q"/>		Delete

Add rule

Custom

Custom

Anywhere

My IP

Anywhere

NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.

Cancel Preview changes **Save rules**

aws Services Resource Groups IAM VPC EC2 S3 Ro AWSReservedSSO_Administrat... N. California Support

New EC2 Experience Tell us what you think

Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts **New**
Capacity Reservations

▼ IMAGES
AMIs
Bundle Tasks

▼ ELASTIC BLOCK STORE
Volumes
Snapshots
Lifecycle Manager

▼ NETWORK & SECURITY
Security Groups **New**
Elastic IPs **New**
Placement Groups **New**
Key Pairs **New**
Network Interfaces

▼ LOAD BALANCING
Load Balancers
Target Groups

▼ AUTO SCALING
Launch Configurations
Auto Scaling Groups

Inbound security group rules successfully modified on security group (sg-0aa48dadd0ceaec1b | SSH Access)

Details

EC2 > Security Groups

Security Groups (1/2) Info

Filter security groups

	Name	Security group ID	Security group name	VPC ID	Description
<input checked="" type="checkbox"/>	-	sg-0aa48dadd0ceaec1b	SSH Access	vpc-0a8c496e5ea60c325	launch-wizard-1 create
<input type="checkbox"/>	-	sg-00508a250815797142	default	vpc-0a8c496e5ea60c325	default VPC security gr

sg-0aa48dadd0ceaec1b - SSH Access

Details Inbound rules Outbound rules Tags

Inbound rules Edit inbound rules

Type	Protocol	Port range	Source	Description - optional
HTTP	TCP	80	0.0.0.0/0	-
HTTP	TCP	80	:::/0	-
SSH	TCP	22	0.0.0.0/0	SSH Access

To revoke ports on Sec Groups, you have to edit the inbound rules:

EC2 > Security Groups > sg-0aa48dadd0ceaec1b - SSH Access > Edit inbound rules

Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info

Type	Protocol	Port range	Source	Description - optional
HTTP	TCP	80	Custom 0.0.0.0/0	
HTTP	TCP	80	Custom :::/0	
SSH	TCP	22	Custom 0.0.0.0/0	SSH Access

Add rule

NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.

Cancel Preview changes **Save rules**

Lab 4A using Command Line (Windows)

```
rem Setear las variables
set vpcn_Mask="10.0.0.0/16"
set pbsn1_Mask="10.0.0.0/24"
set prsn2_Mask="10.0.1.0/24"
set first_az="us-east-1a"
set second_az="us-east-1b"
```

Create VPC, Public Subnet, IGW and Route Table

```
rem Crear la VPC
aws ec2 create-vpc --cidr-block %vpcn_Mask%|jq ".Vpc.VpcId" >tmpFile
set /p vpcn_Id= < tmpFile

rem Crear subred Publica
aws ec2 create-subnet --vpc-id %vpcn_Id% --cidr-block %pbsn1_Mask% --
availability-zone %first_az%|jq ".Subnet.SubnetId" >tmpFile
set /p pbsn1_Id= < tmpFile

rem Crear el Internet Gateway IGW y asignarlo a la VPC
aws ec2 create-internet-
gateway|jq ".InternetGateway.InternetGatewayId" >tmpFile
set /p IGW_Id= < tmpFile
aws ec2 attach-internet-gateway --vpc-id %vpcn_Id% --internet-gateway-
id %IGW_Id%

rem Crear tabla de ruteo publica y asignarle IGW como ruta por defecto
aws ec2 create-route-table --vpc-
id %vpcn_Id%|jq ".RouteTable.RouteTableId" >tmpFile
set /p Public_RT_Id= < tmpFile
aws ec2 create-route --route-table-id %Public_RT_Id% --destination-cidr-
block 0.0.0.0/0 --gateway-id %IGW_Id%
rem Revisar Rutas de la Tabla de Ruteo
aws ec2 describe-route-tables --route-table-id %Public_RT_Id%
```

```

C:\Code\bsg-saa-c02\AWS_SAA\Code\s4c1\CLI>set vpcn_Mask="10.0.0.0/16"
C:\Code\bsg-saa-c02\AWS_SAA\Code\s4c1\CLI>set pbsn1_Mask="10.0.0.0/24"
C:\Code\bsg-saa-c02\AWS_SAA\Code\s4c1\CLI>set prsn2_Mask="10.0.1.0/24"
C:\Code\bsg-saa-c02\AWS_SAA\Code\s4c1\CLI>aws ec2 create-vpc --cidr-block %vpcn_Mask%|jq ".Vpc.VpcId" >tmpFile
C:\Code\bsg-saa-c02\AWS_SAA\Code\s4c1\CLI>set /p vpcn_Id= < tmpFile
C:\Code\bsg-saa-c02\AWS_SAA\Code\s4c1\CLI>aws ec2 create-subnet --vpc-id %vpcn_Id% --cidr-block %pbsn1_Mask% --availability-zone %first_az%|jq ".Subnet.SubnetId" >tmpFile
C:\Code\bsg-saa-c02\AWS_SAA\Code\s4c1\CLI>set /p pbsn1_Id= < tmpFile
C:\Code\bsg-saa-c02\AWS_SAA\Code\s4c1\CLI>aws ec2 create-internet-gateway|jq ".InternetGateway.InternetGatewayId" >tmpFile
C:\Code\bsg-saa-c02\AWS_SAA\Code\s4c1\CLI>set /p IGW_Id= < tmpFile
C:\Code\bsg-saa-c02\AWS_SAA\Code\s4c1\CLI>aws ec2 attach-internet-gateway --vpc-id %vpcn_Id% --internet-gateway-id %IGW_Id%

C:\Code\bsg-saa-c02\AWS_SAA\Code\s4c1\CLI>aws ec2 create-route-table --vpc-id %vpcn_Id%|jq ".RouteTable.RouteTableId" >tmpFile
C:\Code\bsg-saa-c02\AWS_SAA\Code\s4c1\CLI>set /p Public_RT_Id= < tmpFile
C:\Code\bsg-saa-c02\AWS_SAA\Code\s4c1\CLI>aws ec2 create-route --route-table-id %Public_RT_Id% --destination-cidr-block 0.0.0.0/0 --gateway-id %IGW_Id%
{
  "Return": true
}

C:\Code\bsg-saa-c02\AWS_SAA\Code\s4c1\CLI>aws ec2 describe-route-tables --route-table-id %Public_RT_Id%
{
  "RouteTables": [
    {
      "Associations": [],
      "PropagatingVgws": [],
      "RouteTableId": "rtb-00928f9319847ff6f",
      "Routes": [
        {
          "DestinationCidrBlock": "10.0.0.0/16",
          "GatewayId": "local",
          "Origin": "CreateRouteTable",
          "State": "active"
        },
        {
          "DestinationCidrBlock": "0.0.0.0/0",
          "GatewayId": "igw-02666aa3671e69214",
          "Origin": "CreateRoute",
          "State": "active"
        }
      ],
      "Tags": [],
      "VpcId": "vpc-0191cac28409315b9",
    }
  ]
}

```

rem Asociar la tabla de ruta a la subred

```
aws ec2 associate-route-table --subnet-id %pbsn1_Id% --route-table-id %Public_RT_Id%
```

rem Permitir que las instancias que se ejecutan en la subred se hagan public as

```
aws ec2 modify-subnet-attribute --subnet-id %pbsn1_Id% --map-public-ip-on-launch
```

```

C:\Code\bsg-saa-c02\AWS_SAA\Code\s4c1\CLI>aws ec2 associate-route-table --subnet-id %pbsn1_Id% --route-table-id %Public_RT_Id%
{
  "AssociationId": "rtbassoc-0d333946210ba99b3",
  "AssociationState": {
    "State": "associated"
  }
}

C:\Code\bsg-saa-c02\AWS_SAA\Code\s4c1\CLI>aws ec2 modify-subnet-attribute --subnet-id %pbsn1_Id% --map-public-ip-on-launch

```

Create EC2 Keys, Sec Groups. Choose AMI and create EC2 Instances.

```
rem Crear las llaves para el SSH a las nuevas instancias y convertirlas a PP
K para usar Putty ya sea con puttygen o winscp
aws ec2 create-key-pair --key-name Lab4a --query "KeyMaterial" --
output text > Lab4a.pem
winscp.com /keygen "Lab4a.pem" /output="Lab4a.ppk"
```

```
rem Crear los Security Groups para esa instancia
aws ec2 create-security-group --group-name "SSHAccess" --
description "Security group for SSH access" --vpc-
id %vpcn_Id% |jq ".GroupId">tmpFile
set /p SSH_Sec_Group_Id= < tmpFile
aws ec2 authorize-security-group-ingress --group-id %SSH_Sec_Group_Id% --
protocol tcp --port 22 --cidr 0.0.0.0/0
```

```
rem En el laboratorio de EC2 Inicial se mostrar la importancia de buscar una
AMI correcto.
```

```
aws ec2 describe-images --owners amazon --filters "Name=name,Values=amzn2-
ami-hvm-2.0.?????????.?-x86_64-gp2" "Name=state,Values=available" --
query "reverse(sort_by(Images, &CreationDate))[0].ImageId" --
output text >tmpFile
set /p AMI= < tmpFile
aws ec2 run-instances --image-id %AMI% --count 1 --instance-type t2.micro --
key-name Lab4a --security-group-ids %SSH_Sec_Group_Id% --subnet-
id %prsn1_Id% --tag-
specifications "ResourceType=instance,Tags=[{Key=ServerName,Value=A}]"
```

```
C:\Code\bsg-saa-c02\AWS_SAA\Code\s4c1\CLI>aws ec2 create-key-pair --key-name Lab4a --query "KeyMaterial" --output text > Lab4a.pem
C:\Code\bsg-saa-c02\AWS_SAA\Code\s4c1\CLI>winscp.com /keygen "Lab4a.pem" /output="Lab4a.ppk"
Key saved to "Lab4a.ppk".

C:\Code\bsg-saa-c02\AWS_SAA\Code\s4c1\CLI>aws ec2 create-security-group --group-name "SSHAccess" --description "Security group for SSH access" --vpc-id %vpcn_Id% |jq ".GroupId">tmpFile
C:\Code\bsg-saa-c02\AWS_SAA\Code\s4c1\CLI>set /p SSH_Sec_Group_Id= < tmpFile
C:\Code\bsg-saa-c02\AWS_SAA\Code\s4c1\CLI>aws ec2 authorize-security-group-ingress --group-id %SSH_Sec_Group_Id% --protocol tcp --port 22 --cidr 0.0.0.0/0

C:\Code\bsg-saa-c02\AWS_SAA\Code\s4c1\CLI>aws ec2 describe-images --owners amazon --filters "Name=name,Values=amzn2-ami-hvm-2.0.?????????.?-x86_64-gp2" "Name=state,Values=available" --query "reverse(sort_by(Images, &CreationDate))[0].ImageId" --output text >tmpFile
C:\Code\bsg-saa-c02\AWS_SAA\Code\s4c1\CLI>set /p AMI= < tmpFile
C:\Code\bsg-saa-c02\AWS_SAA\Code\s4c1\CLI>aws ec2 run-instances --image-id %AMI% --count 1 --instance-type t2.micro --key-name Lab4a --security-group-ids %SSH_Sec_Group_Id% --subnet-id %prsn1_Id% --tag-specifications "ResourceType=instance,Tags=[{Key=ServerName,Value=A}]"
{
  "Groups": [],
  "Instances": [
    {
      "AmiLaunchIndex": 0,
      "ImageId": "ami-04e59c85167ea7bd5",
      "InstanceId": "i-02aad94a8fa2b097",
      "InstanceType": "t2.micro",
      "KeyName": "Lab4a",
      "LaunchTime": "2020-06-20T12:50:47+00:00",

```

Create Private Subnet, EIP, NAT Gateway, Private Route Table and EC2 Instance

```
rem Crear subred Privada
```

```
aws ec2 create-subnet --vpc-id %vpcn_Id% --cidr-block %prsn2_Mask% --
availability-zone %second_az%|jq ".Subnet.SubnetId" >tmpFile
set /p prsn2_Id= < tmpFile
```

```
rem Solicitar una IP Elastica para hacer el Nat Gateway
aws ec2 allocate-address --domain vpc |jq ".AllocationId" >tmpFile
set /p NAT_EIP= < tmpFile
```

```
rem Crear el NAT Gateway, asignarlo a una EIP Anterior.
aws ec2 create-nat-gateway --subnet-id %pbsn1_Id% --allocation-
id %NAT_EIP%|jq ".NatGateway.NatGatewayId" >tmpFile
set /p NATGW_Id= < tmpFile
```

```
rem Crear tabla de ruteo para las redes privadas y asignar el NAT GW como ru
ta por defecto. Asociarla
aws ec2 create-route-table --vpc-
id %vpcn_Id%|jq ".RouteTable.RouteTableId" >tmpFile
set /p Private_RT_Id= < tmpFile
aws ec2 create-route --route-table-id %Private_RT_Id% --destination-cidr-
block 0.0.0.0/0 --nat-gateway-id %NATGW_Id%
aws ec2 associate-route-table --subnet-id %prsn2_Id% --route-table-
id %Private_RT_Id%
```

```
rem Genera la segunda Instancia
aws ec2 run-instances --image-id %AMI% --count 1 --instance-type t2.micro --
key-name Lab4a --security-group-ids %SSH_Sec_Group_Id% --subnet-
id %prsn2_Id% --tag-
specifications "ResourceType=instance,Tags=[{Key=ServerName,Value=B}]]"
```

```
C:\Code\bsg-saa-c02\AWS_SAA\Code\s4c1\CLI>aws ec2 create-subnet --vpc-id %vpcn_Id% --cidr-block %prsn2_Mask% --availability-zone %second_az%|jq ".Subnet.SubnetId" >tmpFile
C:\Code\bsg-saa-c02\AWS_SAA\Code\s4c1\CLI>set /p prsn2_Id= < tmpFile
C:\Code\bsg-saa-c02\AWS_SAA\Code\s4c1\CLI>aws ec2 allocate-address --domain vpc |jq ".AllocationId" >tmpFile
C:\Code\bsg-saa-c02\AWS_SAA\Code\s4c1\CLI>set /p NAT_EIP= < tmpFile
C:\Code\bsg-saa-c02\AWS_SAA\Code\s4c1\CLI>aws ec2 allocate-address --domain vpc |jq ".AllocationId" >tmpFile
C:\Code\bsg-saa-c02\AWS_SAA\Code\s4c1\CLI>set /p NAT_EIP= < tmpFile
C:\Code\bsg-saa-c02\AWS_SAA\Code\s4c1\CLI>aws ec2 create-nat-gateway --subnet-id %pbsn1_Id% --allocation-id %NAT_EIP%|jq ".NatGateway.NatGatewayId" >tmpFile
C:\Code\bsg-saa-c02\AWS_SAA\Code\s4c1\CLI>set /p NATGW_Id= < tmpFile
C:\Code\bsg-saa-c02\AWS_SAA\Code\s4c1\CLI>aws ec2 create-route-table --vpc-id %vpcn_Id%|jq ".RouteTable.RouteTableId" >tmpFile
C:\Code\bsg-saa-c02\AWS_SAA\Code\s4c1\CLI>set /p Private_RT_Id= < tmpFile
C:\Code\bsg-saa-c02\AWS_SAA\Code\s4c1\CLI>aws ec2 create-route --route-table-id %Private_RT_Id% --destination-cidr-block 0.0.0.0/0 --nat-gateway-id %NATGW_Id%
{
  "Return": true
}

C:\Code\bsg-saa-c02\AWS_SAA\Code\s4c1\CLI>aws ec2 associate-route-table --subnet-id %prsn2_Id% --route-table-id %Private_RT_Id%
{
  "AssociationId": "rtbassoc-014aff5ad82f09a966",
  "AssociationState": {
    "State": "associated"
  }
}

C:\Code\bsg-saa-c02\AWS_SAA\Code\s4c1\CLI>aws ec2 run-instances --image-id %AMI% --count 1 --instance-type t2.micro --key-name Lab4a --security-group-ids %SSH_Sec_Group_Id% --subnet-id %prsn2_Id% --tag-specifications "ResourceType=instance,Tags=[{Key=ServerName,Value=B}]]"
{
  "Groups": [],
  "Instances": [
    {
      "AmiLaunchIndex": 0,
      "ImageId": "ami-04e59c05167ea7bd5",
      "InstanceId": "i-01d080a894833e5d1",
      "InstanceType": "t2.micro",
      "KeyName": "Lab4a",
      "LaunchTime": "2020-06-20T12:52:21+00:00",
      "SubnetId": "subnet-014aff5ad82f09a966",
      "VpcId": "vpc-014aff5ad82f09a966"
    }
  ]
}
```


Get Information about Instances

rem Traer estados de la Instancias

```
aws ec2 describe-  
instances | jq "[.Reservations | .[] | .Instances | .[] | {InstanceId: .Inst  
anceId, State: .State.Name, SubnetId: .SubnetId, VpcId: .VpcId, Name: (.Tags  
[]), PrivateIpAddress: .PrivateIpAddress, PublicIpAddress: .PublicIpAddress}  
]"
```

```
[{}], PrivateIpAddress: .PrivateIpAddress, PublicIpAddress: .PublicIpAddress]]"  
{  
  "InstanceId": "i-81d086a884833e5d1",  
  "State": "pending",  
  "SubnetId": "subnet-8292b04f8f6653117",  
  "VpcId": "vpc-8191cac2840931509",  
  "Name": {  
    "Key": "ServerName",  
    "Value": "B"  
  },  
  "PrivateIpAddress": "10.0.1.235",  
  "PublicIpAddress": null  
},  
{  
  "InstanceId": "i-82aad94a8fa32b097",  
  "State": "running",  
  "SubnetId": "subnet-8de359c860ccc3f11",  
  "VpcId": "vpc-8191cac2840931509",  
  "Name": {  
    "Key": "ServerName",  
    "Value": "A"  
  },  
  "PrivateIpAddress": "10.0.0.54",  
  "PublicIpAddress": "54.151.26.21"  
}  
]  
  
C:\Code\bsg-saa-c02\AWS_5A\Code\s4\CLI>aws ec2 describe-Instances | jq "[.Reservations | .[] | .Instances | .[] | {InstanceId: .InstanceId, State: .State.Name, SubnetId: .SubnetId, VpcId: .VpcId, Name: (.Tags  
[]), PrivateIpAddress: .PrivateIpAddress, PublicIpAddress: .PublicIpAddress}]"  
{  
  "InstanceId": "i-81d086a884833e5d1",  
  "State": "running",  
  "SubnetId": "subnet-8292b04f8f6653117",  
  "VpcId": "vpc-8191cac2840931509",  
  "Name": {  
    "Key": "ServerName",  
    "Value": "B"  
  },  
  "PrivateIpAddress": "10.0.1.235",  
  "PublicIpAddress": null  
},  
{  
  "InstanceId": "i-82aad94a8fa32b097",  
  "State": "running",  
  "SubnetId": "subnet-8de359c860ccc3f11",  
  "VpcId": "vpc-8191cac2840931509",  
  "Name": {  
    "Key": "ServerName",  
    "Value": "A"  
  },  
  "PrivateIpAddress": "10.0.0.54",  
  "PublicIpAddress": "54.151.26.21"  
}  
]  
]
```

After seconds...

rem Traer Datos especificos de instancia A. Revisar contenido de Read_A.jq

```
aws ec2 describe-instances | jq -f Read_A.jq  
aws ec2 describe-instances | jq -  
f Read_A.jq|jq ".[].PublicIpAddress" >tmpFile  
set /p A_IP= < tmpFile
```

```

C:\Code\bsg-saa-c02\AWS_SAA\Code\s4c1\CLI>aws ec2 describe-instances
[{"PrivateIpAddress": ".PrivateIpAddress", "PublicIpAddress": ".PublicIpAddress"},
[
  {
    "InstanceId": "i-01d086a884833e5d1",
    "State": "running",
    "SubnetId": "subnet-0292b94f8f6653117",
    "VpcId": "vpc-0191cac28409315b9",
    "Name": {
      "Key": "ServerName",
      "Value": "B"
    },
    "PrivateIpAddress": "10.0.1.235",
    "PublicIpAddress": null
  },
  {
    "InstanceId": "i-02aad94a8fa32b097",
    "State": "running",
    "SubnetId": "subnet-0de359c860ccc3f11",
    "VpcId": "vpc-0191cac28409315b9",
    "Name": {
      "Key": "ServerName",
      "Value": "A"
    },
    "PrivateIpAddress": "10.0.0.54",
    "PublicIpAddress": "54.151.26.21"
  }
]

```

Review Configurations using Putty, SFTP and Browser

rem Enviar la llave a la Instancia Publica para luego desde alli conectarse a la IP Privada

rem Aquí la IP A es la IP de la Instancia Publica

psftp.exe -i "Lab4a.ppk" ec2-user@%A_IP%

rem Luego alli enviar el codigo para subir el certificado y salir

put Lab4a.pem

chmod 400 Lab4a.pem

exit

rem Ingresar a la instancia publica por SSH y dejar ejecutando en el SSH "sudo python -m SimpleHTTPServer 80"

putty.exe -i "Lab4a.ppk" ec2-user@%A_IP%

rem Mirar la configuracion de la maquina actual

ip a

rem Conectarse por SSH a la Instancia Privada y desde alli escribir

rem Aquí la Ip mencionada es la IP de la instancia privada

```
ssh -i "Lab4a.pem" ec2-user@10.0.1.235
rem Mirar la configuracion de la maquina actual y revisar conectividad
ip a
ping 8.8.8.8
exit
```

```

Labs4c1.bat - AWS_SAA - Visual Studio Code
Labs4c1.bat X  Read_Ajq  Labs4c1.docx  TODO

Code > s4c1 > CLI > Labs4c1.bat
94 rem Enviar la llave a la Instancia Publica para luego desde alli conectar
95 psftp.exe -i "Lab4a.ppk" ec2-user@%A_IP%
96 rem Luego alli enviar el codigo para subir el certificado y salir
97 put Lab4a.pem
98 chmod 400 Lab4a.pem
99 exit
100
101 rem Ingresar a la instancia publica por SSH y dejar ejecutando en el SSH
102 putty.exe -i "Lab4a.ppk" ec2-user@%A_IP%
103 rem Mirar la configuracion de la maquina actual
104 ip a
105 rem Conectarse por SSH a la Instancia Privada y desde alli escribir
106 ssh -i "Lab4a.pem" ec2-user@10.0.1.235
107 rem Mirar la configuracion de la maquina actual y revisar conectividad
108 ip a
109 ping 8.8.8.8

PROBLEMS  OUTPUT  DEBUG CONSOLE  TERMINAL

C:\Code\bsg-saa-c02\AWS_SAA\Code\s4c1\CLI>psftp.exe -i "Lab4a.ppk" ec2-user@%A_IP%
Using username "ec2-user".
Remote working directory is /home/ec2-user
psftp> put Lab4a.pem
local: Lab4a.pem => remote:/home/ec2-user/Lab4a.pem
psftp> chmod 400 Lab4a.pem
/home/ec2-user/Lab4a.pem: 0664 -> 0400
psftp> exit

C:\Code\bsg-saa-c02\AWS_SAA\Code\s4c1\CLI>putty.exe -i "Lab4a.ppk" ec2-user@%A_IP%

C:\Code\bsg-saa-c02\AWS_SAA\Code\s4c1\CLI>

ec2-user@ip-10-0-1-235:~$
Using username "ec2-user".
Authenticating with public key "imported-openssh-key"
Last login: Sat Jun 20 17:49:04 2020 from 181.61.208.101

Amazon Linux 2 AMI

https://aws.amazon.com/amazon-linux-2/
4 package(s) needed for security, out of 10 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-10-0-0-54 ~]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 02:c7:6d:80:b1:25 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.54/24 brd 10.0.0.255 scope global dynamic eth0
        valid_lft 2225sec preferred_lft 2225sec
    inet6 fe80::c7:6d:ff:fe80:b125/64 scope link
        valid_lft forever preferred_lft forever

[ec2-user@ip-10-0-1-235 ~]$ ssh -i "Lab4a.ppk" ec2-user@10.0.1.235
Last login: Sat Jun 20 17:49:54 2020 from 10.0.0.54

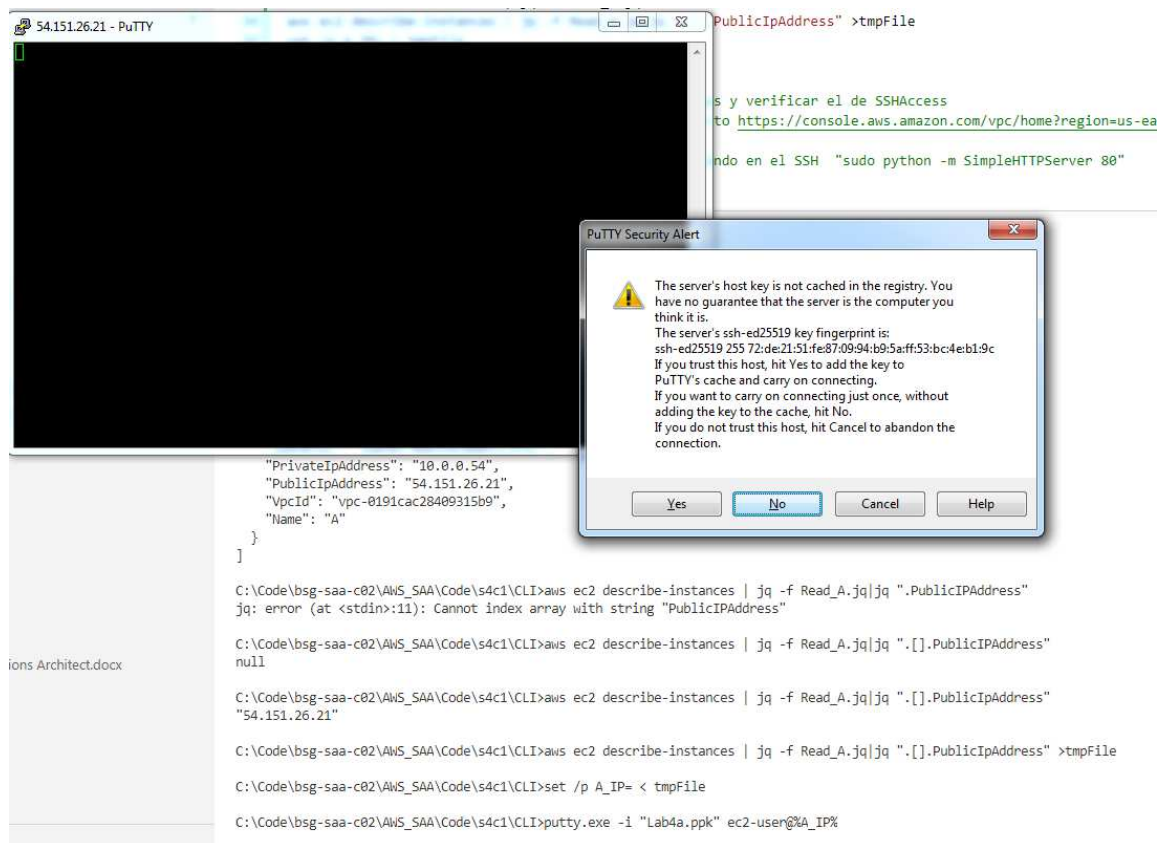
Amazon Linux 2 AMI

https://aws.amazon.com/amazon-linux-2/
4 package(s) needed for security, out of 10 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-10-0-1-235 ~]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 06:91:36:e3:eb:ef brd ff:ff:ff:ff:ff:ff
    inet 10.0.1.235/24 brd 10.0.1.255 scope global dynamic eth0
        valid_lft 1988sec preferred_lft 1988sec
    inet6 fe80::491:36:ff:fe80:ebef/64 scope link
        valid_lft forever preferred_lft forever

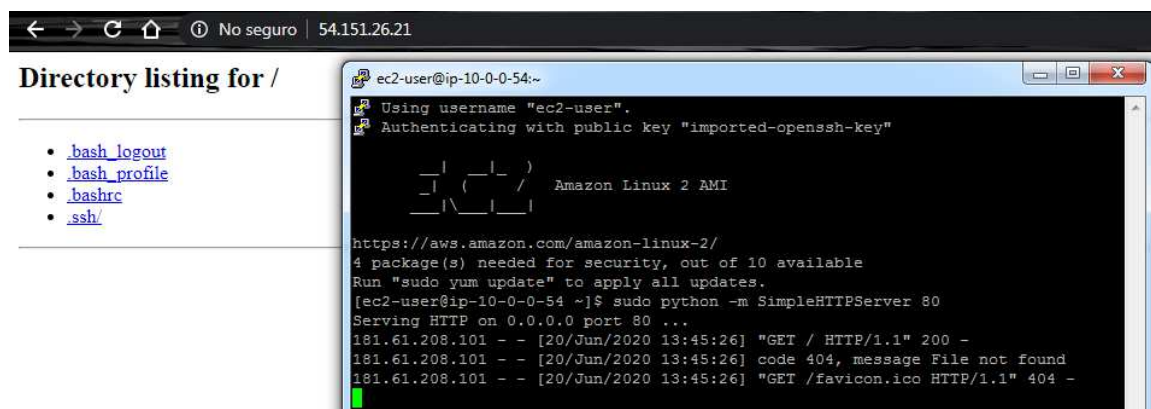
[ec2-user@ip-10-0-1-235 ~]$ ping 8.8.8.8
PING: send=10.0.0.1-235 -18 ping 8.8.8.8
6 bytes from 8.8.8.8: icmp_seq=1 ttl=112 time=2.39 ms
6 bytes from 8.8.8.8: icmp_seq=2 ttl=112 time=2.24 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=112 time=2.13 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 2.138/2.296/2.390/0.110 ms

```

```
rem Dentro de la instancia ejecutar
sudo python -m SimpleHTTPServer 80
Add Port to Security Group
rem Intentar ingresar por un navegador a esa IP Publica
rem Modificar el Security Group para habilitar el puerto 80
aws ec2 authorize-security-group-ingress --group-id %SSH_Sec_Group_Id% --
protocol tcp --port 80 --cidr 0.0.0.0/0
```



rem Intentar ingresar por un navegador a esa IP Publica



Delete Port to Security Group

rem Eliminar el ingreso del Security Group anterior

```
aws ec2 revoke-security-group-ingress --group-id %SSH_Sec_Group_Id% --  
protocol tcp --port 80 --cidr 0.0.0.0/0  
rem Volver a intentar ingresar por un navegador a esa IP
```

Clean resources

For Web Management Console

EC2: Terminate Instances

EC2: Security Groups

EC2: KeyPairs

VPC: NAT Gateway

VPC: EIP (Release)

VPC: IGW (Detach and then Delete)

VPC: Subnets

VPC: RT

VPC: VPC

For Command Line (Windows)

```
rem ----- ELIMINAR RECURSOS -----  
aws ec2 terminate-instances --instance-ids "i-01d086a884833e5d1" "i-  
02aad94a8fa32b097"  
aws ec2 delete-security-group --group-id %SSH_Sec_Group_Id%  
aws ec2 delete-subnet --subnet-id %prsn2_Id%  
aws ec2 delete-nat-gateway --nat-gateway-id %NATGW_Id%  
aws ec2 delete-route-table --route-table-id %Private_RT_Id%  
aws ec2 release-address --allocation-id %NAT_EIP%  
aws ec2 delete-subnet --subnet-id %pbsn1_Id%  
aws ec2 delete-route-table --route-table-id %Public_RT_Id%  
aws ec2 detach-internet-gateway --internet-gateway-id %IGW_Id% --vpc-  
id %vpcn_Id%  
aws ec2 delete-internet-gateway --internet-gateway-id %IGW_Id%  
aws ec2 delete-vpc --vpc-id %vpcn_Id%
```

Evidences to send

To have a review, the student has to send some screenshots to instructor email:

1. The first screenshot of [Review Configurations using Putty, SFTP and Browser](#). Showing SSH connection from Public Instance to Private Instances, and both different IPs.
2. The last screenshot of [Review Configurations using Putty, SFTP and Browser](#). Showing the browser with list of users and pythons script running.