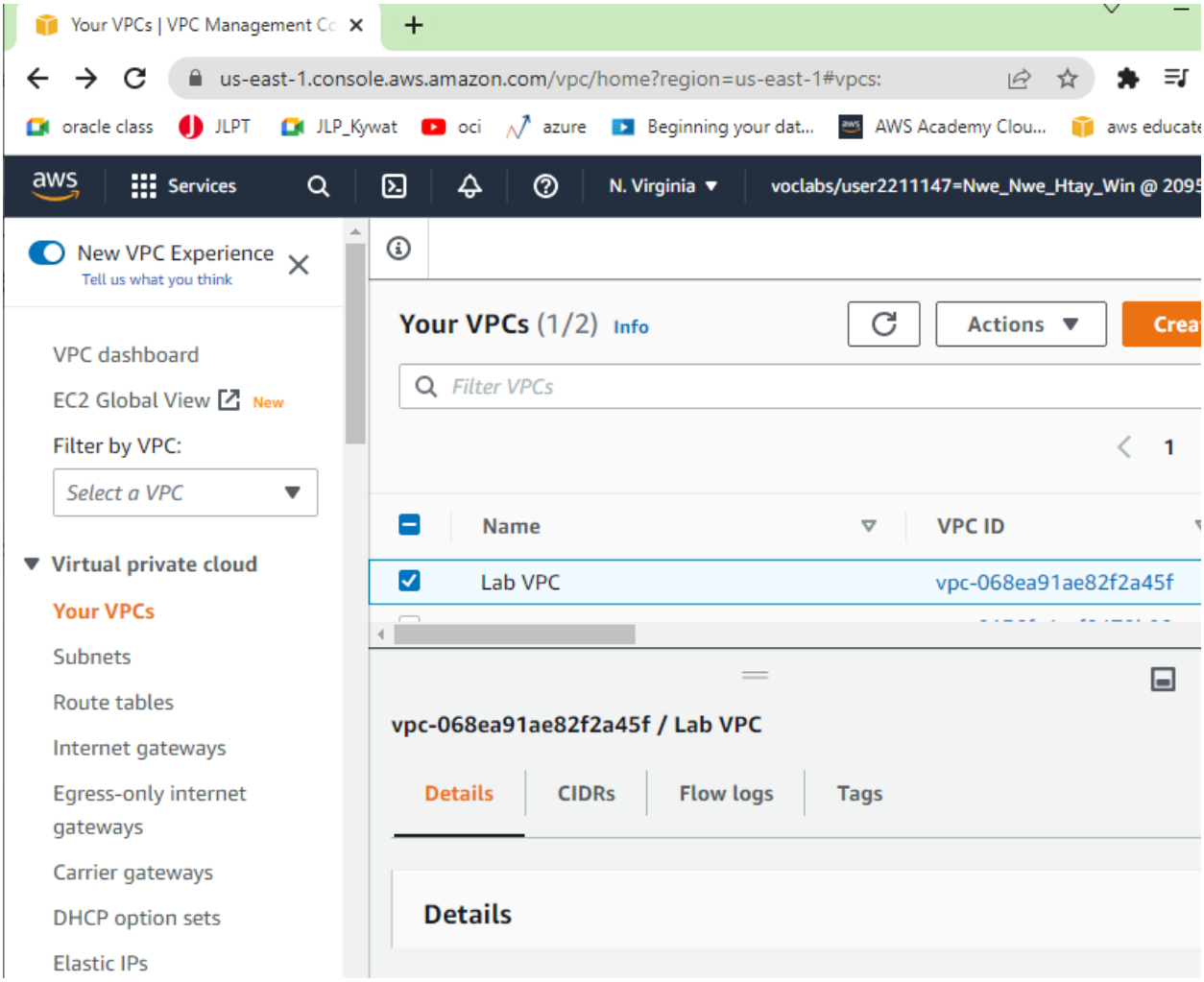
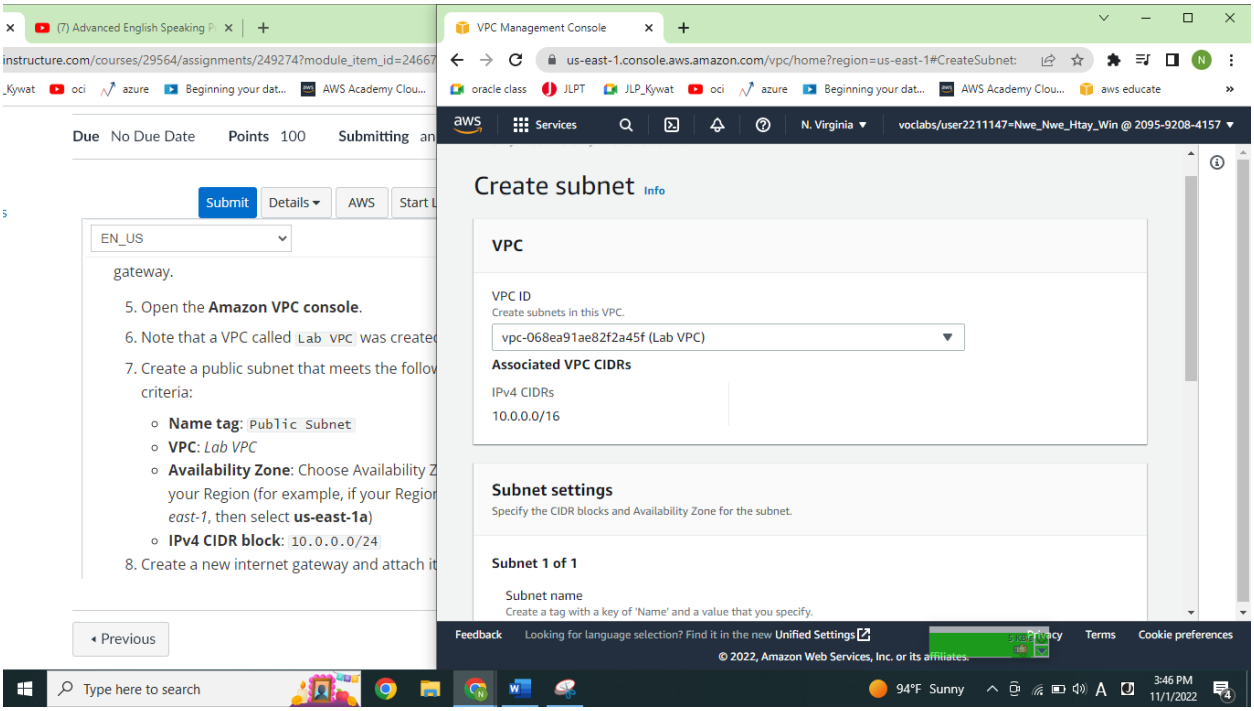
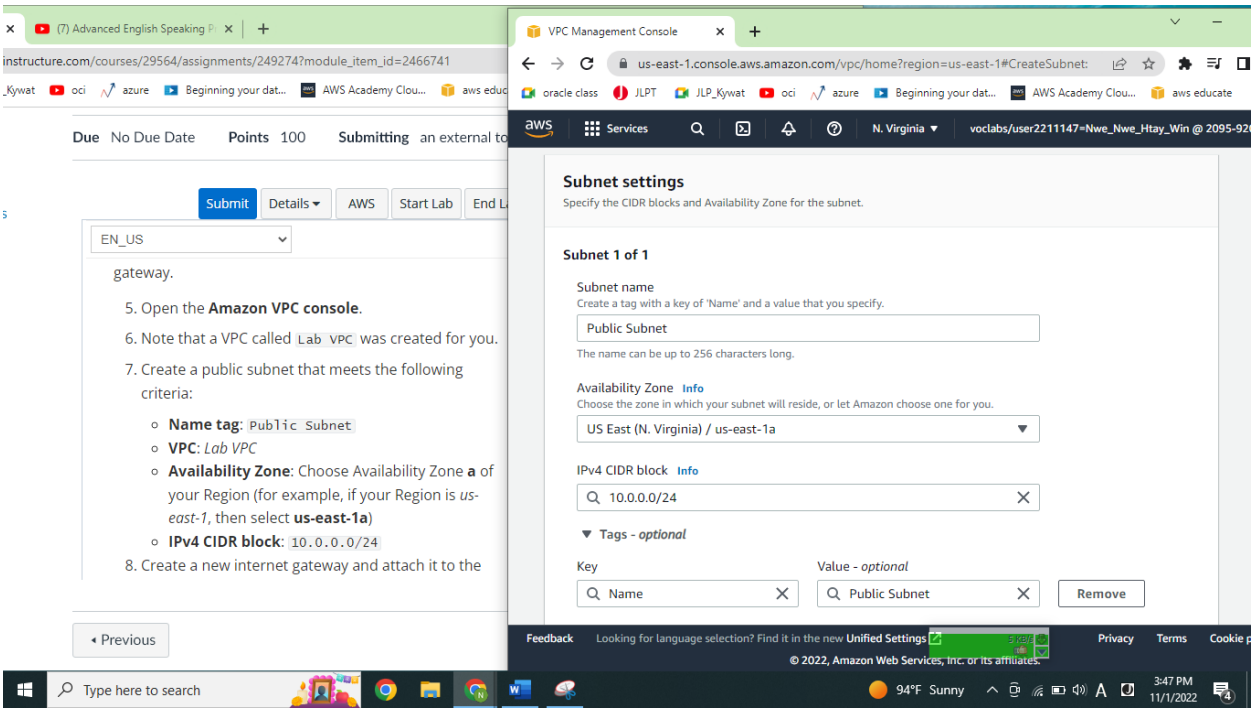
Module 6 Challenge Lab - Creating a VPC Networking Environment for the Cafe

Use Lab PVC which was already created in last GL




Due No Due Date Points 100 Submitting an
Submit Details AWS Start L
EN_US
gateway.
5. Open the Amazon VPC console.
6. Note that a VPC called Lab VPC was create
7. Create a public subnet that meets the follov criteria:
Name tag: Public Subnet
VPC: Lab VPC
Availability Zone: Choose Availability Z your Region (for example, if your Regior east-1, then select us-east-1a)
IPv4 CIDR block: 10.0.0.0/24
8. Create a new internet gateway and attach it
Previous
VPC Management Console
us-east-1.console.aws.amazon.com/vpc/home?region=us-east-1#CreateSubnet:
Create subnet Info
VPC
VPC ID
Create subnets in this VPC.
vpc-068ea91ae82f2a45f (Lab VPC)
Associated VPC CIDRs
IPv4 CIDRs
10.0.0.0/16
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.
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy Terms Cookie preferences
Type here to search
94°F Sunny
3:46 PM 11/1/2022


Due No Due Date Points 100 Submitting an external to
Submit Details AWS Start Lab End L
EN_US
gateway.
5. Open the Amazon VPC console.
6. Note that a VPC called Lab VPC was created for you.
7. Create a public subnet that meets the following criteria:
Name tag: Public Subnet
VPC: Lab VPC
Availability Zone: Choose Availability Zone a of your Region (for example, if your Region is us-east-1, then select us-east-1a)
IPv4 CIDR block: 10.0.0.0/24
8. Create a new internet gateway and attach it to the
Previous
VPC Management Console
us-east-1.console.aws.amazon.com/vpc/home?region=us-east-1#CreateSubnet:
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 Subnet
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.
US East (N. Virginia) / us-east-1a
IPv4 CIDR block Info
10.0.0.0/24
Tags - optional
Key
Value - optional
Name
Public Subnet
Remove
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy Terms
Type here to search
94°F Sunny
3:47 PM 11/1/2022

Create IG

Due No Due Date Points 100 Submitting an external to

Submit Details AWS Start Lab End L

EN_US

- **VPC**: *Lab VPC*
- **Availability Zone**: Choose Availability Zone **a** of your Region (for example, if your Region is *us-east-1*, then select **us-east-1a**)
- **IPv4 CIDR block**: `10.0.0.0/24`

8. Create a new internet gateway and attach it to the `Lab VPC`.
9. Edit the route table that was created in your VPC. Add the route `0.0.0.0/0`. For the target, select the internet gateway that you created in the previous step

   Hint: To successfully complete this task, you must create a few resources. If you get stuck, refer to the

Previous

Internet gateways | VPC Manage

us-east-1.console.aws.amazon.com/vpc/home?region=us-east-1#igws:

New VPC Experience
Tell us what you think

VPC dashboard
EC2 Global View New
Filter by VPC:
Select a VPC

Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
Elastic IPs

Internet gateways (1/1) Info

Actions Create internet gateway

Filter internet gateways

Name	Internet gateway ID	Sta
	igw-02323ca9b4eefb12a	

Details Tags

Details

Due No Due Date Points 100 Submitting an external to

Submit Details AWS Start Lab End L

EN_US

- **VPC**: *Lab VPC*
- **Availability Zone**: Choose Availability Zone **a** of your Region (for example, if your Region is *us-east-1*, then select **us-east-1a**)
- **IPv4 CIDR block**: `10.0.0.0/24`

8. Create a new internet gateway and attach it to the `Lab VPC`.
9. Edit the route table that was created in your VPC. Add the route `0.0.0.0/0`. For the target, select the internet gateway that you created in the previous step

   Hint: To successfully complete this task, you must create a few resources. If you get stuck, refer to the

Previous

Create internet gateway | VPC M

us-east-1.console.aws.amazon.com/vpc/home?region=us-east-1#CreateInternet...

Internet gateway settings

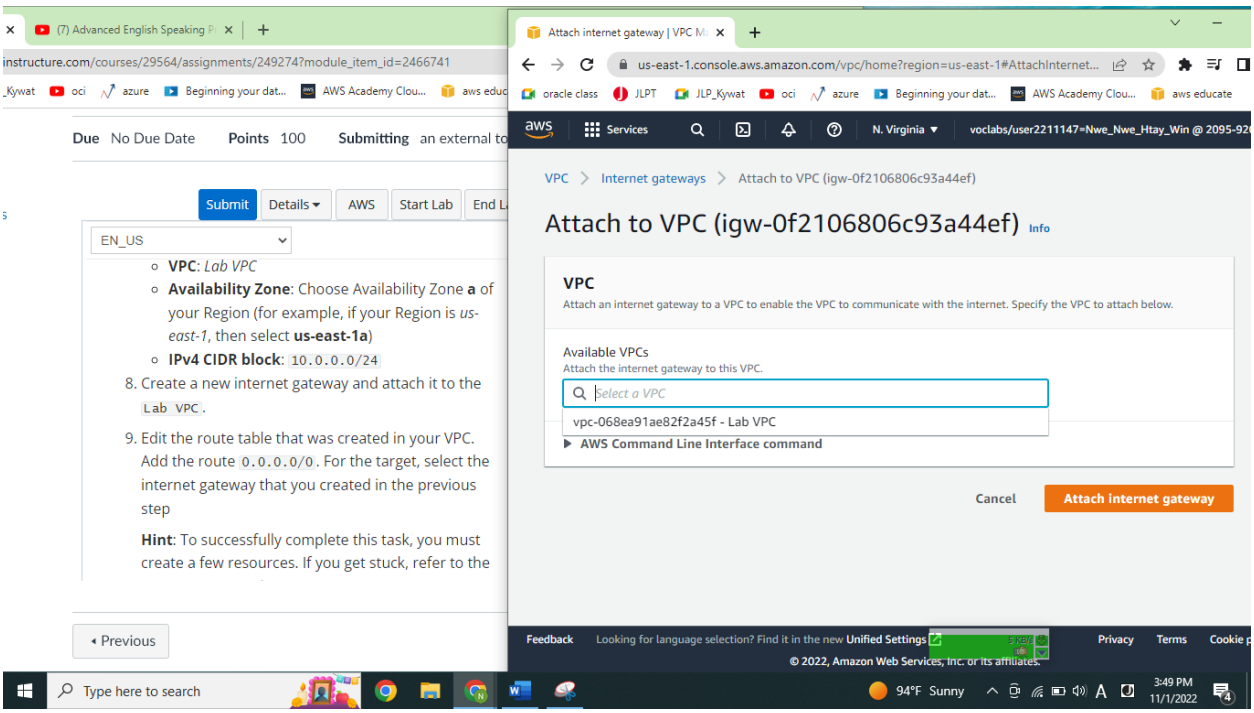
Name tag
Creates a tag with a key of 'Name' and a value that you specify.
Lab Gateway

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*	
Name	Lab Gateway	Remove

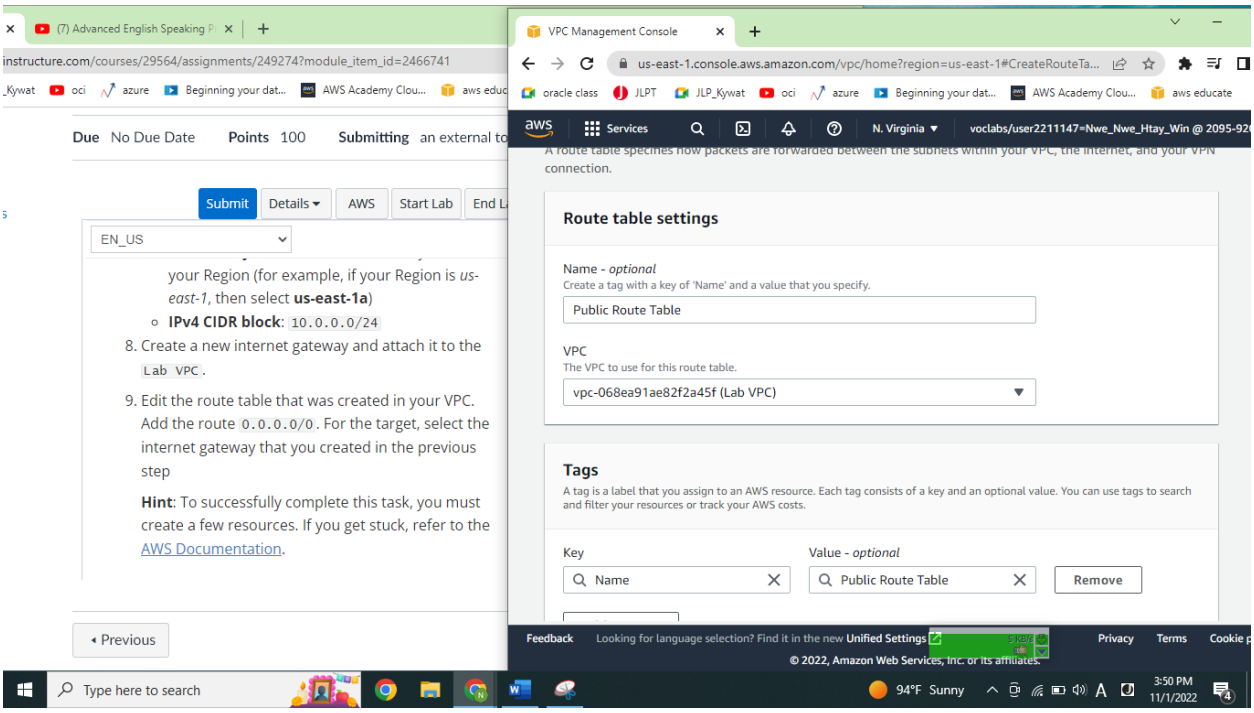
Add new tag
You can add 49 more tags.

Cancel Create internet gateway



Let's create route table

Public and private



VPC Management Console

us-east-1.console.aws.amazon.com/vpc/home?region=us-east-1#EditRoutes:RouteTableId=rtb-05ba4e4564d265521

VPC > Route tables > rtb-05ba4e4564d265521 > Edit routes

Edit routes

Destination	Target	Status	Propagated	
10.0.0.0/16	local	Active	No	
0.0.0.0/0		–	No	Remove

Add route

Carrier Gateway
Core Network
Egress Only Internet Gateway
Gateway Load Balancer Endpoint
Instance
Internet Gateway
local Internet Gateway
NAT Gateway

Cancel | Preview | Save changes

VPC Management Console

us-east-1.console.aws.amazon.com/vpc/home?region=us-east-1#RouteTableDetails:RouteTableId=rtb-05ba4e4564d265521

New VPC Experience
Tell us what you think

VPC dashboard
EC2 Global View New
Filter by VPC:
Select a VPC

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

Updated routes for rtb-05ba4e4564d265521 / Public Route Table successfully
Details

vpc-068ea91ae82f2a45f | Lab VPC | 209592084157

Routes | Subnet associations | Edge associations | Route propagation | Tags

Routes (2)

Edit routes

Filter routes | Both | 1

Destination	Target	Status	Propagated
0.0.0.0/0	igw-0f2106806c93a44ef	Active	No
10.0.0.0/16	local	Active	No

VPC Management Console

us-east-1.console.aws.amazon.com/vpc/home?region=us-east-1#CreateRouteTable:

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

Private Route Table

VPC
The VPC to use for this route table.

vpc-068ea91ae82f2a45f (Lab VPC)

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*	
Name	Private Route Table	Remove

Add new tag

You can add 49 more tags.

Cancel | Create route table

Route tables | VPC Management

us-east-1.console.aws.amazon.com/vpc/home?region=us-east-1#RouteTables:

Route table rtb-0dd81d88377febbde | Private Route Table was created successfully.

Route tables (4) Info

Actions | Create route table

Filter route tables

Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC
Public Route Table	rtb-05ba4e4564d265521	–	–	No	vpc-068ea91ae82
–	rtb-0211540387225425c	–	–	Yes	vpc-068ea91ae82
–	rtb-0dc7eb0719832c310	–	–	Yes	vpc-0136fc4cef84
Private Route Table	rtb-0dd81d88377febbde	–	–	No	vpc-068ea91ae82

New VPC Experience
Tell us what you think

VPC dashboard
EC2 Global View New
Filter by VPC:
Select a VPC

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

instructure.com/courses/29564/assignments/249274?module_item_id=2466741

Due No Due Date Points 100 Submitting an external tool

Submit Details AWS Start Lab End Lab

EN_US

Task 2: Creating a bastion host

In this task, you will create a bastion host in the *Public Subnet*. In later tasks, you will create an EC2 instance in a private subnet and connect to it from this bastion host.

10. From the **Amazon EC2 console**, create an EC2 instance in the `Public Subnet` of the *Lab VPC* that meets the following criteria:
    - **Amazon Machine Image (AMI)**: *Amazon Linux 2 AMI (HVM)*
    - **Instance type**: *t2.micro*

Previous

Route tables | VPC Management

us-east-1.console.aws.amazon.com/vpc/home?region=us-east-1#RouteTables:

EC2

Services (9) Features (51) Blogs (1,821) Documentation (123,638) Knowledge Articles (30)

EC2
Virtual Servers in the Cloud

EC2 Image Builder
A managed service to automate build, customize and deploy OS images

AWS Firewall Manager
Central management of firewall rules

GuardDuty
Intelligent Threat Detection to Protect Your AWS Accounts and Workloads

AWS Compute Optimizer
Recommend optimal AWS Compute resources for your workloads

Feedback Looking for language selection? Find it in the new Unified Settings Privacy Terms

instructure.com/courses/29564/assignments/249274?module_item_id=2

Due No Due Date Points 100 Submitting

Submit Details AWS

EN_US

Task 2: Creating a bastion h

In this task, you will create a bastion host in
Subnet. In later tasks, you will create an EC2
private subnet and connect to it from this b

10. From the **Amazon EC2 console**, create
    instance in the `Public Subnet` of the *L*
    meets the following criteria:
    - **Amazon Machine Image (AMI)**: *An*
      AMI (HVM)
    - **Instance type**: *t2.micro*

Previous

Dashboard | EC2 Management C

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Home:

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
Dedicated Hosts
Scheduled Instances
Capacity Reservations

Easily size, configure, and deploy Microsoft SQL Server Always On availability groups on AWS using the AWS Launch Wizard for SQL Server. Learn more

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

Note: Your instances will launch in the US East (N. Virginia) Region

Service health

AWS Health Dashboard

Region
US East (N. Virginia)

Status
This service is operating normally

Scheduled events

Zones

instructure.com/courses/29564/assignments/249274?module_item_id=2466741

Due No Due Date Points 100 Submitting an external tool

Submit Details AWS Start Lab End Lab

EN_US

instance in the `Public Subnet` of the *Lab VPC* that meets the following criteria:

- **Amazon Machine Image (AMI)**: *Amazon Linux 2 AMI (HVM)*
- **Instance type**: *t2.micro*
- **Auto-assign Public IP**: This setting should be disabled
- **Name**: `Bastion Host`
- Security group called `Bastion Host SG` that only allows the following traffic:
  - **Type**: *SSH*
  - **Port**: `22`

Previous

Launch an instance | EC2 Manag

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstanc...

Search our full catalog including 1000s of application and OS images

Quick Start

Amazon Linux | macOS | Ubuntu | Windows | Re

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type — Free tier eligible

ami-09d3b3274b6c5d4aa (64-bit (x86)) / ami-081dc0707789c2daf (64-bit (Arm))

Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Amazon Linux 2 Kernel 5.10 AMI 2.0.20221004.0 x86_64 HVM gp2

Architecture AMI ID

Verified provider

Feedback Looking for language selection? Find it in the new Unified Settings Privacy Terms

Type here to search 94°F Sunny 3:54 PM 11/1/2022

instructure.com/courses/29564/assignments/249274?module_item_id=2466741

Due No Due Date Points 100 Submitting an external tool

Submit Details AWS Start Lab End Lab

EN_US

instance in the `Public Subnet` of the *Lab VPC* that meets the following criteria:

- **Amazon Machine Image (AMI)**: *Amazon Linux 2 AMI (HVM)*
- **Instance type**: *t2.micro*
- **Auto-assign Public IP**: This setting should be disabled
- **Name**: `Bastion Host`
- Security group called `Bastion Host SG` that only allows the following traffic:
  - **Type**: *SSH*
  - **Port**: `22`

Previous

Launch an instance | EC2 Manag

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchIn...

auto-assi 1/1

pair

Network settings Info

VPC - *required* Info

vpc-0136fc4cef8478b92 (default)

172.31.0.0/16

Subnet Info

No preference — Create new subne

Auto-assign public IP Info

Enable

Enable

Disable

Create security group — Select existing security group

Security group name - *required*

Feedback Looking for language selection? Find it in the new Unified Settings Privacy Terms

Type here to search 94°F Sunny 3:56 PM 11/1/2022

Launch an instance | EC2 Manag

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:

oracle class | JLPT | JLP_Kywat | oci | azure | Beginning your dat... | AWS Academy Clou... | aws educate | aws ra | Teamup

auto-assi 1/1

aws | Services | Search for services, features, blogs, docs, and more [Alt+S] | N. Virginia | voclabs/user2211147=Nwe_Nwe_Htay_Win @ 2095-9208-4157

Network settings Info

VPC - *required* Info

vpc-068ea91ae82f2a45f (Lab VPC)
10.0.0.0/16

Subnet Info

subnet-02dadfe1bd4b73a10 Public Subnet
VPC: vpc-068ea91ae82f2a45f Owner: 209592084157
Availability Zone: us-east-1a IP addresses available: 251 CIDR: 10.0.0.0/24)

Create new subnet

Auto-assign public IP Info

Disable

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 reach your instance.

Create security group | Select existing security group

Security group name - *required*

launch-wizard-1

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*

Summary

Number of instances Info

1

Software Image (AMI)
Amazon Linux 2 Kernel 5.10 AMI...read more
ami-09d3b3274b6c5d4aa

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

Cancel | Launch instance

Feedback | Looking for language selection? Find it in the new Unified Settings | © 2022, Amazon Web Services, Inc. or its affiliates. | Privacy | Terms | Cookie preferences

Type here to search | 94°F Sunny | 3:57 PM 11/1/2022

Launch an instance | EC2 Manag

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:

oracle class | JLPT | JLP_Kywat | oci | azure | Beginning your dat... | AWS Academy Clou... | aws educate | aws ra | Teamup

auto-assi 1/1

aws | Services | Search for services, features, blogs, docs, and more [Alt+S] | N. Virginia | voclabs/user2211147=Nwe_Nwe_Htay_Win @ 2095-9208-4157

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

Create security group | Select existing security group

Security group name - *required*

Bastion Host SG

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*

Description - *required* Info

launch-wizard-1 created 2022-11-01T09:24:14.960Z

Inbound security groups rules

Security group rule 1 (TCP, 22, 103.231.95.13/32) | Remove

Type Info	Protocol Info	Port range Info
ssh	TCP	22

Source type Info	Name Info	Description - *optional* Info
My IP	Add CIDR, prefix list or security	e.g. SSH for admin desktop
	103.231.95.13/32	

Summary

Number of instances Info

1

Software Image (AMI)
Amazon Linux 2 Kernel 5.10 AMI...read more
ami-09d3b3274b6c5d4aa

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

Cancel | Launch instance

Feedback | Looking for language selection? Find it in the new Unified Settings | © 2022, Amazon Web Services, Inc. or its affiliates. | Privacy | Terms | Cookie preferences

Type here to search | 93°F Mostly sunny | 4:08 PM 11/1/2022

Launch an instance | EC2 Manag

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:

following the simple steps below.

Name and tags Info

Name

Bastion Host

Add additional tags

Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

Quick Start

Amazon Linux | macOS | Ubuntu | Windows | Red Hat | Browse more AMIs

Summary

Number of instances Info

1

Software Image (AMI)

Amazon Linux 2 Kernel 5.10 AMI...read more

ami-09d3b3274b6c5d4aa

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Cancel | Launch instance

Feedback | Looking for language selection? Find it in the new Unified Settings | © 2022, Amazon Web Services, Inc. or its affiliates. | Privacy | Terms | Cookie preferences

Launch an instance | EC2 Manag

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:

EC2 > Instances > Launch an instance

Success

Successfully initiated launch of instance (i-0731f2a149788d9bd)

Launch log

Next Steps

Create billing and free tier usage alerts

To manage costs and avoid surprise bills, set up email notifications for billing and free tier usage thresholds.

Create billing alerts

Connect to your instance

Once your instance is running, log into it from your local computer.

Connect to instance

Learn more

Connect an RDS database New

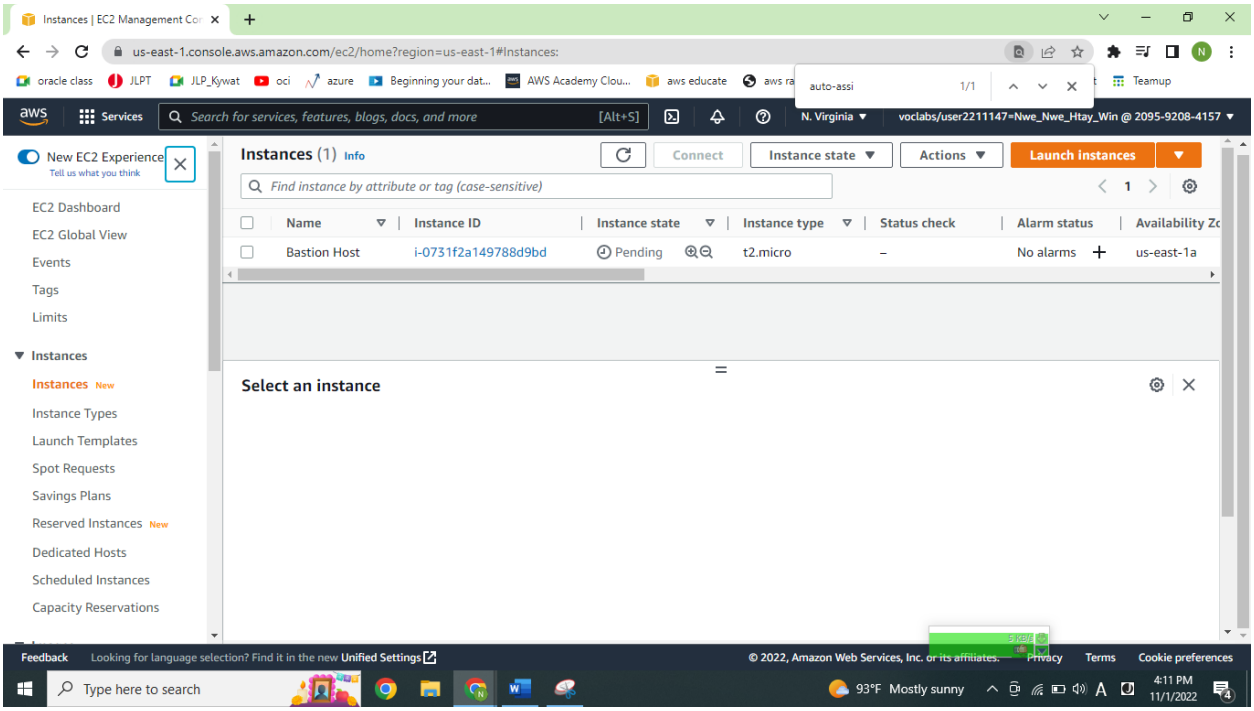
Configure the connection between an EC2 instance and a database to allow traffic flow between them.

Connect an RDS database

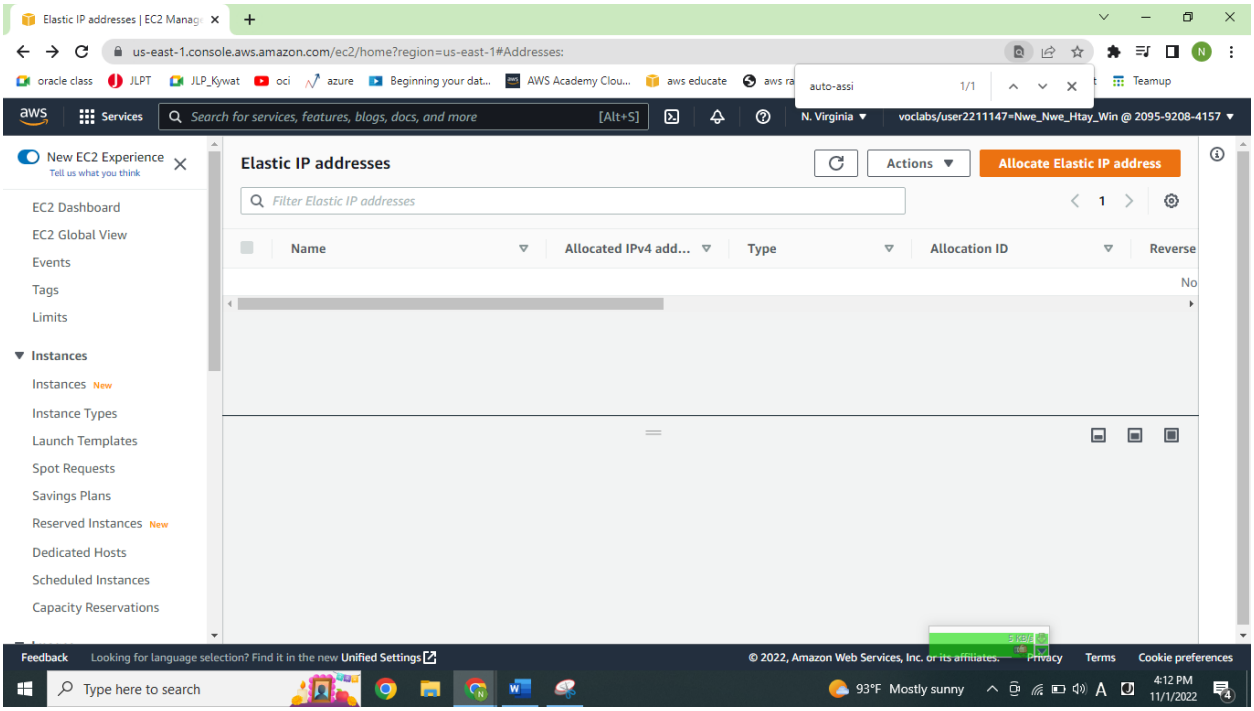
Create a new RDS database | Learn more

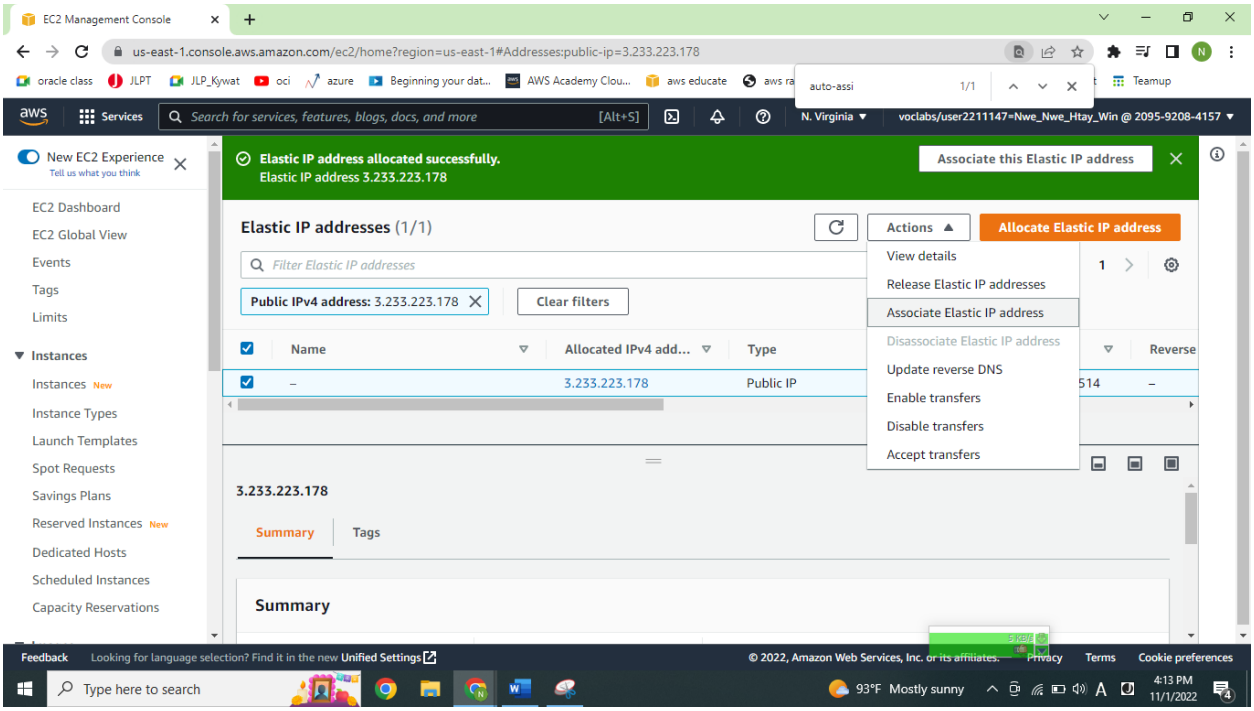
https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Instances:

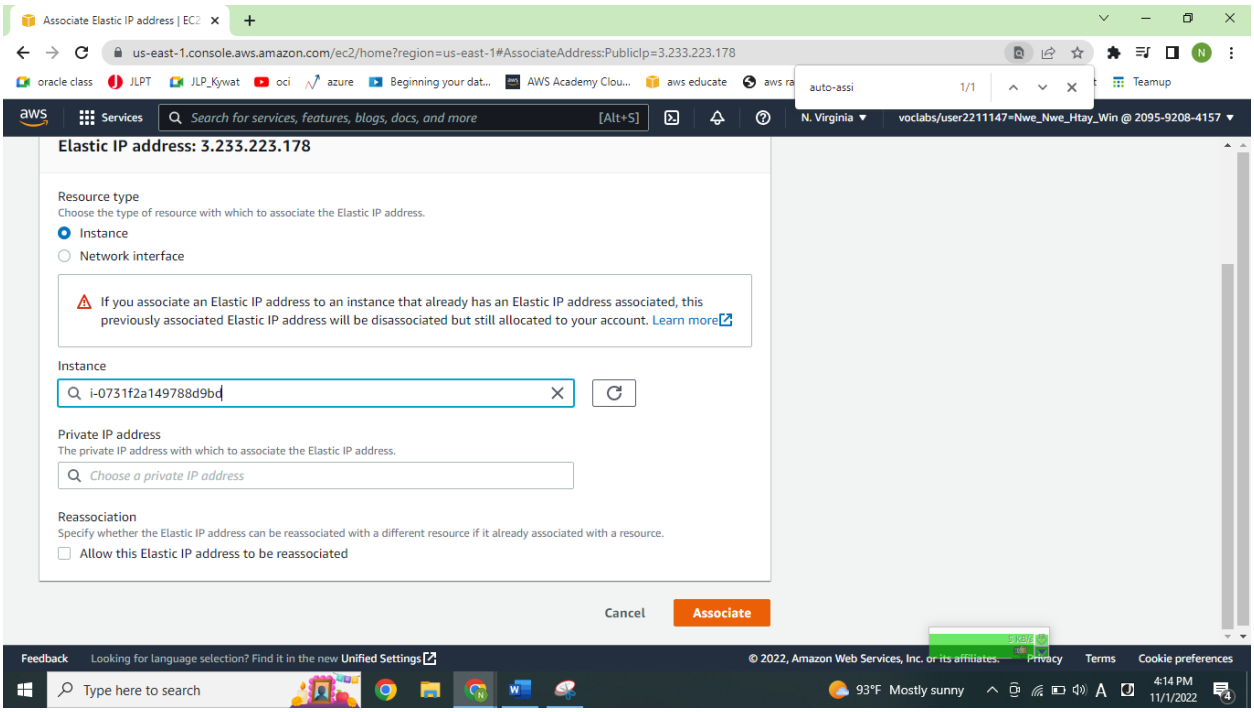
© 2022, Amazon Web Services, Inc. or its affiliates. | Privacy | Terms | Cookie preferences


Instances | EC2 Management Co
us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Instances:
Services
Search for services, features, blogs, docs, and more
N. Virginia
voclabs/user2211147=Nwe_Nwe_Htay_Win @ 2095-9208-4157
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
Dedicated Hosts
Scheduled Instances
Capacity Reservations
Instances (1) Info
Connect
Instance state
Actions
Launch instances
Find instance by attribute or tag (case-sensitive)
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Bastion Host
i-0731f2a149788d9bd
Pending
t2.micro
No alarms
us-east-1a
Select an instance
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
93°F Mostly sunny
4:11 PM
11/1/2022

Elastic IP

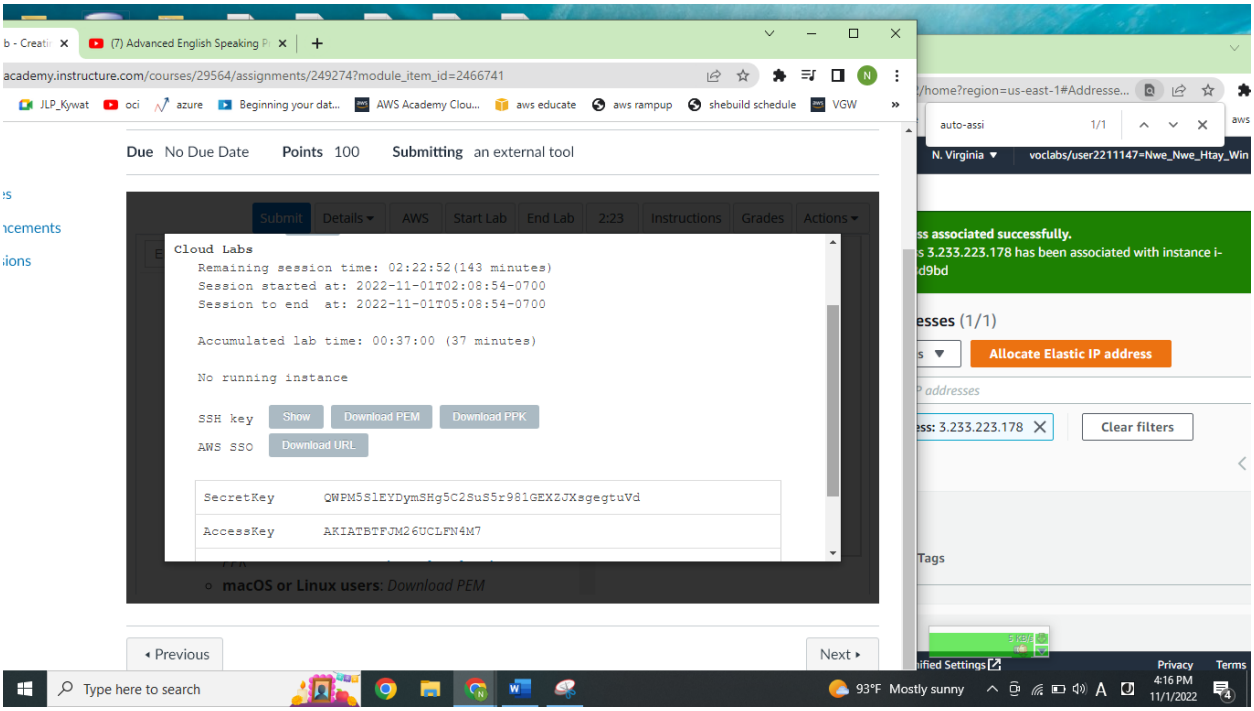

Elastic IP addresses | EC2 Manag
us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Addresses:
Services
Search for services, features, blogs, docs, and more
N. Virginia
voclabs/user2211147=Nwe_Nwe_Htay_Win @ 2095-9208-4157
New EC2 Experience
Tell us what you think
EC2 Dashboard
EC2 Global View
Events
Tags
Limits
Instances
Instances New
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances New
Dedicated Hosts
Scheduled Instances
Capacity Reservations
Elastic IP addresses
Actions
Allocate Elastic IP address
Filter Elastic IP addresses
Name
Allocated IPv4 add...
Type
Allocation ID
Reverse
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
93°F Mostly sunny
4:12 PM
11/1/2022



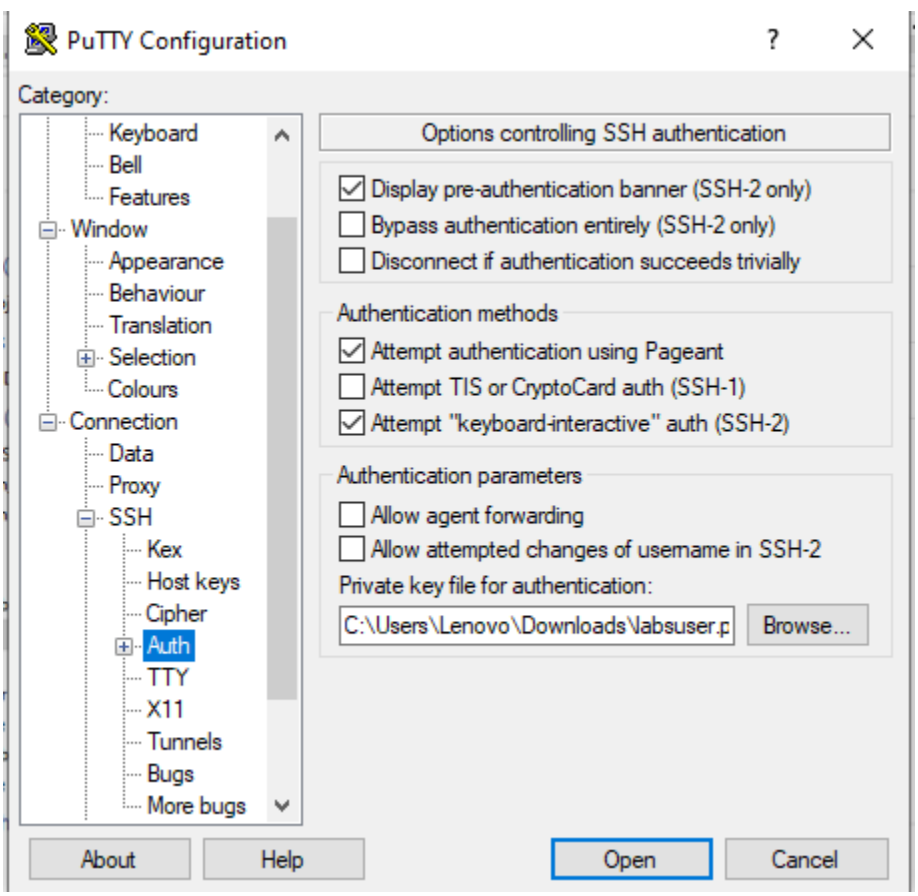


Choose Bation Host instance

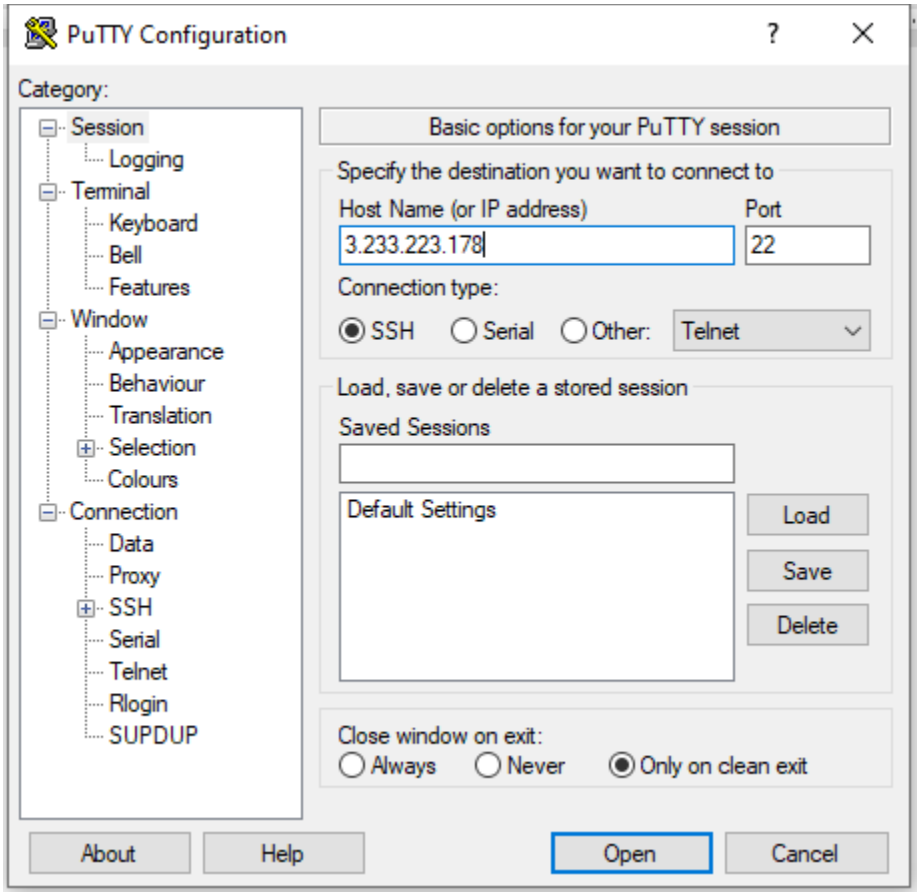
Download PPK

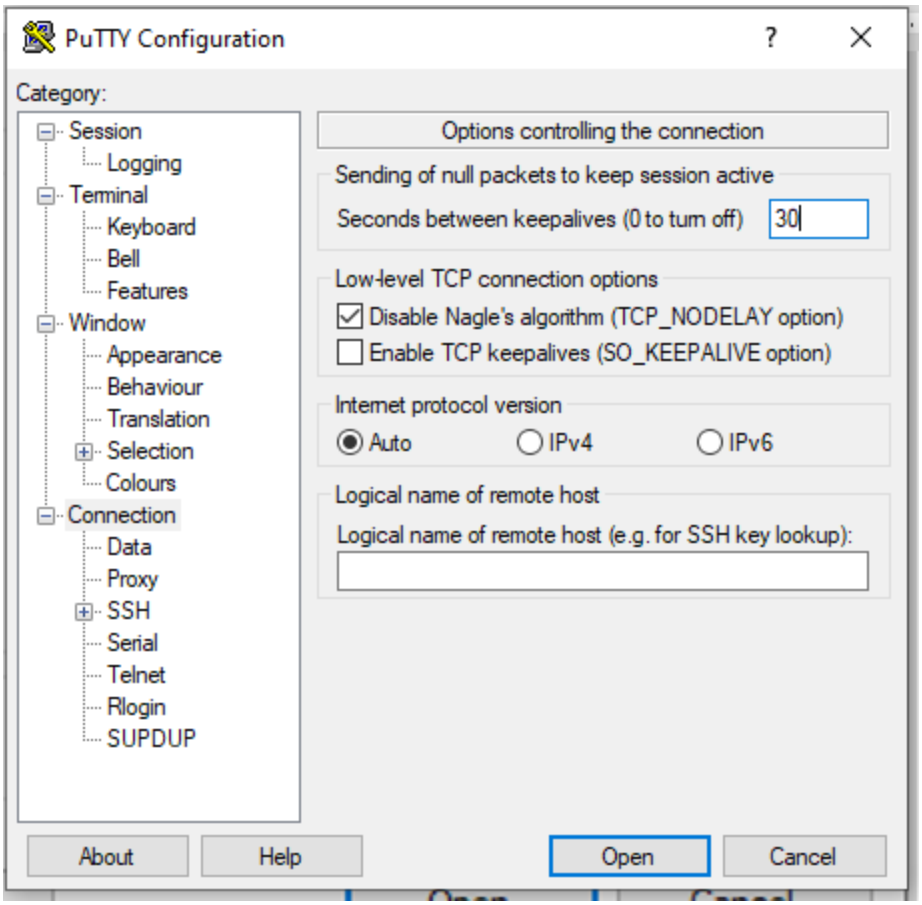


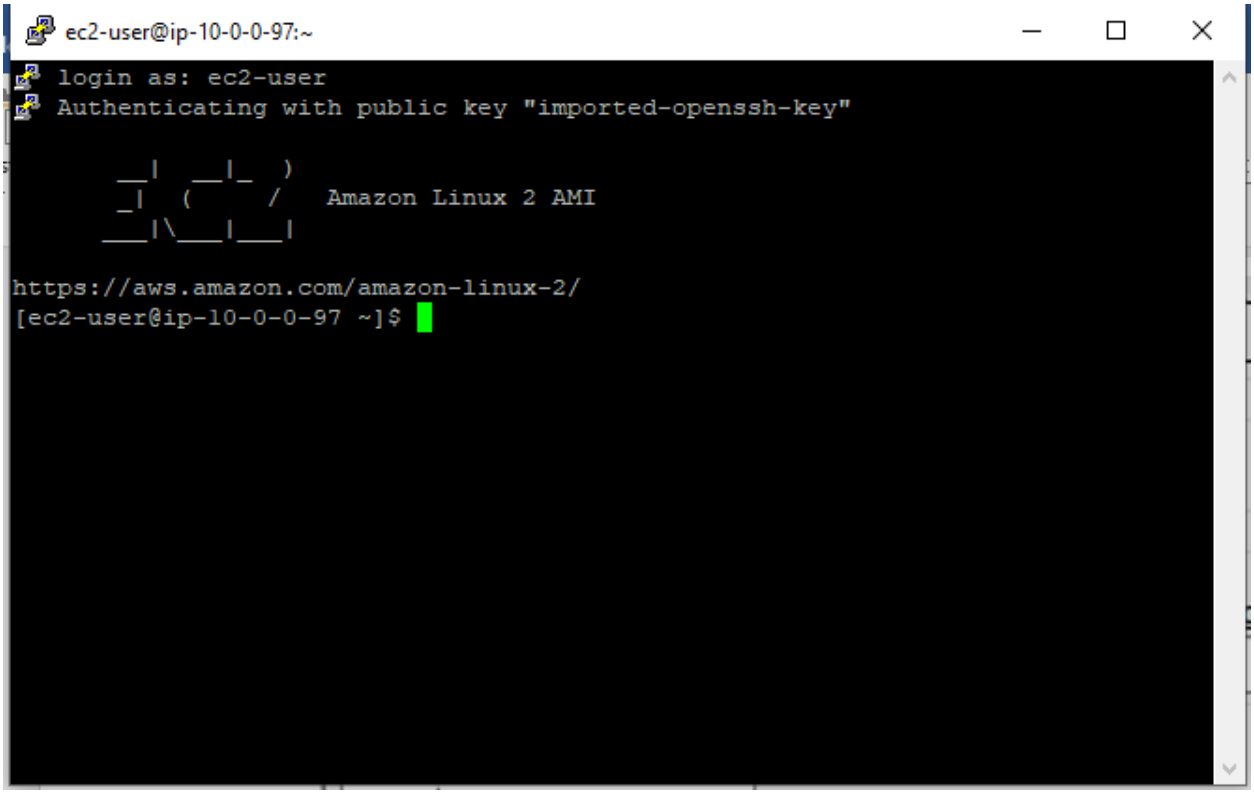
Add bahstion host instance ipv4 address and check in ssh

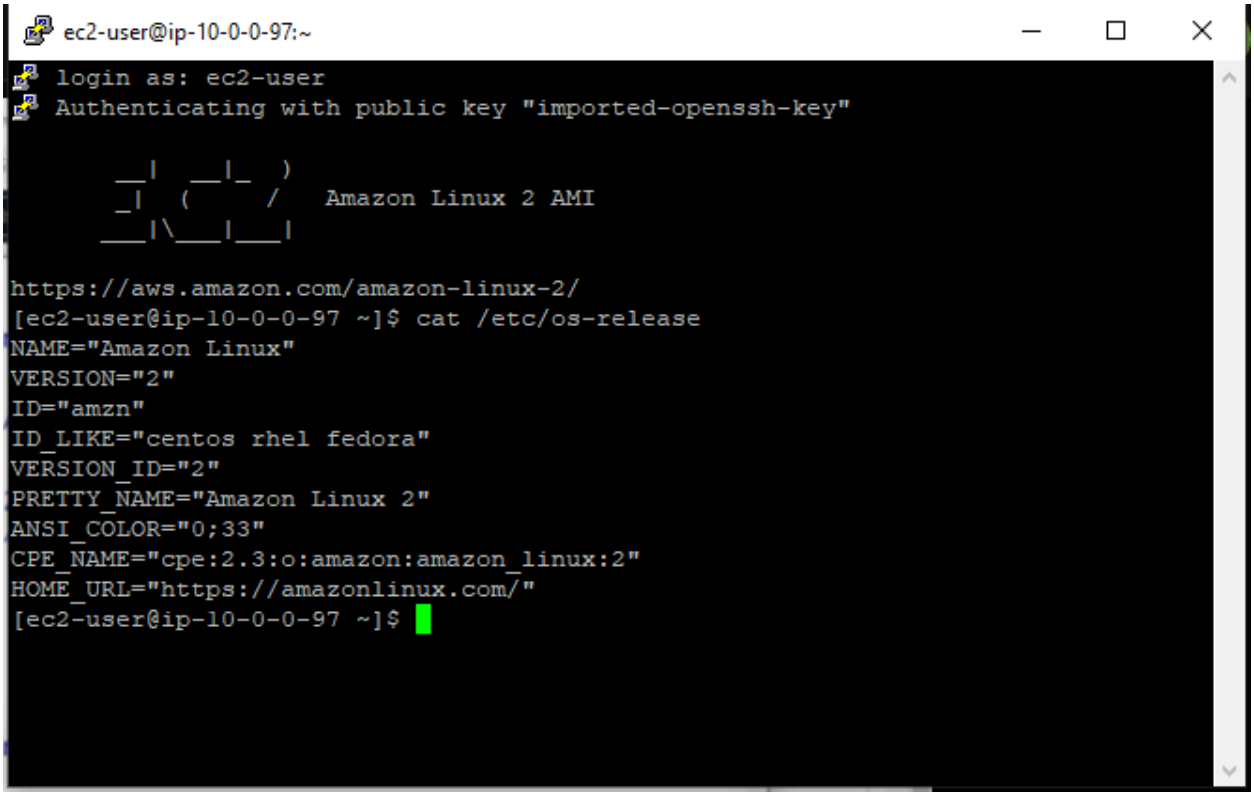


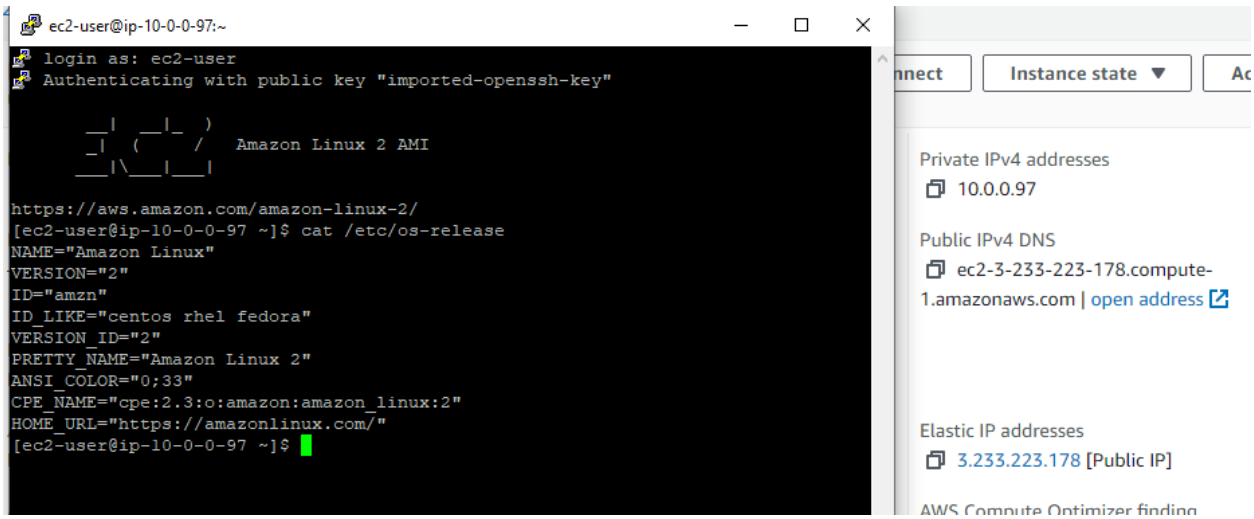
Add file


PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
SSH
Serial
Telnet
Rlogin
SUPDUP
Basic options for your PuTTY session
Specify the destination you want to connect to
Host Name (or IP address)
Port
3.233.223.178
22
Connection type:
SSH
Serial
Other:
Telnet
Load, save or delete a stored session
Saved Sessions
Default Settings
Load
Save
Delete
Close window on exit:
Always
Never
Only on clean exit
About
Help
Open
Cancel


PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
SSH
Serial
Telnet
Rlogin
SUPDUP
Options controlling the connection
Sending of null packets to keep session active
Seconds between keepalives (0 to turn off)
30
Low-level TCP connection options
Disable Nagle's algorithm (TCP_NODELAY option)
Enable TCP keepalives (SO_KEEPALIVE option)
Internet protocol version
Auto
IPv4
IPv6
Logical name of remote host
Logical name of remote host (e.g. for SSH key lookup):
About
Help
Open
Cancel

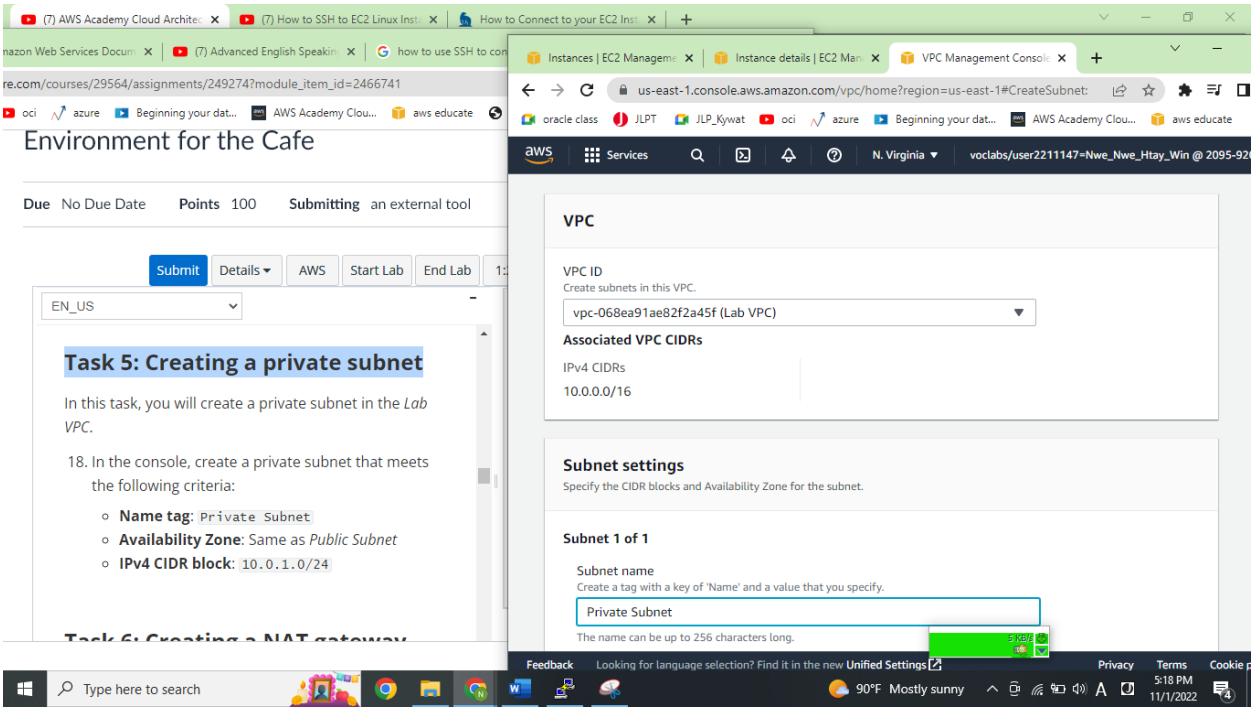

ec2-user@ip-10-0-0-97:~
login as: ec2-user
Authenticating with public key "imported-openssh-key"
Amazon Linux 2 AMI
https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-0-97 ~]$

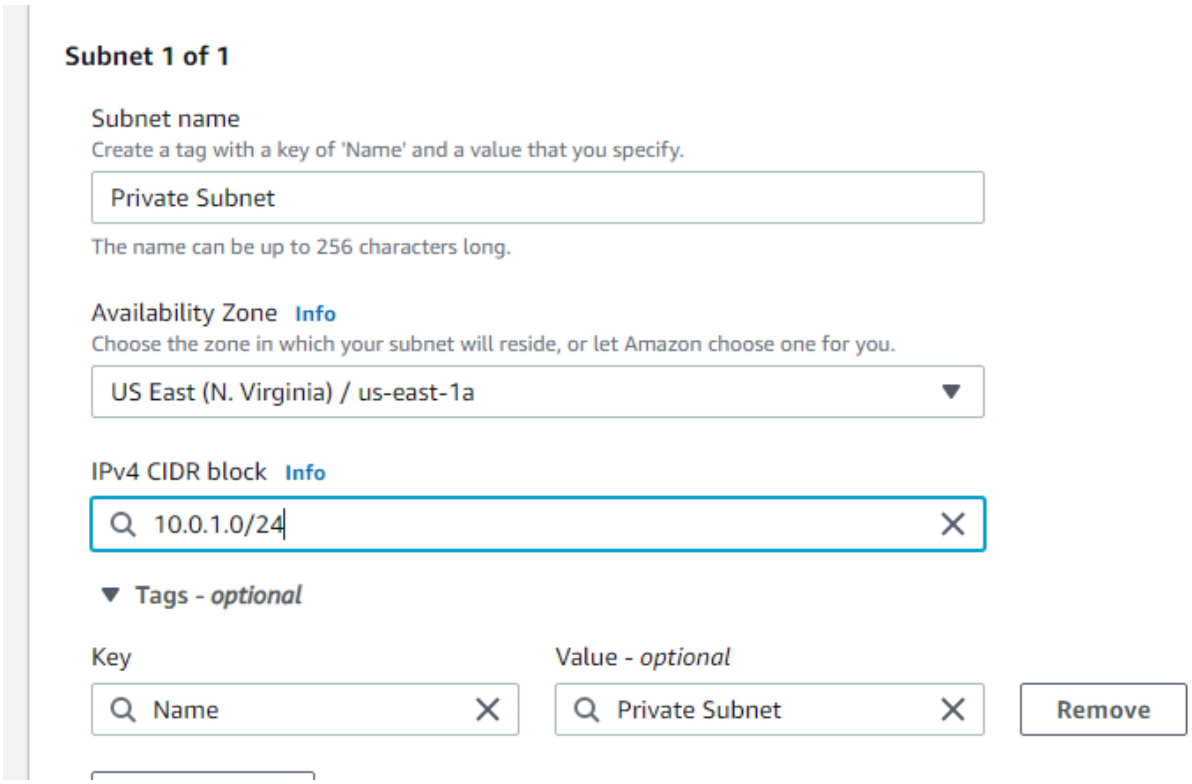




Private ip: 10.0.0.97

Task 5: Creating a private subnet


Environment for the Cafe
Due No Due Date Points 100 Submitting an external tool
Submit Details AWS Start Lab End Lab
EN_US
Task 5: Creating a private subnet
In this task, you will create a private subnet in the Lab VPC.
18. In the console, create a private subnet that meets the following criteria:
Name tag: Private Subnet
Availability Zone: Same as Public Subnet
IPv4 CIDR block: 10.0.1.0/24
VPC
VPC ID
Create subnets in this VPC.
vpc-068ea91ae82f2a45f (Lab VPC)
Associated VPC CIDRs
IPv4 CIDRs
10.0.0.0/16
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.
Private Subnet
The name can be up to 256 characters long.


Subnet 1 of 1
Subnet name
Create a tag with a key of 'Name' and a value that you specify.
Private Subnet
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.
US East (N. Virginia) / us-east-1a
IPv4 CIDR block Info
10.0.1.0/24
Tags - optional
Key
Value - optional
Name
Private Subnet
Remove

Subnets (8) Info

Filter subnets

Name	Subnet ID	State	VPC
Public Subnet	subnet-02dadfe1bd4b73a10	Available	vpc-068e
–	subnet-0a3fd87810c7bb794	Available	vpc-0136
–	subnet-041d702462540a04e	Available	vpc-0136
Private Subnet	subnet-01d6dcd430bae1c47	Available	vpc-068e
–	subnet-0c8f6ab2915cbf24f	Available	vpc-0136
–	subnet-0c508432eded3919a	Available	vpc-0136
–	subnet-0cb944672d6c45ec5	Available	vpc-0136
–	subnet-0348b8ecbbaedc4fe	Available	vpc-0136

NAT gateway

- 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
  - NAT gateways
  - Peering connections
- Security

NAT gateways Info

Actions | Create NAT gateway

Filter NAT gateways

1

Name	NAT gateway ID	Connectivit...

Select a NAT gateway

NAT gateway settings

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

Lab NAT Gateway

The name can be up to 256 characters long.

Subnet
Select a subnet in which to create the NAT gateway.

subnet-02dadfe1bd4b73a10 (Public Subnet)

Connectivity type
Select a connectivity type for the NAT gateway.

- (●) Public
- ( ) Private

Elastic IP allocation ID Info
Assign an Elastic IP address to the NAT gateway.

eipalloc-07df6b2a6319c9a8d

Allocate Elastic IP

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.

Private Subnet Route Table

VPC
The VPC to use for this route table.

vpc-068ea91ae82f2a45f (Lab VPC)

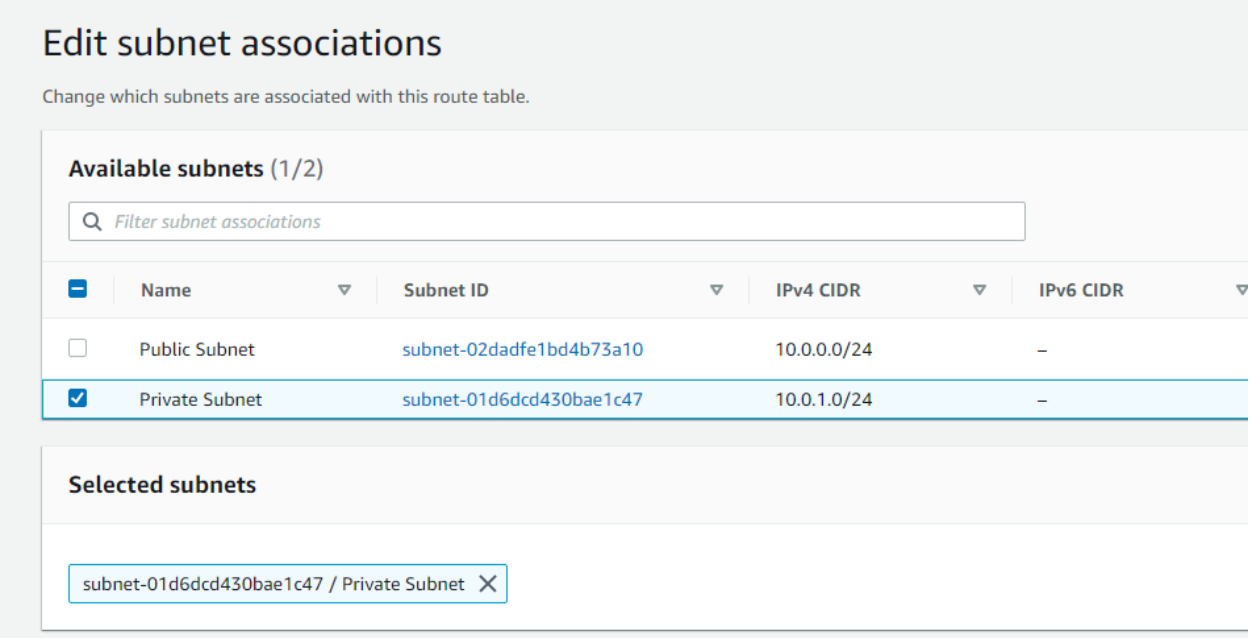
Edit routes

Destination	Target	Status	Propagated	
10.0.0.0/16	local	Active	No	
0.0.0.0/0	nat-	–	No	Remove

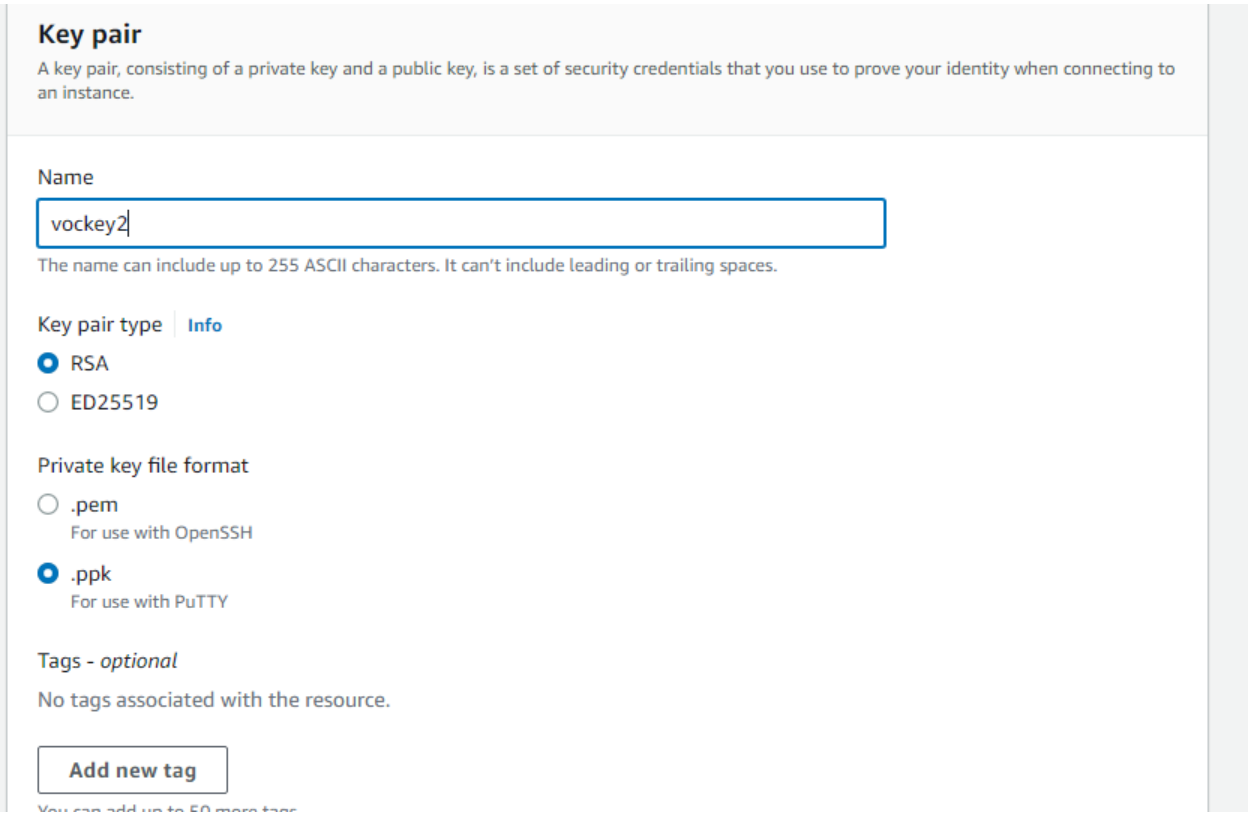
Add route

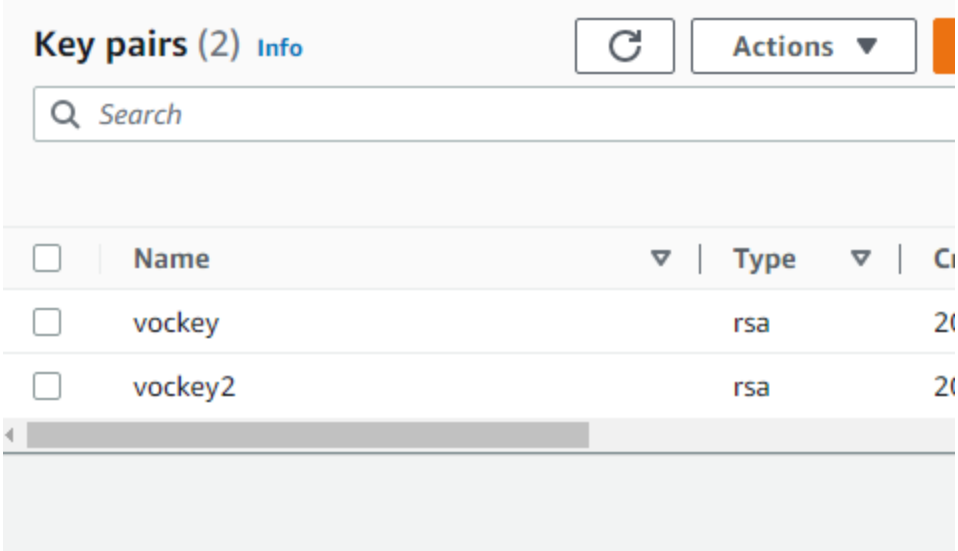
Cancel Preview Save changes

Attach this NAT to private VPC

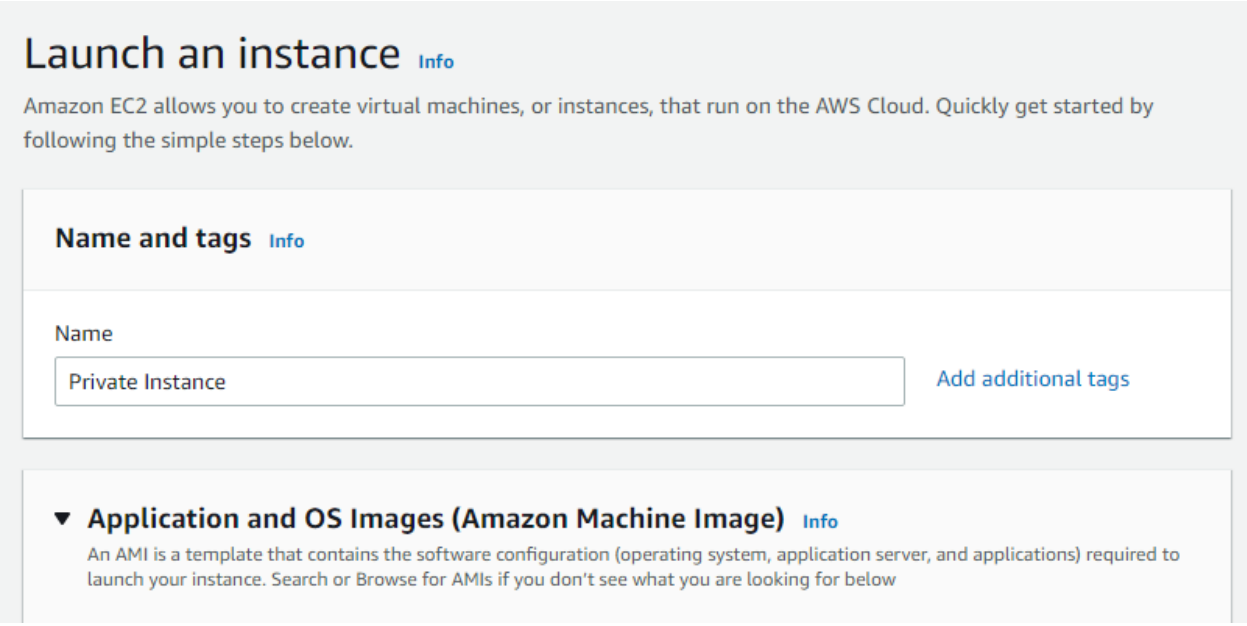


Task 7: Creating an EC2 instance in the private subnet





Let’s create an instance to run in private subnet with vockey2 keypair



Recents | Quick Start

Amazon Linux | macOS | Ubuntu | Windows | Red Hat | S

Browse

Includi
AWS, Ma
the C

Amazon Machine Image (AMI)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type — Free tie
ami-09d3b3274b6c5d4aa (64-bit (x86)) / ami-081dc0707789c2daf (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Amazon Linux 2 Kernel 5.10 AMI 2.0.20221004.0 x86_64 HVM gp2

Architecture: 64-bit (x86)

AMI ID: ami-09d3b3274b6c5d4aa — Verified provider

Instance type

t2.micro — Free tier eligible
Family: t2 1 vCPU 1 GiB Memory
On-Demand Linux pricing: 0.0116 USD per Hour
On-Demand Windows pricing: 0.0162 USD per Hour

Compare instance types

Key pair (login) Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you laun
the instance.

Key pair name - *required*

vockey2

Create new key pa

Network settings Info

VPC - *required* Info

vpc-09f1261cd4ee9b205 (Lab VPC)
10.0.0.0/16

Subnet Info

subnet-0dadcabf0683c0492 Private Subnet
VPC: vpc-09f1261cd4ee9b205 Owner: 209592084157
Availability Zone: us-east-1a IP addresses available: 251
CIDR: 10.0.1.0/24)

Create new subnet

Auto-assign public IP Info

Disable

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 reach your instance.

Auto-assign public IP Info

Disable

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 reach your instance.

- ○ Create security group
- ◉ Select existing security group

Common security groups Info

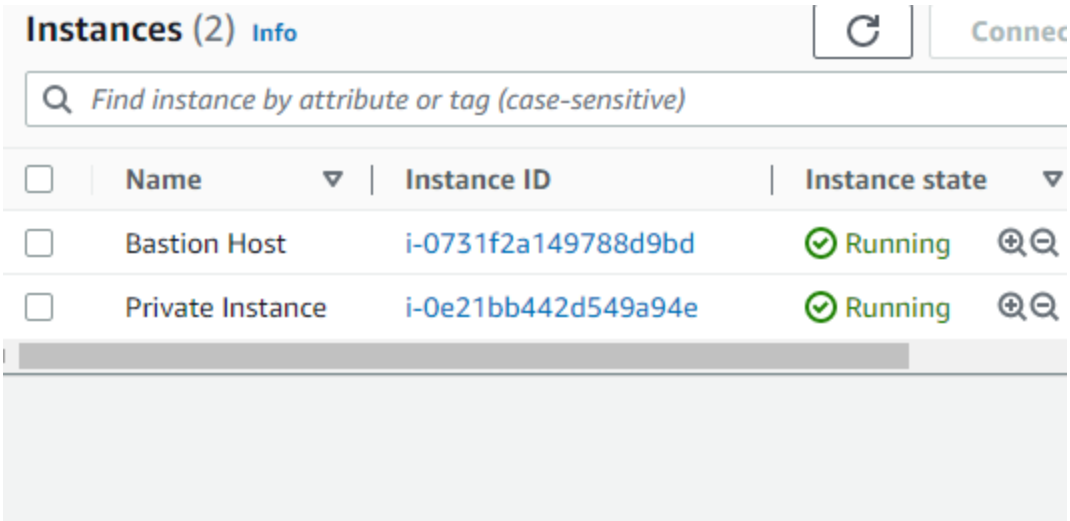
Select security groups

Compare security group rules

Bastion Host SG sg-074ca3bd07ee5f425 ✕
VPC: vpc-09f1261cd4ee9b205

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

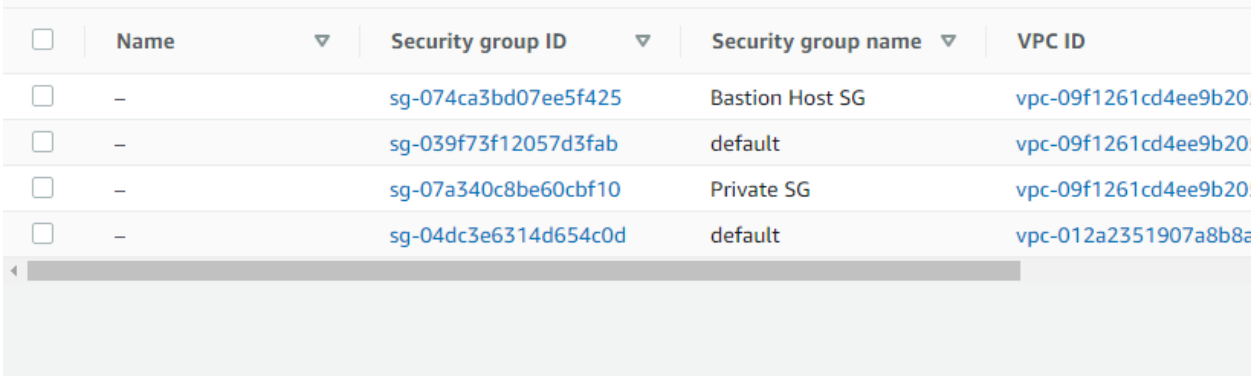
▶ **Advanced network configuration**



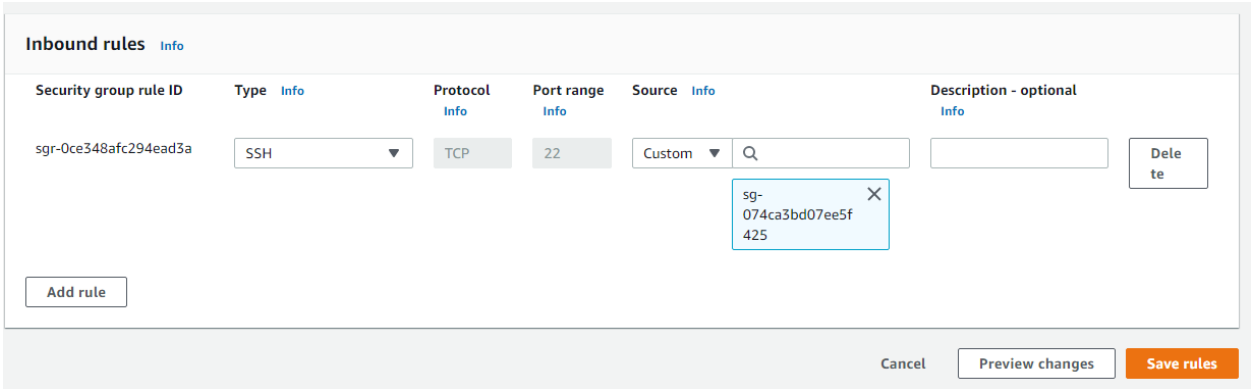
Private Instance Security Group

Create new and source must be Bastion Host SG

Private SG



Its inbound rules



Download pageant.exe

chiark.greenend.org.uk/~sgtatham/putty/latest.html

oracle class | JLPT | JLP_Kywat | oci | azure | Beginning your dat... | AWS A

Source code

Unix source archive

.tar.gz: putty-0.78.tar.gz (signature)

Windows source archive

.zip: putty-src.zip (signature)

git repository

Clone: https://git.tartarus.org/simon/putty.git

gitweb: main | 0.78 release tag

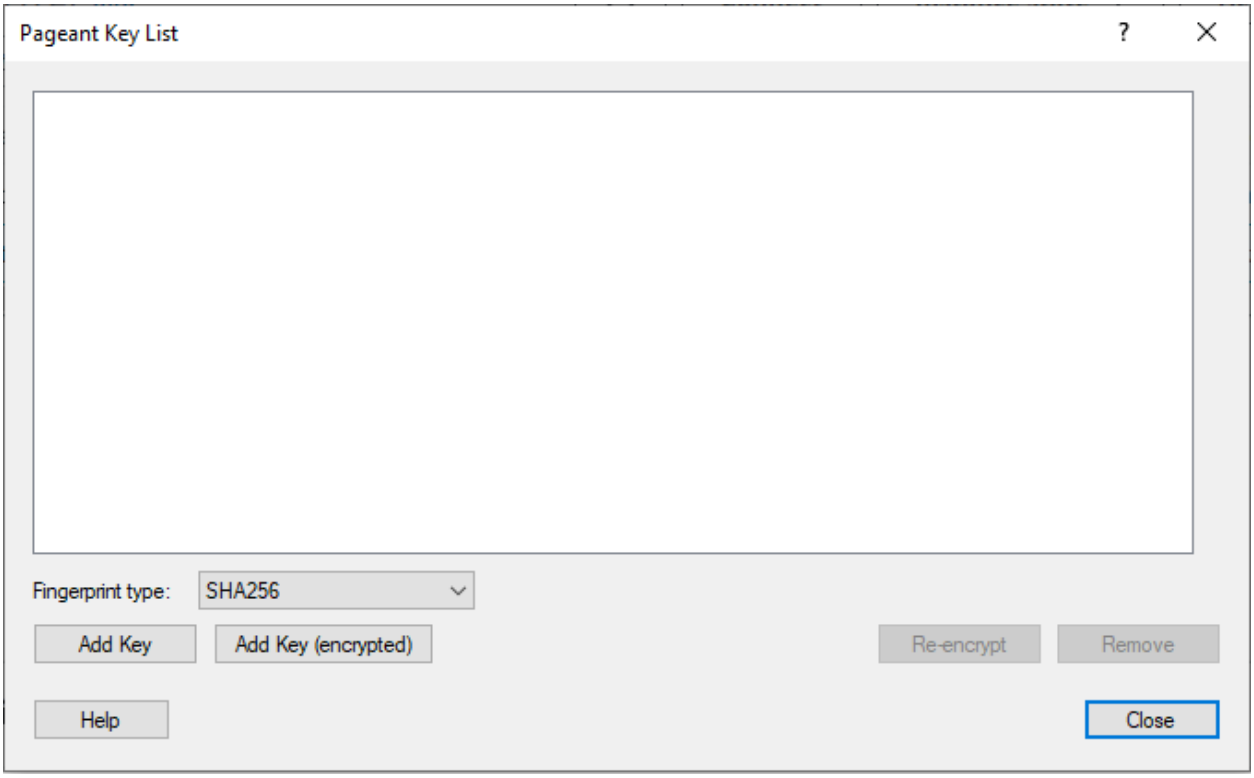
Downloads for 32-bit Windows on Arm

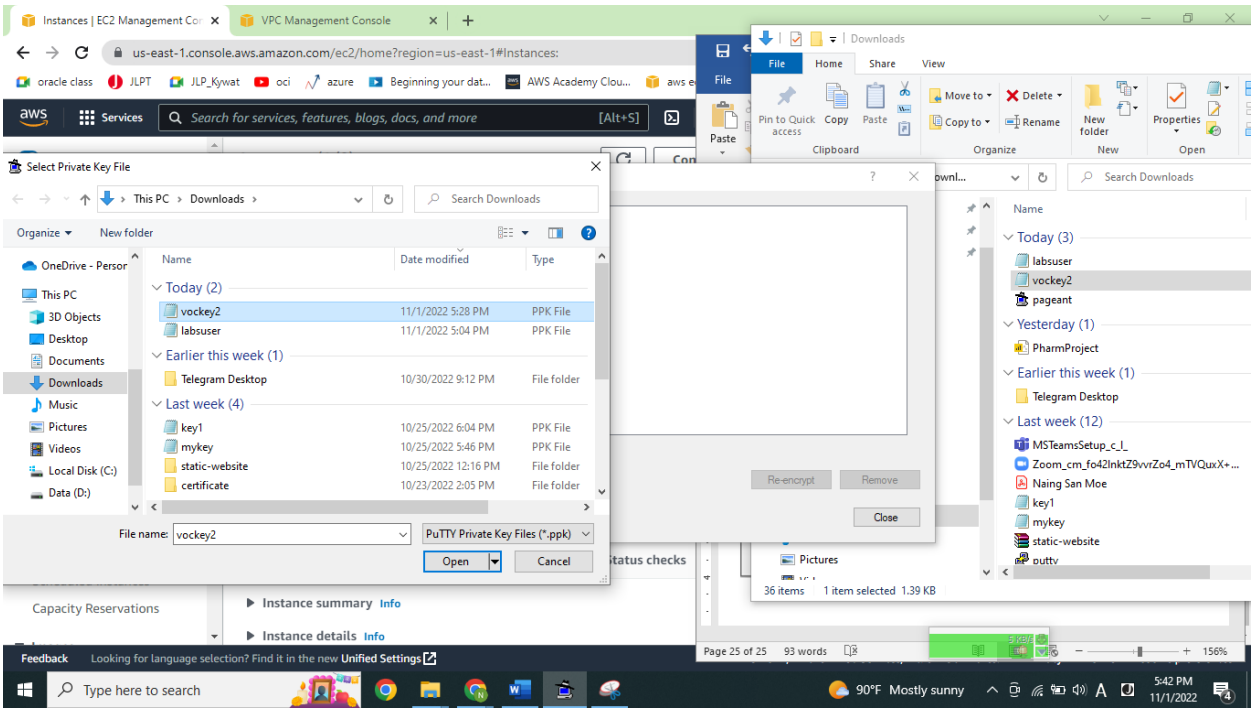
Compiled executable files for 32-bit Windows on Arm. We've had reports that these ca

32-bit Windows on Arm installer

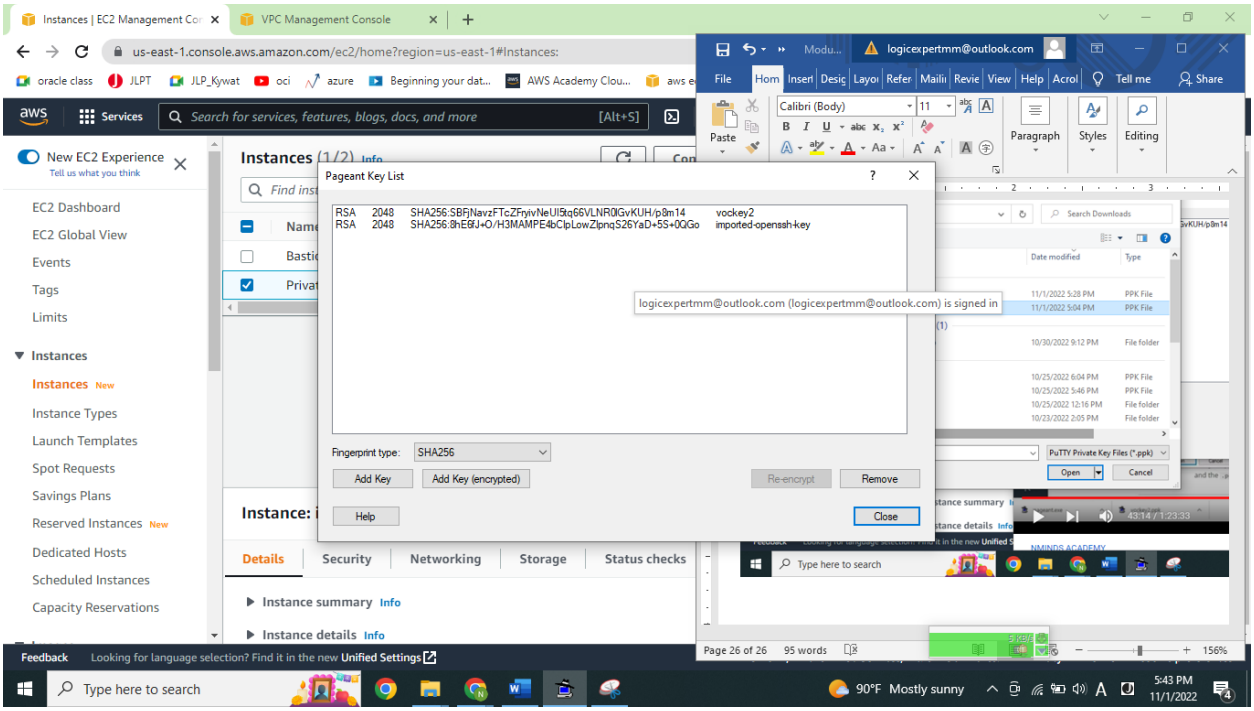
32-bit Arm: putty-arm32-0.78-installer.msi (signature)

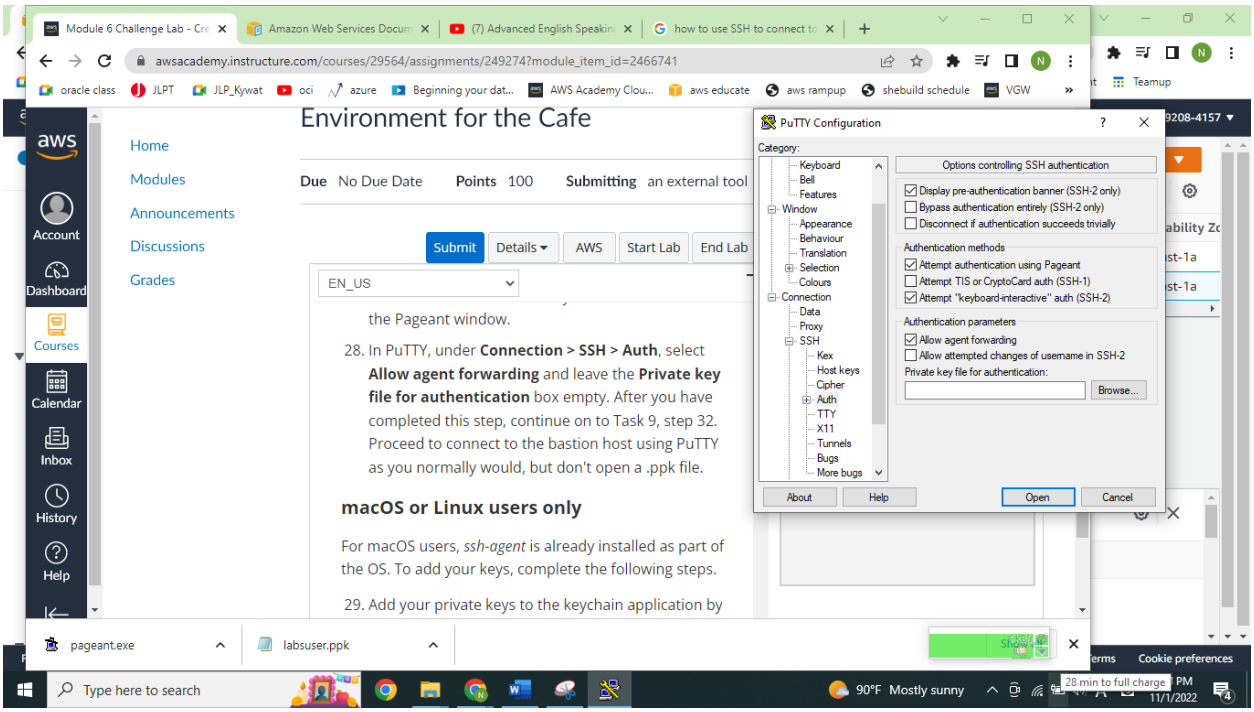
pageant.exe | labsuser.ppk


Pageant Key List
Fingerprint type:
SHA256
Add Key
Add Key (encrypted)
Re-encrypt
Remove
Help
Close


Select Private Key File
This PC › Downloads ›
Search Downloads
Organize
New folder
Name
Date modified
Type
Today (2)
vockey2 11/1/2022 5:28 PM PPK File
labsuser 11/1/2022 5:04 PM PPK File
Earlier this week (1)
Telegram Desktop 10/30/2022 9:12 PM File folder
Last week (4)
key1 10/25/2022 6:04 PM PPK File
mykey 10/25/2022 5:46 PM PPK File
static-website 10/25/2022 12:16 PM File folder
certificate 10/23/2022 2:05 PM File folder
File name: vockey2
PuTTY Private Key Files (*.ppk)
Open
Cancel
Re-encrypt
Remove
Close
Today (3)
labsuser
vockey2
pageant
Yesterday (1)
PharmProject
Earlier this week (1)
Telegram Desktop
Last week (12)
Naing San Moe
key1
mykey
static-website
Instance summary Info
Instance details Info
Capacity Reservations

Add labuser





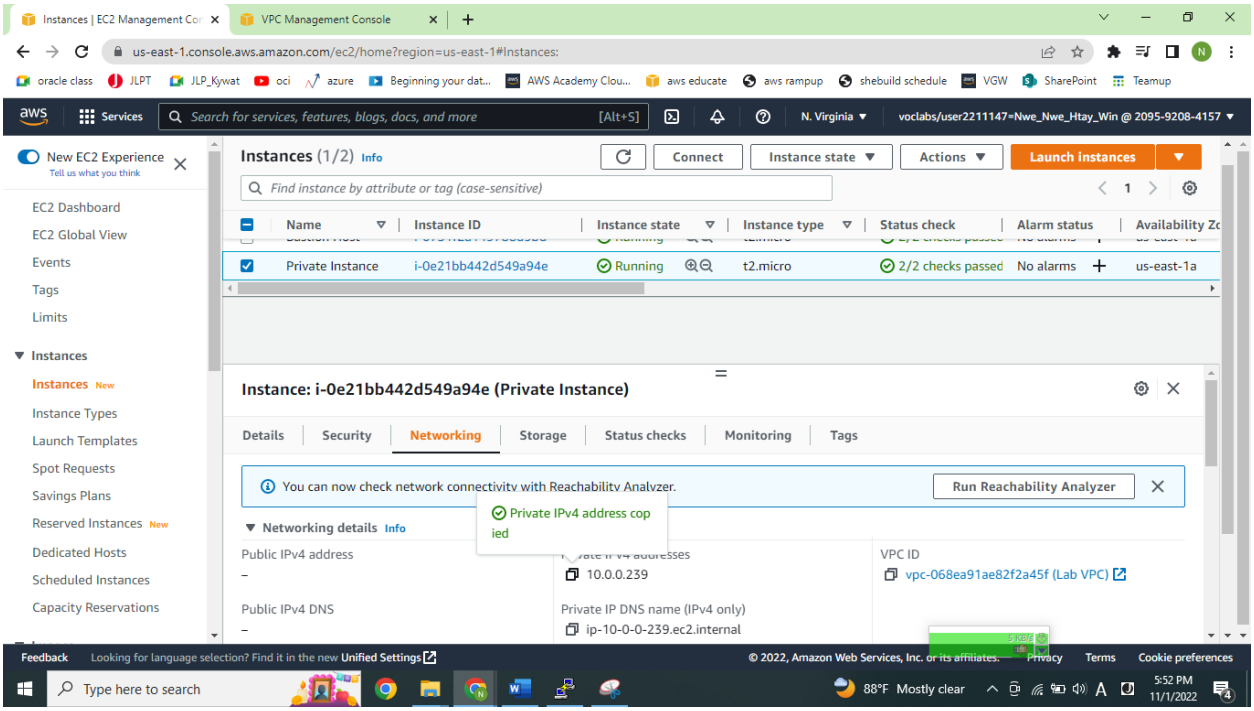
Connect Bashionhost with putty

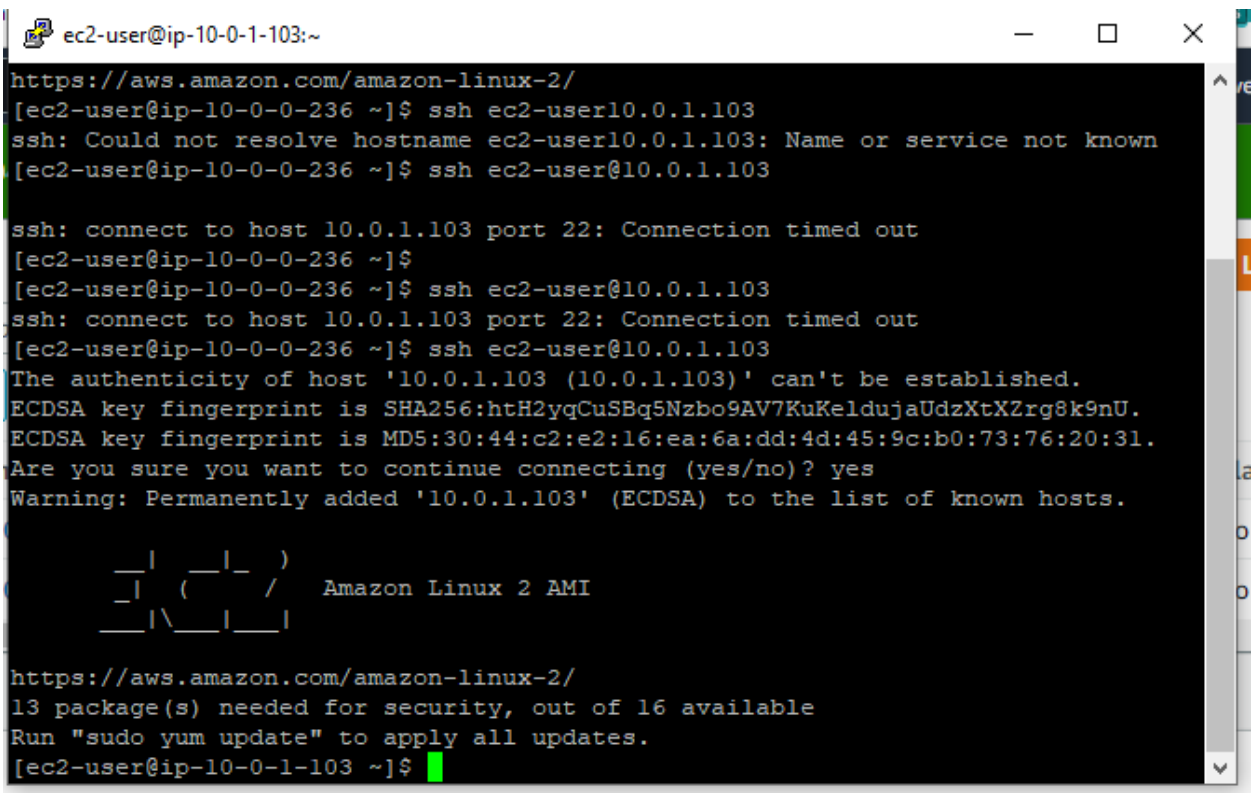
ec2-user@ip-10-0-0-97:~

```
login as: ec2-user
Authenticating with public key "imported-openssh-key" from agent
Last login: Tue Nov  1 10:44:33 2022 from 103.231.95.13

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-0-97 ~]$
```

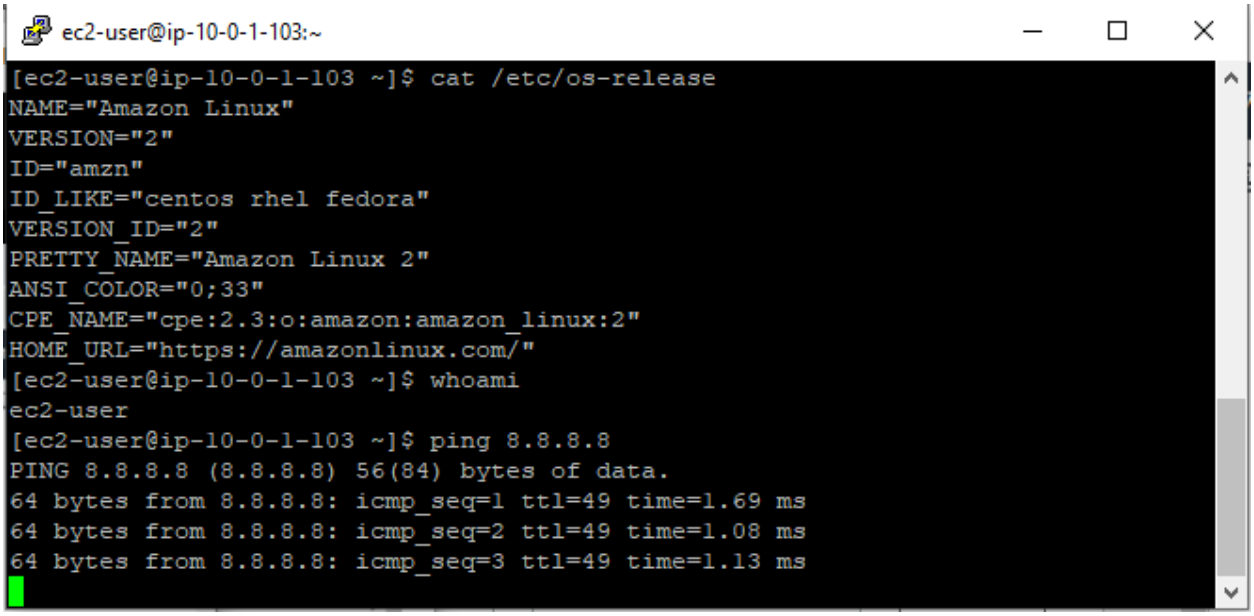
3.233.223.178 - PuTTY

```
login as:
```

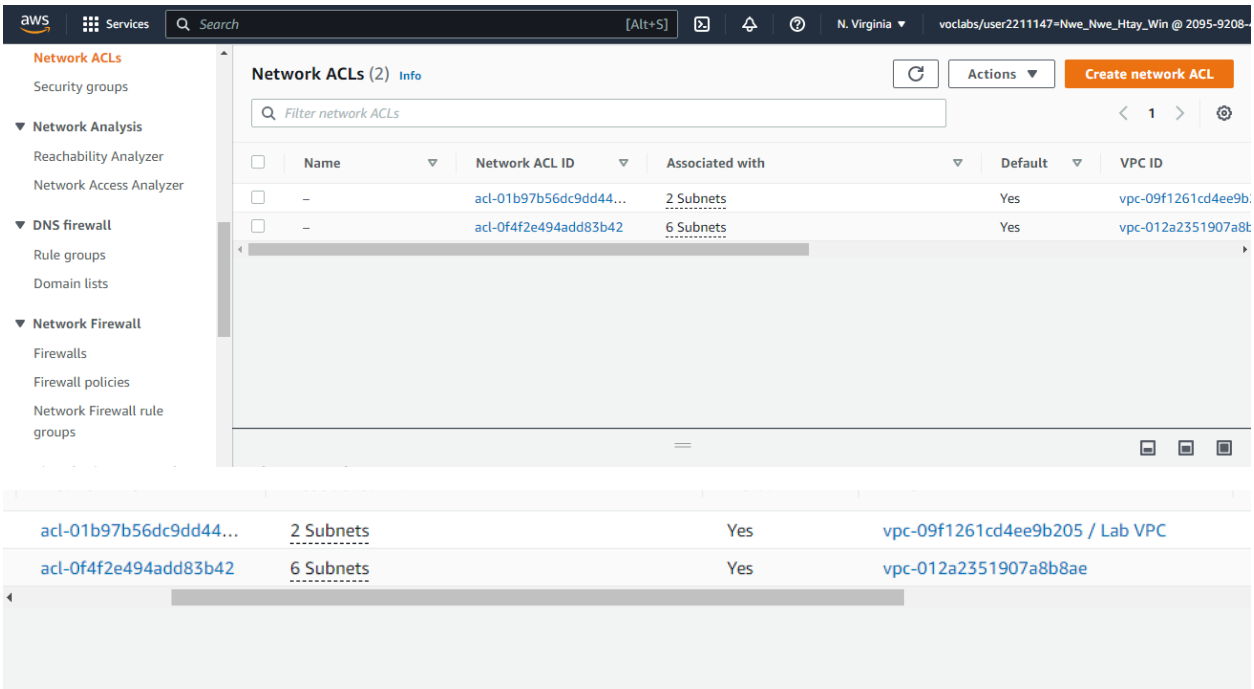




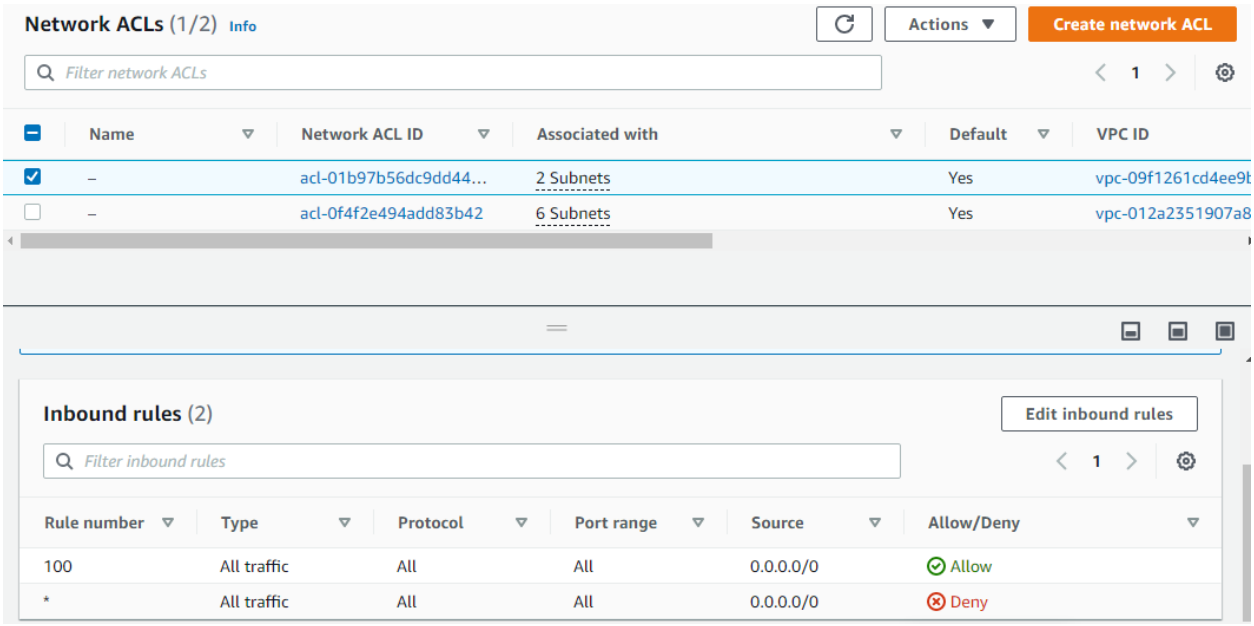
Now ec2-user run at private ID of private Subnet 10.0.1.103



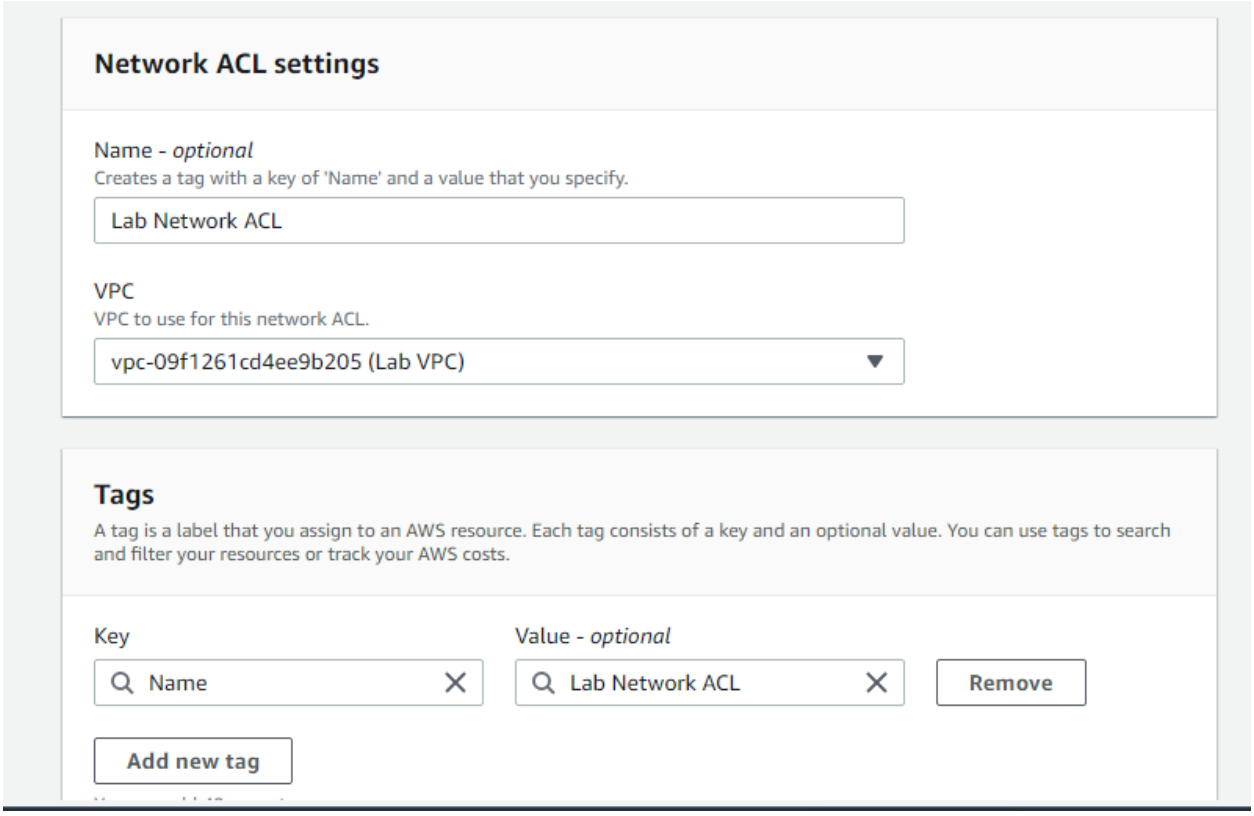
Network ACLs



LabVPC has 2 subnets



Create network ACL



-Default ACL allows all traffic inbound and outbounds

-custom ACl deny all inbound and outbound traffic

VPC > Network ACLs > acl-0b6527bb5262018e1 / Lab Network ACL > Edit inbound rules

Edit inbound rules Info

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

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

Add new rule | Sort by rule number

Cancel | Preview changes | Save changes

Edit outbound rules Info

Outbound rules control the outgoing traffic that's allowed to leave the VPC.

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

Add new rule | Sort by rule number

Cancel | Preview changes | Save changes

Edit subnet associations Info

Change which subnets are associated with this network ACL.

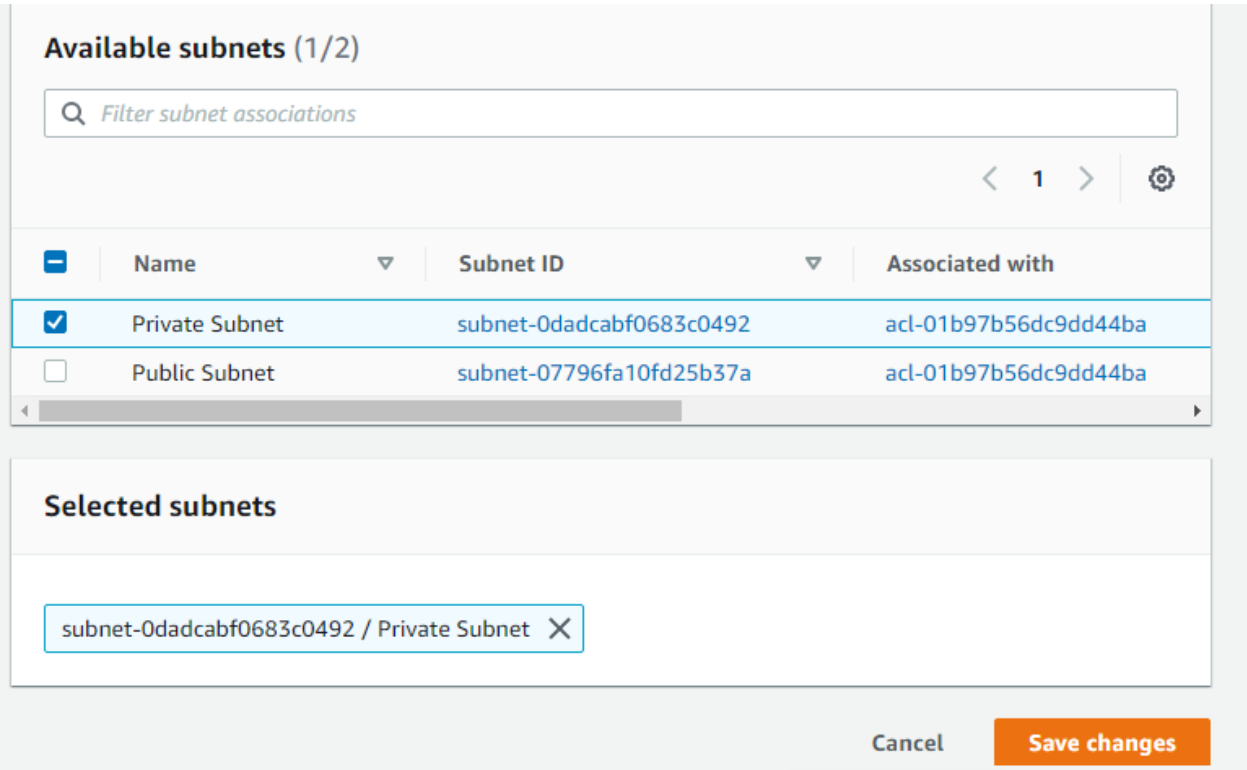
Available subnets (2)

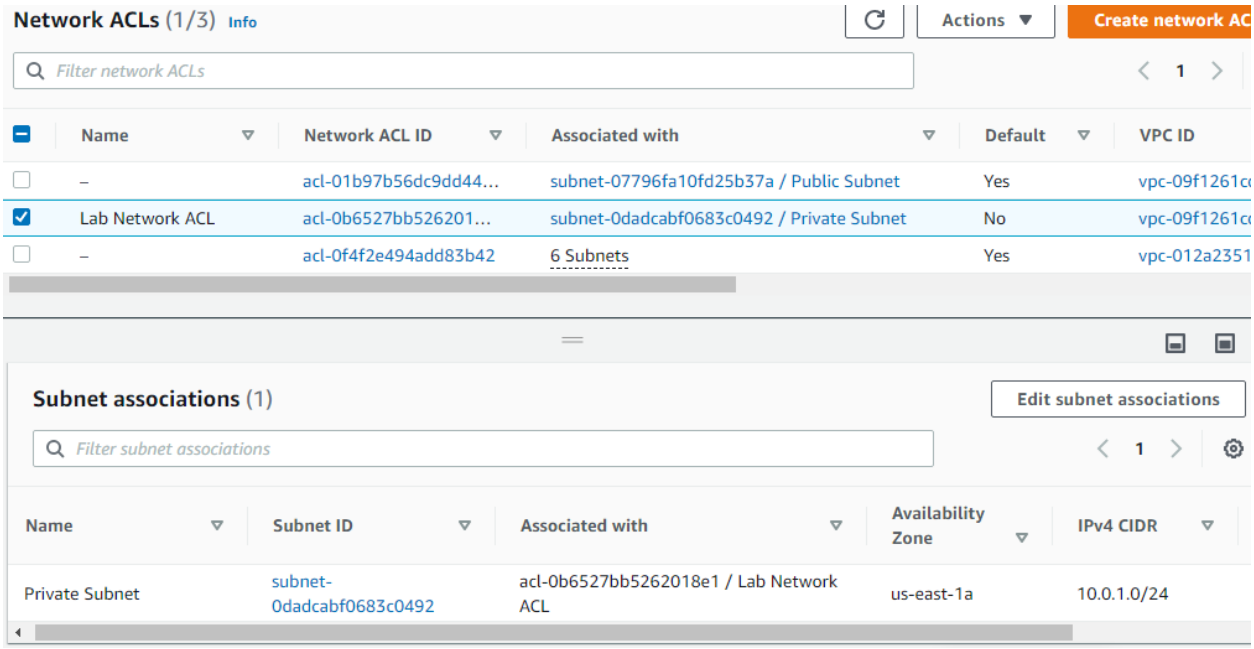
Filter subnet associations

1

Name	Subnet ID	Associated with
Private Subnet	subnet-0dadcabf0683c0492	acl-01b97b56dc9dd44ba
Public Subnet	subnet-07796fa10fd25b37a	acl-01b97b56dc9dd44ba

Cancel | Save changes





Let’s create Test Instance in Public Subnet

EC2 > Instances > Launch an instance

Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name

Test Instance

Add additional tags

Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Network settings Info

VPC - *required* Info

vpc-09f1261cd4ee9b205 (Lab VPC)
10.0.0.0/16

Subnet Info

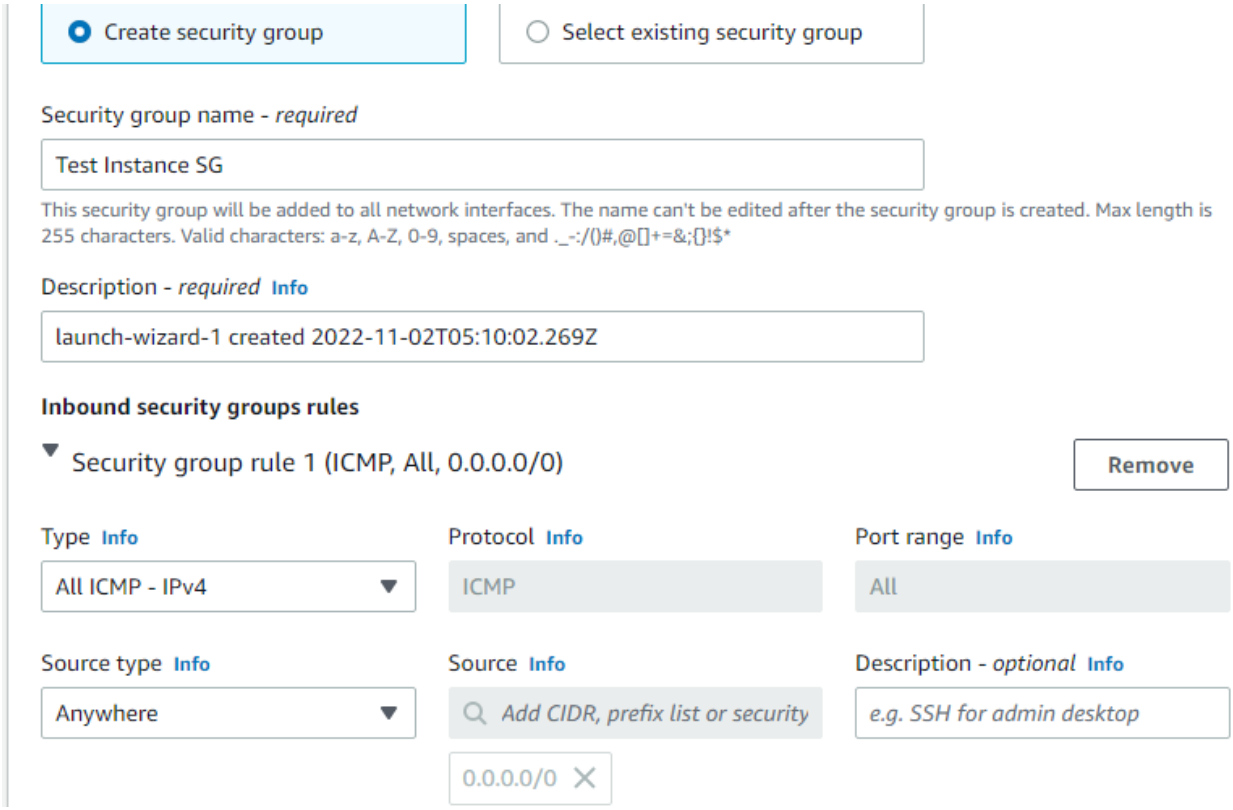
subnet-07796fa10fd25b37a Public Subnet
VPC: vpc-09f1261cd4ee9b205 Owner: 209592084157
Availability Zone: us-east-1a IP addresses available: 249 CIDR: 10.0.0.0/24)

Create new subnet

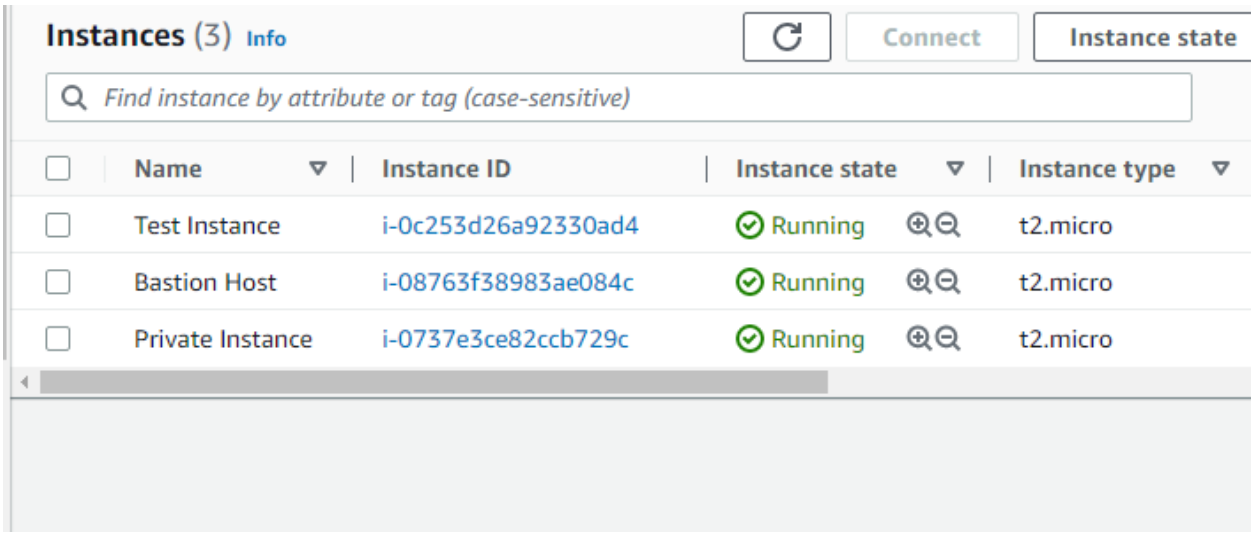
Auto-assign public IP Info

Disable

Firewall (security groups) Info



Proceed without a key

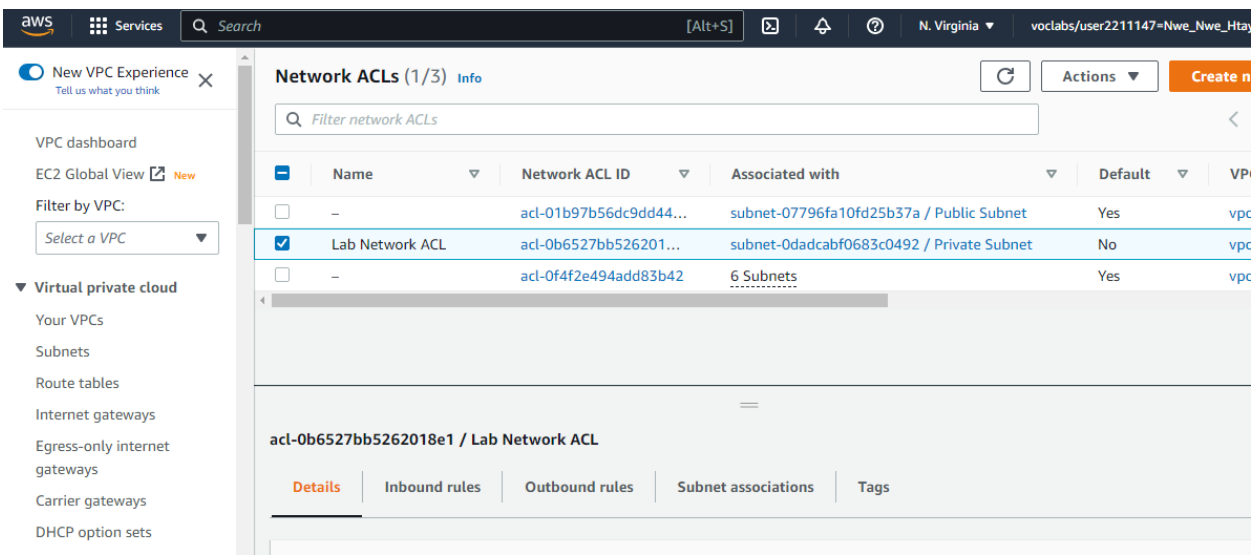


Test instance private ip - 10.0.0.131

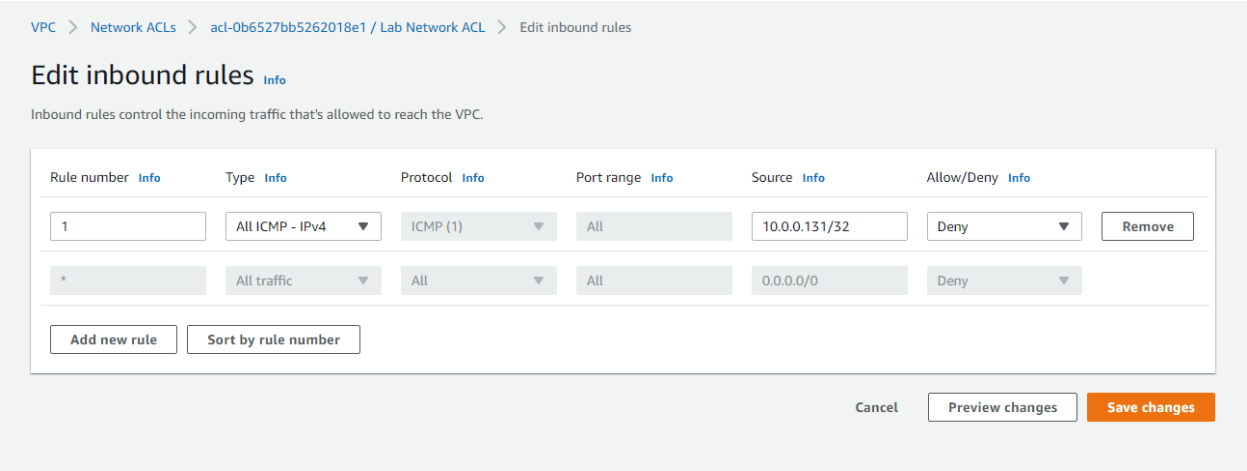
Ping to that ip

```
ec2-user@ip-10-0-1-103:~
64 bytes from 8.8.8.8: icmp_seq=90 ttl=49 time=1.23 ms
64 bytes from 8.8.8.8: icmp_seq=91 ttl=49 time=1.12 ms
64 bytes from 8.8.8.8: icmp_seq=92 ttl=49 time=1.10 ms
64 bytes from 8.8.8.8: icmp_seq=93 ttl=49 time=1.05 ms
64 bytes from 8.8.8.8: icmp_seq=94 ttl=49 time=1.09 ms
64 bytes from 8.8.8.8: icmp_seq=95 ttl=49 time=1.11 ms
64 bytes from 8.8.8.8: icmp_seq=96 ttl=49 time=1.23 ms
64 bytes from 8.8.8.8: icmp_seq=97 ttl=49 time=1.11 ms
^C
--- 8.8.8.8 ping statistics ---
97 packets transmitted, 97 received, 0% packet loss, time 96121ms
rtt min/avg/max/mdev = 1.045/1.144/1.690/0.080 ms
[ec2-user@ip-10-0-1-103 ~]$ ping 10.0.0.131
PING 10.0.0.131 (10.0.0.131) 56(84) bytes of data.
64 bytes from 10.0.0.131: icmp_seq=1 ttl=255 time=0.979 ms
64 bytes from 10.0.0.131: icmp_seq=2 ttl=255 time=0.468 ms
64 bytes from 10.0.0.131: icmp_seq=3 ttl=255 time=0.516 ms
```

Lets change setting of netacl



Deny specific private ip/32



Now, ssh cannot ping because it was blocked.