



Placement Empowerment Program
Cloud Computing and DevOps Centre

Secure Access with a Bastion Host
Set up a bastion host in a public subnet to securely access instances in a private subnet.

Name: Aswin J Department:
ADS



Introduction

In cloud environments, securing access to private instances is crucial. A **Bastion Host** (or Jump Box) is a special-purpose instance that acts as a secure gateway to access EC2 instances in a private subnet. Instead of exposing private instances directly to the internet, users connect to the Bastion Host first and then access the private instances from there.

This setup **enhances security** by limiting direct SSH access to private instances and applying strict security controls.

Overview

We will set up a **Bastion Host** in a **public subnet** that provides controlled SSH access to instances inside a **private subnet**.

What We Will Do?

1. **Create a VPC with a Public and Private Subnet.**
2. **Set Up a Bastion Host** in the Public Subnet.
3. **Launch a Private EC2 Instance** in the Private Subnet.
4. **Configure Secure SSH Access** via the Bastion Host.

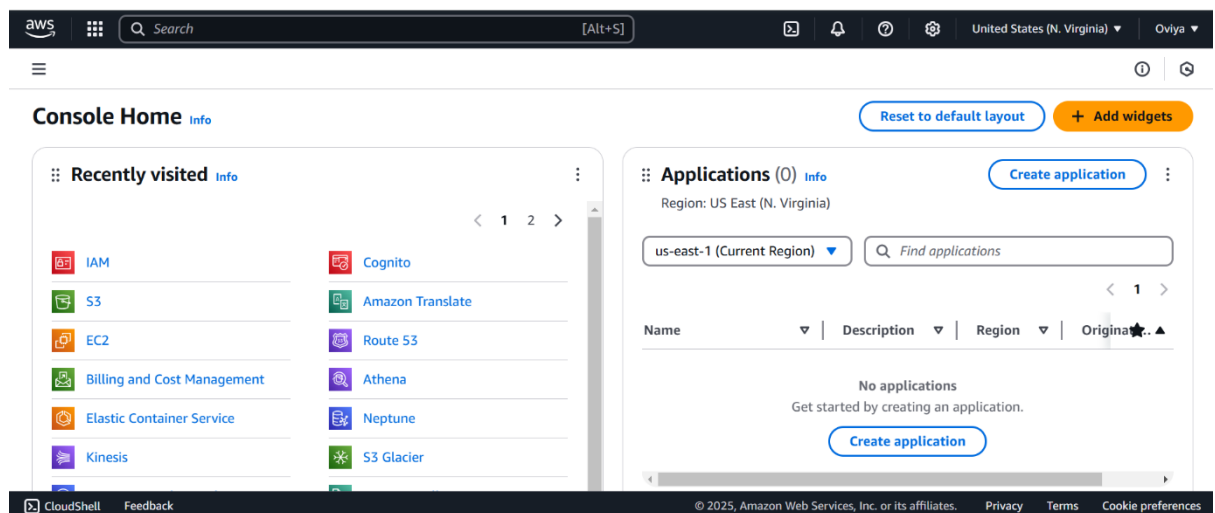
5. **Enhance Security** by restricting SSH access and considering AWS Systems Manager as an alternative.

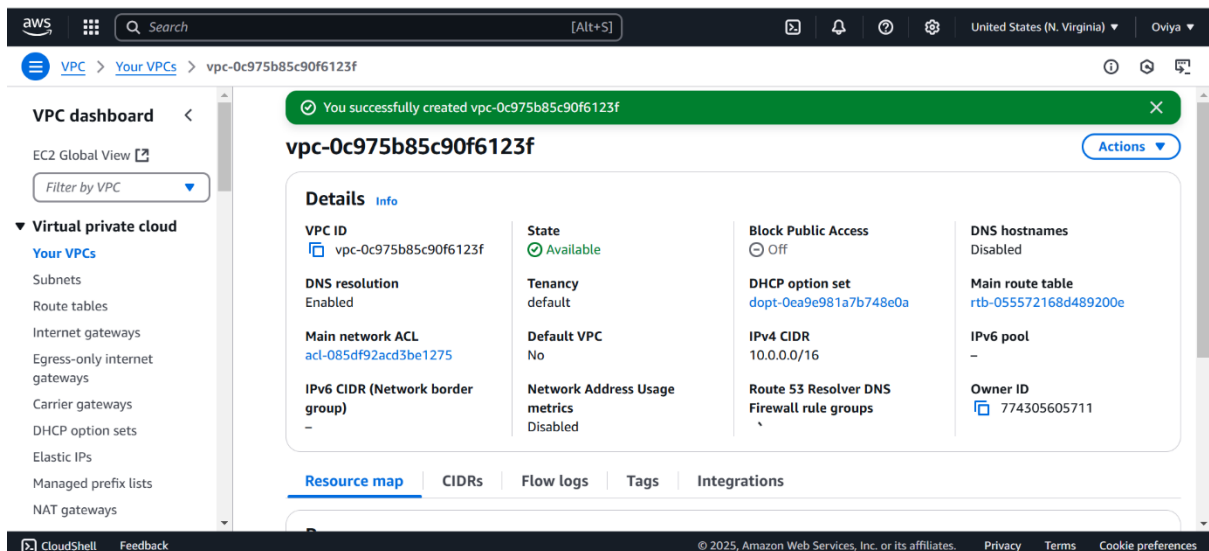
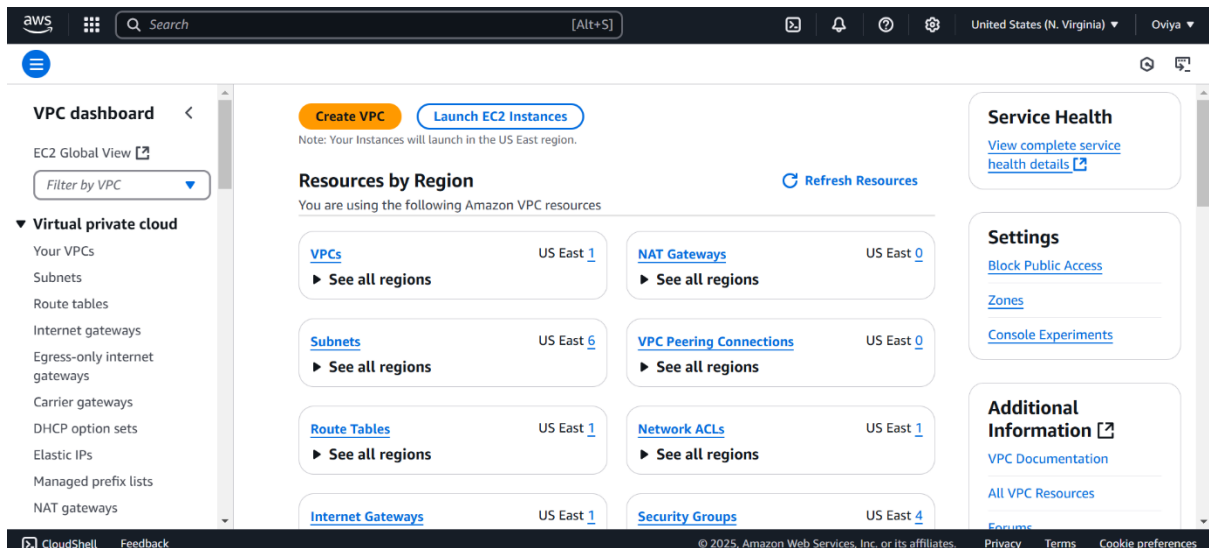
Step 1:

Create a VPC with Public and Private Subnets

1.1 Create a VPC

- Go to AWS Console → VPC Dashboard.
- Click Create VPC and name it MyVPC.
- Set IPv4 CIDR Block: 10.0.0.0/16.
- Click Create VPC.





1.2 Create a Public Subnet

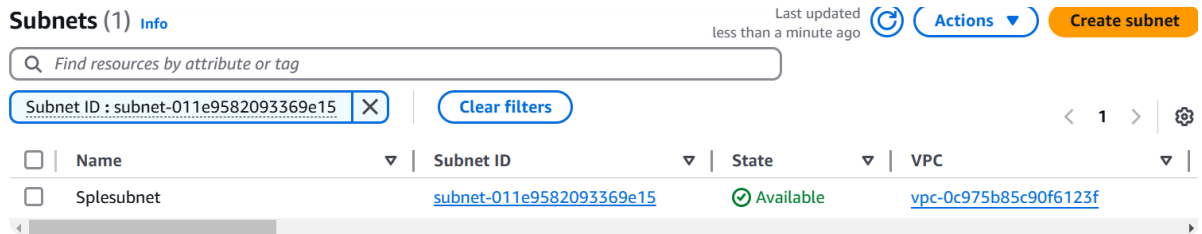
- Go to **Subnets** → **Create Subnet**.
- Select **MyVPC** and set CIDR block 10.0.1.0/24.
- Enable **Auto-Assign Public IP**.

1.3 Create a Private Subnet

- Repeat the same process, but use CIDR block

10.0.2.0/24.

- **Do not enable** Auto-Assign Public IP.

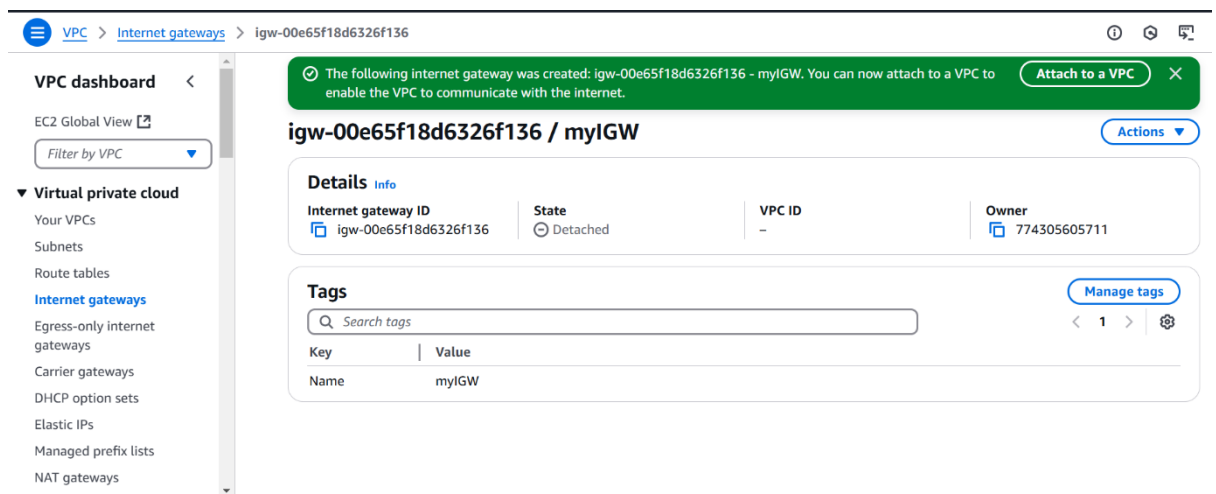


Step 2:

Configure Public Subnet for Internet Access

2.1 Create an Internet Gateway (IGW)

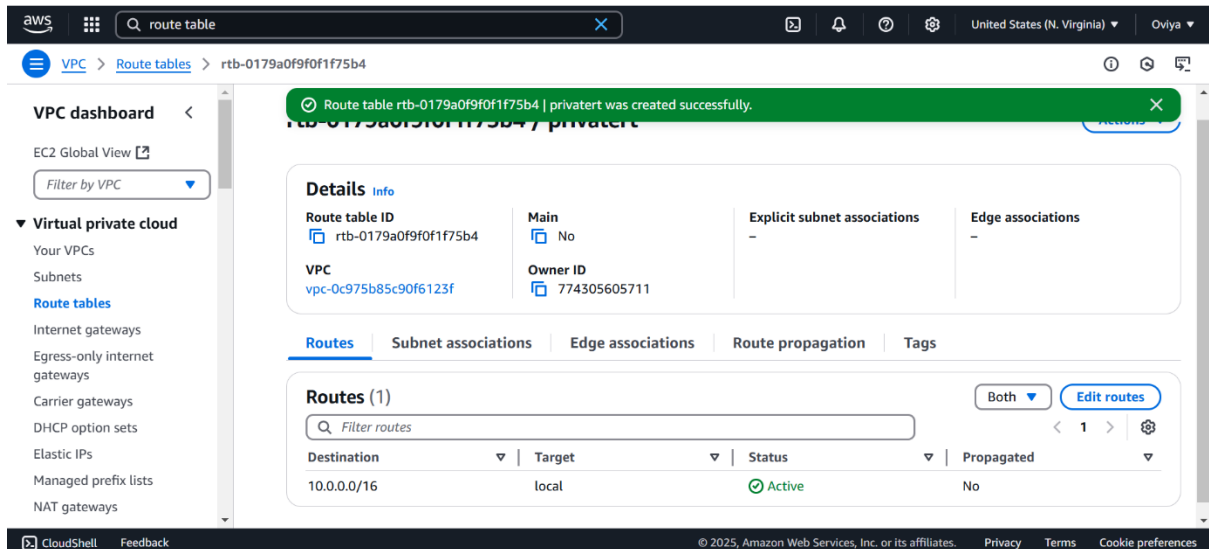
- Go to **Internet Gateways** → Click **Create Internet Gateway**.
- Name it **MyIGW**, attach it to **MyVPC**.



2.2 Update Public Route Table

- Go to **Route Tables** → **Create Route Table**

- Name it **PublicRouteTable**.
- Associate it with **PublicSubnet**.
- Add a route:
 - **Destination:** 0.0.0.0/0
 - **Target:** Internet Gateway (MyIGW)

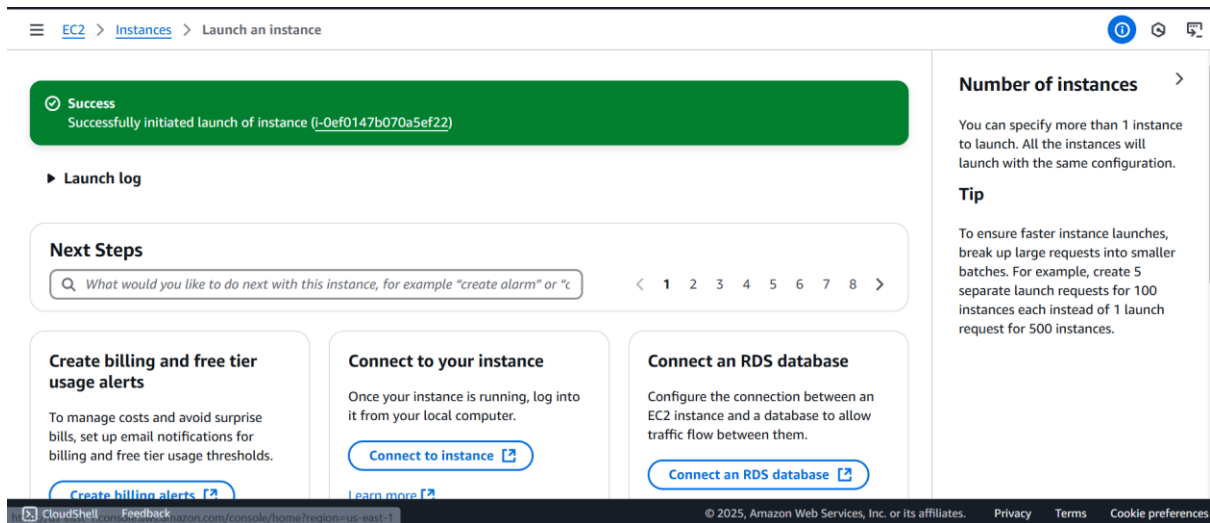


Step 3:

Launch a Bastion Host (Public Subnet)

1. Go to **EC2 Dashboard** → **Launch Instance**.
2. Select **Amazon Linux 2** (or **Ubuntu**).
3. Choose **t2.micro** (**Free Tier Eligible**).
4. Place it in **PublicSubnet** with **Auto-Assign Public IP** enabled.
5. Create a **Security Group (BastionSG)**:
 - Allow **SSH (Port 22)** from **Your IP** (xx.xx.xx.xx/32).
6. Create or use an **existing key pair** (e.g., bastion-key.pem).

7. Click **Launch**.



Step 4:

Launch a Private EC2 Instance

1. Go to **EC2 Dashboard** → **Launch Instance**.
2. Choose **Amazon Linux 2** (or **Ubuntu**).
3. Choose **t2.micro** and place it in **PrivateSubnet**.
4. **Disable Auto-Assign Public IP**.
5. Create a **Security Group (PrivateSG)**:
 - Allow **SSH (Port 22)** only from **Bastion Host's Security Group**.
6. Use the same **key pair** (bastion-key.pem).
7. Click **Launch**.

5.2 SSH from Bastion to Private Instance

- ## 1.Copy the bastion-key.pem file to the Bastion Host:

```
scp -i bastion-key.pem bastion-key.pem ec2-  
user@<bastion-public-ip>:~/
```

- ## 2. Connect to the Bastion Host:

```
ssh -i bastion-key.pem ec2-user@<bastion-public-  
ip>
```

- ### 3. Change permissions for the key file:

```
chmod 400 bastion-key.pem
```

- #### 4.SSH into the Private Instance from the Bastion Host:

```
ssh -i bastion-key.pem ec2-user@<private-  
instance-ip>
```

(Replace <private-instance-ip> with the private IP of your instance.)

```

[ec2-user@ip-10-0-1-218:~] + ~
PS C:\Users\oviya\Downloads> scp -i sam.pem sam.pem ec2-user@54.210.90.216:~/
sam.pem
PS C:\Users\oviya\Downloads> ^C
PS C:\Users\oviya\Downloads> ssh -i sam.pem ec2-user@54.210.90.216
Last login: Wed Feb  5 09:20:14 2025 from 182.74.154.218

      #_
     _###_
    _\#####\
   _\#####\
  _\#####\
 _\#####\
#/_
V/_
A new version of Amazon Linux is available!

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

[ec2-user@ip-10-0-1-218 ~]$ chmod 400 sam.pem
[ec2-user@ip-10-0-1-218 ~]$ ssh -i sam.pem ec2-user@10.0.1.218
The authenticity of host '10.0.1.218 (10.0.1.218)' can't be established.
ECDSA key fingerprint is SHA256:Y6FPLIZSIAtMnwnbl3Yq1SXQPKRyey1HTZPbylOrLY.
ECDSA key fingerprint is MD5:d4:a6:0d:fa:99:92:df:21:ca:36:0f:39:5f:ed:ba:ed.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.1.218' (ECDSA) to the list of known hosts.
Last login: Wed Feb  5 14:18:12 2025 from 223.178.84.112

      #_
     _###_
    _\#####\
   _\#####\
  _\#####\
 _\#####\
#/_
V/_
A new version of Amazon Linux is available!

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

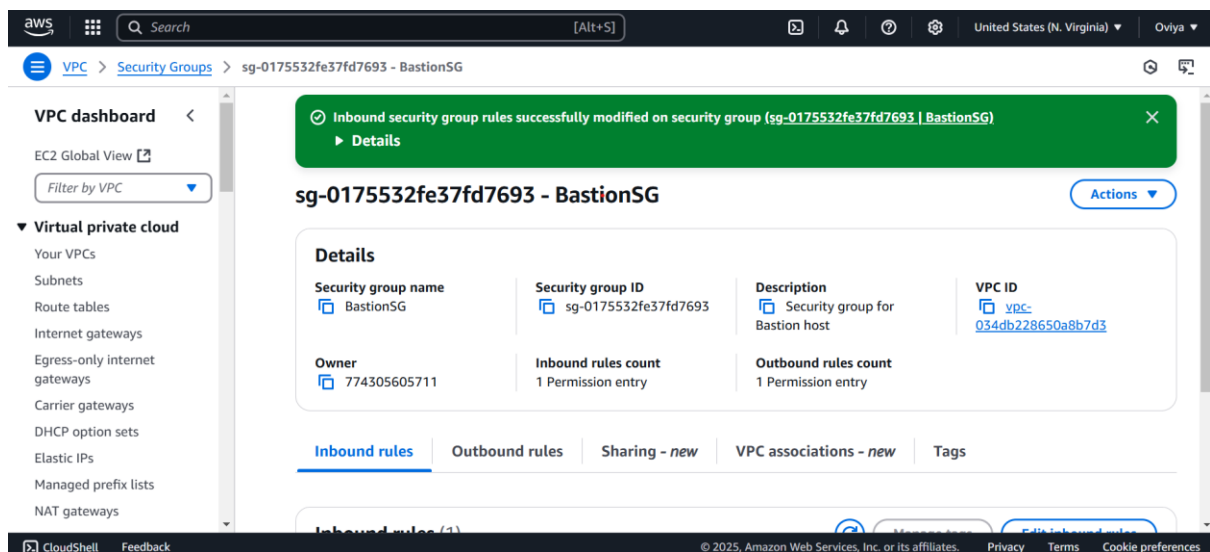
[ec2-user@ip-10-0-1-218 ~]$ |

```

Step 6: Secure Your Bastion Host

6.1 Restrict SSH Access

- **Go to Security Group (BastionSG) → Edit Inbound Rules.**
- **Allow SSH only from your IP address (xx.xx.xx.xx/32) instead of allowing all (0.0.0.0/0)**



6.2 Disable Password Authentication

1. Edit SSH config:

```
sudo nano /etc/ssh/sshd_config
```

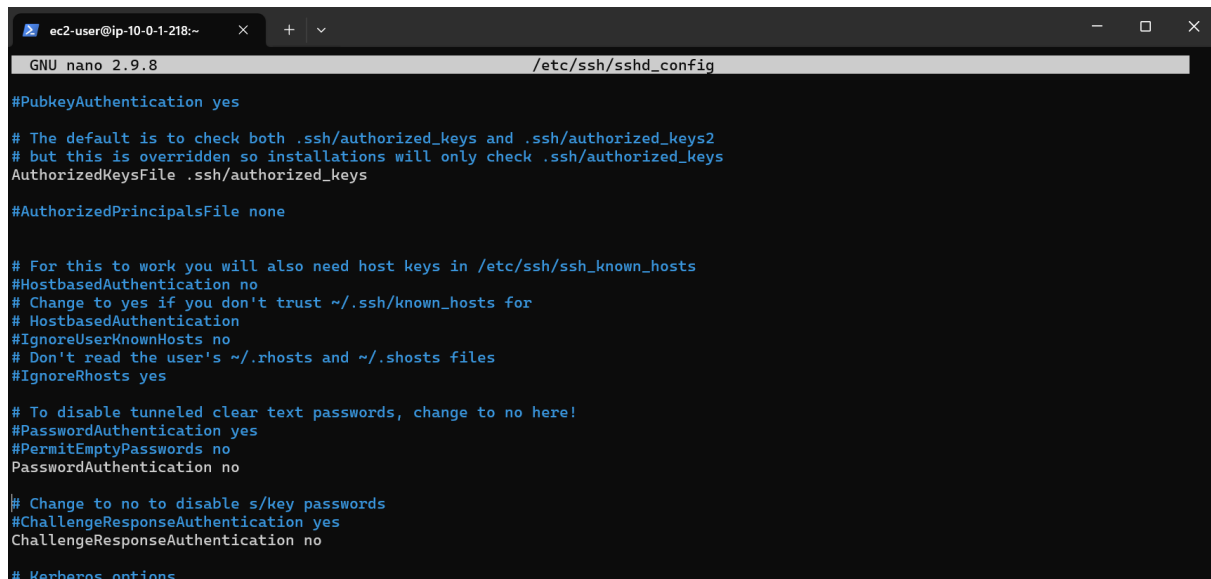
2. Find and update these lines:

```
PasswordAuthentication no
```

```
PermitRootLogin no
```

1. Restart SSH service:

```
sudo systemctl restart sshd
```

A screenshot of a terminal window with a dark background. The window title is 'ec2-user@ip-10-0-1-218:~'. The terminal shows the contents of the '/etc/ssh/sshd_config' file being edited with 'GNU nano 2.9.8'. The configuration includes settings for PubkeyAuthentication (yes), AuthorizedKeysFile (.ssh/authorized_keys), AuthorizedPrincipalsFile (none), HostbasedAuthentication (no), IgnoreUserKnownHosts (no), IgnoreRhosts (yes), PasswordAuthentication (no), PermitEmptyPasswords (no), ChallengeResponseAuthentication (yes), and Kerberos options. The file is partially visible, showing comments and configuration lines.

```
ec2-user@ip-10-0-1-218:~  
GNU nano 2.9.8 /etc/ssh/sshd_config  
#PubkeyAuthentication yes  
# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2  
# but this is overridden so installations will only check .ssh/authorized_keys  
AuthorizedKeysFile .ssh/authorized_keys  
#AuthorizedPrincipalsFile none  
  
# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts  
#HostbasedAuthentication no  
# Change to yes if you don't trust ~/.ssh/known_hosts for  
# HostbasedAuthentication  
#IgnoreUserKnownHosts no  
# Don't read the user's ~/.rhosts and ~/.shosts files  
#IgnoreRhosts yes  
  
# To disable tunneled clear text passwords, change to no here!  
#PasswordAuthentication yes  
#PermitEmptyPasswords no  
PasswordAuthentication no  
  
# Change to no to disable s/key passwords  
#ChallengeResponseAuthentication yes  
ChallengeResponseAuthentication no  
  
# Kerberos options
```

Step 7:

Alternative - Use AWS Systems Manager (SSM) Instead of SSH

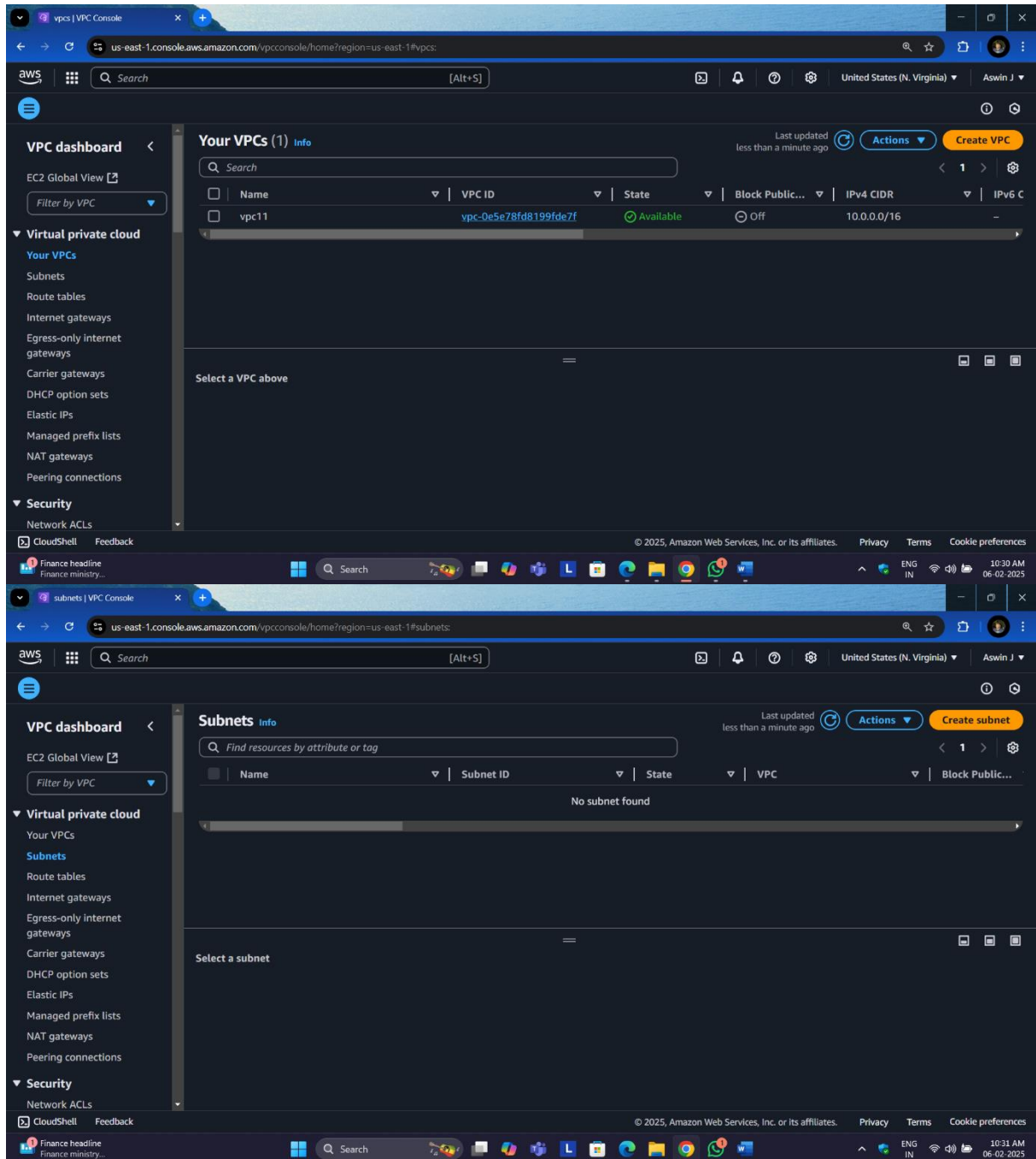
1. **Attach SSM Managed Policy to EC2 IAM Role** (AmazonSSMManagedInstanceCore).
2. **Enable SSM Agent** (Pre-installed on Amazon Linux & Ubuntu).
3. Use **AWS Systems Manager > Session Manager** to connect to instances without SSH.

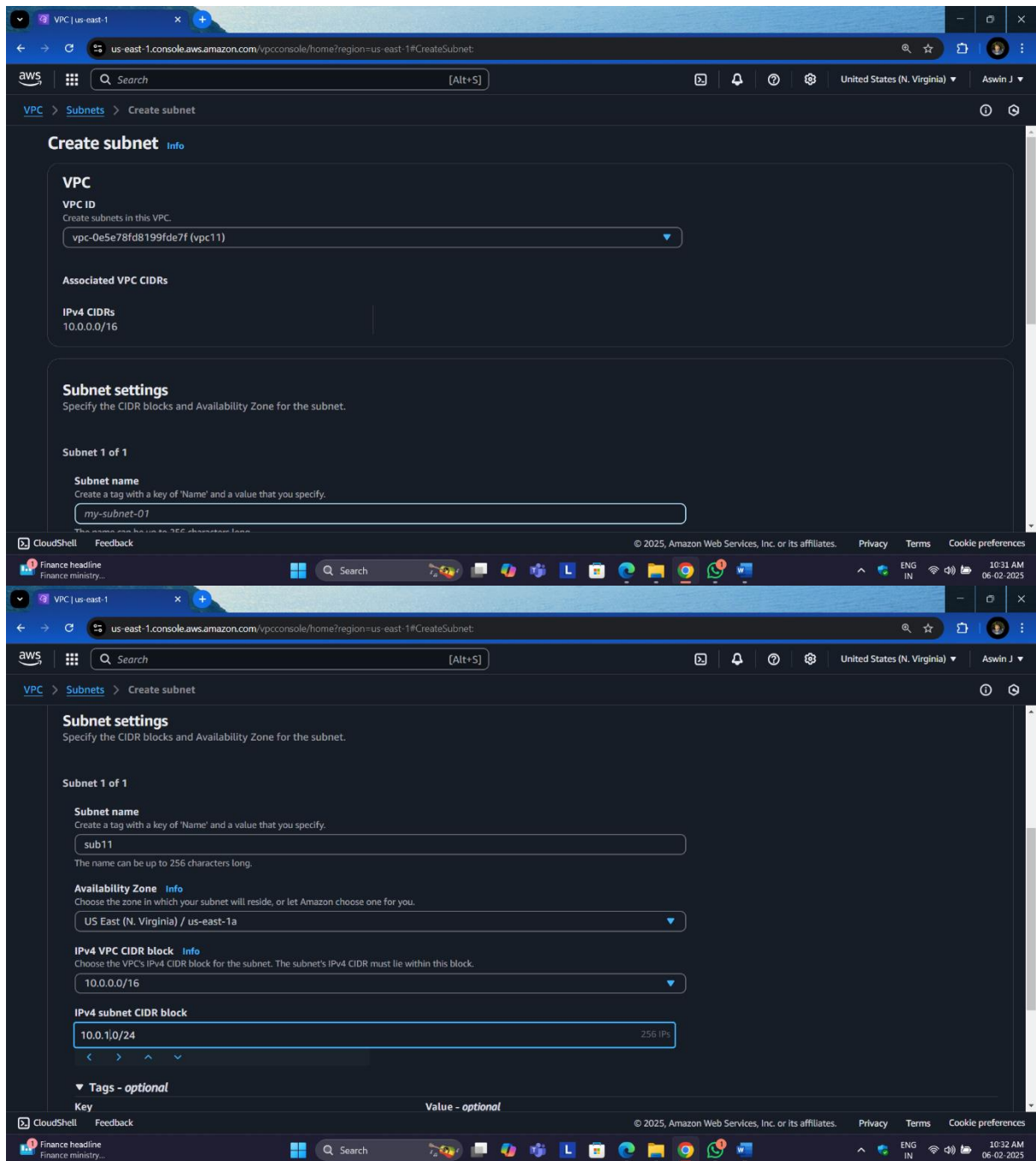
Conclusion

Using a Bastion Host significantly enhances security by acting as a controlled access point to private instances. This setup prevents direct internet exposure, enforces security group rules, and allows monitoring/logging of access.

For even better security, consider eliminating SSH and using AWS Systems Manager (SSM) Session Manager instead.

Practices:





subnets | VPC Console

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#subnets:subnetid=subnet-0a532a021384f1082

Search [Alt+S]

United States (N. Virginia) Aswin J

VPC dashboard

EC2 Global View

Filter by VPC

Virtual private cloud

Subnets

Route tables

Internet gateways

Egress-only internet gateways

Carrier gateways

DHCP option sets

Elastic IPs

Managed prefix lists

NAT gateways

Peering connections

Security

Network ACLs

You have successfully created 1 subnet: subnet-0a532a021384f1082

Subnets (1) Info

Find resources by attribute or tag

Subnet ID: subnet-0a532a021384f1082

Clear filters

1

Subnet ID Name Subnet ID State VPC Block Public...

sub11 subnet-0a532a021384f1082 Available vpc-0e5e78fd8199fde7f | vpc11 Off

Select a subnet

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

28°C Mostly sunny

Search

10:32 AM 06-02-2025

VPC | us-east-1

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#CreateSubnet

Search [Alt+S]

United States (N. Virginia) Aswin J

VPC > Subnets > Create subnet

Create subnet Info

VPC

VPC ID

Create subnets in this VPC.

Select a VPC

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Select a VPC first to create new subnets.

Add new subnet

Cancel Create subnet

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

28°C Mostly sunny

Search

10:33 AM 06-02-2025

VPC | us-east-1

us-east-1.console.aws.amazon.com/vpconsole/home?region=us-east-1#CreateSubnet

Search [Alt+S]

United States (N. Virginia) Aswin J

VPC > Subnets > Create subnet

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

sub12

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 VPC CIDR block Info

Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

10.0.0.0/16

IPv4 subnet CIDR block

10.0.2.0/24 256 IPs

Tags - optional

Key

Value - optional

Q Name X Q sub12 X Remove

Add new tag

You can add 49 more tags.

Remove

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

28°C Mostly sunny

subnets | VPC Console

us-east-1.console.aws.amazon.com/vpconsole/home?region=us-east-1#subnets:subnetId=subnet-0b101ec1e08de4df7

Search [Alt+S]

United States (N. Virginia) Aswin J

VPC dashboard

EC2 Global View

Filter by 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

NAT gateways

Peering connections

Security

Network ACLs

You have successfully created 1 subnet: subnet-0b101ec1e08de4df7

Subnets (1) Info

Last updated less than a minute ago Actions Create subnet

Find resources by attribute or tag

Subnet ID: subnet-0b101ec1e08de4df7 Clear filters

	Name	Subnet ID	State	VPC	Block Public...
<input type="checkbox"/>	sub12	subnet-0b101ec1e08de4df7	Available	vpc-0e5e78fd8199fde7f vpc11	Off

Select a subnet

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

28°C Mostly sunny

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#RouteTableDetails:routeTableId=rtb-093992e48235cb40a

Search [Alt+S]

United States (N. Virginia) Aswin J

VPC > Route tables > rtb-093992e48235cb40a

VPC dashboard

EC2 Global View

Filter by 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

NAT gateways

Peering connections

Security

Network ACLs

Route table rtb-093992e48235cb40a | r11 was created successfully.

rtb-093992e48235cb40a / r11

Actions

Details Info

Route table ID

rtb-093992e48235cb40a

VPC

vpc-0e5e78fd8199fde7f | vpc11

Main

No

Owner ID

183631322302

Explicit subnet associations

-

Edge associations

-

Routes

Subnet associations

Edge associations

Route propagation

Tags

Routes (1)

Filter routes

Both

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#EditRoutes:routeTableId=rtb-093992e48235cb40a

Search [Alt+S]

United States (N. Virginia) Aswin J

VPC > Route tables > rtb-093992e48235cb40a > Edit routes

Edit routes

Destination

10.0.0.0/16

Target

local

Q local

Internet Gateway

Q igw-

Status

Active

Propagated

No

Q 0.0.0.0/0

Remove

Add route

Cancel

Preview

Save changes

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

Search [Alt+S]

United States (N. Virginia) Aswin J

VPC dashboard

EC2 Global View

Filter by 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

NAT gateways

Peering connections

Security

Network ACLs

Internet gateways info

Search

Name Internet gateway ID State VPC ID

No internet gateways found in this Region

Select an Internet gateway above

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

28°C Mostly sunny

Search

10:50 AM 06-02-2025

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#RouteTableDetails:routeTableId=rtb-093992e48235cb40a

Search [Alt+S]

United States (N. Virginia) Aswin J

VPC dashboard

EC2 Global View

Filter by 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

NAT gateways

Peering connections

Security

Network ACLs

Updated routes for rtb-093992e48235cb40a / r11 successfully

Details

rtb-093992e48235cb40a / r11

Actions

Details info

Route table ID

rtb-093992e48235cb40a

Main

No

Explicit subnet associations

Edge associations

VPC

vpc-0e5e78fd8199fde7f | vpc11

Owner ID

183631322302

Routes

Subnet associations

Edge associations

Route propagation

Tags

Routes (2)

Filter routes

Both Edit routes

Destination Target Status Propagated

0.0.0.0/0 igw-Deebe55627868bb15 Active No

10.0.0.0/16 local Active No

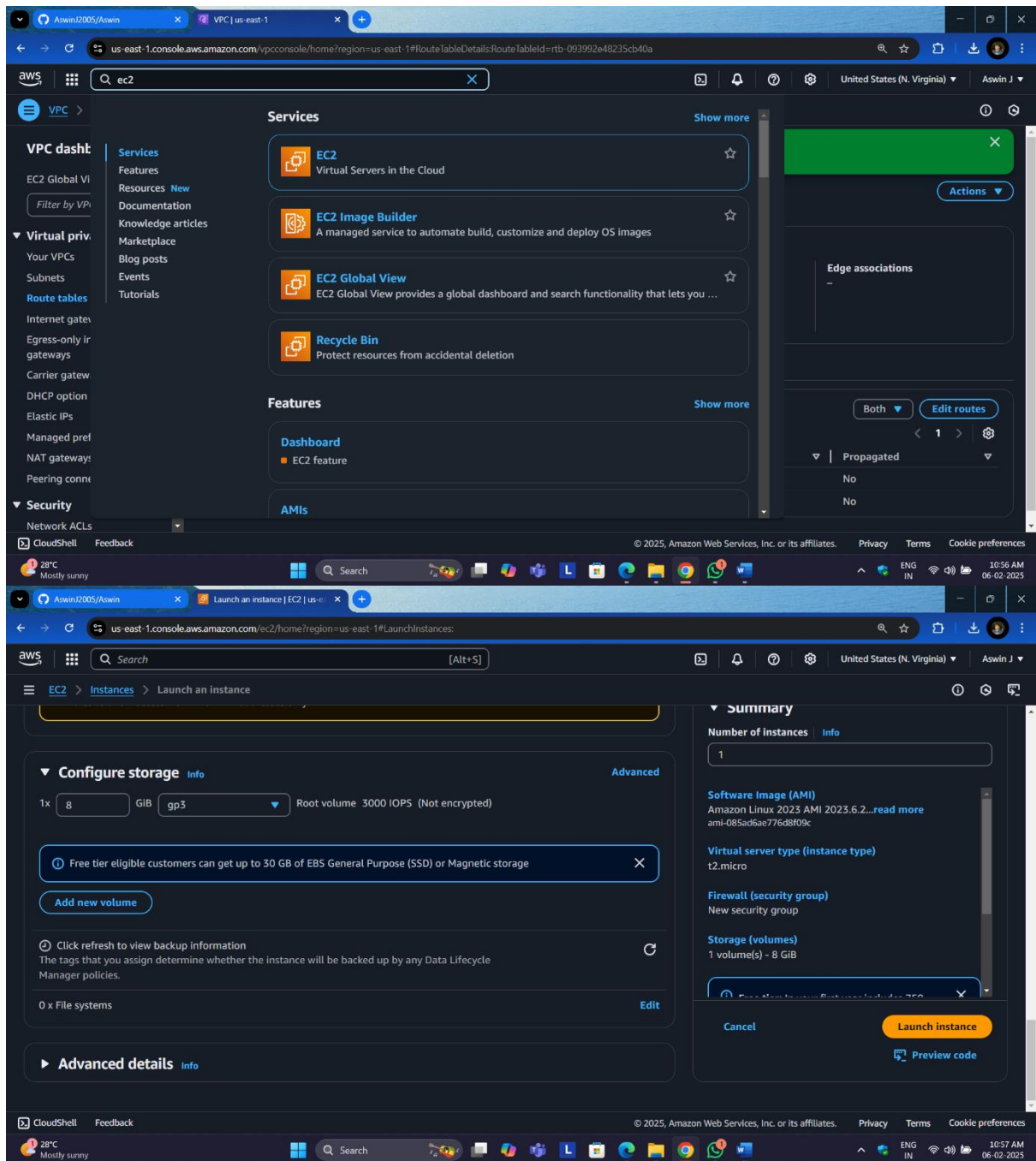
CloudShell Feedback

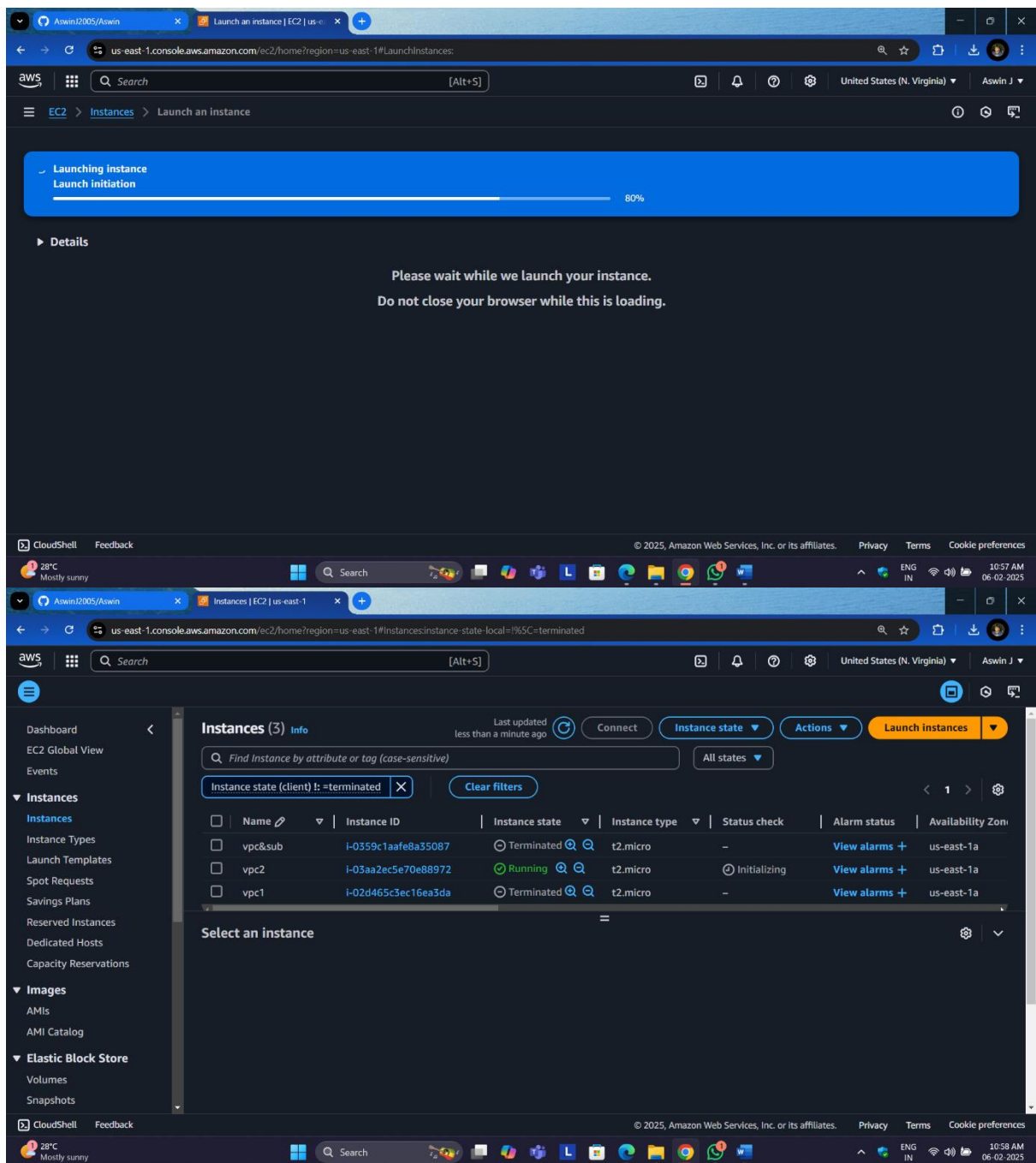
© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

28°C Mostly sunny

Search

10:54 AM 06-02-2025





Aswin13005/Aswin

EC2 | us-east-1

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

Search [Alt+S]

United States (N. Virginia) Aswin J

Dashboard

EC2 Global View

Events

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

Images

AMIs

AMI Catalog

Elastic Block Store

Volumes

Snapshots

Successfully initiated termination (deletion) of i-03aa2ec5e70e88972

Instances (2/3) Info

Last updated less than a minute ago

Connect

Instance state

Actions

Launch instances

Find Instance by attribute or tag (case-sensitive)

All states

1

2 instances selected

Monitoring

Configure CloudWatch agent

Alarm recommendations

3h 1d 1w 1h

UTC timezone

Add to dashboard

CPU utilization (%)

Network in (bytes)

Network out (bytes)

Network packets in...

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
<input checked="" type="checkbox"/>	vpc22	i-0f4b488ebee757438	Running	t2.micro	Initializing	View alarms +	us-east-1a
<input type="checkbox"/>	vpc2	i-03aa2ec5e70e88972	Terminated	t2.micro	-	View alarms +	us-east-1a
<input checked="" type="checkbox"/>	vpc2	i-05344d547cdd09bee	Running	t2.micro	Initializing	View alarms +	us-east-1a

© 2025, Amazon Web Services, Inc. or its affiliates.

Privacy Terms Cookie preferences

28°C Mostly sunny

Search

11:03 AM 06-02-2025