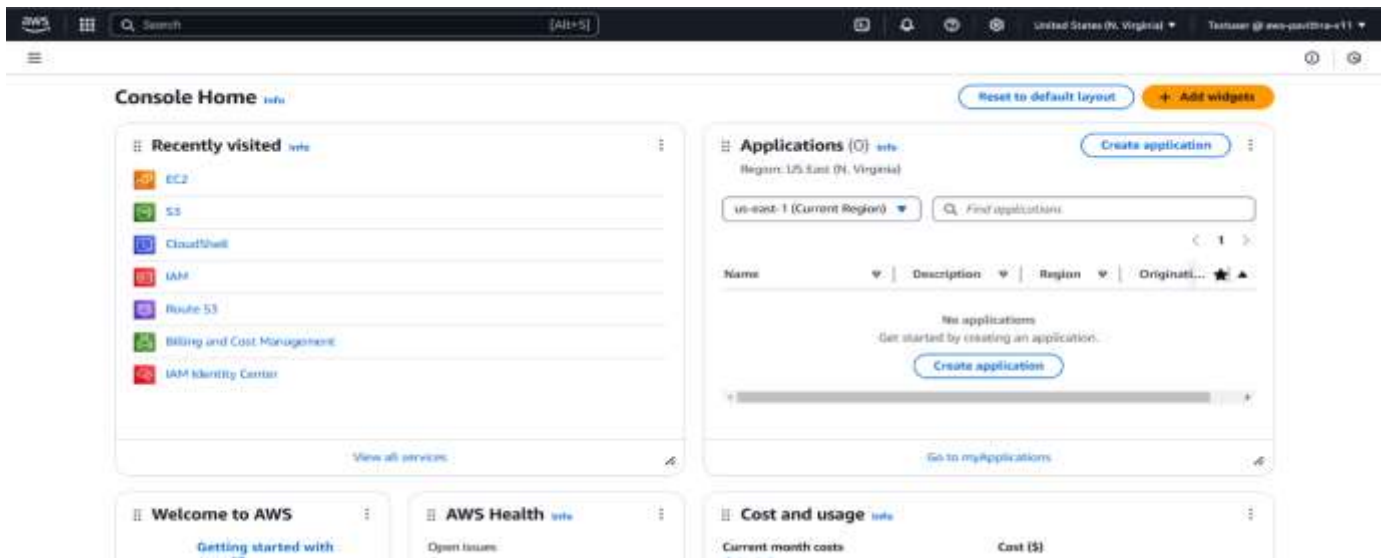


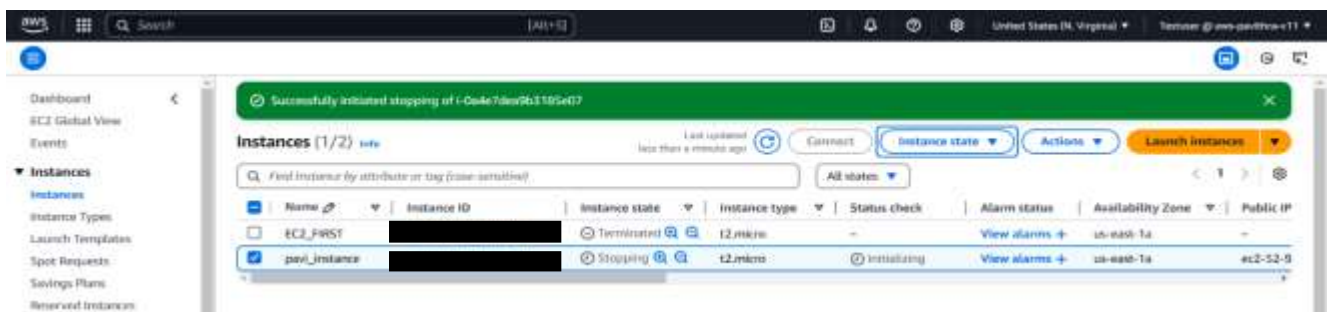
# Creating and Connecting to a Windows EC2 Instance on AWS

## Step 1: Log In to the AWS Management Console

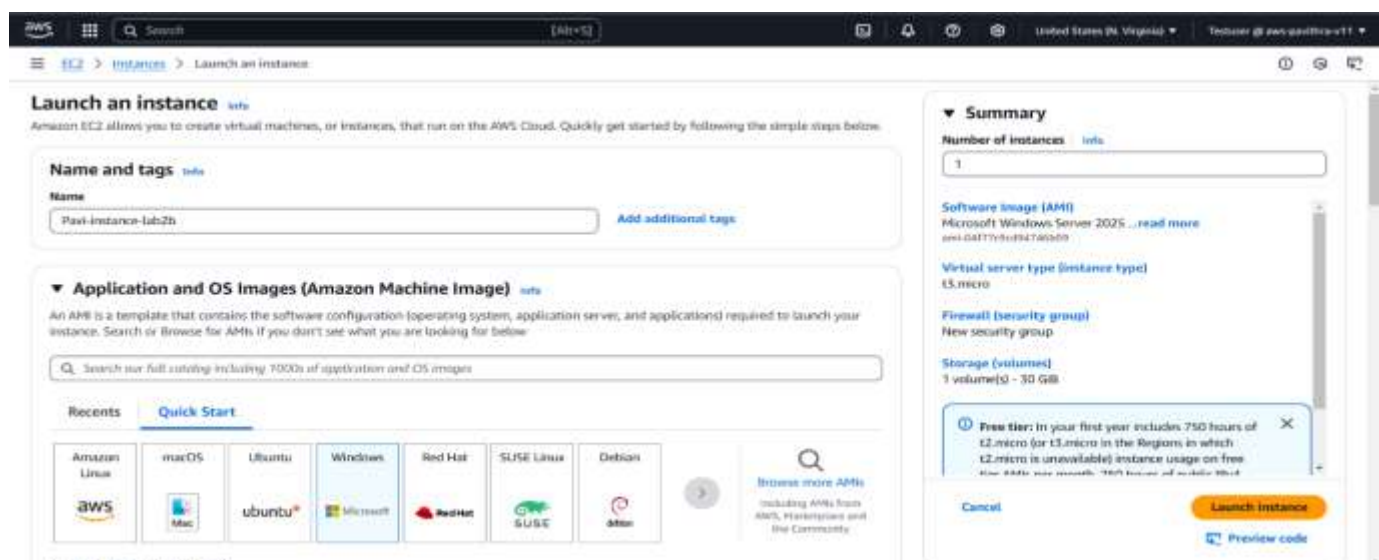


## Step 2: Launch an EC2 Instance

### 1. Go to the EC2 Dashboard:



### 2. 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. 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

Recents Quick Start

Amazon Linux macOS Ubuntu Windows Red Hat SUSE Linux Debian

Amazon Machine Image (AMI)

Microsoft Windows Server 2025 Base  
ami-04f77c9d94746b09 (64-bit x86)  
Virtualization: x86\_64 enabled true Root device type: ebs

Description

Microsoft Windows 2025 Datacenter edition. [English]  
Microsoft Windows Server 2025 Full Locale English AMI provided by Amazon

Architecture 64-bit (x86) AMI ID ami-04f77c9d94746b09 Username root

Free tier eligible

Verify provider

Summary

Number of instances 1

Software Image (AMI)  
Microsoft Windows Server 2025 ...read more  
ami-04f77c9d94746b09

Virtual server type (instance type)  
t3.micro

Firewall (security group)  
New security group

Storage (volumes)  
1 volume(s) - 30 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier. AMIs per month: 100 hours of public IP address usage.

Cancel Launch instance Preview code

### 3. Select Instance Type:

Search [Alt+S]

United States (N. Virginia) Testuser @ aws-paill@aws11

Instances > Launch an instance

64-bit (x86) ami-04f77c9d94746b09

Instance type

Instance type

t3.micro  
Family t3 - 2 vCPU, 1 GiB Memory - EBS-optimized true  
On-Demand Ubuntu Pro base pricing: 0.0159 USD per Hour  
On-Demand Ubuntu base pricing: 0.0104 USD per Hour  
On-Demand Linux base pricing: 0.0104 USD per Hour  
On-Demand Windows base pricing: 0.0190 USD per Hour

All generations Compare instance types

Additional costs apply for AMIs with pre-installed software

Key pair (login)

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

Key pair name - required

lab2b-paill Create new key pair

For Windows instances, you use a key pair to decrypt the administrator password. You then use the decrypted password to connect to your instance.

Network settings

VPC - required

vpc-09a86c566a0ed0962 (default)

Subnet

No preference Create new subnet

Auto-assign public IP

Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups)

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-5

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 \_-.,/:[@](+&#39;~.

Description - required

launch-wizard-5 created 2025-02-12T03:51:25.722Z

Inbound Security Group Rules

Summary

Number of instances 1

Software Image (AMI)  
Microsoft Windows Server 2025 ...read more  
ami-04f77c9d94746b09

Virtual server type (instance type)  
t3.micro

Firewall (security group)  
New security group

Storage (volumes)  
1 volume(s) - 30 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier. AMIs per month: 100 hours of public IP address usage.

Cancel Launch instance Preview code

### 4. Configure Instance Details:

Network settings

VPC - required

vpc-09a86c566a0ed0962 (default)

Subnet

No preference Create new subnet

Auto-assign public IP

Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups)

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-5

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 \_-.,/:[@](+&#39;~.

Description - required

launch-wizard-5 created 2025-02-12T03:51:25.722Z

Inbound Security Group Rules

Summary

Number of instances 1

Software Image (AMI)  
Microsoft Windows Server 2025 ...read more  
ami-04f77c9d94746b09

Virtual server type (instance type)  
t3.micro

Firewall (security group)  
New security group

Storage (volumes)  
1 volume(s) - 30 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier. AMIs per month: 100 hours of public IP address usage.

Cancel Launch instance Preview code

## 5. Add Storage:

My IP: [Add CIDR, prefix list or security group] e.g. SSH for admin desktop

30 GB gp3 Root volume: 3000 IOPS (Not encrypted)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage

Add new volume

The selected AMI contains more instance store volumes than the instance allows. Only the first 0 instance store volumes from the AMI will be accessible from the instance.

Click refresh to view backup information

The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems

Summary

Number of instances: 1

t3.micro

Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 30 GB

Free tier in your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel Launch Instance Preview code

## 5. Add Tags:

## 6. Configure Security Group:

Create security group Select existing security group

Security group name - required: launch-wizard-5

Description - required: launch-wizard-5 created 2025-02-12T05:51:25.722Z

Inbound Security Group Rules

Security group rule 1 (TCP: 3389, 69-290.81.88/128)

Type: rdp Protocol: TCP Port range: 3389

Source type: My IP Name: e.g. SSH for admin desktop

Add security group rule

Summary

Number of instances: 1

t3.micro

Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 30 GB

Free tier in your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel Launch Instance Preview code

## 7. Review and Launch:

64-bit (x86)

04f77c3cd94746909

Instance type

t3.micro

Family: t3, 2 vCPU, 1 GB Memory, Current generation: true

On-Demand Linux (base pricing): 0.0189 USD per Hour

On-Demand Linux (base pricing): 0.0189 USD per Hour

On-Demand Linux (base pricing): 0.0189 USD per Hour

On-Demand Linux (base pricing): 0.0189 USD per Hour

Additional costs apply for AMIs with pre-installed software

Key pair (login)

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

Key pair name - required: lab2b-pw1

Create new key pair

Network settings

VPC - required

Summary

Number of instances: 1

t3.micro

Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 30 GB

Free tier in your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel Launch Instance Preview code

### Step 3: Find the Public IP Address of Your Windows Instance

The screenshot shows the AWS Management Console interface. On the left, the navigation menu includes 'Dashboard', 'EC2 Global View', 'Events', 'Instances', 'Instance Types', 'Launch Templates', 'Spot Requests', 'Savings Plans', 'Reserved Instances', 'Dedicated Hosts', 'Capacity Reservations', 'Images', 'AMI Catalog', 'Elastic Block Store', 'Volumes', 'Snapshots', 'Lifecycle Manager', and 'Network & Security'. The main content area displays the 'Instances' page with a table of instances. The instance 'Pavi-instance-lab2b' is selected, and its details are shown below the table. The details include the Instance ID, Instance type, Instance state, Public IPv4 address, Private IPv4 addresses, Public IPv4 DNS, and Private IP DNS name.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
pavi_instance	[REDACTED]	Stopped	t2.micro	-	View alarms +	us-east-1a	-
Pavi-instance-lab2b	i-01192ab471f12f68d	Running	t3.micro	Initializing	View alarms +	us-east-1c	ec2-3-80-248-112.compute-1.amazonaws.com

**i-01192ab471f12f68d (Pavi-instance-lab2b)**

**Instance summary**

Instance ID: [REDACTED]

IPv4 address: [REDACTED]

Hostname type: [REDACTED]

Public IPv4 address: 3.80.248.112 | [open address](#)

Instance state: Running

Private IPv4 addresses: 172.31.47.183

Public IPv4 DNS: ec2-3-80-248-112.compute-1.amazonaws.com | [open address](#)

Private IP DNS name (IPv4 only): [REDACTED]

### Step 4: Use Remote Desktop Connection (RDP) to Connect For Windows Users:

The screenshot shows the AWS Management Console interface. On the left, the navigation menu includes 'Dashboard', 'EC2 Global View', 'Events', 'Instances', 'Instance Types', 'Launch Templates', 'Spot Requests', 'Savings Plans', 'Reserved Instances', 'Dedicated Hosts', 'Capacity Reservations', 'Images', 'AMI Catalog', 'Elastic Block Store', 'Volumes', 'Snapshots', 'Lifecycle Manager', and 'Network & Security'. The main content area displays the 'Instances' page with a table of instances. The instance 'Pavi-instance-lab2b' is selected, and its details are shown below the table. The details include the Instance ID, Instance type, Instance state, Public IPv4 address, Private IPv4 addresses, Public IPv4 DNS, and Private IP DNS name. A Windows 'Run' dialog box is overlaid on the console, showing the IP address 3.80.248.112.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
pavi_instance	i-0a4e7d9a	Stopped	t2.micro	-	View alarms +	us-east-1a	-
Pavi-instance-lab2b	i-01192ab4	Running	t3.micro	Initializing	View alarms +	us-east-1c	ec2-3-80-248-112.compute-1.amazonaws.com

**i-01192ab471f12f68d (Pavi-instance-lab2b)**

**Instance summary**

Instance ID: [REDACTED]

IPv4 address: [REDACTED]

Hostname type: [REDACTED]

Public IPv4 address: 3.80.248.112 | [open address](#)

Instance state: Running

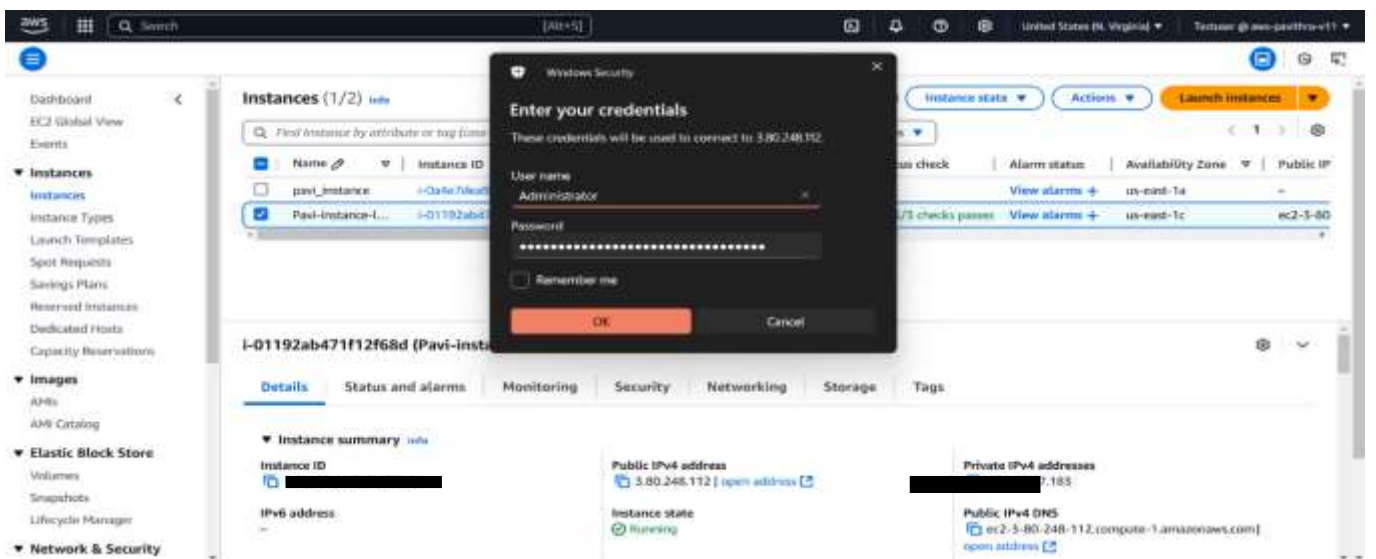
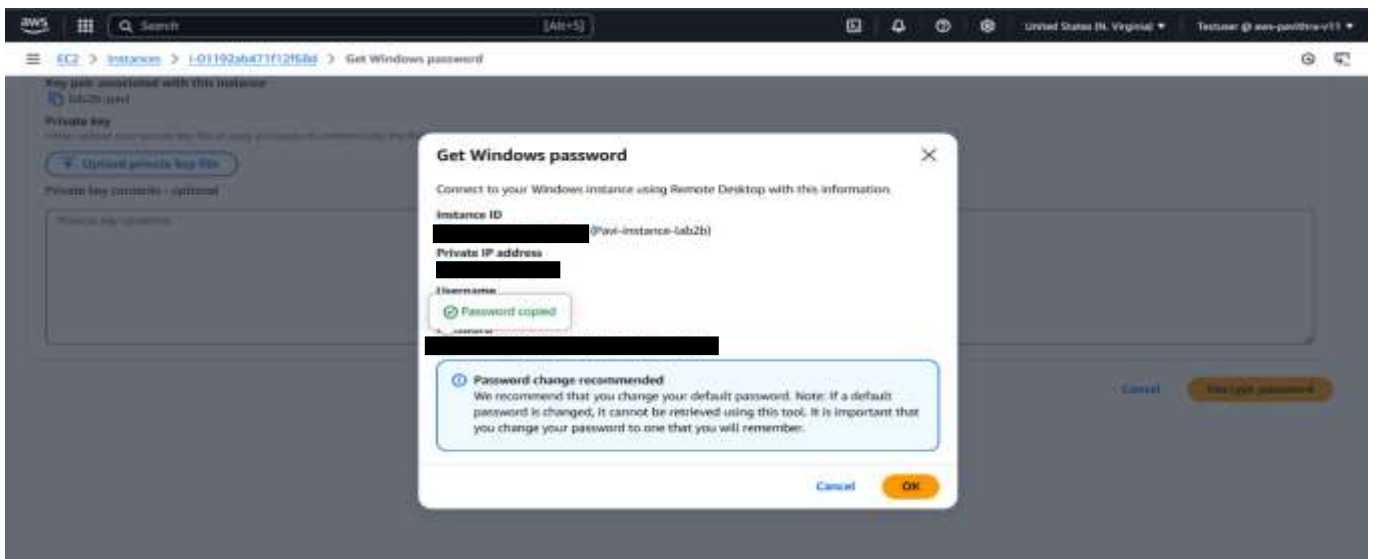
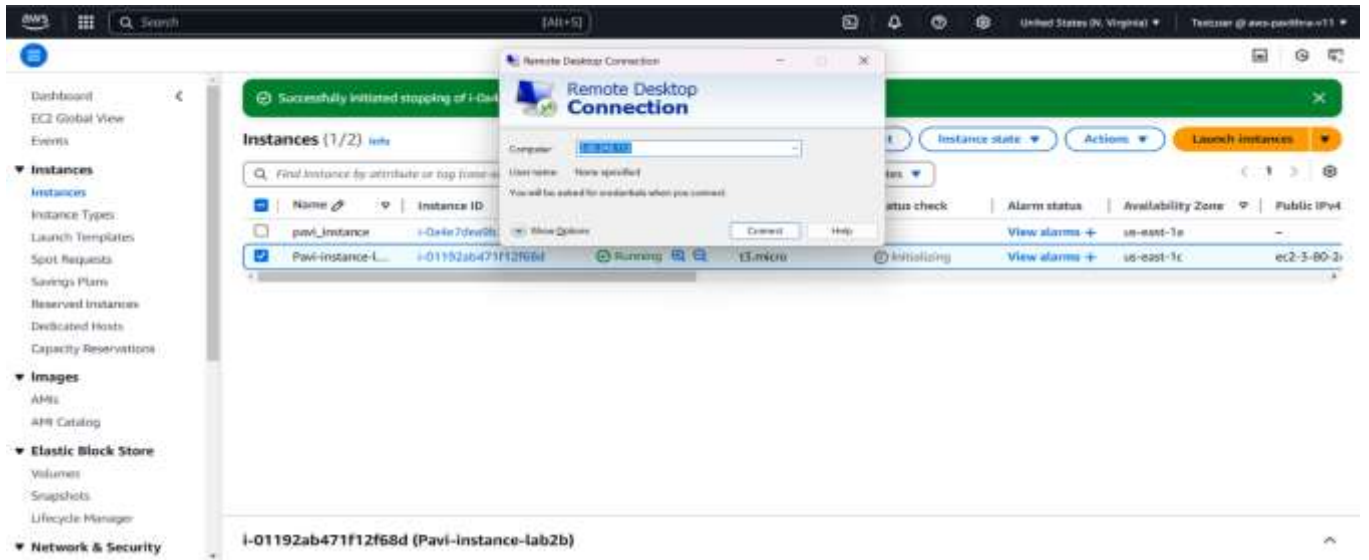
Private IPv4 addresses: 172.31.47.183

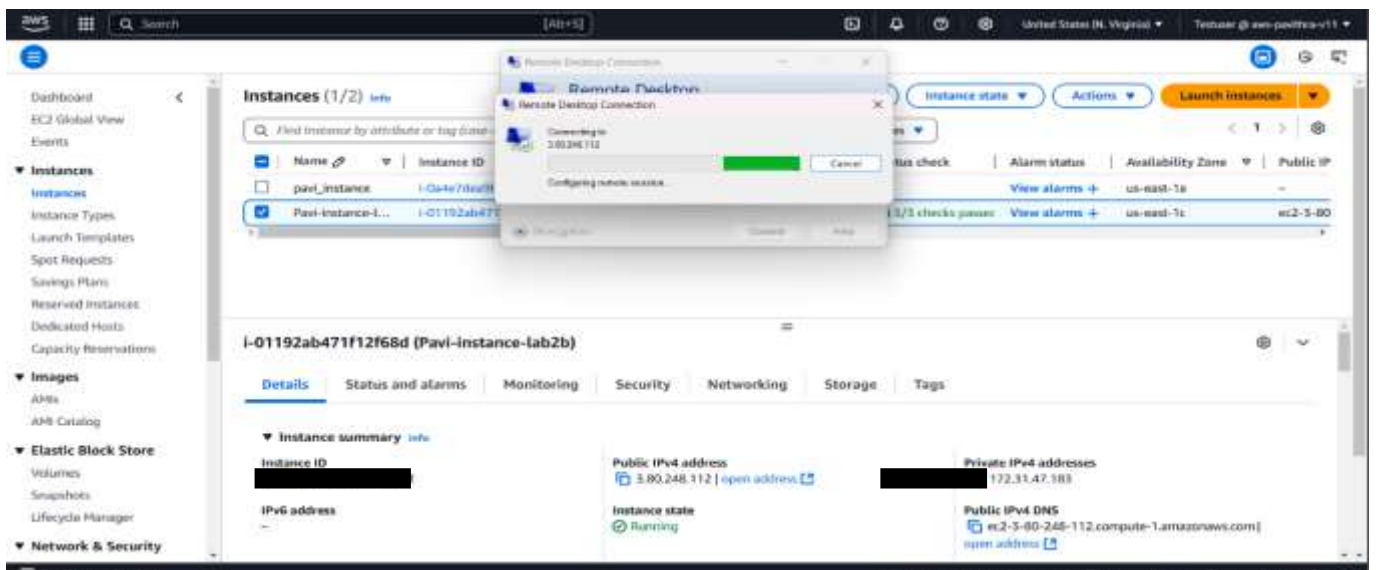
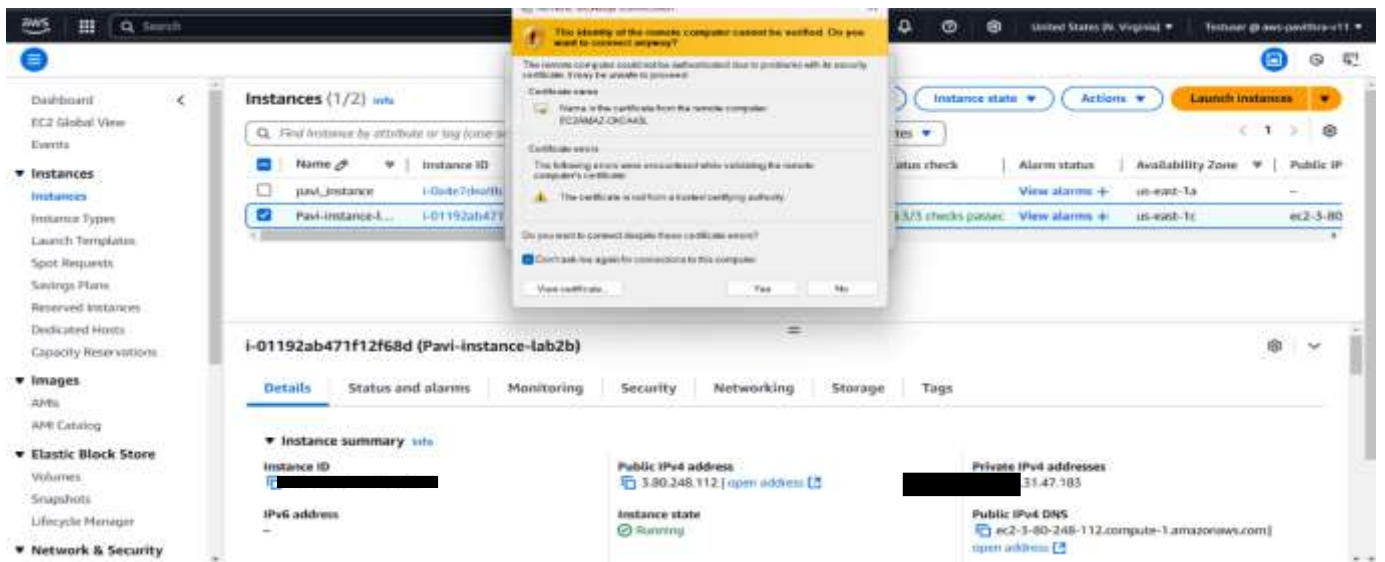
Public IPv4 DNS: ec2-3-80-248-112.compute-1.amazonaws.com | [open address](#)

Private IP DNS name (IPv4 only): [REDACTED]



In the Computer field, enter the Public IPv4 Address from Step 3.

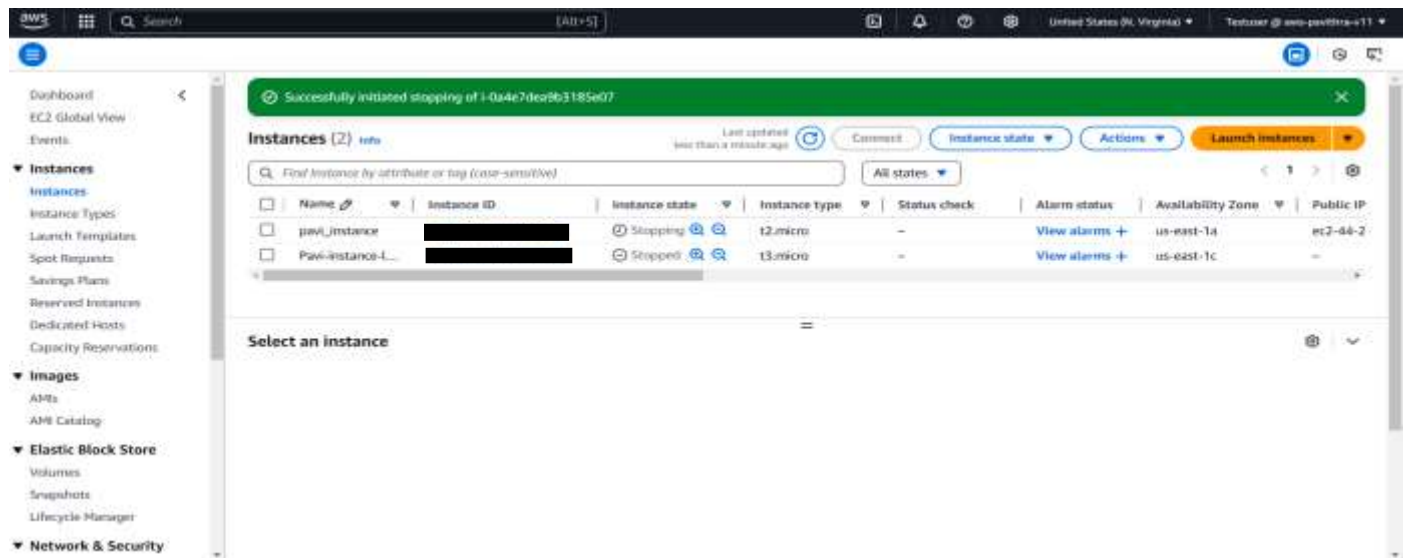




## Step 5: Verify Connection



## Step 6: Clean Up (Optional)



## Troubleshooting

### Issue: Connection Refused or Timeout-VERIFIED

- Ensure the Windows instance is running in AWS.
- Confirm Security Group allows RDP (Port 3389) from your IP.
- Verify that your Public IPv4 Address is correctly entered in the RDP client.

### Issue: Incorrect Password-VERIFIED

- Make sure you retrieved the password after the instance launched.
- Re-download and decrypt the password using the .pem file.

## 1. Summary Report:

### Steps Performed:

#### 1. Log In to AWS Management Console

- Accessed the AWS Management Console using login credentials.

#### 2. Launch an EC2 Instance

- Navigated to the EC2 Dashboard.
- Selected an Amazon Machine Image (AMI): Chose a Windows AMI for the instance.
- Selected an Instance Type: Picked an instance type based on requirements.
- Configured Instance Details: Set up instance parameters such as network settings, IAM role, and shutdown behavior.
- Added Storage: Configured the necessary disk size and type.
- Added Tags: Labeled the instance for easier identification.
- Configured Security Group: Allowed RDP (port 3389) to enable remote access.
- Reviewed and Launched the Instance.

#### 3. Find the Public IP Address of the Windows Instance

- Located the instance in the AWS EC2 dashboard and retrieved the Public IPv4 Address.

#### **4. Use Remote Desktop Connection (RDP) to Connect**

- Opened Remote Desktop Connection (RDP).
- Entered the Public IPv4 Address in the "Computer" field.
- Provided the administrator username and password to log in.

#### **5. Verify Connection**

- Successfully accessed the Windows EC2 instance using RDP.

#### **6. Clean Up (Optional)**

- **If** required, terminated the instance to avoid unnecessary billing.

---

### **Issues Faced and Resolutions: Retrieving Password for Windows EC2 Instance**

Issue: Unable to Retrieve the Administrator Password for RDP Login

- The main issue faced was how to get the password for the Windows EC2 instance after launching it.

Resolution Steps:

1. Access the AWS Management Console
  - Logged in to the AWS Management Console.
  - Navigated to EC2 Dashboard.
2. Select the Running Instance
  - Located the Windows EC2 instance in the Instances section.
  - Selected the instance for which the password was needed.
3. Retrieve the Administrator Password
  - Clicked on Actions > Security > Get Windows Password.
  - Selected the private key file (.pem) used during instance creation.
  - Clicked Decrypt Password to reveal the Administrator password.
4. Use the Retrieved Password in RDP
  - Opened Remote Desktop Connection (mstsc) using Win + R → typed mstsc → hit Enter.
  - Entered the Public IPv4 Address in the "Computer" field.
  - Used Username: Administrator.
  - Pasted the decrypted password retrieved from AWS.
  - Clicked OK and accepted the security warning to proceed.

Final Outcome:

- Successfully retrieved the Windows password and used it to connect to the EC2 instance via Remote Desktop Connection (RDP).