

Lesson 03 Demo 04

Starting and Accessing a Windows Instance on EC2

Objective: To launch a Windows-based EC2 instance on Amazon Web Services (AWS) and securely access it using the Remote Desktop Protocol (RDP)

Tools required: AWS account

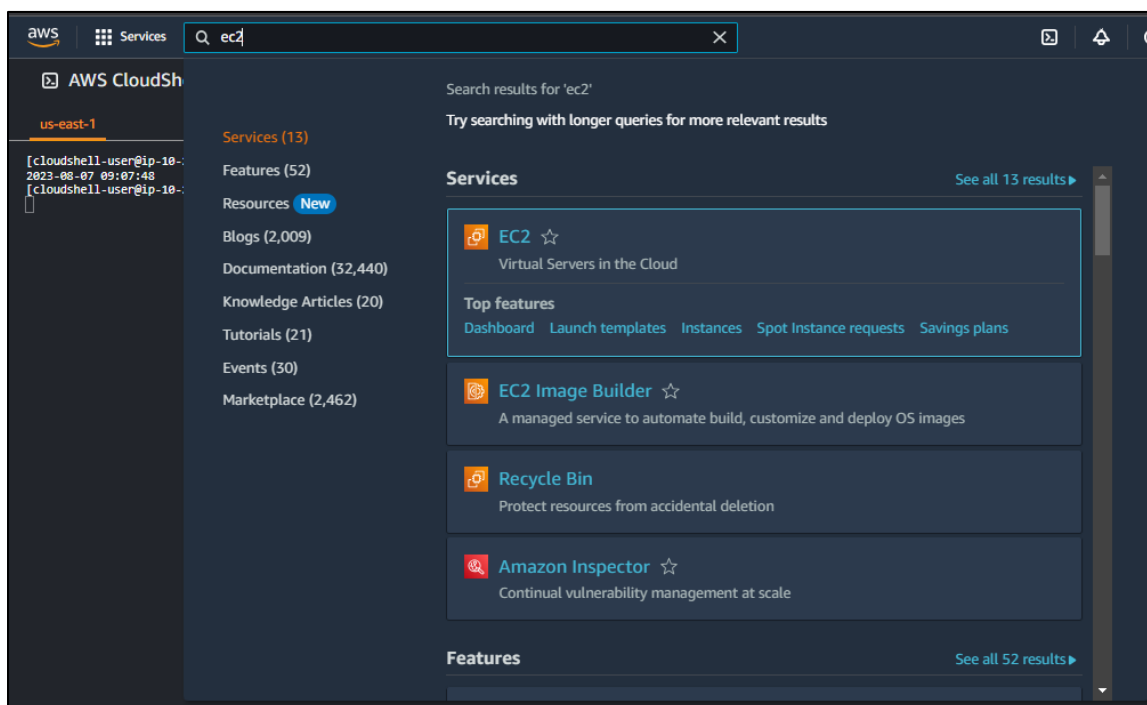
Prerequisites: NA

Steps to be followed:

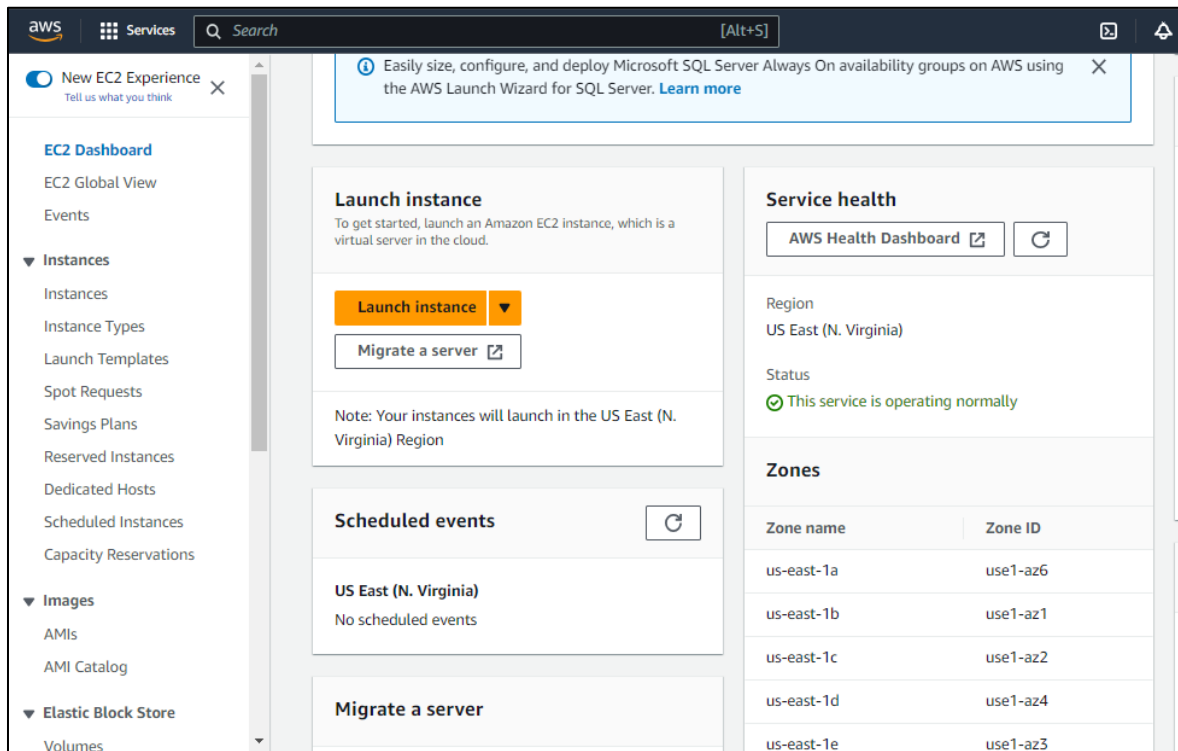
1. Launch an EC2 instance
2. Access the EC2 instance via RDP

Step 1: Launch an EC2 instance

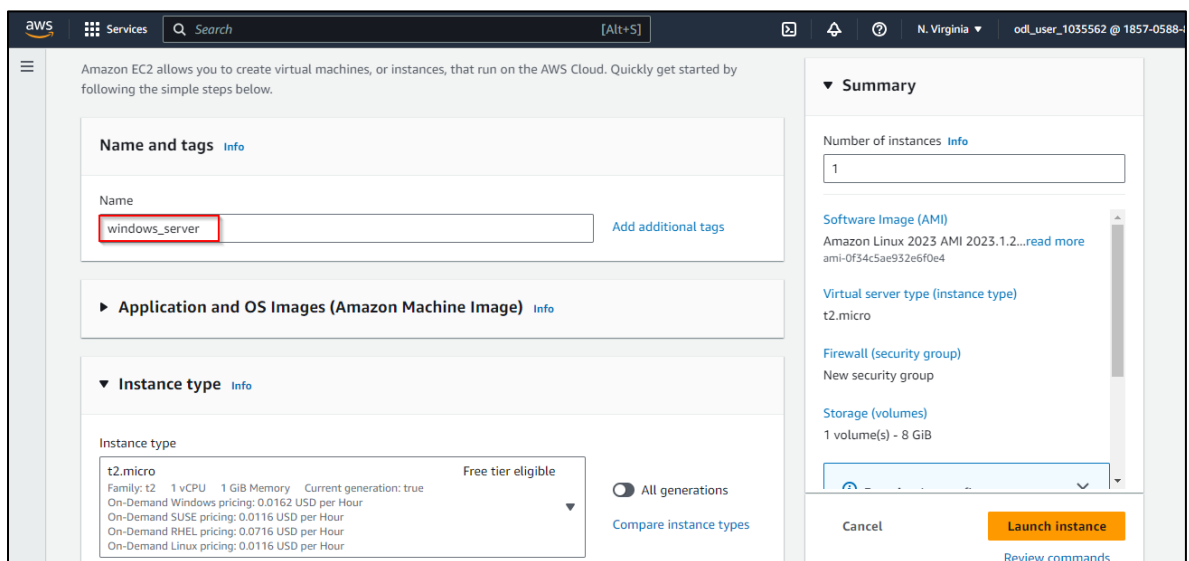
1.1 In the AWS Management Console, search for **EC2** and click on the **EC2** instance



1.2 In the EC2 dashboard, click on **Launch instance**



1.3 Enter any arbitrary name as **windows_server** for the instance



1.4 Select the **Windows** OS

▼ **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

Ubuntu

Windows

Red Hat

SUSE Linux

[Browse more AMIs](#)

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Microsoft Windows Server 2019 Base

ami-041306c411c38a789 (64-bit (x86))

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

Free tier eligible ▼

1.5 Select the **t2.micro** instance type

64-bit (x86) ami-0fc682b2a42e57ca2 verified provider

▼ **Instance type** [Info](#)

Instance type

t2.micro

Family: t2 1 vCPU 1 GiB Memory Current generation: true

On-Demand Windows pricing: 0.0162 USD per Hour

On-Demand SUSE pricing: 0.0116 USD per Hour

On-Demand RHEL pricing: 0.0716 USD per Hour

On-Demand Linux pricing: 0.0116 USD per Hour

Free tier eligible ▼

☐ All generations [Compare instance types](#)

▼ **Key pair (login)** [Info](#)

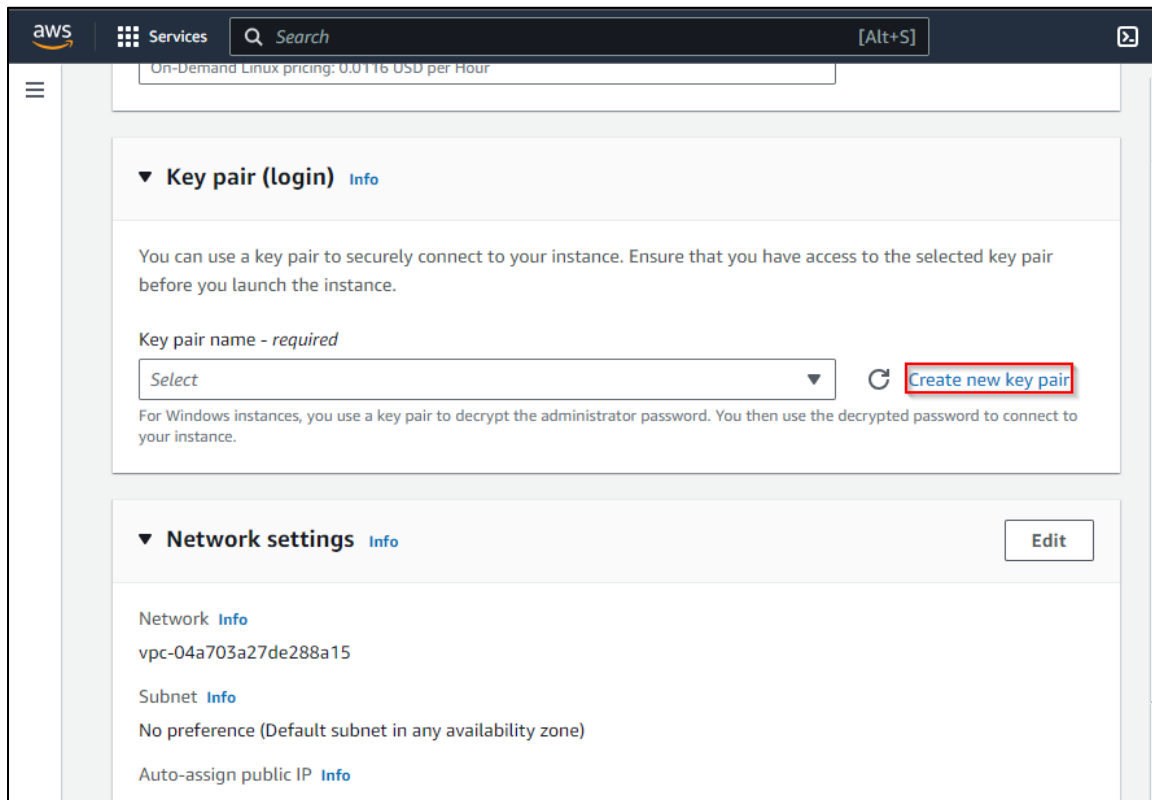
You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

Select ▼ [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 the instance.

1.6 After selecting the instance type, click on **Create new key pair**



The screenshot shows the AWS Management Console interface. At the top, there is a navigation bar with the AWS logo, a 'Services' menu, a search bar, and a keyboard shortcut '[Alt+S]'. Below the navigation bar, a banner displays 'On-Demand Linux pricing: 0.0116 USD per Hour'. The main content area is divided into sections. The first section is titled 'Key pair (login)' with an 'Info' link. It contains a paragraph explaining that a key pair is used to securely connect to an instance. Below this, there is a label 'Key pair name - required' and a dropdown menu with 'Select' as the current option. To the right of the dropdown is a circular refresh icon and a button labeled 'Create new key pair', which is highlighted with a red rectangular box. Below the dropdown, a note states: 'For Windows instances, you use a key pair to decrypt the administrator password. You then use the decrypted password to connect to your instance.' The second section is titled 'Network settings' with an 'Info' link and an 'Edit' button. It lists three settings: 'Network' with value 'vpc-04a703a27de288a15', 'Subnet' with value 'No preference (Default subnet in any availability zone)', and 'Auto-assign public IP' with value 'Info'.

aws Services Search [Alt+S]

On-Demand Linux pricing: 0.0116 USD per Hour

▼ 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 launch the instance.

Key pair name - required

Select ▼ ↻ 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 Info Edit

Network Info
vpc-04a703a27de288a15

Subnet Info
No preference (Default subnet in any availability zone)

Auto-assign public IP Info

1.7 In the **Key pair** window, do the following configuration:

- Enter an arbitrary name for the key pair
- Select **.pem** for private key pair file type, and then click on **Create key pair**

Create key pair [X]

Key pair name
Key pairs allow you to connect to your instance securely.

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

Key pair type

☒ **RSA**
RSA encrypted private and public key pair

☐ **ED25519**
ED25519 encrypted private and public key pair (Not supported for Windows instances)

Private key file format

☒ **.pem**
For use with OpenSSH

☐ **.ppk**
For use with PuTTY

⚠ When prompted, store the private key in a secure and accessible location on

Cancel **Create key pair**

1.8 In the **Firewall (security groups)** option, select **Create security group** and then the **Edit** option

▼ **Network settings** [Info](#)

Edit

Network [Info](#)

vpc-04a703a27de288a15

Subnet [Info](#)

No preference (Default subnet in any availability zone)

Auto-assign public IP [Info](#)

Enable

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

We'll create a new security group called 'launch-wizard-2' with the following rules:

☒ Allow RDP traffic from

Helps you connect to your instance

Anywhere
0.0.0.0/0

☐ Allow HTTPS traffic from the internet

To set up an endpoint, for example when creating a web server

1.9 Click on **Add security group rule**

Type [Info](#)

rdp

Protocol [Info](#)

TCP

Port range [Info](#)

3389

Source type [Info](#)

Anywhere

Source [Info](#)

Add CIDR, prefix list or security

0.0.0.0/0

Description - optional [Info](#)

e.g. SSH for admin desktop

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.

Add security group rule

▼ Configure storage [Info](#)

Advanced

1x

30

GiB

gp2

Root volume (Not encrypted)

1.10 Now, select **rdp** in **Type** field and **Anywhere** in **Source type** field

The screenshot displays the AWS Security Groups console. At the top, there is a search bar and a dropdown menu set to 'Anywhere'. Below this, a red error message box states: 'A security group rule with the same protocol, port range, and source has already been added to this security group. Each rule must have a unique combination of protocol, port range, and source.' Below the error message, a rule is listed: 'Security group rule 2 (TCP, 3389, 0.0.0.0/0)'. The rule configuration shows 'Type' set to 'rdp', 'Protocol' set to 'TCP', 'Port range' set to '3389', 'Source type' set to 'Anywhere', and 'Source' set to '0.0.0.0/0'. The 'Description - optional' field is empty. Below the rule configuration, there is a 'Remove' button. The bottom part of the screenshot shows the AWS Management Console header with the 'Name and tags' section, where the 'Name' field is set to 'windows_server'.

If the user gets a security group error as shown in the screenshot above, it means that there is an existing security group with the same name. In such a case, please modify the name accordingly.

1.11 Click on **Launch Instance**

The screenshot shows the AWS Management Console interface for launching an EC2 instance. The 'Configure storage' section is expanded, showing a single 30 GiB gp2 root volume. The 'Summary' section on the right shows the configuration: 1 instance, Microsoft Windows Server 2022 AMI, t2.micro instance type, and a new security group. The 'Launch instance' button is highlighted with a red box. Below the wizard, a success message states: 'Successfully initiated launch of instance (i-0139d661c54ee4a28)'.

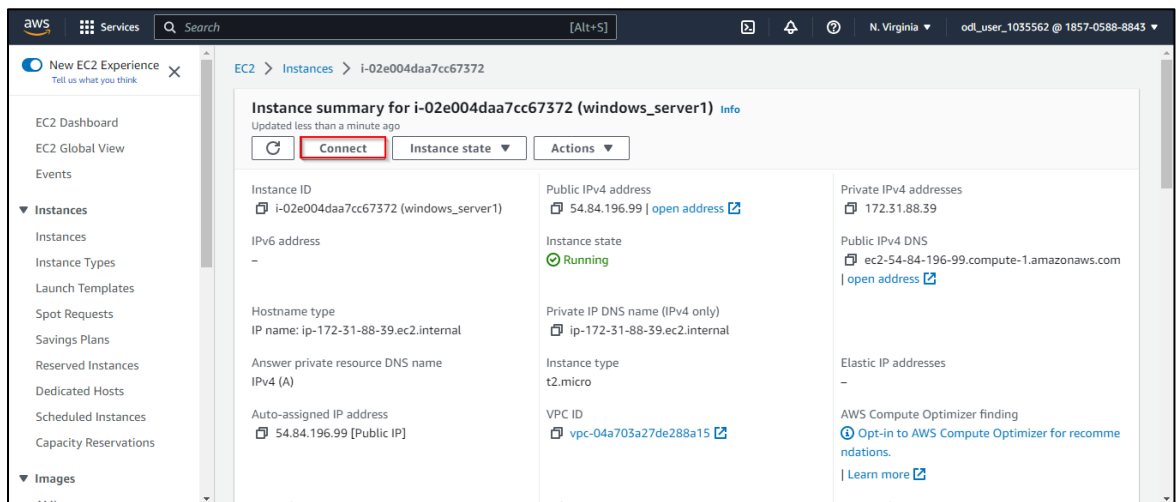
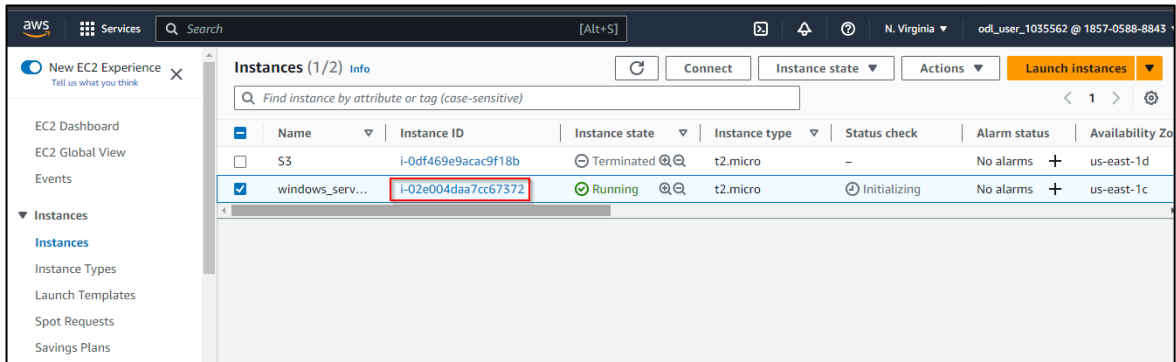
Instance is successfully initiated.

1.12 Click on **View all instances**

The screenshot shows the AWS Management Console interface after launching an instance. The 'Next Steps' section is visible, providing guidance on getting notified of estimated charges, how to connect to the instance, and where to find more resources. The 'View all instances' button is highlighted with a red box.

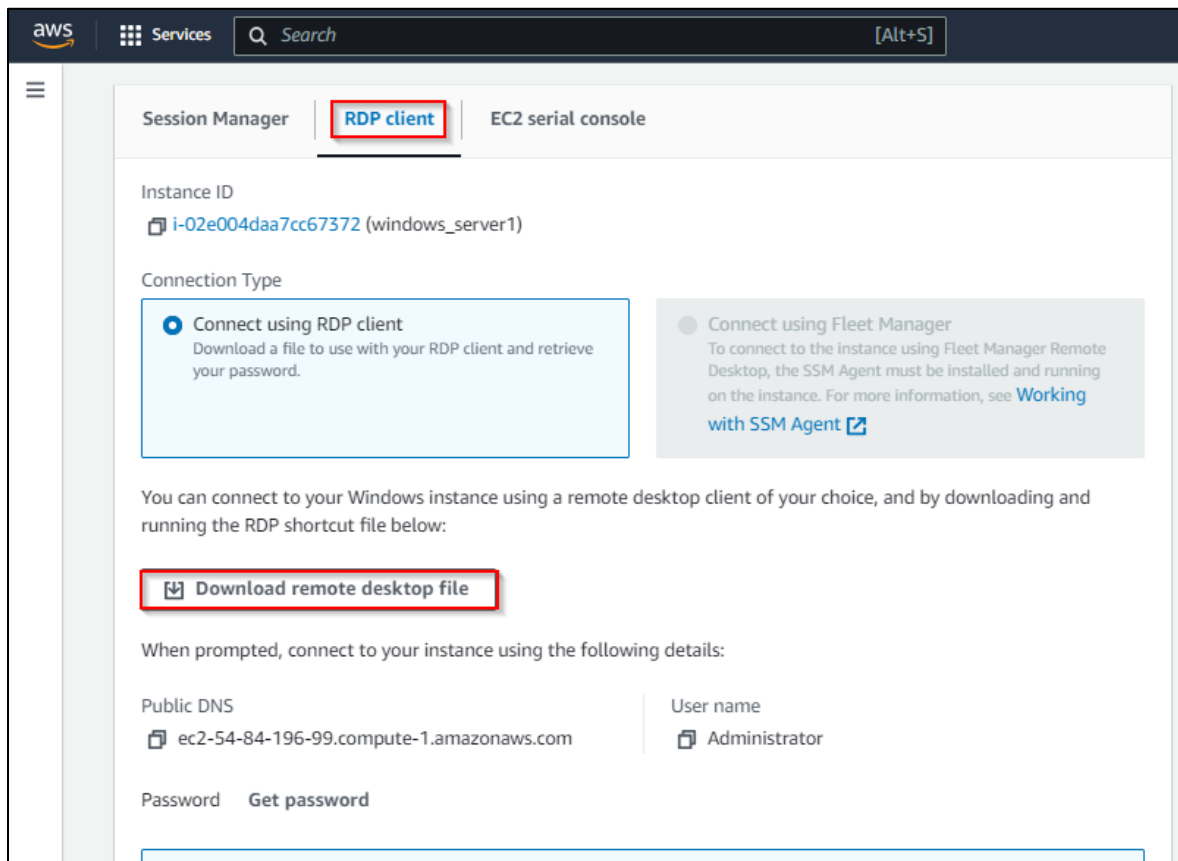
Step 2: Access the EC2 instance via RDP

2.1 Click on the **Instance ID** and then click on **Connect**

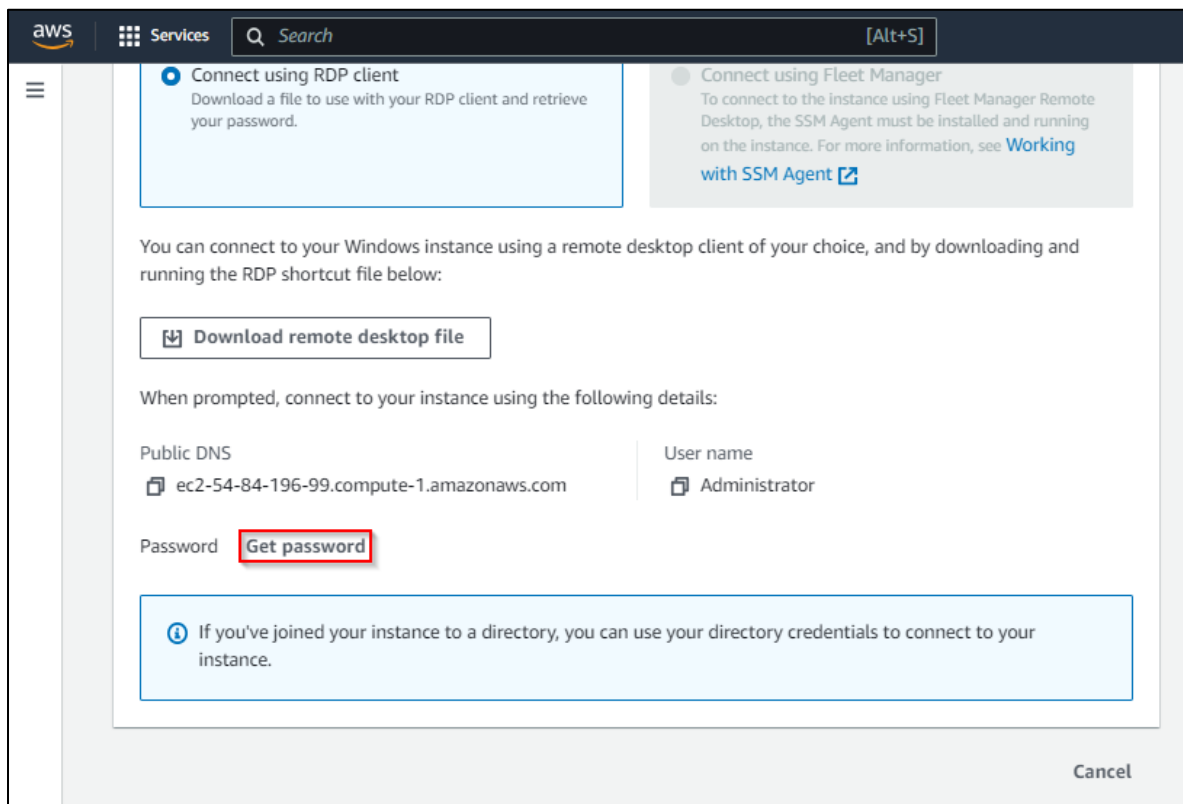


2.2 Go to the **RDP client** tab, and follow the steps as shown in the screenshot below:

- Select **RDP client**
- Click on **Download remote desktop file** and run that **.exe** file



2.3 Click on Get Password



2.4 Click on **Upload private key file**, select the key pair generated for this instance, and then click on **Decrypt password**

aws Services Search [Alt+S]

Instance ID
i-02e004daa7cc67372 (windows_server1)

Key pair associated with this instance
windows_server

Private key
Either upload your private key file or copy and paste its contents into the field below.

Upload private key file

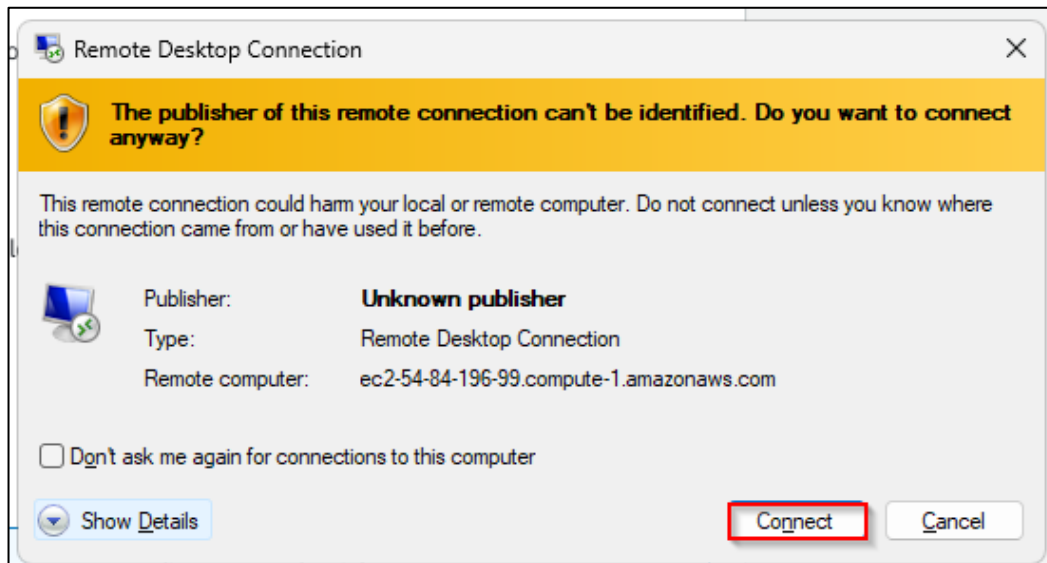
✓ windows_server.pem
1.674KB

Private key contents - optional

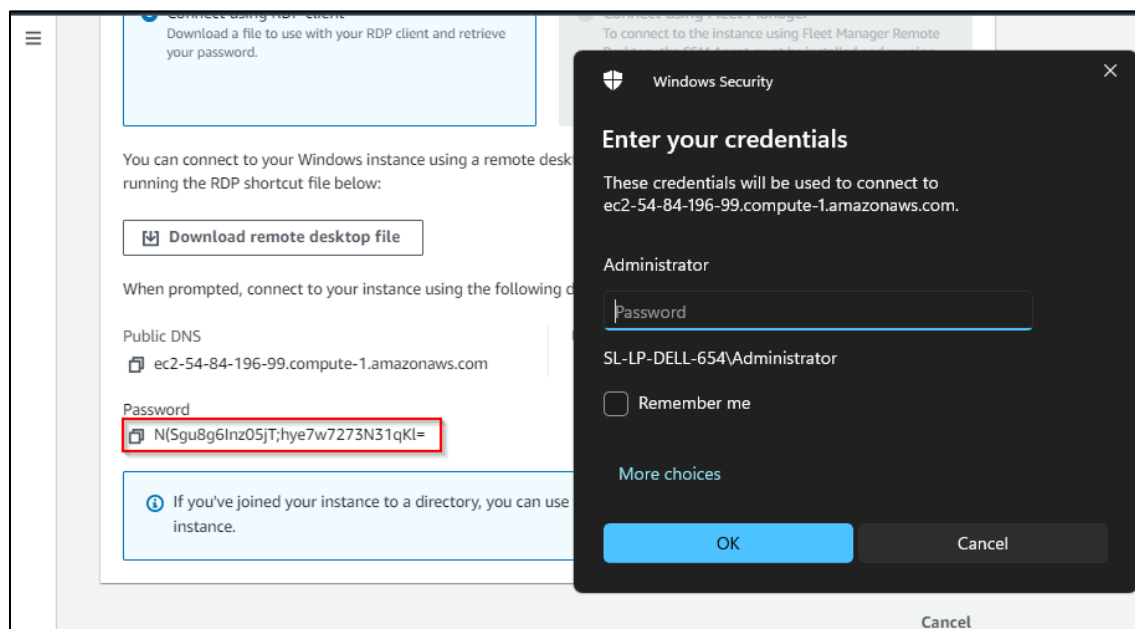
```
-----BEGIN RSA PRIVATE KEY-----
MIIIEowIBAAKCAQEAxnvFf7lbZz5GpVF3dlpMxxRR4/SmQl41jTwWCzTUcY6z9s/g
AHvDCmIRC4CBUeaZZJY0sriEO2FNzH1hcUn0Y70QHy7wrcGcJQganulKh+MLqsoO
CrX4NjdP+sLJ/r+T99i6HPhwRCd8btbkD7wExeCGTMwR9nR6hYFJgANh6asEtDDu
KpKLHZFhKjfhYMyidZ5EibRlMua7fN0wHwF1G7EKAHq2rjTirRxxDdbp3AlbsmE
+JEMvj8ZPqWKM+Dwbxr8JbUNCcT08ua3d/blkZ1Ju/kle13ETNIXFW49NsQGilO
yaXQ6HBTMCD0FJWHxRJkwGGg6RfoRVoI+n5hQQIDAQABAolBAQCRMVdvMGOJqce6
BVcx/D1RPssMyxmYMRxRfaPOfM3vZ+mD4drF38L0ZHp9hHqVM+//4dUY69tnKK3l
-----
```

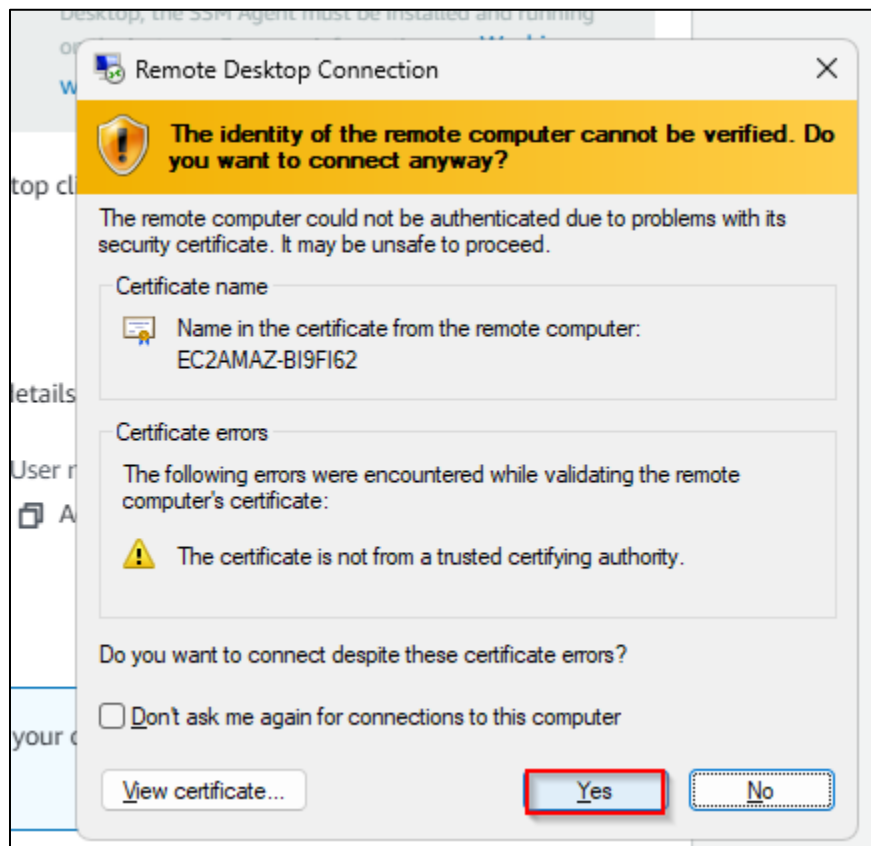
Cancel Decrypt password

2.5 Run the .exe file downloaded in **step 2.2**, and click on **Connect**

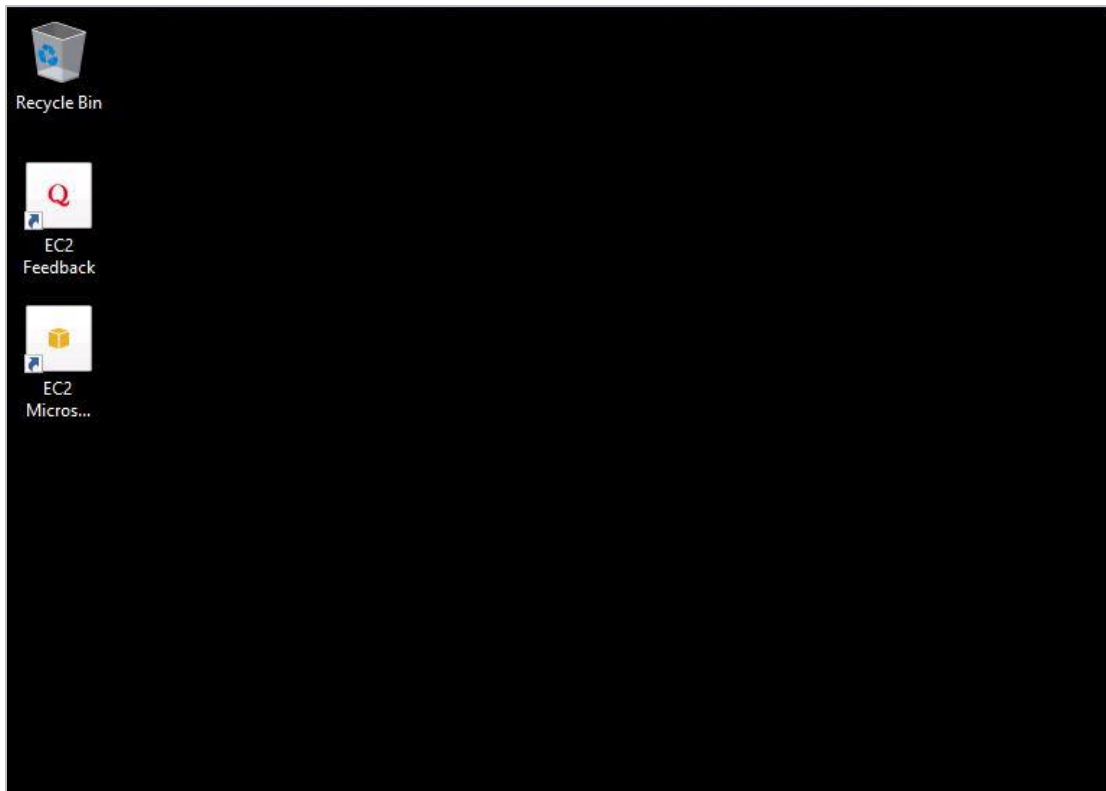


2.6 Copy the password and paste it in **Windows server**



2.7 Click on **Yes**2.8 Add the password under **Administrator** and click **OK**

You will be logged into the Windows instance.



Note: The windows instance is launched successfully.

By following these steps, you will be able to successfully launch a Windows-based EC2 instance on Amazon Web Services (AWS).