

Guided Lab: How to launch an Amazon EC2 Windows instance

Description

Amazon Elastic Compute Cloud (Amazon EC2) is a web service that allows you to easily create and manage virtual servers in the cloud. With Amazon EC2, you can set up and configure your own operating system and applications as per your requirements.

An Amazon EC2 instance is a virtual server that can be launched on AWS Cloud. When you launch an instance, it is secured with a key pair, which is used to prove your identity, and a security group that works as a virtual firewall to control incoming and outgoing traffic. When connecting to your instance, you must provide the private key of the key pair that you specified while launching the instance.

In this lab, you will be using Amazon EC2 to launch a virtual server with Windows as the operating system. This hands-on experience with cloud computing will help you understand how to use Amazon EC2 as a start for your own projects.

Objectives

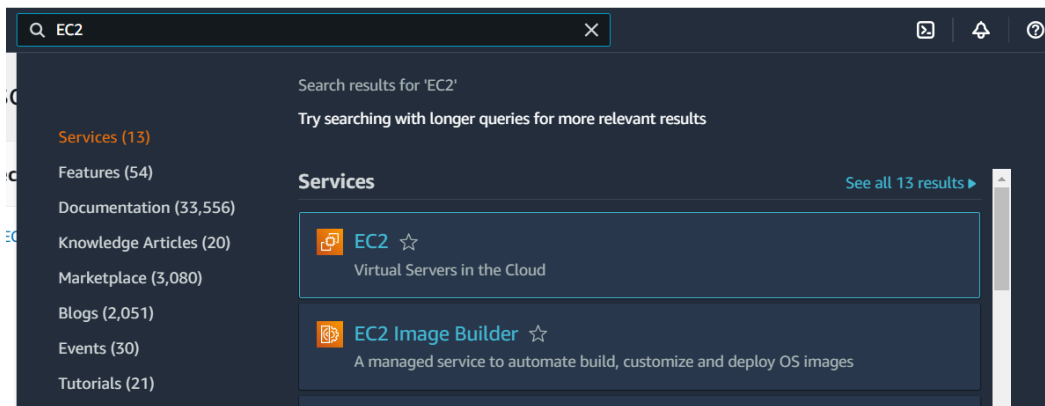
In this lab, you will learn how to:

- Create an EC2 instance (t2.micro)
- Configure a security group for Remote Desktop Protocol (RDP) access
- Connect to the instance via RDP
- Learn about the Stop, Reboot, and Terminate operations

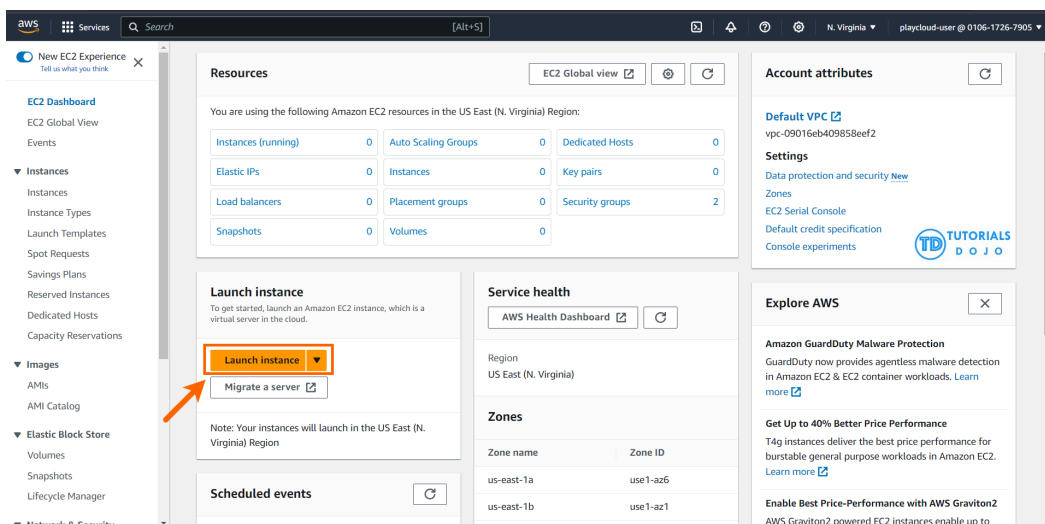
Lab Steps

Creating an Amazon EC2 instance (Windows)

1. Navigate to the search bar, type "EC2", and click to open the EC2 Dashboard.



2. Click on the 'Launch Instance' button.



3. In the "Name and tags" section, you can add a name and create tags as key/value pairs. It's recommended to tag AWS resources in production environments to stay organized, but it's not mandatory. You can skip this section if you don't want to create any tags for this lab.


4. You will need to select an Amazon Machine Image (AMI), which is basically a template of an Operating System platform that you can use as a foundation to create your instance.


For this lab, choose Windows.


▼ 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


Quick Start



Amazon Linux



macOS


Ubuntu


Windows


Red Hat


SUSE Linux


[Browse more AMIs](#)
Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)


Microsoft Windows Server 2022 Base
ami-005f8adf84f8c5057 (64-bit (x86))
Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible ▼

Description
Microsoft Windows Server 2022 Full Locale English AMI provided by Amazon

Architecture	AMI ID
64-bit (x86)	ami-005f8adf84f8c5057


Verified provider



5. For the EC2 instance type, choose t2.micro.


6. In the Key pair section, you can create a new key pair by clicking on the "Create new key pair" button. Once you do this, enter "my-key-pair" as the name of the key pair, keep the default values for Key pair type and Private key file format, and then click the "Create key pair" button. This will initiate the download of the key pair as a file named "my-key-pair.pem" on your local system. This file contains a private key that you can use to connect to the EC2 instance.

▼ 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

 [Create new key pair](#)

Create key pair

Key pair name

Key pairs allow you to connect to your instance securely.

my-key-pair

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 your computer. **You will need it later to connect to your instance.** [Learn more](#) 

Cancel

Create key pair

7. In the Network Settings section, ensure that Allow RDP traffic from the checkbox is checked and Anywhere is selected under Security groups (Firewall).

▼ Network settings

Info

Edit

Network

Info

vpc-09016eb409858eef2

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-7' 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

☐ Allow HTTP traffic from the internet

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

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.

AWS Warning: The default configuration for the security group that is about to be created will allow RDP access from any source IP address (0.0.0.0/0). This warning is to remind you that production environments should have more restrictive security controls. However, for the purposes of this lab, this configuration is acceptable.

8. In the Configure storage section, ensure the default values of 8 GiB and gp2 Root volume are selected.

▼ Configure storage

Info

Advanced

1x

30

GiB

gp2

Root volume (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

0 x File systems



Edit

9. Expand the section by clicking on Advanced Details, and take a moment to review the available configurations.

▼ Advanced details Info



Domain join directory Info

Select ▼

 [Create new directory](#) 

IAM instance profile Info

Select ▼

 [Create new IAM profile](#) 

Hostname type Info

IP name ▼

DNS Hostname Info

☒ Enable IP name IPv4 (A record) DNS requests

☒ Enable resource-based IPv4 (A record) DNS requests

☐ Enable resource-based IPv6 (AAAA record) DNS requests

Instance auto-recovery Info

Select ▼

Shutdown behavior Info


Stop ▼

Stop - Hibernate behavior Info

Select ▼

Termination protection Info

Select ▼



10. Before clicking on the 'Launch instance' button to create your instance, make sure to review all of your settings.

▼ Summary



Number of instances [Info](#)

1

Software Image (AMI)

Microsoft Windows Server 2022 ...[read more](#)
ami-005f8adf84f8c5057

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 30 GiB

Cancel

Launch instance

[Review commands](#)

11. After clicking on the 'Launch instance' button, a confirmation page will appear to let you know that the process has started.

[EC2](#) > [Instances](#) > Launch an instance



✓ Success

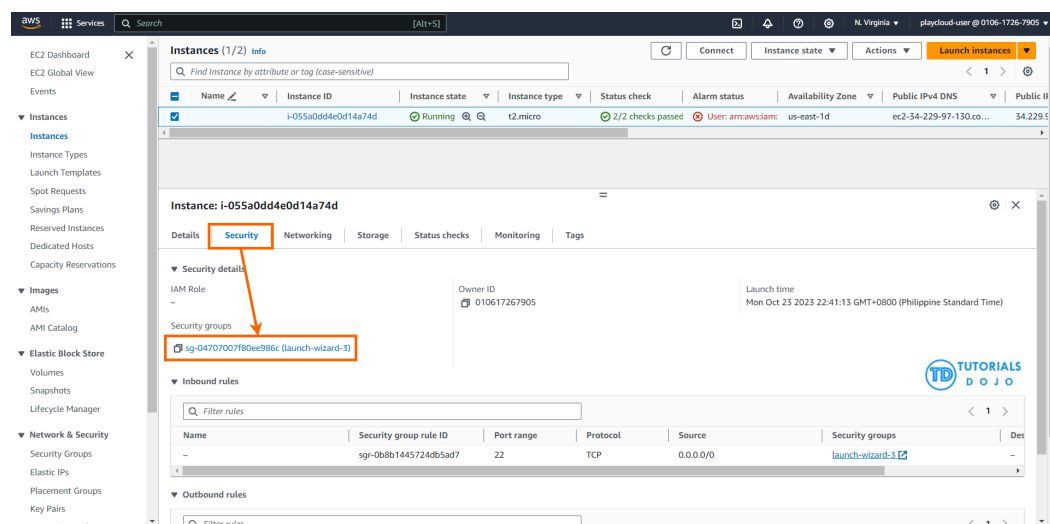
Successfully initiated launch of instance ([i-0376fa7b74cbf04bb](#))

▼ Launch log

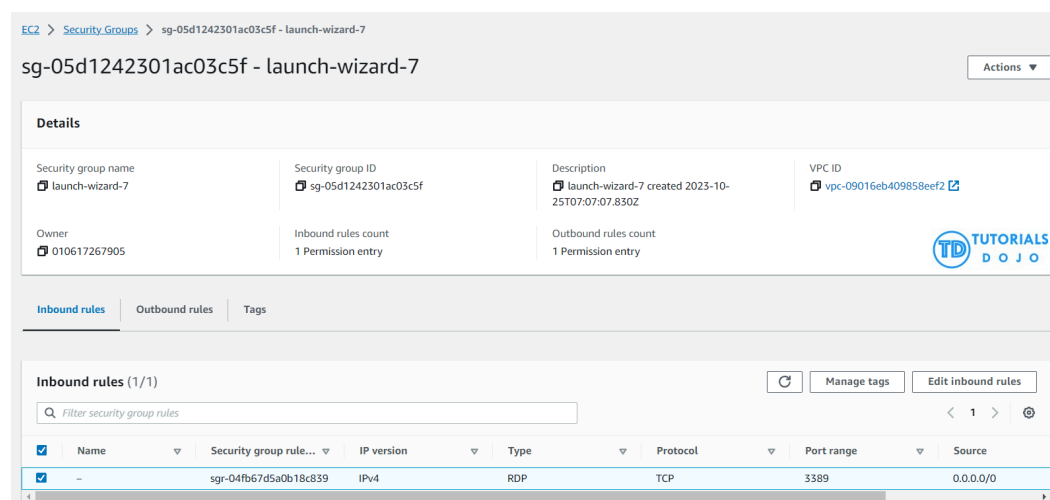
Initializing requests	✓ Succeeded
Creating security groups	✓ Succeeded
Creating security group rules	✓ Succeeded
Launch initiation	✓ Succeeded

Configuring a security group for Remote Desktop Protocol (RDP) access

1. Go to EC2 Dashboard and click the “Instances (running)” under Resources.
2. Select the instance you want to set up Security groups for by clicking the checkbox.
3. Navigate to the Security tab. Then, click on the security group ID, which typically begins with “sg-”.



4. To connect to your Windows instance using RDP from your IP address, you can add rules to a security group.



Edit inbound rules [Info](#)

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

Security group rule ID	Type	Protocol	Port range	Source	Description - optional
sgr-0aee4dc19d28bb1b	SSH	TCP	22	My IP Custom Anywhere-IPv4 Anywhere-IPv6 My IP	

[Add rule](#) [Cancel](#) [Preview changes](#) [Save rules](#)

To enhance the security of your instance, it is important to only authorize a specific IP address or range of addresses when setting up a rule to access it. Using 0.0.0.0/0 will allow all IPv4 addresses to access your instance via RDP. Similarly, using ::/0 will enable all IPv6 addresses to access your instance. To avoid these two options and provide a more secure solution, it is recommended to specify a particular IP address or range of addresses.

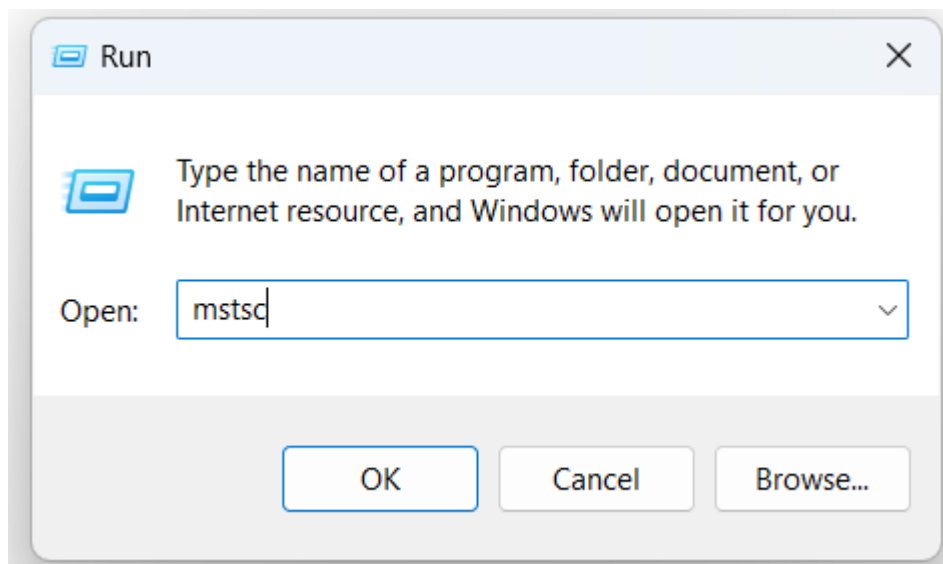
Connecting to the instance through RDP

1. After launching an instance, it may take a few minutes for it to be ready for connection.
2. Find the public DNS name or IP address of your instance. You'll use this to connect.

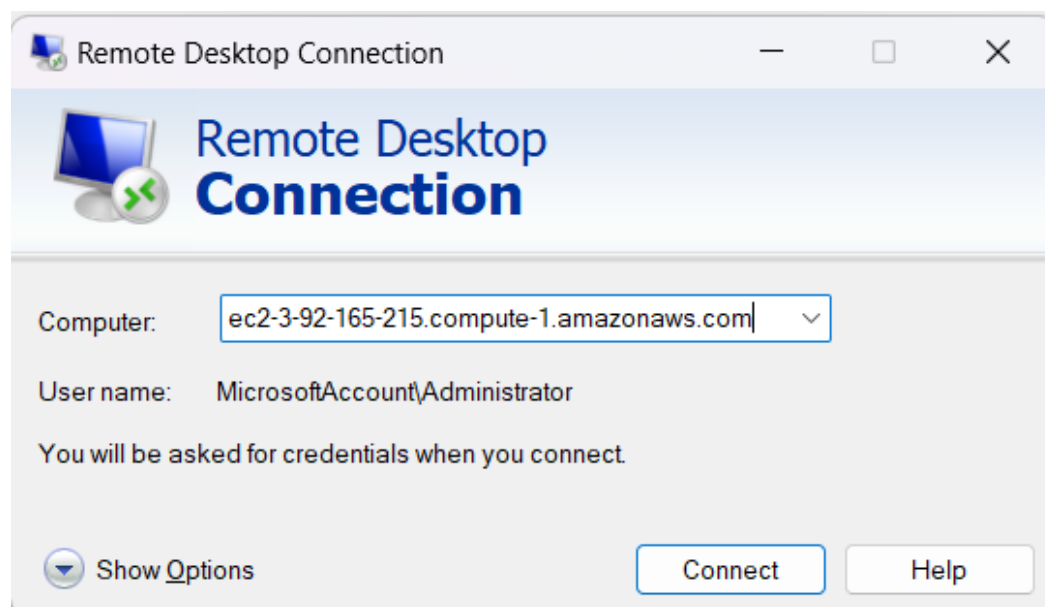
The screenshot shows the AWS Management Console interface. On the left, the navigation menu includes 'Instances', 'Images', 'Elastic Block Store', and 'Network & Security'. The main panel displays the 'Instances' page with a table of instances. The instance 'i-055a0dd4e0d14a74d' is selected and its details are shown. The 'Networking' tab is active, displaying the following information:

- Public IPv4 address:** 3.87.80.110 (with a link to 'open address')
- Public IPv4 DNS:** ec2-3-87-80-110.compute-1.amazonaws.com (with a link to 'open address')
- Subnet ID:** subnet-08d517815803970d8 (with a link to 'open address')
- Availability zone:** us-east-1d
- Private IPv4 addresses:** 172.31.22.188
- Private IP DNS name (IPv4 only):** ip-172-31-22-188.ec2.internal
- VPC ID:** vpc-09016eb409858eef2 (with a link to 'open address')
- Secondary private IPv4 addresses:** -
- Outpost ID:** -
- Carrier IP addresses (ephemeral):** -
- Answer RBN DNS hostname IPv4:** Disabled

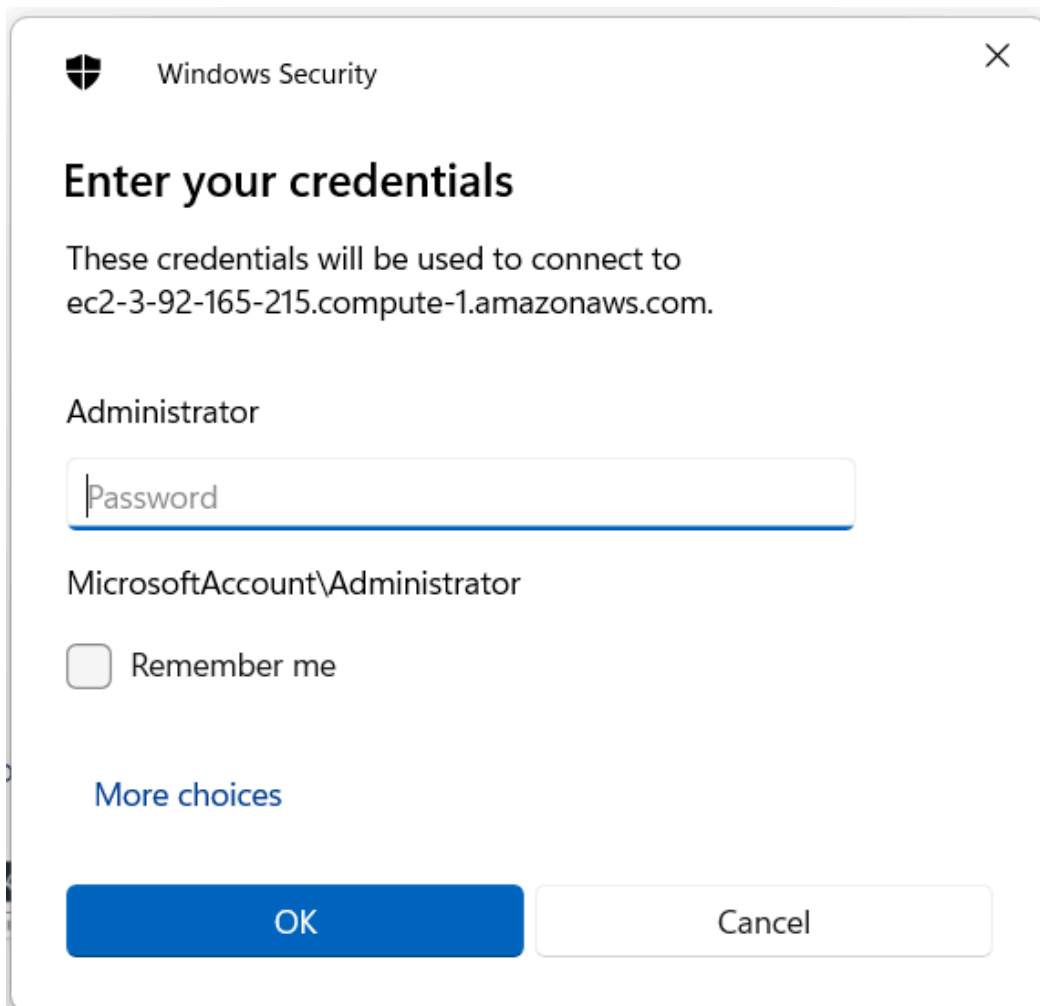
3. On your local machine, open the Remote Desktop Client application. You can do this by pressing Win + R, typing "mstsc," and hitting Enter on Windows. On macOS, you can use the "Remote Desktop Connection" app or other RDP clients like Microsoft Remote Desktop from the App Store.



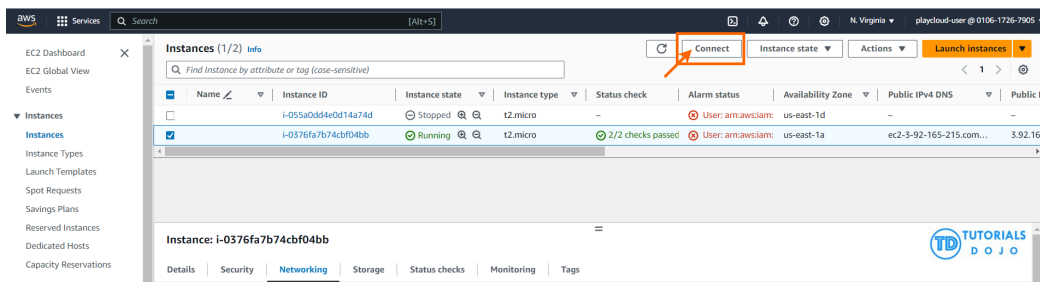
4. In Remote Desktop Connection, enter the public IP address or hostname of the Windows instance you want to connect to in the "Computer" field.



5. Click the "Connect" button to initiate the RDP connection.



6. You will be prompted to enter your Windows instance username and password which can be found under the Connect settings of your instance.



- Under RDP Client, you can find here the Username and Password.

Connect to instance [Info](#)

Connect to your instance i-0376fa7b74cbf04bb using any of these options

Session Manager
RDP client
EC2 serial console

Instance ID
i-0376fa7b74cbf04bb

Connection Type

☒ Connect using RDP client
Download a file to use with your RDP client and retrieve your password.

☐ Connect using Fleet Manager
To connect to the instance using Fleet Manager Remote Desktop, the SSM Agent must be installed and running on the instance. For more information, see [Working with SSM Agent](#)

You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:

Download remote desktop file

When prompted, connect to your instance using the following details:

Public DNS
ec2-3-92-165-215.compute-1.amazonaws.com

User name
Administrator

Password
Get password

If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.

Cancel

- Click the Get password.
- Upload the key pair associated with your instance.

Get Windows password [Info](#)

Use your private key to retrieve and decrypt the initial Windows administrator password for this instance.

Instance ID
i-0376fa7b74cbf04bb

Key pair associated with this instance
my-key-pair

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

Upload private key file

Private key contents - optional

Private key contents

Cancel
Decrypt password

- After uploading the file, you need to click on the “Decrypt Password” button.

EC2 > Instances > i-0376fa7b74cbf04bb > Get Windows password

Get Windows password [Info](#)

Use your private key to retrieve and decrypt the initial Windows administrator password for this instance.

Instance ID
i-0376fa7b74cbf04bb

Key pair associated with this instance
my-key-pair

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

☒ my-key-pair.pem
1.674KB

Private key contents - optional

```
-----BEGIN RSA PRIVATE KEY-----
MIIeowIBAAKCAQEAh3qoG0EoHizkLfw/bA3UyQwRZV3AijEpzLMu4QYPpUZCvKSL
JiLyYqfEOzO9f4iht+CAti1ihD3YkXOuA1AKsEpVsyKLWKKXGehDTzRG0MSZyJGL
wYlgIEyXLZTrcD/4jXNgz1X9XQfPmQrZkQxTxkB3H1bkNAO3Pt9+zwY7lcrqjlyq
iDCSgSL/HlmvrirMfRXNC2PmeC9cbf4+7xoo1y5H6kASHbLwA4G7E1r5yZzuu9Na
Wc08iAkyPIQvO8UQ57qHRnGsGI++Naupm+Ft4Em8iZux90k2xLejFzeg8pUT4zkb
3dweZDAApBHNauRt+VOL2bk+DB8fPcjs4sV6wIDAQABAoIBADF7GurZYUOMKEqg
9skARDcpsTDUjP3r9thMmVKWZCB5CObdO3QyT1S48aoxu4RY4rfFxxbGfLTP4ck9
-----
```

- Once done, you will be directed to the “Connect to Instance” page, where the RDP password will be generated automatically.

Connect to instance [Info](#)

Connect to your instance i-0376fa7b74cbf04bb using any of these options

Session Manager

RDP client

EC2 serial console

Instance ID
i-0376fa7b74cbf04bb

Connection Type

☒ **Connect using RDP client**
Download a file to use with your RDP client and retrieve your password.

☐ **Connect using Fleet Manager**
To connect to the instance using Fleet Manager Remote Desktop, the SSM Agent must be installed and running on the instance. For more information, see [Working with SSM Agent](#)

You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:


Download remote desktop file


When prompted, connect to your instance using the following details:

Public DNS
ec2-3-92-165-215.compute-1.amazonaws.com

User name
Administrator

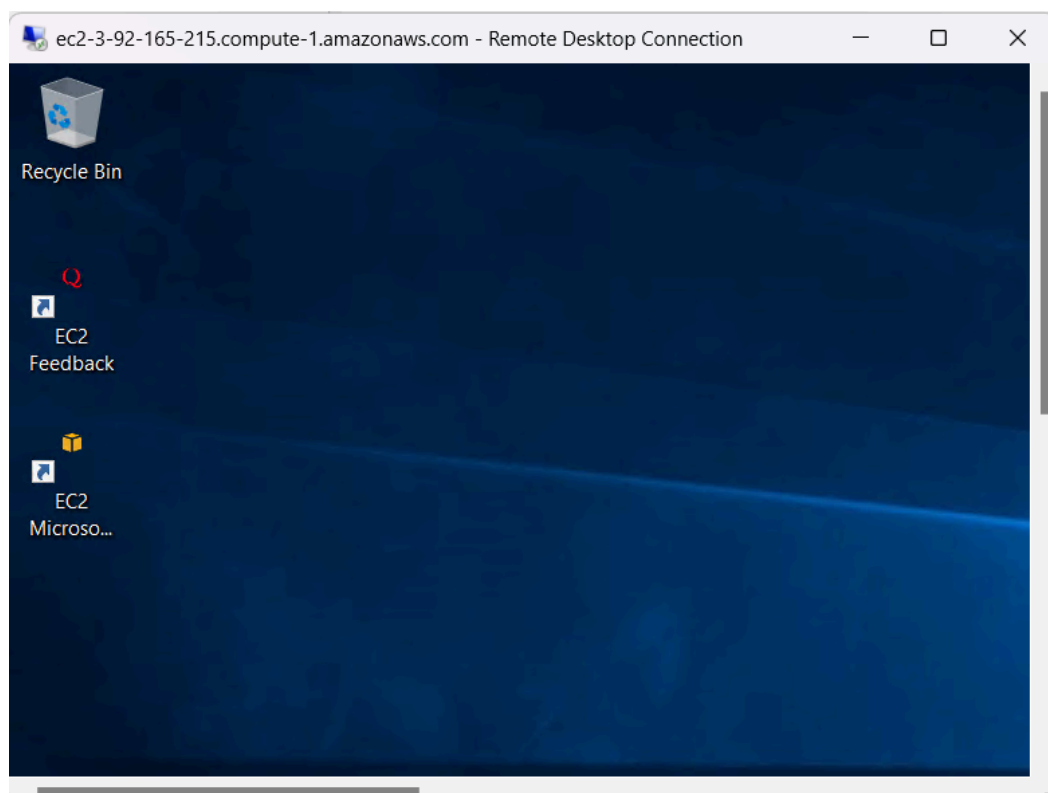
Password
IXWV71OvQ?wl;?ro-Aj-NM2GnKN9Ph.Z

 **TUTORIALS**
DOJO

 If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.

Cancel

7. After entering the credentials, click "OK" or "Connect" to start the connection. You might see a warning about the certificate; this is normal. You can choose to connect anyway.



PEM (Privacy Enhanced Mail) and PPK (PuTTY Private Key) are both formats for storing private keys, which are used in public key cryptography. Here's a comparison of the two:

PEM:

- It is a base64 container format for encoding keys and certificates.
- It is kind of the de facto standard for Linux, Mac, and Windows PowerShell users.
- The .pem file is what you download from AWS when you create your key pair. This is a one-time download, and you cannot download it again.

PPK:

- PPK is a format used by PuTTY, a Windows SSH client.
- It does not support the .pem format. Hence, you have to convert it to .ppk format using PuTTYgen.
- To use a PPK file with PuTTY, you need to load the PPK file in PuTTYgen and then save it as a private key. You can then use this private key to log into your server.

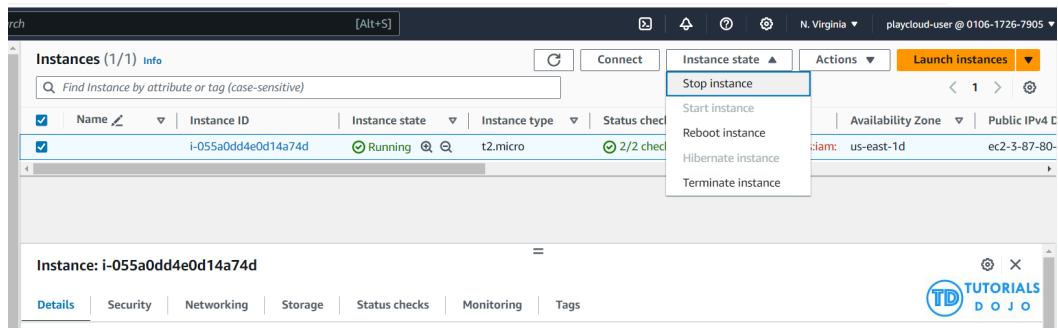
It's crucial to keep private keys secure and never share them with unauthorized individuals as they are essential for secure communication over networks.

Learn about the Stop, Reboot, and Terminate operations

Stopping an EC2 instance

Steps:

- Navigate to the EC2 dashboard.
- Select the instance you want to stop.
- Click the "Actions" button.
- Click the "Instance State" option.
- Click "Stop" from the dropdown menu.



Effects:

When you stop an instance, the following is lost:

- Data stored on the RAM.
- Data stored on the instance store volumes.
- The public IPv4 address that Amazon EC2 automatically assigns to the instance upon launch or start. To retain a public IPv4 address that never changes, you can associate an Elastic IP address with your instance.

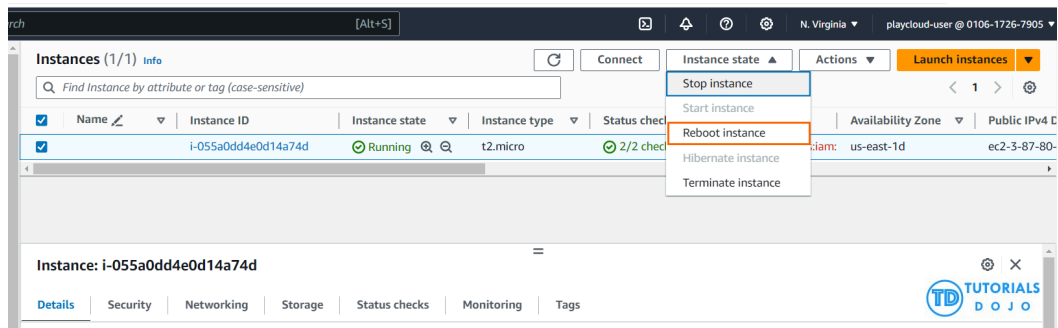
When you stop an instance, the following *persists*:

- Any attached Amazon EBS volumes.
- Data is stored on the attached Amazon EBS volumes.
- Private IPv4 addresses.
- IPv6 addresses.
- Elastic IP addresses associated with the instance. Note that you are charged for the associated Elastic IP addresses when the instance is stopped.

Rebooting an EC2 instance

Steps:

- Navigate to the EC2 dashboard.
- Select the instance you want to reboot.
- Click the "Actions" button.
- Click the "Instance State" option.
- Click "Reboot" from the dropdown menu.



Effects:

An instance reboot is equivalent to an operating system reboot. In most cases, it takes only a few minutes to reboot your instance.

When you reboot an instance, it keeps the following:

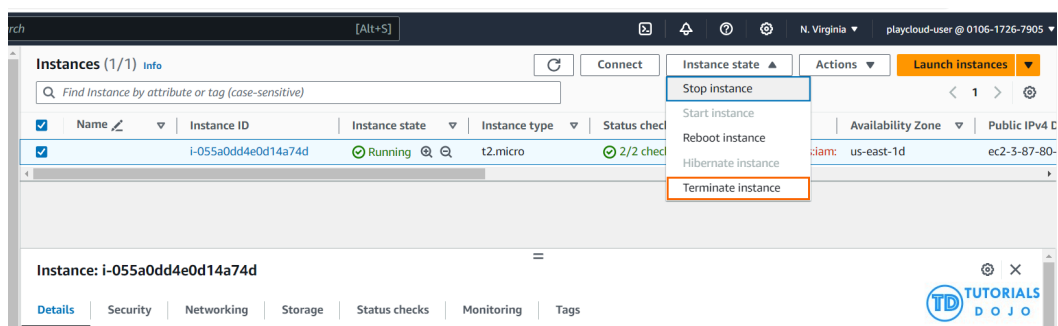
- Public DNS name (IPv4)
- Private IPv4 address
- Public IPv4 address
- IPv6 address (if applicable)
- Any data on its instance store volumes

Rebooting an instance doesn't start a new instance billing period (with a minimum one-minute charge), unlike stopping and starting your instance.

Terminating an EC2 instance:

Steps:

- Navigate to the EC2 dashboard.
- Select the instance you want to terminate.
- Click the "Actions" button.
- Click the "Instance State" option.
- Click "Terminate" from the dropdown menu.



Effects:

- The instance will be shut down, and the virtual machine that was provisioned for you will be permanently taken away, and you will no longer be charged for instance usage.
 - Any data that was stored locally on the instance will be lost.
 - Any attached EBS volumes will be detached and deleted unless they are set to persist after termination.
-