St. Francis Institute of Technology
(An Autonomous Institution)
AICTE Approved | Affiliated to University of Mumbai

A+ Grade by NAAC: CMPN, EXTC, INFT NBA Accredited: ISO 9001:2015 Certified

Department of Information Technology

A.Y. 2025-2026
Class: BE-IT A/B, Semester: VIII
Subject: Cloud Computing Lab

Student Name: Durva Kadam Student Roll No: 23

Experiment – 3 : Infrastructure as A Service

Aim: To study and Implement Infrastructure As a Service using different cloud platform AWS / GC / AZURE (Free Tier Cloud Platforms).

Objective: After performing the experiment, the students will be able to –

- Launch an instance
- install any security updates
- execute bootstrap script
- EC2 instance store life
- access the instance metadata from the OS
- Amazon EBS Volume life

Lab objective mapped : ITL802 : To **implement** IAAS services.

Prerequisite: Concept of Operating System, Infrastucture.

Requirements: Cloud Login**,** Desktop, Browser, Internet etc.

Pre-Experiment Theory:

CLOUD SERVICES

IAAS.

Procedure
Launch and Connect to a Linux Instance, log in with SSH, and install any security updates.

1. Launch an instance in the Amazon EC2 console.

2. Choose the Amazon Linux AMI.

3. Choose the t2.micro instance type.

4. Launch the instance in the default VPC.

5. Assign the instance a public IP address.

6. Add a tag to the instance of Key: Name, Value: Exercise 3.1.

7. Create a new security group called Cert Book.

8. Add a rule to Cert Book allowing SSH access from the IP address of your workstation (www.WhatsMyIP.org is a good way to determine your IP address).

9. Launch the instance.

10. When prompted for a key pair, choose a key pair you already have or create a new one and download the private portion.

Amazon generates a keyname.pem file, and you will need a keyname.ppk file to connect to the instance via SSH. Puttygen.exe is one utility that will create a .ppk file from a .pem file.

11. SSH into the instance using the public IP address, the user name ec2-user, and the keyname.ppk file.

12. From the command-line prompt, run sudo yum update—security -y.

13. Close the SSH window.

Launch a Windows Instance with Bootstrapping

Specify a very simple bootstrap script. then confirm that the bootstrap script was executed on the instance.

1. Launch an instance in the Amazon EC2 console.

2. Choose the Microsoft Windows Server 2012 Base AMI.

3. Choose the t2.micro instance type.

4. Launch the instance in either the default VPC.

5. Assign the instance a public IP address.

6. In the Advanced Details section, enter the following text as UserData:

<script>

md c:\temp

</script>

7. Add a tag to the instance of Key: Name, Value: Exercise 3.2.

8. Use the Cert Book security group from Exercise 3.1.

9. Launch the instance.

10. Use the key pair from Exercise 3.1.

11. On the Connect Instance UI, decrypt the administrator password and then download the RDP file to attempt to connect to the instance. Your attempt should fail because the Cert Book security group does not allow RDP access.

12. Open the Cert Book security group and add a rule that allows RDP access from your IP address.

13. Attempt to access the instance via RDP again.

14. Once the RDP session is connected, open Windows Explorer and confirm that the c:\temp folder has been created.

15. End the RDP session and terminate the instance.

Post-Experiments Exercise

Create an Amazon EBS Volume and observe that it remains after the instance is terminated. Amazon EBS volume persists beyond the life of an instance.

1. Launch an instance in the Amazon EC2 console.

2. Choose the Amazon Linux AMI.

3. Choose the t2.micro instance type.

4. Launch the instance in the default VPC.

5. Add a second Amazon EBS volume of size 10 GB. Note that the Root Volume is set to Delete on Termination.

7. Add a tag to the instance of Key: Name, Value

8. Use the Cert Book security group from earlier exercises.

9. Launch the instance.

10. Find the two Amazon EBS volumes on the Amazon EBS console. Name them both Exercise 3.6.

11. Terminate the instance.

Notice that the boot drive is destroyed, but the additional Amazon EBS volume remains and now says Available. Do not delete the Available volume.

Extended Theory:

1. What is bootstrap in a computer? (to be written in hand)
2. RDP (to be written in hand)
3. Discuss procedure to connect to your Linux instance using PuTTY (soft copy form)

Results/Calculations/Observations:

Fill the following observation tables-(to be written in hand)

Sr. No		
1.	SSH port no	
2.	Linux VM Public IP	
3.	t2.micro RAM and CPU capacity	
4.	Decrypted pwd length	
5.	name of security grp for windows instance	

Post Experimental Exercise-

Questions:

1. Short note on EBS volume?(soft copy form)

Conclusion:

1. Write what was performed in the experiment
2. Mention a few applications of what was studied.
3. Write the significance of the studied topic

References:

[1] [Online] https://download.virtualbox.org/virtualbox/5.1.22/UserManual.pdf
[2] [Online] https://phoenixnap.com/kb/virtualbox-vs-vmware
[3] Samjhana Rayamajhi, Zinnia Sultana "Comparative Performance Analysis of the Virtualization Technologies in Cloud Computing", Volume 03, Issue 09 (September 2014),IJERT

Extended Theory:

3. Discuss procedure to connect to your Linux instance using PuTTY (soft copy form)
ANS: Procedure to Connect to a Linux Instance Using PuTTY

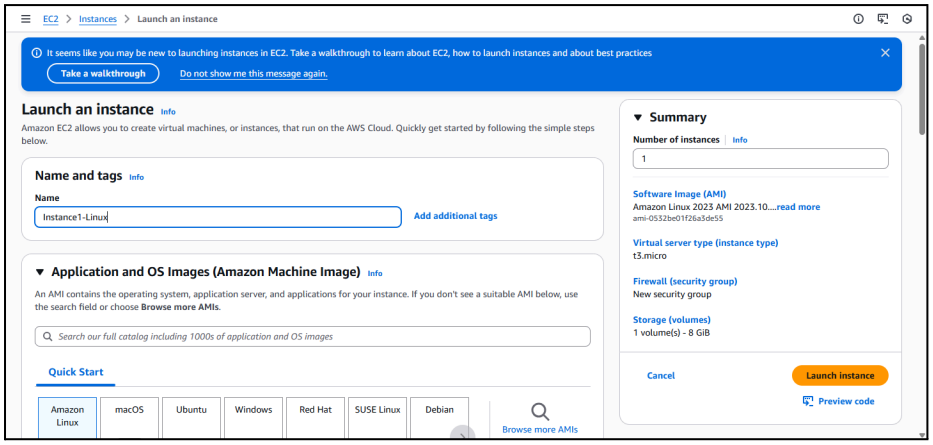
PuTTY is an SSH client used on Windows systems to establish a secure remote connection with a Linux instance.

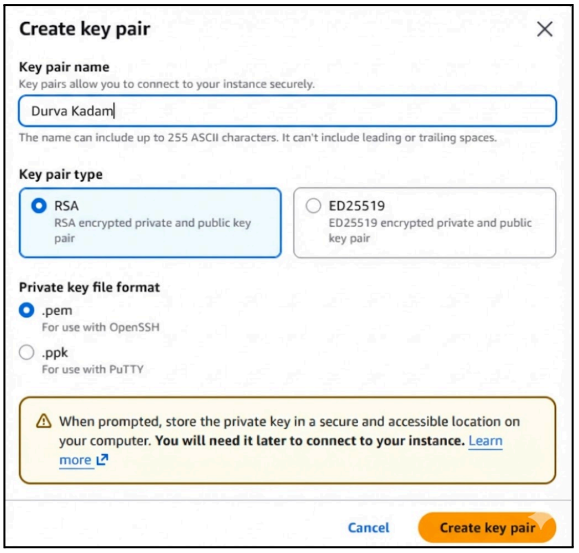
1. First, PuTTY software is downloaded and installed on the Windows system from the official PuTTY website.
2. The required connection details such as the public IP address of the Linux instance, SSH port number (default 22), username, and private key file are collected before initiating the connection.
3. If the private key is available in .pem format, it is converted into .ppk format using PuTTYgen, as PuTTY supports only .ppk keys.
4. After launching PuTTY, the public IP address (or hostname) of the Linux instance along with the username is entered in the **Host Name** field, and the connection type is set to **SSH**.
5. The private key file (.ppk) is then configured by navigating to **Connection → SSH → Auth** and browsing to select the key file.
6. Once the configuration is completed, the session is opened by clicking the **Open** button, and the security alert (if shown) is accepted.
7. After successful authentication, the Linux terminal window appears, indicating that the connection to the Linux instance has been established successfully.

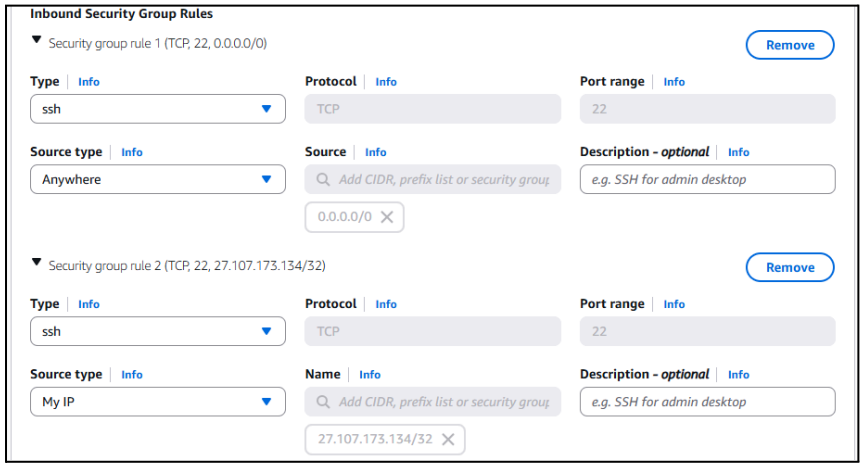
Post Experimental Exercise-
Questions:

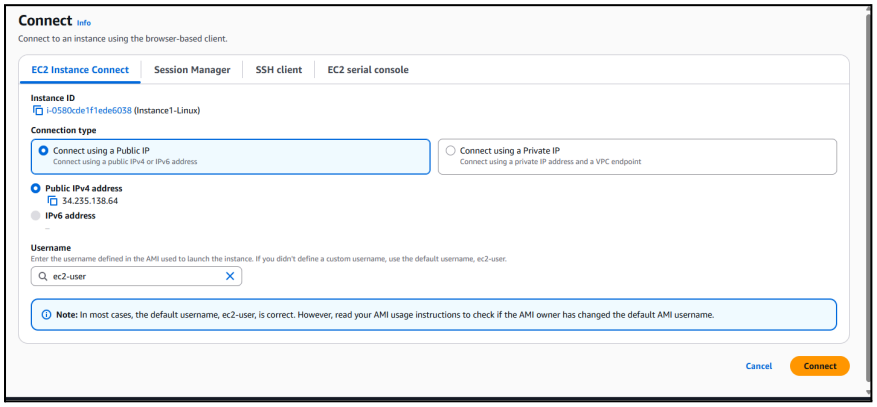
1. Short note on EBS volume?(soft copy form)
ANS:

1. Amazon Elastic Block Store (EBS) is a block-level storage service provided by Amazon Web Services for Amazon EC2 instances.
2. An EBS volume works like a virtual hard disk and can be attached or detached from EC2 instances as required.
3. It provides persistent storage, so data remains safe even if the EC2 instance is stopped, rebooted, or terminated.
4. EBS volumes are automatically replicated within the same Availability Zone to ensure high durability and reliability.
5. EBS supports multiple volume types such as General Purpose SSD, Provisioned IOPS SSD, Throughput Optimized HDD, and Cold HDD.
6. Users can increase or decrease the size of an EBS volume without stopping the instance.
7. EBS supports snapshots, which allow users to create backups and restore volumes when needed.
8. It provides encryption to protect data at rest and in transit.
9. EBS volumes are commonly used for storing operating systems, databases, applications, and log files.


EC2 > Instances > Launch an instance
It seems like you may be new to launching instances in EC2. Take a walkthrough to learn about EC2, how to launch instances and about best practices
Take a walkthrough
Do not show me this message again.
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
Instance1-Linux
Add additional tags
Application and OS Images (Amazon Machine Image) Info
An AMI contains the operating system, application server, and applications for your instance. If you don't see a suitable AMI below, use the search field or choose Browse more AMIs.
Search our full catalog including 1000s of application and OS images
Quick Start
Amazon Linux
macOS
Ubuntu
Windows
Red Hat
SUSE Linux
Debian
Browse more AMIs
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.10....read more
ami-0532be01f26a3de55
Virtual server type (instance type)
t3.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Cancel
Launch instance
Preview code

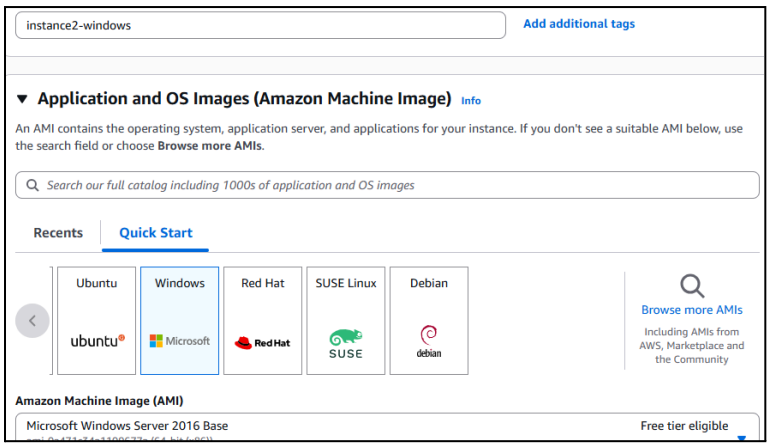

Create key pair
Key pair name
Key pairs allow you to connect to your instance securely.
Durva Kadam
The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.
Key pair type
RSA
RSA encrypted private and public key pair
ED25519
ED25519 encrypted private and public key pair
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

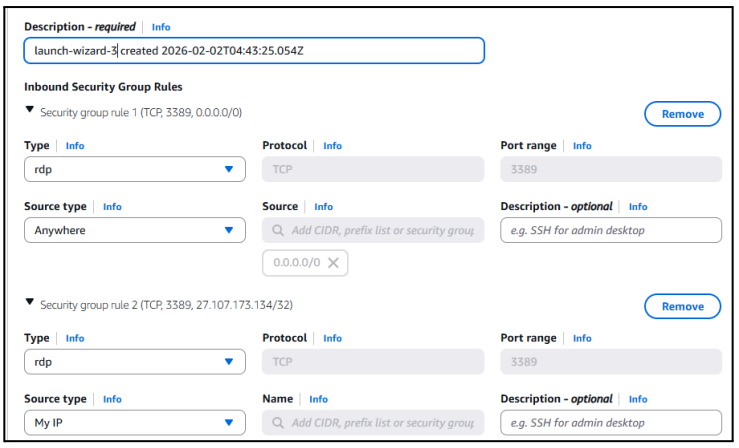

Inbound Security Group Rules
Security group rule 1 (TCP, 22, 0.0.0.0/0)
Remove
Type Info
ssh
Protocol Info
TCP
Port range Info
22
Source type Info
Anywhere
Source Info
Add CIDR, prefix list or security group
0.0.0.0/0
Description - optional Info
e.g. SSH for admin desktop
Security group rule 2 (TCP, 22, 27.107.173.134/32)
Remove
Type Info
ssh
Protocol Info
TCP
Port range Info
22
Source type Info
My IP
Name Info
Add CIDR, prefix list or security group
27.107.173.134/32
Description - optional Info
e.g. SSH for admin desktop

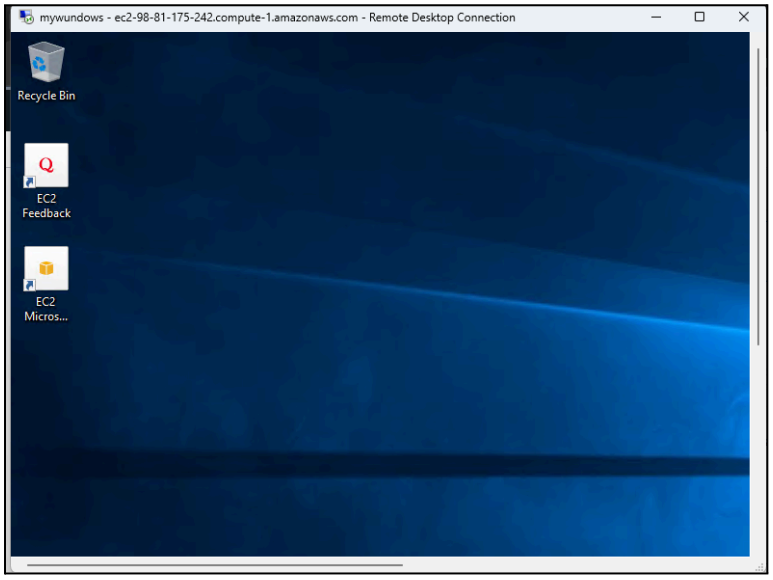

Connect Info
Connect to an instance using the browser-based client.
EC2 Instance Connect
Session Manager
SSH client
EC2 serial console
Instance ID
i-0580cde1f1ede6038 (Instance1-Linux)
Connection type
Connect using a Public IP
Connect using a public IPv4 or IPv6 address
Connect using a Private IP
Connect using a private IP address and a VPC endpoint
Public IPv4 address
34.235.138.64
IPv6 address
Username
Enter the username defined in the AMI used to launch the instance. If you didn't define a custom username, use the default username, ec2-user.
ec2-user
Note: In most cases, the default username, ec2-user, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.
Cancel
Connect

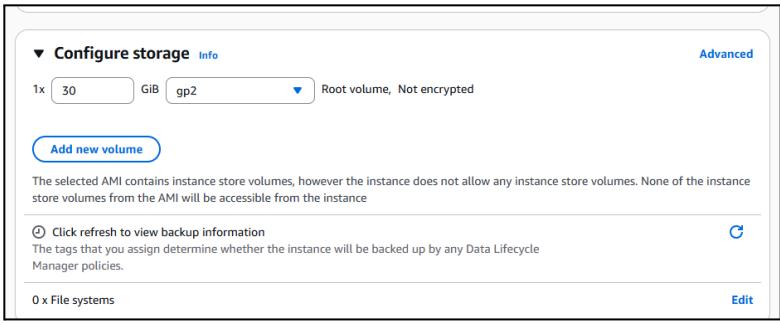

Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023
[ec2-user@ip-172-31-22-189 ~]$

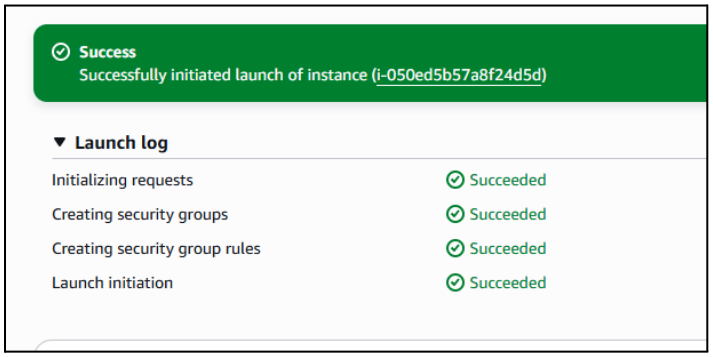
Windows

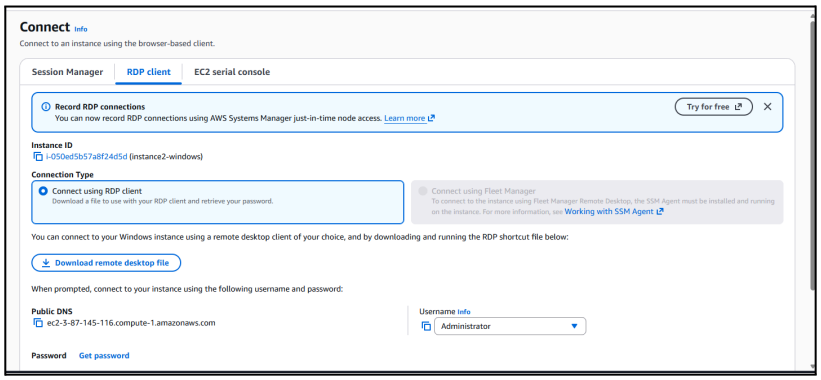

instance2-windows
Add additional tags
Application and OS Images (Amazon Machine Image) Info
An AMI contains the operating system, application server, and applications for your instance. If you don't see a suitable AMI below, use the search field or choose Browse more AMIs.
Search our full catalog including 1000s of application and OS images
Recents
Quick Start
Ubuntu
Windows
Red Hat
SUSE Linux
Debian
Browse more AMIs
Including AMIs from AWS, Marketplace and the Community
Amazon Machine Image (AMI)
Microsoft Windows Server 2016 Base
Free tier eligible


Description - required Info
launch-wizard-3 created 2026-02-02T04:43:25.054Z
Inbound Security Group Rules
Security group rule 1 (TCP, 3389, 0.0.0.0/0)
Remove
Type Info
rdp
Protocol Info
TCP
Port range Info
3389
Source type Info
Anywhere
Source Info
Add CIDR, prefix list or security group
0.0.0.0/0
Description - optional Info
e.g. SSH for admin desktop
Security group rule 2 (TCP, 3389, 27.107.173.134/32)
Remove
Type Info
rdp
Protocol Info
TCP
Port range Info
3389
Source type Info
My IP
Name Info
Add CIDR, prefix list or security group
Description - optional Info
e.g. SSH for admin desktop


mywundows - ec2-98-81-175-242.compute-1.amazonaws.com - Remote Desktop Connection
Recycle Bin
EC2 Feedback
EC2 Micros...


Configure storage Info
Advanced
1x
30
GiB
gp2
Root volume, Not encrypted
Add new volume
The selected AMI contains instance store volumes, however the instance does not allow any instance store volumes. None of the 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
Edit


Success
Successfully initiated launch of instance (i-050ed5b57a8f24d5d)
Launch log
Initializing requests
Succeeded
Creating security groups
Succeeded
Creating security group rules
Succeeded
Launch initiation
Succeeded


Connect Info
Connect to an instance using the browser-based client.
Session Manager
RDP client
EC2 serial console
Record RDP connections
You can now record RDP connections using AWS Systems Manager just-in-time node access. Learn more
Try for free
Instance ID
i-050ed5b57a8f24d5d (instance2-windows)
Connection Type
Connect using RDP client
Download a file to use with your RDP client and retrieve your password.
Connect using Fleet Manager
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 username and password:
Public DNS
ec2-3-87-145-116.compute-1.amazonaws.com
Username Info
Administrator
Password
Get password