

Cloud Computing Lab

Experiment No.: 3

Infrastructure as a Service

Experiment No. 3

1. **Aim:** To study and Implement Infrastructure as a Service using AWS
2. **Objectives:** To demonstrate the steps to create and run virtual machines inside Public cloud platform. This experiment should emphasize on creating and running Linux/Windows Virtual machine inside Amazon EC2 Compute and accessing them using RDP or VNC tools.
3. **Outcomes:** The learner will be able to

Analyze various cloud computing service models and implement them to solve the given problems.

4. **Hardware / Software Required:** Internet Connection, Internet browser.

5. **Theory:**

Infrastructure as a Service (IaaS) is one of the three fundamental service models of cloud computing alongside Platform as a Service (PaaS) and Software as a Service (SaaS). As with all cloud computing services it provides access to computing resources in a virtualized environment, “the Cloud”, across a public connection, usually the internet. In the case of IaaS the computing resource provided is specifically that of virtualized hardware, in other words, computing infrastructure. The definition includes such offerings as virtual server space, network connections, bandwidth, IP addresses and load balancers. Physically, the pool of hardware resource is pulled from a multitude of servers and networks usually distributed across numerous data centers, all of which the cloud provider is responsible for maintaining. The client, on the other hand, is given access to the virtualized components in order to build their own IT platforms.

In common with the other two forms of cloud hosting, IaaS can be utilised by enterprise customers to create cost effective and easily scalable IT solutions where the complexities and expenses of managing the underlying hardware are outsourced to the cloud provider. If the scale of a business customer’s operations fluctuate, or they are looking to expand, they can tap into the cloud resource as and when they need it rather than purchase, install and integrate hardware themselves.

IaaS customers pay on a per-use basis, typically by the hour, week or month. Some providers also charge customers based on the amount of virtual machine space they use. This pay-as-you-go model eliminates the capital expense of deploying in-house hardware and software. However, users should monitor their IaaS environments closely to avoid being charged for unauthorized services.

Because IaaS providers own the infrastructure, systems management and monitoring may become more difficult for users. Also, if an IaaS provider experiences downtime, users' workloads may be affected.

For example, if a business is developing a new software product, it might be more cost-effective to host and test the application through an IaaS provider. Once the new software is tested and refined, it can be removed from the IaaS environment for a more traditional in-house deployment or to save money or free the resources for other projects.

Leading IaaS providers include Amazon Web Services (AWS), Windows Azure, Google Compute Engine, Rackspace Open Cloud, and IBM SmartCloud Enterprise.

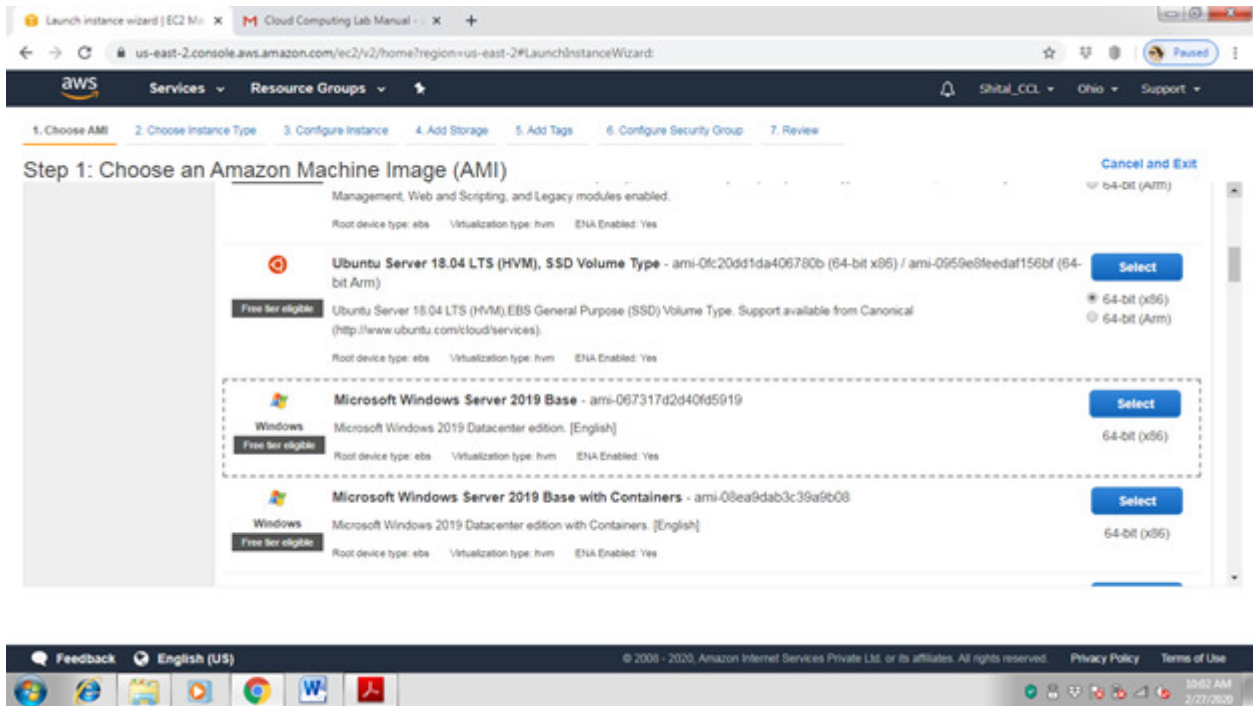
6. Procedure:

Step 1 -: Login to AWS portal and Select EC2 service from admin console

Step 2-: The EC2 resource page will appear which will show you the summary of instances.

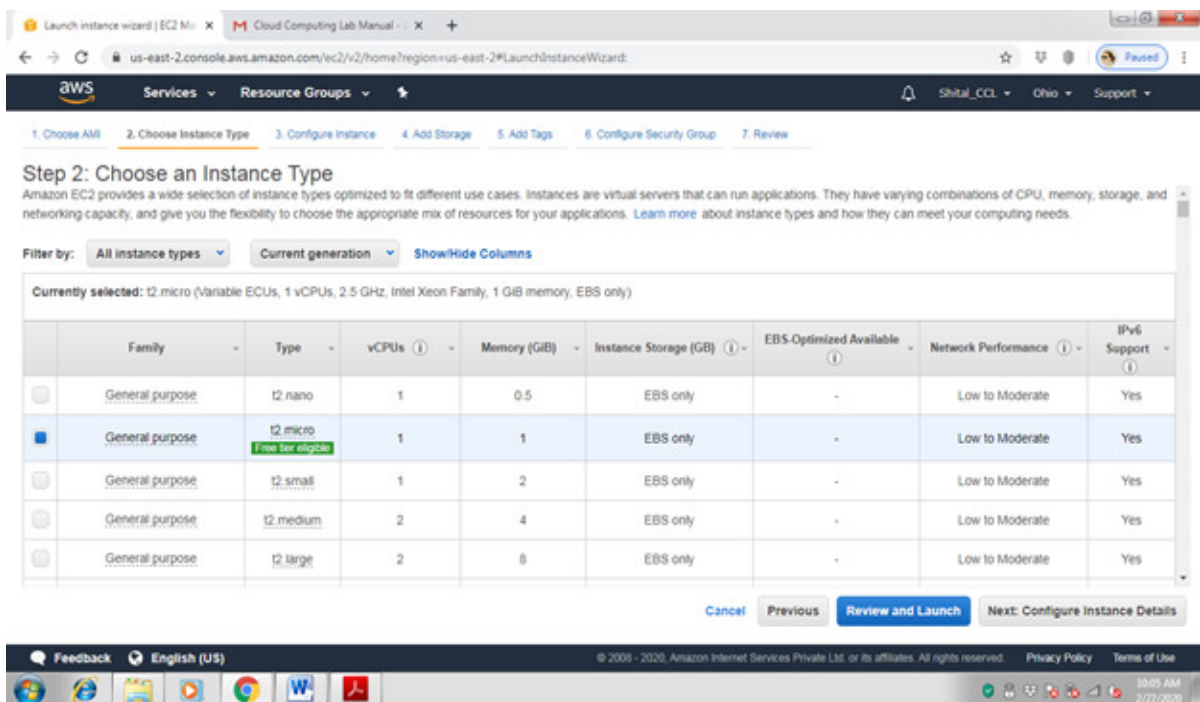
Now click on launch instance to select the VM instance type

Step 3-: Select the operating system type in AMI format. In this example we have selected Windows server instance which is eligible for free tier and click on Next.



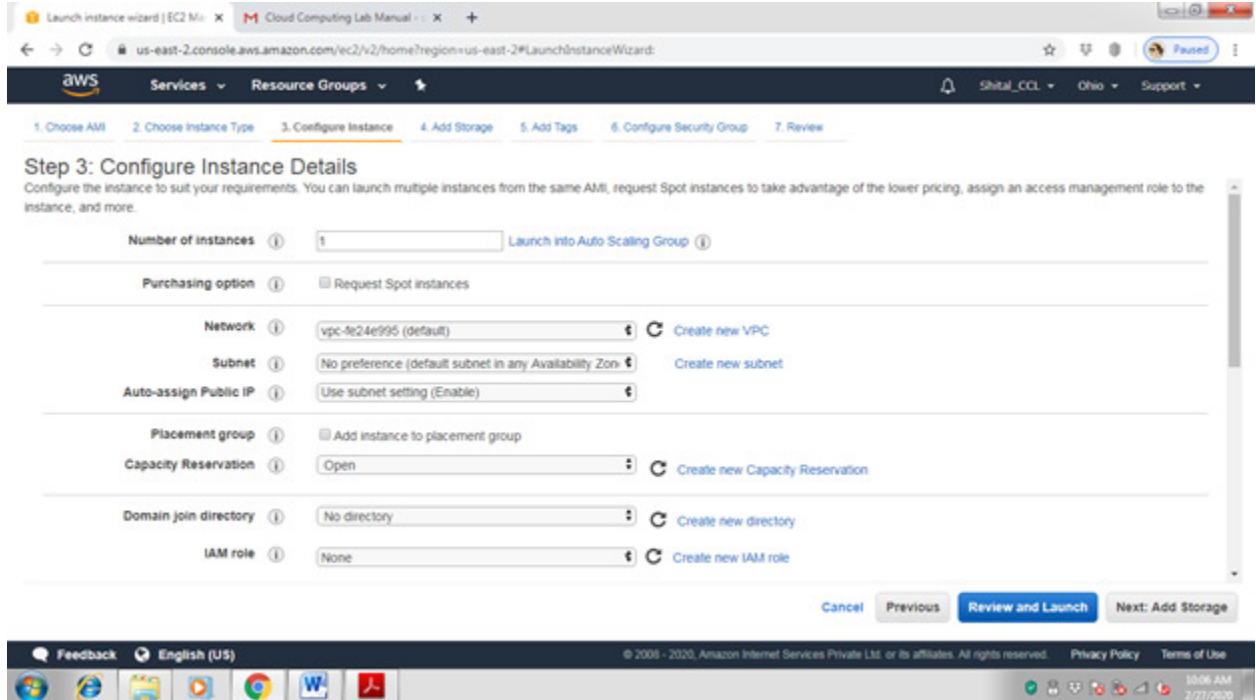
Step 4 -: Now select the hardware type for Virtual machine. In this example we have selected free tier eligible General purpose hardware and click on Next.

Step 5:- Now specify the instance details like Number of instances, networking options like VPC, Subnet or dhcp public IP etc. and click on Next



Step 6:- Specify the storage space for VM and click on Next

Step 6:- Click on Add tag to specify VM Name and click on Next



The screenshot shows the AWS Launch Instance Wizard, Step 3: Configure Instance Details. The wizard is for launching an EC2 instance in the us-east-2 region. The steps are: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Add Tags, 6. Configure Security Group, 7. Review.

Step 3: Configure Instance Details
 Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances: 1 [Launch into Auto Scaling Group](#)

Purchasing option: ☐ Request Spot instances

Network: vpc-4e24e995 (default) [Create new VPC](#)

Subnet: No preference (default subnet in any Availability Zone) [Create new subnet](#)

Auto-assign Public IP: Use subnet setting (Enable)

Placement group: ☐ Add instance to placement group

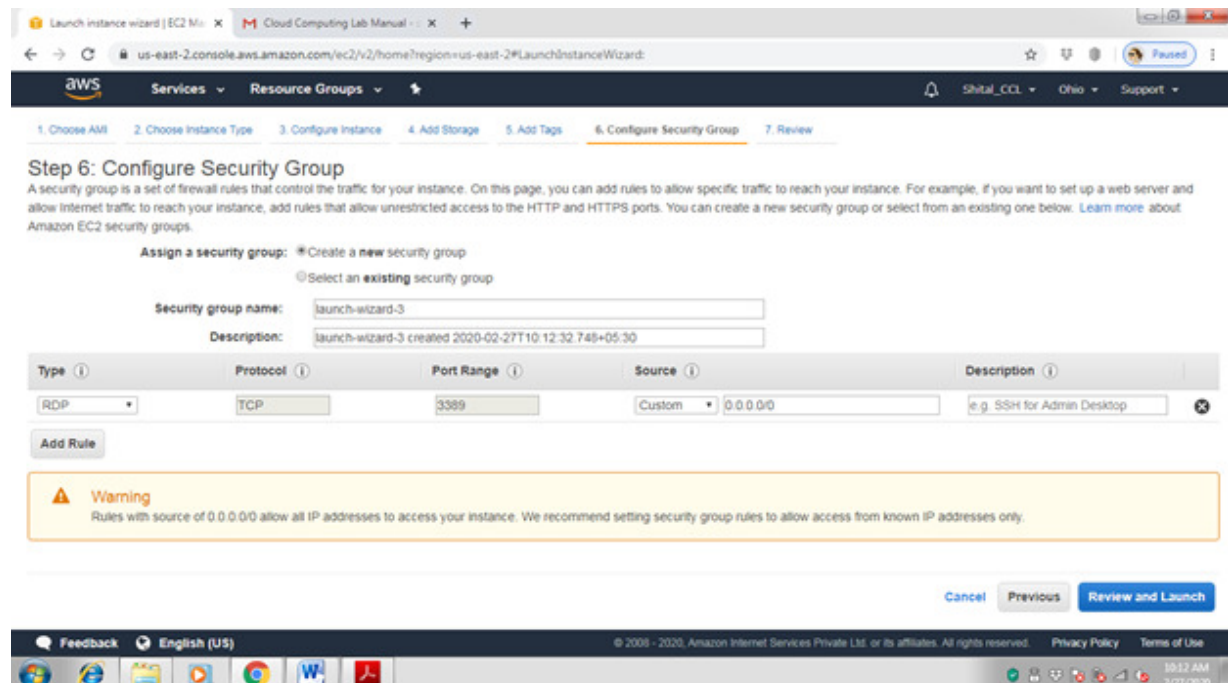
Capacity Reservation: Open [Create new Capacity Reservation](#)

Domain join directory: No directory [Create new directory](#)

IAM role: None [Create new IAM role](#)

Buttons: Cancel, Previous, Review and Launch, Next: Add Storage

Step 6:- Configure security group to provide access to VM using different protocols. In this example we have selected default RDP protocol.



The screenshot shows the AWS Launch Instance Wizard, Step 6: Configure Security Group. The wizard is for launching an EC2 instance in the us-east-2 region. The steps are: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Add Tags, 6. Configure Security Group, 7. Review.

Step 6: Configure Security Group
 A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: ☒ Create a new security group ☐ Select an existing security group

Security group name: launch-wizard-3

Description: launch-wizard-3 created 2020-02-27T10:12:32.748+05:30

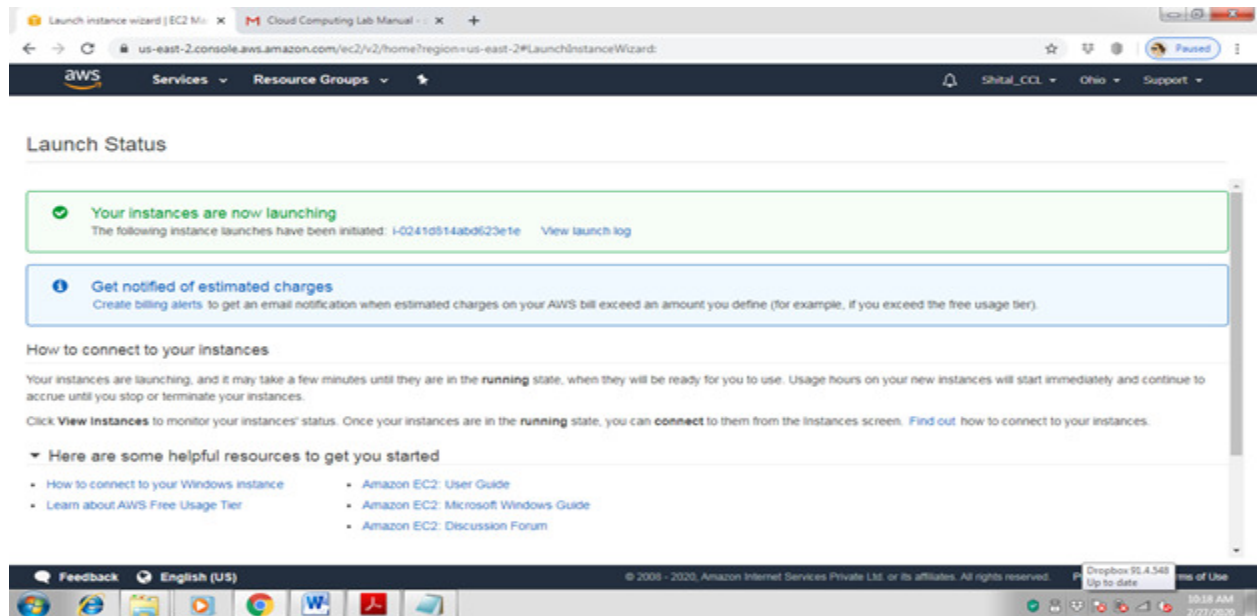
Type	Protocol	Port Range	Source	Description
RDP	TCP	3389	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop

Add Rule

Warning
 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.

Buttons: Cancel, Previous, Review and Launch

Step 7:- Now Review the instance and click on Launch button

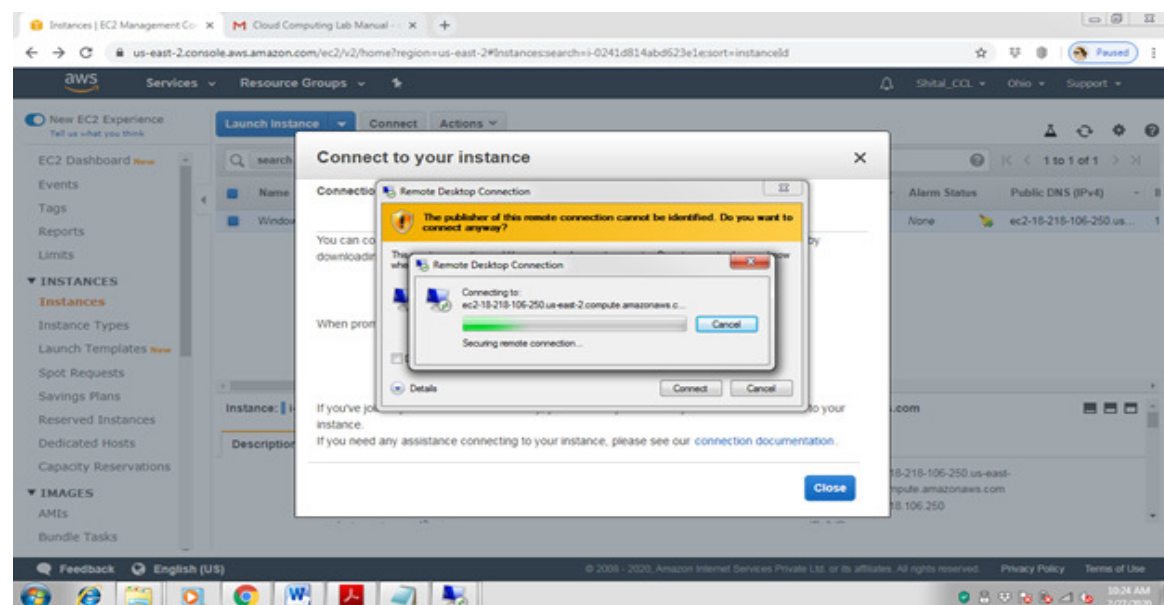


Step 8:- Now to secure VM instance, Encrypt it using public key and create a private key pair to decrypt that. Here specify key pair name and download key pair.

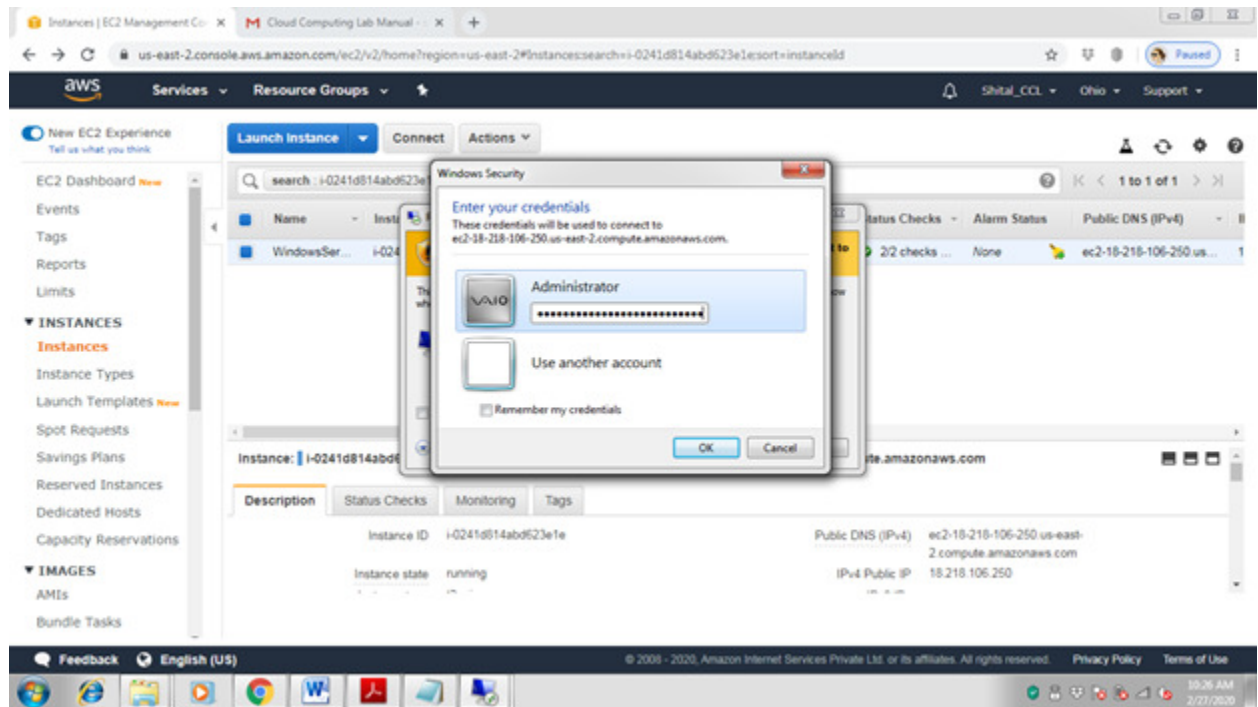
Step 8:- Finally Click on launch instance to Launch VM

Step 9:- Now from summary page click on View instance to see the instance state. After some time you will see the running instance of your VM.

Step 10:- Now Click on Connect to get the password for VM to access it over RDP protocol.

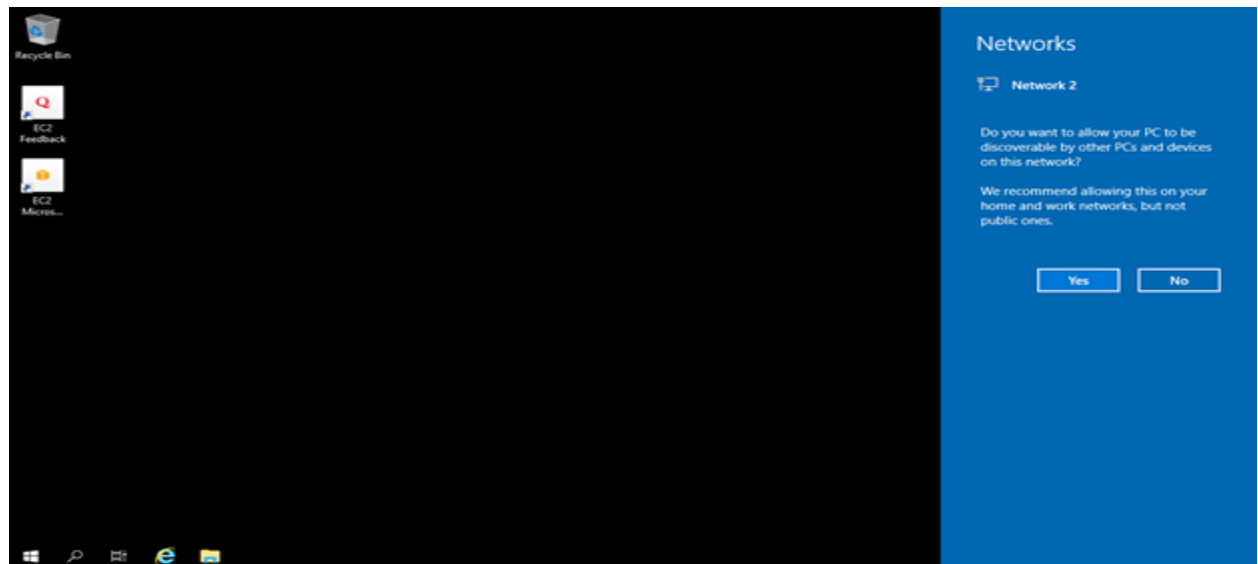


Step 11 -: Select the downloaded key pair file to decrypt the password.



Step 12 -: Now connect the instance using RDP tool by using Ip Address/DNS, username and Password decrypted in the last step.

Step 13-: Once you click on connect, you will see the running Windows virtual machine as shown below.



Step 14-: You can shut down instance by selecting instance state followed by stop

Step 15-: You can delete the instance permanently by selecting instance state followed by stop

7. Conclusion: