**Exercise 1. VM Ware Software and Ubuntu OS Installation.**

**AIM**: Installation of VMware Workstation 14 player and running Ubuntu OS.

**PROCEDURE:**

**About**: When it comes to desktop’s virtualization world, VMware workstation 14 player is the most enhanced virtualization software amongst all. Key point to use VMware workstation is that it is the flawless choice for users to keep their initial windows intact. On the other hand, operators can also set up

Networking labs, software development programs, and testing environments. Specifically, VMware Workstation 14 is a free version for subjective consumption since it gives an idea about virtual machinery.

*Features:*

* Simplifying and streamlining the virtualization of computer systems
* Compatibility with Windows 10
* User-friendly interface with powerful 3D graphics
* Support DirectX 10 and OpenGL 3.3 for running 3D software; With this feature, you can run all the software that you need to run DirectX 10 in a virtual machine.
* Possibility to use Intel-based tablets using Workstation Player’s virtual tablet sensors
* Display of high resolutions including 4K UHD (3840 x 2160) and QHD + (3200×1800)
* Support for the latest HD audio, USB 3.0, Bluetooth to connect the printer, headset, and webcam to the virtual machine
* Run virtual machines limited and expired **Requirements:**

Operating Systems: Windows XP, Vista, 7, 8 as well as 10 (64- bit)

|  |  |
| --- | --- |
| Processor: | 1.3 GHz multi-core |
| RAM: | 2 GB |
| Hard Disk Space: | 1.2. GB Free |
| Screen Resolution: | 1024 \* 768 |

Steps:

1. Open the destination folder where you have stored the Workstation 14 Player, setup file. For example, on the download folder. Click on the setup.exe file to start the installation wizard.
2. Next, you will be guided to the installation wizard page with a summary of information about VMware 14 Player. Whether to continue the installation or Cancel to exit the setup wizard.
3. Kindly read the end user license agreement carefully. Before commuting to accept the terms.
4. You can change the default installation destination folder. To a different drive and folder.
5. Every important part, to be up to date when using any software. You must confirm to check for product update on every startup.
6. Shortcuts will help to access any software quickly. So make sure to create the shortcuts on your desktop even your start menu.
7. Finally, you are a click away to begin the installation after passing the basic steps.
8. Completed VMware Workstation 14 Player installation, click on **Finish**.

1. After opening VMware Workstation 14 Player. You will see a page asking for the license key. If you have one, but it’s the free version you can select to use as non-commercial. And the product will get you the next page, thanks for using VMware Workstation 14 Player. Click on finish to get into VMware Workstation Player home page.
2. You have successfully installed VMware Workstation 14 Player, in your computer. If you are deciding to create a new virtual machine and stall any operating system on VMware on Windows.
3. How To Create a New Virtual Machine?

Before going to install any operating system on VMware, you have to create a new virtual machine first.

Next, you can continue to the installation of any operating system as a guest inside VMware. To do so, you need to open the VMware Player Application. On the Home Page click on “Create A New Virtual Machine. You will be guided to the page where you have to select how you want to install an operating system.

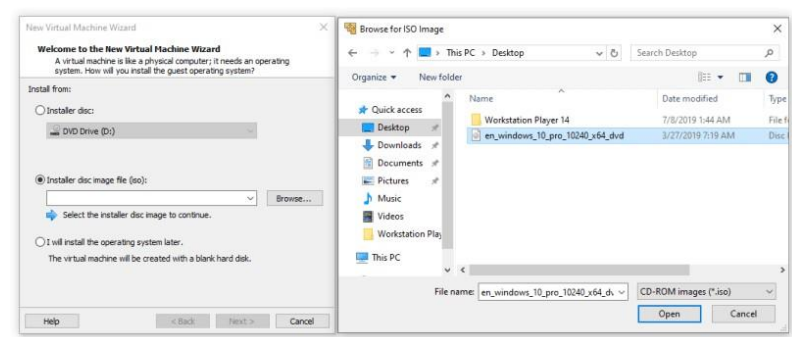
If you already have an installation media, Such as Windows 10 ISO or Ubuntu ISO, you can select the ISO file and continue.

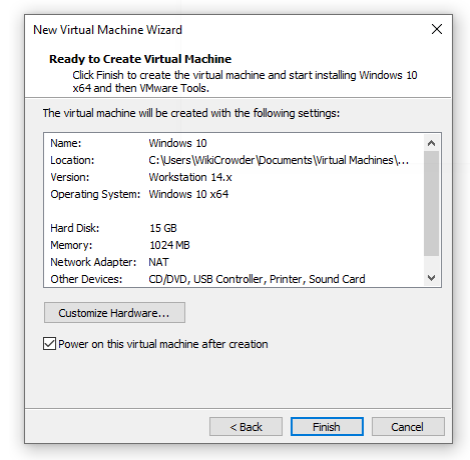
page, you see the installation information like providing Product Key, Windows 10 Version, Name, and Password. If you don’t have any product key skip that option and go next.

1. Type a name which you would like to use for this virtual machine. And even you can change the location where you want to store.
2. Specify the disk capacity of your virtual machine and store the virtual machine file as a single file.

1. Finally, installation is done .Click on finish to create the Windows 10 virtual machine and continue to the installation of windows 10.

**Result:** Successfully created a new virtual machine.



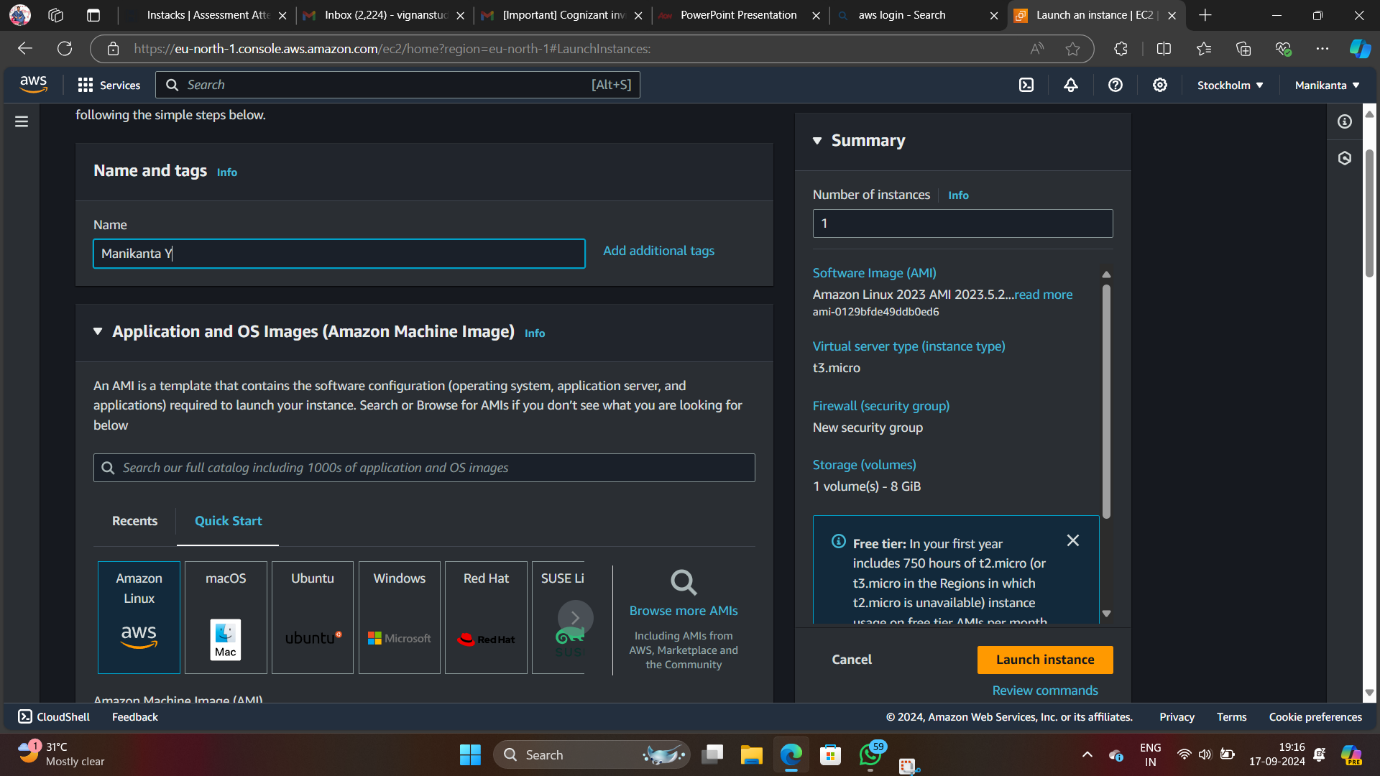


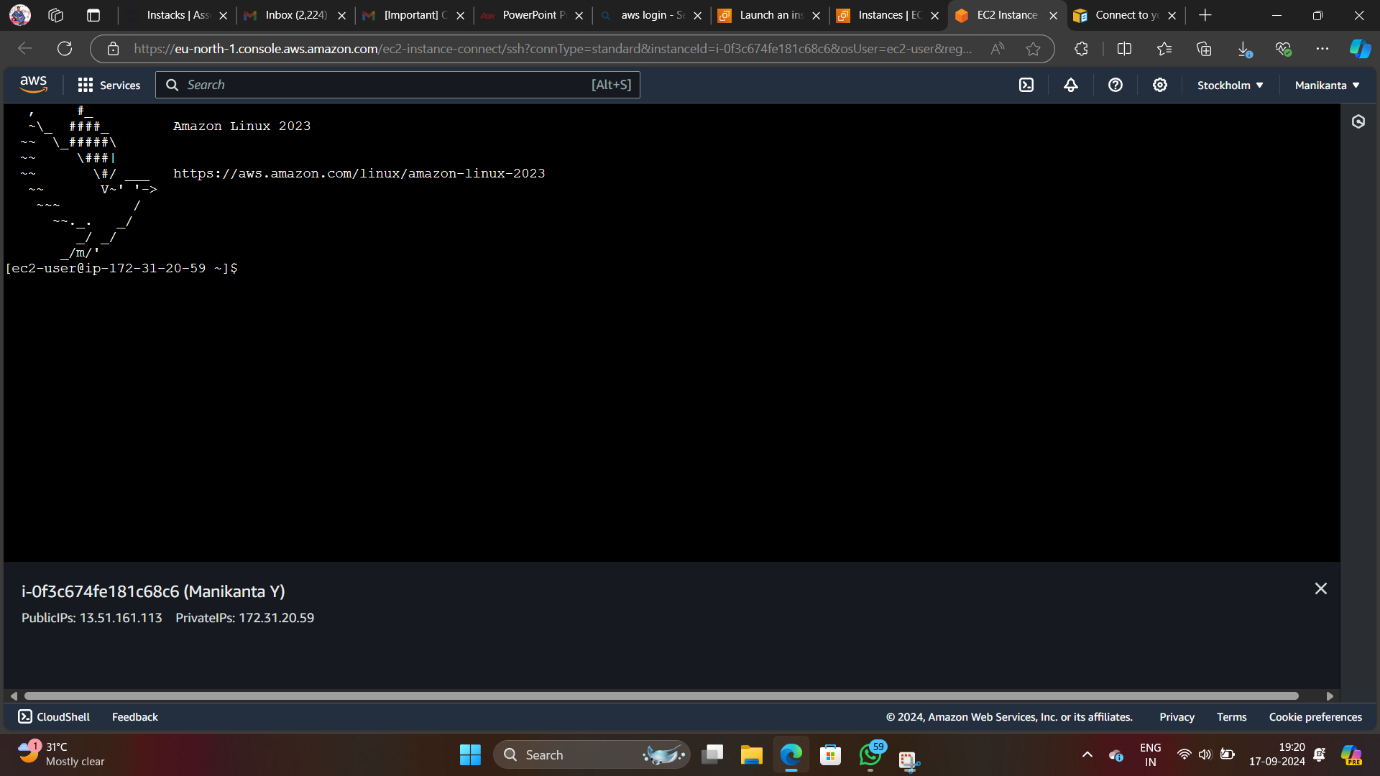
**Exercise 2:**

**Aim:** To connect to Amazon Linux instance from Linux Operating System.

**PROCEDURE:   
Amazon EC2:** Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud. It is designed to make web-scale computing easier for developers. It is a simple web service interface allows you to obtain and configure capacity with minimal friction. It provides you with complete control of your computing resources and lets you run on Amazon’s proven computing environment.  
**➔Launching Amazon Linux EC2 Instance   
Step 1: 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. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.  
**Step 2: Choose an Instance Type Amazon**

EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications.  
**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.  
**Step 4: Add Storage**   
Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes

**Step 5: Add Tags**   
A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver  
**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 .  
  
  
**Step 7: Review Instance Launch**   
Please review your instance launch details. You can go back to edit changes for each section. Click Launch to assign a key pair to your instance and complete the launch process.  
  




**Exercise 3:**

**AIM**: To connect to Amazon Windows instance from Linux client operating system

**PROCEDURE:**

Amazon EC2 instances created from most Windows Amazon Machine Images (AMIs) enable you to connect using Remote Desktop. Remote Desktop uses the Remote Desktop Protocol (RDP) and enables you to connect to and use your instance in the same way you use a computer sitting in front of you. It is available on most editions of Windows and available for Mac OS.

-> To Launch Windows EC2 instance

**Step 1:** An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications.

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.

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes afterlaunching an instance, but not instance store volumes.(Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage.)

Step 5 : Add a tag

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.A copy of a tag can be applied to volumes, instances or both.Tags will be applied to all instances and volumes.

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. If want to launch a windows remote desktop, allow the port RDP with port range- 3389.

Step7:Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

**3.1 To connect to Amazon Windows instance from linux client operating system**

Login to client operating system

-> Open linux terminal

**Note: rdesktop or xfreerdp { RHEL-6,7 } package should be installed**

**$ rdesktop -u Administrator <Pub\_DNS\_name/Public\_IP>**

Or

$ **xfreerdp -u Administrator <Pub\_DNS\_name/Public\_IP>**

In **{ RHEL-6,7 } ->**

**-u -> user name**

**Once e logged in Windows, Desktop is available.{ If you are going to use the instance,terminate the instance }**

**3.2 To connect Windows instance from Windows client operating system**

->In the navigation pane, under Instances, choose Instances.

Browse to and choose your Windows Server instance in the list.

-> Choose **Connect** and click on **Get Password**

**->** Choose **Browse**. Browse to and choose the Amazon EC2 instance **key pair** file associated with the Windows

Server Amazon EC2 instance, and then choose Open

.->Choose **Decrypt Password**. Make a note of the password that is displayed. Later You need it.

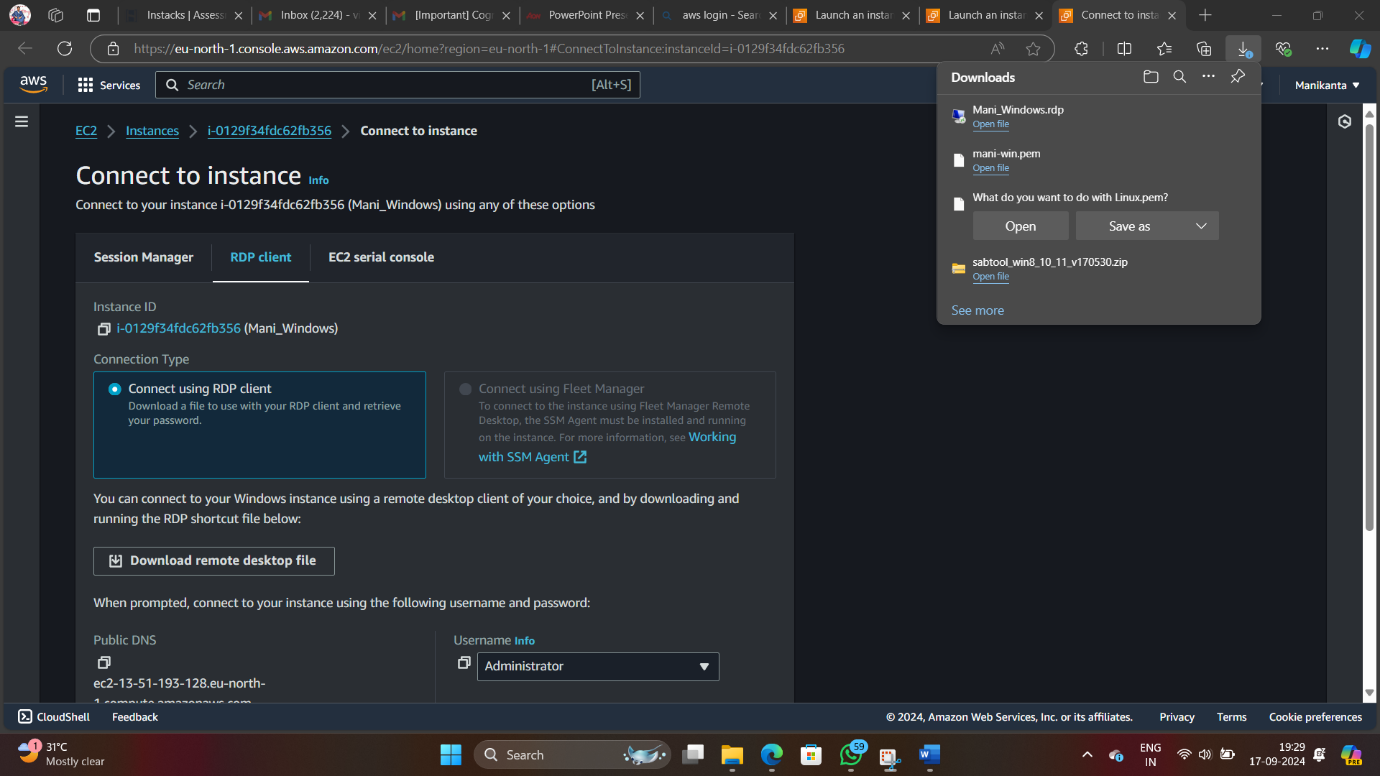
-> Choose **Download Remote Desktop File**, and then open the file.

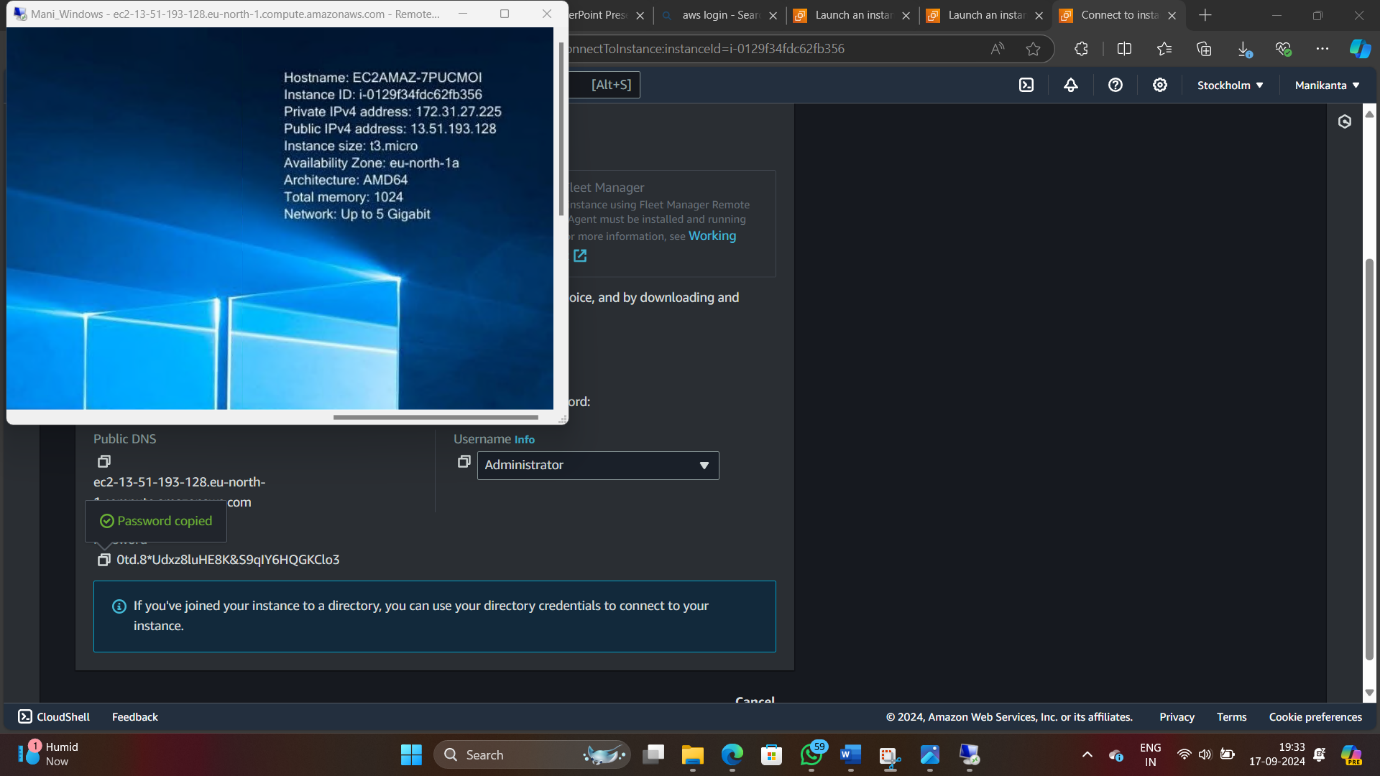
-> f you are prompted to connect even though the publisher of the remote connection can't be identified, proceed.

->Type the password you noted in step 7, and then proceed. (If your RDP connection client application prompts you for a user name, type **Administrator**.)

->If you are prompted to connect even though the identity of the remote computer cannot be verified, proceed.

->After you are connected, the desktop of the Amazon EC2 instance running Windows Server is displayed.





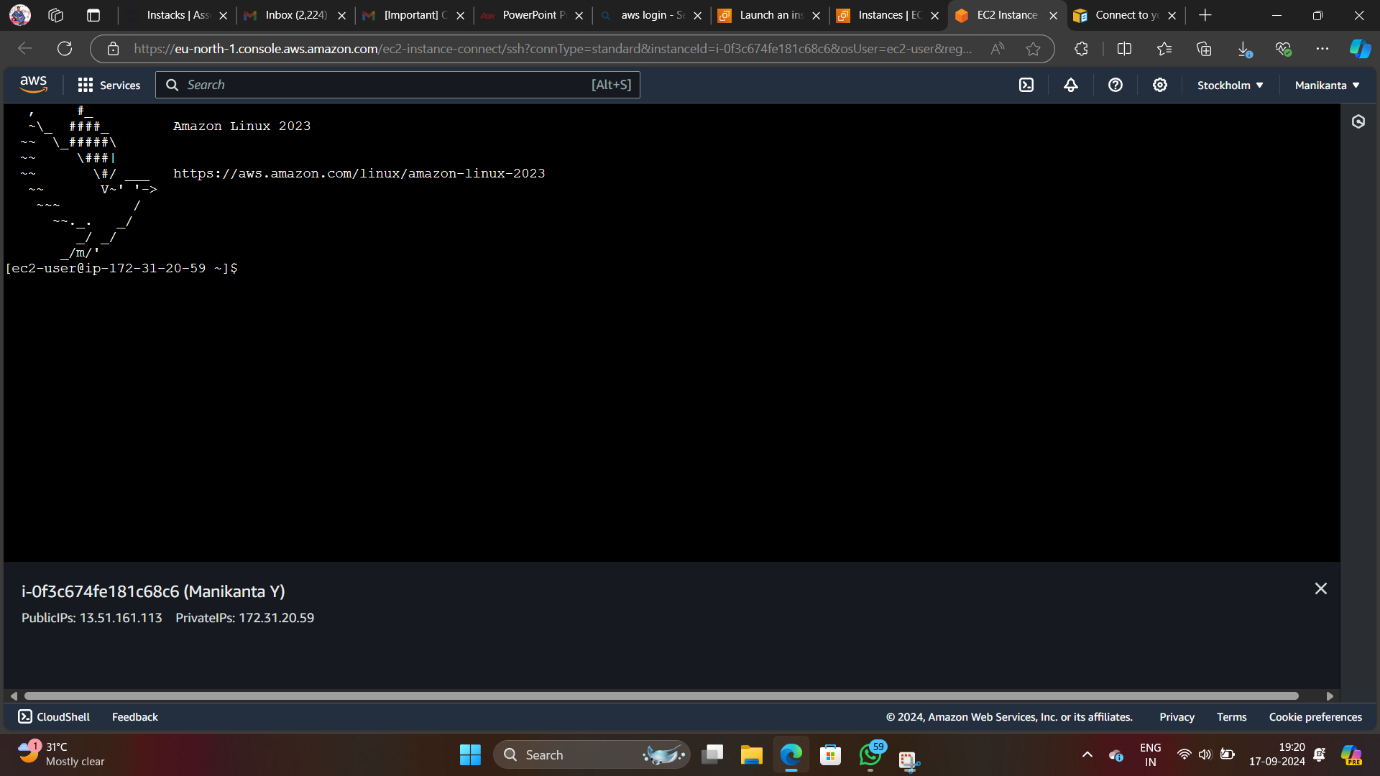
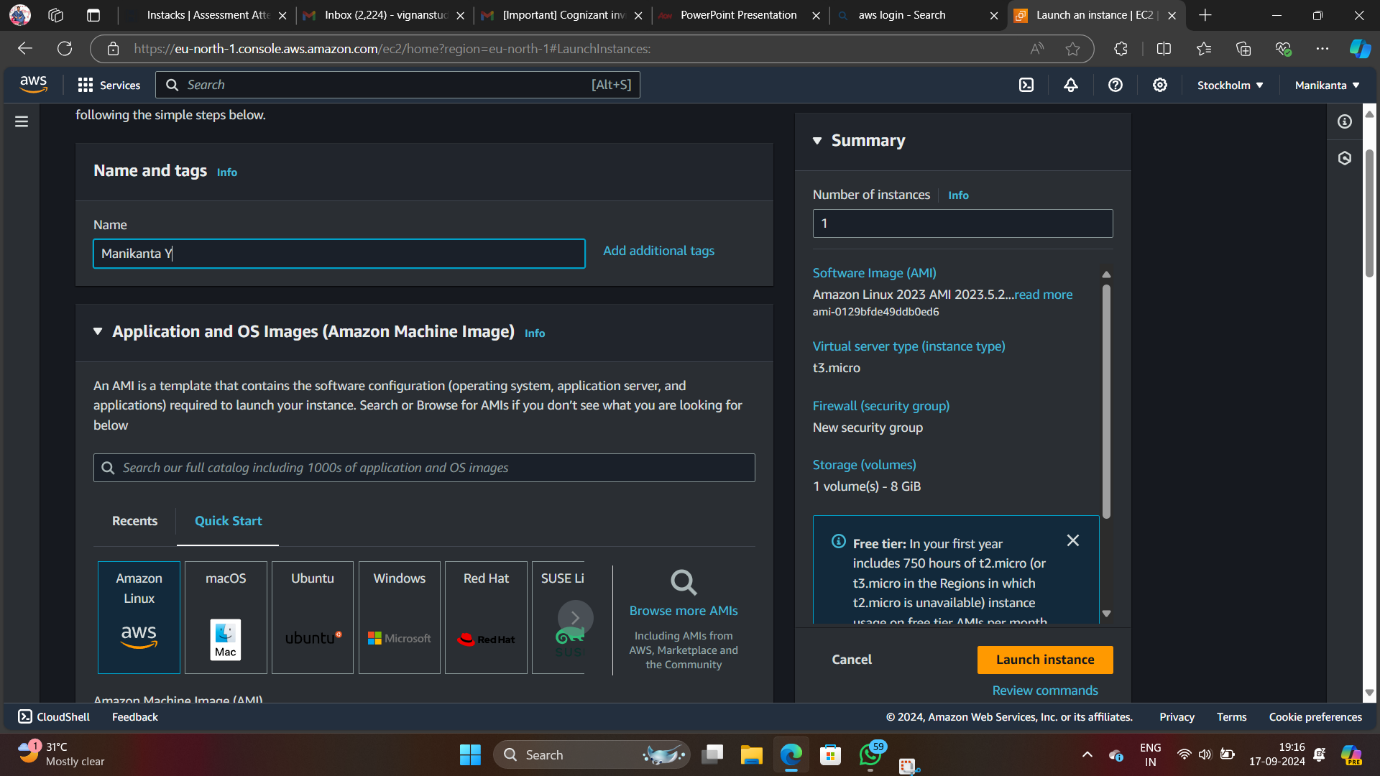
**Exercise 4:**

**Aim:** To connect to Amazon Linux instance from windows Operating System.

**PROCEDURE:   
Amazon EC2:** Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud. It is designed to make web-scale computing easier for developers. It is a simple web service interface allows you to obtain and configure capacity with minimal friction. It provides you with complete control of your computing resources and lets you run on Amazon’s proven computing environment.  
**➔Launching Amazon Linux EC2 Instance   
Step 1: 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. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.  
**Step 2: Choose an Instance Type Amazon**

EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications.  
**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.  
**Step 4: Add Storage**   
Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes

**Step 5: Add Tags**   
A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver  
**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 .  
  
  
**Step 7: Review Instance Launch**   
Please review your instance launch details. You can go back to edit changes for each section. Click Launch to assign a key pair to your instance and complete the launch process.



**Exercise 5:**

**AIM**: To connect to Amazon Windows instance from windows client operating system

**PROCEDURE:**

Amazon EC2 instances created from most Windows Amazon Machine Images (AMIs) enable you to connect using Remote Desktop. Remote Desktop uses the Remote Desktop Protocol (RDP) and enables you to connect to and use your instance in the same way you use a computer sitting in front of you. It is available on most editions of Windows and available for Mac OS.

-> To Launch Windows EC2 instance

**Step 1:** An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications.

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.

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes afterlaunching an instance, but not instance store volumes.(Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage.)

Step 5 : Add a tag

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.A copy of a tag can be applied to volumes, instances or both.Tags will be applied to all instances and volumes.

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. If want to launch a windows remote desktop, allow the port RDP with port range- 3389.

Step7:Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

**3.1 To connect to Amazon Windows instance from linux client operating system**

Login to client operating system

-> Open linux terminal

**Note: rdesktop or xfreerdp { RHEL-6,7 } package should be installed**

**$ rdesktop -u Administrator <Pub\_DNS\_name/Public\_IP>**

Or

$ **xfreerdp -u Administrator <Pub\_DNS\_name/Public\_IP>**

In **{ RHEL-6,7 } ->**

**-u -> user name**

**Once e logged in Windows, Desktop is available.{ If you are going to use the instance,terminate the instance }**

**3.2 To connect Windows instance from Windows client operating system**

->In the navigation pane, under Instances, choose Instances.

Browse to and choose your Windows Server instance in the list.

-> Choose **Connect** and click on **Get Password**

**->** Choose **Browse**. Browse to and choose the Amazon EC2 instance **key pair** file associated with the Windows

Server Amazon EC2 instance, and then choose Open

.->Choose **Decrypt Password**. Make a note of the password that is displayed. Later You need it.

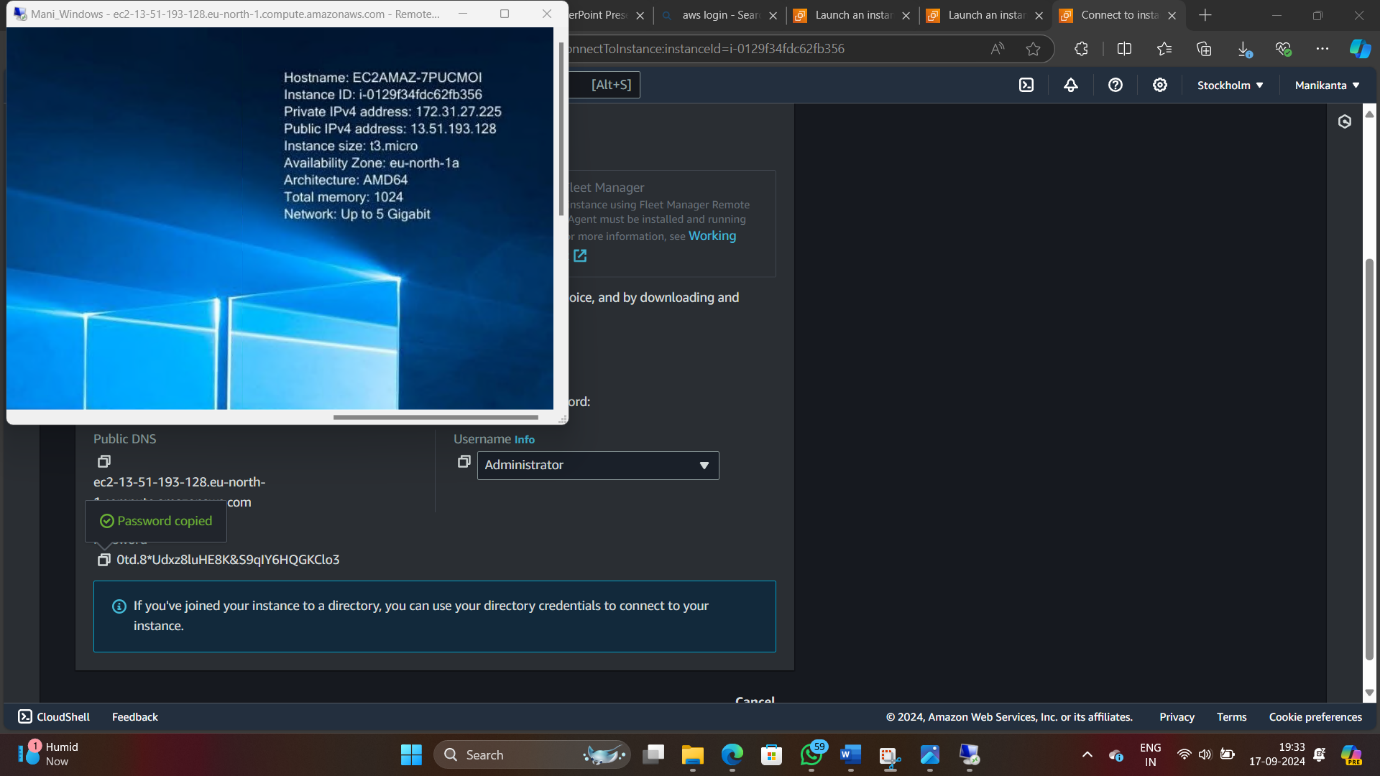
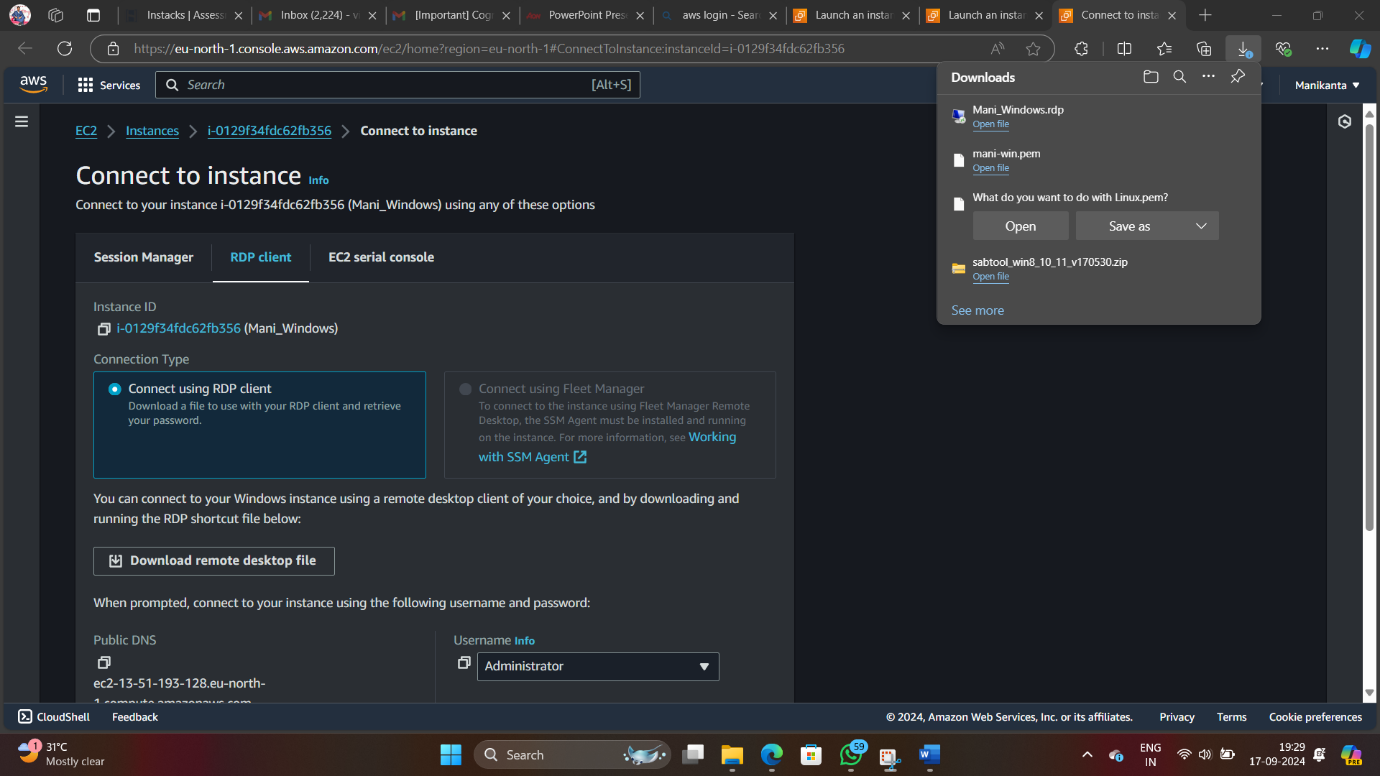
-> Choose **Download Remote Desktop File**, and then open the file.

-> f you are prompted to connect even though the publisher of the remote connection can't be identified, proceed.

->Type the password you noted in step 7, and then proceed. (If your RDP connection client application prompts you for a user name, type **Administrator**.)

->If you are prompted to connect even though the identity of the remote computer cannot be verified, proceed.

->After you are connected, the desktop of the Amazon EC2 instance running Windows Server is displayed.



**Exercise 6:**

**AIM:** To Assign Elastic IP address

**PROCEDURE:**

Elastic IP Add (IPv4)

An Elastic IP address is a public IPv4 address that you can allocate to your account. You can associate it to and from instances as you require, and it's allocated to your account until you choose to release it.

To allocate an Elastic IP and associate it with an Amazon Web Services (AWS) instance, do the following:

1. Open the AWS Management Console, click the EC2 link, and display the page associated with your region.Click the **Elastic IPs** link in the **EC2 Dashboard**.
2. Click **Allocate New Address** and choose **VPC** or **EC2** from the drop-down list, depending whether you're going to associate this IP with an instance in Amazon EC2-Virtual Private Cloud (VPC) or Amazon EC2-Classic, respectively. Click **Yes, Allocate** to confirm your choice.
3. Right-click the newly created Elastic IP and choose **Associate Address**.
4. Choose your desired EC2 instance from the drop-down list of running instances and click **Associate**.

To release Elastic IP

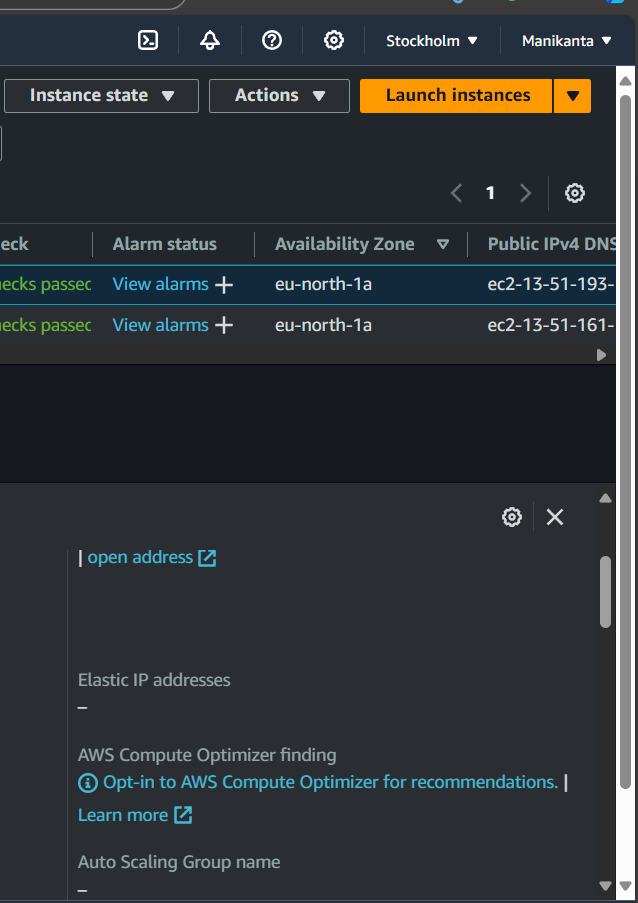
Open the console EC2 Dashboard

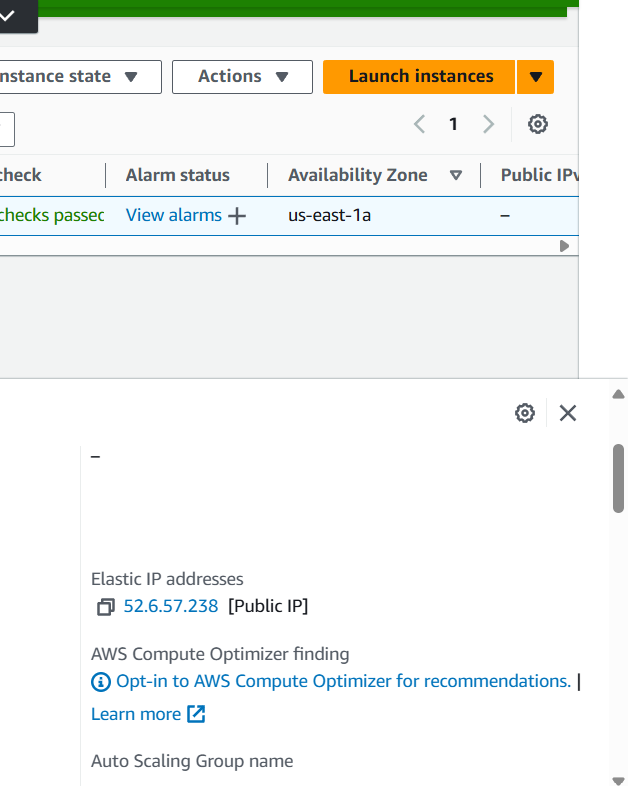
Select **Elastic IP** and click on **Action** button Select

Disassociate Address

Click on Disassociate address

Click On Action Button and then click on Release Address





Exercise 7:

AIM: To Configure Amazon Simple Storage Service (Amazon s3)

PROCEDURE:

Amazon Simple Storage Service is storage for the Internet. It is designed to make web-scale computing easier for developers. Amazon S3 has a simple web services interface that you can use to store and retrieve any amount of data, at any time, from anywhere on the web. It gives any developer access to the same highly scalable, reliable, fast, inexpensive data storage infrastructure that Amazon uses to run its own global network of websites. The service aims to maximize benefits of scale and to pass those benefits on to developers. Amazon s3 Bucket. A bucket is a logical unit of storage in Amazon Web Services (AWS) object storage service, Simple Storage Solution S3. Buckets are used to store objects, which consist of data and metadata that describes the data.

When you subscribe to the data feed, you must specify an Amazon S3 bucket to store the data feed files. Before you choose an Amazon S3 bucket for the data feed, consider the following: You must use a bucket from the US East. You must have FULL\_CONTROL permission to the bucket.

If you're the bucket owner, you have this permission by default. Otherwise, the bucket owner must grant your AWS account this permission.

When you create your data feed subscription, Amazon S3 updates the ACL of specified bucket to allow the AWS data feed account read and write permissions

Removing the permissions for the data feed account does not disable the data feed. If you remove those permissions but don't disable the data feed, we restore those permissions the next time that the data feed account needs to write to the bucket.

Each data feed file has its own ACL. The bucket owner has FULL\_CONTROL permission to the data files. The data feed account has read and write permissions. If you delete your data feed subscription, Amazon EC2 doesn't remove the read and write permissions for the data feed account on either the bucket or the data files. You must remove these permissions yourself.

To create an S3 bucket

1. Sign in to the AWS Management Console and open the Amazon S3 console
2. Choose Create bucket. The bucket name you choose must be globally unique across all existing bucket names in Amazon S3 (that is, across all AWS customers).

In Region, choose Region and Click on Create. When Amazon S3 successfully creates your bucket, the console displays your empty bucket in the Buckets pane

Step 2: Upload a File to Your Amazon S3 Bucket Now that you've created a bucket, you're ready to add an object to it. An object can be any kind of file: a document, a photo, a video, a music file, or other file type.

In the Amazon S3 console, choose the bucket where you want to upload an object, choose Upload, and then choose Add Files.

In the Upload dialog box, do one of the following:

a. Drag and drop more files and folders to the console window that displays the Upload dialog box. To add more files, you can also choose Add more files. This option works only for files, not folders.

b. To immediately upload the listed files and folders without granting or removing permissions for specific users or setting public permissions for all of the files that you're uploading, choose Upload.

c. To set permissions or properties for the files that you are uploading, choose.

Next.

-> On the Set Permissions page, under Manage users you can change the permissions for the AWS account owner. The owner refers to the AWS account root user, and not an AWS Identity and Access Management (IAM) user.

->Under Manage public permissions you can grant read access to your objects to the general public (everyone in the world), for all of the files that you're uploading. Granting public read access is applicable to a small subset of use cases such as when buckets are used for websites. We recommend that you do not change the default setting ofDo not grant public read access to this object(s). You can always make changes to object permissions after you upload the object. -> When you're done configuring permissions, choose Next.

On the Set Properties page, choose the storage class and encryption method to use for the files that you are uploading. You can also add or modify metadata. Choose a storage class for the files you're uploading.

Choose the type of encryption for the files that you're uploading. If you don't want to encrypt them, choose None.

1. To encrypt the uploaded files using keys that are managed by Amazon S3, choose Amazon S3 master-key.
2. ii. To encrypt the uploaded files using the AWS Key Management Service (AWS KMS), choose AWS KMS master-key. Then choose a master key from the list of AWS KMS master keys.

Note To encrypt objects in a bucket, you can use only keys that are available in the same AWS Region as the bucket.

You can give an external account the ability to use an object that is protected by an AWS KMS key. To do this, select Custom KMS ARN from the list and enter the Amazon Resource Name (ARN) for the external account. Administrators of an external account that have usage permissions to an object protected by your AWS KMS key can further restrict access by creating a resourcelevel IAM policy.

Metadata for Amazon S3 objects is represented by a name-value (key-value) pair. There are two kinds of metadata: system-defined metadata and user-defined metadata. If you want to add Amazon S3 system-defined metadata to all of the objects you are uploading, for Header, select a header. You can select common HTTP headers, such as Content-Type and Content-Disposition. Type a value for the header, and then choose Save.

Any metadata starting with prefix x-amz-meta- is treated as user-defined metadata. Userdefined metadata is stored with the object, and is returned when you download the object.

To add user-defined metadata to all of the objects that you are uploading, type x- amz- metaplus a custom metadata name in the Header field. Type a value for the header, and then choose Save. Both the keys and their values must conform to US- ASCII standards. User-defined metadata can be as large as 2 KB.

Object tagging gives you a way to categorize storage. Each tag is a key-value pair. Key and tag values are case sensitive. You can have up to 10 tags per object.

To add tags to all of the objects that you are uploading, type a tag name in the Key field. Type a value for the tag, and then choose Save. A tag key can be up to 128 Unicode characters in length and tag values can be up to 255 Unicode characters in length.

➢ Choose Next.

➢ On the Upload review page, verify that your settings are correct, and then choose Upload. To make changes, choose Previous.

To see the progress of the upload, choose In progress at the bottom of the browser window.

To see a history of your uploads and other operations, choose Success.

Hosting a Static Website on Amazon S3

You can host a static website on Amazon Simple Storage Service (Amazon S3). On a static website, individual web pages include static content. They might also contain client-side scripts. By contrast, a dynamic website relies on server-side processing, including server-side scripts such as PHP, JSP, or ASP.NET. Amazon S3 does not support server-side scripting.

➔ To host a static website, you configure an Amazon S3 bucket for website hosting, and then upload your website content to the bucket. This bucket must have public read access. It is intentional that everyone in the world will have read access to this bucket. The website is then available at the AWS Region- specific website endpoint of the bucket,

➔ After successful completion of code uploaded to S3, then select all object in bucket make it as public as shown below slide.

-->Open the bucket Properties pane, choose Static Website Hosting, and do the following:

➔ Choose Use this bucket to host a website.

➔ In the Index Document box, type the name of your index document. The name is typically index.html.

➔ Choose Save to save the website configuration.

➔ Write down the Endpoint.

Step 2: Adding a Bucket Policy That Makes Your Bucket Content Publicly Available

1. In the Properties pane for the bucket, choose Permissions.
2. Choose Add Bucket Policy.
3. To host a website, your bucket must have public read access. It is intentional that everyone in the world will have read access to this bucket. Copy the following bucket policy, and then paste it in the Bucket Policy Editor.
4. 4.{ "Version":"2012-10-17",

"Statement":[{

"Sid":"PublicReadForGetBucketObjects",

"Effect":"Allow",

"Principal":

"Action":["s3:GetObject"],

"Resource":["arn:aws:s3:::example-bucket/\*"

] } ] }

5. In the policy, replace example-bucket with the name of your bucket.

6. Choose Save.

7. Testing Your Website Type the following URL in the browser, replacing example-bucket with the name of your bucket and website-region with the name of the AWS Region where you deployed your bucket.

➔ This is the Amazon S3-provided website endpoint for your bucket. You use this endpoint to test your website is running or not by pasting the Endpoint into your browser.

If your browser displays your index.html page, the website was successfully deployed.

Note : HTTPS access to the website is not supported. You now have a website hosted on Amazon S3. This website is available at the Amazon S3 website endpoint. However, you might have a domain, such as example.com, that you want to use to serve the content from the website you created. You might also want to use Amazon S3 root domain support to serve requests for both http://www.example.com and http://example.com