Vidyavardhini's College of Engineering and Technology

Department of Artificial Intelligence & Data Science

AY: 2023-24

Class:		**Semester:**	
Course Code:		**Course Name:**	

Name of Student:	
Roll No. :	
Experiment No.:	2
Title of the Experiment:	To study and Implement Infrastructure as a Service using AWS EC2 by creating a Windows Virtual Machine through RDP protocol and change volume of attached storage.
Date of Performance:	
Date of Submission:	

Evaluation

Performance Indicator	Max. Marks	Marks Obtained
Performance	5	
Understanding	5	
Journal work and timely submission	10	
Total	20	

Performance Indicator	Exceed Expectations (EE)	Meet Expectations (ME)	Below Expectations (BE)
Performance	4-5	2-3	1
Understanding	4-5	2-3	1
Journal work and timely submission	8-10	5-8	1-4

Checked by

Name of Faculty :
Signature :
Date :

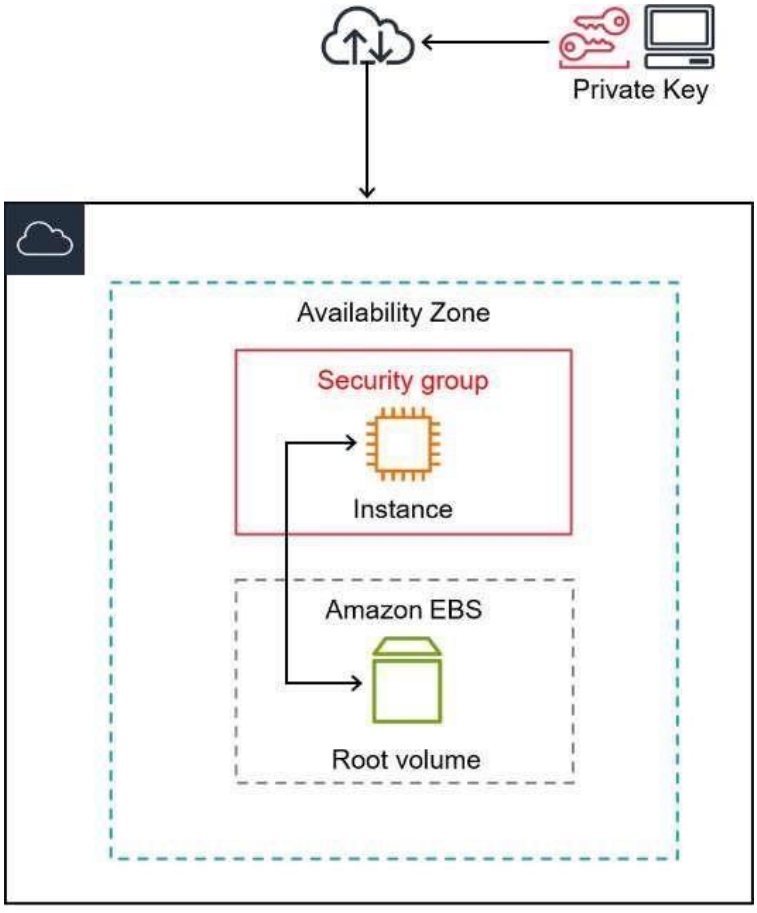
Experiment No. 2

Aim: To study and Implement Infrastructure as a Service using AWS EC2 by creating a Windows Virtual Machine through RDP protocol and change volume of attached storage.

Theory:

An instance is a virtual server in the AWS Cloud. With Amazon EC2, you can set up and configure the operating system and applications that run on your instance.

When you launch your instance, you secure it by specifying a key pair (to prove your identity) and a security group (which acts as a virtual firewall to control ingoing and outgoing traffic). When you connect to your instance, you must provide the private key of the key pair that you specified when you launched your instance.



Steps:

To launch an instance

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. From the EC2 console dashboard, in the Launch instance box, choose Launch instance.
3. Under Name and tags, for Name, enter a descriptive name for your instance.
4. Under Application and OS Images (Amazon Machine Image), do the following:
    a. Choose Quick Start, and then choose Windows. This is the operating system (OS) for your instance.
    b. From Amazon Machine Image (AMI), select the AMI for Windows Server 2016 Base or later.. Notice that these AMIs are marked Free Tier eligible. An Amazon Machine Image (AMI) is a basic configuration that serves as a template for your instance. Note

       AL2023 is the successor to Amazon Linux 2. For more information, see Launching AL2023 using the Amazon EC2 console.
5. Under Instance type, from the Instance type list, you can select the hardware configuration for your instance. Choose the t2.micro instance type, which is selected by default. The t2.micro instance type is eligible for the Free Tier. In Regions where t2.micro is unavailable, you can use a t3.micro instance under the Free Tier. For more information, see AWS Free Tier.
6. Under Key pair (login), for Key pair name, choose the key pair that you created when getting set up. Note that you must select an RSA key. ED25519 keys are not supported for Windows instances. Warning

   Do not choose Proceed without a key pair (Not recommended). If you launch your instance without a key pair, then you can't connect to it.
7. Next to Network settings, choose Edit. For Security group name, you'll see that the wizard created and selected a security group for you. You can use this security group, or alternatively you can select the security group that you created when getting set up using the following steps:
    a. Choose Select existing security group.
    b. From Common security groups, choose your security group from the list of existing security groups.
8. Keep the default selections for the other configuration settings for your instance.

9. Review a summary of your instance configuration in the Summary panel, and when you're ready, choose Launch instance.
10. A confirmation page lets you know that your instance is launching. Choose View all instances to close the confirmation page and return to the console.
11. On the Instances screen, you can view the status of the launch. It takes a short time for an instance to launch. When you launch an instance, its initial state is pending. After the instance starts, its state changes to running and it receives a public DNS name. If the Public IPv4 DNS column is hidden, choose the settings icon (⚙) in the top-right corner, toggle on Public IPv4 DNS, and choose Confirm.
12. It can take a few minutes for the instance to be ready for you to connect to it. Check that your instance has passed its status checks; you can view this information in the Status check column.

To connect to your Windows instance using an RDP client

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. In the navigation pane, choose Instances.
3. Select the instance and then choose Connect.
4. On the Connect to instance page, choose the RDP client tab.
5. For Username, choose the default username for the Administrator account. The username you choose must match the language of the operating system (OS) contained in the AMI that you used to launch your instance. If there is no username in the same language as your OS, choose Administrator (Other).
6. Choose Get password.
7. On the Get Windows password page, do the following:

- Choose Upload private key file and navigate to the private key (.pem) file that you specified when you launched the instance. Select the file and choose Open to copy the entire contents of the file to this window.
- Choose Decrypt password. The Get Windows password page closes, and the default administrator password for the instance appears under Password, replacing the Get password link shown previously.
- Copy the password and save it in a safe place. This password is required to connect to the instance.

8. Choose Download remote desktop file. Your browser prompts you to either open or save the RDP shortcut file. When you have finished downloading the file, choose Cancel to return to the Instances page.

1. If you opened the RDP file, you'll see the Remote Desktop Connection dialog box.
2. If you saved the RDP file, navigate to your downloads directory, and open the RDP file to display the dialog box.

9. You might get a warning that the publisher of the remote connection is unknown. Choose Connect to continue to connect to your instance.
10. The administrator account is chosen by default. Paste the password that you copied previously, and then choose Continue.
11. Due to the nature of self-signed certificates, you might get a warning that the security certificate could not be authenticated. Use the following steps to verify the identity of the remote computer. Alternatively, if you trust the certificate, choose Yes (Windows) or Continue (Mac OS X) to skip the following steps.

- [Windows] Choose View certificate.

1. [Mac OS X] Choose Show Certificate.

- [Windows] Choose the Details tab, and scroll down to Thumbprint.

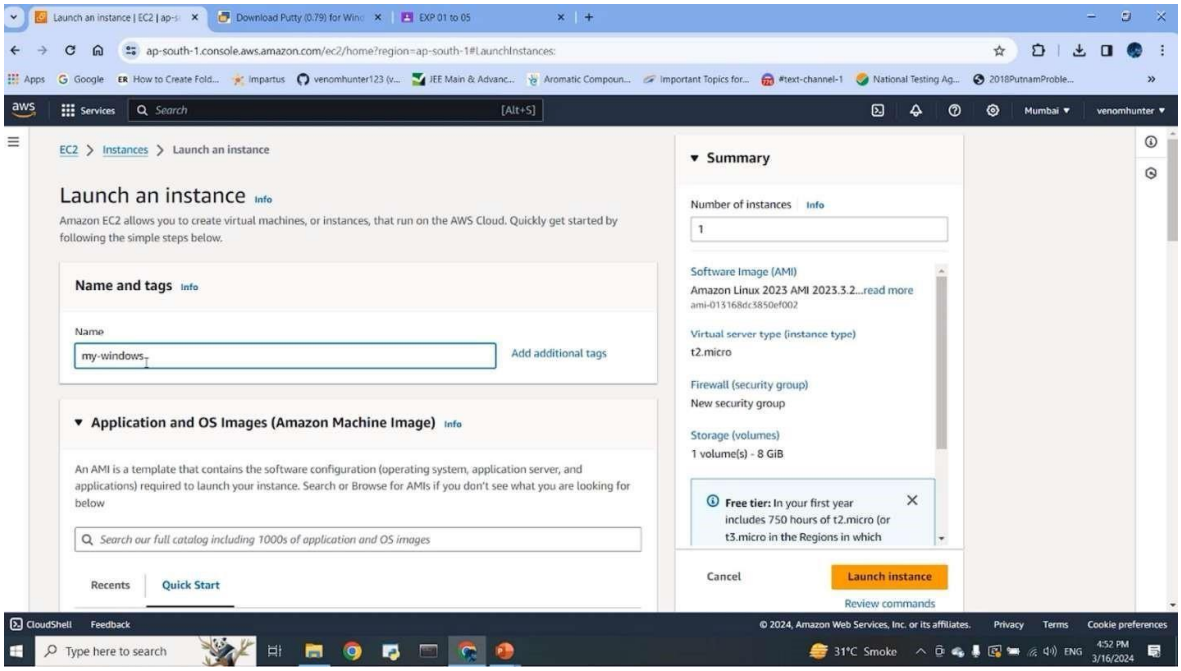
1. [Mac OS X] Expand Details, and scroll down to SHA1 Fingerprints.
2. This is the unique identifier for the remote computer's security certificate.

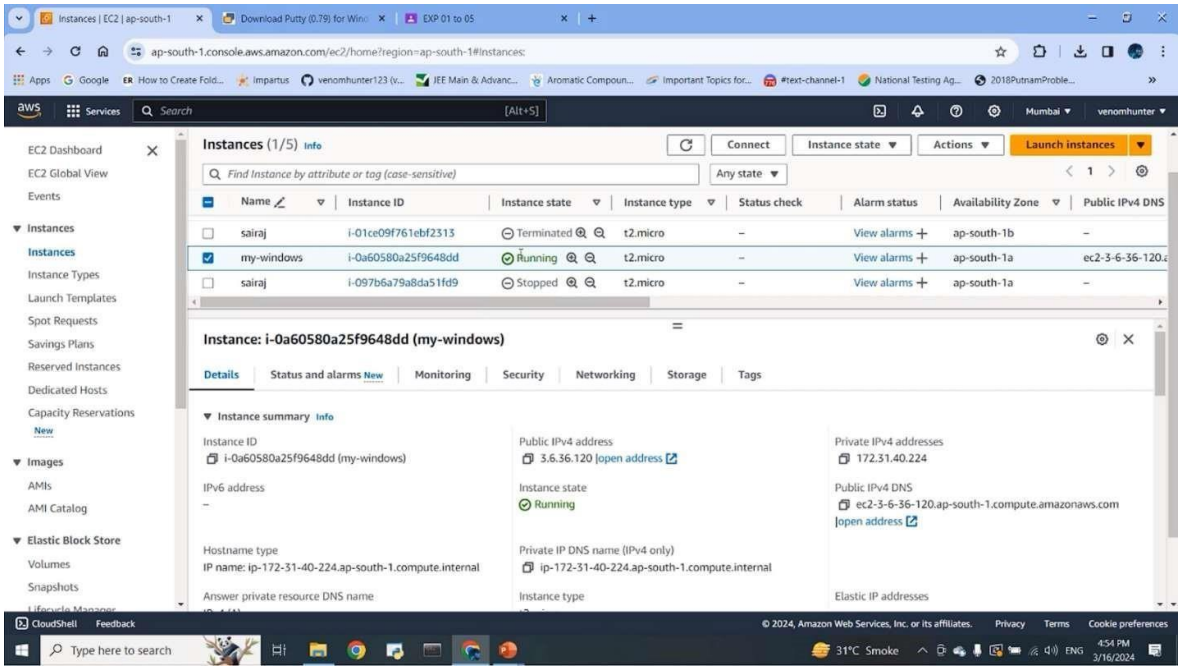
- In the Amazon EC2 console, select the instance, and then choose Actions, Monitor and troubleshoot, Get system log.
- In the system log output, look for RDPCERTIFICATE-THUMBPRINT. If this value matches the thumbprint (Windows) or fingerprint (Mac OS X) of the certificate, you have verified the identity of the remote computer.
- [Windows] Return to the Certificate dialog box and choose OK.

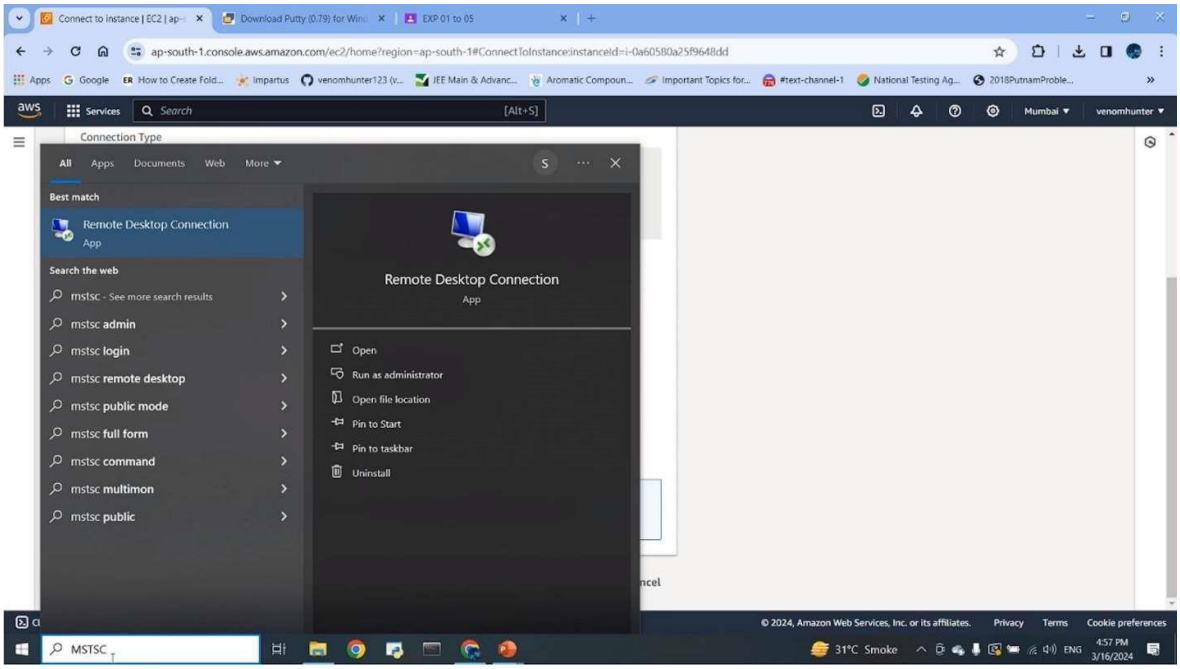
1. [Mac OS X computer] Return to the Verify Certificate dialog box and choose Continue.

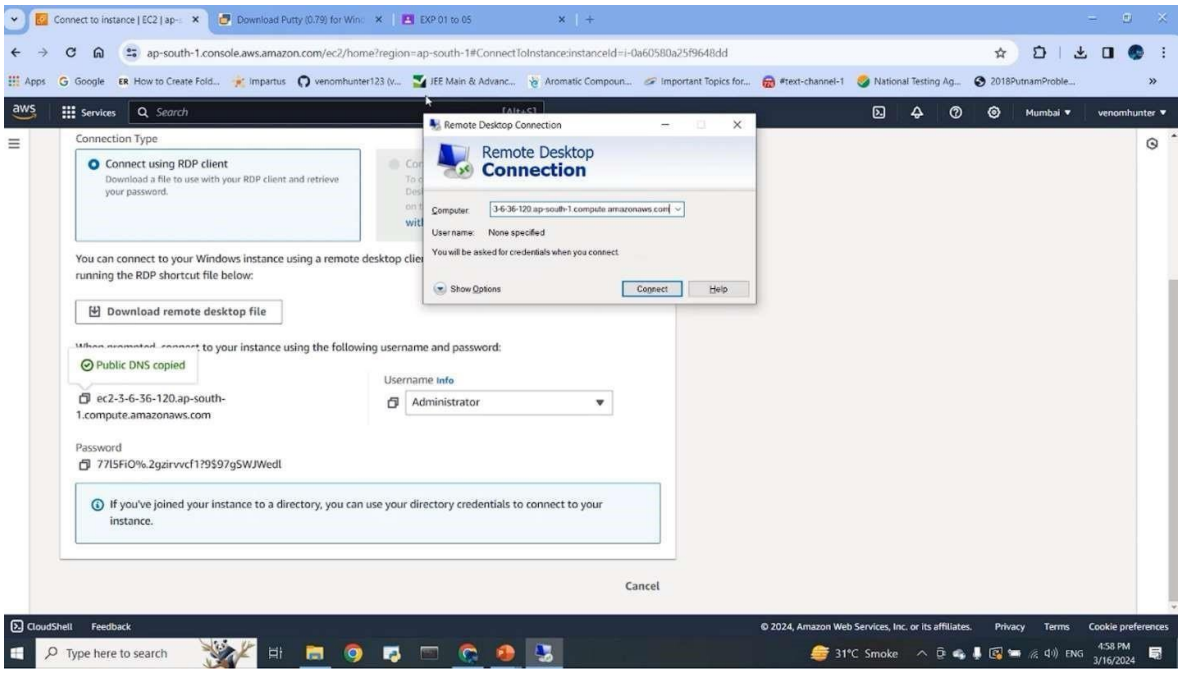
- [Windows] Choose Yes in the Remote Desktop Connection window to connect to your instance.

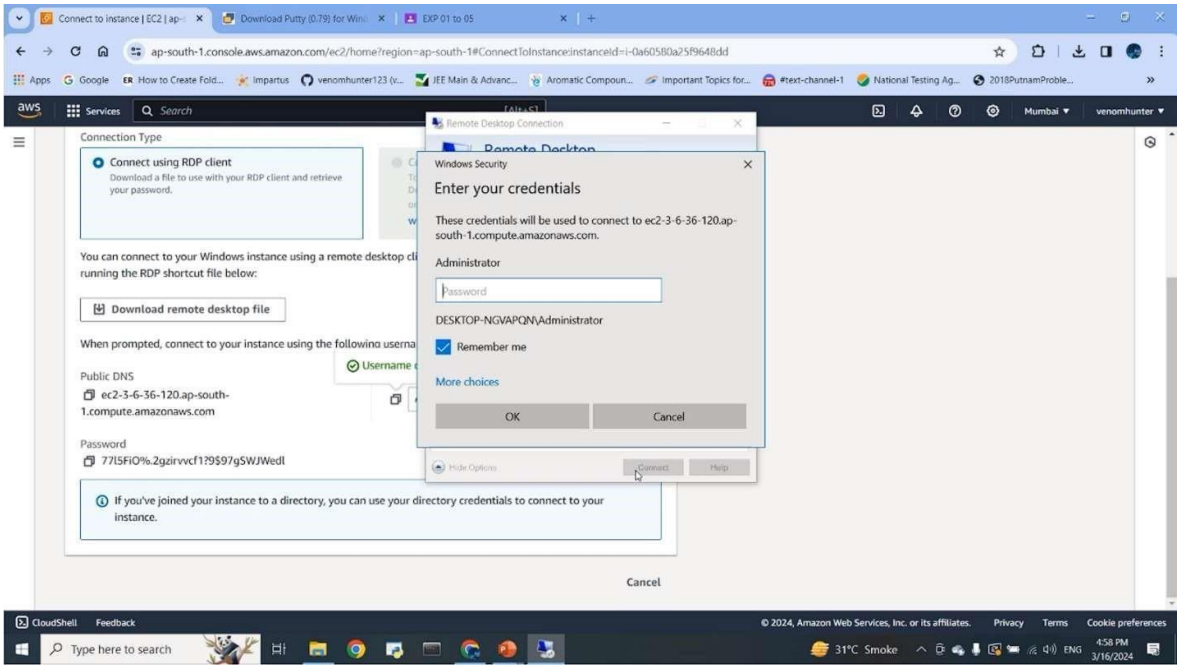
Output /Observation:






Connection Type
All
Apps
Documents
Web
More
Best match
Remote Desktop Connection
App
Search the web
mstsc - See more search results
mstsc admin
mstsc login
mstsc remote desktop
mstsc public mode
mstsc full form
mstsc command
mstsc multimon
mstsc public
Remote Desktop Connection
App
Open
Run as administrator
Open file location
Pin to Start
Pin to taskbar
Uninstall
MSTSC
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Connection Type
Connect using RDP client
Download a file to use with your RDP client and retrieve your password.
You can connect to your Windows instance using a remote desktop client running the RDP shortcut file below:
Download remote desktop file
Public DNS copied
ec2-3-6-36-120.ap-south-1.compute.amazonaws.com
Username Info
Administrator
Password
7?l5FiO%.2gzirvvcf1?9$97gSWJWedl
If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.
Cancel
Remote Desktop Connection
Remote Desktop Connection
Computer:
User name:
None specified
You will be asked for credentials when you connect.
Show Options
Connect
Help
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Connect to instance | EC2 | ap-
Download Putty (0.79) for Win
EXP 01 to 05
ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#ConnectToInstance:instanceId=i-0a60580a25f9648dd
Apps
Google
How to Create Fold...
Impartus
venomhunter123 (v...
JEE Main & Advanc...
Aromatic Compoun...
Important Topics for...
#text-channel-1
National Testing Ag...
2018PutnamProble...
aws
Services
Search
Mumbai
venomhunter
Connection Type
Connect using RDP client
Download a file to use with your RDP client and retrieve your password.
You can connect to your Windows instance using a remote desktop cli
running the RDP shortcut file below:
Download remote desktop file
When prompted, connect to your instance using the followina userna
Public DNS
ec2-3-6-36-120.ap-south-1.compute.amazonaws.com
Password
77l5FiO%.2gzirvvcf1?9$97gSWJWedl
If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.
Cancel
Remote Desktop Connection
Windows Security
Enter your credentials
These credentials will be used to connect to ec2-3-6-36-120.ap-south-1.compute.amazonaws.com.
Administrator
Password
DESKTOP-NGVAPQN\Administrator
Remember me
More choices
OK
Cancel
Hide Options
Connect
Help
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
31°C Smoke
ENG
4:58 PM
3/16/2024


ec2-3-6-36-120.ap-south-1.compute.amazonaws.com
Recycle Bin
EC2 Feedback
EC2 Microso...
Hostname : EC2AMAZ-A1V67M9
Instance ID : i-0a60580a25f9648dd
Private IP Address : 172.31.40.224
Public IP Address : 3.6.36.120
Instance Size : t2.micro
Availability Zone : ap-south-1a
Architecture : AMD64
Total Memory : 1024
Network : Low to Moderate
Type here to search
11:31 AM
3/16/2024

Conclusion:

The use of the Remote Desktop Protocol (RDP) for Windows Virtual Machines (VMs) presents several key benefits. Firstly, RDP enables remote access to Windows VMs, allowing users to connect to their virtual desktop environments from anywhere with an internet connection, enhancing flexibility and productivity. Secondly, RDP provides a secure communication channel between the client and the VM, ensuring data confidentiality and integrity during remote sessions. Additionally, RDP facilitates seamless collaboration and support by enabling multiple users to simultaneously access and interact with a Windows VM, fostering teamwork and troubleshooting efforts. Overall, RDP streamlines remote access to Windows VMs, promoting efficiency, security, and collaboration in modern computing environments.