Lab 10: Implement Data Protection Report

Yunis Mohamed

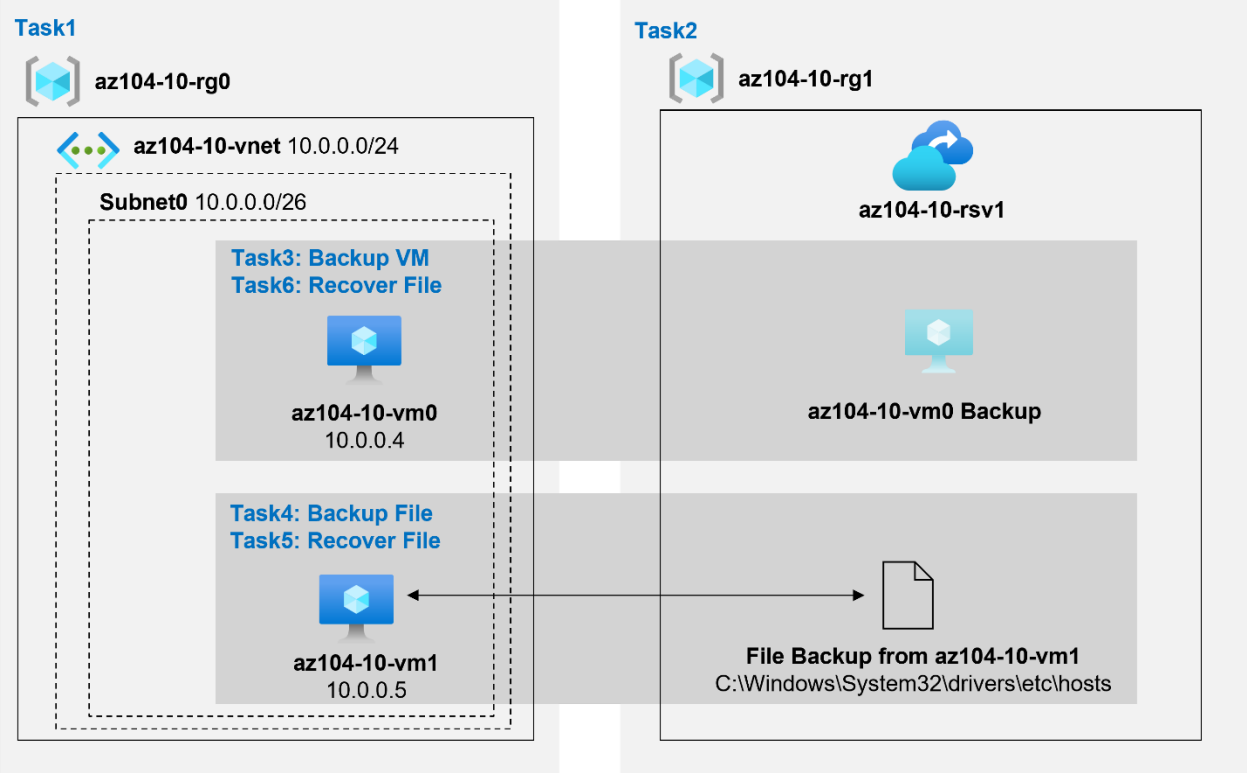
MICROSOFT AZURE LAB 10

Contents

Introduction

This report provides a comprehensive overview of Lab 10, "Implement Data Protection," conducted in Microsoft Azure. The lab consisted of multiple tasks, including provisioning the lab environment, creating a Recovery Services vault, implementing Azure virtual machine-level backup, enabling File and Folder backup, performing file recovery using the Azure Recovery Services agent, exploring file recovery with Azure virtual machine snapshots, and reviewing the functionality of Azure Recovery Services soft delete. Through an analysis of the objectives, methodologies, and outcomes of each task, this report aims to deliver a comprehensive understanding of implementing effective data protection measures in Azure.

Architecture diagram

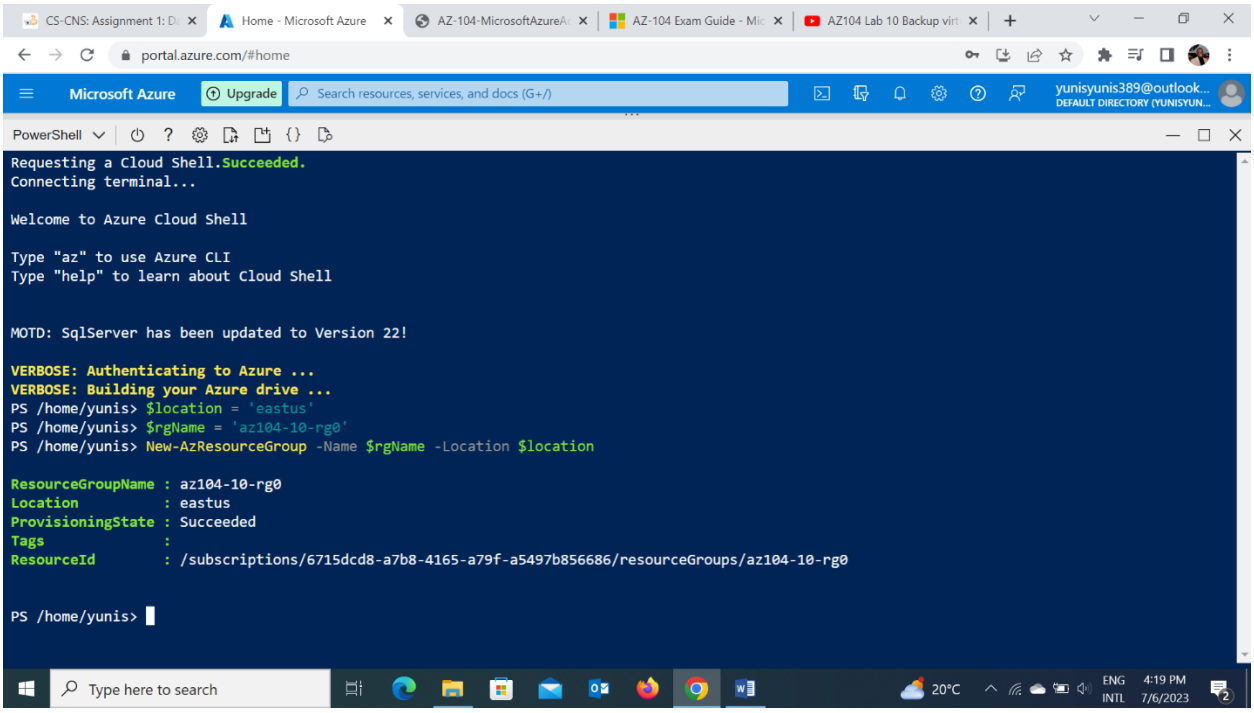


Task 1: Provision the lab environment

1. Sign in to the Azure portal.
2. In the Azure portal, open the **Azure Cloud Shell** by clicking on the icon in the top right of the Azure Portal.
3. If prompted to select either **Bash** or **PowerShell**, select **PowerShell**.
4. In the toolbar of the Cloud Shell pane, click the Upload/Download files icon, in the drop-down menu, click Upload and upload the files \Allfiles\Labs\10\az104-10-vms-edge-

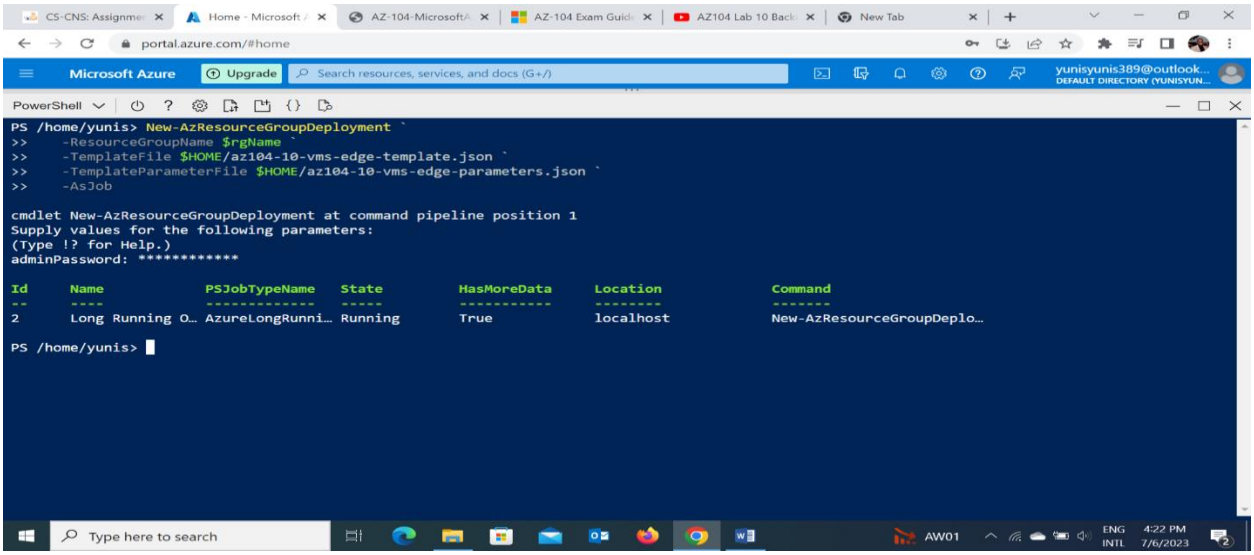
template.json and \Allfiles\Labs\10\az104-10-vms-edge-parameters.json into the Cloud Shell home directory.

5. From the Cloud Shell pane, run the following to create the resource group that will be hosting the virtual machines (replace the [Azure_region] placeholder with the name of an Azure region where you intend to deploy Azure virtual machines). Type each command line separately and execute them separately:



6. From the Cloud Shell pane, run the following to create the first virtual network and deploy a virtual machine into it by using the template and parameter files you uploaded:

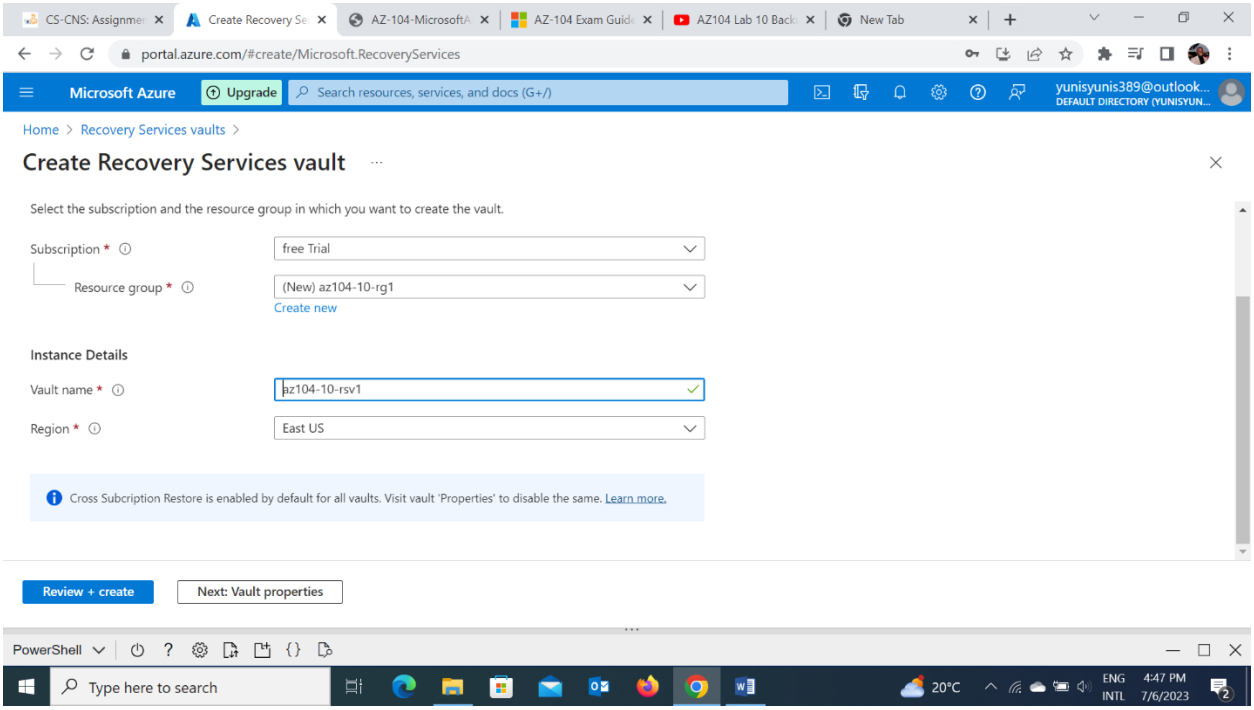
7. Minimize Cloud Shell (but do not close it).



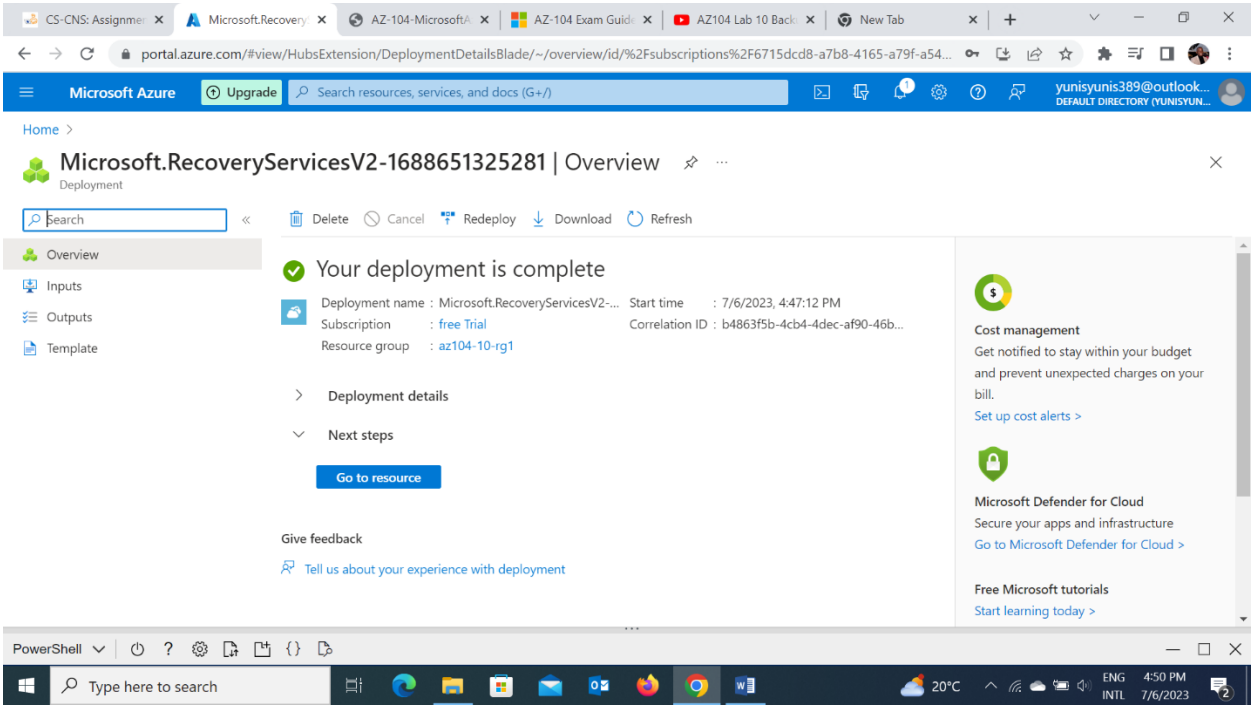
Task 2: Create a Recovery Services vault

1. In the Azure portal, search for and select **Recovery Services vaults** and, on the **Recovery Services vaults** blade, click **+ Create**.

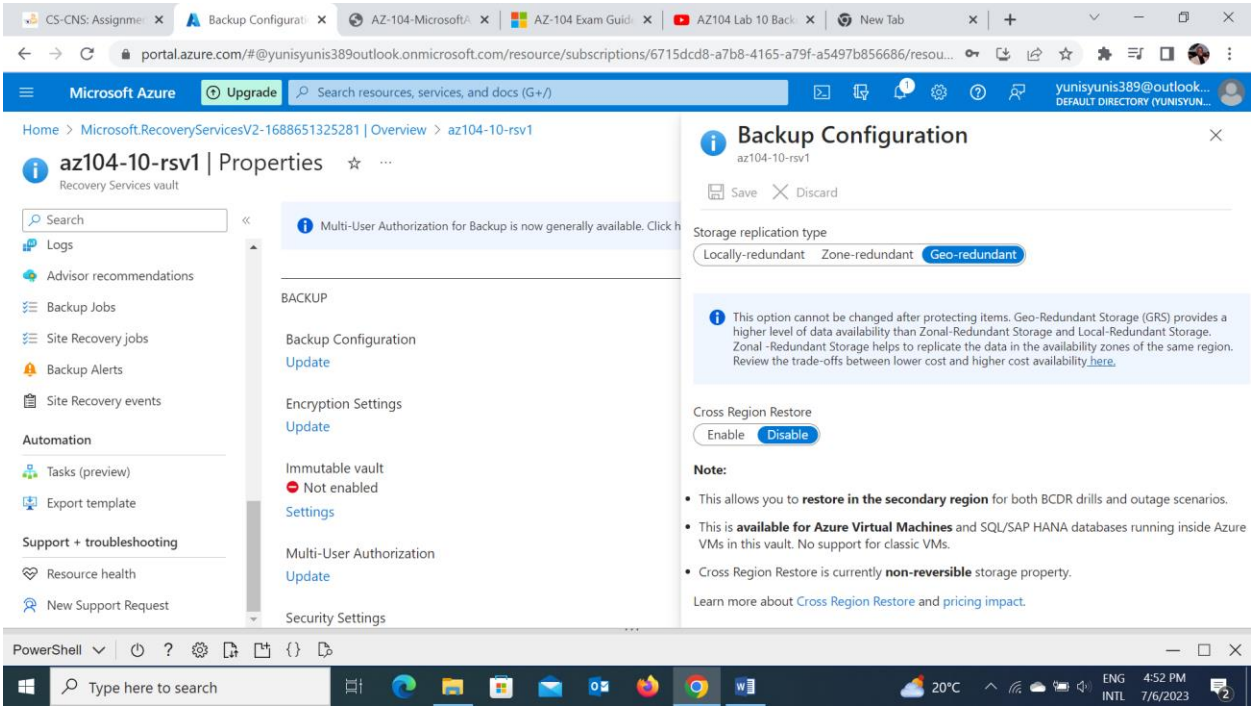
2. On the **Create Recovery Services vault** blade, specify the following settings:



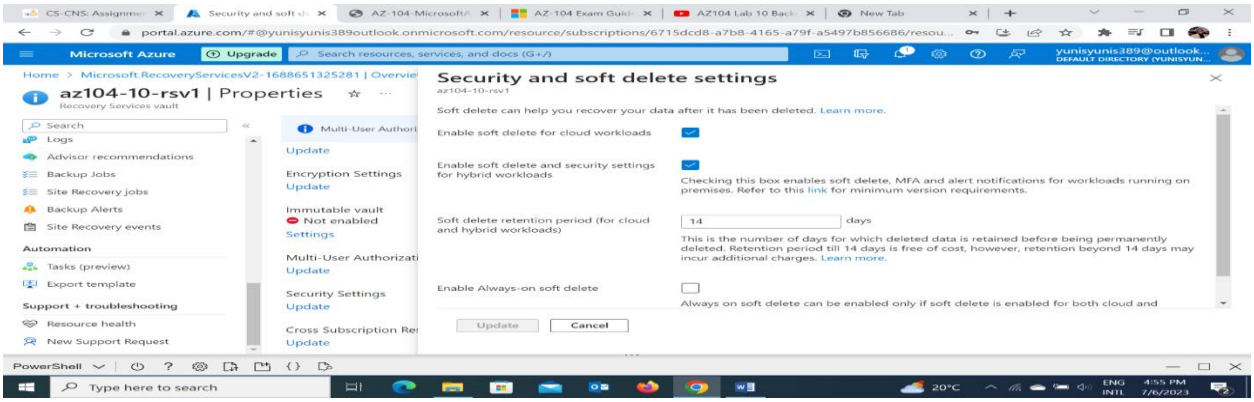
3. Click **Review + Create**, ensure that the validation passed and click **Create**.



4. When the deployment is completed, click Go to Resource.
5. On the **az104-10-rsv1** Recovery Services vault blade, in the Settings section, click Properties.
6. On the **az104-10-rsv1** - Properties blade, click the Update link under Backup Configuration label.
7. On the Backup Configuration blade, note that you can set the Storage replication type to either **Locally-redundant** or **Geo-redundant**. Leave the default setting of Geo-redundant in place and close the blade.



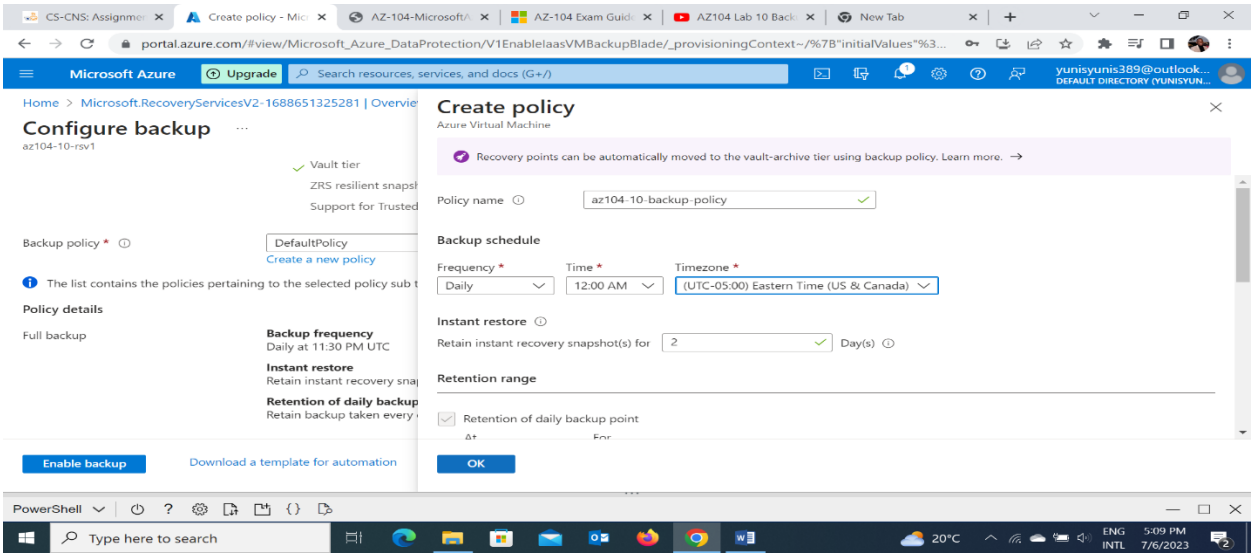
8. Back on the az104-10-rsv1 - Properties blade, click the Update link under Security Settings label.
9. On the Security Settings blade, note that Soft Delete (For workload running in Azure) is Enabled.



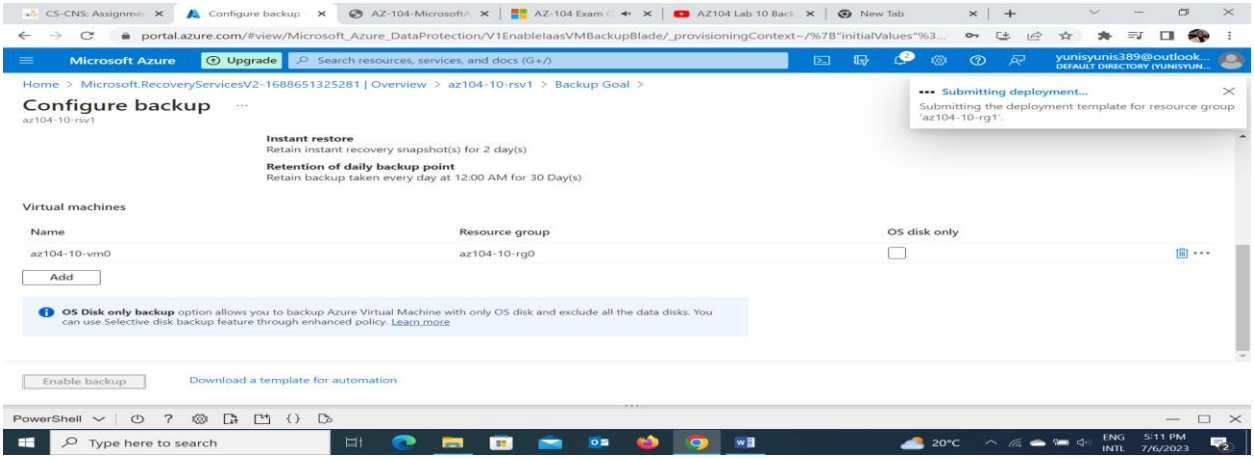
10. Close the Security Settings blade and, back on the az104-10-rsv1 Recovery Services vault blade, click Overview.

Task 3: Implement Azure virtual machine-level backup

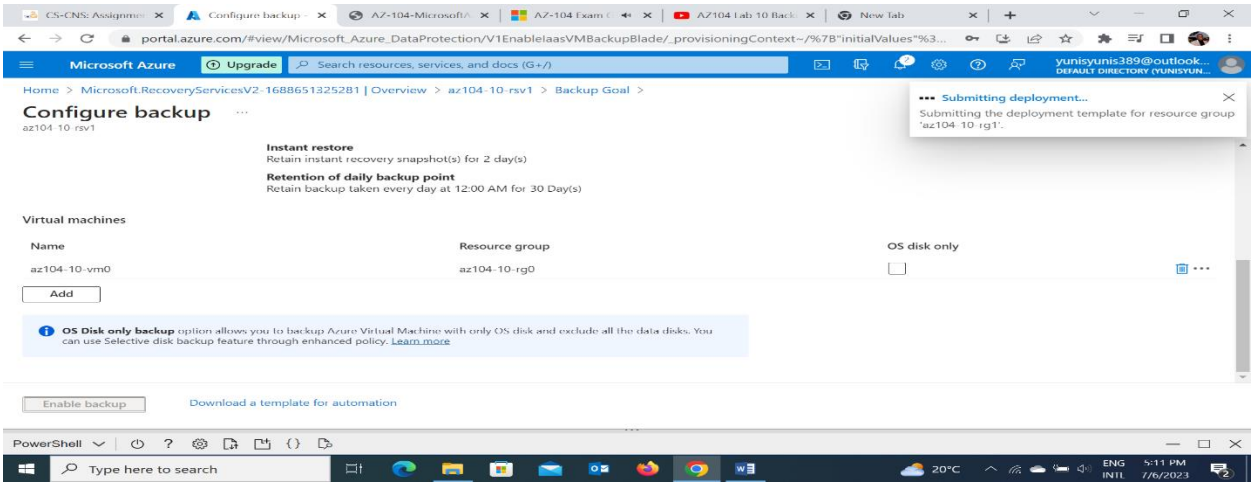
1. On the **az104-10-rsv1** Recovery Services vault blade, click **Overview**, then click **+ Backup**.
2. On the **Backup Goal** blade, specify the following settings:
3. On the Backup Goal blade, click Backup.
4. On the Backup policy, review the **DefaultPolicy** settings and select Create a **new policy**.
5. Define a new backup policy with the following settings (leave others with their default values):



6. Click **OK** to create the policy and then, in the Virtual Machines section, select **Add**.
7. On the Select virtual machines blade, select az-104-10-vm0, click OK, and, back on the Backup blade, click Enable backup.



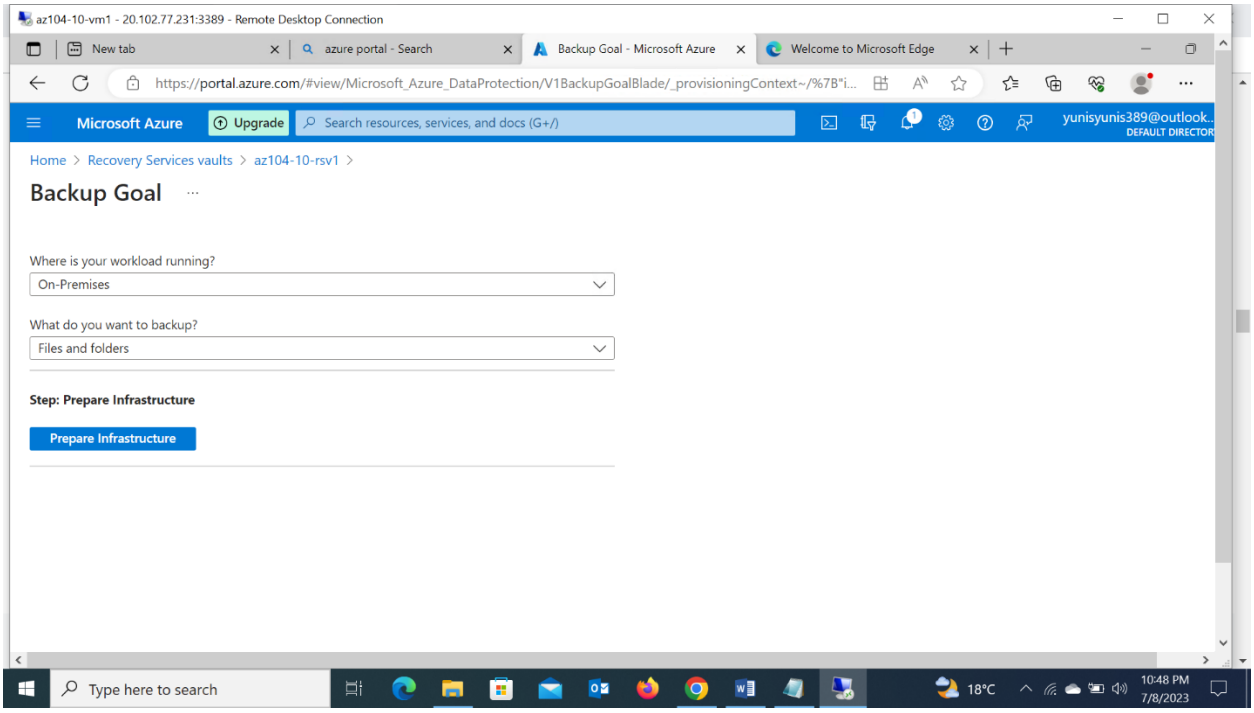
8. Navigate back to the az104-10-rsv1 Recovery Services vault blade, in the Protected items section, click Backup items, and then click the Azure virtual machine entry.
9. On the Backup Items (Azure Virtual Machine) blade select the View details link for az104-10-vm0, and review the values of the Backup Pre-Check and Last Backup Status entries.
10. On the az104-10-vm0 Backup Item blade, click Backup now, accept the default value in the Retain Backup Till drop-down list, and click OK.



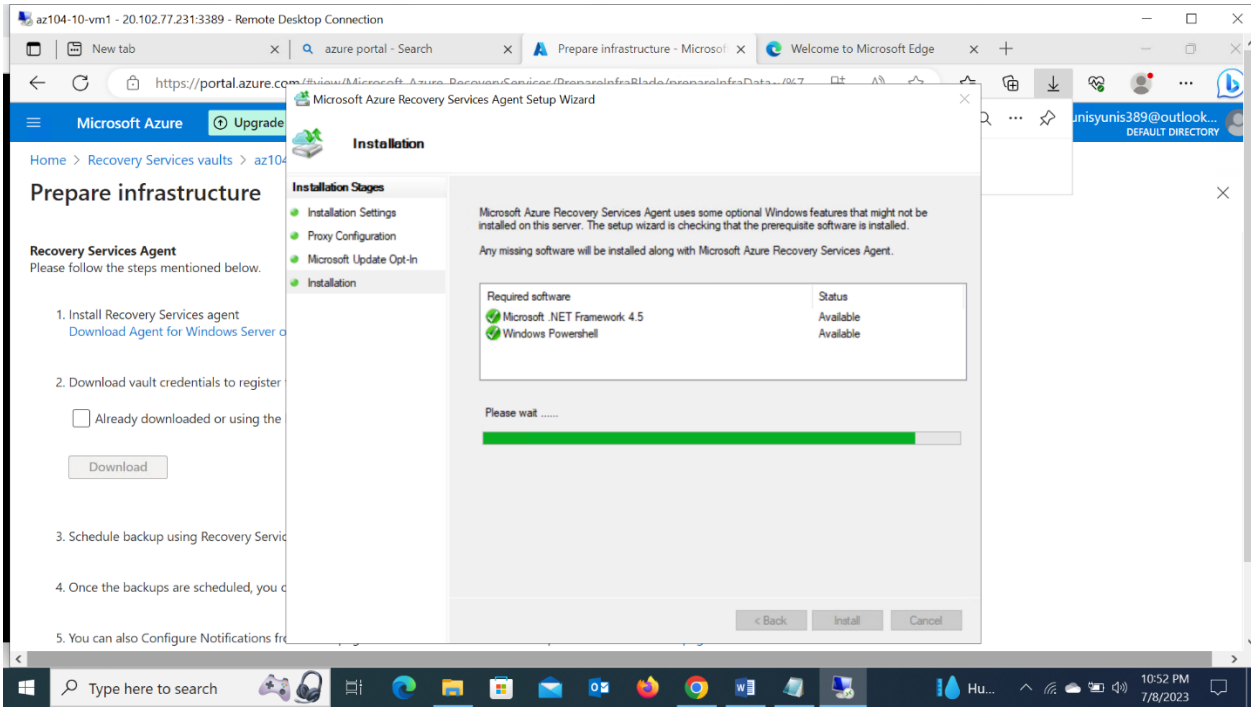
Task 4: Implement File and Folder backup

In this task, you will implement file and folder backup by using Azure Recovery Services.

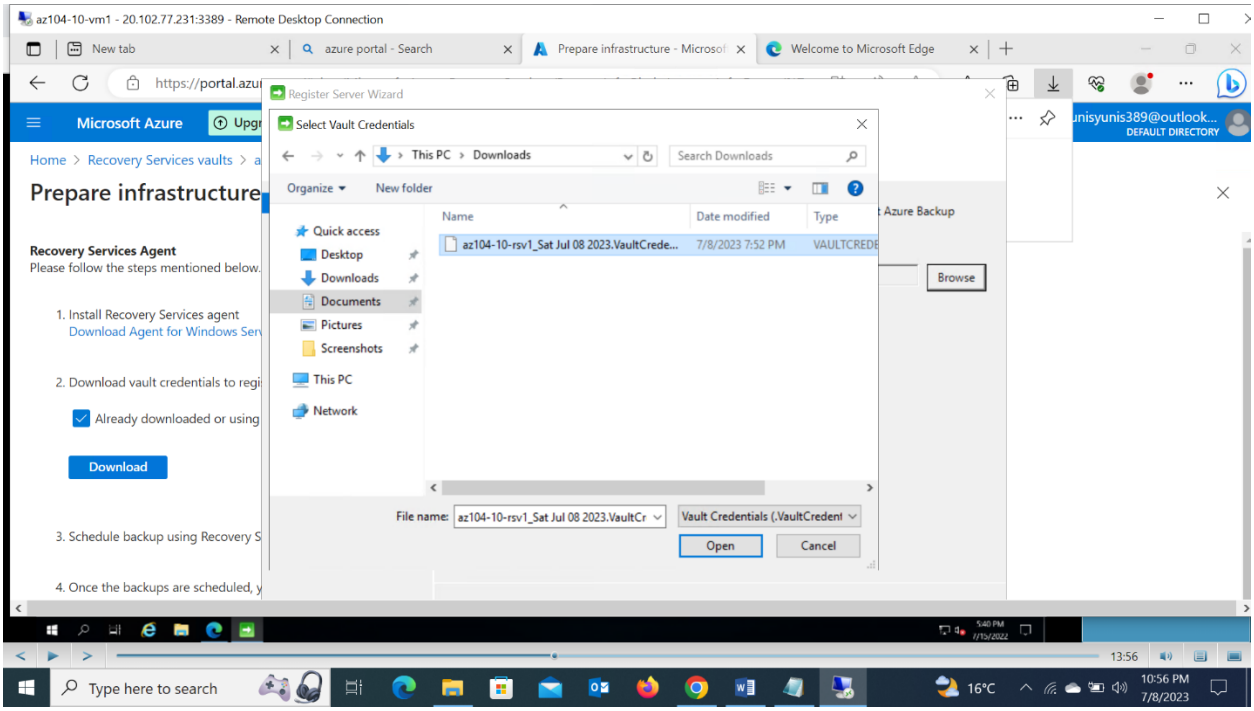
1. In the Azure portal, search for and select **Virtual machines**, and on the **Virtual machines** blade, click **az104-10-vm1**.
2. On the **az104-10-vm1** blade, click **Connect**, in the drop-down menu, click **RDP**, on the **Connect with RDP** blade, click **Download RDP File** and follow the prompts to start the Remote Desktop session.
3. When prompted, sign in by using the Student username and the password from the parameters file.
4. Within the Remote Desktop session to the az104-10-vm1 Azure virtual machine, start an Edge web browser, browse to the Azure portal, and sign in using your credentials.
5. In the Azure portal, search for and select Recovery Services vaults and, on the Recovery Services vaults, click az104-10-rsv1.
6. On the az104-10-rsv1 Recovery Services vault blade, click + Backup.
7. On the Backup Goal blade, specify the following settings:



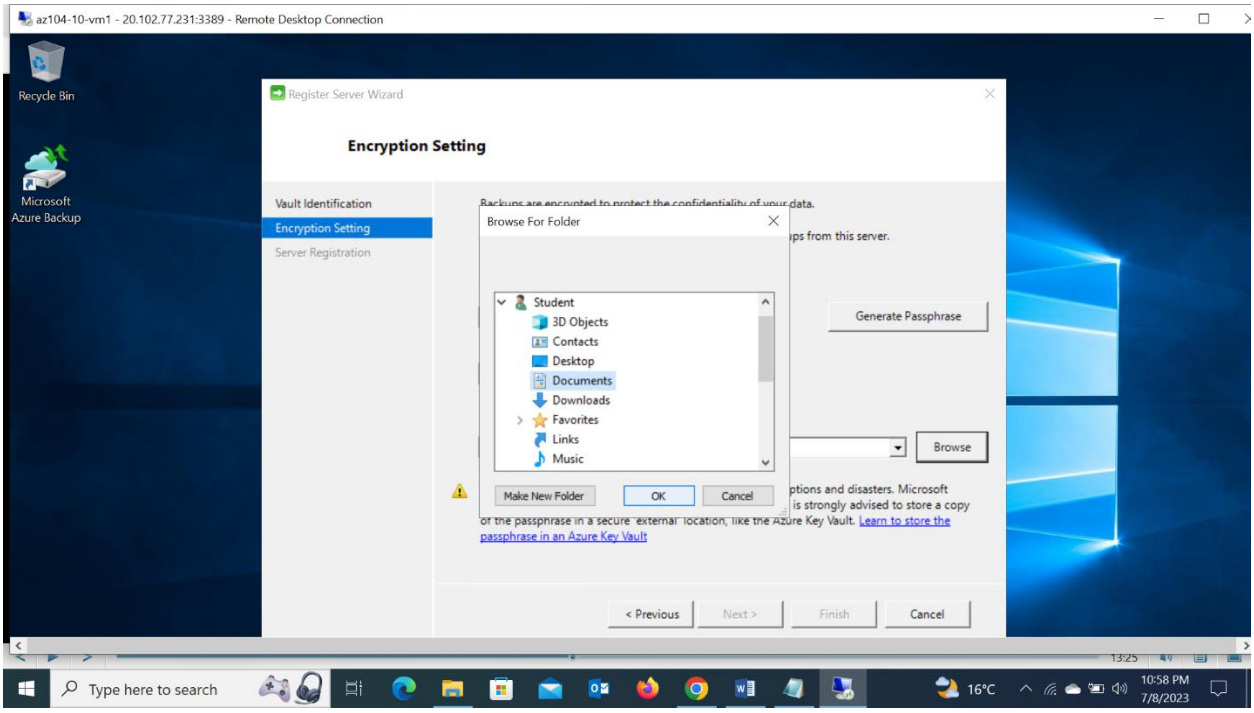
8. On the Backup Goal blade, click Prepare infrastructure.
9. On the Prepare infrastructure blade, click the Download Agent for Windows Server or Windows Client link.
10. When prompted, click Run to start installation of MARSAgentInstaller.exe with the default settings.



11. On the Installation page of the Microsoft Azure Recovery Services Agent Setup Wizard, click Proceed to Registration. This will start Register Server Wizard.
12. Switch to the web browser window displaying the Azure portal, on the Prepare infrastructure blade, select the checkbox Already downloaded or using the latest Recovery Server Agent, and click Download.
13. When prompted, whether to open or save the vault credentials file, click Save. This will save the vault credentials file to the local Downloads folder.
14. Switch back to the Register Server Wizard window and, on the Vault Identification page, click Browse.
15. In the Select Vault Credentials dialog box, browse to the Downloads folder, click the vault credentials file you downloaded, and click Open.



16. Back on the Vault Identification page, click Next.
17. On the Encryption Setting page of the Register Server Wizard, click Generate Passphrase.
18. On the Encryption Setting page of the Register Server Wizard, click the Browse button next to the Enter a location to save the passphrase.
19. In the Browse For Folder dialog box, select the Documents folder and click OK.



20. Click Finish, review the Microsoft Azure Backup warning and click Yes, and wait for the registration to complete.

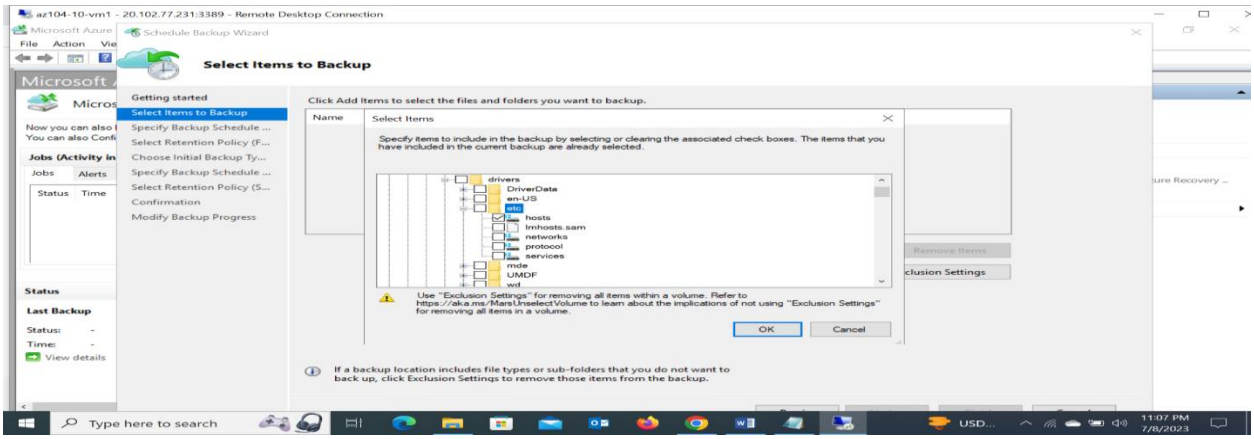
21. On the Server Registration page of the Register Server Wizard, review the warning regarding the location of the passphrase file, ensure that the Launch Microsoft Azure Recovery Services Agent checkbox is selected and click Close. This will automatically open the Microsoft Azure Backup console.

22. In the Microsoft Azure Backup console, in the Actions pane, click Schedule Backup.

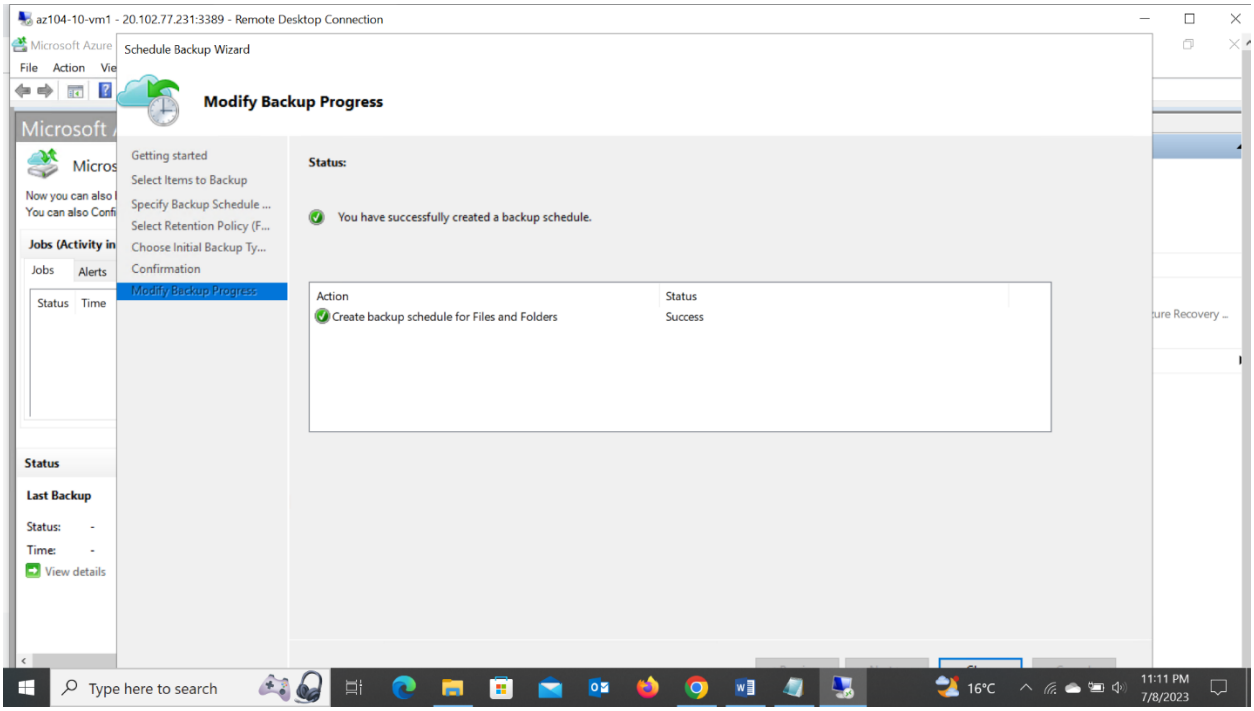
23. In the Schedule Backup Wizard, on the Getting started page, click Next.

24. On the Select Items to Backup page, click Add Items.

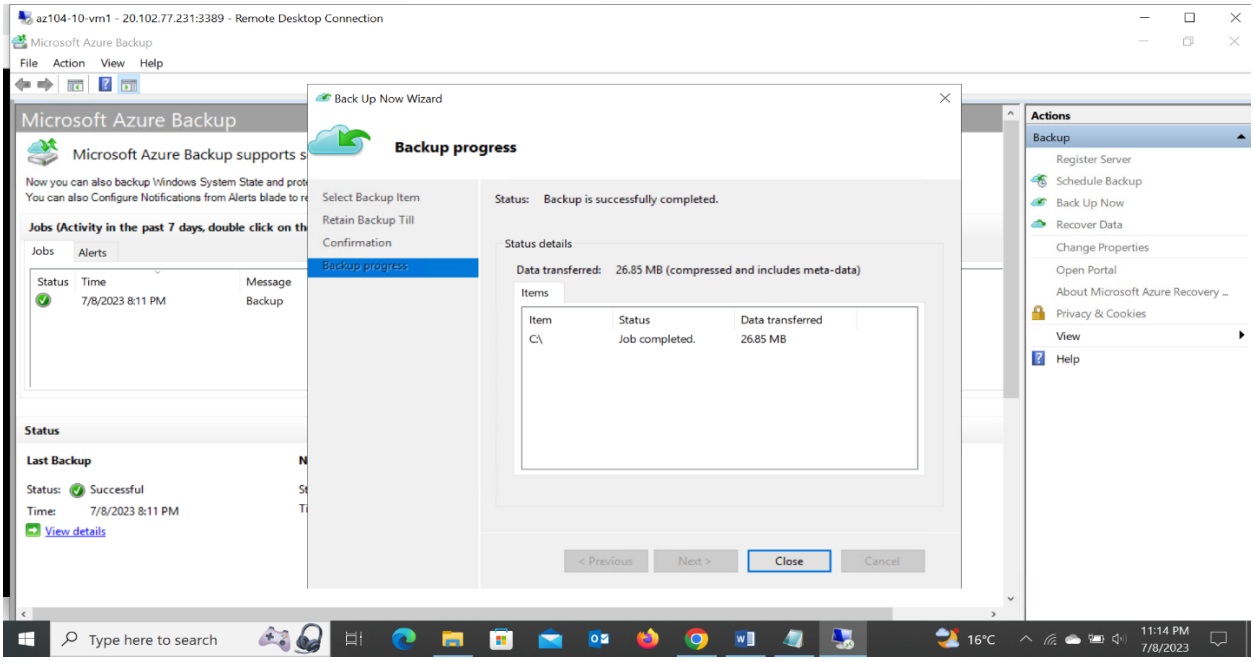
25. In the Select Items dialog box, expand C:\Windows\System32\drivers\etc\, select hosts, and then click OK:



26. On the Select Items to Backup page, click Next.
27. On the Specify Backup Schedule page, ensure that the Day option is selected, in the first drop-down list box below the At following times (Maximum allowed is three times a day) box, select 4:30 AM, and then click Next.
28. On the Select Retention Policy page, accept the defaults, and then click Next.
29. On the Choose Initial Backup type page, accept the defaults, and then click Next.
30. On the Confirmation page, click Finish. When the backup schedule is created, click Close.



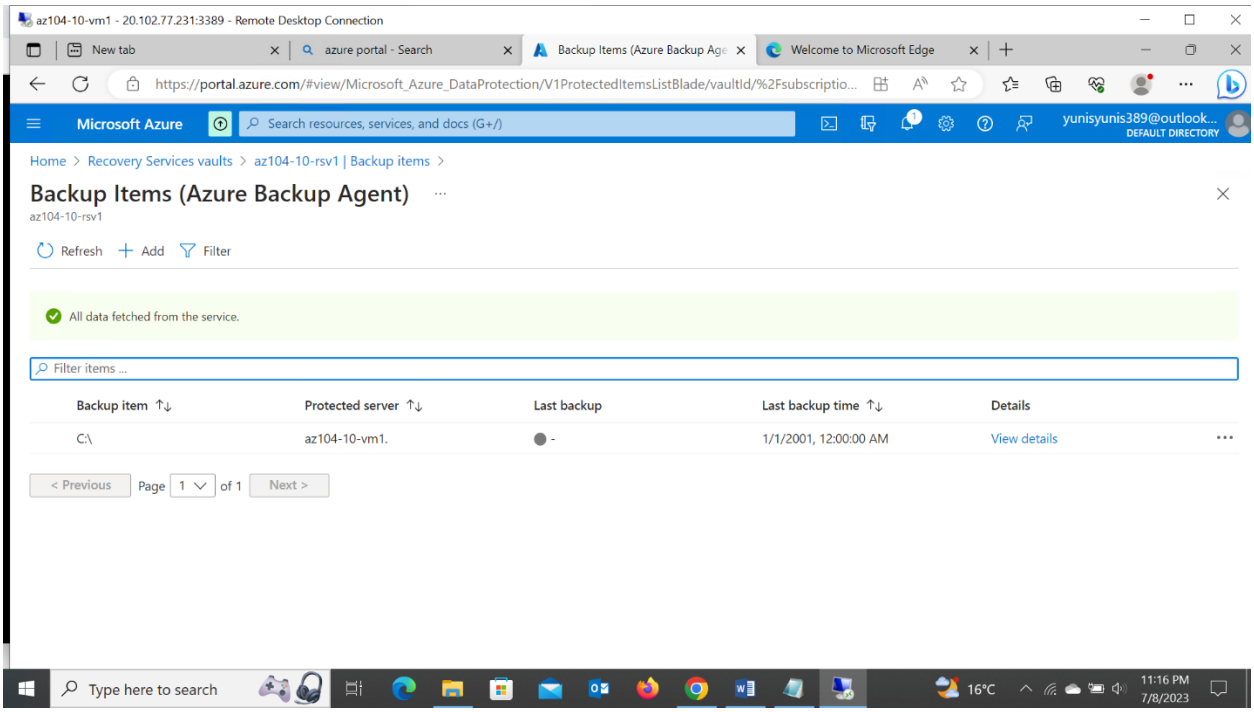
31. In the Microsoft Azure Backup console, in the Actions pane, click Back Up Now.
32. In the Back Up Now Wizard, on the Select Backup Item page, ensure that the Files and Folders option is selected and click Next.
33. On the Retain Backup Till page, accept the default setting and click Next.
34. On the Confirmation page, click Back Up.
35. When the backup is complete, click Close, and then close Microsoft Azure Backup.



36. Switch to the web browser window displaying the Azure portal, navigate back to the Recovery Services vault blade, in the Protected items section, and click Backup items.

37. On the az104-10-rsv1 - Backup items blade, click Azure Backup Agent.

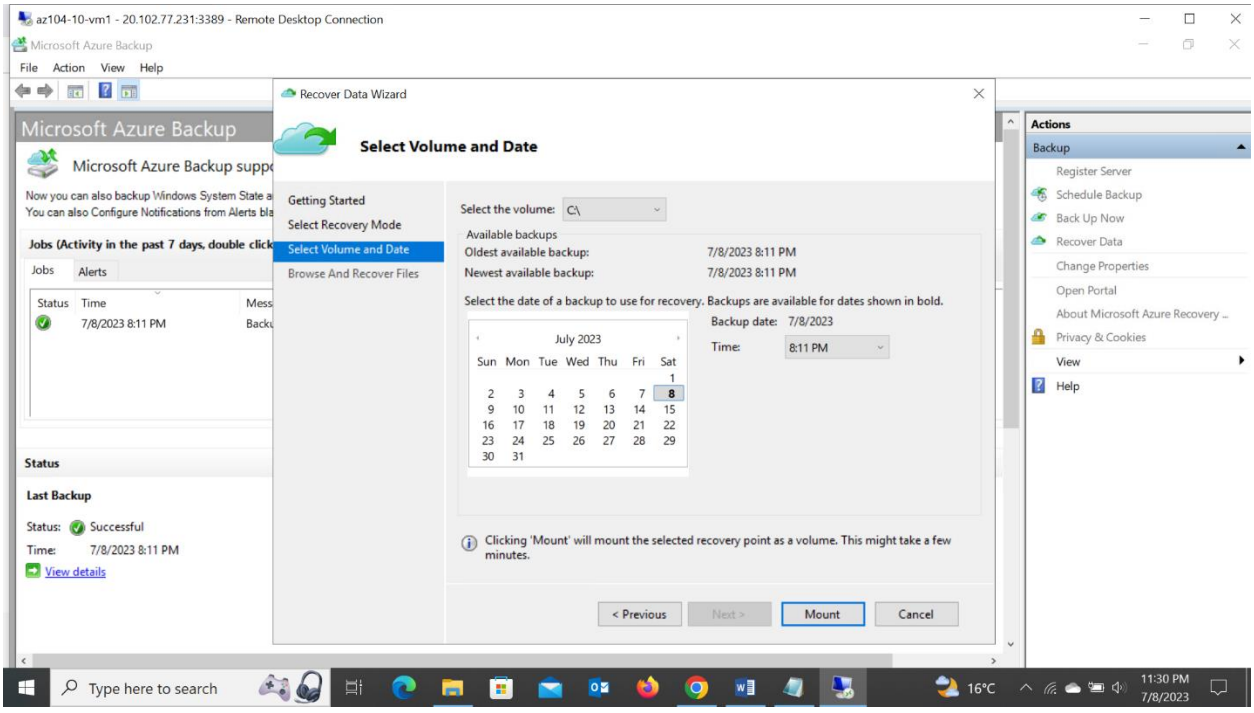
38. On the Backup Items (Azure Backup Agent) blade, verify that there is an entry referencing the C:\ drive of az104-10-vm1.



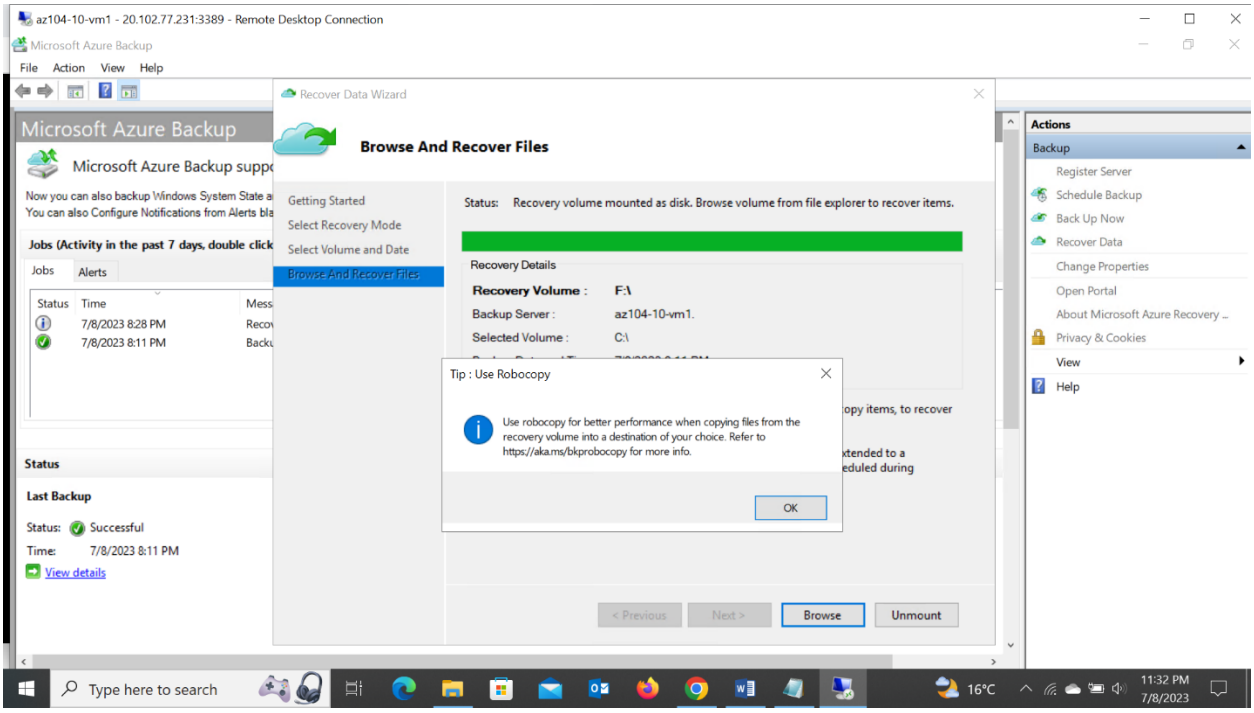
Task 5: Perform file recovery by using Azure Recovery Services agent (optional)

In this task, you will perform file restore by using Azure Recovery Services agent.

1. Within the Remote Desktop session to **az104-10-vm1**, open File Explorer, navigate to the **C:\Windows\System32\drivers\etc** folder and delete the **hosts** file.
2. Open Microsoft Azure Backup and click **Recover data** in the **Actions** pane. This will start **Recover Data Wizard**.
3. On the **Getting Started** page of **Recover Data Wizard**, ensue that **This server (az104-10-vm1.)** option is selected and click **Next**.
4. On the **Select Recovery Mode** page, ensure that **Individual files and folders** option is selected, and click **Next**.
5. On the **Select Volume and Date** page, in the **Select the volume** drop down list, select **C:**, accept the default selection of the available backup, and click **Mount**.

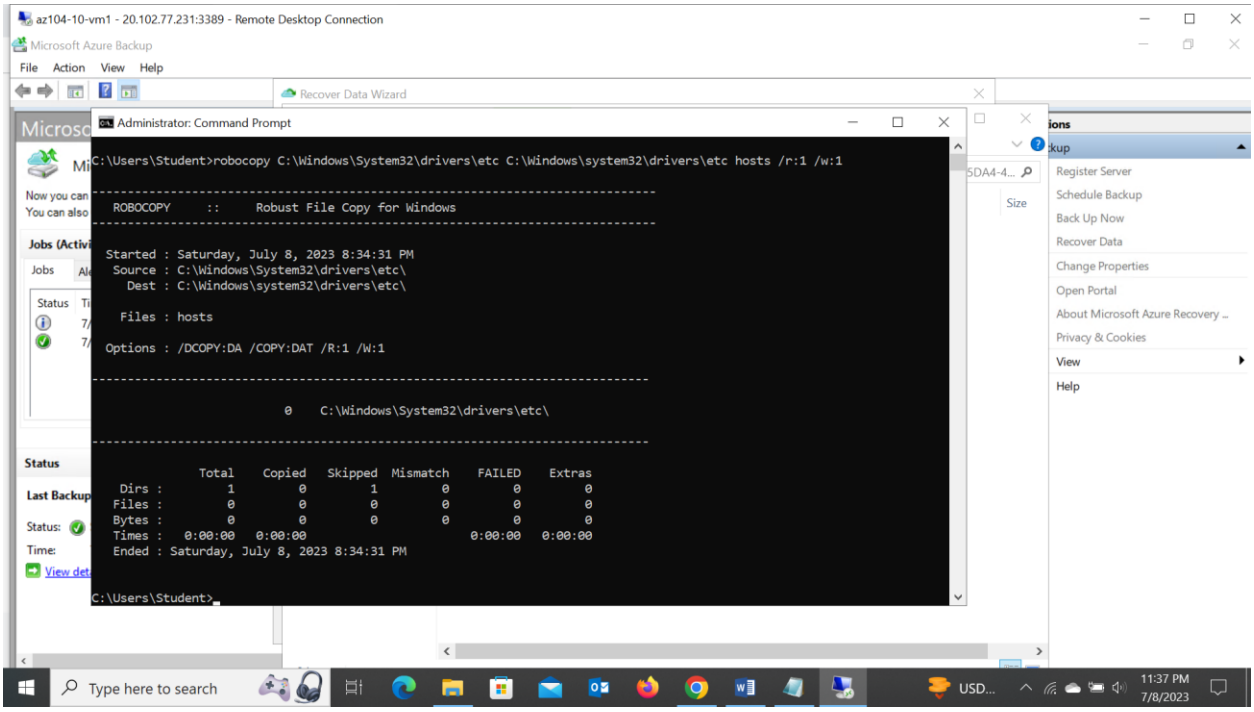


6. On the Browse And Recover Files page, note the drive letter of the recovery volume and review the tip regarding the use of robocopy.

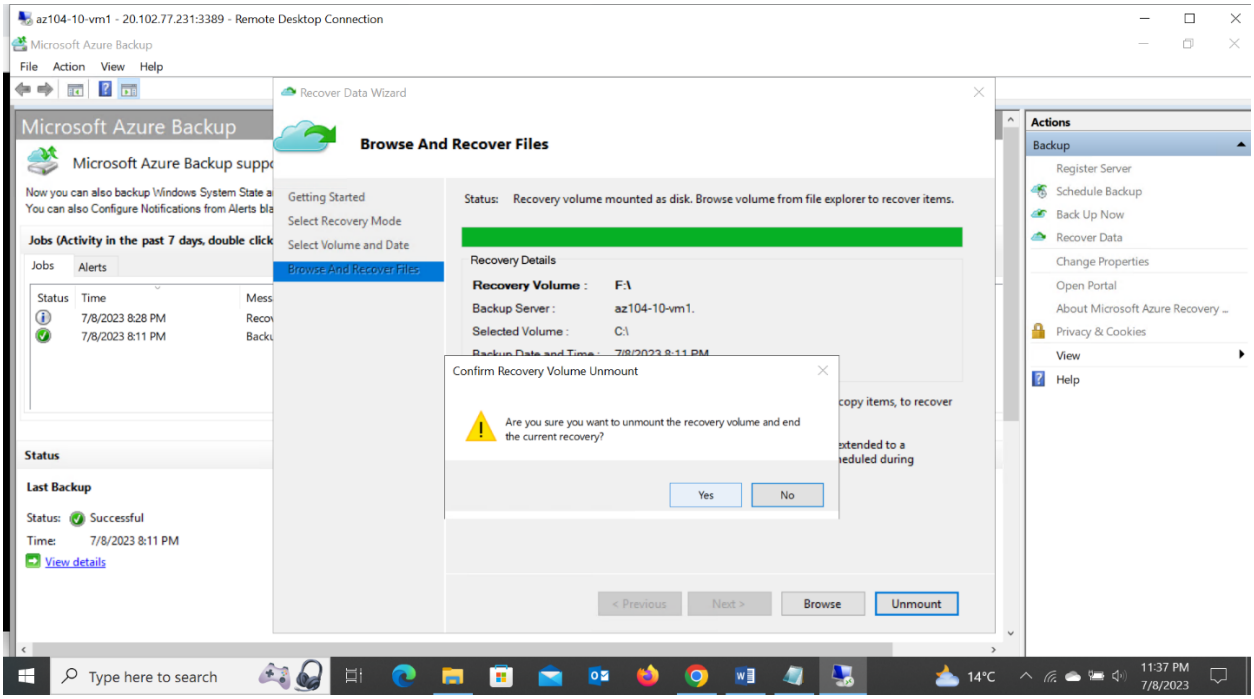


7. Click Start, expand the Windows System folder, and click Command Prompt.

8. From the Command Prompt, run the following to copy the restore the hosts file to the original location (replace [recovery_volume] with the drive letter of the recovery volume you identified earlier):



9. Switch back to the Recover Data Wizard and, on the Browse and Recover Files, click Unmount and, when prompted to confirm, click Yes.

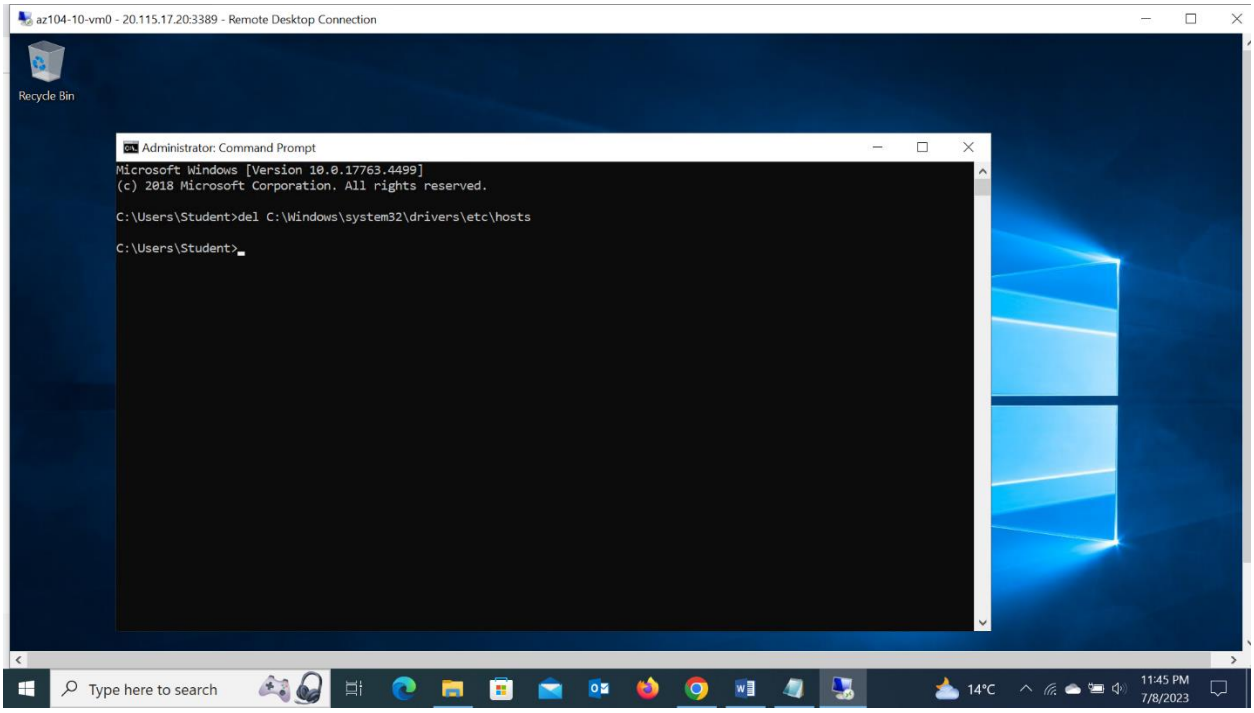


10. Terminate the Remote Desktop session.

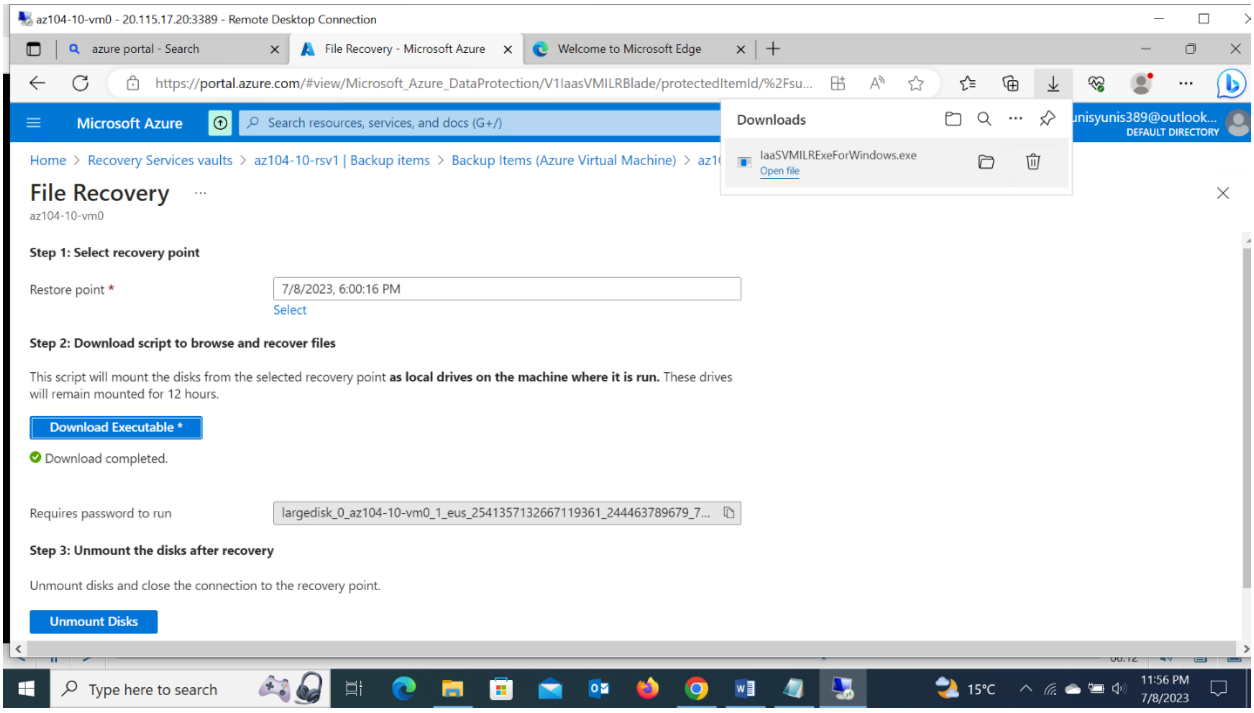
Task 6: Perform file recovery by using Azure virtual machine snapshots (optional)

In this task, I will restore a file from the Azure virtual machine-level snapshot-based backup.

1. Switch to the browser window running on your lab computer and displaying the Azure portal.
2. In the Azure portal, search for and select **Virtual machines**, and on the **Virtual machines** blade, click **az104-10-vm0**.
3. On the **az104-10-vm0** blade, click **Connect**, in the drop-down menu, click **RDP**, on the **Connect with RDP** blade, click **Download RDP File** and follow the prompts to start the Remote Desktop session.
4. When prompted, sign in by using the **Student** username and the password from the parameters file.
5. Within the Remote Desktop session to the az104-10-vm0, click Start, expand the Windows System folder, and click Command Prompt.
6. From the Command Prompt, run the following to delete the hosts file:



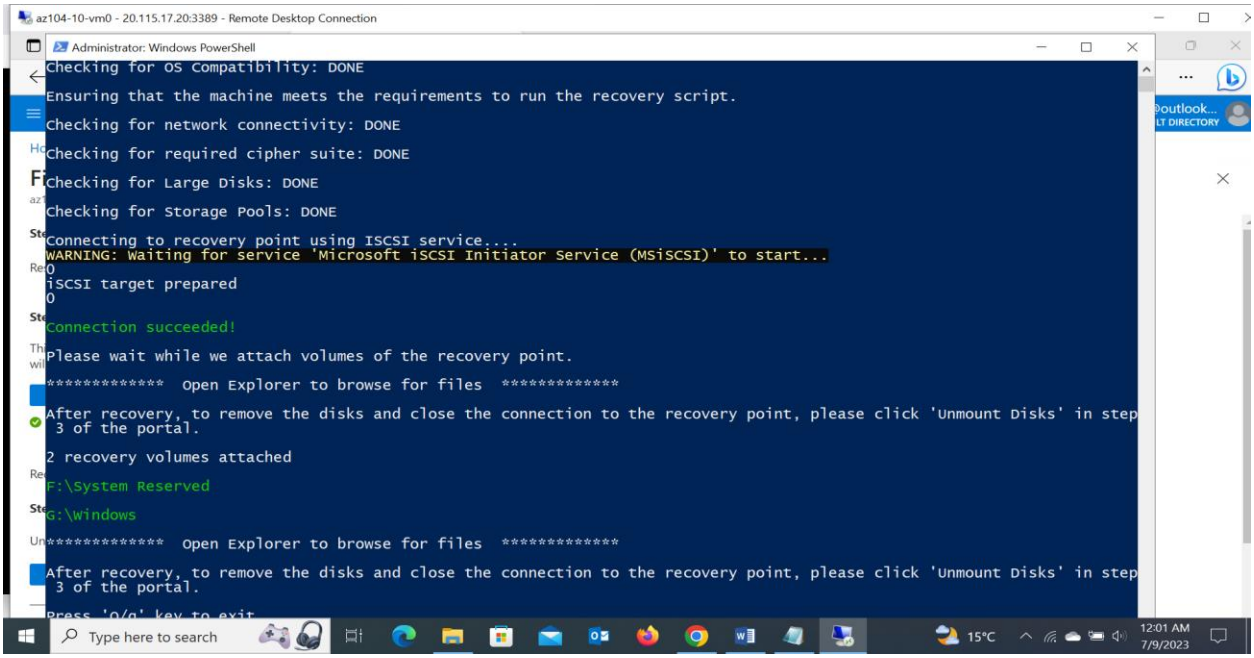
7. Within the Remote Desktop session to the az104-10-vm0 Azure virtual machine, start an Edge web browser, browse to the Azure portal, and sign in using your credentials.
8. In the Azure portal, search for and select Recovery Services vaults and, on the Recovery Services vaults, click az104-10-rsv1.
9. On the az104-10-rsv1 Recovery Services vault blade, in the Protected items section, click Backup items.
10. On the az104-10-rsv1 - Backup items blade, click Azure Virtual Machine.
11. On the Backup Items (Azure Virtual Machine) blade, select View details for az104-10-vm0.
12. On the az104-10-vm0 Backup Item blade, click File Recovery.
13. On the **File Recovery** blade, accept the default recovery point and click **Download Executable**.
14. Click Download and, when prompted whether to run or save IaaSVMILRExeForWindows.exe, click Save.



15. Back in the File Explorer window, double-click the newly downloaded file.

16. When prompted to provide the password from the portal, copy the password from the Password to run the script text box on the File Recovery blade, paste it at the Command Prompt, and press Enter.

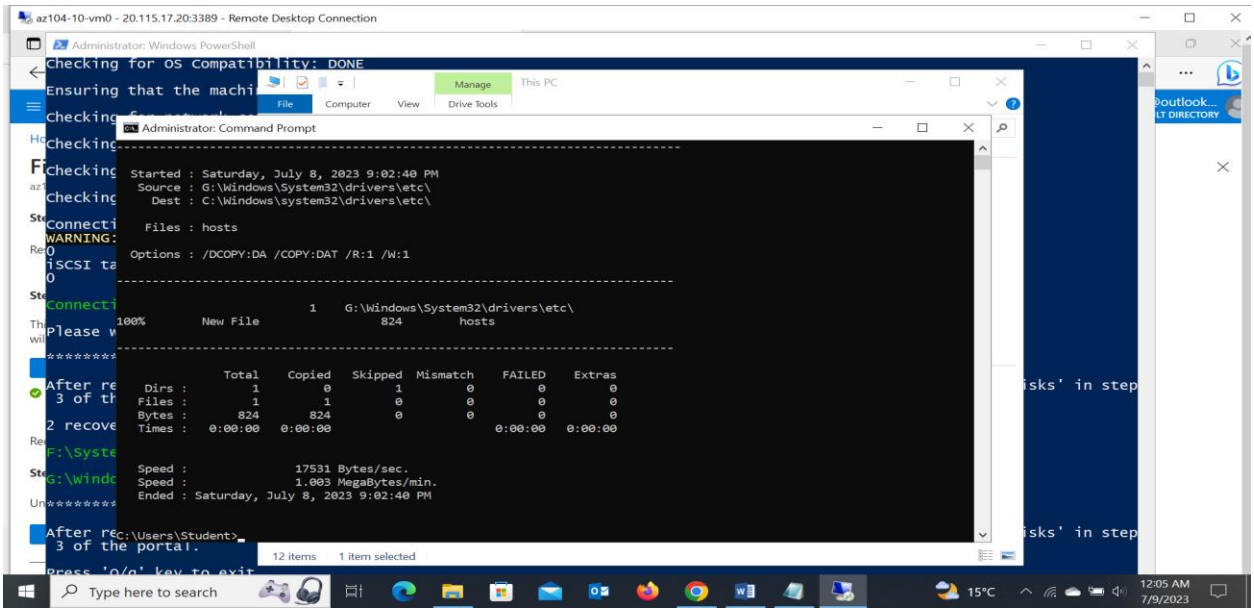
17. Wait for the mount process to complete, review the informational messages in the Windows PowerShell window, note the drive letter assigned to the volume hosting Windows, and start File Explorer.



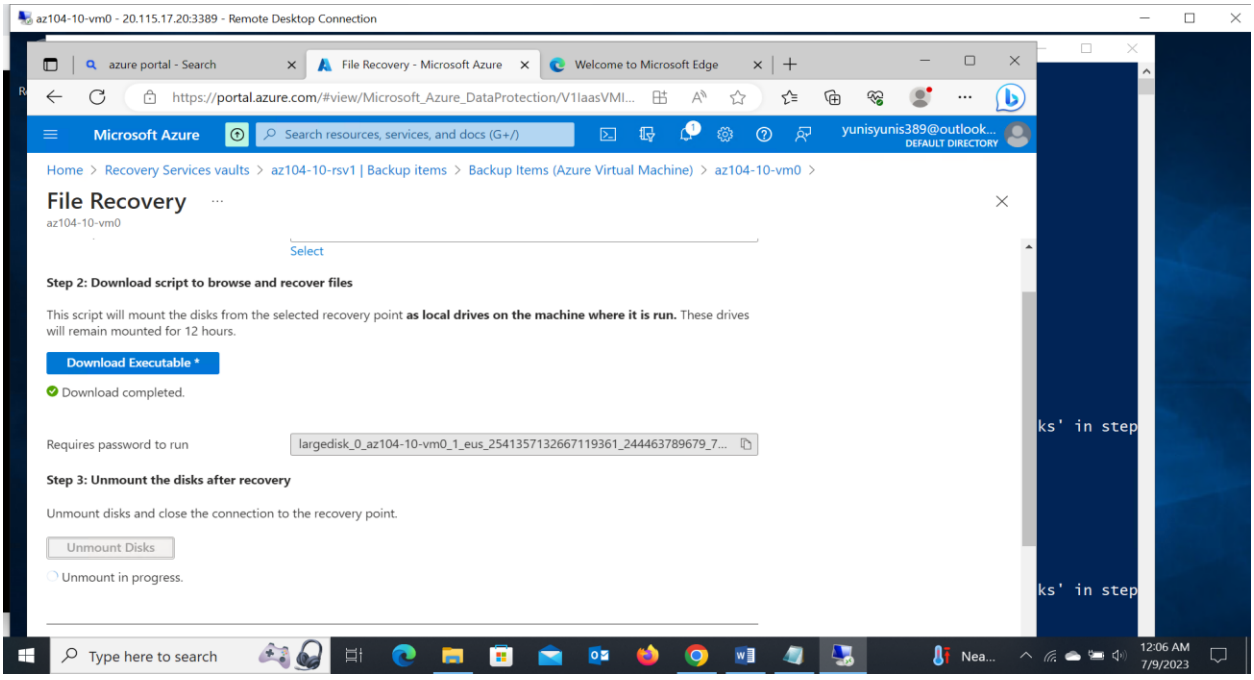
18. In File Explorer, navigate to the drive letter hosting the snapshot of the operating system volume you identified in the previous step and review its content.

19. Switch to the Command Prompt window.

20. From the Command Prompt, run the following to copy the restore the hosts file to the original location (replace [os_volume] with the drive letter of the operating system volume you identified earlier):



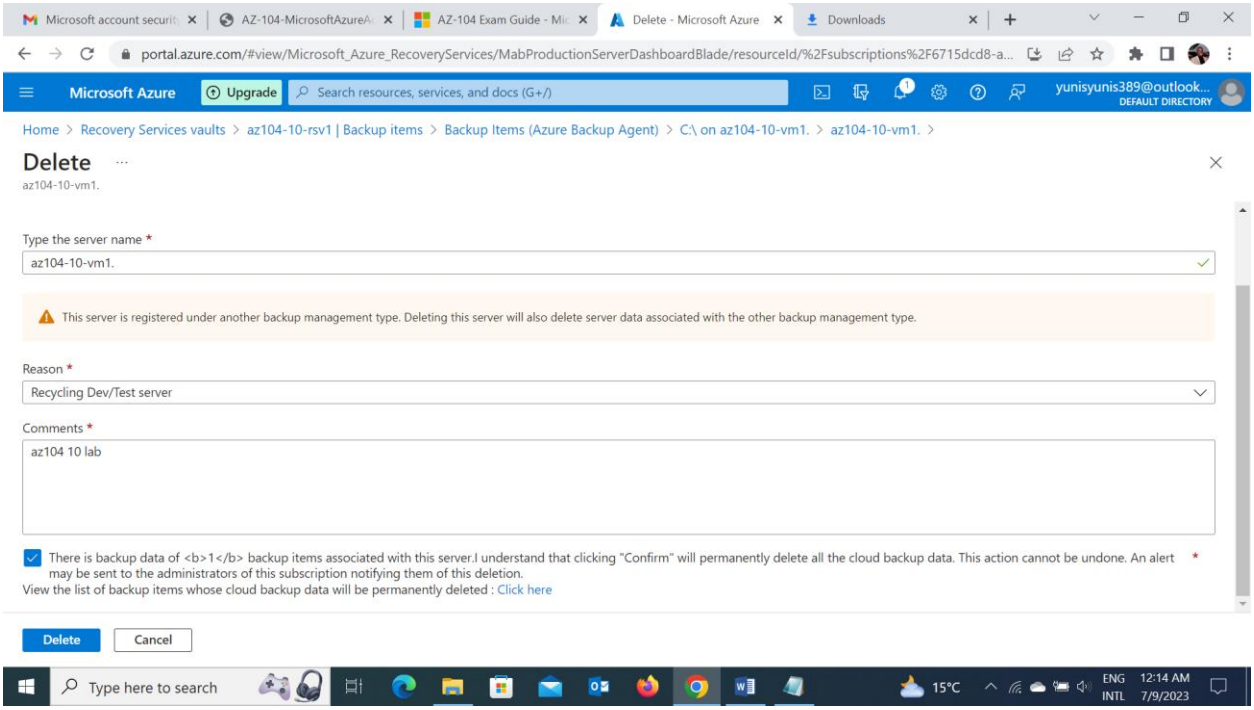
21. Switch back to the File Recovery blade in the Azure portal and click Unmount Disks.



22. Terminate the Remote Desktop session.

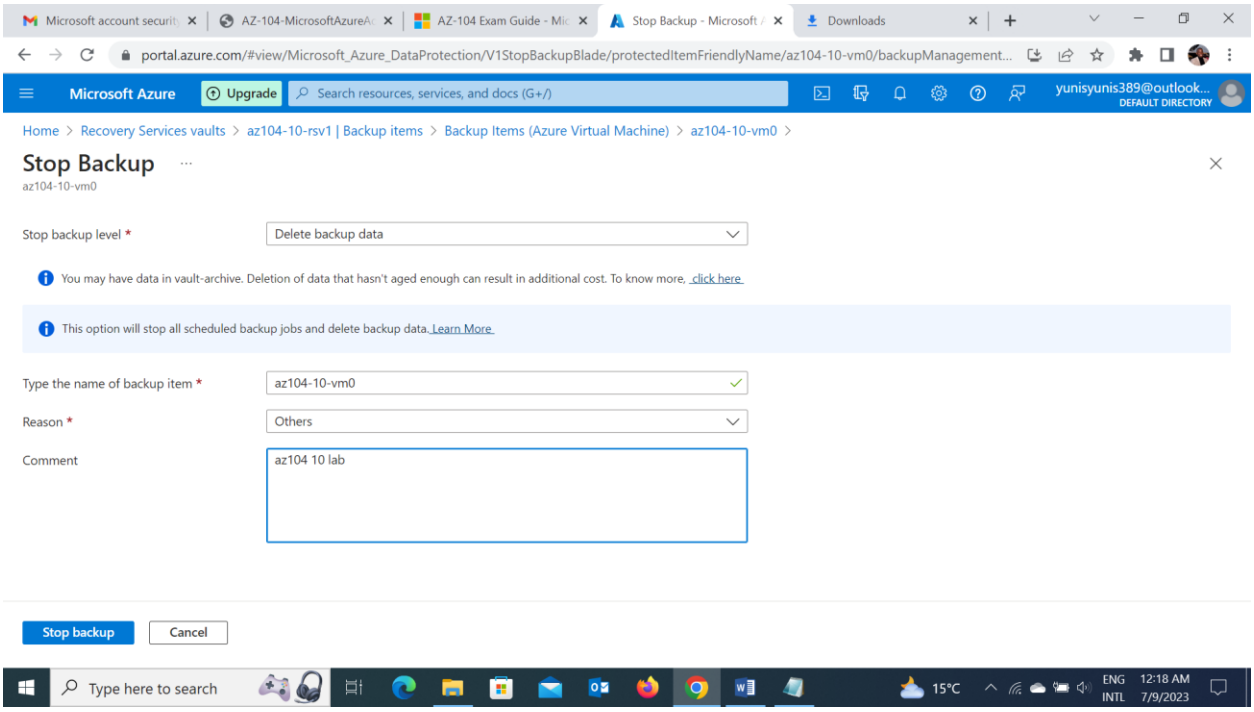
Task 7: Review the Azure Recovery Services soft delete functionality

1. On the lab computer, in the Azure portal, search for and select **Recovery Services vaults** and, on the **Recovery Services vaults**, click **az104-10-rsv1**.
2. On the **az104-10-rsv1** Recovery Services vault blade, in the **Protected items** section, click **Backup items**.
3. On the **az104-10-rsv1 - Backup items** blade, click **Azure Backup Agent**.
4. On the **Backup Items (Azure Backup Agent)** blade, click the entry representing the backup of **az104-10-vm1**.
5. On the **C:\ on az104-10-vm1.** blade, select **View details** for **az104-10-vm1.** .
6. On the Detail blade, click on **az104-10-vm1**.
7. On the **az104-10-vm1.** Protected Servers blade, click **Delete**.
8. On the **Delete** blade, specify the following settings.

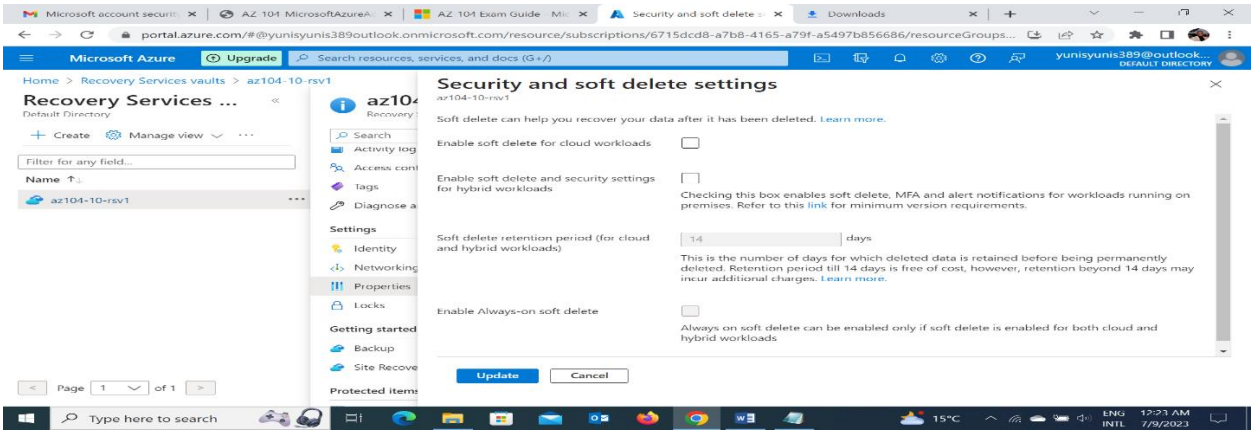


9. Enable the checkbox next to the label **There is backup data of 1 backup items associated with this server. I understand that clicking "Confirm" will permanently delete all the cloud backup data. This action cannot be undone. An alert may be sent to the administrators of this subscription notifying them of this deletion** and click **Delete**.

10. Navigate back to the az104-10-rsv1 - Backup items blade and click Azure Virtual Machines.
11. On the az104-10-rsv1 - Backup items blade, click Azure Virtual Machine.
12. On the Backup Items (Azure Virtual Machine) blade, select View details for az104-10-vm0.
13. On the az104-10-vm0 Backup Item blade, click Stop backup.
14. On the Stop backup blade, select Delete Backup Data, specify the following settings and click Stop backup:



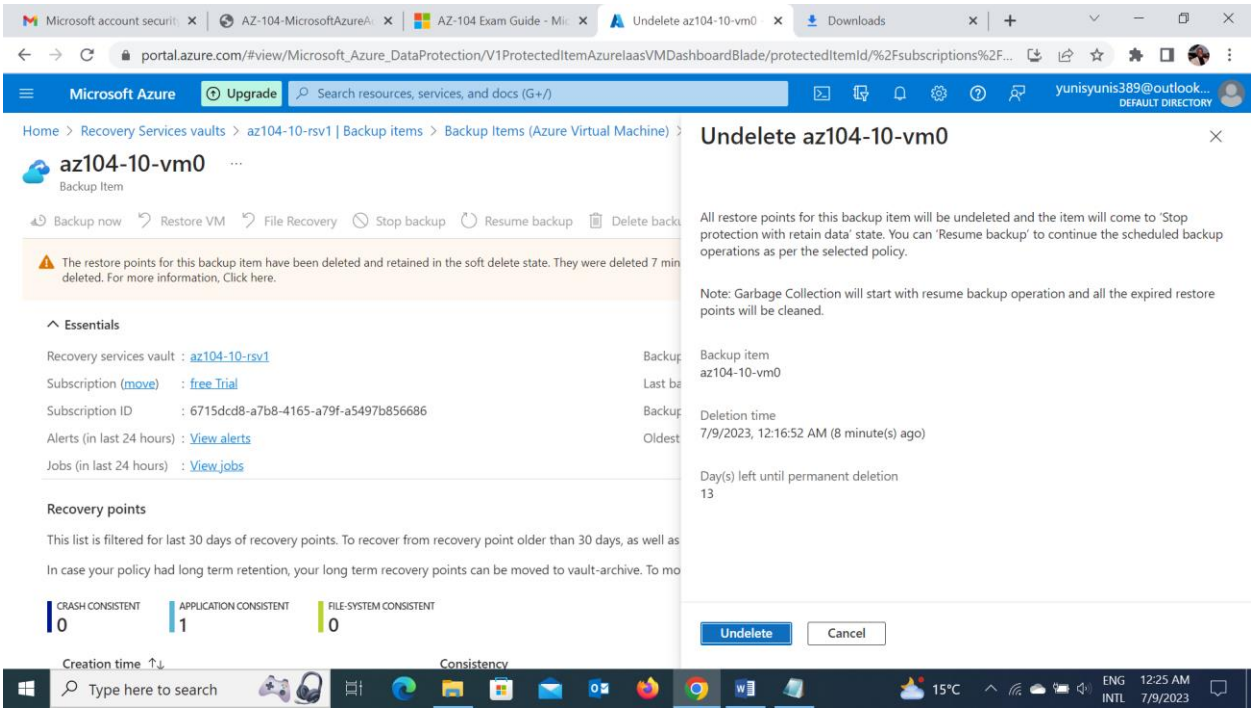
15. Navigate back to the az104-10-rsv1 - Backup items blade and click Refresh
16. Click the Azure Virtual Machine entry and, on the Backup Items (Azure Virtual Machine) blade, click the az104-10-vm0 entry.
17. On the az104-10-vm0 Backup Item blade, note that you have the option to Undelete the deleted backup.
18. Navigate back to the az104-10-rsv1 Recovery Services vault blade, and in the Settings section, click Properties.
19. On the az104-10-rsv1 - Properties blade, click the Update link under Security Settings label.
20. On the Security Settings blade, Disable Soft Delete (For workloads running in Azure) and also disable Security Features (For workloads running on-premises) and click Save.



21. Close the Security Settings blade and, back on the az104-10-rsv1 Recovery Services vault blade, click Overview.

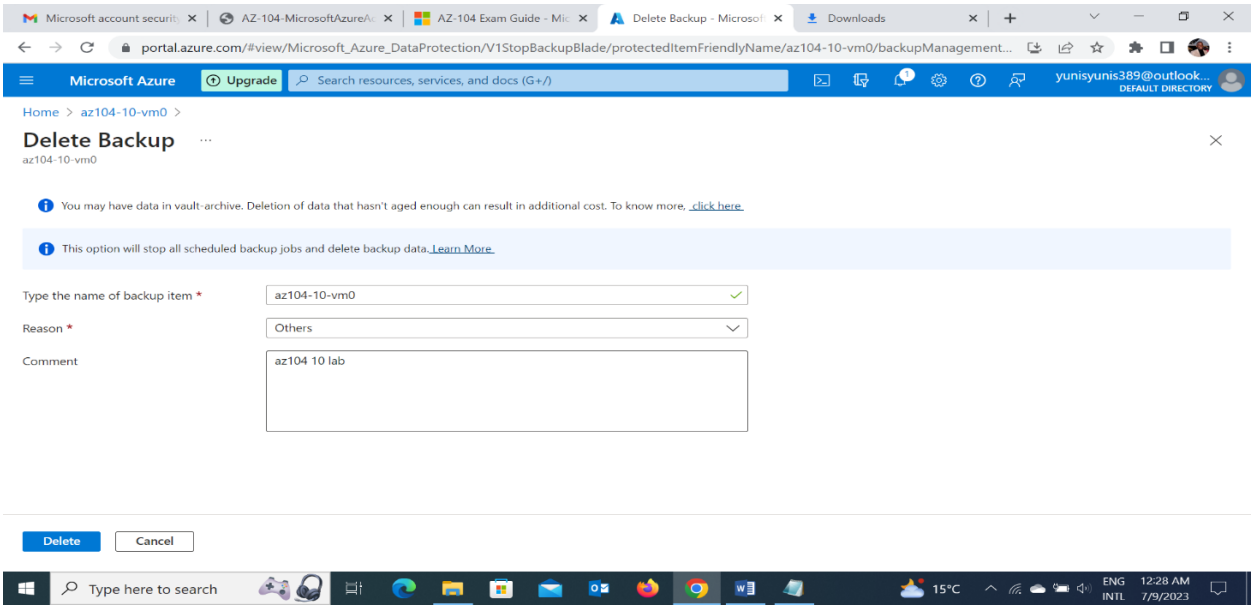
22. Navigate back to the az104-10-vm0 Backup Item blade and click Undelete.

23. On the Undelete az104-10-vm0 blade, click Undelete.

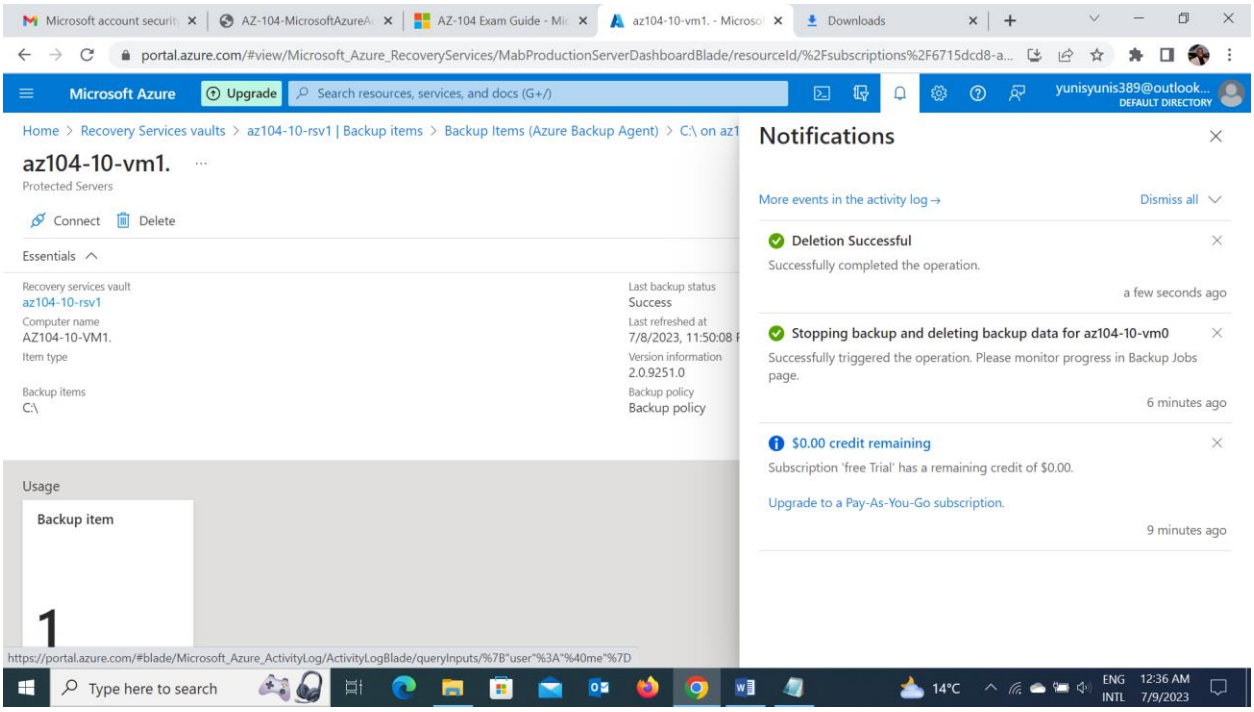


24. Wait for the undelete operation to complete, refresh the web browser page, if needed, navigate back to the az104-10-vm0 Backup Item blade, and click Delete backup data.

25. On the Delete Backup Data blade, specify the following settings and click Delete:



26. Repeat the steps at the beginning of this task to delete the backup items for az104-10-vm1.



Conclusion

In conclusion, this lab has provided a comprehensive and practical learning experience in the field of data protection practices. Through a series of tasks, I was able to gain valuable insights and skills in provisioning lab environments, creating Recovery Services vaults, implementing virtual machine-level and file/folder backups, performing file recoveries using Azure Recovery Services agent, and exploring optional features such as Azure virtual machine snapshots and Azure Recovery Services soft delete functionality. The lab emphasized the importance of robust data protection measures in safeguarding critical information, mitigating data loss risks, and ensuring business continuity. Armed with the knowledge gained from this lab, I am now better prepared to implement data protection strategies in Azure, effectively protecting valuable assets and ensuring system resilience. This experience serves as a solid foundation for real-world scenarios where data protection is essential, reinforcing the significance of securing sensitive information in today's ever-changing digital landscape.