😊 Azure Backup MARS Agent

Azure Backup MARS (Microsoft Azure Recovery Services) Agent is a tool used for backing up on-premises data to Azure. It provides a way to protect files, folders, system state, and other data, allowing for recovery in case of data loss, corruption, or disaster.

Here are key points about Azure Backup MARS Agent:

1. **Backup to Azure:** The MARS Agent enables direct backup of data from on-premises servers to Azure.
2. **Files and Folders:** It allows the backup of individual files and folders.
3. **System State Backup:** Supports system state backup, crucial for recovering a server to a previous state.
4. **No Infrastructure Required:** Does not require additional infrastructure; data is backed up directly to Azure.
5. **Compression and Encryption:** Data is compressed and encrypted before transmission to ensure security and reduce storage costs.
6. **Scheduling and Retention:** Offers flexible backup schedules and retention policies to meet various recovery point objectives (RPOs).
7. **Integration with Azure:** Works seamlessly with Azure services, providing a unified solution for data protection.

😄 Use cases of MARS agent:

1. **File and Folder Backup:** Use Azure Backup MARS Agent to regularly back up critical files and folders from on-premises servers to Azure. This ensures that important documents, configurations, and user data are protected against accidental deletion, corruption, or hardware failure.
2. **System State Protection:** Employ Azure Backup MARS Agent to back up the system state of Windows servers. This includes critical operating system components, registry settings, and Active Directory data. System state backups are essential for restoring server functionality in case of system crashes or configuration errors.
3. **Disaster Recovery:** Leverage Azure Backup MARS Agent as part of your disaster recovery strategy. By replicating on-premises data to Azure, organizations can ensure business continuity in the event of site outages, natural disasters, or other catastrophic events. Azure provides geo-redundancy and high availability, enhancing data resilience.
4. **Branch Office Backup:** Use Azure Backup MARS Agent to centralize backup operations for branch offices or remote locations. Instead of relying on local backup infrastructure at each site, data can be securely transmitted to Azure, reducing management overhead and ensuring consistent backup policies across the organization.
5. **Compliance and Data Governance:** Employ Azure Backup MARS Agent to meet regulatory compliance requirements and data governance standards. By

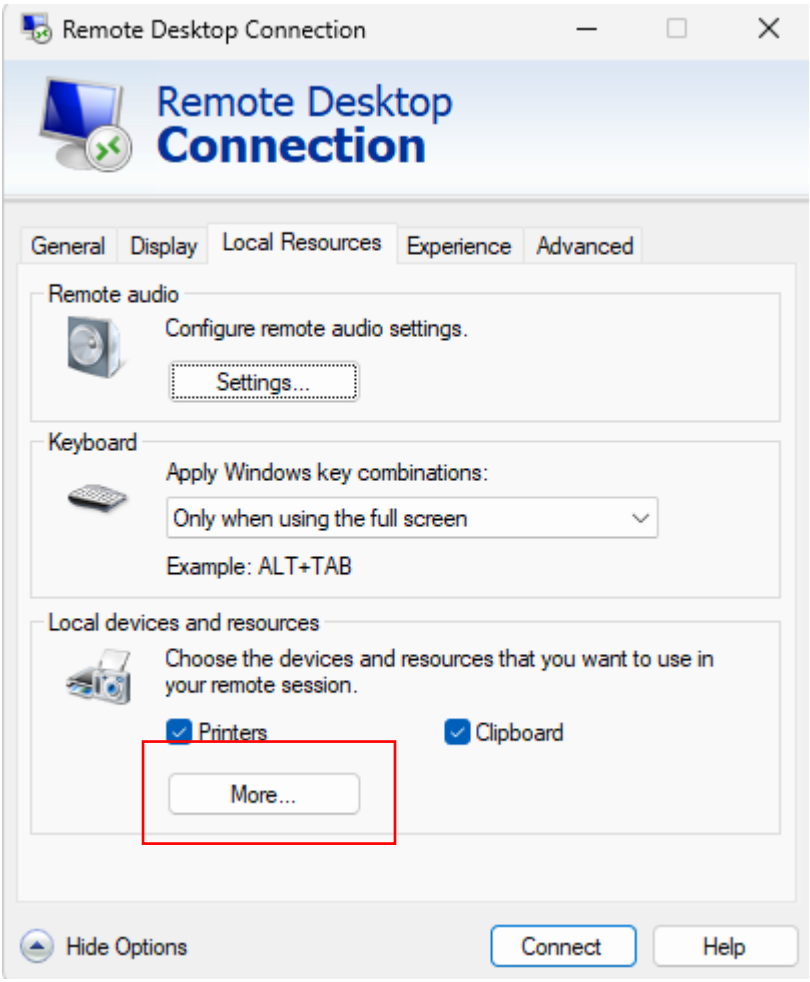
maintaining off-site backups in Azure, organizations can demonstrate adherence to data protection regulations and industry best practices, such as GDPR, HIPAA, or PCI DSS.

6. **Test and Development Environments:** Utilize Azure Backup MARS Agent to create sandbox environments for testing and development purposes. By restoring backups to isolated environments in Azure, developers can safely experiment with new applications, configurations, or updates without risking production data.
7. **Hybrid Cloud Backup:** Implement Azure Backup MARS Agent in hybrid cloud environments to seamlessly integrate on-premises and cloud-based backup solutions. This allows organizations to leverage the scalability and cost-effectiveness of Azure while maintaining control over sensitive data stored locally.
8. **Long-Term Data Retention:** Archive historical data using Azure Backup MARS Agent to meet long-term retention requirements. By storing backups in Azure, organizations can benefit from cost-effective storage options and easily retrieve data when needed for auditing, analysis, or legal purposes.

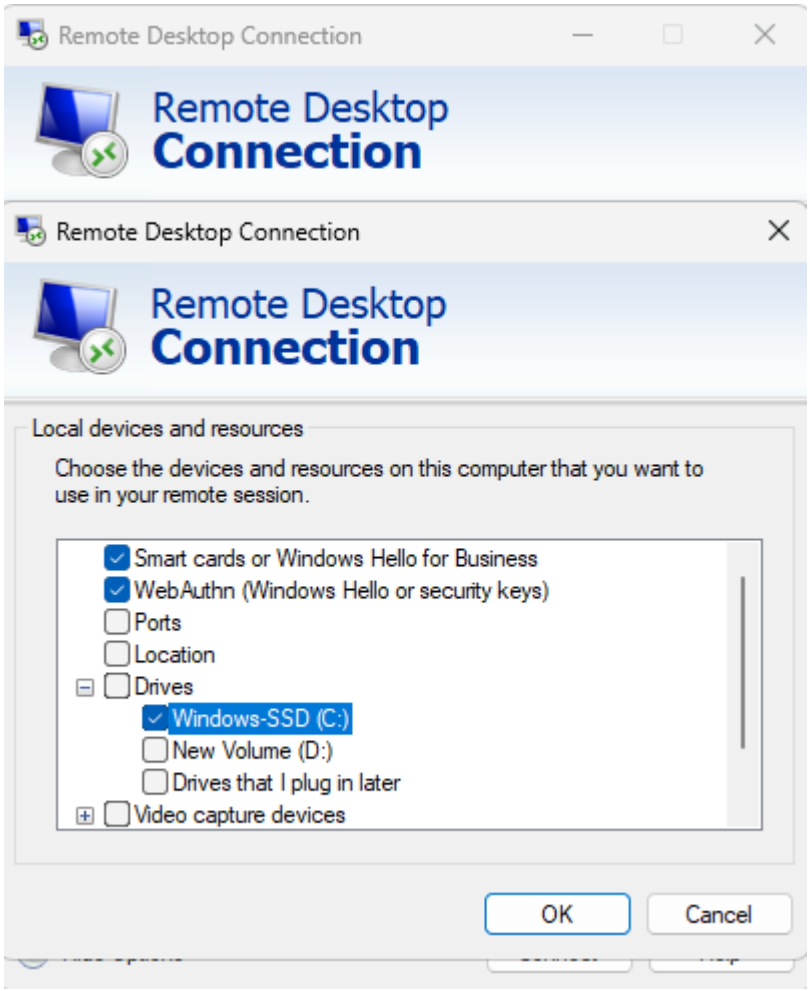
In this lab exercise, we are setting up Azure Backup MARS Agent to back up on-premises data to Azure. The end goal is to demonstrate the process of installing and configuring the MARS Agent, performing backups of files and folders, and then recovering data from these backups. This exercise helps users understand how to leverage Azure services for data protection, disaster recovery, and ensuring business continuity.

😄 To begin with the Lab:

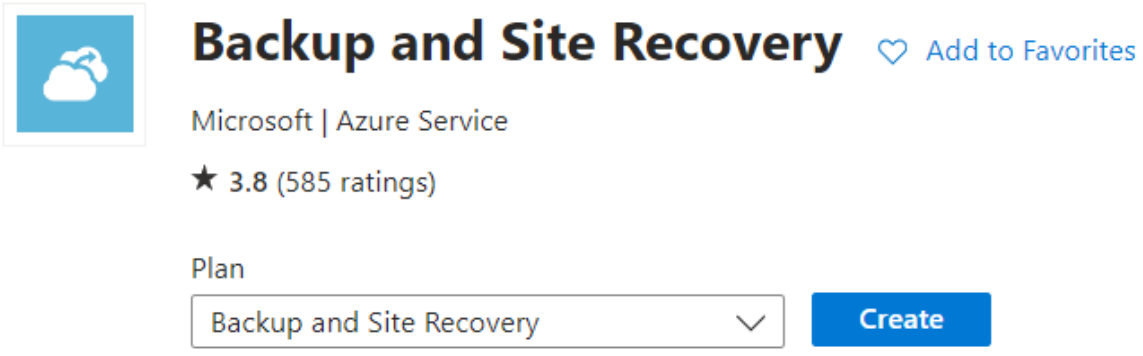
1. Now you are going to create a VM based on Windows Server 2022. After it is deployed then you need to download the RDP file.
2. Then you need to go to the file location on your laptop and right click on the file and click on the Edit button. Then you need to go to local resources and for local devices and resources click on more.



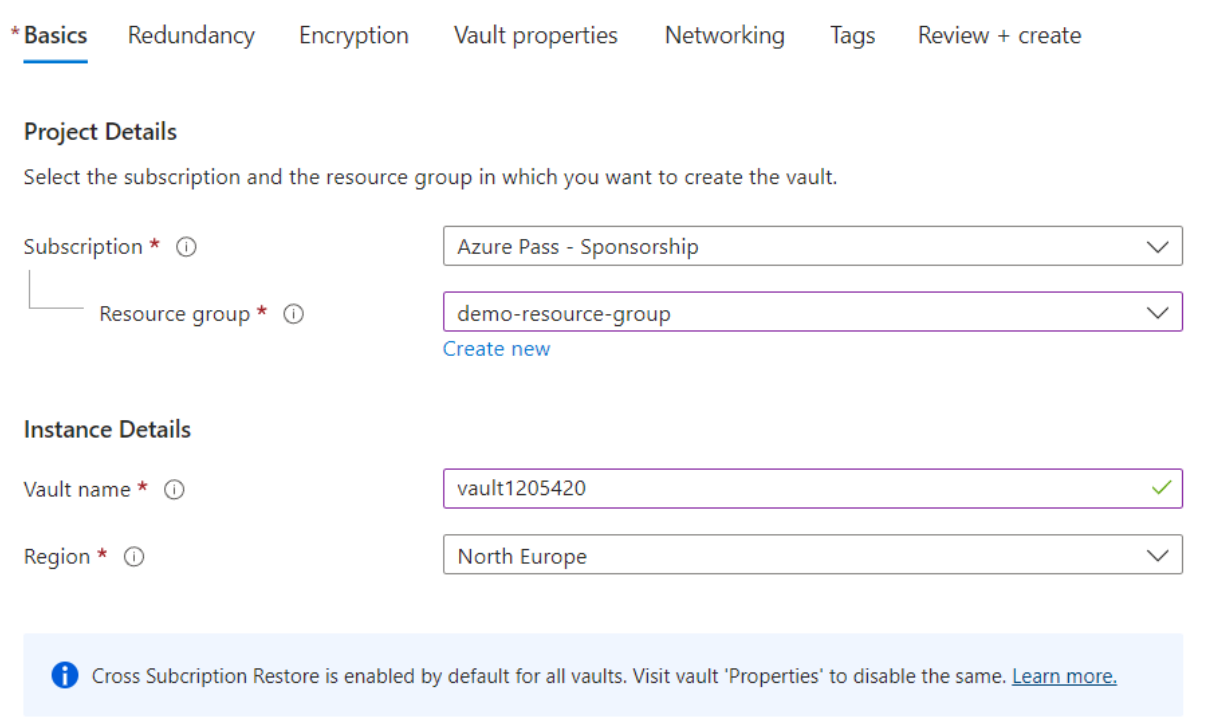
3. Now you need to expand the drive options and choose the C drive or D drive. It means that you enable your VM to establish a local connection between your laptop.
4. After that click on OK and then connect with your VM.



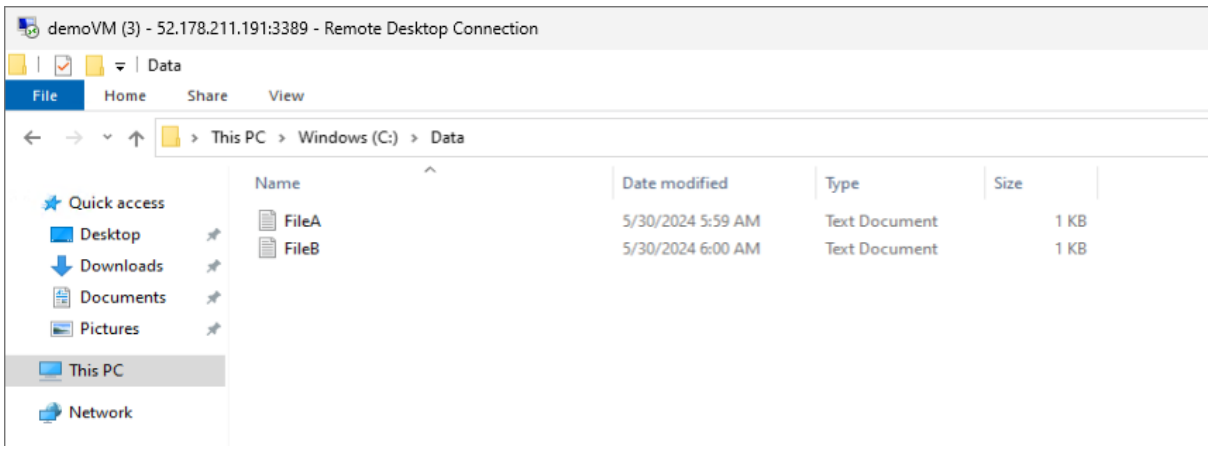
5. Now while it is connecting go back to Portal and create a back and site recovery. This will create a vault for us, for that go to marketplace and search it then choose this service accordingly.



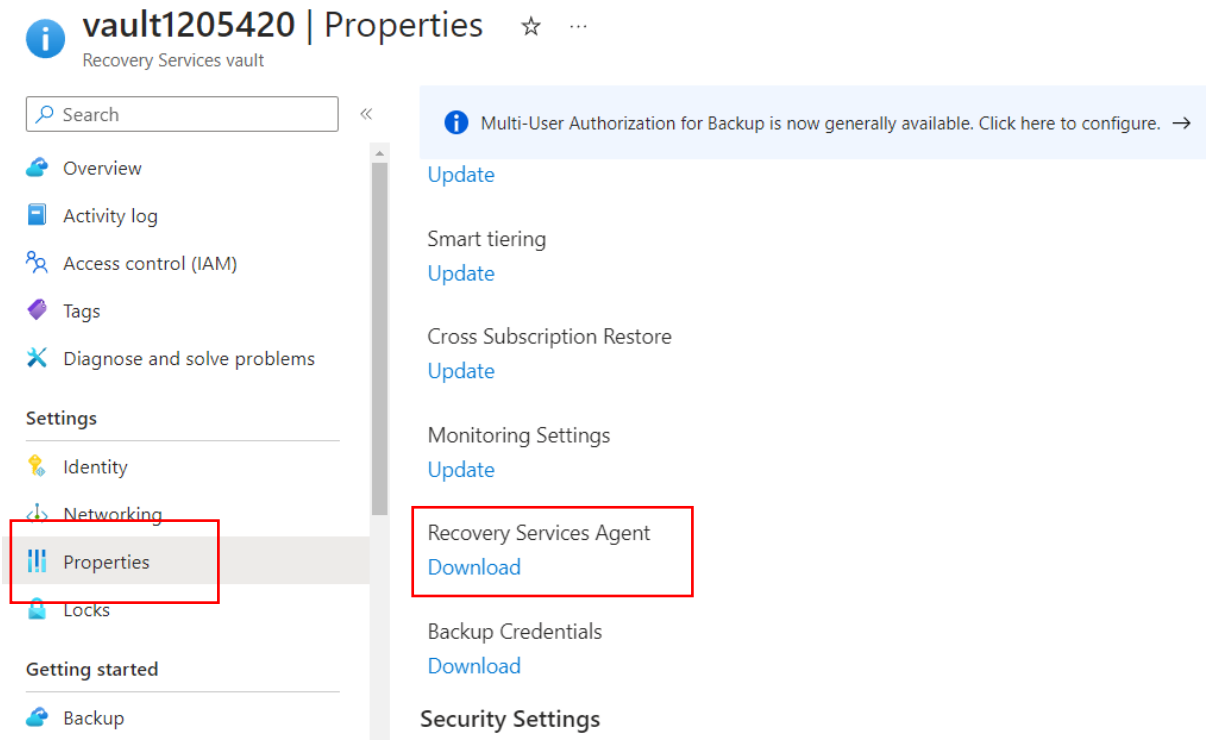
6. First choose your resource group and then give it a unique name.



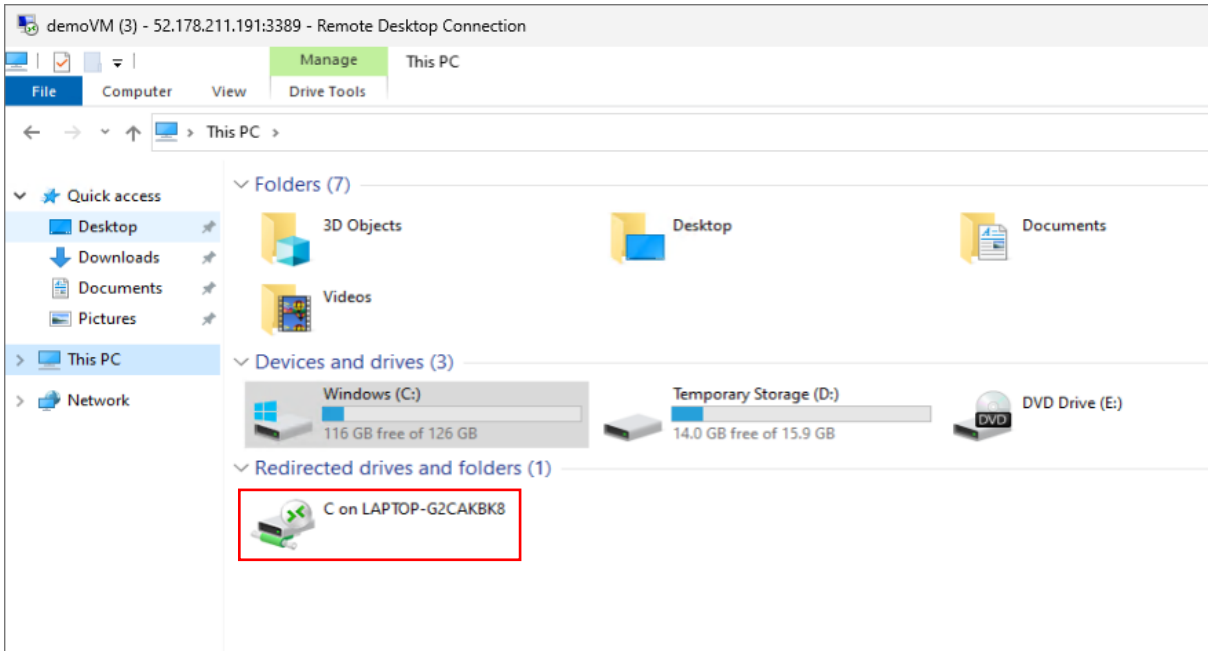
7. Then, for redundancy, choose LRS, move to the review page, and create your vault.
8. Now you need to go to your VM in your C drive to create a new folder, open up the Notepad, create two files, write something in those files, and save them onto that folder.



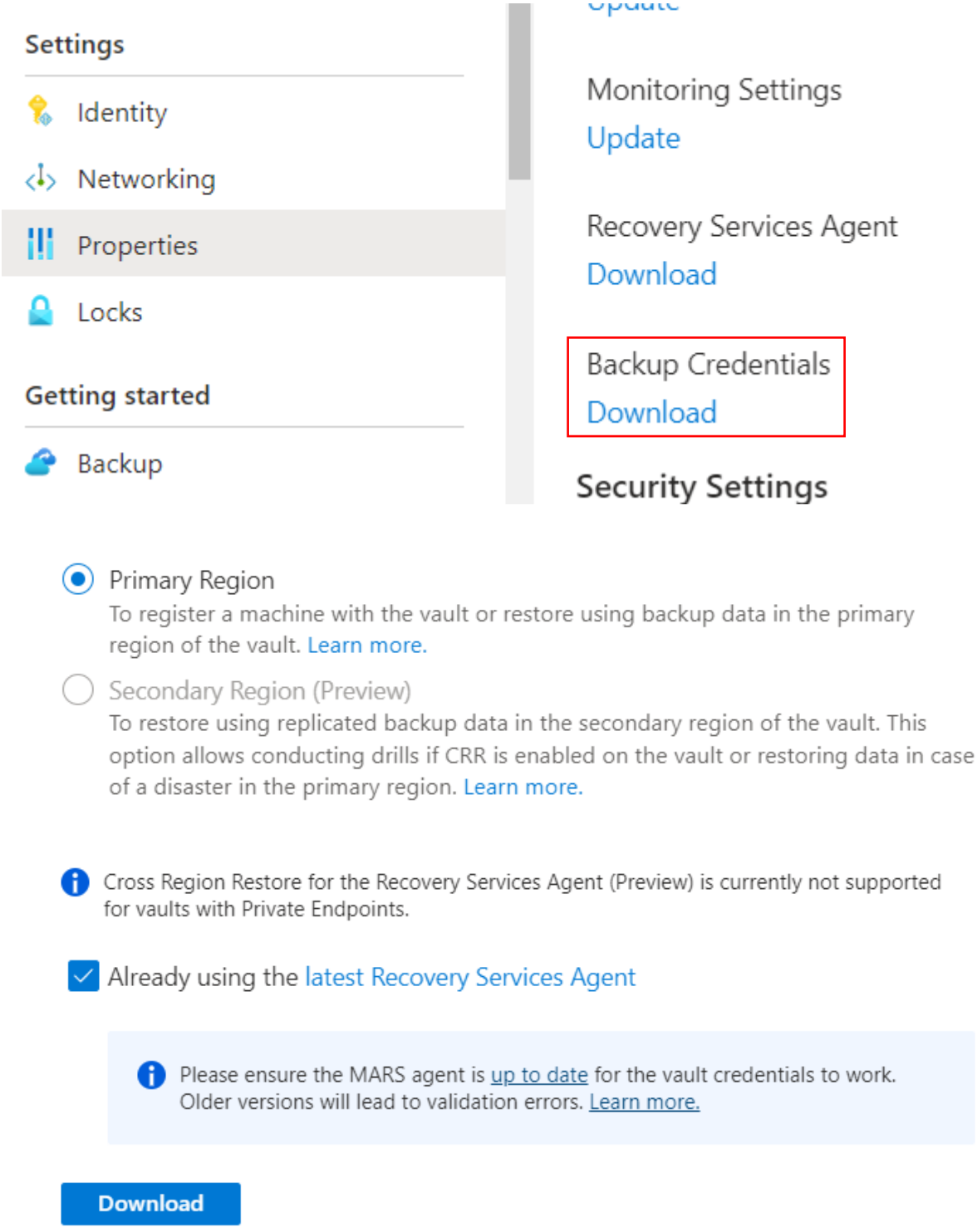
9. Then come back to Portal, open your vault, and navigate to properties here you will see that we can download the recovery services agent. Click on it to download the file.



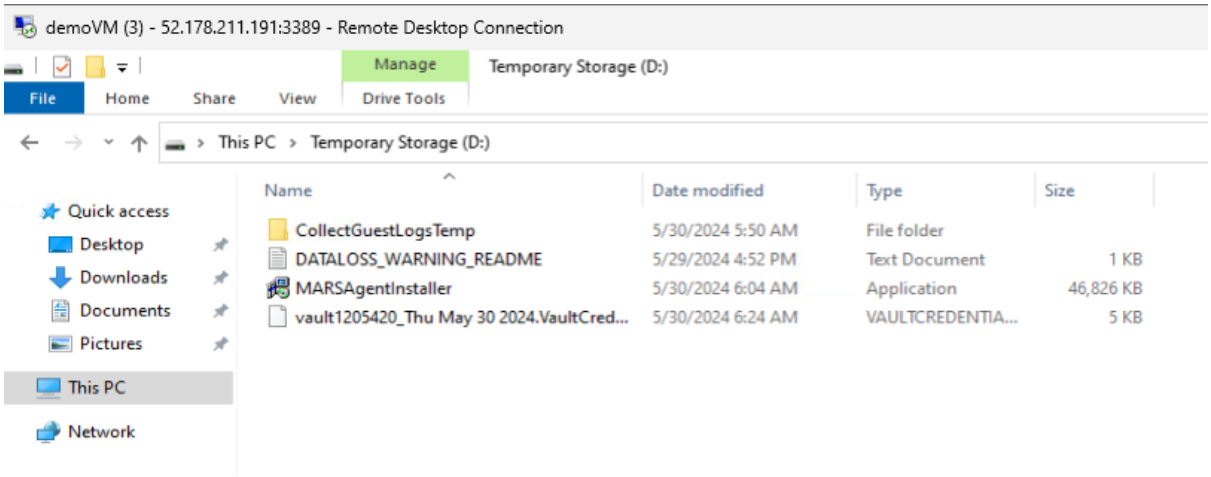
10. After that come back to your VM and go to File Explorer in it, here you will see that you have the connection to access the C drive of your laptop, from here you can copy the agent file and paste it onto your VM.
11. So, open your C drive and go to the folder where you have downloaded the file.



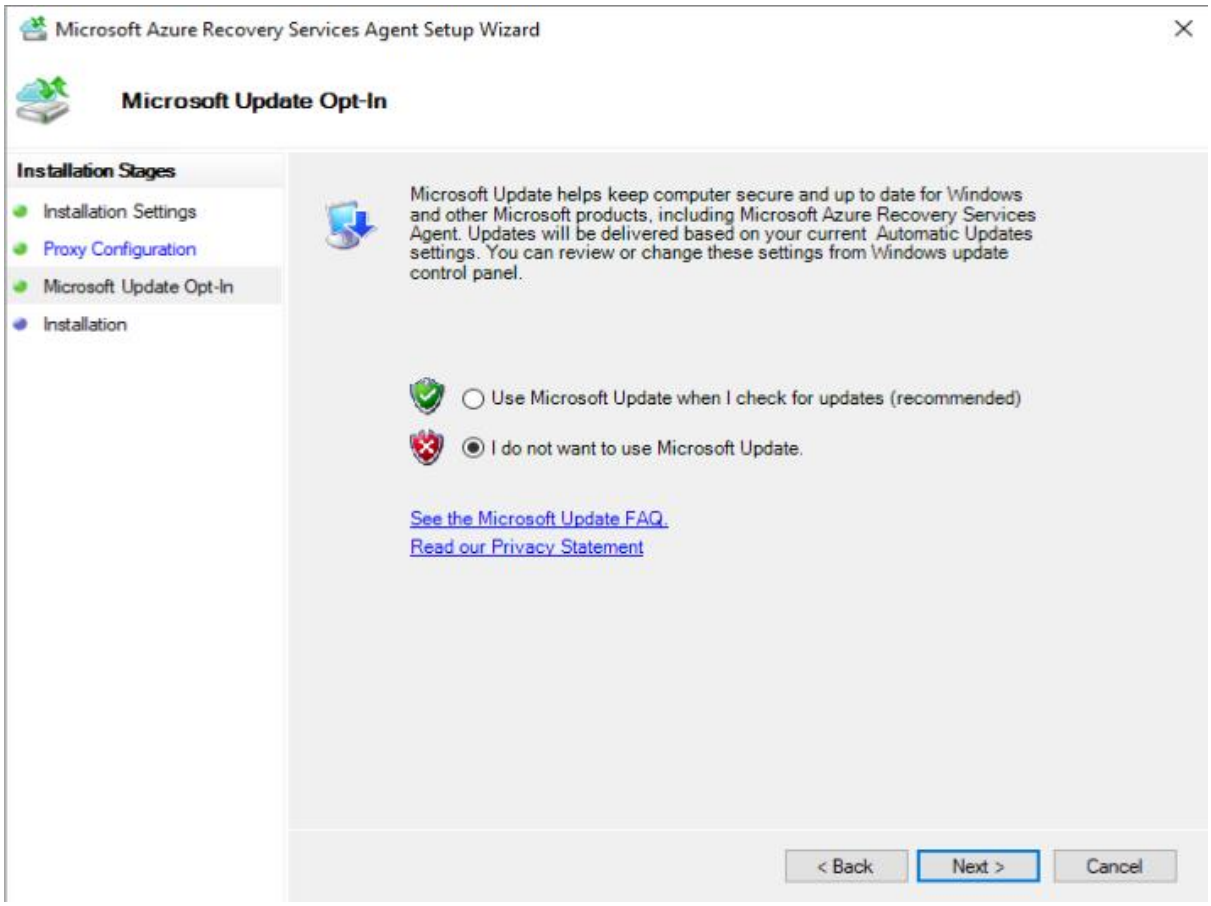
12. Copy the file and paste it into the D drive. After that come back to Portal and go to your Vault.
13. From where you downloaded the recovery agent, just below you will see backup credentials now you need to download it.

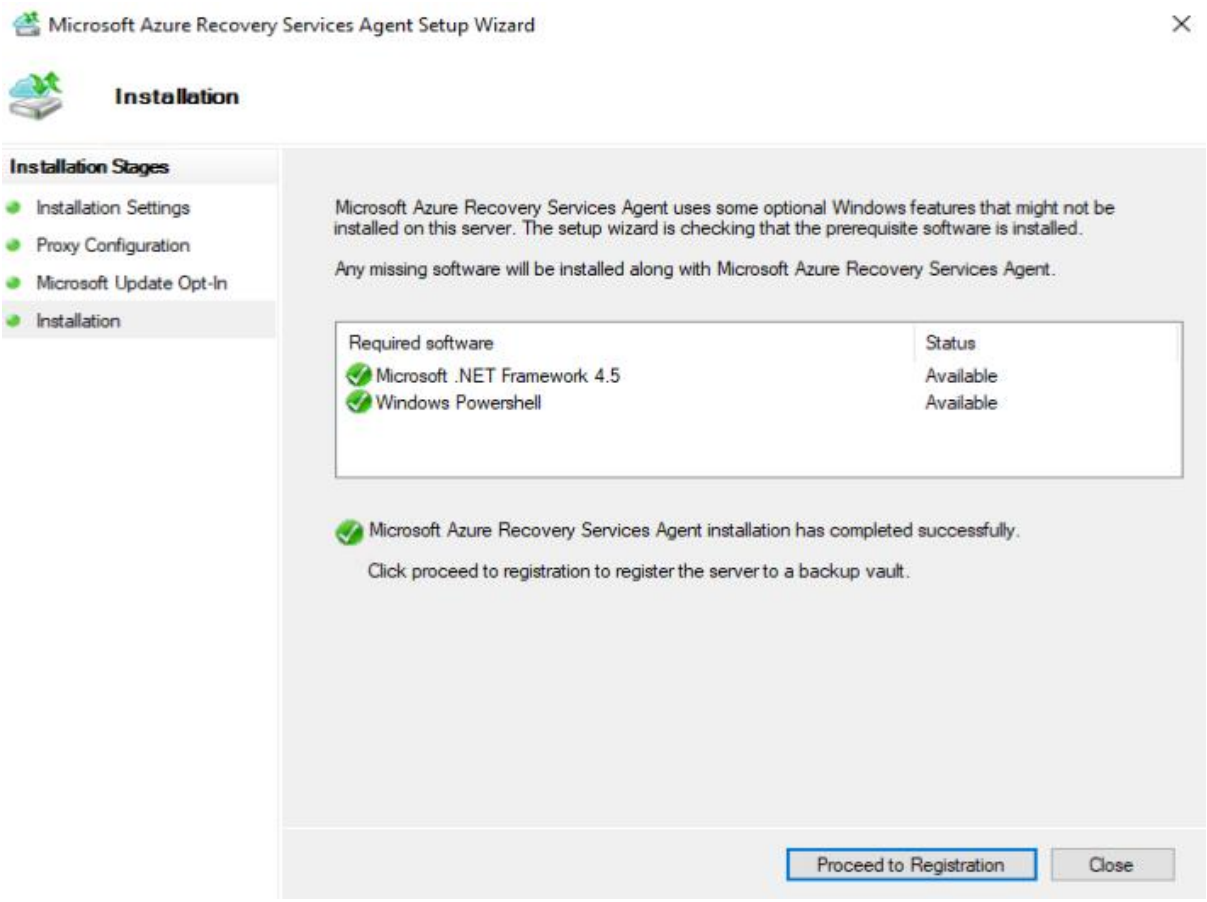


14. Then again go back to the VM and copy the credentials file and paste it onto the D drive. Below you can both of the files in D drive. Now we are going to install the MARS agent.

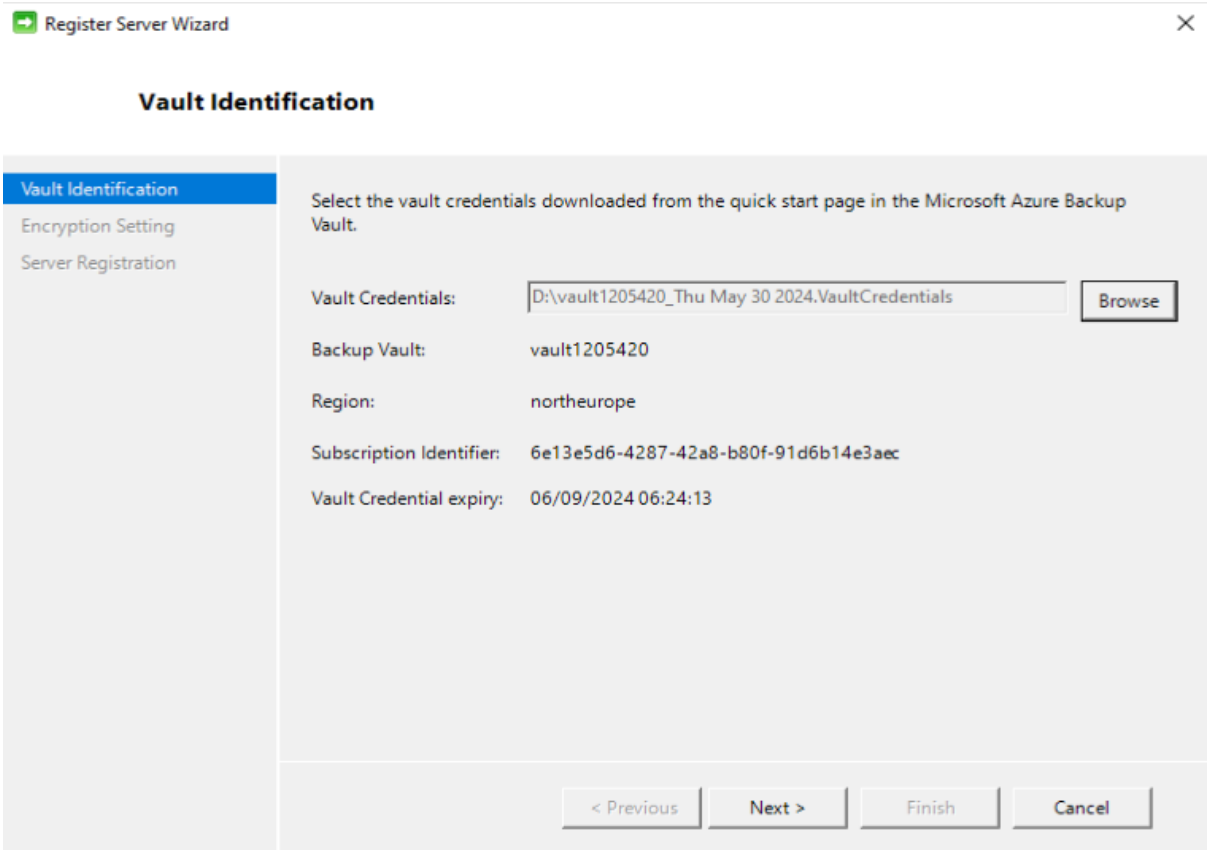


15. While installing it follow the steps shown below in the snapshot.

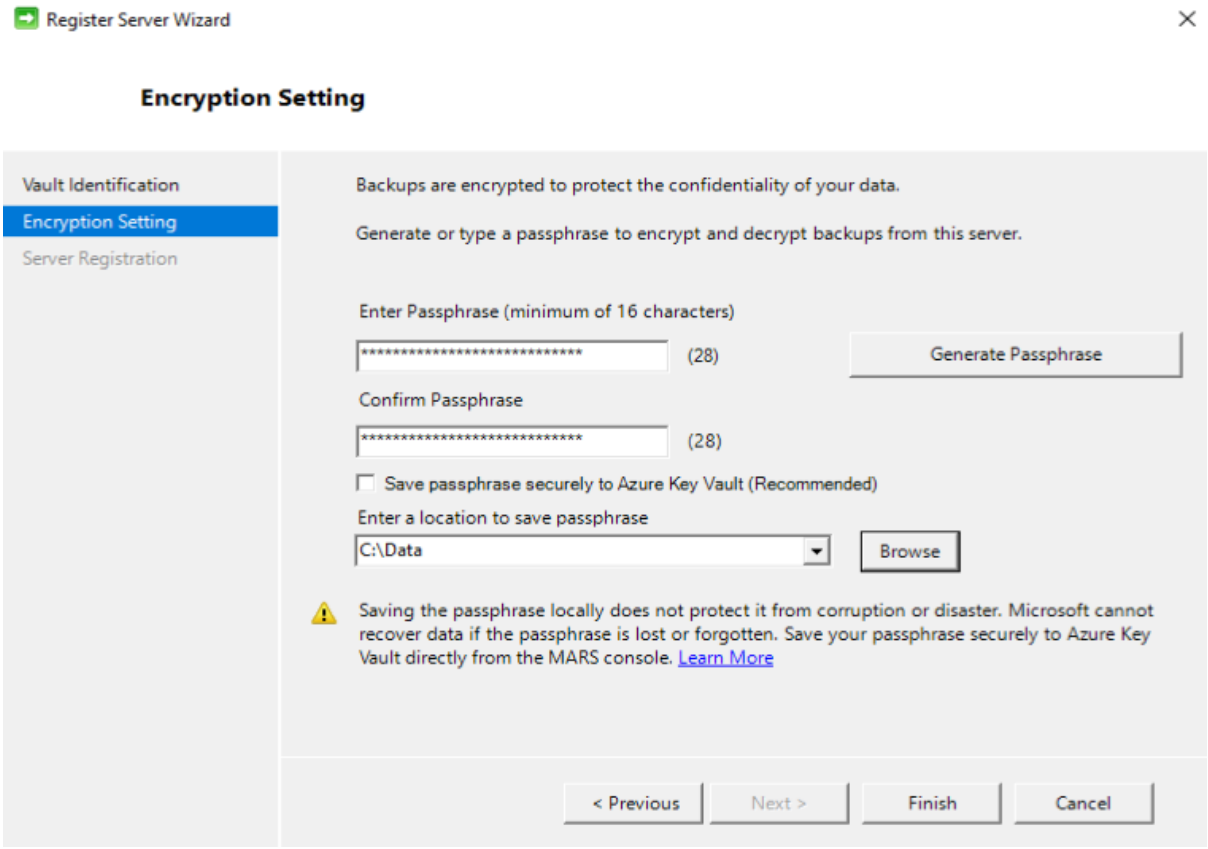


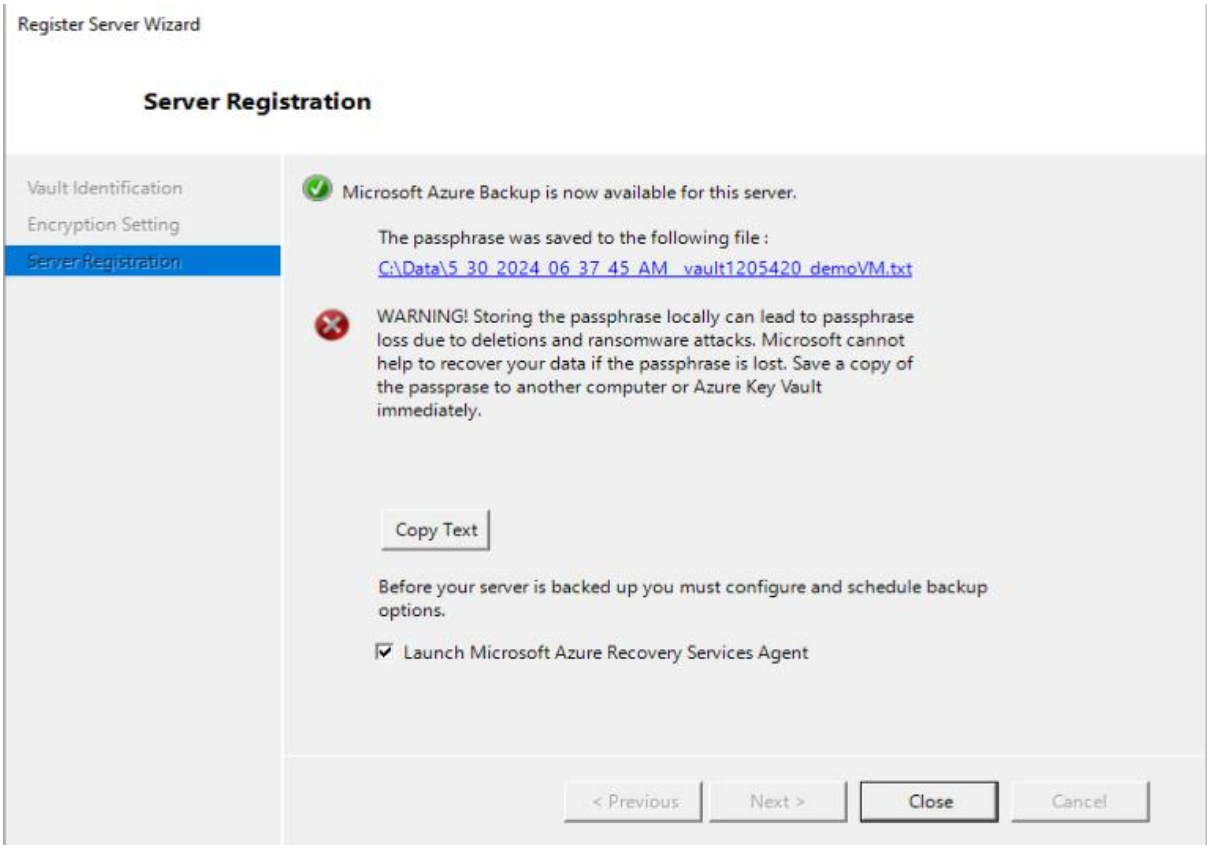


16. Here you need to give the location of the credentials file.

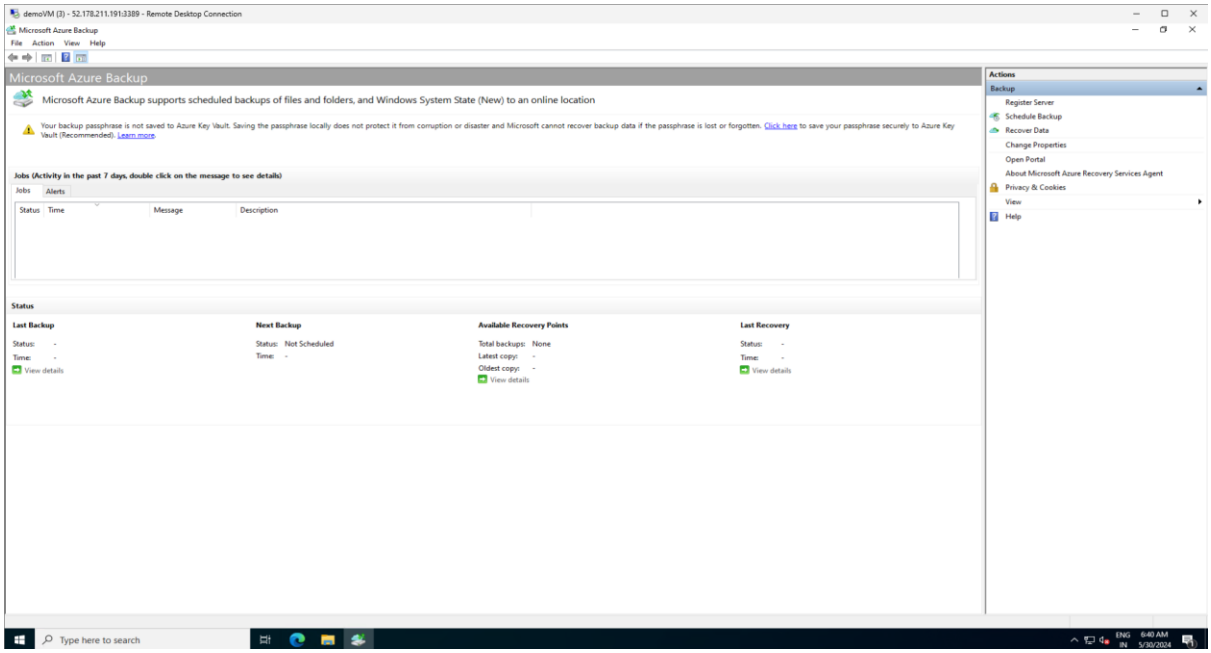


17. Then you need to enter a paraphrase and save at any location inside your VM or you can generate paraphrase and save it on the azure key vault.

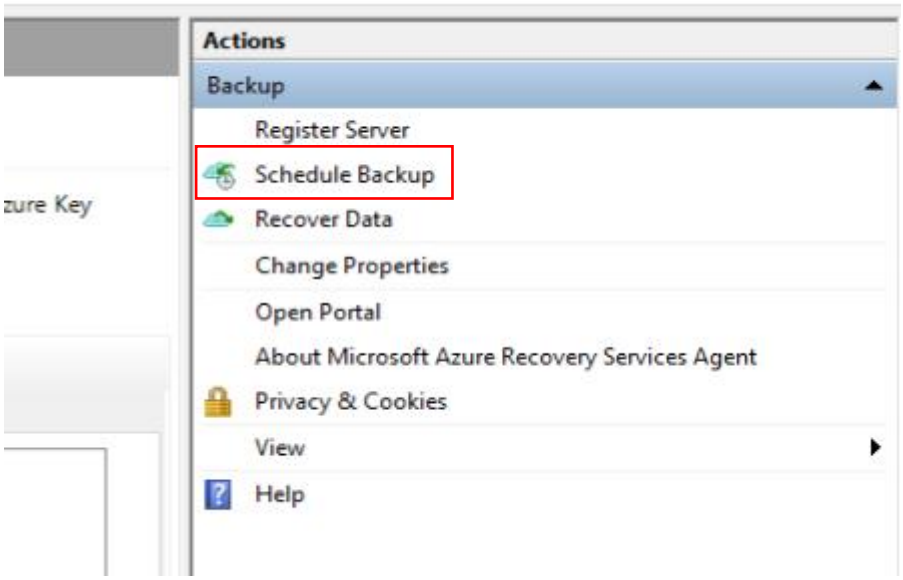




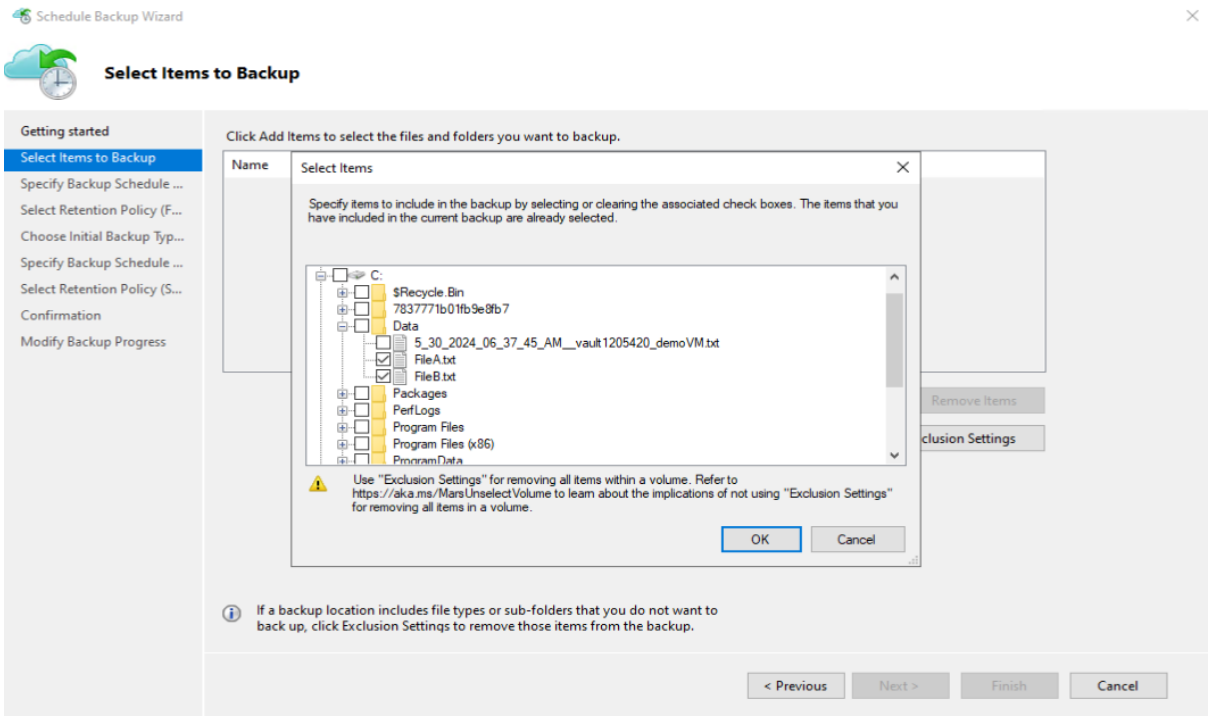
18. Below you can see the agent is ready.

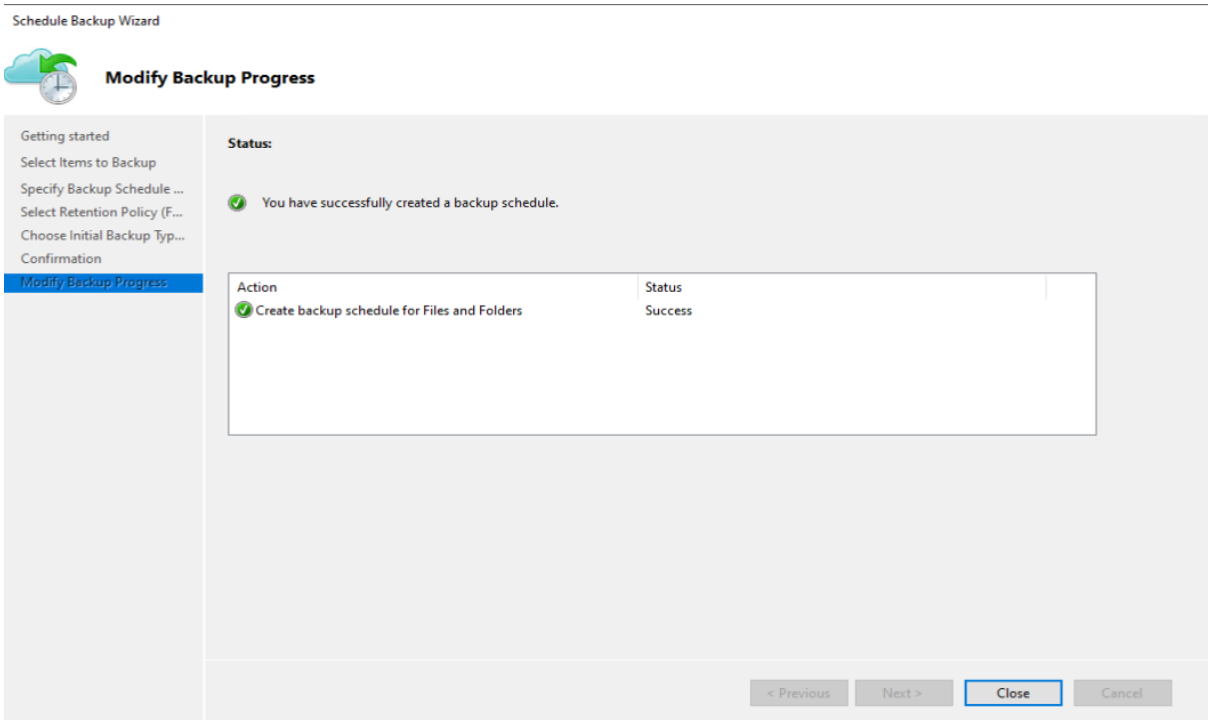


19. Now you need to click on schedule backup.

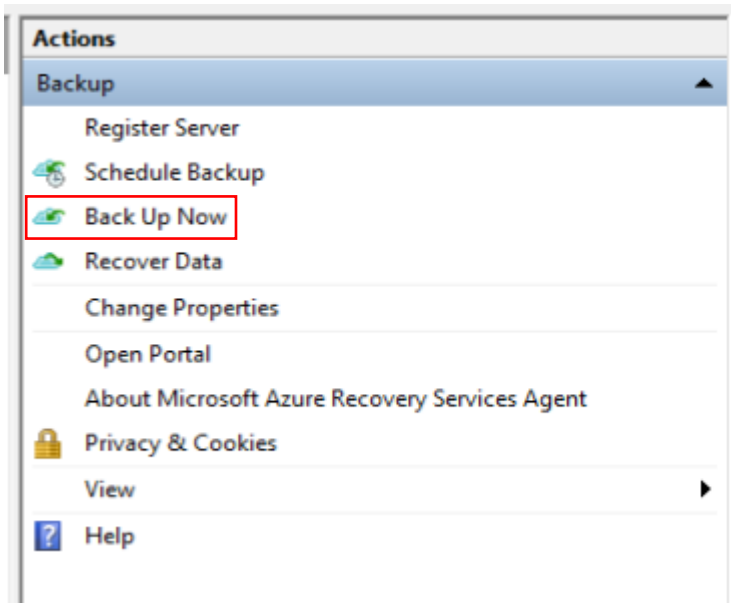


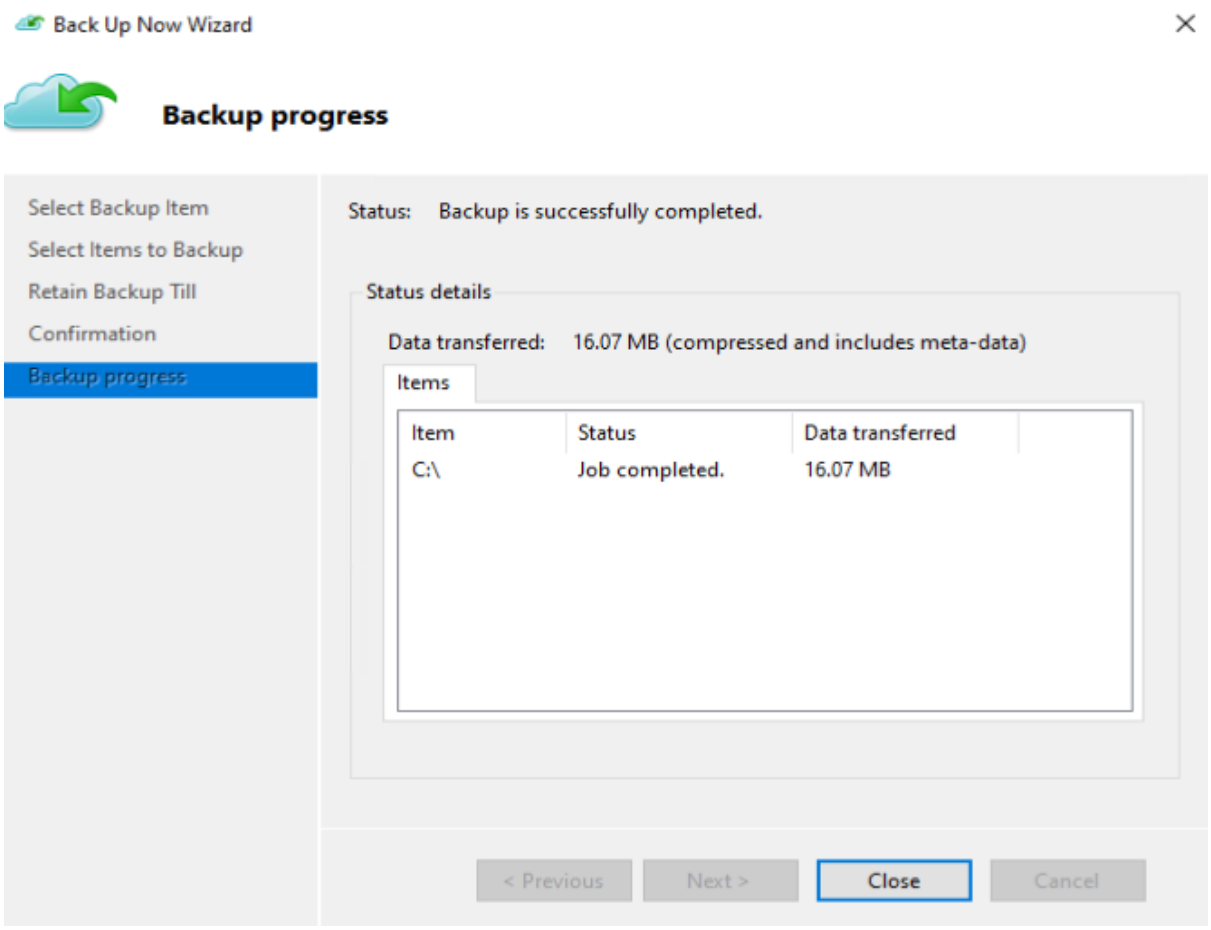
20. Then you need to add File A and B from your C drive. After that keep everything to default and create it.



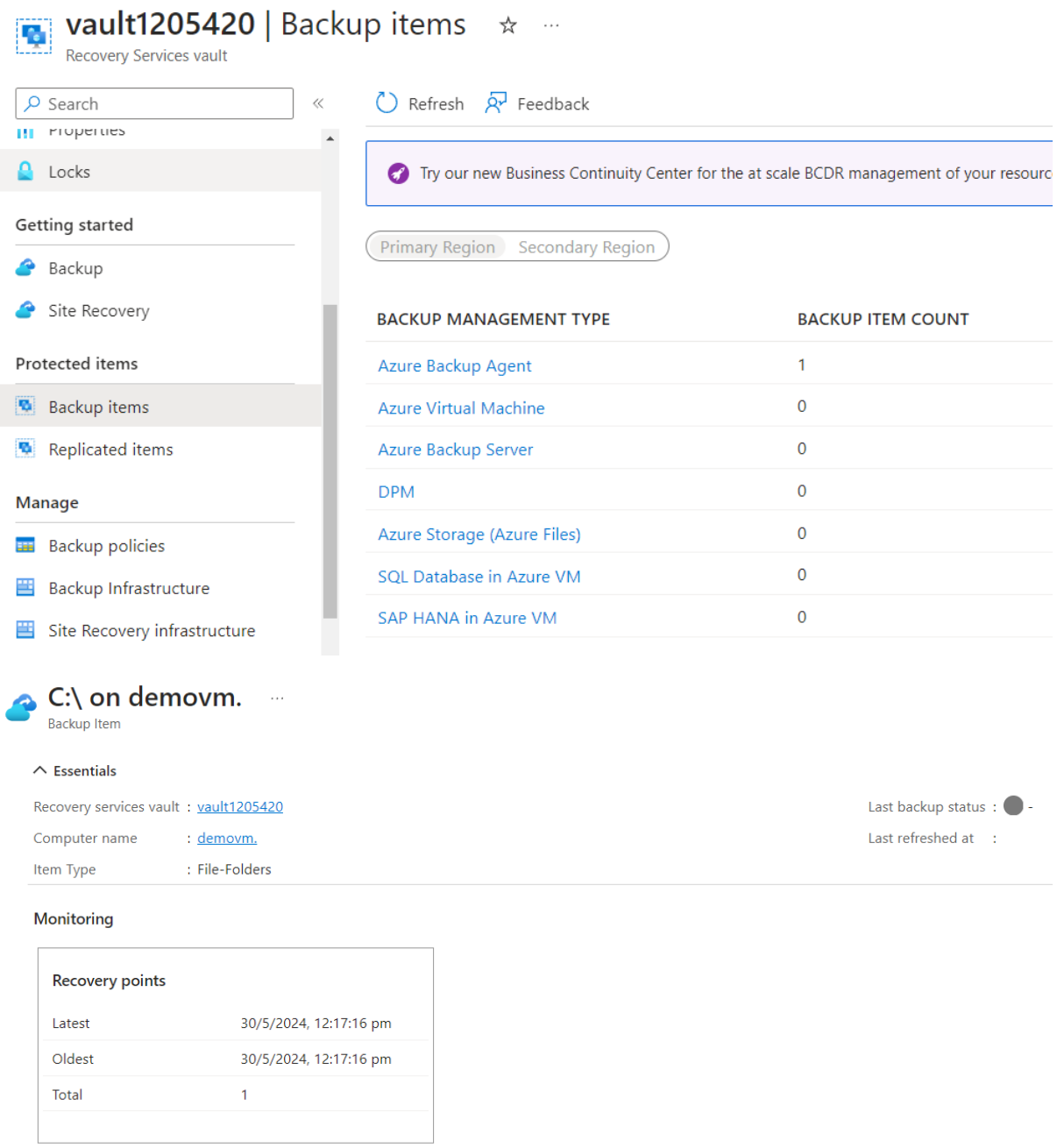


21. Now we are going to click on backup. Just keep everything to default and create a backup.

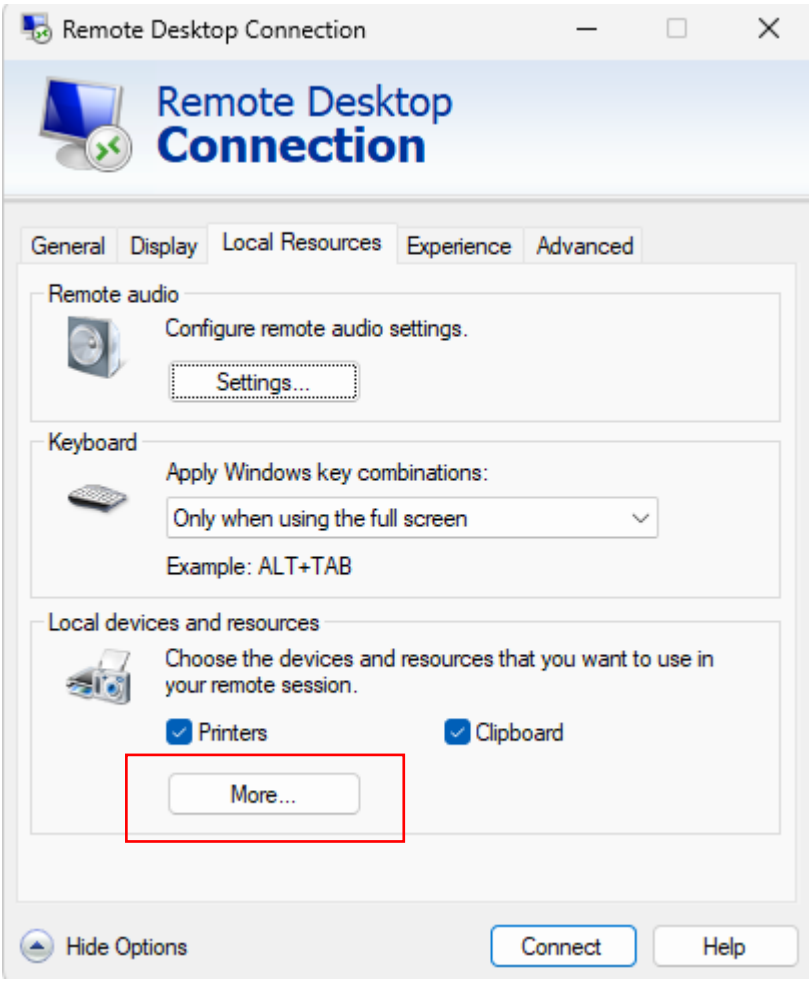


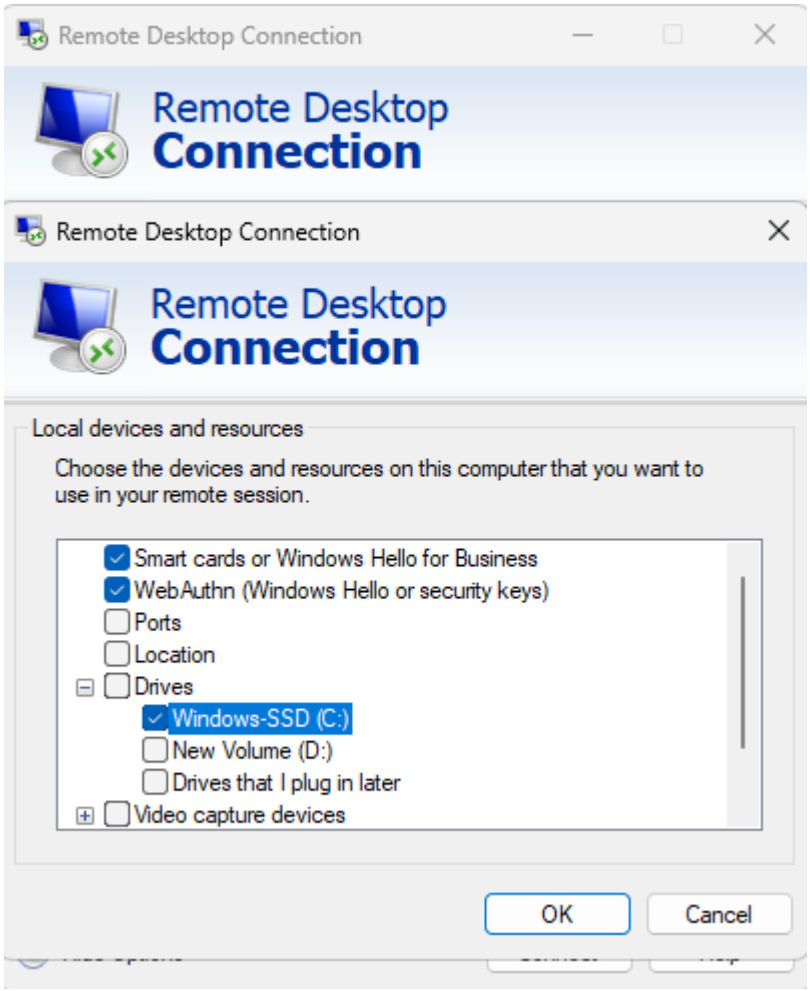


22. Once the backup is complete then you need to go to vault service and go to backup items and open the azure backup agent. Then inside click on view details and you will see the details of your backup items.

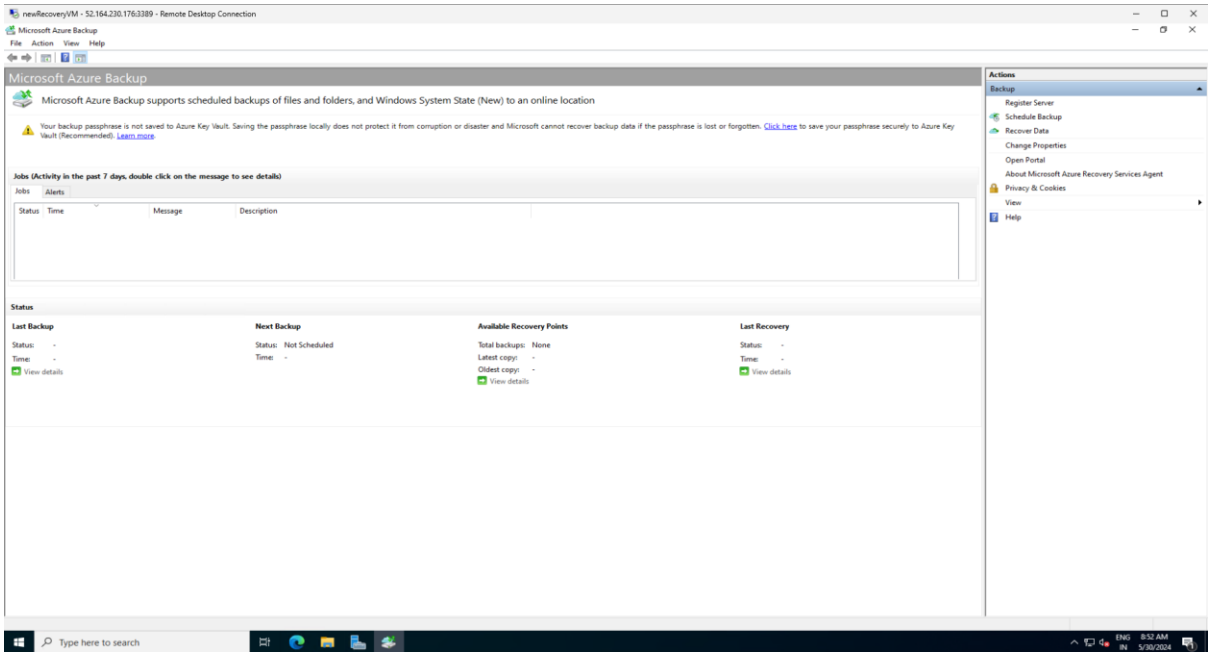


23. Now we are going to stop our VM. So, we can create a scenario where we can't get our files from our VM.
24. So, now we are going to create a new VM based on Windows Server 2022 and it should be in the same network as our last VM.
25. Now in this VM again we are going to install the MARS agent for that once your VM is deployed then you need to download the RDP file and, in your laptop, right click on the RDP file choose more from local devices and resources. Then again choose any of disk then just login to your VM.

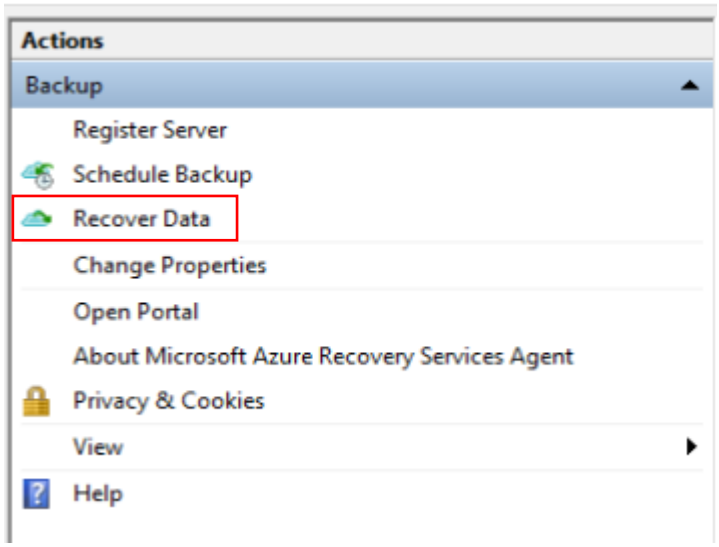

Remote Desktop Connection
Remote Desktop
Connection
General
Display
Local Resources
Experience
Advanced
Remote audio
Configure remote audio settings.
Settings...
Keyboard
Apply Windows key combinations:
Only when using the full screen
Example: ALT+TAB
Local devices and resources
Choose the devices and resources that you want to use in your remote session.
Printers
Clipboard
More...
Hide Options
Connect
Help



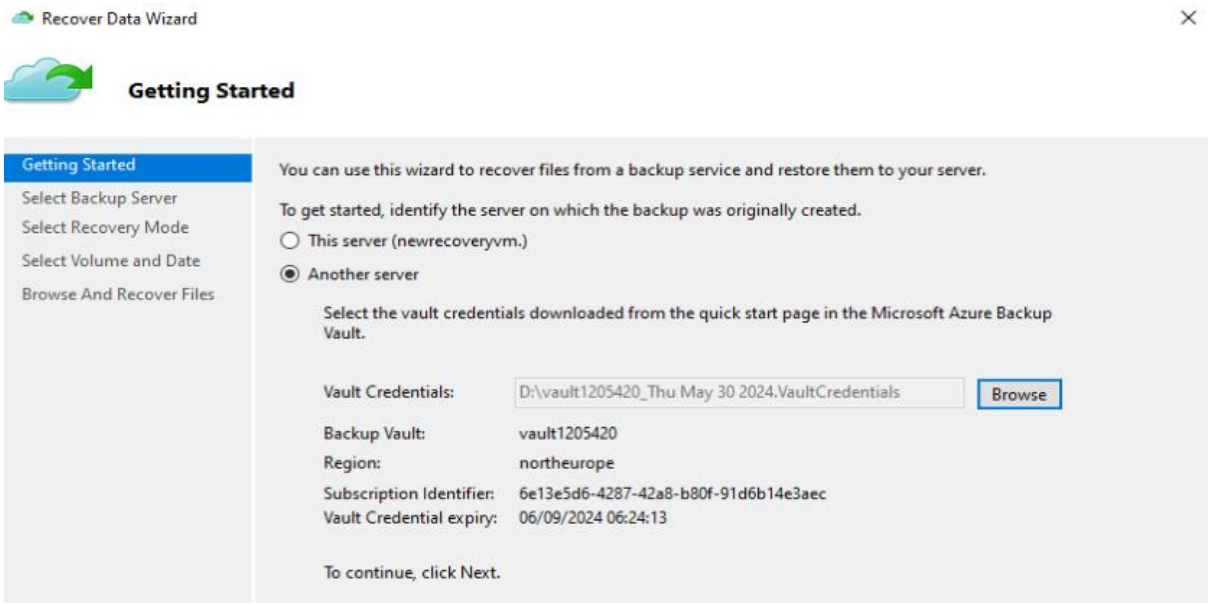
26. Then again you need to copy the MARS recovery agent and the credentials file and paste it in the D drive of your VM. Then install the agent like you did before.
27. Also, in this new VM we don't have any files in place, we will recover the data from our previous VM.
28. Once the files are pasted successfully into your D drive now you need to install the agent. The installation process is the same.
29. Below you can see that the agent is installed successfully.



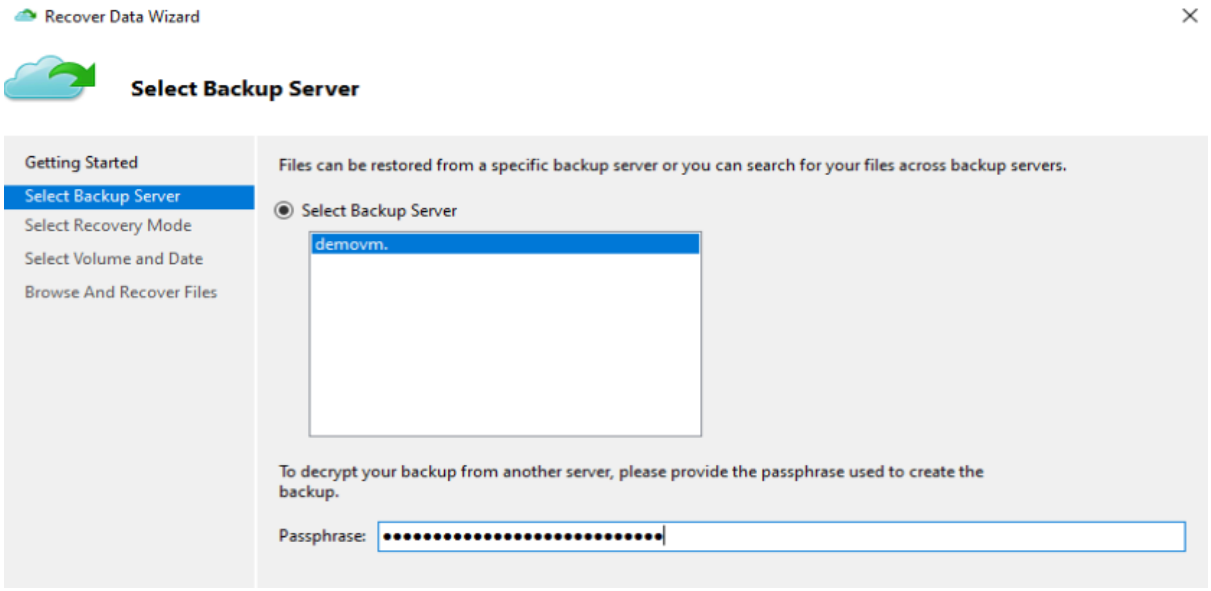
30. Now you need to click on the option to recover data.



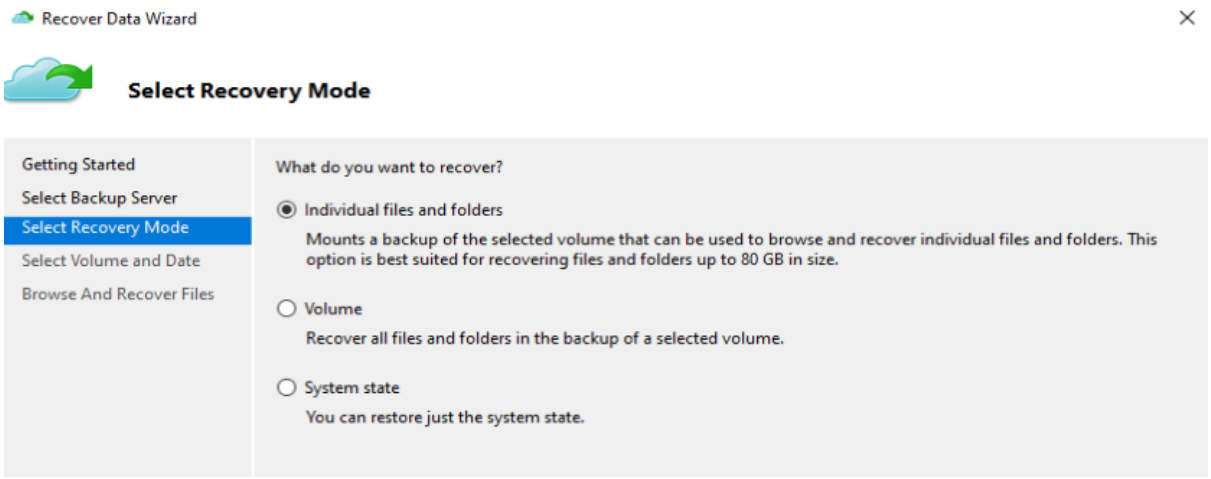
31. Then you need to choose another server and then browse for the vault credentials and click on next.



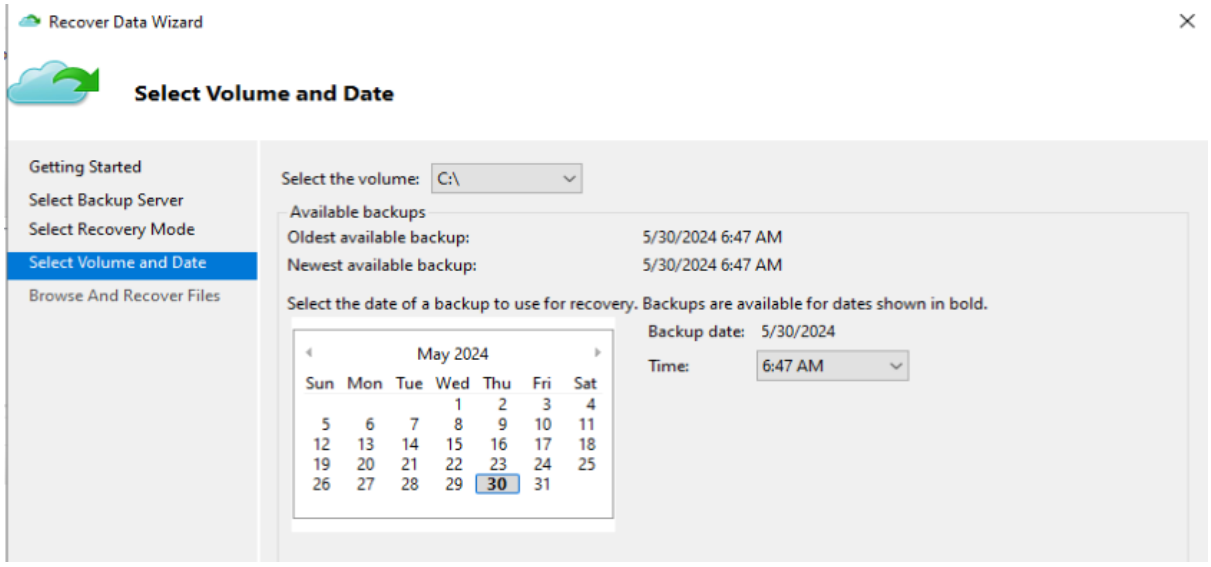
32. Now you'll see that you can choose your Demo VM and then you need to write the Paraphrase and click on next.



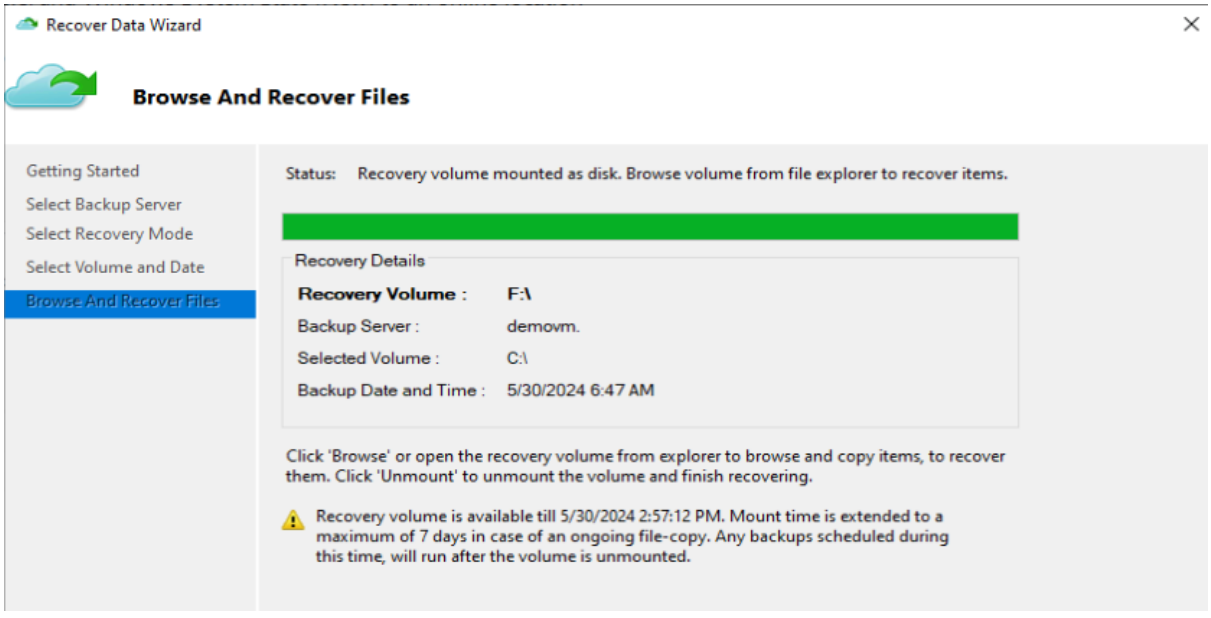
33. And choose individual files and folders, click on next.



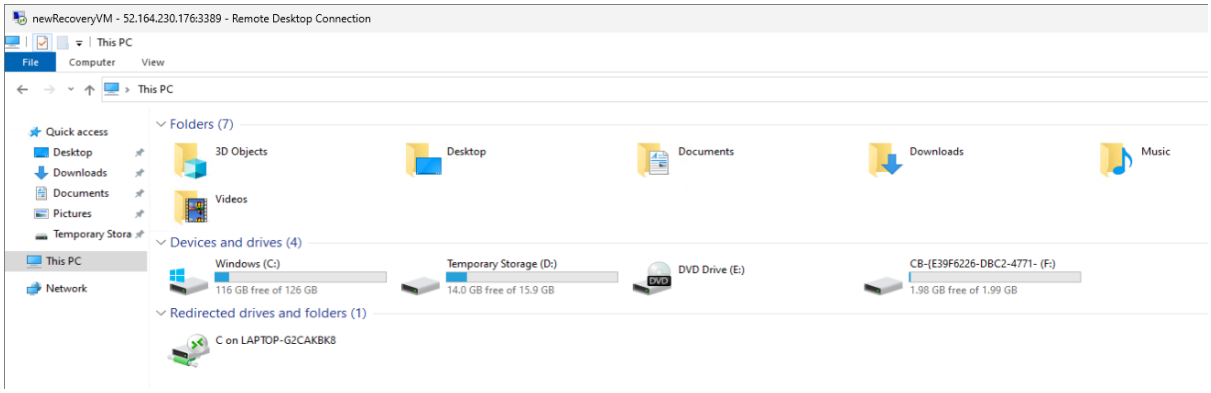
34. Then you have choose your volume which is C drive and it will give you the backup, then you need to click on mount.



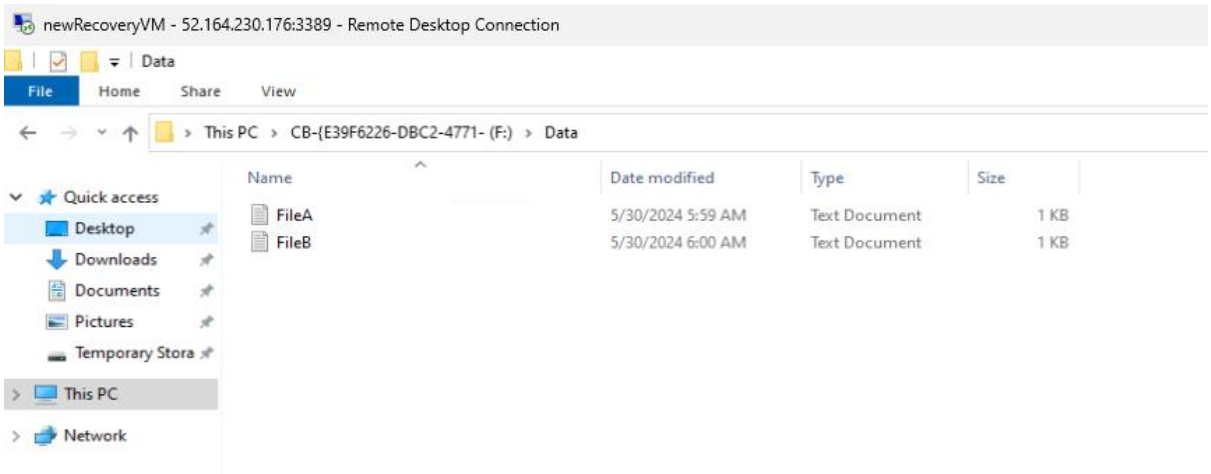
35. Below you can see that it created a new volume with the name of F drive.



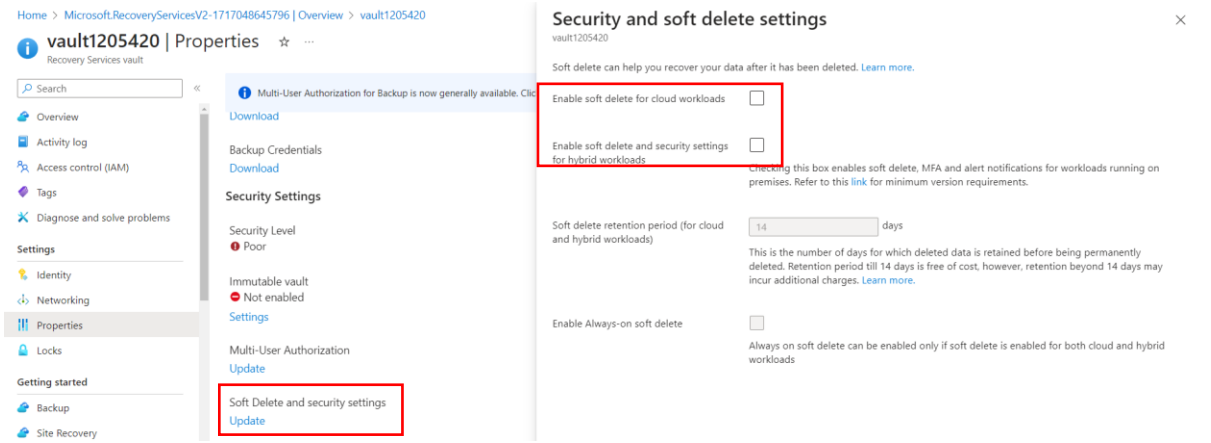
36. Now if you go to the file explorer in your VM. Here you can see the F drive.



37. And if you go inside of it, you will see your files in place.

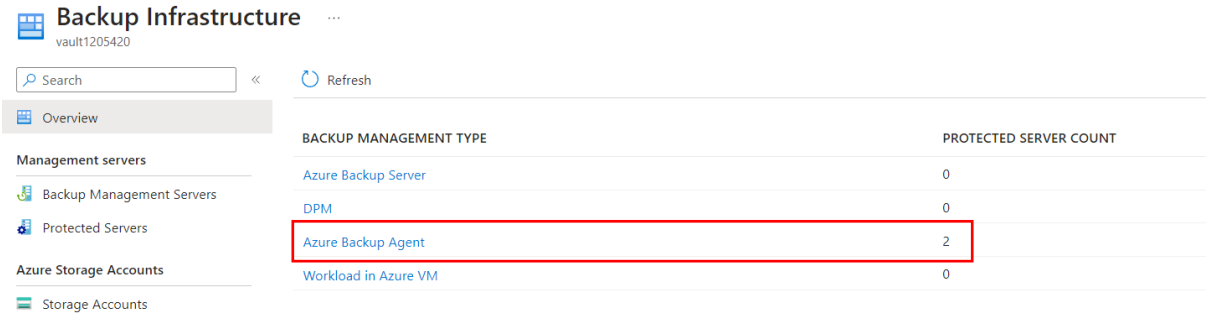


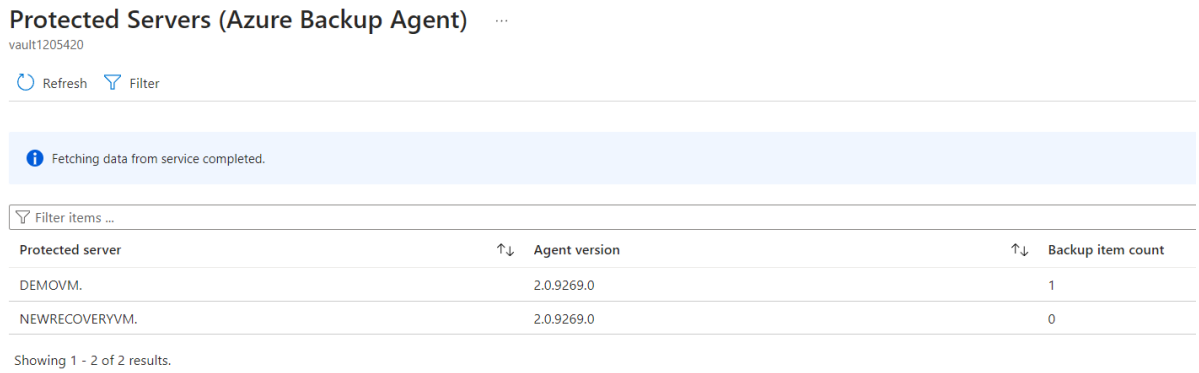
38. Once you are done just unmount the F drive.
39. Now we are going to delete of the resources but before that let us delete our recovery vault.
40. For that go to Portal and open the vault. Then go to properties and open soft delete and security settings then you need to uncheck both of the options that are highlighted.



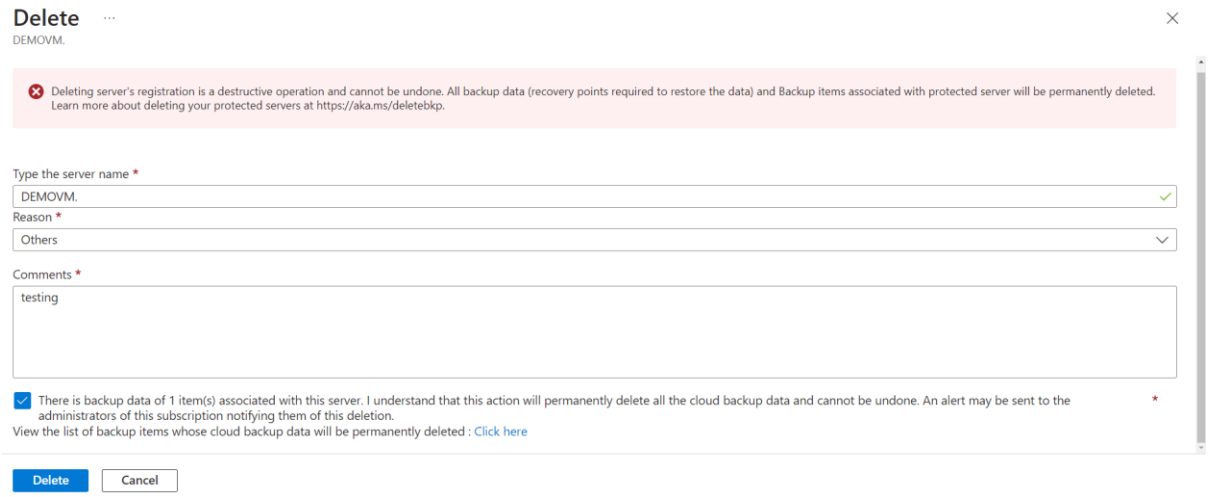
41. Then you need to go to the backup infrastructure from the left pane and you need to delete the azure backup agent.

42. Now to delete them you need to open them one by one and then delete them.





43. Below you can see that we have one server by writing its name and in reason choose others then in comments write testing.



44. Once these both server are deleted then go to the overview of vault service and delete it.
45. After that delete the other resources.