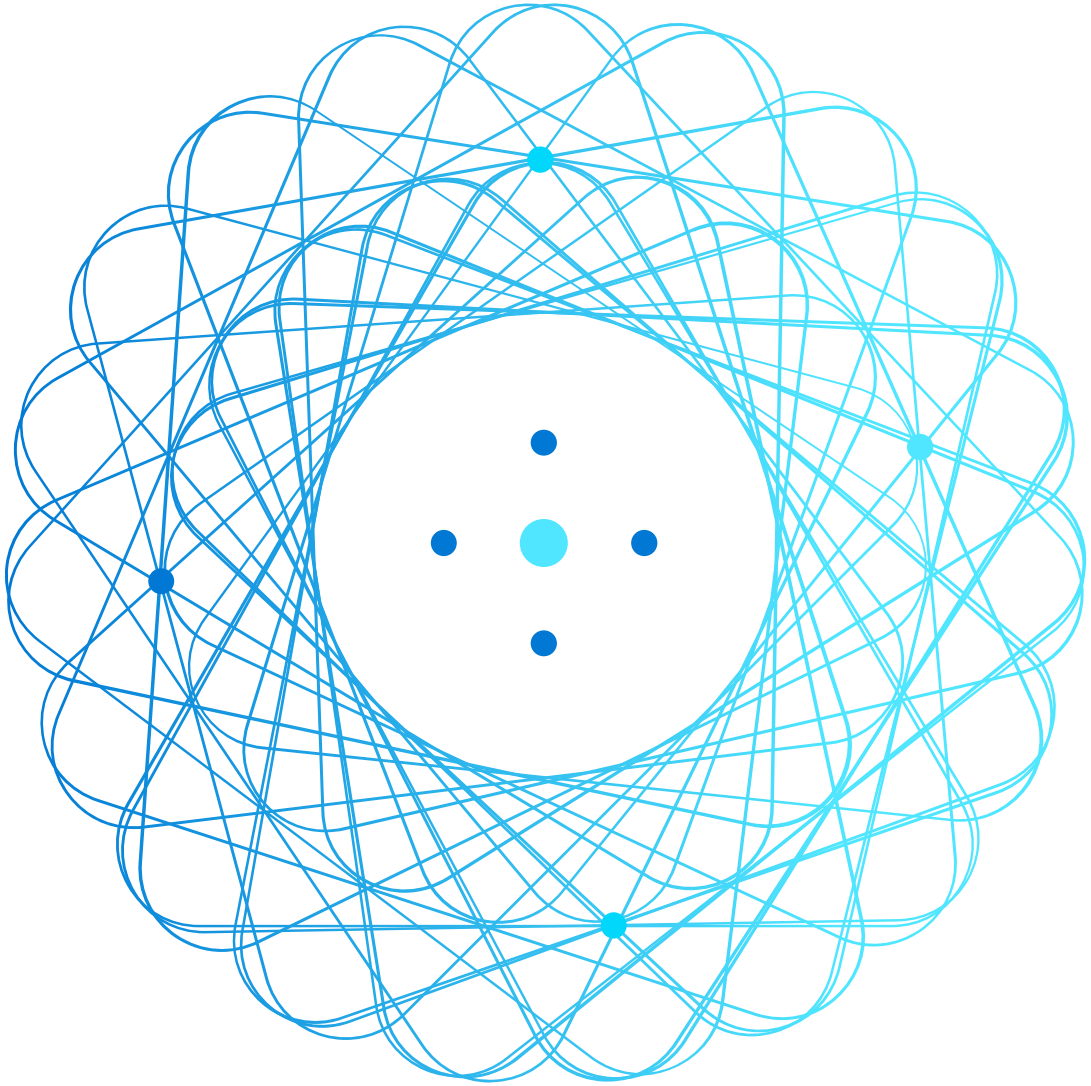
Microsoft Azure

AZ-140

Configuring and Operating Azure Virtual Desktop



AZ-140 Agenda

Learning Path 1

1. Azure Virtual Desktop Architecture
2. Design the Azure Virtual Desktop architecture
3. Design for user identities and profiles

Learning Path 2

4. Implement and manage networking for AVD
5. Implement and manage storage for AVD
6. Create and configure host pools and session hosts for AVD
7. Create and manage session host image for AVD

Learning Path 3

8. Manage access for AVD
9. Manage security for AVD

Learning Path 4

10. Implement and manage FSLogix
11. Configure user experience settings
12. Install and configure apps on a session host

Learning Path 5

13. Plan for disaster recovery
14. Automate Azure Virtual Desktop management tasks
15. Monitor and manage performance and health

Implement and manage storage for Azure Virtual Desktop

Introduction

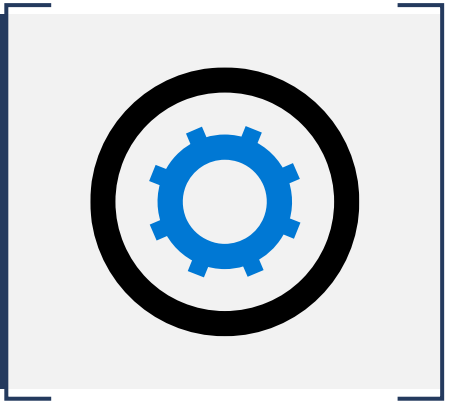
- Storage for FSLogix components
- Configure storage for FSLogix components
- Configure storage accounts
- Configure disks
- Create file shares

AZ-140: Implement an Azure Virtual Desktop infrastructure (25-30%)

Implement and manage networking for Azure Virtual Desktop

- Conceptual knowledge of Azure compute solutions.
- Working experience with virtual machines, virtual networks, and app service.

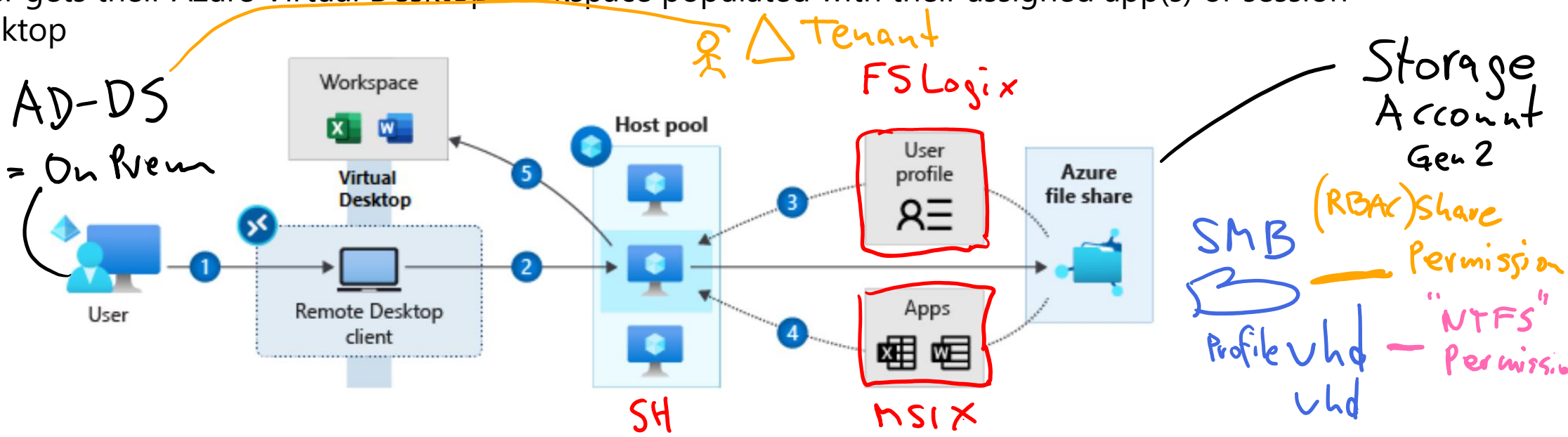
Storage for FSLogix components



Azure AD-DS Kerberos Nachbau

The process of accessing a user profile after signing into a RD client

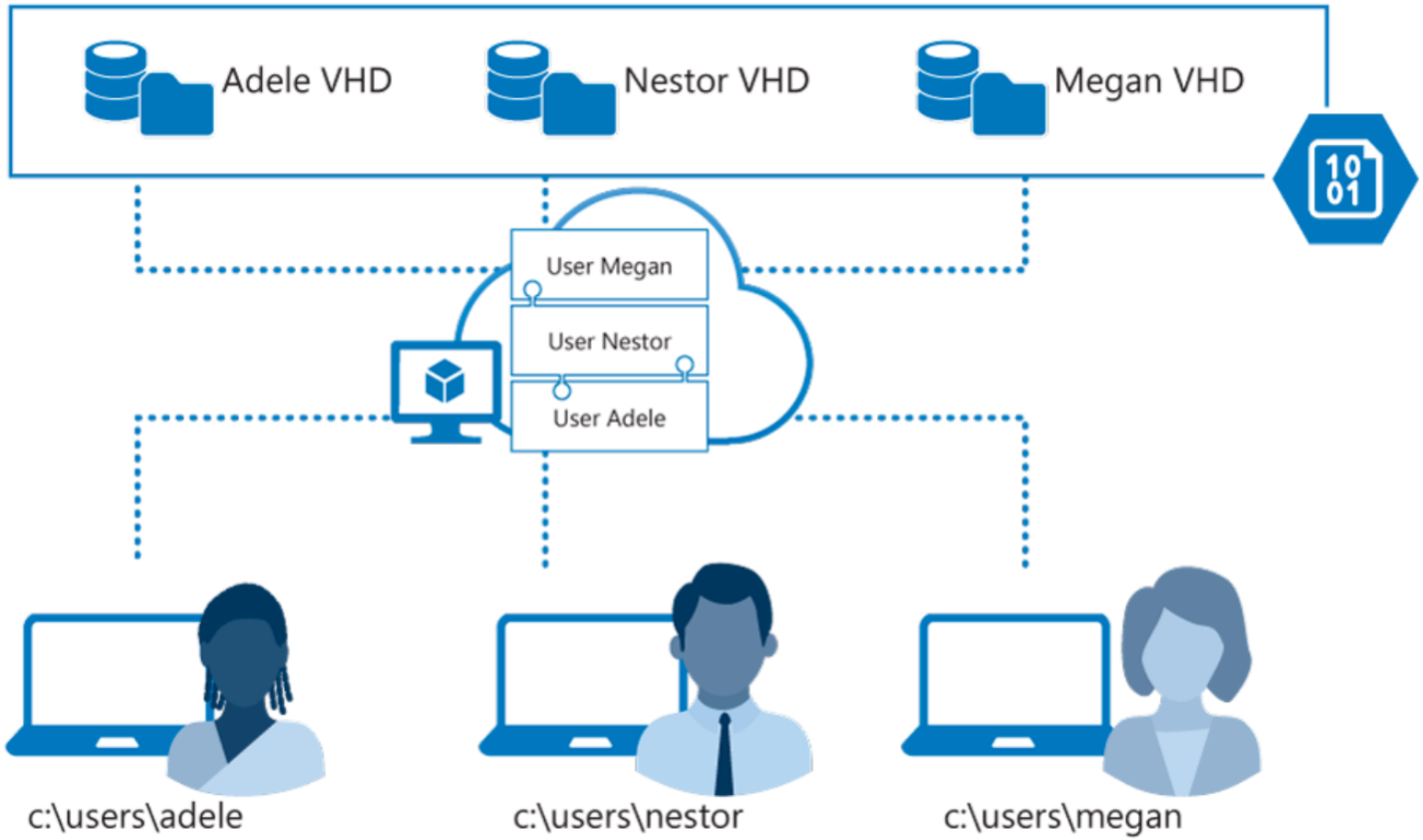
1. User signs into the Remote Desktop client
2. User gets assigned to a session host virtual machine (VM)
3. VM gets the user profile from the Azure file share
4. If MSIX app attach configured, apps are dynamically delivered to the session host VM. MSIX app attach uses FSLogix storage concepts, but for applications
5. User gets their Azure Virtual Desktop workspace populated with their assigned app(s) or session desktop



User Profiles and FSLogix components

FSLogix profile containers are the Azure Virtual Desktop user profile solution.

- FSLogix is designed to roam profiles in remote computing environments.
- It stores a complete user profile in a single container.
- At sign in, this container is dynamically attached to the computing environment using natively supported VHD and VHDX.
- The VHD or VHDX files are stored to this location and attached to users the next time they sign in.



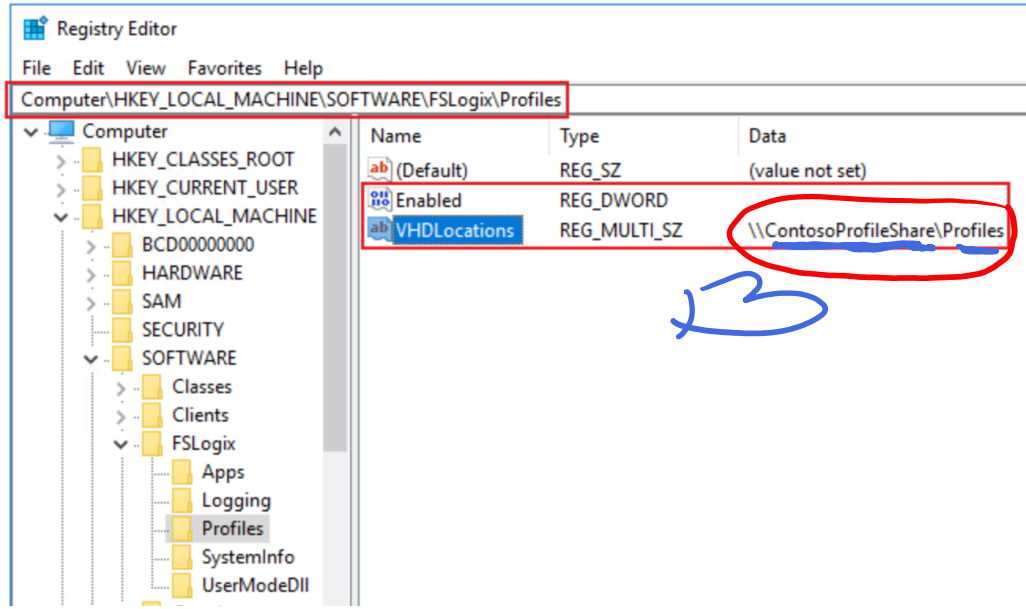
Configure storage for FSLogix components

To configure the virtual machines with the FSLogix software, do the following on each machine registered to the host pool:

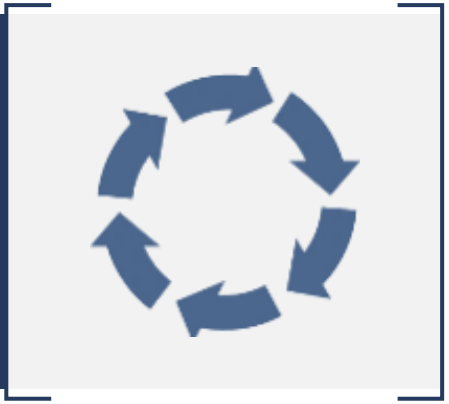
- Connect to the virtual machine with the credentials you provided when creating the virtual machine.
- Launch an internet browser and navigate to download the FSLogix agent.
- Navigate to either *\Win32\Release* or *\X64\Release* in the .zip file and run **FSLogixAppsSetup** to install the FSLogix agent.

4. Navigate to **Program Files > FSLogix > Apps** to confirm the agent installed.
5. From the start menu, run **RegEdit** as an administrator. Navigate to **Computer\HKEY_LOCAL_MACHINE\software\FSLogix**
6. Create a key named **Profiles**.
7. Create the following values for the Profiles key:

Name	Type	Data/Value
Enabled	DWORD	1
VHDLocations	Multi-String Value	"Network path for file share"



Configure storage accounts



Azure supports multiple types of storage accounts for different storage scenarios.

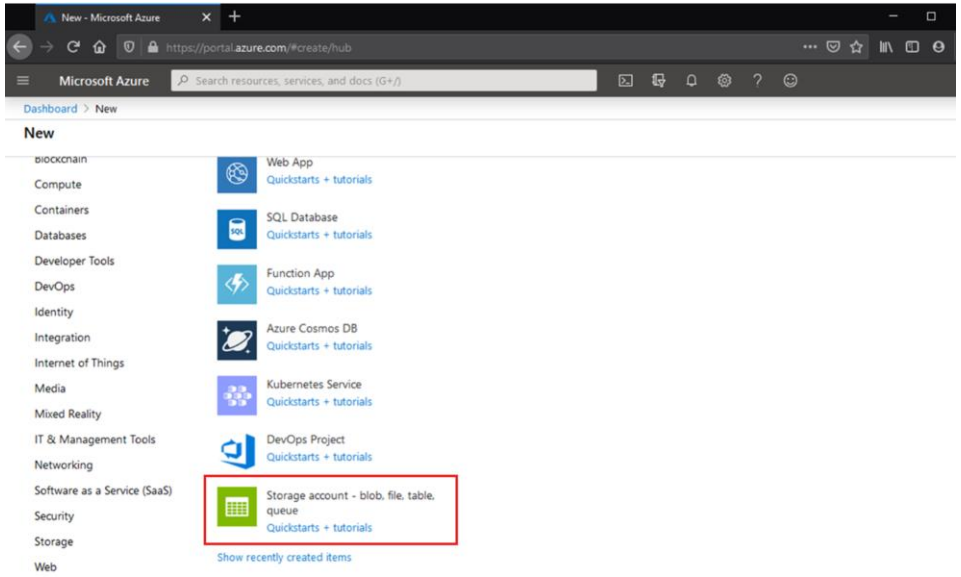
There are two main types of storage accounts for Azure Files.

General purpose version 2 (GPv2) storage accounts: Allow you to deploy Azure file shares on standard/hard disk-based (HDD-based) hardware.

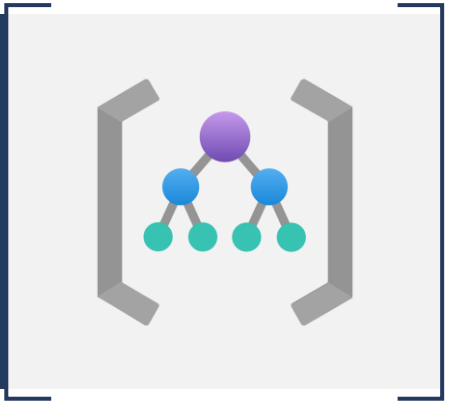
- In addition to storing Azure file shares, GPv2 storage accounts can store other storage resources such as blob containers, queues, or tables.
- File shares can be deployed into the transaction optimized (default), hot, or cool tiers.

FileStorage storage accounts: FileStorage storage accounts allow you to deploy Azure file shares on premium/solid-state disk-based (SSD-based) hardware.

- FileStorage accounts can only be used to store Azure file shares; no other storage resources (blob containers, queues, tables, etc.) can be deployed in a FileStorage account.



Create file shares



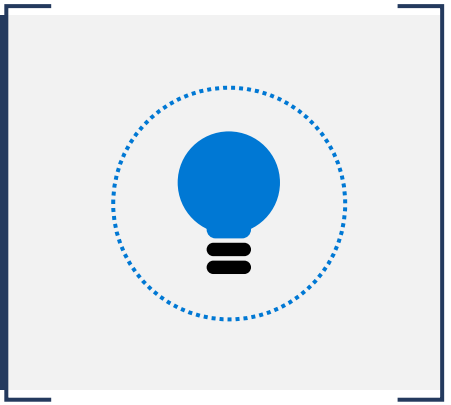
Once you've created a storage account, all that is left is to create your file share.

The process is the same for a premium file share or a standard file share.

You should consider the following differences:

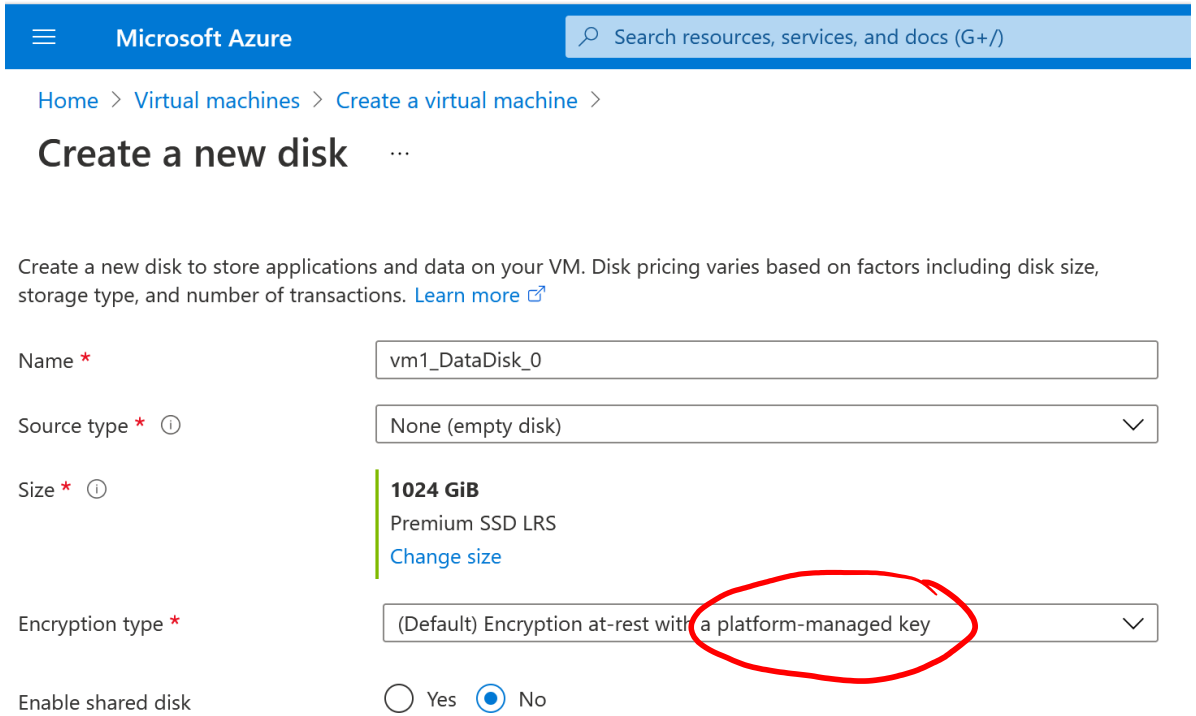
- Standard file shares may be deployed into one of the standard tiers:
  - transaction optimized (default)
  - Hot
  - Cool
- This is a per file share tier that is not affected by the **blob access tier** of the storage account.
- You can change the tier of the share at any time after it has been deployed.
- Premium file shares cannot be directly converted to standard file shares in any standard tier.
- You can move file shares between tiers within GPv2 storage account types (transaction optimized, hot, and cool).

Configure disks



Add a data disk

- Go to the Azure portal to add a data disk. Search for and select **Virtual machines**.
- Select a virtual machine from the list.
- On the **Virtual machine** page, select **Disks**.
- On the **Disks** page, select **Add data disk**.
- In the drop-down for the new disk, select **Create disk**.
- In the **Create managed disk** page, type in a name for the disk and adjust the other settings as necessary. When you're done, select **Create**.
- In the **Disks** page, select **Save** to save the new disk configuration for the VM.
- After Azure creates the disk and attaches it to the virtual machine, the new disk is listed in the virtual machine's disk settings under **Data disks**.



Knowledge check and Summary

Check your knowledge

What you learned:

- Choose appropriate storage for FSLogix components.
- Configure storage for FSLogix components.
- Configure storage accounts for Azure Files.
- Configure a new managed data disk to a Windows virtual machine for Azure Virtual Desktop.
- Create file shares for a storages account for Azure Virtual Desktop.

End of presentation