

Episode Title: Troubleshoot disk encryption

Objectives:

At the end of this episode, I will be able to:

1. Understand Key Vault Permissions
2. Explain VM SKUs and sizes
3. Troubleshoot VMs

Key Points:

Key Point 1

Azure Disk Encryption relies on access to an Azure Key Vault to store the encryption key. If the key was disabled, permissions or policy changed then the VM might not be able to decrypt the disk. This could also cause the VM to not start.

Key Point 2

Microsoft Azure offers a wide range of virtual machine (VM) sizes to cater to various workload requirements, from general-purpose computing to memory-intensive, GPU-accelerated, and storage-optimized workloads. However, some SKUs do not support disk encryption, such as Basic and A-series VMs. If you cannot enable disk encryption, ensure that you are using an appropriate SKU size.

Key Point 3

When troubleshooting VM issues, it's essential to correlate information from both Boot Diagnostics and Activity Logs. The serial console that boot diagnostics provide can provide useful information in troubleshooting.

- If additional resources are used during the episode, they can be obtained using the download link on the overview episode (e.g. diagrams, no powerpoints)

External Resources:

If external resources were used during this episode, you can reference the following external resources for supplementary tools and information, if none were used, then this section will be blank.:

- Azure Disk Encryption troubleshooting guide
: <https://learn.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-troubleshooting>