

Episode Title: Manage disk encryption for Azure VMs

Objectives:

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

1. Explain how to use Azure Disk Encryption.
2. Configure a key in Azure Key Vault.
3. Enable disk encryption using the key vault key.

Key Points:

Key Point 1

Azure Disk Encryption provides encryption for both Windows and Linux VMs. Windows uses BitLocker and Linux uses the dm-crypt module.

Key Point 2

Azure Disk Encryption requires that the key used for the encryption be stored in an Azure Key Vault.

Key Point 3

The Key Vault must be enabled for use with Azure Disk Encryption, and the VM identity must have permissions to get the key from the vault.

- 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:

- Overview of managed disk encryption options
: <https://learn.microsoft.com/en-us/azure/virtual-machines/disk-encryption-overview>