TM1953 VirtualMachines-002 Azure Disk Encryption for Non-Boot Disk Volumes

Risk Level: Medium
Rule ID: VirtualMachines-002

Ensure that your Microsoft Azure virtual machine (VM) data volumes (i.e. non-boot volumes) are encrypted using Azure Disk Encryption in order to meet security and compliance requirements. ADE encrypts the OS and data disks of Azure virtual machines (VMs) inside your VMs using the CPU via the DM-Crypt feature for Linux or the BitLocker feature for Windows. ADE is integrated with Azure Key Vault to help you control and manage the disk encryption keys and secrets. The VM data volume encryption and decryption is handled transparently and does not require any additional action from you, your Azure virtual machine, or your application.

Azure Disk Encryption helps protect and safeguard your data to meet your organizational security and compliance commitments. It uses the DM-Crypt feature of Linux and the BitLocker feature of Windows to provide volume encryption for the OS and data disks of Azure virtual machines (VMs), and is integrated with Azure Key Vault to help you control and manage the disk encryption keys and secrets. When your cloud applications work with sensitive data such as PII (Personally Identifiable Information), it is strongly recommended to enable encryption to protect this data from unauthorized access and fulfill compliance requirements for data-at-rest encryption within your organization. By encrypting your Azure virtual machine non-boot volumes, you have the guarantee that your entire VM data is fully unrecoverable without the protected key and therefore provides protection from unauthorized reads.

Audit

To determine if encryption at rest is enabled for all your Azure VM data volumes, perform the following actions:

Using Azure CLI

01 Run **vm list** command (Windows/macOS/Linux) using custom query filters to list the ID of each virtual machine (VM) provisioned in the current Azure subscription:

```
az vm list
   --query '[*].id'
```

02 The command output should return the requested VM server identifiers (IDs):

```
[
  "/subscriptions/abcdabcd-1234-abcd-1234-abcd1234abcd/resourceGroups/CLOUD-SHELL-STORAGE-WESTEUROPE/providers/Microsoft.Compute/virtualMachines/cc-warehouse-app-server",
  "/subscriptions/abcdabcd-1234-abcd-1234-abcd1234abcd/resourceGroups/CLOUD-SHELL-STORAGE-WESTEUROPE/providers/Microsoft.Compute/virtualMachines/cc-internal-app-server"
]
```

03 Run **vm encryption show** command (Windows/macOS/Linux) using the ID of the virtual machine that you want to examine as identifier parameter to obtain the encryption status set for the non-boot (data) disk volumes attached to the selected Azure VM:

```
az vm encryption show
  --ids "/subscriptions/abcdabcd-1234-abcd-1234-abcd1234abcd/resourceGroups/CLOUD-SHELL-STORAGE-WESTEUROPE/providers/Microsoft.Compute/virtualMachines/cc-warehouse-app-server"
  --query 'dataDisk'
```

04 The command output should return the requested VM non-boot volume encryption status:

```
Azure Disk Encryption is not enabled
```

If the **vm encryption show** command output returns the following message: **Azure Disk Encryption is not enabled**, the non-boot disk volumes attached to the selected Microsoft Azure virtual machine (VM) are not configured to encrypt data at rest.

05 Repeat step no. 3 and 4 for every Azure virtual machine launched within the current subscription.

06 Repeat steps no. 1 – 5 for each subscription available in your Microsoft Azure cloud account.

Using Azure Console

01 Sign in to Azure Management Console.

02 Navigate to **All resources** blade at https://portal.azure.com/#blade/HubsExtension/BrowseAll to access all your Microsoft Azure resources.

03 Choose the Azure subscription that you want to access from the **Subscription** filter box.

04 From the **Type** filter box, select**Virtual machine** to show only the virtual machines (VMs) available in the selected subscription.

05 Click on the name of the virtual machine that you want to examine.

06 In the navigation panel, under **Settings**, select **Disks** to view the disk volumes attached to the selected Azure VM.

07 On the **Disks** overview page, under **Data disks**, check the disk volume encryption status, available in the **ENCRYPTION** column, for each data volume attached. If the encryption status is set to **Not enabled** or does not explicitly mention **ADE (Azure Disk Encryption)**, the non-boot (data) volumes attached to the selected Microsoft Azure virtual machine (VM) are not encrypted using Azure Disk Encryption.

08 Repeat steps no. 4 – 7 for each Azure virtual machine available in the selected subscription.

09 Repeat steps no. 3 – 8 for each subscription created in your Microsoft Azure cloud account.

Azure Official Documentation

- Azure Disk Encryption for Linux VMs
- Azure Disk Encryption for Windows VMs
- Azure Disk Encryption for virtual machines and virtual machine scale sets
- Virtual Machine series
- CIS Microsoft Azure Foundations

Azure Command Line Interface (CLI) Documentation

- Quickstart: Create and encrypt a Linux VM with the Azure CLI
- Quickstart: Create and encrypt a Windows VM with the Azure CLI
- az vm
- az vm list
- az vm encryption
- az vm encryption show
- az vm encryption enable
- az keyvault
- az keyvault create