TM1954VirtualMachines-003 Azure Disk Encryption for Unattached Disk Volumes

Risk Level: Medium
Rule ID: VirtualMachines-003

Ensure that your detached Microsoft Azure virtual machine (VM) disk 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 unattached disk volumes 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 disk volumes detached from your Microsoft Azure virtual machines, you have the assurance that your data is unrecoverable without an encryption key and thus provides protection from unwarranted reads. Even if the disk volumes are not attached to any of the VMs provisioned within your Azure cloud account, there is always a risk where a compromised user account with administrative privileges can mount/attach these unencrypted disks, and this action can lead to sensitive information disclosure and/or data leakage.

Audit

To determine if encryption at rest is enabled for your unattached VM disk volumes, perform the following actions:

Note 1: Azure Disk Encryption encrypts the disk volume itself. This is distinct from Server-Side Encryption (also referred to as encryption-at-rest or Azure Storage encryption), which encrypts the data stored on the disk.

Note 2: Getting the Azure Disk Encryption status for the detached Azure VM disk volumes using Microsoft Azure Management Console (Azure Portal) is not currently supported.

Using Azure CLI

01 Run **disk list** command (Windows/macOS/Linux) using custom query filters to list the ID of each unattached managed disk volume available in the current Azure subscription:

```
az disk list
        --query '[?diskState == `Unattached`].id'
```

02The command output should return the requested disk volume identifiers (IDs):

```
[
"/subscriptions/abcdabcd-1234-abcd-1234-abcd1234abcd/resourceGroups/CLOUD-SHELL-STORAGE-WESTEUROPE/providers/Microsoft.Compute/disks/cc-warehouse-app_DataDisk_0",
"/subscriptions/abcdabcd-1234-abcd-1234-abcd1234abcd/resourceGroups/CLOUD-SHELL-STORAGE-WESTEUROPE/providers/Microsoft.Compute/disks/cc-warehouse-app_DataDisk_1"
]
```

03 Run **disk show** command (Windows/macOS/Linux) using the ID of the managed disk volume that you want to examine as identifier parameter to obtain the encryption configuration settings available for the selected unattached VM disk volume:

```
az disk show
  --ids "/subscriptions/abcdabcd-1234-abcd-1234-abcd1234abcd/resourceGroups/CLOUD-SHELL-STORAGE-WESTEUROPE/providers/Microsoft.Compute/disks/cc-warehouse-app_DataDisk_0"
  --query '{encryptionSettingsCollection: encryptionSettingsCollection}'
```

04 The command output should return the configuration settings for the specified disk volume:

```
{
  "encryptionSettingsCollection": null
}
```

If the **disk show** command output returns **null** as value for the "**encryptionSettingsCollection**" attribute, as shown in the example above, the unattached Azure VM disk volume is not currently encrypted.

05 Repeat step no. 3 and 4 for each Azure disk volume detached from a virtual machine, provisioned in the current subscription.

06 Repeat steps no. 1 – 5 for each subscription available within 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
- 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 disk
- az disk list
- az disk show
- az disk update
- az keyvault
- az keyvault create