Microsoft

Reactor

Welcome!

MEA Series: *Azure Disk Encryption*

– Windows

– Linux

Please visit:

aka.ms/Reactor-MEA-Series

Event ID: 14126

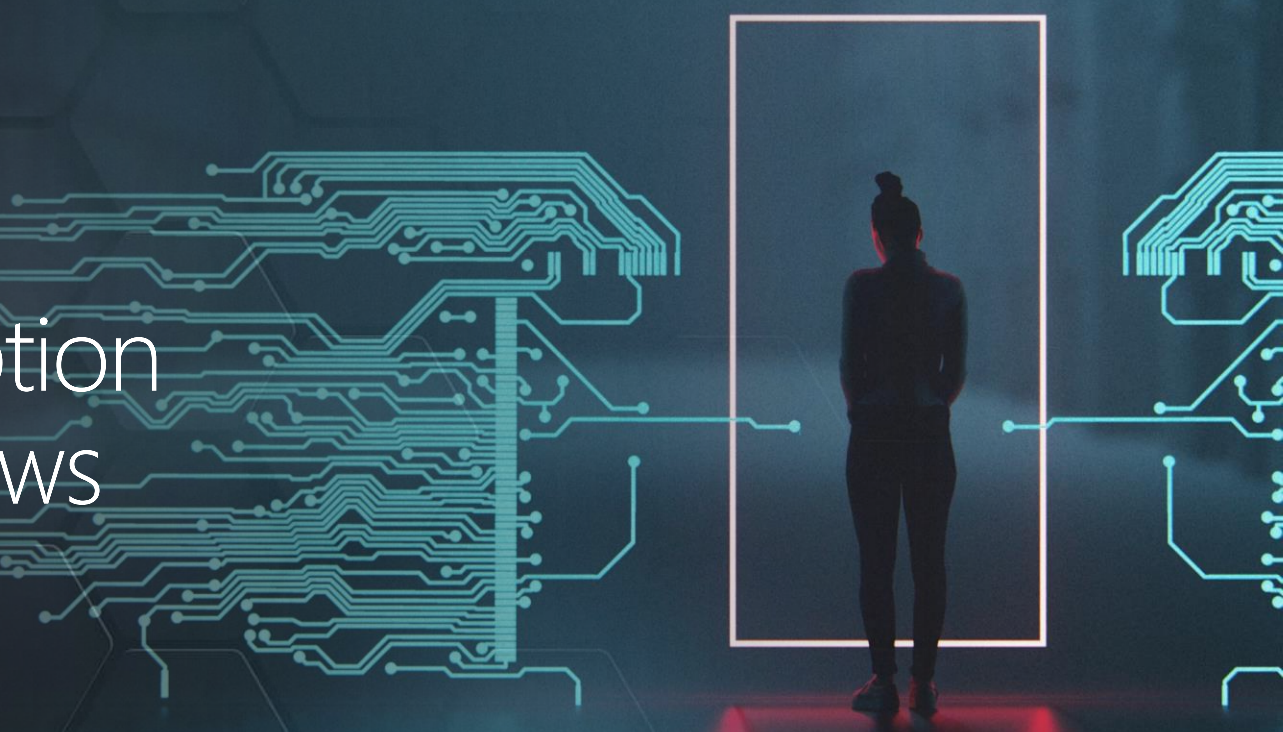
Event ID: 14127

Microsoft

Reactor

Microsoft Azure Disk Encryption Windows

Event Code: 14126



Agenda

1	Introduction to Azure Encryption
2	Data Encryption at rest in Microsoft cloud
3	Azure Disk Encryption
4	Encryption Comparison
5	Azure VM Extensions
6	ADE with PowerShell in Cloud Shell
7	ADE with PowerShell in Azure DevOps
8	Q & A
9	
10	

Speaker

Mallikarjuna Reddy Tunga

Cloud Solution Architect

ArjunReddyTunga

MallikarjunaReddyTunga

Speaker Bio: 14 years of extensive IT experience in developing and deploying enterprise scale software applications on Cloud and On-Premise Data Center's. Specialized in DevOps and Containers. Speaker and Happy to share real-time experiences with people and Azure tech group communities to take advantage of Cloud adoption.

Red Hat CERTIFIED SPECIALIST OpenShift
Red Hat CERTIFIED SPECIALIST Containers Kubernetes
Terraform ASSOCIATE HashiCorp CERTIFIED
OPENHACK: CONTAINERS Microsoft Challenge Complete
OPENHACK: DEVOPS Microsoft Challenge Complete
Microsoft CERTIFIED AZURE ADMINISTRATOR ASSOCIATE
Microsoft CERTIFIED DEVOPS ENGINEER EXPERT
Microsoft CERTIFIED AZURE SOLUTIONS ARCHITECT EXPERT
MICROSOFT CERTIFIED TRAINER Microsoft MCT Trainer 2021 - 2022
PMI PMP

https://www.meetup.com/AzureQatar/events/

https://www.youtube.com/c/AzureArjunReddy

https://github.com/AzureArjunReddy

Introduction to Azure Encryption

https://www.meetup.com/Microsoft-Reactor-Abu-Dhabi

Azure Encryption

Azure Disk Encryption

Azure Storage Service Encryption

Client-side encryption of Azure blobs

Encryption of data at rest with Azure SQL Database

Azure VPN encryption

Encryption of data in transit

Server Side Encryption

Service-managed keys.

Customer-managed keys.

Service-managed keys in customer-controlled hardware.

Client Side Encryption

Performed outside of Azure.

Data encrypted by an application that's running in the customer's datacenter.

Data that is already encrypted when it is received by Azure.

Encryption at host

Double Encryption

Data at rest

- **Disk encryption using customer-managed keys**. You provide your own key for disk encryption. You can bring your own keys to your Key Vault (BYOK – Bring Your Own Key), or generate new keys in Azure Key Vault to encrypt the desired resources.
- **Infrastructure encryption using platform-managed keys**. By default, disks are automatically encrypted at rest using platform-managed encryption keys.

Data in transit

- **Transit encryption using Transport Layer Security (TLS) 1.2 to protect data when it's traveling between the cloud services and you**. All traffic leaving a datacenter is encrypted in transit, even if the traffic destination is another domain controller in the same region. TLS 1.2 is the default security protocol used.
- **Additional layer of encryption provided at the infrastructure layer**. A data-link layer encryption method using the IEEE 802.1AE MAC Security Standards (also known as MACsec)

Data Encryption at Rest
Microsoft Cloud Services

https://www.meetup.com/Microsoft-Reactor-Abu-Dhabi

Microsoft
Reactor

Encryption at rest

Encryption is the secure encoding of data used to protect confidentiality of data

Azure use symmetric encryption to encrypt and decrypt large amounts of data quickly according to a simple conceptual model.

- A symmetric encryption key is used to encrypt data as it is written to storage.
- The same encryption key is used to decrypt that data as it is readied for use in memory.
- Data may be partitioned, and different keys may be used for each partition.
- Keys must be stored in a secure location with identity-based access control and audit policies.
- Data encryption keys are often encrypted with a key encryption key in Azure Key Vault to further limit access.

Purpose of Encryption at rest

Encryption at rest provides data protection for stored data (at rest).

- Attacks against data at-rest
- Attempts to obtain physical access to the hardware on which the data is stored

Encryption at rest is designed to prevent the attacker from accessing the unencrypted data by ensuring the data is encrypted when on disk.

- If an attacker obtains a hard drive with encrypted data but not the encryption keys
- The attacker must defeat the encryption to read the data

Encryption at rest may also be required by an organization's need for data governance and compliance efforts.

- Industry and government regulations such as HIPAA, PCI and FedRAMP
- Encryption at rest is a mandatory measure required for compliance with some of those regulations

Microsoft Cloud Services

Encryption at rest

IaaS

Infrastructure as a Service

Customers can have a variety of services and applications in use.

IaaS services can enable encryption at rest in their Azure hosted VM's

VHDs using Azure Disk Encryption.

PaaS

Platform as a Service

Customer's data typically resides in a storage service such as Blob Storage but may also be cached.

Stored in the application execution environment, such as a VM`s

SaaS

Software as a Service

Customers typically have encryption at rest enabled.

Available in each service.

Azure Disk Encryption(ADE)

Azure Disk Encryption(ADE)

Any customer using Azure Infrastructure as a Service (IaaS) features can achieve encryption at rest for their IaaS VMs and disks through Azure Disk Encryption.

Azure Disk encryption can be applied to:

Windows Virtual Machines

Linux Virtual Machines

Virtual Machine Scale Sets

Azure Disk Encryption(ADE) for Windows VMs

BitLocker is an industry-recognized Windows volume encryption technology that's used to enable disk encryption on Windows VMs..

Supported operating systems

- Windows client: Windows 8 and later.
- Windows Server: Windows Server 2008 R2 and later.

Supported VMs

- VMs not with a less than 2 GB of memory
- Not available on Basic, A-series VMs
- Not available on VM Sizes without temp disks

Disable encryption, You can disable encryption

- Disabling data disk encryption on Windows VM when both OS and data disks have been encrypted doesn't work as expected. Disable encryption on all disks instead.

Azure Disk Encryption – Requirement ?

- If your requirements include encrypting only data at rest with customer-managed key, then use
  - **Server-side encryption with customer-managed keys**.
- If you are using a scenario called out in unsupported scenarios for Windows, consider
  - **Server-side encryption with customer-managed keys**.
- If your organization's policy allows you to encrypt content at rest with an Azure-managed key, then no action is needed
  - **No Action Required**.
- If your requirements include encrypting all of the above and end-to-end encryption, use
  - **Azure Disk Encryption**
- You cannot encrypt a disk with both **Azure Disk Encryption** and Storage **server-side encryption with customer managed keys**.

Comparison

	Encryption at rest (OS and data disks)	Temp disk encryption	Encryption of caches	Data flows encrypted between Compute and Storage	Customer control of keys	Azure Security Center disk encryption status
Encryption at rest with platform-managed key (SSE+PMK)	☑	×	×	×	×	Unhealthy, not applicable if exempt
Encryption at rest with customer-managed key (SSE+CMK)	☑	×	×	×	☑	Unhealthy, not applicable if exempt
Azure Disk Encryption	☑	☑	☑	☑	☑	Healthy
Encryption at Host	☑	☑	☑	☑	☑	Unhealthy, not applicable if exempt

SSE Server Side Encryption | PMK Platform Managed Keys | CMK Costumer Managed Keys

Azure Disk Encryption

What is required ?

Azure Key Vault

Key Vault is a cryptographic, key management service that's based on Federal Information Processing Standards (FIPS).

Azure Disk Encryption is permitted to retrieve secrets from the vault and unwrap keys.

Key encryption key (KEK)

The asymmetric key (RSA 2048) that you can use to protect or wrap the secret.

You can provide a hardware security module (HSM)-protected key or software-protected key

Azure VM Extension

Azure Disk Encryption for Windows/Linux

How to perform ?

Azure CLI

The Azure CLI is optimized for managing and administering Azure resources from the command line.

Azure PowerShell cmdlets

Azure PowerShell is a set of cmdlets for managing Azure resources directly from the PowerShell command line.

Azure DevOps

PowerShell Task

AzCLI Task

Terraform Task

Azure Virtual Machine Extensions

https://www.meetup.com/Microsoft-Reactor-Abu-Dhabi

Azure VM Extensions

- Extensions are small applications that provide post-deployment configuration and automation on Azure VMs.
- The Azure platform hosts many extensions covering VM configuration, monitoring, security, and utility applications.
- Publishers take an application, wrap it into an extension, and simplify the installation.
- All you need to do is provide mandatory parameters.

AzVMBackupExtension

AzVMChefExtension

AzVMCustomScriptExtension

AzVMDiagnosticsExtension

AzVMDiskEncryptionExtension

AzVMDscExtension

AzVMSqlServerExtension

AzVmssDiskEncryptionExtension

AzVMAccessExtension

ADE PowerShell Code

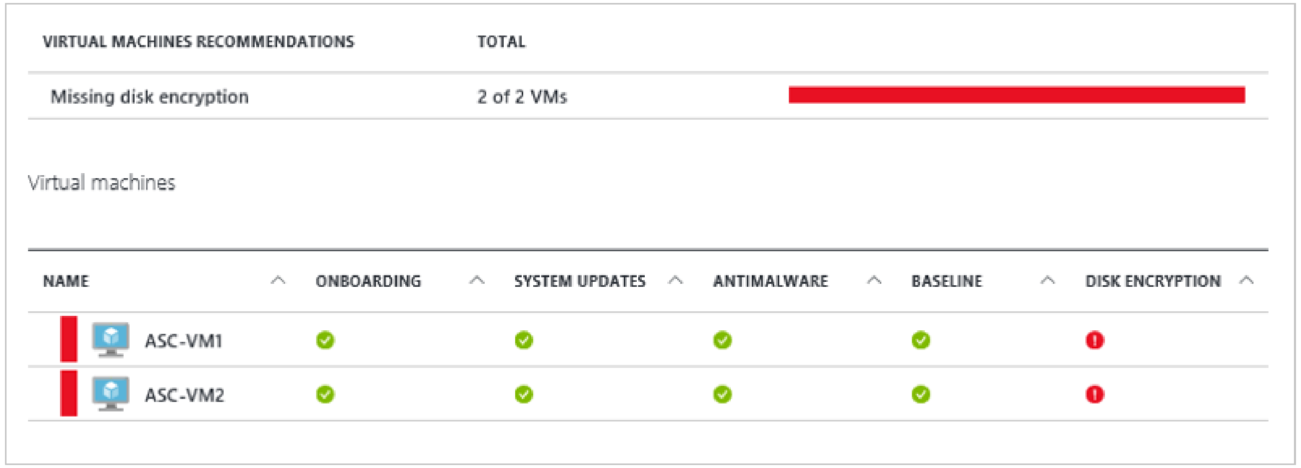
```
$vmName = "WEUWINVM01";        $location = "westeurope";     $keyVaultName = "weuskv01";
$rgName = "winvm-rg";          $keyrgName = "keyvault-rg";   $keyVaultKey = "WinVMKvKek01";

$KeyVault = Get-AzureRmKeyVault -VaultName $keyVaultName -ResourceGroupName $keyrgName;
$VaultUrl = $keyVault.VaultUri;
$VaultId = $keyVault.ResourceId;
$KeyUrl = (Get-AzureKeyVaultKey -VaultName $keyVaultName -Name $keyVaultKey).Key.kid;

Set-AzureRmVMDiskEncryptionExtension -Name "WinDiskEncryption" -
ResourceGroupName $rgName -VMName $vm -DiskEncryptionKeyVaultUrl $VaultUrl -
DiskEncryptionKeyVaultId $VaultId -KeyEncryptionKeyUrl $KeyUrl -
KeyEncryptionKeyVaultId $VaultId -VolumeType 'ALL' -skipVmBackup -Force

Get-AzureRmVMDiskEncryptionStatus -ResourceGroupName $rgName -VMName $vm -
Name "WinDiskEncryption"
```

Azure Security Center



VIRTUAL MACHINES RECOMMENDATIONS	TOTAL
Missing disk encryption	2 of 2 VMs

Virtual machines

NAME	ONBOARDING	SYSTEM UPDATES	ANTIMALWARE	BASELINE	DISK ENCRYPTION
🟥 ASC-VM1	✓	✓	✓	✓	!
🟥 ASC-VM2	✓	✓	✓	✓	!

- If you use Azure Security Center, you're alerted if you have VMs that aren't encrypted.

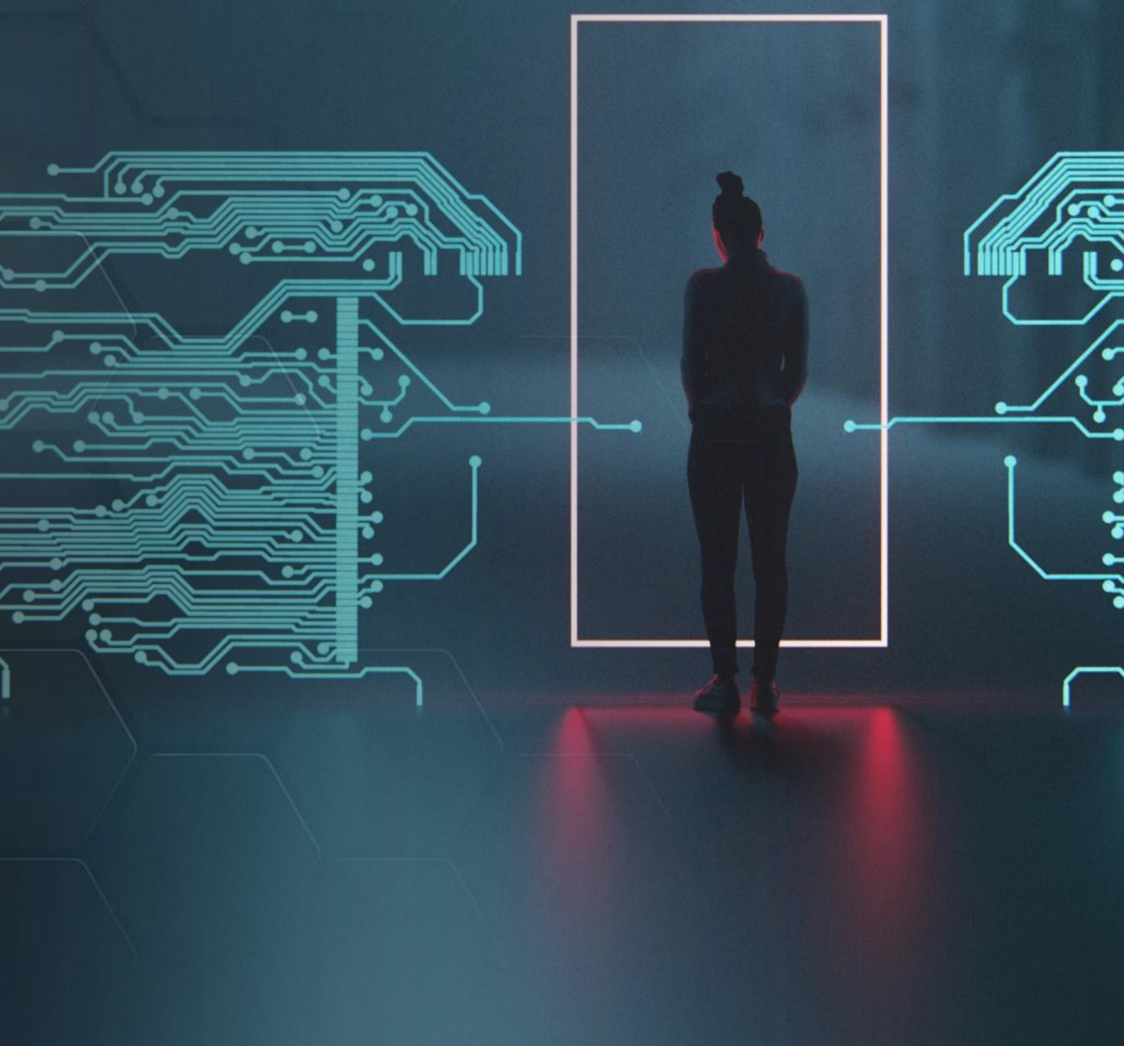
- The alerts show as High Severity and the recommendation is to encrypt these VMs.

Microsoft

Reactor

Microsoft Azure Disk Encryption Linux

Event Code: 14127



Azure Disk Encryption(ADE) for Linux VMs

DM-Crypt feature of Linux provides full disk encryption of the OS disk* and data disks.

Supported operating systems

- Only the gallery Linux images for the supported distributions.
- RHEL Pay-As-You-Go images
- RHEL Bring-Your-Own-Subscription Gold Images
- Can't apply ADE on custom Linux image

Supported VMs

- Linux VMs not with a less than 2 GB of memory to encrypt only Data Disks.
- Linux VMs not with a less than 8 GB of memory to encrypt OS and Data Disks.
- Not available on Basic, A-series VMs

https://docs.microsoft.com/en-us/azure/virtual-machines/linux/disk-encryption-overview

Azure Disk Encryption - Linux

The encryption process can take between 3-16 hours to finish on a Gallery image.

Microsoft strongly recommend to avoid SSH logins while the encryption is in progress to avoid issues blocking any open files

All user-space processes that are not running as SYSTEMD services should be killed with a SIGKILL and Reboot the VM.

Recommend to have VM Boot diagnostics enabled.

Resize of an ADE encrypted OS disk is currently not supported.

Disabling encryption on the OS volume isn't supported.

Disabling encryption is only allowed on Data volumes

https://docs.microsoft.com/en-us/answers/topics/azure-disk-encryption.html

Azure Disk Encryption - Linux

Recommended to take snapshot and/or backup a managed disk based VM instance outside of, and prior to enabling Azure Disk Encryption.

A snapshot of the managed disk can be taken from the portal, or through Azure Backup. Backups ensure that a recovery option is possible in the case of any unexpected failure during encryption

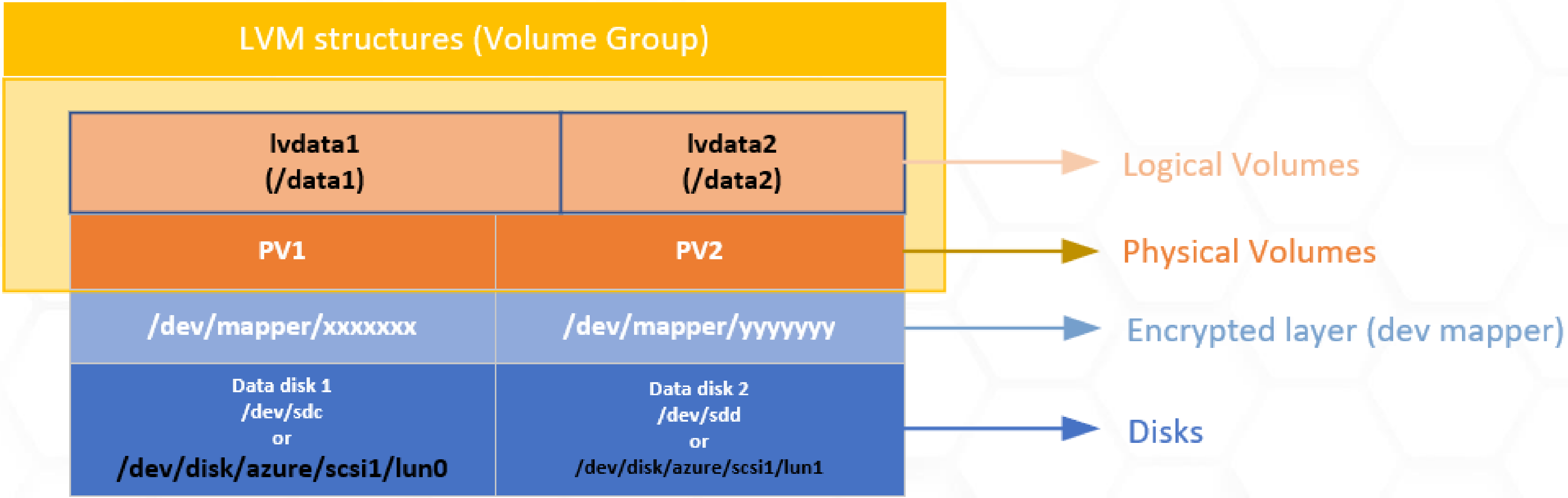
"Bek Volume" or "/mnt/azure_bek_disk“

The "Bek volume" is a local data volume that securely stores the encryption keys for Encrypted Azure VMs.

Do not delete or edit any contents in this disk. Do not unmount the disk since the encryption key presence is needed for any encryption operations on the IaaS VM.

Azure Disk Encryption – Linux

Traditional LVM and LVM-on-crypt



LVM-on-crypt, Using EncryptFormatAll feature for data disks on Linux VMs.

Not recommend mixing traditional LVM encryption and LVM-on-crypt on the same VM

https://docs.microsoft.com/en-us/azure/virtual-machines/linux/how-to-configure-lvm-raid-on-crypt

Demo of Azure Disk Encryption

Windows Virtual Machine

https://www.meetup.com/pro/microsoft-reactor/

Q & A

https://www.meetup.com/Microsoft-Reactor-Abu-Dhabi

Microsoft

Reactor

Thank You!

https://www.meetup.com/Microsoft-Reactor-Abu-Dhabi

@MSFTReactor

http://www.youtube.com/c/MicrosoftReactor

aka.ms/ReactorEmailSignUp