**Practical Work Experience and Portfolio Building**

**Evidence Reporting Document**

* **Introduction**

*The main goal of this document is to keep track of the practical hands-on work experience and lab challenges you will complete throughout the program. By doing so, at the end of the program, you will have a great portfolio that you can use for evidence of your practical skills, and you can also come back for review whenever needed. This evidence is essential in the long run and keeps you on track with the time you will spend on your career upgrade process. These notes will also play a vital role in identifying the skills and tools to reflect on your marketing materials like your CV/resume or LinkedIn Page.*

* **General Details**

**Date: 14 May 2024**

**Your Name: LOK HIM TAM (Himson)**

**Email-address:** himsom0528@gmail.com

**Name of the Challenge:** Configure Azure Disk Encryption

**Access Details (URL or source):** AZ500

**Details of the Challenge:**

In this lab I have working following exercise:

* Create an Azure virtual machine
  + Create an Azure virtual machine
  + Verify that **webVM1** contains one OS disk that uses **SSE with PMK** encryption
  + [Server-side encryption](https://docs.microsoft.com/en-us/azure/virtual-machines/disk-encryption) (SSE) of Azure Disk Storage is enabled by default and encrypts disks at the storage server level by using a platform-managed key (PMK). The encryption key is managed automatically by the platform, in this case Azure, including protection and regular rotation. You can use server-side encryption with a customer-managed key (SSE with CMK) to manage the encryption key manually for compliance reasons. You can combine SSE with Azure Disk Encryption (ADE), which additionally encrypts the disk at the OS level by using technologies such as BitLocker (Windows) or DM-Crypt (Linux), for what is called double encryption at rest high security requirements.
  + created an Azure virtual machine named webVM1 that is encrypted with a platform-managed key.
* Add a new data disk to the Azure virtual machine
  + Create a new disk for VM
  + Connect to **webVM1** by using **RDP**
  + Initialize the new disk as a simple volume by using the drive letter **F**, the **NTFS** file system, and new volume labels
* Enable Azure Disk Encryption
  + creating a key vault in azure and applied **Azure Disk Encryption for volume encryption**
  + Launch an Azure **Cloud Shell** **PowerShell** session
  + retrieving the properties of a key vault by using powershell
    - $KeyVault = Get-AzKeyVault -VaultName KV40647575 -ResourceGroupName corp-datalod40647575
  + enabling Azure Disk Encryption by using powershell
    - Set-AzVMDiskEncryptionExtension -ResourceGroupName corp-datalod40647575 -VMName webVM1 -DiskEncryptionKeyVaultUrl $KeyVault.VaultUri -DiskEncryptionKeyVaultId $KeyVault.ResourceId
  + verifying that the encryption succeeded
    - Get-AzVmDiskEncryptionStatus -VMName webVM1 -ResourceGroupName corp-datalod40647575
  + verifying the updated disk specifications in the Azure portal

**Lab Topology**

Create an Azure virtual machine by using the values in the following table. For any property that is not specified, use the default value.

| **Property** | **Value** |
| --- | --- |
| Resource group | **corp-datalod40647575** |
| Virtual machine name | webVM1 |
| Image | **Windows Server 2019 Datacenter - Gen2** |
| Size | **Standard\_B2ms** |
| Username | AzureAdmin |
| Password | Az!40647575! |
| Public inbound ports | **Allow selected ports** |
| Select inbound ports | **RDP (3389)** |
| OS disk type | **Standard HDD** |
| Boot diagnostics | **Disable** |

Create an Azure key vault by using the values in the following table. For any property that is not specified, use the default value.

| **Property** | **Value** |
| --- | --- |
| Resource group | **corp-datalod40647575** |
| Key vault name | KV40647575 |
| Pricing tier | **Standard** |
| Azure Disk Encryption for volume encryption | **Selected** |

Launch an Azure **Cloud Shell** **PowerShell** session by using the values in the following table. For any property that is not specified, use the default value.

| **Property** | **Value** |
| --- | --- |
| Resource group | **corp-datalod40647575** |
| Storage account | cs40647575 |
| File share | cloudshell |

* **Challenge Details**

**Before starting the challenge:**

1. Be sure that the lab is in the scope of your niche.
2. You have enough time to solve the full lab or have a proper plan to solve a part of it and complete the remaining sections later.
3. Try to build a good learning environment with less distraction for at least 30 minutes to an hour.

**After completing the challenge:**

1. Were you able to finish the lab? Did you need extra time? Was the lab relevant to your expectations? Did you need additional help to solve the lab?

* Yes I am able to finish the lab within 45 mins. It is relevant to my expectations. And I can finish it without additional help.

1. Write down your learning outcomes, skills you developed or improved and the tools you used in this challenge.

*(You may use the keywords listed in the lab details or add your own skills that you think you acquired.)*

* Create an Azure virtual machine
  + I leant how to create an Azure virtual machine
  + I leant how to verify that **webVM1** contains one OS disk that uses **SSE with PMK** encryption
  + I learnt what is [Server-side encryption](https://docs.microsoft.com/en-us/azure/virtual-machines/disk-encryption) (SSE).
  + I created an Azure virtual machine named webVM1 that is encrypted with a platform-managed key.
* Add a new data disk to the Azure virtual machine
  + I create a new disk for VM
  + I leant how to connect to **webVM1** by using **RDP**
  + I learnt how to Initialize the new disk as a simple volume by using the drive letter **F**, the **NTFS** file system, and new volume labels in RDP
* Enable Azure Disk Encryption
  + I learn how to create a key vault in azure and applied **Azure Disk Encryption for volume encryption**
  + I leant how to launch an Azure **Cloud Shell** **PowerShell** session
  + I leant how to retrieve the properties of a key vault by using powershell
  + I learnt how to enable Azure Disk Encryption by using powershell
  + I learnt how to verify that the encryption succeeded
  + I learnt how to verify the updated disk specifications in the Azure portal

1. Prepare a self-reflection and reporting video using any screen recording tool (like Loom) and share the link.

*(The report may include but is not limited to your thoughts about the problem solved, difficulties encountered, any notes to discuss with your peers, anything to ask the mentors and last but not least how it may help you in your ideal job. Please prepare the summary in a way that you are presenting this to your managers and colleagues in your ideal workplace)*

**URL:** [**https://www.loom.com/share/a95e529a6fd9422daefd4b1ffd4c3da1?sid=f5e2956f-c3e3-48aa-8127-503cfc6594ca**](https://www.loom.com/share/a95e529a6fd9422daefd4b1ffd4c3da1?sid=f5e2956f-c3e3-48aa-8127-503cfc6594ca)