**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: 17 May 2024**

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

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

**Name of the Challenge:** Can You Harden Virtual Machines in Azure [Advanced]

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

**Details of the Challenge:**

In this lab I have working following exercise:

Create an Azure virtual network by using a network security group

Create a virtual network in the Azure portal

Create a network security group named webNSG in the **corp-datalod41228009** resource group

Associate the webNSG network security group to the **web** subnet in the **webVNET** virtual network.

# Deploy an Azure virtual machine for a web app by using an application security group

* Create an application security group named webASG in the **corp-datalod41228009** resource group.
* Create an Azure virtual machine
* Associate the VM1 virtual machine network interface to the **webASG** application security group.

# Enable web connectivity by using an application security group

Add an inbound security rule

Connect to VM1 through **RDP**

* Install **IIS** on **VM1** by using **Windows PowerShell**®.

# Enable Azure Disk Encryption

Create an Azure key vault

Launch an Azure **Cloud Shell** **PowerShell**

Enable Azure Disk Encryption on VM1 in the corp-datalod41228009 resource group by using the Set-AzVMDiskEncryptionExtension PowerShell cmdlet and a vault name of KV41228009

Verify that the encryption succeeded by using the Get-AzVmDiskEncryptionStatus cmdlet.

**Lab Topology**

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

| **Property** | **Value** |
| --- | --- |
| Resource group | **corp-datalod41228009** |
| Name | webVNET |
| IPv4 address space | 10.10.0.0/16 |
| Subnet name | web |
| Subnet address range | 10.10.0.0/26 |

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

| **Property** | **Value** |
| --- | --- |
| Resource group | **corp-datalod41228009** |
| Virtual machine name | VM1 |
| Image | **Windows Server 2019 Datacenter - Gen2** |
| Size | **Standard\_B2s - 2 vcpus 4 GiB memory** |
| Username | AzureAdmin |
| Password | Az!41228009! |
| Public inbound ports | **None** |
| Virtual network | **webVNET** |
| Subnet | **web (10.10.0.0/26)** |
| NIC network security group | **None** |
| Boot diagnostics | **Disable** |

Add an inbound security rule to webNSG to allow HTTP and HTTPS traffic by using the values in the following table. For any property that is not specified, use the default value.

| **Setting** | **Value** |
| --- | --- |
| Destination | **Application security group** |
| Destination application security group | **webASG** |
| Destination port ranges | 80,443 |
| Name | AllowAllWeb |

Add a second inbound security rule to webNSG to allow RDP traffic by using the values in the following table. For any property that is not specified, use the default value.

| **Property** | **Value** |
| --- | --- |
| Destination | **Application security group** |
| Destination application security group | **webASG** |
| Destination port ranges | 3389 |
| Name | AllowRDP |

Connect to VM1 through **RDP** by using the values in the following table. For any property that is not specified, use the default value.

| **Property** | **Value** |
| --- | --- |
| IP address | **Public IP address** |
| Username | AzureAdmin |
| Password | Az!41228009! |

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-datalod41228009** |
| Key vault name | KV41228009 |
| Pricing tier | **Standard** |
| Azure Disk Encryption for volume encryption | **Selected** |

* **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.)*

* I have learnt how to create a virtual network in the Azure portal and create a network security group
* I have learnt how to associate network security group to the **web** subnet in the **webVNET** virtual network.
* I have learnt how to deploy an azure virtual machine for web app by using application security group
* And then associate that VM to network interface
* I have learnt how to enable web connectivity by using an application security group
* I have learnt how to add inbound security rules to that application security group
* I have learnt how to install IIS by using PowerShell in VM
* I have learnt how to enable azure disk encryption
* I have learnt how to create azure key vault
* I have learnt how to enable Azure Disk Encryption by using the Set-AzVMDiskEncryptionExtension PowerShell cmdlet
* I have learnt how to Verify that the encryption succeeded by using the Get-AzVmDiskEncryptionStatus cmdlet.

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/4092a9956ebf47378ca71b636911fe09?sid=908027ec-6266-4f60-a39a-0db2c2786835**](https://www.loom.com/share/4092a9956ebf47378ca71b636911fe09?sid=908027ec-6266-4f60-a39a-0db2c2786835)