# Lab Answer Key: Module 4: Managing virtual machines

# Lab: Managing Azure virtual machines

## Exercise 1: Configuring front-end web tier

#### Task 1: Review the existing deployment

1. Ensure that you are signed in to MIA-CL1 as **Student** with the password **Pa55w.rd**. Ensure that the Add-20533EEnvironment script successfully completed.
2. Start Microsoft Edge, browse to [**https://portal.azure.com**](https://portal.azure.com), and sign in by using the Microsoft account that is the Service Administrator of your Azure subscription.
3. In the Azure portal, in the hub menu, click **Resource groups**.
4. On the Resource groups blade, click **20533E0401-LabRG**.
5. On the 20533E0401-LabRG blade, review the list of resources. Note that includes an availability set named 20533E0401-avset.
6. Click **20533E0401-avset**.
7. On the 20533E0401-avset blade, note that the availability set has 2 fault domains, 5 update domains, and it contains two virtual machines. Also note that each VM has a unique fault domain and update domain.
8. Leave the Microsoft Edge window with the Azure portal open.

#### Task 2: Implement an Azure Load Balancer

1. On MIA-CL1, in the Azure portal, in the hub menu, click **+ Create resource**, click **Networking**, and then click **Load Balancer**.
2. On the **Create load balancer** blade, specify the following settings:

* Name: **20533E0401-ilb**
* Type: **Public**
* SKU: **Basic**
* Public IP address: click **Choose a public IP address**, on the Choose public IP address blade, click **Create new**, on the **Create public IP address** blade, in the **Name** text box type **20533E0401-ilbfe**, ensure that the **Dynamic** option is selected, and click **OK**.
* Subscription: the name of your Azure subscription
* Resource group: click **Use existing** and, in the drop-down list, click **20533E0401-LabRG**
* Location: the same Azure region you chose when running the provisioning script at the beginning of this module

1. Click **Create**. Wait for the deployment to complete.
2. In the hub menu, click **All services**, in the service menu, click **Load Balancers**, and then on the Load balancers blade, click **20533E0401-ilb**.
3. On the 20533E0401-ilb blade, click **Backend pools**, and then click **Add**.
4. On the Add backend pool blade, in the **Name** text box, type **20533E0401-ilb-bepool**, click **IPv4**, and then, in the **Associated to** drop down list, click **Availability set**
5. In the **Availability set** drop down list, click **20533E0401-avset**.
6. Click **Add a target network IP configuration**, in the **Target virtual machine** drop down list, click **20533E0401-vm0** and, in the **Network IP configuration** drop down list, click the **ipconfig1** entry.
7. Click **Add a target network IP configuration**, in the **Target virtual machine** drop down list, click **20533E0401-vm1** and, in the **Network IP configuration** drop down list, click the **ipconfig1** entry.
8. Click **OK**. Wait until the operation completes.
9. On the 20533E0401-ilb blade, click **Health probes**, and then click **Add**.
10. On the **Add health probe** blade, specify the following settings, and then click **OK**:

* Name: **20533E0401-ilb-probetcp80**
* Protocol: **HTTP**
* Port: **80**
* Path: **/**
* Interval: **5**
* Unhealthy threshold: **2**

1. Wait until the operation completes.
2. On the 20533E0401-ilb blade, click **Load balancing rules**, and then click **Add**.
3. On the **Add load balancing rule** blade, complete the following , and then click **OK**:

* Name: **20533E0401-ilb-ruletcp80**
* IP Version: **IPv4**
* Frontend IP address: **LoadBalancerFrontEnd**
* Protocol: **TCP**
* Port: **80**
* Backend port: **80**
* Backend Pool: **20533E0401-ilb-bepool (2 virtual machines)**
* Probe: **20533E0401-ilbprobetcp80 (HTTP:80)**
* Session persistence: **None**
* Idle timeout: **4**
* Floating IP (direct server return): **Disabled**

1. Wait until the operation completes.
2. On the 20533E0401-ilb blade, click **Inbound NAT rules** and then click **Add**.
3. On the Add inboud NAT rule blade, specify the following settings and click **OK**:

* Name: **20533E0401-ilb-natrulerdpvm0**
* Frontend IP address: **LoadBalancerFrontEnd**
* Service: **Custom**
* Protocol: **TCP**
* Port: **33890**
* Associated to: **20533E0401-avset (availability set)**
* Target virtual machine: **20533E0401-vm0**
* Network IP configuration: **ipconfig1**
* Port mapping: **Custom**
* Floating IP (direct server return): **Disabled**
* Target port: **3389**

1. On the 20533E0401-ilb blade, click **Inbound NAT rules** and then click **Add**.
2. On the Add inboud NAT rule blade, specify the following settings and click **OK**:

* Name: **20533E0401-ilb-natrulerdpvm1**
* Frontend IP address: **LoadBalancerFrontEnd**
* Service: **Custom**
* Protocol: **TCP**
* Port: **33891**
* Associated to: **20533E0401-avset (availability set)**
* Target virtual machine: **20533E0401-vm1**
* Network IP configuration: **ipconfig1**
* Port mapping: **Custom**
* Floating IP (direct server return): **Disabled**
* Target port: **3389**

**Note:** This configuration will allow you to connect to both Azure VMs via RDP even though they do not have directly assigned public IP address.

1. On the 20533E0401-ilb blade, click **Overview**. In the **Essentials** section, you should be able to identify the public IP address assigned to the load balancer. Note that at this point, you will not be able to connect to the two virtual machines in the backend pool, because they are not running a web server and the connectivity is additionally restricted by default network security group settings and the operating system-level firewall. You will change these settings later in this lab.

#### Task 3: Install and configure IIS on Azure VMs by using DSC and Windows PowerShell

1. On MIA-CL1, click **Start**, in the Start menu, expand the **Windows PowerShell** folder, right-click **Windows PowerShell ISE**, click **More**, and then click **Run as administrator**. When prompted by User Account Control for confirmation, click **Yes**.
2. In the Windows PowerShell Integrated Scripting Environment (ISE) window, open the **IISInstall.ps1** file located in the **F:\Labfiles\Lab04\Starter** folder.
3. Review the content of the file. Note that this is a DSC configuration that controls the installation of the Windows Server Web-Server role.
4. In the Windows PowerShell ISE window, open the **F:\Labfiles\Lab04\Starter\Deploy-20533E0401DSC.ps1** file.
5. Review the content of the script. Note the variables that it uses, including the storage account and its key. The script first retrieves the storage account from the resource group, and then publishes the DSC configuration defined in the **Install.ps1** into it, placing it in the default DSC container named **windows-powershell-dsc**, stores the resulting module URL in a variable, and then sets the Azure Agent VM DSC extension on two virtual machines deployed by the provisioning script by referencing that URL. The script generates a shared access signature token that provides read only access to the blob representing the DSC configuration archive.
6. Start the execution of the script. When prompted, sign in using the Microsoft account that is the Service Administrator of your subscription. Wait until the script completes.
7. Switch to the Azure portal in the Microsoft Edge window.
8. On the **Virtual machines** blade, click ellipsis to the right of the **20533E0401-vm0** entry and click **Connect**.
9. On the **Connect to virtual machine** blade, click **Download RDP File**. When prompted, click **Open**.
10. If a Remote Desktop Connection warning message displays, select **Don't ask me again for connections to this computer**, and then click **Connect**.
11. In the Windows Security dialog box, type the following credentials, and then click **OK**:

* User name: **Student**
* Password: **Pa55w.rd1234**

1. If another Remote Desktop Message displays, select the **Don't ask me again for connections to this computer** checkbox, and then click **Yes**.
2. If prompted in the Remote Desktop session whether to allow your PC to be discoverable, click **No**.
3. After you establish a Remote Desktop session to the VM, wait for the Server Manager window to open. In the Server Manager window, verify that **IIS** appears in the left pane, indicating that the Web Server (IIS) server role is installed.
4. Repeat steps 9 through 14 for the other virtual machine **20533E0401-vm1**.
5. After completing the tasks, switch back to your lab computer MIA-CL1. Leave both Remote Desktop sessions open.

#### Task 4: Test the DSC configuration and virtual machine availability

1. On MIA-CL1, in Microsoft Edge, in the Azure portal, in the hub menu, click **Resource groups**.
2. On the Resource groups blade, click **20533E0401-LabRG**.
3. On the 20533E0401-LabRG blade, in the list of resources, click **20533E0401-web-nsg**. This will open the corresponding blade.
4. On the 20533E0401-web-nsg network security group blade, click **Inbound security rules**.
5. Click **Add**.
6. On the Add inbound security rule blade, ensure that **Basic** appears in the upper left corner, and specify the following settings:

* Source: **Any**
* Source port ranges: **\***
* Destination: **Any**
* Destination port ranges: **80**
* Protocol: **TCP**
* Action: **Allow**
* Priority: **1100**
* Name: **allow-http**

1. Click **OK**.
2. Navigate back to the 20533E0401-LabRG blade.
3. On the 20533E0401-LabRG blade, in the list of resources, click **20533E0401-ilb**, representing the load balancer.
4. On the 20533E0401-ilb blade, note the value of its **Public IP address** entry.
5. Open a new InPrivate Microsoft Edge window, in the navigation bar, type **http://** followed by the IP address that you noted in the previous step, and then press the **Enter** key.
6. Verify that you can access the default IIS webpage.
7. Switch to the Remote Desktop session on **20533E0401-vm0**. In the **Server Manager** window, click **Tools** and, in the drop down menu, click **Services**.
8. In the **Services** window, scroll down to the **World Wide Web Publishing Service** entry, right click on it, and click **Stop** in the right-click menu.
9. Switch to the Remote Desktop session on **20533E0401-vm1**. In the **Server Manager** window, click **Tools** and, in the drop down menu, click **Services**.
10. In the **Services** window, scroll down to the **World Wide Web Publishing Service** entry, right click on it, and click **Stop** in the right-click menu.
11. Switch back to MIA-CL1. From MIA-CL1, refresh the InPrivate Microsoft Edge window.
12. Verify that the **Hmm, we can't reach this page** message appears.
13. Switch back to the **Services** window the Remote Desktop session on 20533E0401-vm0.
14. In the **Services** window, right-click the **World Wide Web Publishing Service** entry, and then click **Start** in the right-click menu.
15. Once the service is running, switch back to MIA-CL1 and refresh the InPrivate Microsoft Edge window. Verify that you can again access the default IIS webpage. Note that you might need to wait about a minute after you start the **World Wide Web Publishing Service** service.

**Note:** Optionally you can repeat this sequence, but this time stopping the **World Wide Web Publishing Service** on 20533E0401-vm0 and starting it on 20533E0401-vm1. As long as the service is running on at least one of the two virtual machines, you should be able to access the webpage.

**Result**: After completing this exercise, you should have created and configured a load balancer in front of two Azure VMs in the same availability set and implemented DSC-based configuration on these VMs.

## Exercise 2: Implementing Storage Space-based volumes

#### Task 1: Attach VHDs to an Azure VM

1. On MIA-CL1, in the Azure portal, on the 20533E0401-LabRG blade, in the list of resources, click **20533E0401-vm2**.
2. On the 20533E0401-vm2 blade, click **Disks**.
3. Click **+ Add data disk**.
4. In the Data disks section, click the drop down list in the NAME column and then click **Create disk**
5. On the Create managed disk blade, specify the following settings and then click **Create**:

* Name: **20533E0401-vm2-data01**
* Resource group: ensure that the **Use existing** option is selected and **20533E0401-LabRG** appears in the drop down list.
* Account type: **Standard HDD**
* Source type: **None (empty disk)**
* Size: **128**

1. Wait for the operation to complete.
2. Back on the 20533E0401-vm2 blade, ensure that the HOST CACHING column contains the **None** entry.
3. Click **+ Add data disk**.
4. In the Data disks section, click the drop down list in the NAME column and then click **Create disk**
5. On the Create managed disk blade, specify the following settings and then click **Create**:

* Name: **20533E0401-vm2-data02**
* Resource group: ensure that the **Use existing** option is selected and **20533E0401-LabRG** appears in the drop down list.
* Account type: **Standard HDD**
* Source type: **None (empty disk)**
* Size: **128**

1. Back on the **20533E0401-vm2 - Disks** blade, ensure that the HOST CACHING column contains the **None** entry and then click **Save**. Wait for the operation to complete.

#### Task 2: Configure a Storage Spaces simple volume

1. On MIA-CL1, in the Azure portal, on the 20533E0401-vm2 virtual machine blade, click **Overview**.
2. In the toolbar, click **Connect**.
3. On the **Connect to virtual machine** blade, click **Download RDP File**. When prompted, click **Open**.
4. If a Remote Desktop Connection warning message displays, select **Don't ask me again for connections to this computer**, and then click **Connect**.
5. In the Windows Security dialog box, type the following credentials, and then click **OK**:

* User name: **Student**
* Password: **Pa55w.rd1234**

1. If another Remote Desktop Message displays, select the **Don't ask me again for connections to this computer** checkbox, and then click **Yes**.
2. If prompted in the Remote Desktop session whether to allow your PC to be discoverable, click **No**.
3. After you establish a Remote Desktop session to the VM, wait for the Server Manager window to open. In the Server Manager window, click **File and Storage Services**.
4. In the navigation pane on the left side, click **Storage Pools**.
5. In the **STORAGE POOLS** pane, click the **TASKS** menu, and then click **New Storage Pool** on the drop-down menu. This will open the New Storage Pool Wizard.
6. On the **Before you begin** page, click **Next**.
7. On the **Specify a storage pool name and subsystem** page, type **StoragePool1** in the **Name** text box, and then click **Next**.
8. On **Select physical disks for the storage pool**, select the check boxes next to the two physical disk entries (which represent disks you attached from the Azure portal), and then click **Next**.
9. On the **Confirm selections** page, click **Create**.
10. On the **View results** page, select the **Create a virtual disk when this wizard closes** check box, and then click **Close**.
11. In the **Select the storage pool** dialog box, ensure that **StoragePool1** is selected and click **OK**. This will launch the New Virtual Disk Wizard.
12. On the **Before you begin** page, click **Next**.
13. On the **Specify the virtual disk name** page, type **VirtualDisk1** in the **Name** text box, and then click **Next**.
14. On the **Enclosure Awareness** page, click **Next**.
15. On the **Select the storage layout** page, click **Simple**, and then click **Next**.
16. On the **Specify the provisioning type** page, ensure that **Fixed** is selected, and then click **Next**.
17. On the **Specify the size of the virtual disk**, select **Maximum size**, and then click **Next**.
18. On the **Confirm selections** page, click **Create**.
19. On the **View results** page, ensure that the **Create a volume when this wizard closes** check box is selected, and then click **Close**. This will open the New Volume Wizard.
20. On the **Before you begin** page, click **Next**.
21. On the **Select the server and disk** page, ensure that **VirtualDisk1** is selected, and then click **Next**.
22. On the **Specify the size of the volume** page, accept the default volume size, and then click **Next**.
23. On the **Assign to a drive letter or folder** page, ensure that the **Drive letter** is set to **F**, and then click **Next**.
24. On the **Select file system settings** page, accept the default settings (NTFS with default allocation unit size), and then click **Next**.
25. On the **Confirm selections** page, click **Create**.
26. On the **Completion** page, click **Close**.
27. From the desktop of 20533E0401-vm2, open File Explorer, and then verify that there is a new drive **F:** available for use.
28. Close the Remote Desktop session to 20533E0401-vm2.

#### Task 3: Remove the lab environment.

1. On MIA-CL1, close all open windows without saving any files.
2. On the taskbar, right-click the **Windows PowerShell** icon, and then click **Run as Administrator**. In the User Account Control dialog box, click **Yes**.
3. Type the following command, and then press **Enter**:

Remove-20533EEnvironment

1. When prompted, sign in by using the Microsoft account that is the Service Administrator of your Azure subscription.
2. If you have multiple Azure subscriptions, select the one you want the script to target.
3. If prompted, specify the current lab number.
4. When prompted for confirmation, type **y**.
5. Start Microsoft Edge, browse to the Azure portal at [**https://portal.azure.com**](https://portal.azure.com), and sign in by using the Microsoft account that is the Service Administrator of your Azure subscription.
6. In the Azure portal, on Dashboard, click **Edit**.
7. Right-click unoccupied area of the dashboard and, in the right-click menu, click **Reset to default state**. When prompted to confirm, click **Yes**.
8. Click **Done customizing**.
9. Close all open windows.

**Result**: After completing this exercise, you should have implemented Storage Space-based volumes

©2016 Microsoft Corporation. All rights reserved.

The text in this document is available under the [Creative Commons Attribution 3.0 License](https://creativecommons.org/licenses/by/3.0/legalcode), additional terms may apply. All other content contained in this document (including, without limitation, trademarks, logos, images, etc.) are **not** included within the Creative Commons license grant. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it. Some examples are for illustration only and are fictitious. No real association is intended or inferred. Microsoft makes no warranties, express or implied, with respect to the information provided here.