Networking

Hands-On Lab

Table of Contents

[Change Log 3](#_Toc526882471)

[Before you Begin 3](#_Toc526882472)

[Virtual Networks 4](#_Toc526882473)

[Log in to Azure 4](#_Toc526882474)

[Create a virtual network 4](#_Toc526882475)

[Create virtual machines 4](#_Toc526882476)

[Create two VMs in the virtual network: Create the first VM 4](#_Toc526882477)

[Create two VMs in the virtual network: Create the second VM 5](#_Toc526882478)

[Connect to a VM from the internet 5](#_Toc526882479)

[Communicate between VMs 5](#_Toc526882480)

[Load Balancer 6](#_Toc526882481)

[Create a Basic load balancer 6](#_Toc526882482)

[Create back-end servers 6](#_Toc526882483)

[Create a virtual network 6](#_Toc526882484)

[Create LBVM1 7](#_Toc526882485)

[Create LBVM2 7](#_Toc526882486)

[Create NSG rules 8](#_Toc526882487)

[Install IIS 10](#_Toc526882488)

[Create resources for the Basic load balancer 10](#_Toc526882489)

[Create a back-end address pool 10](#_Toc526882490)

[Create a health probe 11](#_Toc526882491)

[Create a load balancer rule 12](#_Toc526882492)

[Test the load balancer 12](#_Toc526882493)

[Traffic Manager 13](#_Toc526882494)

[Prerequisites 13](#_Toc526882495)

[Create East US Web App 13](#_Toc526882496)

[Create West US Web App 13](#_Toc526882497)

[Create a Traffic Manager profile 14](#_Toc526882498)

[Add Traffic Manager endpoints 14](#_Toc526882499)

[Test Traffic Manager profile 15](#_Toc526882500)

[Determine the DNS name 15](#_Toc526882501)

[View Traffic Manager in action 15](#_Toc526882502)

[Network Watcher 16](#_Toc526882503)

[Enable network watcher 16](#_Toc526882504)

[Packet Capture and examination 16](#_Toc526882505)

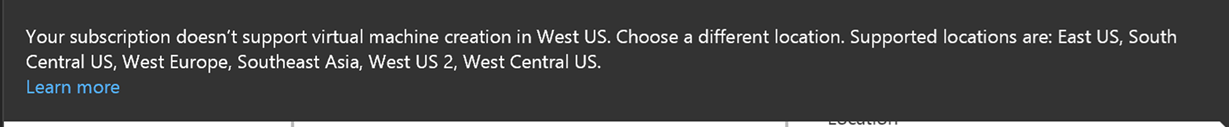
# Change Log

|  |  |  |
| --- | --- | --- |
| Date | Version | Comments |
| October 2018 | 1 | Original Document |

# Before you Begin

If you are using a Microsoft Azure subscription that was provided to you by Microsoft, you are limited to a specific set of Microsoft Azure regions that you can use. **Please use either the East US, South Central US, West Europe, Southeast Asia, West US 2, or West Central US locations.**

Otherwise you will receive the following error in the portal if you select an unsupported region and attempt to build anything in Microsoft Azure.



# Virtual Networks

## Log in to Azure

1. Log in to the Azure portal at [https://portal.azure.com](https://portal.azure.com/).

## Create a virtual network

1. Select **+ Create a resource** on the upper left corner of the Azure portal.
2. Select **Networking**, and then select **Virtual network**.
3. Enter, or select, the following information, accept the defaults for the remaining settings, and then select **Create**:
   1. Name: vNet01
   2. Address Space: 10.0.1.0/24
   3. Resource Group: myVNets
   4. Subnet Name: subnet1
   5. Subnet address range: 10.0.1.0/24

## Create virtual machines

### Create two VMs in the virtual network: Create the first VM

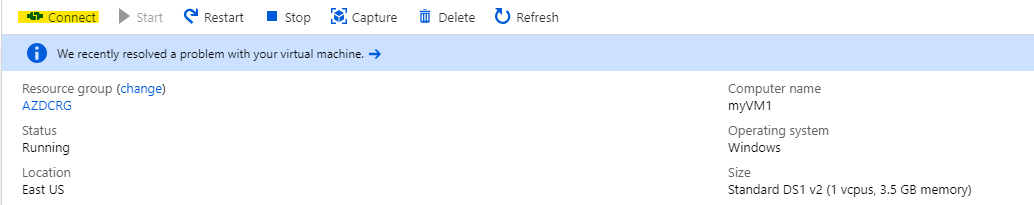
1. Select **+ Create a resource** found on the upper, left corner of the Azure portal.
2. Select **Compute**, and then select **Windows Server 2016 Datacenter**.
3. Enter, or select, the following information, accept the defaults for the remaining settings:
   1. Name: myVM1
   2. Username: *pick a username*
   3. Password: *pick a complex password*
   4. Confirm Password: *pick a complex password*
   5. Public inbound ports: Open RDP
   6. select **Next:Disks**
4. Select **Create and attach a new disk** and then select **OK**. Click **Next: Networking.**
5. Set the virtual network to **vNet01** and then select **Next: Management.**
6. Click **Create new** for diagnostic storage account, enter <yourinitials><shortdate>, ensure the name resolves (e.g. abc1009), **click OK**, and then click **Next: Guest config.**
7. Review the items and then click **Next: Tags.**
8. Review the items and then click **Next: Review + create.**
9. Once validation passes click **Create.**

### Create two VMs in the virtual network: Create the second VM

Complete the previous steps but name the VM myVM2 and use the same diagnostics storage account.

## Connect to a VM from the internet

1. After myVm1 is created, connect to it. At the top of the Azure portal, enter myVm1. When **myVm1** appears in the search results, select it. Select the **Connect** button.



1. After selecting the **Connect** button, click on Download RDP file.
2. If prompted, select **Connect**. Enter the user name and password you specified when creating the VM. You may need to select **More choices**, then **Use a different account**, to specify the credentials you entered when you created the VM.
3. Select **OK**.
4. Click **Yes** on the Networks blade.

### Communicate between VMs

1. From PowerShell, enter ping myvm2. Ping fails, because ping uses the Internet Control Message Protocol (ICMP), and ICMP is not allowed through the Windows firewall, by default.
2. To allow myVm2 to ping myVm1 in a later step, enter the following command from PowerShell, which allows ICMP inbound through the Windows firewall:

New-NetFirewallRule –DisplayName “Allow ICMPv4-In” –Protocol ICMPv4

1. Close the remote desktop connection to myVM1.
2. Complete the steps in [Connect to a VM from the internet](#_Connect_to_a)again, but connect to myVM2. From a command prompt, enter ping myvm1.

You receive replies from myVm1, because you allowed ICMP through the Windows firewall on the myVm1 VM in a previous step.

# Load Balancer

Load balancing provides a higher level of availability and scale by spreading incoming requests across multiple virtual machines (VMs). You can use the Azure portal to create a load balancer that will load balance virtual machines. In this lab you will learn how to create network resources, back-end servers, and a load balancer at the Basic pricing tier.

## Create a Basic load balancer

In this section, you create a public Basic load balancer by using the portal. The public IP address is automatically configured as the load balancer's front end when you create the public IP and the load balancer resource by using the portal. The name of the front end is **myLoadBalancer**.

1. On the upper-left side of the portal, select **Create a resource** > **Networking** > **Load Balancer**.
2. In the **Create load balancer** pane, enter these values:
   * **LB01** for the name of the load balancer
   * **Public** for the type of the load balancer
   * **SKU** set as **Basic**
   * **LBPublicIP** for the public IP with an **Assignment** set as **Dynamic**
   * **LBRG** for the name of the new resource group
3. Select **Create**.

## Create back-end servers

In this section, you create a virtual network, and you create two virtual machines for the back-end pool of your Basic load balancer. Then you install Internet Information Services (IIS) on the virtual machines to help test the load balancer.

### Create a virtual network

1. On the upper-left side of the portal, select **New** > **Networking** > **Virtual network**.
2. In the **Create virtual network** pane, enter these values, and then select **Create**:
   * **LBVnet** for the name of the virtual network
   * **10.1.0.0/16** as the address space
   * **LBRG** for the name of the existing resource group
   * **myBackendSubnet** for the subnet name

### Create LBVM1

1. Select **+ Create a resource** > **Compute**, and then select **Windows Server 2016 Datacenter**.
2. Enter, or select, the following information, accept the defaults for the remaining settings:
   1. Resource Group: LBRG
   2. Name: **LBVM1**
   3. Availability option: choose **Availability set** > **Create New** > **LBAVSet** > **Ok.**
   4. Change the VM size to DS2\_v2 or similar
   5. Username: *pick a username*
   6. Password: *pick a complex password*
   7. Confirm Password: *pick a complex password*
   8. Public inbound ports: Open RDP
   9. select **Next: Disks**
3. Select **Create and attach a new disk** and then select **OK**. Click **Next: Networking.**
4. Set the virtual network to **LBVnet** and then select **Next: Management.**
5. Ensure the diagnostic storage account is set to the previous storage account created and then click **Next: Guest config.**
6. Review the items and then click **Next: Tags.**
7. Review the items and then click **Next: Review + create.**
8. Once validation passes click **Create.**

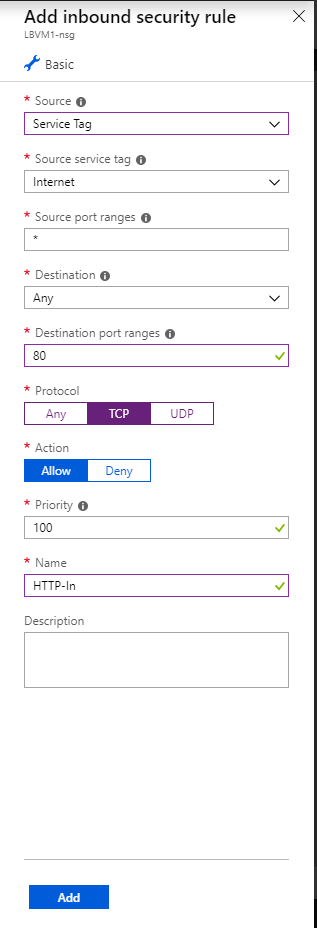
### Create LBVM2

1. By following previous steps 1 to 8, create a second VM named **LBVM2**, with:
   * **LBAVSet** as the availability set.
   * **LBVnet** as the virtual network.
   * **myBackendSubnet** as the subnet.

## Create NSG rules

In this section, you create NSG rules to allow inbound connections that use HTTP and RDP.

1. Select **Resource Groups** on the left menu. From the resource list, select **LBRG** then **LBVM1-nsg**.
2. Under **Settings**, select **Inbound security rules**, and then select **Add**.
3. Enter the following values for the inbound security rule named **myHTTPRule** to allow for inbound HTTP connections that use port 80. Then select **OK**.
   * **Service Tag** for **Source**
   * **Internet** for **Source service tag**
   * **80** for **Destination port ranges**
   * **TCP** for **Protocol**
   * **Allow** for **Action**
   * **100** for **Priority**
   * **HTTP-In** for **Name**
   * **Allow HTTP** for **Description**



1. Repeat the steps except from the resource list, select **LBRG** then **LBVM2-nsg**.

## Install IIS

1. Select **All resources** on the left menu. From the resource list, select **LBVM1** in the **LBRG** resource group.
2. On the **Overview** page, select **Connect** to RDP into the VM.
3. Sign in to the VM with your username and password.
4. Click **Yes** on the Networks blade.
5. In Server Manager, select **Manage**, and then select **Add Roles and features**.
6. In the Add Roles and Features Wizard, use the following values:
   1. On the **Select installation type** page, select **Role-based or feature-based installation**.
   2. On the **Select destination server** page, select **LBVM1**.
   3. On the **Select server role** page, select **Web Server (IIS)** then **Add Features**.
   4. Follow the instructions to complete the rest of the wizard using default settings.
   5. Repeat steps 1 to 6 for the virtual machine **LBVM2**.
7. Once IIS is installed, on each VM edit the default web page by:
   1. In **Server Manager**, click **Tools** then **IIS Manager**
   2. Expand the left tree, right-click on **Default web site,** and then choose **Explore**
   3. Edit the iisstart.html by opening wit with notepad.
   4. Change the <title> line to read: <title>IIS Windows Server LBVM1</title>
   5. Save the file, repeat the same steps for LBVM2 and change the line to state <title>IIS Windows Server LBVM2</title>

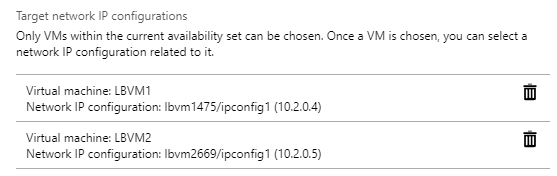
## Create resources for the Basic load balancer

In this section, you configure load balancer settings for a back-end address pool and a health probe. You also specify load balancer and NAT rules.

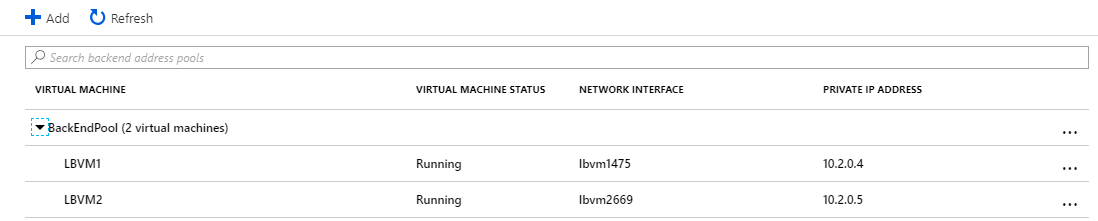
### Create a back-end address pool

To distribute traffic to the VMs, a back-end address pool contains the IP addresses of the virtual NICs that are connected to the load balancer. Create the back-end address pool **myBackendPool** to include **LBVM1** and **LBVM2**.

1. In the Azure portal select **All resources** on the left menu, and then select **LB01** from the resource list.
2. Under **Settings**, select **Backend pools**, and then select **Add**.
3. On the **Add a backend pool** page, do the following, and then select **OK**:
   * For **Name**, enter **BackEndPool**.
   * For **Associated to**, from the drop-down menu, select **Availability set**.
   * For **Availability set**, select **LBAVSet**.
   * Select **Add a target network IP configuration** to add each virtual machine (**myVM1** and **myVM2**) that you created to the back-end pool.



1. Make sure that your load balancer's back-end pool setting displays both the VMs **LBVM1** and **LBVM2**.



### Create a health probe

To allow the Basic load balancer to monitor the status of your app, you use a health probe. The health probe dynamically adds or removes VMs from the load balancer rotation based on their response to health checks. Create a health probe named **LBHP** to monitor the health of the VMs.

1. Under **Settings**, select **Health probes**, and then select **Add**.
2. Use these values, and then select **OK**:
   * **LBHP** for the name of the health probe
   * **HTTP** for the protocol type
   * **80** for the port number
   * **5** for **Interval**, the number of seconds between probe attempts
   * **2** for **Unhealthy threshold**, the number of consecutive probe failures that must occur before a VM is considered unhealthy

### Create a load balancer rule

You use a load balancer rule to define how traffic is distributed to the VMs. You define the frontend IP configuration for the incoming traffic and the back-end IP pool to receive the traffic, along with the required source and destination port.

Create a load balancer rule named **HTTPRule**  for listening to port 80 in the front end **LoadBalancerFrontEnd**. The rule is also for sending load-balanced network traffic to the back-end address pool **myBackEndPool**, also by using port 80.

1. Under **Settings**, select **Load balancing rules**, and then select **Add**.
2. Use these values, and then select **OK**:
   * **HTTPRule** for the name of the load balancer rule
   * **TCP** for the protocol type
   * **80** for the port number
   * **80** for the back-end port
   * **BackendPool** for the name of the back-end pool
   * **LBHP** for the name of the health probe

### Test the load balancer

1. Find the public IP address for the load balancer on the **Overview** screen. Select **All resources**, and then select **LBPublicIP**.
2. Copy the public IP address, and then paste it into the address bar of your browser. The default page of IIS web server is displayed in the browser, noting LBVM1 or LBVM2 as you refresh your browser.
3. Shutdown either LBVM1 or LBVM2. As the VM is shutting down, refresh your browser. Once one of the VMs is down, you should only see the live VM rendering you the default website. You may receive a service unavailable if you refresh during probe attempts.

# Traffic Manager

## Prerequisites

This lab requires that you have deploy two instances of a web application running in different Azure regions (East US and West). The two web application instances serve as primary and backup endpoints for Traffic Manager.

## Create East US Web App

1. On the top left-hand side of the screen, select **Create a resource** > **Web** > **Web App** > **Create**.
2. In **Web App**, enter or select the following information and enter default settings where none are specified:
   1. App name: <yourinitals>EastWebApp (e.g. abcEastWebApp)
   2. Resource Group: (new) EastWebApps
   3. Select App Service Plan:
      1. + Create New: EastWebApps
      2. App Service plan name: <yourinitals>EastAppSvcPlan
      3. Location: **East US**
      4. Click **OK**
3. Select **Create**. A default website is created when the Web App is successfully deployed.

## Create West US Web App

1. On the top left-hand side of the screen, select **Create a resource** > **Web** > **Web App**.
2. In **Web App**, enter or select the following information and enter default settings where none are specified:
   1. App name: <yourinitals>WestWebApp (e.g. abcEastWebApp)
   2. Resource Group: (new) WestWebApps
   3. Select App Service Plan:
      1. + Create New:
      2. App Service plan name: <yourinitals>AppSvcPlan
      3. Location: **West US**
      4. Click **OK**
3. Select **Create**. A default website is created when the Web App is successfully deployed.

## Create a Traffic Manager profile

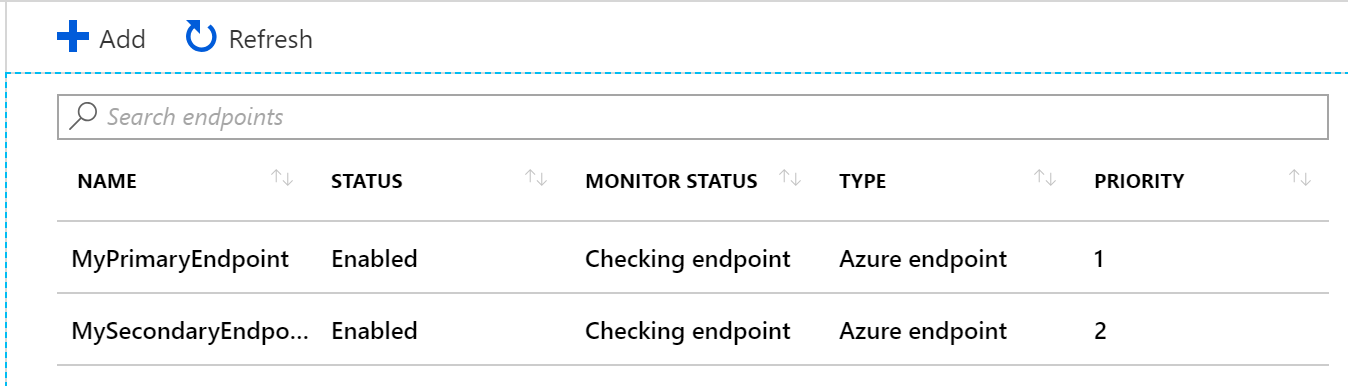
Create a Traffic manager profile that directs user traffic based on endpoint priority.

1. On the top left-hand side of the screen, select **Create a resource** > **Networking** > **Traffic Manager profile**.
2. In the **Create Traffic Manager profile**, enter or select, the following information, accept the defaults for the remaining settings, and then select **Create**:
   1. Name: <yourinitials>TM (This name needs to be unique within the trafficmanager.net zone and results in the DNS name, trafficmanager.net which is used to access your Traffic Manager profile.)
   2. Routing method: Priority
   3. Resource Group: **EastWebApps**

## Add Traffic Manager endpoints

Add the website in the East US as primary endpoint to route all the user traffic. Add the website in West Europe as a backup endpoint. When the primary endpoint is unavailable, traffic is automatically routed to the secondary endpoint.

1. In the portal’s search bar, search for the Traffic Manager profile name that you created in the preceding section and select the profile in the results that the displayed.
2. In **Traffic Manager profile**, in the **Settings** section, click **Endpoints**, and then click **Add**.
3. Enter, or select, the following information, accept the defaults for the remaining settings, and then select **OK**:
   1. Type: Azure endpoint
   2. Name: MyPrimaryEndpoint
   3. Target resource type: App Service
   4. Target Resource: <yourinitals>EastWebApp
   5. Priority: 1
4. Enter, or select, the following information, accept the defaults for the remaining settings, and then select **OK**:
   1. Type: Azure endpoint
   2. Name: MySecondaryEndpoint
   3. Target resource type: App Service
   4. Target Resource: <yourinitals>WestWebApp
   5. Priority: 2



## Test Traffic Manager profile

In this section, you first determine the domain name of your Traffic Manager profile and then view how the Traffic Manager fails over to the secondary endpoint when the primary endpoint is unavailable.

### Determine the DNS name

1. Click **Overview** and the **Traffic Manager profile** displays the DNS name of your newly created Traffic Manager profile.

### View Traffic Manager in action

1. In a web browser, type the DNS name of your Traffic Manager profile to view your Web App's default website. In this lab scenario, all requests are routed to the primary endpoint that is set to **Priority 1**.
2. To view Traffic Manager failover in action, disable your primary site as follows:
   1. In the Traffic Manager Profile page, select **Settings**>**Endpoints**>MyPrimaryEndpoint.
   2. In MyPrimaryEndpoint, select **Disabled**.
   3. The primary endpoint MyPrimaryEndpoint status now shows as **Disabled**.
3. Copy the DNS name of your Traffic Manager Profile from the preceding step to successfully view the website in a web browser. When the primary endpoint is disabled, the user traffic gets routed to the secondary endpoint.

# Network Watcher

To test network communication with Network Watcher, first enable a network watcher in at least one Azure region, and then use Network Watcher's IP flow verify capability.

## Enable network watcher

1. In the portal, select **All services**. In the **Filter box**, enter Network Watcher. When **Network Watcher** appears in the results, select it.
2. Enable a network watcher in the region where you deployed your VMs. Select **Regions**, to expand it, and then select **...** to the right of **East US**.
3. Select **Enable Network Watcher**.

## Packet Capture and examination

1. Under **Network diagnostics tools**, select **Packet Capture**, the **Add**.
2. Enter the following and click **Ok**:
   1. Resource Group: **LBGR**
   2. Target VM: **LBVM1**
   3. Packet Capture Name: **Packets**
   4. Capture configuration: **Storage Account**
   5. Storage Accounts: Select the storage account previously provisioned
3. Find the public IP address for the load balancer **LBPublicIP**.
4. Shutdown LBVM2 and then copy the public IP address and paste it into the address bar of your browser. The default page of IIS web server is displayed in the browser, noting LBVM1 or LBVM2 as you refresh your browser.
5. Stop the packet capture by returning to **Network Watcher** > **Packet Capture** > **Right-Click** > **Stop**.
6. If you click on the .cap file it will display the blob properties. Download the file to your documents folder on your local computer.
7. Install network monitor from the following:
   1. <https://www.microsoft.com/en-US/download/details.aspx?id=4865>
8. Launch Network Monitor and open the capture file from your Documents folder. Examine the contents of your packet capture session.