



Microsoft Cloud Workshop

Load Balancers, Traffic Manager, and Application Gateway
Hands-on lab step-by-step

August 2018

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The names of manufacturers, products, or URLs are provided for informational purposes only and Microsoft makes no representations and warranties, either expressed, implied, or statutory, regarding these manufacturers or the use of the products with any Microsoft technologies. The inclusion of a manufacturer or product does not imply endorsement of Microsoft of the manufacturer or product. Links may be provided to third party sites. Such sites are not under the control of Microsoft and Microsoft is not responsible for the contents of any linked site or any link contained in a linked site, or any changes or updates to such sites. Microsoft is not responsible for webcasting or any other form of transmission received from any linked site. Microsoft is providing these links to you only as a convenience, and the inclusion of any link does not imply endorsement of Microsoft of the site or the products contained therein.

© 2017 Microsoft Corporation. All rights reserved.

Microsoft and the trademarks listed at <https://www.microsoft.com/en-us/legal/intellectualproperty/Trademarks/Usage/General.aspx> are trademarks of the Microsoft group of companies. All other trademarks are property of their respective owners.

Load Balancers, Traffic Manager, & Application Gateways

hands-on lab step-by-step

Abstract and learning objectives

The student will build a series of resources over a few labs that will present a logical network, covering Azure native networking services in Azure. All step-by-step configurations will be done via the portal to build familiarity.

Attendees will be better able to understand all the proper technical terminology surrounding Azure Networking as well as design robust networking in Azure.

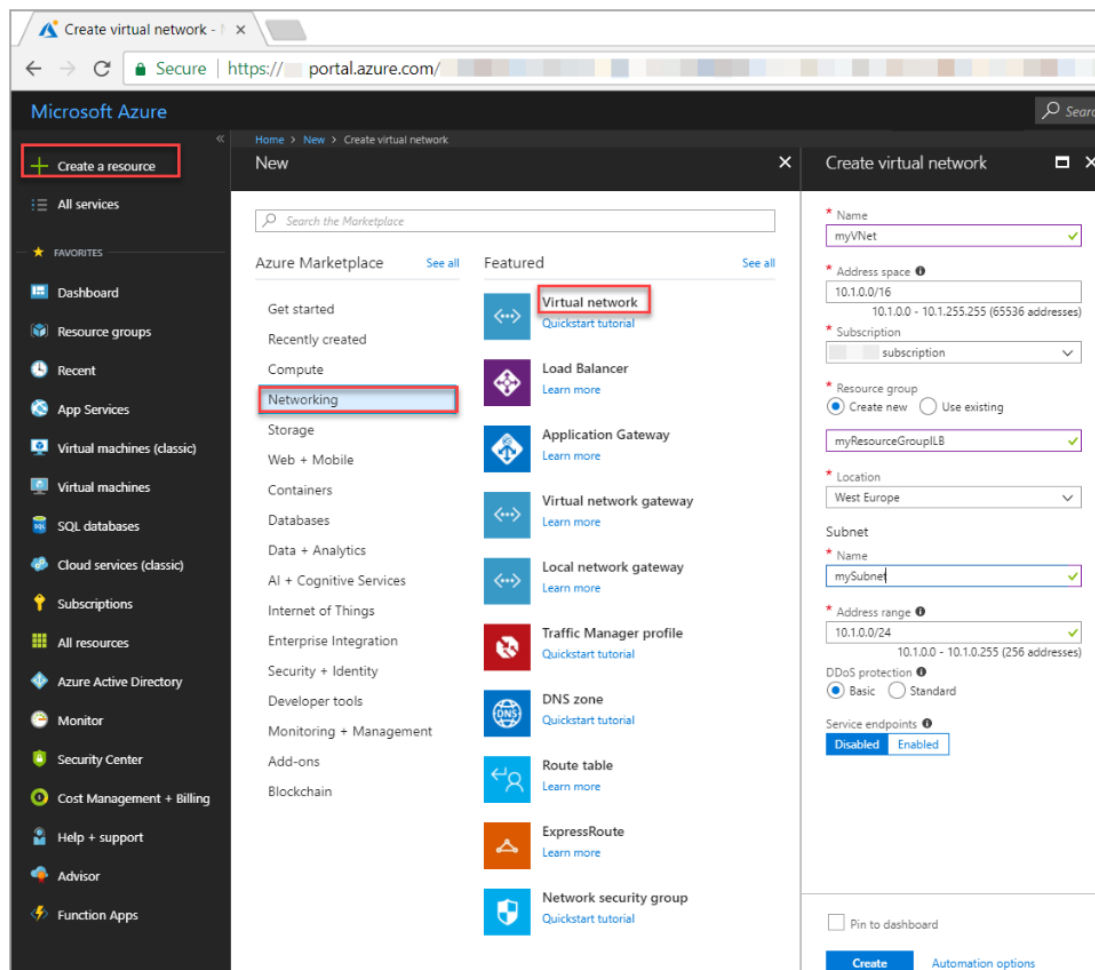
Networking References

- 1) [Azure Virtual Network Overview](#)
- 2) [Azure Virtual Network FAQ](#)
- 3) [IP Addresses](#)
 - a. [Public IP Addresses](#)
 - b. [Internal IP Addresses](#)
- 4) DNS
 - a. [Azure DNS](#)
 - b. [Name Resolution for Azure VNets](#)
- 5) Connectivity for Azure Virtual Networks
 - a. [Site-to-Site VPN](#)
 - b. [VNet-to-VNet VPN](#)
 - c. [Point-to-Site VPN](#)
 - d. [Regional VNet Peering](#)
 - e. [Global VNet Peering](#)
 - f. [ExpressRoute Overview](#)
- 6) Load Balancers
 - a. [Azure Load Balancer](#)
 - b. [Azure Traffic Manager](#)
 - c. [Azure Application Gateway](#)
- 7) Network Security Strategies
 - a. [DMZ Between Azure and On-Premises](#)
 - b. [DMZ Between Azure and the Internet](#)
 - c. [Network Security Groups](#)
 - d. [User Defined Routes](#)
 - e. [Virtual Network Service Tunneling](#)
 - f. [Web Application Firewall](#)
 - g. [Service Endpoints](#)
 - h. [Network Virtual Appliances](#)
- 8) Monitoring
 - a. [Network Watcher](#)
 - b. [Network Performance Monitor Overview](#) & [Solution](#)
 - c. [ExpressRoute Monitor](#)
 - d. [DNS Analytics](#)
 - e. [Service Endpoint Monitoring](#)

Load Balance Internal Traffic with Basic Load Balancer

Task 1: Create a Virtual Network

1. On the top left-hand side of the screen click **New > Networking > Virtual network** and enter these values for the virtual network:
 - *myVnet* - for the name of the virtual network.
 - *myResourceGroupILB* - for the name of the existing resource group
 - *myBackendSubnet* - for the subnet name.
2. Click **Create** to create the virtual network.



Task 2: Create a Basic Load Balancer

Create an internal Basic Load Balancer using the portal.

1. On the top left-hand side of the screen, click **Create a resource > Networking > Load Balancer**.
2. In the **Create a load balancer** page enter these values for the load balancer:
 - *myLoadBalancer* - for the name of the load balancer.

- **Internal** - for the type of the load balancer.
 - **Basic** - for SKU version.
 - **10.1.0.7** - for the static private IP address.
 - *myVNet* - for virtual network that you choose from the list of existing networks.
 - *mySubnet* - for subnet that you choose from the list of existing subnets.
 - *myResourceGroupILB* - for the name of the new resource group that you create.
3. Click **Create** to create the load balancer.

Task 3: Create Backend Servers

1. On the top left-hand side of the screen, click **Create a resource** > **Compute** > **Windows Server 2016 Datacenter** and enter these values for the virtual machine:
 - *myVM1* - for the name of the virtual machine.
 - *azureuser* - for the administrator user name.
 - *myResourceGroupILB* - for **Resource group**, select **Use existing**, and then select *myResourceGroupILB*.
2. Click **OK**.
3. Select **DS1_V2** for the size of the virtual machine, and click **Select**.
4. Enter these values for the VM settings:
 - *myAvailabilitySet* - for the name of the new Availability set that you create.
 - *myVNet* - ensure it is selected as the virtual network.
 - *myBackendSubnet* - ensure it is selected as the subnet.
5. Under **Network Security Group**, select **Advanced**. Next, for **Network security group (firewall)**, select **None**.
6. Click **Disabled** to disable boot diagnostics.
7. Click **OK**, review the settings on the summary page, and then click **Create**.
8. Using steps 1-6, create a second VM, named, *VM2* with *myAvailabilityset* as the Availability set, *myVnet* as the virtual network, *myBackendSubnet* as subnet, and select **None** for the **Network security group (firewall)**.

Task 4: Install IIS and Customize Default Web Page

1. Click **All resources** in the left-hand menu, and then from the resources list click **myVM1** that is located in the *myResourceGroupILB* resource group.
2. On the **Overview** page, click **Connect** to RDP into the VM.
3. Log into the VM.
4. On the server desktop, navigate to **Windows Administrative Tools > Server Manager**.
5. Launch Windows PowerShell on VM1 and using the following commands to install IIS server and update the default htm file.

```
# Install IIS
Install-WindowsFeature -Name Web-Server -IncludeManagementTools

# Remove default htm file
Remove-Item C:\inetpub\wwwroot\iisstart.htm

#Add custom htm file
Add-Content -Path "C:\inetpub\wwwroot\iisstart.htm" -Value $("Hello World from " +
$env:computername)
```

6. Repeat steps 1-5 with *myVM2* to install IIS and customize the default web page.

Task 5: Create a Backend Address Pool

To distribute traffic to the VMs, a back-end address pool contains the IP addresses of the virtual (NICs) connected to the load balancer. Create the backend address pool *ajgBackendPool* to include *VM1* and *VM2*.

1. Click **All resources** in the left-hand menu, and then click **myLoadBalancer** from the resources list.
2. Under **Settings**, click **Backend pools**, then click **Add**.
3. On the **Add a backend pool** page, do the following:
 - For name, type *myBackEndPool*, as the name for your backend pool.
 - For **Associated to**, from the drop-down menu, click **Availability set**
 - For **Availability set**, click, **myAvailabilitySet**.
 - Click **Add a target network IP configuration** to add each virtual machine (*myVM1* & *myVM2*) that you created to the backend pool.
 - Click **OK**.

Home > Resource groups > myResourceGroupILB > myLoadBalancer - Backend pools > Add backend pool

Add backend pool
myLoadBalancer

* Name
myBackendPool ✓

IP version ⓘ
IPv4

Associated to ⓘ
Availability set

Availability set ⓘ
myAvailabilitySet
number of virtual machines: 2

Target network IP configurations
Only VMs within the current availability set can be chosen. Once a VM is chosen, you can select a network IP configuration related to it.

Virtual machine: myVM1
Network IP configuration: myvm1129/ipconfig1 (10.1.0.4)

* Target virtual machine ⓘ
myVM2
size: Standard_DS1_v2, network interfaces: 1

* Network IP configuration ⓘ
ipconfig1 (10.1.0.5)

+ Add a target network IP configuration

OK

1. Check to make sure your load balancer backend pool setting displays both the VMs **VM1** and **VM2**.

Task 6: 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 *myHealthProbe* to monitor the health of the VMs.

1. Click **All resources** in the left-hand menu, and then click **myLoadBalancer** from the resources list.
2. Under **Settings**, click **Health probes**, then click **Add**.
3. Use these values to create the health probe:
 - *myHealthProbe* - for the name of the health probe.
 - **HTTP** - for the protocol type.

- 80 - for the port number.
- 15 - for number of **Interval** in seconds between probe attempts.
- 2 - for number of **Unhealthy threshold** or consecutive probe failures that must occur before a VM is considered unhealthy.

4. Click **OK**.

Home > myLoadBalancer - Health probes > Add health probe

Add health probe
myLoadBalancer

* Name
myHealthProbe ✓

IP version
IPv4

Protocol
HTTP TCP

* Port
80

* Path ⓘ
Healthprobe.aspx ✓

* Interval ⓘ
15 ✓
seconds

* Unhealthy threshold ⓘ
2
consecutive failures

OK

Task 7: Create a Load Balancer Rule

A Load Balancer rule is used to define how traffic is distributed to the VMs. You define the front-end 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 *myLoadBalancerRuleWeb* for listening to port 80 in the frontend *LoadBalancerFrontEnd* and sending load-balanced network traffic to the backend address pool *myBackEndPool* also using port 80.

1. Click **All resources** in the left-hand menu, and then click **myLoadBalancer** from the resources list.
2. Under **Settings**, click **Load balancing rules**, then click **Add**.
3. Use these values to configure the load balancing rule:
 - *myHTTPRule* - for the name of the load balancing rule.
 - **TCP** - for the protocol type.
 - 80 - for the port number.

- 80 - for the backend port.
- *myBackendPool* - for the name of the backend pool.
- *myHealthProbe* - for the name of the health probe.

4. Click **OK**.

Home > myLoadBalancer - Load balancing rules > Add load balancing rule

Add load balancing rule

myLoadBalancer

* Name
myHTTPRule

* IP Version
☒ IPv4 ☐ IPv6

* Frontend IP address
LoadBalancerFrontEnd

Protocol
☒ TCP ☐ UDP

* Port
80

* Backend port
80

Backend pool
myBackendPool (2 virtual machines)

Health probe
myHealthProbe (HTTP:80/Healthprobe.aspx)

Session persistence
None

Idle timeout (minutes)
4

Floating IP (direct server return)
 Disabled Enabled

OK

Task 7: Create a Virtual Machine to Test the Load Balancer

In order to test the internal load balancer, you must create a virtual machine that is located in the same virtual network as the backend server VMs.

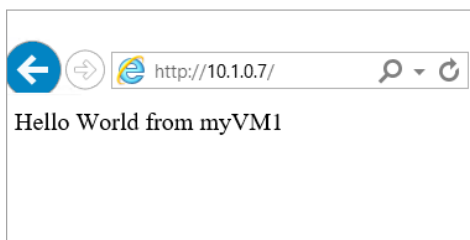
1. On the top left-hand side of the screen, click **Create a resource** > **Compute** > **Windows Server 2016 Datacenter** and enter these values for the virtual machine:
 - *myVMTest* - for the name of the virtual machine.
 - *myResourceGroupILB* - for **Resource group**, select **Use existing**, and then select *myResourceGroupILB*.
2. Click **OK**.
3. Select **DS1_V2** for the size of the virtual machine, and click **Select**.
4. Enter these values for the VM settings:
 - *myVNet* - ensure it is selected as the virtual network.
 - *myBackendSubnet* - ensure it is selected as the subnet.

5. Click **Disabled** to disable boot diagnostics.
6. Click **OK**, review the settings on the summary page, and then click **Create**.

Task 8: Use Virtual Machine to Test the Load Balancer

1. In the Azure portal, get the Private IP address for the Load Balancer on the **Overview** screen. To do so: a. Click **All resources** in the left-hand menu, and then click **myLoadBalancer** from the resources list. b. In the **Overview** details page, copy the Private IP address (in this example, it is 10.1.0.7).
2. Create a remote connection to *myVMTest* as follows: a. Click **All resources** in the left-hand menu, and then from the resources list click **myVMTest** that is located in the *myResourceGroup/LB* resource group.
3. On the **Overview** page, click **Connect** to start a remote session with the VM.
4. Log into the *myVMTest*.
5. Paste the Private IP address into the address bar of the browser in *myVMTest*. The default page of IIS Web server is displayed on the browser.

To see the load balancer distribute traffic across both VMs running your app, you can force-refresh your web browser.



Task 9: Clean up resources

When no longer needed, delete the resource group, load balancer, and all related resources. To do so, select the resource group that contains the load balancer and click **Delete**.

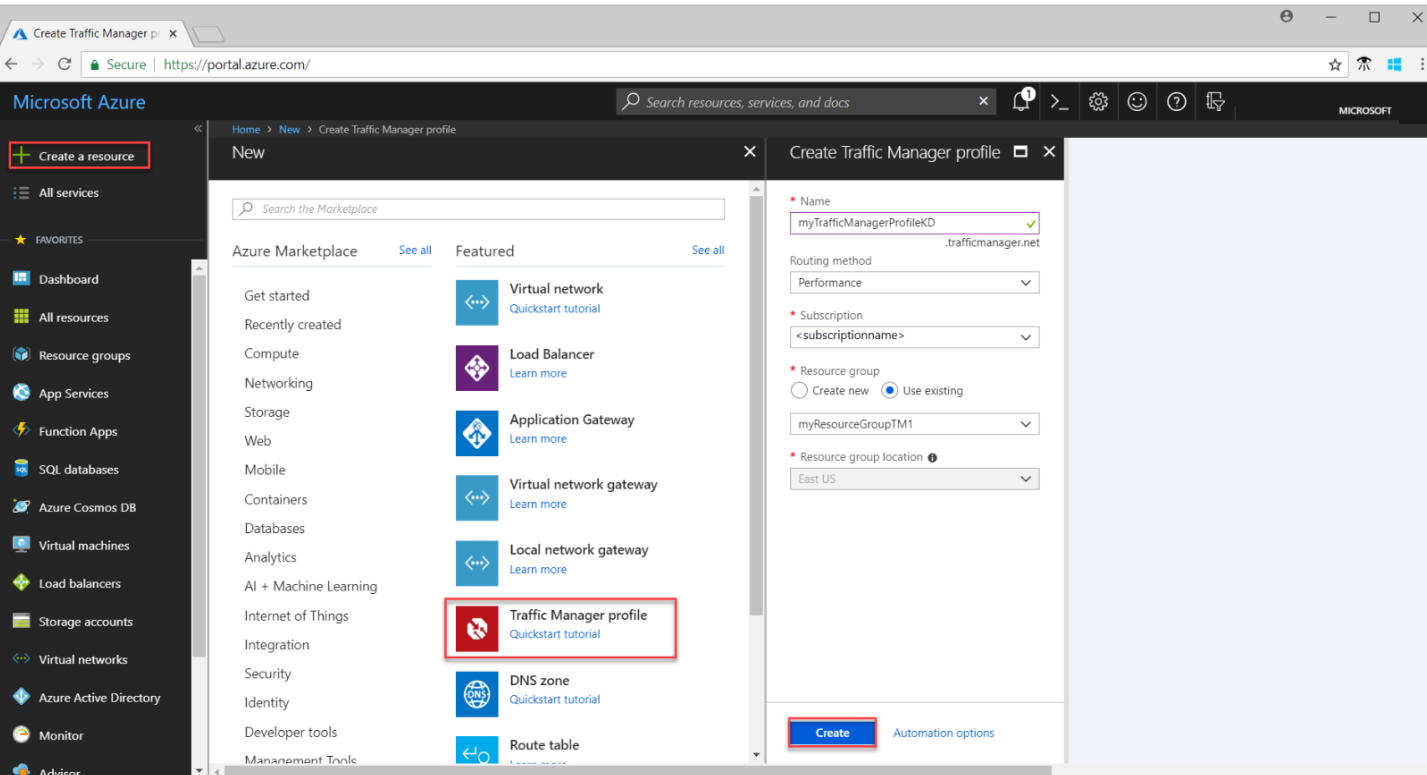
Create a Traffic Manager Profile for a Highly Available Web Application

Task 1: 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 > Create**.
2. In the **Create Traffic Manager profile**, enter or select, the following information, accept the defaults for the remaining settings, and then select **Create**:

Setting	Value
Name	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.
Routing method	Select the Priority routing method.
Subscription	Select your subscription.
Resource group	Select Existing and then select <i>myResourceGroupTM1</i> .
Location	This setting refers to the location of the resource group and has no impact on the Traffic Manager profile that will be deployed globally.



Task 2: 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**:

Setting	Value
Type	Azure endpoint
Name	myPrimaryEndpoint
Target resource type	App Service

Setting	Value
Target resource	Choose an app service to show the listing of the Web Apps under the same subscription. In Resource , pick the App service that you want to add as the first endpoint.
Priority	Select 1 . This results in all traffic going to this endpoint if it is healthy.

- Repeat steps 2 and 3 for the next Web Apps endpoint. Make sure to add it with its **Priority** value set at **2**.
- When the addition of both endpoints is complete, they are displayed in **Traffic Manager profile** along with their monitoring status as **Online**.

Search resources

Home > myTrafficManagerProfileKD - Endpoints > Add endpoint

Add endpoint
myTrafficManagerProfileKD

Type ⓘ
Azure endpoint

* Name
myPrimaryEndpoint ✓

Target resource type
App Service

* Target resource
myWebAppEastUSKD >

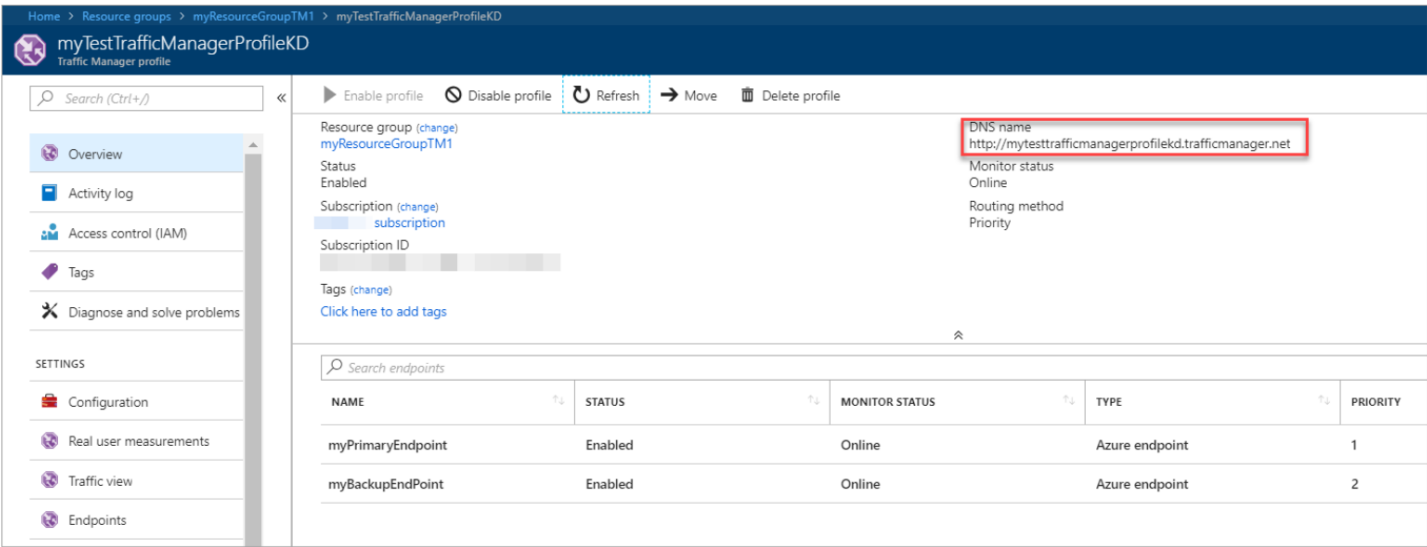
* Priority
1

☐ Add as disabled

OK

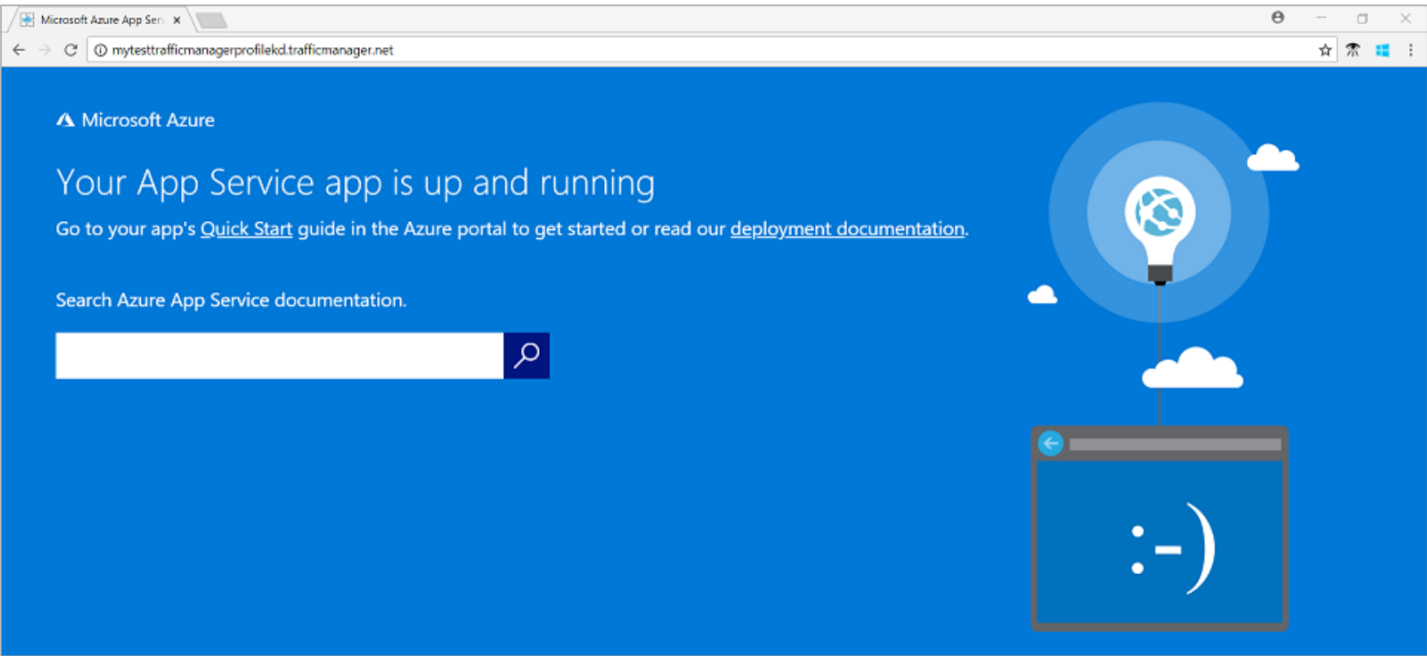
Task 3: Determine the DNS Name

- In the portal's search bar, search for the **Traffic Manager profile** name that you created in the preceding section. In the results that are displayed, click the traffic manager profile.
- Click **Overview**.
- The **Traffic Manager profile** displays the DNS name of your newly created Traffic Manager profile.



Task 4: 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 quickstart scenario, all requests are routed to the primary endpoint that is set to **Priority 1**.



- 1. To view Traffic Manager failover in action, disable your primary site as follows:
 - a. In the Traffic Manager Profile page, select **Settings>Endpoints>MyPrimaryEndpoint**.
 - b. In *MyPrimaryEndpoint*, select **Disabled**.
 - c. The primary endpoint *MyPrimaryEndpoint* status now shows as **Disabled**.

2. 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.

Task 5: Clean up Resources

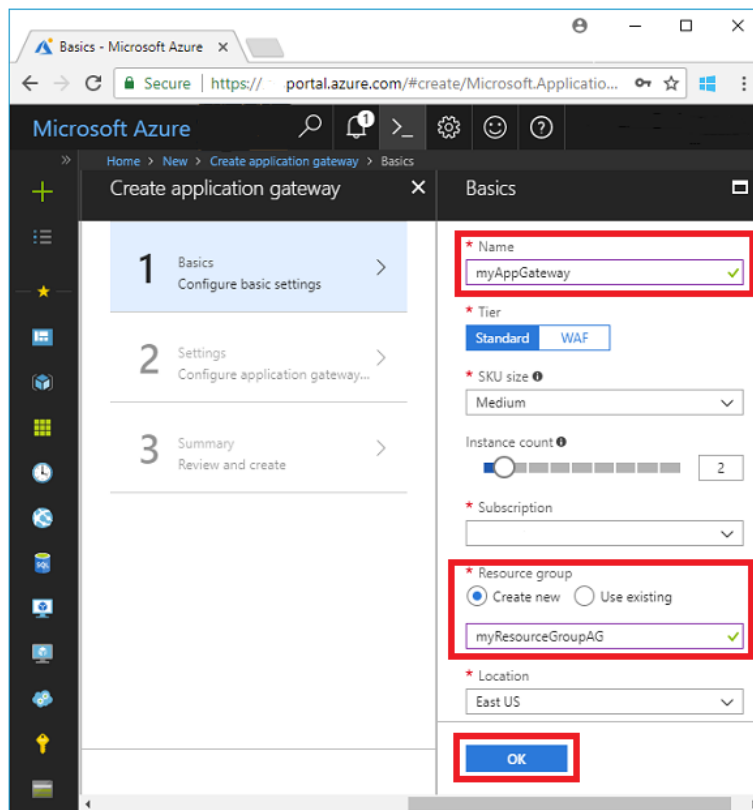
When no longer needed, delete the resource groups, web applications, and all related resources. To do so, select the resource groups (*myResourceGroupTM1* and *myResourceGroupTM2*) and click **Delete**.

Direct Web Traffic with Azure Application Gateway

Task 1: Create an Application Gateway

You need to create a virtual network for the application gateway to be able to communicate with other resources. You can create a virtual network at the same time that you create the application gateway. Two subnets are created in this example: one for the application gateway, and the other for the virtual machines.

1. Click **Create a resource** found on the upper left-hand corner of the Azure portal.
2. Select **Networking** and then select **Application Gateway** in the Featured list.
3. Enter these values for the application gateway:
 - *myAppGateway* - for the name of the application gateway.
 - *myResourceGroupAG* - for the new resource group.



4. Accept the default values for the other settings and then click **OK**.
5. Click **Choose a virtual network** > **Create new**, and then enter these values for the virtual network:
 - *myVNet* - for the name of the virtual network.
 - *10.0.0.0/16* - for the virtual network address space.
 - *myAGSubnet* - for the subnet name.
 - *10.0.0.0/24* - for the subnet address space.

Create virtual network

* Name
myVNet ✓

* Address space
10.0.0.0/16
10.0.0.0 - 10.0.255.255 (65536 addresses) ✓

* Subnet name
myAGSubnet ✓

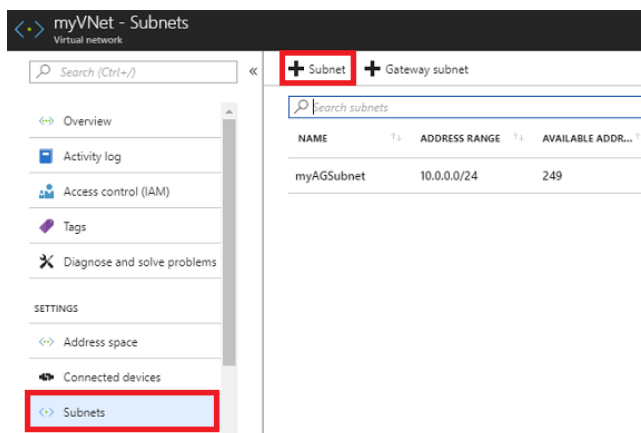
* Subnet address range ⓘ
10.0.0.0/24
10.0.0.0 - 10.0.0.255 (256 addresses)

OK

- Click **OK** to create the virtual network and subnet.
- Click **Choose a public IP address > Create new**, and then enter the name of the public IP address. In this example, the public IP address is named *myAGPublicIPAddress*. Accept the default values for the other settings and then click **OK**.
- Accept the default values for the listener configuration, leave the web application firewall disabled, and then click **OK**.
- Review the settings on the summary page, and then click **OK** to create the virtual network, the public IP address, and the application gateway. It may take up to 30 minutes for the application gateway to be created, wait until the deployment finishes successfully before moving on to the next section.

Task 2: Add a Subnet

- Click **All resources** in the left-hand menu, and then click **myVNet** from the resources list.
- Click **Subnets > Subnet**.



- Enter *myBackendSubnet* for the name of the subnet and then click **OK**.

Task 3: Create Backend Servers

In this example, you create two virtual machines to be used as backend servers for the application gateway.

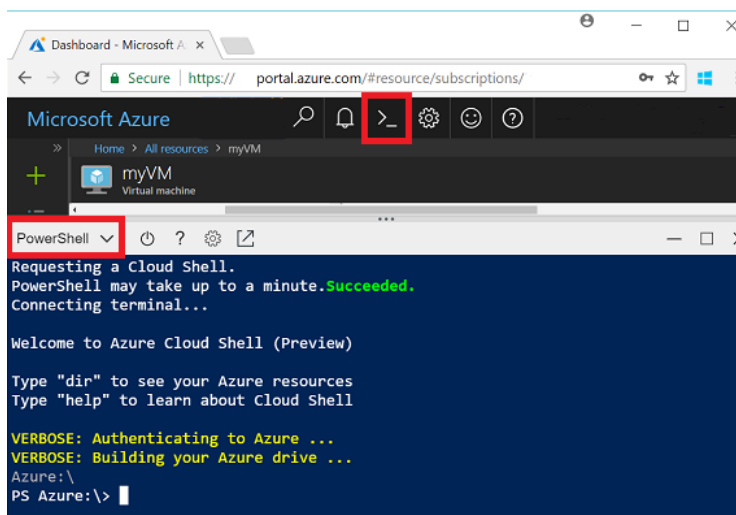
Create a Virtual Machine

1. Click **New**.
2. Select **Compute** and then select **Windows Server 2016 Datacenter** in the Featured list.
3. Enter these values for the virtual machine:
 - *myVM* - for the name of the virtual machine.
 - *azureuser* - for the administrator user name.
 - *Azure123456!* for the password.
 - Select **Use existing**, and then select *myResourceGroupAG*.
4. Click **OK**.
5. Select **DS1_V2** for the size of the virtual machine and then click **Select**.
6. Make sure that **myVNet** is selected for the virtual network and the subnet is **myBackendSubnet**.
7. Click **Disabled** to disable boot diagnostics.
8. Click **OK**, review the settings on the summary page, and then click **Create**.

Install IIS

You install IIS on the virtual machines to verify that the application gateway was successfully created.

1. Open the interactive shell and make sure that it is set to **PowerShell**.



2. Run the following command to install IIS on the virtual machine:

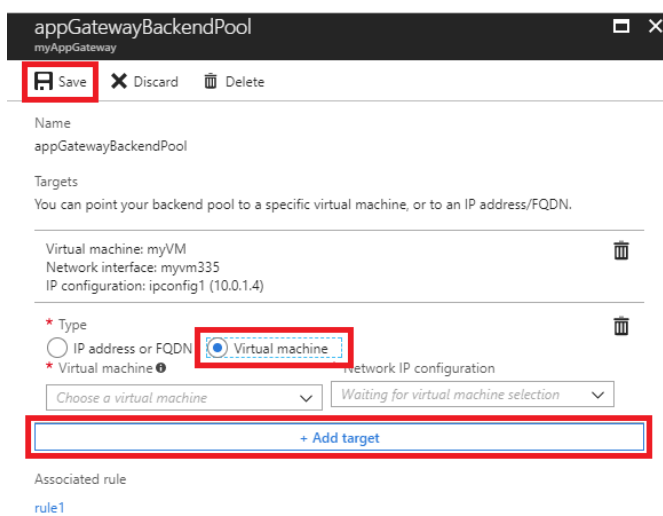
```
Set-AzureRmVMExtension `
  -ResourceGroupName myResourceGroupAG `
  -ExtensionName IIS `
  -VMName myVM `
  -Publisher Microsoft.Compute `
  -ExtensionType CustomScriptExtension `
  -TypeHandlerVersion 1.4 `
  -SettingString '{"commandToExecute":"powershell Add-WindowsFeature Web-Server; powershell Add-Content -Path \"C:\\inetpub\\wwwroot\\Default.htm\" -Value $($env:computername)"}' `
  -Location EastUS
```

3. Create a second virtual machine and install IIS using the steps that you just finished. Enter *myVM2* for its name and for VMName in Set-AzureRmVMExtension.

Add Backend Servers

After you create the virtual machines, you need to add them to the backend pool in the application gateway.

1. Click **All resources** > **myAppGateway**.
2. Click **Backend pools**. A default pool was automatically created with the application gateway. Click **appGatewayBackendPool**.
3. Click **Add target** > **Virtual machine**, and then select *myVM*. Select **Add target** > **Virtual machine**, and then select *myVM2*.

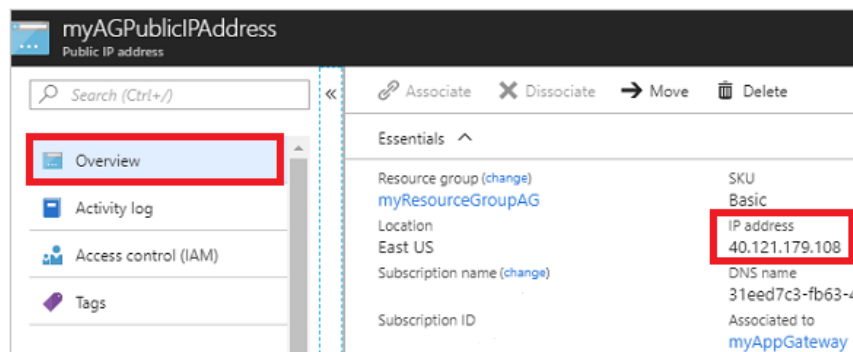


4. Click **Save**.

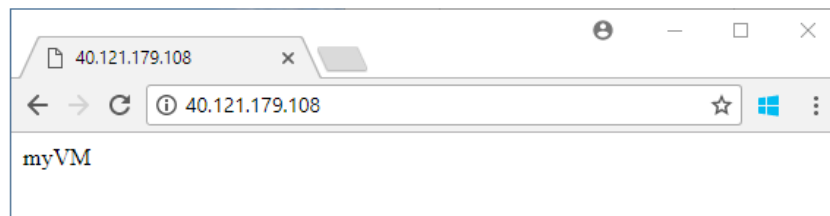
Task 4: Test the Application Gateway

Installing IIS is not required to create the application gateway, but you installed it in this quickstart to verify whether the application gateway was successfully created.

1. Find the public IP address for the application gateway on the Overview screen. Click **All resources** > **myAGPublicIPAddress**.



2. Copy the public IP address, and then paste it into the address bar of your browser.



When you refresh the browser, you should see the name of the other VM appear.

Task 4: Clean Up Resources

First explore the resources that were created with the application gateway, and then when no longer needed, you can delete the resource group, application gateway, and all related resources. To do so, select the resource group that contains the application gateway and click **Delete**.