

Module 7: Assignment- 2

Tasks To Be Performed:

Create an application gateway with the following configuration:

- /vm1 should point to VM1
- /vm2 should point to VM2

The screenshot shows the Microsoft Azure portal interface. The left sidebar contains the navigation menu with options like Virtual machines, Network settings, Load balancing, Application security groups, Network manager, Settings, Disks, Extensions + applications, Configuration, Advisor recommendations, Properties, Locks, Availability + scale, and Size. The main content area displays the 'vm1 | Network settings' page. The 'Essentials' section shows the network interface 'vm1555_x1' with its configuration details: Virtual network/subnet (v-net-AGW / subnet1), Public IP address (20.40.40.151), Private IP address (10.1.1.4), and Admin security rules (0). The 'Rules' section shows the network security group 'vm1-nsg' with its inbound port rules. The rules table is as follows:

Priority	Name	Port	Protocol	Source	Destination	Action
300	SSH	22	TCP	Any	Any	Allow
320	HTTP	80	TCP	Any	Any	Allow
65000	AllowVirtualNetwork	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Module 7: Assignment- 2

The image displays two screenshots of the Microsoft Azure portal interface, showing the configuration of a virtual machine (VM) and an Application Gateway (AppGW).

Top Screenshot: Virtual machines | Network settings

The left sidebar shows the navigation menu with "Virtual machines" selected. The main content area displays the "vm2 | Network settings" page. The "Network interface / IP configuration" section shows the primary network interface "vm2956_e1" attached to the VM. The "Rules" section shows the "Network security group vm2-nsg" attached to the network interface. The "Inbound port rules" table lists the following rules:

Priority	Name	Port	Protocol	Source	Destination	Action
300	SSH	22	TCP	Any	Any	Allow
320	HTTP	80	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Bottom Screenshot: Load balancing | Application Gateway

The left sidebar shows the navigation menu with "Load balancing | Application Gateway" selected. The main content area displays the "AppGW" page. The "Overview" section shows the "AppGW" resource. The "Configuration" section shows the "Frontend IP configurations" and "Backend settings". The "Monitoring" section shows the "Sum Total Requests" and "Sum Failed Requests" graphs. The "Sum Total Requests" graph shows a peak of approximately 100 requests per second. The "Sum Failed Requests" graph shows a peak of approximately 10 failed requests per second.

Module 7: Assignment- 2

The screenshot shows the 'Edit backend pool' page in the Microsoft Azure portal. The page title is 'Edit backend pool'. Below the title, there is a description: 'A backend pool is a collection of resources to which your application gateway can send traffic. A backend pool can contain virtual machines, virtual machines scale sets, IP addresses, domain names, or an App Service.' The 'Name' field is set to 'backendpool'. The 'Add backend pool without targets' toggle is set to 'No'. Under 'Backend targets', there are 2 items. The first item is a 'Virtual machine' with target 'vm1555_z1'. The second item is a 'Virtual machine' with target 'vm2958_z1'. The 'Associated rule' is set to 'virtualmachine'. At the bottom, there are 'Save' and 'Cancel' buttons.

The screenshot shows the 'AppGW | Listeners' page in the Microsoft Azure portal. The page title is 'AppGW | Listeners'. The left sidebar shows the 'Load balancing | Application Gateway' section with 'AppGW' selected. The main content area shows the 'Listeners' tab. There is a table with the following data:

Name	Port	Protocol	Frontend IP	Associated rule	Host name
listenrv1	80	HTTP	Public	virtualmachine	> -

Below the table, there is a section for 'SSL Policy'. It states: 'The SSL policy defines the SSL protocol version and available ciphers. Choose from one of the predefined policies or create a custom security policy to match your organizational security requirements. These policies apply to all HTTPS listeners unless they are overridden by listener specific SSL Policy under SSL settings. Learn more about SSL policy.' The 'Selected SSL Policy: Default (change)' is shown. The 'Min protocol version' is 'TLSv1.2'. The 'Cipher suites' are listed as follows:

- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

Module 7: Assignment- 2

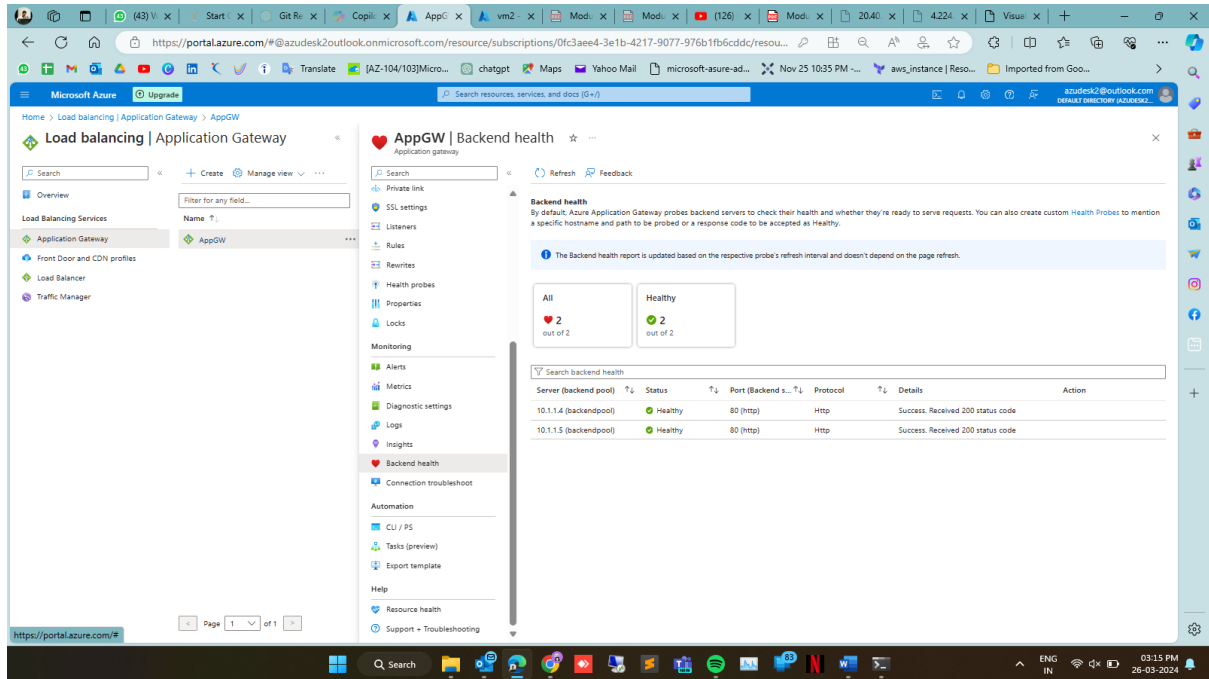
The screenshot shows the Microsoft Azure portal interface. The left sidebar contains the 'Load balancing | Application Gateway' section with options like 'Overview', 'Application Gateway', 'Front Door and CDN profiles', 'Load Balancer', and 'Traffic Manager'. The main content area is titled 'AppGW | Rules' and shows a table of rules. The table has columns for Name, Type, Listener, and Priority. One rule is listed: 'virtualmachine' with Type 'Basic' and Listener 'listenervm1'.

Name	Type	Listener	Priority
virtualmachine	Basic	listenervm1	10

The screenshot shows the Microsoft Azure portal interface. The left sidebar contains the 'Load balancing | Application Gateway' section with options like 'Overview', 'Application Gateway', 'Front Door and CDN profiles', 'Load Balancer', and 'Traffic Manager'. The main content area is titled 'AppGW | Backend settings' and shows a table of backend settings. The table has columns for Name, Port, Protocol, Cookie based affinity, and Custom probe. One setting is listed: 'http' with Port '80' and Protocol 'Http'.

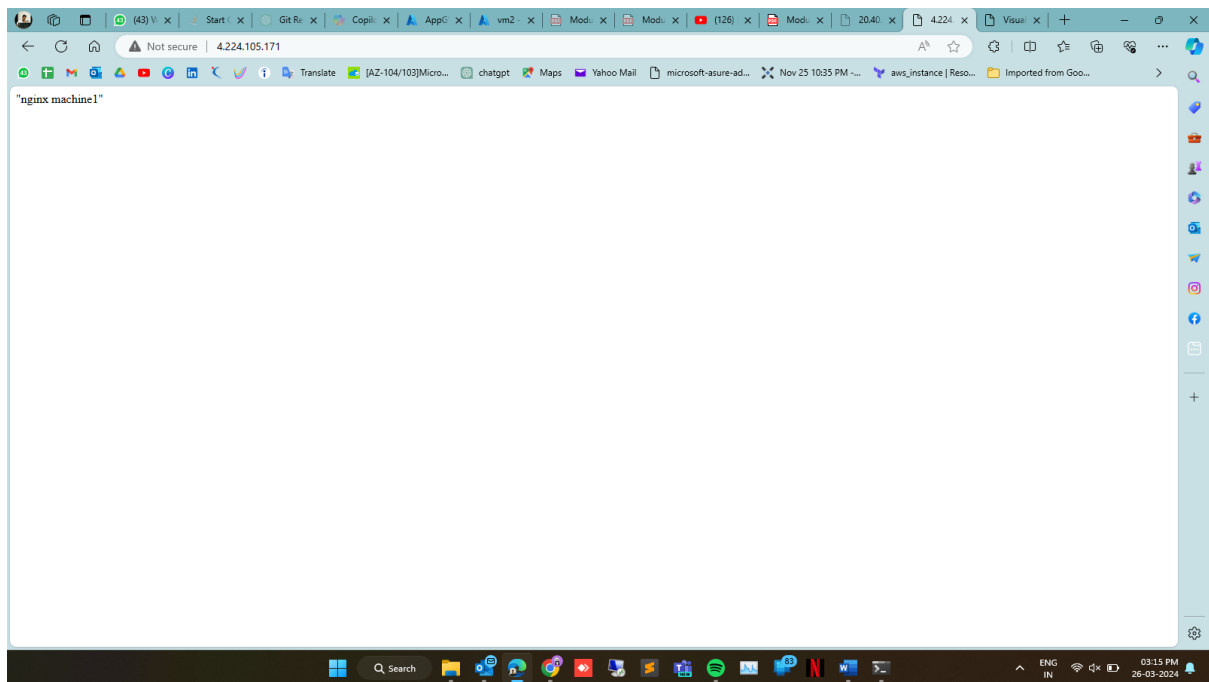
Name	Port	Protocol	Cookie based affinity	Custom probe
http	80	Http	Disabled	-

Module 7: Assignment- 2



Enter frontend ip in browser.

Reload the webpage



Module 7: Assignment- 2

