

Microsoft Cloud Workshop

Building an IaaS Architecture

September 2018

© 2017 Microsoft Corporation. All rights reserved. This document is confidential and proprietary to Microsoft. Internal use only. This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.

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.

Contents

Microsoft Cloud Workshop (MCW)	4
Building an IaaS Architecture	4
Overview and key objectives.....	4
Help references	4
Architecture.....	5
Used Services.....	5
Exercise 1: Environment Setup.....	7
Task 1: Create the Virtual Network in Region 1	7
Task 2: Create a Windows Jump Box system in Region 1.....	9
Exercise 2: Prepare the infrastructure Region 1	11
Task 1: Create Webserver VMs	11
Task 2: Create internal Loadbalancer	14
Task 3: Create Application Gateway.....	18
Task 4: Configure Backups of IaaS Servers	23

Microsoft Cloud Workshop (MCW)

This hands-on lab is based on content provided by the Microsoft Cloud Workshop (MCW) project. You can find more labs at <https://github.com/Microsoft/MCW>

Building an IaaS Architecture

Overview and key objectives

In the Infrastructure track you are building a architecture from ground up on Microsoft Azure. The session is focused on IaaS deployments and will cover Business Continuity and Disaster Recovery aspects as well. In the end you are able to understand key concept for designing a high availability architecture in the cloud.

Key objectives in the hackathon:

- Virtual Networks
- Virtual Machine deployment and Availability Sets
- Securing Network access with network security groups and Layer 7 firewall
- Load balancing (Layer 4 / DNS based)
- Backup

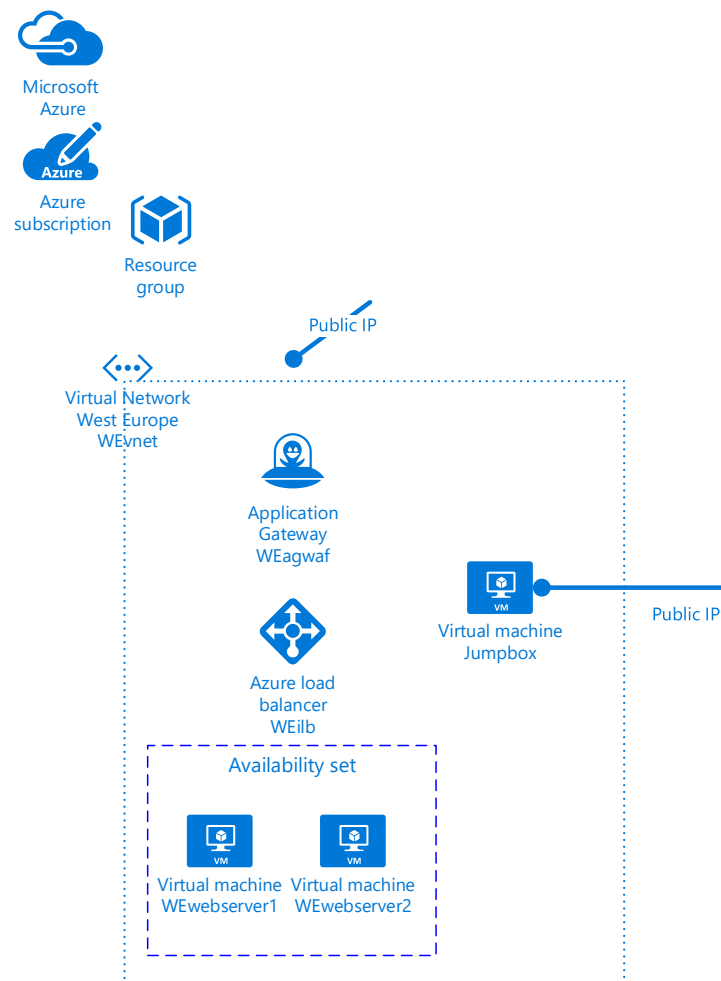
Help references

Please choose the nearest paired region for your deployment. In this hackathon we are using West Europe as primary region 1 and North Europe as region 2

<https://docs.microsoft.com/en-us/azure/best-practices-availability-paired-regions>

Tip: You have to create a lot of different services during this hackathon. Use the bold text to search for the service. Example: Create the second **Virtual Network**

Architecture



Used Services

Virtual network

The Microsoft Azure Virtual Network service enables Azure resources to securely communicate with each other in a virtual network. A virtual network is a logical isolation of the Azure cloud dedicated to your subscription. You can connect virtual networks to other virtual networks, or to your on-premises network.

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview>

Virtual Machine

Microsoft Azure provides a scalable computing platform that allows you to only pay for what you use, when you want it - without having to invest in on-premises hardware. Azure is ready when you are to scale your solutions up and out to whatever scale you require to service the needs of your clients.

<https://docs.microsoft.com/en-us/azure/virtual-machines/linux/overview>

Loadbalancer

Azure Load Balancer delivers high availability and network performance to your applications. It is a Layer 4 (TCP, UDP) load balancer that distributes incoming traffic among healthy instances of services defined in a load-balanced set.

<https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview>

Application Gateway

Microsoft Azure Application Gateway is a dedicated virtual appliance providing application delivery controller (ADC) as a service. It offers various layer 7 load balancing capabilities for your application. It allows customers to optimize web farm productivity by offloading CPU intensive SSL termination to the application gateway. It also provides other layer 7 routing capabilities including round robin distribution of incoming traffic, cookie-based session affinity, URL path-based routing, and the ability to host multiple websites behind a single Application Gateway. A web application firewall (WAF) is also provided as part of the application gateway WAF SKU. It provides protection to web applications from common web vulnerabilities and exploits. Application Gateway can be configured as internet facing gateway, internal only gateway, or a combination of both.

<https://docs.microsoft.com/en-us/azure/application-gateway/application-gateway-introduction>

Network Security Group

A network security group (NSG) contains a list of security rules that allow or deny network traffic to resources connected to Azure Virtual Networks (VNet). NSGs can be associated to subnets, individual VMs (classic), or individual network interfaces (NIC) attached to VMs (Resource Manager). When an NSG is associated to a subnet, the rules apply to all resources connected to the subnet. Traffic can further be restricted by also associating an NSG to a VM or NIC.

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-nsg>

Azure Backup

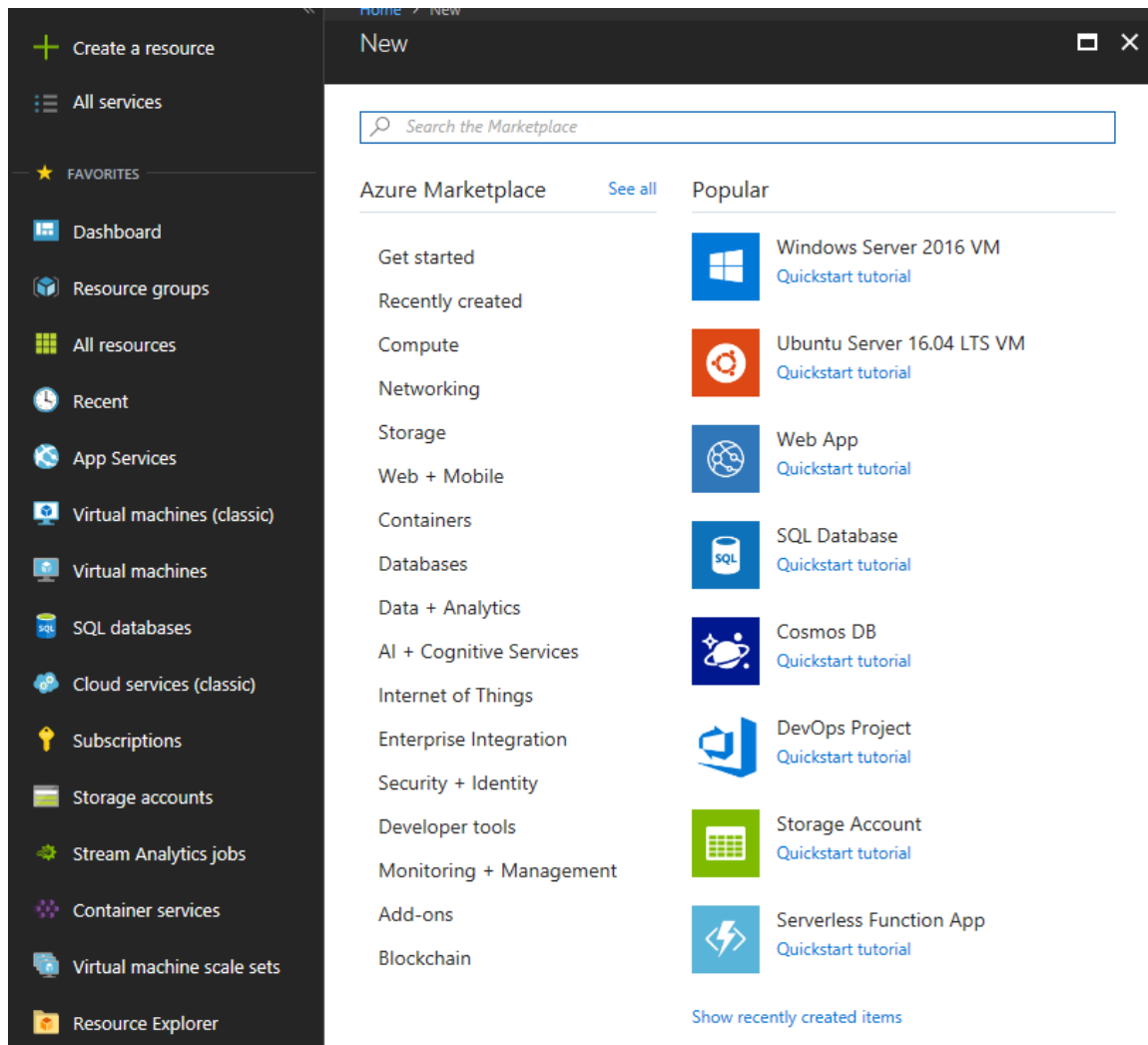
Azure Backup is the Azure-based service you can use to back up (or protect) and restore your data in the Microsoft cloud. Azure Backup replaces your existing on-premises or off-site backup solution with a cloud-based solution that is reliable, secure, and cost-competitive. Azure Backup offers multiple components that you download and deploy on the appropriate computer, server, or in the cloud.

<https://docs.microsoft.com/en-us/azure/backup/backup-introduction-to-azure-backup>

Exercise 1: Environment Setup

Task 1: Create the Virtual Network in Region 1

1. Browse to the Azure Portal and authenticate at <https://portal.azure.com/>
2. In the left pane, click + **Create a resource**



3. Search for **Virtual Network** and create the first one
 - a. Name: **WEvnet**
 - b. Address space: **172.16.0.0/16**
 - c. Subscription: **Choose your subscription**
 - d. Resource group: **Create New → WErg01**
 - e. Location: **West Europe**
 - f. Subnet name: **Webserver**
 - g. Subnet address range: **172.16.0.0/24**
 - h. Service endpoints: **Disabled**
 - i. Click the **Create** button to continue.

Create virtual network ✕

* Name

* Address space ⓘ
 ✓
 10.1.0.0 - 10.1.0.255 (256 addresses)

* Subscription
 ▼

* Resource group
☒ Create new ☐ Use existing

* Location
 ▼

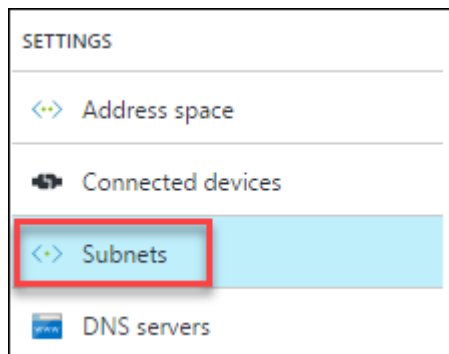
Subnet

* Name

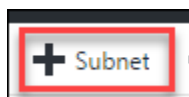
* Address range ⓘ
 ✓
 10.1.0.0 - 10.1.0.255 (256 addresses)

Service endpoints (Preview) ⓘ

4. Once the deployment is complete, add two more subnets to the VNET. To do this, select the **Subnets** > icon in the **Settings** area



5. Click the + **Subnet** option and enter the following settings



- a. Name: *Management*
- b. Address range (CIDR block): **172.16.1.0/24**
- c. Network security group: **None**
- d. Route Table: **None**

- e. Service endpoints: **0 selected**
- f. Click the **OK** button to add this subnet.

Home > WEvnet - Subnets > Add subnet

Add subnet

WEvnet

* Name
Management ✓

* Address range (CIDR block) ⓘ
172.16.1.0/24
172.16.1.0 - 172.16.1.255 (251 + 5 Azure reserved addresses)

Network security group
None >

Route table
None >

Service endpoints
Services ⓘ
0 selected ▼

Subnet delegation
Delegate subnet to a service ⓘ
None ▼

6. Once complete, you will see two subnets defined for **WEvnet**

Search subnets			
NAME	↑↓ ADDRESS RANGE	↑↓	AVAILABLE ADDRESSES
Webserver	172.16.0.0/24		251
Management	172.16.1.0/24		251

Task 2: Create a Windows Jump Box system in Region 1

1. Create a **Windows Server 2016 Datacenter** Virtual machine
 - a. Subscription: **Select your subscription**
 - b. Resource group: **Choose your resource group**
 - c. Name: **Jumpbox**
 - d. Region: **West Europe**
 - e. Leave the settings for Availability options, Image and Size as is
 - f. User name: ***Your Userid***
 - g. Password: ***Your password***

h. Confirm Password: **Your password**

Basics Disks Networking Management Guest config Tags Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization.

Looking for classic VMs? [Create VM from Azure Marketplace](#)

PROJECT DETAILS

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

* Subscription ⓘ

* Resource group ⓘ [Create new](#)

INSTANCE DETAILS

* Virtual machine name ⓘ ✓

* Region ⓘ ✓

Availability options ⓘ ✓

* Image ⓘ ✓
[Browse all images and disks](#)

* Size ⓘ **Standard DS1 v2**
1 vcpu, 3.5 GB memory
[Change size](#)

ADMINISTRATOR ACCOUNT

* Username ⓘ ✓

* Password ⓘ ✓

* Confirm password ⓘ ✓

- i. Change to the Networking tab
- j. Virtual network: **WEvnet**
- k. Subnet: **Management**
- l. Public IP address: **(new) Jumpbox-ip**
- m. Network security group: **Advanced**
- n. Configure Network security group: **(new) Jumpbox-nsg**
- o. Click on **Review + Create**
- p. On the summary page click on **Create**

Exercise 2: Prepare the infrastructure Region 1

Task 1: Create Webserver VMs

1. Create an **Availability Set**
 - a. Name: **WEas**
 - b. Subscription: **Select your subscription**
 - c. Resource group: **Choose your resource group**
 - d. Location: **West Europe**
 - e. Fault domains: **2**
 - f. Update domains: **2**
 - g. Use managed disks: **Yes (Aligned)**

Create availability set

* Name
WEas ✓

* Subscription
Microsoft Azure Internal Consumption

* Resource group
☐ Create new ☒ Use existing
MyRG

* Location
West Europe

Fault domains ⓘ
2

Update domains ⓘ
2

Use managed disks ⓘ

- h. Click on **Create**
2. Create the first of the two **Windows Server 2016 Datacenter** webserver
 - a. Subscription: **Select your subscription**
 - b. Resource group: **Choose your resource group**
 - c. Name: **WEwebserver1**
 - d. Region: **West Europe**
 - e. Availability options: **Availability Set**
 - f. Availability Set: **WEas**
 - g. Leave the settings for Image and Size as is
 - h. User name: **Your Userid**

- i. Password: ***Your password***
- j. Confirm Password: ***Your password***

Basics Disks Networking Management Guest config Tags Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization.
Looking for classic VMs? [Create VM from Azure Marketplace](#)

PROJECT DETAILS

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

* Subscription ⓘ ▼

* Resource group ⓘ ▼
[Create new](#)

INSTANCE DETAILS

* Virtual machine name ⓘ ✓

* Region ⓘ ▼

Availability options ⓘ ▼

* Availability set ⓘ ▼
[Create new](#)

* Image ⓘ ▼
[Browse all images and disks](#)

* Size ⓘ **Standard DS1 v2**
1 vcpu, 3.5 GB memory
[Change size](#)

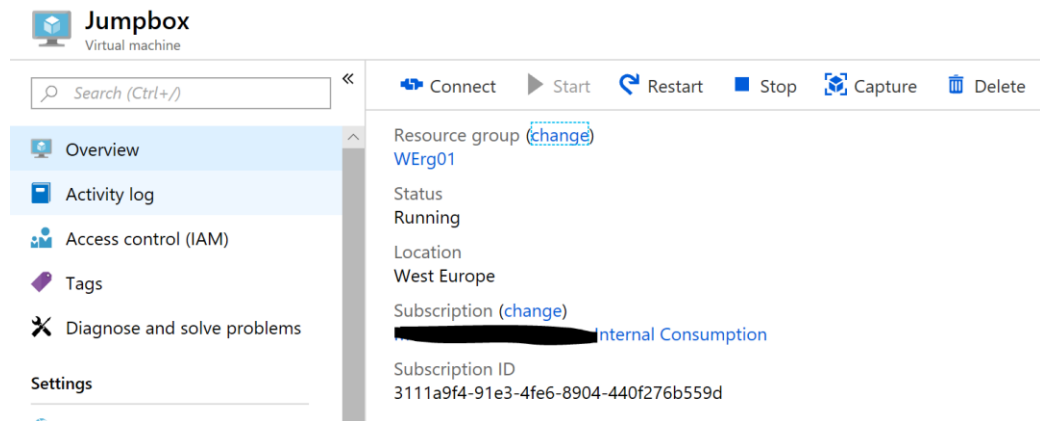
ADMINISTRATOR ACCOUNT

* Username ⓘ ✓

* Password ⓘ ✓

* Confirm password ⓘ ✓

- k. Change to the Networking tab
 - l. Virtual network: **WEvnet**
 - m. Subnet: **Webserver**
 - n. Public IP address: **None**
 - o. Network security group: **Basic**
 - p. Click on **Review + Create**
 - q. On the summary page click on **Create**
3. Create the second **Windows Server 2016 Datacenter** Webserver. Use the same steps as above. Just take a different name like **WEwebserver2**
4. Install a Webserver on both servers. As the Virtual machines are not accessible via the public internet we must use our management Jump box for administration.
- a. Navigate to the jumpbox system in the Azure portal, for example using the **Virtual machines** section



- b. Click Connect
- c. Enter your user credentials to connect
- d. From this machine we can now reach all the internal virtual machines.
For an IP Address overview open the **WEvnet** and click on **Connected devices**

WEvnet
Virtual network

Search (Ctrl+/)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Address space
- Connected devices

DEVICE	TYPE	IP ADDRESS	SUBNET
wewebserver1583	Network interface	172.16.0.4	Webserver
wewebserver2187	Network interface	172.16.0.5	Webserver
jumpbox973	Network interface	172.16.1.4	Management

- e. Log into the first Webserver with the internal IP **172.16.0.4** and execute the following command in a PowerShell prompt.
Install-WindowsFeature -name Web-Server -IncludeManagementTools
- f. Repeat the steps above steps for the second webserver

Task 2: Create internal Loadbalancer

1. Create a **Load Balancer** and configure with an internal facing IP.
 - a. Name: **WEilb**
 - b. Type: **Internal**
 - c. Virtual network: **WEvnet**
 - d. Subnet: **Webserver**
 - e. IP address assignment: **Dynamic**
 - f. Subscription: **Select your subscription**
 - g. Resource group: **Choose your resource group**
 - h. Location: **West Europe**

Create load balancer

*

Name

WEilb

✓

*

Type ⓘ

☒ Internal

☐ Public

*

Virtual network

WEvnet

>

*

Subnet

Webserver (172.16.0.0/24)

>

*

IP address assignment

☐ Static

☒ Dynamic

*

Subscription

Microsoft Azure Internal Consumption

▼

*

Resource group

☐ Create new

☒ Use existing

MyRG

▼

*


Location


West Europe


▼


- i. Click on **Create**
2. Add health probe to the internal Loadbalancer **WEilb** for our Webserver

SETTINGS

 Frontend IP configuration

 Backend pools

 Health probes

 Load balancing rules

 Inbound NAT rules

 Properties

- Name: **WEilbHttpProbe**
- Protocol: **HTTP**
- Port: **80**
- Path: **/**
- Interval: **5**
- Unhealthy threshold: **2**

Add health probe

☐ ☐ X

WEilb


* Name

WEilbHttpProbe



IP version

IPv4

Protocol 

HTTP



* Port 

80


* Path 

/

* Interval 

5

seconds

* Unhealthy threshold 


2


consecutive failures


- Click on **OK**


- Configure the internal Loadbalancer **WEilb** Backendpool to balance between our Webservers

SETTINGS

 Frontend IP configuration

 Backend pools

 Health probes

 Load balancing rules

- Name: **WEilbbackend**
- Associated to: **Availability set**
- Availability set: **WEas**
- + Add a target network IP configuration: **Add all your Webserver VMS and IPs**

Add backend pool



WEilb

* Name

WEilbbackend



IP version ⓘ

IPv4

Associated to ⓘ

Availability set



Availability set ⓘ

WEas

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: WEwebserver1

Network IP configuration: wewebserver1583/ipconfig1 (172.16.0.4)



Virtual machine: WEwebserver2

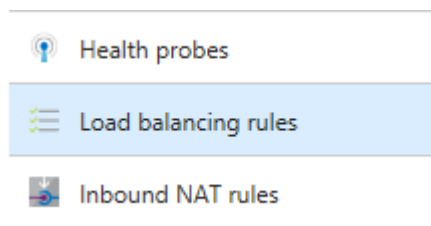
Network IP configuration: wewebserver2187/ipconfig1 (172.16.0.5)



+ Add a target network IP configuration

- Click on **OK**

4. Add Load balancing rule to the internal Loadbalancer **WEilb**



- a. Name: **WEilbLoadBalancingRule**
- b. IP Version: **IPv4**
- c. Front IP address: **<your IP> (LoadBalancerFrontEnd)**
- d. Protocol: **TCP**
- e. Port: **80**
- f. Backend port: **80**
- g. Backend pool: **WEilbbackend**
- h. Health probe: **WEilbHttpProbe (HTTP:80)**
- i. Session persistence: **None**
- j. Idle timeout (minutes): **4**
- k. Floating IP: **Disabled**

Add load balancing rule
WElib

* Name
WElibLoadBalancingRule

* IP Version
☒ IPv4 ☐ IPv6

* Frontend IP address ⓘ
172.16.0.6 (LoadBalancerFrontEnd)

Protocol
☒ TCP ☐ UDP

* Port
80

* Backend port ⓘ
80

Backend pool ⓘ
WElibbackend

Health probe ⓘ
WElibHttpProbe (HTTP:80)

Session persistence ⓘ
None

Idle timeout (minutes) ⓘ
 4

Floating IP (direct server return) ⓘ
 Disabled Enabled

I. Click on **OK**

Task 3: Create Application Gateway

1. Add a dedicated Subnet to our existing Virtual Network **WEvnet**
 - a. Name: **ApplicationGateway**
 - b. Address range (CIDR block): **172.16.3.0/24**
 - c. Network security group: **None**
 - d. Route table: **None**

- e. Service Endpoints: **0 selected**

Add subnet

WEvnet

*

Name

ApplicationGateway

✓

*

Address range (CIDR block) ⓘ

172.16.3.0/24

172.16.3.0 - 172.16.3.255 (251 + 5 Azure reserved addresses)

Network security group

None

>

Route table

None

>

Service endpoints (Preview)

Services ⓘ

0 selected

▼

- f. Click on **OK**
2. Create the **Application Gateway** with an L7 Firewall
- Name: **WEagwaf**
 - Tier: **WAF**
 - SKU size: **Medium**
 - Instance count: **2**
 - Subscription: **Select your subscription**
 - Resource group: **Choose your resource group**

- g. Location: **West Europe**

Basics

✕

★ Name

WEagwaf

✓

★ Tier

Standard

WAF

★ SKU size ⓘ

Medium

▼

Instance count ⓘ

2

★ Subscription

Microsoft Azure Internal Consumption

▼

★ Resource group

☐ Create new

☒ Use existing

MyRG

▼

★ Location

West Europe

▼

- h. Click on **OK**
- i. Virtual network: **WEvnet**
- j. Subnet: **ApplicationGateway (172.168.3.0/24)**
- k. Frontend IP configuration: **Public IP**
- l. Public IP type: Create new **WEagwafpip**
- m. Listener Configuration: **HTTP**
- n. Port: **80**
- o. Select **Upgrade to WAF** tier and set Firewall status to: **Enabled**

p. Firewall mode: **Prevention**

Settings

×

Subnet configuration

* Virtual network ⓘ

WEvnet

>

* Subnet ⓘ

ApplicationGateway (172.16.3.0/24)

▼

Frontend IP configuration

* IP address type

☒ Public ☐ Private

* Public IP address ⓘ

☒ Create new ☐ Use existing

WEagwafpip

✓

▼ Configure public IP address

Listener configuration

* Protocol

☒ HTTP ☐ HTTPS

* Port

80

✓

Additional Settings

* HTTP2

Disabled

Enabled

Web application firewall

⚠

Web application firewall is only available for application gateways in the WAF tier.

☒

Upgrade to WAF tier

* Firewall status

Disabled

Enabled

* Firewall mode

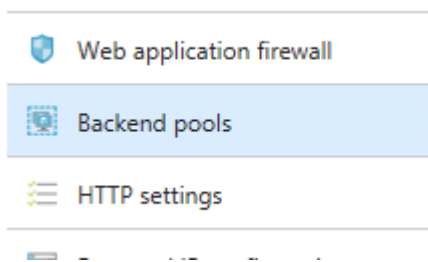
Detection

Prevention

q. Click on **OK**

r. On the summary blade click on **OK**

3. Add the Internal Loadbalancer IP to the Backend Pool.



- a. IP address or FQDN: **172.16.0.6** (The private IP of the **WEilb**)

A screenshot of the 'appGatewayBackendPool' configuration window in the Azure portal. The window has a title bar with the name 'appGatewayBackendPool' and a close button. Below the title bar are three buttons: 'Save', 'Discard', and 'Delete'. The main content area has a 'Name' field with the value 'appGatewayBackendPool'. Below that is a 'Targets' section with the text 'You can point your backend pool to a specific virtual machine, or to an IP address/FQDN.' There is a table with one row containing the IP address '172.16.0.6' and a delete icon. Below the table is a 'Type' section with two radio buttons: 'IP address or FQDN' (selected) and 'Virtual machine'. Below the radio buttons is a text input field with the placeholder '10.0.0.0 or www.contoso.com'. At the bottom of the targets section is a '+ Add target' button. Below the targets section is an 'Associated rule' section with a dropdown menu showing 'rule1'.

- b. Click on **Save**

Task 4: Configure Backups of IaaS Servers

1. Create a **Backup and Site Recovery (OMS)** service.
 - a. Name: **WEbackup**
 - b. Subscription: **Select your subscription**
 - c. Resource group: **Choose your resource group**
 - d. Location: **West Europe**

Recovery Services vault

* Name

WEbackup

* Subscription

Microsoft Azure Internal Consumption

* Resource group

☐ Create new ☒ Use existing

MyRG

* Location

West Europe

- e. Click on **Create**
2. Configure the Backup for the two Webserver in region 1

GETTING STARTED

Backup

Site Recovery

- a. Where is your workload running: **Azure**

- b. What do you want to backup: Virtual Machine

Where is your workload running?

Azure

What do you want to backup?

Virtual machine

Step: Configure Backup

Backup

- c. Click on **Backup**
- d. Chooses backup policy: **DefaultPolicy**

Backup

1 Backup policy
DefaultPolicy

2 Items to backup
Select

Backup policy

Choose backup policy

DefaultPolicy

BACKUP FREQUENCY
Daily at 7:00 PM

RETENTION RANGE
Retention of daily backup point
Retain backup taken every day at 7:00 PM for 30 Day(s)

- e. Click on **OK**
- f. Select the two Webservers

Backup

1 Backup policy
DefaultPolicy

2 Items to backup
Select

Select virtual machines

Filter items ...

	VIRTUAL MACHINE NAME	RESOURCE GROUP
<input type="checkbox"/>	Jumpbox	MyRG
<input checked="" type="checkbox"/>	WEwebserver1	MyRG
<input checked="" type="checkbox"/>	WEwebserver2	MyRG

- g. Click on **OK**
- h. Click on **Enable backup**