Microsoft Cloud Workshop

Building an IaaS Architecture

September 2018

Contents

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:

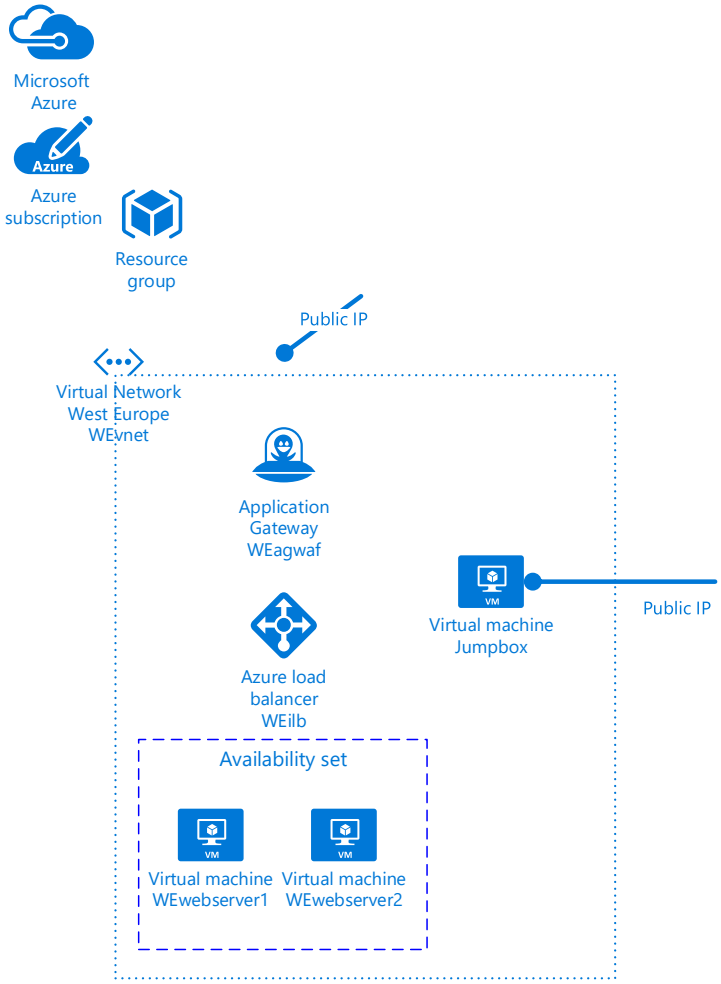
- Virtual Networks
- Virtual Machine deployment and Availability Sets
- Securing Network access with network security groups and Layer 7 firewall
- Load balancing (Layer 4 / DNS based)
- Backup

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

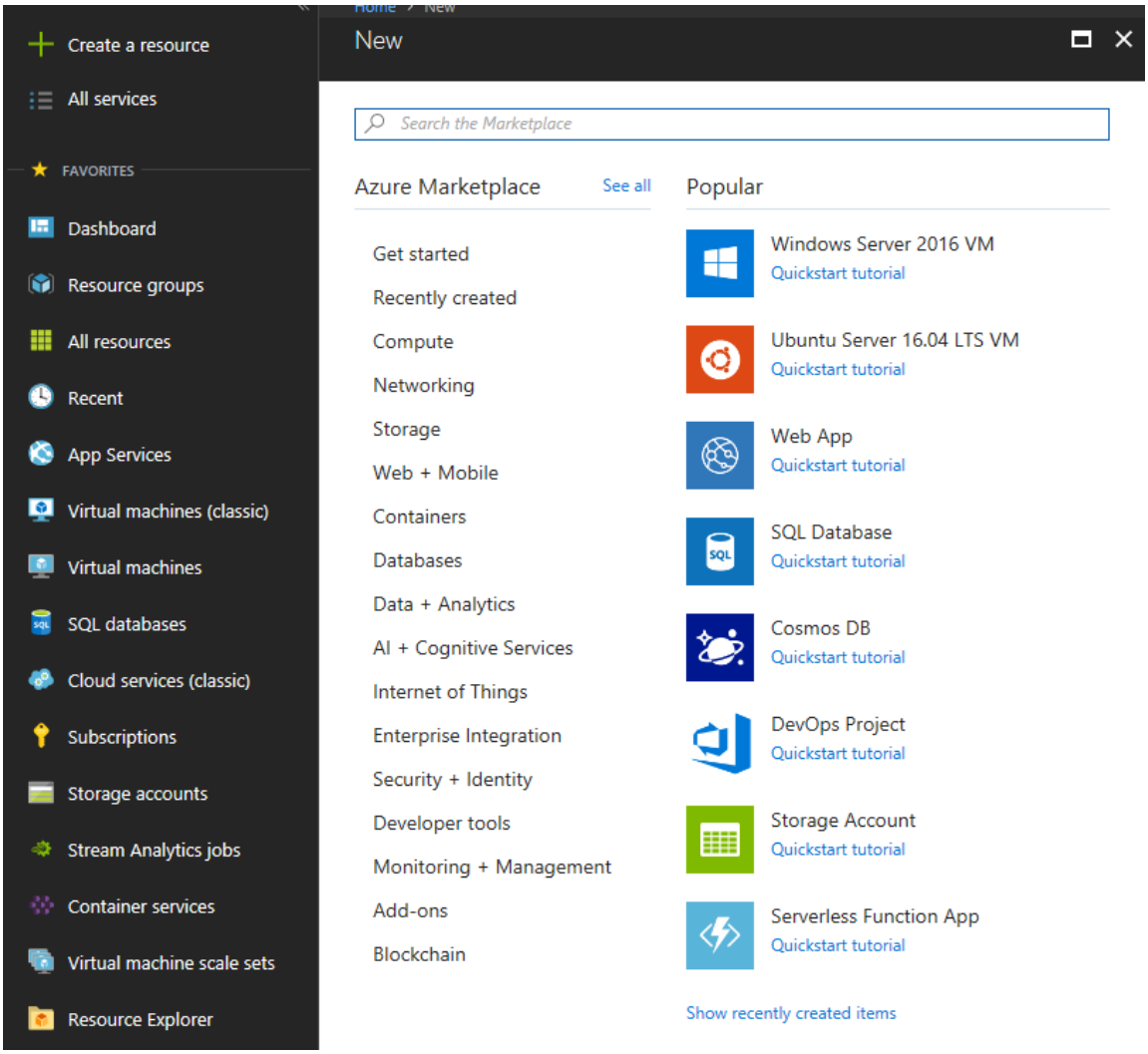
Azure Backup is the Azure-based service you can use to back up (or protect) and restore your data in the Microsoft cloud. Azure Backup replaces your existing on-premises or off-site backup solution with a cloud-based solution that is reliable, secure, and cost-competitive. Azure Backup offers multiple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

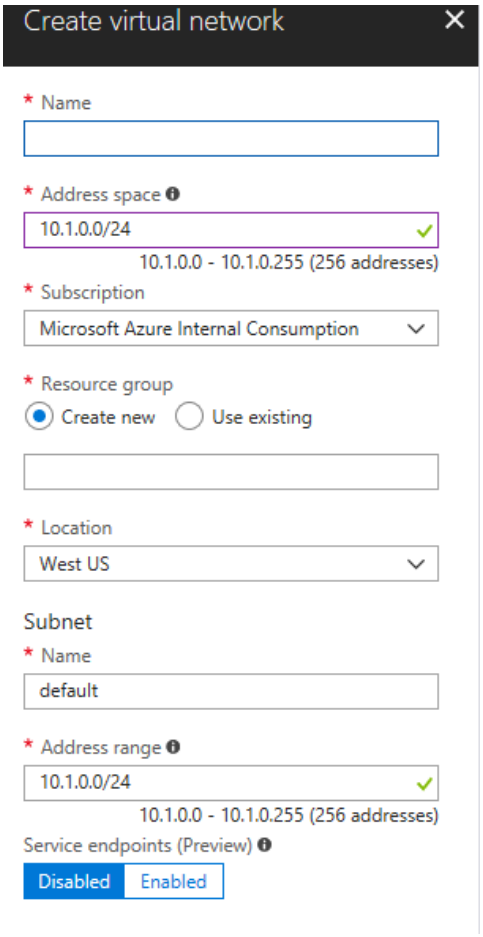
Exercise 1: Environment Setup

Task 1: Create the Virtual Network in Region 1

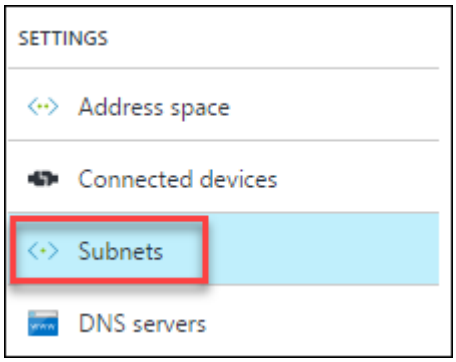
1. Browse to the Azure Portal and authenticate at https://portal.azure.com/
2. In the left pane, click **+ Create a resource**



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.



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

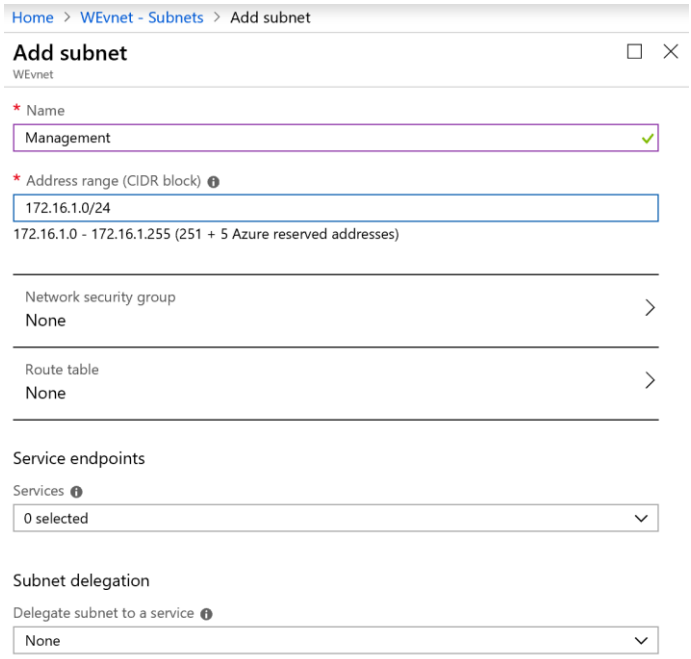


5. Click the **+ Subnet** option and enter the following settings

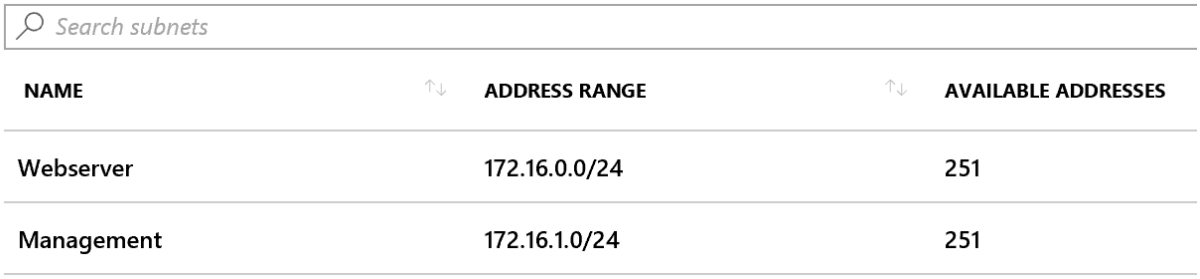
   a. Name: *Management*
   b. Address range (CIDR block): **172.16.1.0/24**
   c. Network security group: **None**
   d. Route Table: **None**

e. Service endpoints: **0 selected**

f. Click the **OK** button to add this subnet.



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



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**

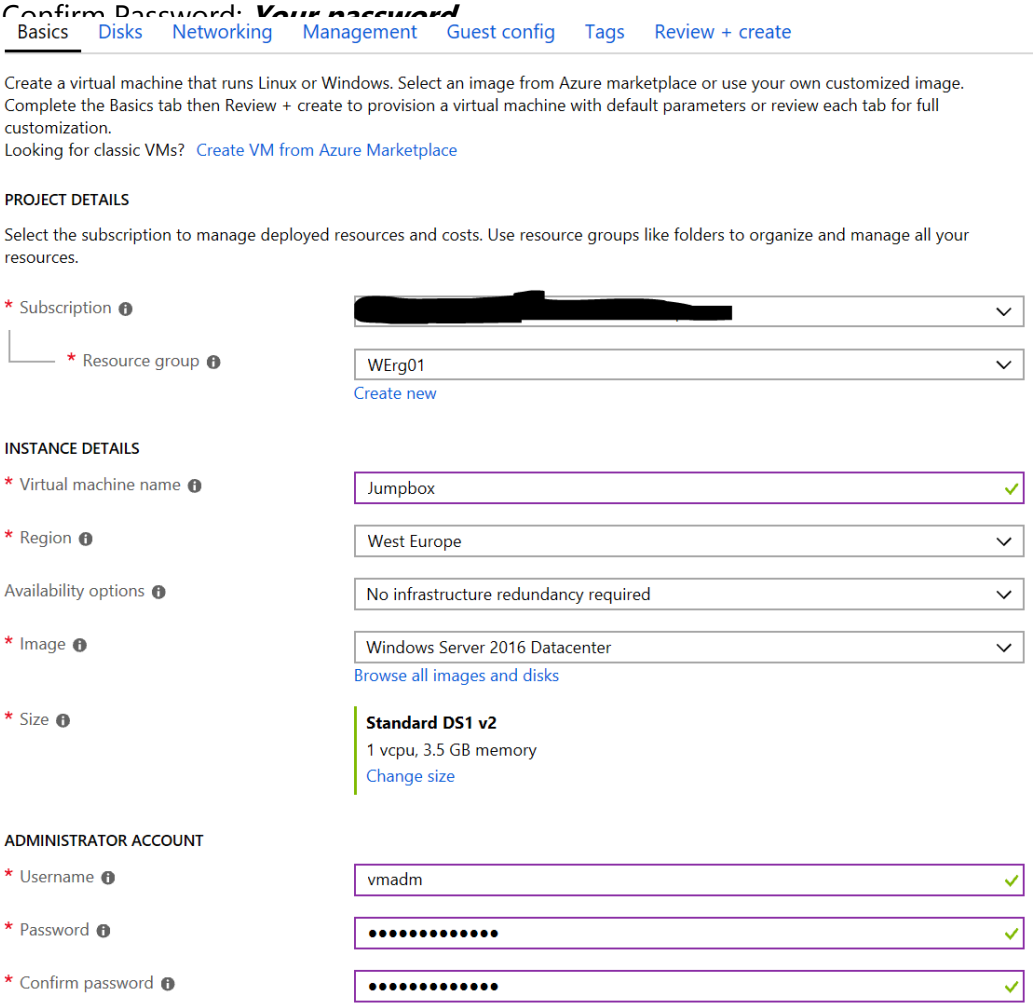
   d. Region: **West Europe**

   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***



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**

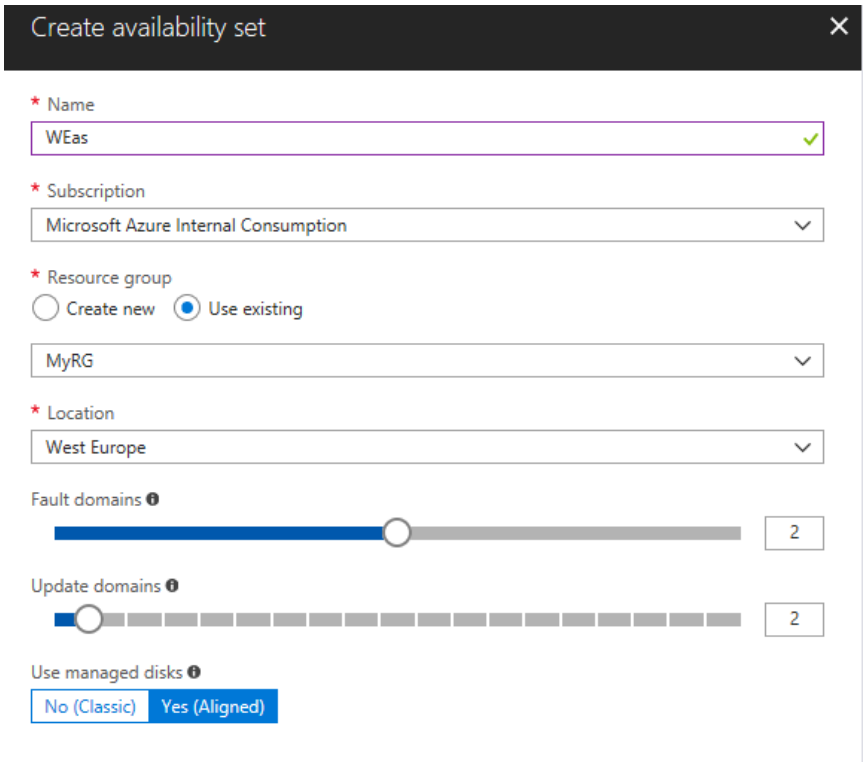
o. Click on **Review + Create**

p. On the summary page click on **Create**

Exercise 2: Prepare the infrastructure Region 1

Task 1: Create Webserver VMs

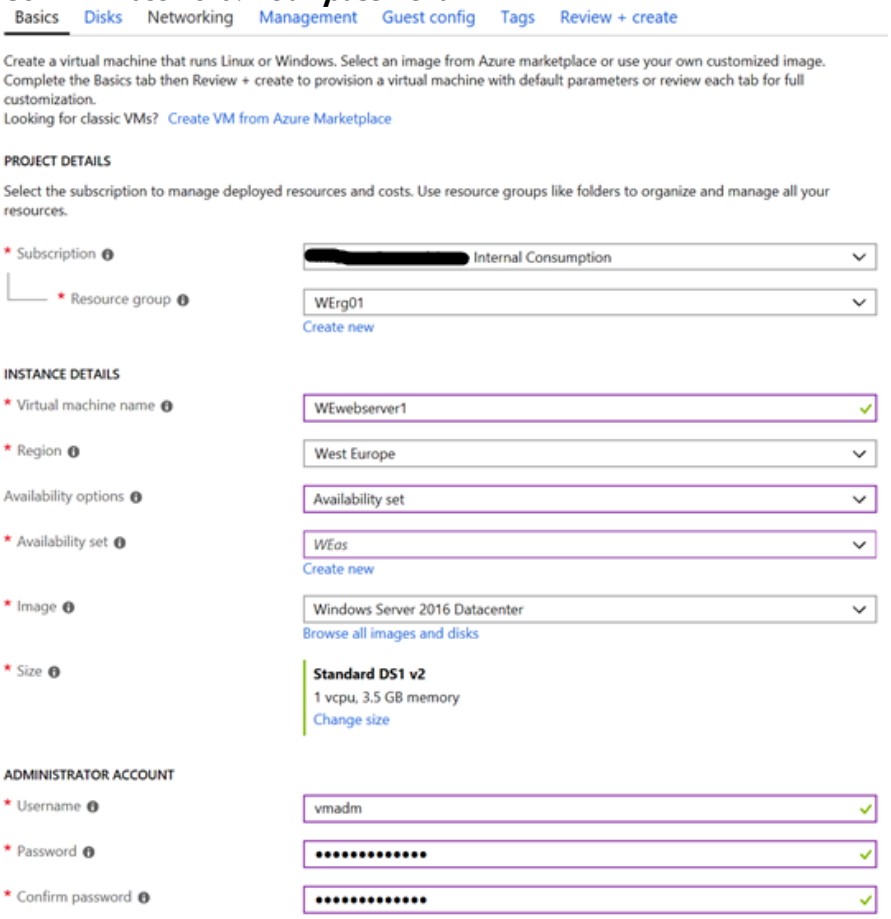
1. Create an **Availability Set**
    a. Name: **WEas**
    b. Subscription: **Select your subscription**
    c. Resource group: **Choose your resource group**
    d. Location: **West Europe**
    e. Fault domains: **2**
    f. Update domains: **2**
    g. Use managed disks: **Yes (Aligned)**



    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 fo, Image and Size as is
    h. User name: ***Your Userid***

i. Password: ***Your password***

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



k. Change to the Networking tab

l. Virtual network: **WEvnet**

m. Subnet: **Webserver**

n. Public IP address: **None**

o. Network security group: **Basic**

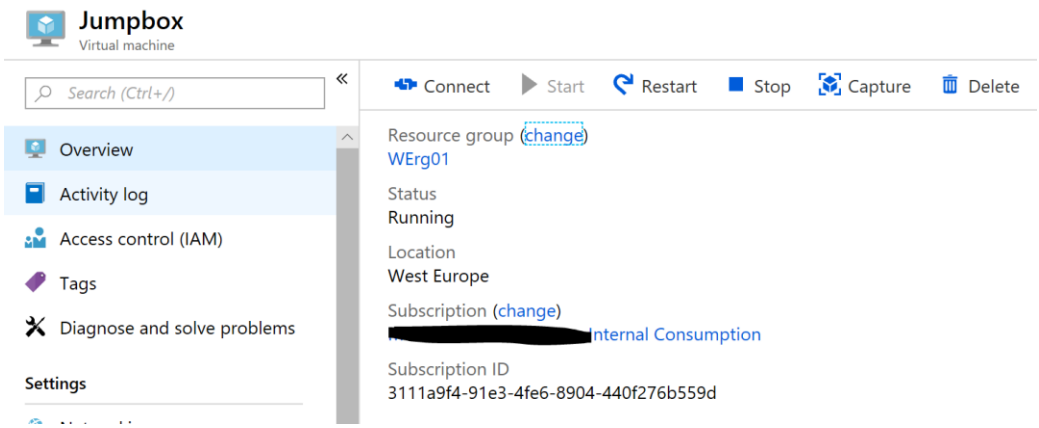
p. Click on **Review + Create**

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.

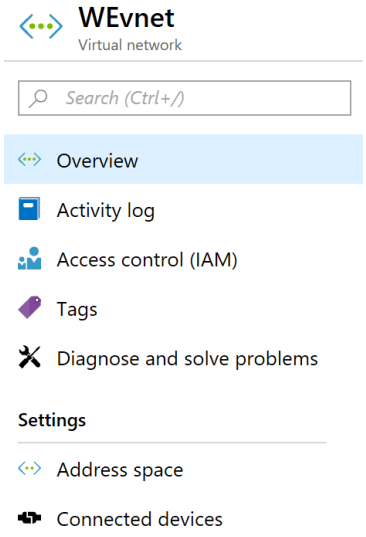
    a. Navigate to the jumpbox system in the Azure portal, for example using the **Virtual machines** section



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**



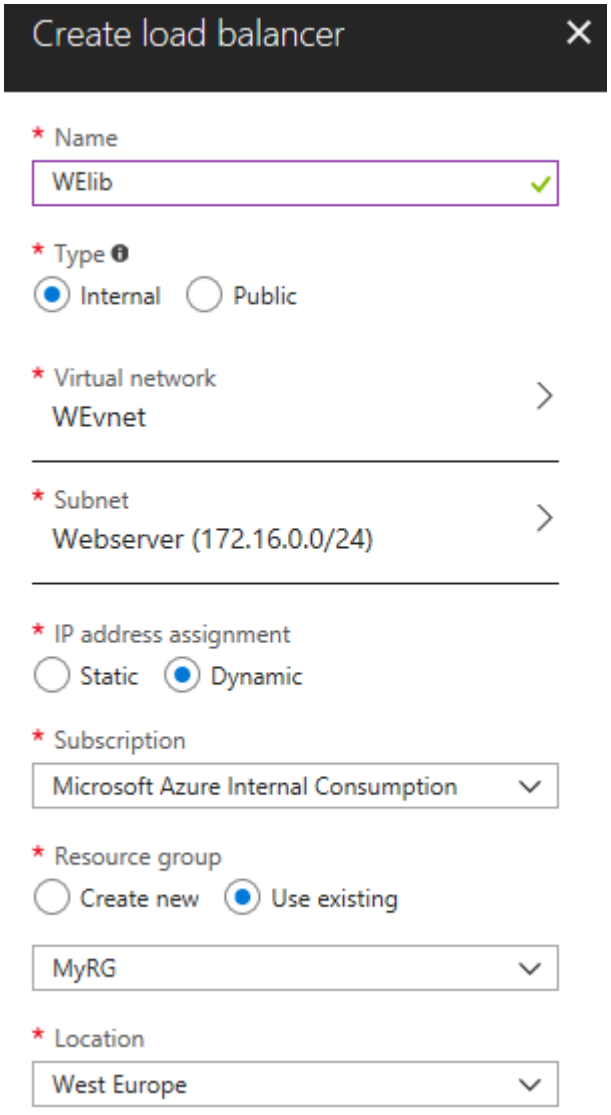
DEVICE	TYPE	IP ADDRESS	SUBNET
wewebserver1583	Network interface	172.16.0.4	Webserver
wewebserver2187	Network interface	172.16.0.5	Webserver
jumpbox973	Network interface	172.16.1.4	Management

e. Log into the first Weberver 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

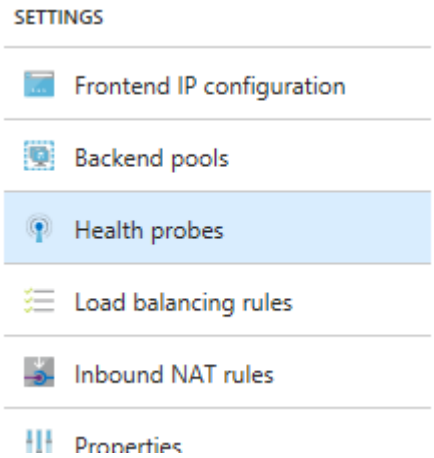
Task 2: Create internal Loadbalancer

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**

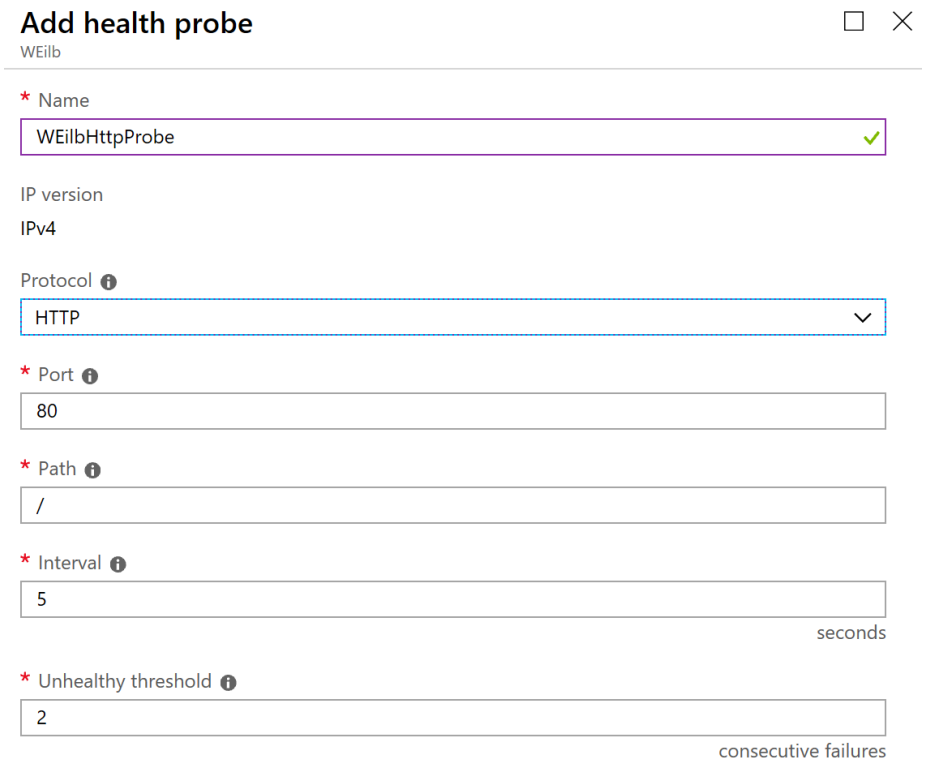


    i. Click on **Create**

2. Add health probe to the internal Loadbalancer **WEilb** for our Webserver

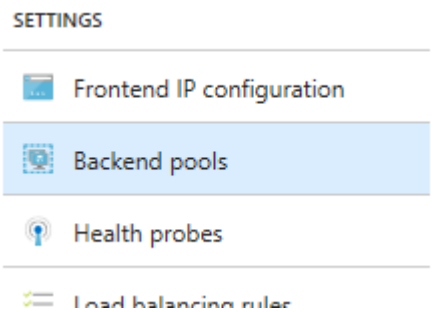


a. Name: **WEilbHttpProbe**
b. Protocol: **HTTP**
c. Port: **80**
d. Path: **/**
e. Interval: **5**
f. Unhealthy threshold: **2**



g. Click on **OK**

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

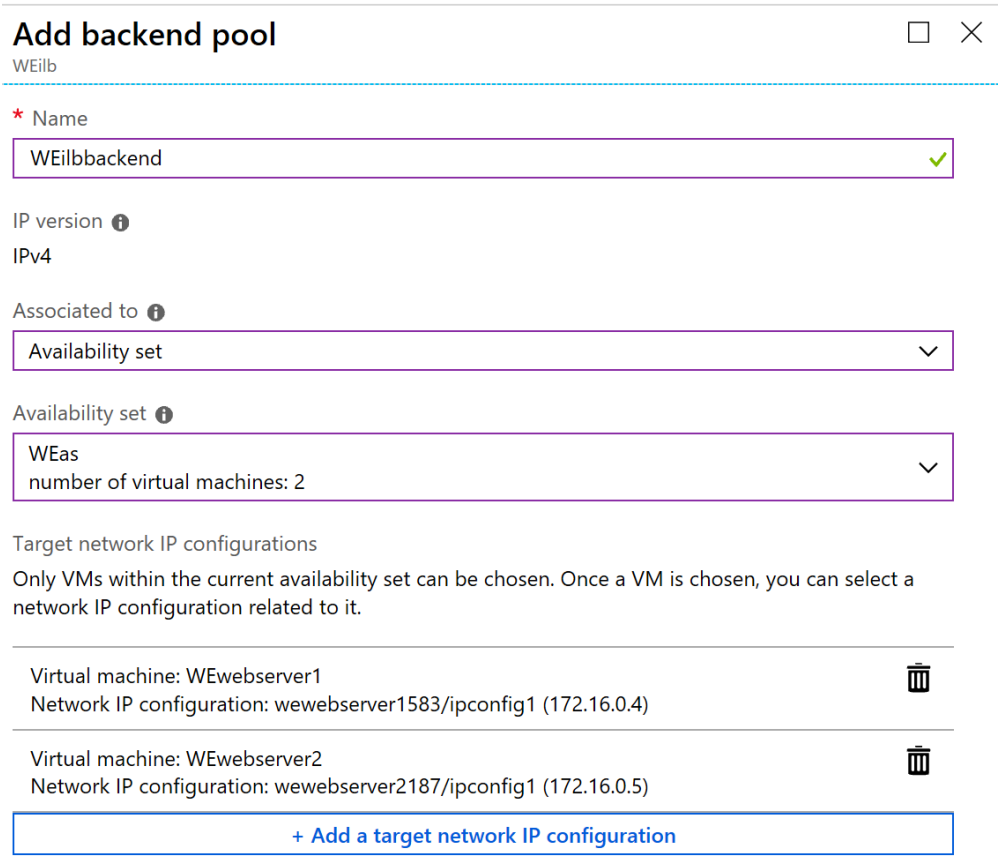


a. Name: **WEilbbackend**

b. Associated to: **Availability set**

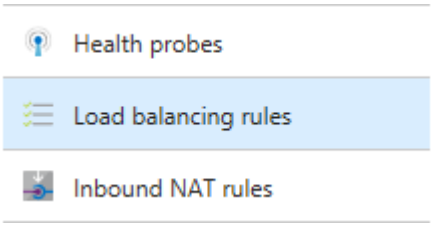
c. Availability set: **WEas**

d. + Add a target network IP configuration: **Add all your Webserver VMS and IPs**

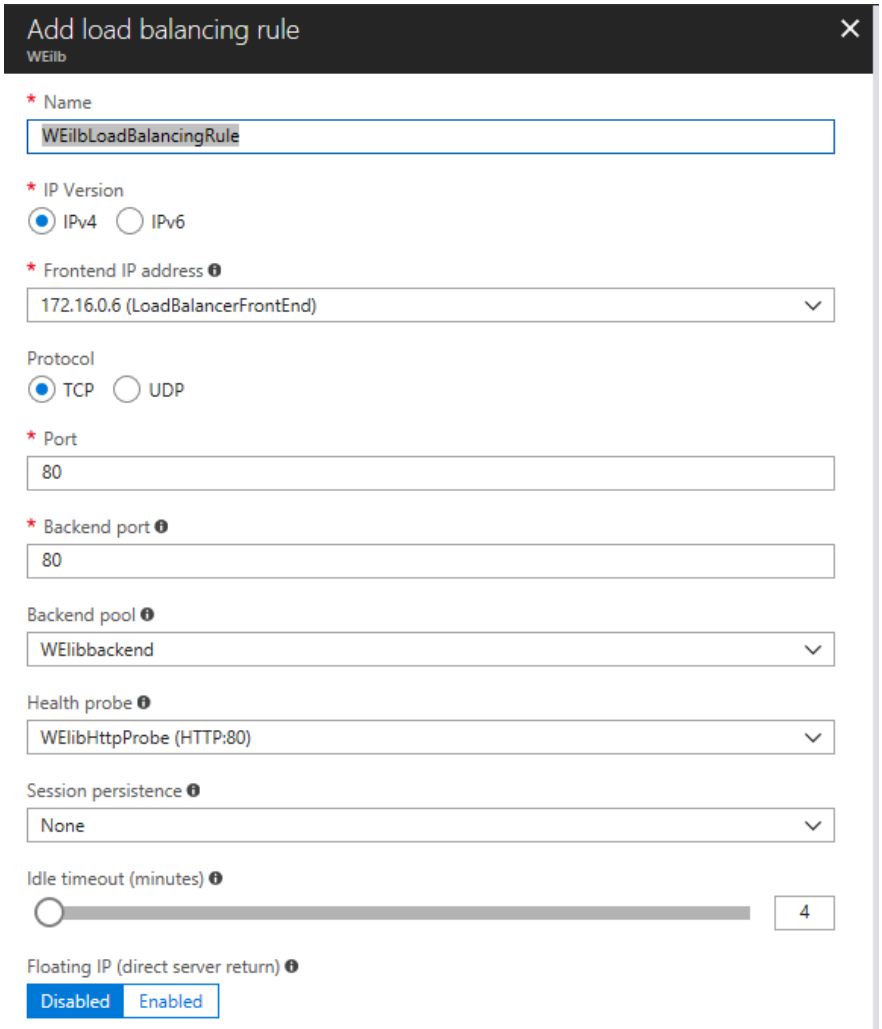


e. Click on **OK**

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**

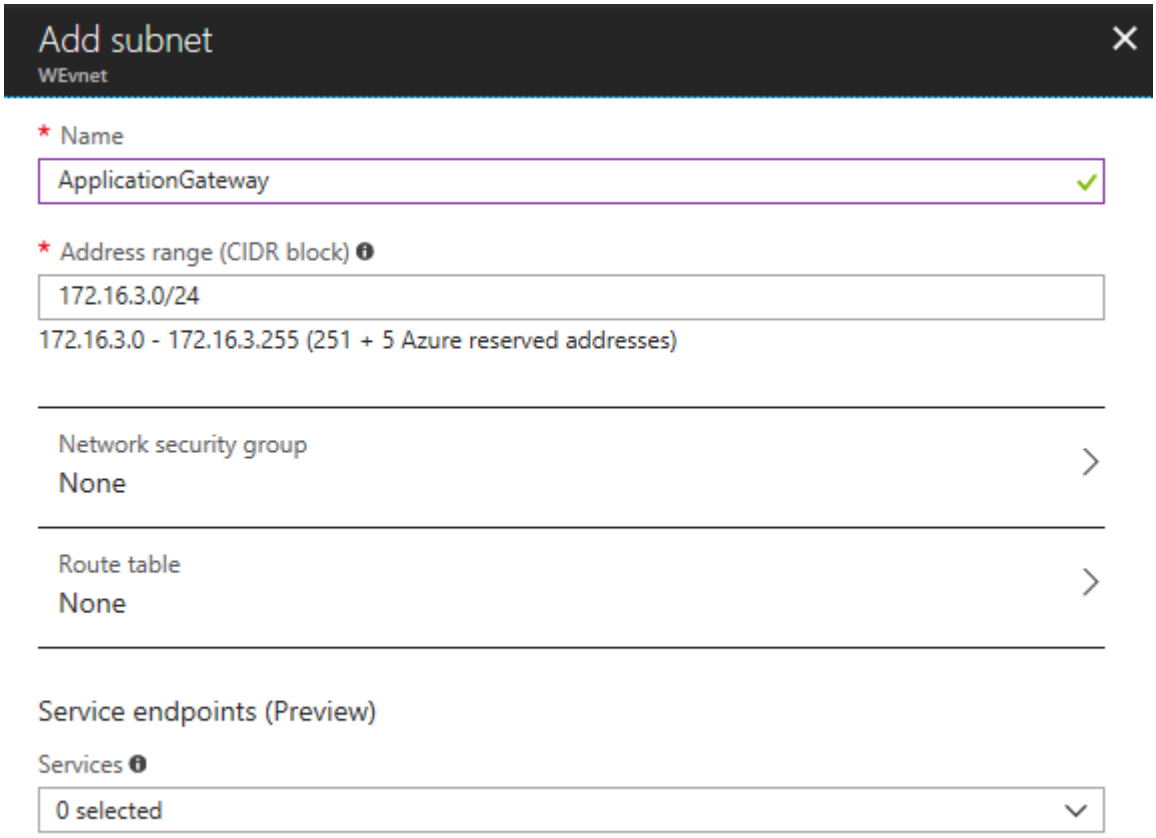


l. Click on **OK**

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**

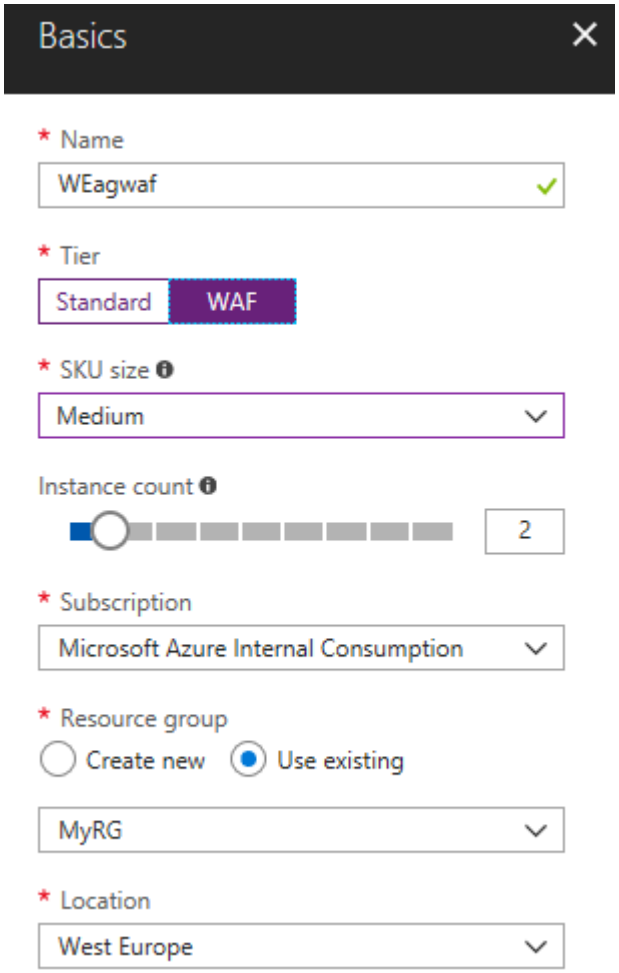
e. Service Endpoints: **0 selected**



f. Click on **OK**

2. Create the **Application Gateway** with an L7 Firewall
    a. Name: **WEagwaf**
    b. Tier: **WAF**
    c. SKU size: **Medium**
    d. Instance count: **2**
    e. Subscription: **Select your subscription**
    f. Resource group: **Choose your resource group**

g. 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**

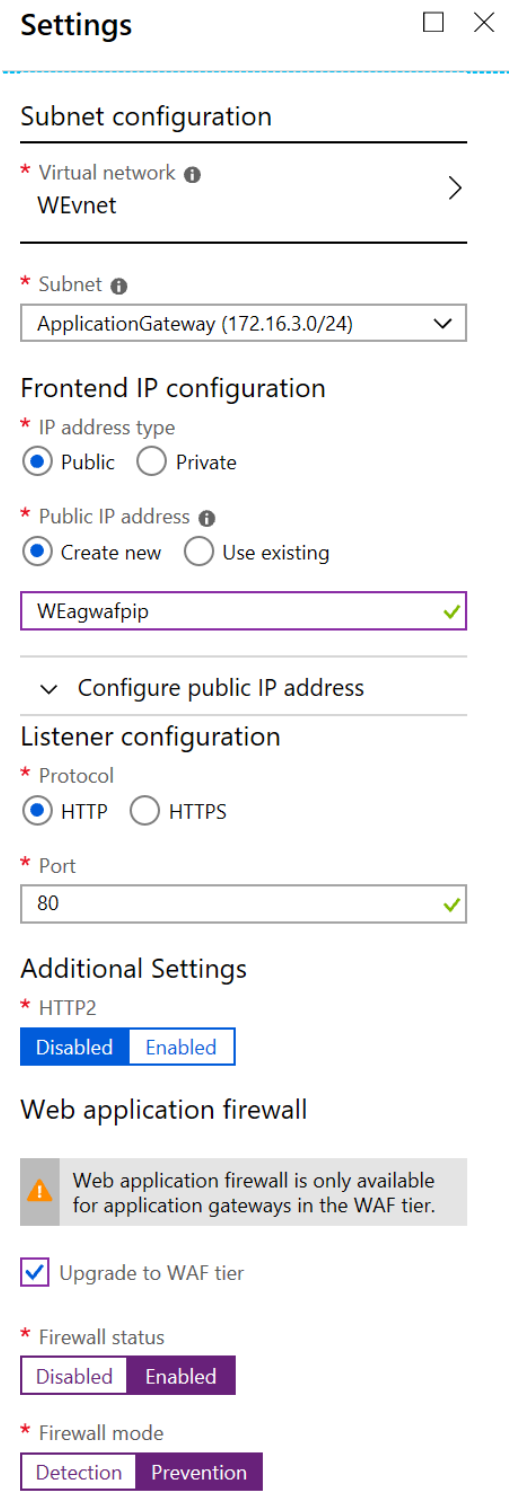
l. Public IP type: Create new **WEagwafpip**

m. Listener Configuration: **HTTP**

n. Port: **80**

o. Select **Upgrade to WAF** tier and set Firewall status to: **Enabled**

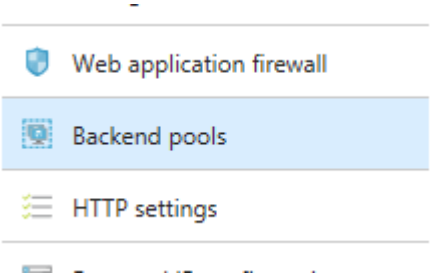
p. Firewall mode: **Prevention**



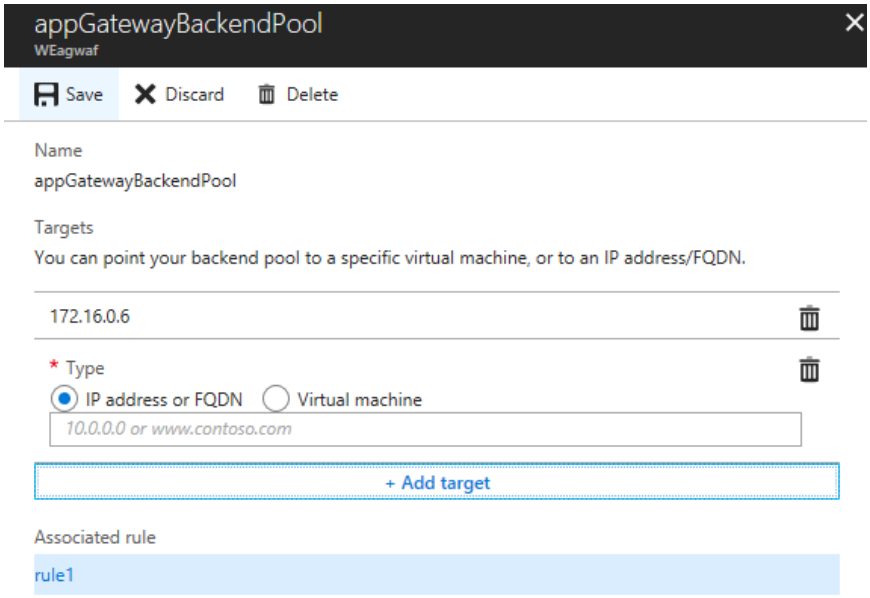
q. Click on **OK**

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

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



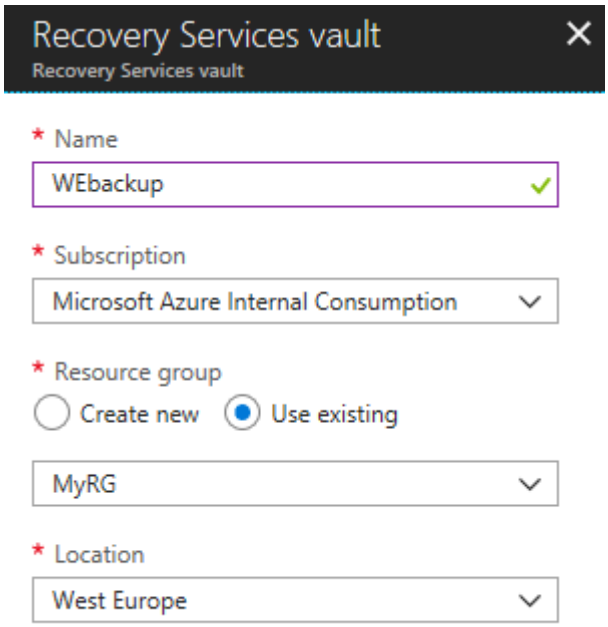
a. IP address or FQDN: **172.16.0.6** (The private IP of the **WEilb**)



b. Click on **Save**

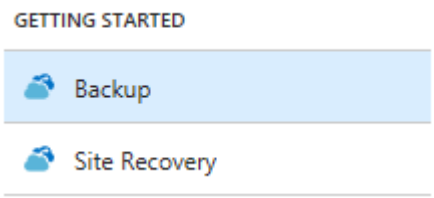
Task 4: Configure Backups of IaaS Servers

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**



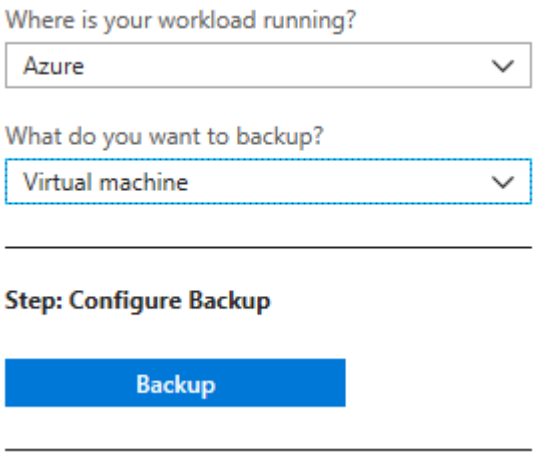
    e. Click on **Create**

2. Configure the Backup for the two Webserver in region 1



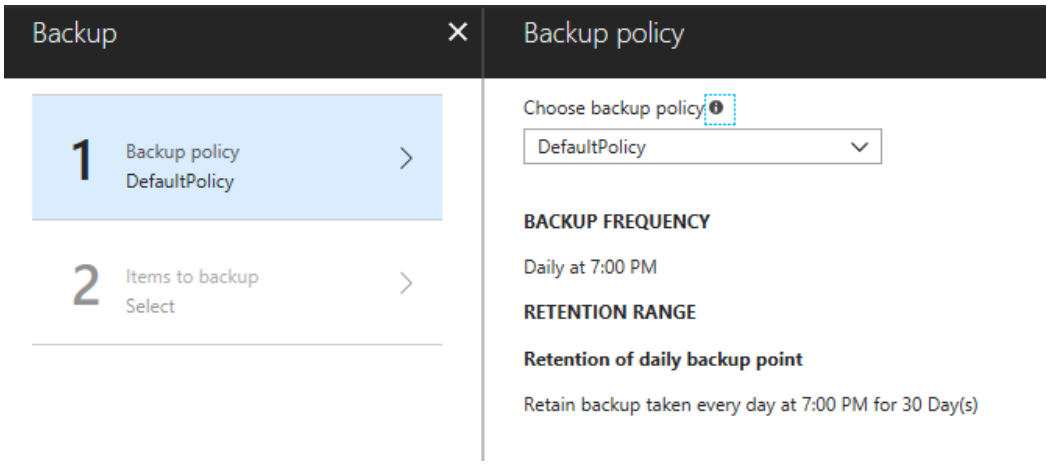
    a. Where is your workload running: **Azure**

b. What do you want to backup: Virtual Machine



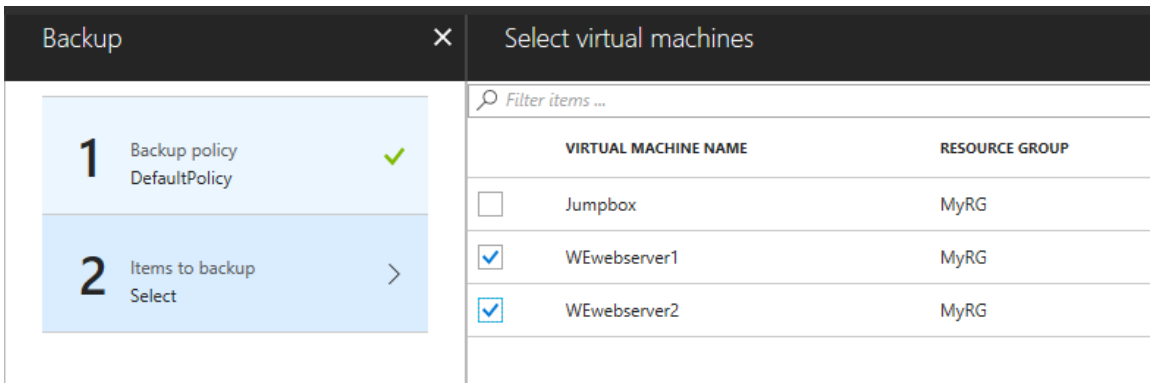
c. Click on **Backup**

d. Chooses backup policy: **DefaultPolicy**



e. Click on **OK**

f. Select the two Webservers



g. Click on **OK**

h. Click on **Enable backup**