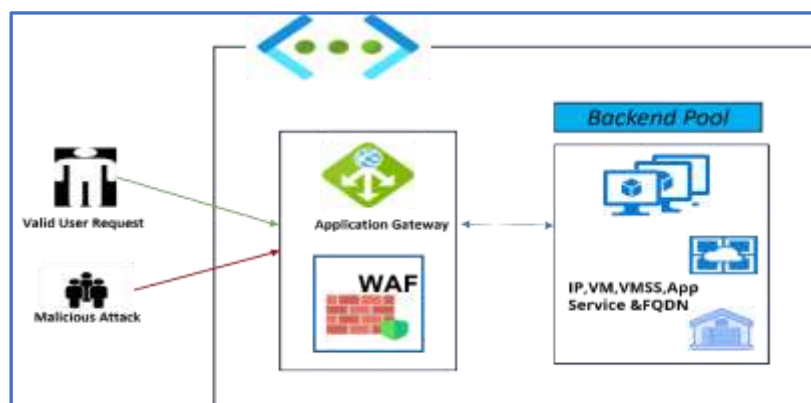


## How to Deploy and Configure Application Gateway

Azure Application Gateway is Layer 7 web traffic load balancer that enables you to manage traffic to web applications and provides security mechanism for our application using WAF.

Benefits:

- Protects Web Application from Vulnerability and attack
- DDos Protection
- WAF integrated with Microsoft Defender for Monitoring.
- Connection Draining
- Host Multiple Sites
- Secure SSL
- URL based Routing (Route request to Pool based on Content Type)
- Redirection to external site based on Rules.
- Supports Autoscaling & Zone Redundancy.



Client sends a request to an application gateway. The WAF determines if the Request is valid or security Threat. If the WAF is in **Protection Mode** the Invalid Request or Malicious attacks are blocked. The AG accepts the Request from Listener and Routes to the Backend Pool.

Application Gateway can be **Internet facing** which uses public IP or **Internal Application Gateway** which Uses Private IP.

**Frontend IP:** Frontend IP address is the IP address associated with an application gateway. The frontend IP can be Public or Private.

**Listener:** The frontend IP is associated with Listener. There are 2 Types of Listeners, **Basic** listens to single site and **Multi-site** for multi-site host.

The application gateway accepts incoming traffic on one or more listeners.

**Rules:** The Routing Rule binds the listener, and the backend server pool/HTTP settings. Based on the Routing Rule the request is sent to backend Pool. There are 2 Types of Rules, **Basic & Path** based.

**Backend Pool:** There can be multiple backend server pool (NIC, Virtual Machine scale set, App service, Public/Internal IP, FQDN) as per Requirement.

Here we create a simple Application Gateway (Internet facing) with basic listener hosting single site, with 3 VM in the backend Pool Server.

1. **Create Resource Group RG01.**
2. **Create Virtual Network VNET01, with 2 subnet Subnet1AG and Subnet2BP.**
3. **Create 3 Virtual Machine VM01, VM02 & VM03 for Backend pool Servers.**
4. **Create Application Gateway AG01.**
5. **Test Connection & Cleanup the Resource.**

### Create Resource Group RG01.

Home > Resource groups >  
**Create a resource group**

**Basics** | Tags | Review + create

Resource group - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. [Learn more](#)

**Project details**

Subscription \*

Resource group \*

**Resource details**

Region \*

### Create Virtual Network VNET01, with 2 subnet SubnetAG and SubnetBP.

SubnetAG for Application Gateway and SubnetBP for Backend pool VM's.

Home > Virtual networks >  
**Create virtual network**

**Basics** | IP Addresses | Security | Tags | Review + create

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the Internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation. [Learn more about virtual network](#)

**Project details**

Subscription \*

Resource group \*

**Instance details**

Name \*

Region \*

Rename the default subnet and add one more Subnet to the VNET01 as below


Home > Virtual networks >


## Create virtual network ...

Basics IP Addresses Security Tags Review + create



The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).

**IPv4 address space**



10.0.0.0/16 10.0.0.0 - 10.0.255.255 (65536 addresses) 

Add IPv6 address space 

The subnet's address range in CIDR notation (e.g. 192.168.1.0/24). It must be contained by the address space of the virtual network.

 Add subnet  Remove subnet

<input type="checkbox"/> Subnet name	Subnet address range	NAT gateway
<input type="checkbox"/> SubnetBP	10.0.0.0/24	-
<input type="checkbox"/> SubnetAG	10.0.1.0/24	-

 A NAT gateway is recommended for outbound internet access from subnets. Edit the subnet to add a NAT gateway. [Learn more](#) 

[Review + create](#) [< Previous](#) [Next : Security >](#) [Download a template for automation](#)

**Create 3 Virtual Machine VM01, VM02 & VM03 for Backend pool Servers.**

# Create a virtual machine

- Basics
- Disks
- Networking
- Management
- Monitoring
- Advanced
- 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. [Learn more](#)

### 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

Security type   
[Configure security features](#)

Image \*   
[See all images](#) | [Configure VM generation](#)

VM architecture:  Arm64  x64

Run with Azure Spot discount

Size \*   
[See all sizes](#)

### Administrator account

Authentication type:  SSH public key  Password

Username \*

Password \*

Confirm password \*

### Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports \*  None  Allow selected ports

Select inbound ports \*

**i** All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.

Note: Add ssh & http inbound Port  
Refer: [How to Create Virtual Machine in Azure](#)

# Create a virtual machine ...

Basics   Disks   **Networking**   Management   Monitoring   Advanced   Tags   Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution.

[Learn more](#)

## Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network *	<input type="text" value="VNET01"/>
	<a href="#">Create new</a>
Subnet *	<input type="text" value="SubnetBP (10.0.0.0/24)"/>
	<a href="#">Manage subnet configuration</a>
Public IP	<input type="text" value="(new) VM01-ip"/>
	<a href="#">Create new</a>
NIC network security group	<input type="radio"/> None <input checked="" type="radio"/> Basic <input type="radio"/> Advanced
Public inbound ports *	<input type="radio"/> None <input checked="" type="radio"/> Allow selected ports

[Review + create](#)   [< Previous](#)   [Next : Management >](#)

Repeat the above steps to Create 3 VM.

## Virtual machines

cloudsolutiontalks (hemalatharrbgmail.onmicrosoft.com)

[+](#) Create   [↔](#) Switch to classic   [🕒](#) Reservations   [⚙️](#) Manage view   [🔄](#) Refresh   [↓](#) Export to CSV   [🔗](#) O

  [Subscription equals all](#)   [Type equals all](#)   [Resource group equals all](#)   [Location](#)

Showing 1 to 3 of 3 records.

<input type="checkbox"/>	Name ↑↓	Resource group ↑↓	Virtual network ↑↓	Location ↑↓	Public IP
<input type="checkbox"/>	VM01	RG01	VNET01	East US	168.62.5
<input type="checkbox"/>	VM02	RG01	VNET01	East US	172.173.
<input type="checkbox"/>	VM03	RG01	VNET01	East US	20.172.2

3 Virtual Machines Created

Now Connect to 3 VM's one by one to install nginx web server.

Open PowerShell

```
Ps>ssh azureadmin@vmiipaddress
```

```
azureadmin@VM01:~$ sudo apt-get install nginx
```

Use below command to just add a text to nginx default page

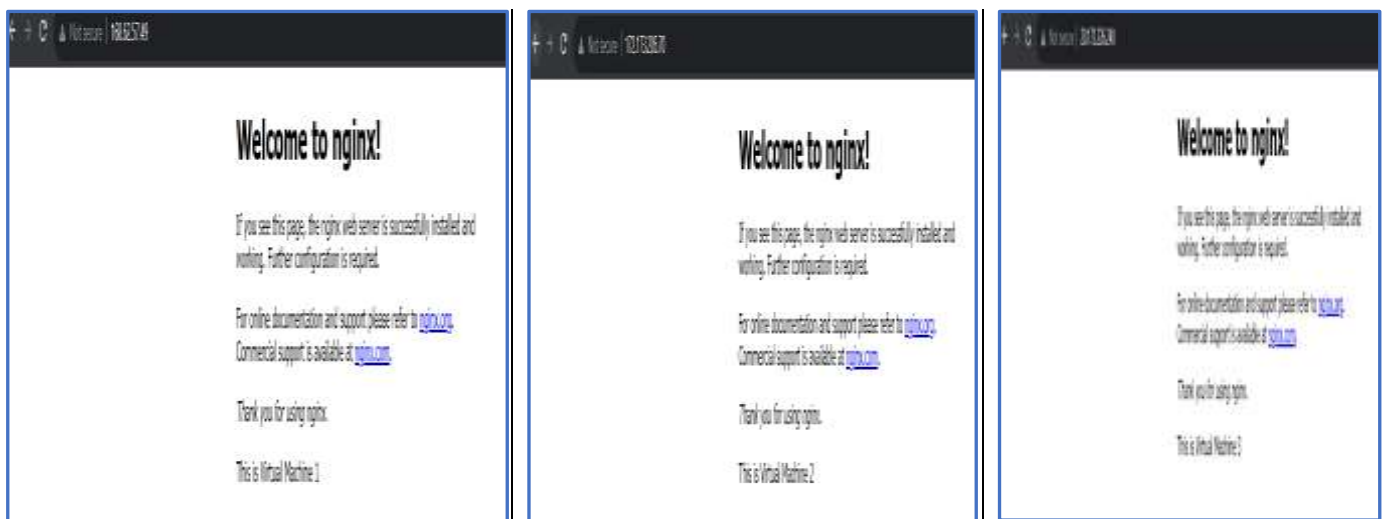
```
cd /var/www/html
```

```
azureadmin@VM01:/var/www/html$ sudo chmod -R 777 index.nginx-debian.html
```

```
azureadmin@VM01:/var/www/html$ echo " This is Virtual Machine 1" >> index.nginx-debian.html.
```

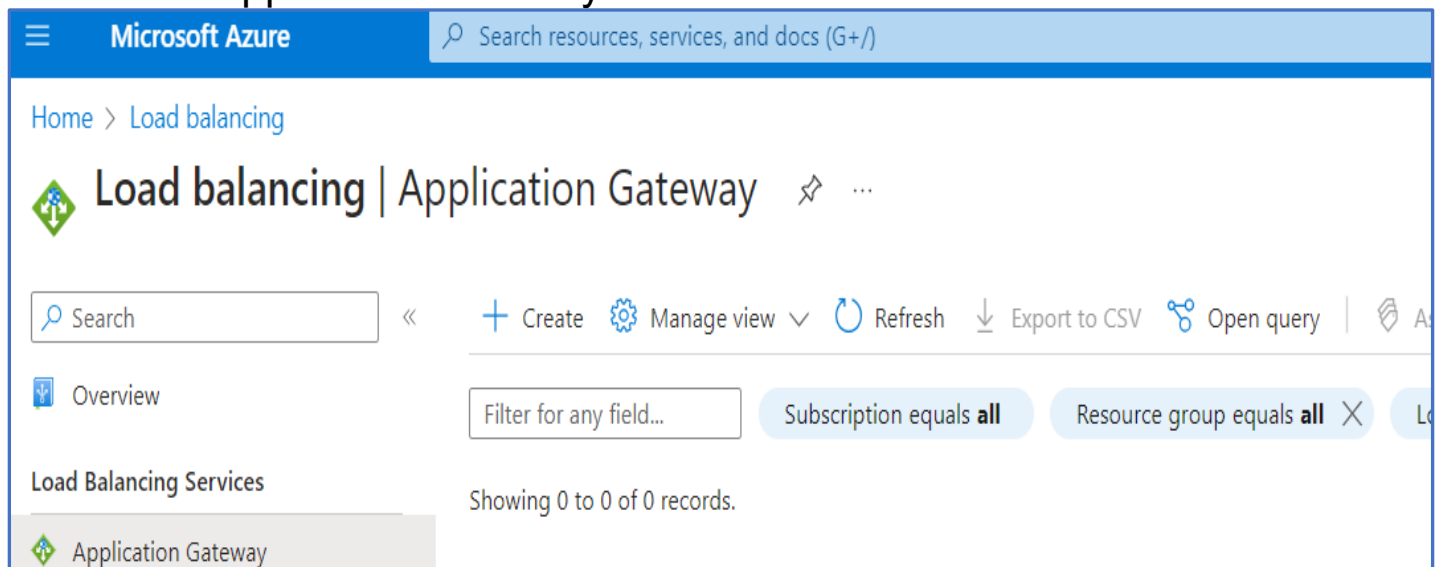
Repeat for all the 3 VM's

Now paste the VM public Ip in the browser (as below)



## Create Application Gateway AG01.

Search for Application Gateway and Create.



## Create application gateway

### Instance details

Application gateway name \*  ✓

Region \*  ▼

Tier ⓘ  ▼

Enable autoscaling  Yes  No

Minimum instance count \* ⓘ

Maximum instance count

Availability zone ⓘ  ▼

HTTP2 ⓘ  Disabled  Enabled

### Configure virtual network

Virtual network \* ⓘ  ▼

[Create new](#)

Subnet \* ⓘ  ▼

[Manage subnet configuration](#)

[Previous](#)

[Next : Frontends >](#)

Else select Tier as WAF, if WAF has to be applied for this application Gateway.

Tier ⓘ  ▼

Instance count \* ⓘ

SKU size ⓘ  ▼

WAF status ⓘ  Disabled  Enabled

WAF mode ⓘ  Detection  Prevention

HTTP2 ⓘ  Disabled  Enabled

Select **SubnetAG** in VNET01.

In this Example I have selected Standard v2 Tier.

## Configure Frontend Ip

[Home](#) > [Load balancing](#) | [Application Gateway](#) >

### Create application gateway ...

✓ Basics   **2 Frontends**   ③ Backends   ④ Configuration   ⑤ Tags   ⑥ Review + create

Traffic enters the application gateway via its frontend IP address(es). An application gateway can use a public IP address, private IP address, or one of each type. [↗](#)

Frontend IP address type ⓘ    Public    Private    Both

Public IP address \*

Choose public IP address

[Add new](#)

#### Add a public IP

Name \*   AGFrontIP ✓

SKU    Basic    Standard

Assignment    Dynamic    Static

Availability zone   None

OK

Cancel

Previous

Next : Backends >

## Add a Backend Pool



Home > Load balancing | Application Gateway >

## Create application gateway

✓ Basics ✓ Frontends **3 Backends** 4 Configuration 5 Tags 6 Review + create

A backend pool is a collection of resources to which your application gateway can send traffic. A backend pool can contain virtual machines, virtual machine scale sets, app services, IP addresses, or fully qualified domain names (FQDN). <sup>1</sup>

Add a backend pool

Backend pool	Targets
No results	

Previous Next: Configuration >

### Add a backend pool.

A backend pool is a collection of resources to which your application gateway can send traffic. A backend pool can contain virtual machines, virtual machine scale sets, IP addresses, domain names, or an App Service.

Name \*

Add backend pool without targets

Add all the 3 VM targets.

Home > Load balancing | Application Gateway >

## Create application gateway

✓ Basics ✓ Frontends **3 Backends** 4 Configuration 5 Tags 6 Review + create

A backend pool is a collection of resources to which your application gateway can send traffic. A backend pool can contain virtual machines, virtual machine scale sets, app services, IP addresses, or fully qualified domain names (FQDN). <sup>1</sup>

Add a backend pool

Backend pool	Targets
AGBackPool	0 targets

Previous Next: Configuration >

### Add a backend pool.

A backend pool is a collection of resources to which your application gateway can send traffic. A backend pool can contain virtual machines, virtual machine scale sets, IP addresses, domain names, or an App Service.

Name \*

Add backend pool without targets

Backend targets

3 items


Target type	Target
Virtual machine	vm01802
Virtual machine	vm02767
Virtual machine	vm03379 (10.0.0.4)
IP address or FQDN	<input type="text"/>

Home > Load balancing | Application Gateway >

## Create application gateway

✓ Basics ✓ Frontends ✓ Backends **4 Configuration** 5 Tags 6 Review + create

Create routing rules that link your frontend(s) and backend(s). You can also add more backend pools, add a second frontend IP configuration if you haven't already, or edit previous configurations. <sup>1</sup>



**Frontends**

+ Add a frontend IP

Public (new) AGFrontIP ⋮



**Routing rules**

+

Add a routing rule



**Backend pools**

+ Add a backend pool

AGBackPool ⋮

# Add Routing Rules

## Add a routing rule

Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target.

Rule name \*

Priority \*

**\* Listener**    **\* Backend targets**

A listener "listens" on a specified port and IP address for traffic that uses a specified protocol. If the listener criteria are met, the application gateway will apply this routing rule.

Listener name \*

Frontend IP \*

Protocol  HTTP     HTTPS

Port \*

Listener type  Basic     Multi site

**Custom error pages**

Show customized error pages for different response codes generated by Application Gateway. This section lets you configure Listener-specific error pages. [Learn more](#)

Bad Gateway - 502

Forbidden - 403

[Show more status codes](#)

## Add Backend setting

[← Discard changes and go back to routing rules](#)

Backend settings name \*

Backend protocol  HTTP     HTTPS

Backend port \*

**Additional settings**

Cookie-based affinity  Enable     Disable

Connection draining  Enable     Disable

Request time-out (seconds) \*

Override backend path

**Host name**

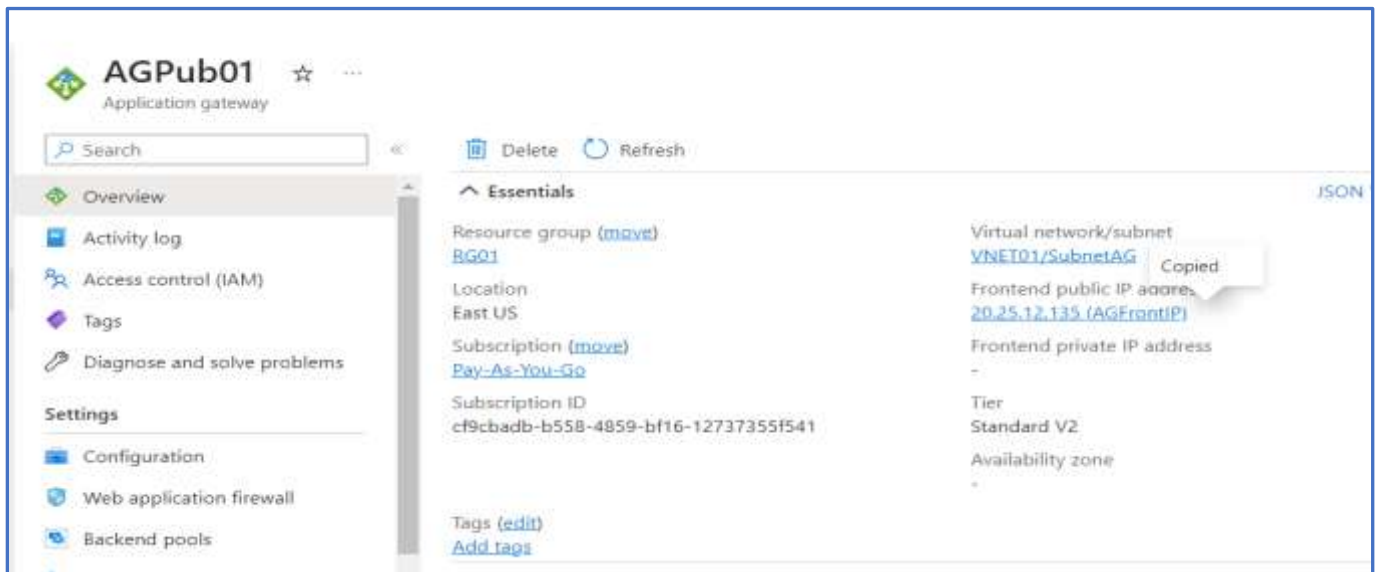
By default, the Application Gateway sends the same HTTP host header to the backend as it receives from the client. If your backend application/service requires a specific host value, you can override it using this setting.

Override with new host name

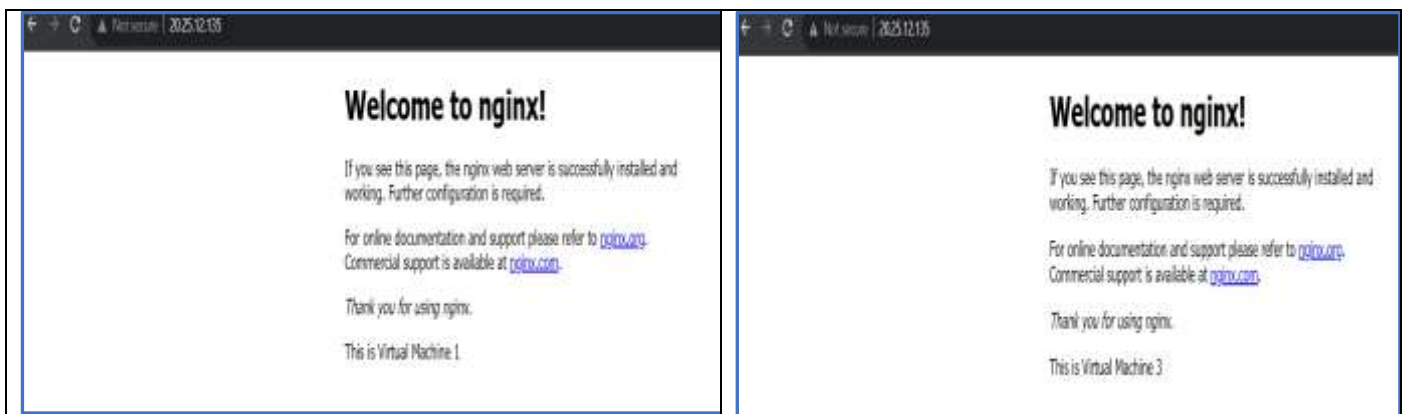
Create custom probes

Click Create Button and wait for Application Gateway to Create.  
**Test the Application Gateway**

## Paste AG Public IP in the Browser



Paste AG Public IP in the Browser. On Refreshing the Browser, we can see the AG connects to other VM's in Backend Pool Server.



## Cleanup the Resource

Select RG01 and Delete.