

DEVOPS with MULTI-CLOUD

Practice Tasks

Institute Name : V Cube software solutions
Course : DevOps with Multi-Cloud
Batch : 30
Trainer : Krishna reddy sir

Prepared by : G.Bhavish
(MCD-AZ30-024)

TASK-7 : Application Security Group (ASG).

Date : 29/01/26

Objective :-

To implement an Azure Application Security Group (ASG) to logically group virtual machines and simplify Network Security Group (NSG) rules by controlling traffic based on application roles rather than IP addresses.

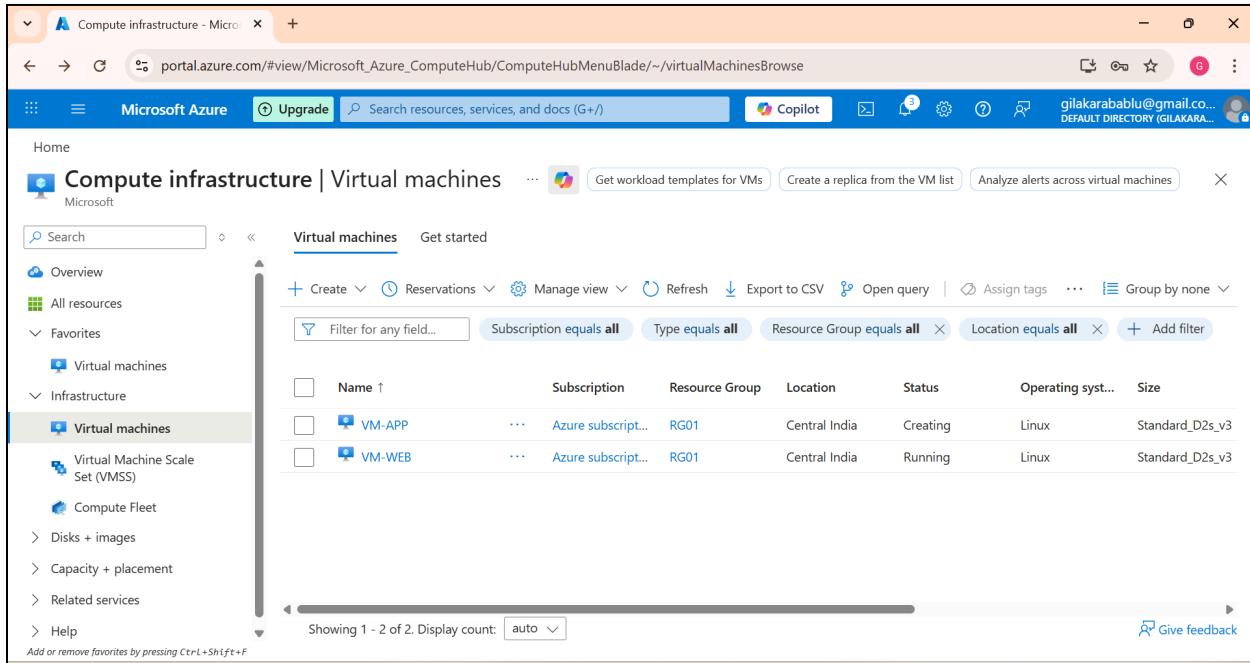
Application Security Group (ASG) :-

- The application security group will logically group the virtual machines and tags them so that it becomes easier for the nsg to create rules.
- The ASG helps the NSG to create rules with the tags rather than the ip addresses.
- Application security group scales automatically when the virtual machines are added.
- To maintain the virtual machine more precisely we use the ASG.
- The prerequisite of the ASG is it works within the virtual network.

To Implement the ASG :-

- Create VM-WEB under the resource group RG01 and virtual network VN01 with subnet SN-WEB.

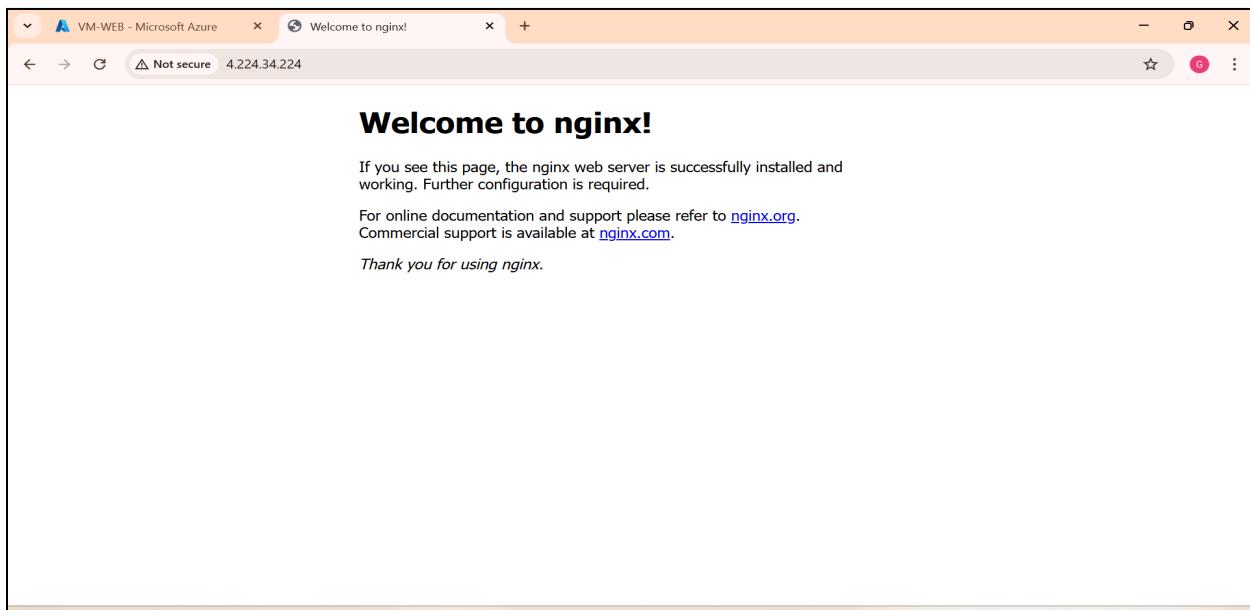
→ Create VM-APP under the resource group RG01 and virtual network VN01 with subnet SN-APP.



The screenshot shows the Microsoft Azure Compute infrastructure Virtual machines page. The left sidebar has 'Virtual machines' selected. The main area displays a table of virtual machines with the following data:

Name	Subscription	Resource Group	Location	Status	Operating system	Size
VM-APP	Azure subscription	RG01	Central India	Creating	Linux	Standard_D2s_v3
VM-WEB	Azure subscription	RG01	Central India	Running	Linux	Standard_D2s_v3

Fig (1) successfully created vm-web and vm-app.



The screenshot shows a web browser displaying the 'Welcome to nginx!' page for the VM-WEB instance. The URL is 4.224.34.224. The page content includes:

Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

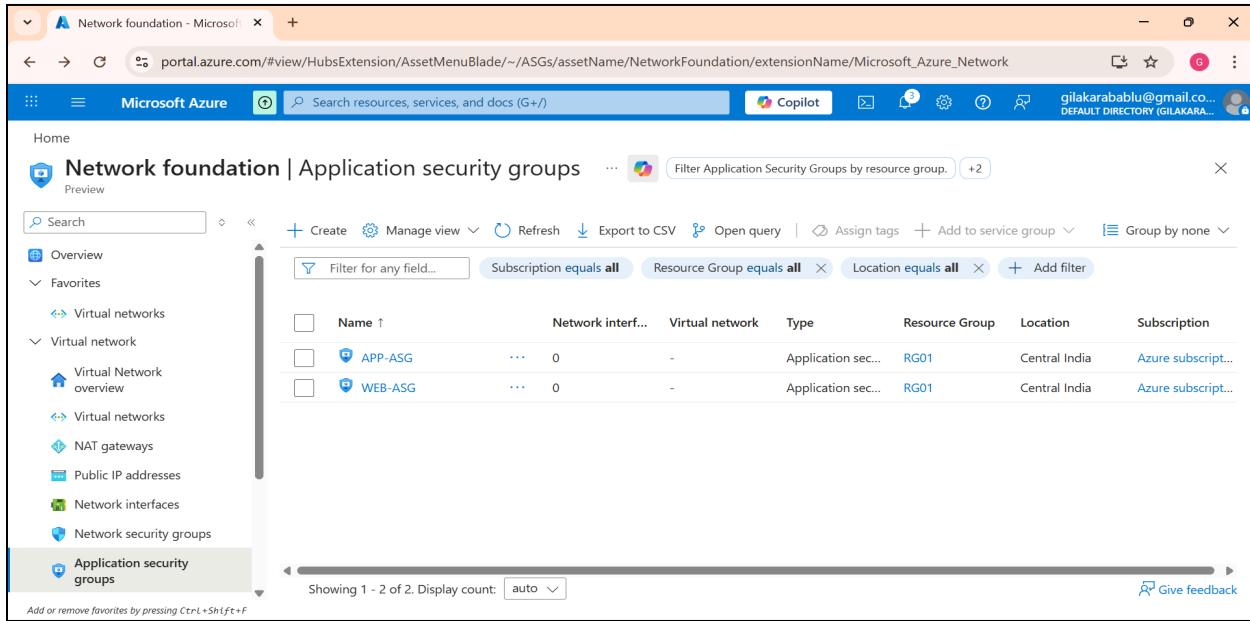
For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.

Fig (2) successfully installed nginx in vm-web.

→ Normally created nsg for vm-web to validate and deleted after successfully installing nginx.

→ Now create asg for the virtual machines vm-web & vm-app.



The screenshot shows the Microsoft Azure portal interface for managing Application Security Groups (ASGs). The left sidebar navigation includes 'Overview', 'Favorites' (with 'Virtual networks'), 'Virtual network' (containing 'Virtual Network overview', 'Virtual networks', 'NAT gateways', 'Public IP addresses', 'Network interfaces', and 'Network security groups'), and 'Application security groups'. The main content area displays a table of ASGs with the following data:

Name	Network interface count	Virtual network	Type	Resource Group	Location	Subscription
APP-ASG	0	-	Application sec...	RG01	Central India	Azure subscript...
WEB-ASG	0	-	Application sec...	RG01	Central India	Azure subscript...

fig(3) successfully created asg for both vm's

→ Now we need to add these asg to their respective virtual machines.

→ Now we can create NSG and write rules using the asg tags.

→ While writing the rules we will use the asg tags instead of the ip addresses.

- For eg:- In the source and destination of the nsg rules we will mention the asg tags rather than the virtual machines ip addresses.

→ After creating the nsg and writing the rules we need to associate it to the nic-level of the virtual machines.

The screenshot shows the Microsoft Azure portal interface for managing Network Security Groups (NSGs). The left sidebar navigation bar is visible, showing options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Resource visualizer, Settings, Inbound security rules (which is selected and highlighted in blue), Outbound security rules, Network interfaces, Subnets, and Properties. The main content area is titled "NSG-1 | Inbound security rules" and displays a table of security rules. The table has columns for Name, Port, Protocol, Source, Destination, and Action. There are six rules listed:

Name	Port	Protocol	Source	Destination	Action
ALLOW-80	80	Any	Any	WEB-ASG	Allow
ALLOW	8080	Any	Any	WEB-ASG	Allow
AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
AllowAzureLoadBalanc...	Any	Any	AzureLoadBalancer	Any	Allow
DenyAllInBound	Any	Any	Any	Any	Deny

fig (4) successfully created nsg and the rules with asg tags.

The screenshot shows the Microsoft Azure portal interface for managing Network Security Groups (NSGs). The left sidebar navigation bar is visible, showing options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Resource visualizer, Settings, Inbound security rules, Outbound security rules (which is selected and highlighted in blue), Network interfaces (selected), Subnets, and Properties. The main content area is titled "NSG-1 | Network interfaces" and displays a table of network interfaces associated with the NSG. The table has columns for Name, Public IP address, Private IP address, and Virtual machine. Two network interfaces are listed:

Name	Public IP address	Private IP address	Virtual machine
vm-app27	104.211.73.103	172.16.1.4	VM-APP
vm-web188	4.224.34.224	172.16.0.4	VM-WEB

Fig (5) successfully associated the nsg to the vm's.