12 Days of Azure

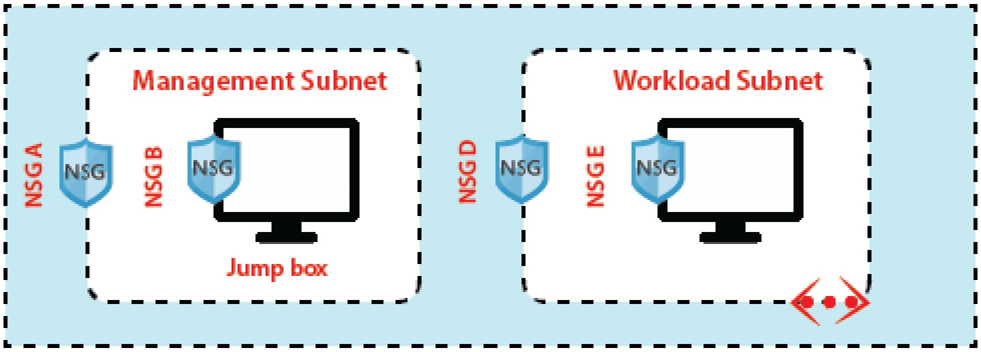
Azure Cloud & Its Services

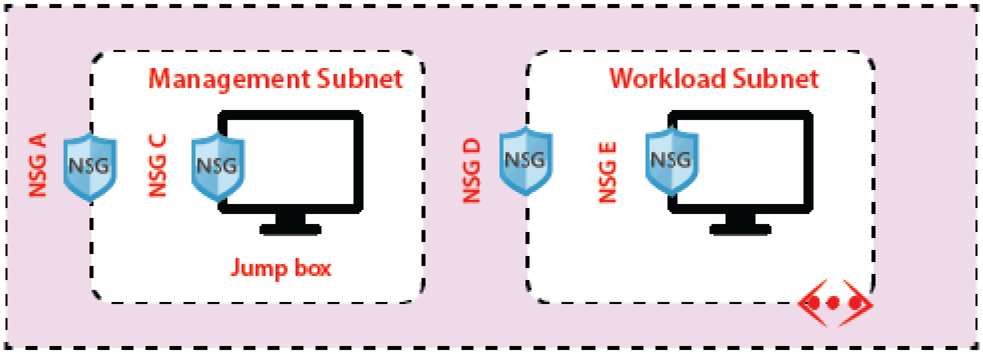
Mrunali Jibhakate

DAY-6

Azure Network Security

A network security group consists of security rules that allow or deny inbound/Outbound network traffic to or from different types of Azure resources that we will host in our Azure virtual network. And we can apply the network security group at different levels. For example:





Security rule properties:

Name: The name of the network should be unique within the network security group.

Priority: Security rules are processed in priority order with a lower number has the highest priority.

Source or Destination: (The IP address, CIDR (Classless inter-domain routing) block, service tag, or application security group) The ability to specify multiple individual IP addresses and ranges in a rule is referred to as augmented security rules.

Protocol: TCP, UDP, etc.

Port range: we can specify an individual or range of ports

Action: Allow or Deny

Service Tags

Service tag represents a group of IP address prefixes to help minimize complexity for security rule creation. We cannot create our service tag, nor specify which Ip address is included within a tag. Microsoft manages the address prefixes encompassed by the service tag, and automatically updates the service tag as an address change.

Earlier, if we want to allow communication to Azure service from our virtual machine, we need to configure IoT of outbound rules because Microsoft is providing list of IP addresses for each service you need to configure those list of IP addresses in our NSG rule to allow outbound connection from our virtual machine to that particular service and also in case if Microsoft is changing the addresses you need to change your rules.

Using service tags will simplify your NSG rules a lot, for example:

Storage: This tag denotes the IP address space for the Azure Storage service. If you specify Storage for the value, traffic is allowed or denied to storage.

SQL: This tag denotes the address prefixes of the Azure SQL Database, Azure Database for MySQL, Azure Database for PostgreSQL, and Azure SQL Data Warehouse services.

Azure CosmosDB: This tag denotes the address prefixes of the Azure Cosmos Database services.

AzureKeyVault: This tag denotes the address prefixes of the Azure KeyVault service. If you specify AzureKeyVault for the value, traffic is allowed or denied to AzureKeyVault.

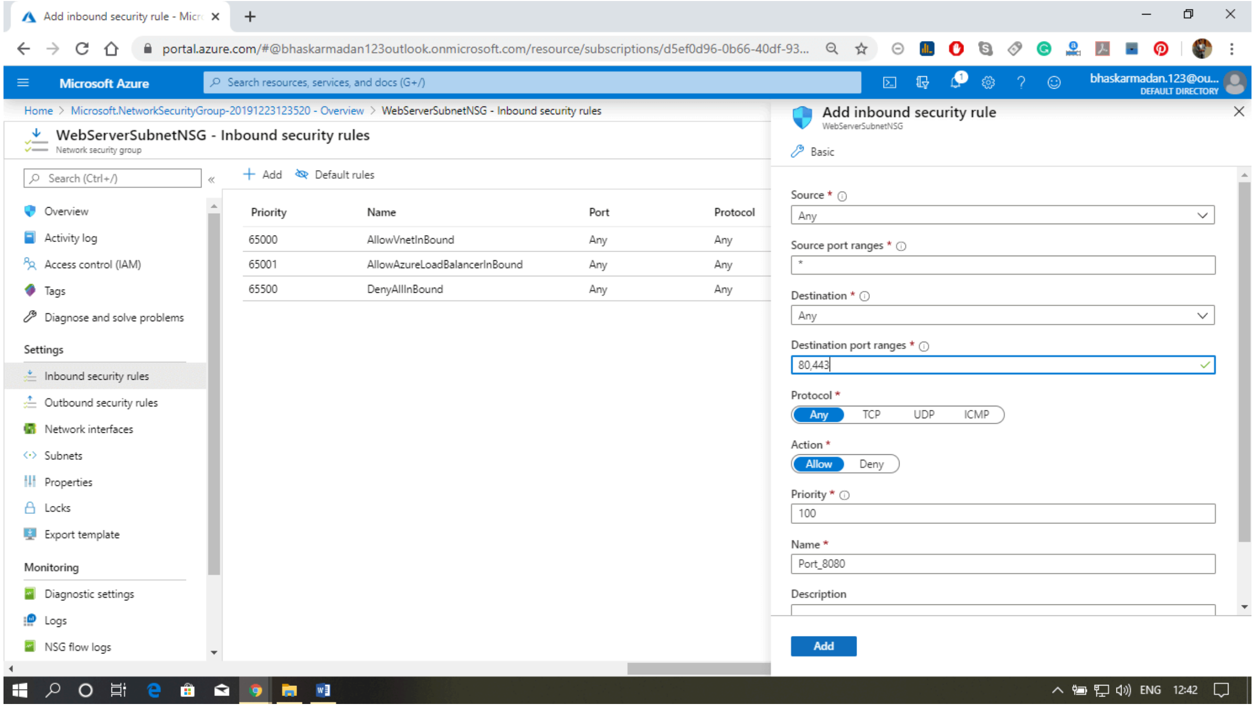
EventHub: This tag denotes the address prefixes of the Azure EventHub service. If you specify EventHub for the value, traffic is allowed or denied to EventHub.

Default Rules

Some default rules are created by default when we create NSG. There are two types of default rules.

Inbound Security rules

- **AllowVNetInbound:** Traffic is allowed from any resources within the VNet
- **AllowAzureLoadBalancerInbound:** Any traffic originating from Azure load-balancer to any of the virtual machines within the network is permitted.
- **DenyAllInbound:** By default, virtual machines in the virtual network can communicate with each other, and also Azure load balancer can communicate with virtual machines within the virtual network.



Add inbound security rule - Micr
portal.azure.com/#@bhaskarmadan123outlook.onmicrosoft.com/resource/subscriptions/d5ef0d96-0b66-40df-93...
Microsoft Azure
Search resources, services, and docs (G+/)
bhaskarmadan.123@ou...
DEFAULT DIRECTORY
Home > Microsoft.NetworkSecurityGroup-20191223123520 - Overview > WebServerSubnetNSG - Inbound security rules
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Inbound security rules
Outbound security rules
Network interfaces
Subnets
Properties
Locks
Export template
Monitoring
Diagnostic settings
Logs
NSG flow logs
+ Add
Default rules
Basic
Add
ENG
12:42

WebServerSubnetNSG - Inbound security rules
Network security group

Priority	Name	Port	Protocol
65000	AllowVnetInBound	Any	Any
65001	AllowAzureLoadBalancerInBound	Any	Any
65500	DenyAllInBound	Any	Any

Add inbound security rule
WebServerSubnetNSG

Source *: Any

Source port ranges *: *

Destination *: Any

Destination port ranges *: 80,443

Protocol *: [✓ Any] TCP UDP ICMP

Action *: [✓ Allow] Deny

Priority *: 100

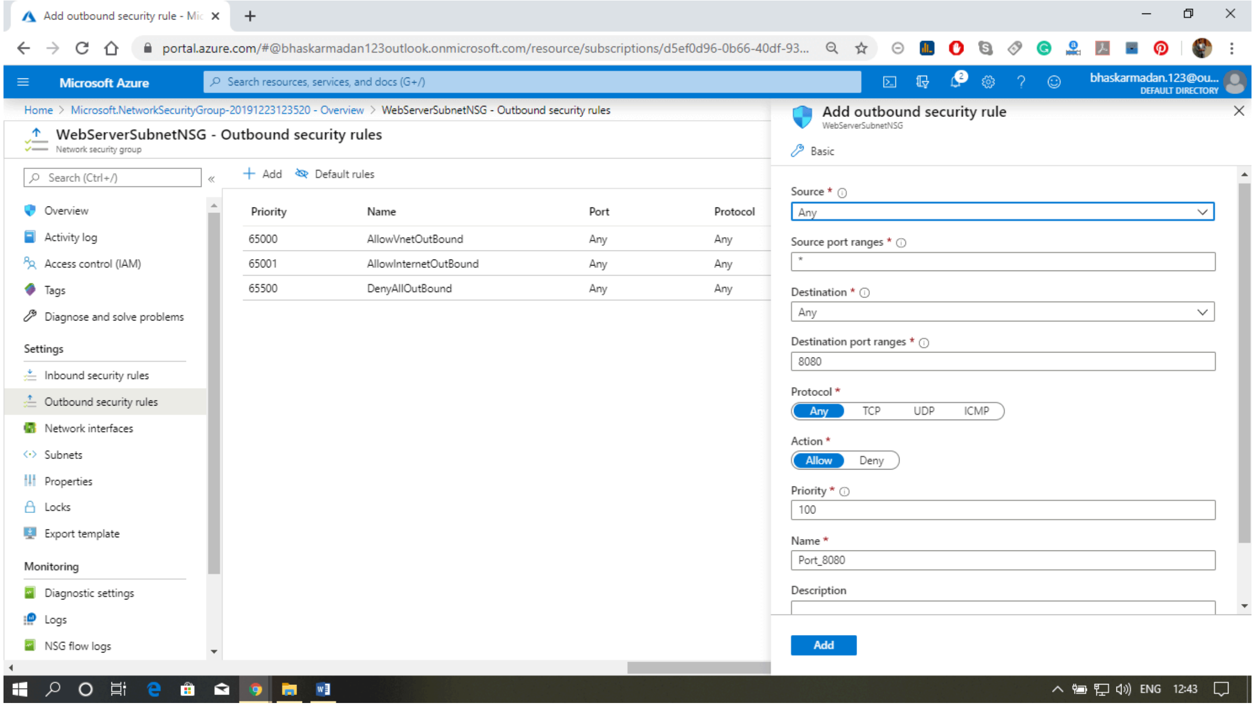
Name *: Port_8080

Description

Outbound Security rules

- **AllowVNetOutBound:** Traffic is allowed through any resources within the VNet
- **AllowInternetOutBound:** Traffic originating from any resources in the VNet to the Internet is allowed.

- ○ **DenyAllOutBound:** By default, virtual machines in a virtual network can communicate with each other, and also Azure load balancer can interact with the virtual machine within the virtual network.



Add outbound security rule - Mic
portal.azure.com/#@bhaskarmadan123outlook.onmicrosoft.com/resource/subscriptions/d5ef0d96-0b66-40df-93...
Microsoft Azure
Search resources, services, and docs (G+/)
bhaskarmadan.123@ou...
DEFAULT DIRECTORY
Home > Microsoft.NetworkSecurityGroup-20191223123520 - Overview > WebServerSubnetNSG - Outbound security rules
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Inbound security rules
Outbound security rules
Network interfaces
Subnets
Properties
Locks
Export template
Monitoring
Diagnostic settings
Logs
NSG flow logs
+ Add
Default rules
ENG
12:43

WebServerSubnetNSG - Outbound security rules
Network security group

Priority	Name	Port	Protocol
65000	AllowVnetOutBound	Any	Any
65001	AllowInternetOutBound	Any	Any
65500	DenyAllOutBound	Any	Any

Add outbound security rule
WebServerSubnetNSG

Basic

Source *: Any

Source port ranges *: *

Destination *: Any

Destination port ranges *: 8080

Protocol *: [✓ Any] TCP UDP ICMP

Action *: [✓ Allow] Deny

Priority *: 100

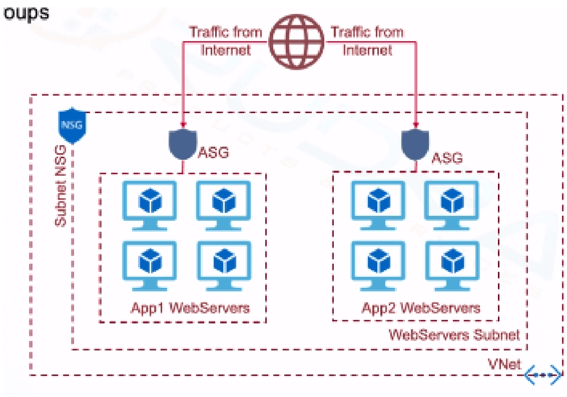
Name *: Port_8080

Description:

Add

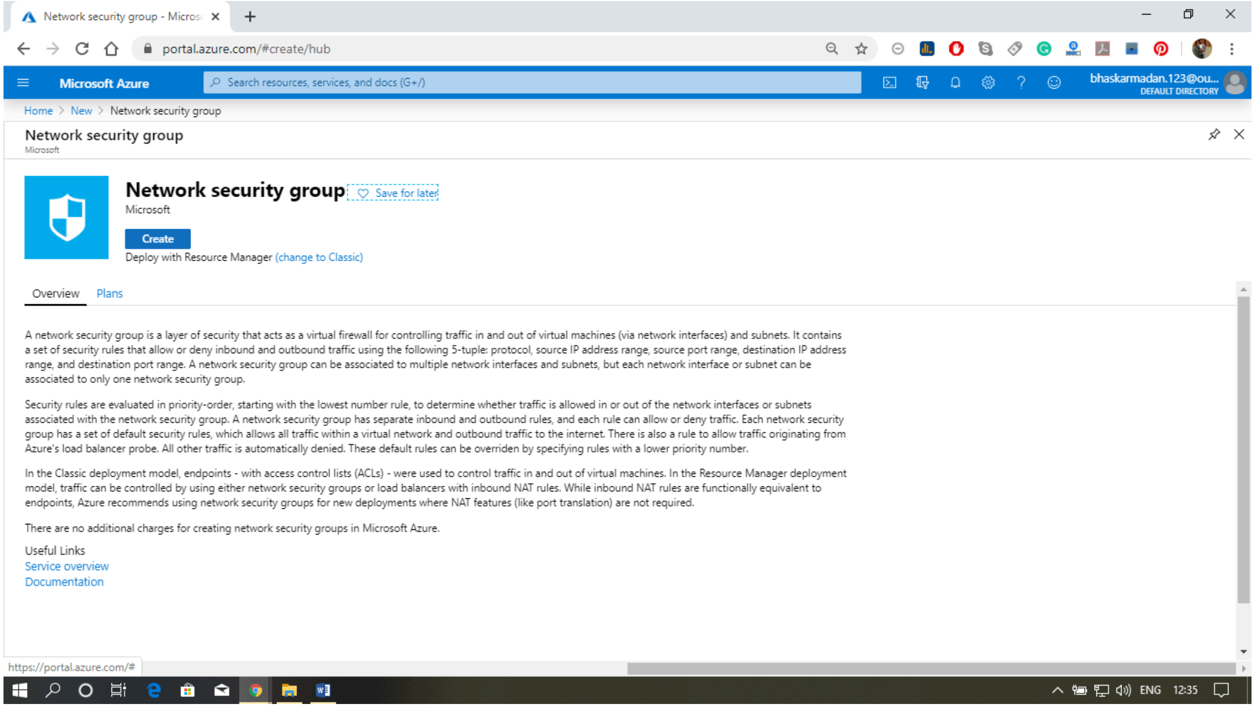
Application Security Groups

Application security groups enable you to configure network security as a natural extension of an application's structure, allowing you to group virtual machines and define network security policies based on those groups. For example -



Configuring an NSG at Subnet and VM level

Step 1: Click on create a resource button and type-in Network Security Group. Then select Network Security Group, and click on create button


Network security group - Micros
portal.azure.com/#create/hub
Microsoft Azure
Search resources, services, and docs (G+/)
bhaskarmadan.123@ou...
DEFAULT DIRECTORY
Home > New > Network security group
Network security group
Microsoft
Save for later
Create
Overview
Plans
https://portal.azure.com/#
ENG
12:35

Network security group

Microsoft

Deploy with Resource Manager (change to Classic)

A network security group is a layer of security that acts as a virtual firewall for controlling traffic in and out of virtual machines (via network interfaces) and subnets. It contains a set of security rules that allow or deny inbound and outbound traffic using the following 5-tuple: protocol, source IP address range, source port range, destination IP address range, and destination port range. A network security group can be associated to multiple network interfaces and subnets, but each network interface or subnet can be associated to only one network security group.

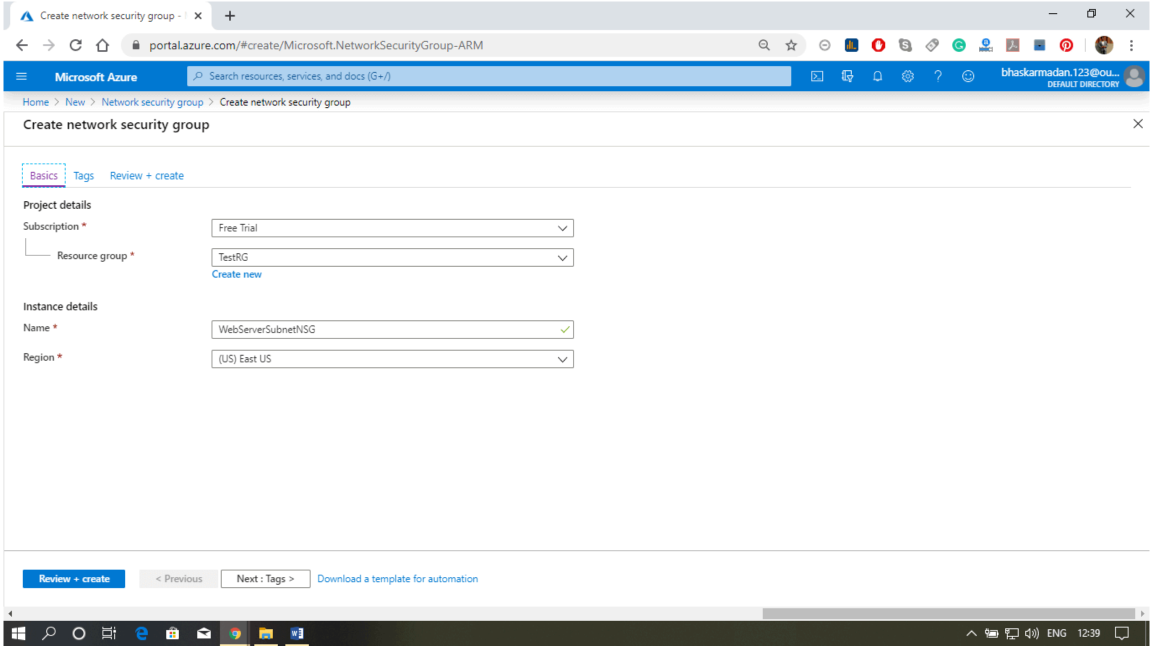
Security rules are evaluated in priority-order, starting with the lowest number rule, to determine whether traffic is allowed in or out of the network interfaces or subnets associated with the network security group. A network security group has separate inbound and outbound rules, and each rule can allow or deny traffic. Each network security group has a set of default security rules, which allows all traffic within a virtual network and outbound traffic to the internet. There is also a rule to allow traffic originating from Azure's load balancer probe. All other traffic is automatically denied. These default rules can be overriden by specifying rules with a lower priority number.

In the Classic deployment model, endpoints - with access control lists (ACLs) - were used to control traffic in and out of virtual machines. In the Resource Manager deployment model, traffic can be controlled by using either network security groups or load balancers with inbound NAT rules. While inbound NAT rules are functionally equivalent to endpoints, Azure recommends using network security groups for new deployments where NAT features (like port translation) are not required.

There are no additional charges for creating network security groups in Microsoft Azure.

Useful Links
Service overview
Documentation

Step 2: Now, you are on the Network Security Group creation page. Select the resource group, fill the name, select the region, and click on review+create.


Create network security group - ×
portal.azure.com/#create/Microsoft.NetworkSecurityGroup-ARM
Microsoft Azure
Search resources, services, and docs (G+/)
bhaskarmadan.123@ou...
DEFAULT DIRECTORY
Home > New > Network security group > Create network security group
Basics
Tags
Review + create
Create new
Review + create
< Previous
Next : Tags >
Download a template for automation
ENG
12:39

Create network security group

Project details

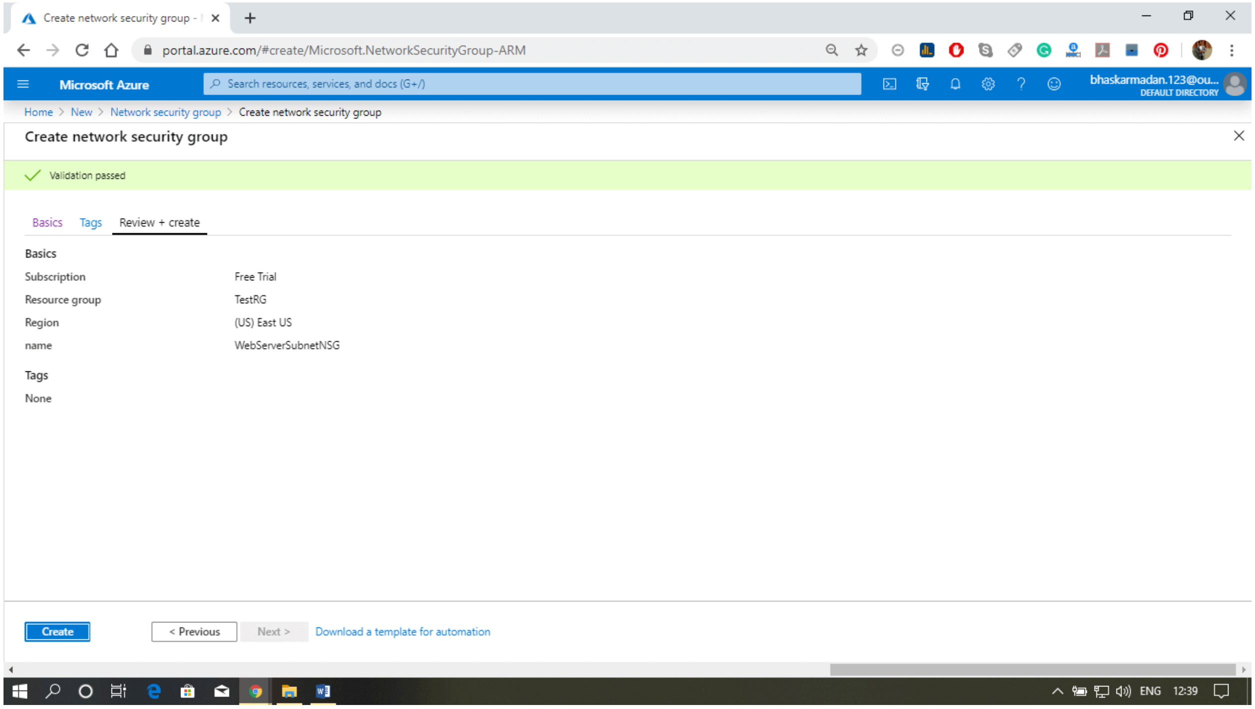
Subscription * Free Trial

Resource group * TestRG

Instance details

Name * WebServerSubnetNSG

Region * (US) East US



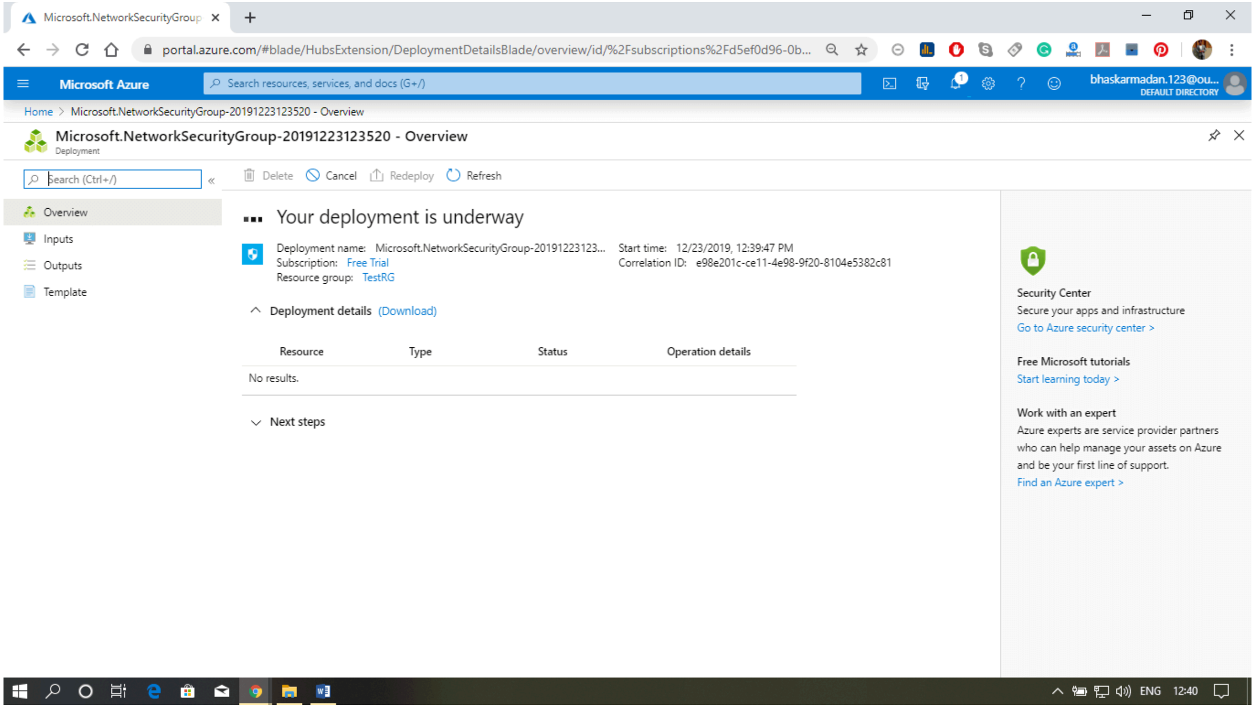
Create network security group

Validation passed

Basics	
Subscription	Free Trial
Resource group	TestRG
Region	(US) East US
name	WebServerSubnetNSG
Tags	
None	

portal.azure.com/#create/Microsoft.NetworkSecurityGroup-ARM
Microsoft Azure
Home > New > Network security group > Create network security group
Basics
Tags
Review + create
Create
< Previous
Next >
Download a template for automation

Step 3: Your NSG is created, now we will associate this NSG with the subnet.



Microsoft.NetworkSecurityGroup-20191223123520 - Overview

Your deployment is underway

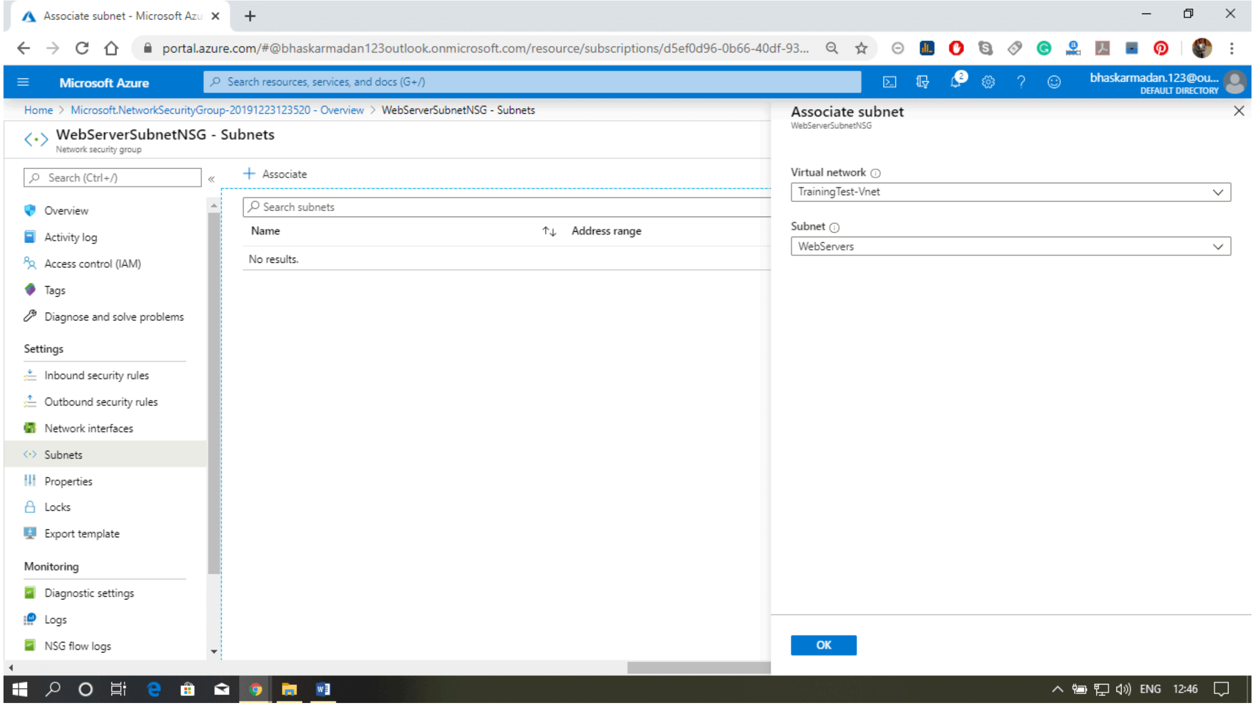
Deployment name: Microsoft.NetworkSecurityGroup-20191223123...
Subscription: Free Trial
Resource group: TestRG
Start time: 12/23/2019, 12:39:47 PM
Correlation ID: e98e201c-ce11-4e98-9f20-8104e5382c81

Deployment details (Download)

Resource	Type	Status	Operation details
No results.			

portal.azure.com/#blade/HubsExtension/DeploymentDetailsBlade/overview/id/%2Fsubscriptions%2Fd5ef0d96-0b...
Microsoft Azure
Home > Microsoft.NetworkSecurityGroup-20191223123520 - Overview
Deployment
Overview
Inputs
Outputs
Template
Delete
Cancel
Redeploy
Refresh
Next steps
Security Center
Secure your apps and infrastructure
Go to Azure security center >
Free Microsoft tutorials
Start learning today >
Work with an expert
Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support.
Find an Azure expert >

Step 4: Click on the subnet, then click on add Associate. Select the virtual network and subnet with which you want to associate this NSG.



Virtual network: TrainingTest-Vnet

Subnet: WebServers

Step 5: Finally, click on the ok button. Your NSG is now associated with the subnet.

FOLLOW FOR MORE!

THANK YOU

Mrunali Jibhakate