QA Consulting

Azure CLI Network Security Groups

TRAINING MATERIALS - MODULE HANDOUT

Contacts

robert.crutchley@qa.com

team.qac.all.trainers@qa.com

www.consulting.qa.com

Contents

Overview

You could think of Network Security Groups (**NSG**) as a Firewall effectively. They are groups that resources can be added to, which allow or deny inbound or outbound traffic according to a set of rules. Just like firewalls, these rules can be applied depending on IP addresses, ports and protocols.

Creating

Basic Usage

The name and Resource Group need to be provided when creating a Network Security Group.

```
az network nsg create --resource-group [RESOURCE_GROUP] --name [NSG_NAME]
```

```
az network nsg create --resource-group MyResourceGroup --name
MyNetworkSecurityGroup
```

Deleting

Basic Usage

Provide the name and Resource Group of the Network Security Group

```
az network nsg delete --resource-group [RESOURCE_GROUP] --name [VNET_NAME]
```

```
az network nsg delete --resource-group MyResourceGroup --name
MyVirtualNetwork
```

Rules

Rules for Network Security Groups are what make them useful. Here we can define what effect is going to be made when a resource is added to the NSG.

Create

To create a new Rule it must have a name, priority, NSG name and of course a resource group. The priority determines the authority in a way over other rules, if a rule has a higher priority over others, then it will override the ones with a lower priority. Priorities range from 100-4096, 100 being the highest.
All the rules within an NSG must have different priorities.

Basic “Allow” rule with a priority of 500 on port 80, port 80 is the default port.

```
az network nsg rule create --resource-group [RESOURCE_GROUP] --name [VNET_NAME] --priority [PRIORITY] --nsg-name [NSG_NAME]
```

```
az network nsg rule create --resource-group MyResourceGroup --name MyVirtualNetwork --priority 500 --nsg-name MyNetworkSecurityGroup
```

Allow a Port

If you would like to allow a port, it’s going to be best practice to deny access to all other ports, with a lower priority, fortunately Azure does this for us automatically. By default rules are for **Inbound** connections. Here’s an example allowing incoming traffic on port 22 with any protocol.

```
az network nsg rule create --resource-group [RESOURCE_GROUP] --name [VNET_NAME] --priority [PRIORITY] --nsg-name [NSG_NAME] --destination-port-ranges [DESITNATION_PORT_RANGES]
```

```
az network nsg rule create --name SSH --destination-port-ranges 22 --nsg-name MyNetworkSecurityGroup --priority 400
```

Tasks

- Create a Resource Group called **NetworkSecurityGroupExercises**
- Create a new Network Security Group called **MyNetworkSecurityGroup**
- Create a Rule for your new network group that allows port 22
- Create a Rule that allows port 443
- Delete the **NetworkSecurityGroupExercises** Resource Group