greatlearning
Learning for Life

Azure | Lab Brief

Working with Azure Networks
(Configure a load balancer using Traffic Manager and build a Virtual Network architecture for a web application)

greatlearning
Learning for Life

Learning Outcomes

1. Create resource groups in different regions
2. Add an app with an App Service plan to a Resource group
3. Create Traffic Manager Profiles
4. Add Endpoints to Traffic Manager Profiles
5. Create Network Security Groups
6. Define rules for Network Security Groups

How To Do It?-1

1) Create 2 resource groups in different regions
2) Create a Web App inside each Resource group and add each to a different App Service Plan
3) Create a third resource group in any region of your choice
4) Create a Traffic Manager profile inside the third Resource Group in Performance mode.
5) In the Traffic Manager profile created, add the URLs of the 2 Web Apps created previously as endpoints or by selecting the App Service names.
6) Use the following tool to check which endpoint is being queried by entering the DNS name of the Traffic Manager profile
   https://www.ultratools.com/tools/dnsLookup
7) Disable the endpoint being queried in the previous step by stopping the corresponding App Service and confirm that traffic is now being routed to the other endpoint by repeating step 6.

How To Do It? -2

8) Inside NSGTest, create 2 network security groups according to the following rules

a)Group 1 name : FrontEndNSG

i) Inbound Allow Port 80 from anywhere ,priority 100

ii) Outbound Allow Port 4531 from 172.168.1.0/28 to 172.168.1.16/28, priority 110

iii) Inbound Deny All from Anywhere, priority 20000

iv) Outbound Deny All to Anywhere , priority 20000

b) Group 2 name : BackEndNSG

i) Inbound Allow Port 4531 from 172.168.1.0/28 to 172.168.1.16/28, priority100

ii) Outbound Allow Port 3306 to anywhere, priority 110

iii) Inbound Deny All from Anywhere, priority 20000

iv) Outbound Deny All to Anywhere , priority 20000