

Lab 6: Azure Application Gateway (cont..)

Objective

1. Adding Health probe
2. Enabling WAF

Note:

1. All the steps are to be done within Azure Portal.
2. There will be breakout rooms assigned and each room will have a group number [1-5]
3. Login into Azure Portal
 - a. Go to <https://portal.azure.com>
 - b. Login with the supplied credentials (username and password).
 - i. Each group has a unique integer for their login [1-5] eg. usergroup[1-5]
 - ii. For example, group number 5 will have
 1. Username: usergroup5@makecloudwork.com
 2. Password: will be provided during the class.
 - c. You will then see the landing Azure homepage. Dismiss any popups/message boxes

It's important that you enter all the resource names same as mentioned.

Section 1: Adding Health Probe

Steps

1. Within the Application Gateway, click on **Health probes** under Settings
2. Click on **"Add"**
 - a. Name: Enter **"vm_probe"**
 - b. Protocol : Select **"HTTP"**
 - c. Host: Enter **"10.0.0.4"**
 - d. Pick hostname from backend settings: Select **"No"**
 - e. Pick port from backend settings: Select **"Yes"**
 - f. Path: Enter **"/"**
 - g. Backend settings: Select **"be_setting_http_vm"**
 - a. Click on **"Test"**
 - b. Once it passes, click on **"Save"**
3. Click on **Backend health** under Monitoring
 - a. Wait for it to run and notice the status and Details

Section 2: Enabling Web Application Firewall (WAF)

Steps

1. Within the Application Gateway, click on **Web application firewall** under Settings
2. Change the Tier to **"WAF V2"**
 - a. WAF status: Change to **"Enabled"**
 - b. WAF mode: Select **"Prevention"**
 - c. Max request body size: Enter **"128"**
 - d. Select **"Rules"** tab
 - i. Ensure that the Rule set is **"OWASP 3.2"**
 - e. Click on **"Save"**

Observations

1. Once that is completed, you may call the Application gateway on [https://appgatewaysb\[1-5\].makecloudwork.com](https://appgatewaysb[1-5].makecloudwork.com). You should see the secured nginx homepage.

End of Lab.