**Overview**

In this exercise, you will be configuring some additional Azure-related resources and configurations along with looking at a server 2003 migration

**Tasks**

1. Review Log analytics queries and create some alerts based of the data collected. Examples include:-

* VM heart beat alert

1. The customer wants to make the http connection publicly accessible using an Application Gateway and removing the UbuntuWAF VM
   1. Create self-signed certificate
   2. Create Application Gateway and assign self-signed SSL certificate
   3. SSL-offload to happen on Application Gateway, back-end web pool still Http
2. Internet access of VMs to be restricted to specific URLs only – setup this configuration with Azure Firewall (Azure Route tables to be used)
   1. See below URL whitelist
3. Review Azure Security centre recommendations (can any be implemented?) – Currently Azure Security centre free tier is enabled
4. Configure start/stop solution of VMs (9am-5pm GMT)
5. Customer has mentioned the use of Azure Bastion rather than accessing VMs via RDP from Hyper-V host – can this also be implemented
6. Customer wants the server 2003 migrated to Azure, how can this be done? Review and plan accordingly to attempt on migrating server 2003 successfully into Azure

**AzureFirewall URL Whitelist**

**Application Rule Collection**

* MicrosoftActiveProtectionService
* WindowsDiagnostics
* WindowsUpdate
* AzureBackup

**Target FQDNs**

|  |  |  |
| --- | --- | --- |
| Name | Protocol | FQDNs |
| Microsoft-related | https | \*.microsoft.com |
| Azure-Monitor | https | \*.ods.opinsights.azure.com  \*.oms.opinsights.azure.com |
| Log-Analytics | https | dc.applicationinsights.microsoft.com  dc.services.visualstudio.com |
| Azure-Automation | https | \*.azure-automation.net |
| Azure-Site-recovery | https | \*.blob.core.windows.net  login.microsoftonline.com  \*.hypervrecoverymanager.windowsazure.com  \*.servicebus.windows.net |
| AV | https | www.msftncsi.com |

**Exercise targets**

1. Create Log Analytics alerts for at least the below and confirm a successful test:-

* VM heart beat alert

1. Deploy Azure Firewall successfully with required firewall rules & NAT’ing
2. Create SSL configuration to work with Azure Firewall
3. Restrict internet access of VMs with Azure Firewall and routing
4. Review Azure Security Centre (free tier) & confirm any recommendations that you would consider
5. Implement and configure Azure Bastion
6. Configure start/stop solution of VMs (9am-5pm GMT)
7. Have server2003 VM accessible in Azure