**Trainer notes for exercises :-**

1. **UbuntuWAF will be deployed with incorrect IP/Route , commands below:-**

Ifconfig eth0 10.2.2.15 netmask 255.255.255.0

route add default gw 10.2.2.1 eth0

Confirm nginx redirect is set OK to SmartHotelWeb1

/etc/nginx/nginx.conf

Configured with static IP in /etc/network/interfaces

Change to:-

auto eth0

iface eth0 inet dhcp

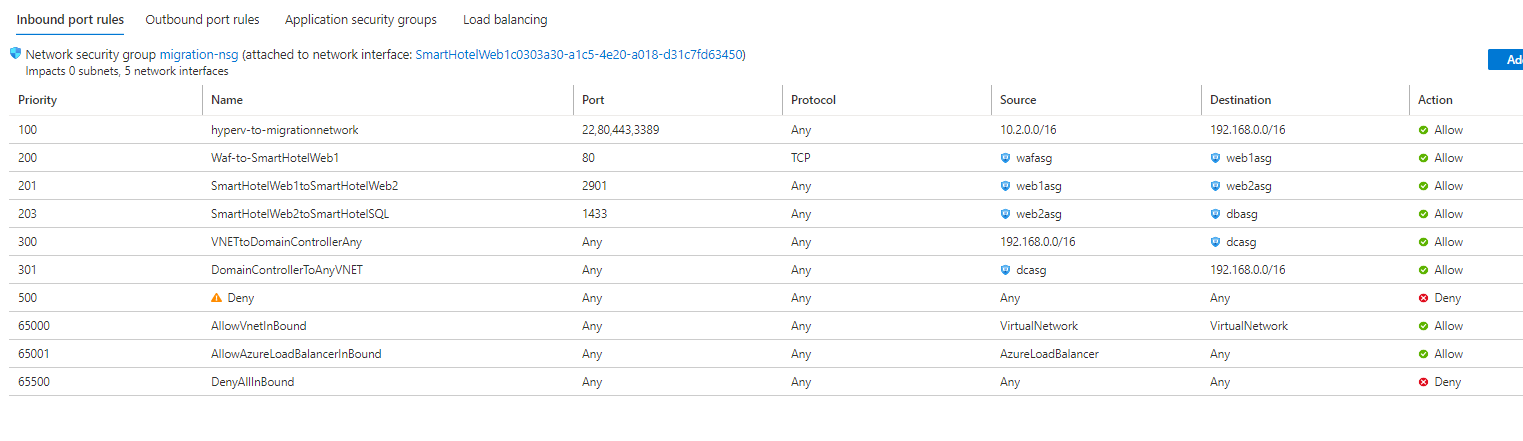
Restart VM or

ifdown eth0; ifup eth0

**Easter Eggs:-**

1. UbuntuWAF has a different IP/route to the hyper-v network and currently not communicating with LA
2. UbuntuWAF has been configured with a static IP in /etc/network/interfaces if they change only ifconfig, when VM reboots it will recreate with static IP (Will cause issues if not noticed when migrated into Azure)
3. UbuntuWAF also has wrong IP in nginx config to redirect to SmartHotelWeb1
4. SmartHotelSQL1 has allow remote connections disabled. If they do not confirm all RDP connections are successful from the host, it will be fine until migrated and attempt to RDP
5. SmartHotelSQL1 has got firewall tcp/1433 restricted to hyper-v /24 network
6. Show them dependency view & log analytics queries if required (Initial preparation will show how to query using log analytics)
7. NSG Rulelist for successful communication

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Priority | Name | Port | Protocol | Source | Destination |
| 100 | HypervHosttoWAF | 80 | TCP | HyperVHost IP | WAFasg |
| 101 | HyperVhosttoNetwork | 3389,22 | TCP | HyperVHost IP | vNETIP |
| 200 | WAFtoSmartHotelWeb1 | 80 | TCP | WAFasg | Web1asg |
| 300 | SmartHotelWeb1toSmartHotelWeb2 | 2901 | TCP | Web1asg | Web2asg |
| 400 | SmartHotelWeb2toSmartHotelSQL | 1433 | TCP | Web2asg | SQL1asg |
| 500 | DomainControllerToAnyVNET | \* | TCP/UDP | DCasg | vnetIP |
| 600 | VNETtoDomainControllerAny | \* | TCP/UDP | vNetIP | DCasg |
| 700 | Deny | \* | \* | Deny | Deny |



**Overview**

In this exercise you will review server assessments that the Technical Architect has setup as part of the discovery stage.

The setup for server assessment includes:-

* Dependency agent installed on each VM
* Log Analytics agent installed on each VM and configured to Log Analytics workspace

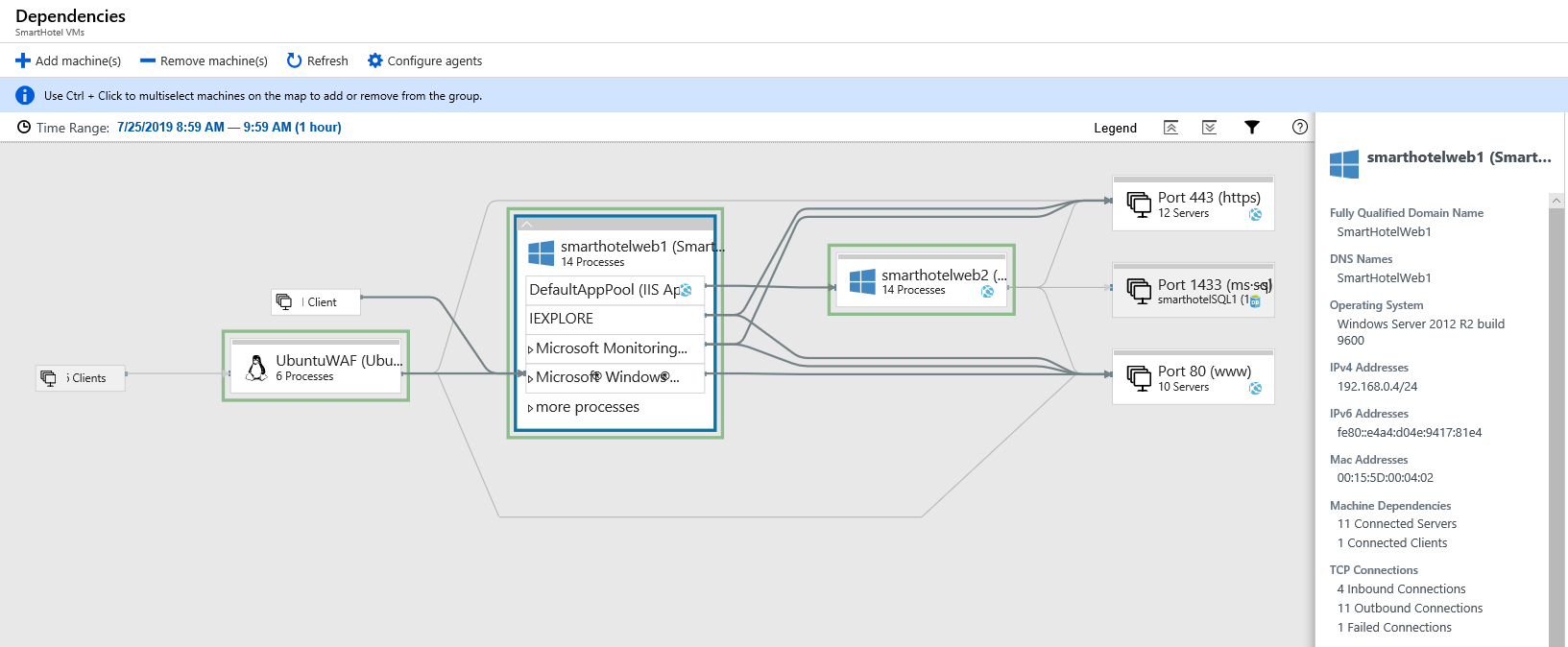
**Exercise targets**

1. Confirm all VMs are accessible and communicating with Log analytics
2. Review dependency view & log analytics queries
3. Build a firewall ruleset for the SmartHotel app that will be used to deploy Network Security Group (NSG) & Application Security Groups (ASG)
   * Note:- DomainController activity to have any:any connectivity
4. Build a firewall ruleset for the SmartHotel app that will be used to deploy Network Security Group (NSG) & Application Security Groups (ASG) – deploy via Terraform

**Additional information to help**

**Additional information to help**

1. Visualisation similar to below shows dependency view (DO not worry about domain controller activity for this workshop):-



Sample Log analytics queries that can be used to query serviceMap

*VMConnection*

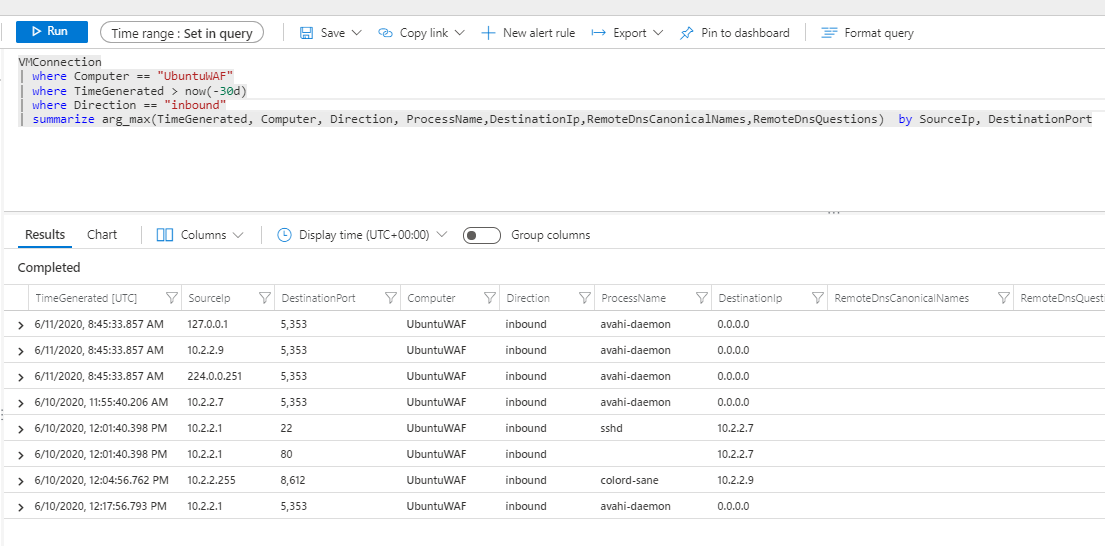
*| where Computer == " vmname"*

*| where TimeGenerated > now(-30d)*

*| where Direction == "inbound"*

*| summarize arg\_max(TimeGenerated, Computer, Direction, ProcessName,DestinationIp,RemoteDnsCanonicalNames,RemoteDnsQuestions)  by SourceIp, DestinationPort*

1. *VMConnection*
2. *| where Computer == "vmname"*
3. *| where TimeGenerated > now(-30d)*
4. *| where Direction == "outbound"*
5. *| summarize arg\_max(TimeGenerated, Computer, Direction, ProcessName,SourceIp,RemoteDnsCanonicalNames,RemoteDnsQuestions)  by DestinationIp, DestinationPort*
6. Review VMs, what is configured on WFE’s, DB, Ubuntu etc



NSG/ASG Ruleset build, for this exercise only consider inbound configuration for NSG as below

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Priority | Name | Port | Protocol | Source | Destination |
| 100 | ActiveDirectory | \* | \* | DomaincontrollerASG | VNET |
| 101 | ActiveDirectory2 | \* | \* | VNET | DomainControllerASG |