**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:-

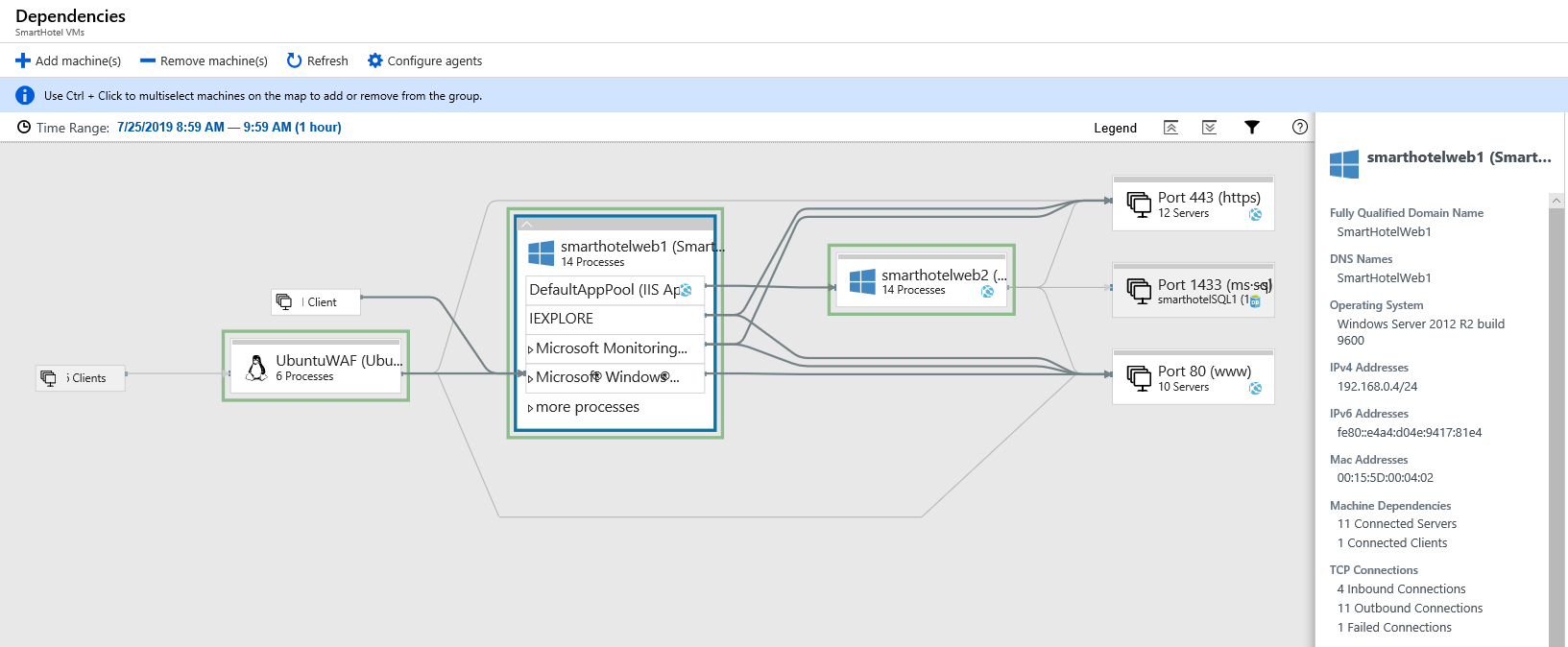
* Dependency agent installed on each VM
* Log Analytics agent installed on each VM and configured to Log Analytics workspace

**Exercise targets**

1. Confirm all VMs can be RDP/SSH from Hyper-V host -> VMs and that all have internet access
2. Confirm all VMs are accessible and communicating with Log analytics
3. Review dependency view & log analytics queries
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**

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



1. 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*

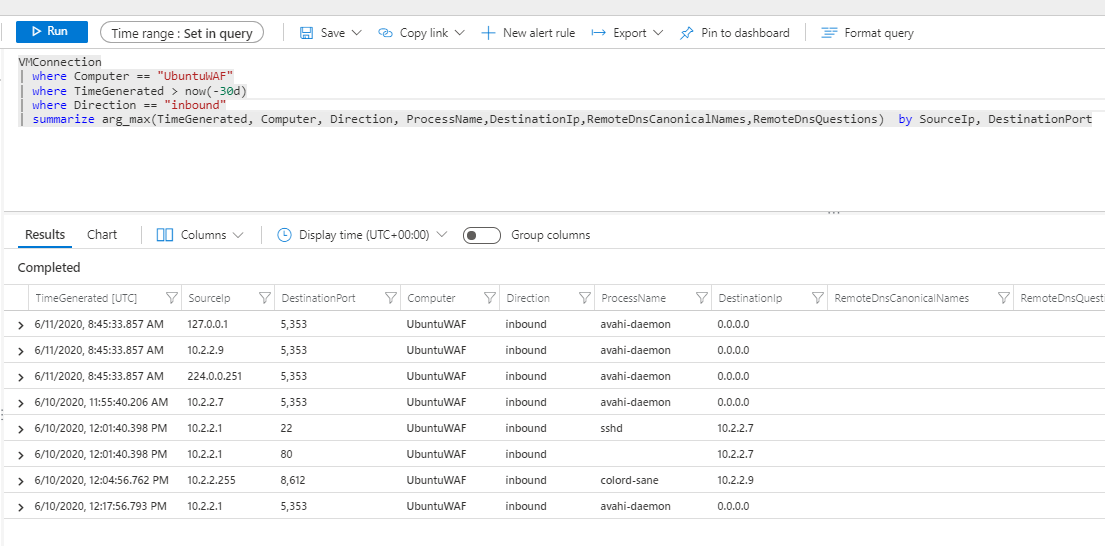
*VMConnection*

*| where Computer == "vmname"*

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

*| where Direction == "outbound"*

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



1. 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 |