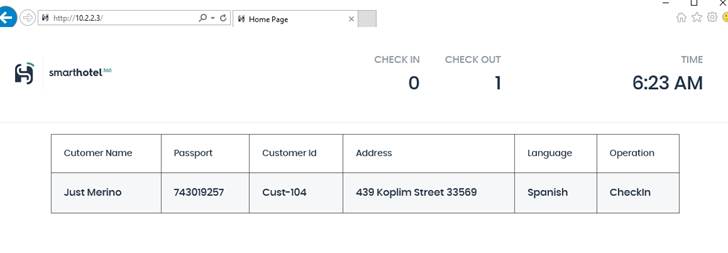
**Overview**

The customer has a test Hyper-V environment that has been deployed onto a Virtual Machine in Azure, it hosts a Microsoft-created application that displays as below. The customer wants to use this setup to act as an “on-premise” environment to review how a migration would happen with its on-premise Hyper-V environments using Azure Migrate.



They Hyper-V environment consists of a three-tier application, domain controller and a standalone server 2003 Virtual Machine

**Hyper-V VMs**

|  |  |  |  |
| --- | --- | --- | --- |
| **Server Type** | **VM Name** | **Server OS** | **IP Address** |
| Domain Controller | Domaincontroller1 | Server 2016 | 10.2.2.5 |
| WAF/Reverse Proxy | UbuntuWAF | Ubuntu | 10.2.2.15 |
| Web | SmartHotelWeb1 | Server2012R2 | 10.2.2.3 |
| App | SmartHotelWeb2 | Server2012R2 | 10.2.2.4 |
| Database | SmartHotelSQL | Server 2016 | 10.2.2.2 |
| Server2003 | Server2003 | Server 2003 | 10.2.2.7 |

**VM info**

Domain: kmigration.cloud

Username: kmigration\administrator

Password: Password123!

Localuser for UbuntuWAF, SmartHotelWeb1, SmartHotelWeb2, SmartHotelSQL1,

Local Username: demouser

Local Password: demo!pass123

Hyper-V host Login

Username:- administrator1 , administrator2

Password: Password123!

**Hyper-V Network Setup**

Virtual Switch Name:- Nested (Internal Only)

NAT & Static Routes configured with Routing/SRAS Service  
DHCP Service Configured

**Basic Requirements (throughout exercises, more requirements will appear)**

1. Azure VMs to have a Network Security Group (NSG) attached to each VM, Application Security Group (ASG) applied along with specific rules of communication between each VM *(Note:- Domain controller for this exercise can be lenient and allow any:any source/destination ports)*
2. Log analytics to be configured on each VM after migration and ensure heartbeat alert is configured
3. VMs to be backed up daily except for server2003
4. VMs to have Azure Site Recovery enabled as well except for server2003
5. If Recovery Services cannot be used, review if time a configuration that may work for a backup and in the event of DR (server2003 related only)
6. To start and stop VMs outside of business hours (9am-5pm GMT)
7. When migrated to Azure, VMs cannot have direct internet access
8. SSL on website if accessible publicly (localhost DNS can be suffice for this and self-signed ssl certificate)

**Discussion Points**

1. Investigate the application stack, how is it configured? How does it communicate between the tiers etc
2. Initial deployment, RDP/ssh access to Azure VMs primarily from Hyper-V host, how can this be achieved? (requirement of IKEv2 VPN using VPN Windows Service(Routing & remote access)
3. From 1. After the initial deployment,consider Azure Bastion at a later stage
4. The domain cannot be down at any stage throughout the migration; what can be done to assist with this the Azure Migration?
5. VMs cannot have direct internet access, review Azure Firewall and how it can be implemented on a later task
6. SSL is not currently configured, for Public access of the website, this is a requirement – where/how will SSL offload/terminate?

**Changes to Hyper-V VMs or host**

Do not automatically make changes to the Hyper-V host, vNET, VMs etc until you have confirmed changes with trainer