High Level Design

Azure Virtual Data Center

#client# #project#

NOTES

- **Variable $IP is used throughout as the second octet in the IP scheme as this will need to be defined by current network design at time of deployment. Find and replace will be required**

23/07/2020	Flora McFlimsey	Initial Prep	V0.01b

TABLE OF CONTENTS

1. INTRODUCTION 4

1.1 PURPOSE 4

1.2 SCOPE 4

1.2.1 In Scope 4

1.2.2 Out of Scope 4

2. SOLUTION OVERVIEW 5

2.1 AS-IS ARCHITECTURE 5

2.2 TO-BE ARCHITECTURE 6

2.2.1 General Azure resources 7

2.2.1.1 Azure Tenant 7

2.2.1.2 Azure Subscription 7

2.2.1.3 Azure Resource Groups 7

2.2.2 Network resources 7

2.2.2.1 Virtual Network and subnets 7

2.2.2.2 Gateway Subnet 8

2.2.2.3 Virtual Network Gateway 8

2.2.2.4 Local VPN Gateway 8

2.2.2.5 Site-to-Site Connector 8

2.2.2.6 Network Security Groups 8

2.2.3 Infrastructure Resources 9

2.2.3.1 Hop Box 9

2.2.3.2 Domain Controller 9

2.2.3.3 DNS 10

2.3 OTHER OPTIONS CONSIDERED 10

2.3.1 Cloud vs On-Premise 10

2.3.2 Cloud Vendors 10

2.4 NON-FUNCTIONAL DESIGN 11

2.4.1 Scalability 11

2.4.2 Resilience 11

2.4.3 Disaster Recovery and Continuity 11

2.4.4 Security 12

3. PROJECT IMPLEMENTATION 14

3.1 TRANSITION PLANNING 14

3.2 CONFIGURATION & RELEASE 14

3.3 TESTING 14

4. RISKS & ISSUES 16

4.1 PEOPLE ..... **ERROR! BOOKMARK NOT DEFINED.**

4.2 PROCESSES ..... ERROR! BOOKMARK NOT DEFINED.
4.3 DATA ..... ERROR! BOOKMARK NOT DEFINED.
4.4 INFRASTRUCTURE ..... ERROR! BOOKMARK NOT DEFINED.
4.5 RISKS & ISSUES SUMMARY 16
5. SERVICE MANAGEMENT 17
5.1 SERVICE SUPPORT 17
5.2 CAPACITY MONITORING 17
5.3 PERFORMANCE MONITORING 17
5.4 SERVICE MONITORING ..... ERROR! BOOKMARK NOT DEFINED.
5.5 BACKUP 17
5.6 PATCHING AND AV 17
6. LICENSING 18
7. REFERENCES 19
7.1 DOCUMENT REFERENCES 19
7.2 GLOSSARY 19
APPENDIX A – CODE SNIPPETS 20
APPENDIX A.1 CREATE RESOURCE GROUP 20
APPENDIX A.2 CREATE VNETS AND SUBNETS 20
APPENDIX A.3 CREATE GATEWAY SUBNET 20
APPENDIX A.4 CREATE VIRTUAL NETWORK (VPN) GATEWAY 20
APPENDIX A.5 CREATE LOCAL NETWORK (VPN) GATEWAY 21
APPENDIX A.6 CREATE SITE-TO-SITE VPN CONNECTION WITH PSK 21
APPENDIX A.7 NETWORK SECURITY GROUPS 21
APPENDIX A.8 BUILD AZHOP01 23
APPENDIX A.9 BUILD AZDC01 AND INSTALL AD DOMAIN SERVICES 23
APPENDIX A.10 SET VNET DNS SERVER 24

1. Introduction

1.1 Purpose

This document sets out the high-level solution design for the implementation of a Virtual Data Centre in Microsoft Azure Cloud.

This will provide both a structure to deploy new servers to support future service implementations and a structure and process via which existing servers can be migrated to the cloud.

1.2 Scope

The project is delivered over several phases and looks to deliver a dynamically expandable structure which has no definitive "completion" so the scope of this project is fixed to providing the structure and a fully documented mechanism for continuous growth and change.

1.2.1 In Scope

The solution will create a virtual data centre and associated basic infrastructure complete with necessary resources for core services (Authentication, DNS, DHCP). Initially Data, Compute and Migration Networks will be defined and built with processes, scripts and conventions designed for adding further resources

In scope for this phase of the project are:

- Outline of connectivity into Azure from current network
- Delivery of a functional infrastructure network and extension of AD into azure site.
- Delivery of a functional migration network
- Delivery of a functional DMZ network
- Delivery of functional 3-tier network for future applications and services and for existing resources to be rebuilt or redeployed into.
- Overview of monitoring recommendations and interoperability with current tools (ServiceNow, etc)
- Overview of conventions, processes and methodology for extending with further resources (Virtual networks, Subnets, Servers

1.2.2 Out of Scope

The project will not deliver the following which will need to be examined at a later date:

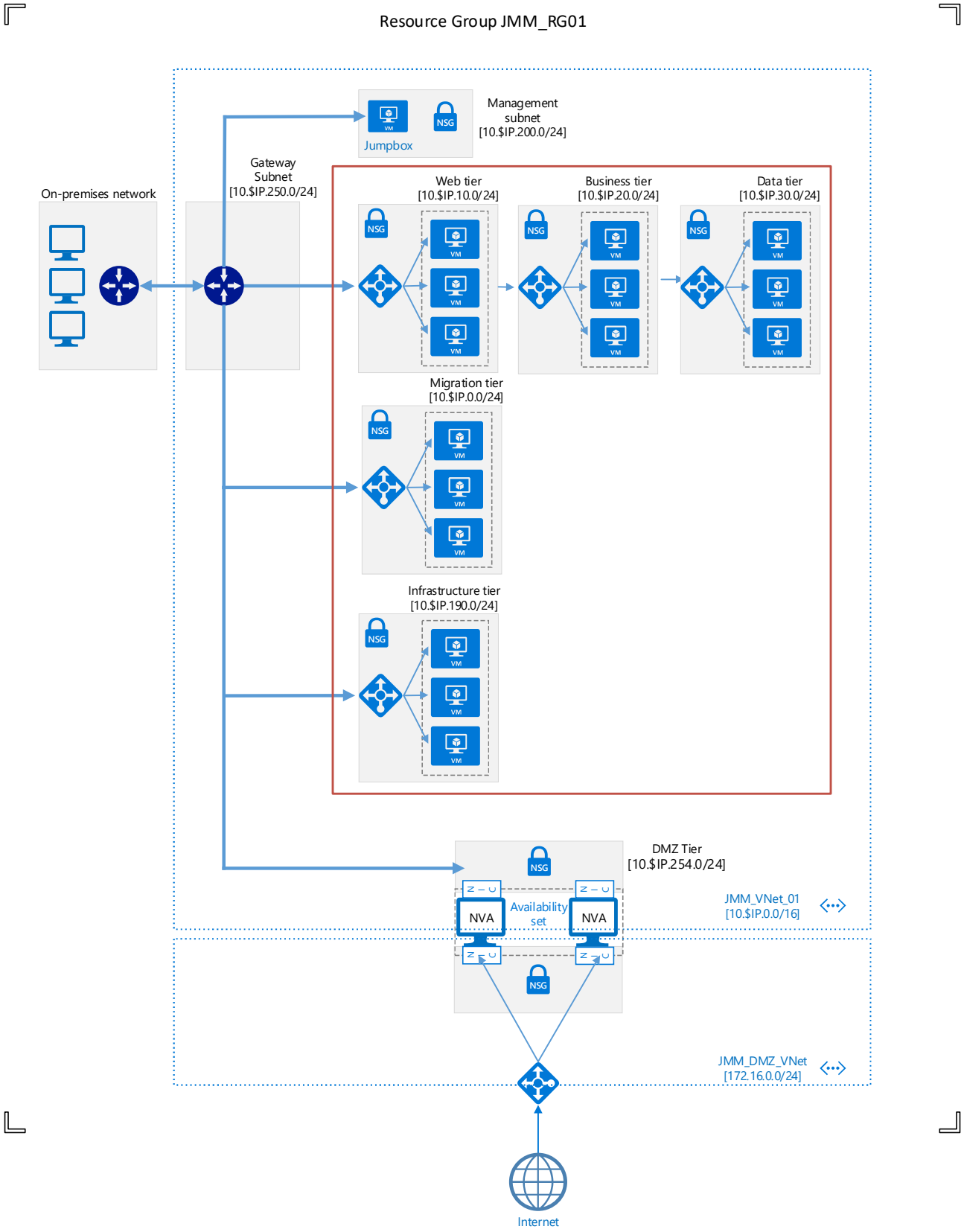
- Detailing connectivity. The connectivity option on this project is a simple VPN endpoint. The definition of the Local (On Prem) side of this will be decided in conjunction with the existing network owner. This design presents a simplified model which can be easy modified to work with whatever technology and configuration they require.
- Detail of Network Virtual Appliances. These have been included in the design but not specified or detailed.
- Full network monitoring and proactive capabilities. This will be dependent on tooling; outline recommendations are included
- Disaster Recovery planning and configuration. As the services that are going into azure are not currently known Disaster recovery and planning for them is out of scope of this solution. However, this has been considered as far as possible and some recommendations provided under Section 2.4 – Non-Functional Design.

2. Solution Overview

2.1 Existing Architecture

The current solution is ….

2.2 Target Architecture



The architecture is based around multiple subnets (‘tiers’) in an Azure virtual network connected to the existing network via a site to site IPSec VPN.

The solution is designed around a 3-tier paradigm with all applications broken into their Web (User), Business (App) and Data (Storage and SQL) components and separated into the subnets to provide security, control and

isolation. Applications are then accessed via the DMZ network controlled by Azure network security groups and other firewall/network virtual appliance solutions.

As the current application stack is not compatible with that goal a “Migration” tier has been designed which has no restrictions on access – anything on the virtual or on-premise networks can access it exactly as if it was an On-Premise site LAN segment.. This can act as a single tiered subnet where application/data/user servers can all coexist as per the current on-site network design until adoption of a more structured and secured approach.

An infrastructure tier has been specified which will hold infrastructure services – Active Directory, DNS, etc. The extension of AD into this virtual site and deployment of a single domain controller is delivered in this design. DNS and LDAP lookups can then be allowed to the infrastructure network from the other tiers as required to support lookups and authentication for applications and services within them.

A management tier has been specified along with a single Non-Member server. This will have access to all other tiers and can be used as a hop box so RDP does not need to be opened across the VPN to every tier. The dynamic nature of the Azure cloud also means it can be immediately given and extern IP address and used as an emergency method of access should there be a failure in the VPN link(s).

The DMZ Tier (Inside) is addressable by any other tier or the On-Prem network. Outbound security from that tier is then controlled by network virtual appliance to by designed and controlled by the network security team. The NVAs will be deployed with one interface on this DMZ tier and one on the DMZ network from which outbound connections can be set up.

Detail of individual components follows. The majority of the infrastructure is to be deployed as code, code snippets for each component are included in Appendix A. This allows the infrastructure to be deployed as designed while maintaining more flexibility than deploying as a single template.

2.2.1 General Azure resources

2.2.1.1 Azure Tenant

All resources can be created in a single or existing tenant. For the benefit of future Azure AD integration, it may be preferable to use the tenant for the already existing Directory.

2.2.1.2 Azure Subscription

A new subscription will be created for the virtual data canter.

The subscription name has not been specified in this design as future usage may prefer to use isolated subscriptions per application with Cross-Subscription network peering resulting in multiple subscriptions for which a naming convention will need to be created.

2.2.1.3 Azure Resource Groups

A single resource Group called JMM_RG01 will be created in region UK South.

A code snippet for this component is included as Appendix A.1

2.2.2 Network resources

2.2.2.1 Virtual Network and subnets

An Azure virtual network called JMM_Vnet01 will be created in the resource group. It will have an IP Scope of 10.$IP.0.0/16.

Multiple infrastructure subnets are created:

ManagementSubnet	10.$IP.200.0/24
WebSubnet	10.$IP.10.0/24
BusinessSubnet	10.$IP.20.0/24
DataSubnet	10.$IP.30.0/24
MigrationSubnet	10.$IP.0.0/24

InfrastructureSubnet	10.$IP.190.0/24

A second virtual network called JMM_DMZ_VNet will be created in the resource group. It will have an IP Scope of 172.16.0.0/24 and a single subnet for the whole range. This can be changed as required on an application by application basis in conjunction with the design, build and configuration of the network virtual appliances/firewalls (Out of Scope)

A code snippet for this component is included as Appendix A.2

2.2.2.2 Gateway Subnet

A gateway subnet containing the reserved IP Addresses [10.$IP.255.0/27] for the virtual network gateway is created as JMM_GatewaySubnet

A code snippet for this component is included as Appendix A.3

2.2.2.3 Virtual Network Gateway

A virtual network gateway is deployed to end point vpn(s) from on premise networks. This is likely to be replaced/augmented/upgraded to a virtual network appliance as the Azure estate grows,

The endpoint as per this design uses a basic gateway solution and dynamic external IP to reduce costs during implementation/scale out phases.

A code snippet for this component is included as Appendix A.4

2.2.2.4 Local VPN Gateway

This defines the local (on-premise) side of the VPN into the Azure cloud solution. As per the scoping of this design what is presented is a simplified example configuration – the full network requirements are out of scope.

A code snippet for this component with example configuration is included in Appendix A.5

2.2.2.5 Site-to-Site Connector

As per the design an IPSec VPN connector is created on the Virtual Network Gateway to connect the Virtual Network Gateway and the Local VPN gateway defined previously.

This will use a preshared key which will be rotated regularly.

A code snippet for this component is included as Appendix A.6. There is an included temporary pre-shared key which much be changed when building any live resources.

2.2.2.6 Network Security Groups

The connectivity between subnets is controlled by network security groups.

Each tier subnet has a single network security group for global control of communication between tiers. Individual resources can also have their own NSG to provide further security as necessary however this in envisaged as unlikely and out of scope for this design.

The default allow rules are noted below, they can be changed instantly by editing the associated NSG. All other ports and connections are denied.

No application allow rules have been allowed in the Business Tier as these will be created as application are deployed.

An Allow rule for default SQL ports has been created in the Data Tier, this is illustrative of the capabilities rather than operational.

Network Security Group	From	To	Port/Service
ManagementNSG	LoadBalancerProbe	Management Tier	*
ManagementNSG	Any	Management Tier	RDP TCP3389

WebNSG	LoadBalancerProbe	Web Tier	*
WebNSG	Management Tier	Web Tier	RDP TCP3389
WebNSG	Any	Web Tier	HTTP TCP80
WebNSG	Any	Web Tier	HTTPS TCP443
BusinessNSG	LoadBalancerProbe	Web Tier	*
BusinessNSG	Management Tier	Web Tier	RDP TCP3389
InfrastructureNSG	LoadBalancerProbe	Infrastructure Tier	*
InfrastructureNSG	Management Tier	Infrastructure Tier	RDP TCP3389
InfrastructureNSG	*	Infrastructure Tier	RPC Endpoint TCPUDP135
InfrastructureNSG	*	Infrastructure Tier	LDAP TCPUDP389
InfrastructureNSG	*	Infrastructure Tier	LDAP SSL TCP636
InfrastructureNSG	*	Infrastructure Tier	LDAP GC TCP3268
InfrastructureNSG	*	Infrastructure Tier	LDAP GCSSL TCP3269
InfrastructureNSG	*	Infrastructure Tier	KERB TCPUDP88
InfrastructureNSG	*	Infrastructure Tier	DNS TCPUDP53
InfrastructureNSG	*	Infrastructure Tier	SMB TCPUDP445
InfrastructureNSG	*	Infrastructure Tier	DFSR SYSVOL TCP5722
InfrastructureNSG	*	Infrastructure Tier	WIN TIME UDP123
InfrastructureNSG	*	Infrastructure Tier	KERB PW TCPUDP464
InfrastructureNSG	*	Infrastructure Tier	DFS GP UDP138
InfrastructureNSG	*	Infrastructure Tier	NETLOGON UDP137
InfrastructureNSG	*	Infrastructure Tier	NETLOGON TCP139

A Code snippet to create and attach these NSGs and set up the default rules as designed is attached as Appendix A.7

2.2.3 Infrastructure Resources

2.2.3.1 Hop Box

A hop box AZHOP01 [10.$IP.200.4] is created on the management subnet. This will be accessible for RDP from the On-Premise network and have RDP access to all Azure tiers. It is not specified as a domain member by this design.

It is set to turn off every evening so is only brought online when required.

A code snippet to create this machine is included as Appendix A.8. The script includes an administrative password which must be changed before the script is used for deployment.

2.2.3.2 Domain Controller

A single domain controller on the Infrastructure network is deployed. This will provide authentication and DNS services for the cloud-based resources.

A code snippet to build the machine AZDC01 [10.$IP.190.20] and install Domain services is included in Appendix A.9. The script includes an administrative password which must be changed before the script is used for deployment.

Once built the machine should be promoted to a domain controller and joined to the On premise domain. The domain can then be extended with a new site “Azure” and the new domain controller and 10.$IP.0.0/16 subnets configured in the AD site.

The domain controller can then be set to use itself for DNS and appropriate forwarders to corporate DNS servers created.

2.2.3.3 DNS

Virtual network JMM_VNet01 should be set to use the new DC as the primary DNS server when using DHCP addressing.

A Code snippet to set the Virtual network DNS servers is attached as Appendix A.10.

2.3 Other Options Considered

2.3.1 Cloud vs On-Premise

The current solution uses on premise servers and networking equipment with a mix of physical baremetal, Hyper-V virtualised and VMWare virtualised infrastructure.

When designing this solution, the expansion and modernisation of this infrastructure has been considered as an alternative to a virtual datacentre.

As <<Business>> move into a “Cloud first” strategy many applications and services will likely be delivered as SaaS, either entirely externally or as services run by IT services and delivered back into the business. This model will result in the retiring and decommissioning of a large part of the server estate.

A possible solution then is to repurpose the more modern hardware, supplement it with new where necessary, and deliver an On-premise solution.

This would seem more cost effective in the short term as no or minimal new infrastructure, subscriptions or licenses would be needed.

However much of the hardware and software <<Business>> have is approaching or has passed end of life and over 3-5 years would need replacing plus the costs of maintenance and support of hardware and software across multiple sites proves this a false economy.

Additionally, <<Business>> have suffered multiple outages of critical services which would not have occurred if they were running a fully, or even predominantly cloud solution.

2.3.2 Cloud Vendors

The solution as proposed could be delivered in almost any cloud vendor. Those considered were Google GCloud and Amazon AWS.

As all three vendors can provide almost identical platforms they have been assessed on cost, reliability, environmental impact and service integration.

Assessing cost is extremely difficult as we don’t know how many servers and other resources will eventually be used and whether we would be using on demand or committed instances so we can only use generic costings from industry sources. The references used are included in section 7 (References 1-4) of this document. Generally speaking, for storage Azure is 4% cheaper than rivals, compute is around even as is data ingress/egress.

Reliability-wise all three vendors quote an SLA of 99.95% uptime.

Each vendor has a commitment to minimise environmental impact and move to renewable energy sources.

Service integration is the genuine differentiator. Microsoft services integrate seamlessly with already existing technologies – AD, AAD, SQL, etc. The other providers can use and provide these services however there is additional cost and support requirements.

Conclusively since <<Business>> are already operating in the Microsoft stack and moving cloud resources to Microsoft Azure outstrips any other provider at present.

2.4 Non-Functional Design

2.4.1 Scalability

The solution is designed around providing a working architecture and infrastructure that is also a framework for future extensions in volume and capabilities.

Each tier can support 250 servers which provides far more capacity that <<Business>> currently use and far in excess of any potential usage, however the capacity exists to use the design and scripts in this solution as to add further Vnets and tiers should the company requirements grow unexpectedly.

The total possible scale is effectively limitless.

2.4.2 Resilience

The solution is built in Azure which quotes a 99.5% uptime for SLA purposes. Actual experienced uptime is generally higher.

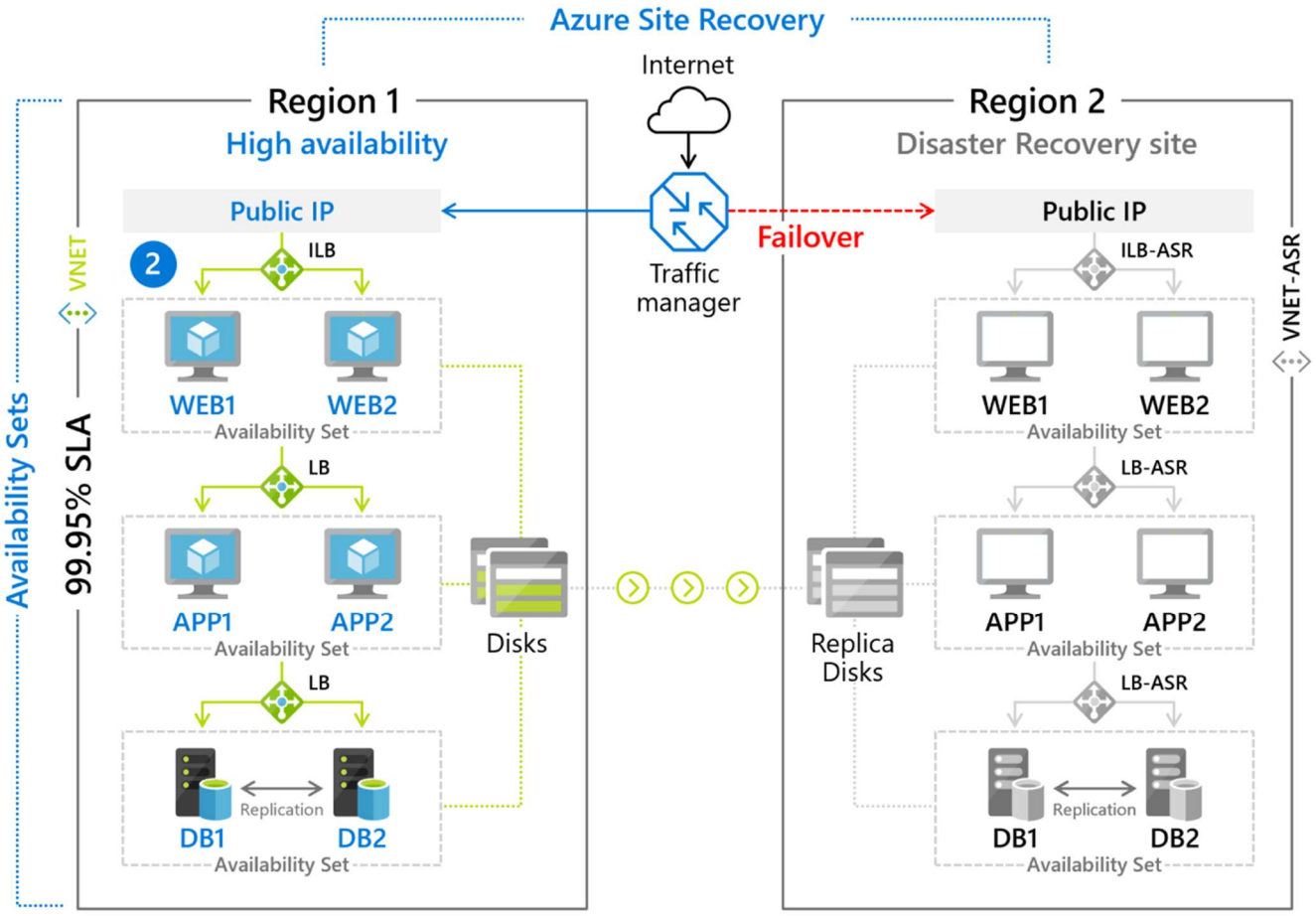
The main point lacking resilience is the VPN back to <<Business>> on-premise resources. This design indicates an Azure Network gateway supporting a VPN. This arrangement is fully functional and resilient enough for most uses however improvements beyond the scope of this design should be considered and implemented

- Short term - use two vpn devices on two separate lines in two separate physical sites on the on-premise side. This is the most likely failure point.
- Medium term – implement a virtual network appliance in Azure which can support a fully mesh vpn with all physical <<Business>> sites. (EG Meraki VMX or Silver Peak VX)
- Long Term – all future solutions should be delivered through the web front end and DMZ. Authentication should generally be with Azure Active Directory and core services should be moved to run entirely from Azure. The VPON at that point will be a simple replication link for limited On-premise resources (Domain controller replication, etc)

2.4.3 Disaster Recovery and Continuity

Disaster recovery and Continuity planning are out of scope for this solution however has been considered when designing the solution.

Azure offer a full Site recovery capability (diagram is generalised not specific to this solution):



Source: ***https://azure.microsoft.com/en-us/services/site-recovery/***

In summary a second copy of all or selected resources is maintained at a second Microsoft Regional data centre and on a failure the traffic is failed from the primary to the copy.

However, there is a non-trivial expense and the primary region already has a 99.95% uptime, so this solution is generally overkill for any services that are not extremely mission or even safety- or life- critical.

If individual applications which are to be migrated or deployed into the solution as designed are assessed as requiring a higher than 99.95% SLA it is recommended to, where possible, use a second region and application level technologies to provide failover capabilities (EG Always on availability groups for SQL, load balancers for web, etc)

2.4.4 Security

The solution is intrinsically secured by leveraging multiple technologies.

2.4.4.1 Network security

Each tier is protected by a network security group. This means that should a server or application be misbehaving (for example due to malicious or badly written code) it cannot access all other tiers by default.

There are two network ingress/egress points, web and VPN.

The VPN is site-to-site and thus secured by default as only a specified local (on premise) IP address can connect to it.

The web front end is where future services should be presented. It is protected by a DMZ network and a pair of network virtual appliances (firewalls)

2.4.4.2 Account security

The accounts used to administer the infrastructure will be azure active directory accounts synced from on premise AD. Numerous technologies can then be used to further secure the accounts

- Multi Factor Authentication – All administrative accounts should have MFA forced for every logon.
- Conditional Access – Most administrative account should have strict conditional access policies allowing access only from <<Business>> offices. Some users should be able to log in from anywhere in order to manage the infrastructure in special circumstances however the “Risky logons” feature of Azure Active Directory should be configured to immediately raise incidents with the service desk for moderate to high risk logons. This will indicate if a user is login in from an unfamiliar IP or locations.

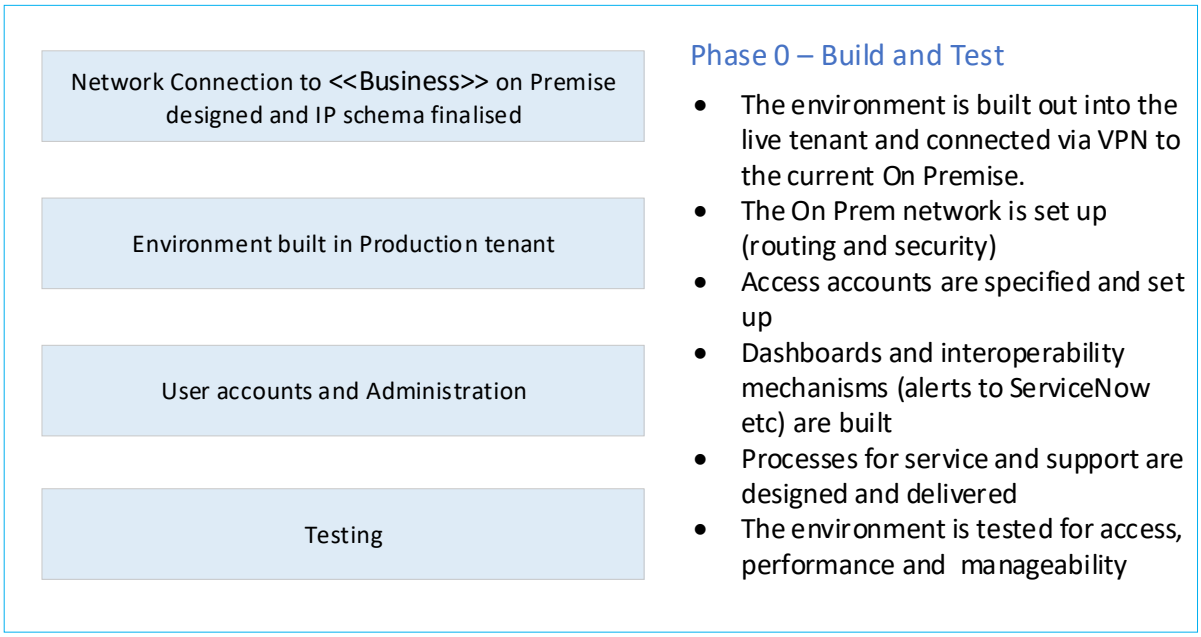
2.4.4.3 Access control

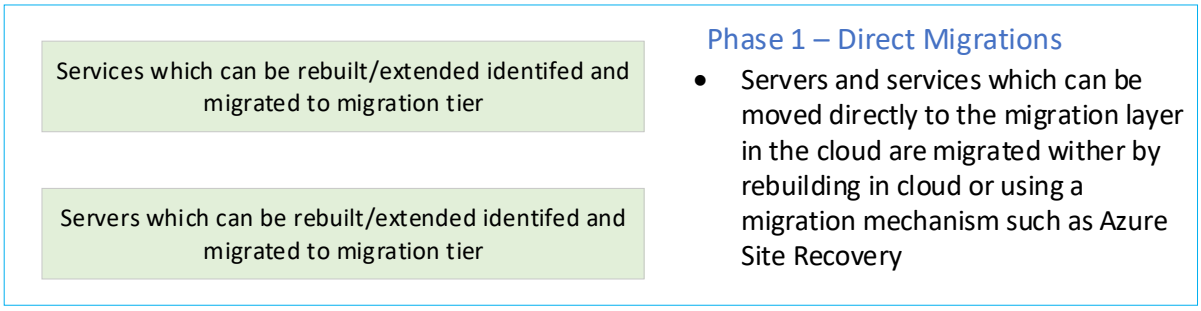
The only network with full access to all tiers is the management network. The hop box and any further VMSs should have Just In Time access enabled. This allows an admin to have the RDP port locked by default and opened only when management access is required. The result being that no one will be able to log onto any server in the virtual datacentre unless an incident or change is running and the access has been enabled.

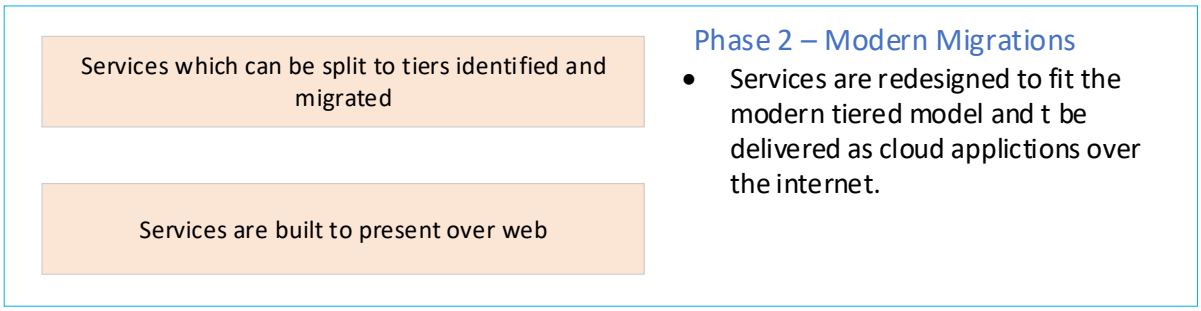
3. Project Implementation

3.1 Transition Planning

The solution is designed around a multi-phase transition plan







3.2 Configuration & Release

The design contains scripts which can build the solution extremely quickly. There will be no effect on currently running services until the build out is complete and applications re assessed for migration then moved.

3.3 Testing

The testing program should assess the environment access and performance. Access will likely need to be tuned in the network security groups.

Every application should be fully tested running in the cloud as some older applications may have issues. The connectivity back <<Business>> will run on fast links but it is delivered over IPSec VPN which is very cryptographically “heavy” and may introduce an unacceptable TTL. Almost every modern application should have no issue at all.

4. Risks & Issues

4.1 Risks & Issues Summary

Risk/Issue Description	Probability	Impact	Risk Mitigation Plan
User Account compromised	Low	High	MFA, Conditional Access
Server Compromised	Low	High	Multi-tiered design
Network Outage <<Business>>	Medium	Medium	VPN from multiple locations, eventual move to Mesh
Network Outage Microsoft	Extremely Low	High	Indicated possibility of using multiple sites for extremely critical resources
Hardware Failure	Extremely Low	High	Machines and resources can be deployed into availability group.

5. Service Management

5.1 Service Support

Integration with service desk tools is out of scope but have been considered. In the short term the service can be supported within the current support arrangements – the entire stack is Microsoft so can be supported suitable qualified and experience persons and entirely standard technology.

Moving forward however there is a lot of scope for improvements. The service desk tool used by <<Business>> is ServiceNow which has a lot of capabilities, from automated incident logging based on azure outputs to basic and advantaged automatic incident and request responses using the PowerShell interface into Azure. Anything from access request to entire server builds can be scripted from the service desk tooling.

5.2 Capacity Monitoring

The capacity of all servers and services in azure is hugely elastic, there is no envisioned situation in which any workload will be outside the capabilities of the solution.

5.3 Performance and Service Monitoring

Current tooling for performance and monitoring in <<Business>> is extremely limited but an assessment is underway. Custom dashboards in Azure would expose performance and usage information and allow a massive improvement in proactive capabilities however as the company will be using a large degree of on-premise compute for the foreseeable future the performance monitoring of cloud services should be integrated with the on-premise solution. Solutions such as SolarWinds provided a fully integrated and contiguous experience for cloud and on-premise monitoring however the discussion of such is out of scope for this solution.

5.4 Backup

It is envisaged that once servers and services start to move to cloud the backup solution will likely change to Azure recovery Vaults as this provides a more integrated and capable experience however this can be considered at a later date, all resources can be backed up using the existing technology.

5.5 Patching and AV

The update management capabilities of Azure will in the long term replace the heavy overhead of keeping on premise servers up to date however this will be assessed per resource and is out of scope of this solution.

6. Licensing

All licensing in Azure is subscription based so would avoid the current issue of lack of clarity of license usage.

7. References

7.1 Document References

Ref	Document Name	Version	Date	Document Location
1	https://www.cloudberrylab.com/resources/blog/amazon-s3-azure-and-google-cloud-prices-compare/			
2	https://www.datamation.com/cloud-computing/aws-vs-azure-vs-google-cloud-comparison.html#pricing			
3	https://calculator.unigma.com/#/instances			
4	https://www.simform.com/compute-pricing-comparison-aws-azure-googlecloud/			

Table 1: References

7.2 Glossary

Term	Definition
BI	Business Intelligence
GB	Gigabytes
KB	Kilobytes
Kb	Kilobits
MB	Megabytes
MI	Management Information
On Prem	On Premises System
TB	Terabytes

Table 2: Glossary of Terms

Appendix A – Code Snippets

The code snippets below allow the deployment of resources as defined.

They assume the Azure RM powershell modules are installed and up to date and a GA account is attached to Azure Tenant via `connect-azurermaccount` and the subscription is created and targeted when tested with `get-azurermcontext`

Appendix A.1 Create Resource Group

```
New-AzureRmResourceGroup -Name "JMM_RG01" -Location UKSouth
```

Appendix A.2 Create VNets and Subnets

```
New-AzureRmVirtualNetwork -Name JMM_VNet01 -ResourceGroupName "JMM_RG01" -Location UKSouth -
AddressPrefix "10.$IP.0.0/16"

$vnet = Get-AzureRmVirtualNetwork -name JMM_VNet01 -ResourceGroupName JMM_RG01
Add-AzureRmVirtualNetworkSubnetConfig -Name ManagementSubnet -VirtualNetwork $vnet -
AddressPrefix '10.$IP.200.0/24' |Set-AzureRmVirtualNetwork

$vnet = Get-AzureRmVirtualNetwork -name JMM_VNet01 -ResourceGroupName JMM_RG01
Add-AzureRmVirtualNetworkSubnetConfig -Name WebSubnet -VirtualNetwork $vnet -AddressPrefix
'10.$IP.10.0/24' |Set-AzureRmVirtualNetwork

$vnet = Get-AzureRmVirtualNetwork -name JMM_VNet01 -ResourceGroupName JMM_RG01
Add-AzureRmVirtualNetworkSubnetConfig -Name BusinessSubnet -VirtualNetwork $vnet -
AddressPrefix '10.$IP.20.0/24' |Set-AzureRmVirtualNetwork

$vnet = Get-AzureRmVirtualNetwork -name JMM_VNet01 -ResourceGroupName JMM_RG01
Add-AzureRmVirtualNetworkSubnetConfig -Name DataSubnet -VirtualNetwork $vnet -AddressPrefix
'10.$IP.30.0/24' |Set-AzureRmVirtualNetwork

$vnet = Get-AzureRmVirtualNetwork -name JMM_VNet01 -ResourceGroupName JMM_RG01
Add-AzureRmVirtualNetworkSubnetConfig -Name MigrationSubnet -VirtualNetwork $vnet -
AddressPrefix '10.$IP.0.0/24' |Set-AzureRmVirtualNetwork

$vnet = Get-AzureRmVirtualNetwork -name JMM_VNet01 -ResourceGroupName JMM_RG01
Add-AzureRmVirtualNetworkSubnetConfig -Name InfrastructureSubnet -VirtualNetwork $vnet -
AddressPrefix '10.$IP.190.0/24' |Set-AzureRmVirtualNetwork

$vnet = Get-AzureRmVirtualNetwork -name JMM_VNet01 -ResourceGroupName JMM_RG01
Add-AzureRmVirtualNetworkSubnetConfig -Name DMZSubnet -VirtualNetwork $vnet -AddressPrefix
'10.$IP.254.0/24' |Set-AzureRmVirtualNetwork

$vnet = New-AzureRmVirtualNetwork -Name JMM_DMZ_VNet -ResourceGroupName "JMM_RG01" -Location
UKSouth -AddressPrefix "172.16.0.0/24"
Add-AzureRmVirtualNetworkSubnetConfig -Name DMZSubnetPublic -VirtualNetwork $vnet -
AddressPrefix '172.16.0.0/24' |Set-AzureRmVirtualNetwork
```

Appendix A.3 Create Gateway Subnet

```
$vnet = Get-AzureRmVirtualNetwork -name JMM_VNet01 -ResourceGroupName JMM_RG01
Add-AzureRmVirtualNetworkSubnetConfig -Name GatewaySubnet -VirtualNetwork $vnet -
AddressPrefix '10.$IP.255.0/27' |Set-AzureRmVirtualNetwork
```

Appendix A.4 Create Virtual Network (VPN) Gateway

```
$pubIP = New-AzureRmPublicIpAddress -Name 'JMM_VNet01Gateway_PublicIP' -ResourceGroupName
JMM_RG01 -Location UKSouth -AllocationMethod Dynamic
$vnet = Get-AzureRmVirtualNetwork -name 'JMM_VNet01' -ResourceGroupName JMM_RG01
$subnet = Get-AzureRmVirtualNetworkSubnetConfig -Name 'GatewaySubnet' -VirtualNetwork $vnet
$pubIPconfig = New-AzureRmVirtualNetworkGatewayIpConfig -Name 'JMM_VNet01Gateway_PublicIP' -
SubnetId $subnet.Id -PublicIpAddressId $pubIP.Id
New-AzureRmVirtualNetworkGateway -Name JMM_VNet01Gateway -ResourceGroupName JMM_RG01 -
Location UKSouth -IpConfigurations $pubIPconfig -GatewayType Vpn -VpnType RouteBased
```

Appendix A.5 Create Local Network (VPN) Gateway

This is an example command $LocalExtAddress must be replaced with the external IP of the on premise VPN gateway device. $AddressPrefix should be replaced with the addresses (CIDR formatted) which should be routed back through the gateway from Azure.

```
New-AzureRMLocalNetworkGateway -Name OnPremiseGateway -ResourceGroupName JMM_RG01 -Location
UKSouth -GatewayIpAddress '$LocalExtAddress' -AddressPrefix '$AddressPrefix'
```

Appendix A.6 Create Site-To-Site VPN Connection with PSK

The preshared key in this snippet is NOT secure and MUST be changed prior to deployment.

```
$gateway = Get-AzureRMVirtualNetworkGateway -Name JMM_VNet01Gateway -ResourceGroupName
JMM_RG01
$local = Get-AzureRMLocalNetworkGateway -Name OnPremiseGateway -ResourceGroupName JMM_RG01
New-AzureRMVirtualNetworkGatewayConnection -Name JMM_VNNet01ToONPrem -ResourceGroupName
JMM_RG01 -Location UKSouth -VirtualNetworkGateway1 $gateway -LocalNetworkGateway2 $local -
ConnectionType IPsec -RoutingWeight 10 -SharedKey 'abc123'
```

Appendix A.7 Network Security Groups

```
$nsg = New-AzureRmNetworkSecurityGroup -Name ManagementNSG -ResourceGroupName JMM_RG01 -
Location UKSouth
$vnet = Get-AzureRmVirtualNetwork -ResourceGroupName JMM_RG01 -Name JMM_VNET01
$subnet = Get-AzureRmVirtualNetworkSubnetConfig -VirtualNetwork $vnet -name ManagementSubnet
$subnet.NetworkSecurityGroup = $nsg
Set-AzureRmVirtualNetwork -VirtualNetwork $vnet
$nsg | Add-AzureRmNetworkSecurityRuleConfig -Name AllowLoadBalancer -Description "Allows
Azure Probe" -Access Allow -Protocol * -Priority 4095 -SourceAddressPrefix AzureLoadBalancer
-SourcePortRange * -DestinationAddressprefix * -DestinationPortRange * -Direction Inbound |
Set-AzureRmNetworkSecurityGroup
$nsg | Add-AzureRmNetworkSecurityRuleConfig -Name AllowRDP -Description "Allows RDP from any
Subnet" -Access Allow -Protocol TCP -Priority 1024 -SourceAddressPrefix VirtualNetwork -
SourcePortRange * -DestinationAddressprefix * -DestinationPortRange 3389 -Direction Inbound |
Set-AzureRmNetworkSecurityGroup
$nsg | Add-AzureRmNetworkSecurityRuleConfig -Name Block_VNet1 -Description "Blocks Subnet to
Subnet Traffic" -Access Deny -Protocol * -Priority 4096 -SourceAddressPrefix VirtualNetwork -
SourcePortRange * -DestinationAddressprefix VirtualNetwork -DestinationPortRange * -Direction
Inbound | Set-AzureRmNetworkSecurityGroup

$nsg = New-AzureRmNetworkSecurityGroup -Name WebNSG -ResourceGroupName JMM_RG01 -Location
UKSouth
$vnet = Get-AzureRmVirtualNetwork -ResourceGroupName JMM_RG01 -Name JMM_VNET01
$subnet = Get-AzureRmVirtualNetworkSubnetConfig -VirtualNetwork $vnet -name WebSubnet
$subnet.NetworkSecurityGroup = $nsg
Set-AzureRmVirtualNetwork -VirtualNetwork $vnet
$nsg | Add-AzureRmNetworkSecurityRuleConfig -Name AllowHTTPS -Description "Allows HTTPS
traffic" -Access Allow -Protocol TCP -Priority 1022 -SourceAddressPrefix * -SourcePortRange *
-DestinationAddressprefix * -DestinationPortRange 443 -Direction Inbound | Set-
AzureRmNetworkSecurityGroup
$nsg | Add-AzureRmNetworkSecurityRuleConfig -Name AllowHTTP -Description "Allows HTTP
traffic" -Access Allow -Protocol TCP -Priority 1023 -SourceAddressPrefix * -SourcePortRange *
-DestinationAddressprefix * -DestinationPortRange 80 -Direction Inbound | Set-
AzureRmNetworkSecurityGroup
$nsg | Add-AzureRmNetworkSecurityRuleConfig -Name AllowLoadBalancer -Description "Allows
Azure Probe" -Access Allow -Protocol * -Priority 4095 -SourceAddressPrefix AzureLoadBalancer
-SourcePortRange * -DestinationAddressprefix * -DestinationPortRange * -Direction Inbound |
Set-AzureRmNetworkSecurityGroup
$nsg | Add-AzureRmNetworkSecurityRuleConfig -Name AllowRDP -Description "Allows RDP from
Management Tier" -Access Allow -Protocol TCP -Priority 1024 -SourceAddressPrefix
10.$IP.200.0/24 -SourcePortRange * -DestinationAddressprefix * -DestinationPortRange 3389 -
Direction Inbound | Set-AzureRmNetworkSecurityGroup
$nsg | Add-AzureRmNetworkSecurityRuleConfig -Name Block_VNet1 -Description "Blocks Subnet to
Subnet Traffic" -Access Deny -Protocol * -Priority 4096 -SourceAddressPrefix VirtualNetwork -
SourcePortRange * -DestinationAddressprefix VirtualNetwork -DestinationPortRange * -Direction
Inbound | Set-AzureRmNetworkSecurityGroup

$nsg = New-AzureRmNetworkSecurityGroup -Name BusinessNSG -ResourceGroupName JMM_RG01 -
Location UKSouth
$vnet = Get-AzureRmVirtualNetwork -ResourceGroupName JMM_RG01 -Name JMM_VNET01
$subnet = Get-AzureRmVirtualNetworkSubnetConfig -VirtualNetwork $vnet -name BusinessSubnet
$subnet.NetworkSecurityGroup = $nsg
Set-AzureRmVirtualNetwork -VirtualNetwork $vnet
```

```
$nsg | Add-AzureRmNetworkSecurityRuleConfig -Name AllowLoadBalancer -Description "Allows
Azure Probe" -Access Allow -Protocol * -Priority 4095 -SourceAddressPrefix AzureLoadBalancer
-SourcePortRange * -DestinationAddressprefix * -DestinationPortRange * -Direction Inbound |
Set-AzureRmNetworkSecurityGroup
$nsg | Add-AzureRmNetworkSecurityRuleConfig -Name AllowRDP -Description "Allows RDP from
Management Tier" -Access Allow -Protocol TCP -Priority 1024 -SourceAddressPrefix
10.$IP.200.0/24 -SourcePortRange * -DestinationAddressprefix * -DestinationPortRange 3389 -
Direction Inbound | Set-AzureRmNetworkSecurityGroup
$nsg | Add-AzureRmNetworkSecurityRuleConfig -Name Block_VNet1 -Description "Blocks Subnet to
Subnet Traffic" -Access Deny -Protocol * -Priority 4096 -SourceAddressPrefix VirtualNetwork -
SourcePortRange * -DestinationAddressprefix VirtualNetwork -DestinationPortRange * -Direction
Inbound | Set-AzureRmNetworkSecurityGroup

$nsg = New-AzureRmNetworkSecurityGroup -Name DataNSG -ResourceGroupName JMM_RG01 -Location
UKSouth
$vnet = Get-AzureRmVirtualNetwork -ResourceGroupName JMM_RG01 -Name JMM_VNET01
$subnet = Get-AzureRmVirtualNetworkSubnetConfig -VirtualNetwork $vnet -name DataSubnet
$subnet.NetworkSecurityGroup = $nsg
Set-AzureRmVirtualNetwork -VirtualNetwork $vnet
$nsg | Add-AzureRmNetworkSecurityRuleConfig -Name AllowSQL -Description "Allows SQL from
Business Tier" -Access Allow -Protocol TCP -Priority 1023 -SourceAddressPrefix 10.$IP.20.0/24
-SourcePortRange * -DestinationAddressprefix * -DestinationPortRange 1433 -Direction Inbound
| Set-AzureRmNetworkSecurityGroup
$nsg | Add-AzureRmNetworkSecurityRuleConfig -Name AllowLoadBalancer -Description "Allows
Azure Probe" -Access Allow -Protocol * -Priority 4095 -SourceAddressPrefix AzureLoadBalancer
-SourcePortRange * -DestinationAddressprefix * -DestinationPortRange * -Direction Inbound |
Set-AzureRmNetworkSecurityGroup
$nsg | Add-AzureRmNetworkSecurityRuleConfig -Name AllowRDP -Description "Allows RDP from
Management Tier" -Access Allow -Protocol TCP -Priority 1024 -SourceAddressPrefix
10.$IP.200.0/24 -SourcePortRange * -DestinationAddressprefix * -DestinationPortRange 3389 -
Direction Inbound | Set-AzureRmNetworkSecurityGroup
$nsg | Add-AzureRmNetworkSecurityRuleConfig -Name Block_VNet1 -Description "Blocks Subnet to
Subnet Traffic" -Access Deny -Protocol * -Priority 4096 -SourceAddressPrefix VirtualNetwork -
SourcePortRange * -DestinationAddressprefix VirtualNetwork -DestinationPortRange * -Direction
Inbound | Set-AzureRmNetworkSecurityGroup

$nsg = New-AzureRmNetworkSecurityGroup -Name MigrationNSG -ResourceGroupName JMM_RG01 -
Location UKSouth
$vnet = Get-AzureRmVirtualNetwork -ResourceGroupName JMM_RG01 -Name JMM_VNET01
$subnet = Get-AzureRmVirtualNetworkSubnetConfig -VirtualNetwork $vnet -name MigrationSubnet
$subnet.NetworkSecurityGroup = $nsg
Set-AzureRmVirtualNetwork -VirtualNetwork $vnet

$nsg = New-AzureRmNetworkSecurityGroup -Name InfrastructureNSG -ResourceGroupName JMM_RG01 -
Location UKSouth
$vnet = Get-AzureRmVirtualNetwork -ResourceGroupName JMM_RG01 -Name JMM_VNET01
$subnet = Get-AzureRmVirtualNetworkSubnetConfig -VirtualNetwork $vnet -name
InfrastructureSubnet
$subnet.NetworkSecurityGroup = $nsg
Set-AzureRmVirtualNetwork -VirtualNetwork $vnet
$nsg | Add-AzureRmNetworkSecurityRuleConfig -Name AllowRPC -Description "Allows RPC Endpoint
mapper" -Access Allow -Protocol * -Priority 1023 -SourceAddressPrefix * -SourcePortRange * -
DestinationAddressprefix * -DestinationPortRange 135 -Direction Inbound | Set-
AzureRmNetworkSecurityGroup
$nsg | Add-AzureRmNetworkSecurityRuleConfig -Name AllowLDAP -Description "Allows LDAP" -
Access Allow -Protocol * -Priority 1022 -SourceAddressPrefix * -SourcePortRange * -
DestinationAddressprefix * -DestinationPortRange 389 -Direction Inbound | Set-
AzureRmNetworkSecurityGroup
$nsg | Add-AzureRmNetworkSecurityRuleConfig -Name AllowLDAPSSL -Description "Allows LDAP SSL"
-Access Allow -Protocol TCP -Priority 1021 -SourceAddressPrefix * -SourcePortRange * -
DestinationAddressprefix * -DestinationPortRange 636 -Direction Inbound | Set-
AzureRmNetworkSecurityGroup
$nsg | Add-AzureRmNetworkSecurityRuleConfig -Name AllowLDAPGC -Description "Allows LDAP GC" -
Access Allow -Protocol TCP -Priority 1020 -SourceAddressPrefix * -SourcePortRange * -
DestinationAddressprefix * -DestinationPortRange 3268 -Direction Inbound | Set-
AzureRmNetworkSecurityGroup
$nsg | Add-AzureRmNetworkSecurityRuleConfig -Name AllowLDAPGCSSL -Description "Allows LDAP GC
SSL" -Access Allow -Protocol TCP -Priority 1019 -SourceAddressPrefix * -SourcePortRange * -
DestinationAddressprefix * -DestinationPortRange 3269 -Direction Inbound | Set-
AzureRmNetworkSecurityGroup
$nsg | Add-AzureRmNetworkSecurityRuleConfig -Name AllowKerb -Description "Allows Kerberos" -
Access Allow -Protocol * -Priority 1018 -SourceAddressPrefix * -SourcePortRange * -
DestinationAddressprefix * -DestinationPortRange 88 -Direction Inbound | Set-
AzureRmNetworkSecurityGroup
$nsg | Add-AzureRmNetworkSecurityRuleConfig -Name AllowDNS -Description "Allows DNS" -Access
Allow -Protocol * -Priority 1017 -SourceAddressPrefix * -SourcePortRange * -
DestinationAddressprefix * -DestinationPortRange 53 -Direction Inbound | Set-
AzureRmNetworkSecurityGroup
```

```
$nsg | Add-AzureRmNetworkSecurityRuleConfig -Name AllowSMB -Description "Allows SMB" -Access
Allow -Protocol * -Priority 1016 -SourceAddressPrefix * -SourcePortRange * -
DestinationAddressprefix * -DestinationPortRange 445 -Direction Inbound | Set-
AzureRmNetworkSecurityGroup
$nsg | Add-AzureRmNetworkSecurityRuleConfig -Name AllowDFSR -Description "Allows DFSR SYSVOL"
-Access Allow -Protocol TCP -Priority 1015 -SourceAddressPrefix * -SourcePortRange * -
DestinationAddressprefix * -DestinationPortRange 5722 -Direction Inbound | Set-
AzureRmNetworkSecurityGroup
$nsg | Add-AzureRmNetworkSecurityRuleConfig -Name AllowWTIME -Description "Allows WIN TIME" -
Access Allow -Protocol UDP -Priority 1014 -SourceAddressPrefix * -SourcePortRange * -
DestinationAddressprefix * -DestinationPortRange 123 -Direction Inbound | Set-
AzureRmNetworkSecurityGroup
$nsg | Add-AzureRmNetworkSecurityRuleConfig -Name AllowKerbPW -Description "Allows Kerberos
PW" -Access Allow -Protocol * -Priority 1013 -SourceAddressPrefix * -SourcePortRange * -
DestinationAddressprefix * -DestinationPortRange 464 -Direction Inbound | Set-
AzureRmNetworkSecurityGroup
$nsg | Add-AzureRmNetworkSecurityRuleConfig -Name AllowDFSGP -Description "Allows DFS GP" -
Access Allow -Protocol UDP -Priority 1012 -SourceAddressPrefix * -SourcePortRange * -
DestinationAddressprefix * -DestinationPortRange 138 -Direction Inbound | Set-
AzureRmNetworkSecurityGroup
$nsg | Add-AzureRmNetworkSecurityRuleConfig -Name AllowNETLOGONUDP -Description "Allows
NETLOGON UDP" -Access Allow -Protocol UDP -Priority 1010 -SourceAddressPrefix * -
SourcePortRange * -DestinationAddressprefix * -DestinationPortRange 137 -Direction Inbound |
Set-AzureRmNetworkSecurityGroup
$nsg | Add-AzureRmNetworkSecurityRuleConfig -Name AllowNETLOGONTCP -Description "Allows
NETLOGON TCP" -Access Allow -Protocol TCP -Priority 1009 -SourceAddressPrefix * -
SourcePortRange * -DestinationAddressprefix * -DestinationPortRange 139 -Direction Inbound |
Set-AzureRmNetworkSecurityGroup
$nsg | Add-AzureRmNetworkSecurityRuleConfig -Name AllowLoadBalancer -Description "Allows
Azure Probe" -Access Allow -Protocol * -Priority 4095 -SourceAddressPrefix AzureLoadBalancer
-SourcePortRange * -DestinationAddressprefix * -DestinationPortRange * -Direction Inbound |
Set-AzureRmNetworkSecurityGroup
$nsg | Add-AzureRmNetworkSecurityRuleConfig -Name AllowRDP -Description "Allows RDP from
Management Tier" -Access Allow -Protocol TCP -Priority 1024 -SourceAddressPrefix
10.$IP.200.0/24 -SourcePortRange * -DestinationAddressprefix * -DestinationPortRange 3389 -
Direction Inbound | Set-AzureRmNetworkSecurityGroup
$nsg | Add-AzureRmNetworkSecurityRuleConfig -Name Block_VNet1 -Description "Blocks Subnet to
Subnet Traffic" -Access Deny -Protocol * -Priority 4096 -SourceAddressPrefix VirtualNetwork -
SourcePortRange * -DestinationAddressprefix VirtualNetwork -DestinationPortRange * -Direction
Inbound | Set-AzureRmNetworkSecurityGroup

$nsg = New-AzureRmNetworkSecurityGroup -Name DMZNSG -ResourceGroupName JMM_RG01 -Location
UKSouth
$vnet = Get-AzureRmVirtualNetwork -ResourceGroupName JMM_RG01 -Name JMM_VNET01
$subnet = Get-AzureRmVirtualNetworkSubnetConfig -VirtualNetwork $vnet -name DMZSubnet
$subnet.NetworkSecurityGroup = $nsg
Set-AzureRmVirtualNetwork -VirtualNetwork $vnet
```

Appendix A.8 Build AZHOP01

```
$VMName = "AZHOP01"
$VMSize = "Standard_D2_V2"
$MachineUserName = "JMMAdmin"
$MachinePassword = "JMMSecurePassword!"
$MachineSecurePassword = ConvertTo-SecureString $MachinePassword -AsPlainText -Force
$MachineCredential = New-Object System.Management.Automation.PSCredential ($MachineUserName,
$MachineSecurePassword);
$IPconfig = New-AzureRmNetworkInterfaceIpConfig -Name "IPConfig1" -PrivateIpAddressVersion
IPv4 -PrivateIpAddress "10.$IP.200.4" -Subnet (Get-AzureRmVirtualNetworkSubnetConfig -name
ManagementSubnet -VirtualNetwork (Get-AzureRmVirtualNetwork -name JMM_VNet01 -
ResourceGroupName JMM_RG01))
$NICName = $VMName+'_NIC01'
$NICObj = New-AzureRmNetworkInterface -Name $NICName -ResourceGroupName JMM_RG01 -Location
UKSouth  -IpConfiguration $IPconfig  -WarningAction SilentlyContinue
$VirtualMachine = New-AzureRmVMConfig -VMName $VMName -VMSize $VMSize
$VirtualMachine = Set-AzureRmVMOperatingSystem -VM $VirtualMachine -Windows -ComputerName
$VMName -Credential $MachineCredential -ProvisionVMAgent -EnableAutoUpdate
$VirtualMachine = Add-AzureRmVMNetworkInterface -VM $VirtualMachine -Id $NICObj.Id
$VirtualMachine = Set-AzureRmVMSourceImage -VM $VirtualMachine -PublisherName
'MicrosoftWindowsServer' -Offer 'WindowsServer' -Skus '2016-Datacenter' -Version latest
$VirtualMachineObj = New-AzureRmVM -ResourceGroupName JMM_RG01 -Location UKSouth -VM
$VirtualMachine -WarningAction SilentlyContinue
```

Appendix A.9 Build AZDC01 and install AD Domain Services

```
$VMName = "AZDC01"
```

```
$VMSize = "Standard_D2_V2"
$MachineUserName = "JMMAdmin"
$MachinePassword = "JMMSecurePassword!"
$MachineSecurePassword = ConvertTo-SecureString $MachinePassword -AsPlainText -Force
$MachineCredential = New-Object System.Management.Automation.PSCredential ($MachineUserName,
$MachineSecurePassword);
$IPconfig = New-AzureRmNetworkInterfaceIpConfig -Name "IPConfig1" -PrivateIpAddressVersion
IPv4 -PrivateIpAddress "10.$IP.190.20" -Subnet (Get-AzureRmVirtualNetworkSubnetConfig -name
InfrastructureSubnet -VirtualNetwork (Get-AzureRmVirtualNetwork -name JMM_VNet01 -
ResourceGroupName JMM_RG01))
$NICName = $VMName+'_NIC01'
$NICObj = New-AzureRmNetworkInterface -Name $NICName -ResourceGroupName JMM_RG01 -Location
UKSouth  -IpConfiguration $IPconfig  -WarningAction SilentlyContinue
$VirtualMachine = New-AzureRmVMConfig -VMName $VMName -VMSize $VMSize
$VirtualMachine = Set-AzureRmVMOperatingSystem -VM $VirtualMachine -Windows -ComputerName
$VMName -Credential $MachineCredential -ProvisionVMAgent -EnableAutoUpdate
$VirtualMachine = Add-AzureRmVMNetworkInterface -VM $VirtualMachine -Id $NICObj.Id
$VirtualMachine = Set-AzureRmVMSourceImage -VM $VirtualMachine -PublisherName
'MicrosoftWindowsServer' -Offer 'WindowsServer' -Skus '2016-Datacenter' -Version latest
$VirtualMachineObj = New-AzureRmVM -ResourceGroupName JMM_RG01 -Location UKSouth -VM
$VirtualMachine -WarningAction SilentlyContinue
Remove-Item .\ADscript.ps1
New-Item -ItemType File -Path .\ADscript.ps1
$Content = 'install-windowsfeature AD-Domain-Services'
Add-Content .\ADscript.ps1 $Content
Invoke-AzureRmVMRunCommand -ResourceGroupName JMM_RG01 -Name $VMName -CommandId
'RunPowerShellScript' -ScriptPath .\ADscript.ps1
Remove-Item .\ADscript.ps1
```

Appendix A.10 Set VNet DNS server

```
$vnet = Get-AzureRmVirtualNetwork -ResourceGroupName JMM_RG01 -name JMM_VNet01
$vnet.DhcpOptions.DnsServers = 10.$IP.190.20
Set-AzureRmVirtualNetwork -VirtualNetwork $vnet
```