|  |  |
| --- | --- |
| [Type the document title] | Azure Cloud Design |
| This document articulates the Microsoft Azure Hosting Platform Technical Solution Design and key configuration specifications | Document Status:  Author: **MV, Radhakrishna (Cognizant)** |
| Last updated: |

1. DOCUMENT INFORMATION
   1. Version History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Version* | *Date* | *Document Name* | *Role* | *Comments* |
| 0.1 | **xx/dd/yyyy** | **Generic Design** | **Architect** | **Initial document** |
| 1.0 | **xx/dd/yyyy** | **Generic Design** | **PM** | **Consolidated document** |
| 1.2 | **xx/dd/yyyy** | **Generic Design** | **PM** | **Split Documentation** |
| 1.3 | **xx/dd/yyyy** | **Generic Design** | **PM** | **Adjusted chapters** |
| 1.4 | **xx/dd/yyyy** | **Generic Design** | **PM** | **Workshop adjustments** |
| 1.5 /1.15 | **xx/dd/yyyy** | **Generic Design** | **PM** | **Adjusted after review** |
| 1.16 | **xx/dd/yyyy** | **Generic Design** | **PM** | **Added version** |

***Table 1 - Version history***

* 1. Review and Approvals

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Version* | *Date* | *Document Name* | *Role* | *Comments* |
| 0.1 | **xx/dd/yyyy** | **Generic Design** | **Architect** | **Initial document** |
| 0.2-0.9 | **xx/dd/yyyy** | **Generic Design** | **MS/Cognizant** | **Separate documents** |
| 1.0 | **xx/dd/yyyy** | **Generic Design** | **PM** | **Consolidated document** |
| 1.1 | **xx/dd/yyyy** | **Generic Design** | **<EA Customer>** | **Review** |
| 1.3 | **xx/dd/yyyy** | **Generic Design** | **<EA Customer>** | **Review chapter 2 and 3** |
| 1.4 | **xx/dd/yyyy** | **Generic Design** | **MS/Cognizant** | **Review chapter 9** |
| 1.6 | **xx/dd/yyyy** | **Generic Design** | **MS** | **Review full** |
| 1.15 | **xx/dd/yyyy** | **Generic Design** | **PM** | **Review** |
| 1.16 | **xx/dd/yyyy** | **Generic Design** | **MS/Cognizant/ <EA Customer>** |  |

***Table 2 - Review and approvals***

* 1. Distribution List

|  |  |  |  |
| --- | --- | --- | --- |
| *Version* | *Date* | | *To* |
| 0.1 | **xx/dd/yyyy** | **Project team** | |
| 1.0 /1.12 | **xx/dd/yyyy** | **Project team** | |
| 1.16 | **xx/dd/yyyy** | **Project team** | |

***Table 3 – Distribution List***

* 1. Stakeholders

|  |  |  |  |
| --- | --- | --- | --- |
| *Name* | *Role/Title* | | *Organization* |
|  |  |  | |
|  |  |  | |
|  |  |  | |

***Table 3 – Stakeholders List***

* 1. DISCLAIMER

System and product names described in this document are not always accompanied by their Vendors or Owners trademark symbols (™, ®). It is hereby acknowledged that all trademarks are the property of their respective owners. Furthermore, any extracts from vendor documents implies that there is no intent not to acknowledge or violate any vendor’s copyrights.

**Table of Contents**

[1. DOCUMENT INFORMATION 2](#_Toc476153212)

[1.1 Version History 2](#_Toc476153213)

[1.2 Review and Approvals 2](#_Toc476153214)

[1.3 Distribution List 2](#_Toc476153215)

[1.4 Stakeholders 3](#_Toc476153216)

[1.5 DISCLAIMER 3](#_Toc476153217)

[1. Introduction 7](#_Toc476153218)

[2. Purpose/Audience 8](#_Toc476153219)

[3. Executive Summary 9](#_Toc476153220)

[4. Goals and Objectives 10](#_Toc476153221)

[5. Solution Overview 11](#_Toc476153222)

[5.1 Risks, Assumptions & Dependencies 11](#_Toc476153227)

[5.2 Scope 13](#_Toc476153228)

[5.3 Requirements, assumptions and pre-conditions 13](#_Toc476153229)

[6. Solution Architecture 15](#_Toc476153230)

[6.1 AS-IS System Architecture 15](#_Toc476153231)

[6.2 Azure solution Architecture (Logical) 15](#_Toc476153234)

[6.3 Azure deployment architecture 16](#_Toc476153237)

[6.4 Network architecture 17](#_Toc476153238)

[6.5 Security architecture 17](#_Toc476153239)

[6.6 Governance architecture 18](#_Toc476153240)

[6.7 Application architecture 18](#_Toc476153241)

[6.8 Data architecture 19](#_Toc476153242)

[6.9 HA/DR architecture 20](#_Toc476153243)

[6.10 Backup & Recovery architecture 20](#_Toc476153244)

[6.11 Hybrid architecture – VPN (nice to have) 22](#_Toc476153245)

[6.12 Subscription Management 22](#_Toc476153246)

[7. Design Considerations 23](#_Toc476153247)

[7.1 Scalability considerations 23](#_Toc476153248)

[7.1.1 Scale up & Scale out - Auto-scale, VM Scale sets 23](#_Toc476153250)

[7.2 Availability considerations 23](#_Toc476153251)

[7.2.1 Recovery services – Backup, DR 23](#_Toc476153253)

[7.2.2 SLA 23](#_Toc476153254)

[7.3 Manageability considerations 23](#_Toc476153255)

[7.4 Security considerations 23](#_Toc476153256)

[7.5 Subscription considerations 23](#_Toc476153257)

[8. Solution deployment 24](#_Toc476153258)

[9. Validation 25](#_Toc476153259)

[10. Handover to managed services 26](#_Toc476153260)

[10.1 Azure Components 26](#_Toc476153267)

[10.1.1 Azure Storage 26](#_Toc476153268)

[10.1.2 Azure Virtual Machines 26](#_Toc476153269)

[10.1.3 Azure Internal Load Balancer 27](#_Toc476153270)

[10.2 Network Configuration 27](#_Toc476153271)

[10.2.1 Static Internal Private IP 27](#_Toc476153272)

[10.2.2 Networks / Vnets 28](#_Toc476153273)

[10.2.3 Subnets 28](#_Toc476153274)

[10.2.4 VPN Setup 28](#_Toc476153275)

[10.3 AD Configuration 29](#_Toc476153276)

[10.3.1 AD Group Policy 29](#_Toc476153277)

[10.3.2 AD Users and Groups 30](#_Toc476153278)

[10.3.3 AD Trust 31](#_Toc476153279)

[10.3.4 Conditional Forward 31](#_Toc476153280)

[10.4 VM Configuration 31](#_Toc476153281)

[10.4.1 Hardening setup 31](#_Toc476153282)

[10.4.2 Access management 31](#_Toc476153283)

[10.4.3 Append the DNS suffixes. 32](#_Toc476153284)

[10.5 WSUS 32](#_Toc476153285)

[10.6 Anti-Virus 32](#_Toc476153286)

[10.7 Backup 32](#_Toc476153287)

[10.7.1 Backup Vault 32](#_Toc476153288)

[10.7.2 VM Backup 33](#_Toc476153289)

[10.7.3 Folder and file backup 33](#_Toc476153290)

[10.8 Environment Creation 34](#_Toc476153291)

[10.9 Monitoring 34](#_Toc476153292)

[10.10 Email alert notification process 34](#_Toc476153293)

[10.11 Contacts 34](#_Toc476153294)

[11. Glossary 35](#_Toc476153295)

[12. References 36](#_Toc476153296)

1. Introduction

This document outlines the detailed technical specification for the Microsoft Azure Cloud platform solution. The technical design will outline the configuration for the overall architecture as well as specific technical configuration and design decisions for:

* Compute
* Storage
* Networking
* Backup
* DR

1. Purpose/Audience

This document helps architects and developers with the required information to manage, operate and support the Microsoft Azure platform capability. The solution design document illustrates the various architectural components and security controls implemented.

This documents audience is aimed primarily at architects and technical operations staff to validate the design against best practices from an Infrastructure and security controls perspective.

1. Executive Summary

<Customer> is strategically looking to minimize its on-premise server footprint, and capitalize on the benefits of cloud based services. As part of this strategy, there is an aim to migrate all on premise applications onto suitable cloud to allow for optimized and enhanced cloud-based service delivery, while leveraging the cost benefits of the cloud. <Customer> has embarked on a strategic initiative to modernize its IT infrastructure leveraging Microsoft Azure as the target cloud platform. The targeted environments of <customer> will be hosted in Microsoft’s Azure public cloud to actualize the following key benefits:

* Reduced cost of infrastructure and services
* Flexible options to manage capacity for both peak and non-peak demands
* A robust Governance model for environment management
* Increased automation so that the majority of requests can be automatically provisioned in minutes
* Embedded security within environments to meet compliance needs as required
* Charging based on the Azure consumption model, paying for use on an hourly basis with the ability to suspend servers

As part of this initiative, <Customer> aims to set up an <Azure Foundation Infrastructure>, provide cost-effective, scalable cloud-based design of the selected applications on the target cloud.

*Note: [Articulate Executive summary with the help from the customer. Many a times, customer own this section based the organizational strategy. Bring part of it from the SoW.]*

1. Goals and Objectives

The overall cloud design for <Customer> targets for the following design goals:

* Build a scalable IT Infrastructure
* Enabling Rapid deployment of IT services
* Implement a high level of self-deployment and automation of IT services
* Provide the right levels of Availability, Confidentiality and Integrity (based on workload and requirements)
* Reduce IT cost

1. Solution Overview

The proposed solution is completely in consideration with the existing application tech stack and its current infrastructure information provided. Infrastructure as a Service is being proposed as a solution with Azure IaaS v2.0 (ARM). The solution is envisioned with the relevant information shared so far from the application team and various <Customer’s IT> team input.

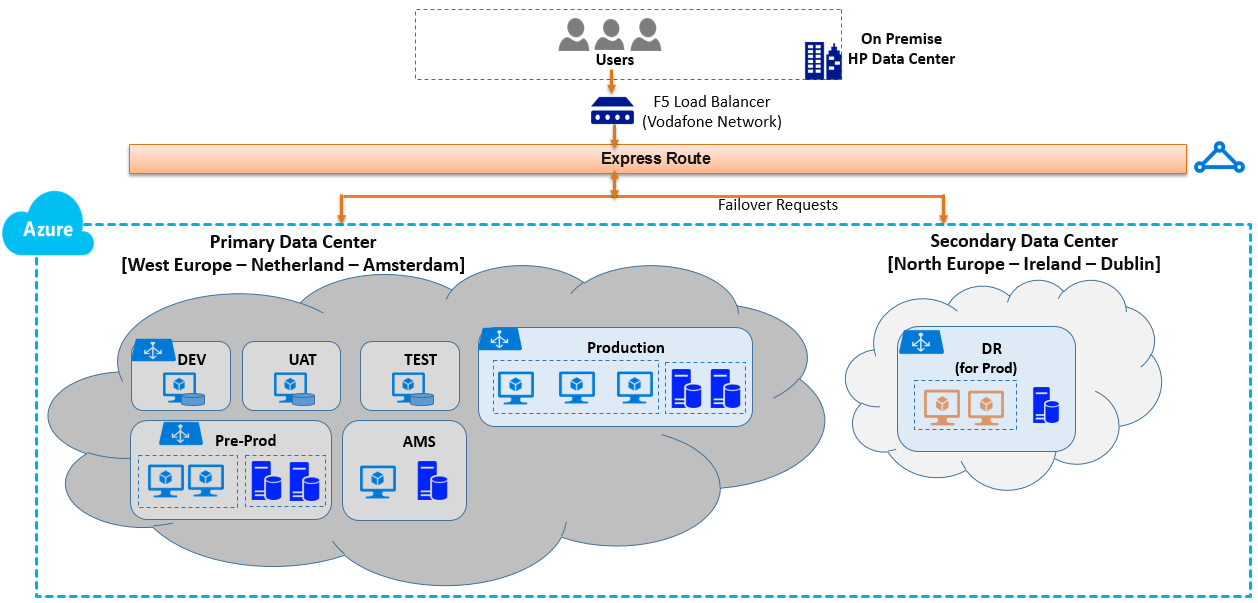


Figure 1: Azure Landscape Diagram for all Environments

The target deployment architecture will have suggested infrastructure details for various deployment environments.

The common services and networking information are captured under respective sections as necessary.

4. 1. Risks, Assumptions & Dependencies

Following are the risks, assumptions and dependencies on the high-level block-based solution as shown in Figure-1.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Risks | | |  |  |
| Ref. | **Type** | **Risks** | **Severity** | **Mitigation** |
| R001 | Data | No data will be migrated directly from xxx. It will be loaded from the Cognizant desktop machines | High | Dev/Test delivery is enabling learning of the Azure service |

|  |  |  |
| --- | --- | --- |
| Assumptions | | |
| Ref. | **Type** | **Description** |
| A001 | Data | No data will be migrated directly from Verizon. It will be loaded from the Cognizant desktop machines |
| A002 | Data | All of the data will be sanitized i.e. It will contain no customer details |
| A003 | Data | No data archiving is required |
| A004 | Access | Cognizant offshore support and development teams will need access to the servers (inc. RDP) |
| A005 | Access | Cognizant onshore Intranet team will need access to the servers (inc. RDP) |
| A006 | Access | <CUSTOMER> onshore test teams will need access for testing (no RDP) |
| A007 | Access | No more than two RDP connections are required simultaneously to each server |
| A008 | Access | All user access (account set up and deletion) will be managed by the Cognizant Intranet team |
| A009 | Availability | The Azure load balancer will be used for the web servers of the Test environment i.e the web servers will belong to a "Cloud Service". All other Test tiers are load balanced by Sharepoint. The Dev environments will have no HA/load balancing |
| A010 | Availability | The core hours for the service will be Monday to Friday, 02:30 to 18:00 UK time |
| A011 | Availability | Each pair of servers in the Test environment will be in an Availability Set to ensure at least one is always available |
| A012 | Availability | Environments will be made available on request via TSR – at other times they will be shut down to reduce costs |
| A013 | Integration | All testing will use stubs for interfaces – no integration to other <CUSTOMER> Development and Test services is required |
| A014 | Integration | All servers require access to the Team Foundation Server platform in HP |
| A015 | Integration | All servers require external web access via the Squid proxy |
| A016 | Platform | All VMs will be Azure IaaS VMs – no PaaS services will be used |
| A017 | Platform | All server OSs will be Windows 2008 R2 |
| A018 | Directory Services | Cognizant will build and maintain AD including DNS. Any DNS entries required for access to <CUSTOMER> will be manually added by Cognizant. This is an isolated environment and won't require a trust established with the UK domain |
| A019 | Database | Cognizant Intranet team will install and maintain the SQL DBs – this is the same approach as used in Verizon |
| A020 | Data Transfers | All data transfers to the servers will be from Cognizant desktops over the RDP protocol |
| A021 | Licensing | Sufficient MSDN licences exist to cover the SharePoint Development and Test environments and RDP CALs |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Dependencies | | |  |  |
| Ref. | **Type** | **Dependency Items** | **Dependent On** | **Comments** |
| D001 |  | Software licenses & ownership |  |  |

* 1. Scope

**In Scope**

* Implement the correct department setup topology for <Customer> in the Azure portal (functional, business division or geo);
* Implement the right org. level, who is responsible for cloud budgets and apply the same on Azure account owners;
* Design the Azure public cloud EA infrastructure: accounts, subscriptions and resource group strategy;
* Set-up organization model in the EA
* Perform several workshops with <Customer> to discuss the enterprise structure design;
* Create basic monthly cloud cost control reporting for the Account owners, based on the 3 cost center levels (subscription, account, department level);

**Out of Scope**

* The application design and application configuration
* The SharePoint Production and Pre-Production environments
* Extended financial analyst reporting for cloud finances (Complex financial management tools like X, Y will be covered in a separate project)
* Reporting on Capacity management, usage and user management
* Re-designing or maintaining the old Azure infrastructure (ASM is frozen);
* Deviations caused by big unforeseen changes in the <Customer> organization.
  1. Requirements, assumptions and pre-conditions

**Functional requirements**

* The Azure enterprise cloud structure must support global user workloads
* The cloud structure model must reflect and comply with the <Customer> org structure
* Department names, account names and subscription names must meet naming conventions

**Non-functional requirements**

* The cloud enterprise structure is easy recognizable and is as simple as possible;
* It’s based on resource groups for separate functions and not on separate subscriptions per function, there will be as less Azure subscriptions as possible for the Global and Centrality production workloads;
* The cloud enterprise structure user permissions shall be handled by the new RBAC standard.

**Assumptions**

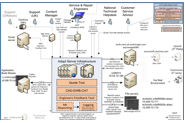
* The enterprise portal is accessible and ready for implementing the new cloud infra design;
* <Customer> has sufficient knowledge to create and maintain new Azure Subscription workloads;
* Account holders in Azure will be fully compliant with their responsibilities as account owner and budget holder within the business;

**Pre-conditions**

* The project team will get full enterprise admin access to the <Customer> enterprise portal ea.azure.com;
* <Customer> to deliver a cost center structure, organizational structure for the cloud enterprise structure design.

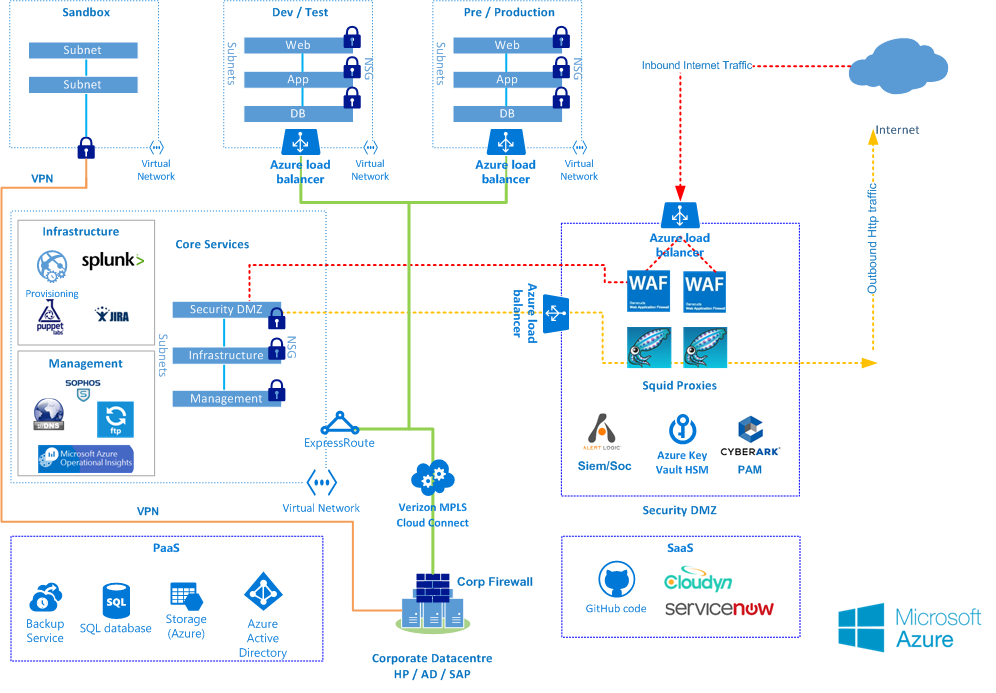
1. Solution Architecture
   1. AS-IS System Architecture

* Provide a write-up on the current logical and deployment architecture of the application-landscape
* Provide the current design behavior w.r.t. HA, DR and backup
* Provide the technology stack details as a reference to customer’s shared data. If stack is small, provide a tabular detailing

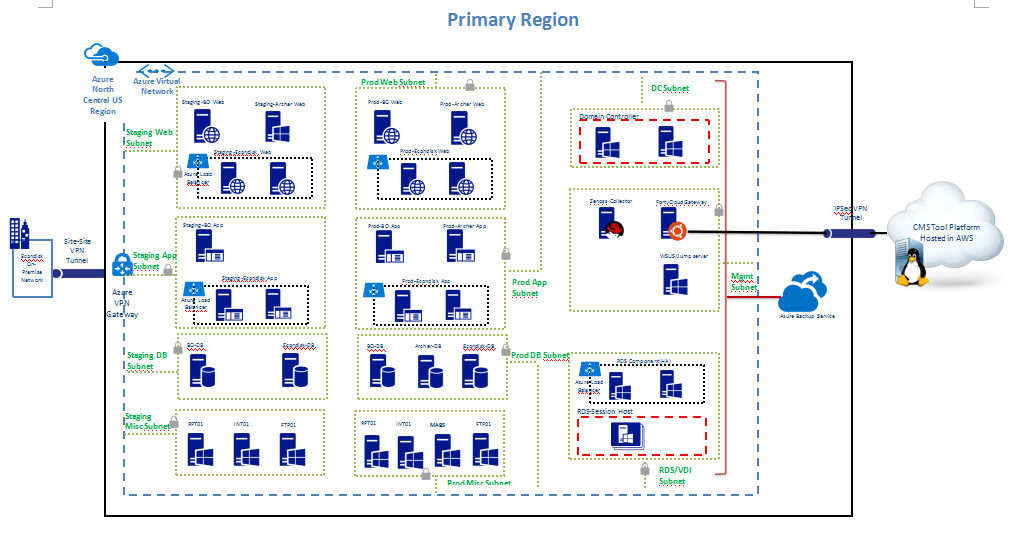


2. 1. Azure solution Architecture (Logical)

* Provide details on the logical/service components (PaaS, SaaS, IaaS) of Azure being planned at data-center level at a high level
* Provide on positioning different environments along with the Sandbox environment
* Sandbox environment can be expanded with DevTest Labs, if being planned
* Map on-premise solution building blocks to Azure solution architecture (logical)



2. 1. Azure deployment architecture



Architectural Overview:

<Customer> has opted to use Microsoft Azure as its preferred public cloud platforms. This document defines the technical solution design specifically for Microsoft Azure. The platforms are both designed to be as standardized, embedding operational controls ‘by design’. In certain cases, there are technical capabilities and differences that are unique to both public cloud platforms.

Connectivity can be from an any-to-any (IP VPN) network, a point-to-point Ethernet network, or a virtual cross-connection through a connectivity provider at a co-location facility. ExpressRoute connections do not go over the public Internet. This allows ExpressRoute connections to offer more reliability, faster speeds, lower latencies, and higher security than typical connections over the Internet.

Describe components of the architecture:

* + 1. ***Compute***
* Azure Virtual Machine is one of several types of on-demand, scalable computing resources that Azure offers. Typically, it is advised to choose a virtual machine if need is for more control over the computing environment than the other choices offer.
* An Azure virtual machine gives the flexibility of virtualization without having to buy and maintain the physical hardware that runs the virtual machine. However, there is still a need to maintain the virtual machine -- configuring, patching, and maintaining the operating system and any other software that runs on the virtual machine.

This table will be helpful to compare the choices offered by Azure.

|  |  |
| --- | --- |
| Compute Options | Audience |
| App Service | Scalable Web Apps, Mobile Apps, API Apps, and Logic Apps for any device |
| Cloud Services | Highly available, scalable n-tier cloud apps with more control of the OS |
| Virtual Machines | Customized Windows and Linux VMs with complete control of the OS |

Azure Virtual Machines lets you create and use virtual machines in the cloud. Providing what's known as Infrastructure as a Service (IaaS), virtual machine technology can be used in variety of ways. Some examples are:

•Virtual machines (VMs) for development and test. Development groups commonly use VMs because they offer a quick, easy way to create a computer with specific configurations required to code and test an application. Azure Virtual Machines provides a straightforward and economical way to create these VMs, use them, then delete them when they're no longer needed.

•Running applications in the cloud. It makes economic sense to run some applications in the public cloud. One example is an application that has large spikes in demand. Although you could equip your own data center with enough hardware to handle peak demand, that hardware might be underutilized much of the time. Running this application on Azure lets you pay for extra VMs only when you need them and shut them down when you don't. Or, suppose you're a start-up that needs on-demand computing resources quickly and with no commitment. Once again, Azure can be the right choice.

•Extending your own datacenter into the public cloud. When you use Azure Virtual Network, your organization can create a virtual network (VNET) that's an extension of your own on-premises network and add VMs to that VNET. This allows running applications such as SharePoint, SQL Server and others on an Azure VM. This approach might be easier to deploy or less expensive than running them in VMs your own datacenter.

Rather than paying continuously for a backup datacenter that's rarely used, IaaS-based disaster recovery lets you pay for the computing resources you need only when you really need them. For example, if your primary datacenter goes down, you can create VMs running on Azure to run essential applications, then shut them down when they're no longer needed.

VMs can be managed using a browser-based portal, command-line tools with support for scripting, or directly through the REST API. Microsoft partners such as RightScale and ScaleXtreme also provide management services that rely on the REST API.

Along with the OS, other configuration choices you have with VMs include:

•The size, which determines factors such as how many disks you can attach and the processing power. Azure offers a wide variety of sizes to support many types of uses.

•The Azure region where your new VM will be hosted, such as in the US, Europe, or Asia.

•VM extensions, which give your virtual machine additional capabilities, such as running anti-virus or using the Desired State Configuration feature of Windows PowerShell.

Other benefits to consider for VMs include:

Pay-as-you-go -- Azure charges an hourly price based on the VM’s size and operating system. For partial hours, Azure charges only for the minutes of use. Storage is priced and charged separately.

Resiliency -- Azure monitors the physical hardware that hosts each running VM. If a physical server running a VM fails, Azure notices this, moves the VM to new hardware and restarts the VM. This process is sometimes called service healing. Azure also protects a virtual machine's data, by keeping redundant copies of the VHDs in blob storage.

**Azure Regions:**

Microsoft allows deploying Virtual Machines into so called ‘Azure Regions’. An Azure Region may be one or multiple data centers that are located in close proximity. For most of the geopolitical regions in the world Microsoft has at least two Azure Regions. E.g. in Europe there is an Azure Region of ‘North Europe’ and one of ‘West Europe’. Such two Azure Regions within a geopolitical region are separated by significant enough distance so that natural or technical disasters do not affect both Azure Regions in the same geopolitical region. Since Microsoft is steadily building out new Azure Regions in different geopolitical regions globally, the number of these regions is steadily growing and as of Dec 2015 reached the number of 20 Azure Regions with additional Regions announced already. You as a customer can deploy SAP systems into all these regions, including the two Azure Regions in China. For current up to date information about Azure regions see this website: <https://azure.microsoft.com/regions/>

**Azure Availability Sets**

Azure Virtual Machines within one Azure Availability Set will be distributed by the Azure Fabric Controller over different Fault and Upgrade Domains. The purpose of the distribution over different Fault and Upgrade Domains is to prevent all VMs of an SAP system from being shut down in the case of infrastructure maintenance or a failure within one Fault Domain. By default, VMs are not part of an Availability Set. The participation of a VM in an Availability Set is defined at deployment time or later on by a reconfiguration and re-deployment of a VM.

* + 1. ***Storage***

An Azure storage account is a secure account that gives you access to services in Azure Storage. Your storage account provides the unique namespace for your storage resources. There are two types of storage accounts:

* A standard storage account includes Blob, Table, Queue, and File storage. To create a standard storage account.
* A premium storage account currently supports Azure Virtual Machine disks only.

Windows Azure Storage provides durability by constantly maintaining multiple healthy replicas for your data. To achieve this, replication is provided within a single location (e.g., EU West), across different fault and upgrade domains. This provides durability within a given location. But what if a location has a regional disaster (e.g., wild fire, earthquake, etc.) that can potentially affect an area for many miles?

Azure supports a feature called geo-replication, which replicates customer data hundreds of miles between two locations (i.e., between North and West Europe, and between East and Southeast Asia) to provide disaster recovery in case of regional disasters. The geo-replication is in addition to the multiple copies maintained by the DFS layer within a single location described above.

* + 1. ***Databases***

**SQL IaaS**

You can host SQL Server on Azure Virtual Machines in a variety of configurations, ranging from a single database server to a multi-machine configuration using AlwaysOn Availability Groups and an Azure Virtual Network.

These databases are managed and configured like they would be today

**SQL Azure**

Microsoft Azure SQL Database is a relational database-as-a-service that delivers predictable performance, scalability, business continuity, data protection, and near-zero administration to cloud developers and solution architects. Developers building software-as-a-service (SaaS) applications can use Azure SQL Database to provide flexibility to support both explosive growth and profitable business models. For workloads with unpredictable database resource consumption, the elastic database model gives you the ability to pool resources to use among a group of databases. Instead of overprovisioning to meet peak demand, you can use an elastic database pool to let hundreds or thousands of databases use resources within a budget that you control. You can drive cost efficiencies with a purchase model that lets you maintain control over price and performance across a group of databases.

* + 1. ***Networking***

The network design on Azure has been proposed keeping security controls in consideration. Each environment has been proposed to be provisioned in separate VMs.

Each environment is further subdivided into separate subnets for individual tier. This is also in line with security best practice with each tier being behind a further set of firewalls than the previous tier.

The existing CT MPLS link will be connected to Azure through ExpressRoute as shown in Figure using 1Gbp links. ExpressRoute has been chosen over a regular connection over the Internet to allow for higher bandwidth as well as secure connectivity. Since the Azure platform will be the strategic hosting location going forward, it is imperative that connectivity to this platform is secured from the internal network. This also allows Azure to be treated as just another Data Centre along with London and some of the global sites currently linked through MPLS.

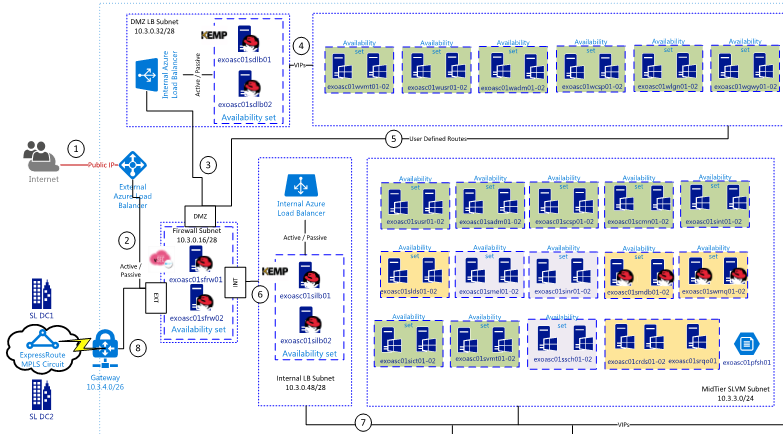
For high availability, Azure VMs in individual tiers have been load balanced. Azure Load Balancer has been used in respective tiers of each of the VNets as shown in deployment architecture diagram in section 6.3. There are two levels of load balancing available for Azure infrastructure services:

* DNS Level: Load balancing for traffic to different cloud services located in different data centers, to different Azure websites located in different data centers, or to external endpoints. This is done with Azure Traffic Manager and the Round Robin load balancing method.
* Network Level: Load balancing of incoming Internet traffic to different virtual machines of a cloud service, or load balancing of traffic between virtual machines in a cloud service or virtual network. This is done with the Azure load balancer.

Please refer next section for detailed network architecture.

* 1. Network architecture

Considering the requirement/existing infrastructure of <Customer/project/application> below is the Network Architecture



<*Attach the Network diagram that depicts the Network components used in the project such as* ***Vnet****,* ***Subnet****,* ***S2S****,* ***Express route****,* ***Firewall****,* ***NSG, UDR*** *and* ***Load balancers*** *with “Figure No” and refer that on the explanation*>

* **Vnets** : <*Short intro on the network deployment and design decision information* *Ex: Class B of range 172.16.0.0/16 is chosen as the number of host is more than 3000 and network is 100 also as not to overlap with the OnPrem Network IP range* >
  + Vnet Name and IP address range in a tabular column as below

|  |  |  |
| --- | --- | --- |
| **Environment** | **Vnet Name** | **IP Range with CIDR** |
| Production | <*XXEASC01VNPRD01*> | <*10.3.0.0/20*> |
| Non Production | <*XXEASC01VNPRD01*> | <*172.16.0.0/16*> |

* + Subnet details along with the purpose as similar to below tabular column

|  |  |  |
| --- | --- | --- |
| **Subnet Name** | **IP Range with CIDR** | **Purpose** |
| DMZSubnet | 192.168.2.1 | All the internet facing VMs are added |

* **Site to Site : <***short intro on the connectivity, explaining the need and the connected datacenter**details***>**
  + Attach document of OnPrem device details and Azure VPN Gateway & Connection details
  + VNet Gateway information
    - Gateway Subnet details
    - VPN Type – Route/policy based
    - Public IP address
  + Connections
    - Connection type : Site to Site or Vnet to Vnet
    - Provide all connection details that are made on the Gateway
* **Express Route**: <provide details on express route if any>
* **Azure Load Balancers(internal/External)**: <*short intro on the necessity and reason of choosing LB with metrics – ex: the web servers which are on high availability needs load balancer at the network level with bare minimum requirements so opted for the Azure LB*>
  + **Internal Load Balancer:** provide details in the following table format

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **LB Name** | **Vnet and Subnet Name** | **Private IP** | **VMs attached** | **Protocol/ Port** | **Healthcheck** |
| <xxx> | <xxx> | 198.162.1.3 | \* VM1  \* VM2 | TCP/IP - 1433 |  |

* + **External Load Balancer :** provide details in the following table format

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **LB Name** | **Public IP Address** | **VMs attached** | **Port/Protocol** | **Healthcheck** |
| <xxx> | 40.162.1.3 | \* VM1  \* VM2 | TCP/IP - 1433 |  |

* **Any Third Party Load balancers(F5/KEMP)**: <*short intro on the necessity of choosing third party load balancer and comparison on the LB list considered with data – ex: since the required throughput cannot be achieved on Azure load balancer it is decided to go with third party LB appliances, among which XX lb is chosen because of the metrics mentioned in the table*>
  + Comparison table(if any)

|  |  |  |  |
| --- | --- | --- | --- |
| **Specs.** | **F5 LTM** | **Azure Load Balancer** | **KEMP Loadmaster** |
| L4 / L7 Support | Available | Available (AG for L7) | Available |
| One arm / Two arm | One ARM | One ARM | - |
| Throughput | 1. GBPS | N/A (email attached) | 10 GBPS |
| SSL Offload | Yes | Yes (via AG) | Yes |
| Health Probes | Yes | Yes | Yes |
| HA mode | Active-Active via Azure LB | AG – 99.9% | - |
| WAF Security | Available (Separate Purchase – ASM) | No | Available |

* + Chosen LB details

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **LB Name** | **Public IP Address** | **VMs attached** | **Port/Protocol** | **Healthcheck** |
| <xxx> | 40.162.1.3 | \* VM1  \* VM2 | TCP/IP - 1433 |  |

* **Traffic Manager**: <*short intro on the decision of choosing traffic Manager ex: as the application is distributed across 3 datacenter(US, Europe and Asia) to have better performance for the user accessing it from anywhere in the world , TM is suggested and used to route the traffic to nearest datacenter*>
  + Traffic Manager details

|  |  |  |  |
| --- | --- | --- | --- |
| **TM Name** | **DNS Address** | **Services attached** | **Type** |
| <xxx> | xx.trafficmangers.net | \* CS1  \* CS2 | Performance |

* **Application Gateway: <***short intro on the reason behind choosing AG – Ex: The application server requires a high availability with load balancing but is has a sticky session, to cater this it is agreed to use the AG***>**
  + **Provide AG details in the following format**

|  |  |  |  |
| --- | --- | --- | --- |
| **AG Name** | **Vnet and Subnet Name with IP** | **Public/Private IP** | **workloads attached** |
| <xxx> |  | 40.2.3.4 | \* VM1  \* VM2 |

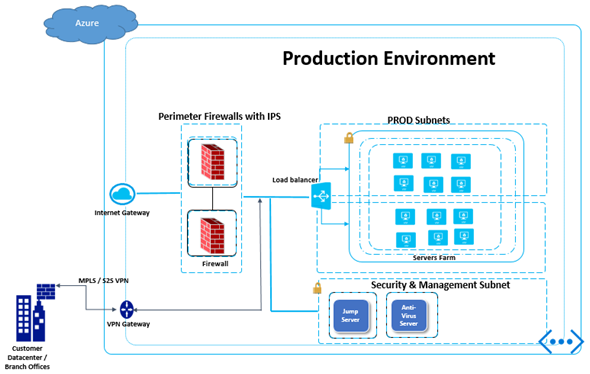
* **Network File Share**(if any): provide details on the network file share

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Storage Account Name** | | **Storage Size** | **Machines Attached with drive letter** | **Additional details(if any)** |
| <xxx> |  | | VM1 | \* VM1  \* VM2 |

* **Network Security Group** : <*Attach the NSG rules excel sheet here*>



* **User Defined Route : <***Attach the route table excel***>**
* **Firewall: <***short intro on the firewall components used and add design decisions if any***>**
* **Traffic Flow Explanation: <***add step by step statement on how the traffic flow when user try to access any particular machine or VM***> - Example below**
  + ***Step 1 :*** *Internet users trying to access the application/Machine*
  + ***Step 2:*** *traffic routed to firewall LB …………………….*
* **~~DR Network~~ : <***assuming HA/DR will cover***>**
  1. Security architecture



Present the security related components of the solution:

1. Security (setup & implementation, AV, Anti-malware)
2. Identity (identity mgmt. between applications, AD)
3. Third-party (appliances, AV, Anti-malware)
4. RBAC rule on resource group level or resource level.
5. Azure security center
6. Any log analysis VM from azure marketplace or any existing tools for security team
7. 3rd party network virtual appliance firewalls like Cisco, Barracuda etc
8. Firewall rules to be defined on 3rd party Network VA, and NGS

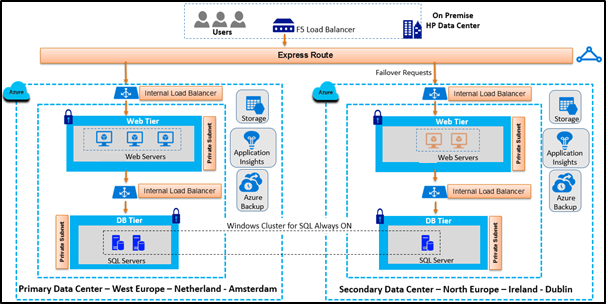
Create template to collect the firewall rules.

1. Azure key vault for key management
2. IDS server VM, either from the marketplace or any existing tool.
   1. Governance architecture

Covers the decision making **processes, criteria and policies** involved in the planning, architecture, acquisition, deployment, operation (quota management, access to resources) and management of a cloud enabled solution. Suitable for LLD

Elaborate on the following:

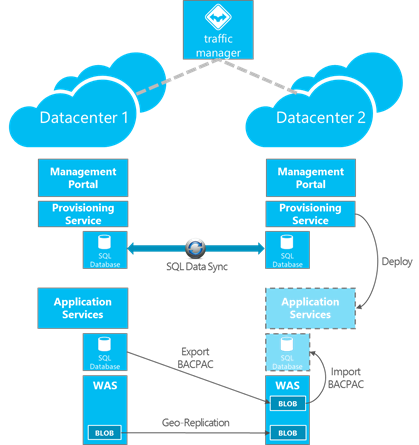
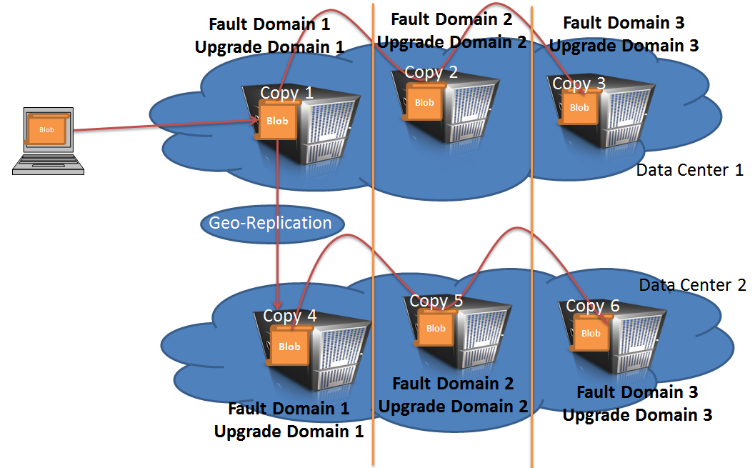
1. Identity Management, Policies
2. Data Policies
3. RBAC
   1. Application architecture



Individual application level architecture if any

Reference Workload architecture (SAP, Oracle, Sharepoint, 3-tier web application)

* 1. Data architecture
* Provide details on kind of replication on storage front with details around FD, UD.
* Provide details on data level replication on DB-tier level based on the technology, technique being used
* Replication
* Security



**Storage Account**:

**Storage Account Design**: <provide design details on storage account such as number of VMs/disk per storage account>

Details on Standard Storage Table:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Storage Account Name** | **Account type** | **Replication** | **VM OS disk** | **VM data Disk** | **Encryption** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Details Premium Storage Table

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Storage Account Name** | **Account type** | **Replication** | **VM OS disk** | **VM data Disk** | **Encryption** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Data Import/Export**: <*Provide details on the Data import/export strategy from OnPrem to Cloud*>

**Storage Account Security**: <Add details on the security features enabled and implemented>

* SAS
* Encryption (Data at rest and transit)

**SQL Server Clustering –** Add sql server clustering design if used any, such as

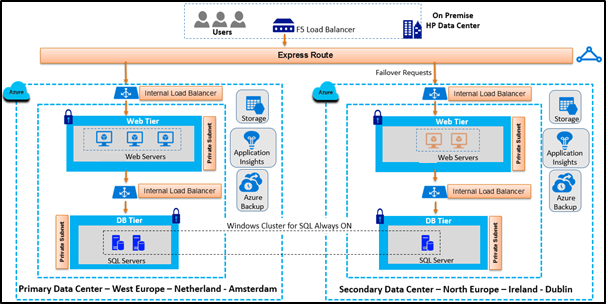
* Cluster technology - Always on/Data Guard
* Number of primary, secondary and witness instances
* Failover and Failback design
* Setup diagram that includes sql server instances, AD and flow

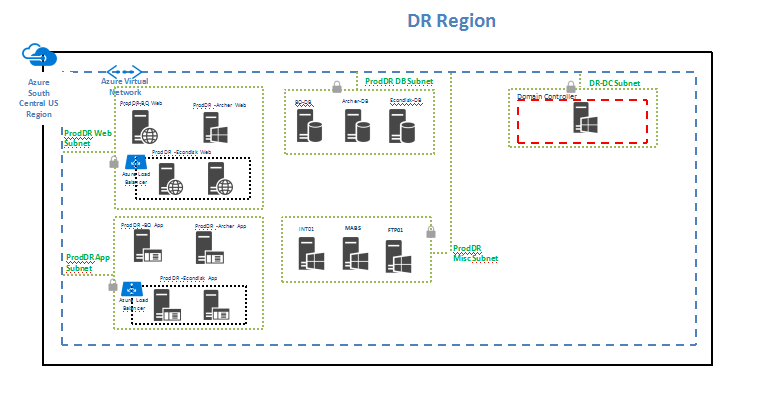
**SQL Server data replication**

* Data replication design
* Frequency
* Recovery process

**SQL Server data backup strategy**

* RTO/RPO on Data recovery and restore
* Policy/Frequency of Incremental, Transactional and Full databackup
  1. HA/DR architecture
* HA/DR architecture detailing at “overall Azure Landscape diagram” level, at app-level
* Provide the design decisions on providing HA solution keeping availability-SLA in mind
* Provide the design decisions on providing DR solution keeping RTO/RPO in mind





1. Region Selection (also include reason like component availability, complains, user location and etc.) [Note: regional pairs as Secondary is preferred due to Platform-provided replication, Region recovery order, Sequential updates, Data residency]
2. Finalized RTO and RPO for each application.
3. DR approach (Warm/Hot/Cold/CA) / (Same/Reduced configuration)
   1. Client requirement on disaster process.
   2. Reason for considering particular approach
4. DR implementation process.
   1. How components are designed in secondary region (VM, Storage, Web Apps and etc.).
   2. How data replication is implemented for each and every component (SQL, AD, Files and etc.).
   3. How DNS, IP, Connection strings are managed in secondary region?
   4. Application wise Design for failure over.
   5. What are the automation done?
   6. Fail over and Fail Back workflow process.
5. Features available in the Secondary Region
   1. Monitoring secondary site.
   2. HA on secondary site
   3. Backup strategy enabled for secondary site
6. DR Audit/testing and training process.
   1. Fail over test
   2. Fail back test
   3. DR Training
7. DR Activate Scenario
   1. What are all the situations are considered as Disaster and we are activating the DR Process.
   2. What are all the process related steps involved before activate DR Process
8. Fail Over Process
9. Fail Back Process
10. Change management process
    1. If any changes made in primary how we are going to incorporate this?

HA

1. Basic details about HA for the application.
   1. What is the availability percentage expected.
   2. If HA is not required then proper reason and client acceptance
   3. How VMs are grouped and availability set is configured
2. How load balancer are configured and details about those

High Availability implementation

|  |  |
| --- | --- |
| **Application** | **HA Approach** |
| Web application on VM | Multiple VM with Availability Set/Single VM with Premium disk |
| MS SQL on VM | Always On Availability Groups/ Always On Failover Cluster Instances/ SQL Mirroring/etc. |
| Etc | Etc. |

* 1. Backup & Recovery architecture

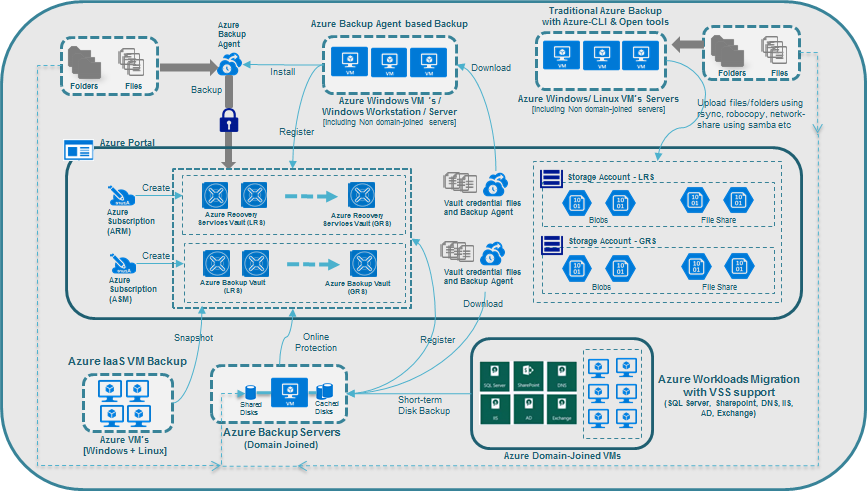


Figure 3: Backup Solution Architecture

The backup solution architecture as shown in Figure 3 provides a pictorial view of fitment of necessary Azure backup components to be used for <Customer> workloads. As per the solution architecture,

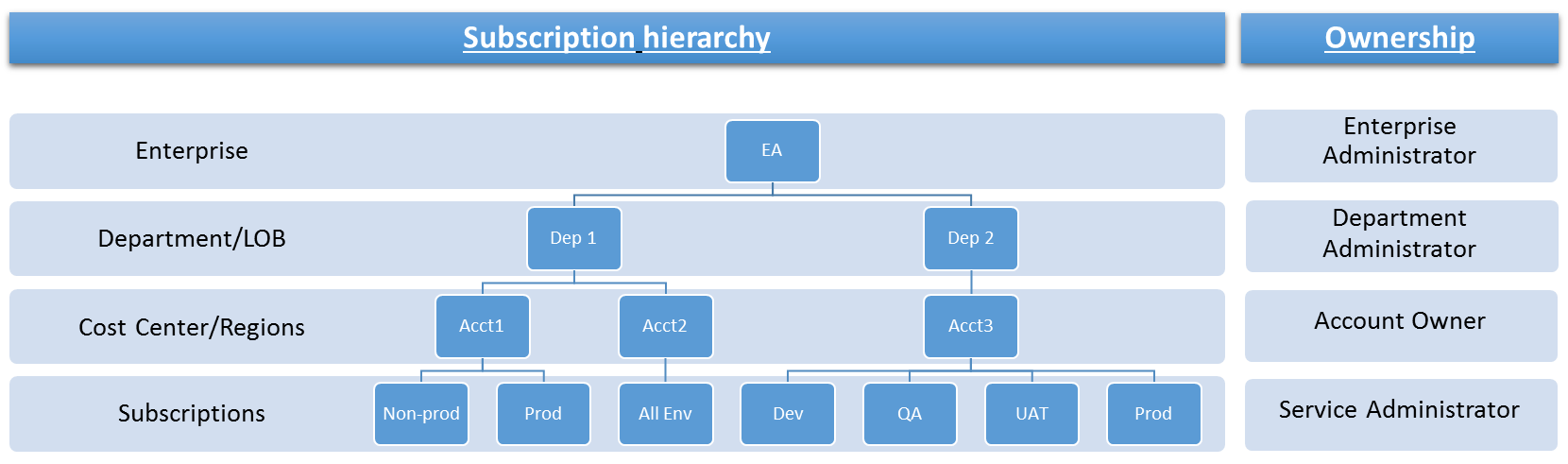
* *Azure Recovery Services Vault’s* will be used for ARM subscription based VMs, while *Azure Backup Vault’s* will be used for ASM subscription based VMs.
* Every recovery vault registers the target VMs to be backed up if it is agent-based backup using *Azure Backup Agent*. Multiple vaults might be required as there is a limit-restriction on the registration of maximum number of VMs. Please refer the facts & limitation sub-section below for additional details.
* Recovery/Backup vaults would be associated with different storage accounts whether in LRS or GRS based on the requirements. Please refer the criteria on choosing either LRS or GRS in the design decision section.
* Azure File-Share would be the option to be used for automating the backing up file/folders majorly for Linux VMs.
* Following Azure backup components can be used for snapshot (image and volume), file/folders level backup based on the type of workloads:

1. Azure IaaS VM Backup: Mainly for Windows VMs (app-aware) and Linux VMs (file-consistent, not app-aware), and also VMs which are not domain-joined
2. *Azure Backup*
3. Agent-based Backup using *Azure Backup Agent (ABA)* : Mainly for Windows workloads
4. Traditional backup using automation for majorly Linux VMs – as an alternate solution for backup of Linux VMs (mainly) at file/folders level.

* Any single *MABS* will be chosen to backup VMs in a specific domain. MABS can have multiple disks attached to it to have local backup for the latest data with an option of online-backup on associated recovery vault.
* There can be multiple MABS based on the **Facts & Limitations.**
* Hybrid backup scenario
* DPM tool
  1. Hybrid architecture – VPN (nice to have)
  2. Subscription Management

During migration planning, Cloud subscription management is another importance aspect to work on. This will help to determine the roles and challenges involved when planning and managing subscriptions. Here are some of the points to consider:

In order to deploy service in azure, client would need access to azure subscription. There are multiple ways to procure it.

1. **Pay as you go: -** No minimums or commitments. Use credit card to sign-up. Cancel anytime. Click [here](https://azure.microsoft.com/en-in/offers/ms-azr-0003p/) to know more
2. **Buy from a Microsoft Reseller**
   1. Cloud Solution Provider: - With the Cloud Solution Provider program, work directly with a partner to design and implement a solution that meets your unique needs. Click [here](https://azure.microsoft.com/en-in/offers/ms-azr-0145p/) to know more
   2. Open: - Work with the same resellers from whom you may currently purchase Microsoft software under the Open Volume License Program. Already have an Azure in Open license key? Activate a new subscription or add more credits here. Click [here](https://azure.microsoft.com/en-in/offers/ms-azr-0111p/) to know more
3. **EA - <Customer Name>**: - This is an Enterprise agreement procured by <Customer Name> by directly working with Microsoft. Please find below a diagram that depicts a suggested subscription hierarchy and Ownership with <Customer Name> EA

**Subscription hierarchy**

* 1. Enterprise :- Create on agreement for the entire <Customer Name> organization that can be leveraged across departments and verticals within organization
  2. Department/LOB :- Create a department for each LOB( like Accounting, Sales etc..) or corporate functions(like HR, Finance etc..) within the organization
  3. Cost Center/Regions :- Create accounts based on a combination of cost center and regions
  4. Subscriptions:- Depending on Metering and Billing requirements non-prod and prod environments can be created

**Ownership**

1. Enterprise Administrator (<Customer Name> <Infrastructure Service Delivery Manager>)

* Has the ability to add other Enterprise and Department Administrators, add Departments, add or associate Accounts to the Enrolment
* Can view usage and charges Data across all Accounts and Subscriptions
* Can view the monetary commitment balance associated to the Enrolment.
* There is no limit to the number of Enterprise Administrators on an Enrolment.

1. Department Administrator (<Customer Name> <Business Unit Manager>)

* Has the ability to edit their department name and cost Centre, manage department admins, add accounts to the enrolment and their departments, remove accounts from their departments
* Can view Department charges if enabled by the Enterprise Administrator

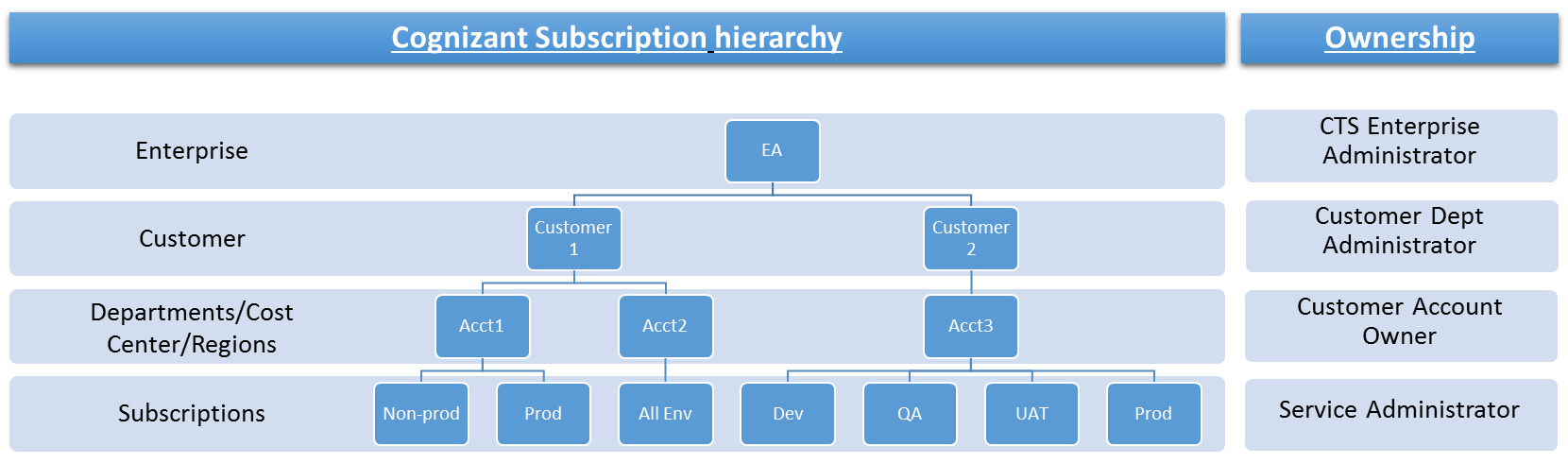
1. Account Owner (<Customer Name> <Technical Lead of Business Unit>)

* Can add Subscriptions for their Account, update the Service Administrator and Co-Administrator for an individual Subscription, and view usage Data for their Account within the Account Portal
* The Account Owner will be the default Service Administrator on new subscriptions

1. Service Administrator (<Customer Name> <Program Manager>)

* Has the ability to access and manage Subscriptions within the Azure Management Portal
* Up to 199 Service Co-Administrators per Subscription

1. **EA - Cognizant: -** This is an Enterprise agreement procured by Cognizant by working with Microsoft. This option should only be considered if managed services for the workloads hosted in the subscriptions are provided by Cognizant. Please find below a diagram that depicts a suggested subscription hierarchy and Ownership with Cognizant EA



Please find attached below couple of documents for requesting Azure subscription in cognizant EA



**Subscription hierarchy**

* 1. Enterprise :- Agreement entered by cognizant with Microsoft
  2. Customer :- Create customer as department
  3. Departments/Cost Center/Regions:- Create an account for each LOB( like Accounting, Sales etc..) or corporate functions(like HR, Finance etc..) within the organization using a combination of cost center and region
  4. Subscriptions:- Depending on Metering and Billing requirements non-prod and prod environments can be created

**Ownership**

1. CTS Enterprise Administrator (CTS ITRMG)

* Has the ability to add other Enterprise and Department Administrators, add Departments, add or associate Accounts to the Enrolment
* Can view usage and charges Data across all Accounts and Subscriptions
* Can view the monetary commitment balance associated to the Enrolment.
* There is no limit to the number of Enterprise Administrators on an Enrolment.

1. Department Administrator (<Customer Name> <Delivery Manager>)

* Has the ability to edit their department name and cost Centre, manage department admins, add accounts to the enrolment and their departments, remove accounts from their departments
* Can view Department charges if enabled by the Enterprise Administrator

1. Account Owner (CTS Program Manager)

* Can add Subscriptions for their Account, update the Service Administrator and Co-Administrator for an individual Subscription, and view usage Data for their Account within the Account Portal
* The Account Owner will be the default Service Administrator on new subscriptions

1. Service Administrator (CTS Architect)

* Has the ability to access and manage Subscriptions within the Azure Management Portal
* Up to 199 Service Co-Administrators per Subscription

1. Design Considerations

This section describes many of the areas which need to be addressed or resolved before attempting to devise a complete design solution.

* 1. Scalability considerations

Explain how the solution will tackle scalability requirements



## Scale up & Scale out - Auto-scale, VM Scale sets

* 1. Availability considerations

Explain how the solution will tackle Availability requirements



## Recovery services – Backup, DR

**Looks it is already covered in DR and HA Architecture do we need hear**

* What is the Aggregate availability for the application and is it satisfying the customer need?
* How the application will handle the data corruption/data loss?
* How the application will handle the Outage
  + Partial outage
  + Full Outage
  + Performance degradation
* How our DR approach will satisfy the customer RTO and RPO.
* Is it global outage considered
* Do our application run in downgraded functionality when some components goes down?
* Do out environment designed to self-heal

## SLA

* 1. Manageability considerations

This section will cover application management & maintenance topics like Diagnostics, Logging, Health Monitoring etc

* 1. Security considerations
* Security appliances should be HA
* In case of using BYOL for 3rd party VA, please define the ownership.
* Use UDR to route the traffic from 3rd party VA
* Use template to collect firewall rules for 3rd Party VA, and NSG
* Use key vault for resource group security and storage security as well, if possible
* Enable RBAC on resource group, and resources and assign access only on demand to maintain proper access governance.
* In case of multitenant scenario, create separate vnet for all management VMs, and peer this management vNet with other vNet.
* Avoid using public IP on a VM for RDP, if S2S VPN or express route is in place.
  1. Subscription considerations
* POC v/s actual implementations
* Financial commitment
* Roadmap of transformation
* Scale of organization
* Access Levels
* Metering and chargeback
* Limits of subscription
* Maintenance Overhead

1. Solution deployment

Provide details on how the solution will be deployed

1. Validation
2. Handover to managed services

The following lists the details to be shared with MSS team

6. 1. Azure Components

## Azure Storage

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Status** | **Location** | **Status** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## 

## Azure Virtual Machines

**<<Need to update/Change the content>>**Azure **Virtual Machine** (**VM**) is an operating system OS or application environment that is provisioned on Azure which imitates dedicated hardware. Microsoft Azure Virtual Machines allow you to deploy a wide range of computing solutions in an agile way. With Virtual Machines, you can deploy nearly instantaneously and you pay only by the minute. With Windows, Linux, SQL Server, Oracle, IBM, SAP and BizTalk, you can deploy any workload, any language, on nearly any operating system. Azure has two different deployment models for creating and working with resources they are Resource Manager and classic.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Environment** | **VM Name** | **Azure Instance Name** | **VM Type (CPU/RAM)** | **OS** | **Status** |
| Production |  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Monitor |  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Non Production |  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Azure Internal Load Balancer

**<<Need to update/Change the content>>**Azure Internal Load Balancer (ILB) is a security enhancement over the Internet facing load balancer that is offered in Azure. Access to the ILB can only be done by resources inside the cloud service or using VPN to access the Azure infrastructure to reach the ILB. The infrastructure restricts the accessibility and creates a trust boundary between the load balanced virtual IP addresses to a Cloud Service or a Virtual Network and will never be exposed to an Internet endpoint directly. This enables internal Line of Business applications to run in Azure and be accessed within the cloud or from on-premises.

An Azure load-balanced set is a Layer 4 load balancer that works with TCP and UDP workloads. By default, it uses a 5-tuple load-balancing algorithm which uses protocol, source port, destination port, source and destination IP address. Two additional distribution modes can be configured using PowerShell to help enable additional stickiness: 2-tuple or and 3-tuple.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Environment** | **ILBName** | **ILB Ip** | **App VMs** | **App VM Ips** |
|  |  |  |  |  |
|  |  |
|  |  |  |  |  |

* 1. Network Configuration

## Static Internal Private IP

<<Need to update/Change the content>>VMs in a virtual network will automatically receive an internal IP address from a range that we specify. But in certain cases, specifying a static IP address for a particular VM makes sense. Using static Internal Private IP option Azure provides the ability to predict which IP address of virtual machine will have at boot time and as long as the virtual machine is not re-provisioned that IP address will remain the same.

|  |  |  |
| --- | --- | --- |
| **Environment** | **VM Name** | **Static Internal Private IP** |
| Production |  |  |
|  |  |
|  |  |
|  |  |
| Non Production |  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| Monitoring |  |  |
|  |  |
|  |  |

## Networks / Vnets

<<Need to update/Change the content>>An Azure virtual network (VNet) is a representation of the own network in the cloud. It is a logical isolation of the Azure cloud dedicated to our subscription. We can fully control the IP address blocks, DNS settings, security policies, and route tables within this network. We can also further segment your VNet into subnets and launch Azure IaaS virtual machines (VMs) and/or Cloud services (PaaS role instances). Additionally, we can connect the virtual network to your on-premises network using one of the connectivity options available in Azure. In essence, we can expand the network to Azure, with complete control on IP address blocks with the benefit of enterprise scale Azure provides.

|  |  |  |
| --- | --- | --- |
| **Environment** | **Network Name** | **Location** |
|  |  |  |
|  |  |  |

## 

## Subnets

<<Need to update/Change the content>>A subnet, is a logical, visible subdivision of an IP network. The practice of dividing a network into two or more networks is called subnetting. Using subnets will decrease the size of the broadcast domain, allowing data to reach its destination much faster.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Environment** | **Network Name** | **Subnet Name** | **CIDR** | **Virtual Machines** |
| Production |  |  |  |  |
|  |  |  |
| Non Production |  |  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## VPN Setup

<<Need to update/Change the content>>A virtual private network also known as a VPN is a private network that extends across a public network or internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. VPNs can be either remote-access (connecting a computer to a network) or site-to-site (connecting two networks). A Site-to-Site connection is a connection over IPsec/IKE (IKEv1 or IKEv2) VPN tunnel. This type of connection requires a VPN device or Windows Server RRAS on-premises.

VPN Gateway is a collection of settings that are used to send network traffic between virtual networks and on-premises locations. VPN Gateway is used for Site-to-Site, Point-to-Site, and ExpressRoute connections. VPN Gateway is also used to send traffic between multiple virtual networks within Azure (VNet-to-VNet). VPN Gateway can be added to a virtual network to create a connection. Each virtual network can have only one VPN Gateway and there are specific configuration steps for each connection.

|  |  |  |
| --- | --- | --- |
| **Gateway** | **Type** | **IP** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

* 1. AD Configuration

## AD Group Policy

<<Need to update/Change the content>>Group Policy is a feature of the Microsoft Windows NT family of operating systems that controls the working environment of user accounts and computer accounts. Group Policy provides the centralized management and configuration of operating systems, applications, and users' settings in an Active Directory environment.

|  |  |  |
| --- | --- | --- |
| Default Domain Policy (Prod & Non Prod) | | |
| GPO Path | Policy | Value |
|  |  |  |
|  |  |
|  |  |
|  |  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |  |
|  |  |
|  |  |

|  |  |  |
| --- | --- | --- |
| <<Custom Policy>> | | |
| GPO Path | Policy | Value |
|  |  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |  |
|  |  |
|  |  |
|  |  |
|  |  |

## AD Users and Groups

<<Need to update/Change the content>>A great part of network administration involves management of users and groups. Only properly authenticated users can logon to the network and that each network resource.

|  |  |  |  |
| --- | --- | --- | --- |
| **Environment/FQDN** | **Users** | **Member Of** | **Type** |
| Non Prod / << FQDN >> |  |  | User |
|  |  | User |
|  |  | User |
|  |  | User |
|  |  | User |
|  |  | User |
|  |  | User |
|  |  | User |
|  |  | Group |
|  |  | User |
| Prod / << FQDN >> |  |  | User |
|  |  | User |
|  |  | User |
|  |  | User |
|  |  | User |
|  |  | User |
|  |  | Group |

## AD Trust

<<Need to update/Change the content>>A one-way trust is a unidirectional authentication path that is created between two domains. This means that in a one-way trust between Domain A and Domain B, users in Domain A can access resources in Domain B. However, users in Domain B cannot access resources in Domain A. A one-way, outgoing, external trust will allow resources in your domain (the domain that you are logged on to at the time that you run the New Trust Wizard) to be accessed by users in a different Active Directory domain (outside your forest) or in a Windows NT 4.0 domain.

|  |  |
| --- | --- |
| **Environment** | **Outgoing Trust** |
|  |  |
|  |  |

## Conditional Forward

<<Need to update/Change the content>>Conditional forwarders are DNS servers that forward queries according to domain names. Rather than having a DNS server forward all queries it cannot resolve locally to a forwarder, you can configure DNS servers to forward queries to different forwarders according to the specific domain names that are contained in the queries.

|  |  |  |
| --- | --- | --- |
| **Environment** | **DNS servers** | **IP** |
| Production |  |  |
|  |  |
| Non-Production |  |  |
|  |  |
|  |  |

* 1. VM Configuration

## Hardening setup

Attach the OS hardening checklist

## Access management

Attached the Excel which contains groups/users having permissions to System administration, Remote Desktop in to VMs, MS SQL management and access shared folders.

## Append the DNS suffixes.

<<Need to update/Change the content>>We have to add the below DNS in the same order for applications resolve machine name correctly. When performing a name resolution request, this will append the DNS suffix of the machine and DNS suffix for this connection. In the IPv4 “Advanced IP Settings” window select the Tab “DNS”. In the DNS Suffixes list box below entries should be added in all the machines.

|  |
| --- |
| **DNS Suffixes** |
|  |
|  |
|  |

* 1. WSUS

<<Need to update/Change the content>>Windows Server Update Services (WSUS), is a computer program developed by Microsoft Corporation that enables administrators to manage the distribution of updates and hotfixes released for Microsoft products to computers in a corporate environment. WSUS downloads these updates from the Microsoft Update website and then distributes them to computers on a network. WSUS runs on Windows Server and is free to licensed Microsoft customers.

* 1. Anti-Virus

<<Need to update/Change the content>>The modern threat landscape for cloud environments is extremely dynamic, increasing the pressure on business IT cloud subscribers to maintain effective protection in order to meet compliance and security requirements. Microsoft Antimalware for Azure Cloud Services and Virtual Machines is a real-time protection capability that helps identify and remove viruses, spyware, and other malicious software, with configurable alerts when known malicious or unwanted software attempts to install itself or run on your Azure systems.

The solution is built on the same antimalware platform as Microsoft Security Essentials [MSE], Microsoft Forefront Endpoint Protection, Microsoft System Center Endpoint Protection, Windows Intune, and Windows Defender for Windows 8.0 and higher. Microsoft Antimalware for Azure is a single-agent solution for applications and tenant environments, designed to run in the background without human intervention. You can deploy protection based on the needs of your application workloads, with either basic secure-by-default or advanced custom configuration, including antimalware monitoring.

* 1. Backup

## 

## Backup Vault

<<Need to update/Change the content>>Backup Vaults are storage containers within an online disk where backup data resides for a single computer. A Backup Vault allows for block-level data de-duplication within and across multiple files and versions of files as well as compression for all data, which means greatly improved backup speeds and less total data stored. Backup Vaults cannot be browsed via the Network Drive or Web Access features. Backup Vaults are designed and optimized specifically for backup and restore procedures only.

|  |  |  |
| --- | --- | --- |
| **Vault Name** | **Region** | **Subscriptions Name** |
|  |  |  |
|  |  |  |
|  |  |  |

## 

## VM Backup

<<Need to update/Change the content>>When the Azure Backup service initiates a backup job at the scheduled time, it triggers the backup extension to take a point-in-time snapshot. This snapshot is taken in coordination with the Volume Shadow Copy Service (VSS) to get a consistent snapshot of the disks in the virtual machine without having to shut it down.

After the snapshot is taken, the data is transferred by the Azure Backup service to the backup vault. To make the backup process more efficient, the service identifies and transfers only the blocks of data that have changed since the last backup.

|  |  |  |
| --- | --- | --- |
| **Vault Name** | **VMs** | **Scheduled time** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Folder and file backup

<<Need to update/Change the content>>The Azure Backup agent can be deployed on any Windows Server VM that runs in Azure or physical machine it will push the files and folders to the azure vault.

Database backup and application backup are moved to backup Vault for long time persistence.

|  |  |  |  |
| --- | --- | --- | --- |
| **Vault Name** | **Azure Instance Name** | **Drive / Folder** | **Scheduled time** |
|  |  |  |  |
|  |  |  |  |

* 1. Environment Creation

<<Need to update/Change the content>> The entire environment was created by PowerShell / ARM.

* 1. Monitoring

Monitoring Parameters and Configurations

* 1. Email alert notification process

All monitoring email alert notifications will be sent from email address [xyz@cognizant.com](mailto:xyz@cognizant.com) and reply-to address in the email alerts would be donotreply@cognizant.com.

* 1. Contacts

|  |  |  |
| --- | --- | --- |
|  | **Contact Name** | **Details** |
| **<<Project>> Team** |  |  |
| **Cognizant MSS** |  |  |

1. Glossary

Provide definitions of all terms, acronyms, and abbreviations that might exist to properly interpret this document

1. References

*This section is optional.*

List any documents or resource, if any, which were used as sources of information