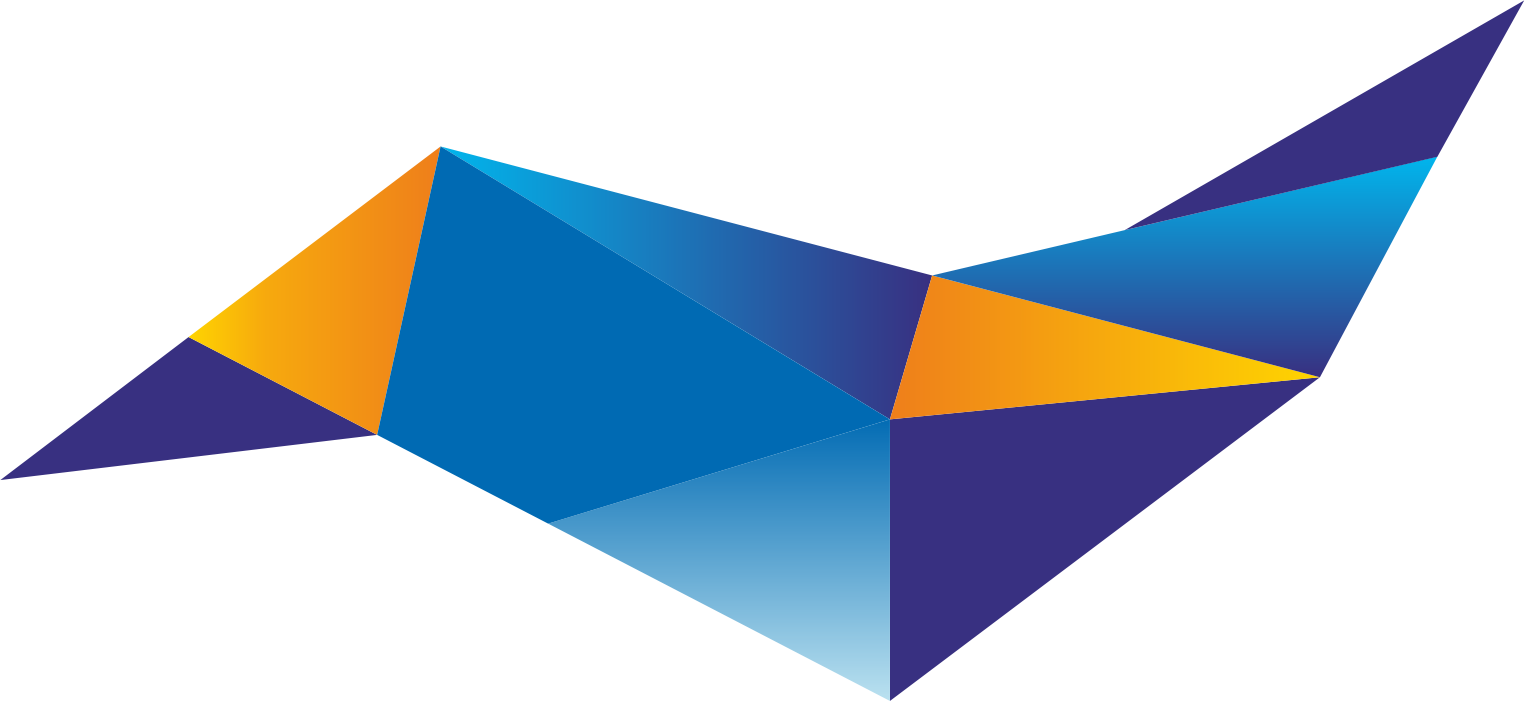


**AZURE CLOUD LANDING ZONE  
DESIGN DOCUMENT**





**Document Revision History:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version No.** | **Authored/Modified By** | **Reviewed By** | **Approved**  **By** | **Last modified  Date** | **Modifications Done** |
| 1.0 | Gowrishankar M | Aktar Shaikh |  |  |  |
|  |  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Role** | **Contact details** | Signature Date |
| Gowrishankar M | Cloud Architect | [Gowrishankar.muddalingachat@lntinfotech.com](mailto:Gowrishankar.muddalingachat@lntinfotech.com) |  |
|  |  |  |  |
|  |  |  |  |

**Table of Contents**

[1 Introduction 5](#_Toc96331596)

[2 Document Purpose 5](#_Toc96331597)

[3 Document Scope 5](#_Toc96331598)

[4 Scope of Work 5](#_Toc96331599)

[4.1 In-Scope 6](#_Toc96331600)

[4.2 Out of-Scope 6](#_Toc96331601)

[5 Target Audience 6](#_Toc96331602)

[6 Validation Methodology 8](#_Toc96331603)

[7 General Azure Design Considerations 8](#_Toc96331604)

[8 Design Considerations 8](#_Toc96331605)

[8.1 Region 9](#_Toc96331606)

[8.2 Networking 9](#_Toc96331607)

[8.3 Security 10](#_Toc96331608)

[8.3.1 Azure Firewall 10](#_Toc96331609)

[8.3.2 Azure Bastion 10](#_Toc96331610)

[8.3.3 Azure Application Gateway 10](#_Toc96331611)

[8.3.4 Antivirus 10](#_Toc96331612)

[8.3.5 Vulnerability Management 10](#_Toc96331613)

[8.3.6 SIEM 10](#_Toc96331614)

[8.4 IDAM 10](#_Toc96331615)

[8.5 Monitoring 11](#_Toc96331616)

[8.6 Patch management 11](#_Toc96331617)

[9 High Level Design Architecture 11](#_Toc96331618)

[10 Management Groups 12](#_Toc96331619)

[11 Subscription Layout 13](#_Toc96331620)

[12 Azure Networking 14](#_Toc96331621)

[12.1 Network Topology 14](#_Toc96331622)

[12.2 Virtual Network 14](#_Toc96331623)

[12.2.1 IP Address Space 15](#_Toc96331624)

[12.2.2 HUB Virtual Network 15](#_Toc96331625)

[12.2.3 SPOKE Virtual Network 16](#_Toc96331626)

[12.2.4 VNet Peering 17](#_Toc96331627)

[12.3 Azure Subnets 18](#_Toc96331628)

[12.4 User Defined Routing ( UDR ) 20](#_Toc96331629)

[12.5 Site to Site VPN 20](#_Toc96331630)

[13 Security 22](#_Toc96331631)

[13.1 Azure Firewall 22](#_Toc96331632)

[13.2 Azure Bastion 24](#_Toc96331633)

[13.3 Network security groups 24](#_Toc96331634)

[13.4 User Defined Routable ( UDR ) 26](#_Toc96331635)

[13.5 SIEM 26](#_Toc96331636)

[13.6 Anti-Virus 26](#_Toc96331637)

[13.7 Multifactor authentication 26](#_Toc96331638)

[14 Azure Storage 27](#_Toc96331639)

[14.1 Disk Types 27](#_Toc96331640)

[14.2 Disk Model 27](#_Toc96331641)

[15 Azure Compute 28](#_Toc96331642)

[16 Azure Site Recovery 29](#_Toc96331643)

[16.1 Disaster recovery 29](#_Toc96331644)

[17 BAU Operation 30](#_Toc96331645)

[17.1 Azure Monitoring 30](#_Toc96331646)

[17.2 Azure Backup 31](#_Toc96331647)

[17.3 Patch Management 32](#_Toc96331648)

[18 Azure Governance 32](#_Toc96331649)

[18.1 Resource Groups 32](#_Toc96331650)

[18.2 Resource Tags 33](#_Toc96331651)

[18.3 Identity 33](#_Toc96331652)

[18.4 Conditional Access Control 34](#_Toc96331653)

[18.5 Role-based access control 35](#_Toc96331654)

[18.6 Resource Manager Policies 36](#_Toc96331655)

[18.7 Azure Resource Locks 39](#_Toc96331656)

[19 Naming Conventions 39](#_Toc96331657)

[19.1 Azure Infra Naming 39](#_Toc96331658)

[19.2 Azure Instance Naming 40](#_Toc96331659)

[20 Architectural Decision Summary 41](#_Toc96331660)

[21 Acronyms 43](#_Toc96331661)

# 

# Introduction

This document details the Landing Zone Design for MUBADALA Shared Services and Hosted Applications planned on Microsoft Azure IAAS designed by LTI. This document accomplishes the business requirements of Agile/Scalable infrastructure to be built on Azure. This would be Green-Field Deployment.

# Document Purpose

The purpose of this document is to define the Azure Landing Zone Layout for MUBADALA Infrastructure and applications. It refers to design considerations, design decisions, recommendations, and constraints that MUBADALA should be aware of and sign-off on the architecture before moving on to the design & implementation phase.

This document will assist the following teams: -

* Build Team - The LTI team will use this document as the basis for the solution implementation.
* Delivery Team – To understand what infrastructure is deployed to be managed and monitored for BAU
* Application Team – To understand the underlying infrastructure on Cloud to support & develop the application.

# Document Scope

This document covers the detailed design for Azure IAAS Landing Zone Services covering Azure Networking, Security, Storage, Compute, High Availability, Disaster Recovery, Governance & Monitoring.

This document does not cover detailed design of common services like Network Virtual Appliance, Load Balancer, Active Directory, Anti-Virus, Encryption Servers, SIEM and other Non-Native solutions.

# Scope of Work

LTI will design the Azure landing zone setup covering the foundational services to host any services in Azure. The landing zone covers Azure subscription governance and policies implementation, network and connectivity, shared service setup (VM Only), cloud native security services implementation and other cloud management services. The LTI will also work towards implementing and testing the Azure foundation setup by extending connectivity and integration to the Mi Cloud setup.

## In-Scope

* Design Azure Landing Zone Architecture aligned with Microsoft Cloud Adoption Framework
* Define organizations Resource Hierarchy, Tagging and Naming Conventions Standards.
* Subscription Layout for Prod and Pre-Pod Environment based on Business/Application Requirement
  + HUB – All Common Services: Azure Firewall, Active Directory, SIEM, Patching etc.
  + Spoke – Business Applications: EDM, FIN, Corp, other applications.
* Design Network Connectivity Flow covering On-Prem and Internet aided with Azure Firewall and S2S connectivity.
* Define Network Topology model for Landing Zone eg: HUB and Spoke Model, Logs
* NSGs, Azure Security Policies, Charge Back/Billing Recommendations, VNet Peering, RBAC, Backup and Monitoring, Log Analytics for Azure Landing Zone Setup
* Define Built-In Azure Policies, Backup Policies and Firewall Policies
* Define Azure Storage Accounts, Compute Type and Disk Types aligned with Application Portfolio
* Define Disaster Recovery solution in paired Azure Region.
* Provide overall Best-Practices and Recommendations for Landing Zone Setup

## Out of-Scope

* Software & hardware procurement
* Integration of any third-party tools with applications
* Workload Migration
* Any code changes needed on application side for DevOps/Infra implementation
* End user communication during implementation
* Any type of Functional or Development related activities
* Any configuration of network/firewall components/CPEs On-Premise
* Any other activity not mentioned in the scope of work
* WAN establishment including any configuration of Network / Firewall component on-Premises

# Target Audience

This document is intended for a technical audience, including the following:

|  |  |
| --- | --- |
| Name | Title |
| Sadatullah Khan |  |
| Sarfaraz Muneer |  |
| Sarith Bhavan |  |

Table 1: Target Audience

# Validation Methodology

We have defined a validation methodology to define and decide on the components in the target environment. The decision was made following the below factors

**Workshop:**

Internal workshop was conducted with each tower to understand the existing landscape and what would be required in the Target infrastructure.

**Q & A Session:**

Discussions were conducted with the Application and Infra stakeholders to derive at the final number of inventory & landscape components required for the target infrastructure.

**SME Session**

Based on the internal discussion and the Q & A Sessions the target infra components were defined. The limitations and requirements were defined to conclude the solution.

# General Azure Design Considerations

* Microsoft Azure is dynamically growing every day with new features and enhancement of existing features.
* Azure Services considered in this document may enhance, integrate, or retire in future as per Microsoft release.
* Cost and Availability of Azure features are subject to Azure region
* LTI followed Microsoft Azure Cloud Adoption Framework guidelines for designing Azure Subscriptions, Virtual Network, and other Azure components.
* LTI accounted the Azure Limitations and Quotas while designing Azure Infrastructure
* LTI considered only Generally Available Azure Services as of Dec 2022 while designing Azure Landing Zone.
* Azure region is selected as UAE North for primary and West Europe for secondary Azure region for Azure Target environment, as per best practice of Azure Paired Regions
* Given Model will be replicated to Prod Subscription

# Design Considerations

The Azure Well-Architected Framework is a set of guiding tenets that can be used to improve the quality of a workload. The framework consists of five pillars of architecture excellence: Cost Optimization, Operational Excellence, Performance Efficiency, Reliability, and Security.

## Region

Based on the understanding target Azure landing zone will be built on region **UAE North** for Primary site and **West Europe** for secondary site is considered for the target infrastructure. As per best practices Azure Paired Region is considered for DR Site.

|  |  |  |
| --- | --- | --- |
| Components | UAE North | West Europe |
| Location | UAE North | West Europe |
| Paired Region | UAE North | TBD |
| Availability Zone | Yes | Yes |
| Service Availability | All | All |
| Data residency | UAE North | West Europe |

Table 2: Azure Regions

## Networking

Based on our understanding of the environment and as per best practices, we will go with **HUB & SPOKE** model for each tenant like “**Production**” & **Pre-Production**” a separate landing zone.

HUB will host 1 VNET & 1 Subscriptions and Spoke will host 4 VNet & 4 Subscriptions for Production and similar approach will be for Pre-Production and both environments isolated from connectivity. We will have separate Subnets for each environment as per Microsoft’s recommendations and best practises.

To ensure cloud-based applications are visible to the corporate network we will establish the connection using Site to Site VPN. Proposed bandwidth is **1Gbps** for On-Prem to Azure Cloud and to accommodate connectivity for business and operations.



Figure 1 : Azure Regions

## Security

### Azure Firewall

Azure firewall is a cloud native network security service. It offers fully stateful network and application-level traffic filtering for VNet resources, with built-in high availability and cloud scalability delivered as a service. We will leverage Azure firewall for filtering inbound and outbound traffic from **On-Prem to Azure**

### Azure Bastion

Azure Bastion is deployed to a virtual network and supports virtual network peering. Specifically, Azure Bastion manages RDP/SSH connectivity to VMs created in the local or peered virtual networks.

### Azure Application Gateway

Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications. It operates at OSI model layer-7 and is application aware and can make intelligent routing decisions based on different requirements. It is a regional service. Its comes with WAF feature.

### Azure Front Door

Azure Front Door is a global, scalable entry-point that uses the Microsoft global edge network to create fast, secure, and widely scalable web applications. With Front Door, you can transform your global consumer and enterprise applications into robust, high-performing personalized modern applications with contents that reach a global audience through Azure.

### Antivirus

Crowd strike is considered as the endpoint security solution on Cloud. ATP delivers preventative protection, post-breach detection, automated investigation, and response. Design and implementation will be taken care by the Security team as a parallel project.

### Vulnerability Management

**Nessus Pro** is the solution considered on cloud to manage vulnerabilities and reduce risk. Nessus allows you to scan Azure cloud environments and assets. Features include vulnerability detection, compliance misconfiguration detection, and malware detection. Design and implementation will be taken care by the Security team as a parallel project.

### SIEM

**SIEM** ensures constant threat monitoring of Azure. In addition to standard benefits, such as analyzing user entitlements and events to look for malicious activity, the platform also supports multiple built-in Microsoft Azure specific use cases. Design and implementation are taken care by the Security team as a parallel project. Mubadala will use **Azure Sentinel** for SIEM integration with On-Premises SIEM solution.

## IDAM

**Active directory** would be extended to cloud for identity and access management solution.

A dedicated virtual data disk for storing the database, logs, and SYSVOL for Active Directory will be created to keep them separate from the Operating System disk and ensured to set the Host Cache preference setting on the data disk to ‘None’. Two VMs as Domain Controllers will be implemented and added to availability zone. No Public IP will be assigned to the DC and all ports on Domain Controllers except those necessary for authentication, authorization and synchronization will be closed.

## Monitoring

**Azure Monitor** is built-in monitoring for Azure resources. It offers out of the box host and guest-level metrics (e.g. CPU and Disk metrics). Diagnostic logs (e.g. Windows event system logs, Linux syslog) can also be captured into a storage account.

## Patch management

Server Patching with Azure Update Management will be used for Azure Servers

# High Level Design Architecture



Figure 2 :WIP Architecture Diagram

**Summary:** The above diagrams shows the High-Level Design for MUBADALA Target Azure environment. It includes Azure IAAS components, Network layout, Connectivity, and other components at a broader level. The same has been elaborated in low level design in multiple sections and detailed diagrams.

Below is the summarized list of components considered in the target architecture

|  |  |  |
| --- | --- | --- |
| Components | Details | Decision |
| Subscription | Prod/Pre-Production Region | UAE North |
| Subscription | DR Region | North/West Europe |
| Network | Virtual Network Model | Hub & spoke |
| Network | Connectivity to On-Premises | Site to Site VPN |
| Network | Connectivity between VNet | VNet Peering |
| Security | Internal Firewall | Azure Firewall |
| Security | Within Subnets | Network Security Group |
| Security | Load Balancer | Application Gateway/WAS |
| Security | SIEM | Azure Sentinel |
| Security | Vulnerability Scanner | Nessus Pro |
| Security | Antivirus | Crowd Strike |
| Storage | Disk | Managed Disk |
| Operations | Patch Management | Azure Native |
| Operations | Backup | Azure Backup |
| IDAM | Domain Services | Active Directory |

Table 3 : Azure HLD

# Management Groups

Management group structures within an Azure Active Directory (Azure AD) tenant support organizational mapping. Consider your management group structure thoroughly as your organization plans its Azure adoption at scale



Figure 3 : Management Hierarchy

|  |  |  |
| --- | --- | --- |
| Components | Production | Pre-Production |
| Management Group Name | **AEN-MG-PRD01** | **AEN-MG-PP01** |
| Management ID | TBD | TBD |

Table 4 : Management Groups

|  |  |
| --- | --- |
| **\*** | **Design Decision**   * Dedicated Management Group for each tenant * Name **AEN-MG-PRD01 for Production** * Name **AEN-MG-PP01 for Pre-Production** |

# Subscription Layout

Azure Subscription, the doorway to the Azure environment for deploying resources and Azure services. It covers the requirements of different LOBs, such as setting up differentiated levels of access and authorization along with a unique subscriber ID, billing location and a set of available resources.

As per the design, we will have two separate azure landing zone for each environment like “Production” & “Pre-Production” and each individual landing zone will have 1 Hub & 4 Spoke subscriptions



Figure 4 : HUB Layout``1``

|  |  |  |
| --- | --- | --- |
| Subscription | Production | Pre-Production |
| Subscription Name | AEN-HUB-PRD01  AEN-SPK-PRD01  AEN-SPK-PRD02  AEN-SPK-PRD03  AEN-SPK-PRD04 | AEN-HUB-PP01  AEN-SPK-PP01  AEN-SPK-PP02  AEN-SPK-PP03  AEN-SPK-PP04 |
| Subscription ID | TBD | TBD |
| Plan | Azure Plan – EA Agreement | Azure Plan – EA Agreement |
| Billing | Monthly | Monthly |
| Coverage Term | Active until cancelled | Active until cancelled |
| PAYG | TBD | TBD |
| Reserved Instance | TBD | TBD |

**Recommendations**

* Assign a minimum number of users as Subscription Owners.
* Use Azure Resource Management RBAC whenever possible to control the amount of access that administrators have, and log what changes are made to the environment

|  |  |
| --- | --- |
| **\*** | **Design Decision**   * There would be dedicated Landing Zones for Prod and Pre-Prod * Every Landing Zone will have 1 Hub Subscription and 4 Spoke Subscription * Onboarding of New Subscription will be based on Application Portfolio * Region – UAE North & West Europe ( DR) |

# Azure Networking

## Network Topology

Hub & Spoke model is commonly used for hybrid cloud architectures and can be simpler to implement and maintain in the long term. The hub is a virtual network that acts as a central location for managing external connectivity, and hosting services used by multiple workloads. The hub coordinates all communications to and from the spokes. IT rules or processes like security can inspect, route, and centrally manage traffic. The spokes are virtual networks that host workloads and connect to the central hub through virtual network peering.

Hub-spoke topologies offer several business benefits:

* A centrally managed connection to your on-premises environment.
* Integration of separate working environments into a central location for shared services.
* Traffic routing through the central hub, so workloads can be managed centrally.

## Virtual Network

A virtual network (VNET) allows Azure services and VMs to communicate directly and securely with each other in the Azure cloud using internal IP addresses. The virtual network represents a traffic isolation and trust boundary: traffic is unrestricted within the virtual network and external (inbound Internet) traffic is controlled by defined endpoint connections. A virtual network can be also connected with on-premises networks.

The below diagram represents multiple Azure Virtual Network in a Hub and Spoke Architecture, On-Premise Connectivity, and VNET Peering.



Figure 5 : Azure HLD

### IP Address Space

Mubadala network team shared the below IP Address space to be used in the building the target Azure landing zone considering the UAE North Primary and North/West Europe as secondary regions.

|  |  |  |  |
| --- | --- | --- | --- |
| Components | PROD | PRE-PROD | DR |
| Address Space | 10.53.0.0/16  10.53.0.0/20 | 10.83.0.0/16 10.83.0.0/20 | 10.53.0.0/16  10.53.128.0/20 |

### HUB Virtual Network

Hub is the central zone that controls and inspects ingress and/or egress traffic between different zones: Internet, on-premises, and the spokes. Hub contains the common service components consumed by the spokes.

|  |  |  |  |
| --- | --- | --- | --- |
| Components | PROD | PRE-PROD | DR |
| Name | AEN-HUB-VNET-PRD01 | AEN-HUB-VNET-PP01 | EUW-HUB-VNET-01 |
| Address space | 10.53.0.0/20 | 10.83.0.0/20 | 10.53.128.0/20 |
| DR Allow gateway transit | Yes | Yes | Yes |
| Allow forwarded traffic | Yes | Yes | Yes |
| Network traffic | UDR will be configured to route all internet and internal traffic via Hub Network | |  |
| DNS server | Custom - Internal Prod DNS Server (DC in Prod) | Custom - Internal DR DNS Server (DC in DR) |  |
| Location | UAE North | UAE North | North/West Europe |
| DDoS protection | Basic | Basic | Basic |

HUB Virtual Network is designed for both UAE North and North/West Europe individually.

Each HUB Virtual Network will host common services like:

* + Gateway Subnet
  + Azure Firewall
  + Azure Bastion
  + Load Balancers
  + Active Directory
  + Vulnerability Scanning Connectivity
  + Azure Backup
  + Azure Monitor
  + CA Servers
  + Other Common Services

|  |  |  |
| --- | --- | --- |
| VNet Name | CIDR Block | Address Space |
| AEN-HUB-VNET-PRD01 | 10.53.0.0/20 |  |
| AEN-SPK-VNET-PRD01 | 10.53.16.0/20 |  |
| AEN-SPK-VNET-PRD02 | 10.53.32.0/20 |  |
| AEN-SPK-VNET-PRD03 | 10.53.48.0/20 |  |
| AEN-SPK-VNET-PRD04 | 10.53.64.0/20 |  |

Table 5: Production VNet

|  |  |  |
| --- | --- | --- |
| VNet Name | CIDR Block | Address Space |
| EUW-HUB-VNET-DR01 | 10.53.128.0/20 |  |
| EUW-SPK-VNET-DR01 | 10.53.144.0/20 |  |
| EUW-SPK-VNET-DR02 | 10.53.160.0/20 |  |
| EUW-SPK-VNET-DR03 | 10.53.186.0/20 |  |
| EUW-SPK-VNET-DR04 | 10.53.128.0/20 |  |

Table 6 : DR VNet

|  |  |  |
| --- | --- | --- |
| VNet Name | CIDR Block | Address Space |
| AEN-HUB-VNET-PP01 | 10.83.0.0/20 |  |
| AEN-SPK-VNET-PP01 | 10.83.16.0/20 |  |
| AEN-SPK-VNET-PP02 | 10.83.32.0/20 |  |
| AEN-SPK-VNET-PP03 | 10.83.48.0/20 |  |
| AEN-SPK-VNET-PP04 | 10.83.64.0/20 |  |

Table 7 : Pre-Production VNet

|  |  |
| --- | --- |
| **\*** | **Design Decision**   * All the common shared services will host in the HUB VNet, Example: AD, SIEM etc., * Production & Pre-Production environments will have separate landing zone. |

### SPOKE Virtual Network

The role of spoke is to host different types of workloads and to provide a modular approach for further deployments (for example: Business acquisitions)

|  |  |  |  |
| --- | --- | --- | --- |
| Components | PROD | DR | Pre-Prod |
| Name | AEN-SPK-VNET-PRD01  AEN-SPK-VNET-PRD02  AEN-SPK-VNET-PRD03  AEN-SPK-VNET-PRD04 | EUW-SPK-VNET-01  EUW-SPK-VNET-02  EUW-SPK-VNET-03  EUW-SPK-VNET-04 | AEN-SPK-VNET-PP01  AEN-SPK-VNET-PP02  AEN-SPK-VNET-PP03  AEN-SPK-VNET-PP04 |
| Address space | 10.53.16.0/20  10.53.32.0/20  10.53.48.0/20  10.53.64.0/20 | 10.53.128.0/20  10.53.144.0/20  10.53.160.0/20  10.53.186.0/20 | 10.83.16.0/20  10.83.32.0/20  10.83.48.0/20  10.83.64.0/20 |
| Allow remote gateway | Yes | Yes | Yes |
| Network traffic | UDR will be configured to route all internet and internal traffic via Hub Network | |  |
| DNS server | Custom - Internal Prod DNS Server (DC in Prod) | Custom - Internal DR DNS Server (DC in DR) |  |
| Location | UAE North | North Europe |  |
| DDoS protection | Basic | Basic |  |

4 Spoke Virtual Network for each region UAE North and North/West Europe) hosting business applications Workload on each Spoke Virtual Network environment will be divided into

|  |  |
| --- | --- |
| **\*** | **Design Decision**   * Spoke Virtual Networks segregated further into different environments based on Application portfolio * **4 Spoke VNETs will be deployed per environment like EDM, FIN, CORP etc.,** |

### VNet Peering

Virtual network peering enables you to seamlessly connect two Azure [virtual networks](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview). Once peered, the virtual networks appear as one, for connectivity purposes. The traffic between virtual machines in the peered virtual networks is routed through the Microsoft backbone infrastructure, much like traffic is routed between virtual machines in the same virtual network, through *private* IP addresses only

#### Production VNet Peering

|  |  |
| --- | --- |
| VNET Peering | Name |
| AEN-HUB-PER-SPK01  AEN-SPK01-PER-HUB | HUB to SPOKE 1 |
| AEN-HUB-PER-SPK02  AEN-SPK02-PER-HUB | HUB to SPOKE 2 |
| AEN-HUB-PER-SPK03  AEN-SPK03-PER-HUB | HUB to SPOKE 3 |
| AEN-HUB-PER-SPK04  AEN-SPK04-PER-HUB | HUB to SPOKE 4 |

Table 8 : Production Peering

#### Pre-Production VNet Peering

|  |  |
| --- | --- |
| VNET Peering | Name |
| AEN-HUB-PER-SPK01  AEN-SPK01-PER-HUB | HUB to SPOKE 1 |
| AEN-HUB-PER-SPK02  AEN-SPK02-PER-HUB | HUB to SPOKE 2 |
| AEN-HUB-PER-SPK03  AEN-SPK03-PER-HUB | HUB to SPOKE 3 |
| AEN-HUB-PER-SPK04  AEN-SPK04-PER-HUB | HUB to SPOKE 4 |

Table 9 : Pre-Production Peering

**Recommendation:**

* The peered virtual networks must have non-overlapping IP address spaces.
* Address ranges cannot be added to or deleted from the address space of a virtual network once a virtual network is peered with another virtual network. If you need to add address ranges to the address space of a peered virtual network, you must remove the peering, add the address space, and then add the peering again.
* Virtual network peering is between two virtual networks. There is no derived transitive relationship across peering. For example, if ‘Virtual Network A’ is peered with ‘Virtual Network B’, and ‘Virtual Network B’ is peered with ‘Virtual Network C’, ‘Virtual Network A’ is not peered to ‘Virtual Network C’.
* Though the communication between virtual machines in peered virtual networks has no additional bandwidth restrictions, there is a maximum network bandwidth depending on the virtual machine size that still applies.
* VNet can be across subscriptions that use the same Azure AD tenant.

|  |  |
| --- | --- |
| **\*** | **Design Decision**   * All spoke subscription VNet will be peered with HUB NET * All the spoke VNets will be isolated, will not communicated with each other * Virtual Network Peering between regions for DR replication |

## Azure Subnets

A subnet is a child resource of a VNet and helps define segments of address spaces within a CIDR block, using IP address prefixes.

* Azure reserves 5 private IP addresses from each subnet that cannot be used: the first and last addresses of the address space (for the subnet address, and multicast) and 3 addresses to be used internally (for DHCP and DNS purposes).
* Azure resources deployed in a virtual network can communicate with each other using private IP addresses, even if the resources are deployed in different subnets within same virtual network.
* Multiple Subnets are used to isolate different layer of workloads and to implement DMZ infrastructure on Azure, below is the Subnet Segregation with respective workloads.

|  |  |  |  |
| --- | --- | --- | --- |
| **SUBNET** | **CIDR Block** | **IP Range** | **Usable IP** |
| GatewaySubnet | 10.53.0.0/26 | 10.53.0.1-62 | 62 |
| AzureFirewallSubnet | 10.53.0.64/26 | 10.53.0.65-126 | 62 |
| AzureBastionSubnet | 10.53.0.128/26 | 10.53.0.129-190 | 62 |
| AEN-SNET-INF-SHR-PRD01 | 10.53.2.0/25 | 10.53.2.1-126 | 126 |
| AEN-SNET-INF-SEC-PRD01 | 10.53.1.0/26 | 10.53.1.1-62 | 62 |
| AEN-SNET-INF-ALB-PRD01 | 10.53.3.0/24 | 10.53.3.1-254 | 254 |
| AEN-SNET-EDM-PRD01 | 10.53.16.0/24 | 10.53.16.1-254 | 254 |
| AEN-SNET-EDM-PRD02 | 10.53.17.0/24 | 10.53.17.1-254 | 254 |
| AEN-SNET-EDM-PRD03 | 10.53.18.0/24 | 10.53.18.1-254 | 254 |
| AEN-SNET-FIN-PRD01 |  |  |  |
| AEN-SNET-FIN-PRD02 |  |  |  |
| AEN-SNET-FIN-PRD03 |  |  |  |

Table 10 : Prod-Subnets

|  |  |  |  |
| --- | --- | --- | --- |
| **SUBNET** | **CIDR Block** | **IP Range** | **Usable IP** |
| GatewaySubnet | 10.83.0.0/26 | 10.83.0.1-62 | 62 |
| AzureFirewallSubnet | 10.83.0.64/26 | 10.83.0.65-126 | 62 |
| AzureBastionSubnet | 10.83.0.128/26 | 10.83.0.129-190 | 62 |
| AEN-SNET-INF-SHR-PP01 | 10.83.2.0/25 | 10.83.2.1-126 | 126 |
| AEN-SNET-INF-SEC-PP01 | 10.83.1.0/26 | 10.83.1.1-62 | 126 |
| AEN-SNET-INF-ALB-PP01 | 10.83.2.128/25 | 10.83.2.129-254 |  |
| AEN-SNET-EDM-STG-PP01 | 10.83.16.0/24 | 10.83.16.1-254 | 254 |
| AEN-SNET-EDM-UAT-PP01 | 10.83.17.0/24 | 10.83.17.1-254 | 254 |
| AEN-SNET-EDM-DEV-PP01 | 10.83.18.0/24 | 10.83.18.1-254 | 254 |
| AEN-SNET-FIN-STG-PP01 | 10.83.32.0/24 | 10.83.32.1-254 | 254 |
| AEN-SNET-FIN-UAT-PP01 | 10.83.33.0/24 | 10.83.33.1-254 | 254 |
| AEN-SNET-FIN-DEV-PP01 | 10.83.34.0/24 | 10.83.34.1-254 | 254 |
| AEN-SNET-CRP-STG-PP01 | 10.83.48.0/24 | 10.83.48.1-254 | 254 |
| AEN-SNET-CRP-UAT-PP01 | 10.83.49.0/24 | 10.83.49.1-254 | 254 |
| AEN-SNET-CRP-DEV-PP01 | 10.83.50.0/24 | 10.83.50.1-254 | 254 |

Table 11 : Pre-Prod Subnet

|  |  |
| --- | --- |
| **\*** | **Design Decision**   * HUB will host Subnets for Gateway, Firewall, Bastion, Security & Infra Common Services subnets * Production Spoke will have subnets per application like EDM, Fin & Corp * Pre-Production Spoke will have 3 subnets ( Staging, UAT & Dev ) per application as above |

## User Defined Routing ( UDR )

We create custom, or user-defined(static), routes in Azure to override Azure's default system routes, or to add additional routes to a subnet's route table. In Azure, you create a route table, then associate the route table to zero or more virtual network subnets. Each subnet can have zero or one route table associated to it.

UDR’s Assigned at Subnet level

|  |  |  |
| --- | --- | --- |
| **UDR name** | **Subnet Assigned** | **Subscription** |
| AEN-HUB-UDR-GTW | GatewaySubnet | AEN-HUB-PRD01 |
| AEN-HUB-UDR-SEC | AEN-SNET-INF-SHR-PRD01 | AEN-HUB-PRD01 |
| AEN-HUB-UDR-SHR | AEN-SNET-INF-SEC-PRD01 | AEN-HUB-PRD01 |
| AEN-HUB-UDR-ALB | AEN-SNET-INF-ALB-PRD01 | AEN-HUB-PRD01 |
| AEN-HUB-UDR-EDM-PRD | AEN-SNET-EDM-PRD01 | AEN-SPK-PRD01 |
|  |  |  |
|  |  |  |

Table 12: Prod UDR

|  |  |  |
| --- | --- | --- |
| **UDR name** | **Subnet Assigned** | **Subscription** |
| AEN-HUB-UDR-GTW | GatewaySubnet | AEN-HUB-PP01 |
| AEN-HUB-UDR-SEC | AEN-SNET-INF-SEC-PP01 | AEN-HUB-PP01 |
| AEN-HUB-UDR-SHR | AEN-SNET-INF-SHR-PP01 | AEN-HUB-PP01 |
| AEN-HUB-UDR-EDM-STG | AEN-SNET-EDM-STG-PP01 | AEN-SPK-PP01 |
| AEN-HUB-UDR-EDM-UAT | AEN-SNET-EDM-UAT-PP01 | AEN-SPK-PP01 |
| AEN-HUB-UDR-EDM-DEV | AEN-SNET-EDM-DEV-PP01 | AEN-SPK-PP01 |

Table 13: Pre-Production UDR

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Address prefix | Next hop type | Next hop IP |
| AEN-HUB-UDR-GTW |  |  |  |
| AEN-HUB-UDR-SHR |  |  |  |
| AEN-HUB-UDR-SEC |  |  |  |
| AEN-SPK-UDR-EDM-PRD01 |  |  |  |

Table 14 : Prod UDR Rules

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Address prefix | Next hop type | Next hop IP |
| AEN-HUB-UDR-GTW |  |  |  |
| AEN-HUB-UDR-SHR |  |  |  |
| AEN-HUB-UDR-SEC |  |  |  |
| AEN-SPK-UDR-EDM-STG |  |  |  |
| AEN-SPK-UDR-EDM-UAT |  |  |  |
| AEN-SPK-UDR-EDM-DEV |  |  |  |

Table 15: Pre-Prod UDR Rules

## Site to Site VPN

A Site-to-Site VPN gateway connection is used to connect your on-premises network to an Azure virtual network over an IPsec/IKE (IKEv1 or IKEv2) VPN tunnel. Site-to-site VPN can provide better continuity for your workloads in hybrid cloud setup with AZURE.



Figure 6 : S2S VPN

The table below summarizes the S2S VPN configuration

|  |  |
| --- | --- |
| Site to Site VPN | |
| VPN Connection |  |
| Shared Key |  |
| IKE Protocol | IKEv2 |
| Virtual network gateway |  |
| VNG PIP: |  |
| Local network gateway |  |
| LNG PIP (On-prem Public Facing) |  |
| VPN Type | Route based |
| Resource group |  |
| Virtual Network |  |

Table 16 :S2S VPN Parameters Production

|  |  |
| --- | --- |
| Site to Site VPN | |
| VPN Connection – IDC1 | AEN-VPN-IDC01 |
| VPN Connection – Symantec WSS | AEN-VPN-WSS-AUH |
| PS Key – IDC1 | **kHcuhqL`z@pdXi5#** |
| PS Key – Symantec WSS | **aqceDXW@KwSTuA** |
| IKE Protocol | IKEv2 |
| Virtual Network Gateway | AEN-VPN-GTW-SN01 |
| VNG PIP: | AEN-VPN-GTW-IP01 - 20.203.120.92 |
| Local Network Gateway | AEN-VPN-LGW-SN01 – IDC1 |
|  | AEN-VPN-LGW-SN02 – Symantec WSS |
| LNG Public IP – IDC1 | 94.56.95.86 |
| LNG Public IP – Symantec WSS | 168.149.175.164 |
| VPN Type | Route-Based |
| Resource group | AEN-HUB-PP-INF-RG01 |
| Virtual Network | AEN-HUB-PP01 - 10.83.0.0/20 |

Table 17 : S2S VPN Parameters for Pre-Production

* A VPN Gateway must have a gateway subnet with a /26 CIDR
* Virtual Network Gateway subnet will be named as “Gateway Subnet”
* Limited to use pre-shared keys (PSK) for authentication

|  |  |
| --- | --- |
| **\*** | **Design Decision**   * IDC1 & IDC2 would be connected to Azure over S2S VPN Tunnel for Production * IDC1 would be connected to Azure over S2S VPN Tunnel for Pre-Production * Additional 4 VPN tunnels for Branch Offices * Identical setup will be created for DR Region * Bandwidth 1 GBPS (Gateway Type VPNGW2) |

# Security

Below are the security components considered in the Target environment.

## Azure Firewall

Azure Firewall is a cloud native network security service. It offers fully stateful network and application-level traffic filtering for VNet resources, with built-in high availability and cloud scalability delivered as a service. You can protect your VNets by filtering outbound, inbound, spoke-to-spoke, and VPN traffic.

Diagram

Description automatically generated

Figure 7 : Azure Firewall

|  |  |
| --- | --- |
| Component | Decision |
| Internal Firewall | Azure Firewall |
| Internal Security | NSG |
| On-Prem Firewall | Cisco Firepower & Fortinet (On-Prem devices) |
| Load Balancer | Application Gateway/Azure WAF |
| SIEM | SIEMs - Sentinel |
| Antivirus | Crowdstrike |

Table 18 : Azure Firewall

|  |  |
| --- | --- |
| Feature ​ | Azure Firewall​ |
| Application FQDN filtering rules | Yes​ |
| Threat intelligence | Yes |
| Custom DNS | Yes |
| Outbound SNAT support | Yes |
| Inbound DNAT support | Yes |
| Built-in HA | Yes |
| Web categories | Yes |
| Azure Monitor logging | Yes |
| Network traffic filtering rules | Yes |
| Forced tunnelling | Yes |
| Availability Zones | Yes |
| FQDN in network rules​ | Yes |

Table 19: Azure Firewall Parameters

Traffic from On-premises to Azure will pass through Azure firewall. Hub and spoke VNet will be configured with UDR so that traffic from both the VNet is restricted to go via Azure Firewall in Hub VNet.

The table below summarizes the Azure Firewall configuration:

|  |  |
| --- | --- |
| Azure Firewall | |
| Azure Firewall name | AEN-FRW-01 |
| Firewall public IP | AEN-FRW-PIP01 |
| Firewall private IP | 10.53.x.x |
| Resource group | AEN-HUB-INF-RG01 |
| Location | UAE North |
| Firewall subnet | AzureFirewallSubnet |
| Virtual Network | AEN-HUB-PRD01 |
| Firewall Policy Name | AEN-HUB-FRW-PLC01 |

Table 20 : Azure Firewall Parameters - Production

|  |  |
| --- | --- |
| Azure Firewall | |
| Azure Firewall name | AEN-FRW-PP01 |
| Firewall public IP | AEN-FWR-PP-IP01 |
| Firewall private IP | 10.83.0.68 |
| Resource group | AEN-HUB-PP-INF-RG01 |
| Location | UAE North |
| Firewall subnet | AzureFirewallSubnet |
| Virtual Network | AEN-HUB-VNET-PP01 |
| Firewall Policy Name | AEN-HUB-FRW-PLC01 |

Table 21 : Azure Firewall Parameters - Pre-Production

## Azure Bastion

Azure Bastion is a service you deploy that lets you connect to a virtual machine using your browser and the Azure portal. The Azure Bastion service is a fully platform-managed PaaS service that you provision inside your virtual network. It provides secure and seamless RDP/SSH connectivity to your virtual machines directly from the Azure portal over TLS. When you connect via Azure Bastion, your virtual machines do not need a public IP address, agent, or special client software.

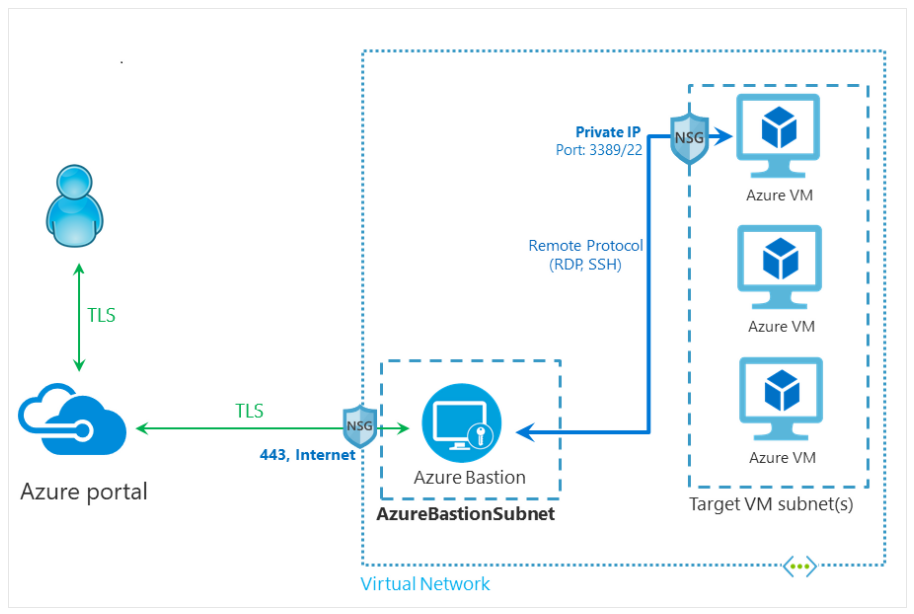


Figure 8 : Azure Bastion

|  |  |
| --- | --- |
| Azure Bastion | |
| Azure Bastion name | AEN-HUB-BASTION-01 |
| Bastion public IP | AEN-HUB-BST-PIP01 – 20.x.x.x |
| Public IP address SKU | Standard |
| Resource group | AEN-HUB-INF-RG01 |
| Location | UAE North |
| Firewall subnet | AzureBastionSubnet |
| Virtual Network | AEN-HUB-VNET-PRD01 |

Table 22: Azure Bastion Production

|  |  |
| --- | --- |
| Azure Bastion | |
| Azure Bastion name | AEN-HUB-BASTION-PP01 |
| Bastion public IP | AEN-HUB-BST-IP01 - 20.74.246.203 |
| Public IP address SKU | Standard |
| Resource group | AEN-HUB-PP-INF-RG01 |
| Location | UAE North |
| Firewall subnet | AzureBastionSubnet |
| Virtual Network | AEN-HUB-VNET-PP01 |

Table 23 : Azure Bastion Pre-Production

## Network security groups

Azure network security groups can be used to filter network traffic to and from Azure resources in an Azure virtual network. A network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several typesexpress of Azure resources. For each rule, we can specify source and destination, port, and protocol.

Azure network security groups can be associated to a subnet or to a network interface of a VM. To avoid unexpected communication problems, it is recommended to attach NSG to a subnet, or a network interface, but not both.

NSG rule consists of the following components:

* Name – A unique name which should be easy for administrators to use to find the rule.
* Priority – This is an integer between 100 and 4096, which should be unique. This value defines the processing order of the rule, with rules containing lower values (higher priority) being executed first.
* Source or destination – This field indicates which application or user(s) the rule is applicable for. This can be an IP Address, IP Address range or Azure resource.
* Protocol – The TCP, UDP or ICMP protocol which will be analyzed.
* Direction – This indicates whether the traffic is inbound or outbound.
* Port Range – This will specify which port or range of ports the rule is applicable for.
* Action – Setting either Allow (the traffic through) or Deny (and block the traffic) will specify the action to be taken by the NSG when network traffic matching the rule is identified.

Microsoft Azure automatically creates a few default rules in each Network Security Group.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Inbound | Priority | Source | Source Ports | Destination | Destination Ports | Protocols | Access |
| [AllowVNetInBound](https://docs.microsoft.com/en-us/azure/virtual-network/security-overview) | 65000 | VirtualNetwork | 0-65535 | VirtualNetwork | 0-65535 | All | Allow |
| [AllowAzureLoad BalancerInBound](https://docs.microsoft.com/en-us/azure/virtual-network/security-overview) | 65001 | AzureLoad Balancer | 0-65535 | 0.0.0.0/0 | 0-65535 | All | Allow |
| [DenyAllInbound](https://docs.microsoft.com/en-us/azure/virtual-network/security-overview) | 65500 | 0.0.0.0/0 | 0-65535 | 0.0.0.0/0 | 0-65535 | All | Deny |
|  |  |  |  |  |  |  |  |

Table 24 : NSG Inbound

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Outbound | Priority | Source | Source Ports | Destination | Destination Ports | Protocols | Access |
| [AllowVnetOutBound](https://docs.microsoft.com/en-us/azure/virtual-network/security-overview) | 65000 | VirtualNetwork | 0-65535 | VirtualNetwork | 0-65535 | All | Allow |
| [AllowInternet OutBound](https://docs.microsoft.com/en-us/azure/virtual-network/security-overview) | 65001 | 0.0.0.0/0 | 0-65535 | Internet | 0-65535 | All | Allow |
| [DenyAllOutBound](https://docs.microsoft.com/en-us/azure/virtual-network/security-overview) | 65500 | 0.0.0.0/0 | 0-65535 | 0.0.0.0/0 | 0-65535 | All | Deny |

Table 25 : NSG Outbound

In MUBADALA NSGs will be configured at subnet level. As a best practice for network security rules, it is to start by denying all traffic, and then creating rules only for traffic which is known to be safe.

**NSG names below:**

|  |  |  |
| --- | --- | --- |
| **NGS name** | **Subnet Assigned** | **Subscription** |
| AEN-HUB-NSG-SEC-PRD01 | AEN-SNET-INF-SEC-PRD01 | AEN-HUB-PRD01 |
| AEN-HUB-NSG-SHR-PRD01 | AEN-SNET-INF-SHR-PRD01 | AEN-HUB-PRD01 |
| AEN-HUB-NSG-EDM-PRD01 | AEN-SNET-EDM-STG-PRD01 | AEN-SPK-PRD01 |

Table 26 : NSG Production

|  |  |  |
| --- | --- | --- |
| **NGS name** | **Subnet Assigned** | **Subscription** |
| AEN-HUB-NSG-SEC | AEN-SNET-INF-SEC-PP01 | AEN-HUB-PP01 |
| AEN-HUB-NSG-SHR | AEN-SNET-INF-SHR-PP01 | AEN-HUB-PP01 |
| AEN-HUB-NSG-EDM-STG | AEN-SNET-EDM-STG-PP01 | AEN-SPK-PP01 |
| AEN-HUB-NSG-EDM-UAT | AEN-SNET-EDM-UAT-PP01 | AEN-SPK-PP01 |
| AEN-HUB-NSG-EDM-DEV | AEN-SNET-EDM-DEV-PP01 | AEN-SPK-PP01 |

Table 27: NSG Pre-Production

## SIEM

Azure Sentinel is the proposed SIEM solution on Cloud. It combines log management, UEBA and security incident response into a complete, end-to-end security operations platform. Security team will implement the same in the target Cloud environment.

## Anti-Virus

Crowdstrike is a unified endpoint security platform for preventative protection, post-breach detection, automated investigation, and response.

In MUBADALA, based on the current security solutions, policies will be applied to carry on Deep scans and Quick scans as and when required. Also, ATP provides an option to create custom policies along with built in policies. ATP is deployed by security team for the complete infrastructure.

## Multifactor authentication

Azure Multi-Factor Authentication is an easy to use, scalable, and reliable solution that provides a second method of authentication to protect your users.

* Easy to Use - Azure Multi-Factor Authentication is simple to set up and use. The extra protection that comes with Azure Multi-Factor Authentication allows users to manage their own devices. Best of all, in many instances it can be set up with just a few simple clicks.
* Scalable - Azure Multi-Factor Authentication uses the power of the cloud and integrates with your on-premises AD and custom apps. This protection is even extended to your high-volume, mission-critical scenarios.
* Always Protected - Azure Multi-Factor Authentication provides strong authentication using the highest industry standards.
* Reliable - Microsoft guarantees 99.9% availability of Azure Multi-Factor Authentication. The service is considered unavailable when it is unable to receive or process verification requests for the two-step verification

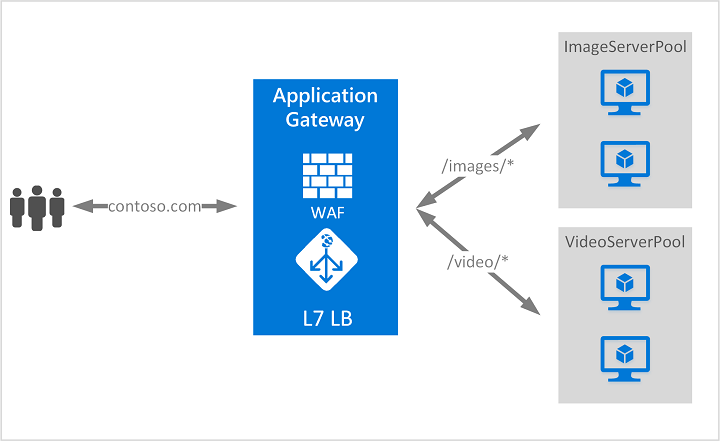
**Recommendation:**

* LTI Recommends Single Azure Directory tenant, as subscription will only trust one directory
* To configure Conditional Access and have Control over Identity Access and Security enforce multi-factor authentication (MFA) for users

|  |  |
| --- | --- |
| **\*** | **Design Decision**   * To use single AD tenant and link it to Hub & Spoke Subscription * To Enforce, SSO, Two Factor Authentication or MFA |

## Azure Application Gateway

Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications. It operates at OSI model layer-7 and is application aware and can make intelligent routing decisions based on different requirements. It is a regional service. Its comes with WAF feature.



|  |  |
| --- | --- |
| **\*** | **Design Decision**   * For Public (HTTP/HTTPS) endpoint to be published at the regional revel we will use application gateway. * In future for global load balancing Azure Front door will be used in front of azure load balancer. |

# Azure Storage

Azure Storage is the cloud storage solution for modern applications that rely on durability, availability, and scalability. Azure Storage is massively scalable, so you can store and process hundreds of terabytes of data to support the big data scenarios required by scientific, financial analysis, and media applications

* **Standard Storage** performance tier which allows you to store Tables, Queues, Files, Blobs and Azure virtual machine disks. This tier is hosted on Hard Disk Drives (HDD)
* **Premium Storage** performance tier which currently only supports Azure virtual machine disks. This tier is hosted on Solid State Drives (SSD).
* **Archive Storage:** It is optimized for storing data that is rarely accessed and stored for at least 180 days with flexible latency requirements (on the order of hours).

## Disk Types

A Microsoft Azure virtual machine is created from an image or a disk. All virtual machines use one operating system disk, a temporary local disk, and they enable the use of multiple data disks depending on the selected size of the virtual machine. All images and disks, except the temporary local disk, are created from virtual hard disk (VHD) files that are stored as page blobs in a storage account in Microsoft Azure.

Following are the different type of disks attached to VMs:

* **Operating system disks:** The default operating system disk that is used in the virtual machine. This disk is durable, but it has Write-behind disk caching enabled.
* **Data disks:** Additional durable disks that have Write-behind disk caching disabled
* **Temporary disks:** The contents are wiped away during reboot. This disk is intended for paging files, so that paging files don’t count against the storage quota.

|  |  |
| --- | --- |
| **\*** | **Design Decision**   * **All the machine critical disks will on Premium SSD and rest all will be Standard SSD** * 128 GB of OS Disk for New virtual machines * Additional Data Disk will be a combination Standard SSD and Premium SSD as per Application/Server requirements |

## Disk Model

There are two type of Disk model available Managed Disk and Un Managed Disk

**Managed Disk -** Azure Managed Disks simplifies disk management for Azure IaaS VMs by managing the storage accounts associated with the VM disks.

* No Storage Account Management overhead
* Disk snapshots
* Predictable performance with no throttling
* Integration with Availability Sets
* Disk level RBAC permission
* No Custom Size
* Pay for complete disk size

**Un-Managed Disk -** Unmanaged disks are the traditional type of disks that have been used by VMs, and additionally we should manage storage accounts associated with disks.

* Pay what you use
* LRS, GRS supported.

Listed below is the disk comparison available in Azure & what is recommended for MUBADALA.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Feature | Ultra Disk | Premium SSD | Standard SSD | Standard HDD |
| Disk type | SSD | SSD | SSD | HDD |
| Scenario | IO-intensive workloads | Production and performance sensitive workloads | Web servers, lightly used enterprise applications and dev/test | Backup, non-critical, infrequent access |
| Example | Transaction heavy SQL, Oracle DB | DB Servers | Prod App / DB Servers | Dev / Test Workloads |
| Max throughput | 2,000 MB/s | 900 MB/s | 750 MB/s | 500 MB/s |
| Max IOPS | 160,000 | 20,000 | 6,000 | 2,000 |

|  |  |
| --- | --- |
| **\*** | **Design Decision**   * All the disk used will be Managed Disk * Prod Server should use Standard SSD by default * DB Servers will leverage Premium SSD as per the requirement |

# Azure Compute

Azure provides Virtual Machines types based on storage, memory, Network, Graphics and CPU capacity.

Below table defines the different type of VM along with the purpose relevant to MUBADALA environment

|  |  |  |  |
| --- | --- | --- | --- |
| Series | Purpose | Use Case | Environment |
| A Series | Entry-level economical VMs for dev/test | Development and test Servers | Dev / SIT / Test |
| D Series | General purpose | Enterprise grade application & relational DB | UAT / PROD |
| F Series | Compute optimized | Batch processing & Web Servers | UAT / PROD |
| G Series | Memory and storage optimized | Large SQL DB | PROD |
| M Series | Memory optimized | SAP& SQL Servers | PROD |

|  |  |
| --- | --- |
| **\*** | **Design Decision**   * AHUB benefit will be applied while deploying VMs to leverage existing licenses * To Provision the services azure hardened images (Golden Images) * Extensions for Domain Join & Temp drive will be integrated in the ARM Template * VM Series will be limited to D & F Series so it would be easier to manage Reserved Instance * PAY AS You Go Model for domains hybrid license model * All the required agents will be launched from azure golden images. |

# VA Scanner Solution

# Cofense Solution

# (WIP )

## Disaster recovery

Azure Site Recovery service contributes to your business continuity and disaster recovery (BCDR) strategy by keeping your business apps up and running available during planned and unplanned outages.

Figure 17.2 -ASR - Replication

**Summary:** Above diagram represent the failover process of Azure Site Recovery between two Azure Region.

**Design Principles**

* LTI recommends using Azure Site Recovery for Azure IAAS VMs considering WEST EUROPE as DR region.
* LTI recommends enabling native replication for critical applications such as Active Directory, SQL Always on for SQL Servers and DFS for File Servers
* IaaS Virtual Machines will be replicated to secondary region using three simple steps:
  + Create Recovery Vault
  + Enable Replication
  + Failover/Fail-Back

|  |  |
| --- | --- |
| **\*** | **Design Decision**   * TBD. |

# BAU Operation

## Azure Monitoring

Azure Monitor is an important tool to help you in this process. It enables you to gather monitoring and diagnostic information about the health of your services. You can use this information to visualize and analyze the causes of problems that might occur in your app.

Logging and monitoring the health of your services is a vital component of production applications. Azure Administrators determine the causes of failures and try to identify any problems before they occur.

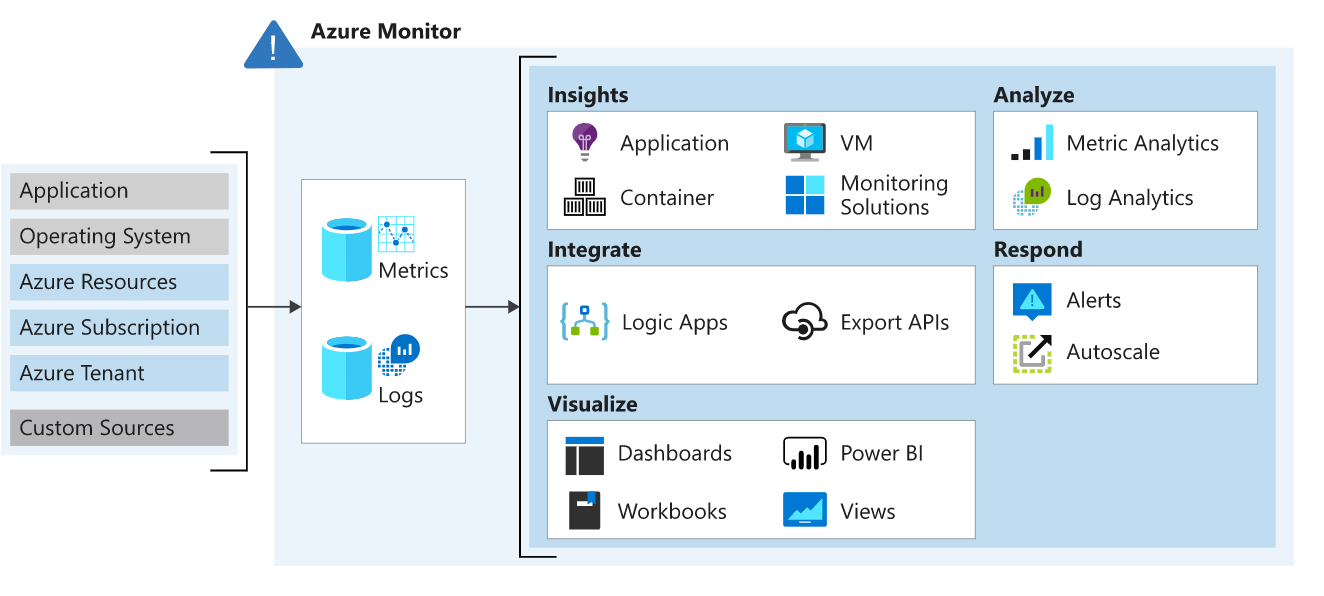


Figure 18.1 – Azure Monitor

Below is the sample of metrics that will be configured for the workloads

|  |  |
| --- | --- |
| Configuration | Values |
| Metric | Percentage CPU |
| Condition Type | Static |
| Period | Over the last 5 Mins |
| Frequency | 5 Min |
| Operator | Greater than |
| Threshold | 85 |

**Recommendations:**

* LTI Recommends:  Enable Diagnostics on virtual machines, particularly if a monitoring agent isn’t being installed.  Boot diagnostics are particularly useful for troubleshooting VM boot issues
* Tracking the availability of the system, storage and Network and its component elements Availability monitoring of resources is closely related to health monitoring
* Monitoring the day-to-day usage of the system and spotting trends that might lead to problems if they're not addressed.
* Tracking issues that occur, from initial report through to analysis of possible causes, rectification, consequent software updates, and deployment

|  |  |
| --- | --- |
| **\*** | **Design Decision**   * Azure Monitor – Log Analytics, Network Performance Monitoring, Service Map and Network watcher will be used for Azure Resources Monitoring |

## Azure Backup

Azure Backup is a cloud-based backup solution. Though cloud-native, it is also possible to use Azure Backup on-premises as well as in the cloud. Azure Backup is simple to configure and use, offering consistent copies with security features and management controls via the Azure portal.

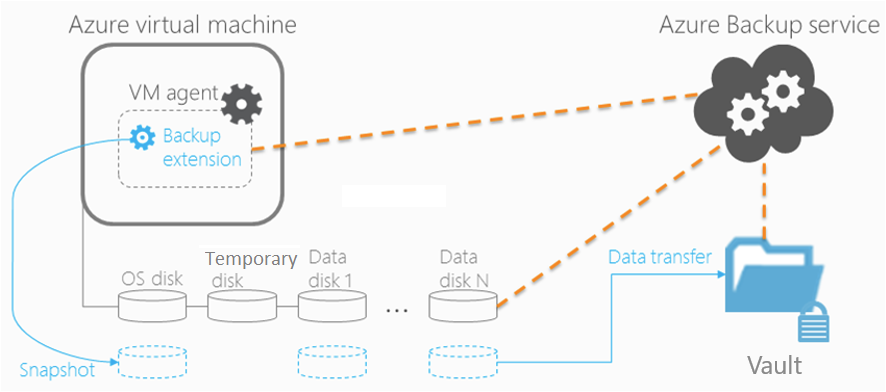


Figure 18.2 – Azure Backup

**Azure Recovery Vault**

**As per the design, we have created the recovery vault per subscription in Prod and Pre-Prod environment**

|  |  |  |
| --- | --- | --- |
| Recovery Vault Name | Region | Subscription |
| AEN-HUB-RSV-PRD01 | **UEA North** | **AEN-HUB-PRD01** |
| AEN-SPK-RSV-PRD01 | **UEA North** | **AEN-SPK-PRD01** |
| AEN-SPK-RSV-PRD02 | **UEA North** | **AEN-SPK-PRD02** |
| AEN-SPK-RSV-PRD03 | **UEA North** | **AEN-SPK-PRD03** |
| AEN-SPK-RSV-PRD04 | **UEA North** | **AEN-SPK-PRD04** |

|  |  |  |
| --- | --- | --- |
| Recovery Vault Name | Region | Subscription |
| AEN-HUB-RSV-PP01 | **UEA North** | **AEN-HUB-PP01** |
| AEN-SPK1-RSV-PP01 | **UEA North** | **AEN-SPK-PP01** |
| AEN-SPK2-RSV-PP01 | **UEA North** | **AEN-SPK-PP02** |
| AEN-SPK3-RSV-PP01 | **UEA North** | **AEN-SPK-PP03** |

**Azure Backup Policies**

|  |  |  |  |
| --- | --- | --- | --- |
| **Resource Backup** | **Type of Backup** | **Default policy** | **Retention** |
| Azure VM Backup | Full and Incremental | Daily at 11:00 PM UTC | Retain backup taken every day at 11:00 PM for 30 Day(s) |
| SQL Server Backup | Full | Daily at 11:00 PM UTC | Retain backup taken every day at 11:00 PM for 30 Day(s) |
| Log | Every 1 hour | Retained for 30 days |
| Simple (recovery model)  Full Backup Log backup is skipped | Daily at 11:00 PM UTC | Retained for 30 days |
| MARS Backup (Files and Folder Backup) | Full and Incremental | Daily at 11:00 PM UTC | Retained for 30 days |
| MARS backup (System state backup) | Full | Daily at 11:00 PM UTC | Retained for 30 days |
| Azure file share | Full and Incremental | Daily at 12:30 PM UTC | Retained for 30 days |

**Note**: Backup policies are changed by the Operations team based on the Cost & business requirement

## Patch Management

Azure Patch Management solution will be leverage for patching Azure workloads

Below is the update schedule for the workloads based on Environment

|  |  |  |
| --- | --- | --- |
| **UPDATE SCHEDULE** | | |
| Type | Day and Time | |
| Production Servers | 4th week of Every Month | Friday 8 PM GMT +1 |
| Pre-Production Servers | 3rd week of Every Month | Friday 8 PM GMT +1 |

# Azure Governance

Governance in Azure is one aspect of Azure Management. Management refers to the tasks and processes required to maintain the business applications and the resources that support them.

## Resource Groups

Resource Group is grouping of resources into meaningful groups for management, billing, or natural affinity. Resources that life cycle together are grouped together into a resource group.

LTI recommends using a Resource Group to all resources which shares common lifecycle or share a similar attribute:

|  |  |
| --- | --- |
| RG Details | Naming Convention |
| HUB Infra RG | AEN-HUB-INF-RG01 |
| Spoke RG | AEN-SPK-EDM-RG01 |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Table 28 : RG for Production

|  |  |
| --- | --- |
| RG Details | Naming Convention |
| HUB Infra RG | AEN-HUB-PP-INF-RG01 |
| Spoke RG | AEN-SPK-EDM-RG01 |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Table 29: RG for Pre-Production

|  |  |
| --- | --- |
| **\*** | * Resource Groups will be provisioned based on resources who shares common lifecycle |

## Resource Tags

Resource Tags are defined as **Key-Value pairs** assigned to resources or resource groups and can be used in scenarios where customer business processes and organizational hierarchy call for a complex collection of resource groups and resources and subscription assets need to be structured per established policies.

|  |  |
| --- | --- |
| Key | Value |
| BuildOwner |  |
| TechOwner |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

|  |  |
| --- | --- |
| **\*** | **Design Decision**   * Resource Tags to be used to facilitate resource categorization for billing or management per ‘Environment’ and ‘Application’. |

## Identity

Azure Active Directory Identity Protection is a feature of the **Azure AD Premium P1 & P2** edition that enables the organization to:

• Detect potential vulnerabilities affecting the organization’s identities.

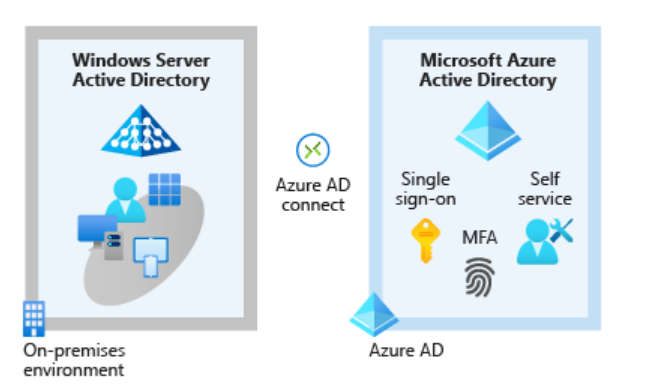
• Configure automated responses to detect suspicious actions that are related to the organization’s identities.

• Investigate suspicious incidents and take appropriate action to resolve them.

While best results are obtained by enrolling all user accounts in Azure AD Identity Protection. MUBADALA to implement Azure AD ID protection for user accounts synced to Azure AD. Since the Azure AD Identity protection is part of Azure AD P1 & P2 license, enabling the ID protection on all users would be beneficial and help detect and prevent vulnerabilities affecting the MUBADALA’s identities.

Azure AD Connect synchronizes user identities between on-premises Active Directory and Azure AD. Azure AD Connect synchronizes changes between both identity systems, so you can use features like SSO, multifactor authentication, and self-service password reset under both systems. Self-service password reset prevents users from using known compromised passwords.

Here's a diagram that shows how Azure AD Connect fits between on-premises Active Directory and Azure AD:



## Conditional Access Control

Conditional Access is a tool that Azure Active Directory uses to allow (or deny) access to resources based on identity signals. These signals include who the user is, where the user is, and what device the user is requesting access from.

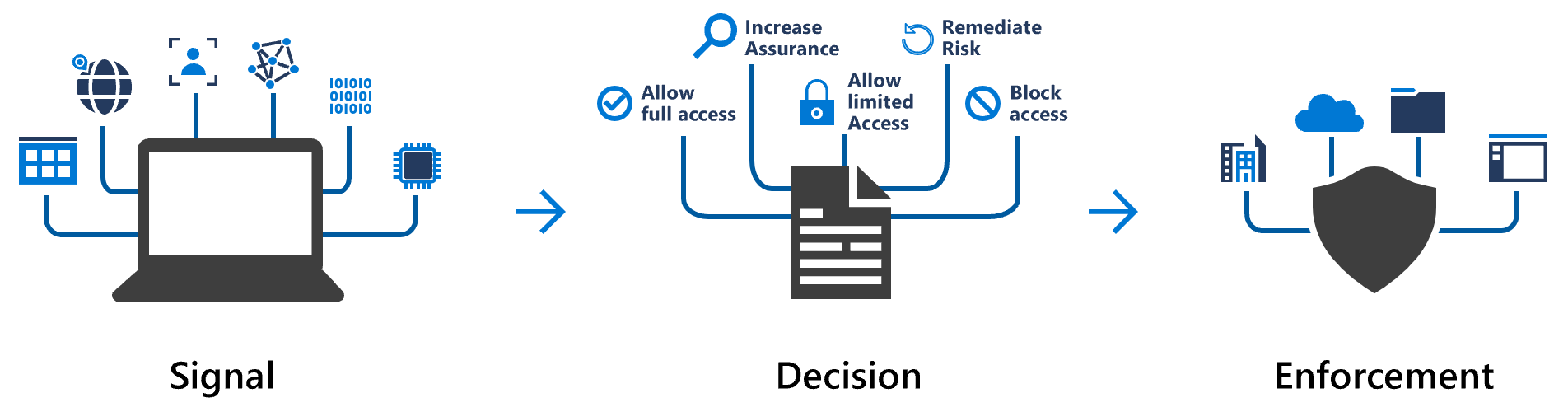
Conditional Access helps:

* Empower users to be productive wherever and whenever.
* Protect the organization's assets.

Conditional Access also provides a more granular multifactor authentication experience for users. For example, a user might not be challenged for second authentication factor if they're at a known location. However, they might be challenged for a second authentication factor if their sign-in signals are unusual or they're at an unexpected location.

During sign-in, Conditional Access collects signals from the user, makes decisions based on those signals, and then enforces that decision by allowing or denying the access request or challenging for a multifactor authentication response.

Here's a diagram that illustrates this flow:



|  |  |
| --- | --- |
| **\*** | **Design Decision**   * Currently Mubadala has two AD tenants subscribed to root Azure subscription * One tenant for production **“micaue.onmicrosoft.com”** * One tenant for Pre-Production **“micpp1.onmicrosoft.com”** * Administrative access will be granted based roles and responsibility |

## Role-based access control

RBAC is a security model to perform access control of resources by users on a more granular level. Users specified in RBAC permissions can access and execute actions on the resources within their scope of work. RBAC allows more users to manage their Azure Services. There are forty-three built-in Azure RBAC role definitions for controlling access to Azure resources

Each role definition has three major components:

* Actions – the permissions that are allowed in a role definition
* Not-Actions – the permissions that are disallowed in a role definition
* Scope – the role definition can be applied at three different scopes
  1. Management Groups
  2. Subscription
  3. Resource Group
  4. At any Azure Resource

LTI recommends using some of the **built in** RBAC role definitions below:

|  |  |
| --- | --- |
| Built in RBAC Roles | Description |
| Owner | The Owner can perform all management operations for a resource and its child resources, including access management or granting access to others. |
| Contributor | The Contributor can perform all management operations for a resource, including creating and deleting resources. A contributor cannot grant access to others. |
| Reader | The Reader has Read-only access to a resource and its child resources. A Reader cannot read secrets. |
| Automation Operator | The Automation Operator lets users start, stop, suspend and resume jobs. |
| Monitoring Contributor Service Role | The Monitoring Contributor Service Role lets users read all monitoring data and update monitoring settings. |
| Monitoring Reader Service Roles | The Monitoring Reader Service Role lets users read all monitoring data. |
| Network Contributor | The Network Contributor lets users manage all network resources, but not manage access to them. |
| Security Manager | The Security Manager lets users manage security components, security policies and virtual machines. |
| SQL DB Contributor | The SQL DB Contributor lets users manage SQL Databases, but not manage access to them. Users also cannot manage security-related policies or parent SQL servers. |
| Storage Account Contributor | The Storage Account Contributor lets users manage storage accounts, but not manage access to them. |
| User Access Administrator | The User Access Administrator lets users manage user access to Azure resources. |
| Virtual Machine Contributor | The Virtual Machine Contributor lets users manage virtual machines but not the VNet or Storage Account to which they are connected. |

More details can be found in below URL:   
<https://docs.microsoft.com/en-us/azure/active-directory/role-based-access-built-in-roles>

In addition to the built in RBAC roles definitions, it is possible to create **custom role** definitions that can be loaded into a subscription and scoped at the entire subscription or a resource group. Custom roles can be used to create new role definitions or the tweaking of existing role definitions.

|  |  |
| --- | --- |
| **\*** | **Design Decision**   * RBAC will be used to restrict access to resources on Azure at granular level. * **Owner, Contributor, Reader will be granted access.** |

## Resource Manager Policies

Azure Resource Manager allows controlling access through custom policies (currently in preview). With policies, it can prevent users in organization from breaking conventions that are needed to manage organization's resources. Policy definitions are created to describe the actions or resources that are specifically denied. It assigns those policy definitions at the desired scope, such as the **subscription, resource group, or an individual resource**

There are a few key differences between policy and role-based access control, but the first thing to understand is that policies and RBAC work together. To be able to use policy, the user must be authenticated through RBAC. Unlike RBAC, policy is a default allow and explicit deny system.

LTI recommends using below Azure RBAC Policies:

|  |  |
| --- | --- |
| Policies | Details |
| Allowed Locations | This policy enables you to restrict the locations your organization can specify when deploying resources. Use to enforce your geo-compliance requirements. |
| Allowed Storage Account SKUs | This policy enables you to specify a set of storage account SKUs that your organization can deploy. |
| Allowed Virtual Machine SKUs | This policy enables you to specify a set of virtual machine SKUs that your organization can deploy. |
| Enforces required tag and its value. | Enforces a required tag and its value. |
| Audit VMs that do not use managed disks | This policy audits VMs that do not use managed disks |
| Audit Windows VMs on which the Log Analytics agent is not connected as expected | This policy audits Windows virtual machines on which the Log Analytics agent is not connected to the specified workspaces. |
| Audit Windows VMs that contain certificates expiring within the specified number of days | This policy audits Windows virtual machines that contain certificates expiring within the specified number of days. |
| Audit Windows VMs on which the DSC configuration is not compliant | This policy audits Windows VMs on which the Desired State Configuration (DSC) configuration is not compliant. This policy is only applicable to machines with WMF 4 and above |
| Audit Windows VMs with a pending reboot | This policy audits Windows virtual machines with a pending reboot. |
| Audit Windows VMs on which the Log Analytics agent is not connected as expected | This initiative deploys the policy requirements and audits Windows virtual machines on which the Log Analytics agent is not connected to the specified workspaces. |
| Enable Azure Monitor for VMs | Enable Azure Monitor for the Virtual Machines (VMs) in the specified scope (Management group, Subscription or resource group). Takes Log Analytics workspace as parameter. |
| Azure Monitor log profile should collect logs for categories 'write,' 'delete,' and 'action' | This policy ensures that a log profile collects logs for categories 'write,' 'delete,' and 'action' |
| Deploy Dependency agent for Windows VMs | Deploy Dependency agent for Windows VMs if the VM Image (OS) is in the list defined and the agent is not installed. The list of OS images will be updated over time as support is updated. |
| Storage Accounts should use a virtual network service endpoint | This policy audits any Storage Account not configured to use a virtual network service endpoint. |
| Network interfaces should not have public Ips | This policy denies the network interfaces which are configured with any public IP. Public IP addresses allow internet resources to communicate inbound to Azure resources, and Azure resources to communicate outbound to the internet. This should be reviewed by the network security team. |
| Network Watcher should be enabled | Network Watcher is a regional service that enables you to monitor and diagnose conditions at a network scenario level in, to, and from Azure. Scenario level monitoring enables you to diagnose problems at an end to end network level view. Network diagnostic and visualization tools available with Network Watcher help you understand, diagnose, and gain insights to your network in Azure. |
| RDP access from the Internet should be blocked | This policy audits any network security rule that allows RDP access from Internet |
| SSH access from the Internet should be blocked | This policy audits any network security rule that allows SSH access from Internet |
| Email notification for high severity alerts should be enabled | Enable emailing security alerts to the security contact, in order to have them receive security alert emails from Microsoft. This ensures that the right people are aware of any potential security issues and are able to mitigate the risks |
| Email notification to subscription owner for high severity alerts should be enabled | Enable emailing security alerts to the subscription owner, in order to have them receive security alert emails from Microsoft. This ensures that they are aware of any potential security issues and can mitigate the risk in a timely fashion |
| MFA should be enabled accounts with write permissions on your subscription | Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with write privileges to prevent a breach of accounts or resources. |
| MFA should be enabled on accounts with owner permissions on your subscription | Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with owner permissions to prevent a breach of accounts or resources. |
| Subnets should be associated with a Network Security Group | Protect your subnet from potential threats by restricting access to it with a Network Security Group (NSG). NSGs contain a list of Access Control List (ACL) rules that allow or deny network traffic to your subnet. |

|  |  |
| --- | --- |
| **\*** | **Design** Decision   * Mubadala will go with default Azure Policies. |

## Azure Resource Locks

Azure Resource Manager provides the ability to restrict operations on resources through resource management locks. Locks are policies which enforce a lock level at a scope. The scope can be a subscription, resource group or resource.

The lock level identifies the type of enforcement for the policy, which presently has two values – **CanNotDelete** and **ReadOnly**. **CanNotDelete** means authorized users can still read and modify resources, but they can't delete any of the restricted resources. **Read-only** means authorized users can only read from the resource, but they can't modify or delete any of the restricted resources. Locks can be applied using ARM templates, ARM REST API, or ARM Azure PowerShell.

|  |  |
| --- | --- |
| **\*** | **Design** Decision   * Resource Locks will be used to highly lock value assets such S2S VPN, Critical Virtual Machines like AD, etc., * Resource Locks will be used to the objects that are mostly static from a configuration perspective. |

# PAAS SERVICE (WIP)

## Azure Data Explorer

Data Factory

Data Lake Storage

Databricks

Azure Purview

Azure Synapse

HD Insight.

# Naming Conventions

Before MUBADALA leaps into any significant Azure adoption, one of many important planning exercises should be adoption of a standardized naming system for services and resources, proper planning and naming guidance surely Validates

* Unnecessary increase on management overhead as the object collection expands over time.
* Consistent naming conventions make resources easier to locate. They can also indicate the role of a resource in a solution.
* This will avoid the chance of any deployments failing due to bad naming.

Region

|  |  |
| --- | --- |
| DC | Character |
| Azure Region UAE Central | AEC |
| Azure Region UAE North | AEN |

## Azure Infra Naming

The below table suggests the naming convention as per our understanding for MUBADALA

|  |  |  |
| --- | --- | --- |
| Resource | Pattern | Example |
| Management Group | Region-Resource-environment | AEN-MG-PRD01  AEN-MG-PPRD01 |
| Subscription | Region<Hub/Spoke>Environment | AEN-HUB-PRD01, AEN-SPK-PRD01 |
| Resource Group | Region<Hub/Spoke>Apps-RG-Sequence | AEN-HUB-INF-RG01 |
| Virtual Network | Region<Hub/Spoke>VNet-Environment | AEN-HUB-VNET-PRD01 AEN-HUB-VNET-PPRD01  AEN-HUB-VNET-DR01  AEN-SPK-VNET-PRD01 |
| Subnet | Region-VirtualNetwork-Services-Environment –FunctionalServices-Subnet.Sequence | AEN-SNET-HUB-PRD01-ADS-SN01  AEN-SNET-HUB-PRD01-AFW-SN01 |
| Network Security Group | Region-VirtualNetwork-Services-Environment –FunctionalServices-Subnet.Sequence -Network Security Group-Sequence | AEN-NSG-HUB-PRD01- ADS-SN01  AEN-NSG-HUB-PRD01-AFW-SN01 |
| UDR | Region-VirtualNetwork-Services-Environment –FunctionalServices-Subnet.Sequence -Routetable | AEN-UDR-HUB-PRD01-AFW-SN01  AEN-UDR-HUB-PRD01-AFW-SN01 |
| VPN Gateway | Region-VirtualNetwork-Services-Environment-Virtual gateway network sequence | AEN-VPN-HUB-PRD01-GTW-SN01 |
| Public IP | ResourceName-PublicIP | AEN-HUB-PRD01-AZFW01-PIP1 |
| Network Interface | VMName-NetworkInterfaceCard.Sequence | AENHUBADC01-NIC01  AENHUBADC02-NIC01 |
| Storage Account Name | Region-Services-Environment-Storage. Sequence | euhubinfsac01 |
| Disk | VMName-Purpose-Disk Type-Sequence | AENHUBADC101-OS AENHUBADC101-Data01 |
| Virtual Machine | Region.Services.ApplicationName.Environment.Sequence | AENHUBADC01  AENHUBADC02 |
| Load Balancer | Region-VirtualNetwork-Services-Environment –LoadBalancer sequence | AEN-ELB-HUB-PRD01-ILB01  AEN-ELB-HUB-PRD01-PLB01 |

**Note:** Operations Team has defined new naming convention for resources on Cloud based on the business & project requirement.

## Azure Instance Naming

Please find the Azure instance naming convention details

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Count | 3 Char | 1 Num | 2 Char | 1 Char | 1 Char | 3 Char | 3 Num |
| Description | DC | Tenant | Workload Type | OS | Environment | Role | ID |
| Sample Name | AEC | 3 | VS | W | P | SQL | 001 |

|  |  |
| --- | --- |
| Workload type | Character |
| Cluster | CL |
| Virtual Appliance | VA |
| Virtual Server | VS |
| Availability Group | AG |
| Listener | LR |

|  |  |
| --- | --- |
| OS | Character |
| Linux | L |
| Windows | W |
|  |  |

|  |  |
| --- | --- |
| Environment | Character |
| DEV | D |
| Production | P |
| Staging / PreProd | S |
| Test | T |
| UAT | U |

|  |  |
| --- | --- |
| Role | Character |
| SQL Server | SQL |
| App Name | xxx |

# Architectural Decision Summary

Several Architectural Decisions have been made while writing this document. These decisions can be found in individual components entitled Design Decisions.” However, a summary of these decisions is provided below: -

|  |  |  |
| --- | --- | --- |
| Decision Summary | | |
| Sr. No. | **Title** | **Reasoning and Description** |
| 1 | Azure Subscription | Single Subscription **AEN-HUB-PRD01** |
| 2 | Hub-Spoke Technology | Hub Virtual Network to be act as a central point of connectivity to on premise and Internet. Spoke virtual network to be used to isolate workloads. |
| 3 | Network Security Group | Dedicated NSG individual Subnets to control Port and IP based communication |
| 4 | VNET-to-VNET | In order to support connectivity between Spoke & Hub infrastructure and connectivity between Prod & DR VNET |
| 6 | Availability Zone | Identical VMs to be placed in Availability Zones to achieve 99.99% SLA |
| 7 | Firewall | Azure Firewall will be deployed to secure internal traffic between Azure & On-Premises |
| 8 | Load Balancer | Azure Application Gateway will be deployed to manage and load balance traffic to applications |
| 9 | Vulnerability Management | Tenable Appliance will be deployed in Azure |
| 10 | Patch Management | Azure Native Patching leveraged for patching workloads in the azure cloud  Ivanti For 3 rd Party Tool |
| 11 | Monitoring | Azure Monitor is the proposed solution which will be implemented in Cloud |
| 12 | Backup | Azure backup is the solution to be used for backup on Cloud |
| 14 | CA | CA Server will be hosted in a Hub subscription. |

# Acronyms

|  |  |  |
| --- | --- | --- |
| **Term** | **Definition** |  |
| IAAS | Infrastructure As a Service |  |
| RBAC | Role Based Access Control |  |
| VPN | Virtual Private Network |  |
| VNET | Virtual Network |  |
| NSG | Network Security Group |  |
| UDR | User Defined Route |  |
| VM | Virtual Machine |  |
| S2S | Site to Site |  |
| WAF | Web Application Firewall |  |
| ILB | Internal Load Balancer |  |
| ASR | Azure Site Recovery |  |
| RHEL | Red Had Enterprise Linux |  |