a

Design and Plan



Azure Platform Design

Prepared for

Ave Health Singapore

8/28/2023

Version 0.1.1 Final

Table of Contents

[Introduction 8](#_Toc107744981)

[Project Overview 10](#_Toc107744982)

[Document Purpose 10](#_Toc107744983)

[Intended Audience 10](#_Toc107744984)

[Related Project Documents 10](#_Toc107744985)

[Design 11](#_Toc107744986)

[Enterprise Agreement Hierarchy 13](#_Toc107744987)

[Subscription Organization and Governance 13](#_Toc107744988)

[Management Groups 13](#_Toc107744989)

[Azure Subscriptions 16](#_Toc107744990)

[Resource Groups 18](#_Toc107744991)

[Networking 22](#_Toc107744992)

[Design Considerations 22](#_Toc107744993)

[Design Decisions 23](#_Toc107744994)

[High Level – Hub and Spoke Network Design 24](#_Toc107744995)

[High Level - Point to Site Network Design 25](#_Toc107744996)

[Network Insight – Core Network Infrastructure 25](#_Toc107744997)

[Design Pattern: Hub/Spoke Interconnect Virtual Networks (Hub/Spoke VNet 27](#_Toc107744998)

[Design Pattern: Network Segmentation 28](#_Toc107744999)

[Design Pattern: Virtual Networks Connectivity 29](#_Toc107745000)

[Design Pattern: VNET Peering 30](#_Toc107745001)

[Network Address Spaces and Subnets 31](#_Toc107745002)

[Design Pattern: Name Resolution (DNS) 33](#_Toc107745003)

[Native security services 35](#_Toc107745004)

[Network Components Design 35](#_Toc107745005)

[Policy Management 35](#_Toc107745006)

[Technical Overview 35](#_Toc107745007)

[Design Considerations and Requirements 37](#_Toc107745008)

[Design Decisions 38](#_Toc107745009)

[Platform Automation and DevOps 43](#_Toc107745010)

[Requirements 43](#_Toc107745011)

[Design Recommendations 43](#_Toc107745012)

[Design Considerations 44](#_Toc107745013)

[Design Decisions 44](#_Toc107745014)

[Design Pattern: Landing Zone Release (LZR) 45](#_Toc107745015)

[Platform Management and Monitoring 50](#_Toc107745016)

[Introduction 50](#_Toc107745017)

[Azure Naming Convention 50](#_Toc107745018)

[Azure Role Based Access Control 52](#_Toc107745019)

[Design Decision - RBAC 55](#_Toc107745020)

[Azure Tags 58](#_Toc107745021)

[Azure Resource Locks 60](#_Toc107745022)

[Azure Cost Management 60](#_Toc107745023)

[Azure Advisor 62](#_Toc107745024)

[Azure Platform Monitoring 63](#_Toc107745025)

[Azure Platform Updates and Patching 68](#_Toc107745026)

[Azure Backup and BCDR 73](#_Toc107745027)

[Design Considerations 73](#_Toc107745028)

[Design Decisions 74](#_Toc107745029)

[Business Continuity and Disaster Recovery Overview 74](#_Toc107745030)

[Business Continuity Risks 74](#_Toc107745031)

[Business Continuity Plan Development 75](#_Toc107745032)

[Security 81](#_Toc107745033)

[Defender for Cloud 81](#_Toc107745034)

[Azure Key Vault 84](#_Toc107745035)

[Azure Data Encryption 84](#_Toc107745036)

[Identity 87](#_Toc107745037)

[Identity and Access Management 87](#_Toc107745038)

[Technical Overview 87](#_Toc107745039)

[Design Considerations & Requirements 87](#_Toc107745040)

[Design Decisions 87](#_Toc107745041)

[Appendix 99](#_Toc107745042)

[HLD Network Architecture – Ave Health and IHH Infra in Ave Health Azure Platform (Interim Solution) 99](#_Toc107745043)

[References 99](#_Toc107745044)

[Glossary of terms 100](#_Toc107745045)

Table of Figures

[Figure 1: Management Group Structure Overview. 10](#_Toc106222366)

[Figure 2: Management Group Structure Overview. 15](#_Toc106222367)

[Figure 3 Spoke Virtual Networks connected to the Hub Virtual Network 25](#_Toc106222368)

[Figure 1 Sample Three Tier Application Network Security Group 26](#_Toc106222369)

[Figure 6: DNS resolution topology 30](#_Toc106222370)

[Figure 8: Evaluation order flow diagram for the different policy conditions 33](#_Toc106222371)

[Figure 10: Azure Platform Management and Monitoring Overview 40](#_Toc106222372)

[Figure 11 Monitoring Model 52](#_Toc106222373)

[Figure 15 Backup and Disaster Recovery 60](#_Toc106222374)

Table of Tables

[Table 1: Guiding principles 10](#_Toc109818620)

[Table 2: Requirements and Considerations for Management Group structure. 14](#_Toc109818621)

[Table 3: Design Decisions - Management Groups 15](#_Toc109818622)

[Table 4: Requirements and Considerations - Subscriptions 17](#_Toc109818623)

[Table 5: Design Decisions - Subscriptions 18](#_Toc109818624)

[Table 6: Design decisions - Resource Groups 23](#_Toc109818625)

[Table 7 VNETs Information 30](#_Toc109818626)

[Table 8 VNETs Information 32](#_Toc109818627)

[Table 9 Address Space and Subnets 33](#_Toc109818628)

[Table 10: DNS resolution topology description 34](#_Toc109818629)

[Table 11: Requirements and Considerations - Azure Policy 37](#_Toc109818630)

[Table 12: Design Decisions - Azure Policy 41](#_Toc109818631)

[Table 13: Requirements and Considerations - Azure Naming Convention 50](#_Toc109818632)

[Table 14: Design Decisions - Azure Naming Convention 50](#_Toc109818633)

[Table 15: Mapping of RBAC Roles 53](#_Toc109818634)

[Table 16: RBAC Design Decisions 55](#_Toc109818635)

[Table 17: Design Decisions - Azure Tags 56](#_Toc109818636)

[Table 18: Suggestion for initial tags 58](#_Toc109818637)

[Table 19: Requirements and Considerations - Resource Locks 58](#_Toc109818638)

[Table 20: Design Decisions - Resource Locks 58](#_Toc109818639)

[Table 21: Design Decisions - Azure Advisor 60](#_Toc109818640)

[Table 22 Platform Monitoring Design Considerations 61](#_Toc109818641)

[Table 23 Platform Monitoring Decision Decisions 62](#_Toc109818642)

[Table 24 Azure Monitoring Tools 65](#_Toc109818643)

[Table 25 Platform Monitoring Design Considerations 68](#_Toc109818644)

[Table 26 Azure Updates Support Information 71](#_Toc109818645)

[Table 27 Azure Backup and BCDR Design Decisions 73](#_Toc109818646)

[Table 28: Azure Security Center feature comparison 81](#_Toc109818647)

[Table 29: Design Decisions - Defender for Cloud 81](#_Toc109818648)

[Table 30: Design Decisions - Key Vault 82](#_Toc109818649)

[Table 31: Microsoft Encryption Options 83](#_Toc109818650)

[Table 32: Azure Encryption Technologies 83](#_Toc109818651)

[Table 33: Design Decisions - Azure Data Encryption 84](#_Toc109818652)

[Table 34: Requirements and Considerations - Identity and Access Control 85](#_Toc109818653)

[Table 35: Design Decisions - Identity and Access Control 85](#_Toc109818654)

[Table 36: Design Decisions - Identity Provider 86](#_Toc109818655)

[Table 39: External Identities Design decisions 87](#_Toc109818656)

[Table 37: SSPR Design Decisions 88](#_Toc109818657)

[Table 38: Group Management Design Decisions 89](#_Toc109818658)

[Table 40: Identity Protection Design Decisions 91](#_Toc109818659)

[Table 41: MFA Design Decisions 92](#_Toc109818660)

[Table 43: CA Policies Design Decisions 95](#_Toc109818661)

[Table 44:Terms of Use Design Decisions 96](#_Toc109818662)

[Table 45: Design Decisions – PIM 96](#_Toc109818663)

[Table 46: PIM Design Decisions 97](#_Toc109818664)

[Table 48: References 99](#_Toc109818665)

[Table 49: Glossary of Terms 100](#_Toc109818666)

Introduction

This document is delivered to AVE Health SG to detail the design and plan for Azure Platform architecture that implements an application-centric, archetype neutral, democratized cloud-scale Landing Zone.

This reference architecture extends the current or green field setup/environment into cloud. While giving direction to AVE Health SG on how to deploy their own Azure environment in a standardized, secure, and controlled way, this document is not intended to be a general reference design for all the services available on Azure. The focus is to provide a Landing Zone to allow AVE Health SG to support the deployment of Business Entities workload and further prepare for future deployment of workloads and applications in Azure in a secure and compliant.

There is an immediate need for a new Azure Platform to support the deployment of workloads/business systems for the Business entities within their own Landing Zones.

Azure Landing Zones are environments that consider scale, security, governance, and identity to support application migration or greenfield deployments based on common design principles. These principles are formed as part of the Enterprise Scale framework for Landing Zones.

Enterprise Scale is a strategic design path that implements guard rails and architecture to ensure compliance and security whilst providing an application-centric democratized model to allow business entities application teams to deliver applications to AVE Health SG Platform.

Enterprise scale is like building a city, it is the foundation allowing people to come in and build houses how they see fit based on regulations e.g., number of stories or size, Enterprise Scale provides the power, water, roads, regulations, and permission etc.

Building an Enterprise Scale-compliant Landing Zone will prepare Azure for Business Entities and beyond. Coupled with Modern Service Management strategies, the CCoE/Cloud Platform Team will be able to provide modern application delivery and capabilities AVE Health SG; demonstrating the value of cloud to support Tech Intensity.

This design document describes the proposed cloud architecture, based on Microsoft Azure for Enterprise Scale Landing Zones. This architecture will establish an Azure AD configuration that will initially be Hybrid/cloud-based Authentication, role-based access, and identity management will be administered centrally in the cloud.

This document does not explain in detail how to create environments or how certain features work. Instead, it reports the choices and concepts that are valid for the specific AVE Health SG context and identified scenarios. Utmost care was taken to ensure that the design meets all requirements voiced by AVE Health SG in the discovery workshops and it is pointed out where these requirements are conflicting with established best practices.

Furthermore, we base our design recommendations on the following principles as agreed upon with AVE Health SG stakeholders:

|  |  |
| --- | --- |
| Principle | Description & Reasoning |
| Whenever possible use cloud native technologies | Cloud native technologies allow easier integration into Azure and other clouds and new tools. |
| Choose Azure-native over non-Azure-native solutions | Using Azure-native solutions, such as Azure Firewall over 3rd party NVAs. |
| Data born in Azure stays in Azure | As a principle data produced in Azure should stay in Azure unless there is a strong reason to export it to another environment. This allows better control over the data and reduces potential egress costs |
| SaaS > PaaS > IaaS | Where possible SaaS offerings should be preferred over PaaS offerings and PaaS over IaaS. Essentially, this means that when choosing an Azure solution for a particular use case, products should be preferred that provide AVE Health SG with the smallest responsibility for management (while still meeting the required amount of configurability).  This reduces the operative effort for AVE Health SG as well as the risks associated with wrong configuration or maintenance. Furthermore, SaaS and PaaS offerings usually provide a higher availability and security level than IaaS. |
| Use identity as primary security boundary | With the advent of public clouds and hybrid networks, traditional security boundaries such as Demilitarized Zones (DMZs) with Firewalls (FWs) are no longer sufficient as the sole line of defense and identity has become the primary boundary. In this document we will provide in-depth advice as to how to use identities to limit a user’s rights to the bare minimum and to protect user’s identities from being breached. |
| Azure AD as the Core Identity to Cloud Services | Organizations often have hundreds of applications that users depend on to get their work done. Users access these applications from many devices and locations. New applications are added, developed, and sun-setted every day. With so many applications and access points, it's more critical than ever to use a cloud-based solution to manage user access to all applications. Azure Active Directory (AD) simplifies the way applications are managed by providing a single identity system for both cloud and on-premises apps. |
| Base architecture on well-established best practices and use Microsoft's Enterprise-Scale architecture as reference architecture (as far as appropriate) | [Microsoft’s Enterprise-Scale architecture](https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/architecture) is an architectural approach and reference implementation that enables effective construction and operationalization of Landing Zones on Azure for large and complex enterprises. This concept is in line with Azure best practices and has been successfully used to onboard multiple large companies with complex on-premises architectures to Azure and therefore offers a good foundation for designing AVE Health SG’s Landing Zone. |

Table 1: Guiding principles

Project Overview

AVE Health SG has engaged Microsoft Consulting Services to implement and Enterprise Scale design. This document details the design and plan for an Enterprise Scale platform.

Document Purpose

The purpose of this document is to detail the design for this solution and the high-level plan for its delivery. Its content is based on information gathered and decisions made during the workshop that were conducted with AVE Health SG between the 23rd may and 10th 2022. Decisions made during subsequent planning meetings have also been captured in this document.

Intended Audience

This document is intended for the AVE Health SG project resources who will be responsible for the solution after it’s delivered. It assumes a basic working knowledge of Azure Platform, Cloud Services, Infrastructure- and Platform-as-a-Service.

Related Project Documents

This document is one of several that are being produced by Microsoft Services for the project. The following table details other project documents that are closely related to or referenced by this design and plan document.

|  |  |
| --- | --- |
| Document | Description |
| Azure Platform – Preparation of Plan and Design Checklist | Document, the preparation of Plan and Design which must be completed and the resources which must be procured before the work for Azure Platform Design can be completed. |
| Azure Platform Design Decision tracker checklist | Document captures workshops outcomes and be baseline for the Plan and Design document |

Design

The following diagram represents the logical view of the Enterprise Scale cloud platform and its relation to Landing Zones for AVE Health SG. This design includes the Core Cloud Platform, its supporting services.

Diagram

Description automatically generated

Figure 1: Management Group Structure Overview.

The core cloud platform encompasses a variety of services and resources including connectivity. Figure 1 shows the logical view of these network, services, and connectivity topology in further detail.

Note: This Enterprise-scale design includes considerations for future services in the Core Cloud Platform, such as Planning, restructuring and deployment of Active Directory Domain Services, which are not part of this current project scope.

Core Cloud Platform Components

1. One Connectivity/Network subscription will be provisioned in Southeast Asia, for catering the connectivity requirement of AVE Health SG. AVE Health SG will be establishing connectivity between AVE Health SG Az Platform with IHH & Health Catalyst Platform using S2S/VPN/IPsec.
2. AVE Health SG Az Platform will have single Virtual WAN Instance with Single hub to support establishing connectivity with IHH and Health Catalyst Platform. Also, AVE Health SG will have customer managed Hub provisioned in connectivity/Network subscription to support all four environment which include Production, Preproduction, QA and Development.
3. Azure Firewall standard edition will be deployed in the Connectivity/Network Subscription to monitor the private traffic between AVE Health SG Az Platform and IHH & Health Catalyst.
4. No ExpressRoute circuits will be provisioned in the connectivity/Network subscription. Since AVE Health SG does not have requirement to establish connectivity to on-premise or remote site other than integrating with IHH & Health Catalyst using VPN/S2S/IPsec.
5. AVE Health SG IT Administrator will connect remotely to Azure Platform using Point to Site VPN. To support all connectivity which includes S2S/IPsec connectivity between IHH & Health Catalyst site. Ave Health IT admins will connect via Point to Site VPN. Virtual WAN HUB will have Site to Site VPN and Point to Site Gateway provisioned.
6. AVE Health SG Partners will use Azure Bastion Service to access the VMs in Azure Platform with appropriate access granted through RBAC.
7. Azure Firewall Standard will manage both Private Traffic and internet traffic (Egress only) to and from Azure. Azure Firewall will provide routing access cross applications/spoke VNETS based on the Firewall Rules. In additional to Azure Firewall, No Web Application Firewall (WAF V2) will be deployed to cater ingress traffic. AVE Health SG doesn’t have any requirement to deploy WAF / L7 cloud native Firewall. Deploying and configuring 3rd party or next generation firewall, choice of customer is currently not in scope of this engagement.
8. Azure Firewall deployed in Connectivity VNET will be Zone Redundant.
9. Azure Monitor will be used to monitor Network/Gateway (and any future private connection components) latency, bandwidth utilization and loss at the Gateway level.
10. As per the Hub-and-Spoke topology followed, VNet Peering is enabled between the Hub (Connectivity) VNet, Compliance VNet and the Identity and Landing Zone VNets. This allows for Business systems for Business entities to access shared services while maintaining an isolation as per Enterprise Scale architecture.
11. An Identity VNet will be created which will contain any future AD DS servers for any applications which might require AD authentication.
12. A centralized Log Analytics workspace will be created in the security Subscription to collect all the security related (Azure Defender /Azure Security Center) activity across the subscriptions in the Azure Tenant.
13. A centralized Log Analytics workspace will be created in the Management Subscription to collect all the Network and platform activities across the subscriptions in the Azure Tenant.
14. Azure Key Vault will be provisioned within the respective Subscriptions to contain all secrets and keys for services across the AVE Health SG Cloud Azure Tenant as required.
15. All subscriptions will be configured with Azure Defender/Azure Security Center Standard Tier for all four environments (Production, Preproduction, QA and Development), and Azure Monitor to ensure compliance and optimal performance of all Azure resources.
16. Azure DDOS Standard plan will be deployed in the Connectivity subscriptions to protect Az Firewall and Azure Bastion Services. The same plan will be extended to provide protection to all the spoke VNets.
17. Azure Active Directory will be used as the identity source for access to the cloud platform.
18. Management Groups and subscription level will be used to manage access and governance at scale.

Enterprise Agreement Hierarchy

AVE Health SG is planning to purchase Azure services using Enterprise Agreement enrolment model.

Subscription Organization and Governance

Management Groups

Technical Overview

A Management Group (MG) structure within an Azure AD tenant supports organizational mapping to efficiently manage access, policies, and compliance for multiple Subscriptions. Subscriptions (and MGs too) can be organized into containers called MGs and governance conditions can be applied to the MGs such that all child MGs, Subscriptions, and resources within the parent MG automatically inherit the conditions applied to the parent MG.

Each Azure AD Tenant is given a single top-level MG called the ‘Tenant Root Group’. This root MG is built into the hierarchy to have all MGs and Subscriptions fold up to it. This root MG allows for Azure policies and Role-Based Access Control (RBAC) assignments to be applied at the directory level. No one is given default access to the root management group. Azure AD global administrators are the only users that can elevate themselves to gain access. Once they have access to the root MG, the global administrators can assign any RBAC role to other users to manage it. An MG tree can support up to six levels of depth. This limit doesn't include the root or Subscription level.

MGs will help AVE Health SG build a flexible structure of Subscriptions to organize resources into a hierarchy for unified policy and access management. For example, a policy can be applied to an MG that limits the regions available for VM creation. This policy would be applied to all MGs, Subscriptions, and resources under that MG by only allowing VMs/resources to be created in that region.

Design Considerations and Requirements

|  |
| --- |
| Requirements |
| AVE Health SG IT Team would like to remain in control of shared services (core services) and certain LZ aspects. |
| Enterprise Scale will be used as the framework for the Management Group structure. |
| The structure needs to be “future-proof” by allowing AVE Health SG to abide by regulatory requirements enforced by Regulatory Bodies in the future. |

Table 2: Requirements and Considerations for Management Group structure.

The following table documents the design decisions related to the creation of MGs:

|  |  |  |
| --- | --- | --- |
| Management Group  Display Name | Management Group Id | Reasoning |
| Tenant Root Group | Azure AD Tenant Id | The root Management Group is created in the directory by default. It will not be used directly, allowing for greater flexibility in the future to incorporate an equivalent environment for end-to-end Azure architecture. There is no requirement to change its display name. Azure AD Tenant’s Primary domain:  Default Domain: <TBD>  Primary Domain: <TBD> |
| Ave Health SG DW Root Management Group | avesgroot-mg | This is the top-level MG implemented within the AVE Health SG production tenant and will serve as the container for global policy and role assignments. For policy and role assignments at this scope, the target state is to ensure security and autonomy for the platform as additional sub scopes are created, such as child MGs and Subscriptions. |
| Platform Core Management Group | platform-mg | For management and governance of the Subscriptions that will host the Monitoring, Security, Management and any future Azure Cloud Operation related services. |
| Network Core Management Group | cor-network-mg | For all services included in the governance of all Connectivity-related services such as Virtual WAN, Azure Firewall & Azure Bastion Services within the Connectivity Subscription. |
| Management Core Management Group | cor-platform-mg | For all the Azure Management related which include monitoring will hosted within the Core Management. |
| Identity Core Management Group | cor-identity-mg | For all future services included in the governance of all Identity-related services such as the ADDS servers in the Identity Subscription. |
| Landingzone Management Group | landingzone-mg | All Subscriptions that have applications deployed are will be grouped in the Landing Zone Management Group. This allows for a generic yet more granular approach to policy assignments to separate active Landing Zones from any other workloads. |
| Production Management Group | prd-mg | Further granularity around the Production Workloads is grouped for AVE HEALTH SG entities. These are currently separated at the MG level as they are developed and managed by various business entities. |
| Dev Management Group | dev-mg | Further granularity around the Development/Non-Production Workloads is grouped for AVE HEALTH SG entities. These are currently separated at the MG level as they are developed and managed by various business entities. |
| Pre-Production Management Group | preprd-mg | Further granularity around the Pre-Production Workloads is grouped for AVE HEALTH SG entities. These are currently separated at the MG level as they are developed and managed by various business entities. |
| QA Management Group | qa-mg |  |
| Decommission Management Group | dcom-mg |  |
| Sandbox | Sbx-mg |  |

Table 3: Design Decisions - Management Groups

These decisions are summarized in the following diagram:

Chart, box and whisker chart

Description automatically generated

Figure 2: Management Group Structure Overview

Azure Subscriptions

Technical Overview

Subscriptions are a unit of management, billing, and scale within Azure, and play a critical role when designing for Azure adoption. Subscriptions provide a management boundary for governance and isolation, creating a clear separation of concerns. An Azure Subscription is a container for Azure resources. Each resource in Azure, such as a VM or VNet, is contained within a Subscription. When a resource is created, an Azure Subscription is also chosen to deploy that resource

Multiple Subscriptions can be created to separate workloads by financial and administration logic. A Subscription has a trust relationship with Azure AD tenant to authenticate users, services, and devices. An Azure AD directory can be trusted by multiple Subscriptions while a Subscription can only trust a single directory.

A Subscription is not tied to a specific Azure region. However, each Azure resource is deployed to only one region. Resources can be created in multiple regions within the same Subscription.

Requirements and Considerations

Following requirements will influence the Subscription design pattern:

|  |
| --- |
| Requirement |
| Target Subscriptions will be based on to services/projects with a breakdown depending on deployment environment (e.g., dev/QA/prod/PreProd) |
| Subscription breakdown is driven at a service level to ensure proper cost allocation is performed on resources used by projects. |
| Subscriptions will be used for all those falling under the Platform MG and cost allocation can be done to split those common costs between the different Landing Zones (as required). |
| Where services are to be shared between landing zones, they should be located within one of the Platform subscriptions e.g., Connectivity. |
| Services shared between components within Landing Zones should be deployed within the Landing Zones themselves, e.g., Private Link for Production Database should be located within the production subscription of the relevant Landing Zone. |

Table 4: Requirements and Considerations - Subscriptions

Design Decisions

The following table documents the design decisions related to Subscriptions:

|  |  |  |  |
| --- | --- | --- | --- |
| Description | Subscription Name | | Reasoning |
| Security Subscription | ave-cor-security | | ## Compliance and Security. #AVE Health SG -Azure Defender-Security and compliance Log |
| Platform Automation Subscription | ave-cor-automation | | ## Build and Automation. |
| Management Subscription | ave-cor-management | | ## Shared services for all three environments.  ## AVE Health SG -Platform-Audit / Log  This is separated by environment since AVE HEALTH SG can deploy Anti-Virus or service Endpoints for PreProd, Non-Prod or Production. |
| Connectivity Subscription | ave-cor-network | | # Connectivity production for hubs  Azure Virtual WAN, Azure Hub (Customer Managed HUB), Virtual Network Gateway will be deployed to support Production, Dev, QA and Preproduction |
| Identity Subscription | ave-cor-identity | | Dedicated subscription to host or extended the Active Directory Domain Controller to support authentication and Authorization for the application infrastructure hosted in the Azure. |
| QA | ave-qa-workload | | ##AVE Health SG QA instance / workloads |
| PreProduction | ave-preprod-Workload | | ##AVE Health SG PreProd/Staging instance / workloads |
| Production | | ave-prod-workload | ## AVE Health SG Production Instance / Workloads Published to Internet Access |
| Development | | ave-dev-workload | ## AVE Health SG Development Instance / Workloads Published to Intranet Access |
| Sandbox | | ave-sbx-workload | ## AVE Health SG Platform SANDBOX  SANDBOX for Automation / Deployment / Testing |
| Decommissioned | | ave-dcom-workload | ## AVE Health SG decommissioned Instance / Workloads |

Table 5: Design Decisions - Subscriptions

**Subscription Design Consideration**:

Azure Subscription can be democratized for application with two options

1. Single subscription model: In single subscription model, one or more workloads/applications will be deployed having resource group as a boundary/Isolation.
2. Multiple subscription model: Each workload or application will be hosted or deployed in an individual subscription having subscription as boundary/Isolation.

After understanding AVE Health SG requirements, Microsoft recommends AVE Health SG to have single subscription model per environment. Each environment will have a subscription to support the workload deployment.

Resource Groups

Technical Overview

Resource Groups (RGs) are logical containers that are used to group related resources in a Subscription and allow for granular grouping within a Subscription. Each resource can exist in only one RG. RGs are commonly used to represent a collection of assets required to support a workload, application, or specific function within a Subscription. Resource Groups also provide a way to isolate workload management and access to the right audience.

Design Decisions

The following table documents the design decisions related to RGs:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Subscription Name | Resource Group Region | Resource Group Name | Description | Comment |
| ave-cor-network | Southeast Asia | ave-sea-cor-arg-network | VNET and network resources e.g., VNET, Route tables and Network Security Groups | The resource group will be created during Platform deployment |
| Southeast Asia | ave-sea-cor-arg-vwan | Virtual WAN deployment | The resource group will be created during Platform deployment |
| Southeast Asia | ave-sea-cor-arg-bas | Azure Bastion Service Deployment | The resource group will be created during Platform deployment |
| Southeast Asia | ave-sea-cor-arg-backup | For the Recovery Vault & Backup | The resource group will be created during Platform deployment |
| Southeast Asia | ave-sea-cor-arg-fw | For the Azure Firewall deployment | The resource group will be created during Platform deployment |
| Southeast Asia | ave-sea-cor-arg-fwp | For the Az Firewall policy | The resource group will be created during Platform deployment |
| Southeast Asia | ave-sea-cor-arg-ddos | DDOS Plan deployment | The resource group will be created during Platform deployment |
| ave-cor-identity | Southeast Asia | ave-sea-cor-arg-backup | Recovery Vault and Backup | The resource group will be created during Platform deployment |
| Southeast Asia | ave-sea-cor-arg-id\_network | For the VNET and NSG etc | The resource group will be created during Platform deployment |
| ave-cor-management | Southeast Asia | ave-sea-cor-arg-backup | Recovery Vault and Backup | The resource group will be created during Platform deployment |
| Southeast Asia | ave-sea-cor-arg-mgmt\_network | VNET and network resources e.g., Route tables and Network Security Groups | The resource group will be created during Platform deployment |
|  | Southeast Asia | ave-sea-cor-arg-logs | Log Analytics Workspace for Azure Monitor | The resource group will be created during Platform deployment |
| ave-cor-security | Southeast Asia | ave-sea-cor-arg-backup | Recovery Vault and Backup | The resource group will be created during Platform deployment |
| Southeast Asia | ave-sea-cor-arg-logs | Log Analytics Workspace for Azure defender/ Azure Security Center | The resource group will be created during Platform deployment |
| Southeast Asia | ave-sea-cor-arg-sec\_network | Azure VNET and network resources e.g., Route tables and Network Security Groups | The resource group will be created during Platform deployment |
| ave-dcom-workload | Southeast Asia | ave-sea-cor-arg-dcom\_network | VNET and network resources e.g., Route tables and Network Security Groups | The resource group will be created during Platform deployment |
| Southeast Asia | ave-sea-cor-arg-backup | Recovery Vault and Backup | The resource group will be created during Platform deployment |
| ave-sbx-workload | Southeast Asia | ave-sea-cor-arg-sbx\_network | VNET and network resources e.g., Route tables and Network Security Groups | The resource group will be created during Platform deployment |
| Southeast Asia | ave-sea-cor-arg-backup | Recovery Vault and Backup | The resource group will be created during Platform deployment |
| ave-prd-Workload | Southeast Asia | ave-sea-cor-arg-prd\_network | VNET and network resources e.g., Route tables and Network Security Groups | The resource group will be created during Platform deployment |
| Southeast Asia | ave-sea-cor-arg-backup | Recovery Vault and Backup | The resource group will be created during Platform deployment |
| ave-qa-workload | Southeast Asia | ave-sea-cor-arg-qa\_network | VNET and network resources e.g., Route tables and Network Security Groups | The resource group will be created during Platform deployment |
| Southeast Asia | ave-sea-cor-arg-backup | Recovery Vault and Backup | The resource group will be created during Platform deployment |
| ave-dev-workload | Southeast Asia | ave-sea-cor-arg-dev\_network | VNET and network resources e.g., Route tables and Network Security Groups | The resource group will be created during Platform deployment |
| Southeast Asia | ave-sea-cor-arg-backup | Recovery Vault and Backup | The resource group will be created during Platform deployment |
| ave-preprod-workload | Southeast Asia | ave-sea-cor-arg-preprod\_network | VNET and network resources e.g., Route tables and Network Security Groups | The resource group will be created during Platform deployment |
|  | Southeast Asia | ave-sea-cor-arg-backup | Recovery Vault and Backup | The resource group will be created during Platform deployment |
| ave-cor-automation | Southeast Asia | ave-sea-cor-arg-auto\_network | VNET and network resources e.g., Route tables and Network Security Groups | The resource group will be created during Platform deployment |
| Southeast Asia | ave-sea-cor-arg-backup | Recovery Vault and Backup | The resource group will be created during Platform deployment |

Table 6: Design decisions - Resource Groups

Networking

This section describes Azure Networking design details which includes the following.

* + Design Considerations
  + Design Decisions
  + Design Patterns and Technical Details

Design Considerations

|  |  |
| --- | --- |
| ID | Description |
| DC1 | AVE Health SG made decision to have all customer data must be resident in Southeast / Singapore Region only for now. |
| DC2 | CIDR Address space / IP Address assignments are managed by AVE Health SG network team |
| DC3 | All communications between virtual networks must be secured |
| DC4 | No default direct connectivity between workloads /Spoke VNETs. |
| DC7 | Isolation of workloads based on the environment (Production, PreProduction, QA and Development will be achieved via Azure Firewall. |
| DC8 | Design should provide redundant connectivity between Azure Platform and IHH & Health Catalyst |
| DC9 | AVE Health SG does not have Ingress requirement and no so design consideration for WAF/3rd party L7 Firewall. |

Design Decisions

|  |  |
| --- | --- |
| ID | Description |
| DD1 | Single Virtual WAN instance with Single Hub will be created in the Southeast Asia region |
| DD2 | AVE Health SG has no on-premises connectivity requirements. So, no design consideration for ExpressRoute/ Hybrid Connectivity. |
| DD3 | Connectivity between AVE Health SG Azure Platform and IHH & Health Catalyst will be established using Site to Site VPN/IPsec. |
| DD4 | Point to Site VPN will be established in AVE Health SG to allow the AVE Health SG IT team to access the platform remotely for the administration |
| DD | All the Network resource deployment will be in Southeast Asia Region |
| DD6 | The formation of Spoke Virtual Networks and subnet-associated Network Security Groups must be managed by AVE Health SG. Environment specific VNETs and Subnets associated NSGs are managed by AVE Health SG. |
| DD7 | AVE Health SG controls IPV4 Address spaces assignments to Subscriptions including LOB/Workloads |
| DD8 | AVE Health SG will Standalone/Bind DNS for the Azure Platform Name resolution. AVE Health SG will configure DNS server in Identity subscription to support all four environments. |

High Level – Hub and Spoke Network Design

Diagram

Description automatically generated

Core Network Components

1. All the network connectivity related Azure services which include Virtual WAN HUB, customer managed HUB VNet, Azure Firewall and Azure Bastion will be hosted in the Connectivity/Network subscriptions.
2. A Virtual WAN Hub will have Site to Site VPN Gateway and Point to Site VPN Gateway provisioned.
3. Azure Firewall will regulate the private traffic between AVE Health Azure Platform and IHH & Health Catalyst.
4. A Hub-and-Spoke topology will be configured to access shared services.
5. All the Partner / External Entities will access the IaaS/VMs using Azure Bastion Services. All the AVE Health IT administrators will connect to Azure Platform remotely via Point to Site VPN. This principle will remain same for both Ave Health Az Platform and IHH Az Platform.

The above diagram depicts different traffic flow for the AVE Health SG.. All outbound internet traffic(egress) will also pass via Azure Firewall. Traffic between VNets will traverse though Azure firewall. This provides a central point to route and filters all the traffic. This routing is configured with the help of User defined routes (UDRs) configured within route tables. No inbound Https/Http traffic from the internet is allowed by design.

High Level - Point to Site Network Design

Diagram

Description automatically generated

**Azure P2S VPN design consideration and design decision**:

Azure Point to Site VPN design will the following decision

1. Azure Point to Site VPN will have Azure AD Authentication.
2. Azure Point to Site VPN Tunnel Type will OpenVPN.
3. Azure Point to Site VPN Gateway will have 2 scale unit SKU. Supports 1 Gbps speed and up to 500 clients.
4. VPN CIDR for the client address [TBD] /24

Network Insight – Core Network Infrastructure

The section provides sizing and SKU recommendation for the core network infrastructure.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Azure Infrastructure | Subscription | VNET  Subnet | SKU Recommendation | |  |
| Azure Firewall | ave-cor-network | VNET:ave-sea-cor-vnt-10.166.4.0 Subnet :  AzureFirewallSubnet -  10.166.4.0/26 | |  |  | | --- | --- | | Region | SEA - Southeast Asia | | Availability Zone - Public IP | Zone Redundant | | Firewall Management (Classic / Firewall Policy) | FW Policy | | Firewall Policy (Existing) | NA | | SKU | Standard | |  | |
| Azure Bastion | ave-cor-network | ave-sea-cor-vnt-10.166.4.0  Subnet :  AzureBastionSubnet -  10.166.5.0/26 | |  |  | | --- | --- | | Tier SKU | Standard | | Instance Count | 3 | | Public IP Address SKU | Standard | | Assignment | Static | |  | |
| Azure DDOS Plan | ave-cor-network | ave-sea-cor-vnt-10.166.4.0 | |  |  | | --- | --- | | Region | Southeast Asia | | Tier | Standard Plan | | Protection | All VNETs,  Az Firewall,  Azure Bastion,  Gateways. | |  | |
| Virtual WAN | ave-cor-network | 10.166.0.0/22 | |  |  | | --- | --- | | Hub Type | Standard -  User VPN (P2S) VPN (site-to-site) | | Single Hub or Multiple Hub? | Single Hub. Connectivity between the virtual network  connections assumes, by default, a maximum total of 2000  VM workload across all  VNets connected to a single virtual Hub.  This limit can be increased opening an online customer support request | | Default Route Table or Custom Route Table (Isolation based on Environment) |  | |  | | Default Route Table and  VNET: ave-sea-cor-vnt  -10.166.4.0 will be the  Only VNET added as  connection | |  | |  | | Region | SEA | | Name | ave-sea-cor-vhub-001 | | Hub Private Address Space | 10.166.0.0/22 | | Hub (VPN Gateway) AS Number | Default / 65515 | | Hub (VPN Gateway) Routing Preference | Microsoft Network | | Hub (VPN Gateway) Gateway Scale Unit | 3 Scale Unit | |  | |
|  |  |  |  |  | |

Design Pattern: Hub/Spoke Interconnect Virtual Networks (Hub/Spoke VNet

Hub and Spoke Interconnect Virtual Networks will enable AVE Health SG to form a connectivity. The model is intended to be repeatable as a pattern that can be stamped across regions, with peering formed as necessary through programmatic controls.

The Interconnect can include a security stack set as the default route across Peering links with User Defined Routes but uses Azure native capabilities as default selections to meet requirements. ACL is effectively set with subnet-level network security groups and route control.

Graphical user interface, diagram

Description automatically generated

Figure 3 Spoke Virtual Networks connected to the Hub Virtual Network

Design Pattern: Network Segmentation

A network security best practice is to make sure there are network access controls between network constructs. These constructs can represent virtual networks, or subnets within those virtual networks. This works to protect and contain Southeast Asia traffic within your cloud network infrastructure. A common practice is to implement Network Security Groups to control lateral traffic.

Subnets will be planned based on common roles and functions. Simple example: application tier and data tier will be segregated into different subnets; Network Security Group rules will be adjusted for each to further restrict access.

If needed Application Security Groups (ASG) can also be created, allowing us to group virtual machines and define network security policies based on these groups. Regardless, the intention is to use patterned ASG/NSG as automated ACL that are defined based on the required landing zone and application.

Graphical user interface, text, application

Description automatically generated

Figure 1 Sample Three Tier Application Network Security Group

As documented in the subscription design section, AVE Health SGhas decided to share the subscription with dedicated VNET for the workloads/landing zone in their respective environment. This creates a clear segmentation based on their business requirements. Each Environment may have one or more virtual networks. Virtual network connectivity will be based on AVE Health SG decision and will be authorized by AVE Health SG.

The NSGs come with default rules to block incoming connection from outside the VNet. Only the needed inbound ports will be opened as required by the workloads in the virtual network.

The default rule set for NSGs for inbound ports is depicted below.

Inbound

AllowVNetInBound

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Priority | Source | Source ports | Destination | Destination ports | Protocol | Access |
| 65000 | VirtualNetwork | 0-65535 | VirtualNetwork | 0-65535 | Any | Allow |

AllowAzureLoadBalancerInBound

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Priority | Source | Source ports | Destination | | Destination ports | Protocol | Access |
| 65001 | AzureLoadBalancer | 0-65535 | | 0.0.0.0/0 | 0-65535 | Any | Allow |

DenyAllInbound

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Priority | Source | Source ports | Destination | Destination ports | Protocol | Access |
| 65500 | 0.0.0.0/0 | 0-65535 | 0.0.0.0/0 | 0-65535 | Any | Deny |

Design Pattern: Virtual Networks Connectivity

We can categorize the VNETs deployed in AVE Health SG Azure cloud environment into 5 types:

|  |  |
| --- | --- |
| VNET Type | Purpose and Characteristics |
| Hub VNET | * Hub is created under the Connectivity Subscription to support all three environments in Singapore region. It allows multiple spoke VNETs to share the network connectivity. * Work as a network hub to provide connectivity, for other spoke VNETs. * Work as a routing hub to route traffic between spoke VNETs. * It provides secure inbound and outbound Internet connectivity, for Azure workloads running in Hub and Spoke VNETs in the local Azure region. * It is the only VNET that allows public IP address to be assigned in the NVA VMs or Azure Load Balancers. |
| Spoke / Workload VNET | * It is the VNET on which Azure workloads of a Project / LOB are deployed. * It is created under the Subscription charged to Project / LOB in their respective environment. * It is created in one region Southeast Asia. * It is connected to one Hub VNET via VNET peering. It allows communication with the Hub VNET and on-premises networks. |
| Shared Services VNET  Management VNET  Security VNET | * It is the VNET built specifically to provide common core services to be shared across the workloads deployed in spoke VNETs in their respective environment. * It is created under the Management, Security Subscription. * It is connected to each Spoke VNET using VNET peering connection with Hub. * No other Azure workload should be deployed in this VNET, except the shared services. |
| Identity VNET | * It is the VNET built specifically to provide Identity services to be shard across the workloads deployed in spoke VNETs in their respective environment. * It is created under the Identity Subscription. * It is connected to each Spoke VNET using VNET peering connection with Hub. * No other Azure workload should be deployed in this VNET, except the Identity related services. |
| Isolated VNET  Decommissioned  Sandbox | * It is the VNET built specifically to Sandbox Environment * It is created under the Decommissioned & Sandbox Subscription. * It is isolated VNET and not connected with Hub. |

Table 7 VNETs Information

Design Pattern: VNET Peering

Virtual network peering enables to seamlessly connect two or more [Virtual Networks](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview) in Azure. The traffic between virtual machines in peered virtual networks uses the Microsoft backbone infrastructure.

The network topology in Azure for AVE HEALTH SG uses a hub and spokes model. The hub virtual network acts as a central point of connectivity to many spoke virtual networks. The hub is also be used as the connectivity point to other remote networks which include IHH and Health Catalyst.

The network hub will be connected to the spokes via peering as shown in the table below.

|  |  |  |  |
| --- | --- | --- | --- |
| Hub VNET Name | Spoke VNET | Peering (Hub to Spoke) | Peering (Spoke to Hub) |
| ave-sea-cor-vnt-10.166.4.0 | ave-sea-cor-vnt-10.166.8.0 | vnet-10.166.4.0-TO-vhub-vnet-10.166.8.0 | vnet-10.166.8.0-TO-vhub-vnet-10.166.4.0 |
| ave-sea-cor-vnt-10.166.4.0 | ave-sea-cor-vnt-10.166.9.0 | vnet-10.166.4.0-TO-vhub-vnet-10.166.9.0 | vnet-10.166.9.0-TO-vhub-vnet-10.166.4.0 |
| ave-sea-cor-vnt-10.166.4.0 | ave-sea-cor-vnt-10.166.10.0 | vnet-10.166.4.0-TO-vhub-vnet-10.166.10.0 | vnet-10.166.10.0-TO-vhub-vnet-10.166.4.0 |
| ave-sea-cor-vnt-10.166.4.0 | ave-sea-prd-vnt-10.166.11.0 | vnet-10.166.4.0-TO-vhub-vnet-10.166.11.0 | vnet-10.166.11.0-TO-vhub-vnet-10.166.4.0 |
| ave-sea-cor-vnt-10.166.4.0 | ave-sea-npe-vnt-10.166.12.0 | vnet-10.166.4.0-TO-vhub-vnet-10.166.12.0 | vnet-10.166.12.0-TO-vhub-vnet-10.166.4.0 |
| ave-sea-cor-vnt-10.166.4.0 | ave-sea-prd-vnt-10.166.16.0 | vnet-10.166.4.0-TO-vhub-vnet-10.166.160 | vnet-10.166.16.0-TO-vhub-vnet-10.166.4.0 |
| ave-sea-cor-vnt-10.166.4.0 | ave-sea-npe-vnt-10.166.20.0 | vnet-10.166.4.0-TO-vhub-vnet-10.166.20.0 | vnet-10.166.20.0-TO-vhub-vnet-10.166.4.0 |
| ave-sea-cor-vnt-10.166.4.0 | ave-sea-npe-vnt-10.166.24.0 | vnet-10.166.4.0-TO-vhub-vnet-10.166.24.0 | vnet-10.166.24.0-TO-vhub-vnet-10.166.4.0 |

Network Address Spaces and Subnets

AVE Health SG has two on-premises datacenters in Malaysia. Microsoft Azure will be connected via ER where network address space must be designed accordingly.

|  |  |  |  |
| --- | --- | --- | --- |
| VNET Name | Subscription | Azure Region | Connectivity and other Requirements |
| ave-sea-cor-vnt-10.166.4.0 | ave-cor-network | Southeast Asia | Core network Hub and will be connected to the vWAN HUB. |
| ave-sea-cor-vnt-10.166.8.0 | ave-cor-identity | Southeast Asia | Spoke VNET will be connected to Core network Hub. Will not be connected vWAN Hub. |
| ave-sea-cor-vnt-10.166.9.0 | ave-cor-management | Southeast Asia | Spoke VNET will be connected to Core network Hub. Will not be connected vWAN Hub |
| ave-sea-cor-vnt-10.166.10.0 | ave-cor-automation | Southeast Asia | Spoke VNET will be connected to Core network Hub. Will not be connected vWAN Hub |
| ave-sea-cor-vnt-10.166.11.0 | ave-cor-security | Southeast Asia | Spoke VNET will be connected to Core network Hub. Will not be connected vWAN Hub |
| ave-sea-prd-vnt-10.166.12.0 | ave-prd-workload | Southeast Asia | Spoke VNET will be connected to Core network Hub. Will not be connected vWAN Hub |
| ave-sea-dev-vnt-10.166.16.0 | ave-dev-workload | Southeast Asia | Spoke VNET will be connected to Core network Hub. Will not be connected vWAN Hub |
| ave-sea-qa-vnt-10.166.20.0 | ave-qa-workload | Southeast Asia | Spoke VNET will be connected to Core network Hub. Will not be connected vWAN Hub |
| ave-sea-pprd-vnt-10.166.24.0 | ave-pprd-workload | Southeast Asia | Spoke VNET will be connected to Core network Hub. Will not be connected vWAN Hub |

Table 8 VNETs Information

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Environment | Environment type | | Virtual network | IP address range with Subnets | Comments |
| Core | | network | ave-sea-cor-vnt-10.166.4.0 | |  |  | | --- | --- | | AzureFirewallSubnet | 10.166.4.0/26 | | AzurePrivateEndpoint | 10.166.4.192/27 | | AzureBastionSubnet | 10.166.5.0/26 | | sub-iaas | 10.166.4.64/27 | | sub-paas | 10.166.4.128/27 | | Core Network Hub |
| Core | | identity | ave-sea-cor-vnt-10.166.8.0 | |  |  | | --- | --- | | ave-sea-cor-sub-identity | 10.166.8.0/25 | | AzurePrivateEndpoint | 10.166.8.128/27 | | Identity  Workload |
| Core | | management | ave-sea-cor-vnt-10.166.9.0 | |  |  | | --- | --- | | ave-sea-cor-sub-management | 10.166.9.0/25 | | AzurePrivateEndpoint | 10.166.9.128/27 | | Management  Workload |
| Core | | automation | ave-sea-cor-vnt-10.166.10.0 | |  |  | | --- | --- | | ave-sea-cor-sub-automation | 10.166.10.0/25 | | AzurePrivateEndpoint | 10.166.10.128/27 | | Automation  E.g., DevOPS Agent |
| Core | | security | ave-sea-cor-vnt-10.166.11.0 | |  |  | | --- | --- | | ave-usw2-cor-sub-sec | 10.166.11.0/25 | | AzurePrivateEndpoint | 10.166.11.128/27 | | Security Azure  Defender, Log Analytic  Workspace |
| Landing Zone | | Production | ave-sea-prd-vnt-10.166.12.0 | |  |  | | --- | --- | | sub-paas | 10.166.12.0/24 | | sub-iaas | 10.166.13.0/24 | | AzurePrivateEndpoint | 10.166.14.0/26 | | Dedicated Databricks host subnet | 10.166.15.0/25 | | Dedicated Databricks container subnet | 10.166.15.128/25 | | Production Workload |
| Landing Zone | | Development | ave-sea-dev-vnt-10.166.16.0 | |  |  | | --- | --- | | sub-paas | 10.166.16.0/24 | | sub-iaas | 10.166.17.0/24 | | AzurePrivateEndpoint | 10.166.18.0/26 | | Dedicated Databricks host subnet | 10.166.19.0/25 | | Dedicated Databricks container subnet | 10.166.19.128/25 | | Development  Workload |
| Landing Zone | | QA | ave-sea-qa-vnt-10.166.20.0 | |  |  | | --- | --- | | sub-paas | 10.166.20.0/24 | | sub-iaas | 10.166.21.0/24 | | AzurePrivateEndpoint | 10.166.22.0/26 | | Dedicated Databricks host subnet | 10.166.23.0/25 | | Dedicated Databricks container subnet | 10.166.23.128/25 | | QA Workload |
| Landing Zone | | PreProduction | ave-sea-pprd-vnt-10.166.24.0 | |  |  | | --- | --- | | sub-paas | 10.166.24.0/24 | | sub-iaas | 10.166.25.0/24 | | AzurePrivateEndpoint | 10.166.26.0/26 | | Dedicated Databricks host subnet | 10.166.27.0/25 | | Dedicated Databricks container subnet | 10.166.27.128/25 | | Pre-Production  Workload |

Table 9 Address Space and Subnets

Design Pattern: Name Resolution (DNS)

The following topology is the Microsoft recommendation for name resolution. It is also a resilient architecture as Azure resources will still be able to resolve.

Diagram

Description automatically generated

Figure 6: DNS resolution topology

The following table describes key aspects of option Number

|  |  |
| --- | --- |
| S.no | Description |
| 1 | IHH DNS Server |
| 2 | Set DNS Zone Conditional Forwarder from IHH to AVE Health SG Vice Versa |
| 3 | Ave Health SG Az Platform standalone/bind DNS IaaS servers |
| 4 | Ave Health SG Az Platform standalone /bind DNS IaaS Servers will have a forwarder configured to 168.63.129.16. |
| 5 | Virtual Network in Identity Subscription will be linked to Private DNS private zone. |
| 6 | All the spoke VNET DNS will set to custom DNS set the IP addresses of the primary and secondary IaaS hosted DNS servers in the Identity subscription. This provides resolution to Azure based resources to Azure based resources. |

Table 10: DNS resolution topology description

|  |  |  |  |
| --- | --- | --- | --- |
| Subscription | Server | IP Address | Comments |
| TBD | TBD | TBD | TBD |
| TBD | TBD | TBD | TBD |
| TBD | TBD | TBD | TBD |
| TBD | TBD | TBD | TBD |
| TBD | TBD | TBD | TBD |
| TBD | TBD | TBD | TBD |

Native security services

**Native security services**

* DDoS (Standard) protection for Public Ips – to be implemented in the connectivity VNET and extended to all the spoke VNETS.
* Azure Firewall (Standard SKU) —Full VNET egress and ingress (http and https) protection – to be implemented in the connectivity subscription as the central point of network routing and filtering device.
* NSG—Internal VNET segmentation based on policy configurations. – to eb associated with subnets to provide mechanism to filter ports based upon the application needs.
* Azure Bastion Service – Secure Remote Access – to be implemented to provide mechanism to securely manage VMs from browser.
* Service endpoints/Private Link—Secure access to public PaaS resources – to be created based upon the PaaS components needed by application to securely access them without sending traffic over internet.

Network Components Design

Any application specific requirements which include Azure Load Balancers and Application Gateway or WAF will be covered in the workload onboarding planning document for supporting application/workload adoption.

Policy Management

Technical Overview

Azure Policy is a service in Azure that is used to create, assign, and manage policies which enforce different rules and effects over Azure resources, so that the resources stay compliant.

Azure Policy will help AVE Health SG ensure that the Azure environment conforms with their specified design, regulatory, and security requirements. It will help evaluate Azure resources for non-compliance with assigned policies. For example, a policy to allow creation of new resources only in Southeast Asia and no new resources in any other region and will mark existing resources in any other region as non-compliant.

There are several built-in policies in Azure. A collection of policies is called an ‘Initiative’. A built-in initiative called ‘Enable Monitoring in Azure Security Centre’ is automatically assigned to every Subscription with a goal to monitor all the available security recommendations in Azure Security Centre.

Several other built-in Initiatives are also available to follow various regulatory requirements, including:

Azure Security Benchmark v.3 – which encompasses both the CIS 7.1 and NIST-800-53r4 standards.

Policies can be used for a variety of use cases, such as:

* Regulatory compliance
  + Ensure compliance to defined standards, as described above.
* Security
  + RBAC role assignment.
  + Key Vault certificate.
* Inventory management
  + Require specified tag.
  + Add or replace tag.
* Cost management
  + Define allowed VM or Storage SKUs.

A policy can be assigned at a specific scope,it can be aManagement Group, a Subscription, or a Resource Group. Policy assignments are inherited by all child resources. This design means that a policy applied to a Resource Group is also applicable to resources in that Resource Group. However, there is flexibility to exclude a sub-scope from the policy assignment. For example, at the Subscription scope, a policy can be assigned that prevents the creation of networking resources. A Resource Group could be excluded in that Subscription that is intended for networking infrastructure. Then access can be granted to this networking Resource Group to users that are trusted with creating networking resources.

There are six effects that are supported in a policy definition:

* Disabled: This effect is useful for testing situations or for when the policy definition has parameterized the effect. This flexibility makes it possible to disable a single assignment instead of disabling all that policy's assignments.
* Append: Append is used to add additional fields to the requested resource during creation or update. For example, adding tags on resources such as ‘Cost Center’ or specifying allowed IPs for a storage resource.
* Deny: Deny is used to prevent a resource request that doesn't match defined standards through a policy definition and fails the request.
* Audit: Audit is used to create a warning event in the activity log when evaluating a non-compliant resource, but it doesn't stop the request.
* AuditIfNotExists: AuditIfNotExists enables auditing on resources that match the ‘if’ condition but doesn't have the components specified in the details of the ‘then’ condition.
* DeployIfNotExists: DeployIfNotExists executes a template deployment when the condition is met.

These are evaluated in the following order:

Graphical user interface, diagram, application

Description automatically generated

Figure 8: Evaluation order flow diagram for the different policy conditions

Design Considerations and Requirements

|  |  |
| --- | --- |
| No | Design Requirements |
| 1 | Through policy-driven management, AVE Health SG policy implementation will ensure new Azure subscriptions and resources will immediately be brought to their target compliant state. |
| 2 | Default initiative ‘Enable Monitoring in Azure Defender/Azure Security Center’ will be assigned to all Subscriptions to ensure compliance. |
| 3 | Azure Policy will be used to enforce compliance across all Azure subscriptions. The following Azure Policy initiatives will be applied:  Azure Security Benchmark v3 (Azure Security Center baseline) |
| 4 | Management Group and Subscriptions hierarchy will be considered when assigning Policies.  • Relevant policies will be assined at the top-level root management group so that they can be assigned at inherited scopes.  • In general, policy assignments will be managed at the highest appropriate level with exclusions at bottom levels, if required. |
| 5 | Enterprise Scale recommended policies should be applied and complemented by other policies/initiatives which will help AVE Health SG meet their internal security policies. |

Table 11: Requirements and Considerations - Azure Policy

Design Decisions

The following table documents the policies that will be implemented along with the default Initiative:

|  |  |  |
| --- | --- | --- |
| PolicyName | Scope | Note |
| Enforce Monitoring in Azure Security Centre | Root |  |
| Enforce Azure Security Monitoring | Root |  |
| Enforce Azure Security Center alerts | Root |  |
| Enforce audit of KeyVault | Root |  |
| Enforce Subscription tags | Root |  |
| Azure Security Benchmark V3 | Root |  |
| Allowed regions for Resource Groups and resource | Root |  |
| Network interfaces should not have public Ips (Exemption Network Subscription) | Root |  |
| SSH access from the Internet should be blocked (Exemption Network) | Root |  |
| RDP access from the Internet should be blocked (3389) | Root |  |
| Enable Azure Monitor for VMs+ Auto-provision agent in VMs within ASC | Root |  |
| Secure transfer to storage accounts should be enabled | Root |  |
| Enforce NSG on every Subnet (Default NSG will be created and applied at subnets) | Root |  |
| Enforce UDR on Virtual Network injected services Subnet | Root |  |
| Add Virtual Network to Azure DDoS Protection (Standard Version) in Network Subscription | Root |  |
| Deny IP forwarding on NIC (Exemption is Network Management Sub/Server Appliance deployed) | Root |  |
| Enforce diagnostics/metrics to platform workspace  Deploy Diagnostic setting for Automation to Log Analytics Workspace  Deploy Diagnostic setting for containers to Log Analytics Workspace  Deploy Diagnostic setting for Container Registry to Log Analytics Workspace  Deploy Diagnostic setting for Analysis Services to Log Analytics Workspace  Deploy Diagnostic setting for API Management to Log Analytics Workspace  Deploy Diagnostic setting for Application Gateway to Log Analytics Workspace  Deploy Diagnostic setting for CDN Endpoint to Log Analytics Workspace  Deploy Diagnostic setting for cognitive Services to Log Analytics Workspace  Deploy Diagnostic setting for Cosmos DB to Log Analytics Workspace  Deploy Diagnostic setting for Databricks to Log Analytics Workspace  Deploy Diagnostic setting for Azure Data Explorer Cluster to Log Analytics Workspace  Deploy Diagnostic setting for Azure Data Factory to Log Analytics Workspace  Deploy Diagnostic setting for Azure Data Lake to Log Analytics Workspace  Deploy Diagnostic setting for Event Grid to Log Analytics Workspace  Deploy Diagnostic setting for Azure Firewall to Log Analytics Workspace  Deploy Diagnostic setting for Azure Frontdoor to Log Analytics Workspace  Deploy Diagnostic setting for Azure Function to Log Analytics Workspace  Deploy Diagnostic setting for HDinsight to Log Analytics Workspace  Deploy Diagnostic setting for load balancer to Log Analytics Workspace  Deploy Diagnostic setting for logic apps integration to Log Analytics Workspace  Deploy Diagnostic setting for Azure Media Service to Log Analytics Workspace  Deploy Diagnostic setting for MariaDB to Log Analytics Workspace  Deploy Diagnostic setting for Network Security Groups to Log Analytics Workspace  Deploy Diagnostic setting for Network Interface to Log Analytics Workspace  Deploy Diagnostic setting for Database PostgreSQL to Log Analytics Workspace  Deploy Diagnostic setting for Power BI Embedded to Log Analytics Workspace  Deploy Diagnostic setting for Redis Cache to Log Analytics Workspace  Deploy Diagnostic setting for relay to Log Analytics Workspace  Deploy Diagnostic setting for SignalR to Log Analytics Workspace  Deploy Diagnostic setting for SQL Elastic Pools to Log Analytics Workspace  Deploy Diagnostic setting for SQL Managed Instance to Log Analytics Workspace  Deploy Diagnostic setting for Virtual Network to Log Analytics Workspace  Deploy Diagnostic setting for Virtual Machine to Log Analytics Workspace  Deploy Diagnostic setting for Virtual Machine Scaliest to Log Analytics Workspace  Deploy Diagnostic setting for Virtual Network Gateway to Log Analytics Workspace  Deploy Diagnostic setting for VPN Gateway to Log Analytics Workspace  Deploy Diagnostic setting for App Service Plan to Log Analytics Workspace  Deploy Diagnostic setting for Azure Firewall Manager Policy to Log Analytics Workspace  Restrict Classic ServicesAll | Root |  |
| Allowed Virtual Machine Image (Optional) | Root |  |
| Https only on App Services | Root |  |
| Keyvault soft delete should be enabled. | Root |  |
| Web Application should be accessible over HTTPS. | Root |  |
| Deny the Creation of private DNS. | Root |  |
| Deny the creation of public IP (Exemption Network) | Root |  |
| RDP Access from the Internet should be blocked. | Root |  |
| SHH Access from the internet should be blocked. | Root |  |
| Azure SQL Database should have the minimal TLS Version set to the highest version. | Root |  |
| Storage Account set to minimum TLS and secure transfer should be enabled. | Root |  |
| Subnet should have a network security group. | Root |  |
| Subnet should have a user defined route. | Root |  |
| Deploy DDOS Protection Standard Plan | Root |  |

Table 12: Design Decisions - Azure Policy

Further restrictions can be applied at the Business Entities management group or subscription level, or Resource Group as required.

Prod and Prod/NonProd (QA, Dev, PreProd) Log Analytic workspace are different therefore many policies above must be created twice to attach them with appropriate decisions. For example, Diagnostic logs of Prod Key Vault will be sent to Prod LA and likewise Pre/NonProd Key Vault logs will be sent to Pre/NonProd LA.

Platform Automation and DevOps

Requirements

|  |  |
| --- | --- |
| ID | Description |
| RQ-01 | Adopt and apply governance DevOps across application landscape to promote consistency and security for deployed services |
| RQ-02 | Use automation to enhance predictability with operations for teams and administrators |
| RQ-03 | Increase overall team efficiencies |
| RQ-04 | Leverage infrastructure as code to mitigate “drift” of deployed services |
| RQ-05 | Increase collaboration, implement code, and best practices sharing across teams. |
| RQ-06 | Incorporate automated security scanning to enhance overall system security posture and provide development teams guidance to creating secure applications |
| RQ-07 | Track work using Azure Boards and implement an Agile methodology using Scrum |
| RQ-08 | Use Azure DevOps Wiki for documentation management of project-specific content. |
| RQ-09 | Incorporate best practices around coded reviews and implement branch policies that enable control over code merge operations |
| RQ-10 | Approach automated deployment of services in a Secure by Default fashion ensuring sensitive data is not revealed unnecessarily |
| RQ-11 | Incorporate the use of Application Insights to fulfill Application Performance Monitoring needs |

Design Recommendations

|  |  |
| --- | --- |
| ID | Description |
| DR-01 | Azure DevOps should be used to manage backlog items, execute builds and pipelines, and store/track source code |
| DR-02 | Infrastructure should be defined as modules and stored in a separate repository managed in a centralized way |
| DR-03 | YAML multi-stage pipelines should be used to represent the entire flow of build and release of infrastructure and application components |
| DR-04 | Azure Policies should be used to enforce patterns and governance. Policy definitions will be stored in a separate repository |
| DR-05 | All code should join respective trunks only after being reviewed by a peer |
| DR-06 | Pipelines should use dedicated Service Connections for production subscriptions. Non-production subscriptions can be shared by Service Principal. |
| DR-07 | Linting tools should be used for infrastructure scripts to ensure conformance to the standards set forth by Ave health |

Design Considerations

|  |  |
| --- | --- |
| ID | Description |
| DC1 | Avehealth team will reuse the pipelines and code to deploy to other tenants. (other Hospitals) |
| DC2 | The Repo Structure and pipelines to be more reusable and user friendly. |
| DC3 | Documentation on the usage of pipelines and source code for templates needs to be clear and in detail to enable avehealth team. |

Design Decisions

|  |  |
| --- | --- |
| ID | Description |
| DD-01 | Ave health will leverage Bicep scripts written in a module first fashion to represent infrastructure. These scripts should be templatized to encourage repeat and idempotency |
| DD-02 | Ave health will use Azure DevOps for source management tool, work item tracking pipeline execution tool |
| DD-03 | Ave health will use the infrastructure-as-Code (IaC) approach where possible through Azure DevOps. As a part of the build solution, scripts will be written to maximize reuse |
| DD-04 | Ave health will start off using the Managed Azure DevOps build agents. Self-hosted agents will be deployed if Managed instances cannot fulfill needs of Ave health.  Update: Self-Hosted Agents to be deployed in order to support data Pipelines and also the implementation of private endpoints. |
| DD-05 | Ave health will not use Bicep scripts to deploy subscriptions or management groups. Deployment will be manual and could use Azure Blueprints. |
| DD-06 | Ave health will segregate environments by using subscriptions. Each environment will have a dedicated service principal. |
| DD-07 | Ave health will use Bicep linter to ensure all Bicep scripts comply with agreed upon standards and guidelines |
| DD-08 | Ave health will use **main** as the *trunk* for source control and protect it with specific branch policies and require pull requests before code is allowed be merged |
| DD-09 | Teams will leverage a Trunk-based development model within Git repos for building Hub and Spoke components and pipeline |

Design Pattern: Landing Zone Release (LZR)

#### 2.5.5.1 Service Principal and Management Group Design

As Shown below the intent is to create 10 service principals each with “Contributor” and “User Access Administrator” This way we can keep the isolation of subscriptions and RBAC respectively isolated to the management groups.

Chart, scatter chart, box and whisker chart

Description automatically generated  
Figure: Management Group and Service Principal Structure

#### 2.5.5.2 Understanding Module First Infrastructure as Code

Infrastructure as Code (IaC) provides two principal benefits for teams:

1. It allows definitions for infrastructure to be defined and versioned in code. This allows changes to be reviewed in the same way that code changes are reviewed. Strict enforcement of GitOps principles also minimizes potential drift and offers an easy to correct drift.
2. It allows infrastructure definitions to be codified into modules and shared between teams. In effect, this allows centralization of definition that promotes tighter control over resources deployed. This can ensure not just that resources are deployed consistently and are immediately conformant to organizational needs but, it can mitigate the risk of resources being deployed incorrectly potentially create security attack vectors.

For Ave health, the value of going module-first is tremendous due to the relative inexperience of the team regarding large scale cloud application maintenance. The process provided by Microsoft will leverage Azure DevOps as the central drop point for Bicep modules.

Diagram

Description automatically generated

The goal with this approach is to give, by the end, Ave health a suite of modules that can aid in deploying additional resources in a controlled, secure, and repeatable way. This allows teams to better leverage the cloud without having to understand all of the nuances of the services being used.

Using Artifacts will allow intuitive versioning, each time a new change is made and published this is published as a new version to the existing artifact in the feed. This enables us to use the most stable version while deploying and also parallelly work on the development of a new version.

#### 2.5.5.3 Landing Zone Level Based Deployment.

##### Level 0 Landing Zone Deployment.

Azure landing zones are the output of a multi-subscription Azure environment that accounts for scale, security, governance, networking, and identity. Azure landing zones enable application migration, modernization, and innovation at enterprise-scale in Azure.

Launchpad and level0 are deployed manually from the console to seed the environment, but all higher levels are deployed using pipelines as defined by the pipelines configuration.

Level 0 consists of Prerequisite to start the build process, i.e. it is the transition from manual to automation.

1. Creating Service Principals : Service principals at each level above mentioned need to be created manually.
2. Creating service connections: Service Connections on Azure DevOps Needs to be created with the above service principals.
3. Creating management groups: Management Groups on Azure Tenant need to be created to represent the MG structure mentioned in section 2.2.1.
4. Azure DevOps Integration: Creation if Repos to host the source code, Create Artifact feed to store template artifacts. Setup Microsoft hosted agent.
5. RBAC assignments: Assign Permissions to MCS team and Service Principals.
6. Azure Key Vaults: Deploy Key vaults to store the Secrets, one in each subscriptions.
7. Tags: Decide on the tags and Assign tags to all resources being deployed.

##### Level 1 Landing Zone Deployment.

Level 1: Core security, Governance and Accounting

Level 1 is responsible for Role Based Access Control (RBAC) enforcement of the subscriptions, subscription behavior configuration using Azure Management groups. Azure Policies ensures deployment of preventive and reactive controls. This level is also in charge of deploying the fundamental configuration for Azure Monitor and Log analytics & shared security services.

1. Log Analytics Workspaces.
2. Mapping existing subscription groups to Management groups.
3. Role definitions/ custom roles (if any).
4. Diagnostics profile.
5. Policies at root.

##### Level 2 Landing Zone Deployment.

Level 2: Shared services/Networking

Shared services include each environment's core networking components (using hub and spoke or any other network topology).

1. Networking Hub.
2. Egress/ Ingress DMZ.
3. Transit Vnet.
4. Hub and Spoke - networking.
5. Public/ Private DNS.
6. Backup and DR.

As part of Level 2 Deployment of Various Networking Resources is to be completed,  
Which may contain but not only limited to:

Azure bastions, Firewall, DDOS plan, Vhub, Vwan, Private Endpoints, S2S and P2S vpns,  
VPN Gateways, Subnets, Virtual networks, Public/Private Dns Zones, Vnet Peerings.

##### Level 3 Landing Zone Deployment.

Level 3 : Application Infrastructure

Level 3 consists of Application Infrastructure. I.e all the Services/resources on azure on which the application is to be hosted, in our case the data related services used by the Data team.

1. Application Subscriptions.
2. SQL Databases
3. Azure Synapse.

#### 2.5.5.4 Deployment Methodology

The Deployment to the landing zones has been designed keep reusability and ease of use in mind,

1. We have 3 Repositories created in the [AveHealth Platform](https://dev.azure.com/AveHealth/AveHealth%20Platform):

* Landing Zone: Used to deploy resources to various subscriptions.
* Shared Components: Used to store the source code for the templates of resources   
  used in the deployment, this source code is packed and published as an artifact that can be reused across the project.
* Azure Policies: This Repository is used to Deploy Policies to the Management groups and the subscriptions.

2. With the help of the above three repositories we deploy to the various subscriptions,  
Under the landing zone repository, we have created the Folder structure to reperesent the various parts of the project the Data and ACF workloads, this may change as we intend to merge a lot of the code as the project progresses.  
  
We have created two pipelines for the deployment of the resources,

* Hub-Pipeline
* Spoke Deployment-Pipeline

The Hub Deployment pipeline is intended to deploy resources into the **ave-cor-network** Subscription, as there is no explicit need to parameterize the deployment of a hub, only one hub exists per tenant.

The Spoke Deployment pipeline takes the subscription name as a parameter, which is used to determine the environment and the service connection to be used for the deployment to the spoke, the way we have created the folder structure In the landing zone repo also plays an important part here as the name of the subscription is also the name of the folder that houses pipelines, templates for the deployment of resources which are not common across all the other subscriptions, and also the parameters for the resources to be deployed with the Spoke Deployment-Pipeline.  
  
Folder Structure in Repositories:  
A picture containing graphical user interface

Description automatically generated A picture containing table

Description automatically generated Background pattern

Description automatically generated with low confidence

Spoke Deployment Pipeline Taking Subscription Name as parameter.

Graphical user interface, text, application, email

Description automatically generated

The folder Structure of pipelines is below.

Graphical user interface, text, application

Description automatically generated

Platform Management and Monitoring

Introduction

Azure Naming Convention

Technical Overview

Applying well-defined naming and metadata tagging convention are ways to aid operational management and support accounting requirements. A naming and tagging strategy include business and operational details as components of resource names and metadata tags:

* The business side of this strategy ensures that resource names and tags include the organizational information that's needed to identify the teams.
* The operational side ensures that names and tags include information that IT teams can use to identify the workload, application, environment, criticality, and other information useful for managing resources.
* An effective naming convention assembles resource names by using important resource information as parts of its name.

Requirements

The chosen naming convention is based on the following requirements:

|  |
| --- |
| Requirement |
| All Azure resources must have a unique name within the AVE Health SG organization. |

Table 13: Requirements and Considerations - Azure Naming Convention

Design Decisions

The following table documents the design decisions related to naming conventions.

|  |  |  |
| --- | --- | --- |
| Assert Type | Format and Example | Comments |
| Subscriptions | ave-cor-network  ave-cor-identity  ave-cor-management  ave-cor-security  ave-dev-workload  ave-prd-workload | Subscription Naming Standard [AVE]-AVE Health SG,[COR]-Core Platform or Environment Type [PRD/QA/DEV/Pre Prod] -Workload/Landing zone Type |
| Resource Group | ave-sea-prd-arg-001,  ave-sea-npe-arg-001  ave-sea-cor-arg-001,  ave-sea-cor-arg-002  ave-sea-cor-arg-fw-001  ave-sea-cor-arg-vwan-001  ave-sea-cor-arg-fwp-001  ave-sea-cor-arg-app-001 | Resource Group Naming Standard [AVE]-AVE Health SG,[SEA]-Azure Region/Location, [COR]- or [PRD/QA/DEV/Pre Prod] Core Platform or Environment Type -Workload/Landing zone Type,[arg] – Azure Resource Group,[Fw/vWAN] – Azure Resource will deployed e.g Azure Firewall or Azure Virtual WAN. [001] – instance number  [Abbreviations for Azure resource types](https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-best-practices/resource-abbreviations) |
| Resources | IP Address (prod) - ave-sea-prd-pip-001  Keyvault (prod) - ave-sea-prd-akv-001  VNet (non-prod) - ave-sea-pprd-vnt-001  StorageAccount(core) - aveseacorsta003  AppGateWay (non-prod) - ave-sea-npe-agw-002 |  |
| Virtual Machine Name | VM Name (non-prod) - msea0wnapweb001  VM Name (prod) - msea0lptrexx001 | VM Naming Standard [M]-Cloud Provider,[SEA]-Region,[0-3]availablityZone,[L/W]-OS,[P/D/N]-Environment,[ADCDE]-Role,[000]-Increament |

Table 14: Design Decisions - Azure Naming Convention

Azure Role Based Access Control

ARM (Azure Resource Manager) provides a granular Role-Based Access Control (RBAC) model for assigning administrative privileges at the resource level. Under Resource Manager, RBAC currently has over 130 in-built roles available out of the box.

Reference**:**

The following link provides more information on the RBAC roles currently available within Azure: <https://docs.microsoft.com/en-us/azure/active-directory/role-based-access-built-in-roles>

|  |  |  |
| --- | --- | --- |
| General Ave Health Roles | Roles | Description |
|  | [Owner](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#owner) | Grants full access to manage all resources, including the ability to assign roles in Azure RBAC. |
| Platform Engineer/ Infra Engineer | [Contributor](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#contributor) | Grants full access to manage all resources but does not allow you to assign roles in Azure RBAC, manage assignments in Azure Blueprints, or share image galleries. |
|  | [Reader](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#reader) | View all resources but does not allow you to make any changes. |
| Security IAM Officer | [User Access Administrator](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#user-access-administrator) | Manage user access to Azure resources. |
| Platform Engineer/ Infra Engineer | [Virtual Machine Administrator Login](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#virtual-machine-administrator-login) | View Virtual Machines in the portal and login as administrator |
| Platform Engineer/ Infra Engineer | [Virtual Machine Contributor](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#virtual-machine-contributor) | Create and manage virtual machines, manage disks and disk snapshots, install and run software, reset password of the root user of the virtual machine using VM extensions, and manage local user accounts using VM extensions. This role does not grant you management access to the virtual network or storage account the virtual machines are connected to. This role does not allow you to assign roles in Azure RBAC. |
| Network Engineer | [Network Contributor](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#network-contributor) | Manage networks, but not access to them. |
| Backup Operator | [Backup Contributor](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#backup-contributor) | Manage backup service, but can't create vaults and give access to others |
| Backup Operator | [Backup Operator](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#backup-operator) | Manage backup services, except removal of backup, vault creation and giving access to others |
| Backup Operator | [Backup Reader](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#backup-reader) | Can view backup services, but can't make changes |
| Security Officer | [Log Analytics Contributor](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#log-analytics-contributor) | Log Analytics Contributor can read all monitoring data and edit monitoring settings. Editing monitoring settings includes adding the VM extension to VMs; reading storage account keys to be able to configure collection of logs from Azure Storage; adding solutions; and configuring Azure diagnostics on all Azure resources. |
| Security Officer | [Log Analytics Reader](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#log-analytics-reader) | Log Analytics Reader can view and search all monitoring data as well as and view monitoring settings, including viewing the configuration of Azure diagnostics on all Azure resources. |
| Security IAM Officer | [Managed Identity Contributor](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#managed-identity-contributor) | Create, Read, Update, and Delete User Assigned Identity |
| Security IAM Officer | [Managed Identity Operator](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#managed-identity-operator) | Read and Assign User Assigned Identity |
| Security Officer | [Azure Sentinel Contributor](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#azure-sentinel-contributor) | Azure Sentinel Contributor |
| Security Officer | [Azure Sentinel Reader](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#azure-sentinel-reader) | Azure Sentinel Reader |
| Security Officer | [Azure Sentinel Responder](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#azure-sentinel-responder) | Azure Sentinel Responder |
| Security Officer | [Key Vault Administrator](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#key-vault-administrator) | Perform all data plane operations on a key vault and all objects in it, including certificates, keys, and secrets. Cannot manage key vault resources or manage role assignments. Only works for key vaults that use the 'Azure role-based access control' permission model. |
| Security Officer | [Key Vault Contributor](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#key-vault-contributor) | Manage key vaults, but does not allow you to assign roles in Azure RBAC, and does not allow you to access secrets, keys, or certificates. |
| Security Officer | [Key Vault Reader](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#key-vault-reader) | Read metadata of key vaults and its certificates, keys, and secrets. Cannot read sensitive values such as secret contents or key material. Only works for key vaults that use the 'Azure role-based access control' permission model. |
| Security Officer | [Security Admin](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#security-admin) | View and update permissions for Security Center. Same permissions as the Security Reader role and can also update the security policy and dismiss alerts and recommendations. |
| Security Officer | [Security Assessment Contributor](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#security-assessment-contributor) | Push assessments to Security Center |
| Security Officer | [Security Reader](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#security-reader) | View permissions for Security Center. Can view recommendations, alerts, a security policy, and security states, but cannot make changes. |
| Security Officer | [Monitoring Contributor](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#monitoring-contributor) | Can read all monitoring data and edit monitoring settings. |
| Security Officer | [Monitoring Reader](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#monitoring-reader) | Can read all monitoring data (metrics, logs, etc.). |
| Security Officer | [Workbook Contributor](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#workbook-contributor) | Can save shared workbooks. |
| Security Officer | [Workbook Reader](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#workbook-reader) | Can read workbooks. |
| Cost Manager + Asset Manager | [Billing Reader](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#billing-reader) | Allows read access to billing data |
| Cost Manager + Asset Manager | [Cost Management Contributor](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#cost-management-contributor) | Can view costs and manage cost configuration (e.g. budgets, exports) |
| Cost Manager + Asset Manager | [Cost Management Reader](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#cost-management-reader) | Can view cost data and configuration (e.g. budgets, exports) |
| Platform Engineer/ Infra Engineer | [Site Recovery Contributor](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#site-recovery-contributor) | Manage Site Recovery service except vault creation and role assignment |
| Platform Engineer/ Infra Engineer | [Site Recovery Operator](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#site-recovery-operator) | Failover and failback but not perform other Site Recovery management operations |
| Platform Engineer/ Infra Engineer | [Site Recovery Reader](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#site-recovery-reader) | View Site Recovery status but not perform other management operations |
| Security Officer | [Tag Contributor](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#tag-contributor) | Manage tags on entities, without providing access to the entities themselves. |
| Endpoint Manager | [Intune Service Administrator](https://docs.microsoft.com/en-us/mem/intune/fundamentals/role-based-access-control) | Manages custom Intune roles and adds assignments for built-in Intune roles. It's the only Intune role that can assign permissions to Administrators. |

Table 15: Mapping of RBAC Roles

Design Decision - RBAC

The following RBAC roles will be implemented in AVE HEALTH SG Azure Platform.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Roles | Description | Group Name | Level | MG name or Subscription Name | Permanent Assignment or PIM |
| [Owner](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#owner) | Grants full access to manage all resources, including the ability to assign roles in Azure RBAC. | OWNER\_ROOT | Root Management | avesgroot-mg | PIM |
| [User Access Administrator](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#user-access-administrator) | Let’s you manage user access to Azure resources. | USER\_ACCESS\_ADMINISTRATOR\_ROOT | Root Management | avesgroot-mg | PIM |
| [Managed Identity Contributor](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#managed-identity-contributor) | Create, Read, Update, and Delete User Assigned Identity | MANAGED\_IDENTITY\_CONTRIBUTOR\_ROOT | Root Management | avesgroot-mg | PIM |
| [Key Vault Administrator](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#key-vault-administrator) | Perform all data plane operations on a key vault and all objects in it, including certificates, keys, and secrets. Cannot manage key vault resources or manage role assignments. Only works for key vaults that use the 'Azure role-based access control' permission model. | KEY\_VAULT\_ADMINISTRATOR\_ROOT | Root Management | avesgroot-mg | PIM |
| [Security Reader](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#security-reader) | View permissions for Security Center. Can view recommendations, alerts, a security policy, and security states, but cannot make changes. | SECURITY\_READER\_ROOT | Root Management | avesgroot-mg | Permanent |
| [Billing Reader](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#billing-reader) | Allows read access to billing data | BILLING\_READER\_ROOT | Root Management | avesgroot-mg | Permanent |
| [Site Recovery Reader](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#site-recovery-reader) | Lets you view Site Recovery status but not perform other management operations | SITE\_RECOVERY\_READER\_ROOT | Root Management | avesgroot-mg | Permanent |
| [Network Contributor](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#network-contributor) | Lets you manage networks, but not access to them. | NETWORK\_CONTRIBUTOR\_SUB\_NETWORK | Subscription | ave-cor-network | PIM |
| [Log Analytics Contributor](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#log-analytics-contributor) | Log Analytics Contributor can read all monitoring data and edit monitoring settings. Editing monitoring settings includes adding the VM extension to VMs; reading storage account keys to be able to configure collection of logs from Azure Storage; adding solutions; and configuring Azure diagnostics on all Azure resources. | LOG\_ANALYTICS\_CONTRIBUTOR\_SUB\_MANAGEMENT | Subscription | ave-cor-management | PIM |
| [Log Analytics Contributor](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#log-analytics-contributor) | Log Analytics Contributor can read all monitoring data and edit monitoring settings. Editing monitoring settings includes adding the VM extension to VMs; reading storage account keys to be able to configure collection of logs from Azure Storage; adding solutions; and configuring Azure diagnostics on all Azure resources. | LOG\_ANALYTICS\_CONTRIBUTOR\_SUB\_SECURITY | Subscription | ave-cor-security | PIM |
| Security Admin | View and update permissions for Security Center. Same permissions as the Security Reader role and can also update the security policy and dismiss alerts and recommendations. | SECURITY\_ADMIN\_SUB\_SECURITY | Subscription | ave-cor-security | PIM |

Table 16: RBAC Design Decisions

Azure Tags

Technical Overview

Azure includes a tagging feature that facilitates resource categorization by logically organizing them into a taxonomy. Tags are metadata elements attached to resources. Each tag consists of a name and a value pair.

The application of a consistent set of global tags, as part of a comprehensive naming and tagging policy, is a critical part of an overall management and governance strategy.

Tags may be placed on a resource at the time of creation or added to an existing resource. After tags are applied, all the resources can be retrieved with that tag name and value. Tags applied to the resource group are not inherited by the resources in that resource group.

Design Decisions

The chosen Tagging strategy is based on the following requirement:

|  |
| --- |
| Design Decisions |
| Define necessary Tags relevant to AveHealth and support the Cloud operation. |

Table 17: Design Decisions - Azure Tags

|  |  |  |  |
| --- | --- | --- | --- |
| Tag | Enforced | Tag Description |  |
| BusinessUnit | optional | Top-level division of your company that owns the workload | Refer the design decision tracker for more details |
| Env | yes | Deployment environment of the application, workload, or service. | Refer the design decision tracker for more details |
| SolutionName | yes | Name of the associated solution, service, or workload associated with the resource. | Refer the design decision tracker for more details |
| Owner | yes | Owner of the application, workload, or service. | Refer the design decision tracker for more details |
| Secondary | optional | Secondary owner of the application, workload, or service. | Refer the design decision tracker for more details |
| CostCentre | yes | Accounting cost centre associated with this resource. | Refer the design decision tracker for more details |
| SupportDL | yes | Support team’s contact email/distribution list | Refer the design decision tracker for more details |
| Landscapetype | Yes - TBD | Defines if the landscape hosts a dedicated product/service or is shared with multiple products/services/teams | Refer the design decision tracker for more details |
| RequestID | optional | ServiceNow request ID for the account / subscription | Refer the design decision tracker for more details |
| AppEnv | optional | Deployment environment of the application, workload, or service that doesn’t meet the above general environment types | Refer the design decision tracker for more details |
| PurchaseOrder | optional | Accounting Purchase Order associated with the resource. | Refer the design decision tracker for more details |
| GearID | yes | Application ID | Refer the design decision tracker for more details |
| ResourceGroup | yes | Name of Resource Group | Refer the design decision tracker for more details |
| DeploymentType | yes | Defines how the resources are being maintained. | Refer the design decision tracker for more details |
| PlatformBackup | yes | Platform Backup tag | Refer the design decision tracker for more details |
| TTOStatus | Yes - TBD | Completion status of the transition to operation for the landzone | Refer the design decision tracker for more details |
| SupportModel | Yes - TBD | Support model to be used by the landscape after transition to operation | Refer the design decision tracker for more details |
| TTORequest | Yes - TBD | Request number in Service Now for the transition to operations of the landscape | Refer the design decision tracker for more details |
| Department | optional | Assigned to each Resource Group and child resource to identify which department owns the resources. (Line of Business) | Refer the design decision tracker for more details |
| DataClassification | Yes | To allow for identification of workloads that may contain data such as PII or Business Sensitive. | Refer the design decision tracker for more details |
| Criticality | optional | To identify workload SLA requirements. | Refer the design decision tracker for more details |
| Retention | Yes - TBD | For services that allow imaging or snapshots, defines the retention period id days: (0 is no-snapshot/image) | Refer the design decision tracker for more details |
| BackupPolicy | yes | Manual or Policy Based | Refer the design decision tracker for more details |

Table 18: Suggestion for initial tags

Azure Resource Locks

Technical Overview

Azure provides the ability to restrict operations on resources through Locks. RBAC is not sufficient in situations where it is desired for a user to have full access to a resource, but it’s required to prevent inadvertent modification or deletion. Locks can be applied at a Subscription, Resource Group, or resource to prevent users from accidentally deleting or modifying critical resources. The lock level identifies the type of enforcement for the policy, which has two values: Delete and Read-only.

* Delete means authorized users can read and modify resources, but they can't delete any of the restricted resources.
* Read-only means authorized users can only read the resource, but they can't modify or delete any of the restricted resources.

When a Lock is applied at a parent scope, all resources within that scope inherit the same lock. Of the built-in RBAC roles, only **Owner**and**User Access Administrator** can create or delete locks.

Requirements

The chosen Locks strategy is based on the following requirement:

|  |
| --- |
| Requirement(s) |
|  |
| No standard implementation required. Ave Health IT will do it as required on selected components. |

Table 19: Requirements and Considerations - Resource Locks

Design Decisions

The following table documents the design decisions related to resource Locks:

|  |  |  |
| --- | --- | --- |
| Scope | Lock | Reasoning |
| All Subscription | None |  |
| Resource Groups that host  Critical resources  like VPN  Gateway | None | Ave Health IT will enable manually on critical resources like vWAN, Gateway etc. |

Table 20: Design Decisions - Resource Locks

Azure Cost Management

Technical Overview

Azure Cost Management and Billing is a free built-in service accessible via Azure Portal or APIs that provides tools to plan for, monitor, analyze and optimize spending to maximize cloud investment.

Billing

Azure Billing features are used to review invoiced costs and manage access to billing information. A billing account is created when a customer signs up to use Azure. For Cloud Service Provider, a billing account is created when the organization signs with Cloud Service Provider to use Azure. This Cloud Service Provider will manage invoices, payments, and track costs.

Cost Management

Cost Management shows organizational cost and usage patterns with advanced analytics. Reports in Cost Management show the usage-based costs consumed by Azure services and third-party Marketplace offerings. Costs are based on negotiated prices and factor in reservation and Azure Hybrid Benefit discounts. Collectively, the reports show internal and external costs for usage and Azure Marketplace charges. The reports help understand spending and resource use and can help find spending anomalies. Predictive analytics are also available. Cost Management uses Azure management groups, budgets, and recommendations to show clearly how expenses are organized and how costs can be optimized.

Cost Management features that help plan for and control costs include Cost analysis, budgets, recommendations, and exporting cost management data:

* Cost analysis is used to explore and analyze organizational costs. Aggregated costs can be viewed to understand where costs are accrued and to identify spending trends. And accumulated costs can be seen over time to estimate monthly, quarterly, or even yearly cost trends against a budget.
* Budgets help plan for and meet financial accountability in the organization. Budgets help prevent cost thresholds or limits from being surpassed.
* Recommendations show how to optimize and improve efficiency by identifying idle and underutilized resources. Or they can show less expensive resource options.
* If external systems are in use to access or review cost management data, the data can be easily exported from Azure.
* It is also possible to define alerts to be notified if certain budget thresholds are reached.

Azure Advisor

Technical Overview

Azure Advisor is a free service that provides relevant best practices to help improve reliability, security, and performance, achieve operational excellence, and reduce costs. Advisor can be configured to target specific Subscriptions and resource groups, to focus on critical optimizations. Advisor is accessible through the Azure portal, the Azure Command Line Interface (CLI), or the Advisor API if there is a need to integrate it to an existing application landscape. It also integrates natively with Azure Monitor which allows creating alerts to notify automatically about new recommendations.

Azure Advisor runs infrastructure configuration against a growing set of best practices and therefore helps optimize Azure workloads. Examples for recommendations are:

* Showing unused or underutilized VMs (which could be deallocated or deleted to save costs).
* Scaling or resiliency recommendations for VMs and other offers (e.g., listing VMs which are not backed up or not part of an availability set to guarantee availability in case of the primary VM running into an issue).
* VMs with sensitive open ports accessible via the internet (security recommendations are sent to Advisor from Azure Security Center by default).
* Repairing invalid log alert rules.

Design Decisions

The following table documents the design decisions related to Azure Advisor:

|  |
| --- |
| Design Decisions |
| Azure Advisor will be used to optimize Azure resource usage and configuration |
| Utilize Secure Score from Azure Defender/Azure Security Center to manage risk |
| Alert notification on security and non-compliance |

Table 21: Design Decisions - Azure Advisor

Azure Platform Monitoring

Technical Overview

Azure Monitor helps Ave Health maximize the availability and performance of your applications and services. It delivers a comprehensive solution for collecting, analyzing, and acting on telemetry from your cloud and on-premises environments. This information helps you understand how your applications are performing and proactively identify issues affecting them and the resources they depend on.

Ave Health will utilize Azure Monitor features include:

1. Detect and diagnose issues across applications and dependencies with [Application Insights](https://docs.microsoft.com/en-us/azure/azure-monitor/app/app-insights-overview).
2. Correlation of infrastructure issues with [VM insights](https://docs.microsoft.com/en-us/azure/azure-monitor/vm/vminsights-overview), [Network Insights](https://docs.microsoft.com/en-us/azure/azure-monitor/insights/network-insights-overview) and [Container insights](https://docs.microsoft.com/en-us/azure/azure-monitor/containers/container-insights-overview).
3. Review monitoring data with [Log Analytics](https://docs.microsoft.com/en-us/azure/azure-monitor/logs/log-query-overview) for troubleshooting and deep diagnostics.
4. Support operations at scale with [smart alerts](https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-smartgroups-overview) and [automated actions](https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-action-rules).
5. Visualizations with Azure [dashboards](https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/tutorial-logs-dashboards) and [workbooks](https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-overview).
6. Query data from [monitored resources](https://docs.microsoft.com/en-us/azure/azure-monitor/monitor-reference) using [Azure Monitor Metrics](https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/data-platform-metrics).

Design Considerations

|  |  |
| --- | --- |
| ID | Description |
| DC01 | Centralized logging approach for all the resources including VMs, Applications, AKS, and Data services. |
| DC02 | Separate Log Analytics workspace for Security audit logs and Custom sources logs. |
| DC03 | Azure Network insights is needed from different endpoints including Data ingestion pipeline. |
| DC04 | Log retention is default to 30 days and post Interactive retention period logs are needed for 1 year period in archival state. |
| DC05 | Azure Service Map is needed to view Servers connections along with the Processes, Inbound / Outbound connection latency and Ports |
| DC06 | Azure Dashboard and Workbooks are need for VMs, Applications and Data resources performance status. |
| DC07 | 1. Azure Alerts needed for VMs, Applications, Databricks workspace, Synapse Analytics workspace, Key Vaults, AAD. 2. Alert notification can be in the form of email. |
| DC08 | Needs Monitoring capabilities/logs from IHH Tenant resources and want to be monitored centralized place at Ave Health tenant. |

Table 22 Platform Monitoring Design Considerations

Design Decisions

|  |  |
| --- | --- |
| ID | Description |
| DD01 | Ave Health needs a centralized workspace in the Management subscription separately for Prod and Non-Prod [Dev, Test & QA] to collect and store all the resources logs i.e., VMs, Apps, AKS, Data services. |
| DD02 | 1. Ave Health needs a separate workspace for Security Audit logs which will be owned and monitored by the Security Team. 2. Ave Health needs a separate workspace for custom sources logs which come from any VMs, applications running outside Azure infra. |
| DD03 | Ave Health needs Network insights to have visibility on network utilization and performance of resources including Data ingestion pipeline. |
| DD04 | 1. Prod: Ave health needs interactive log retention for 30 days and 1 year for the archival logs in the Storage Account. 2. Non-Prod: Ave health needs interactive log retention for 30 days and 1 year for the archival logs in the Storage Account. |
| DD05 | Predefined Performance Thresholds for Alerts and Notifications  a. CPU Utilization 80% Warning 90% Critical  b. Disk Utilization 70% Alert 80% Warning 90% Critical  c. Memory Utilization 80% Warning 90% Critical  d. Server Up/Down |
| DD06 | Ave Health needs Azure Service Map for the Servers connections along with the Processes, Inbound / Outbound connection latency and Ports in both Prod and Non-Prod environments. |
| DD07 | 1. IHH tenant must have a separate LA workspace configured for all the resources to send logs to it. 2. Need to delegate a permission at IHH Tenant Subscription/RG level for Ave Health tenant users [who are all intended to monitor the IHH tenant resources] through Azure Lighthouse. |
| DD08 | Ave Health needs Azure Dashboards and Workbooks to have visibility on VMs, Applications and Data resources [SQL, Synapse & Databricks] performance in both Prod and Non-prod environments. |
| DD09 | Ave Health needs Azure Alerts for VMs, Applications, Databricks workspace, Synapse Analytics workspace, Key Vaults, AAD in both Prod and Non-prod environments.  Alert notification needs to be in the form of email. |
| DD10 | Preferred log analytics workspace naming as follows for,  Centralized logs,  Prod: ave-sea-cor-prd-log-001  Pre-prod / Non-prod: ave-sea-cor-npe-log-001  Security Audit logs,  Prod: ave-sea-cor-prd-seclog-001  Pre-prod / Non-prod: ave-sea-cor-npe-seclog-001  Custom sources logs [logs from Applications, Servers running in other clouds, On-premise]  ave-sea-cor-custom-log-001 |

Table 23 Platform Monitoring Decision Decisions

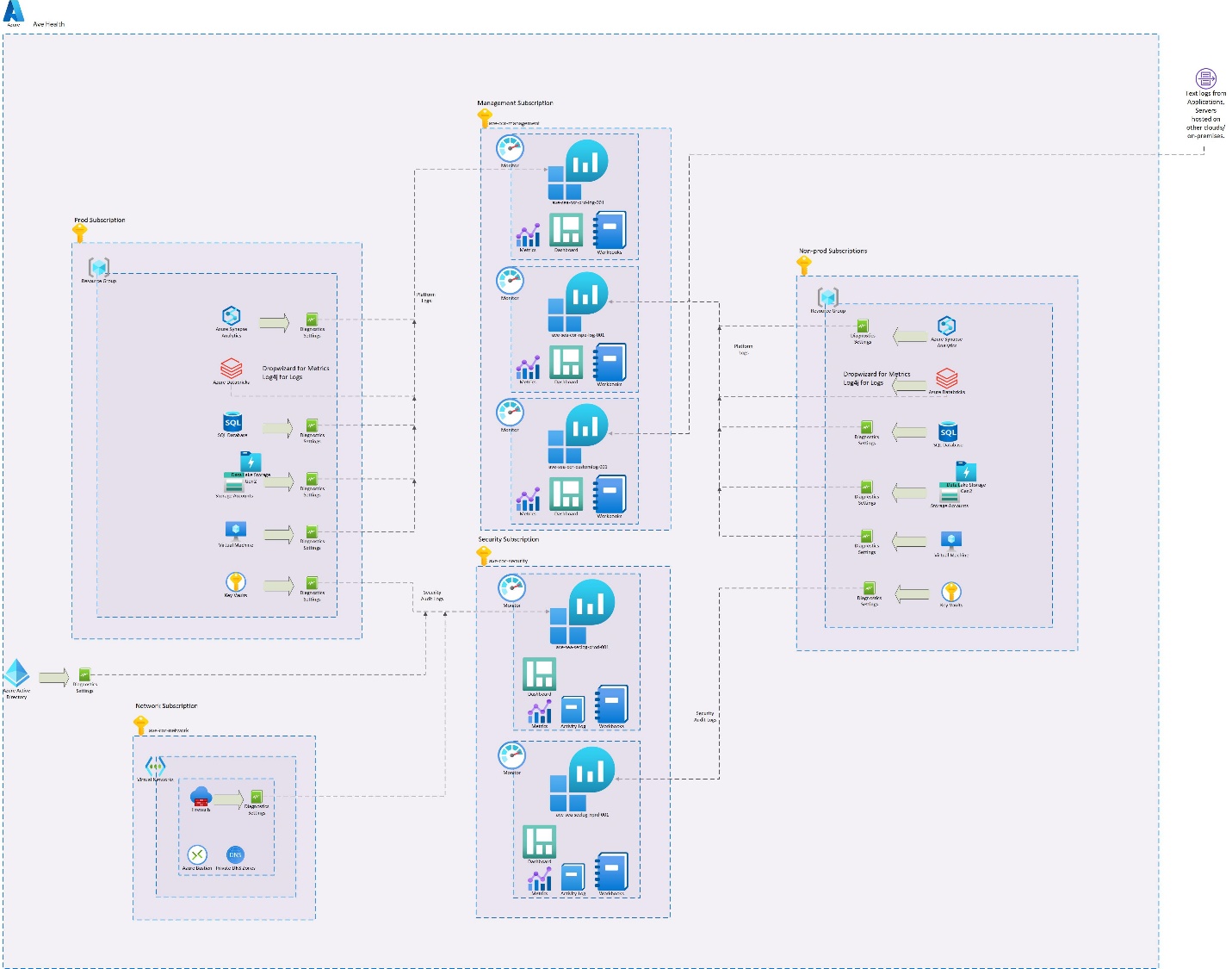


Figure10: Azure Platform Management and Monitoring recommended for AVE HEALTH SG

Design Pattern: Azure Monitor

Azure Monitor can collect data from a variety of sources. This ranges from your application, any operating system, and services it relies on, down to the platform itself. Azure Monitor collects data from each of the following tiers:

1. Application monitoring data: Data about the performance and functionality of the code you have written, regardless of its platform.
2. Guest OS monitoring data: Data about the operating system on which your application is running. This could be running in Azure, another cloud, or on-premises.
3. Azure resource monitoring data: Data about the operation of an Azure resource.
4. Azure subscription monitoring data: Data about the operation and management of an Azure subscription, as well as data about the health and operation of Azure itself.
5. Azure tenant monitoring data: Data about the operation of tenant-level Azure services, such as Azure Active Directory.
6. Azure resource change data: Data about changes within your Azure resource(s) and how to address and triage incidents and issues.

Graphical user interface

Description automatically generated

Figure 11 Monitoring Model

|  |  |
| --- | --- |
| Monitoring Tool | Description |
| Azure Monitor | Data from Azure Infrastructure (Activity Log) and each resource (Diagnostic Logs) |
| Azure Network Watcher | Diagnoses conditions at a network scenario level in, to, and from Azure. Regional service that enables monitoring and diagnosing through insights on the following Azure network resources:   * Topology: Network level graphical topology on Azure networking resources. * Variable Packet Capture: Captures packet data in/out of a VM. Can be stored in blob storage and locally in .cap format. * IP flow verify: Checks if packet is allowed/denied by NSGs based on 5-tuple packet info. * Next hop: Determines next hop for packets being routed in the Azure Network fabric for UDR troubleshooting. * Security Group View: Gets effective and applied security rules that are applied on a VM. * NSG Flow Logging: NSGs logs on traffic that is denied/allowed. * Virtual Network Gateway and Connection troubleshooting: Troubleshoot Virtual Network Gateways and Connections. * Network subscription limits: View network resource usage against limits. * Configuring Diagnostics Log: Enable/Disable Diagnostics logs for network resources in a resource group. |
| Azure Advisor | * Best practices to optimize Azure deployments on performance, security, HA, and costs. Analyzes Azure resource configuration and usage telemetry to provide recommendations on the following: * High Availability: VM Fault tolerance, application gateway fault tolerance, reliability of VM disks, and VM accidental deletion. * Security: Integrates with Azure Security Center to provide recommendations. * Performance: SQL DB databases, Redis Cache, and Azure’s App Service. * Cost: Optimize spending by resizing underutilized instances and implementing cost effective SQL databases. |
| Azure Security Center | * Prevents, detects, and responds to threats on Azure resources. * Create Security Policies * Recommendations * Security Alerts * Partner Solutions available for additional features * Integrate with other SIEM systems through Microsoft Azure Log Integration and export data to PowerBI. * Available in different tiers for Basic vs. Advance threat detection |
| Log Analytics | Holistic monitoring of on-premises, Azure, and third-party clouds like AWS |
| Application Insights | Detection and diagnostics at the application layer of services like App Service Web Apps   * HTTP request rates, response times, success rates. * Dependency (HTTP and SQL) call rates, response times, success rates. * Exception traces from server and client. * Diagnostic log traces. * Page view counts, user and session counts, browser load times, exceptions. * AJAX call rates, response times and success rates. * Server performance counters. * Custom client and server telemetry. * Segmentation by client location, browser version, OS version, server instance, custom dimensions, etc. * Availability tests. * Azure Functions |
| Container Insights | * Monitors the performance of container workloads that are deployed to managed Kubernetes clusters hosted on Azure Kubernetes Service (AKS). * It gives you performance visibility by collecting metrics from controllers, nodes, and containers that are available in Kubernetes through the Metrics API. * Container logs are also collected. After you enable monitoring from Kubernetes clusters, these metrics and logs are automatically collected for you through a containerized version of the Log Analytics agent for Linux |
| Dashboard | * Dashboards are a focused and organized view of your cloud resources in the Azure portal. * Use dashboards as a workspace where you can monitor resources and quickly launch tasks for day-to-day operations. * Build custom dashboards based on projects, tasks, or user roles, for example. |
| Workbooks | * Workbooks provide a flexible canvas for data analysis and the creation of rich visual reports within the Azure portal. * They allow you to tap into multiple data sources from across Azure and combine them into unified interactive experiences. * Workbooks let you combine multiple kinds of visualizations and analyses, making them great for free-form exploration. * Workbooks combine text, log queries, metrics, and parameters into rich interactive reports. |
| Service Map | * Service Map automatically discovers application components on Windows and Linux systems and maps the communication between services. * With Service Map, we can view the servers in the way that as interconnected systems that deliver critical services. * Service Map shows connections between servers, processes, inbound and outbound connection latency, and ports across any TCP-connected architecture, with no configuration required other than the installation of an agent. |

Table 24 Azure Monitoring Tools

Azure Lighthouse for Hybrid Monitoring

Azure Lighthouse enables multi-tenant management with scalability, higher automation, and enhanced governance across resources.

With Azure Lighthouse, service providers can deliver managed services using comprehensive and robust tooling built into the Azure platform. Customers maintain control over who has access to their tenant, which resources they can access, and what actions can be taken. Enterprise organizations managing resources across multiple tenants can use Azure Lighthouse to streamline management tasks.

Cross-tenant management experiences let you work more efficiently with Azure services such as Azure Policy, Microsoft Sentinel, Azure Arc, and many more. Users can see what changes were made and by whom in the activity log, which is stored in the customer's tenant and can be viewed by users in the managing tenant.

* View activity logs, alerts of customer tenants/subscriptions, with the ability to refresh alerts across all subscriptions.
* Using Log analytics, query data from remote workspaces deployed in customer tenants/subscriptions.
* Create, view, and manage metric alerts, log alerts, and activity log alerts in customer tenants/subscriptions.
* Create diagnostic settings in workspaces created in customer tenants, to send resource logs to workspaces in the customer tenants/subscriptions.

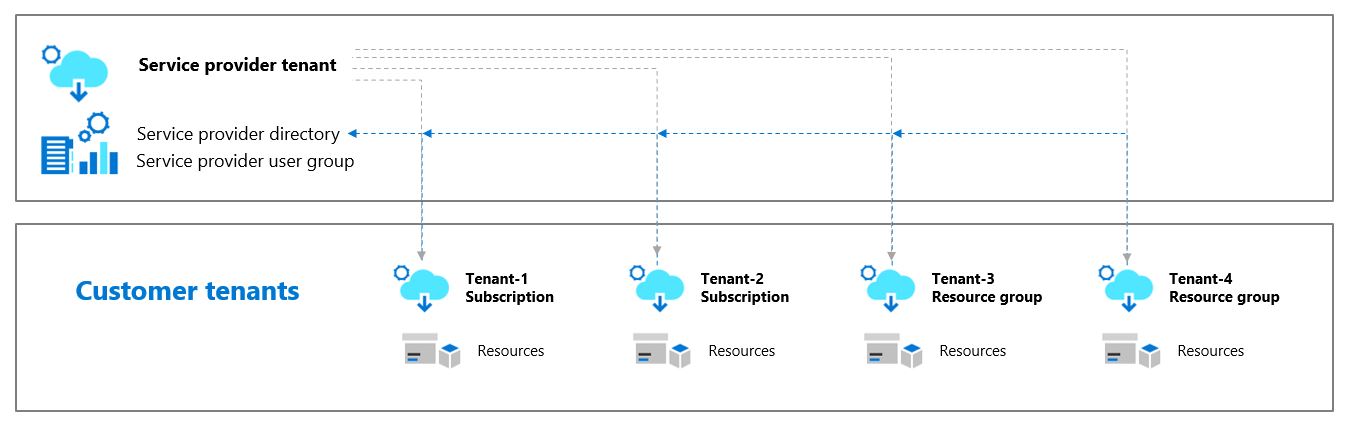


Figure 12 Monitoring Model

Respective Monitoring alert/ Notification per application will be captured through the app / system owner interview and will be captured in Application Questionnaire

Azure Platform Updates and Patching

Software updates in Azure Automation Update Management provides a set of tools and resources that can help manage the complex task of tracking and applying software updates to machines in Azure and hybrid cloud. An effective software update management process is necessary to maintain operational efficiency, overcome security issues, and reduce the risks of increased cyber security threats. However, because of the changing nature of technology and the continual appearance of new security threats, effective software update management requires consistent and continual attention.

Update Management uses a scope configuration within the workspace to target the computers to receive updates. For more information, see [Limit Update Management deployment scope](https://docs.microsoft.com/en-us/azure/automation/update-management/scope-configuration).

Compliance assessment

Before you deploy software updates to your machines, review the update compliance assessment results for enabled machines. For each software update, its compliance state is recorded and then after the evaluation is complete, it is collected and forwarded in bulk to Azure Monitor logs.

* On a Windows machine, the compliance scan is run every 12 hours by default and is initiated within 15 minutes of the Log Analytics agent for Windows is restarted. The assessment data is then forwarded to the workspace and refreshes the **Updates** table. Before and after update installation, an update compliance scan is performed to identify missing updates, but the results are not used to update the assessment data in the table.
* It is important to review our recommendations on how to [configure the Windows Update client](https://docs.microsoft.com/en-us/azure/automation/update-management/configure-wuagent) with Update Management to avoid any issues that prevents it from being managed correctly.
* For a Linux machine, the compliance scan is performed every hour by default. If the Log Analytics agent for Linux is restarted, a compliance scan is initiated within 15 minutes.
* The compliance results are presented in Update Management for each machine assessed. It can take up to 30 minutes for the dashboard to display updated data from a new machine enabled for management.

Review [monitor software updates](https://docs.microsoft.com/en-us/azure/automation/update-management/view-update-assessments) to learn how to view compliance results.

Deploy Updates

After reviewing the compliance results, the software update deployment phase is the process of deploying software updates. To install updates, schedule a deployment that aligns with your release schedule and service window. You can choose which update types to include in the deployment. For example, you can include critical or security updates and exclude update rollups.

Review [deploy software updates](https://docs.microsoft.com/en-us/azure/automation/update-management/deploy-updates) to learn how to schedule an update deployment.

Review update deployments

After the deployment is complete, review the process to determine the success of the update deployment by machine or target group. See [review deployment status](https://docs.microsoft.com/en-us/azure/automation/update-management/deploy-updates#check-deployment-status) to learn how you can monitor the deployment status.

* To learn how to create alerts to notify you about update deployment results, see [create alerts for Update Management](https://docs.microsoft.com/en-us/azure/automation/update-management/configure-alerts).

You can [query Azure Monitor logs](https://docs.microsoft.com/en-us/azure/automation/update-management/query-logs) to analyze update assessments, deployments, and other related management tasks. It includes pre-defined queries to help you get started.

Management for automation, reporting and better patch management for Azure Cloud IaaS

Design Considerations

|  |  |
| --- | --- |
| ID | Description |
| DC01 | Patching update process involve first patching on Development Systems, then Q&A and then Pre-Prod and last Production Systems. |
| DC02 | Patching cycle for the server is every month. |
| DC03 | Patching to be done during non-business hours. |

Table 25 Platform Monitoring Design Considerations

Design Decisions

|  |  |
| --- | --- |
| ID | Description |
| DD01 | Azure Update Management will be used to automate and track patching. |
| DD02 | Patch reporting and compliance can be achieved in a better way with Azure Update Management, it will help Ave Health team to improve the patch management efficiency. |
| DD03 | Patching Cycle for,  Dev – 3rd Saturday [16th July]  Q&A – 3rd Sunday [17th July]  Pre-prod – 4th Saturday [23rd July]  Prod – 1st Saturday [N-1 patches will be deployed for Prod servers] [6th August] |

Update Management

Machines that are managed by Update Management rely on the following to perform assessment and to deploy updates:

* [Log Analytics agent](https://docs.microsoft.com/en-us/azure/azure-monitor/agents/log-analytics-agent) for Windows or Linux
* PowerShell Desired State Configuration (DSC) for Linux
* Automation Hybrid Runbook Worker (automatically installed when you enable Update Management on the machine)
* Microsoft Update or [Windows Server Update Services](https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/get-started/windows-server-update-services-wsus) (WSUS) for Windows machines
* Either a private or public update repository for Linux machines

The following diagram illustrates how Update Management assesses and applies security updates to all connected Windows Server and Linux servers in a workspace:

Diagram

Description automatically generated

Figure 13 Azure Updates Workflow

Update Management can be used to natively deploy to machines in multiple subscriptions in the same tenant, or across tenants using [Azure delegated resource management](https://docs.microsoft.com/en-us/azure/lighthouse/concepts/azure-delegated-resource-management).

After a package is released, it takes 2 to 3 hours for the patch to show up for Linux machines for assessment. For Windows machines, it takes 12 to 15 hours for the patch to show up for assessment after it's been released. When a machine completes a scan for update compliance, the agent forwards the information in bulk to Azure Monitor logs. On a Windows machine, the compliance scan is run every 12 hours by default. For a Linux machine, the compliance scan is performed every hour by default. If the Log Analytics agent is restarted, a compliance scan is started within 15 minutes.

In addition to the scan schedule, the scan for update compliance is started within 15 minutes of the Log Analytics agent being restarted, before update installation, and after update installation.

Update Management reports how up to date the machine is based on what source you're configured to sync with. If the Windows machine is configured to report to [Windows Server Update Services](https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/get-started/windows-server-update-services-wsus) (WSUS), depending on when WSUS last synced with Microsoft Update, the results might differ from what Microsoft Update shows. This behavior is the same for Linux machines that are configured to report to a local repo instead of to a public repo.

You can deploy and install software updates on machines that require the updates by creating a scheduled deployment. Updates classified as optional aren't included in the deployment scope for Windows machines. Only required updates are included in the deployment scope.

The scheduled deployment defines which target machines receive the applicable updates. It does so either by explicitly specifying certain machines or by selecting a [computer group](https://docs.microsoft.com/en-us/azure/azure-monitor/logs/computer-groups) that's based on log searches of a specific set of machines (or on an [Azure query](https://docs.microsoft.com/en-us/azure/automation/update-management/query-logs) that dynamically selects Azure VMs based on specified criteria). These groups differ from [scope configuration](https://docs.microsoft.com/en-us/azure/azure-monitor/insights/solution-targeting), which is used to control the targeting of machines that receive the configuration to enable Update Management. This prevents them from performing and reporting update compliance, and install approved required updates.

While defining a deployment, you also specify a schedule to approve and set a time period during which updates can be installed. This period is called the maintenance window. A 20-minute span of the maintenance window is reserved for reboots, assuming one is needed and you selected the appropriate reboot option. If patching takes longer than expected and there's less than 20 minutes in the maintenance window, a reboot won't occur.

Updates are installed by runbooks in Azure Automation. You can't view these runbooks, and they don't require any configuration. When an update deployment is created, it creates a schedule that starts a master update runbook at the specified time for the included machines. The master runbook starts a child runbook on each agent to install the required updates.

At the date and time specified in the update deployment, the target machines execute the deployment in parallel. Before installation, a scan is run to verify that the updates are still required. For WSUS client machines, if the updates aren't approved in WSUS, update deployment fails.

Having a machine registered for Update Management in more than one Log Analytics workspace (also referred to as multihoming) isn't supported.

Supported Operating Systems

|  |  |
| --- | --- |
| Operating System | Notes |
|  |  |
| * Windows Server 2019 (Datacenter/Standard including Server Core) * Windows Server 2016 (Datacenter/Standard excluding Server Core) * Windows Server 2012 R2(Datacenter/Standard) * Windows Server 2012 | Fully supported |
| Windows Server 2008 R2 (RTM and SP1 Standard) | Update Management supports assessments and patching for this operating system. The [Hybrid Runbook Worker](https://docs.microsoft.com/en-us/azure/automation/automation-windows-hrw-install) is supported for Windows Server 2008 R2. |
| CentOS 6, 7, and 8 (x64) | Linux agents require access to an update repository. Classification-based patching requires yum to return security data that CentOS doesn't have in its RTM releases. For more information on classification-based patching on CentOS, see [Update classifications on Linux](https://docs.microsoft.com/en-us/azure/automation/update-management/view-update-assessments#linux). |
| Red Hat Enterprise 6, 7, and 8 (x64) | Linux agents require access to an update repository. |
| SUSE Linux Enterprise Server 12, 15, and 15.1 (x64) | Linux agents require access to an update repository. For SUSE 15.x, Python 3 is required on the machine. |
| Ubuntu 14.04 LTS, 16.04 LTS, and 18.04 LTS (x64) | Linux agents require access to an update repository. |

Table 26 Azure Updates Support Information

Azure Backup and BCDR

Backup and Disaster Recovery services contribute to business continuity and disaster recovery (BCDR). BCDR consists of two broad aims:

* Keep your business data safe and recoverable when outages occur.
* Keep your apps and workloads up and running during planned and unplanned downtimes.

The concept of Business Continuity and Disaster Recovery requirements often triggered by regulators recognized the need to mitigate the effects that disruptive events such as a cyberattack have on society, with businesses recognizing their interdependence. Business Continuity programs are designed to ensure that critical business functions can continue working with minimal downtime in the event of an interruption, while disaster recovery plans (DR plans) consider how to restore business processes within a certain amount of time — the recovery time objective (RTO) –in the event of a disaster.

Cloud providers such as Microsoft Azure provide capabilities that support availability and a variety of disaster recovery services to adapt to different scenarios by building Azure recovery services to contribute to an enterprise-level BCDR strategy. The following are two disaster recovery services:

* Azure Backup service: This keeps your data safe and recoverable by backing it up to Azure.
* Site Recovery service: This is used to replicate workloads running on physical and virtual machines from a primary site to a secondary region. Users can failover to a secondary location if an outage occurs at the primary region and users can fall back to it when the primary region is back to normal.

Design Considerations

|  |  |
| --- | --- |
| ID | Description |
| DC01 | Develop a high-level Business Continuity and Disaster Recovery plan to accommodate key business applications needs and provide Microsoft Azure BCDR capabilities |
| DC02 | Use Azure Backup to backup VMs where applicable, as it is the cloud native PaaS service. |
| DC03 | Leverage Azure Site Recovery capabilities for Virtual Machine based applications |
| DC04 | Application workload should be implemented with an Active-Active disaster recovery for production workloads wherever possible. If the application does not or cannot support an active-active configuration or a hot Active-Passive, the Cold Active-Passive solution should be followed using Azure Site Recovery. |
| DC05 | Design HA/DR per application based on a set of baseline patterns to enforce a consistent approach and avoiding ‘one size fits all’. |
| DC06 | Design a baseline backup policy on a per-application category basis. They define how often backups should occur and what retention period should be applied. |
| DC07 | Use Azure zone within Southeast Asia region when planning for BCDR. |
| DC08 | No multiple and peering locations for ExpressRoute connectivity required, as AVE HEALTH SG will be using Zone based DR strategy (Zone based DR is available in Southeast Asia region) |

Design Decisions

|  |  |
| --- | --- |
| ID | Description |
| DD01 | As per compliance and business requirement AVE HEALTH SG has decided to use within a single region DR (disaster recovery systems) by using ASR (Azure Site Recovery) capabilities which is available for the Southeast Asia Azure region. |
| DD02 | AVE HEALTH SG will use Azure Backup services, and Backup (Recovery Services) Vault will be created in Southeast Region. |
| DD03 | ASR capabilities to be used for Zone-to-Zone replication in Production environment. |
| DD04 | Recovery Vault to be provisioned in each subscription. |
| DD05 | Azure Backup Vault Naming convention to be used – “sea-bak-prod-<App>-vault-01” |
| DD06 | All VMs include PROD, Pre-Prod, QA, Dev will require Azure Image Backup. |
| DD07 | Frequency and retention required for Production VM backup:   |  |  | | --- | --- | | Frequency | Daily | | Instant Restore | Yes | | Retention Of daily Backup Point | 30 days | | Policy Type | Azure Virtual Machine | |
| DD08 | Frequency and retention required for Pre-Prod, QA, Dev VM backup:   |  |  | | --- | --- | | Frequency | Weekly | | Instant Restore | Yes | | Retention Of daily Backup Point | 30 days | | Policy Type | Azure Virtual Machine | |

Table 27 Azure Backup and BCDR Design Decisions

Business Continuity and Disaster Recovery Overview

A Business Continuity Plan (BCP) most often begins with a business impact analysis (BIA) that determines the plan’s scope; determines legal, contractual, and regulatory obligations; and provides a basis for planning and justifying the costs of the BC program. A BIA often gets conducted in tandem with a risk assessment. It also considers the impact on your business that could occur if disaster strikes your service providers.

Business Continuity Risks

As with any risk identification process, you need to understand your IT infrastructure. Some questions to consider include:

* What information, systems, networks, and software are critical to maintaining our business operations? How do they connect to one another?
* What natural disasters could affect these critical systems, networks, and software?
* What cyber risks threaten these systems, networks, and software?
* What third-party services or vendors are critical to maintaining business operations?
* What controls are in place to prevent cyber risks to our critical systems, networks, and software?
* What controls are in place to prevent critical third-party service providers and vendors from affecting business operations?
* What backup systems do we use? Do we have a data center or other data backup and recovery service off-site?
* Do we maintain in-transit encryption for remote access in the event of a business interruption?
* Do we maintain endpoint encryption in the event of business interruption?
* Do we have a process for emergency administrative authorizations to maintain continuous business operations?

Business Continuity Plan Development

Developing BCP starts by assessing your business processes, determining which areas are vulnerable, and the potential losses if those processes go down for a day, a few days, or a week. This is essentially a BIA.

This involves six general steps:

1. Identify the scope of the plan.
2. Identify key business areas.
3. Identify critical functions.
4. Identify dependencies between various business areas and functions.
5. Determine acceptable downtime for each critical function.
6. Create a plan to maintain operations.

One common business continuity planning tool is a checklist that includes supplies and equipment, the location of data backups and backup sites, where the plan is available and who should have it, and contact information for emergency responders, key personnel and backup site providers.

Design Patterns 1 - IaaS Applications

Business Continuity, IaaS workloads should be implemented with an Active-Active disaster recovery wherever possible. If the application does not or cannot support an Active-Active configuration or a Hot Active-Passive, the Cold Active-Passive solution should be followed using Azure Site Recovery.

ASR allows protection of Windows or Linux-based computers, physical servers, VMware, or Hyper-V. It also integrates well with [applications](https://docs.microsoft.com/azure/site-recovery/site-recovery-workload?WT.mc_id=itopstalk-blog-salean) such as SharePoint, Exchange, Dynamics, SQL Server and Active Directory, as well as Oracle SAP and Red Hat.

Azure Site Recovery contributes to your business continuity and disaster recovery (BCDR) strategy, by orchestrating and automating replication of Azure VMs between regions, on-premises virtual machines and physical servers to Azure, and on-premises machines to a secondary datacenter.

As per compliance and business requirement AVE HEALTH SG has decided to use within a single region DR by using ASR capabilities which is available for Southeast Asia Azure region.

For a typical 2-3 tier applications leveraging IaaS platform, Azure Site Recovery is the Microsoft recommended solution. Utilizing Azure Traffic Manager and multi region, AVE HEALTH SG can deploy Active-Passive or Active-Active BCDR solution.

There are various measures taken by Site Recovery to ensure data integrity. A secure connection is established between all services by using the HTTPS protocol. This makes sure that any malware or outside entities can't tamper the data. Another measure taken is using checksums. The data transfer between source and target is executed by computing checksums of data between them. This ensures that the transferred data is consistent.

For additional information, refer to the following link [About Azure Site Recovery - Azure Site Recovery | Microsoft Docs](https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-overview)

For additional questions, refer to the following link [General questions about the Azure Site Recovery service - Azure Site Recovery | Microsoft Docs](https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-faq)

Design Pattern 2 - Zone Redundancy

An Availability Zone is a high availability offering that protects your applications and data from datacenter failures. Availability Zones are unique physical locations within an Azure region. Each zone is made up of one or more datacenters equipped with independent power, cooling, and networking. To ensure resiliency, there's a minimum of three separate zones in all enabled regions. The physical separation of Availability Zones within a region protects applications and data from datacenter failures. Zone-redundant services replicate your applications and data across Availability Zones to protect from single-points-of-failure. With Availability Zones, Azure offers industry best 99.99% VM uptime SLA. The full Azure SLA explains the guaranteed availability of Azure as a whole.

An Availability Zone in an Azure region is a combination of a fault domain and an update domain. For example, if you create three or more VMs across three zones in an Azure region, your VMs are effectively distributed across three fault domains and three update domains. The Azure platform recognizes this distribution across update domains to make sure that VMs in different zones are not scheduled to be updated at the same time.

Build high availability into your application architecture by co-locating your compute, storage, networking, and data resources within a zone and replicating in other zones. Azure services that support Availability Zones fall into two categories:

* **Zonal services** – where a resource is pinned to a specific zone (for example, virtual machines, managed disks, Standard IP addresses), or
* **Zone-redundant services** – when the Azure platform replicates automatically across zones (for example, zone-redundant storage, SQL Database).

To achieve comprehensive business continuity on Azure, build your application architecture using the combination of Availability Zones with Azure region pairs. You can synchronously replicate your applications and data using Availability Zones within an Azure region for high-availability and asynchronously replicate across Azure regions for disaster recovery protection.

For Additional information, please refer to the following link <https://docs.microsoft.com/en-us/azure/availability-zones/az-overview>

Recommended Zone redundancy for.

* Azure Load Balancer supports availability zones scenarios. AVE HEALTH SG can use Standard Load Balancer to increase availability throughout your scenario by aligning resources with, and distribution across zones. Review this document to understand these concepts and fundamental scenario design guidance. Standard SKU Load Balancer can either be zone redundant, zonal, or non-zonal. To configure the zone related properties (mentioned above) for your load balancer, select the appropriate type of frontend needed. for more information, please refer to the following link <https://docs.microsoft.com/en-us/azure/architecture/high-availability/building-solutions-for-high-availability>
* For a VPN gateway, the two gateway instances will be deployed in any 2 out of these three zones to provide zone-redundancy.
* For an ExpressRoute gateway, since there can be more than two instances, the gateway can span across all the three zones.
* An Application Gateway or WAF deployment can span multiple Availability Zones, removing the need to provision separate Application Gateway instances in each zone with a Traffic Manager. You can choose a single zone or multiple zones where Application Gateway instances are deployed, which makes it more resilient to zone failure. The backend pool for applications can be similarly distributed across availability zones.

AVE HEALTH SG can’t use multi region DR, as per compliance and business requirement, therefore will take appropriate decision to use ZRS based High Availability capability for critical applications which will be discussed and decided per application bases during application onboarding.

Design Pattern 3 - Azure Backup

For backing up Azure VMs running production workloads, AVE HEALTH SG service owners can leverage Azure Backup. Azure Backup supports application-consistent backups for both Windows and Linux VMs.

Backup Center provides a single unified management experience in Azure for enterprises to govern, monitor, operate, and analyze backups at scale. As such, it's consistent with Azure’s native management experiences.

Diagram

Description automatically generated

Figure 15 Backup and Disaster Recovery

Some of the key benefits of Backup center include:

* Single pane of glass to manage backups – Backup center is designed to function well across a large and distributed Azure environment. You can use Backup center to efficiently manage backups spanning multiple workload types, vaults, subscriptions, regions, and Azure Lighthouse tenants.
* Data source-centric management I– Backup center provides views and filters that are centered on the data sources that you're backing up (for example, VMs and databases). This allows a resource owner or a backup admin to monitor and operate backups of items without needing to focus on which vault an item is backed up to. A key feature of this design is the ability to filter views by data source-specific properties, such as data source subscription, data source resource group, and data source tags. For example, if your organization follows a practice of assigning different tags to VMs belonging to different departments, you can use Backup center to filter backup information based on the tags of the underlying VMs being backed up without needing to focus on the tag of the vault.
* Connected experiences – Backup center provides native integrations to existing Azure services that enable management at scale. For example, Backup center uses the Azure Policy experience to help you govern your backups. It also leverages Azure workbooks and Azure Monitor Logs to help you view detailed reports on backups. So, you don't need to learn any new principles to use the varied features that Backup center offers. You can also discover community resources from the Backup center.
* All your backed-up data is automatically encrypted when stored in the cloud using Azure Storage encryption, which helps you meet your security and compliance commitments. This data at rest is encrypted using 256-bit AES encryption, one of the strongest block ciphers available, and is FIPS 140-2 compliant. In addition to encryption at rest, all your backup data in transit is transferred over HTTPS. It always remains on the Azure backbone network.
  + **Using platform-managed keys**: By default, all your data is encrypted using platform-managed keys. You don't need to take any explicit action from your end to enable this encryption. It applies to all workloads being backed up to your Recovery Services vault.
  + **Using customer-managed keys**: When backing up your Azure Virtual Machines, AVE HEALTH SG can choose to encrypt your data using encryption keys owned and managed by the organization. Azure Backup lets you use your RSA keys stored in the Azure Key Vault for encrypting your backups. The encryption key used for encrypting backups may be different from the one used for the source. The data is protected using an AES 256 based data encryption key (DEK), which is, in turn, protected using your keys. This gives you full control over the data and the keys. To allow encryption, it's required that you grant the Recovery Services vault access to the encryption key in the Azure Key Vault. You can disable the key or revoke access whenever needed. However, you must enable encryption using your keys before you attempt to protect any items to the vault. [Learn more here](https://docs.microsoft.com/en-us/azure/backup/encryption-at-rest-with-cmk).
  + **Infrastructure-level encryption**: In addition to encrypting your data in the Recovery Services vault using customer-managed keys, you can also choose to have an additional layer of encryption configured on the storage infrastructure. This infrastructure encryption is managed by the platform. Together with encryption at rest using customer-managed keys, it allows two-layer encryption of your backup data. Infrastructure encryption can only be configured if you first choose to use your own keys for encryption at rest. Infrastructure encryption uses platform-managed keys for encrypting data.
  + **Azure virtual machine backup:** Azure Backup supports backup of VMs with disks encrypted using [platform-managed keys](https://docs.microsoft.com/en-us/azure/virtual-machines/disk-encryption#platform-managed-keys), as well as [customer-managed keys](https://docs.microsoft.com/en-us/azure/virtual-machines/disk-encryption#customer-managed-keys) owned and managed by you. In addition, you can also back up your Azure Virtual machines that have their OS or data disks encrypted using [Azure Disk Encryption](https://docs.microsoft.com/en-us/azure/backup/backup-azure-vms-encryption#encryption-support-using-ade). ADE uses BitLocker for Windows VMs, and DM-Crypt for Linux VMs, to perform in-guest encryption. For additional information <https://docs.microsoft.com/en-us/azure/backup/backup-azure-vms-encryption>
* Azure Advisor provides recommendations in four categories: High Availability, Security, Performance and Cost. With this announcement, Azure Advisor provides recommendations on virtual machines that are not backed up and will let you enable backup on those virtual machines with just a few clicks. Specifically, Advisor will identify any virtual machines in which backup is not enabled and recommend enabling backup. This ensures that critical data will be available and protects you from corruption or accidental deletion of these data.

Azure Backup can be used for

* On-premises - Back up files, folders, system state using the [Microsoft Azure Recovery Services (MARS) agent](https://docs.microsoft.com/en-us/azure/backup/backup-support-matrix-mars-agent). Or use the DPM or Azure Backup Server (MABS) agent to protect on-premises VMs ([Hyper-V](https://docs.microsoft.com/en-us/azure/backup/back-up-hyper-v-virtual-machines-mabs) and [VMware](https://docs.microsoft.com/en-us/azure/backup/backup-azure-backup-server-vmware)) and other [on-premises workloads](https://docs.microsoft.com/en-us/azure/backup/backup-mabs-protection-matrix)
* Azure VMs - [Back up entire Windows/Linux VMs](https://docs.microsoft.com/en-us/azure/backup/backup-azure-vms-introduction) (using backup extensions) or back up files, folders, and system state using the [MARS agent](https://docs.microsoft.com/en-us/azure/backup/backup-azure-manage-mars).
* Azure Managed Disks - [Back up Azure Managed Disks (in preview)](https://docs.microsoft.com/en-us/azure/backup/backup-managed-disks)
* Azure Files shares - [Back up Azure File shares to a storage account](https://docs.microsoft.com/en-us/azure/backup/backup-afs)
* SQL Server in Azure VMs - [Back up SQL Server databases running on Azure VMs](https://docs.microsoft.com/en-us/azure/backup/backup-azure-sql-database)
* SAP HANA databases in Azure VMs - [Backup SAP HANA databases running on Azure VMs](https://docs.microsoft.com/en-us/azure/backup/backup-azure-sap-hana-database)
* Azure Database for PostgreSQL servers (preview) - [Back up Azure PostgreSQL databases and retain the backups for up to 10 years](https://docs.microsoft.com/en-us/azure/backup/backup-azure-database-postgresql)
* Azure Blobs (preview) - [Overview of operational backup for Azure Blobs (in preview)](https://docs.microsoft.com/en-us/azure/backup/blob-backup-overview)

As per decision AVE HEALTH SG will use Azure Backup for all PROD, Pre-Prod, QA and Dev VMs (Total 10 VMs approx.) for Image level backup.

Design Pattern 4 - Azure Storage Availability

Data in an Azure Storage account is always replicated three times in the primary region. Azure Storage offers two options for how your data is replicated in the primary region:

* **Locally redundant storage (LRS)** copies your data synchronously three times within a single physical location in the primary region. LRS is the least expensive replication option but is not recommended for applications requiring high availability.
* **Zone-redundant storage (ZRS)** copies your data synchronously across three Azure availability zones in the primary region. For applications requiring high availability, Microsoft recommends using ZRS in the primary region, and replicating to a secondary region.

Azure Storage offers three options for copying your data to a secondary region:

* **Geo-redundant storage (GRS)** copies your data synchronously three times within a single physical location in the primary region using LRS. It then copies your data asynchronously to a single physical location in the secondary region. Within the secondary region, your data is copied synchronously three times using LRS.
* **Geo-zone-redundant storage (GZRS)** copies your data synchronously across three Azure availability zones in the primary region using ZRS. It then copies your data asynchronously to a single physical location in the secondary region. Within the secondary region, your data is copied synchronously three times using LRS.

**Geo-redundant storage (with GRS or GZRS)** replicates your data to another physical location in the secondary region to protect against regional outages. However, that data is available to be read only if the customer or Microsoft initiates a failover from the primary to secondary region. When you enable read access to the secondary region, your data is available to be read at all times, including in a situation where the primary region becomes unavailable. For read access to the secondary region, enable read-access geo-redundant storage (RA-GRS) or Read-access geo-zone-redundant storage (RA-GZRS).

AVE HEALTH SG will be using LRS for general purpose storage accounts. And for critical application, as per requirements ZRS will be used. Decisions will be taken on per application bases and will be discussed during application migration phase.

AVE HEALTH SG will be using LRS for general purpose storage accounts. And for critical application, as per requirements ZRS will be used. Decision will be taken on per application bases.

Security

When it comes to managing cloud resources, a key aspect of cloud security is identity, the primary security boundary. As mentioned earlier, it is paramount to use RBAC to strictly limit the permissions of users or service principals to the least that are required to perform a particular function. Azure AD also provides conditional access and privileged access management which provide further control granularity on Azure resources and authentication scenarios.

To protect access to deployed VMs on Azure, Microsoft recommends two mechanisms. Both mechanisms restrict management access to VMs via their public IP address by default and audit log all events.

* **Azure Bastion:** Using Azure Bastion allows authorized users to securely connect to a VM without exposing its management ports to the public internet. Admins connect using their web browser, which will open an RDP or SSH session within the browser (secured via HTTPS) using Bastion, which needs to be deployed in a Subnet of the VM’s VNet.
* **Just in time VM access**: This is a functionality provided by Azure Security Center (standard tier) which allows authorized users to request access to a VM. Once approved, Azure will make temporary modifications to all Firewalls or Network Security Groups that are in front of the VM and allow access via the admin port from the public internet (or via Azure using the private IP) for the duration of the request. After the duration has passed, the rules will be reverted, and access restricted once again.

Note that currently the two mechanisms cannot be deployed together, so Microsoft recommends choosing the mechanism that best supports the use case. For scenarios where permanent admin access or frequent access is required, it is advised to use Azure Bastion while for highly sensitive VMs, just in time access might be better suited.

Defender for Cloud

* + - 1. Technical Overview

Defender for Cloud is a unified infrastructure security management system that strengthens the security posture of data centers and provides advanced threat protection across hybrid workloads in the cloud - whether they're in Azure or not - as well as on-premises.

Defender for Cloud automatically collects information from the cloud resources and highlights security recommendations as well as vulnerabilities. PaaS services like storage accounts are monitored and protected without necessitating any deployment. While the free tier comes with automated continuous security assessments, the standard tier offers advanced functionality such as just-in-time VM access, the ability to scan resources for compliance against established industry standards (such as PCI DSS 3.2 or ISO 27001) or Threat protection for IaaS or PaaS offerings.

Besides the ability to define alerts for critical vulnerabilities, Defender for Cloud offers one-click mitigation for many common security issues, allowing for fast and easy fixes. Furthermore, Logic App workflows can be created for issues where no one-click mitigation exists yet, empowering in automating frequently occurring security violations specific to an organizational setup.

For an overview of the Defender for Cloud features, please consult the table below:

|  |  |  |
| --- | --- | --- |
| Feature | Description | Tier |
| Continuous assessment and security recommendations | Provide daily scans of the workloads and configurations and assess them for vulnerabilities. | Free |
| Secure Score | Provide a prioritized and weighted list of security recommendations based on the assessments and offer detailed remediation instructions or one-click remediation process. | Free |
| Just in time VM Access | Use Just-in-Time VM Access to control access and avoid exposure of commonly targeted management ports. Define a break glass access process to allow connection to the VMs. Security Center will automatically handle the required networking changes in the background and revert them once the set timeframe has expired. | Standard |
| Adaptive application controls and network hardening | Adaptive application controls help harden VMs against malware by using machine learning to analyse the applications running on machines and creating an allow list from this intelligence.  Adaptive Network Hardening provides recommendations to further harden the NSG rules based on observing actual traffic patterns. | Standard |
| Regulatory compliance dashboard and reports | Provides insights into compliance posture based on continuous assessments of Azure environment against chosen policies and defined industry standards and regulations. | Standard |
| Threat protection for Azure VMs and non-Azure servers (including Server EDR) | Defender for Cloud integrates with Azure services to monitor and protect VMs and alert any discovered threats.  For Windows based machine it uses the Microsoft Defender Advanced Threat Protection (ATP) to provide advanced endpoint detection and response (EDR) capabilities. It also provides file less attack detection (injection of malicious payloads into memory) by periodically running disk-based scanning techniques.  For Linux machines Security Center collects audit records using audited. These events are collected, enriched, and aggregated into events using the Log Analytics agent for Linux and evaluated against a continuously growing list of known malicious behaviors. | Standard |
| Threat protection for PaaS services | Defender for Cloud also offers threat protection for PaaS offerings, such as SQL Database, SQL Data Warehouse, App Services, Azure Storage Accounts or Azure Kubernetes Services. It will continuously monitor and assess their configuration and end points against known attack patterns and vulnerabilities and send out alerts when triggered. | Standard |

Table 28: Azure Security Center feature comparison

Design Decisions

|  |
| --- |
| Design Decisions |
| AVE Health SG will use Azure Defender/Security Center Standard for all subscriptions and all resources for the environment which include Production, Preproduction, QA and Development. |
| Data collected by Azure Defender will be stored in the central Log Analytics workspace in the Security Subscription.  Azure Defender Data will be stored in Security Subscription (Centrally). Production - Retention policy with 90 days default, PreProd/QA & Development will follow 90 days retention policy in the backend. Post retention, the data from all the environments will be archived to storage account and the data be retained for 1 year. |
| All Windows security events will be collected and stored in central Workspace. |
| MMA /Azure Monitor Agent will be on enabled through policy. |

Table 29: Design Decisions - Defender for Cloud

Azure Key Vault

Technical Overview

Azure Key Vault helps to safeguard cryptographic keys and secrets used by Azure workloads and services. Key Vault provides highly available and scalable secure storage for RSA cryptographic keys backed by FIPS 140-2 Level 2 validated HSMs (Hardware Security Modules).

Key Vault streamlines the key management process and enables customers to fully maintain control of keys that are used to encrypt data, manage, and audit their key usage. All keys are protected by hardware security modules (HSMs). At any time, security administrators can grant (and revoke) permission to keys, as needed.

Furthermore, Key Vaults can be used to manage certificates and their lifecycles (e.g., to automate the renewal of the certificates used for internet facing applications).

A typical use-case for using Key Vault in IaaS is the protection of administrative passwords used during the deployment and to store disk encryption keys. Therefore, the passwords required for the end-to-end VM deployment using ARM Templates will be stored as Secrets in the Key Vault.

Design decisions

|  |
| --- |
| Design Decisions |
| Need data encryption to meet the compliance requirements |
| Default Microsoft managed keys are used for data encryption |
| VM disk encryption will be default |

Table 30: Design Decisions - Key Vault

Azure Data Encryption

This section will elaborate on the data encryption aspects of Azure.

Technical Overview

Microsoft always employs a variety of different encryption mechanisms to keep data safe – both in transit and at rest – across Microsoft’s entire portfolio (Azure, O365/M365, D365):

|  |  |  |  |
| --- | --- | --- | --- |
| Where encryption happens | What is encrypted | Microsoft products | Comments |
| In transit | Data pipes | Transport Layer Security protocol & others | TLS and other standard protocols encrypt data as it moves between client sites and our cloud and between our own data centres. |
| At rest | Disk | BitLocker and others | Encryption of storage devices in Azure data centres protects customer data if devices are stolen or tampered with; also helps comply with data protection laws. |
| Service | Service-level encryption for Office 365, Dynamics 365, Power BI, Azure SQL Database | Goes beyond disk encryption to encrypt all customer data associated with a cloud service; protects data against access by malicious insiders or outside hackers; helps comply with data protection and data residency laws. Service-level encryption can use Microsoft-managed keys, or Customer Key/BYOK. |
| In use | Database | Azure Confidential Computing, Always Encrypted (Database) | Even while being processed by database servers in Azure, customer data can be protected by encryption software or hardware. |
| Anything | Homomorphic encryption | Microsoft Research is developing new methods that may one day make it feasible to encrypt any kind of data while it is being computed on, thus allowing data to remain encrypted at all times. |

Table 31: Microsoft Encryption Options

|  |  |  |
| --- | --- | --- |
| Azure Resource | Encryption Technology | Status |
| Storage Account | Storage Service Encryption (SSE) | Enabled by default |
| Windows VM | Azure Disk Encryption, BitLocker | Not enabled by default |
| Linux VM | Azure Disk Encryption | Not enabled by default |
| SQL Server on Azure VM | Transparent Data Encryption | Not enabled by default |
| Azure SQL Database | Always Encrypted | Not enabled by default |
| Azure SQL Server | Always Encrypted | Not enabled by default |

Table 32: Azure Encryption Technologies

Encryption for Storage Accounts

The Storage Service Encryption (SSE) helps to protect and safeguard data to meet security and compliance commitments. SSE can be enabled for all new Blob services to protect the Storage Accounts. With SSE enabled, all data written to the specific service is encrypted before it is written. The encryption, decryption, and key management are transparent to users.

Azure Disk Encryption for VMs

There are two kinds of encryption for VM Disks: Storage Service Encryption (SSE), which is performed by the underlying storage service, and Azure Disk Encryption, which is enabled on the volume-level for the OS and Data Disks of a VM.

**Note:** SSE is enabled by default for all new Managed Disks, Snapshots and Images and cannot be disabled. Data written to a managed disk will be automatically encrypted-at-rest with keys managed by Microsoft (this can be changed to BYOK).

Azure Disk Encryption for Windows and Linux VMs helps protect and safeguard data to meet organizational security and compliance commitments. It is a capability that helps to encrypt Windows and Linux virtual machine disks. Azure Disk Encryption leverages the industry standard BitLocker feature of Windows and the DM-Crypt feature for Linux to provide volume encryption for the OS and the data disks. The mechanism also ensures that all data on the virtual machine disks are encrypted at rest within the Azure storage (disks are stored as page BLOBs). The solution is integrated with Azure Key Vault to help managing the disk-encryption keys and secrets in the Key Vault.

Design decisions

|  |
| --- |
| Design Decisions |
| AVE Health SG will use Azure Disk Encryption on all VMs in all Subscriptions. |
| Keys for the Storage Account encryption and Azure Disk Encryption will use Microsoft managed keys. |
| Every Subscription will have Key vault to support key management. However, if any application has requirement can have dedicated Key vault for key management, then it will be provisioned accordingly. |

Table 33: Design Decisions - Azure Data Encryption

Identity

Identity and Access Management

Technical Overview

Identity management is the combination of technical systems, policies and processes that create, define, govern, and synchronize the ownership, utilization and safeguarding of identity information.

In any environment, whether on-premises, hybrid, or cloud-only, IT needs to control which administrators, users, and groups have access to resources. Azure Identity and access management (IAM) services enable you to manage access control in the cloud. Microsoft’s identity solutions span on-premises and cloud-based capabilities. These solutions create a common user identity for authentication and authorization to all resources, regardless of location.

Ave Health will be leveraging Cloud only identity infrastructure with user identities coming from another Azure AD tenant (IHH) as guest accounts in Ave Health AAD tenant.

Identity and access management (IAM) is boundary security in the public cloud. It must be treated as the foundation of any secure and fully compliant public cloud architecture. Azure offers a comprehensive set of services, tools, and reference architectures to help organizations make highly secure, operationally efficient environments. In this section of IAM, we will be discussing various Azure AD features that Ave Health has opted for this engagement and the security decisions around those features.

Design Considerations & Requirements

|  |
| --- |
| Design Considerations and Requirements |
| Microsoft team will test the invitation process from IHH demo tenant created and will also share the PowerShell script that can be used to update the Country attribute for the guest users.  Information of users email address and country will be required from IHH to update and use the same in PowerShell Script. |
| List of trusted IP address will be required for Conditional Access Policies, if applicable. |
| Any pending design decision on “notification email, group selection etc.” will be required from Ave Health. |

Table 34: Requirements and Considerations - Identity and Access Control

|  |
| --- |
| Design Decisions |
| Ave Health will have an Azure AD Cloud only environment, with users coming from IHH Azure AD tenant as Guest accounts. |
| Ave Health will be using "Azure AD Premium 2" licensing and leverage most of the enhanced security features provided by Azure AD. |
| Ave Health tenant name: AveHealthPteLtd.onmicrosoft.com |
| Expected Guest user object count 200. |

Table 35: Design Decisions - Identity and Access Control

Identity Provider

|  |
| --- |
| Design Decisions |
| Identity provider for Ave Health tenant Guest accounts will be the Azure AD tenant from where users will be invited which is IHH Singapore Azure AD tenant. |
| For the non-guest users, the Identity provider will be Ave Health tenant only, as this is a Cloud only environment and no users are currently being synced from on-premises or any other cloud environment. |

Table 36: Design Decisions - Identity Provider

Guest Invitation Process

**Pre-requisites:**

For inviting the users to Ave Health tenant, we need to make sure that below pre-requisites are in place:

1) CSV file with email address of the users to be invited.

2) Country attribute for the users to be invited.

The guest invitation process is segregated into two parts.

First is bulk inviting the users from Azure AD portal.

Second is to update the country attribute for these users using PowerShell script.

**Bulk invite process:**

We will be using Azure AD Bulk invite process for inviting users from IHH tenant to Ave Health Azure AD.

The process uses a CSV template file which will be updated with user’s email address to be invited, redirection URL for the users after accepting invitation and an invitation message.

Once the end user accepts the invitation, he/she will be able to access the resource/application for Ave Health tenant as per the permission given.

**Refer:**  [Tutorial for bulk inviting B2B collaboration users - Azure AD](https://docs.microsoft.com/en-us/azure/active-directory/external-identities/tutorial-bulk-invite)

**Updating country attribute:**

After the bulk invite via Azure AD portal, an Ave Health administrator can start with updating the country attribute for these users, irrespective of whether users have accepted invitation or not.

To do that, an administrator needs to create a CSV file which will have the UPN of the invited users with their country attributed concatenated.

E: g. *user@domain.com;singapore* or *user@domain.com;India*

The same CSV file will be used in the PowerShell script to update the Country attribute for the newly invited guest accounts.

PowerShell script will be shared with Global Administrators of Ave Health tenant.

Azure AD B2B

B2B is an identity feature within AAD that enables an organization to invite partner identities as guest users to securely share resources and collaborate on strategic initiatives. It ensures the resource organization maintains control over its corporate data and access control posture, while enabling safe and secure collaboration with any external partner, large or small, even if they don't have Azure AD or an IT department. A simple invitation and redemption process lets partners use their own credentials to access your company's resources.

We will be leveraging the B2B bulk invite process which will be using a comma-separated value (.csv) file with the user information and invitation preferences. Ave Health has the requirement of updating the Country attribute as well for the users who will be invited and that can be taken care using PowerShell scripting.

The following table documents AAD specific design decisions that have been made for this solution component.

|  |  |  |  |
| --- | --- | --- | --- |
| Category | Topic | Captured Information | Notes |
| AAD Tenant External Identity Settings | Guest user Access settings | Guest users’ access is restricted to properties and membership of their own directory objects | NA |
| Guest Invite Settings | Only users assigned to specific admin roles can invite guest users | NA |
| Guest Invite settings | Allow invitations only to the specified domains (most restrictive) | To be updated, once decided. |

Table 39: External Identities Design decisions

Password Management

Self Service Password Reset (SSPR) will be implemented for non-guest users of Ave health SG tenant which gives them capability to reset/change the password as in when required.

|  |  |  |
| --- | --- | --- |
| Parameter Group | Parameter | Value |
| Properties | Self-service password reset enabled | Selected |
| Select Group | GRP\_SSPR |
| Authentication methods | Number of methods required to reset | *2* |
| Methods available to users | All methods selected:   * Email * Mobile phone * Mobile app code * Mobile app notification * Security Questions |
| Registration | Require users to register when signing in | Yes |
| Number of days before users are asked to re-confirm their authentication information | 180 |
| Notifications | Notify users on password resets | Yes (recommended) |
| Notify all admins when other admins reset their password | Yes (recommended) |
| Customization | Customize helpdesk link | Yes |
| Customize helpdesk email or URL | Rodney’s email (To be changed in future) |
| Security Questions | Number of questions required to register | 4 |
| Number of questions required to reset | 3 |
| Select security questions | * In What city does your nearest sibling live. * In what city was your first job? * What is your favorite food? * What school did you attend for sixth grade? * What was the name of your first pet? |
|  |  |

Table 37: SSPR Design Decisions

Azure AD Group Management

Self-service group management enables users to create and manage security groups or Office 365 groups in Azure Active Directory.

Users can request security group or Office 365 group memberships, and then the owner of the group can approve or deny membership.

Self-service group management features are available only for security groups and Office 365 groups, but not for mail-enabled security groups or distribution lists.

Below table documents the design specific decisions that have been made for group management.

|  |  |  |
| --- | --- | --- |
| Parameter Group | Parameter | Value |
| Self-Service Group Management | Owners can manage group membership requests in the Access Panel | Yes |
| Restrict access to Groups in the Access Panel | Yes |
| Security Groups | Users can create security groups in Azure portals | No |
| Office 365 Groups | Users can create Office 365 groups in Azure portals | No |

Table 38: Group Management Design Decisions

Azure AD Administrator Units

An Administrative Unit is an Azure AD resource that acts as a container for other Azure AD resources like users and groups. It can be useful to restrict administrative scope by using administrative units in organizations that are made up of independent divisions of any kind.

Ave Health Azure AD tenant will be using Administrative units to segregate country wise guest users coming from IHH. Ave Health Azure AD Administrators will identify the Guest account from IHH, which will have privileged roles on AU to manage users and groups.

Highlighting some of the key points decided:

* Dynamic group containing country wise users will be managed by Ave Health Administrators.
* Ave Health Administrators will create and add users/groups to country wise AU. Refer: [Add users, groups, or devices to an administrative unit](https://docs.microsoft.com/en-us/azure/active-directory/roles/admin-units-members-add)
* Ave Health Administrators will identify the IHH guest account to be given elevated permission on AU level, based on the Azure AD roles available and requirement. Refer: [Assign Azure AD roles with administrative unit scope](https://docs.microsoft.com/en-us/azure/active-directory/roles/admin-units-assign-roles)
* Since IHH guest user will be given elevated privileges to manage AU ( Admin unit), the user type of such users need to be changed from Guest to Member, so that the user has access to AU.
* RBAC roles can’t be managed via administrative units.

Refer: [Administrative units in Azure Active Directory](https://docs.microsoft.com/en-us/azure/active-directory/roles/administrative-units) for more details on license requirement, constraints, supported scenarios.

Emergency Access

“Break-glass”, or emergency access accounts mitigate the impact of accidental lack of administrative access. Emergency access accounts are highly privileged accounts that are not assigned to any specific individuals. Access to these accounts is limited to emergency scenarios where normal administrative accounts cannot be used. Microsoft recommends that Ave Health restrict these accounts to use only when it is necessary.

Microsoft will work with Ave Health to ensure at least three cloud-only accounts will be excluded from multi-factor authentication from all conditional access policies.

Sign-in and audit log activity will be monitored to trigger notifications to other administrators when emergency accounts are used.

Ave Health will need to ensure that the passwords are stored in physical format, in a secure and fire-proof place – in at least two locations.

Azure AD Identity Protection

Azure AD Identity Protection currently has three policies that may be enforced for users. Each will trigger the enforcement of a specific action:

* **MFA Registration** Use this policy to enforce the registration for Azure MFA. You can give users a grace period of up to 14 days, after which they are required to complete the registration process.
* **User Risk Policy** This policy requires users whose accounts appear to be compromised to change their password.
* **Sign-in Risk** This policy triggers MFA for users when the sign in behaviour indicates an attempt to compromise their account.

Note: The break-glass user is exempt from these policies to negate the possibility that a malicious user could falsely register the break-glass user for Azure MFA (which is a trusted on first use service). It is important that the password for the break-glass user be complex and only used when specifically required.

Identity Protection for B2B users and its limitations on B2B users.

The user risk for B2B collaboration users is evaluated at their home directory. The real-time sign-in risk for these users is evaluated at the resource directory when they try to access the resource.

With Azure AD B2B collaboration, organizations can enforce risk-based policies for B2B users using Identity Protection and this can be configured via Identity Protection and Conditional Access policies, using sign-in risk as condition.

There are limitations in the implementation of Identity Protection for B2B collaboration users in a resource directory due to their identity existing in their home directory. The main limitations are as follows:

* If a guest user triggers the Identity Protection user risk policy to force password reset, **they will be blocked**. This block is due to the inability to reset passwords in the resource directory.
* **Guest users do not appear in the risky user’s report**. This limitation is due to the risk evaluation occurring in the B2B user's home directory.
* Administrators **cannot dismiss or remediate a risky B2B collaboration user** in their resource directory. This limitation is due to administrators in the resource directory not having access to the B2B user's home directory.

|  |  |  |
| --- | --- | --- |
| Category | Topic | Decision |
| MFA registration Policy | Enabled | Yes |
| Assignment | Group name GRP\_MFA\_REGISTRATION\_REQ (Internal and external users), exclude Break glass accounts |
| Control | Require MFA registration |
| User Risk Policy | Enabled | Yes |
| Assignment | Group name GRP\_USER\_RISK, PIM and break glass accounts to be excluded |
| Conditions (risk level) | High |
| Controls | Block |
| Sign-in Risk Policy | Enabled | Yes |
| Assignment | Group name GRP\_SIGN\_IN\_RISK, PIM and break glass accounts to be excluded |
| Conditions (risk level) | High |
| Controls | Block |
| Send Alerts and weekly digest | Enabled | Yes |
| Risk Level | Low and above |
| DL or Recipient email | TBD, Rodney’s email |

Table 40: Identity Protection Design Decisions

**Note:** Further details on how ‘What is risk’ and how risks may be categorised can be found on the Microsoft Docs link - <https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks>

MFA design decisions

The following table documents the design decisions related to the configuration of Azure MFA service.

|  |  |  |
| --- | --- | --- |
| Category | Topic | Decision |
| Azure MFA | Provider | Azure Multi-Factor Authentication (cloud-hosted, Azure AD-integrated) |
| Method of invocation | Conditional access policy |
| Skip MFA for requests from federated users on the intranet | NA |
| Azure MFA | Trusted IP addresses from which MFA will be skipped | Ave Health to provide if applicable |
| Allowed verification options | Call to phone  Text message to phone  Notification through mobile app  Verification code from mobile app |
| App passwords allowed for applications that use legacy authentication? | No |
| Users allowed to remember multi-factor authentication on devices they trust? | Yes |
| Days allowed before a device must re-authenticate | 1 |

Table 41: MFA Design Decisions

Conditional Access design decisions

Named Locations

When defining locations for use in conditional access policies, we recommend that you define these standard locations:

**Trusted IPs / Internal Networks.** These IP subnets represent locations and networks that have physical access restrictions and/or other controls in place, such as computer system management, network level authentication and intrusion detection. These locations are more secure and conditional access enforcement may be relaxed.

**Doing Business In.** It can be useful when designing a policy to divide countries into two location groups. One represented the areas of the world that employees typically work in vs locations that are typically not working from. By having these locations defined, an organization can apply additional controls to requests that originate from outside the areas where the organization normally operates.

**Locations where MFA may be difficult or impossible.** The nature of some work conditions may mean that requiring MFA is not practical to the extent that staff may be impeded from carrying out their duties. For example, frontline staff performing border protection duties at immigration screening points may not have the time or opportunity to respond to frequent MFA challenges. Another example may be locations where RF screening or electrical interference negate the use of mobile devices. Typically, these locations would be afforded other controls and may be trusted.

Location-based access controls rely on the source IP of a request to determine the location of the user at the time of the request. Although it is non-trivial to spoof on the public Internet, protection afforded by network boundaries may be considered less relevant than it once was. We do not recommend relying solely on location as a condition for access. There are no name location defined

In addition to named locations, you can also define the Azure MFA service with IP ranges where MFA will be bypassed. This affects individual users that have been specifically configured to require MFA (i.e., MFA is enforced). While this also affects MFA challenges that have been triggered by conditional access, we recommend that you use named locations in preference to the bypass list because named locations can be combined with other controls to provide flexibility and granularity.

Require MFA for Admins vs MFA enforcement

Prior to the availability of conditional access policies, MFA was enforced on a per user basis. The user was required to respond to an MFA challenge every time the user authenticated. This is appropriate for highly privileged accounts when the risk from a compromised account outweighs the frequency and intrusiveness of MFA challenges. This approach also requires that MFA enforcement be configured explicitly for each privileged account, and this incurs an administrative burden, which is prone to error.

The **Require MFA for admins** policy is a baseline policy that removes this administration overhead by enforcing MFA for any account that has been assigned to one of the following roles:

Global administrator

Application administrator

Authentication Administrator

Billing administrator

Cloud application administrator

Conditional Access administrator

Exchange administrator

Helpdesk administrator

Password administrator

Privileged authentication administrator

Privileged Role Administrator

Security administrator

SharePoint administrator

User administrator

Note: When enabling this policy, exclude the break-glass accounts to ensure that access can be retained in extreme circumstances. This is in keeping with guidance for securing privileged access for [Azure AD](https://aka.ms/breakglass).

Reference: [Conditional Access: Require MFA for administrators](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-admin-mfa)

Legacy protocols

Conditional access policies are evaluated during the processing of modern authentication requests. Legacy authentication protocols bypass conditional access and therefore may be used as an attack vector when a user’s username and password have been compromised. To negate this vector, a conditional access policy will be defined. This policy will explicitly block access requests that do not use a modern authentication protocol.

The ramification of implementing this policy is that software that does not implement modern authentication may not be useable. This affects generally older versions of applications, because most current versions use the OAuth and OpenID Connect protocols. Ave Health will evaluate the client applications that will be used as each cloud application is onboarded and will ensure that client applications do not use legacy authentication protocols.

Reference: [Conditional Access: Block legacy authentication](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-block-legacy)

Ave Health will be implementing the conditional access policies as described in the table below.

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Assignments | Conditions | Controls |
| Require MFA for  Administrators | Include Elevated Directory roles, excluding break-glass users(s)  All Cloud Apps | None | Grant Access: Require  MFA |
| Require multifactor authentication for guest access | All Guest and external users.  All Cloud Apps | None | Grant Access: Require  MFA |
| Require multifactor authentication for All users | All users, excluding break glass accounts  All Apps | None | Grant Access: Require  MFA |
| Block Legacy Authentication | All users, excluding break glass users  All Cloud Apps | Client apps: Exchange ActiveSync clients  Other clients | Block Access |

Table 43: CA Policies Design Decisions

Note: Ave Health will be using the above conditional access policies as baseline policies and will implement more policies in the future as per business requirement.

Terms of Use

The Terms of use (ToU) feature requires the user to consent to detail provided in a written document (typically a PDF file) before the user is granted access to an application. This consent is recorded and can be audited for tracking purposes. When configured, the ToU becomes a control that may be applied alongside the built-in controls and custom controls (if configured).

The following options may be applied to each ToU:

**Require user to expand the terms of use.** This option requires the user to expand the PDF file that contains the terms of use. When this option is not enabled, users can consent without viewing this content.

**Require users to consent on every device.** This option determines whether the user’s consent is applicable for access requests regardless of the device, or if the user must consent from each of their devices separately.

**Expire consents.** This defines how often each user must consent to the ToU. When enabled, you can configure a specific date, requiring all users to re-consent at that time, you can also configure a frequency that requires users to re-consent on a regular basis.

**Duration before re-acceptance required.** This defines the grace period after a ToU has expired before the user is required to re-consent to the ToU. During this grace period, the user is prompted to consent to the ToU but may decline and still be granted access.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Name | Display name | Document | Require user to Expand Terms of Use and expand on every device | Expire Consent | Re-accept after Number of days |
| TBD | TBD | To be provided by Ave Health | On | No (this will be changed later) | NA |

Table 44:Terms of Use Design Decisions

Terms of Use have not been deployed to Ave Health tenant as the ToU document has not been shared yet. As per the design decisions taken, the ToU document will be provided later.

Reference: [Terms of use in Azure Active Directory](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use)

Privileged Identity Management

The following design decisions were made for Privileged Identity Management

|  |
| --- |
| Design Decisions |
| PIM is required to be enabled as per the Table 16 “RBAC Design Decisions”. |
| Microsoft will help to setup the above role on one of the RG, same or different settings can be used to enable it on any other RG level. |

Table 45: Design Decisions – PIM

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Roles | Description | Admin Assigned | Assignment Type | Role Request Approver | Activation Duration |
| Owner on Root MG Level | Grants full access to manage all resources, including the ability to assign roles in Azure RBAC. | Owner\_Root | Require Activation with Approval - Disallow permanent active | Rodney’s account | 4 hours |

|  |  |  |  |
| --- | --- | --- | --- |
| Category | Topic | Decision | Reasoning |
| AAD Privileged Identity Management | Use of MFA contributor role activation | Yes | Default  <https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settings> |
| Require justification on activation/assignment | Enabled | Default |
| Require ticket information on activation | Enabled | Link the PIM audit trail to specific ticketing system items |
| Approval required on activation of each role | Enabled | Protect highly privileged Administrator roles with approval |
| Activation maximum duration (hours) | 4 hours |  |
| Access Reviewers | TBD | Recommended to be **at least** two people |
| Role Approvers | Rodney | Recommended to be **at least** two people |

Table 46: PIM Design Decisions

Same PIM settings have been enabled for all the roles decided as per the “RBAC design decision” table.

Ave Health is not currently using PIM groups to give permission to the users, as there is currently one approver decided.

Appendix

HLD Network Architecture – Ave Health and IHH Infra in Ave Health Azure Platform (Interim Solution)

Graphical user interface, diagram, application

Description automatically generated

References

The following table contains links to information that provides context for the design and plan:

|  |  |
| --- | --- |
| Content | Description |
| [Hub-spoke network topology in Azure](https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke) | This article explains hub-and-spoke network topology in Azure |
| [About cryptographic requirements and Azure VPN gateways](https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-compliance-crypto) | This article discusses configuration of Azure VPN Gateways to satisfy cryptographic requirements for cross-premises S2S VPN tunnels |
| [ExpressRoute and Site-to-Site coexisting connections](https://docs.microsoft.com/en-us/azure/expressroute/expressroute-howto-coexist-resource-manager) | This article discusses configuration of coexisting ExpressRoute and Site-to-Site VPN connections. |
| [Azure DevOps pricing](https://azure.microsoft.com/en-us/pricing/details/devops/azure-devops-services/) | This page provides pricing information for Azure DevOps |
| [Azure Policy samples](https://docs.microsoft.com/en-us/azure/governance/policy/samples/) | This page is an index of built-in Azure Policy definitions |
| [Azure Subscription and service limits, quotas, and constraints](https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/azure-subscription-service-limits) | This article lists some of the Microsoft Azure limits, also called quotas |
| [RBAC for Azure resources](https://docs.microsoft.com/en-us/azure/role-based-access-control/overview) | This article provides information about RBAC for Azure resources |
| [Recommended naming and tagging convention](https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-best-practices/naming-and-tagging) | This guide provides naming and tagging recommendations for Azure resources |
| [Subscription decision guide](https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/decision-guides/subscriptions/) | This decision guide describes different approaches to organizing Management Group and Subscriptions hierarchy. |
| [Update Management solution in Azure](https://docs.microsoft.com/en-us/azure/automation/automation-update-management) | This article provides information about Update Management solution in Azure Automation used to manage Operating System updates |
| [Enterprise-scale architecture](https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/architecture) | This series of articles explain Microsoft’s enterprise-scale architecture blueprint (formerly known as “North Star” architecture), which is optimized for large corporations with complex IT systems. |
| [Azure Monitor](https://docs.microsoft.com/en-us/azure/azure-monitor/overview) | This article introduces Azure Monitor and accompanying services. |
| [Azure Information Protection](https://docs.microsoft.com/en-us/azure/information-protection/what-is-information-protection) | This article provides an overview of Azure Information Protection, which enables DLP together with O365. |
| [Azure Architecture Centre](https://docs.microsoft.com/en-us/azure/architecture/) | This page provides an excellent entry point when planning and designing workloads on Azure. It contains reference architectures, best practices, optimization advise and more. |
| [Azure security best practices and patterns](https://docs.microsoft.com/en-us/azure/security/fundamentals/best-practices-and-patterns) | This page contains links to articles which contain security best practices to use when designing, deploying, and managing cloud solutions in Azure. |
| [Microsoft Cybersecurity Reference Architecture](https://www.microsoft.com/security/blog/2018/06/06/cybersecurity-reference-architecture-security-for-a-hybrid-enterprise/) | This page provides a reference architecture that shows how to integrate existing Azure products and offerings from a security point of view. |
| [Create an Azure support request](https://docs.microsoft.com/en-us/azure/azure-portal/supportability/how-to-create-azure-support-request) | This article shows how to open support tickets in Azure in case of any problems. |
| [Enabling Enterprise Governance in Azure – Case Study](https://www.microsoft.com/en-us/itshowcase/enabling-enterprise-governance-in-azure) | This page contains a case study illustrating how to successfully apply enterprise governance in Azure. |
| [IPv6 on Azure](https://docs.microsoft.com/en-us/azure/virtual-network/ipv6-overview) | The document details considerations for IPv6 on Azure |

Table 48: References

Glossary of terms

|  |  |
| --- | --- |
| Abbreviation | Description |
| API | Application Programming Interface |
| ARM | Azure Resource Manager |
| Azure AD | Azure Active Directory |
| DNS | Domain Name Services |
| IaC | Infrastructure as Code |
| IDaaS | Identity as a Service |
| MFA | Multi Factor Authentication |
| MG | Management Group |
| MMA | Microsoft Monitoring Agent |
| NSG | Network Security Groups |
| RBAC | Role Based Access Control |
| SSL | Secure Socket Layer |
| SSD  HDD | Solid-State Drive  Hard Disk Drive |
| TLS | Transport Layer Security |
| UDR | User Defined Routes |
| VM | Virtual Machine |
| VNet | Virtual Network |
| VPN | Virtual Private Network |

Table 49: Glossary of Terms