<customer logo here>

**Cloud Adoption Framework -**

**Enterprise Scale Landing Zone**

**Design Document**

Prepared for

<Customer\_Name>

12/16/2022

Version 1.0 Draft

Prepared by

**<Author\_Name>**

**<Author\_position>**

**<email\_address>**

Revision and Signoff Sheet

Change Record

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Author | Version | Change Reference |
|  |  |  |  |
|  |  |  |  |

Reviewers

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Version Approved | Position | Date |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1 Background 9](#_Toc122081525)

[2 Glossary of terms 10](#_Toc122081526)

[3 Design Document Sign-off (Optional) 11](#_Toc122081527)

[4 Introduction 12](#_Toc122081528)

[4.1 Project Overview 14](#_Toc122081529)

[4.2 Document Purpose 14](#_Toc122081530)

[4.3 Intended Audience 15](#_Toc122081531)

[5 Intentionally Left Blank 16](#_Toc122081532)

[6 Design Overview 17](#_Toc122081533)

[6.1 Enterprise Agreement Hierarchy 19](#_Toc122081534)

[6.1.1 EA Hierarchy Design Decisions 20](#_Toc122081535)

[6.1.2 EA Cost Management 20](#_Toc122081536)

[6.2 Management Group and Subscription Organization 21](#_Toc122081537)

[6.2.1 Management Groups 21](#_Toc122081538)

[6.2.2 Azure Subscriptions 23](#_Toc122081539)

[6.2.3 Resource Groups 24](#_Toc122081540)

[6.3 Identity and Access Management 26](#_Toc122081541)

[6.3.1 <CUSTOMER\_NAME> Hybrid Identity Setup 26](#_Toc122081542)

[6.3.2 Multi-Factor Authentication 26](#_Toc122081543)

[6.3.3 Design Decisions 26](#_Toc122081544)

[6.3.4 Break Glass Accounts 27](#_Toc122081545)

[6.3.5 Azure AD Groups 27](#_Toc122081546)

[6.4 Networking 31](#_Toc122081547)

[6.4.1 Design Considerations 32](#_Toc122081548)

[6.4.2 Design Decisions 32](#_Toc122081549)

[6.4.3 Design Pattern: Hub/Spoke Virtual Networks Peerings (Hub/Spoke VNET) 33](#_Toc122081550)

[6.4.4 Design Pattern: Network Segmentation 36](#_Toc122081551)

[6.4.5 Design Pattern: Virtual Networks Connectivity 36](#_Toc122081552)

[6.4.6 Design Pattern: Network Expansion for multiple environments 37](#_Toc122081553)

[6.4.7 Network Address Spaces and Subnets 37](#_Toc122081554)

[6.4.8 Azure Hybrid DNS Resolution 38](#_Toc122081555)

[6.4.9 Network Connectivity and Security Components 39](#_Toc122081556)

[6.5 Platform Management and Monitoring 42](#_Toc122081557)

[6.5.1 Overview 42](#_Toc122081558)

[6.5.2 Azure Naming Convention 43](#_Toc122081559)

[6.5.3 Azure Tags 44](#_Toc122081560)

[6.5.4 Azure Resource Locks 45](#_Toc122081561)

[6.5.5 Azure Cost Management 46](#_Toc122081562)

[6.5.6 Azure Advisor 47](#_Toc122081563)

[6.5.7 Azure Automation for Update Management 48](#_Toc122081564)

[6.5.8 Logging and Monitoring 50](#_Toc122081565)

[6.6 High Availability, Backup and Disaster Recovery 52](#_Toc122081566)

[6.6.1 High Availability 52](#_Toc122081567)

[6.6.2 Azure Backup 53](#_Toc122081568)

[6.6.3 Business Continuity and Disaster Recovery 54](#_Toc122081569)

[6.7 Security, Policy and Governance 59](#_Toc122081570)

[6.7.1 Policy Management 59](#_Toc122081571)

[6.7.2 Microsoft Defender for Cloud (used to be Azure Security Center) 68](#_Toc122081572)

[6.7.3 Microsoft Sentinel (used to be Azure Sentinel) 70](#_Toc122081573)

[6.7.4 Azure Key Vault 73](#_Toc122081574)

[6.7.5 Azure Data Encryption 73](#_Toc122081575)

[6.7.6 Managed Images for OS Hardening 75](#_Toc122081576)

[7 Appendix 76](#_Toc122081577)

[7.1 References 76](#_Toc122081578)

Table of Figures

[Figure 1: <CUSTOMER\_NAME> Enterprise Scale Landing Zone Design Overview 22](#_Toc106268802)

[Figure 2: EA Enrolments 24](#_Toc106268803)

[Figure 3: Management Group and Subscription Structure Overview. 28](#_Toc106268804)

[Figure 4 <CUSTOMER\_NAME> - High Level Network Design 37](#_Toc106268805)

[Figure 5: Sample HUB & Spoke Peering 38](#_Toc106268806)

[Figure 6: <CUSTOMER\_NAME> application onboarding network framework 39](#_Toc106268807)

[Figure 7: Network architecture reference for multiple environments 41](#_Toc106268808)

[Figure 8: Hybrid DNS Resolution Architecture Reference 42](#_Toc106268809)

[Figure 9: Azure Firewall 43](#_Toc106268810)

[Figure 10: Azure Platform Management and Monitoring Overview 46](#_Toc106268811)

[Figure 11: Azure Automation for Update Management 52](#_Toc106268812)

[Figure 12: Azure Monitor Overview diagram 54](#_Toc106268813)

[Figure 13: Azure Availability Zones 56](#_Toc106268814)

[Figure 14 Azure Site Recovery over multi-region sample architecture 60](#_Toc106268815)

[Figure 15 Backup and Disaster Recovery 61](#_Toc106268816)

[Figure 16: Evaluation order flow diagram for the different policy conditions 65](#_Toc106268817)

[Figure 17: Microsoft Sentinel 73](#_Toc106268818)

[Figure 18: Microsoft Sentinel Integrability view 74](#_Toc106268819)

Table of Tables

[Table 1: Glossary of Terms 11](#_Toc106268820)

[Table 2: Guiding Principles 19](#_Toc106268821)

[Table 3: EA Hierarchy Design Decisions 25](#_Toc106268822)

[Table 4: EA Cost Management Design Decisions 25](#_Toc106268823)

[Table 5: Requirements and Considerations for Management Group structure. 26](#_Toc106268824)

[Table 6: Design Decisions - Management Groups 27](#_Toc106268825)

[Table 7: Requirements and Considerations – Subscriptions 29](#_Toc106268826)

[Table 8: Design Decisions - Subscriptions 29](#_Toc106268827)

[Table 9: Design decisions - Resource Groups 30](#_Toc106268828)

[Table 10: IAM Design Decisions 31](#_Toc106268829)

[Table 11: Break Glass Accounts Detail 32](#_Toc106268830)

[Table 12: Azure AD Group Decisions 33](#_Toc106268831)

[Table 13: Azure AD Group and RBAC 35](#_Toc106268832)

[Table 14: Networking Design Considerations 36](#_Toc106268833)

[Table 15: Networking Design Decisions 37](#_Toc106268834)

[Table 16: Types of VNETs in Azure 40](#_Toc106268835)

[Table 17: VNET and address Space 41](#_Toc106268836)

[Table 18: Network Components 46](#_Toc106268837)

[Table 19: Naming Convention Requirements 47](#_Toc106268838)

[Table 20: Naming Convention Decisions 47](#_Toc106268839)

[Table 21: Design Decisions - Azure Tags 48](#_Toc106268840)

[Table 22: Suggestion for initial tags 49](#_Toc106268841)

[Table 23: Requirements and Considerations - Resource Locks 49](#_Toc106268842)

[Table 24: Design Decisions - Resource Locks 50](#_Toc106268843)

[Table 25: Azure Billing - Scopes 50](#_Toc106268844)

[Table 26: Design Decisions - Azure Advisor 52](#_Toc106268845)

[Table 27: Automation for Update Management Design Decision 53](#_Toc106268846)

[Table 28: Patch or Update Policy Design Decisions 53](#_Toc106268847)

[Table 29 Platform Monitoring Design Considerations 55](#_Toc106268848)

[Table 30 Platform Monitoring Decision Decisions 55](#_Toc106268849)

[Table 31: Design Decisions 57](#_Toc106268850)

[Table 32 Azure Backup and BCDR Design Considerations 57](#_Toc106268851)

[Table 33 Azure Backup and BCDR Design Decisions 58](#_Toc106268852)

[Table 34: BCDR Design Decisions 58](#_Toc106268853)

[Table 35: Requirements and Considerations - Azure Policy 65](#_Toc106268854)

[Table 36: Design Decisions - Azure Policy 69](#_Toc106268855)

[Table 37: Design Decisions 70](#_Toc106268856)

[Table 38: Microsoft Defender for Cloud feature comparison 72](#_Toc106268857)

[Table 39: Design Decisions – Microsoft Defender for Cloud 72](#_Toc106268858)

[Table 40: Design Decisions - Key Vault 75](#_Toc106268859)

[Table 41: Microsoft Encryption Options 76](#_Toc106268860)

[Table 42: Azure Encryption Technologies 76](#_Toc106268861)

[Table 43: Design Decisions - Azure Data Encryption 77](#_Toc106268862)

[Table 44: References 79](#_Toc106268863)

1. Background

The origin of this document request from <CUSTOMER\_NAME> stems from Microsoft Umbrella Program, which is meant to be an enablement or educational program to guide <CUSTOMER\_NAME> to develop their design. Upon request, this document is prepared to compile the design decisions and write-ups for design understanding.

1. 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 |
| IAM | Identity Access Management |
| IDaaS | Identity as a Service |
| MFA | Multi-Factor Authentication |
| MG | Management Group |
| MMA | Microsoft Monitoring Agent |
| NSG | Network Security Groups |
| MSI | Managed Services Identity |
| RBAC | Role Based Access Control |
| SSL | Secure Socket Layer |
| SSD | Solid-State Drive |
| HDD | Hard Disk Drive |
| TLS | Transport Layer Security |
| UDR | User-Defined Routes |
| VM | Virtual Machine |
| VNET | Virtual Network |
| VPN | Virtual Private Network |
| SEA | Southeast Asia |
| CMK | Customer Managed Keys |
| PMK | Platform Managed Keys |
| PIM | Privileged Identity Management |
| CCoE | Cloud Center of Excellence |
| MVP | Minimum Viable Product |
| B2B | Business to Business |
| EA | Enterprise Agreement |
| ER | Express Route |

Table 1: Glossary of Terms

1. Design Document Sign-off (Optional)

The table lists the respective stakeholders from <CUSTOMER\_NAME>, and their corresponding areas of responsibility, followed by their signatory.

|  |  |
| --- | --- |
| **Landing Zone Area of Responsibility** | **Description** |
| Enterprise Agreement Hierarchy | * Planning for Enterprise Enrolment |
| “Identity and Access Management | * Planning for IAM * Authentication in Landing Zone * Azure AD Tenants |
| Network Topology and connectivity | * Traditional Azure Network Topology * Network Encryption Requirements * Traffic Inspection |
| Platform Management and Monitoring | * Planning for Platform Management and Monitoring |
| Security, Policy and Governance | * Define Encryption and Key Management * Planning for Governance * Define security Monitoring and Audit Policy * Planning for Platform Security |

Reviewed and approved by:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

<Date>

<Approver Name>

<Approver Role>

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

<Date>

<Approver Name>

<Approver Role>

1. Introduction

This document is delivered to <CUSTOMER\_NAME> 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 on-premises architecture into the cloud. While giving direction to <CUSTOMER\_NAME> on deploying their 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 <CUSTOMER\_NAME> 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 workloads/business systems deployment for the Business entities within their Landing Zones.

Azure Landing Zones are environments that consider scale, security, governance, and identity to support application migration or greenfield deployments based on standard 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 the <CUSTOMER\_NAME> 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, 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 <CUSTOMER\_NAME>, 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. Authentication, role-based access, and identity management will be administered centrally in the cloud.

This document does not explain how to create environments or how certain features work. Instead, it reports the choices and valid concepts for the specific <CUSTOMER\_NAME> context and identified scenarios. Utmost care was taken to ensure that the design meets all requirements voiced by <CUSTOMER\_NAME> 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 <CUSTOMER\_NAME> 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 solid 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 for the Platform related services, workload should be the choice of <CUSTOMER\_NAME> based on the system’s needs. Essentially, this means that when choosing an Azure solution for a particular use case, products that provide <CUSTOMER\_NAME> with the slightest responsibility management (while still meeting the required amount of configurability) should be preferred.  This reduces the operative effort for <CUSTOMER\_NAME> and 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 a primary security boundary | With the advent of public clouds and hybrid networks, traditional security boundaries such as perimeter networks 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-set 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 <CUSTOMER\_NAME>’s Landing Zone. |

Table 2: Guiding Principles

* 1. Project Overview

This project is scoped to design an Enterprise Scale Landing Zone (ESLZ) for <CUSTOMER\_NAME> to allow onboarding of upcoming API Management project and other future workloads. An ESLZ is meant to guardrail cloud environment with the required compliance decided by <CUSTOMER\_NAME> or other authoritative organization such as Bank Negara Malaysia.

* 1. 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 <CUSTOMER\_NAME> between the 30th Apr and 17th May 2021. Decisions made during subsequent planning meetings have also been captured in this document.

* 1. Intended Audience

This document is intended for the <CUSTOMER\_NAME> project resources who will be responsible for the solution after it is delivered. It assumes a basic working knowledge of Azure Platform, Cloud Services, Infrastructure- and Platform-as-a-Service.

1. Intentionally Left Blank
2. Design Overview

The following diagram represents the logical view of the Enterprise Scale cloud platform and its relation to Landing Zones for <CUSTOMER\_NAME> . This design includes the Core Cloud Platform, and its supporting services.

<Update diagram based on customer design workshop>

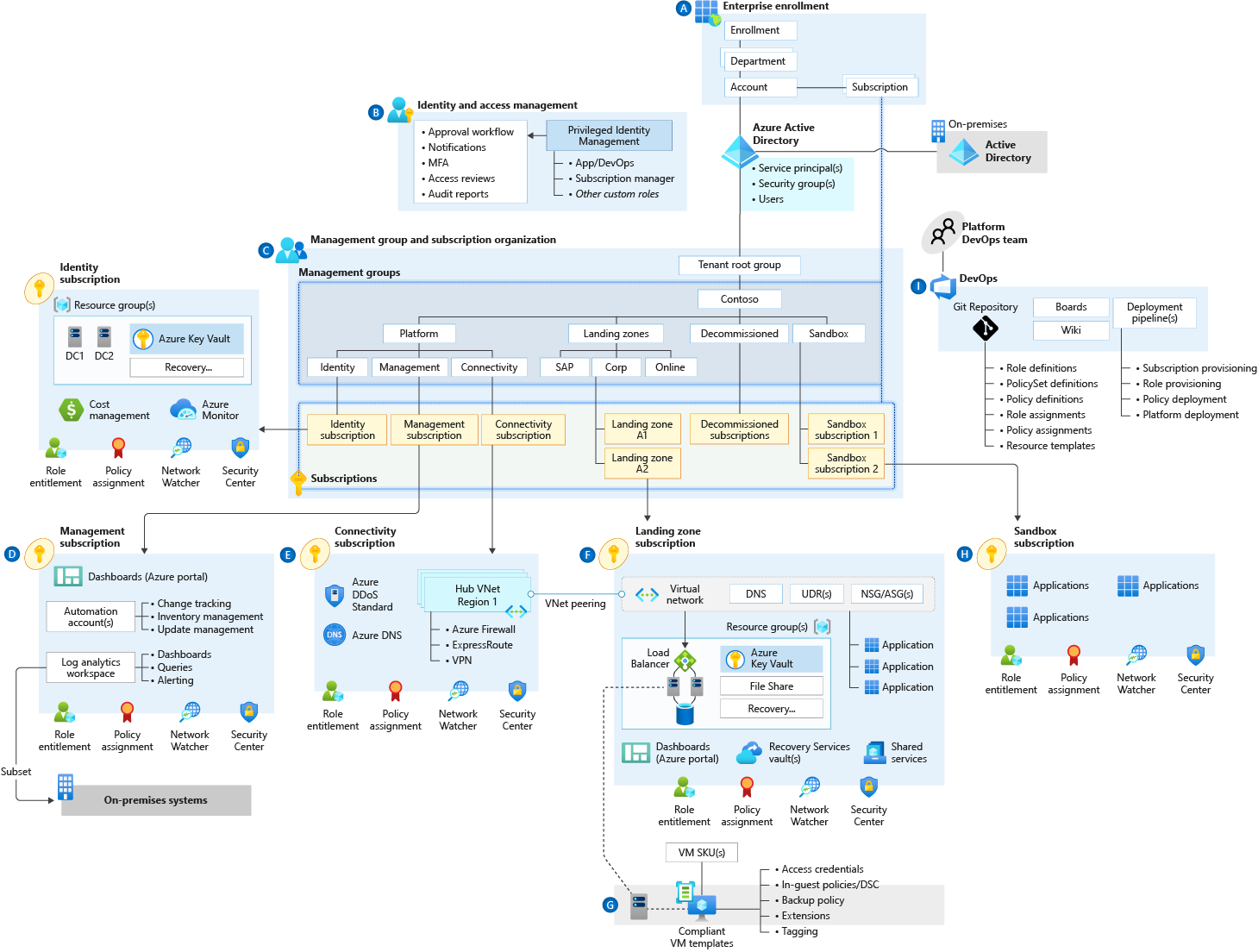


Figure 1: <CUSTOMER\_NAME> Enterprise Scale Landing Zone Design Overview

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

**Note**: This Enterprise-scale design includes considerations for future services in the Core Cloud Platform, such as Active Directory Domain Services, DNS Forwarder, and landing zone resources which are not part of this current project scope.

Core Cloud Platform Components

<Update the following components based on customer input, below are for reference>

A single Connectivity subscription will be provisioned. 2 Hub VNETs will be provisioned in the Connectivity subscription, 1 for production and 1 for non-production.

1. Single Express Route circuit is planned but not within the scope of this project.
2. On-premises network will be connected to VPN Gateway in Hub VNET for S2S connectivity until Express Route circuit and Express Route Gateway is established.
3. Bastion host or Jump host subnet is prepared but the decision and deployment is not within the scope of this project.
4. Azure Firewall will be incorporated in the Hub to manage internet traffic to and from Azure. This will provide routing for cross-application connections as well as further connectivity based on the Firewall Rules.
5. Azure Network Performance Monitoring Agents will be used to monitor Network/Gateway (and any future private connection components) latency, bandwidth utilization and loss at the Gateway level.
6. A centralized Log Analytics workspace will be created in the compliance Subscription to collect all the security related (Microsoft Defender for Cloud) activity across the subscriptions in the Azure Tenant. This does not require network connectivity of any form between target and source.
7. A centralized Log Analytics workspace will be created in the Audit Subscription to collect all the Network and platform related (Microsoft Defender for Cloud) activity across the subscriptions in the Azure Tenant.
8. All subscriptions will be configured with Network Watcher, Microsoft Defender for Cloud Basic Tier and Azure Monitor to ensure compliance and optimal performance of all Azure resources.
9. Azure DDOS Basic Plan will be deployed to the Connectivity Subscription.
10. Azure AD Privileged Identity Management will protect privileged roles.
11. Management Groups and subscription level will be used to manage access and governance at scale.

Landing Zone Specific Components

1. A Landing Zone structure will be set up to cater to the various application and data platform workloads as and when required. Currently it’s not in scope and this design document will not capture any Landing Zone requirements.
   1. Enterprise Agreement Hierarchy

<CUSTOMER\_NAME> is planning to utilize their enterprise agreement to purchase Azure services. An Enterprise Agreement (EA) enrolment represents the commercial relationship with Microsoft and how <CUSTOMER\_NAME> uses Azure. It provides the basis for billing across all Subscriptions and affects administration of Azure. The current breakdown of the <CUSTOMER\_NAME> EA Enrolment structure is as follows:

<Update diagram based on customer design workshop>

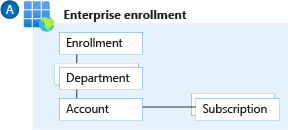


Figure 2: EA Enrolments

<CUSTOMER\_NAME> will have single department (IT) to segment costs into logical groupings and to set a budget or quota will be done at the Management Group level. The quota isn't enforced firmly and is used for reporting purposes.

1. Subscriptions are the smallest unit in the Azure enterprise portal. They are containers for Azure services managed by the service administrator. They are also where an organization deploys Azure services.
2. Accounts are organizational units in the Azure enterprise portal. They can be used to manage Subscriptions and access reports. Accounts can be added, and names can be changed as required.
3. Departments are the parent organizational units for accounts. They can be added, and names can be changed as required.
4. There can be multiple subscriptions under Account and multiple accounts under department.
5. EA enrolment roles link users with their functional role. These roles are:

* Enterprise administrator
* Department administrator
* Account owner
* Service administrator
* Notification contact
  + 1. EA Hierarchy Design Decisions

|  |  |
| --- | --- |
| ID | Description |
| DD01 | Current EA hierarchy only has a single department named “<department\_name>” |
| DD02 | Additional departments will be added as Azure workloads expands across <CUSTOMER\_NAME> organization for management. |
| DD03 | Account Name “<account\_name>” |

Table 3: EA Hierarchy Design Decisions

* + 1. EA Cost Management

Within EA portal, there is a simple cost management tool which allows <CUSTOMER\_NAME> to configure budget and threshold alerts. This alert can be set at department level when the budget usage has reached certain quota thresholds. This only serves as an alerting tool and does not apply a hard spending limit for the subscriptions under the department.

* + - 1. Design Decisions

|  |  |
| --- | --- |
| ID | Description |
| DD01 | <CUSTOMER\_NAME> sets quota threshold alerts at 50%, 70%, and 90% of the budgetary amount |
| DD02 | Current decided budget is 1000$, to be adjusted when new budget is determined |
| DD03 | Quota usage notification will be sent to example@<customer\_name>group.com |

Table 4: EA Cost Management Design Decisions

* 1. Management Group and Subscription Organization
     1. Management Groups
        1. 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 <CUSTOMER\_NAME> 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.

* + - 1. Design Considerations and Requirements

|  |  |
| --- | --- |
| ID | Description |
| DC01 | <CUSTOMER\_NAME> would like to remain in control of shared services and certain workload aspects. |
| DC02 | Enterprise Scale will be used as the framework for the Management Group structure. |
| DC03 | The structure needs to allow <CUSTOMER\_NAME> to abide the regulatory requirements for RMIT |

Table 5: Requirements and Considerations for Management Group structure.

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

|  |  |  |
| --- | --- | --- |
| Management Group  Display Name | Management Group Id | Remarks |
| <CUSTOMER\_NAME>-LZ | <CUSTOMER\_NAME>-LZ | This MG represents the root for <CUSTOMER\_NAME> as an organization. |
| <CUSTOMER\_NAME>-LZ-Platform | <CUSTOMER\_NAME>-LZ-Platform | Platform MG to contain connectivity, identity, and management. |
| <CUSTOMER\_NAME>-LZ-Management | <CUSTOMER\_NAME>-LZ-Management | Child MG of <CUSTOMER\_NAME>-LZ-Platform.  This MG will contain platform management and monitoring resources. |
| <CUSTOMER\_NAME>-LZ-Connectivity | <CUSTOMER\_NAME>-LZ-Connectivity | Child MG of <CUSTOMER\_NAME>-LZ-Platform.  This MG contains connectivity subscription, Azure Hub, and networking resources. |
| <CUSTOMER\_NAME>-LZ-Identity | <CUSTOMER\_NAME>-LZ-Identity | Child MG of <CUSTOMER\_NAME>-LZ-Platform.  Supporting feature management for identity.  Deploying addition Domain Controller.  Policies to manage identity Subscription. |
| <CUSTOMER\_NAME>-LZ-Decommissioned | <CUSTOMER\_NAME>-LZ-Decommissioned | Manage the decommissioned subscriptions |
| <CUSTOMER\_NAME>-LZ-Sandboxes | <CUSTOMER\_NAME>-LZ-Sandboxes | Manage the sandbox subscription.  Policies to manage Sandbox subscriptions. |
| <CUSTOMER\_NAME>-LZ-MY | <CUSTOMER\_NAME>-LZ-MY | This MG will be used to contain all workload, data and application subscription and resources. |
| Group-Digital | Group-Digital | Child MG of <CUSTOMER\_NAME>-LZ-MY. |
| Non-Production | Non-Production | Child MG of Group-Digital. For non-production workloads |
| Production | Production | Child MG of Group-Digital. For production workloads |

Table 6: Design Decisions - Management Groups

These decisions are summarized in the following diagram:



Figure 3: Management Group and Subscription Structure Overview.

* + 1. Azure Subscriptions
       1. 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 to.

Multiple Subscriptions can be created to separate workloads by financial and administrative 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.

Democratization of Subscriptions is also important in an Enterprise Scale Landing Zone to avoid hitting quota limits per subscriptions.

* + - 1. Requirements and Considerations

The following requirements will influence the Subscription design pattern:

|  |  |
| --- | --- |
| ID | Description |
| DC01 | <CUSTOMER\_NAME> wishes to target Subscriptions to services/projects with a breakdown depending on deployment environment (e.g., dev/prod/non prod) |
| DC02 | Subscription breakdown is driven at a service level to ensure proper cost allocation is performed on resources used by projects. |
| DC03 | 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). |
| DC04 | Where services are to be shared between landing zones, they should be located within one of the Platform subscriptions e.g., Identity, Connectivity, Management |

Table 7: Requirements and Considerations – Subscriptions

* + - 1. Design Decisions

The following table documents the design decisions related to Subscriptions:

|  |  |  |
| --- | --- | --- |
| Description | Subscription Name | Remarks |
| Management Subscription | Management | For management resources such as monitoring, automation account |
| Identity Subscription | Identity | For identity related resources such as DC VMs or Azure Active Directory Domain Services (AAD DS) |
| Connectivity Subscription | Connectivity | For network and connectivity related resources e.g. VPN GW, Firewall, DNS forwarder. |
| Dev API Platform Subscription | Dev API Platform | For APIM project resources, which is not part of this scope, only subscription is created before project onboarding |
| UAT API Platform Subscription | UAT API Platform | For APIM project resources, which is not part of this scope, only subscription is created before project onboarding |

Table 8: Design Decisions - Subscriptions

* + 1. Resource Groups
       1. 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.

* + - 1. Design Decisions

The following table documents the design decisions related to RGs:

|  |  |  |  |
| --- | --- | --- | --- |
| Subscription Name | Region | Resource Group Name | Description |
| Management | SEA | Cloud-shell-storage-southeastasia | Azure Portal CLI usage |
| SEA | DefaultResourceGroup-SEA | Azure Portal CLI usage |
| SEA | <CUSTOMER\_NAME>-LZ-MY-mgmt | For management resources |
| Identity | SEA | <CUSTOMER\_NAME>-LZ-MY-vnet-southeastasia | For identity resources such as DC VMs, AAD DS |
|  | NetworkWatcherRG | For network watcher monitoring resource |
| Connectivity | SEA | <CUSTOMER\_NAME>-LZ-MY-vnethub-southeastasia | For Hub resources |
|  | NetworkWatcherRG | For network watcher monitoring resource |
|  | <CUSTOMER\_NAME>-LZ-MY-privatedns | For private DNS resource |
| dev api platform | SEA | <CUSTOMER\_NAME>-LZ-MY-asc-export | For Azure Security Center / Microsoft Defender for Cloud log |
|  | NetworkWatcherRG | For network watcher monitoring resource |
| uat api platform | SEA | <CUSTOMER\_NAME>-LZ-MY-asc-export | For Azure Security Center / Microsoft Defender for Cloud log |

Table 9: Design decisions - Resource Groups

* 1. Identity and Access Management

When it comes to managing cloud resources, a key aspect of cloud security is identity, the primary security boundary. 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 provides further control granularity on Azure resources and authentication scenarios.

* + 1. <CUSTOMER\_NAME> Hybrid Identity Setup

<CUSTOMER\_NAME> has an existing integration between Portaldom AD to Azure AD via AD Connect Sync and leverages on ADFS for authentication. The current setup is a one-way synchronization to Azure AD where all identity management in <CUSTOMER\_NAME> is controlled in Portaldom AD.

* + 1. Multi-Factor Authentication

As identity becomes the core security component, authentication process becomes more important for secure login. In Azure, MFA login is recommended, and Microsoft Authenticator app is recommended for seamless native support.

* + 1. Design Decisions

|  |  |
| --- | --- |
| ID | Description |
| DD01 | MFA to be enforced for all users accessing Azure using Microsoft Authenticator App |
| DD02 | Azure AD PIM to be enabled for CCoE team |
| DD03 | <CUSTOMER\_NAME> to leverage on built-in RBAC roles and determine if custom roles are required |
| DD04 | AD Groups to be created to segregate responsibility and RBAC role assignments |
| DD05 | <CUSTOMER\_NAME> will create two break glass accounts for local admin access to Azure in case all Azure AD admin users are unable to login. |
| DD06 | <CUSTOMER\_NAME> will maintain single Azure AD tenant that is synced with on-premises production AD via AD Connect Sync. |
| DD07 | Azure AD PIM to be expanded to the larger group as more users are onboard to Azure environment. |
| DD08 | All identity management should be controlled from <CUSTOMER\_NAME> Portaldom AD and synchronized one-way via AD Connect Sync only. |
| DD09 | No guest users should be created in Azure AD by global administrator unless justified to prevent floating identities not managed by <CUSTOMER\_NAME> IAM team; No other users should be given access to any AD roles that has permission to create new users or new guest users. |

Table 10: IAM Design Decisions

* + 1. Break Glass Accounts

|  |  |
| --- | --- |
| Username | Metadata |
| emergencyAccount1 | Name : emergency account 1  First name : emergency  Last name : account  Job title : cloud administrator  Department : cloud centre of excellence  Company : <CUSTOMER\_NAME> group |
| emergencyAccount2 | Name : emergency account 2  First name : emergency  Last name : account  Job title : cloud administrator  Department : cloud centre of excellence  Company : <CUSTOMER\_NAME> group |

Table 11: Break Glass Accounts Detail

* + - 1. Ownership of Break Glass Accounts

Request process: TBD (CCoE team to close with IT Security team)

* + 1. Azure AD Groups

Azure Active Directory (Azure AD) lets you use groups to manage access to your cloud-based apps, on-premises apps, and your resources. Your resources can be part of the Azure AD organization, such as permissions to manage objects through roles in Azure AD, or external to the organization, such as for Software as a Service (SaaS) apps, Azure services, SharePoint sites, and on-premises resources.

The following table is the planned groups for <CUSTOMER\_NAME> members:

|  |  |  |
| --- | --- | --- |
| User | Email | Groups |
| Mohammad Faisal Bin Poat Kamal | [mohammad.faisal.poat@<customer\_name>group.com](mailto:mohammad.faisal.poat@rhbgroup.com) | API Platform  LZ Admin |
| Muhammad Ashraf bin Ahmad Fuad | [muhammad.ashraf.ahmad@<customer\_name>group.com](mailto:muhammad.ashraf.ahmad@rhbgroup.com) | API Platform |
| Goh Joon Sern | [goh.joon.sern@<customer\_name>group.com](mailto:goh.joon.sern@rhbgroup.com) | API Platform |
| Mohamed Haikal bin Mohamed Ghazali | [mohamed.haikal.mohamed@<customer\_name>group.com](mailto:mohamed.haikal.mohamed@rhbgroup.com) | API Platform |
| Mohd Khairulnizam bin Md Dahari | [mohd.khairulnizam.md@<customer\_name>group.com](mailto:mohd.khairulnizam.md@rhbgroup.com) | <CUSTOMER\_NAME>.me |
| Mazlan bin Musa | [mazlan.musa@<customer\_name>group.com](mailto:mazlan.musa@rhbgroup.com) | <CUSTOMER\_NAME>.me |
| Muhammad Iqbal bin Arpin | [muhammad.iqbal.arpin@<customer\_name>group.com](mailto:muhammad.iqbal.arpin@rhbgroup.com) | <CUSTOMER\_NAME>.me |
| Mohd Alif bin Jasin | [mohd.alif.jasin@<customer\_name>group.com](mailto:mohd.alif.jasin@rhbgroup.com) | Cloud Architecture |
| Mohd Azlan Bin Hussein | [visnu.mohd.azlan@<customer\_name>group.com](mailto:visnu.mohd.azlan@rhbgroup.com) | Cloud Architecture |
| Matthew Yong Jian Chung | [matthew.yong@<customer\_name>group.com](mailto:matthew.yong@rhbgroup.com) | Cloud Architecture |
| Navenra a/l Balakrishnan  (global admin) | [navenra.balakrishnan@<customer\_name>group.com](mailto:navenra.balakrishnan@rhbgroup.com) | LZ Admin |
| Low Kok Leong | [low.kok.leong@<customer\_name>group.com](mailto:low.kok.leong@rhbgroup.com) | LZ Admin |
| Cheong Jin Shi | cheong.jin.shi@<customer\_name>group.com | LZ Admin |

Table 12: Azure AD Group Decisions

The following table is the decided construct of operational teams in <CUSTOMER\_NAME> with the closest corresponding least-privilege RBAC, until justified otherwise. Users to be populated when they are onboard:

|  |  |  |  |
| --- | --- | --- | --- |
| Group Name | Azure Scope | Azure RBAC | Azure AD Roles |
| API Platform | Dev API Platform Subscription  UAT API Platform Subscription | API Management Service Contributor | NA |
| <CUSTOMER\_NAME>.me  (App B2C) | <CUSTOMER\_NAME>-LZ-MY Management Group | Application Administrator (Role existing in the B2C Tenant post creation) | NA |
| Global Admin (root) | Root tenant Management Group | Owner | Global Administrator |
| LZ Admin (resource admin n user access) | <CUSTOMER\_NAME>-LZ-MY Management Group | Owner | NA |
| IAM Admin | <CUSTOMER\_NAME> Azure AD Tenant  <CUSTOMER\_NAME>-LZ-MY Management Group | User Access Administrator | User Administrator  Authentication administrator |
| Finance Executive | <CUSTOMER\_NAME>-LZ-MY Management Group | Billing Reader  Cost Management Reader | Billing Administrator |
| Network Admin | <CUSTOMER\_NAME>-LZ-MY Management Group | Network Contributor | NA |
| Backup Admin | <CUSTOMER\_NAME>-LZ-MY Management Group | Backup Contributor | NA |
| System Security | <CUSTOMER\_NAME>-LZ-MY Management Group | Security Reader | NA |
| Security Service Delivery | <CUSTOMER\_NAME>-LZ-MY Management Group | Key Vault Contributor  Key Vault Administrator  Network Contributor | NA |
| Security Operation Centre | <CUSTOMER\_NAME>-LZ-MY Management Group | Security Admin  Microsoft Sentinel Automation Contributor  Microsoft Sentinel Contributor  Microsoft Sentinel Responder | NA |
| Security Assurance | <CUSTOMER\_NAME>-LZ-MY Management Group | Security Reader  Microsoft Sentinel Reader  Reader | Directory Readers |
| Database Admin  (Project basis) | (Subscription level on project basis) | Cosmos DB Account Reader Role  Cosmos DB Operator  CosmosBackupOperator  DocumentDB Account Contributor  Redis Cache Contributor  SQL DB Contributor  SQL Server Contributor  SQL Managed Instance Contributor  SQL Security Manager  Reader | NA |
| System Admin | <CUSTOMER\_NAME>-LZ-MY Management Group | Virtual Machine Contributor | NA |
| Developer | <CUSTOMER\_NAME>-LZ-MY Management Group | Application Insights Component Contributor  Log Analytics Reader  Monitoring Reader  Workbook Reader | NA |
| Support (SRE) | <CUSTOMER\_NAME>-LZ-MY Management Group | Log Analytics Reader  Monitoring Reader  Workbook Reader | NA |
| Monitoring | <CUSTOMER\_NAME>-LZ-MY Management Group | Monitoring Contributor  Workbook Contributor  Application Insights Component Contributor  Monitoring Metrics Publisher | NA |
| Reader | <CUSTOMER\_NAME>-LZ-MY Management Group | Reader | NA |

Table 13: Azure AD Group and RBAC

* + - 1. Temporary Project Delivery Access

During the phase of project and service delivery, the team may require elevated access temporarily. In such scenario, temporary AD groups are created by IAM Admins and assign memberships to it. The following is an example for the upcoming APIM Project. There should be two different groups, one is for <CUSTOMER\_NAME> internal team, and another for vendor team.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Group Name | Azure Scope | Azure RBAC | AAD Roles | Timeframe |
| API Project Delivery <CUSTOMER\_NAME> Team | Dev API Platform Subscription  UAT API Platform Subscription | API Management Service Contributor  Contributor | NA | TBD |
| API Project Delivery Vendor Team | Dev API Platform Subscription  UAT API Platform Subscription | API Management Service Contributor | NA | TBD |

* + - 1. Process to request temporary access for project

Project owners will have to request temporary access for vendors and internal <CUSTOMER\_NAME> members from CCoE team to access <CUSTOMER\_NAME> Azure environments for deployments and UATs. Access timeframe should be defined and reviewed for extension at the end of each requested access timeframe.

* + - 1. Azure Built-in RBAC and AD roles

For the full list of built-in RBAC roles and AD roles can be referenced in the links below in order to assign the least-privilege roles to groups or users in the future.  
[Azure AD built-in roles - Azure Active Directory | Microsoft Docs](https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference)  
[Azure built-in roles - Azure RBAC | Microsoft Docs](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles)

* 1. Networking

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

* Design Considerations
* Design Decisions
* Design Patterns and Technical Details
* Hybrid DNS Resolution
* Network components for connectivity and security
  + 1. Design Considerations

|  |  |
| --- | --- |
| ID | Description |
| DC01 | <CUSTOMER\_NAME> made decision to have all customer data must be resident in Singapore Region only for now. |
| DC02 | IP Address assignments are managed by <CUSTOMER\_NAME> network team |
| DC03 | All communications between virtual networks must be secured |
| DC04 | No default direct connectivity between customer specific subscriptions/workload /VNETs. |
| DC05 | Very clear isolation of workloads based on the environment (Production, non-Production & Development) |
| DC06 | Design should provide connectivity between Azure and <CUSTOMER\_NAME> DCs |

Table 14: Networking Design Considerations

* + 1. Design Decisions

|  |  |
| --- | --- |
| ID | Description |
| DD01 | Two Hub VNETs will be created in the Southeast Asia region |
| DD02 | Setup of Express Route is planned for production connectivity |
| DD03 | VPN Gateway will be provisioned to establish S2S VPN Tunnels to on-premises network for non-production and ER Gateway is planned for production hub. |
| DD04 | DDoS Protection Basic tier is enabled for non-production and production Hub VNET |
| DD05 | The formation of Spoke Virtual Networks and subnet-associated Network Security Groups must be managed by <CUSTOMER\_NAME>. LOB specific VNETs and Subnets associated NSGs are managed by respective <CUSTOMER\_NAME> LOB. |
| DD06 | <CUSTOMER\_NAME> controls IPV4 Address spaces assignments to Subscriptions including LOB |
| DD07 | <CUSTOMER\_NAME> will setup hybrid DNS with Azure Private DNS Zones and bind DNS Server when it is required. |
| DD08 | Subnet for AzureBastionHost / Jump host allocated for future deployment of Jumphost or Bastion when required. |
| DD09 | <CUSTOMER\_NAME> will leverage on Cloudflare DDoS whereas WAF protection on Azure Application Gateway |

Table 15: Networking Design Decisions

Graphical user interface

Description automatically generated

Figure 4 <CUSTOMER\_NAME> - High Level Network Design

* + 1. Design Pattern: Hub/Spoke Virtual Networks Peerings (Hub/Spoke VNET)

Connectivity between VNETs is formed via VNET peering. Hub and Spoke model are intended to be repeatable as a pattern that can be stamped across regions, with peering formed as necessary through programmatic controls.

Connectivity between VNETs is further controlled via UDR and NSG to control routing and inter-VNET firewall rules. The current scope of project does not have a spoke VNET as no workloads are defined.

Connectivity for non-production and production should be separated, where production workloads will only connect to production Hub VNET, same goes for non-production.

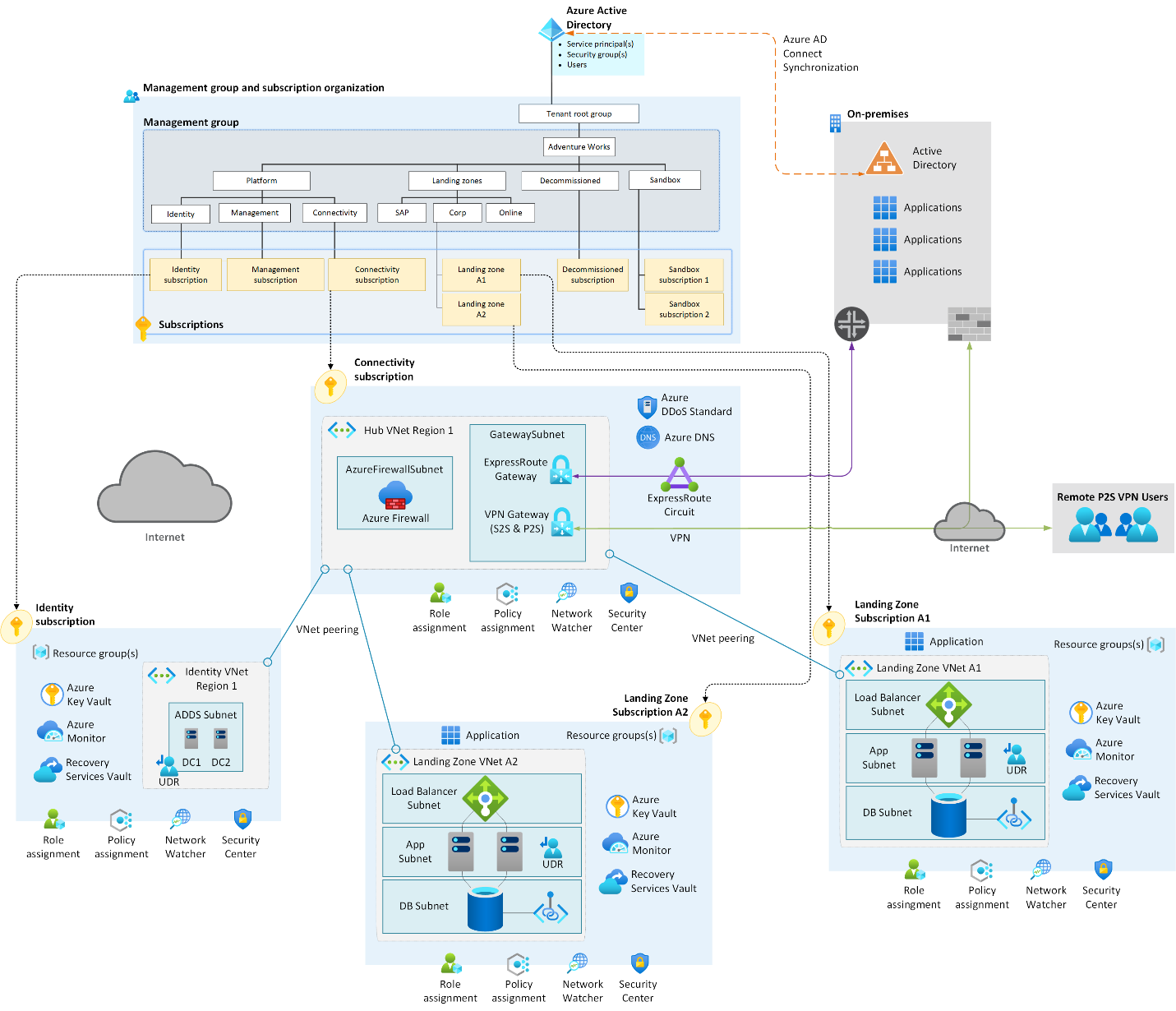


Figure 5: Sample HUB & Spoke Peering

* + - 1. Design Pattern: <CUSTOMER\_NAME> Application Network

Graphical user interface, application, Word

Description automatically generated

Figure 6: <CUSTOMER\_NAME> application onboarding network framework

For new onboarded applications which require public access, it needs to follow the above architecture. New applications will be allocated a new VNET which will be peered to the Hub VNET, no routing should be allowed to other application unless justified necessary. Level 4 traffic will have to flow through Azure Firewall and management of application servers will go through Azure Bastion Host.

For public access on level 7, users will have to go through Application Gateway with WAF enabled. The traffic is then load balanced amongst the web-tier servers and later directed to app tier via Internal Load Balancers. App tier can be further segregated in a different subnet but in <CUSTOMER\_NAME> decision, have placed them into “private subnet” following current practice. For “protected subnet” is used to host database related services.

* + 1. 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.

As documented in the subscription design section, <CUSTOMER\_NAME> has decided to create a subscription with dedicated VNET for each workloads/landing zone in their respective environment. This creates a clear segmentation based on their business requirements. Each workload may have one or more virtual networks. Virtual network connectivity will be based on <CUSTOMER\_NAME> decision and will be authorized by <CUSTOMER\_NAME>.

* + 1. Design Pattern: Virtual Networks Connectivity

We can categories the VNETs deployed in <CUSTOMER\_NAME> Azure cloud environment into 5 types:

|  |  |
| --- | --- |
| VNET Type | Purpose and Characteristics |
| Hub VNET | * 2 Hub VNETs is created under the Connectivity Subscription to allow multiple spoke VNETs to share the on-premises network connectivity for both production and non-production workloads. * Work as a routing hub to route traffic between spoke VNETs. * Provisioned Hub VNET and VPN Gateway for S2S tunnels. * Azure Firewall is deployed in the Hub VNET to secure traffic between external sites and <CUSTOMER\_NAME> Azure environment. |
| Spoke / Workload VNET | * No spoke VNET deployed in this project scope as no workloads are determined. * Spoke VNET serves as landing zones for workload / data / application which will then be peered to Hub VNET with proper routing and firewall filtering to secure connectivity. |

Table 16: Types of VNETs in Azure

* + 1. Design Pattern: Network Expansion for multiple environments

<CUSTOMER\_NAME> will have 2 Hub VNETs for Production and Non-production environment in the same tenant.

Graphical user interface, application

Description automatically generated

Figure 7: Network architecture reference for multiple environments

* + 1. Network Address Spaces and Subnets

<CUSTOMER\_NAME> plans to connect single on-premises datacenters to Azure. Microsoft Azure will be connected to the S2S VPN tunnel.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| VNET Name | Environment | VNET CIDR | Subnet Name | Subnet CIDR |
| <CUSTOMER\_NAME>-LZ-MY-hub-southeastasia | Production | 10.204.0.0/24 | AzureFirewallSubnet  AzureBastionSubnet  GatewaySubnet | 10.204.0.0/26  10.204.0.64/26  10.204.0.128/27 |
| <CUSTOMER\_NAME>-MY-vnet-hub-nonprod-sea-001 | Non-Production | 10.204.6.0/24 | AzureFirewallSubnet  AzureBastionSubnet  GatewaySubnet | 10.204.6.0/26  10.204.6.64/26  10.204.6.128/27 |

Table 17: VNET and address Space

* + 1. Azure Hybrid DNS Resolution

For on-premises workloads to resolve DNS for Azure PaaS services on private endpoint, a Hybrid DNS Resolution solution is required. At this point, since there are not identified PaaS workloads, a DNS Forwarder is not required but this section will provide architectural reference for <CUSTOMER\_NAME> to deploy when it is required. Full documentation can be found [here](https://docs.microsoft.com/en-us/azure/private-link/private-endpoint-dns#dns-configuration-scenarios).

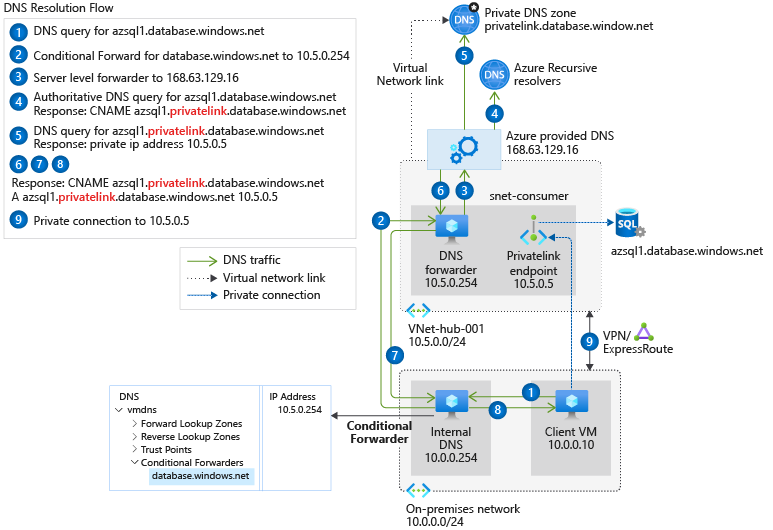


Figure 8: Hybrid DNS Resolution Architecture Reference

As per reference architecture, a DNS forwarder in Azure is required to be able to access the private DNS Zone via [Azure DNS IP 168.63.129.16](https://docs.microsoft.com/en-us/azure/virtual-network/what-is-ip-address-168-63-129-16) to resolve any FQDN to private endpoint IP.

* + 1. Network Connectivity and Security Components
       1. Azure Firewall

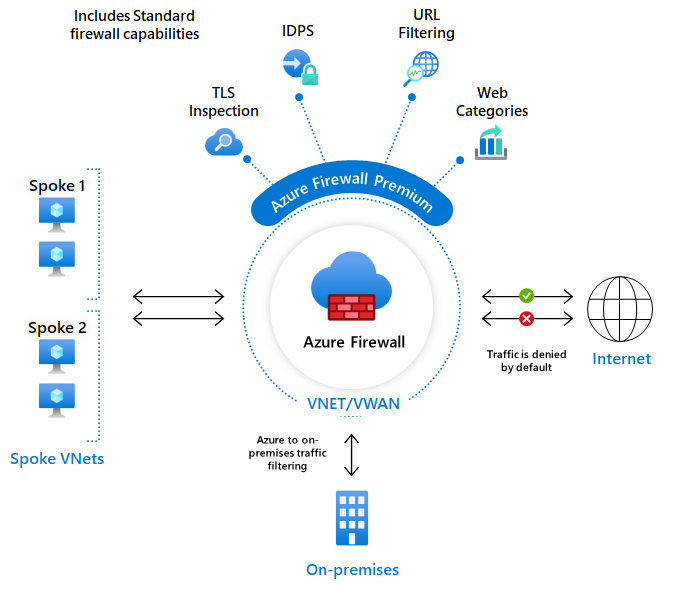


Figure 9: Azure Firewall

Azure Firewall is a cloud-native and intelligent network firewall security service that provides the best breed threat protection for your cloud workloads running in Azure. It's a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability. It provides both east-west and north-south traffic inspection.

Azure Firewall is offered in two SKUs: [Standard](https://docs.microsoft.com/en-us/azure/firewall/features) and [Premium](https://docs.microsoft.com/en-us/azure/firewall/premium-features).

* + - 1. VPN Gateway

VPN Gateway is used to send encrypted traffic between Azure virtual network and on-premises location over the public internet. VPN Gateway comes with multiple connectivity configurations and SKUs. The planning table and SKU features can be found here: [About Azure VPN Gateway | Microsoft Docs](https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways).

* + - 1. Azure Web Application Firewall on Application Gateway

Azure WAF are available in [Application Gateway](https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/ag-overview?toc=/azure/virtual-network/toc.json). Azure WAF on Azure Application Gateway provides centralized protection of your web applications from common exploits and vulnerabilities. Web applications are increasingly targeted by malicious attacks that exploit commonly known vulnerabilities. SQL injection and cross-site scripting are among the most common attacks.

WAF on Application Gateway is based on [Core Rule Set (CRS)](https://owasp.org/www-project-modsecurity-core-rule-set/) 3.1, 3.0, or 2.2.9 from the Open Web Application Security Project (OWASP). Refer to [WAF CRS rule groups and rules](https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/application-gateway-crs-rulegroups-rules?tabs=owasp32) for more configuration details.

The key features of Azure WAF are as follows:

* SQL-injection protection.
* Cross-site scripting protection.
* Protection against other common web attacks, such as command injection, HTTP request smuggling, HTTP response splitting, and remote file inclusion.
* Protection against HTTP protocol violations.
* Protection against HTTP protocol anomalies, such as missing host user-agent and accepting headers.
* Protection against crawlers and scanners.
* Detection of common application misconfigurations (for example, Apache and IIS).
* Configurable request size limits with lower and upper bounds.
* Exclusion lists let you omit certain request attributes from a WAF evaluation. A common example is Active Directory-inserted tokens that are used for authentication or password fields.
* Create custom rules to suit the specific needs of your applications.
* Geo-filter traffic to allow or block certain countries/regions from gaining access to your applications.
* Protect your applications from bots with the bot mitigation ruleset.
* Inspect JSON and XML in the request body
  + - 1. Azure DDoS Standard

Distributed denial of service (DDoS) attacks are some of the largest availability and security concerns facing customers that are moving their applications to the cloud. A DDoS attack attempts to exhaust an application's resources, making the application unavailable to legitimate users. DDoS attacks can be targeted at any endpoint that is publicly reachable through the internet.

The following are the key features of Azure DDoS Standard SKU:

* Native platform integration: Natively integrated into Azure. Includes configuration through the Azure portal. DDoS Protection Standard understands your resources and resource configuration.
* Turnkey protection: Simplified configuration immediately protects all resources on a virtual network as soon as DDoS Protection Standard is enabled. No intervention or user definition is required.
* Always-on traffic monitoring: Your application traffic patterns are monitored 24 hours a day, 7 days a week, looking for indicators of DDoS attacks. DDoS Protection Standard instantly and automatically mitigates the attack, once it is detected.
* Adaptive tuning: Intelligent traffic profiling learns your application's traffic over time and selects and updates the profile that is the most suitable for your service. The profile adjusts as traffic changes over time.
* Multi-Layered protection: When deployed with a web application firewall (WAF), DDoS Protection Standard protects both at the network layer (Layer 3 and 4, offered by Azure DDoS Protection Standard) and at the application layer (Layer 7, offered by a WAF). WAF offerings include [Azure Application Gateway WAF SKU](https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/ag-overview?toc=/azure/virtual-network/toc.json) as well as third-party web application firewall offerings available in the [Azure Marketplace](https://azuremarketplace.microsoft.com/marketplace/apps?page=1&search=web%20application%20firewall).
* Extensive mitigation scale: Over 60 different attack types can be mitigated, with global capacity, to protect against the largest known DDoS attacks.
* Attack analytics: Get detailed reports in five-minute increments during an attack, and a complete summary after the attack ends. Stream mitigation flow logs to Microsoft Sentinel or an offline security information and event management (SIEM) system for near real-time monitoring during an attack.
* Attack metrics: Summarized metrics from each attack are accessible through Azure Monitor.
* Attack alerting: Alerts can be configured at the start and stop of an attack, and over the attack's duration, using built-in attack metrics. Alerts integrate into your operational software like Microsoft Azure Monitor logs, Splunk, Azure Storage, Email, and the Azure portal.
* DDoS Rapid Response: Engage the DDoS Protection Rapid Response (DRR) team for help with attack investigation and analysis. To learn more, see [DDoS Rapid Response](https://docs.microsoft.com/en-us/azure/ddos-protection/ddos-rapid-response).
* Cost guarantee: Receive data-transfer and application scale-out service credit for resource costs incurred as a result of documented DDoS attacks.
  + - 1. Network Connectivity and Network Security Components Design

|  |  |  |  |
| --- | --- | --- | --- |
| Component | Name | Environment | Tier |
| Azure Firewall | <CUSTOMER\_NAME>-MY-afw-prod-sea-001 | Production | Standard |
| VPN Gateway | <CUSTOMER\_NAME>-MY-vgw-prod-sea-001 | Production | VpnGw1 |
| Azure Firewall | <CUSTOMER\_NAME>-MY-afw-nonprod-sea-001 | Non-Production | Standard |
| VPN Gateway | <CUSTOMER\_NAME>-MY-vgw-nonprod-sea-001 | Non-Production | VpnGw1 |

Table 18: Network Components

* 1. Platform Management and Monitoring
     1. Overview

Timeline

Description automatically generated

Figure 10: Azure Platform Management and Monitoring Overview

Log analytics workspace is an administrative boundary security audit logging and achieving a horizontal security lens across the entire customer Azure estate.

Platform Management includes peripheral components such as naming conventions, tags, resource locks and cost management to ensure consistent platform governance, visibility and security.

* + 1. Azure Naming Convention
       1. 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.
  + - 1. Requirements

The chosen naming convention is based on the following requirements:

|  |  |
| --- | --- |
| ID | Description |
| DC01 | <CUSTOMER\_NAME> to follow Azure best practices for naming convention  [Define your naming convention - Cloud Adoption Framework | Microsoft Docs](https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-best-practices/resource-naming) |

Table 19: Naming Convention Requirements

* + - 1. Design Decisions

The chosen naming convention is based on the following requirements:

|  |  |
| --- | --- |
| ID | Description |
| DD01 | <CUSTOMER\_NAME> decision to use the following as convention for azure resources  <org>-<country>-<resource\_type>-<workload/app>-<sub\_desc>-<environment>-<region>-<instance> |
| DD02 | Subnet  <resource\_type>-<workload>-<public/private(tier1,2,n)/protected>-<env>-<instance> |
| DD03 | Public IP  <org>-<country>-<resource\_type>-<workload>-<sub\_desc>-<env>-<instance> |

Table 20: Naming Convention Decisions

|  |  |
| --- | --- |
| Azure Regions | Abbreviations |
| Southeastasia | sea |

|  |  |
| --- | --- |
| Environment | Abbreviations |
| Production | prod |
| Non-Production | nonprod |
| Development | dev |
| System Integration Test | sit |
| User Acceptance Test | uat |

|  |  |
| --- | --- |
| Organization | Abbreviations |
| <CUSTOMER\_NAME> Group | <CUSTOMER\_NAME> |

|  |  |
| --- | --- |
| Country | Abbreviations |
| Malaysia | MY |

* + 1. Azure Tags
       1. 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.

* + - 1. Design Decisions

|  |  |
| --- | --- |
| ID | Description |
| DD01 | <CUSTOMER\_NAME> can use Tags to internally manage resource consumption and costing by filtering cost allocations based on Tags. |
| DD02 | <CUSTOMER\_NAME> may add Tags in the future as the requirement arises. Please see Table below for a suggestion of baseline tags. |

Table 21: Design Decisions - Azure Tags

The following tags were decided for Azure resources where applicable, currently only Cost Centre is enforced to all resources.

|  |  |  |
| --- | --- | --- |
| Tag | Enforced | Tag Value |
| Cost Centre | Yes | 1763633727 |
| Name | No | NA |
| App ID | No | NA |
| Environment | Yes | NA |
| Component | No | NA |
| Compliance Framework | No | NA |
| Business Unit | Yes | NA |
| Data Classification | No | NA |
| Owner | Yes | NA |
| Owner Email | Yes | NA |
| Backup Policy | No | NA |
| Patch Group | No | NA |
| Maintenance window | No | NA |

Table 22: Suggestion for initial tags

* + 1. Azure Resource Locks
       1. 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 ReadOnly.

* Delete means authorized users can read and modify resources, but they can't delete any of the restricted resources.
* ReadOnly 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.

* + - 1. Design Considerations

The chosen Locks strategy is based on the following considerations:

|  |  |
| --- | --- |
| ID | Design Considerations |
| DC01 | No user should be able to delete any Subscription or resource by accident as it could have a business impact. |

Table 23: Requirements and Considerations - Resource Locks

* + - 1. Design Decisions

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

|  |  |
| --- | --- |
| ID | Design Decision |
| DD01 | <CUSTOMER\_NAME> to enable Azure Resource Locks for identified business critical resources. |

Table 24: Design Decisions - Resource Locks

* + 1. Azure Cost Management
       1. 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 Enterprise Agreement (EA), a billing account is created when the organization signs an Enterprise Agreement to use Azure. This billing account can be used to manage invoices, payments, and track costs.

A scope is a node in a billing account used to view and manage billing. It is where billing data, payments and invoices are managed.

For Enterprise Agreements, a scope can be as documented in the following table:

|  |  |
| --- | --- |
| Scope | Definition |
| Billing account | Represents an Enterprise Agreement enrolment. The invoice is generated at the billing account scope. It's structured using departments and enrolment accounts. |
| Department | Optional grouping of enrolment accounts. |
| Enrolment account | Represents a single account owner. Azure Subscriptions are created under the enrolment account scope. |

Table 25: Azure Billing - Scopes

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.
  + 1. Azure Advisor
       1. 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.
  + - 1. Design Decisions

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

|  |  |
| --- | --- |
| ID | Design Decision |
| DD01 | Azure Advisor will be used to optimize Azure resource usage and configuration based on recommendations |
| DD02 | Alert notification on security and non-compliance |

Table 26: Design Decisions - Azure Advisor

* + 1. Azure Automation for Update Management

[Update Management in Azure Automation](https://docs.microsoft.com/en-us/azure/automation/update-management/overview) can be used to manage operating system updates for Windows and Linux virtual machines in Azure, physical or VMs in on-premises environments, and in other cloud environments. You can quickly assess the status of available updates and manage the process of installing required updates for your machines reporting to Update Management.

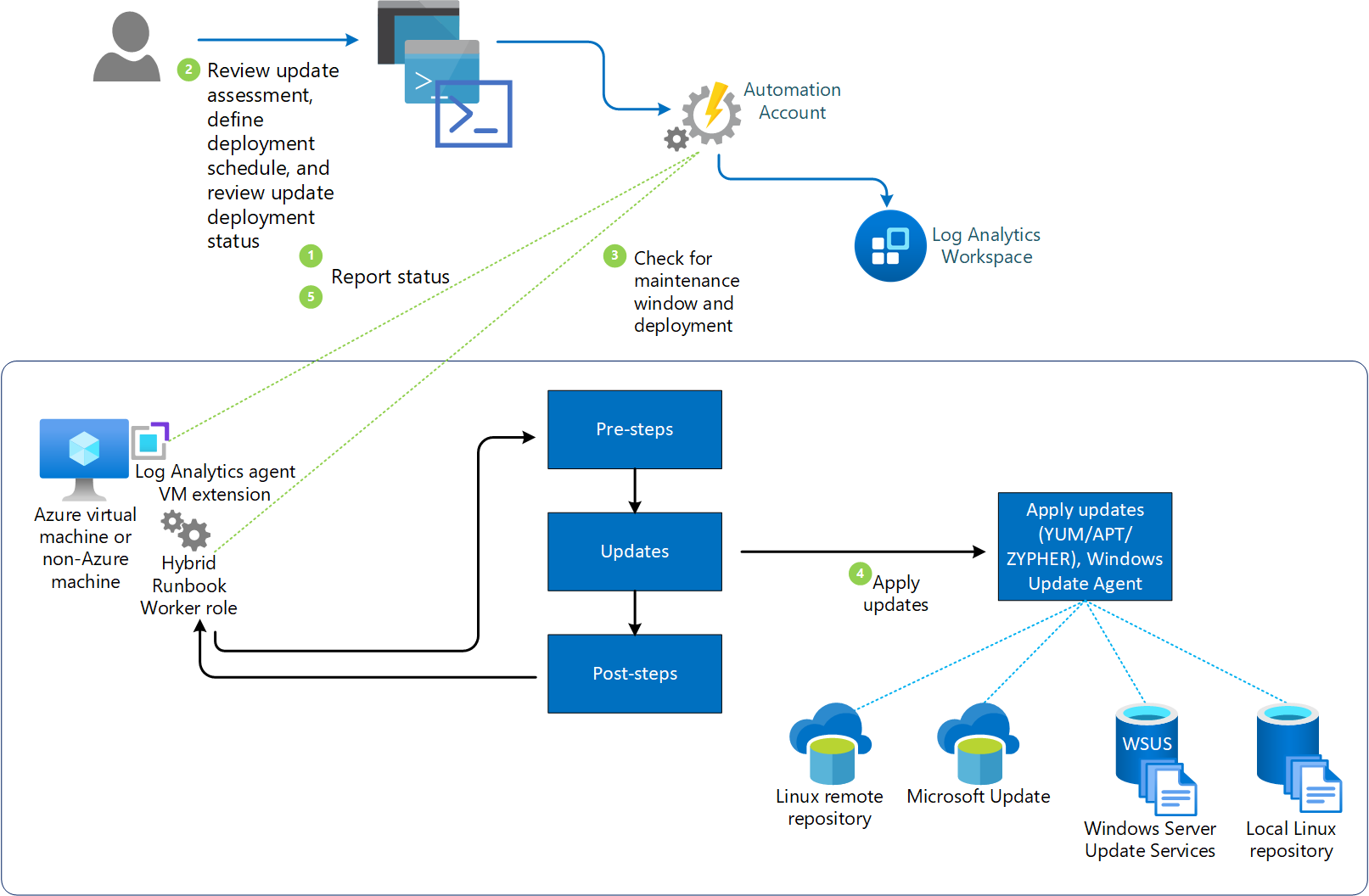


Figure 11: Azure Automation for Update Management

* + - 1. Design Decisions

|  |  |
| --- | --- |
| ID | Description |
| DC01 | Patch and update management tool has yet to be determined as no workloads are on Azure |

Table 27: Automation for Update Management Design Decision

* + - 1. Patch or Update Policy Design Decisions

|  |  |  |  |
| --- | --- | --- | --- |
| IT System Classification | Operating System | Patch Criticality level | Timeline |
| Critical | Windows and RHEL | Critical | 14 days |
| High | 30 days |
| Medium | 60 days |
| Low | 90 days |
| Non-Critical | Windows and RHEL | Critical | 14 days |
| High | 30 days |
| Medium | 60 days |
| Low | 90 days |

Table 28: Patch or Update Policy Design Decisions

* + 1. Logging and Monitoring

<CUSTOMER\_NAME> currently still conducting assessments and pending decisions for 3rd party monitoring integration with Azure Monitor.

* + - 1. Azure Monitor

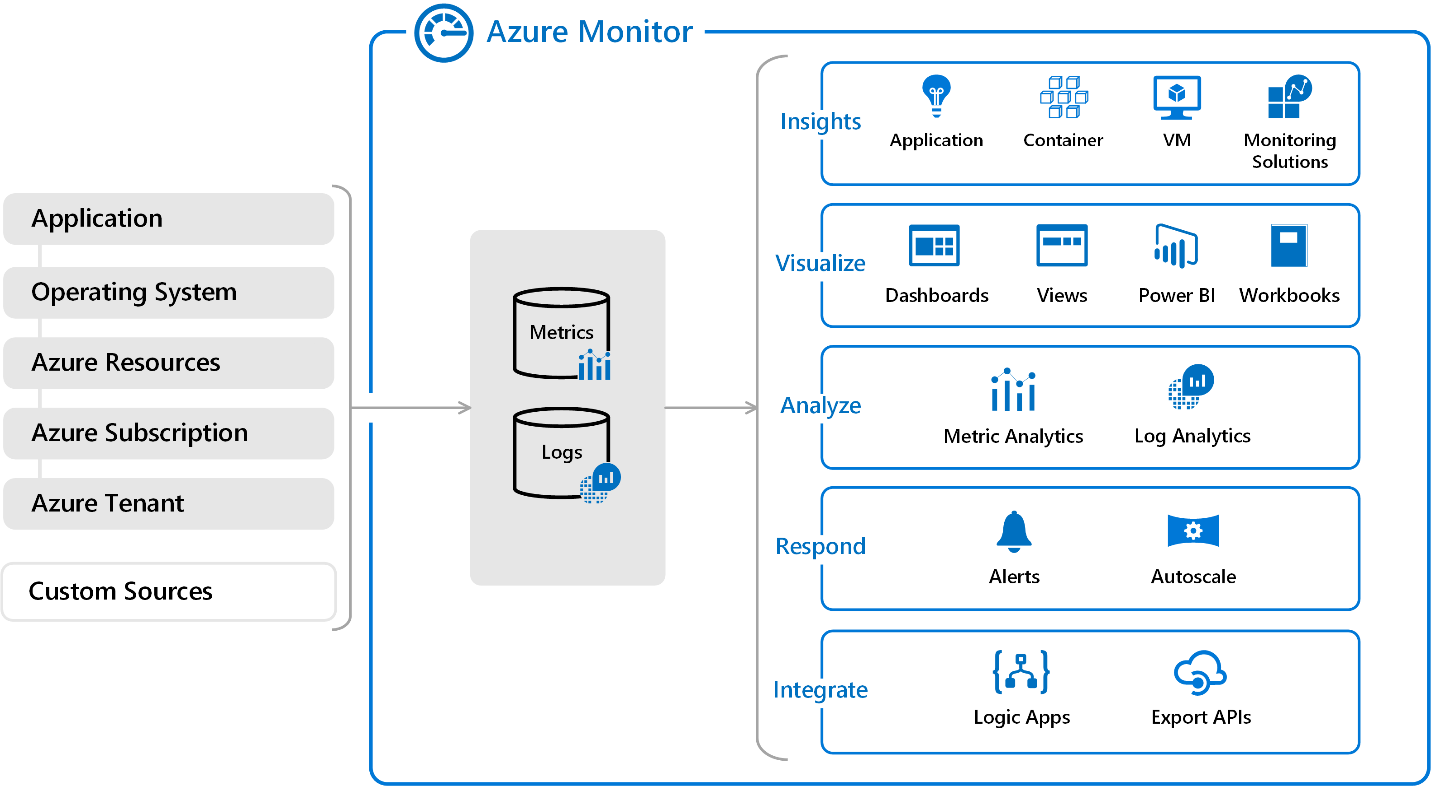


Figure 12: Azure Monitor Overview diagram

Azure platform monitoring is comprised of many services, and each of the services has their own specific role in platform monitoring. The core of Azure native logging and monitoring is Azure Monitor.

The following shows the key features of Azure Monitor

* [Log Analytics Workspace](https://docs.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-workspace-overview) is the central log data storage that can come from Azure Monitor, Microsoft Sentinel, Microsoft Defender for Cloud and external sources.
* [Application Insights](https://docs.microsoft.com/en-us/azure/azure-monitor/app/app-insights-overview) detect and diagnose issues across applications and dependencies.
* Correlate infrastructure issues with [VM insights](https://docs.microsoft.com/en-us/azure/azure-monitor/vm/vminsights-overview) and [Container insights](https://docs.microsoft.com/en-us/azure/azure-monitor/containers/container-insights-overview).
* Drill into your monitoring data with [Log Analytics](https://docs.microsoft.com/en-us/azure/azure-monitor/logs/log-query-overview) for troubleshooting and deep diagnostics.
* 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).
* Create 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).
* Collect 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).
* Collect data from [Activity Logs](https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/activity-log) for Azure resource changes and access.
  + - 1. Network Watcher

[Azure Network Watcher](https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview) provides tools to monitor, diagnose, view metrics and enable or disable logs for resources in an Azure virtual network. Network watcher includes NSG flow logs for traffic analytics capability. Network watcher is designed to monitor and repair the network health of IaaS products including VM, VNET, Application Gateway, Load Balancers, etc. Note: it is not intended for and will not work for PaaS monitoring or web analytics.

The following are the key features of Network Watcher:

* Monitors communication between a VM and an endpoint
* View resources in VNET and their relationship
* Diagnostics
  + Capture packets to-and-from a VM
  + Diagnose Network filtering to-and-from traffic from a VM
  + Diagnose network routing problems from a VM
  + Diagnose outbound connection from a VM
    - 1. Design Considerations

|  |  |
| --- | --- |
| ID | Description |
| DC01 | Leverage on Azure native monitoring tools including Azure Monitor and Log analytics for Azure resources. |
| DC02 | Log retention required to be 3 years and logs after 1 year should be in cool tier storage |
| DC03 | Centralized log analytics workspace |
| DC04 | Logs archival to Storage account for log retention for lower storage cost |

Table 29 Platform Monitoring Design Considerations

* + - 1. Decision Decisions

|  |  |
| --- | --- |
| ID | Description |
| DD01 | Azure monitor to be enabled for all upcoming workloads in Azure |
| DD02 | Enable Network Watcher in all subscriptions |
| DD03 | Utilize log analytics workspace as the logging tool for Azure native workloads |
| DD04 | Post default Azure log retention, logs will be saved in Azure storage account for retention in shared service subscription with lock and access model. |
| DD05 | Centralization, integration and management of logs in hybrid settings to be designed in a separate stream from this project scope |

Table 30 Platform Monitoring Decision Decisions

* 1. High Availability, Backup and Disaster Recovery
     1. High Availability

Azure availability zones are physically separate locations within each Azure region that are tolerant to local failures. Failures can range from software and hardware failures to events such as earthquakes, floods, and fires. Tolerance to failures is achieved because of redundancy and logical isolation of Azure services. To ensure resiliency, a minimum of three separate availability zones are present in all availability zone-enabled regions.

Azure availability zones are connected by a high-performance network with a round-trip latency of less than 2ms. They help your data stay synchronized and accessible when things go wrong. Each zone is composed of one or more datacentres equipped with independent power, cooling, and networking infrastructure. Availability zones are designed so that if one zone is affected, regional services, capacity, and high availability are supported by the remaining two zones.

Diagram

Description automatically generated

Figure 13: Azure Availability Zones

Note: Azure availability zone configuration is implemented on compute and storage level. Network level comes by default with zone redundancy.

* + - 1. Design Decisions

|  |  |
| --- | --- |
| ID | Description |
| DD01 | Production workloads is required to run with high availability |
| DD02 | High availability setup should span across different availability zones |

Table 31: Design Decisions

* + 1. Azure Backup

The Azure Backup service provides simple, secure, and cost-effective solutions to back up your data and recover it from the Microsoft Azure cloud.

* **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](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)
  + - 1. Design Considerations

|  |  |
| --- | --- |
| ID | Description |
| DC01 | Backup policy for future Production and Critical workloads |
| DC02 | Backup policy for future Non-Production and Non-Critical workloads |
| DC03 | DR not discussed as workloads not defined at current stage. |

Table 32 Azure Backup and BCDR Design Considerations

* + - 1. Design Decisions

|  |  |
| --- | --- |
| ID | Description |
| DD01 | Backup Policy (baseline)  Production and Critical Workloads:  Daily: 14 days  Weekly: 5 weeks  Monthly: 7 years  Time Window: 2AM MYT |
| DD02 | Backup Policy (baseline)  Non-Production and Non-Critical Workloads:  Daily: 14 days  Weekly: 5 weeks  Time Window: 2AM MYT |
| DD03 | Backup policy takes application owner decision as priority to overwrite the baseline policy |
| DD04 | Backup data must be encrypted with CMK (Key management, PIC and process to be decided by <CUSTOMER\_NAME>) |

Table 33 Azure Backup and BCDR Design Decisions

* + 1. Business Continuity and Disaster Recovery
       1. Design Decisions

|  |  |
| --- | --- |
| ID | Description |
| DD01 | RTO and RPO are subjective to workloads, to be determined as per workloads needs. |

Table 34: BCDR Design Decisions

Note: The following section is meant to be informative for DR and business continuity design patterns.

* + - 1. 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.

* + - 1. 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. The disaster recovery plan is part of the business continuity plan, so developing a DR plan if <CUSTOMER\_NAME> doesn't already have one should be part of your process.

As <CUSTOMER\_NAME> in the process of creating the BCDR plan, it’s important to consider interviewing key personnel in organizations who have gone through a disaster successfully. People generally like to share "war stories" and the steps and techniques (or clever ideas) that saved the day. Their insights could prove incredibly valuable in helping you to craft a solid plan.

* + - 1. 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.

[Azure Site Recovery (ASR)](https://docs.microsoft.com/azure/site-recovery/site-recovery-overview?WT.mc_id=itopstalk-blog-salean) is the tool you can use to help keep your workloads online when the worst happens. Azure Site Recovery can replicate your workloads from the primary Azure region to secondary Azure region. If any outage happens <CUSTOMER\_NAME> can invoke disaster recovery plan and ASR will fail over to the secondary region which services keep working. When the primary region comes up and running again, <CUSTOMER\_NAME> can fail back to primary region.

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.

Diagram

Description automatically generated

Figure 14 Azure Site Recovery over multi-region sample architecture

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, <CUSTOMER\_NAME> 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)

* + - 1. Design Pattern 2 - 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).

* + - 1. Design Pattern 3 - Azure Backup



Figure 15 Backup and Disaster Recovery

Azure Backup service provides simple, secure and cost-effective solutions to backup data and recover from Microsoft Azure cloud. Backed up data can be restored to on-prem or cross regions in Azure cloud to ensure there is always capacity to host your restored workloads.

Azure Backup delivers these key benefits:

* Offload on-premises backup
* Backup up Azure IaaS VMs
* Scale easily
* Unlimited data transfer: No charges applied for inbound or outbound data transfer to Recovery Service Vault during restore operations.
* Data Security: Secures data in-transit and at-rest.
* Retain long and short-term data
* Centralized monitoring and management with alerting capabilities
* Multiple storage options: LRS, ZRS and GRS
  1. Security, Policy and Governance

The guiding principle of Microsoft security strategy is to assume breach at any given point of time. Microsoft and Azure global incident response teamwork around the clock to mitigate the effects of any kind of attack against all cloud services. Any security is directly built into Microsoft business product and cloud services from the ground up.

Microsoft complies with both international and industry-specific compliance standards and participates in rigorous third-party audits. Among many, Microsoft products and services are available to help meet *<CUSTOMER\_NAME> and RMIT compliance* requirements.

These governance measures help ensure that Azure infrastructure is resilient to attack and safeguards user access to Azure environments and helps keep <CUSTOMER\_NAME> Information’s data and cloud infrastructure secure. Azure’s security approach can be separated into two main segments:

Secure Identity: Configuration of the security auditing features in business products and services, along with access to security audit logs, is restricted to administrators only in Azure. The identities of administrative users are authenticated through Active Directory on Windows Server 2016 (Kerberos based) or Azure Active Directory (AD Graph API) in the cloud.

Secure Infrastructure: Azure provides monitoring, and logging technologies to give maximum visibility into the activity on the cloud-based network, applications, and devices. This enables identification of potential gaps. Collection and analysis of such information and filter it to fit specific criteria is essential for identifying patterns within the network.

* + 1. Policy Management
       1. 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 with the corporate standards and service level agreements.

Azure Policy will help <CUSTOMER\_NAME> 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 Microsoft Defender for Cloud’ is automatically assigned to every Subscription with a goal to monitor all the available security recommendations in Microsoft Defender for Cloud

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

Azure Security Benchmark v.2 – 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 16: Evaluation order flow diagram for the different policy conditions

* + - 1. Design Considerations

|  |  |
| --- | --- |
| ID | Design Considerations |
| DC01 | Through policy-driven management, <CUSTOMER\_NAME>’s policy implementation will ensure new Azure subscriptions and resources will immediately be brought to their target compliant state. |
| DC02 | Management Group and Subscriptions hierarchy will be considered when assigning Policies.  • Relevant policies will be assigned 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. |
| DC03 | Enterprise Scale recommended policies should be applied and complemented by other policies/initiatives which will help <CUSTOMER\_NAME> meet their internal security policies. |

Table 35: Requirements and Considerations - Azure Policy

* + - 1. Design Decisions

The following table documents the policies that will be implemented along with the default Initiative. Policies at the higher hierarchy will be inherited to child Management Groups and thus will still be applied at the specified scope with if no specific policy is assigned. Initiatives are a set of policies grouped together.

The initiatives used are:

* Azure Security Benchmark - [Azure Security Benchmark v2 (Azure Security Center baseline)](https://docs.microsoft.com/en-us/azure/governance/policy/samples/azure-security-benchmark)
* RMIT Malaysia - [Regulatory Compliance for RMIT Malaysia-Azure Policy | Microsoft Docs](https://docs.microsoft.com/en-us/azure/governance/policy/samples/rmit-malaysia?cid=kerryherger)

|  |  |  |
| --- | --- | --- |
| **Scope** | **Policy / Initiative name** | **Assignment Scope** |
| <CUSTOMER\_NAME> Root | Azure Security Benchmark (Initiative) | <CUSTOMER\_NAME>-LZ |
| [Preview]: RMIT Malaysia (Initiative) | <CUSTOMER\_NAME>-LZ |
| Configure Azure Activity logs to stream to specified Log Analytics workspace | <CUSTOMER\_NAME>-LZ |
| Deploy Diagnostic Settings to Azure Services | <CUSTOMER\_NAME>-LZ |
| Deploy Microsoft Defender for Cloud configuration | <CUSTOMER\_NAME>-LZ |
| Enable Azure Monitor for Virtual Machine Scale Sets | <CUSTOMER\_NAME>-LZ |
| Enable Azure Monitor for VMs | <CUSTOMER\_NAME>-LZ |
| Landing Zones | Azure Security Benchmark (Initiative) | <CUSTOMER\_NAME>-LZ |
| [Preview]: RMIT Malaysia (Initiative) | <CUSTOMER\_NAME>-LZ |
| Configure Azure Activity logs to stream to specified Log Analytics workspace | <CUSTOMER\_NAME>-LZ |
| Deploy Diagnostic Settings to Azure Services | <CUSTOMER\_NAME>-LZ |
| Deploy Microsoft Defender for Cloud configuration | <CUSTOMER\_NAME>-LZ |
| Enable Azure Monitor for Virtual Machine Scale Sets | <CUSTOMER\_NAME>-LZ |
| Enable Azure Monitor for VMs | <CUSTOMER\_NAME>-LZ |
| Deploy Azure Policy Add-on to Azure Kubernetes Service clusters | <CUSTOMER\_NAME>-LZ-MY |
| Kubernetes clusters should not allow container privilege escalation | <CUSTOMER\_NAME>-LZ-MY |
| Configure backup on virtual machines without a given tag to a new recovery services vault with a default policy | <CUSTOMER\_NAME>-LZ-MY |
| RDP access from the Internet should be blocked | <CUSTOMER\_NAME>-LZ-MY |
| Deny or Deploy and append TLS requirements and SSL enforcement on resources without Encryption in transit | <CUSTOMER\_NAME>-LZ-MY |
| Kubernetes clusters should be accessible only over HTTPS | <CUSTOMER\_NAME>-LZ-MY |
| Subnets should have a Network Security Group | <CUSTOMER\_NAME>-LZ-MY |
| Deploy Threat Detection on SQL servers | <CUSTOMER\_NAME>-LZ-MY |
| Secure transfer to storage accounts should be enabled | <CUSTOMER\_NAME>-LZ-MY |
| Kubernetes cluster should not allow privileged containers | <CUSTOMER\_NAME>-LZ-MY |
| Auditing on SQL server should be enabled | <CUSTOMER\_NAME>-LZ-MY |
| Network interfaces should disable IP forwarding | <CUSTOMER\_NAME>-LZ-MY |
| Landing Zone - Corp | Azure Security Benchmark (Initiative) | <CUSTOMER\_NAME>-LZ |
| [Preview]: RMIT Malaysia (Initiative) | <CUSTOMER\_NAME>-LZ |
| Configure Azure Activity logs to stream to specified Log Analytics workspace | <CUSTOMER\_NAME>-LZ |
| Deploy Diagnostic Settings to Azure Services | <CUSTOMER\_NAME>-LZ |
| Deploy Microsoft Defender for Cloud configuration | <CUSTOMER\_NAME>-LZ |
| Enable Azure Monitor for Virtual Machine Scale Sets | <CUSTOMER\_NAME>-LZ |
| Enable Azure Monitor for VMs | <CUSTOMER\_NAME>-LZ |
| Enforces the use of vnet injection for Databricks | Group-Digital |
| Enforces the use of Premium Databricks workspaces | Group-Digital |
| Public network access should be disabled for PaaS services | Group-Digital |
| Prevent usage of Databricks with public IP | Group-Digital |
| Configure Azure PaaS services to use private DNS zones | Group-Digital |
| Deploy Azure Policy Add-on to Azure Kubernetes Service clusters | <CUSTOMER\_NAME>-LZ-MY |
| Kubernetes clusters should not allow container privilege escalation | <CUSTOMER\_NAME>-LZ-MY |
| Configure backup on virtual machines without a given tag to a new recovery services vault with a default policy | <CUSTOMER\_NAME>-LZ-MY |
| RDP access from the Internet should be blocked | <CUSTOMER\_NAME>-LZ-MY |
| Deny or Deploy and append TLS requirements and SSL enforcement on resources without Encryption in transit | <CUSTOMER\_NAME>-LZ-MY |
| Kubernetes clusters should be accessible only over HTTPS | <CUSTOMER\_NAME>-LZ-MY |
| Subnets should have a Network Security Group | <CUSTOMER\_NAME>-LZ-MY |
| Deploy Threat Detection on SQL servers | <CUSTOMER\_NAME>-LZ-MY |
| Secure transfer to storage accounts should be enabled | <CUSTOMER\_NAME>-LZ-MY |
| Kubernetes cluster should not allow privileged containers | <CUSTOMER\_NAME>-LZ-MY |
| Auditing on SQL server should be enabled | <CUSTOMER\_NAME>-LZ-MY |
| Network interfaces should disable IP forwarding | <CUSTOMER\_NAME>-LZ-MY |
| Landing Zone - Online | Azure Security Benchmark (Initiative) | <CUSTOMER\_NAME>-LZ |
| [Preview]: RMIT Malaysia (Initiative) | <CUSTOMER\_NAME>-LZ |
| Configure Azure Activity logs to stream to specified Log Analytics workspace | <CUSTOMER\_NAME>-LZ |
| Deploy Diagnostic Settings to Azure Services | <CUSTOMER\_NAME>-LZ |
| Deploy Microsoft Defender for Cloud configuration | <CUSTOMER\_NAME>-LZ |
| Enable Azure Monitor for Virtual Machine Scale Sets | <CUSTOMER\_NAME>-LZ |
| Enable Azure Monitor for VMs | <CUSTOMER\_NAME>-LZ |
| Deploy Azure Policy Add-on to Azure Kubernetes Service clusters | <CUSTOMER\_NAME>-LZ-MY |
| Kubernetes clusters should not allow container privilege escalation | <CUSTOMER\_NAME>-LZ-MY |
| Configure backup on virtual machines without a given tag to a new recovery services vault with a default policy | <CUSTOMER\_NAME>-LZ-MY |
| RDP access from the Internet should be blocked | <CUSTOMER\_NAME>-LZ-MY |
| Deny or Deploy and append TLS requirements and SSL enforcement on resources without Encryption in transit | <CUSTOMER\_NAME>-LZ-MY |
| Kubernetes clusters should be accessible only over HTTPS | <CUSTOMER\_NAME>-LZ-MY |
| Subnets should have a Network Security Group | <CUSTOMER\_NAME>-LZ-MY |
| Deploy Threat Detection on SQL servers | <CUSTOMER\_NAME>-LZ-MY |
| Secure transfer to storage accounts should be enabled | <CUSTOMER\_NAME>-LZ-MY |
| Kubernetes cluster should not allow privileged containers | <CUSTOMER\_NAME>-LZ-MY |
| Auditing on SQL server should be enabled | <CUSTOMER\_NAME>-LZ-MY |
| Network interfaces should disable IP forwarding | <CUSTOMER\_NAME>-LZ-MY |
| Platform | Azure Security Benchmark (Initiative) | <CUSTOMER\_NAME>-LZ |
| [Preview]: RMIT Malaysia (Initiative) | <CUSTOMER\_NAME>-LZ |
| Configure Azure Activity logs to stream to specified Log Analytics workspace | <CUSTOMER\_NAME>-LZ |
| Deploy Diagnostic Settings to Azure Services | <CUSTOMER\_NAME>-LZ |
| Deploy Microsoft Defender for Cloud configuration | <CUSTOMER\_NAME>-LZ |
| Enable Azure Monitor for Virtual Machine Scale Sets | <CUSTOMER\_NAME>-LZ |
| Enable Azure Monitor for VMs | <CUSTOMER\_NAME>-LZ |
| Platform - Connectivity | Azure Security Benchmark (Initiative) | <CUSTOMER\_NAME>-LZ |
| [Preview]: RMIT Malaysia (Initiative) | <CUSTOMER\_NAME>-LZ |
| Configure Azure Activity logs to stream to specified Log Analytics workspace | <CUSTOMER\_NAME>-LZ |
| Deploy Diagnostic Settings to Azure Services | <CUSTOMER\_NAME>-LZ |
| Deploy Microsoft Defender for Cloud configuration | <CUSTOMER\_NAME>-LZ |
| Enable Azure Monitor for Virtual Machine Scale Sets | <CUSTOMER\_NAME>-LZ |
| Enable Azure Monitor for VMs | <CUSTOMER\_NAME>-LZ |
| Platform - Identity | Azure Security Benchmark (Initiative) | <CUSTOMER\_NAME>-LZ |
| [Preview]: RMIT Malaysia (Initiative) | <CUSTOMER\_NAME>-LZ |
| Configure Azure Activity logs to stream to specified Log Analytics workspace | <CUSTOMER\_NAME>-LZ |
| Deploy Diagnostic Settings to Azure Services | <CUSTOMER\_NAME>-LZ |
| Deploy Microsoft Defender for Cloud configuration | <CUSTOMER\_NAME>-LZ |
| Enable Azure Monitor for Virtual Machine Scale Sets | <CUSTOMER\_NAME>-LZ |
| Enable Azure Monitor for VMs | <CUSTOMER\_NAME>-LZ |
| Subnets should have a Network Security Group | <CUSTOMER\_NAME>-LZ-Identity |
| Configure backup on virtual machines without a given tag to a new recovery services vault with a default policy | <CUSTOMER\_NAME>-LZ-Identity |
| Deny the creation of public IP | <CUSTOMER\_NAME>-LZ-Identity |
| RDP access from the Internet should be blocked | <CUSTOMER\_NAME>-LZ-Identity |
| Platform - Management | Azure Security Benchmark (Initiative) | <CUSTOMER\_NAME>-LZ |
| [Preview]: RMIT Malaysia (Initiative) | <CUSTOMER\_NAME>-LZ |
| Configure Azure Activity logs to stream to specified Log Analytics workspace | <CUSTOMER\_NAME>-LZ |
| Deploy Diagnostic Settings to Azure Services | <CUSTOMER\_NAME>-LZ |
| Deploy Microsoft Defender for Cloud configuration | <CUSTOMER\_NAME>-LZ |
| Enable Azure Monitor for Virtual Machine Scale Sets | <CUSTOMER\_NAME>-LZ |
| Enable Azure Monitor for VMs | <CUSTOMER\_NAME>-LZ |
| Configure Log Analytics workspace and automation account to centralize logs and monitoring | <CUSTOMER\_NAME>-LZ-Management |
| Sandbox | Azure Security Benchmark (Initiative) | <CUSTOMER\_NAME>-LZ |
| [Preview]: RMIT Malaysia (Initiative) | <CUSTOMER\_NAME>-LZ |
| Configure Azure Activity logs to stream to specified Log Analytics workspace | <CUSTOMER\_NAME>-LZ |
| Deploy Diagnostic Settings to Azure Services | <CUSTOMER\_NAME>-LZ |
| Deploy Microsoft Defender for Cloud configuration | <CUSTOMER\_NAME>-LZ |
| Enable Azure Monitor for Virtual Machine Scale Sets | <CUSTOMER\_NAME>-LZ |
| Enable Azure Monitor for VMs | <CUSTOMER\_NAME>-LZ |
| Decommissioned | Azure Security Benchmark (Initiative) | <CUSTOMER\_NAME>-LZ |
| [Preview]: RMIT Malaysia (Initiative) | <CUSTOMER\_NAME>-LZ |
| Configure Azure Activity logs to stream to specified Log Analytics workspace | <CUSTOMER\_NAME>-LZ |
| Deploy Diagnostic Settings to Azure Services | <CUSTOMER\_NAME>-LZ |
| Deploy Microsoft Defender for Cloud configuration | <CUSTOMER\_NAME>-LZ |
| Enable Azure Monitor for Virtual Machine Scale Sets | <CUSTOMER\_NAME>-LZ |
| Enable Azure Monitor for VMs | <CUSTOMER\_NAME>-LZ |

Table 36: Design Decisions - Azure Policy

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

* + - 1. Design Decisions

|  |  |
| --- | --- |
| ID | Design Decisions |
| DD01 | <CUSTOMER\_NAME> has yet to decide the means of secure access as there are no workloads on Azure at this stage |

Table 37: Design Decisions

Note: This section meant to be informative for future decisions when it comes to secure access to Azure VMs.

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.

* + 1. Microsoft Defender for Cloud (used to be Azure Security Center)
       1. Technical Overview

[Microsoft Defender for Cloud](https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction) 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.

Microsoft 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, Microsoft 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 Microsoft 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 analyze 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) | Microsoft 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, Microsoft Defender for Cloud collects audit records using auditd. 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 | Microsoft 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 38: Microsoft Defender for Cloud feature comparison

* + - 1. Design Decisions

|  |  |
| --- | --- |
| ID | Design Decisions |
| DD01 | <CUSTOMER\_NAME> will use Microsoft Defender for Cloud Free tier for all subscriptions and all resources for all environments. |

Table 39: Design Decisions – Microsoft Defender for Cloud

* + 1. Microsoft Sentinel (used to be Azure Sentinel)

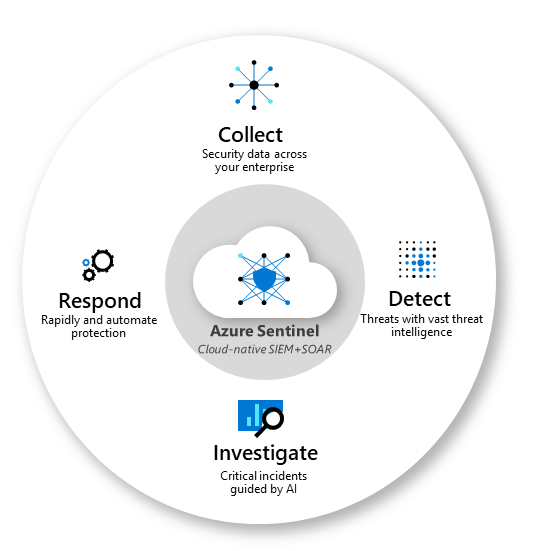


Figure 17: Microsoft Sentinel

[Microsoft Sentinel](https://docs.microsoft.com/en-us/azure/sentinel/overview) is a scalable, cloud-native, security information and event management (SIEM) and security orchestration, automation, and response (SOAR) solution. Microsoft Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for attack detection, threat visibility, proactive hunting, and threat response.

The key **functions** of Microsoft Sentinel are:

* Collect data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds.
* Detect previously undetected threats and minimize [false positives](https://docs.microsoft.com/en-us/azure/sentinel/false-positives) using Microsoft's analytics and unparalleled threat intelligence.
* Investigate threats with artificial intelligence, and hunt for suspicious activities at scale, tapping into years of cyber security work at Microsoft.
* Respond to incidents rapidly with built-in orchestration and automation of common tasks.

The key **features and tools** that come with Microsoft Sentinel are:

* [Data connectors](https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources) provide log ingestion from different sources into Microsoft Sentinel
* [Parsers](https://docs.microsoft.com/en-us/azure/sentinel/normalization-about-parsers) provide log formatting/transformation into ASIM formats, supporting usage across various Microsoft Sentinel content types and scenarios
* [Workbooks](https://docs.microsoft.com/en-us/azure/sentinel/get-visibility) provide monitoring, visualization, and interactivity with data in Microsoft Sentinel, highlighting meaningful insights for users
* [Analytics rules](https://docs.microsoft.com/en-us/azure/sentinel/detect-threats-built-in) provide alerts that point to relevant SOC actions via incidents
* [Hunting queries](https://docs.microsoft.com/en-us/azure/sentinel/hunting) are used by SOC teams to proactively hunt for threats in Microsoft Sentinel
* [Notebooks](https://docs.microsoft.com/en-us/azure/sentinel/notebooks) help SOC teams use advanced hunting features in Jupyter and Azure Notebooks
* [Watchlists](https://docs.microsoft.com/en-us/azure/sentinel/watchlists) support the ingestion of specific data for enhanced threat detection and reduced alert fatigue
* [Playbooks and Azure Logic Apps custom connectors](https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks) provide features for automated investigations, remediations, and response scenarios in Microsoft Sentinel
  + - 1. Microsoft Sentinel Integrability

Timeline

Description automatically generated

Figure 18: Microsoft Sentinel Integrability view

As SIEM needs to monitor all the security logs and events to properly enable threat hunting, security vulnerability monitoring, alert and security incident management, it needs to consolidate logs from all different sources. The diagram shows how other monitoring services are integrated to provide comprehensive SIEM capabilities across different environments.

* + 1. Azure Key Vault
       1. Technical Overview

[Azure Key Vault](https://docs.microsoft.com/en-us/azure/key-vault/general/overview) 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.

* + - 1. Design decisions

|  |  |
| --- | --- |
| ID | Design Decisions |
| DD01 | <CUSTOMER\_NAME> will use CMK for encryption purposes in Azure wherever possible |
| DD02 | Key vaults will be created by workloads requirements |

Table 40: Design Decisions - Key Vault

* + 1. Azure Data Encryption

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

* + - 1. 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 centers. |
| At rest | Disk | BitLocker and others | Encryption of storage devices in Azure data centers 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 always remain encrypted. |

Table 41: 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 42: 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.

* + - 1. Design decisions

|  |  |
| --- | --- |
| ID | Design Decisions |
| DD01 | <CUSTOMER\_NAME> will use Azure Disk Encryption on all VMs in all Subscriptions with CMK when workloads are onboarded to Azure |
| DD02 | Keys for the Storage Account encryption will use CMK when it is deployed in the future. |

Table 43: Design Decisions - Azure Data Encryption

* + 1. Managed Images for OS Hardening

[Managed images](https://docs.microsoft.com/en-us/azure/virtual-machines/windows/capture-image-resource) are helpful in both production and development environment where you need a consistent baseline VM. OS hardening policies can also be included in the managed image to ensure all VM deployed will have consistent hardening policies. A managed image resource can be created from a generalized virtual machine (VM) that is stored as either a managed disk or an unmanaged disk in a storage account. The image can then be used to create multiple VMs.

Users can use any desired custom hardening policies with managed images or leverage on [Azure marketplace](https://docs.microsoft.com/en-us/marketplace/azure-marketplace-overview) to deploy hardened images with CIS standards for [Windows server](https://azuremarketplace.microsoft.com/en-us/marketplace/apps/center-for-internet-security-inc.cis-windows-server-2016-v1-0-0-l1?tab=overview) or [RHEL servers](https://azuremarketplace.microsoft.com/en-us/marketplace/apps/center-for-internet-security-inc.cis-rhel-7-v2-2-0-l1?tab=overview) for example.

1. Appendix
   1. 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. |
| [DevOps solution pricing](https://azure.microsoft.com/en-us/pricing/details/devops/azure-devops-services/) | This page provides pricing information for DevOps solution |
| [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 44: References