A picture containing text, night sky

Description automatically generatedA picture containing text

Description automatically generated

|  |  |
| --- | --- |
| Version | 0.2 |
| Date | 18-04-2023 |
| Status | Draft-Generic |
| Classification | Confidential |

**Mahindra Finance**

**AWS Landing Zone Design**

**References**

**Copyright © 2020, Blazeclan**

**All Rights Reserved**

The following documents have been considered or are referenced in the development of this document:

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Document Title | Version | Link / Location |
| 1 | AWS Landing Zone Design |  |  |

# **Document Control**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Change Description | Author |
| 0.1 | 03-03-2023 | Draft Copy | Ankit Sahai |
| 0.2 | 18-04-2023 | Updated diagrams | Ankit Sahai |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

**Document Control** 2

**Reviewer and Approvers** 2

**1.Document Purpose and Structure** 6

**2.Solution Summary** 7

2.1 Design Principles 7

2.2 Solution Components 7

2.3 Key Considerations 9

2.4 Decisions Register: - 9

**3.** **Landing Zone – Build Requirements** 10

**4.** **Conceptual View** 11

**5.** **Identity and Access Management** 11

5.1 IAM Identity Center (Successor to AWS SSO) 11

5.2 AWS IAM Identity Center Permission Sets 13

5.3 IAM Identity Center built-in permission sets 13

5.4 Proposed Permission Sets 14

5.5 Authentication and Authorization:- 14

5.6 SAML Federation 16

5.7 Single Sign-On 16

6. AWS Organizations and AWS Account Strategy 17

6.1 Key Design Principles: - 18

6.2 Management Account: - 19

6.3 Organizational Units (OU): - 19

6.4 AWS Accounts: - 21

6.5 Quotas for AWS Organization 23

6.6 AWS Service and Service Endpoints and Quotas 24

6.7 AWS Control Tower guardrails: - 26

6.8 Mandatory guardrails: - 27

6.9 Strongly Recommended guardrails: - 29

6.10 Elective guardrails: - 30

6.11 Naming: - 33

6.12 Tagging: - 36

7. Platform Automation and DevOps 38

7.1 Platform Automation: - 38

7.2 DevOps and DevSecOps 38

7.3 Deploy AWS landing zones by using Terraform (AWS AFT) 39

8. Network topology and connectivity 39

8.1 Define an AWS network topology: - 39

8.2 Connectivity: - 42

8.3 Network Security 50

8.4 Connectivity to AWS Services 56

8.5 Private DNS for on-premises and AWS resources 60

8.6 Public DNS for AWS resources: - 61

8.7 DNS resolution priority from AWS VPC……………………………………………………………………………………..62

8.7 Plan for virtual machine remote access: - 63

9. Security 64

9.1.1 AWS Control Tower Controls(Guardrails): - 64

9.1.2 CIS AWS Foundations Benchmark: - 65

9.2 Identity and Access Management: - 65

9.3 Network Security 67

9.4 AWS data security and encryption 67

9.5 Resource Management 70

9.6 Backup and Retention 70

9.7 Golden Images 71

9.8 Patch management 71

10 Governance 73

10.1 Cost Governance: - 73

11 Monitoring 76

11.1 Amazon CloudWatch 76

11.2 CloudWatch Container Insights 76

11.3 ELK Monitoring tool: - 77

11.4 Metrics and thresholds to monitor 77

11.5 Logging: - 79

12. AWS Best Practices 80

12.1 The root user is secured 80

12.2 Account contact information is set 81

# **Document Purpose and Structure**

This document provides a detailed treatment of MAHINDRA FINANCE. architectural requirements and proposes a carefully considered approach to design Landing Zone Architecture to meet these requirements. This approach is informed by detailed requirements gathering workshops that were conducted with key MAHINDRA FINANCE. stakeholders and is also informed by best practice patterns to achieve key cloud goals, including: security, resilience, availability, scalability, and cost optimisation.

The purpose of this document is to provide conceptual and technical design for setting up AWS Landing Zone using AWS Control Tower to support MAHINDRA FINANCE. requirements on the AWS Cloud.

This design document includes details related to key principles considered in making the key design decisions and the related impact and risks. The focus of the solution based on the discussion is limited to the following aspects

* Design the AWS Landing Zone document to meet the MAHINDRA FINANCE. standards and requirements
* Create an Architecture for setting up a new AWS Landing Zone by referring to existing architecture of GCP, AZURE and on-premises environment.
* Network connectivity to MAHINDRA FINANCE. On-premises based on MAHINDRA FINANCE. security policies and segregation of accounts.
* Recommend policy for organizational units and accounts.
* Define security baseline for Landing zone.
* Infrastructure monitoring tools and baseline.

The following areas will be out of scope for this design

* MAHINDRA FINANCE. - On-Premises connectivity solution
* The current Active Directory domains and related objects
* Infrastructure provisioning and setup in application related AWS accounts

This document is intended to form the keystone of a robust cloud foundation for MAHINDRA FINANCE., and ought to be considered a living document that can be revised and updated as new technologies become available and new design patterns emerge as best practices.

# **Solution Summary**

### 2.1 Design Principles

The AWS Landing Zone enables consumption of AWS services based on the following key guiding principles:

* **Infrastructure as Code and Automation**
  + Version Control of the infrastructure definitions / AWS Landing zone management
  + Infrastructure as code for repeatable outcomes in multiple environments
  + Deployment automation to minimise human intervention and errors
* **Define Network connections to flow traffic from external sources**
  + All connections including the Mahindra On-Premises and other clouds (GCP, Azure) are treated as trusted environments. This will not pass-through the Firewall, which logs the traffic.
* **Security Principle** 
  + Meet the AWS best practice security standards.
* **High Resilient Infrastructure:** Delivered solution has to offer highly resilient infrastructure to support deployment of 3 tier applications with External and Internal facing components.
* **Segmentation of Environments:** Administrative and Network Separation of Prod and Non-Prod workloads to ensure that changes to non-Prod infrastructure do not impact Prod applications infrastructure.

### 2.2 Solution Components

| ID | Component | Status | Detail | Impact / In Scope |
| --- | --- | --- | --- | --- |
| 1 | Landing Zone | Planned | * Design the industry standard multi-accounts AWS environment. * Design and build the master account setup * Security, Infra and Project Workload organizational unit structure. * Design, policies and compliance. | Yes |
| 3 | IAM Identity Center (successor to AWS SSO) integration with Azure AD | Planned | * Integration of IAM Identity Center with existing Azure Active Directory as External Identity Provider | Yes |
| 4 | AWS billing | Planned | The AWS landing zone architecture and accounts from AWS offers. | Yes |
| 5 | Security | Planned | Security baseline for AWS landing zone as per AWS security best practices | Yes |
| 6 | Account Model | Planned | Design secured and scalable multi-account model as per enterprise requirement | Yes |
| 7 | Policy enforcement | Planned | Defining organizational policy (Guardrails) which is effective to enforce across your organization. | Yes |
| 8 | Resource consistency | Planned | Deployment consistency  Policy consistency  Hierarchical consistency  Automated consistency | Yes |
| 9 | Resource naming and tagging | Planned | Defining resource naming convention and tagging policy | Yes |
| 10 | Networking | Planned | Designing AWS networking which support cloud workload and services Identify workload networking requirements  Plan Virtual Network  Best Practices for Network security  South-North Internet Traffic  Transit Gateway network topology | Yes |
| 12 | Logging | Planned | Defining logging strategy | Yes |
| 13 | Monitoring & Reporting | Planned | Defining monitoring strategy | No |
| 14 | Cost Management | Planned | The best-practice article outlines decisions and implementation approaches to creating cost tracking mechanisms. | Yes |

### 2.3 Key Considerations

|  |  |
| --- | --- |
| Consideration ID | Details |
| KC#1 | * Establish new target AWS Control Tower Environment for this offering. |

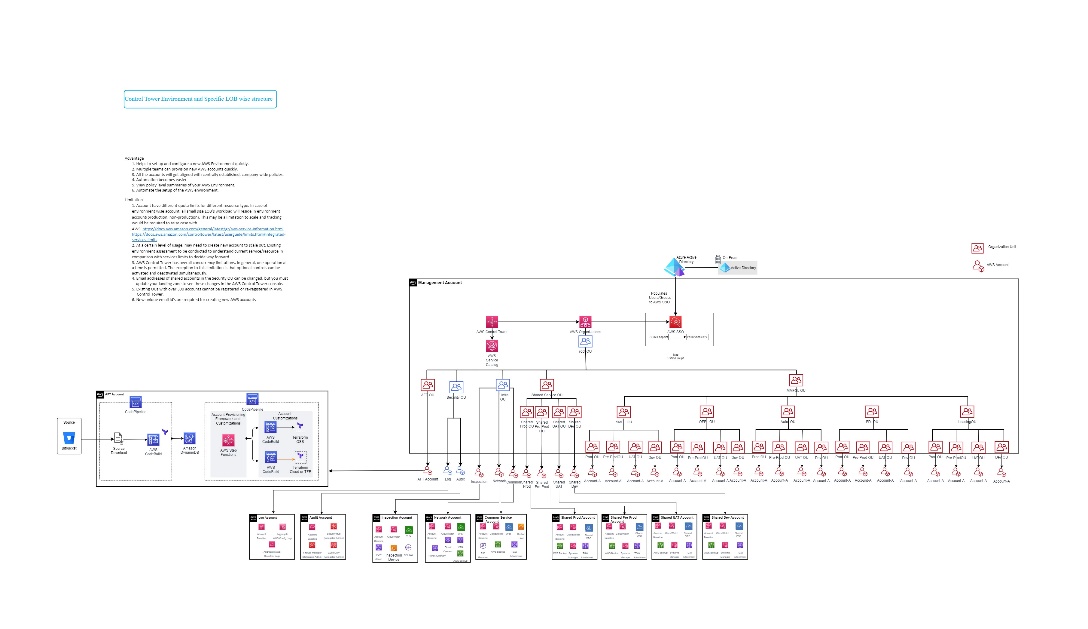
### 2.4 Decisions Register: -

|  |  |  |
| --- | --- | --- |
| Risk ID | Key Design Decision | Status |
| DR#1 | * Region | * Landing zone design need for only 1 Primary region (Asia Pacific-Mumbai). From design perspective proposed DR region is Asia Pacific-Hyderabad |
| DR#2 | * Availability Zone | * 2 availability zones to be used i.e. ap-south-1a and ap-south-1b |
| DR#3 | * IAC tool for LZ setup | * Mahindra Finance AWS Control Tower LZ will be setup with AWS AFT |
| DR#4 | * Monitoring Tool | * Finalized that Mahindra Finance will use any of ELK/Kafka/Dynatrace/riverbed instead of AWS CloudWatch and will be setup by their vendor |
| DR#5 | * Security Group | * Security Group to be applied at Instance level for required IP’s and ports only. |
| DR#6 | * mPaas deployment | * Existing mPaas deployment which is used at organization level, will be extended to AWS cloud and integration of the same will be performed by Mahindra Finance |
| DR#7 | * AWS KMS | * Mahindra Finance has finalized to use Thales LUNA for KMS. They may use AWS KMS along with Thales LUNA |
| DR#8 | * ACM | * Not going to use AWS ACM. Mahindra Finance is yet to finalize 3rd Party Certificate Management Solution. |
| DR#9 | * AWS Firewall Manager | * Not going to use |
| DR#10 | * Internet Egress Inspection | * Centrally Inspect Internet Egress traffic using Zscalar Cloud Connector. Zscalar setup will be done by Zscalar vendor |
| DR#11 | * Internet Ingress Inspection | * Centrally Inspect Internet Ingress traffic using Palo-Alto Firewall. Palo-Alto firewall setup to be done by Palo-Alto vendor. |
| DR#12 | * Traffic Inspection coming from GCP/Azure to AWS | * Centrally inspect traffic coming from GCP/Azure Cloud to AWS using Palo-Alto Firewall. |
| DR#13 | * Guardrails | * Guardrails to be applied at lowest nested OU in the hierarchy |
| DR#14 | * On-Prem to AWS Connectivity | * Direct Connect will be primary service whereas AWS VPN will be used as tertiary backup for connectivity between on-prem and AWS.   As on-prem router doesn’t support BGP routing, the site-to-site VPN will be static |
| DR#15 | * Tagging Policy Enforcement | * Tagging policy enforcement will be made at the mPaas tool level |
| DR#16 | * AWS GuardDuty | * AWS GuardDuty to be enable with Audit as delegated admin |
| DR#17 | * VPC Flow logs | * Enable VPC flow logs and redirect logs to centralize S3 bucket in Log account using AWS AFT |
| DR#18 | * AWS Instance access | * Mahindra Finance is in discussion with tool vendors like Sectona or CyberArk. Finalized vendor will deploy the solution |
| DR#19 | * WAF | * Mahindra Finance will finalize between Cloudflare and F5, which will be deploy by respective vendor |
| DR#20 | * Backup Tool | * 3rd Party backup solution will be finalized by Mahindra Finance and deploy by respective vendor |
| DR#21 | * Patching | * Mahindra Finance will use BigFix for patching, deployment to be done by respective vendor |

# **Landing Zone – Build Requirements**

|  |  |  |
| --- | --- | --- |
| ID | Configuration Item | Value |
| LZ#1 | * LZ root subscription Email Address |  |

# **Conceptual View**



# **Identity and Access Management**

Identity provides the basis for a large percentage of security assurance. It grants access based on identity authentication and authorization controls in cloud services. Access control protects data and resources and helps decide which requests should be permitted.

### 5.1 IAM Identity Center (Successor to AWS SSO)

In AWS Control Tower, AWS IAM Identity Center allows central cloud administrators and end users to manage access to multiple AWS accounts and business applications. AWS Control Tower uses this service to set up and manage access to the accounts created through AWS Service Catalog.

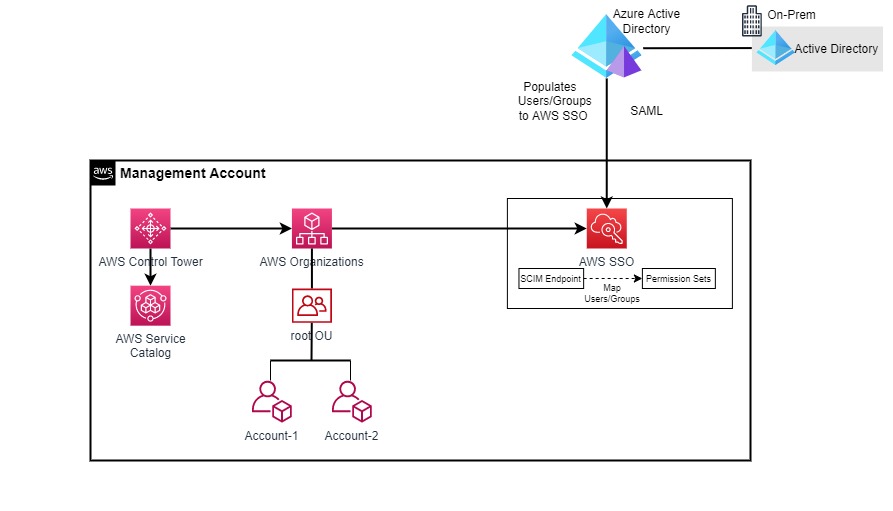
With IAM Identity Center you can manage sign-in security for your workforce by creating or connecting your users and groups to AWS in one place. With *multi-account permissions* you can assign your *workforce identities* access to AWS accounts. With a single click, IAM Identity Center enabled application admins can assign access to your workforce users, and can also use application assignments to assign your users access to software as a service (SaaS) applications.

Based on the discussions and decisions in the workshops, for the current engagement AWS IAM Identity Center will be integrated with Mahindra Finance’s Azure AD which is used as an Identity Store to get access to the Control Tower Landing Zone via AWS IAM Identity Center for this engagement.

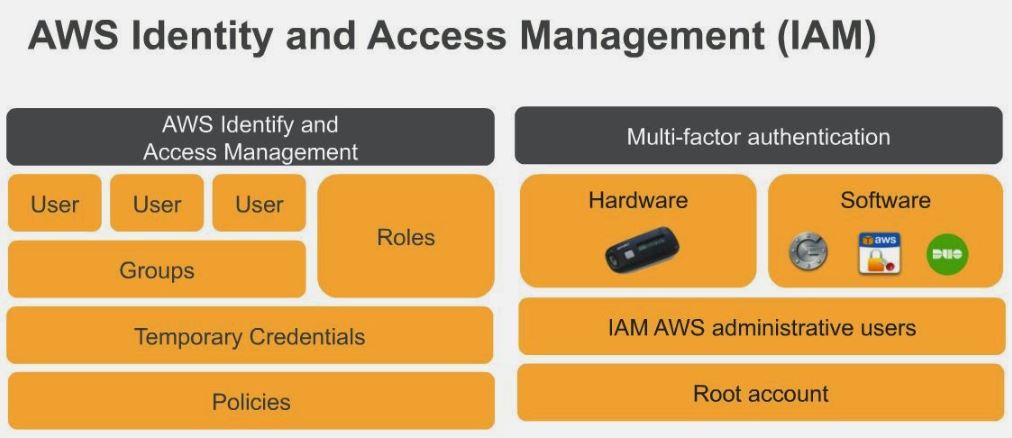
AWS IAM Identity Center supports identity federation with SAML 2.0, allowing integration with AD FS solutions. This helps enterprises migrate to AWS, who have a hybrid environment with on-premises AD FS and need access to AWS accounts and cloud applications. Users can sign in to the AWS access portal URL with their corporate credentials thus reducing the admin overhead of maintaining separate credentials on AWS IAM Identity Center.

Some IdPs do not support SCIM. In that case, you must manually provision the users in AWS IAM Identity Center. The username in AWS IAM Identity Center should be identical to the username configured in your IdP.

Once the users and groups are ready, configure access based on groups and permission sets to respective accounts.



Least-privilege access model will be used that grants users only the permissions required to perform their work. The following diagram shows a suggested pattern for using AWS IAM through this approach.



### 5.2 AWS IAM Identity Center Permission Sets

A permission set is a collection of administrator-defined policies that AWS IAM Identity Center uses to determine a user's effective permissions to access a given AWS account. Permission sets can contain either AWS managed policies or custom policies that are stored in AWS IAM Identity Center. Permission sets ultimately get created as Identity and Access Management (IAM) roles in a given AWS account, with trust policies that allow users to assume the role through AWS SSO. Permission sets define access for human users.

Permission sets define the level of access that users and groups have to an AWS account. More than one permission set can be assigned to a user. Users who have multiple permission sets must choose one when they sign in to the user portal. Users will see these as IAM roles.

Each Permission Set needs to be defined with responsibilities and based on those responsibilities the access permissions are allowed or denied with the help of an IAM Policy. An IAM Policy is a JSON formatted document that provides a list of ‘Allow’ or ‘Deny’ permissions. It consists of one or more statements, each of which describes the set of permissions.

### 5.3 IAM Identity Center built-in permission sets

Below are the AWS built-in permission sets to manage AWS resources

|  |  |
| --- | --- |
| **Built-in Permission Set** | **Description** |
| AWSOrganizationsFullAccess | Provides full access to AWS Organizations. |
| AWSReadOnlyAccess | This policy grants permissions to view resources and basic metadata across all AWS services. |
| AWSAdministratorAccess | Provides full access to AWS services and resources. |
| AWSServiceCatalogAdminFullAccess | Provides full access to AWS Service Catalog admin capabilities. |
| AWSServiceCatalogEndUserAccess | Provides access to the AWS Service Catalog end user console. |
| AWSPowerUserAccess | Provides full access to AWS services and resources, but does not allow management of Users and groups. |

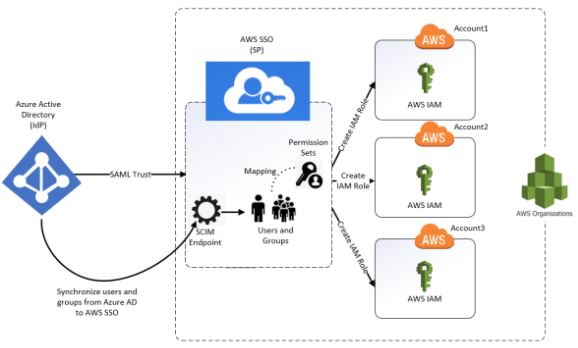
### 5.4 Proposed Permission Sets

Although the permission sets built in to AWS support a wide variety of access control scenarios, they might not meet all the needs of your organization or team. The following table illustrates a common pattern for dividing IT responsibilities into separate custom permission sets

|  |  |  |
| --- | --- | --- |
| **Group** | **PermissionSet name** | **Responsibilities** |
| Billing | Billing | Grants permissions for billing and cost management. This includes viewing account usage and viewing and modifying budgets and payment methods. |
| DatabaseAdministrator | DatabaseAdministrator | Grants full access permissions to AWS services and actions required to set up and configure AWS database services. |
| NetworkAdministrator | NetworkAdministrator | Grants full access permissions to AWS services and actions required to set up and configure AWS network resources. |
| SecurityAudit | SecurityAudit | The security audit template grants access to read security configuration metadata. It is useful for software that audits the configuration of an AWS account. |
| SupportUser | SupportUser | This policy grants permissions to troubleshoot and resolve issues in an AWS account. This policy also enables the user to contact AWS support to create and manage cases. |
| SystemAdministrator | AdministratorAccess | Grants full access permissions necessary for resources required for application and development operations. |
| ViewOnlyAccess | ViewOnlyAccess | This policy grants permissions to view resources and basic metadata across all AWS services. |
| ReadOnlyAccess | ReadOnlyAccess | Provides read-only access to AWS services and resources |
| L1 Team | ReadOnlyAccess | Provides read-only access to AWS services and resources |
| L2 Team | <depend on requirement> | Limited access based on least-privilege permissions |
| L3 Team | AdministratorAccess | Full Admin Access |
| DataScientist | DataScientist | Grants permissions to AWS data analytics services.. |
| Operates features and applications to meet service-level agreements and other quality standards. |

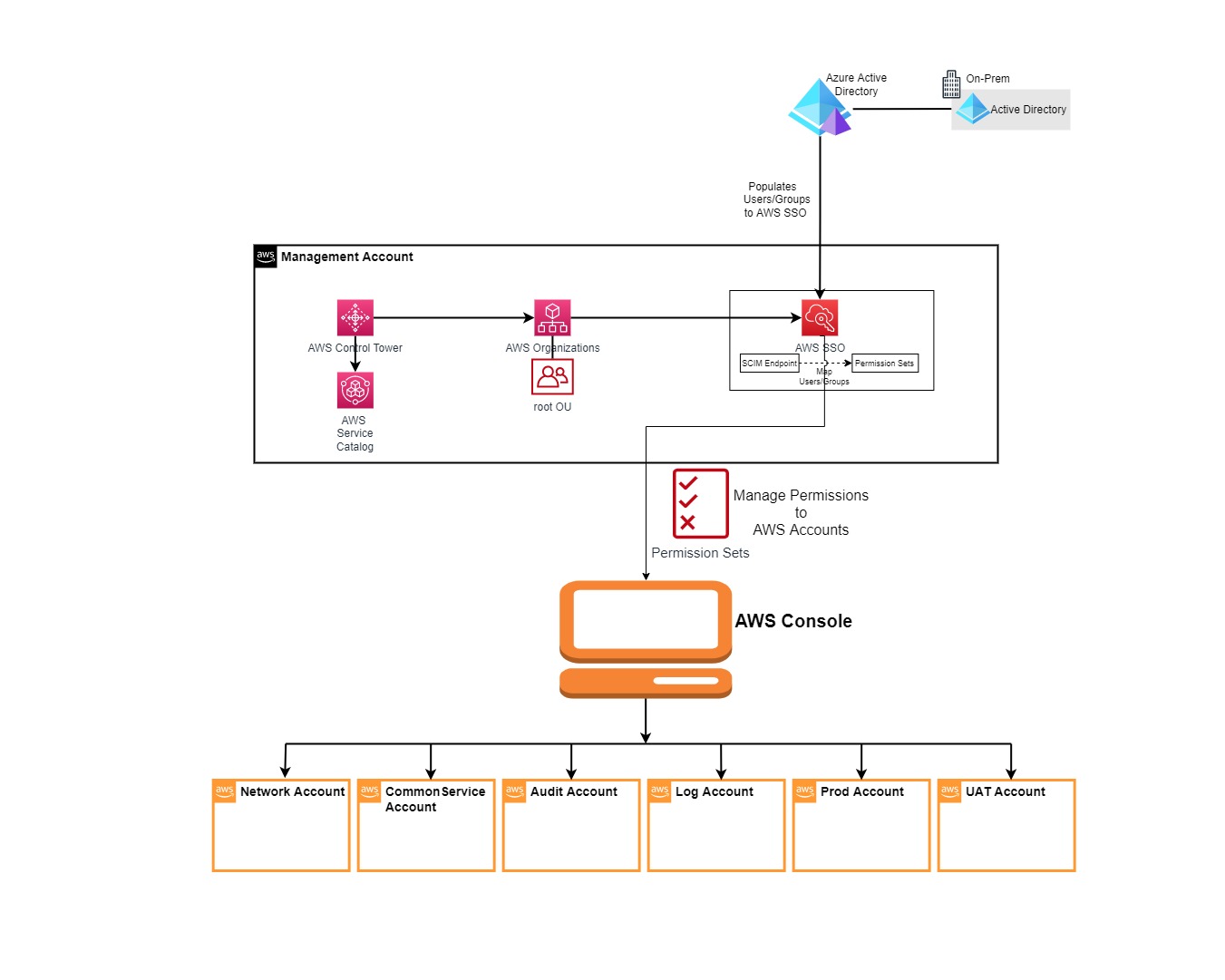
### 5.5 Authentication and Authorization:-

In AWS IAM Identity Center, authentication is the foundation of cloud access. Azure AD will reside at Azure infrastructure and AWS IAM Identity Center will sync identities from Azure AD.



At a high level the workflow for user management will be as follows:

* Azure AD users/groups gets populated to AWS SSO as part of Azure AD integration with AWS SSO.
* Permission Sets will be created based on the level of access to be provided to particular Group or User.
* The process of mapping the AWS Account, and the permission sets will be manual in nature. This combination ensures that the members of the ADFS can only assume the roles they have been assigned in the allowed AWS account.
* User access to different AWS accounts will be managed through the AWS SSO Permission Sets.



### 5.6 SAML Federation

IAM Identity Center supports identity federation with [SAML (Security Assertion Markup Language)](https://wiki.oasis-open.org/security) 2.0. SAML 2.0 is an industry standard used for securely exchanging SAML assertions that pass information about a user between a SAML authority (called an identity provider or IdP), and a SAML consumer (called a service provider or SP). IAM Identity Center uses this information to provide federated single sign-on access for those users who are authorized to use applications within the AWS access portal.

IAM Identity Center adds SAML IdP capabilities to either your AWS Managed Microsoft AD or your IAM Identity Center identity store. Users can then single sign-on into services that support SAML, including the AWS Management Console and third-party applications such as Microsoft 365, SAP Concur, and Salesforce.

.

### 5.7 Single Sign-On

Single sign-on (SSO) is an authentication solution that allows users to log in to multiple applications and websites with one-time user authentication. Given that users today frequently access applications directly from their browsers, organizations are prioritizing access management strategies that improve both security and the user experience. SSO delivers both aspects, as users can access all password-protected resources without repeated logins once their identity is validated.

**Key Benefits**

Provide a better customer experience

* Users are automatically signed into both on-premises and cloud-based applications.
* Users don't have to enter their passwords repeatedly.

Easy to deploy & administer

* No additional components needed on-premises to make this work.
* Users manage fewer passwords and can still securely access the information and apps they need to complete their day-to-day jobs.

Improve security posture

* By minimizing the number of passwords per user, SSO facilitates user access auditing and provides robust access control to all types of data. This reduces the risk of security events that target passwords, while helping organizations comply with data security regulations.

# 6. AWS Organizations and AWS Account Strategy

The basis of a well-architected multi-account AWS environment is AWS Organizations, an AWS service that enables you to centrally manage and govern multiple accounts.

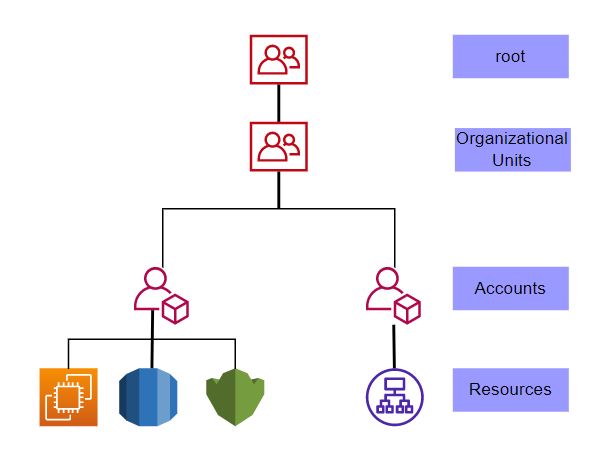
An organizational unit (OU) is a logical grouping of accounts in an AWS Organization. OUs enable you to organize your accounts into a hierarchy, and make it easier for you to apply management controls. AWS Organizations policies are what you use to apply such controls.

AWS organization decisions are a foundation for all compliance-related design areas. The goal of AWS organization planning is to establish consistent patterns for the following areas:

* Naming
* Tagging
* Organizational Unit design
* Account design

A key consideration for AWS organization design is to simplify management across the environment for increased workload numbers and scale. AWS landing zone design and implementation should consider foundational organizational unit (OU) and account structure, to avoid creating scaling constraints later.

The following diagram shows the three scope levels for organizing AWS resources: organizational units, accounts, and resources.



### 6.1 Key Design Principles: -

As Mahindra Finance prepares to build an AWS environment across multiple AWS accounts, AWS Organizations is used to manage the administration and grouping of these accounts. The following design principles helped guide the initial OU and account design and will also help evolve it over time:

1. **Organize based on security and operational needs**: It is recommended that accounts are organized using OUs based on business function, compliance requirements, or a common set of controls rather than mirroring the organization’s reporting structure.
2. **Apply security guardrails to lowest OU in the hierarchy**: Where feasible, it is recommended that security guardrails, for example SCPs, are applied to lowest nested OUs rather than the parent OU. This can help efficiently manage the distribution of guardrails across accounts that have the same or similar requirements.
3. **Avoid deep OU hierarchies**: Overly complicated structures can be difficult to understand and maintain. Although AWS Organizations supports a depth of five levels of OUs, the recommended structure strives to use OUs only when there is sufficient benefit.
4. **Start small, simple and expand as needed**: Start with a subset of the OUs, and expand the structure of AWS accounts when the organization needs call for the creation of new OUs.
5. **Avoid deploying workloads to the organization’s management accou**nt: Since privileged operations can be performed within an organization’s management account and SCPs do not apply to the management account, Blazeclan strongly recommends that Mahindra Finance limit access to the AWS organization’s management account. Mahindra Finance should also limit the cloud resources and data contained in the management account to only those that must be managed in the management account.
6. **Separate production from non-production workloads**: Blazeclan recommends that Mahindra Finance separate production workloads from non-production workloads. For a given type of workload, it typically has multiple instances (e.g. Development, UAT, Production). This setup means that application teams can experiment, develop, and test changes to the workload before you promote and deploy those changes to the production instances of the workload. Separate non-production workload environments are generally required to support the software development lifecycle (SDLC) processes.
7. **Assign a single or small set of related workloads to each account**: In support of Mahindra Finance’s application workloads especially production workloads, AWS recommends that you either assign a single workload to each account or assign a small set of closely related workloads to each account.

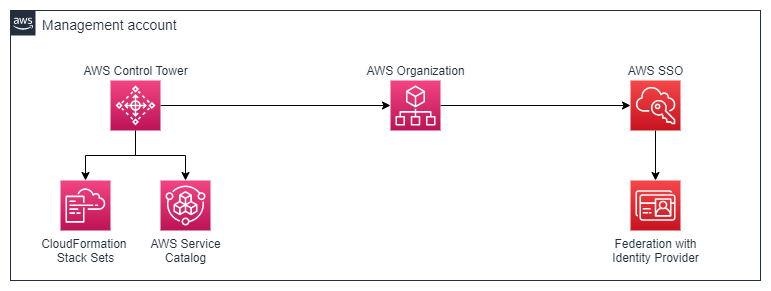
Consider separating workloads that have different owners into their own accounts to simplify access management, streamline change approval processes, and limit the scope of impact for misconfigurations.

1. **Use federated access to help simplify managing human access to accounts**: BlazeClan recommends that you use AWS identity federation capabilities via AWS Identity Provider (successor to AWS SSO). These capabilities will enable Mahindra Finance to use a common identity provider and its existing processes for controlling human user access to AWS accounts.

### 6.2 Management Account: -

The Management Account is the account that gets created specifically for the new landing zone. This account will be used for consolidated billing for everything in the new landing zone. It will also be used for provisioning new AWS accounts through Account Factory, managing AWS Organizations Units & Guardrails and managing user access & permission sets through AWS Identity Provider (AWS Single Sign-On).

It is not recommended to run any type of production workloads from an AWS Control Tower management account.



Details of Management account

|  |  |  |  |
| --- | --- | --- | --- |
| No | Account ID | Account Name | Email ID |
| 1 | 468780636783 | MahindraMahindraFinance | rootawsmmfsl@mahindra.com |

### 6.3 Organizational Units (OU): -

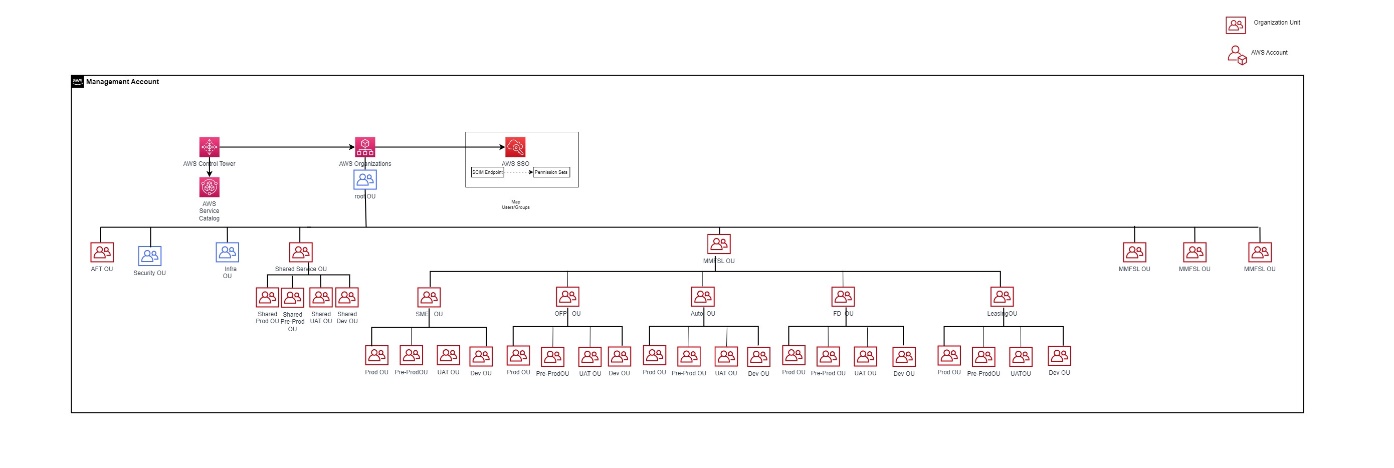
Organizational units (OUs) are used to group accounts together to administer as a single unit. This greatly simplifies the management of your accounts. For example, you can attach a policy-based control to an OU, and all accounts within the OU automatically inherit the policy. You can create multiple OUs within a single organization, and you can create OUs within other OUs. Each OU can contain multiple accounts, and you can move accounts from one OU to another. However, OU names must be unique within a parent OU or root.

Organizational Unit is a tool to help you structure your cloud environments for organization and governance at scale.

Organizational Unit structure is finalized as per below structure: -

Under root OU there will be 8 Organizational units Security OU, Infra OU, AFT OU, Shared Service OU, MMFSL OU, MRHFL OU, MIBL OU, and MMAMC OU.

Proposed Management Account and OU design diagram



|  |  |
| --- | --- |
| **Organizational Unit (OU)** | **Description** |
| **Root** | The parent container for all the accounts for your organization. If you apply a policy to the root, it applies to all organizational units (OUs) and [accounts](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_getting-started_concepts.html#account) in the organization. |
| **Security** | This OU houses a couple of major accounts in Landing Zone design. They are Audit and Log accounts. This follows standard implementation of AWS Control Tower. |
| **Infra** | This OU hosts all AWS Accounts that are used for managing all infrastructures, or become the central access for the whole landing zone. They are Network, Inspection and Common accounts.  The Infra organizational unit for services which are used in the Organization such as Bastion Host, Route53 Resolver. |
| **AFT** | This OU hosts AWS account which is used to run Account Factory for Terraform (AFT) operations. |
| **Shared Service** | This organizational unit contains environment based nested OUs to host AWS accounts which acts as VPC owner for other small project AWS accounts.  This contain nested OUs – Shared Prod, Shared Dev, Shared UAT |
| **MMFSL** | The parent organizational unit for some of the landing zone nested organizational unit.  It will have workload agnostic AWS Guardrail policies assigned to ensure workloads are secure and compliant. This contain nested OUs – SME, OFP, AUTO, FD, LEASING. |
| **MRHFL** | The parent organizational unit for some of the landing zone nested organizational unit.  It will have workload agnostic AWS Guardrail policies assigned to ensure workloads are secure and compliant. This contain nested OUs based on departments. |
| **MIBL** | The parent organizational unit for some of the landing zone nested organizational unit.  It will have workload agnostic AWS Guardrail policies assigned to ensure workloads are secure and compliant. This contain nested OUs based on departments. |
| **MMAMC** | The parent organizational unit for some of the landing zone nested organizational unit.  It will have workload agnostic AWS Guardrail policies assigned to ensure workloads are secure and compliant. This contain nested OUs based on departments. |

### 6.4 AWS Accounts: -

An AWS account acts as a resource container and resource isolation boundary. An AWS account can be associated with billing and payment. An AWS account is different than a user account (sometimes called an [IAM account](https://docs.aws.amazon.com/controltower/latest/userguide/setting-up.html#setting-up-iam)) in AWS Control Tower. Accounts created through the Account Factory provisioning process are AWS accounts. AWS accounts also can be added to AWS Control Tower by means of the account enrolment or OU registration process.

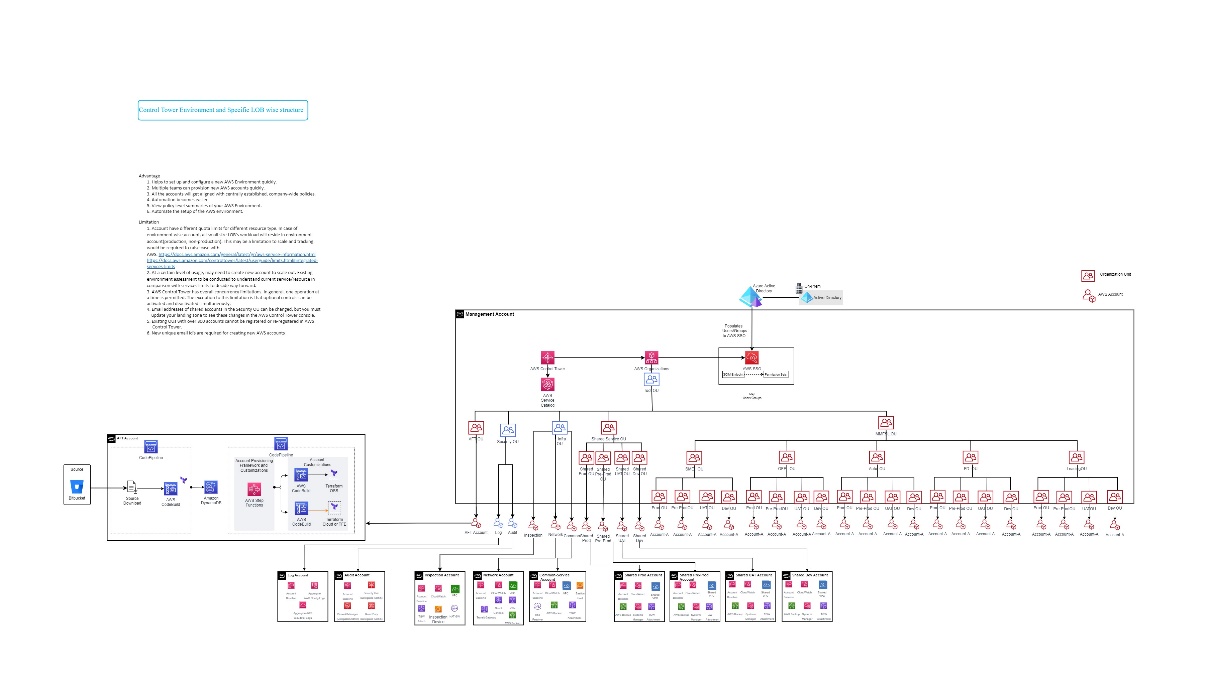
AWS accounts are categorized in below way: -

* Security OU will have 2 AWS accounts that are Audit account, and Log account.
* Infra OU will have 3 AWS accounts that are Network, Inspection, and Common-Service account.
* AFT OU will have 1 AWS account that is AFT account.
* Shared Service OU will have 3 nested OUs which are categorized like environments Prod, Pre-Prod UAT, DEV. Under these nested organizational units there will be single AWS account in each OU that are Shared Prod, Shared Pre-Prod, Shared UAT, and Shared Dev.
* MMFSL OU will have 5 nested OUs i.e. SME, OFP, Auto, FD, and Lease OU and at time of new project, corresponding nested OU will be created. Each nested OU will have further 4 nested OUs which are categorized like environments Prod, Pre-Prod, UAT, and DEV. Under each of the nested organizational units there will be an AWS account that are Prod, Pre-Prod, UAT, Dev in their respective OUs.

AWS accounts details: -

|  |  |  |
| --- | --- | --- |
| **Account Name** | **Account ID** | **Email ID** |
| Account-LZ-Audit | 171594474909 | auditawsmmfsl@mahindra.com |
| Account-LZ-Log-Archive | 565215823508 | logawsmmfsl@mahindra.com |
| AFT-Management-Account | 113110351789 | Aftaws.mmfsl@mahindra.com |
| Account-LZ-Inspection | 763163983206 | iaawsmmfsl@mahindra.com |
| Account-LZ-ComSrv | 453463462350 | csawsmmfsl@mahindra.com |
| Account-LZ-Network | 134764736910 | NWAWSMMFSL@mahindra.com |
|  |  |  |

Approved AWS Account structure diagram-



### 6.5 Quotas for AWS Organization

Organizations is a global service that is physically hosted in the US East (N. Virginia) Region (us-east-1). Therefore, you must use us-east-1 to access Organizations quotas when using the Service Quotas console, the AWS CLI, or an AWS SDK.

|  |  |
| --- | --- |
| Number of AWS accounts in an organization | 10 — The default maximum number of accounts allowed in an organization. If you need more, you can request an increase by using the Service Quotas console. |
| An invitation sent to an account counts against this quota. The count is returned if the invited account declines, the management account cancels the invitation, or the invitation expires. |
| Number of roots in an organization | 1 |
| Number of OUs in an organization | 1000 |
| Number of policies of each type in an organization | 1000 per policy type |
| Maximum size of a policy document | Service control policies: 5120 bytes *(not characters)* |
|  |
| AI services opt-out policies: 2500 characters |
|  |
| Backup policies: 10,000 characters |
|  |
| Tag policies: 10,000 characters |
|  |
| **Note:** If you save the policy by using the AWS Management Console, extra white space (such as spaces and line breaks) between JSON elements and outside of quotation marks, is removed and not counted. If you save the policy using an SDK operation or the AWS CLI, then the policy is saved exactly as you provided and no automatic removal of characters occurs. |
| OU maximum nesting in a root | Five levels of OUs deep under a root. |
| Maximum number of invitations attempts you can perform in a 24-hour period | Either 20 or the maximum number of accounts allowed in your organization, whichever is greater. Accepted invitations don't count against this quota. As soon as one invitation is accepted, you can send another invitation that same day. |
|  |
| If the maximum number of accounts allowed in your organization is less than 20, then you get an "account limit exceeded" exception if you attempt to invite more accounts than your organization can contain. However, you can cancel invitations and send new ones up to the maximum of 20 attempts in one day. |
| Number of member accounts you can create concurrently | 5 — As soon as one finishes, you can start another, but only five can be in progress at a time. |
| Number of member accounts you can close in a 30 day period | 10% of active member accounts in an organization can be closed within a 30 day period. The maximum account closure is 200, even if 10% active accounts exceeds 200. |
| Number of member accounts you can close concurrently | 3 — Only three account closures can be in progress at the same time. As soon as one finishes, you can close another account. |
| Number of entities to which you can attach a policy | Unlimited |
| Number of tags that you can attach to a root, OU, or account | 50 |

### 

### 6.6 AWS Service and Service Endpoints and Quotas

|  |  |  |  |
| --- | --- | --- | --- |
| **Quota name** | **Applied quota value** | **AWS default quota value** | **Adjustable** |
| Auto Scaling groups per region | 500 | 500 | Yes |
| Classic Load Balancers per Auto Scaling group | Not available | 50 | No |
| Launch configurations per region | 200 | 200 | Yes |
| Lifecycle hooks per Auto Scaling group | Not available | 50 | No |
| Scaling policies per Auto Scaling group | Not available | 50 | No |
| Scheduled actions per Auto Scaling group | Not available | 125 | No |
| SNS topics per Auto Scaling group | Not available | 10 | No |
| Step adjustments per step scaling policy | Not available | 20 | No |
| Target groups per Auto Scaling group | Not available | 50 | No |
| All Standard (A, C, D, H, I, M, R, T, Z) Spot Instance Requests | 5 | 5 | Yes |
| AMI sharing | 1,000 | 1,000 | Yes |
| AMIs | 50,000 | 50,000 | Yes |
| Attachments per transit gateway | 5,000 | 5,000 | Yes |
| Attachments per VPC | 5 | 5 | No |
| EC2-VPC Elastic IPs | 5 | 5 | Yes |
| Peering attachments per transit gateway | 50 | 50 | Yes |
| Route Tables per transit gateway | Not available | 20 | Yes |
| Routes per transit gateway | 10,000 | 10,000 | Yes |
| Transit gateways per account | 5 | 5 | Yes |
| Transit gateways per Direct Connect Gateway | Not available | 3 | No |
| Virtual private gateways per region | 5 | 5 | Yes |
| VPN connections per region | 50 | 50 | Yes |
| Buckets | Not available | 100 | Yes |
| Bucket policy | Not available | 20 kilobytes | No |
| Object size | Not available | 5 terabytes | No |
| DB instances | 20 | 40 | Yes |
| DB clusters | 40 | 40 | Yes |
| Read replicas per master | 15 | 15 | Yes |
| Total storage for all DB instances | 100,000 gigabytes | 100,000 gigabytes | Yes |
| Number of groups supported in IAM Identity Center | Not available | 1,00,000 | No |
| Number of permission sets allowed in IAM Identity Center | Not available | 2,000 | Yes |
| Number of permission sets allowed per AWS account | Not available | 50 | Yes |
| Number of users supported in IAM Identity Center | Not available | 1,00,000 | Yes |
| Total number of AWS accounts or applications that can be configured | Not available | 3,000 | Yes |
| ACM certificates | Not available | 2,500 | Yes |
| ACM certificates created in last 365 days | Not available | 5,000 | Yes |
| Domain names per ACM certificate | Not available | 10 | Yes |
| Imported certificates | Not available | 2,500 | Yes |
| Imported certificates in last 365 days | Not available | 5,000 | Yes |
| Application Load Balancers per Region | 50 | 50 | Yes |
| Certificates per Application Load Balancer | 25 | 25 | Yes |
| Classic Load Balancers per Region | 20 | 20 | Yes |
| Listeners per Application Load Balancer | 50 | 50 | Yes |
| Network Load Balancers per Region | 50 | 50 | Yes |
| Targets per Application Load Balancer | 1,000 | 1,000 | Yes |
| Clusters | 100 | 100 | Yes |
| Control plane security groups per cluster | 4 | 4 | No |
| Fargate profiles per cluster | 10 | 10 | Yes |
| Label pairs per Fargate profile selector | 5 | 5 | Yes |
| Managed node groups per cluster | 30 | 30 | Yes |
| Nodes per managed node group | 450 | 450 | Yes |
| Public endpoint access CIDR ranges per cluster | 40 | 40 | No |
| Registered clusters | 10 | 10 | Yes |
| Selectors per Fargate profile | 5 | 5 | Yes |
| CompleteSnapshot requests per account | 10 per second | 10 per second | No |

Refer below links for detailed AWS Service Endpoints and quotas:

*https://docs.aws.amazon.com/general/latest/gr/aws\_service\_limits.html?ref=wellarchitected*

*https://docs.aws.amazon.com/pdfs/general/latest/gr/aws-general.pdf#aws-service-information*



### 6.7 AWS Control Tower guardrails: -

AWS Control Tower implements preventive and detective controls that help govern the resources and monitor compliance across all the AWS accounts in the Landing Zone.

**Guardrail behaviour**

* Prevention – A preventive guardrail will ensure that accounts maintain compliance, because it disallows actions that lead to policy violations. The status of a preventive guardrail will be either enforced or not enabled.
* Detection – A detective guardrail will detect non-compliance of resources within the accounts, such as policy violations, and will provide an alert through the dashboard. The status of a detective guardrail will either be clear, in violation, or not enabled.

**Implementation of guardrail behaviour**

* The preventive guardrails are implemented using Service Control Policies (SCPs), which are part of AWS Organizations.
* The detective guardrails are implemented using AWS Config rules and AWS Lambda functions.

**Note:** The root user and any IAM administrators in the Management account can perform work that preventive guardrails would otherwise deny. This exception will prevent the management account from entering into an unusable state. All actions taken within the management account continue to be tracked in the logs contained within the log archive account, for purposes of accountability and auditing.

AWS Control Tower provides three categories of guidance: mandatory, strongly recommended, and elective guardrails.

When you create a new landing zone, all mandatory guardrails are enabled by default. Strongly recommended and elective guardrails are not enabled by default.

Mahindra Finance will enable recommended Strongly Recommended and Elective guardrails on the nested OUs which is at the bottom in the hierarchy. Further based on application and operations needs if any guardrail needs to be removed for operational reason will be decided on case to case basis.

### 6.8 Mandatory guardrails: -

The following Mandatory guardrails are enabled by default. As AWS continues to improve the AWS Control Tower service additional mandatory guardrails may be added in the future.

|  |  |  |
| --- | --- | --- |
| **Name** | **Behaviour** | **Purpose** |
| Disallow deletion of log archive | Prevention | Prevent deletion of Amazon S3 buckets created by AWS Control Tower in the log archive account. |
| Detect public read access setting for log archive | Detection | Detect public read access setting for Amazon S3 buckets created by AWS Control Tower in the log archive account. |
| Detect public write access setting for log archive | Detection | Detect public write access setting for Amazon S3 buckets created by AWS Control Tower in the log archive account. |
| Disallow configuration changes to CloudTrail | Prevention | Log API activity in a consistent manner by ensuring that your AWS CloudTrail settings do not change. |
| Integrate CloudTrail events with CloudWatch Logs | Prevention | Perform real-time analysis of activity data by sending AWS CloudTrail events to AWS CloudWatch logs. |
| Enable CloudTrail in all available regions | Prevention | Track AWS API call activity within your accounts using AWS CloudTrail, which records call history including the identity of the caller and the time of the call. |
| Enable integrity validation for CloudTrail log file | Prevention | Protect the integrity of account activity logs using AWS CloudTrail log file validation, which creates a digitally signed digest file that contains a hash of each log that CloudTrail writes to Amazon S3. |
| Disallow changes to Amazon CloudWatch set up by AWS Control Tower | Prevention | Prevent changes to Amazon CloudWatch configuration set up by AWS Control Tower to monitor your environment. |
| Disallow deletion of AWS Config Aggregation Authorizations created by AWS Control Tower | Prevention | Prevent deletion of AWS Config aggregation authorizations created by AWS Control Tower. |
| Disallow changes to tags created by AWS Control Tower for AWS Config resources | Prevention | Prevents updates or deletion of tags created by AWS Control Tower for AWS Config resources. |
| Disallow configuration changes to AWS Config | Prevention | Record resource configurations in a consistent manner by ensuring that AWS Config settings don't change. |
| Enable AWS Config in all available regions | Prevention | Identify configuration changes to AWS resources using AWS Config. |
| Disallow changes to AWS Config Rules set up by AWS Control Tower | Prevention | Prevent changes to AWS Config Rules set up by AWS Control Tower. |
| Disallow Changes to Encryption Configuration for AWS Control Tower Created S3 Buckets in Log Archive | Prevention | Prevent encryption configuration changes to Amazon S3 buckets created by AWS Control Tower. |
| Disallow changes to lifecycle configuration for AWS Control Tower created Amazon S3 buckets in log archive | Prevention | Prevent lifecycle configuration changes to Amazon S3 buckets created by AWS Control Tower. |
| Disallow changes to logging configuration for AWS Control Tower created Amazon S3 buckets in log archive | Prevention | Prevent logging configuration changes to the Amazon S3 buckets created by AWS Control Tower. |
| Disallow changes to bucket policy for AWS Control Tower created Amazon S3 buckets in log archive | Prevention | Prevent bucket policy changes to the Amazon S3 buckets created by AWS Control Tower. |
| Detect whether a shared account in the Security organizational unit has AWS CloudTrail or CloudTrail Lake enabled. | Detection | Detects whether a shared account in the Security organizational unit has AWS CloudTrail or CloudTrail Lake enabled. The rule is NON\_COMPLIANT if either CloudTrail or CloudTrail Lake is not enabled in an account. |
| Disallow changes to AWS IAM roles set up by AWS Control Tower and AWS CloudFormation | Prevention | Prevent changes to AWS IAM roles set up for your accounts by AWS Control Tower and AWS CloudFormation. |
| Disallow changes to AWS Lambda functions set up by AWS Control Tower | Prevention | Prevent changes to AWS Lambda functions set up by AWS Control Tower. |
| Disallow changes to Amazon CloudWatch Logs log groups set up by AWS Control Tower | Prevention | Prevent deletion and modification of retention policy for Amazon CloudWatch Logs log groups set up by AWS Control Tower. |
| Disallow changes to Amazon SNS set up by AWS Control Tower | Prevention | Prevent changes to Amazon SNS notification settings set up by AWS Control Tower. |
| Disallow changes to Amazon SNS subscriptions set up by AWS Control Tower | Prevention | Prevent changes to Amazon SNS subscriptions set up by AWS Control Tower to trigger notifications for AWS Config Rule compliance changes. |

### 6.9 Strongly Recommended guardrails: -

The following Strongly Recommended guardrails will be enabled on lowest level nested OU in hierarchy. As AWS continues to improve the AWS Control Tower service additional Strongly Recommended guardrails may be added in the future.

|  |  |  |
| --- | --- | --- |
| **Name** | **Behaviour** | **Purpose** |
| Detect whether an account has AWS CloudTrail or CloudTrail Lake enabled. | Detection | Detects whether an account has AWS CloudTrail or CloudTrail Lake enabled. The rule is NON\_COMPLIANT if either CloudTrail or CloudTrail Lake is not enabled in an account. |
| Detect whether Amazon EBS optimization is enabled for Amazon EC2 instances | Detection | Detect whether Amazon EBS optimization is enabled for your Amazon EC2 instances that can be optimized for EBS. |
| Detect whether Amazon EBS volumes are attached to Amazon EC2 instances | Detection | Detect when an Amazon EBS volume device is not attached to an Amazon EC2 instance. |
| Detect whether encryption is enabled for Amazon EBS volumes attached to Amazon EC2 instances | Detection | Detect if the EBS volumes that are attached to an Amazon EC2 instance are encrypted. |
| Detect whether public access to Amazon RDS database instances is enabled | Detection | Detect Amazon RDS database instances that allow public access. |
| Detect whether public access to Amazon RDS database snapshots is enabled | Detection | Secure your Amazon RDS database snapshots by detecting whether public access is enabled. |
| Detect whether storage encryption is enabled for Amazon RDS database instances | Detection | Detect Amazon RDS database instances that are not encrypting their underlying storage. |
| Detect whether unrestricted incoming TCP traffic is allowed | Detection | Reduce a server's exposure to risk by detecting whether unrestricted incoming TCP traffic is allowed. |
| Detect whether unrestricted internet connection through SSH is allowed | Detection | Detect unrestricted connectivity to remote console services such as SSH. |
| Disallow actions as a root user | Prevention | Secure your AWS accounts by disallowing account access with root user credentials, which are credentials of the account owner and allow unrestricted access to all resources in the account. We recommend that you instead create AWS Identity and Access Management (IAM) users for everyday interaction with your AWS account. |
| Disallow creation of access keys for the root user | Prevention | Secure your AWS accounts by disallowing creation of access keys for the root user, which will allow unrestricted access to all resources in the account. We recommend that you instead create access keys for an AWS Identity and Access Management (IAM) user for everyday interaction with your AWS account. |
| Detect whether MFA for the root user is enabled | Detection | Detect whether root user has Multi-Factor Authentication (MFA) enabled, MFA requires an additional authentication code after the user name and password are successful. |
| Detect whether public read access to Amazon S3 buckets is allowed | Detection | Secure access to data stored in Amazon S3 buckets by detecting whether public read access is allowed. |
| Detect whether public write access to Amazon S3 buckets is allowed | Detection | Secure access to data stored in Amazon S3 buckets by detecting whether public write access is allowed. |

### 6.10 Elective guardrails: -

The following Elective guardrails will be enabled on lowest level nested OU in hierarchy. Elective Guardrails will be implemented and accessed further based on application and operations needs if any rule/guardrails need to be removed for operational reason. As AWS continues to improve the AWS Control Tower service additional Strongly Recommended guardrails may be added in the future.

|  |  |  |
| --- | --- | --- |
| **Name** | **Behaviour** | **Purpose** |
| Disallow Changes to Encryption Configuration for Amazon S3 Buckets | Prevention | Prevent changes to encryption configuration for your Amazon S3 buckets. |
| Disallow Changes to Logging Configuration for Amazon S3 Buckets | Prevention | Prevent changes to bucket logging for your Amazon S3 buckets. |
| Disallow Changes to Bucket Policy for Amazon S3 Buckets | Prevention | Prevent changes to bucket policy for your Amazon S3 buckets. |
| Disallow Changes to Lifecycle Configuration for Amazon S3 Buckets | Prevention | Prevent changes to lifecycle configuration for your Amazon S3 buckets. |
| Detect whether public IP addresses for Amazon EC2 Auto Scaling are enabled through launch configurations | Detection | Detects whether Amazon EC2 Auto Scaling groups have public IP addresses enabled through launch configurations. This rule is NON\_COMPLIANT if the launch configuration for an Auto Scaling group has the value of the field AssociatePublicIpAddress set as True. |
| Disallow cross-region networking for Amazon EC2, Amazon CloudFront, and AWS Global Accelerator | Prevention | Disallow cross-region networking connections from Amazon EC2, Amazon CloudFront, and AWS Global Accelerator services. |
| Disallow internet access for an Amazon VPC instance managed by a customer | Prevention | Disallow internet access for an Amazon Virtual Private Cloud (VPC) instance managed by a customer, rather than by an AWS service. The AWS Control Tower Account Factory setting to provision accounts with VPC internet access overrides this control. |
| Disallow Amazon Virtual Private Network (VPN) connections | Prevention | Disallows Virtual Private Network (VPN) connections (Site-to-Site VPN and Client VPN) to an Amazon Virtual Private Cloud (VPC). |
| Detect whether replication instances for AWS Database Migration Service are public | Detection | Detects whether AWS Database Migration Service replication instances are public. The rule is NON\_COMPLIANT if the value of the PubliclyAccessible field is set as True. |
| Detect whether Amazon EBS snapshots are restorable by all AWS accounts | Detection | Detects whether all AWS accounts have access to restore Amazon EBS snapshots. The rule is NON\_COMPLIANT if any snapshots have the RestorableByUserIds field set to the value All. In that case, the Amazon EBS snapshots are public. |
| Detect whether any Amazon EC2 instance has an associated public IPv4 address | Detection | Detects whether an Amazon Elastic Compute Cloud (Amazon EC2) instance has an associated public IPv4 address. The rule is NON\_COMPLIANT if the public IP field is present in the Amazon EC2 instance configuration item. This control applies only to IPv4 addresses. |
| Detect whether an Amazon EKS endpoint is blocked from public access | Detection | Detects whether an Amazon Elastic Kubernetes Service (Amazon EKS) endpoint is publicly accessible. The rule is NON\_COMPLIANT if the endpoint is publicly accessible. |
| Detect whether an Amazon OpenSearch Service domain is in Amazon VPC | Detection | Detects whether Amazon OpenSearch Service domains are in Amazon Virtual Private Cloud (Amazon VPC). The rule is NON\_COMPLIANT if the OpenSearch Service domain endpoint is public. |
| Detect whether any Amazon EMR cluster master nodes have public IP addresses | Detection | Detects whether any Amazon Elastic MapReduce (EMR) cluster master nodes have public IP addresses. The rule is NON\_COMPLIANT if a master node has a public IP. This control checks clusters that are in RUNNING or WAITING state. |
| Detect whether MFA is enabled for AWS IAM users | Detection | Detect whether multi-factor authentication (MFA) is enabled for any AWS Identity and Access Management (IAM) user using the console. MFA requires an additional authentication code after the user name and password are successful. |
| Detect whether the AWS Lambda function policy attached to the Lambda resource blocks public access | Detection | Detects whether the AWS Lambda function policy attached to the Lambda resource prohibits public access. The rule is NON\_COMPLIANT if the Lambda function policy allows public access. |
| Detect whether MFA is enabled for AWS IAM users of the AWS Console | Detection | Detect whether multi-factor authentication (MFA) is enabled for any AWS Identity and Access Management (IAM) user using the console. MFA requires an additional authentication code after the user name and password are successful. |
| Detect whether public routes exist in the route table for an Internet Gateway (IGW) | Detection | Detects whether public routes exist in the route table associated with an Internet Gateway (IGW). The rule is NON\_COMPLIANT if a route has a destination CIDR block of '0.0.0.0/0' or '::/0' or if a destination CIDR block does not match the rule parameter. |
| Detect whether Amazon Redshift clusters are blocked from public access | Detection | Detects whether Amazon Redshift clusters are blocked from public access. The rule is NON\_COMPLIANT if the publiclyAccessible field is true in the cluster configuration item. |
| Deny access to AWS based on the requested AWS Region | Prevention | Disallows access to unlisted operations in global and regional services outside of the specified Regions. |
| Disallow changes to replication configuration for Amazon S3 buckets | Prevention | Prevent changes to replication configuration for Amazon S3 buckets. |
| Disallow delete actions on S3 buckets without MFA | Prevention | Protect your Amazon S3 buckets by requiring multi-factor authentication (MFA) for delete actions. MFA requires an additional authentication code after the user name and password are successful. |
| Detect whether Amazon S3 settings to block public access are set as true for the account | Detection | Periodically detects whether the required Amazon S3 settings to block public access are configured as true for the account, rather than for a bucket or an access point. |
| Detect whether versioning for Amazon S3 buckets is enabled | Detection | Protect your Amazon S3 buckets by detecting whether versioning is enabled. Versioning allows you to recover objects from accidental deletion or overwrite. |
| Detect whether an Amazon SageMaker notebook instance allows direct internet access | Detection | Detects whether direct internet access is allowed for an Amazon SageMaker notebook instance. The rule is NON\_COMPLIANT if Amazon SageMaker notebook instances allow direct internet access. |
| Detect whether AWS Systems Manager documents owned by the account are public | Detection | Detects whether AWS Systems Manager (SSM) documents owned by the account are public. This rule is NON\_COMPLIANT if any documents with owner 'Self' are public. |
| Detect whether any Amazon VPC subnets are assigned a public IP address | Detection | Detects whether Amazon Virtual Private Cloud (Amazon VPC) subnets are assigned a public IP address. The rule is COMPLIANT if Amazon VPC does not have subnets that are assigned a public IP address. The rule is NON\_COMPLIANT if Amazon VPC has subnets that are assigned a public IP address. |

### 6.11 Naming: -

An effective naming convention composes resource names from important information about each resource. A good name helps you quickly identify the resource's type, associated workload, deployment environment, and the AWS region hosting it.

**Resource Naming**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **#** | **No. of Alphabets** | **Mandatory** | **Description** | **Example** | **Remarks** |
| **1** | 3 | Yes | Hyperscalar Service abbreviation | vpc, ec2, snt (subnet), eks, sgp (Security Group) |  |
| **2** | 3 | Yes | Hyperscallar Provided | aws/gcp/azu |  |
| **3** | 3 | Yes | Entity Name | mfs/mib/rhf/mam | 3 characters from name of MMFSL, MRHFL,MIBL,MMAMC |
| **4** | 5 | Yes | Combination of Region, Environment, Tier | mprdw | mprdw: m->mumbai region; prd->environment;w->web tier |
| **5** | 3 | Yes | Combination of availability zone and number | a01 | a01: a-> az-a; 01->number |
|  | 17 | Total Alphabets |  |  |  |
|  | - | Separator hyphen |  |  |  |
|  | 25 | Total max character |  |  |  |
|  |  |  |  |  |  |
|  | **Example** |  |  |  |  |
|  | **VPC** | vpc-aws-mfs-mprdw-001 |  |  |  |
|  | **Subnet** | snt-aws-mfs-mprdw-a01 |  |  |  |
|  |  |  |  |  |  |

### 6.12 Tagging: -

The following list provides examples of common tags that capture important context and information about a resource:

Tag Info for Accounts

|  |  |  |
| --- | --- | --- |
| **Tag Key** | **Description** | **Required** |
| application-owner | Name Of Application Owner who is responsible for managing the functional Availability of the application i.e. mPaaS Manager approval | Required |
| application-technical-Group | Concern Person who will be able to Provide  technical support related application i.e. This is similar to requestor name and later can be changed as project progresses | Optional |
| requester-name | User that requested the creation of this application. | Required |
| cost-center | Cost centre code | Required |
| business-unit | Business Unit | Required |
| department | Department in case further business specific requirement | Optional |
| created-by | Name of person who is creating the Resource i.e. Secondary approval in mPaaS | Required |
| created-date | Date when the Project is created | Required |
| environment | UAT/Dev/Production/Sandbox etc | Required |
|
|
|
| bussiness-project-name | Name of the specific project for which the resource is created | Required |
| application-landscape | Name of the Specific application- technical name  for which the resource is used | Required |
| shared-dedicate | Is this shared resource ? Shared = Common resources which is used by multiple resources | Required |
| application-criticality | Criticality of the application ( MC Mission Critical/BC Business Critical etc .. ) | Required |
| Default value is Business Critical |
|  |
|  |
| compliance | STD and PDPA /GDPR | Required |
| Default is STD |
| application-sub-group | Name of the Project for which the application / resource will be used | Optional |
| application-owner-secondary | Name Of Application Owner who is responsible for managing the functional Availability of the application i.e. This is to create redundancy if primary contact is not available | Optional |
| instance-type | Type of instance / Resource created | Required |
| reserve-instance | Yes / No if it’s a reserved instance | Conditional |
| schedule | Can this be Auto Start / Stop | Conditional |

# 7. Platform Automation and DevOps

Platform automation and DevOps evaluate opportunities to modernize your approach to environmental deployment with infrastructure as code options.

### 7.1 Platform Automation: -

Platform automation focuses on tools and techniques that enable the streamlining of tasks. These tasks might have been performed manually or using automation tools such as AWS DevOps Services, Jenkins, GitHub, Artifactory.

Platform automation is directly applicable to the outcomes associated with implementing an AWS landing zone, and supports the concept of building repeatable, scalable environments.

Automated processes and tools enable deployment activities to be configured as 'stages' in a pipeline. This sequence of tasks is completed in a prescribed order, which include built-in tests and checks to ensure successful completion.

### 7.2 DevOps and DevSecOps

DevOps processes will encourage the concepts of continuous integration and continuous deployment (CI/CD), which fosters a culture of refinement and improvement.

DevSecOps process will help to keep the pipeline and its components compliance and secured.

**mPass DevSecOps tool: -**

Use inhouse mPass tool for the AWS Landing Zone provisioning and AWS Infrastructure provisioning.

Also mPaas is capable of configuring CICD Pipelines for application releases as well as support DevSecOps processes.

### 7.3 Deploy AWS landing zones by using Terraform (AWS AFT)

The Terraform module(AWS AFT) for AWS landing zones is the official Terraform module for deploying the platform resources from the conceptual architecture for AWS landing zones. The module is designed to simplify the deployment of the accounts, and resources in the network, common-service and inspection-egress accounts.

Deployment of resources to application landing zones is outside the scope of the module. Decisions on the deployment method and tooling are for the team that's responsible for the application.

**Terraform Module: -**

[aws-ia/terraform-aws-control\_tower\_account\_factory: AWS Control Tower Account Factory (github.com)](https://github.com/aws-ia/terraform-aws-control_tower_account_factory)  
[HashiCorp (github.com)](https://github.com/orgs/hashicorp/repositories?q=aft&type=all&language=&sort=)

**AWS Blueprint: -**

[Deploy AWS Control Tower Account Factory for Terraform (AFT) - AWS Control Tower (amazon.com)](https://docs.aws.amazon.com/controltower/latest/userguide/aft-getting-started.html)

[Manage AWS Accounts Using Control Tower Account Factory for Terraform | Terraform | HashiCorp Developer](https://developer.hashicorp.com/terraform/tutorials/aws/aws-control-tower-aft)

# 8. Network topology and connectivity

Network topology is a critical element of landing zone architecture because it defines how applications communicate with each other.

### 8.1 Define an AWS network topology: -

This section discusses in detail about building the landing zone network design. The landing zone network design has three major components which are the collection of AWS Native network services and the industry best practice Firewall solution to ensure highly sophisticated network and secure environment. The components are given below: -

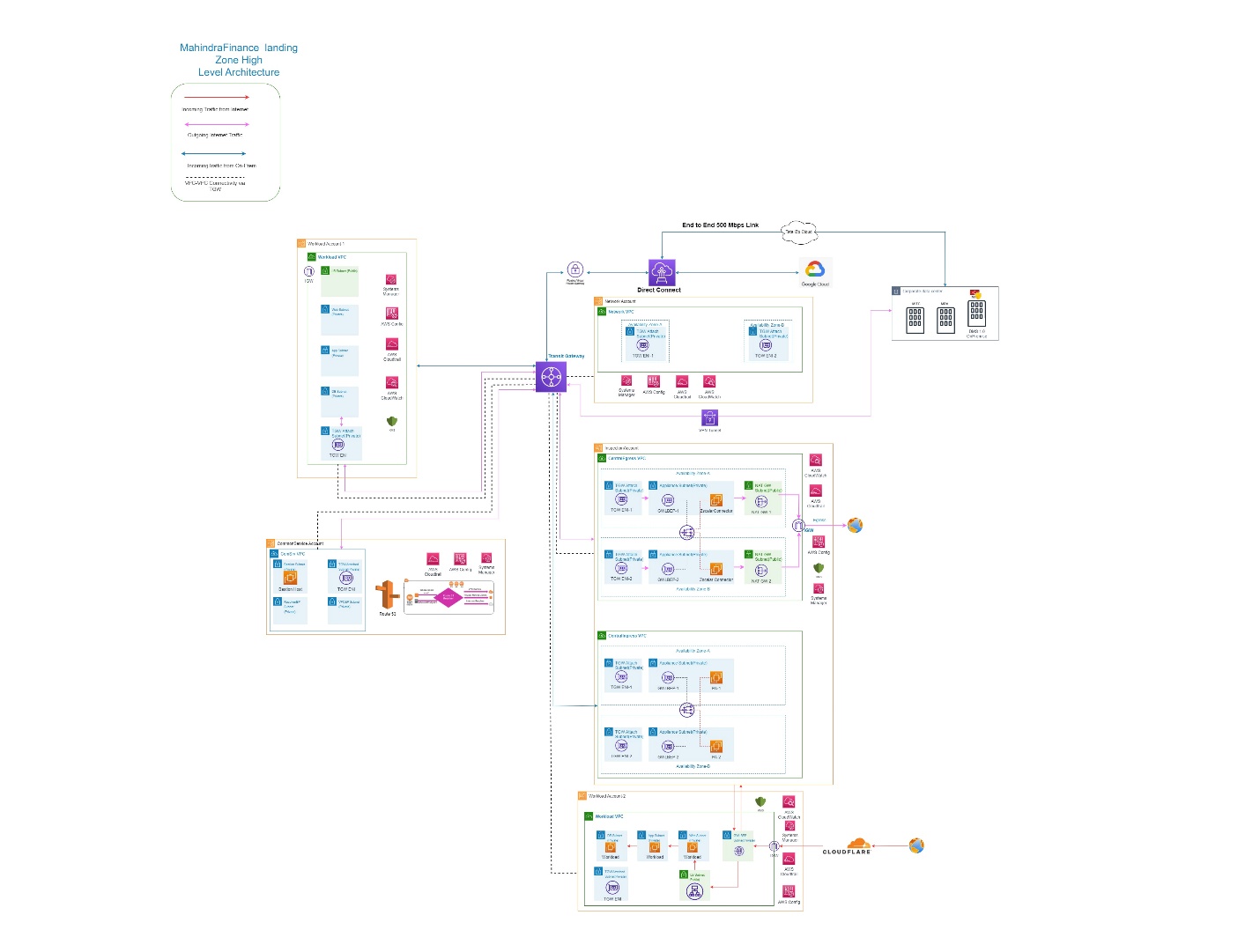
* Resource Isolation through AWS VPC
* Network connectivity (Inter-VPC, On-Premises, Internet, and other clouds)

**Topology**

Proposed AWS Transit Gateway (hub-and-spoke network topology) to build customized secure large-scale networks in AWS with routing and security.

Organization intends to deploy resources across single AWS region.

Reference High Level Network Topology architecture diagram is given below: -



Network Components: -

* Regions – 1 (Asia Pacific-Mumbai)
* VPC--2
* Subnet
* 2 EC2 instances for Zscalar Cloud Connector for internet egress inspection
* Palo-Alto appliances for Internet Ingress and On-Prem to AWS traffic inspection
* AWS Transit Gateway
* AWS Transit Gateway Attachment in each Spoke VPC
* Cloud Flare
* Direct Connect
* VPN
* AWS Direct Connect
* Internet Gateway
* NAT Gateway
* Route Tables
* Security Groups
* Route 53 Resolver
* Gateway Loadbalancer
* Gateway Loadbalancer Endpoints

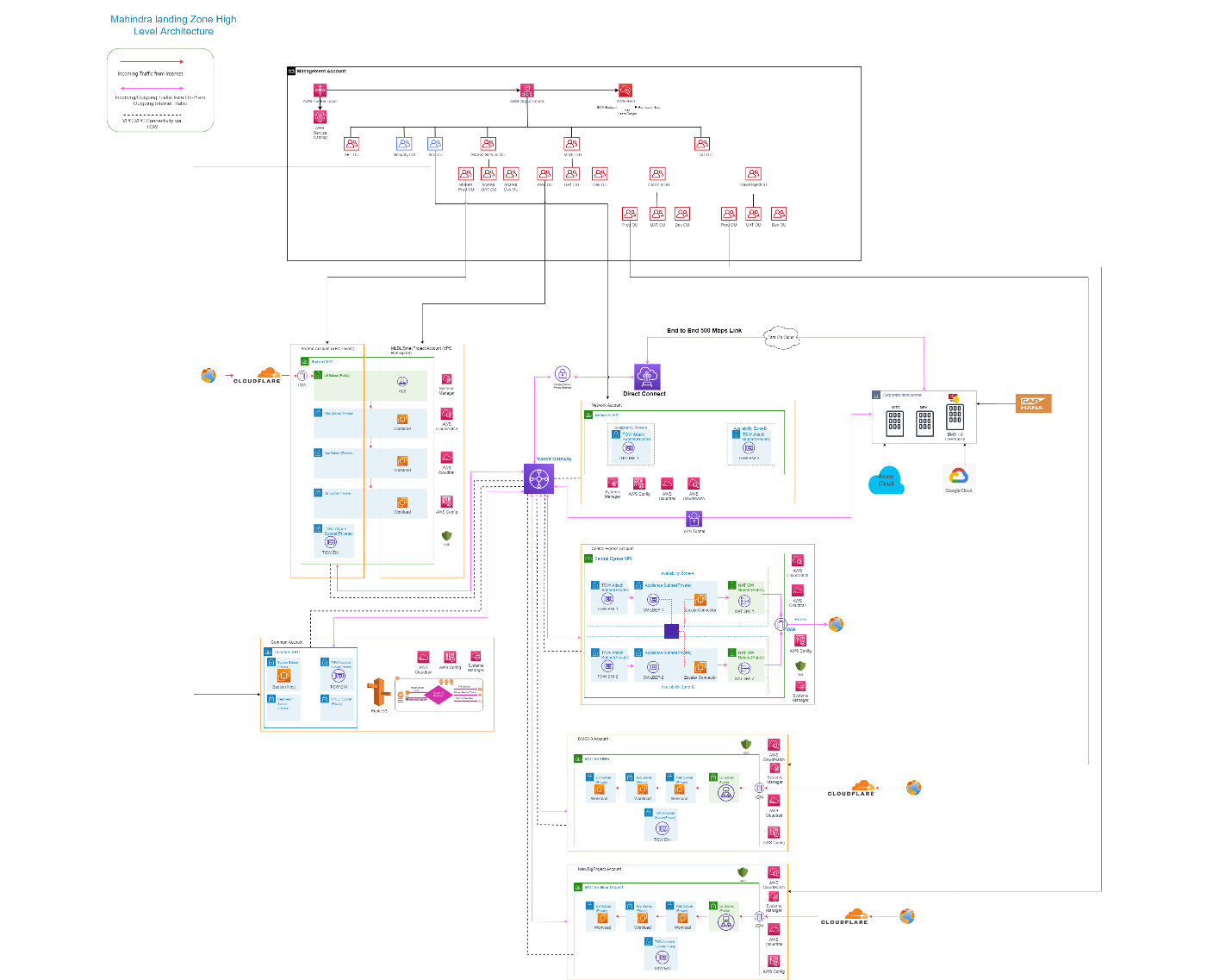
Note:- Below given subnet range is sample subnet range Mahindra Finance can replace the subnet range with approved subnet range.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Account** | **VPC Name** | **Subnet Name** | **AZ** | **CIDR** | **Netmask** | **Subnet Type** |
| **Network** |  |  |  |  |  |  |
|  | vpc-aws-net-mprd-001 |  |  |  |  |  |
|  |  | TGW Attach Subnet | a |  |  | Private |
|  |  | TGW Attach Subnet | b |  |  | Private |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| **Inspection** |  |  |  |  |  |  |
|  | vpc-aws-egr-mprd-001 |  |  |  |  |  |
|  |  | TGW Attach Subnet | a |  |  | Private |
|  |  | TGW Attach Subnet | b |  |  | Private |
|  |  | Firewall Subnet | a |  |  | Private |
|  |  | Firewall Subnet | b |  |  | Private |
|  |  | NAT Gateway Subnet | a |  |  | Public |
|  |  | NAT Gateway Subnet | b |  |  | Public |
|  |  |  |  |  |  |  |
|  | vpc-aws-ing-mprd-001 |  |  |  |  |  |
|  |  | TGW Attach Subnet | a |  |  | Private |
|  |  | TGW Attach Subnet | b |  |  | Private |
|  |  | PA Subnet | a |  |  | Private |
|  |  | PA Subnet | b |  |  | Private |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| **common-service** |  |  |  |  |  |  |
|  | vpc-aws-csr-mprd-001 |  |  |  |  |  |
|  |  | TGW Attach Subnet | a |  |  | Private |
|  |  | TGW Attach Subnet | b |  |  | Private |
|  |  | Bastion Host Subnet | a |  |  | Public |
|  |  | Bastion Host Subnet | b |  |  | Public |
|  |  | Resolver Subnet | a |  |  | Private |
|  |  | Resolver Subnet | b |  |  | Private |
|  |  | VPC Endpoint Subnet | a |  |  | Private |
|  |  | VPC Endpoint Subnet | b |  |  | Private |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| **Shared Prod(VPC Owner)** |  |  |  |  |  |  |
|  | vpc-aws-shrd-mprd-001 |  |  |  |  |  |
|  |  | TGW Attach Subnet | a |  |  | Private |
|  |  | TGW Attach Subnet | b |  |  | Private |
|  |  | ALB Subnet | a |  |  | Public |
|  |  | ALB Subnet | b |  |  | Public |
|  |  | Web | a |  |  | Private |
|  |  | Web | b |  |  | Private |
|  |  | App | a |  |  | Private |
|  |  | App | b |  |  | Private |
|  |  | DB | a |  |  | Private |
|  |  | DB | b |  |  | Private |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| **Shared UAT(VPC Owner)** |  |  |  |  |  |  |
|  | vpc-aws-shrd-muat-001 |  |  |  |  |  |
|  |  | TGW Attach Subnet | a |  |  | Private |
|  |  | TGW Attach Subnet | b |  |  | Private |
|  |  | ALB Subnet | a |  |  | Public |
|  |  | ALB Subnet | b |  |  | Public |
|  |  | Web | a |  |  | Private |
|  |  | Web | b |  |  | Private |
|  |  | App | a |  |  | Private |
|  |  | App | b |  |  | Private |
|  |  | DB | a |  |  | Private |
|  |  | DB | b |  |  | Private |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| **Shared DEV(VPC Owner)** |  |  |  |  |  |  |
|  | vpc-aws-shrd-mdev-001 |  |  |  |  |  |
|  |  | TGW Attach Subnet | a |  |  | Private |
|  |  | TGW Attach Subnet | b |  |  | Private |
|  |  | ALB Subnet | a |  |  | Public |
|  |  | ALB Subnet | b |  |  | Public |
|  |  | Web | a |  |  | Private |
|  |  | Web | b |  |  | Private |
|  |  | App | a |  |  | Private |
|  |  | App | b |  |  | Private |
|  |  | DB | a |  |  | Private |
|  |  | DB | b |  |  | Private |
|  |  |  |  |  |  |  |
| **Shared Pre-Prod(VPC Owner)** | vpc-aws-shrd-mpprd-001 |  |  |  |  |  |
|  |  | TGW Attach Subnet | a |  |  | Private |
|  |  | TGW Attach Subnet | b |  |  | Private |
|  |  | ALB Subnet | a |  |  | Public |
|  |  | ALB Subnet | b |  |  | Public |
|  |  | Web | a |  |  | Private |
|  |  | Web | b |  |  | Private |
|  |  | App | a |  |  | Private |
|  |  | App | b |  |  | Private |
|  |  | DB | a |  |  | Private |
|  |  | DB | b |  |  | Private |

### 8.2 Connectivity: -

This section expands on the network topology to consider recommended models for connecting on-premises locations to AWS.

**Please refer below diagram for Network connectivity.**



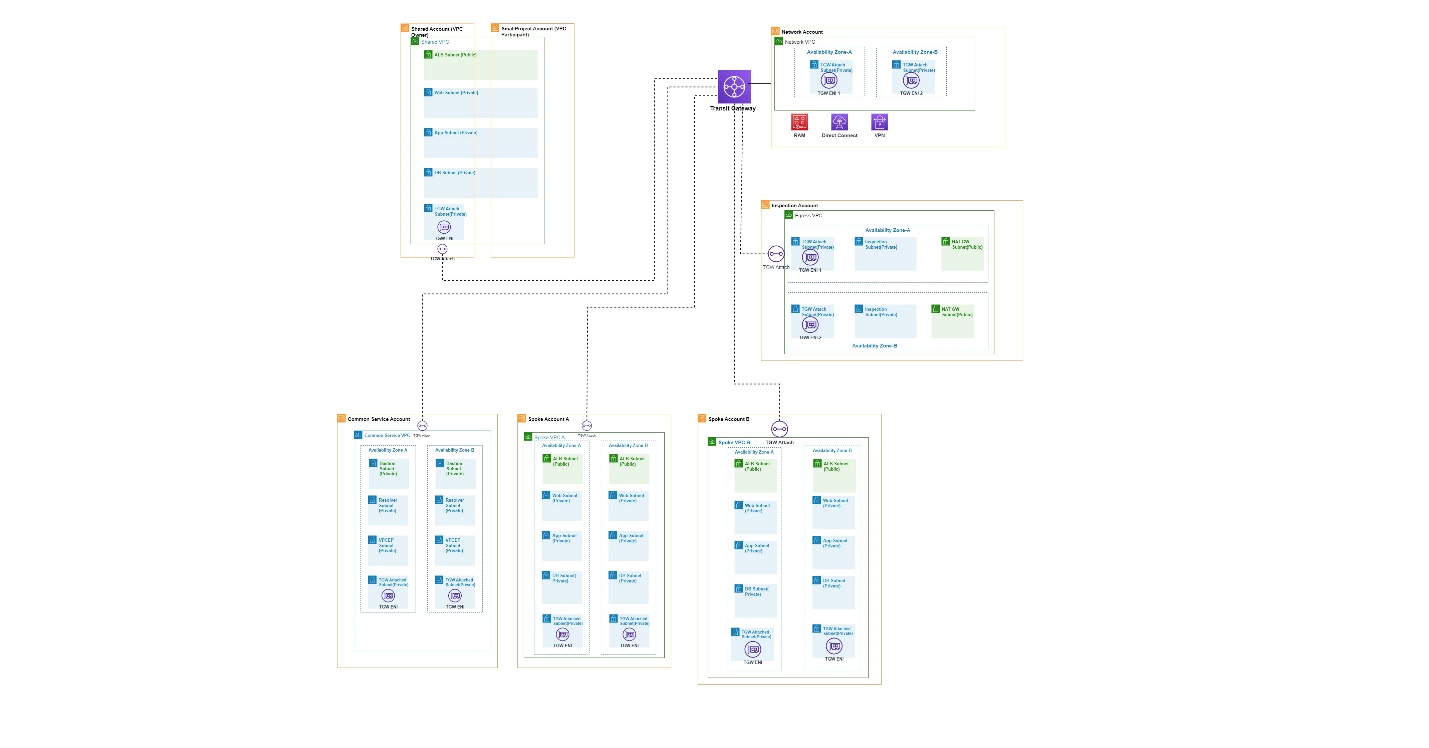
**AWS VPC connectivity via Transit gateway: -**

AWS Transit Gateway provides a hub and spoke design for connecting VPCs and on-premises networks as a fully managed service without requiring you to provision virtual appliances like the Cisco CSRs. No VPN overlay is required, and AWS manages high availability and scalability.

Transit Gateway enables customers to connect thousands of VPCs. You can attach all your hybrid connectivity (VPN and Direct Connect connections) to a single Transit Gateway instance, consolidating and controlling your organization's entire AWS routing configuration in one place. Transit Gateway controls how traffic is routed among all the connected spoke networks using route tables. This hub-and-spoke model simplifies management and reduces operational costs because VPCs only connect to the Transit Gateway instance to gain access to the connected networks.

* VPC to VPC in same region is connected by configuring AWS Transit Gateway in Network Account and use AWS Resource Access Manager (RAM) to share a Transit Gateway for connecting VPCs across multiple accounts in your AWS Organization within the same Region. AWS RAM enables you to easily and securely share AWS resources with any AWS account, or within your AWS Organization.

Below is reference diagram for VPC-to-VPC connectivity: -



* Subnet to subnet within the same VPC can communicate with each other by default. Communication should be made via the private IP address of the resources, to ensure that traffic stays within the VPC. AWS Internal traffic at vm level is control by the Security Group.
* VPC to on-premises are connected by AWS Direct Connect by using Tata MPLS cloud or by AWS VPN to data center.
* VPC to other cloud virtual networks are connected by AWS Direct Connect by using Tata MPLS cloud or by AWS VPN to data center.

**Connectivity to On-premises and other cloud providers: -**

* AWS Direct Connect helps in establishing a private, logical connection from your on-premises network and other cloud providers to AWS infrastructure. This connection lets computers on your on-premises network to directly access virtual machines in AWS and vice versa.
* AWS Direct Connect enables you to securely connect your AWS environment to your on-premises data center or other cloud location. AWS Direct Connect offers dedicated high speed, low latency connection, which bypasses internet service providers in your network path.
* One can also enable access to their remote network from AWS VPC by creating an AWS Site-to-Site VPN (Site-to-Site VPN) connection, and configuring routing to pass traffic through the connection.

A VPN connection refers to the connection between your VPC and your own on-premises network. Site-to-Site VPN supports Internet Protocol security (IPsec) VPN connections. VPN connection will be terminating on Transit Gateway (TGW) as we are using Transit Gateway for VPC to VPC communication.

**Subnetting :- Please go through subnetting details**

**Zscalar Cloud Connector: -**

Enabled by the Zero Trust Exchange, Workload Communications is deployed as Cloud Connector virtual machines and extends the capabilities of Zscaler Internet Access (ZIA).

**North-South Traffic flow: -**

Workload VPC’s

The workload VPC’s called the spoke VPC’s here will be connected to the transit gateway via VPC attachment.

Spoke VPC could have the following subnets based on the needs.

1. Public Subnet – Host Application Load Balancer.

2. Private Subnet – Host workloads need to be published over the Internet.

3. GWLB endpoint subnet – Subnet to host the GWLB endpoint.

4. TGW subnet – Subnet for TGW attachment.

The spoke VPC would have an IGW to allow inbound traffic to workloads published on the Internet or to allow inbound traffic to application load balancer used for receiving inbound traffic for private workloads.

The default route for

1. Public subnet would be GWLBe i.e. all outbound traffic from the public subnet would be handled by

GWLBe.

**For inbound Internet traffic**,

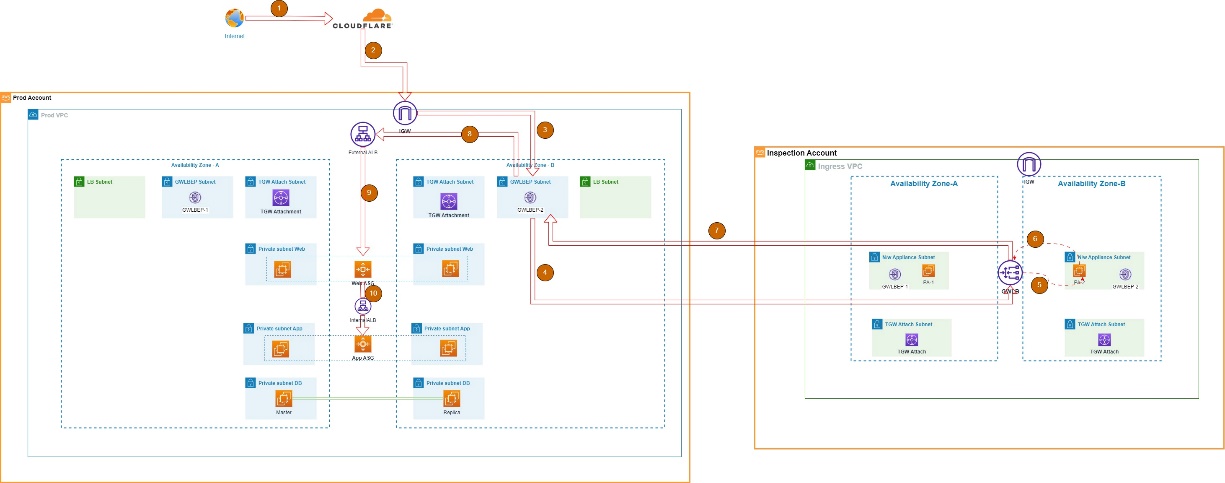
The workloads that have inbound traffic could either be directly in the public subnet of the spoke VPC which could

have a elastic IP assigned to it or it could be via a load balancer to the workloads in the private subnet. For cases where the Traffic is destined to the workloads in the public subnet of the spoke VPC, the below summarises the traffic flow

Internet >> IGW (Spoke VPC) >> GWLBe (Spoke VPC) >> GWLB >> Fortigate Virtual Firewalls >> GWLB >> GWLBe(Spoke VPC) >> Work load (Public Subnet of Spoke VPC) >> GWLBe (Spoke VPC) >> GWLB >> Fortigate Virtual Firewalls >> GWLB >> GWLBe (Spoke VPC) >> IGW (Spoke VPC) >> Internet

In case the traffic is sent to a Application load balancer the below summarises the traffic flow

Internet >> IGW (Spoke VPC) >> GWLBe (Spoke VPC) >> GWLB >> Fortigate Virtual Firewalls >> GWLB >> GWLBe(Spoke VPC) >> ALB >> Work load (Spoke VPC) >> ALB >> GWLBe >> GWLB >> Fortigate Virtual Firewalls >> GWLB>> GWLBe (Spoke VPC) >> IGW (Spoke VPC) >> Internet



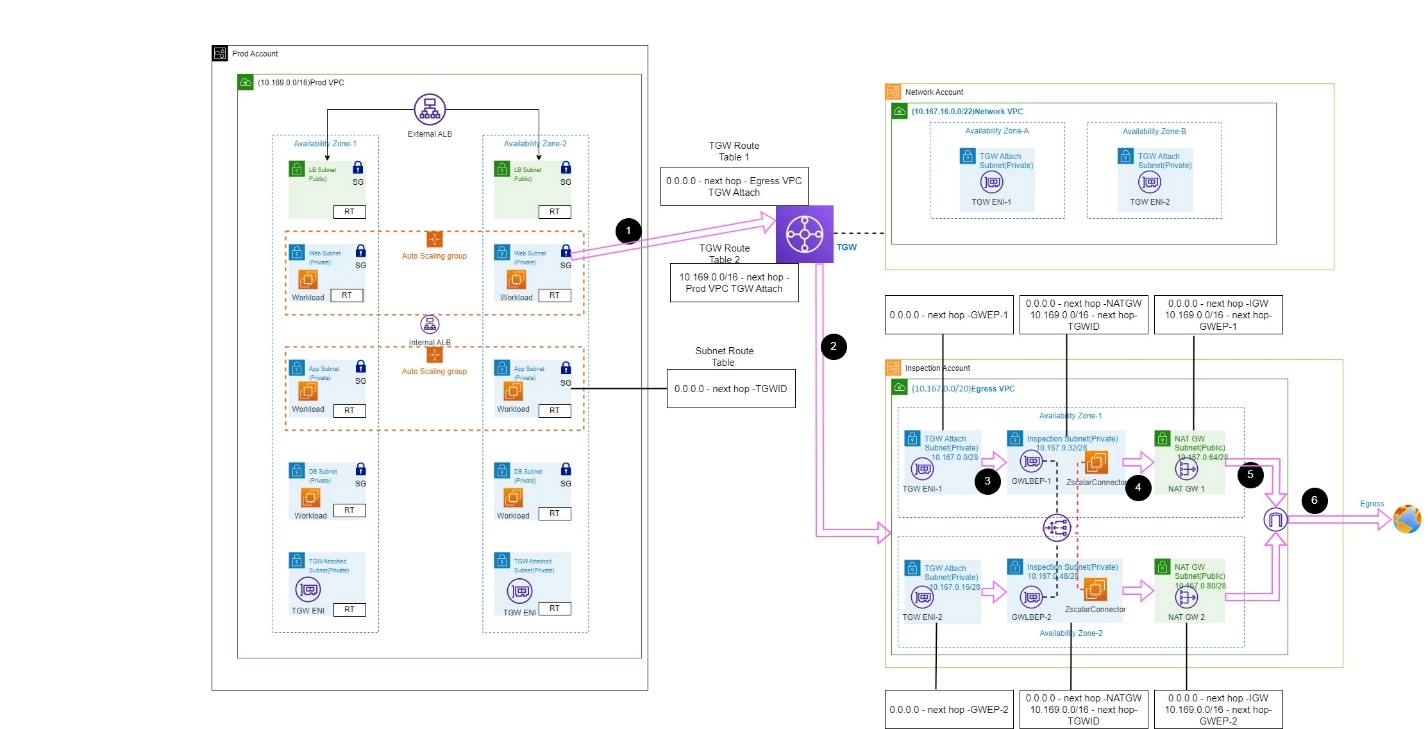
**For outbound Internet Traffic**, User-defined routes on the private subnets in the spoke VPCs direct traffic to the Egress VPC via transit gateway, which shares a subnet with the Zscalar cloud connector instances in firewall subnet.

Spoke VPC attachments are associated with first Transit Gateway Route Table and are propagated to second Transit Gateway Route Table.

Continue to use a default route in first Transit Gateway Route Table pointing all traﬃc to Egress VPC. Transit Gateway will forward all traffic flows to one of the two availability zones in the Egress VPC. Once traffic reaches one of Transit Gateway ENIs in the Egress VPC, you hit a default route which will forward traffic to one of the Zscalar cloud connector instances in their respective availability zone. Zscalar cloud connector instances will then inspect traffic based on the rules you set before forwarding traffic to the NAT gateway using a default route.

Once traffic reaches the NAT gateway, you hit default route which will forward traffic to Internet via Internet Gateway.

Please refer below diagram for Outbound Internet traffic flow.



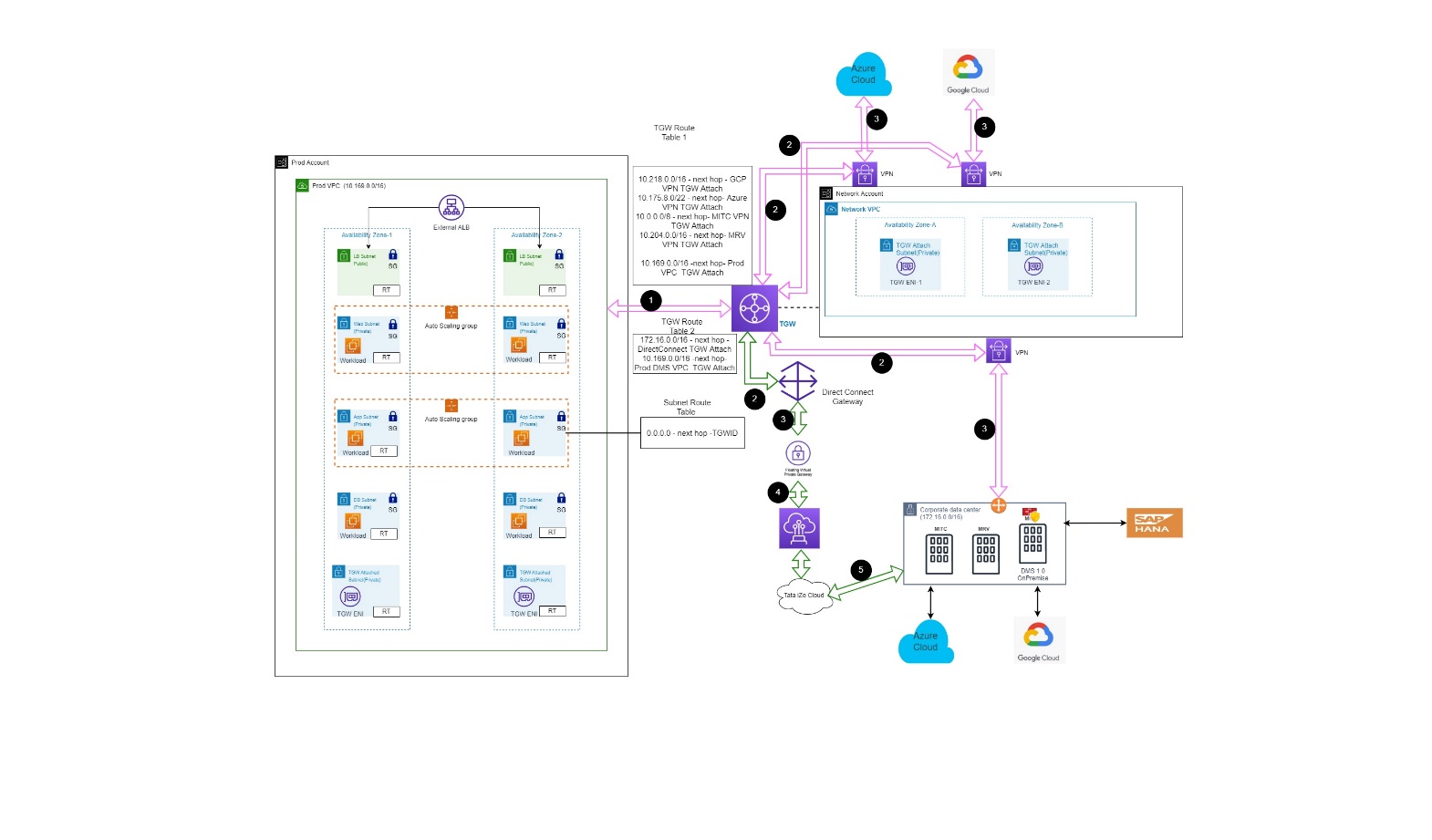
**EAST-WEST traffic**

**Inbound/Outbound Network Traffic to On-Premises and Other Clouds (GCP and Azure)**

When AWS spoke VPC initiate the traffic to reach On-premises/Other Clouds resources that network request reach at first hop that is Spoke VPC attachment in Transit Gateway.

Transit Gateway Route Table decide and routes the request to Direct Connect Gateway attachment or VPN Attachment, which further routes the Network traffic towards the On-Premises.

Please refer below diagram for Inbound/Outbound Network Traffic to On-Premises and Other Clouds



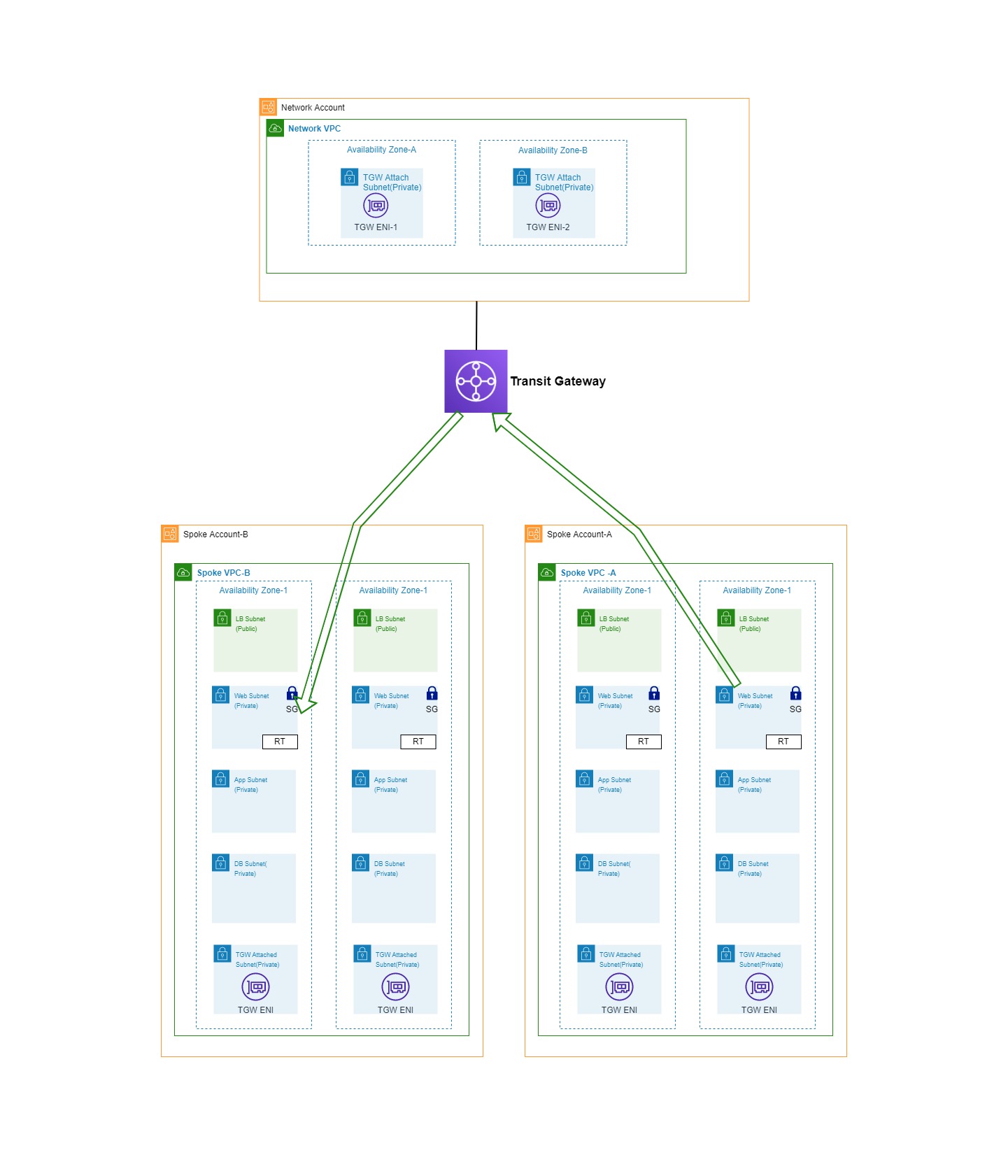
**VPC-to-VPC traffic flow in same region: -**

All spoke VPCs such as Prod VPC, UAT VPC, Dev VPC will communicate with required VPCs via Transit Gateway only.

All spoke VPCs connected to Network/Ingress/Egress/Common VPCs by AWS Transit Gateway by following HUB & spoke network model.

Security Group(SG) will be applied to control the security of network communication between VPCs in the same region.

Routing and SG will be defined in such way that there will be no communication to each other VPCs of Prod, Dev and UAT environments.



Application communication: -

We are inspecting the Application communication over the Internet using Palo-Alto firewall devices as part of this current project scope.

**Internet to Application communication: -**

Users from Internet access the Mahindra Finance Applications or APIs which are hosted on private networks via Cloud Flare.

Users access the Mahidra.com website or API then request first reach at Cloudflare by resolving public DNS IP and then forward to Public Application Load balancer in Public subnet.

Then request gets forward to respective Application server and get the response back to the User through same path.

Please refer **For inbound Internet traffic Network diagram.**

### 8.3 Network Security

Enabled by the Zero Trust Exchange, Workload Communications is deployed as Cloud Connector virtual machines and extends the capabilities of Zscaler Internet Access (ZIA) to cloud native workloads.

Key Features and Benefits

* Security - Secures all inbound and outbound traffic to the internet. The security capabilities that are available through the Zscaler Internet Access platform for server internet access are Secure Sockets Layer (SSL), Intrusion Prevention System (IPS), Firewall, Data Loss Prevention (DLP), etc.
* Connectivity - Provides seamless connectivity from Private/Public cloud applications to the internet.
* Performance - Ensures better end-user experience and application performance by peering relationships with SaaS providers (e.g., Microsoft Office 365, Amazon Web Services, and Microsoft Azure).
* Reduces Cost - Consolidates multiple products (e.g., Squid proxies, firewalls, 3rd party NAT appliances, URL filtering, etc.) into a single solution. Additionally, the same policy applied to user traffic can be applied across the cloud infrastructure.
* Highly Scalable - Ease of implementation across 1K service accounts in public clouds and single solution scales to connect 10K+ server environments in public clouds (e.g., AWS, Azure, etc.).
* Ease of Deployment - Fully orchestrated deployment for AWS using Terraform, and CloudFormation templates.
* Real-Time Visibility - Dashboards and Insights provide unparalleled visibility into your users and applications, and the health of your organization's applications and servers.

Oftentimes, in the realm of networking, we find ourselves asking how we can secure traffic to the cloud. Rarely do we evaluate how traffic is secured within the cloud, as it leaves the cloud, or while in transit between clouds. This attack surface is growing as more and more workloads are being migrated and customers begin operating across multiple cloud service providers. Zscaler Workload Communications can help enable the following use-cases:

**Applications to Internet Communications:** Applications may need to access any Internet or SaaS destination, such as 3rd party APIs, software updates, etc. with a scalable, reliable security solution that inspects all transactions, applying advanced threat prevention and data loss protection controls.

**Application to Application Communication** to other public clouds and corporate data centers for multi/hybrid cloud connectivity, delivered with better security and a dramatically simplified operational model as compared with traditional solutions like proxies, virtual firewalls and IDS/IPS.

**Application to Application Communications within a VPC** by securing process-to-process communications to achieve micro segmentation with no changes to the application or the network.

The solution works by leveraging Cloud Connector and the ZPA App Connector. App Connector is a light-weight VM that gets installed adjacent to on-premise workloads as well as cloud workloads. You can read more about App Connector here. When a cloud workload requests access to another workload, Cloud Connector uses geo-location technology to locate the ZPA Public Service Edge or ZPA Private Service Edge closest to them. Cloud Connector then establishes a secure DTLS tunnel. The Service Edge then retrieves the cloud location’s security policies from the Central Authority, and (depending on the policy result) the Service Edge contacts the appropriate App Connector at the far end (be it in the cloud, or on-premise). After an authentication process, App Connector then builds a DTLS tunnel to the Service Edge. Once the connection is established between the Cloud Connector and the App Connector, the workload can begin sending data over a dedicated tunnel. It is important to note that the workload devices at each end of this connection are communicating with synthetic (proxy) IP addresses hosted on the Cloud Connector and App Connector. Hence, neither end is aware of the “real” IP Addresses involved in the exchange, nor is either network segment directly connected to the other.

There will be 2 Zscalar Cloud Connectors deployed behind Gateway Loadbalancer hosted at Inspection VPC in two different private subnets for outbound internet traffic.

**Cloudflare for WAF** to be used for DDOS protection of all applications which are exposed over the Internet.

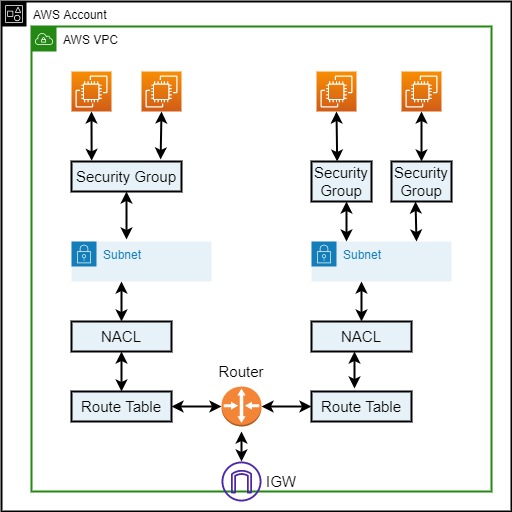
**Security Group (SG)**

A security group controls the traffic that is allowed to reach and leave the resources that it is associated with. For example, after you associate a security group with an EC2 instance, it controls the inbound and outbound traffic for the instance.

A *security group* controls the traffic that is allowed to reach and leave the resources that it is associated with. For example, after you associate a security group with an EC2 instance, it controls the inbound and outbound traffic for the instance.

When you create a VPC, it comes with a default security group. You can create additional security groups for each VPC. You can associate a security group only with resources in the VPC for which it is created.

For each security group, you add *rules* that control the traffic based on protocols and port numbers. There are separate sets of rules for inbound traffic and outbound traffic.



**Route Table(RT)**

A route table contains a set of rules, called routes, that determine where network traffic from your subnet or gateway is directed. Your VPC has an implicit router, and you use route tables to control where network traffic is directed. Each subnet in your VPC must be associated with a route table, which controls the routing for the subnet (subnet route table). You can explicitly associate a subnet with a particular route table. Otherwise, the subnet is implicitly associated with the main route table. A subnet can only be associated with one route table at a time, but you can associate multiple subnets with the same subnet route table.

The following are the key concepts for route tables.

* Main route table—The route table that automatically comes with your VPC. It controls the routing for all subnets that are not explicitly associated with any other route table.
* Custom route table—A route table that you create for your VPC.
* Destination—The range of IP addresses where you want traffic to go (destination CIDR). For example, an external corporate network with the CIDR 172.16.0.0/12.
* Target—The gateway, network interface, or connection through which to send the destination traffic; for example, an internet gateway.
* Route table association—The association between a route table and a subnet, internet gateway, or virtual private gateway.
* Subnet route table—A route table that's associated with a subnet.
* Local route—A default route for communication within the VPC.

**AWS Key Management Service**

AWS Key Management Service (AWS KMS) lets you create, manage, and control cryptographic keys across your applications and more than 100 AWS services. AWS KMS integrates with AWS services to encrypt data at rest using an AWS KMS key.

Types of KMS keys available in AWS:

1. Customer managed keys: The KMS keys that you create are customer managed keys. Customer managed keys are KMS keys in your AWS account that you create, own, and manage. You have full control over these KMS keys, including establishing and maintaining their key policies, IAM policies, and grants, enabling and disabling them, rotating their cryptographic material, adding tags, creating aliases that refer to the KMS keys, and scheduling the KMS keys for deletion.

2. AWS managed keys: AWS managed keys are KMS keys in your account that are created, managed, and used on your behalf by an AWS service integrated with AWS KMS.

Some AWS services let you choose an AWS managed key or a customer managed key to protect your resources in that service. In general, unless you are required to control the encryption key that protects your resources, an AWS managed key is a good choice. You don't have to create or maintain the key or its key policy, and there's never a monthly fee for an AWS managed key.

The KMS keys that you create are customer managed keys. AWS services that use KMS keys to encrypt your service resources often create keys for you. KMS keys that AWS services create in your AWS account are AWS managed keys. KMS keys that AWS services create in a service account are AWS owned keys.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Type of KMS key** | **Can view KMS key metadata** | **Can manage KMS key** | **Used only for my AWS account** | **Automatic rotation** | **Pricing** |
| Customer managed key | Yes | Yes | Yes | Optional. Every year (approximately 365 days) | Monthly fee (pro-rated hourly) |
|  |
| Per-use fee |
| AWS managed key | Yes | No | Yes | Required. Every year (approximately 365 days) | No monthly fee |
|  |
| Per-use fee (some AWS services pay this fee for you) |
| AWS owned key | No | No | No | Varies | No fees |

AWS services integrated with AWS KMS

|  |  |  |  |
| --- | --- | --- | --- |
| Alexa for Business[1] | Amazon Forecast | Amazon Nimble Studio | AWS CloudHSM[2] |
| Amazon AppFlow | Amazon Fraud Detector | Amazon Personalize | AWS CloudTrail |
| Amazon Athena | Amazon FSx | Amazon QLDB | AWS CodeArtifact |
| Amazon Aurora | Amazon GuardDuty | Amazon Redshift | AWS CodeBuild |
| Amazon CloudWatch Logs | Amazon HealthLake | Amazon Rekognition | AWS CodeCommit[1] |
| Amazon CloudWatch Synthetics | Amazon Inspector | Amazon Relational Database Service (RDS) | AWS CodePipeline |
| Amazon CodeGuru | Amazon Kendra | Amazon Route 53 | AWS Control Tower |
| Amazon Comprehend | Amazon Keyspaces (for Apache Cassandra) | Amazon S3 | AWS Database Migration Service |
| Amazon Connect | Amazon Kinesis Data Streams | Amazon SageMaker | AWS Elastic Disaster Recovery |
| Amazon Connect Customer Profiles | Amazon Kinesis Firehose | Amazon Simple Email Service (SES) | AWS Elemental MediaTailor |
| Amazon Connect Voice ID | Amazon Kinesis Video Streams | Amazon Simple Notification Service (SNS) | AWS Glue |
| Amazon Connect Wisdom | Amazon Lex | Amazon Simple Queue Service (SQS) | AWS Glue DataBrew |
| Amazon DocumentDB | Amazon Lightsail[1] | Amazon Textract | AWS IoT SiteWise |
| Amazon DynamoDB | Amazon Location Service | Amazon Timestream | AWS Lambda |
| Amazon DynamoDB Accelerator (DAX)[1] | Amazon Lookout for Equipment | Amazon Transcribe | AWS License Manager |
| Amazon EBS | Amazon Lookout for Metrics | Amazon Translate | AWS Network Firewall |
| Amazon EC2 Image Builder | Amazon Lookout for Vision | Amazon WorkMail | AWS Proton |
| Amazon EFS | Amazon Macie | Amazon WorkSpaces | AWS Secrets Manager |
| Amazon Elastic Container Registry (ECR) | Amazon Managed Blockchain | Amazon WorkSpaces Web | AWS Snowball |
| Amazon Elastic Kubernetes Service (EKS) | Amazon Managed Service for Prometheus | AWS Audit Manager | AWS Snowball Edge |
| Amazon Elastic Transcoder | Amazon Managed Streaming for Kafka (MSK) | AWS Application Cost Profiler | AWS Snowcone |
| Amazon ElastiCache | Amazon Managed Workflows for Apache Airflow (MWAA) | AWS Application Migration Service | AWS Snowmobile |
| Amazon OpenSearch | Amazon MemoryDB | AWS App Runner | AWS Storage Gateway |
| Amazon EMR | Amazon Monitron | AWS Backup | AWS Systems Manager |
| Amazon EMR Serverless | Amazon MQ | AWS Certificate Manager[1] | AWS X-Ray |
| Amazon FinSpace | Amazon Neptune | AWS Cloud9[1] |  |

[1] Supports only AWS managed keys.

[2] AWS KMS supports custom key stores backed by an AWS CloudHSM cluster.

[3] For a list of services integrated with AWS KMS in the AWS China (Beijing) Region, operated by Sinnet and the AWS China (Ningxia) Region, operated by NWCD, please visit AWS KMS Service integration in China.

AWS services not listed above encrypt customer data using keys owned and managed by the respective service.

**AWS Private Link**

AWS PrivateLink provides private connectivity between virtual private clouds (VPCs), supported AWS services, and your on-premises networks without exposing your traffic to the public internet. Interface VPC endpoints, powered by PrivateLink, connect you to services hosted by AWS Partners and supported solutions available in AWS Marketplace.

**AWS GuardDuty**

Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts, Amazon Elastic Compute Cloud (EC2) workloads, container applications, Amazon Relational Database Service Aurora databases (Preview), and data stored in Amazon Simple Storage Service (S3). GuardDuty combines machine learning, anomaly detection, network monitoring, and malicious file dis-covery, utilizing both AWS-developed and industry-leading third-party sources to help protect workloads and data on AWS. GuardDuty is capable of analyzing tens of billions of events across multiple AWS data sources, such as AWS CloudTrail event logs, Amazon Virtual Private Cloud (VPC) Flow Logs, Amazon Elastic Kubernetes Service (EKS) audit logs, and DNS query logs.

Amazon GuardDuty identifies unusual activity within your accounts, analyzes the security relevance of the activity, and gives the context in which it was invoked. This allows a responder to determine if they should spend time on further investigation. GuardDuty findings are assigned a severity, and actions can be automated by integrating with [AWS Security Hub,](https://aws.amazon.com/security-hub/) [Amazon EventBridge](https://aws.amazon.com/eventbridge/), [AWS Lambda](https://aws.amazon.com/lambda/), and [AWS Step Functions](https://aws.amazon.com/step-functions/). [Amazon Detective](https://aws.amazon.com/detective/) is also tightly integrated with GuardDuty, so you can perform deeper forensic and root cause investigation.

### 8.4 Connectivity to AWS Services

AWS PrivateLink provides private connectivity between virtual private clouds (VPCs), supported AWS services, and your on-premises networks without exposing your traffic to the public internet. Interface VPC endpoints, powered by PrivateLink, connect you to services hosted by AWS Partners and supported solutions available in AWS Marketplace.

Key Benefits of Private Link: -

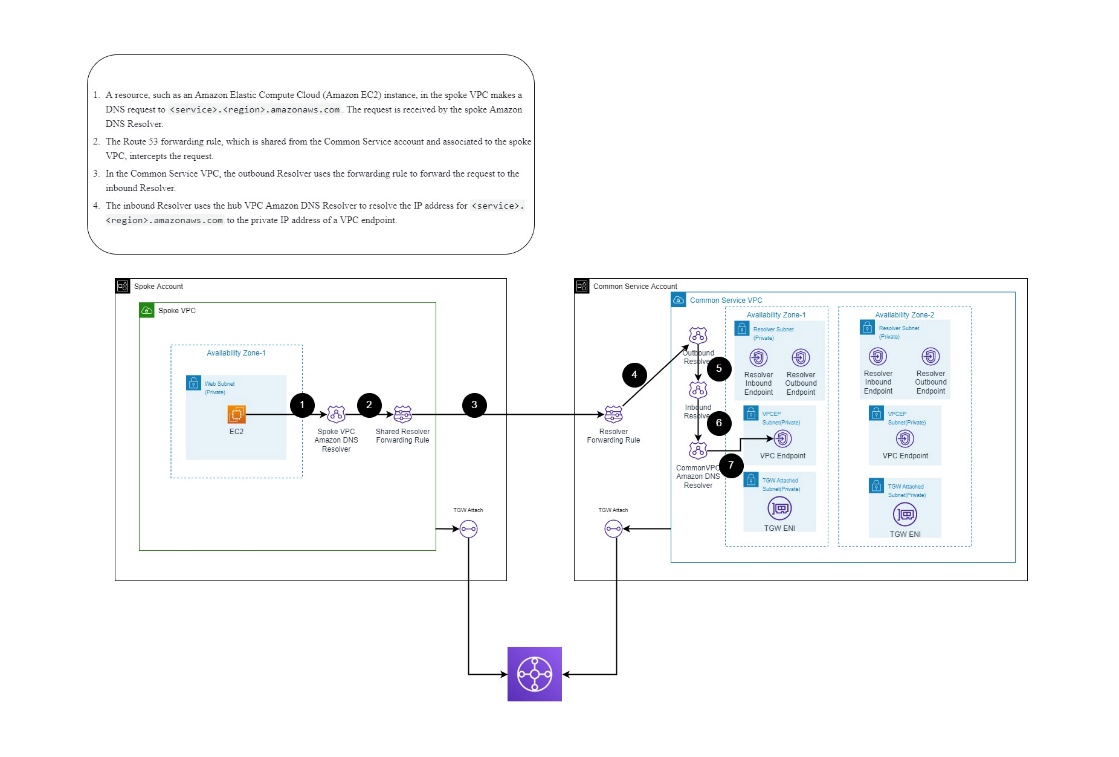
* **Accessing services over AWS PrivateLink**: To use AWS PrivateLink, create an interface VPC endpoint for a service outside of your VPC. This creates an elastic network interface in your subnet with a private IP address that serves as an entry point for traffic destined to the service.
* **Privately connecting to your on-premises applications**: Interface VPC endpoints support private connectivity over AWS Direct Connect, so that applications in your premises will be able to connect to these services via the Amazon private network.
* **Regulatory compliance**: Preventing your sensitive data, such as customer records, from traversing the internet helps you maintain compliance with regulations such as HIPAA, EU-US Privacy Shield, and payment card industry (PCI).
* **Sharing your services over AWS PrivateLink**: You can create your own AWS PrivateLink-powered service (endpoint service) and enable other AWS customers to access your service.

The following AWS services integrate with AWS PrivateLink. You can create a VPC endpoint to connect to these services privately, as if they were running in your own VPC: -

* Access Analyzer
* AWS Account Management
* Amazon API Gateway
* AWS App Mesh
* AWS App Runner
* AWS App Runner services
* Application Auto Scaling
* AWS Application Migration Service
* Amazon AppStream 2.0
* Amazon Athena
* AWS Audit Manager
* Amazon Aurora
* AWS Auto Scaling
* AWS Backup
* AWS Batch
* AWS Billing Conductor
* Amazon Braket
* AWS Private Certificate Authority
* AWS Cloud Control API
* Amazon Cloud Directory
* AWS CloudFormation
* AWS CloudHSM
* AWS CloudTrail
* Amazon CloudWatch
* Amazon CloudWatch Events
* Amazon CloudWatch Logs
* AWS CodeArtifact
* AWS CodeBuild
* AWS CodeCommit
* AWS CodeDeploy
* Amazon CodeGuru Profiler
* Amazon CodeGuru Reviewer
* AWS CodePipeline
* AWS CodeStar Connections
* Amazon Comprehend
* Amazon Comprehend Medical
* AWS Config
* Amazon Connect
* AWS Data Exchange
* AWS Database Migration Service
* AWS DataSync
* Amazon DevOps Guru
* Amazon EBS direct APIs
* Amazon EC2
* Amazon EC2 Auto Scaling
* EC2 Image Builder
* Amazon ECR
* Amazon ECS
* AWS Elastic Beanstalk
* AWS Elastic Disaster Recovery
* Amazon Elastic File System
* Amazon Elastic Inference
* Elastic Load Balancing
* Amazon ElastiCache
* Amazon EMR
* Amazon EMR on EKS
* Amazon EMR Serverless
* Amazon EventBridge
* AWS Fault Injection Simulator
* Amazon FinSpace
* Amazon Forecast
* Amazon Fraud Detector
* Amazon FSx
* AWS Glue
* AWS Glue DataBrew
* Amazon Managed Grafana
* AWS Ground Station
* Amazon HealthLake
* IAM Identity Center
* IAM Roles Anywhere
* Amazon Inspector
* AWS IoT Core
* AWS IoT Core for LoRaWAN
* AWS IoT Greengrass
* AWS IoT RoboRunner
* AWS IoT SiteWise
* AWS IoT TwinMaker
* Amazon Kendra
* AWS Key Management Service
* Amazon Keyspaces (for Apache Cassandra)
* Amazon Kinesis Data Firehose
* Amazon Kinesis Data Streams
* AWS Lake Formation
* AWS Lambda
* Amazon Lex
* AWS License Manager
* Amazon Lookout for Equipment
* Amazon Lookout for Metrics
* Amazon Lookout for Vision
* Amazon Macie
* AWS Mainframe Modernization
* Amazon Managed Service for Prometheus
* Amazon Managed Workflows for Apache Airflow
* Amazon MemoryDB for Redis
* AWS Migration Hub Orchestrator
* AWS Migration Hub Refactor Spaces
* Migration Hub Strategy Recommendations
* Amazon Nimble Studio
* AWS Panorama
* Amazon Pinpoint
* Amazon Polly
* AWS Private 5G
* AWS Proton
* Amazon QLDB
* Amazon RDS
* Amazon RDS Data API
* Amazon Redshift
* Amazon Redshift Data API
* Amazon Rekognition
* AWS RoboMaker
* Amazon S3
* Amazon S3 Multi-Region Access Points
* Amazon S3 on Outposts
* Amazon SageMaker
* AWS Secrets Manager
* AWS Security Hub
* AWS Security Token Service
* AWS Server Migration Service
* AWS Service Catalog
* Amazon SES
* AWS Snow Device Management
* Amazon SNS
* Amazon SQS
* AWS Step Functions
* AWS Storage Gateway
* AWS Systems Manager
* Amazon Textract
* Amazon Transcribe
* Amazon Transcribe Medical
* AWS Transfer for SFTP
* Amazon Translate
* Amazon WorkSpaces
* AWS X-Ray

**Reference:** https://docs.aws.amazon.com/vpc/latest/privatelink/aws-services-privatelink-support.html

Reference diagram to access AWS services by private Link:-



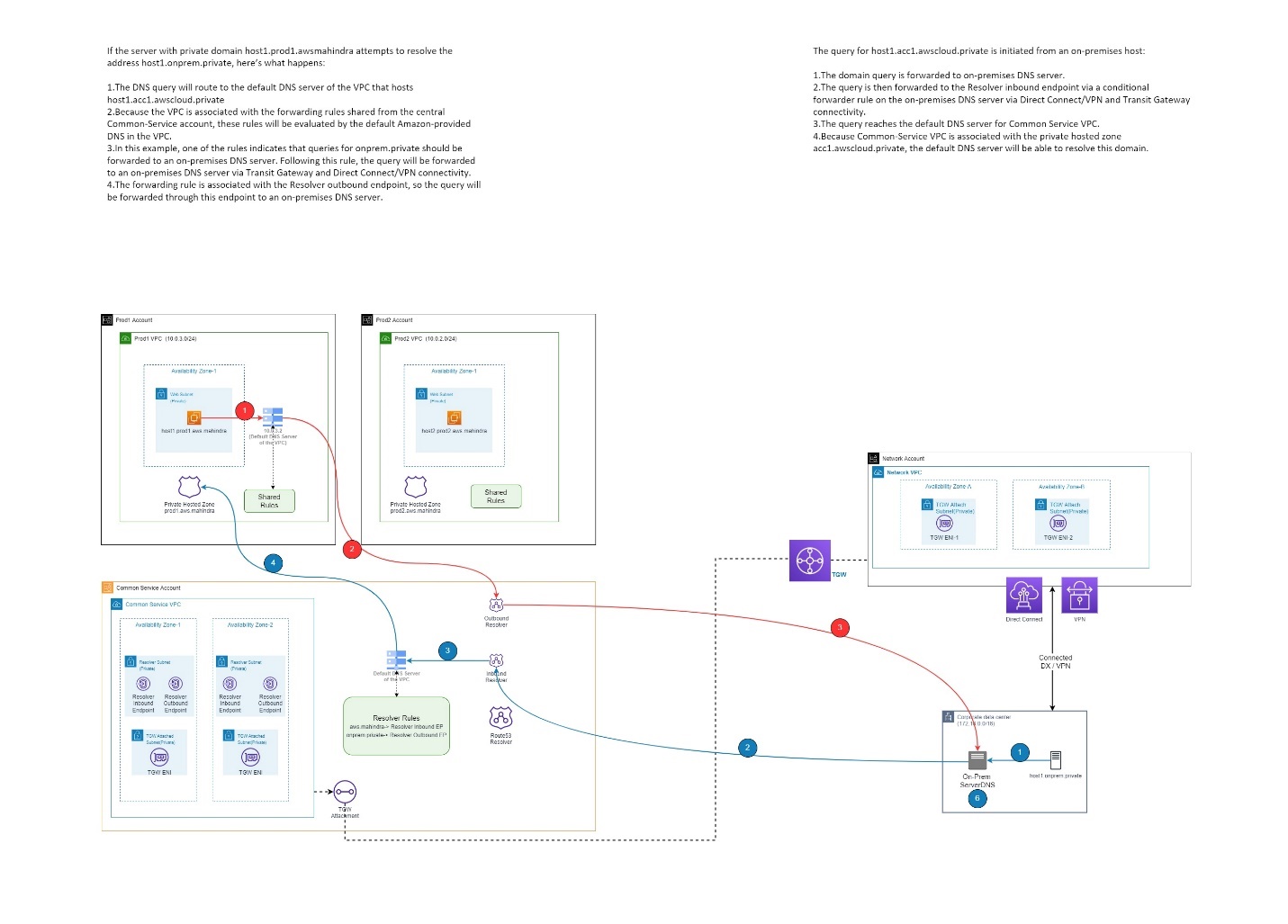
AWS PrivateLink Quotas

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Default** | **Adjustable** | **Comments** |
| Interface and Gateway Load Balancer endpoints per VPC | 50 | Yes | This is a combined quota for interface endpoints and Gateway Load Balancer endpoints |
| Gateway VPC endpoints per Region | 20 | Yes | You can create up to 255 gateway endpoints per VPC |
| VPC endpoint policy size | 20,480 characters | No | The size of a VPC endpoint policy includes white spaces |

### 8.5 Private DNS for on-premises and AWS resources

Name resolution across AWS and on-premises by using Route 53 Resolver. This allows you to resolve domains across multiple accounts and between workloads running on AWS and on-premises without the need to run a domain controller in AWS.

Reference diagram to for Internal Domain resolution:-



### 8.6 Public DNS for AWS resources: -

Use Cloudflare to make public dns entries to resolve the application load balancer dns by public IP over the Internet

8.7 DNS resolution priority from AWS VPC: -

Whenever a DNS lookup is initiated from within AWS VPC, queries are directed towards the Route 53 Resolver service to handle the resolution, which has the VPC CIDR address +2. This resolver provides DNS query capability in your VPC that resolves public domain names and private hosted zones (PHZ).

When a DNS query is issued, the following resolution process is followed:

1. First, the Route 53 Resolver checks Private Hosted Zone (PHZ) associations and determines if the query is destined for private DNS.
2. Then, Route 53 Resolver checks if the query is destined for AWS internal domain names that cover AWS resources, such as EC2 instance names, VPC endpoints, and others.
3. If none of the preceding are matched and no Route 53 forwarding rules exist, the query is sent to a public DNS authority.

### 8.8 Plan for virtual machine remote access: -

* **Bastion Host in Common Service Account:** A bastion host is a server whose purpose is to provide access to a private network from an external network, such as the Internet. Because of its exposure to potential attack, a bastion host must minimize the chances of penetration.
* **Session Manager:** Session Manager is a fully managed AWS Systems Manager capability that lets you manage your Amazon EC2 instances through an interactive one-click browser-based shell or through the AWS CLI. You can use Session Manager to start a session with an instance in your account. After the session is started, you can run bash commands as you would through any other connection type.

Before using Session Manager, make sure your environment meets the following requirements.

**Session Manager prerequisites**

|  |  |
| --- | --- |
| **Requirement** | **Description** |
| Supported operating systems | Session Manager supports connecting to Amazon Elastic Compute Cloud (Amazon EC2) instances, in addition to servers or virtual machines (VMs) in your hybrid environment that use the *advanced-instances* tier. |
| Session Manager supports the following operating system versions: |
|  |
| **Note** |
| Session Manager supports EC2 instances, edge devices, and on-premises servers and virtual machines (VMs) in your hybrid environment that use the advanced-instances tier. For more information about advanced instances, see Configuring instance tiers. |
|  |
| **Linux** |
|  |
| Session Manager supports all the versions of Linux that are supported by AWS Systems Manager. For information, see Systems Manager prerequisites. |
|  |
| **macOS** |
|  |
| Session Manager supports all the versions of macOS that are supported by AWS Systems Manager. For information, see Systems Manager prerequisites. |
|  |
| **Windows** |
|  |
| Session Manager supports Windows Server 2012 through Windows Server 2022. |
|  |
| **Note** |
| Microsoft Windows Server 2016 Nano isn't supported. |
| SSM Agent | At minimum, AWS Systems Manager SSM Agent version 2.3.68.0 or later must be installed on the managed nodes you want to connect to through sessions. |
|  |
| To use the option to encrypt session data using a key created in AWS Key Management Service (AWS KMS), version 2.3.539.0 or later of SSM Agent must be installed on the managed node. |
|  |
| To use shell profiles in a session, SSM Agent version 3.0.161.0 or later must be installed on the managed node. |
|  |
| To start a Session Manager port forwarding or SSH session, SSM Agent version 3.0.222.0 or later must be installed on the managed node. |
|  |
| To stream session data using Amazon CloudWatch Logs, SSM Agent version 3.0.284.0 or later must be installed on the managed node. |
|  |
| For information about how to determine the version number running on an instance, see Checking the SSM Agent version number. For information about manually installing or automatically updating SSM Agent, see Working with SSM Agent. |
|  |
| **About the ssm-user account** |
|  |
| Starting with version 2.3.50.0 of SSM Agent, the agent creates a user account on the managed node, with root or administrator permissions, called ssm-user. (On versions before 2.3.612.0, the account is created when SSM Agent starts or restarts. On version 2.3.612.0 and later, ssm-user is created the first time a session starts on the managed node.) Sessions are launched using the administrative credentials of this user account. For information about restricting administrative control for this account, see Turn off or turn on ssm-user account administrative permissions. |
|  |
| **ssm-user on Windows Server domain controllers** |
|  |
| Beginning with SSM Agent version 2.3.612.0, the ssm-user account isn't created automatically on managed nodes that are used as Windows Server domain controllers. To use Session Manager on a Windows Server machine being used as a domain controller, you must create the ssm-user account manually if it isn't already present, and assign Domain Administrator permissions to the user. On Windows Server, SSM Agent sets a new password for the ssm-user account each time a session starts, so you don't need to specify a password when you create the account. |
| Connectivity to endpoints | The managed nodes you connect to must also allow HTTPS (port 443) outbound traffic to the following endpoints: |
|  |
| ec2messages.*region*.amazonaws.com |
| ssm.*region*.amazonaws.com |
| ssmmessages.*region*.amazonaws.com |
|  |
| Alternatively, you can connect to the required endpoints by using interface endpoints. For more information, see Step 6: (Optional) Use AWS PrivateLink to set up a VPC endpoint for Session Manager. |
| AWS CLI | (Optional) If you use the AWS Command Line Interface (AWS CLI) to start your sessions (instead of using the AWS Systems Manager console or Amazon EC2 console), version 1.16.12 or later of the CLI must be installed on your local machine. |
|  |
| You can call aws --version to check the version. |
|  |
| If you need to install or upgrade the CLI, see Installing the AWS Command Line Interface in the AWS Command Line Interface User Guide. |
|  |
| Important |
| An updated version of SSM Agent is released whenever new capabilities are added to Systems Manager or updates are made to existing capabilities. Failing to use the latest version of the agent can prevent your managed node from using various Systems Manager capabilities and features. For that reason, we recommend that you automate the process of keeping SSM Agent up to date on your machines. For information, see Automating updates to SSM Agent. Subscribe to the SSM Agent Release Notes page on GitHub to get notifications about SSM Agent updates. |
|  |
| In addition, to use the CLI to manage your nodes with Session Manager, you must first install the Session Manager plugin on your local machine. For information, see (Optional) Install the Session Manager plugin for the AWS CLI. |

* **Fleet Manager:** Fleet Manager, a capability of AWS Systems Manager, to connect to your Windows Server 2012 RTM and later instances using the Remote Desktop Protocol (RDP). These Remote Desktop sessions powered by NICE DCV provide secure connections to your instances directly from your browser. With Fleet Manager, you can connect a maximum of four instances per browser window. Currently, Fleet Manager supports only English language inputs. Though you can connect to instances with Fleet Manager using RDP without opening any inbound ports, Fleet Manager only supports operating system configurations that use the default RDP port 3389 at this time. If you've changed the value of the listening port for RDP on your instance, Fleet Manager fails to establish the connection. When connecting to your instance, you can use Windows credentials or the Amazon EC2 key pair (.pem file) associated with the instance for authentication.

# 9. Security

Security is a core consideration of every enterprise environment. When designing and implementing an AWS landing zone, security is a consideration throughout the process.

The security design area focuses on considerations and recommendations for landing zone decisions. The Secure methodology in the Cloud Adoption Framework also provides further in-depth guidance for holistic security processes and tools.

### 9.1.1 AWS Control Tower Controls(Guardrails): -

A control (sometimes called a guardrail) is a high-level rule that provides ongoing governance for your overall AWS environment. It's expressed in plain language. Three kinds of controls exist: preventive, detective, and proactive. Three categories of guidance apply to controls: mandatory, strongly recommended, or elective.

Guardrail behaviour

* Prevention – A preventive guardrail will ensure that accounts maintain compliance, because it disallows actions that lead to policy violations. The status of a preventive guardrail will be either enforced or not enabled.
* Detection – A detective guardrail will detect non-compliance of resources within the accounts, such as policy violations, and will provide an alert through the dashboard. The status of a detective guardrail will either be clear, in violation, or not enabled.

### 9.1.2 CIS AWS Foundations Benchmark: -

The Center for Internet Security (CIS) is a non-profit that developed the CIS AWS Foundations Benchmark. This benchmark serves as a set of security configuration best practices for AWS. These industry-accepted best practices go beyond the high-level security guidance already available in that they provide you with clear, step-by-step implementation and assessment procedures.

* CIS Benchmarks: *CIS Benchmarks* are security best practice guidelines that are specific to vendor products. Ranging from operating systems to cloud services and networks devices, the settings that are applied from a benchmark protect the specific systems that your organization use.
* CIS Controls: CIS Controls*are foundational best practice guidelines for organization-level systems to follow to help protect against known cyberattack vectors.*

### 9.2 Identity and Access Management: -

AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources. You use IAM to control who is authenticated (signed in) and authorized (has permissions) to use resources.

When you create an AWS account, you begin with one sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account *root user* and is accessed by signing in with the email address and password that you used to create the account. We strongly recommend that you do not use the root user for your everyday tasks. Safeguard your root user credentials and use them to perform the tasks that only the root user can perform.

|  |  |
| --- | --- |
| Item | Description |
| Multi Factor Authentication | Multi-factor authentication is a process in which users are prompted during the sign-in process for an additional form of identification, such as a code on their SMS or authentication app. AWS policy will be in place to ensure all users have MFA enabled.  If user only use a password to authenticate a user, it leaves an insecure vector for attack. If the password is weak or has been exposed elsewhere, an attacker could be using it to gain access. When user require a second form of authentication, security is increased because this additional factor isn't something that's easy for an attacker to obtain or duplicate. |
| IAM Roles | IAM roles have specific permissions and provide a way to access AWS by relying on temporary security credentials with a role session. |
| Least Privilege Permissions | When you set permissions with IAM policies, grant only the permissions required to perform a task. You do this by defining the actions that can be taken on specific resources under specific conditions, also known as *least-privilege permissions*. |
| Password policy enforcement | A password policy is applied to all user accounts that are created and managed directly in AWS IAM. In case of Mahindra Finance user creation is managed in Microsoft Active Directory and Azure AD Connect is used to sync data in Azure AD. Azure AD is integrated with AWS Identity Provider(AWS SSO) as an external IdP. Password policy to be implemented where user creation is performed. |
| Policy | Use a policy to control access to resources within IAM or all of AWS. Policies let you specify who has access to AWS resources, and what actions they can perform on those resources. Every IAM user starts with no permissions. In other words, by default, users can do nothing, not even view their own access keys. To give a user permission to do something, you can add the permission to the user (that is, attach a policy to the user). Or you can add the user to a user group that has the intended permission. |
| Access keys | Access keys are long-term credentials for an IAM user or the AWS account root user. You can use access keys to sign programmatic requests to the AWS CLI or AWS API (directly or using the AWS SDK). |
| Access Reviews | User's access can be reviewed on a regular basis to make sure only the right people have continued access. Conduct access reviews to ensure users still need roles which are assigned to them. |



9.3 Network Security

Network security is covered in section 8.3

9.4 AWS data security and encryption

**AWS Key Management Service**

AWS Key Management Service (AWS KMS) lets you create, manage, and control cryptographic keys across your applications and more than 100 AWS services. AWS KMS integrates with AWS services to encrypt data at rest using an AWS KMS key.

Types of KMS keys available in AWS:

1. Customer managed keys: The KMS keys that you create are customer managed keys. Customer managed keys are KMS keys in your AWS account that you create, own, and manage. You have full control over these KMS keys, including establishing and maintaining their key policies, IAM policies, and grants, enabling and disabling them, rotating their cryptographic material, adding tags, creating aliases that refer to the KMS keys, and scheduling the KMS keys for deletion.

2. AWS managed keys: AWS managed keys are KMS keys in your account that are created, managed, and used on your behalf by an AWS service integrated with AWS KMS.

Some AWS services let you choose an AWS managed key or a customer managed key to protect your resources in that service. In general, unless you are required to control the encryption key that protects your resources, an AWS managed key is a good choice. You don't have to create or maintain the key or its key policy, and there's never a monthly fee for an AWS managed key.

The KMS keys that you create are customer managed keys. AWS services that use KMS keys to encrypt your service resources often create keys for you. KMS keys that AWS services create in your AWS account are AWS managed keys. KMS keys that AWS services create in a service account are AWS owned keys.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Type of KMS key** | **Can view KMS key metadata** | **Can manage KMS key** | **Used only for my AWS account** | **Automatic rotation** | **Pricing** |
| Customer managed key | Yes | Yes | Yes | Optional. Every year (approximately 365 days) | Monthly fee (pro-rated hourly) |
|  |
| Per-use fee |
| AWS managed key | Yes | No | Yes | Required. Every year (approximately 365 days) | No monthly fee |
|  |
| Per-use fee (some AWS services pay this fee for you) |
| AWS owned key | No | No | No | Varies | No fees |

AWS services integrated with AWS KMS

|  |  |  |  |
| --- | --- | --- | --- |
| Alexa for Business[1] | Amazon Forecast | Amazon Nimble Studio | AWS CloudHSM[2] |
| Amazon AppFlow | Amazon Fraud Detector | Amazon Personalize | AWS CloudTrail |
| Amazon Athena | Amazon FSx | Amazon QLDB | AWS CodeArtifact |
| Amazon Aurora | Amazon GuardDuty | Amazon Redshift | AWS CodeBuild |
| Amazon CloudWatch Logs | Amazon HealthLake | Amazon Rekognition | AWS CodeCommit[1] |
| Amazon CloudWatch Synthetics | Amazon Inspector | Amazon Relational Database Service (RDS) | AWS CodePipeline |
| Amazon CodeGuru | Amazon Kendra | Amazon Route 53 | AWS Control Tower |
| Amazon Comprehend | Amazon Keyspaces (for Apache Cassandra) | Amazon S3 | AWS Database Migration Service |
| Amazon Connect | Amazon Kinesis Data Streams | Amazon SageMaker | AWS Elastic Disaster Recovery |
| Amazon Connect Customer Profiles | Amazon Kinesis Firehose | Amazon Simple Email Service (SES) | AWS Elemental MediaTailor |
| Amazon Connect Voice ID | Amazon Kinesis Video Streams | Amazon Simple Notification Service (SNS) | AWS Glue |
| Amazon Connect Wisdom | Amazon Lex | Amazon Simple Queue Service (SQS) | AWS Glue DataBrew |
| Amazon DocumentDB | Amazon Lightsail[1] | Amazon Textract | AWS IoT SiteWise |
| Amazon DynamoDB | Amazon Location Service | Amazon Timestream | AWS Lambda |
| Amazon DynamoDB Accelerator (DAX)[1] | Amazon Lookout for Equipment | Amazon Transcribe | AWS License Manager |
| Amazon EBS | Amazon Lookout for Metrics | Amazon Translate | AWS Network Firewall |
| Amazon EC2 Image Builder | Amazon Lookout for Vision | Amazon WorkMail | AWS Proton |
| Amazon EFS | Amazon Macie | Amazon WorkSpaces | AWS Secrets Manager |
| Amazon Elastic Container Registry (ECR) | Amazon Managed Blockchain | Amazon WorkSpaces Web | AWS Snowball |
| Amazon Elastic Kubernetes Service (EKS) | Amazon Managed Service for Prometheus | AWS Audit Manager | AWS Snowball Edge |
| Amazon Elastic Transcoder | Amazon Managed Streaming for Kafka (MSK) | AWS Application Cost Profiler | AWS Snowcone |
| Amazon ElastiCache | Amazon Managed Workflows for Apache Airflow (MWAA) | AWS Application Migration Service | AWS Snowmobile |
| Amazon OpenSearch | Amazon MemoryDB | AWS App Runner | AWS Storage Gateway |
| Amazon EMR | Amazon Monitron | AWS Backup | AWS Systems Manager |
| Amazon EMR Serverless | Amazon MQ | AWS Certificate Manager[1] | AWS X-Ray |
| Amazon FinSpace | Amazon Neptune | AWS Cloud9[1] |  |

[1] Supports only AWS managed keys.

[2] AWS KMS supports custom key stores backed by an AWS CloudHSM cluster.

[3] For a list of services integrated with AWS KMS in the AWS China (Beijing) Region, operated by Sinnet and the AWS China (Ningxia) Region, operated by NWCD, please visit AWS KMS Service integration in China.

AWS services not listed above encrypt customer data using keys owned and managed by the respective service.

**Decentralized Keys: -**

AWS KMS keys would be decentralized and can be managed in each account separately.

Protect Data at Rest

Amazon EBS encryption

Use Amazon EBS encryption as a straight-forward encryption solution for your EBS resources associated with your EC2 instances. With Amazon EBS encryption, you aren't required to build, maintain, and secure your own key management infrastructure. Amazon EBS encryption uses AWS KMS keys when creating encrypted volumes and snapshots.Encryption operations occur on the servers that host EC2 instances, ensuring the security of both data-at-rest and data-in-transit between an instance and its attached EBS storage.

Protect Data in Transit

To protect data in transit, AWS encourages customers to leverage a multi-level approach. All network traffic between AWS data centers is transparently encrypted at the physical layer. All traffic within a VPC and between peered VPCs across regions is transparently encrypted at the network layer when using supported Amazon EC2 instance types. At the application layer, customers have a choice about whether and how to use encryption using a protocol like Transport Layer Security (TLS). All AWS service endpoints support TLS to create a secure HTTPS connection to make API requests.

Using services like AWS KMS, AWS CloudHSM, and AWS ACM, customers can implement a comprehensive data at rest and data in transit encryption strategy across their AWS ecosystem to ensure all data of a given classification shares the same security posture.

Application

Data is transit to be encrypted using at application level by using SSL/TLS or other protocols for added protection.

9.5 Resource Management

Resource access Bastion Host or Sessions Manager or Cloud9 will be used for AWS resource access.

9.6 Backup and Retention

The AWS Backup service is recommended to protect data in simple, secure, and cost-effective way in AWS Cloud for Mahindra Finance

Refer below recommended for backup and retention for each environment for Mahindra Finance Ltd.

|  |  |  |  |
| --- | --- | --- | --- |
| Prod | Backup Type | Daily backup | Retention |
| Volume backup | Y | 14 days |
| **Database backup** |  |  |
| Backup Type | Daily backup | Retention |
| Database backup | Y | 14 days |
|  |  |  |  |
| Prod | Backup Type | Weekly backup | Retention |
| Volume backup | Y | 1 month |
| **Database backup** |  |  |
| Backup Type | Weekly backup | Retention |
| Database backup | Y | 1 month |
|  |  |  |  |
| Prod | Backup Type | Monthly Backup | Retention |
| Volume backup | Y | 1 year |
| **Database backup** |  |  |
| Backup Type | Weekly backup | Retention |
| Database backup | Y | 1 year |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| Non-Prod | Backup Type | Daily backup | Retention |
| Volume backup | Y | 7 days |
| **Database backup** |  |  |
| Backup Type | Daily backup | Retention |
| Database backup | Y | 7 days |

9.7 Golden Images

Golden Images are OS Images which are used to maintain standard OS level security settings and compliance settings.

There should be necessary versions of Operating Systems images of Windows and linux both should be available to create VMs.

VM should be created by OS image with latest patches and security settings, for that customized script to execute on VM once it is created.

The customized script contains steps and commands which are set the latest security settings and updated the latest patches on VM.

9.8 Patch management

**AWS Systems Manager Patch Manager: -**

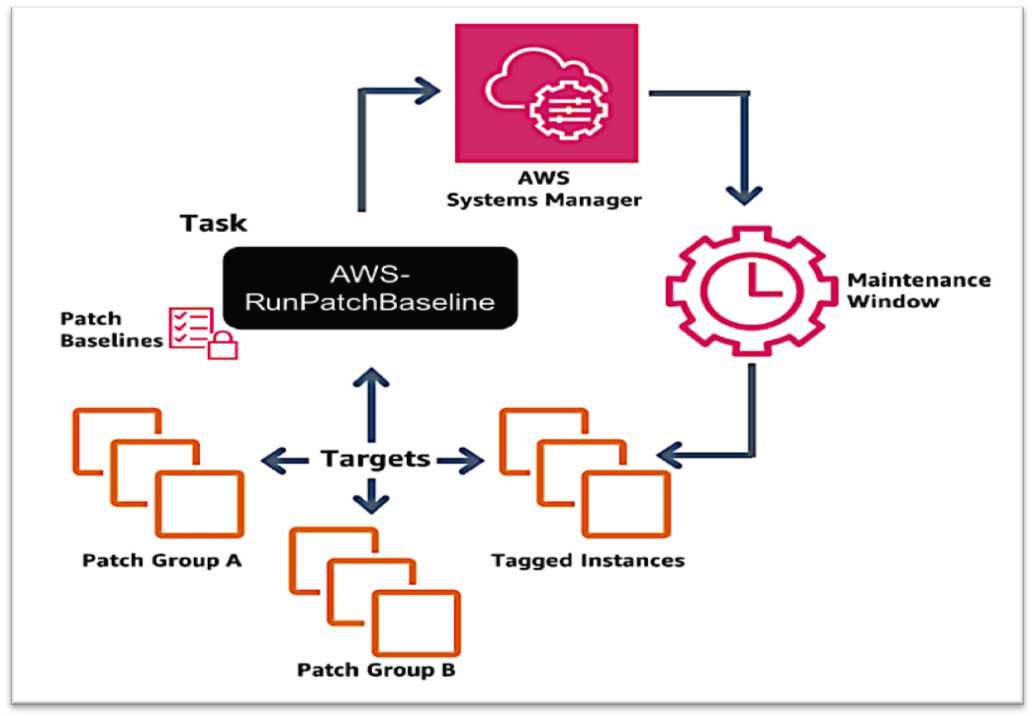
Patch Manager, a capability of AWS Systems Manager, automates the process of patching managed nodes with both security related and other types of updates. You can use Patch Manager to apply patches for both operating systems and applications. (On Windows Server, application support is limited to updates for applications released by Microsoft.) You can use Patch Manager to install Service Packs on Windows nodes and perform minor version upgrades on Linux nodes. You can patch fleets of Amazon Elastic Compute Cloud (Amazon EC2) instances, edge devices, or your on-premises servers and virtual machines (VMs) by operating system type. This includes supported versions of Amazon Linux, Amazon Linux 2, CentOS, Debian Server, macOS, Oracle Linux, Raspberry Pi OS (formerly Raspbian), Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), Ubuntu Server, and Windows Server. You can scan instances to see only a report of missing patches, or you can scan and automatically install all missing patches.

AWS doesn't test patches before making them available in Patch Manager. Also, Patch Manager doesn't support upgrading major versions of operating systems, such as Windows Server 2016 to Windows Server 2019, or SUSE Linux Enterprise Server (SLES) 12.0 to SLES 15.0.

For Linux-based operating system types that report a severity level for patches, Patch Manager uses the severity level reported by the software publisher for the update notice or individual patch. Patch Manager doesn't derive severity levels from third-party sources, such as the Common Vulnerability Scoring System (CVSS), or from metrics released by the National Vulnerability Database (NVD).

Patch Manager uses *patch baselines*, which include rules for auto-approving patches within days of their release, in addition to a list of approved and rejected patches. You can install patches on a regular basis by scheduling patching to run as a Systems Manager maintenance window task. You can also install patches individually or to large groups of managed nodes by using tags. (Tags are keys that help identify and sort your resources within your organization.) You can add tags to your patch baselines themselves when you create or update them.

Please refer below AWS SSM architecture diagram



Patch Manager prerequisites:-

Make sure that you have met the required prerequisites before using Patch Manager, a capability of AWS Systems Manager.

SSM Agent version

Version 2.0.834.0 or later of SSM Agent is running on the managed node you want to manage with Patch Manager.

Python version

For macOS and most Linux operating systems (OSs), Patch Manager currently supports Python versions 2.6 - 3.9. The Debian Server, Raspberry Pi OS, and Ubuntu Server OSs require a supported version of Python 3 (3.0 - 3.9).

Connectivity to the patch source

If your managed nodes don't have a direct connection to the Internet and you're using an Amazon Virtual Private Cloud (Amazon VPC) with a VPC endpoint, you must ensure that the nodes have access to the source patch repositories (repos). On Linux nodes, patch updates are typically downloaded from the remote repos configured on the node. Therefore, the node must be able to connect to the repos so the patching can be performed.

Windows Server managed nodes must be able to connect to the Windows Update Catalog or Windows Server Update Services (WSUS). Confirm that your nodes have connectivity to the Microsoft Update Catalog through an internet gateway, NAT gateway, or NAT instance. If you are using WSUS, confirm that the node has connectivity to the WSUS server in your environment.

S3 endpoint access

Whether your managed nodes operate in a private or public network, without access to the required AWS managed Amazon Simple Storage Service (Amazon S3) buckets, patching operations fail. For information about the S3 buckets your managed nodes must be able to access

WSUS server and YUM Repo: -

To download and store only organization tested patches without internet need to host WSUS server for windows patches and YUM repo for Linux patches.

**AWS PAAS and SAAS Patch management**

AWS PAAS Patch management – No action needed as AWS itself manages PAAS services patches on their own backend infrastructure.

AWS SAAS Patch management - No action needed as AWS itself manages PAAS services patches on their own backend infrastructure.

10 Governance

AWS Control Tower implements preventive and detective controls that help govern the resources and monitor compliance across all the AWS accounts in the Landing Zone via Guardrails.

Identity, Security and naming/tagging is already covered in previous sections. Cost management will be a major focus in this section.

10.1 Cost Governance: -

Cost governance is key to have cost visibility, accountability and optimization. It is important to establish an environment for consistent processes in the classification and organization of all assets.

Assets include all virtual machines, data sources, and applications deployed to the cloud. There should be defined asset classification and organization.

Mahindra Finance have multiple LOBs and Cost centers. Cloud cost is divided into cost centers which can span across LOB’s. Cost centers are used to chargeback Cloud cost to LOB’s.

**Cost management tool**

AWS Cost Management + Billing to be used for setting budgets and gaining visibility into cloud costs for AWS. It gives platform for cost governance and It can also reduce costs and the overhead required to manage organizational assets. Cost Management + Billing is a suite of tools that help you analyse, manage, and optimize the costs of your workloads.

Mahindra Finance have planned to use **FinOps tool** for Cloud Financial Management.

**Cost management model**

Mahindra Finance Ltd has Enterprise Agreement. Enterprise Agreement enrolment represents the commercial relationship with AWS and Mahindra Finance Ltd.

**AWS Cost Management**

The AWS Cost Management console has features that you can use for budgeting and forecasting costs and methods for you to optimize your pricing to reduce your overall AWS bill.

The AWS Cost Management console is integrated closely with the Billing console. Using both together, you can manage your costs in a holistic manner. You can use Billing console resources to manage your ongoing payments, and AWS Cost Management console resources to optimize your future costs.

With the AWS Cost Management console and the Billing console, you can do the following tasks.

|  |  |  |  |
| --- | --- | --- | --- |
| **Use cases** | **Description** | **AWS Cost Management feature names** | **Billing console feature names** |
| Organize | Construct your cost allocation and governance foundation with your own tagging strategy. | - | AWS Cost Categories |
|  |
| [AWS Cost Allocation Tags](https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/cost-alloc-tags.html) |
| Report | Raise awareness and accountability of your cloud spend with the detailed, allocable cost data. | AWS Cost Explorer | AWS Cost and Usage Reports |
| Access | Track billing information across the organization in a consolidated view. | - | AWS Consolidated Billing |
|  |
| AWS Purchase Order Management |
|  |
| AWS Credits |
| Control | Establish effective governance mechanisms with the right guardrails in place. | AWS Cost Anomaly Detection | - |
| Forecast | Estimate your resource utilization and spend with forecast dashboards that you create. | AWS Cost Explorer | - |
|  |
| AWS Budgets |
| Budget | Keep your spend in check with custom budget threshold and auto alert notification. | AWS Budgets | - |
|  |
| AWS Budgets Actions |
| Purchase | Use free trials and programmatic discounts based on your workload pattern and needs. | Savings Plans | AWS Free Tier |
|  |
| AWS Reserved Instances |
| Rightsize | Align your service allocation size to your actual workload demand. | Rightsizing Recommendations | - |
| Inspect | Stay up to date with your resource deployment and cost optimization opportunities. | AWS Cost Explorer | - |

Features of AWS Cost Management

AWS Cost Explorer:-

Use case: Report, Forecast, Inspect

AWS Cost Explorer is a feature that you can use to visualize your cost data for further analysis. Using it, you can filter graphs by several different values. This includes Availability Zone, AWS service, and AWS Region, It also includes other specifics such as custom cost allocation tag, Amazon EC2 instance type, and purchase option. If you use consolidated billing, you can also filter by member account. In addition, you can see a forecast of future costs based on your historical cost data.

AWS Budgets:-

Use case: Forecast, Inspect

AWS Budgets tracks your AWS usage and costs. AWS Budgets uses the cost visualization that's provided by AWS Cost Explorer to show the status of your budgets. This provides forecasts of your estimated costs and tracks your AWS usage, including your AWS Free Tier usage. You can also use AWS Budgets to create Amazon Simple Notification Service (Amazon SNS) notifications for when you exceed your budgeted amounts, or when your estimated costs exceed your budgets.

Rightsizing Recommendations:-

Use case: Control

Rightsizing recommendations is a feature that reviews your historical Amazon EC2 usage for the past 14 days to identify opportunities for greater cost and usage efficiency. The feature identifies cost saving opportunities by downsizing or terminating instances in Amazon EC2.

Savings Plans:-

Use case: Purchase

Savings Plans offers a flexible pricing model that provides savings on AWS usage. Savings Plans provide savings beyond On-Demand rates in exchange for a commitment of using a specified amount of compute power (measured every hour) for a one or three year period. You can manage your plans by using recommendations, performance reporting, and budget alerts in AWS Cost Explorer.

**Chargeback Model**

Mahindra Finance Ltd has multiple LOB’s and dedicated nested OU’s will be created for each project which further has environment wise accounts. Mahindra Finance has decided to follow account wise chargeback model. Resource management has mix model organization which has shared environment-based subscription. Enterprise has shared costs as well for the resources deployed in Corporate Accounts such as identity, networking and security that need to be divided by LOB’s. Tagging policy play a key role in chargeback model in this scenario along with cost allocation rule. Following are key components of chargeback model

1. CostCenter tag
2. bussiness-project-name tag
3. shared-dedicate tag

11 Monitoring

11.1 Amazon CloudWatch

Amazon CloudWatch collects and visualizes real-time logs, metrics, and event data in automated dashboards to streamline your infrastructure and application maintenance.

Amazon CloudWatch monitors your Amazon Web Services (AWS) resources and the applications you run on AWS in real time. You can use CloudWatch to collect and track metrics, which are variables you can measure for your resources and applications.

The CloudWatch home page automatically displays metrics about every AWS service you use. You can additionally create custom dashboards to display metrics about your custom applications, and display custom collections of metrics that you choose.

11.2 CloudWatch Container Insights

Use CloudWatch Container Insights to collect, aggregate, and summarize metrics and logs from your containerized applications and microservices. Container Insights is available for Amazon Elastic Container Service (Amazon ECS), Amazon Elastic Kubernetes Service (Amazon EKS), and Kubernetes platforms on Amazon EC2. Container Insights supports collecting metrics from clusters deployed on Fargate for both Amazon ECS and Amazon EKS.

11.3 ELK Monitoring tool: -

A decision has been made that ELK will be used for monitoring and will be deployed by MnM vendor.

11.4 Metrics and thresholds Recommendation to monitor

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Resource** | **Parameters to monitor** | **Threshold  percentage  for 1st Alarm** | **Threshold  percentage  for 2nd Alarm** | **Threshold  percentage for 3rd Alarm** |
| VM | CPU | 75 | 85 | 90 |
|  | Memory | 75 | 85 | 90 |
|  | Disk | 75 | 85 | 90 |
|  | Network | 75 | 85 | 90 |
| Strorage | Read operations on objects. | 75 | 85 | 90 |
|  | Write operations on objects. | 75 | 85 | 90 |
|  | StorageDelete | 75 | 85 | 90 |
| Paas services |  |  |  |  |
| Functions | **FunctionExecutionCount:-** Function execution count indicates the number of times your function app has executed. This value correlates to the number of times a function runs in your app. | 75% of max Count | 75% of max Count | 90% of max Count |
| **FunctionExecutionUnits: -** Function execution units are a combination of execution time and your memory usage. | 75% of max Count | 75% of max Count | 90% of max Count |
| App services | **CPU Percentage:-** The average CPU used across all instances of the plan. | 75 | 85 | 90 |
|  | **Memory Percentage:-** The average memory used across all instances of the plan. | 75 | 85 | 90 |
|  | **Data In:-** The average incoming bandwidth used across all instances of the plan. | 75 | 85 | 90 |
|  | **Data Out:-**  The average outgoing bandwidth used across all instances of the plan. | 75 | 85 | 90 |
|  | **Disk Queue Length:-**  The average number of both read and write requests that were queued on storage. A high disk queue length is an indication of an app that might be slowing down because of excessive disk I/O. | 75 | 85 | 90 |
|  | **Http Queue Length:-**  The average number of HTTP requests that had to sit on the queue before being fulfilled. A high or increasing HTTP Queue length is a symptom of a plan under heavy load. | 75 | 85 | 90 |
| EKS Node | CPU | 75 | 85 | 90 |
|  | Memory | 75 | 85 | 90 |
|  | disk | 75 | 85 | 90 |
|  | Network | 75 | 85 | 90 |
|  |  |  |  |  |
| Containers | CPU | 75 | 85 | 90 |
|  | Memory | 75 | 85 | 90 |
| PersistentVolumes | Usage capacity | 75 | 85 | 90 |
| DB | CPU percentage:- Percentage of vCores in use | 75 | 85 | 90 |
|  | DTU (Database trasaction Unit) percentage:- Percentage of DTUs in use | 75 | 85 | 90 |
|  | Memory percentage:- Percentage of memory in use | 75 | 85 | 90 |
|  | Storage percentage:- Percentage of database space in use | 75 | 85 | 90 |
|  | Sessions percentage:- Percentage of concurrent sessions in use | 75 | 85 | 90 |

11.5 Logging: -

Monitoring allows you to plan for and respond to potential incidents. Therefore, monitoring is an important part of the well-architected nature of AWS Control Tower. The results of monitoring activities are stored in log files; therefore, logging and monitoring are closely related concepts.

When you set up your landing zone, one of the shared accounts created is the *log archive* account, dedicated to collecting all logs centrally, including logs for all of your other accounts. These log files allow administrators and auditors to review actions and events that have occurred.

AWS Control Tower accomplishes logging of actions and events automatically, through its integration with AWS CloudTrail and AWS Config, and it records them in CloudWatch. All actions are logged, including actions from the AWS Control Tower management account and from your organization's member accounts. Management account actions and events are viewable on the Activities page in the console. You can view member account actions and events in the log archive files.

For example, the status of your controls is monitored constantly. You can see their status at a glance in the AWS Control Tower console. The health and status of the accounts you provisioned in Account Factory also is monitored constantly.

**Logging AWS Control Tower Actions with AWS CloudTrail**

AWS Control Tower is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in AWS Control Tower. CloudTrail captures actions for AWS Control Tower as events. If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for AWS Control Tower.

If you don't configure a trail, you can still view the most recent events in the CloudTrail console in Event history. Using the information collected by CloudTrail, you can determine the request that was made to AWS Control Tower, the IP address from which the request was made, who made the request, when it was made, and additional details.

CloudTrail is enabled on your AWS account when you create the account. When supported event activity occurs in AWS Control Tower, that activity is recorded in a CloudTrail event along with other AWS service events in Event history. You can view, search, and download recent events in your AWS account. For more information, see Viewing Events with CloudTrail Event History.

**Monitoring resource changes with AWS Config**

AWS Control Tower enables AWS Config on all enrolled accounts, so that it can monitor compliance through detective controls, record resource changes, and deliver resource change logs to the log archive account.

If your landing zone version is earlier than 3.0: For your enrolled accounts, AWS Config logs all changes to resources, for all Regions in which the account operates. Each change is modelled as a configuration item (CI), which contains information such as the resource identifier, the Region, the date that each change was recorded, and whether the change relates to a known resource or a newly discovered one.

If your landing zone version is 3.0 or later: AWS Control Tower limits recording for global resources, such as IAM users, groups, roles, and customer managed polices, to your home Region only. Copies of global resource changes are not stored in every Region.

AWS Control Tower sets up an AWS Config delivery channel in all enrolled accounts. Through this delivery channel, it logs all changes recorded by AWS Config in the log archive account, where they are stored to a folder in an Amazon Simple Storage Service bucket.

12. AWS Best Practices

12.1 The root user is secured

The root user has unlimited access to your account and its resources, and using it only by exception helps protect your AWS resources. The AWS root user must not be used for everyday tasks, even administrative ones. If an account is not managed by AWS Organizations, enabling MFA provides an additional control for account sign-in. Programmatic access to AWS APIs should never use the root user. It is best not to generate static an access key for the root user. All of the following must be implemented: IAM Users or IAM Roles are created and used for all routine activities. The root user is only used for tasks that require it. Access keys are not assigned to the root user. Multi-Factor Authentication (MFA) is enabled on the root user.

Below guardrails are Enabled in order to secure root user

* Detect whether MFA for the root user is enabled
* Disallow creation of access keys for the root user
* Disallow actions as a root user

Tasks that require root user credentials - AWS Management Account:

* **Change your account settings** This includes the account name, email address, root user password, and root user access keys. Other account settings, such as contact information, payment currency preference, and AWS Regions, don't require root user credentials.
* **Restore IAM user permissions** If the only IAM administrator accidentally revokes their own permissions, you can sign in as the root user to edit policies and restore those permissions.
* Activate IAM access to the Billing and Cost Management console.
* **View certain tax invoices** An IAM user with the aws-portal:ViewBilling permission can view and download VAT invoices from AWS Europe, but not AWS Inc. or Amazon Internet Services Private Limited (AISPL).
* Close your AWS account.
* Register as a seller in the Reserved Instance Marketplace.
* Configure an Amazon S3 bucket to enable MFA (multi-factor authentication).
* Edit or delete an Amazon Simple Storage Service (Amazon S3) bucket policy that includes an invalid virtual private cloud (VPC) ID or VPC endpoint ID.
* Sign up for GovCloud.

12.2 Account contact information is set

If an account is not managed by AWS Organizations, alternate account contacts help AWS get in contact with the appropriate personnel if needed. Configure the account’s alternate contacts to point to a group rather than an individual. For example, create separate email distribution lists for billing, operations, and security and configure these as Billing, Security, and Operations contacts in each active AWS account. This ensures that multiple people will receive AWS notifications and be able to respond, even if someone is on vacation, changes roles, or leaves the company.

In case of Mahindra Finance, all AWS accounts are managed by AWS Organizations.