Infosys®
Navigate your next

Navigating Nile, Together.

Build. Amplify. Leap.

Technical Design Document

Project	**VANGUARD**
Date	**18-Sep-2020**
Version No.	**2.0**

Response to Request for Proposal

Contact Information

For further information and discussions, please contact	
Name	
Designation	
Address	Infosys Limited
Phone	
Email	

Confidential Information

This proposal is confidential to Infosys Limited ("Infosys") and [Type the company name]. This document contains information and data that Infosys considers confidential and proprietary (“Confidential Information”).

Confidential Information includes, but is not limited to, the following:

- Corporate, employee and infrastructure information about Infosys
- Infosys’ project management and quality processes
- Customer and project experiences provided to illustrate Infosys capability

Any disclosure of Confidential Information to, or use of it by a third party (i.e., a party other than [Type the company name]), will be damaging to Infosys. Ownership of all Confidential Information, no matter in what media it resides, remains with Infosys.

Confidential Information in this document shall not be disclosed outside the buyer’s proposal evaluators and shall not be duplicated, used, or disclosed – in whole or in part – for any purpose other than to evaluate this proposal without specific written permission of an authorized representative of Infosys.

Table of Contents

Index of Figures

Index of Tables

1. Introduction

1.1 Cloud Foundation Overview

This document provides an overview about the various aspects involved in setting up the Green Field AWS cloud environment for Vanguard. The high level activities include provisioning, build and deploy the foundational cloud infrastructure and services required to host, maintain and operate the Modernized Platform (the “Cloud Foundation”). This is in accordance with the scope of work as defined in Annexure 23-B1

As part of the Cloud foundation, this document also captures the architecture using AWS, key design considerations, strategy aligning to the industry best practices, recommendations underlying infrastructure design for AWS to meet Vanguard requirements as enlisted in Attachment 23-B1 – Cloud Implementation Transformation project.

This Document also has reference links to the below listed individual Design Documents (Refer Section–2) that are created in an elaborative manner envisaging all key elements in arriving at suitable design solutions for Vanguard.

1.2 Intended Audiences

Roles	Expectation
Tech Architects	Overall architecture and how AWS fits in the whole secure cloud program w.r.t Company requirements Details of VPC , Subnets NACLs, SOE and all components needed to be deployed
Application and Business Owners	OU , Account structures and Application placements and controls
Company Architecture/Design Review Board	Overall architecture and for review and approval

2. Design & Solution Documents

Below table enlists various Solution & Design documents covering all aspects to implement the AWS Cloud Infrastructure as per the agreed project Scope and the requirements.

Document Ref. #	Design Documents
1	**Cloud Foundation Design Document**
1A	Foundation Design Document
1B	OU & Account Structure Technical Design
1C	Storage & Backup Design Document
1D	Patching Design Document
1E	Infosys PolyCloud Design Document
2	**Network Design Document**
3	**DR Design Document**
4	**Monitoring solution Design Document**
5	**Workspaces Design Document**

3. AWS Cloud Foundation Design Consideration

3.1 AWS Organization

AWS Organizations service will be used to centrally manage & control the use of AWS services across multiple AWS accounts (using Service Control Policies) in order to comply with the security and compliance policies. It enables consolidation of multiple AWS accounts be created and is used for consolidated billing to meet the budgetary, security, and compliance needs of the Company.

3.2 Organization Units & Accounts

An **OU** is a container of **AWS accounts** within a root of an organization. Organizational units (OUs) are used to group accounts together to administer as a single unit. This greatly simplifies the management of the accounts. Service Control policies will be defined and attached to an OU which will be inherited by all accounts inside an OU. Multiple OUs will be created depending on the need of the company and application functionality requirements.

An Account contains all the AWS and other resources and tools (third part). These resources will be deployed to serve specific environment needs Viz. Prod, Dev, Test etc. and application functionality requirements.

There are two types of accounts in an organization: a single account that is designated as the master account, and member accounts.

Below diagram illustrates the OU and Account structure that will be deployed in Vanguard environment.

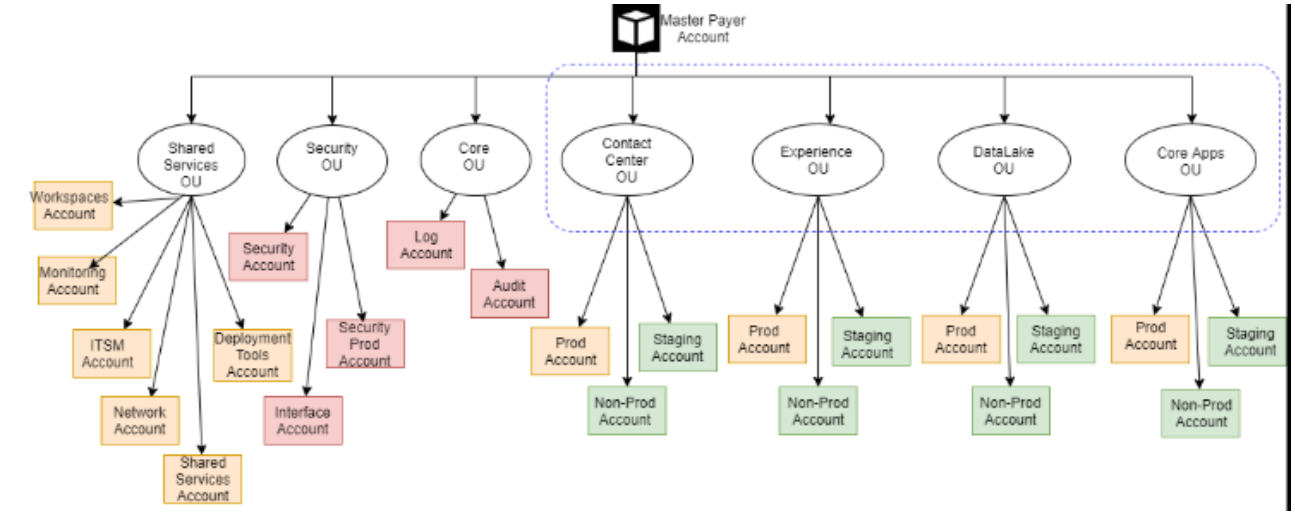


Figure 1 : Vanguard OU & Account Structure

3.3 AWS Regions

AWS Cloud environment for Project Vanguard will be setup in **US East (N. Virginia)** as Primary region and **US West (Oregon)** as Secondary region which will serve as DR site.

AWS Cloud foundation services will be setup in the above regions to cater the needs of the Vanguard. AWS best practices will be incorporated in setting up Cloud Foundation that will include AWS Organizations, Control Tower, Landing Zone, Direct Connect including High Availability, Resilience and Fault Tolerant systems.

AWS Region	Purpose
US East (N. Virginia, US-East-1)	Primary AWS region
US West (Oregon , US-West-2)	DR region

Table 1. AWS Region

3.4 AWS Availability Zones

In order to ensure high availability needs of the Organization, it has been decided to deploy the AWS services in 2 Availability Zones (AZ) in each region.

Also, the AWS foundational services & Organization's Application landscape will be broadly classified under 4 Tiers (Tier 0 – 4) depending on their Business criticality and to take care it's business continuity needs, it has been decided to deploy AWS services across region / AZs as per the below table representation.

AWS Region	Availability Zones	Categorization of Infra , Apps and usage of services across Regions / AZs			
		Tier 0	**Tier 1**	**Tier 3**	**Tier 4**
US East (N. Virginia)	US-East-1A	Y	Y	Y	Y
	US-East-1B	Y	Y	Y	Y
US West (Oregon)	US-West-2A	Y	Y	Y	N
	US-West-2B	Y	Y	N	N

Table 2 : Availability Zones and it's usage

4. Control Tower and related features

4.1 Control Tower

AWS Control Tower will be leveraged in setting up the Greenfield AWS Cloud environment for Vanguard. AWS Control Tower provides the easiest way to set up and govern a secure, compliant, multi-account. With AWS Control Tower, end users on your distributed teams can provision new AWS accounts quickly. Meanwhile the central cloud administrators will know that all accounts are aligned with centrally established, company-wide compliance policies.

Most of the information in this section is directly derived from AWS standardized Control Tower implementation.

Features of Control Tower & it's usage in AWS ME :

Landing Zone – This provides an overview about all resources deployed in Modernized Cloud environment. It's the enterprise-wide container that holds all organizational units (OUs), accounts, users, and other resources that will be subjected to compliance regulation as per organization's need. A landing zone is scalable to fit the enterprise need.

Guardrails - A guardrail is a high-level rule that provides ongoing governance for your overall AWS environment. There are Two kinds of guardrails: preventive and detective

Account Factory – This feature will be used to automate the account provisioning workflow in Cloud environment. Account Factory's configurable account template will be used to provision the new accounts in a standardized and with pre-approved account configurations.

Dashboard – The dashboard offers continuous oversight to monitor provisioned accounts, guardrails enabled for policy enforcement & continuous detection & non-compliant resources (if deployed).

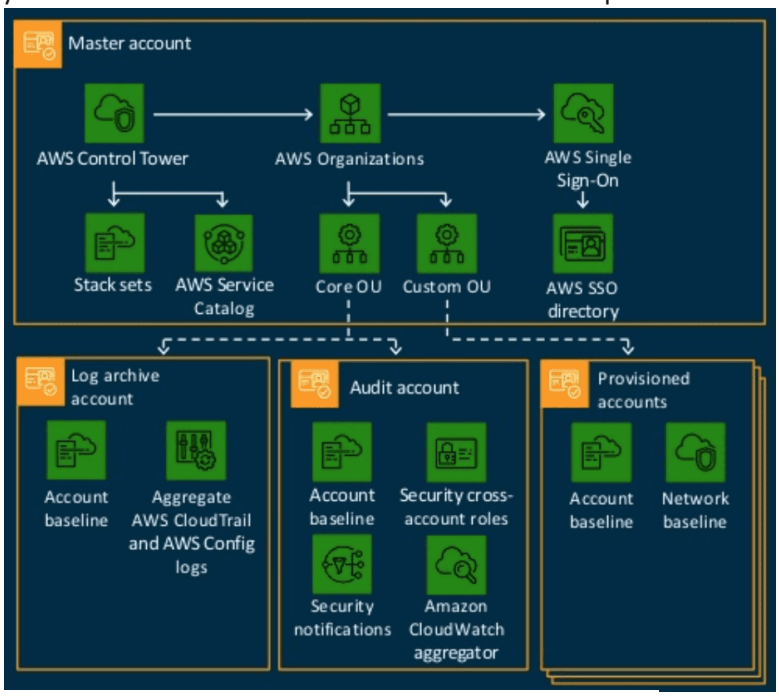


Figure 2 : Control Tower and it's features

Note : For more Vanguard Specific Details on Control Tower - Pls. refer - Section 4 of Project Vanguard OU Structure Technical Design Document v xx.DOC

5. Service Catalog

5.1 Service Catalog Overview

AWS Service Catalog will be used in Vanguard Cloud environment, to centrally manage catalogs of IT services that are approved for use on AWS. These IT services includes everything from virtual machine images, servers, software, and databases to complete multi-tier application architectures.

Deploying the Service Catalog will help in achieving Company's governance and compliance requirements in a consistent manner while enabling users to quickly deploy only the approved AWS services they need.

The Service Catalog provides the following benefits;

Standardization	• Only approved assets could be deployed • Manage & Restrict asset usage in respective accounts • Specified Instance type, configuration options • Standard products across organization
Self-service discovery and launch	• Role based access to different type of Users • Users can List, locate & provision products (services or applications) depending on their access type / levels
Fine-grain access control	• Grant access to users and Groups through IAM • Admins can create portfolios of products from the catalog, add constraints and resource tags to be used at provisioning
Extensibility and version control	• Helps to manage multiple versions of the products in the catalog • Administrators can add a product to any number of portfolios and restrict it without creating another copy • Updating the product with a new version propagates the update to all products in every portfolio that it references

Table 3 : Service Catalog benefits

5.2 Service Catalog adoption - Hub & Spoke Model

Service Catalog will be adopted in Vanguard using Hub & Spoke Model to manage the AWS Service Catalog portfolio and products by a Master Service Catalog Account (Hub) and deploy across multiple child accounts (Spoke) in a controlled manner. A baseline of the products will be created in the Master Account and the portfolio, products along with constraints will be shared with the multiple child Accounts.

- One master account – Creates baseline products and shares the portfolio
- Multiple child accounts – Import portfolios and leverage the products

Products that form the imported master portfolios are added to local portfolios in the child account. Constraints, tags, and users for these products can be added so that users in the child account can deploy any AWS CloudFormation stack implemented as a product.

The usage of Hub and Spoke model is illustrated in the below diagram;

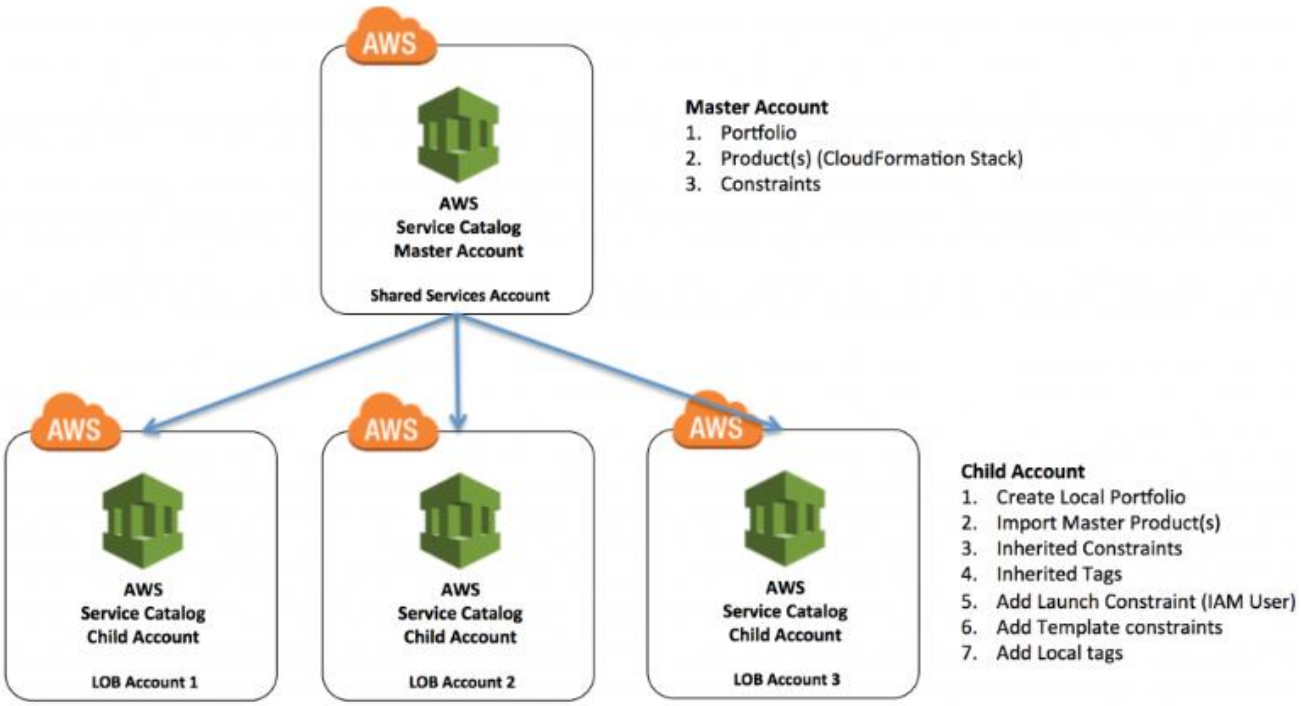


Figure 3 : Service Catalog - Hub & Spoke Model

5.2.1 Standard Parameters of Service Catalog (Will be used in Vanguard – Indicative)

Ref. #	Parameter Description
SC # 001	Granting fine grained permission to Admin and End users
SC # 002	To configure/create the Product through CF Template which define the AWS resources ,relationship between the resources parameter and other attributes requires for the PRODUCT .CF stacks to manage the life cycle of the PRODUCT(CF in YAML format)
SC # 003	Protecting data with encryption at rest and encryption in transit
SC # 004	All the API Calls Captures in AWS Cloud Trail and deliver the log files into Amazon S3 for Auditing purpose .
SC # 005	Maintaining version in Product level instead of creating the new Product .
SC # 006	Define the rules to limit the parameter value for launching Product.
SC # 007	To enable the Auto Tags include tags for the unique identifiers for portfolio, product, user, product version, and provisioned product

SC # 008	Compliance –Aws config (TBD)
SC # 009	Resilience (TBD)
SC # 010	Managing Budget (TBD)

Table 4 : Service Catalog Std. Parameters

5.2.2 Approved AWS Cloud Native Services

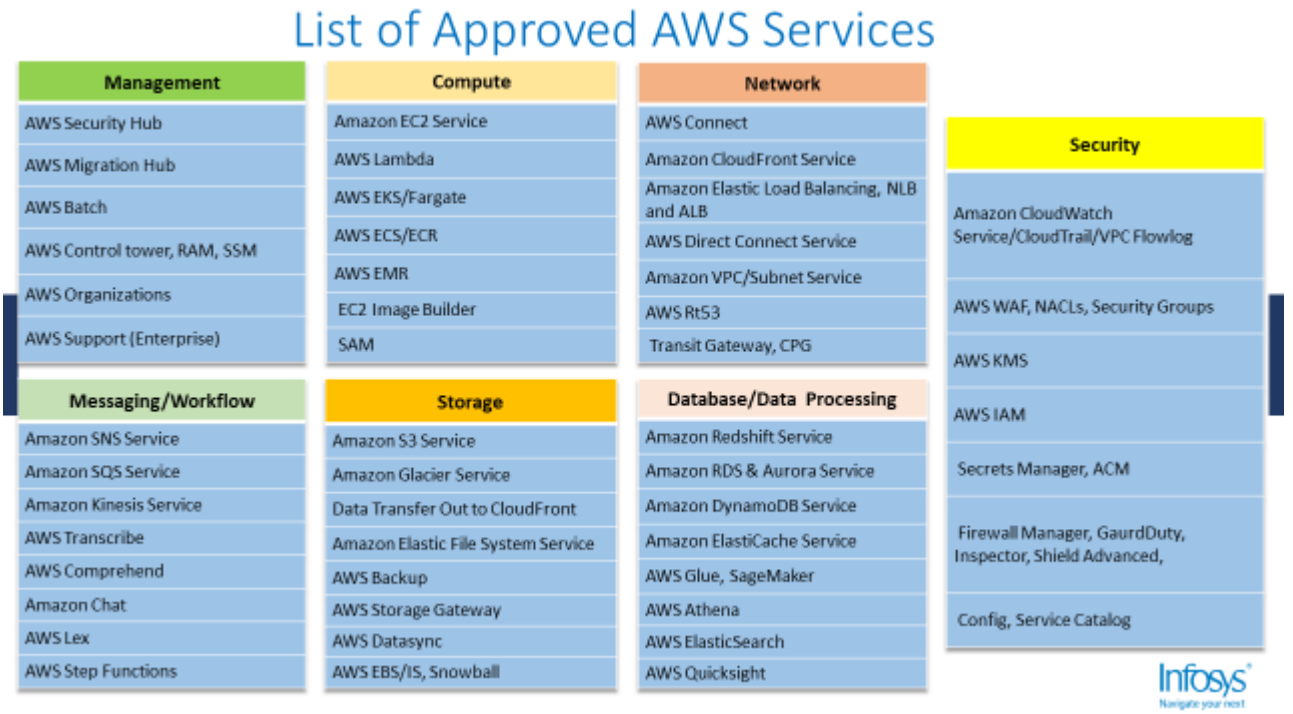


Figure 4 : List of Approved AWS Services

Notes:

- The above list indicates the approved AWS Native services (as per Attachment -12B) that can be used in Vanguard Cloud environment
- These services will be part of the Standard Service Catalog
- Any inclusion of new Service offerings from AWS into the Service Catalog will need to undergo an approval process as defined in Section – 4.2.4

5.2.3 Services used Across Different Account in Vanguard – Indicative

(Legend: Y - Service Used, I – Indicative / TBD)

			Accounts																	
Category	**Services**		**Master**	**Interface**	**Network**	**Log Archive**	**Security**	**Shared Services**	**ODR**	**PE**	**CCE**	**PRS**	**Backoffice**	**CRK**	**Plan Rules**	**Plan Analytics**	**Contact Center**	**DataLake**		
Compute	EC2			I			Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		
	Lambda					Y		Y		Y	Y	Y	Y	Y	Y	Y	Y	Y		
	EKS/Fargate									I	I	I	I	I	I	I	I	I		
	ECS/ECR									Y	Y	Y	Y	Y	Y	Y				
	EMR																	Y		
	EC2 Image Builder																			
	SAM																			
Storage	S3					Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		
	Glacier					Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		
	CloudFront																			
	EFS							Y	Y	Y	Y	Y	Y	Y	Y	Y	I	I		
	Backup			I		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		
	Storage Gateway								I											
	Datasync								I									I		
	EBS- gp, iO1				I	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		
	IS (Instance Store)																			
	Snowball								I											
DB	Redshift																	Y		
	Aurora DB								Y	Y	Y	Y	Y	Y	Y	Y		Y		
	DynamoDB									I	I							Y		
	RDS (MySQL)												I				Y	Y		
	ElastiCache								I	I	I	I	I	I	I	I		Y		
Data Processing	Glue								I	I	I	I	I	I	I	I		Y		
	SageMaker																			
	Athena									I	I	I	I	I	I	I		Y		
	ElasticSearch																	Y		
	Batch								Y	I	I	Y	I	I	I	I		Y		
	Quicksight																	Y		

			Accounts																	
Category	**Services**		**Master**	**Interface**	**Network**	**Log Archive**	**Security**	**Shared Services**	**ODR**	**PE**	**CCE**	**PRS**	**Backoffice**	**CRK**	**Plan Rules**	**Plan Analytics**	**Contact Center**	**DataLake**		
Network	Connect																			
	CloudFront Service																			
	NLB		Y	Y		Y	Y	I	I	I	I	I	I	I	I	I	I			
	ALB					Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y			
	Direct Connect -DX			Y																
	VPC		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y			
	Subnet		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y			
	Route 53		Y	Y	I	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y			
	TGW		Y	Y																
Security	CloudWatch					Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y			
	CloudTrail		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y			
	VPC FlowLog		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y			
	WAF																			
	NACL		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y			
	Security Groups (SG)		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y			
	KMS				Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y			
	IAM		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y			
	Secrets Manager, ACM					Y														
	Firewall Manager					Y														
	GuardDuty	I	I	I	I	Y	I	I	I	I	I	I	I	I	I	I	I			
	Inspector					Y														
	Shiled Advanced					Y														
	Config	I	I	I	I	Y	I	I	I	I	I	I	I	I	I	I	I			
	Service Catalog	Y																		
	Security Hub	I	I	I	I	Y	I	I	I	I	I	I	I	I	I	I	I			

			Accounts																	
Category	**Services**		**Master**	**Interface**	**Network**	**Log Archive**	**Security**	**Shared Services**	**ODR**	**PE**	**CCE**	**PRS**	**Backoffice**	**CRK**	**Plan Rules**	**Plan Analytics**	**Contact Center**	**DataLake**		
Security	Firewall Manager						Y													
	GuardDuty		I	I	I	I	Y	I	I	I	I	I	I	I	I	I	I	I		
	Inspector						Y													
	Shiled Advanced						Y													
	Config		I	I	I	I	Y	I	I	I	I	I	I	I	I	I	I	I		
	Service Catalog		Y																	
	Security Hub		I	I	I	I	Y	I	I	I	I	I	I	I	I	I	I	I		
Messaging / WorkFlow	SNS					I		Y		I	I	I	I	I	I	I		Y		
	SQS					I		Y		I	I	I	I	I	I	I		Y		
	Kinesis					I				I	I	I	I	I	I	I		Y		
	Transcribe																Y			
	Comprehend																Y			
	Chat																Y			
	Lex																Y	Y		
	Step Functions																			
Mgmt.	Control tower		Y																	
	RAM		Y	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I		
	SM		Y																	
	Organizations		Y																	
	Support (Enterprise)		Y																	
	Migration Hub																	Y		
	Account Factory		Y																	
Third Party / Other services	ITSM							Y												
	PolyCloud (IIMS)							Y												
	Dynatrace (APM)							Y												
	AMIs (Market Place)							Y												
	Genesys (SaaS)																Y			

Table 5 : Services Used Across Different Accounts

Notes:

- The Table – 5 shown above is a representative depiction of Approved AWS Services that will be used across Vanguard Cloud environment
- The Service Catalog feature will be used to maintain the Approved AWS Native services
- Portfolios (collection of Products) and Product catalog (collection of AWS Services) will be created and deployed as a best practice which will ease deployment activities across multiple accounts
- These Service Catalog will also be leveraged by Infosys Poly Cloud Platform for controlled deployment of services across various accounts
- The Third party tools that are approved will be part of relevant design Documents

5.2.4 Process for Inclusion of New AWS services into Approved Service Catalog

Any inclusion of new AWS service offerings into the approved Service Catalog list will need to undergo an approval process as described in the below process flow – Fig. 4

The inclusion of services to the Service / Product catalog will be handled as Proactive and Reactive manner

Reactive – Inclusion of any existing AWS services into the existing landscape as an augmentation depending on Application needs.

Proactive – To add any new AWS service offerings which adds value to the existing landscape (process as indicated in below fig.4)

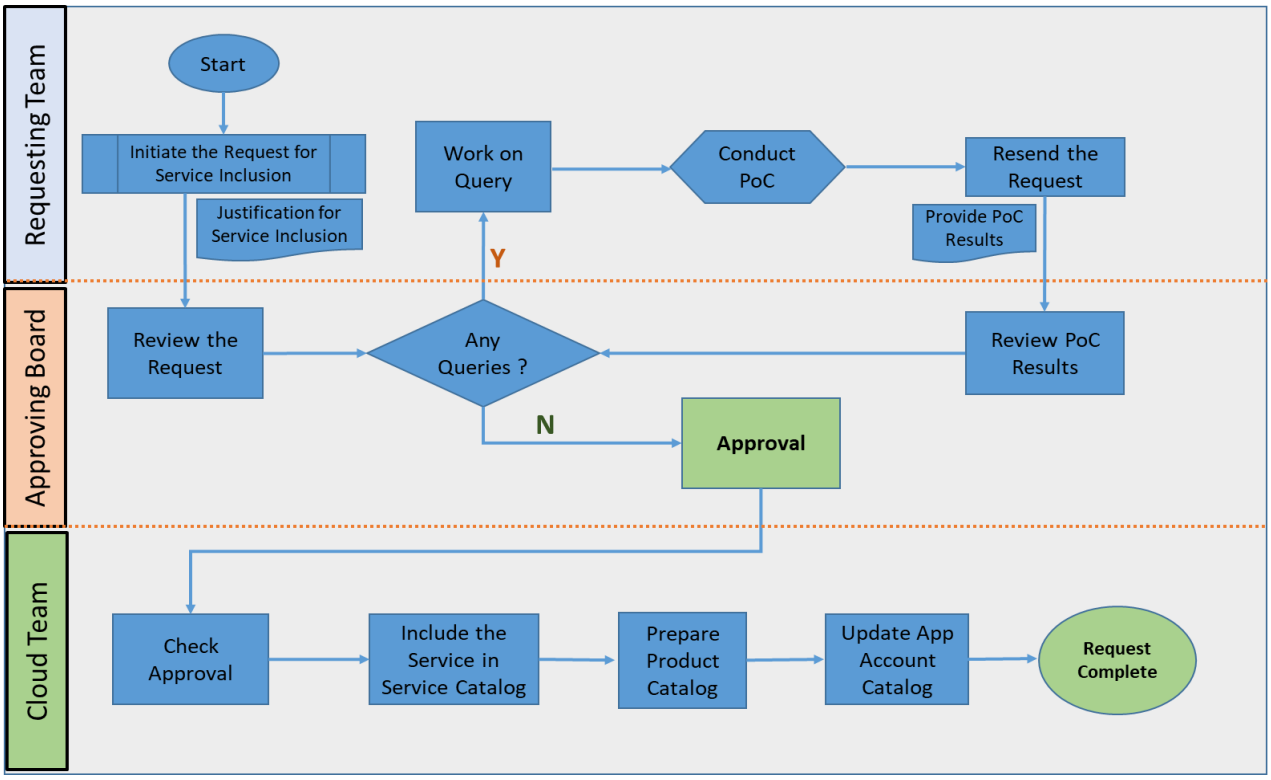


Figure 5 : Process Flow for New AWS Service offerings Inclusion in Service Catalog

Note: Approving Board may involve members from Architecture Review Board, Security and Compliance teams

5.2.5 Process to onboard Third Party Services

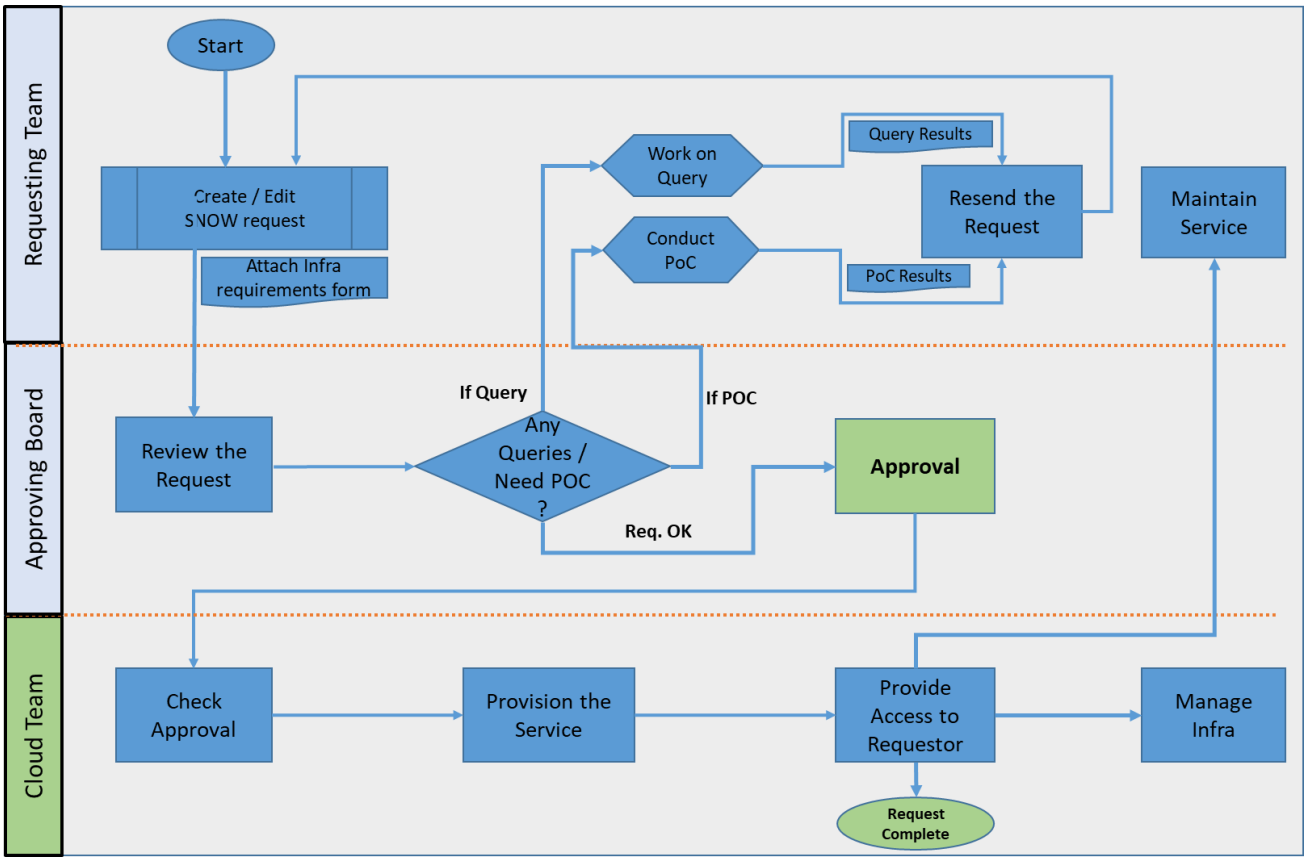


Figure 6 : Process to onboard Third Party Services / Tools

Note: Approving Board may involve members from Architecture Review Board, Security and Compliance teams

5.3 Handling non-functional requirements and AWS services mapping

In order to handle Vanguard non-functional requirements, suitable and proven services will be utilized from the wide range of AWS native services as per non-functional / account specific requirements listed in Table 5.

Below table provides the mapping between non-functional requirement and AWS capabilities

Non-Functional Requirement	AWS Services
Auditing	1. Take advantage of the hosted Platform (AWS IaaS, PaaS) features 2. AWS CloudWatch log, Audit trail 3. VPC Flow Log 4. AWS Inspector
Scalability	1. Take advantage of the hosted platform (AWS IaaS, PaaS) features for scalability 2. Auto scaling 3. Multi AZ /Intra region replication
Security	1. IAM Authentication 2. IAM roles, Groups for Authorization 3. AWS Inspector
Availability and Reliability	1. Take advantage of the AWS IaaS, PaaS platform availability features 2. Autoscaling
Disaster Recovery	1. Take advantage of Multi AZ/Cross region deployments model 2. RDS , EBS Snapshot Backups and S3 replication
Data Encryption	1. Take advantage of KMS (Key Management Systems)
Patching	1. Automated Patching using AWS systems Manager
Authentication	1. MS Active Directory on EC2 instance

Table 6 : AWS Capabilities for Non-Functional Requirements

6. Account Overview

6.1 Shared services Account

Shared services Account will be created under Shared Services OU to host common services that are shared among application and other accounts. The common services that will be placed in the Shared services include;

- Application Monitoring (Dynatrace) related services (Instances, DB etc.)
- Infosys Poly Cloud – Poly Cloud related services (Instances, DB etc.)
- ITSM – Servicenow related services (Instances, DB etc.)
- Testing – Testing related services (Instances, DB etc.)
- Golden AMIs
- Service Catalog portfolios that are shared with Application Accounts
- MS Active Directory on Ec2 launched instances with cross region replication

6.2 Log Archive Account

Log Archive Account is one of the default Account that gets created when a Control Tower is deployed in the environment.
This account works as a repository for logs of API activities and resource configurations from all accounts in the landing zone. These log files allow administrators and auditors to review actions and events that have occurred.
The following AWS resources are created within the Log Archive Account during Control Tower setup.

AWS service	Resource type	Resource Name
CloudFormation	Stacks	StackSet-AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-READ-PROHIBITED-StackSet- AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-WRITE-PROHIBITEDStackSet- AWSControlTowerBP-BASELINE-CLOUDWATCH- StackSet-AWSControlTowerBP-BASELINE-CONFIG- StackSet-AWSControlTowerBP-BASELINE-CLOUDTRAIL- StackSet-AWSControlTowerBP-BASELINE-SERVICE-ROLES- StackSet-AWSControlTowerBP-BASELINE-ROLES- StackSet-AWSControlTowerLoggingResources-
Config	AWS Config Rules	AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_READ_PROHIBITED AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_WRITE_PROHIBIT
CloudTrail	Trails	aws-controltower-BaselineCloudTrail
CloudWatch	CloudWatch Event Rules	aws-controltower-ConfigComplianceChangeEventRule
CloudWatch	CloudWatch Logs	aws-controltower/CloudTrailLogs /aws/lambda/aws-controltower-NotificationForwarder
Identity and Access Management	Roles	aws-controltower-AdministratorExecutionRole aws-controltower-CloudWatchLogsRole

AWS service	Resource type	Resource Name
		aws-controltower-ConfigRecorderRole aws-controltower-ForwardSnsNotificationRole aws-controltower-ReadOnlyExecutionRole AWSControlTowerExecution
Identity and Access Management	Policies	AWSControlTowerServiceRolePolicy
Simple Notification Service	Topics	aws-controltower-SecurityNotifications
Lambda	Applications	StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-*
Lambda	Functions	aws-controltower-NotificationForwarder
Simple Storage Service	Buckets	aws-controltower-logs-* aws-controltower-s3-access-logs-*

Table 7 : AWS Resources List in Log Archive Account

6.2.1 Centralized Log Management

As per the design and security best practices, the below-mentioned AWS service logs will be integrated for log analysis / monitoring purpose and the below logs will be configured in the Log Archive Account for the purpose of auditing and compliance needs.

a) CloudTrail Logs (for AWS API Access)
b) VPC Flow Logs
c) R53 Logs
d) ELB Access Logs

6.2.1.1 CloudTrail

CloudTrail is an AWS service that helps to enable governance, compliance, and operational and risk auditing of AWS accounts.

CloudTrail logs all requests for AWS resources within an account & the below mentioned trails for each event can also be captured which are useful for audit & compliance purpose;

- What service was accessed
- What action was performed
- Who made the request

The events include, sign-in events, API calls made via AWS Management Console, AWS Command Line Interface (CLI), and AWS SDKs and higher-level AWS services (such as AWS CloudFormation).

Once the CloudTrail is enabled, event logs are usually flushed every 5 minutes. But it can take up to 15 minutes to deliver logs of an API call. CloudTrail will be configured in US-East-1 and US-West-2 regions so that it aggregates log files from these two regions into a Central Location (S3 bucket)

AWS CloudTrail includes the following high level points which is depicted in the architectural diagram below:

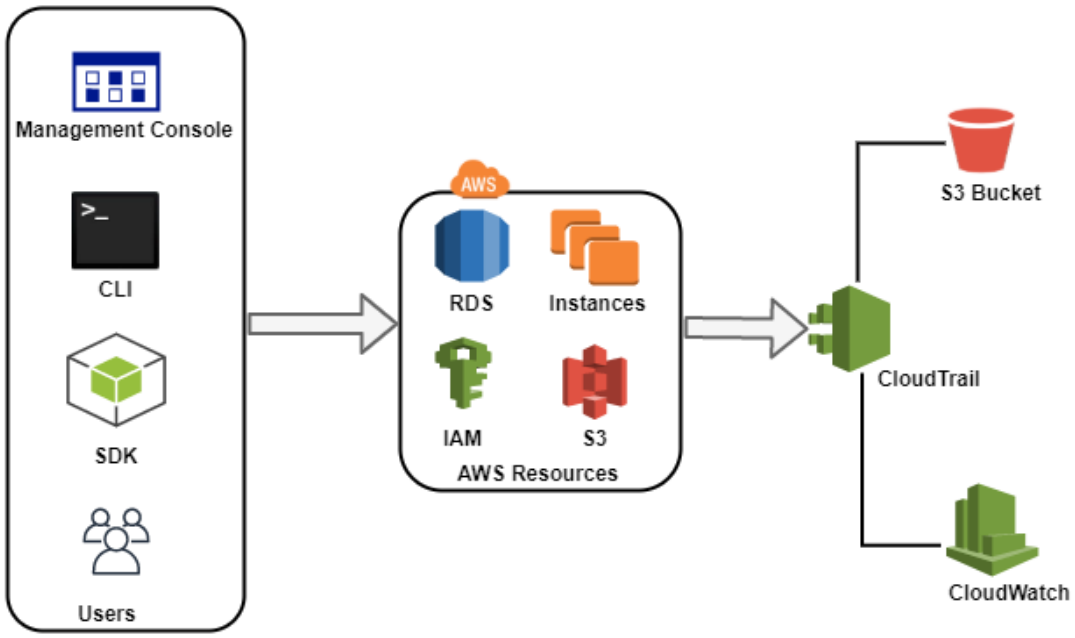


Figure 7 : CloudTrail Architecture

- CloudTrail tracking includes calls made by using the AWS Management Console, AWS SDKs, command line tools and higher-level AWS services (such as AWS CloudFormation)
- AWS CloudTrail captures AWS API calls and related events made by or on behalf of an AWS account and delivers log files to specified S3 bucket (TBD yet)
- CloudTrail can be configured, optionally, to deliver events to a log group to be monitored by CloudWatch Logs
- Log files contain API calls from all CloudTrail Supported Services

The CloudTrail logs will be collected, stored & retained as per the process defined in Section 6.2.2

Below is the flow diagram depicts how CloudTrail records API calls to the Amazon services.

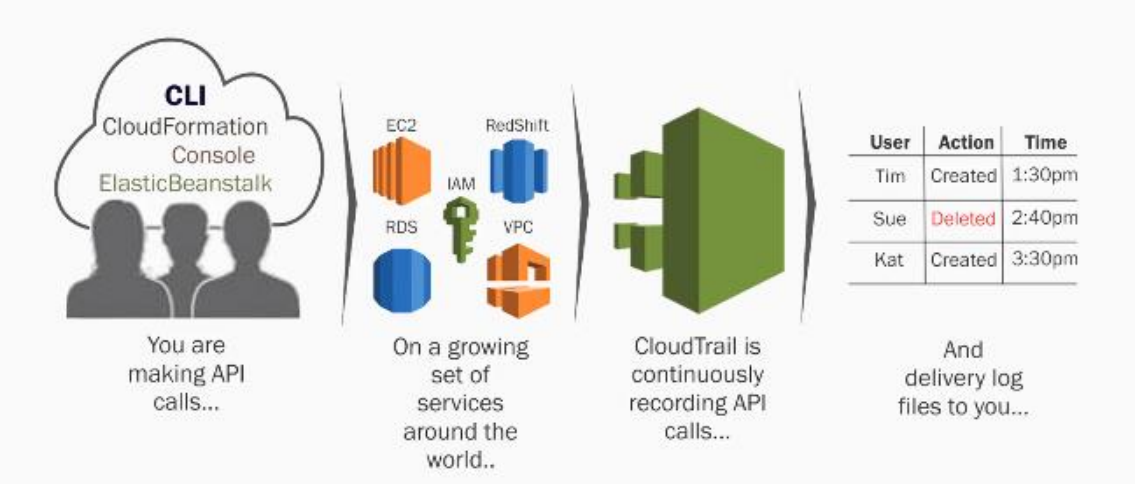


Figure 8 : CloudTrail Flow Diagram

Design considers configuring AWS CloudTrail to deliver events to a log group monitored by CloudWatch Logs which is a feature of CloudWatch. CloudTrail events that are sent to CloudWatch Logs can trigger alarms according to the metric filters.

CloudTrail is a regional service. It creates trails in each region separately. By default, these trails include information for events that occur in those regions, plus events from global services such as IAM and AWS STS (Security Token Service)

6.2.1.2 VPC Flow Logs

VPC flow Logs will be enabled for all VPCs deployed in Vanguard environment to capture information about the IP traffic going to and from network interfaces in a VPC. VPC Flow log data will be published to CloudWatch log groups & to store these logs for Compliance and Audit purpose as per the process defined in Section 6.2.2

Flow Logs will be configured to capture & monitor (thro' CloudWatch) the below mentioned events for VPC, subnet or network interfaces

- The resource to capture the flow logs
- The type of the traffic Viz. Accepted Traffic, Rejected Traffic or all Traffic
- The destination to store the flow log data

Depending on the need, VPC flow log will be created for the following AWS resources with the maximum aggregation interval of 10 mins.

- EC2 Instance
- Elastic Load Balancing
- Amazon RDS
- Amazon ElastiCache
- Amazon Redshift
- NAT gateways
- Transit gateways

The VPC Flow logs will be collected, stored as per the process defined in Section 6.2.2

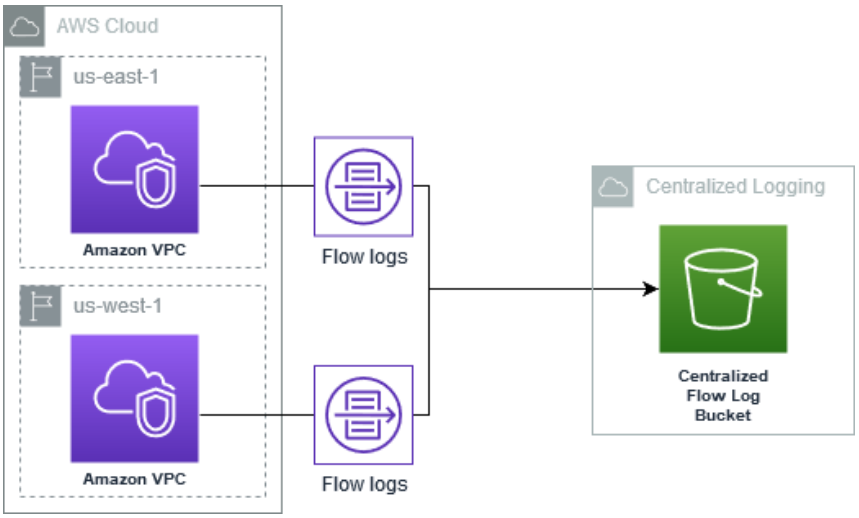


Figure 9 : VPC FlowLog Architecture

6.2.1.3 Elastic Load Balancer (ELB) Access Logs

Access logging is an optional feature of ELB that is disabled by default. If need be, the logging will be enabled on ELB.

Elastic Load Balancing provides access logs that capture detailed information about requests sent to the load balancer. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. The access logs can be used to analyze traffic patterns and troubleshoot issues.

The ELB logs will be collected, stored & retained as per the process defined in Section 6.2.2

6.2.2 Centralized Log Management

For the purpose of having Centralized Log Management requirement, Log Archive Account will be utilized to collect and store various types of logs so that these logs can be utilized for security, monitoring or analytics purposes.

The logs received from various accounts. resources will be stored in a Centralized Log store, manage and enforce restrictions for the logs collected. Depending on the compliance requirements backup and life-cycle policy will be setup for long term retention.

The Log Management is as described in the below process flow.

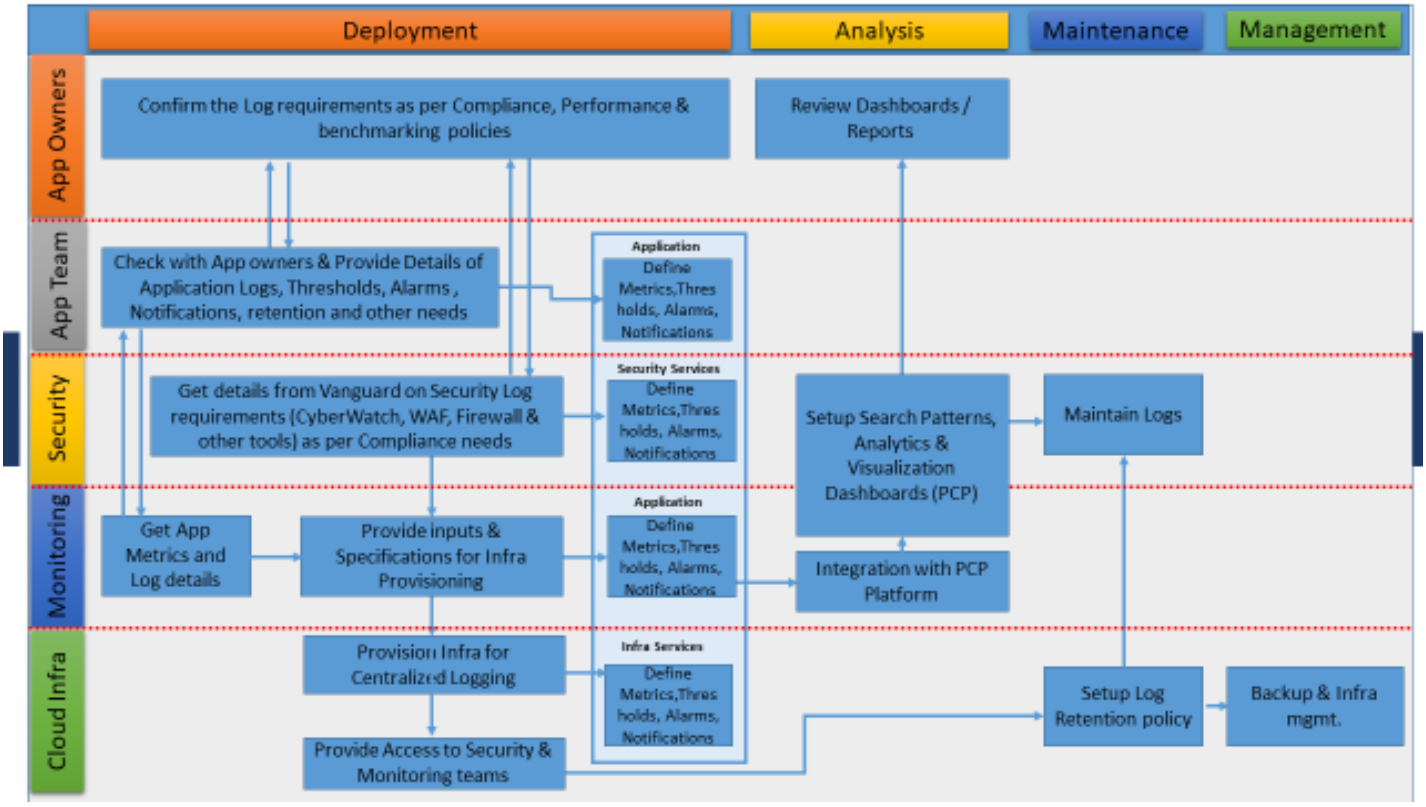


Figure 10 : Centralized Log Management Process Flow

6.3 Application Account

Depending on the close relation & the dependencies the applications has in Vanguard Application Landscape, various application accounts will be created and the same is described in details in the Design Document - ***OU & Account Structure Technical Design***

6.4 Network Account

Network Account will hold the services like Transit gateway (TGW), DX (Direct Connect) Gateway, R53, R53 resolver etc.

The detailed explanation of all Network services, configurations could be found in ***Network Design Document***

Connectivity from Vanguard On-Prem DC to AWS Modernized Cloud Environment

The network Account will have all the services that are needed to handle the Traffic from Vanguard On-prem DC to Modernized AWS Cloud Environment and the same is as explained in the below diagram

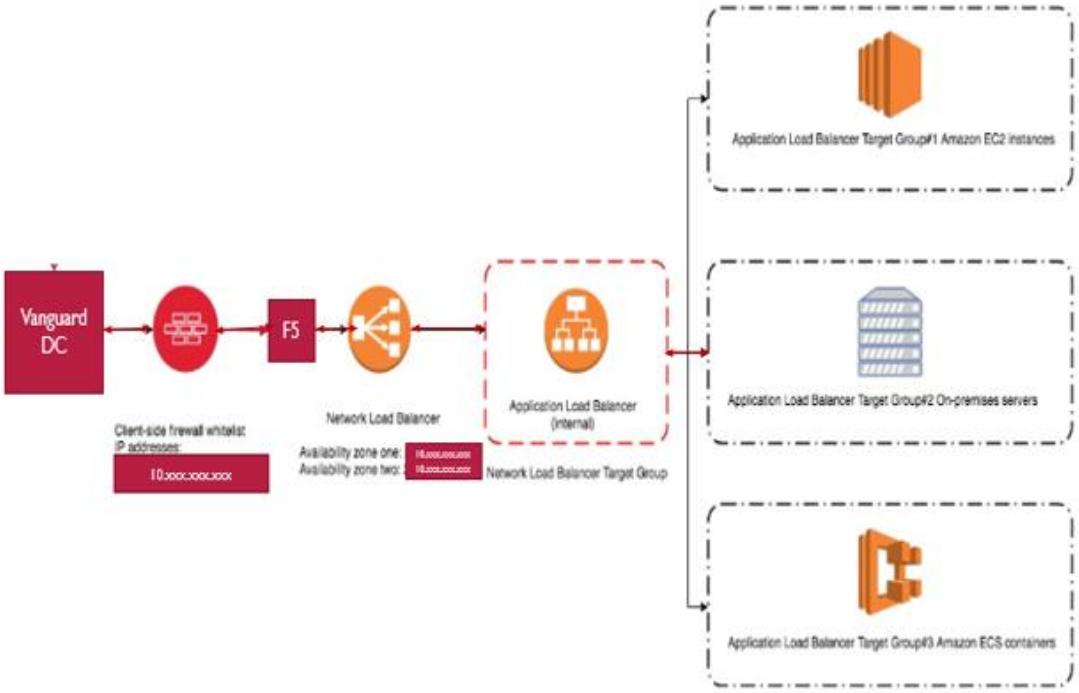
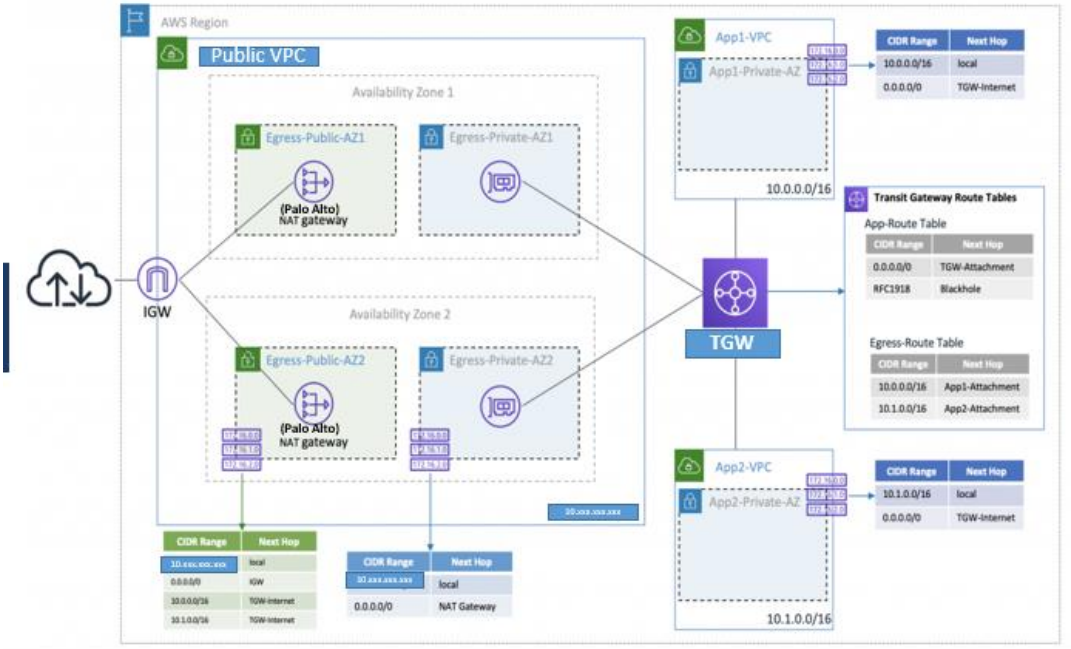


Figure 11 : Traffic from Vanguard DC - AWS Cloud Modernized Environment

- F5 load Balancer in Vanguard DC forwards the traffic to the AWS NLB
- The NLB placed in the individual Accounts, will be configured with a static IP, the individual NLBs static IPs will be whitelisted in Vanguard DC firewall
- TCP listener on a NLB accepts traffic and forwards it to an internal ALB
- The ALB terminates TLS, examines HTTPS headers, and routes requests based on the configured rules to target groups with Cloud instances, servers, or containers.
- AWS Lambda function will be configured which will keep IP addresses of ALB in sync by watching the ALB for IP address changes and updating the NLB target group.

6.5 Interface Account (Public Account)

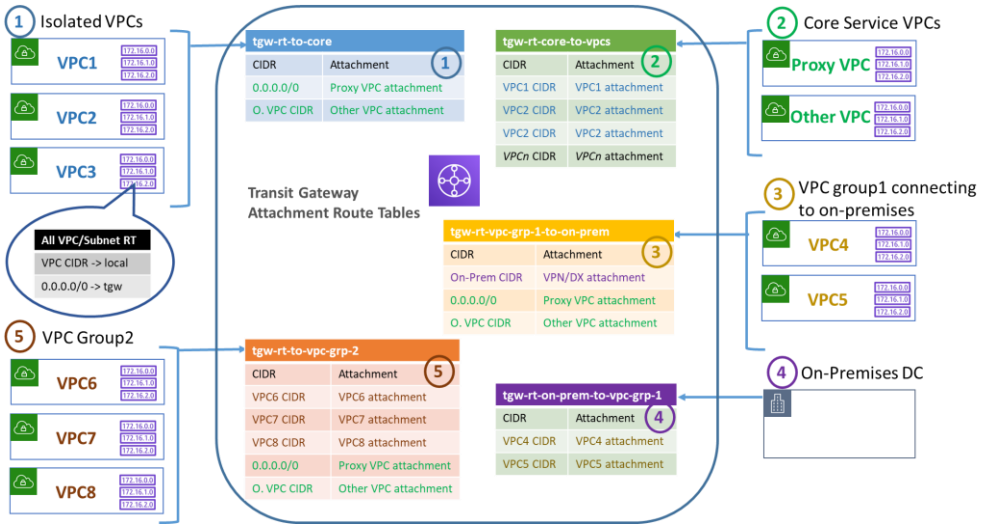
6.5.1 Connectivity from AWS Modernized Cloud Environment to Internet



The above diagram illustrates how to centralize outbound internet traffic from many VPCs without compromising VPC isolation.

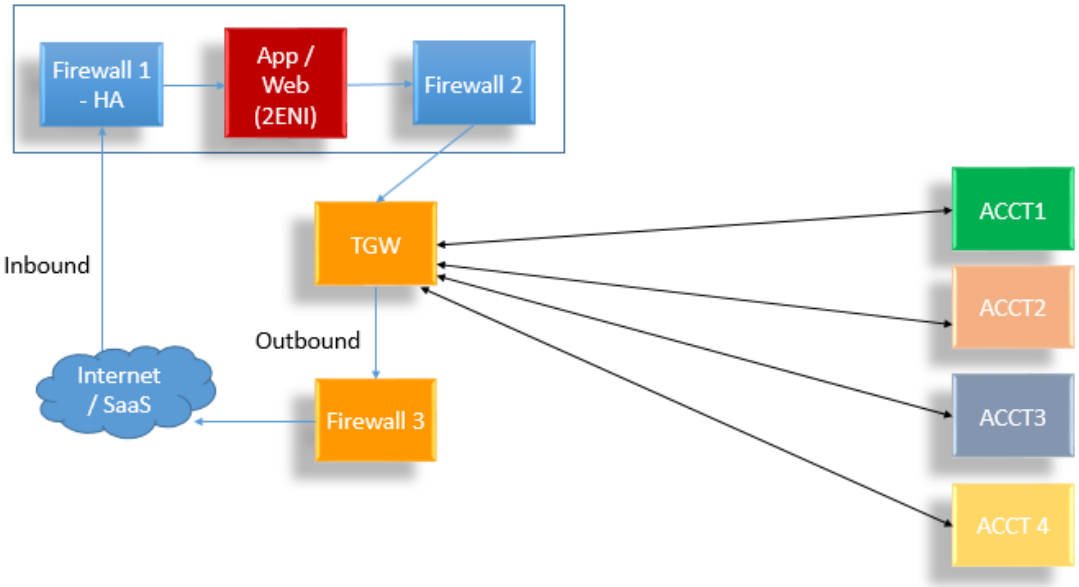
- Transit Gateway will be used to configure a single VPC with multiple NAT gateways (using Palo Alto firewall NAT functionality) to consolidate outbound traffic for several VPCs
- Multiple route tables will be created within the transit gateway to maintain VPC-to-VPC isolation
- Through Hub & Spoke design, all outbound internet communication from AWS environment will be managed from Public VPC in the Interface account

6.5.2 Transit Gateway routing domain



The above diagrams explains how the traffic from different VPCs will be channelized through a Transit Gateway by creating different route tables for different VPC attachments

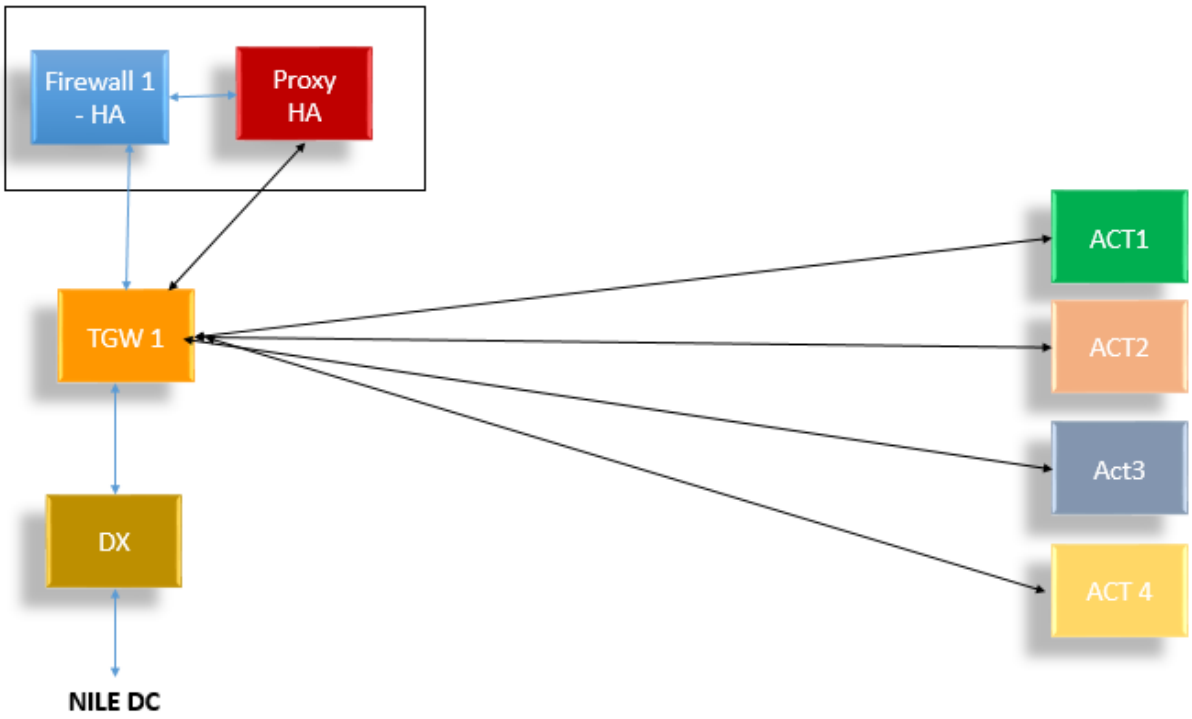
6.5.3 DMZ Full ((To access Internet thro' DMZ))



The DMZ Full will be configured to handle Internet traffic to & from AWS Cloud environment

1) The traffic from the Internet will first go to the Palo Alto before it reaches the TGW
2) Palo Alto will perform the Natting
3) TGW will in turn routes the traffic to the destination
4) Palo Alto in each AZ which will be in Active – Active mode

6.5.4 DMZ Lite (To access Vanguard On-Prem thro' DMZ)



The DMZ Lite will be configured to handle the traffic between Vanguard On-Prem to AWS Cloud thro' DMZ

1) Traffic from On-Prem DC will first go to Palo Alto Firewall before it reaches TGW
2) Palo Alto will perform Natting
3) Palo Alto in each AZ which will be in Active – Passive mode
4) VPC attachment will be created from the DMZ Lite VPC to the Transit Gateway to handle the On-Prem – AWS Modernized environment traffic

7. Deployment Architecture

7.1 Deployment Decision

Design Decision # 1
Objective – 1) Deployment Architecture using separate Deployment Accounts in Non-Prod and Prod environment 2) Usage of source code or Compiled code for deployment purpose
Decision Description – Compiled code will be used in Vanguard for deployment purpose as the Compiled code will be the authorized and tested one in the Non-prod environment
Rationale – 1) Even though the same compiled code should be generated for the same source code every time we go through the compilation process, it is safer to transfer Compiled code rather than Source code because 'that' Compiled Code is certified to upgrade to Prod. 2) The Security and testing tools like Sonarcube, Inspector that the source code goes through will remain the same in Non-Prod and Prod. Therefore, there is no additional advantage in compiling the code again in Prod Deployment account. If there are any sleeper bugs etc., It'll be caught at the Non-Prod level, if that did not happen, then it can't be caught at the Prod level also, because the same rules/checkpoints are used both in Prod and Non-prod. 3) Save compilation time if Compiled code is moved rather than Source code

7.2 Replication Process for Code Deployment

Option 1	Option 2	Option 3
Developer checks in manually in both the Non-Prod accounts of different regions - A/A configuration	Developer checks-in in N. Virginia and then automatically copied to Oregon (snapshot, CRR from S3)	Developer checks-in in N.Virginia and code is deployed into both regions from the N.Virginia instance of Jenkins
i. This is consistent with Apps configuration since they are in A/A configuration. ii. Higher availability - How often do we need to check in code in the event of a disaster? Prioritization of Recovery operations. iii. Manual check-ins is a double-edged sword. We can stop any issues from percolating. But if not done right, then systems will be out-of-sync	i. It is similar to the A/P setup, there may be delay in bringing it up in the event of N. Virginia region shuts down. ii. It is not consistent with the apps that are in A/A configuration. Do we really need deployment plans to be in A/A setup for these apps?	i. Snapshots will be copied into Oregon for recovery operations. No Deployment assets in Oregon. ii. This is typical Pilot Light or Backup and Restore setup and IPP will be used to deploy the assets in case N. Virginia goes down.

7.3 Deployment Approach # 1

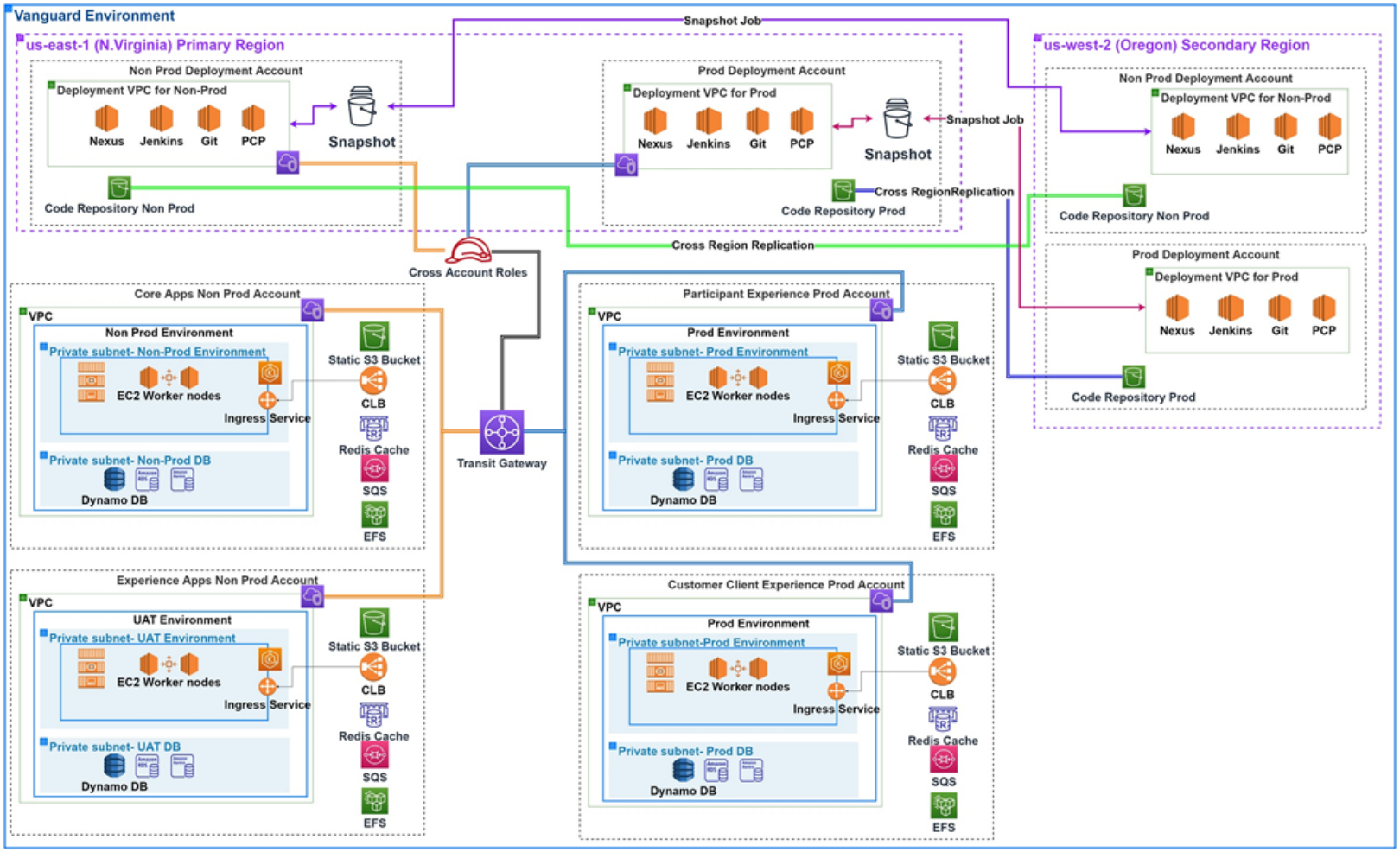


Figure 12 : Deployment Architecture # 1

The Deployment architecture shown in Fig 12, is explained as below;

- Deployment Account will be setup in Shared Services OU
- Deployment account will have Nexus (Compiled code repo), Git (Source code repo) , Jenkins (Deployment Jobs) & Inspector
- Infosys Poly Cloud will be in the SS OU
- Infosys Poly Cloud will be leveraged to deploy the services, Infrastructure & Application codes – ***For more information on PCP refer the Design Document << >>***
- There will be two sets of deployment components placed in different accounts to handle Non-prod and Prod environment deployments
- The resources will be provisioned in US-East 1 and US-West 2
- Cross Account roles will be established for the deployment account to provision resources across all the target accounts in both the regions
- Inter VPC connectivity will be established using Transit Gateway
- The codes deployed in the Primary region from the deployment account will have the copy shared to the Secondary region to function during disaster recovery
- Upon successful deployment & testing in UAT environment, the compiled code in the code repository is considered as approved and ready to be deployed in PROD environment
- Production Deployment account will have an IAM role to access the approved and compiled codes (used in UAT environment) from the code repo to deploy in PROD accounts
- The Source and compiled code repositories of Non-Prod and Prod deployment accounts of the Primary region will be synchronously replicated to the respective deployment accounts in the Secondary region for the purpose of DR
- For all Tier 0 and 1 application; to maintain Active-Active mgmt.. consistency in release management, the instances will be up and running and the plans will be engaged in the event of DR

7.4 Deployment Approach # 2

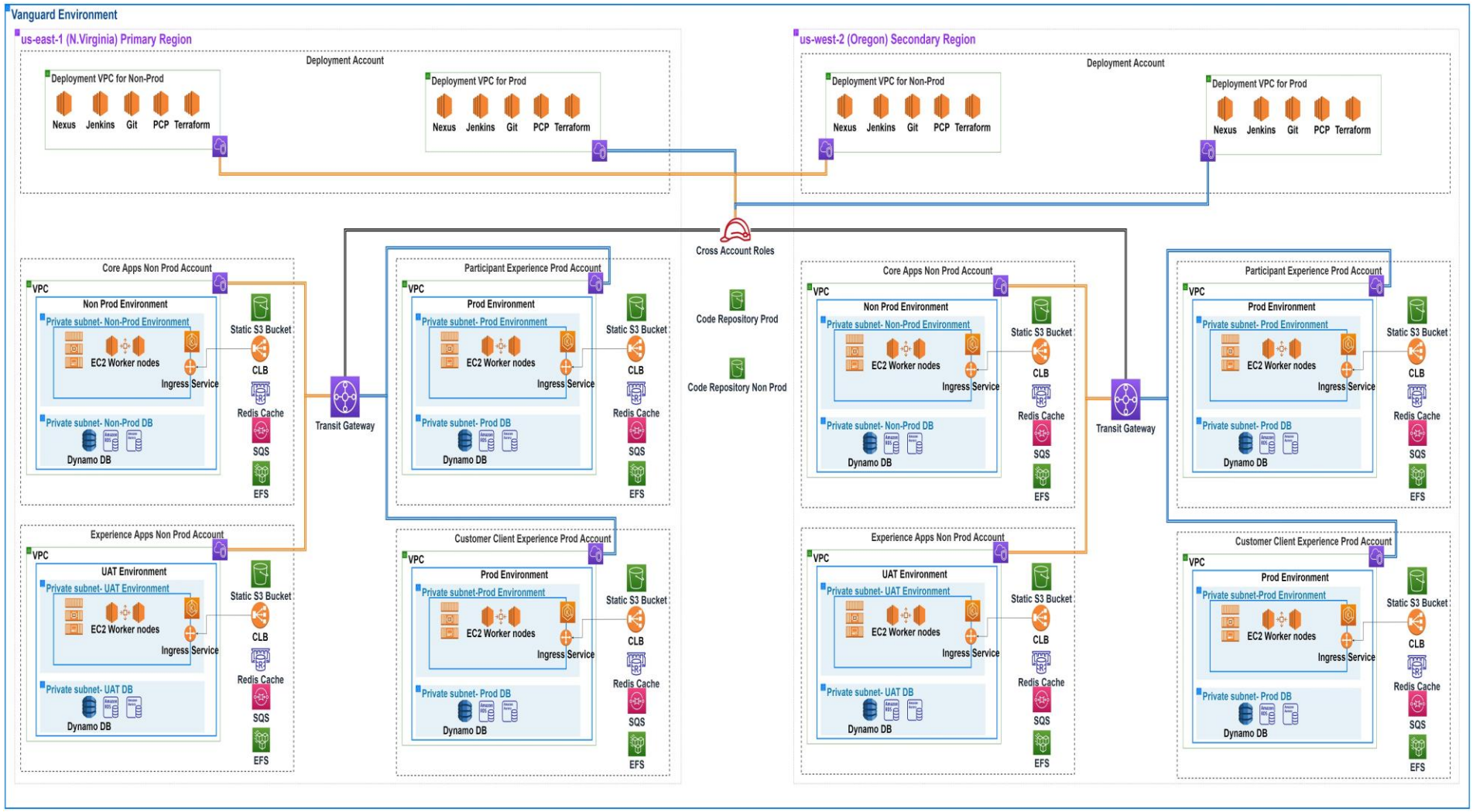


Figure 13 : Deployment Architecture # 2

The Deployment architecture Approach # 2 shown in Fig 13, is explained as below;

- Deployment Account will be setup in Shared Services OU
- Deployment account will have Nexus (Source code repo), Github (Compiled code repo) , Jenkins (Deployment Jobs) & Inspector
- Infosys Poly Cloud will be in the SS OU
- Infosys Poly Cloud will be leveraged to deploy the services, Infrastructure & Application codes – For more information on IPP (Infosys Poly Cloud Platform) refer the IPP Design Document
- There will be two sets of deployment components placed in different accounts to handle Non-prod and Prod environment deployments
- The components in deployment accounts will be provisioned in US-East-1 and US-West-2
- The deployment code will be checked-in both the regions in the code repository with US-East-1 as the Master, the Jenkin jobs will run in both the regions simultaneously to provision resources in their respective regions
- Cross Account roles will be established for the deployment account to provision resources across all the target accounts in both the regions
- Inter VPC connectivity will be established using Transit Gateway
- Upon successful deployment & testing in UAT environment (considered as last Non-prod phase), the deployment codes (artifacts) will be pulled by the Nexus instance (in the Production deployment account)
- The Production Deployment account will have IAM roles to access the resources in the Non-production
- Using the copied artifacts from UAT, the resources will be deployed in Production environment using Production Deployment account

8. Infrastructure (Service) Compliance and Monitoring

8.1 Config Rules

AWS Config service can be leveraged to view the list of AWS resources associated with AWS Cloud accounts. The resources will be deployed in accordance with Organization's approved configuration metrics. Using Config Rule dashboards, an insight of change in configurations of resources and their relationships over the period of time can be visualized.

Config rules will also be used to assess whether the resource configurations comply with Organization's internal practices, industry guidelines and regulations.

As a best practice, the Config Rule will be set in the Master Account to evaluate the list of non-compliant and compliant resources based on the resource ID and Account ID from the child accounts.

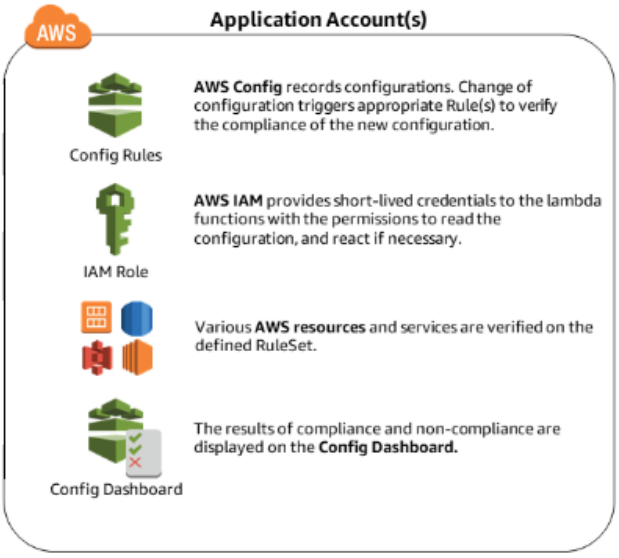


Figure 15 : Config Rules

The above diagram illustrates an overview of Config Rules for AWS resources and describes any deviation from the Config rules are captured and displayed in dashboards in a particular account.

Depending on Company's requirement, Config Rules will be defined for each of the services:
Ref : Appendix 1 – Config Rule

Config Service allows to create upto 150 rules per region in each account. Depending on Company's requirement, a custom rule set will be configured to monitor the compliance status of the rules and resources. Config dashboard will display the list of resources violating the defined Config Rules for various accounts as flags it as non-compliant.

8.2 Infrastructure Monitoring – CloudWatch

AWS Native CloudWatch service will be used to monitor standard Infrastructure metrics in Modernized environment

CloudWatch has a capability to monitor, collect and track metrics logs and actionable insights to monitor and respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health across AWS native services Viz. – EC2, S3, EBS, EFS, ECS, ELB etc.

8.2.1 CloudWatch Key Functions

CloudWatch monitoring service will be configured in <Company's> AWS modernized Cloud environment to perform the below unique actions;

- To provide data in forms of the logs, Metrics and Events, and actionable insights to monitor AWS Cloud services / resources to run it smoothly
- To Optimize the resources utilization

The functional overview of CloudWatch is depicted in the below diagram;

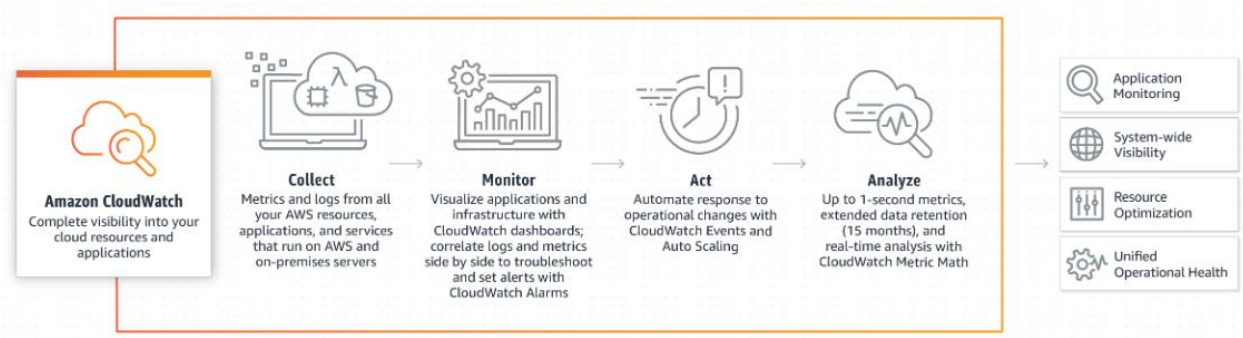


Figure 16 : CloudWatch Functions Source : AWS

Below table depicts some of the native AWS resources where Cloudwatch will be configured to monitor, collect and track Metrics, collect and monitor logs, create alarms to send notifications and initiate appropriate changes to the resources based on the rules configured.

List of AWS services that will be monitored using CloudWatch

AWS Services
Amazon EC2 instances
EKS Clusters , Containers
S3

EBS volumes
Elastic Load Balancers
Auto Scaling groups
RDS DB instances
DynamoDB tables
ElastiCache clusters
RedShift clusters
Route 53 health checks
Storage Gateways
Lambda

Table 8 : AWS Services for CloudWatch Monitoring

The monitoring tasks for above services in the table will be automated to receive notifications when significant events occur. Automation will be built to take action when thresholds are breached / failure is detected, e.g., to replace failed components.

8.2.2 Illustration of CloudWatch functionality

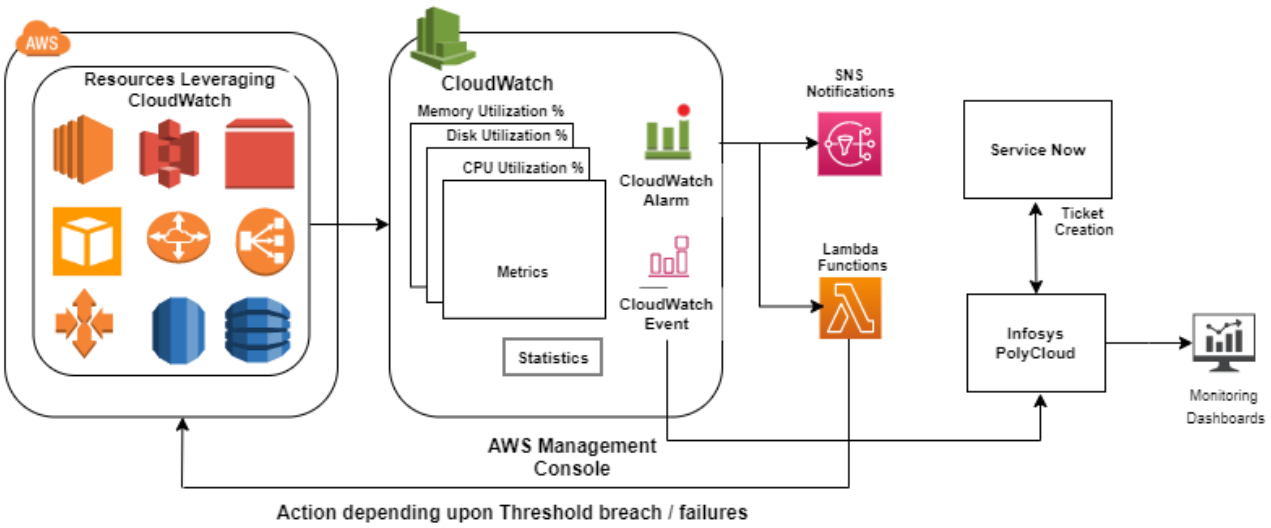


Figure 17 : CloudWatch Functionality

Following points describes CloudWatch functionality as depicted in the diagram:

- AWS resources i.e. EC2 Instances, Amazon RDS DB instances, load balancers etc. will use AWS CloudWatch service for monitoring
- Default and custom metrics will be defined to monitor the resources (Refer Table – 8)
- CloudWatch starts collecting monitoring and operational data in the form of Logs from resources, Metrics and events

- CloudWatch automated dashboards will be leveraged to get unified view of metrics and events for AWS resources
- Alarms for threshold values will be set for resource metrics & automated actions will be configured if alarm gets triggered. This action is described in the below example;
- EC2 instance Auto Scale-in or Scale-out action will be performed by ASG(Auto scaling group), if the EC2 instance's CPU utilization crosses 75% - the threshold value set for an alarm to trigger
- An Amazon Simple Notification Service (SNS) will be used to notify the concerned teams for any alarm and it's action

8.2.3 Monitoring Metrics (Infra level) for Non-Production & Production Environment [Indicative]

Following table indicates some of the common metrics that will be configured for Infra services with Threshold values and appropriate Alert durations in both Non-Prod and Prod environments.

The list of Metrics for other AWS services may be found at Appendix 2 and metrics will be configured depending on the specific need in the environment.

Sr No	Metric Type	CloudWatch Metric	Threshold for Alert in Non-Prod	Threshold for Alert in Prod
1	Elastic Compute Cloud (EC2)	CPU Utilization %	Avg of 15 mins, > 80%	Avg of 5 mins, > 80%
		Disk Space Utilization	Avg of 15 mins, > 80%	Avg of 5 mins, > 80%
		Memory Utilization	Avg of 15 mins, > 85%	Avg of 5 mins, > 85%
		System state Check	2 consecutive failures	2 consecutive failures
2	ELB	UnHealthyHostCount	> 0	> 0
3	RDS	CPUUtilization	Avg of 15 mins, > 80%	Avg of 5 mins, > 80%
		Freeable Memory	Avg of 15 mins, > 80%	Avg of 15 mins, > 80%
		Swap Usage		
		ReplicaLag	only if Read replica used (>600ms)	only if Read replica used (>600ms)
4	DynamoDB	ConsumedReadCapacityUnits	> 80%	> 80%
		ConsumedWriteCapacityUnits	> 80%	> 80%
5	S3	BucketSizeBytes		
		NumberOfObjects		

Table 9 : Monitoring Metrics - Production

8.2.4 SNS Topic configuration for Notifications (Option 1)

An SNS topic will be setup to send notifications to the Group Email ID (or to the concerned stakeholders), when an alert is triggered indicating breach of threshold values set for respective services as described in Table 10

Alarm Name	SNS Topic Name	Email Id
Instance name-parameter	<< TBD >>	<<TBD >>

Table 10 : SNS Configuration

8.2.5 SQS configuration for Notifications (Option2 - TBD)

SQS queue will be setup to receive CloudWatch Events in JSON format, which will act as a trigger to invoke a Lambda function which will in-turn send a API request to SES to send mails to recipients

Figure 18 : CloudWatch Events with SQS

8.2.6 Integration of CloudWatch with PolyCloud

The CloudWatch will be integrated with IIMSS for handling any events of any resource failure or malfunction. IIMS provides the comprehensive solution to capture all kind of alerts, and events across Infrastructure Devices, Security, Application, etc., and enables centralized monitoring workbench, alert management and provide persona based operational workbench. Event Actions configurations in Monitoring tool or IIMS adapters and data agents on CloudWatch, Cyber Watch & Dynatrace

Further, IIMS is integrated with SeviceNOW for auto incident creation for valid alerts, which needs to acted upon and tracked to closure.

Refer : IPP Design Document

8.2.7 CloudWatch Metrics Retention (Std. offering)

By default, CloudWatch data point retention is as follows;

Data point Frequency	Retention Duration
< 60 Seconds (for high resolution custom metric)	3 hrs.
60 Seconds	15 Days
300 Seconds (5 Min)	63 Days
3600 Seconds (1 hr)	455 Days

Table 11 : CloudWatch Log Retention

- PutMetricData API request will be defined to collect and store high-resolution metrics during data aggregation while storing
- GetMetricStatistics API will be defined to retrieve datapoints for offline storage

8.2.8 CloudWatch Logs Storage

An S3 bucket <<S3 bucket name >> will be created to export the CloudWatch logs for offline storage in an encrypted manner. Using Life Cycle policy this can be further sent automatically to low cost storage Viz. S3 IA or Glacier and could be deleted as per the policy needs

8.2.9 CloudWatch: Cross-Account Cross-Region Functionality [TBD]

Cross-Account Cross Region functionality will be configured in CloudWatch console. This functionality provides visibility to dashboards, alarms, metrics, and automatic dashboards across various accounts from a designated monitoring account.

As a best practice, one or more accounts in the proposed organization will be designated as Monitoring accounts and dashboards will be created to summarize the CloudWatch dashboards, alarms, metrics from multiple AWS accounts or multiple regions by enabling sharing in the respective account's CloudWatch.

Similarly, Cross-Region functionality which is built-in feature will also be leveraged to display the metrics from different regions through a designated monitoring accounts.

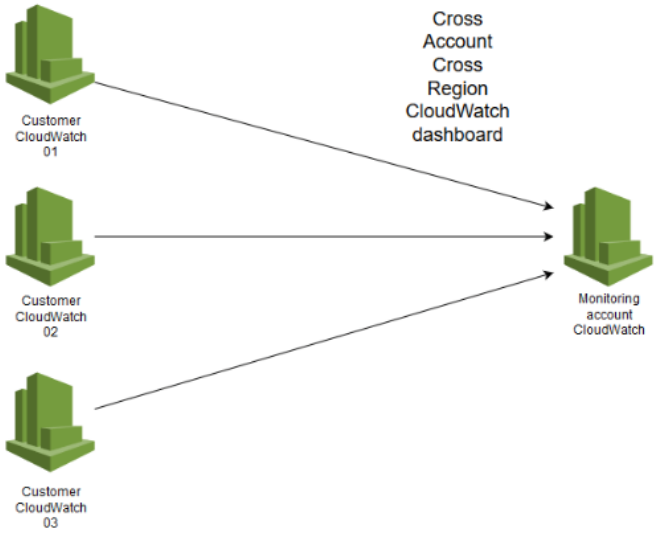


Figure 19 : CloudWatch - Cross Account Cross Region

8.2.10 CloudWatch Container Insights

CloudWatch Container Insights will be used for Amazon Elastic Container Service (Amazon ECS), Amazon Elastic Kubernetes Service (Amazon EKS), and Kubernetes platforms on Amazon EC2.

Container Insights will be used for the collection and aggregation of curated metrics and container ecosystem logs. It collects compute performance metrics such as CPU, memory, network, and disk information from each container as performance events and automatically generates custom metrics used for monitoring and alarming.

Container Insights will be used to collect predefined Amazon EC2 instance logs, Amazon EKS/k8s data plane logs and Amazon EKS control plane logs.

8.2.11 CloudWatch for Estimated charges

CloudWatch alarm will be setup to monitor the estimated charges by enabling / setting up Alerts and Alarms. (***TBD and configured as per company's need)***

Billing Alerts – Billing alerts will be enabled so that the estimated AWS usage charges are monitored.

Billing Alarms – Alarms will be setup to notify through email (thought SNS) once the billing estimates exceeds the threshold value set.

9. ITSM Architecture and Integration with IPP (Infosys PolyCloud)

9.1 ITSM High Level Architecture

The ITSM tool – ServiceNow will be deployed and configured in the AWS modernized Cloud environment by leveraging it's SaaS feature. ServiceNow tool will be integrated with PCP for IT Service Management (ITSM) process for Automated Ticket Management, Incident Management and Change Requests.

The High Level Architecture of Servicenow and it's integration has been depicted in the below diagram.

The configuration and high level integrations of ServiceNow with other services are as described below;

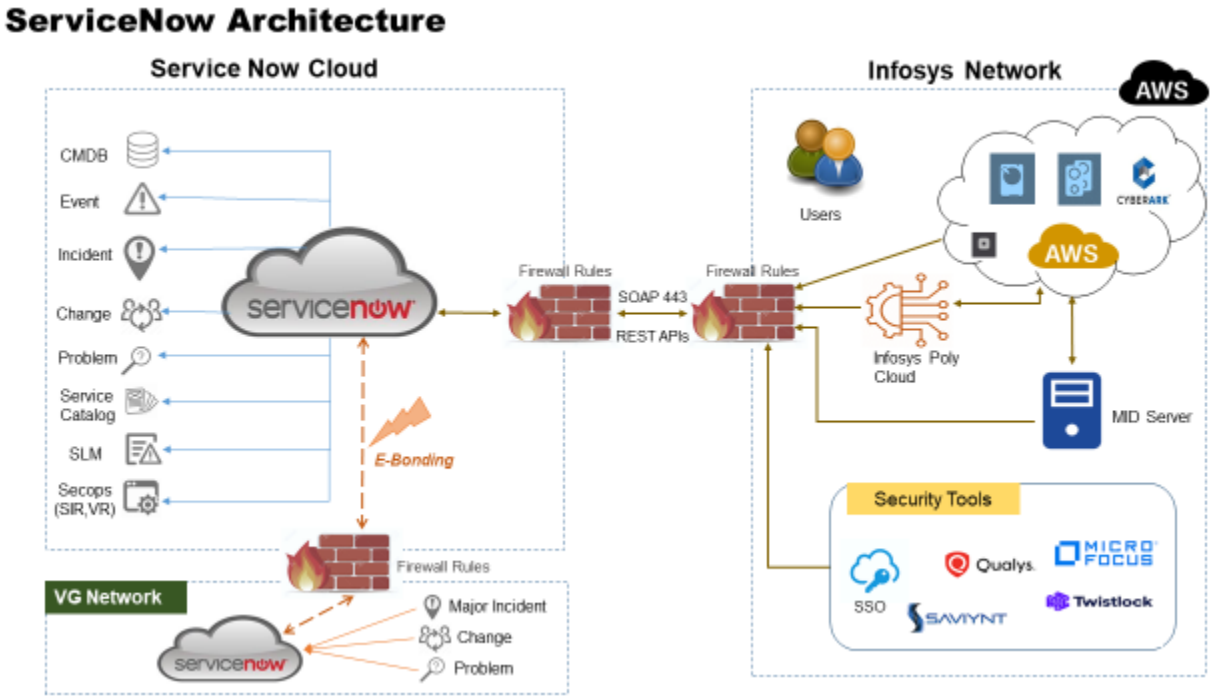


Figure 20 : Servicenow Architecture

- Required Services for ServiceNow Viz. MID server will be deployed in Shared Services Account
- A MID (Management, Instrumentation and Discovery) server will be configured for AD and CMDB. The MID Server facilitates communication and the movement of data between ServiceNow instance and external applications, data sources, and services

9.2 ServiceNow Integrations with Other Services / Resources

ServiceNow will be integrated with other AWS Cloud services for the purpose of achieving authentication and handling

- Integrations with ServiceNow with MS-AD (on EC2) using Service Account for Users / Group management
- Will be integrated with Indigo SSO tool for user authentication
- SAML2.0 configurations for redirecting users from ServiceNow URL to SSO login page
- SSO authentication configurations and redirection to ServiceNow Landing page
- Integration with PCP for Auto ticket creation based on the valid events discovered from PCP
- Integrations with Security tools for handling any Security Incident response, Vulnerability Response and Event Management
- Establish Bi-Directional connectivity between Cloud ServiceNow & VG ServiceNow for Major Incidents, Problem and Change
- Required settings to initiate Major incident/Problem/Change from respective instance if fulfills the predefined rules and criteria and update resolution details by establishing necessary synchronization process between the two ServiceNow instances (VG SNOW and AWS Cloud SNOW)

9.3 ServiceNow Integration with PCP

The below diagram illustrates how the ITSM process Viz. Incident creation, updates and closure activities are handled in an automated way by integrating SNOW with PCP platform

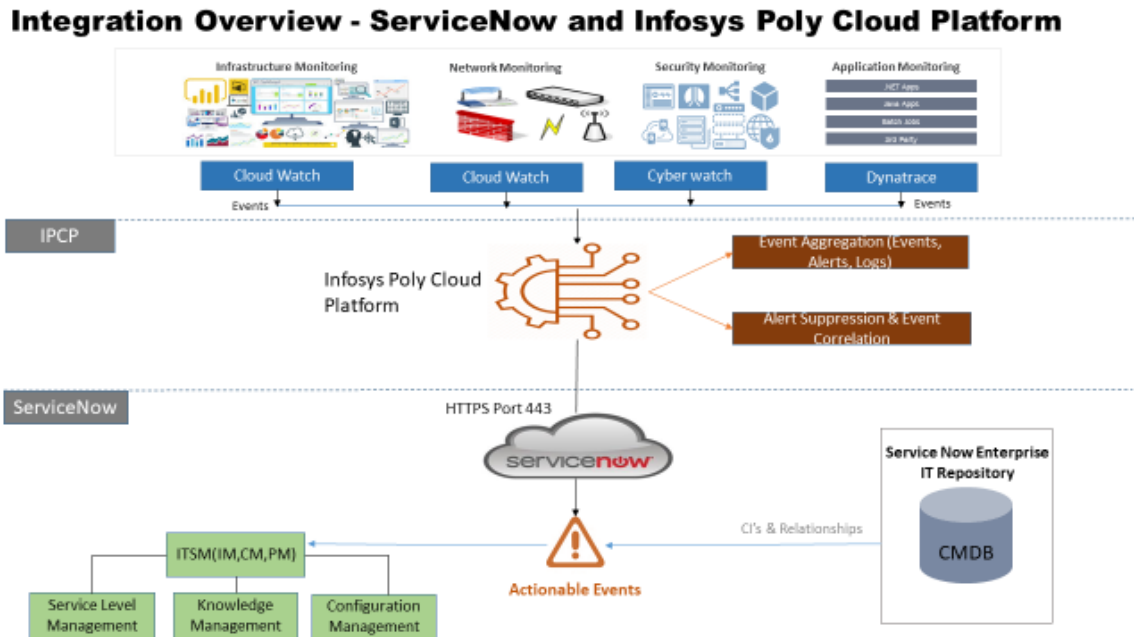


Figure 21 : Integration of ServiceNow with PCP

Below points describes how the capabilities of PCP platform will be leveraged in analyzing events & creating tickets, RCA, Closure of tickets automatically in ServiceNow by integrating with IPP;

- The Events / Logs from various tools Viz. Dynatrace, CloudWatch, CyberWatch etc. will flow through IPP for event management
- IPP performs Event aggregation, Alert suppression and Event correlation
- Actionable events to be identified and sent to service now

❖ Auto creation of incidents for valid events in service now and will follow the Incident lifecycle process till closure

❖ ServiceNow CMDB information to be used in events/Incidents for CI identification & relationships

10. Naming & Tagging Convention (Indicative)

10.1 Naming Standards – EC2

In order to standardize the hostnames, the below naming convention across the Vanguard Cloud Environment will be adopted.

Sample EC2 Naming convention :

Services	Resource Type			Region			AZ	Act Name			Env			OS	App Tier	App Track			Sl No			Sample Naming
EC2	E	C	2	U	S	E	a	S	S	A	D	E	V	L	W	C	C	E	0	0	1	EC2-USE-a -SSA-DEV-L-W-CCE-001

Table 12 : Sample EC2 Naming Strategy

10.2 Naming Standards – Other Resources

Elements	Characters	Values (Sample)	Description
Resource Type	3	EC2, EBS,LAM,RDS	For all Services to be deployed
Region	3	USE , USW	USE - US-East , USW - US-West
AZ	1	a , b	a- US-East-1a , b - US-West-2b
Act Name	3	SSA , INT, SEC , MON, WOR	SSA - Shared Services Account , INT - Interface
Env	3	DEV, SIT,TDT, PCR,STG,PRD	DEV - Development, SIT - Systems Integration
OS	1	W , L	W - Windows 2016 , L - Amazon Linux 2
App Tier	1	W , A , D	W - Web , A - App , D - DB
App Track	3	CCE , PEX , BKO	CCE - Client Comp Exp , PEX - Participant Exp, BKO - Back office
Sl No	3	001	Running Sl #

Table 13 : Naming Strategy - Other Resources

10.3 Tagging

Tags are the metadata assigned to each resources deployed in the Cloud for identification and tracking purpose. It is a simple label consisting of a customer-defined key and an optional value that can make it easier to manage, search for, and filter resources by purpose, owner, environment, or other criteria. Tags can also be used for many other purposes as per the need of the Company.

In Vanguard environment Tagging policy will be enforced on each Account level for both Mandatory and Optional Tags. When a request is raised for including mandatory / optional tags in an account, the policy will be changed only for that particular account.

The table below descries the Tagging convention that will be defined in Vanguard's environment;

10.3.1 Tagging: Key-Value and other Details in Cloud Modernized environment [Indicative]

Tag Name	Value	Mandatory / Optional *	Remarks	Purpose
Name	Hostname	Mandatory	As per naming convention	For Identification of Resources
Account / cost center	Account ID	Mandatory	TBD	For Billing purpose and controls
Owner	Owner email ID	Mandatory	To be provided by App Owners	To identify who owns the resources pertaining to any App / Requestor
OS	Linux/Windows	Mandatory / Optional	Linux 2/ Windows2016	OS identification
Backup	Backup Policy ID	Mandatory / Optional	Schedule / Frequency	To know frequency of backup and schedule for data / resource
Application	Application name	Mandatory / Optional	To be provided by App Owners	To map the resources attached to an Application
Description	Application description	Optional	TBD	Description of Application , Functionality
Environment	Environment based on VPC	Mandatory / Optional	Dev / SIT / Prod	To Identify / list resources based on Environment
SNOW Request Ticket	Ticket No.	Mandatory / Optional	TBD	The ticket no. using which the resources are deployed
MarketPlace AMI	Y/N	Mandatory / Optional	TBD	Whether AMIs are created out of Marketplace (if approved)
Monthly Patching	Monthly Patching based on OS	Mandatory / Optional	Wk No. for patching rollout	To identify Patching Window / Schedule
DC Name	Bangalore , Pune , US	Mandatory / Optional	Which DC has provisioned the Instance	Which DC had deployed the resources as per SNOW ticket

Table 14 : Tagging Strategy

❖ ***Depending on the type of the resource type the Key Value – Madatory / Optional will vary and Table 16 can be referred for Key Value pairs***

The above table represents the Tag keys & their Value Pairs to be used across Vanguard AWS Cloud environment and the relevant Tag fields will be used to tag each of AWS services as in Table - 16

Sample Tags for EC2 instance:

Name	Description	Environment	Account	Owner
PE	Participant Exp	Prod	PE	TBD
PRS	Payroll Services	Development	Finance	TBD

Table 15 : Sample EC2 Tag

10.3.2 Tagging for AWS Services

The necessary and optional tags for approved AWS services which will be deployed in Vanguard environment are represented in the below table;

Legends used in Table: M - Mandatory, O - Optional , NA – Not Applicable

		Tag Keys														
Category	**Services**	Name	Account / cost center	Owner	OS	Backup	Application	Description	Environment	SNOW Request Ticket	MarketPlace AMI	Patching Frequency	DC Name	DB Engine		
Compute	EC2	M	M	M	M	O	M	O	M	M	O	M	O	NA		
	Lambda	M	M	M	NA	NA	M	O	M	M	NA	NA	O	NA		
	EKS/Fargate	M	M	M	M	O	M	O	M	M	O	M	O	NA		
	ECS/ECR	M	M	M	M	O	M	O	M	M	O	M	O	NA		
	EMR	M	M	M	NA	O	M	O	M	M	O	M	O	NA		
	EC2 Image Builder	M	M	M	M	O	M	O	M	M	O	M	O	NA		
	SAM	M	M	M	NA	NA	M	O	M	M	NA	NA	O	NA		
Storage	S3	M	M	M	NA	M	M	O	M	M	NA	NA	O	NA		
	Glacier	M	M	M	NA	M	M	O	M	M	NA	NA	O	NA		
	CloudFront	M	M	M	NA	NA	M	O	M	M	NA	NA	O	NA		
	EFS	M	M	M	NA	M	M	O	M	M	NA	NA	O	NA		
	Backup	M	M	M	NA	NA	M	O	M	M	NA	NA	O	NA		
	EBS / IS	M	M	M	M	M	M	O	M	M	NA	NA	O	NA		
DB	Redshift	M	M	M	NA	NA	O	O	O	M	NA	NA	O	NA		
	Aurora DB	M	M	M	NA	O	O	O	O	M	NA	NA	O	M		
	DynamoDB	M	M	M	NA	O	O	O	O	M	NA	NA	O	NA		
	RDS	M	M	M	NA	O	O	O	O	M	NA	NA	O	M		
	ElastiCache	M	M	M	NA	O	O	O	O	M	NA	NA	O	NA		
Data Processing	Glue	M	M	M	NA	NA	O	O	O	M	NA	NA	O	NA		
	SageMaker	M	M	M	NA	NA	O	O	O	M	NA	NA	O	NA		
	Athena	M	M	M	NA	NA	O	O	O	M	NA	NA	O	NA		
	ElasticSearch	M	M	M	NA	NA	O	O	O	M	NA	NA	O	NA		
	Batch	M	M	M	NA	NA	O	O	O	M	NA	NA	O	NA		
Network	NLB	M	M	M	NA	NA	O	O	M	M	NA	NA	O	NA		
	ALB	M	M	M	NA	NA	O	O	M	M	NA	NA	O	NA		
	Direct Connect -DX	M	M	M	NA	NA	NA	NA	M	M	NA	NA	O	NA		
	VPC	M	M	M	NA	NA	O	O	M	M	NA	NA	O	NA		
	Subnet	M	M	M	NA	NA	O	O	M	M	NA	NA	O	NA		
	Route 53	M	M	M	NA	NA	O	O	M	M	NA	NA	O	NA		
	TGW	M	M	M	NA	NA	O	O	M	M	NA	NA	O	NA		
Security	CloudWatch	M	M	M	NA	NA	NA	NA	M	M	NA	NA	O	NA		
	CloudTrail	M	M	M	NA	NA	O	O	M	M	NA	NA	O	NA		
	VPC FlowLog	M	M	M	NA	NA	O	O	M	M	NA	NA	O	NA		
	NACL	M	M	M	NA	NA	O	O	M	M	NA	NA	O	NA		
	Security Groups (SG)	M	M	M	NA	NA	O	O	M	M	NA	NA	O	NA		
	KMS	M	M	M	NA	NA	O	O	O	O	NA	NA	O	NA		
Messaging / WorkFlow	SNS	M	M	M	NA	NA	O	O	O	O	NA	NA	O	NA		
	SQS	M	M	M	NA	NA	O	O	O	O	NA	NA	O	NA		
	Kinesis	M	M	M	NA	NA	O	O	O	O	NA	NA	O	NA		
	Transcribe	M	M	M	NA	NA	O	O	O	O	NA	NA	O	NA		
	Comprehend	M	M	M	NA	NA	O	O	O	O	NA	NA	O	NA		
	Chat	M	M	M	NA	NA	O	O	O	O	NA	NA	O	NA		
	Lex	M	M	M	NA	NA	O	O	O	O	NA	NA	O	NA		

Table 16 : Tag Fields for AWS Resources

10.3.3 Sample Policy for enforcing Mandatory Tags

Sample
Mandatory-Tag Polic

The above sample file will create IAM policy on EC2 based to enforce mandatory Tags based on Accounts and Owners tag values

10.3.4 Process Flow for a New Tag Inclusion

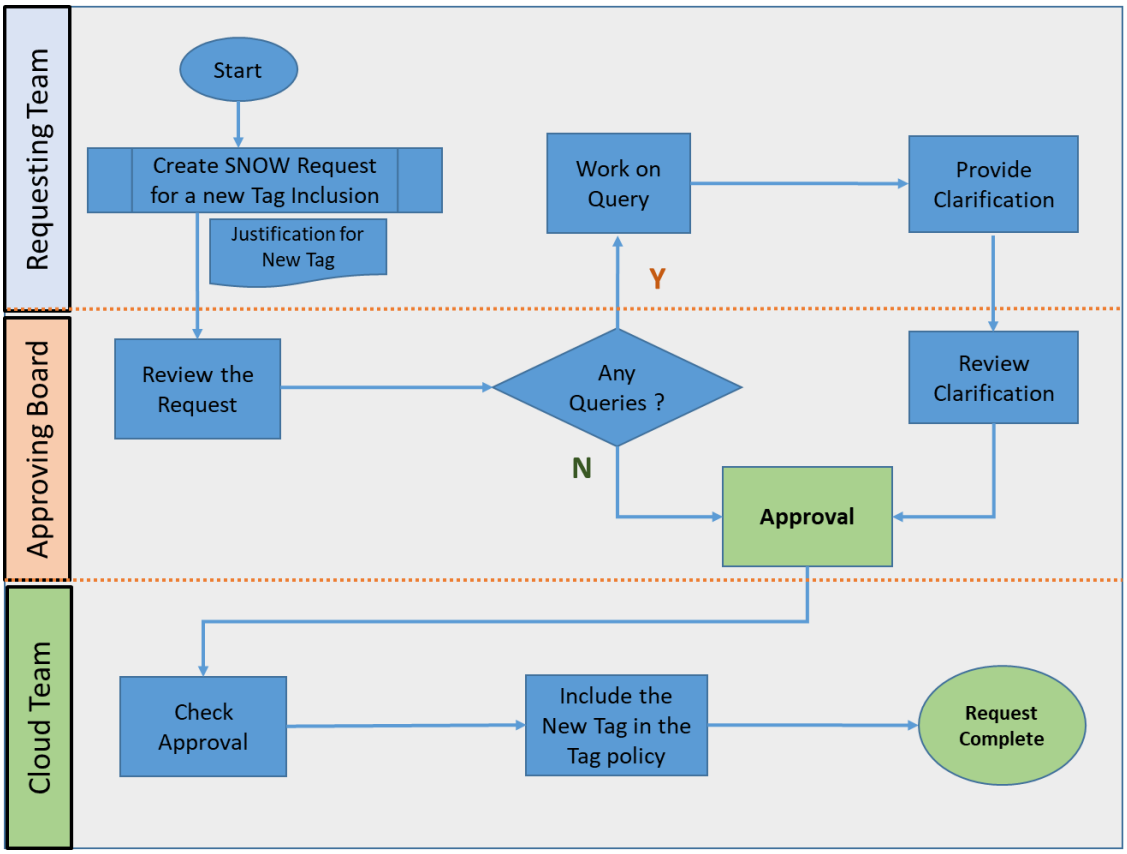


Figure 22 : Process Flow for New Tag Inclusion

11. Application Classification [TBD]

Tier	Services	App Family
Tier 1	PE Portal & Home	PARTICIPANT EXPERIENCE
	PE Txns: PE Withdrawal, PE Loan, PE PD, PE AI, PE AI.	PARTICIPANT EXPERIENCE
	PE Enrollment (1st touch)	PARTICIPANT EXPERIENCE
	MPM Home	MY PLAN MANAGER
	VISION rule parameters	VISION
		PAYROLL SERVICES
Tier 2	PE Non-Transactional	PARTICIPANT EXPERIENCE
	Call Center	PART DECK
	ODR/SOR (Repository of all the database running on perm such as VISTA, VIERA,PRS etc.)	ODR/SOR
	Treasury Apps	VOICE
	MPM Remainder	WMS
	File Ingress / Egress	TRUST APPLICATIONS
	SFF / Tape / Reformatter	DATA EXCHANGE
	Personalization	
	Services consumed externally - EA, Retail, and Plan Sponsors	XIM
	NewGen	REGULATED OUTPUT
		NQP
		ASP
		PARTICIPANT EXPERIENCE AND MY PLAN MANAGER
Tier 3	Backoffice	COMPLIANCE TESTING
	Scanning	EVENT
	Implementation Services	INSTITUTIONAL DESKTOP
	Print (Statements, Confirms, Letters)	ESETUP
	Media Out	MANAGED ACCOUNT PROGRAM
	Data Lake / Mart	DB PENSION PAYROLL
		RKS WEB (INTERNAL BRIDGE)

Table 17 : Application Classification

12. Active Directory

12.1 Active Directory Overview

Active Directory in Vanguard AWS ME will be deployed for the purpose of Authentication of users and to integrate with Third party SSO solution Viz. PingOne and other native AWS service Viz. Workspaces, EFS.

Active Directory will be deployed on EC2 instance in the Primary AZ / Region which will serve as Primary Domain Controller and will have three child domains Viz. Prod.ownyourfuture.local, Non-Prod.ownyourfuture.local & Staging. ownyourfuture.local. For High availability & Disaster Recovery purpose , the Primary Domain Controller will be replicated to secondary AZ / Region.

The high level architecture is as shown below ;

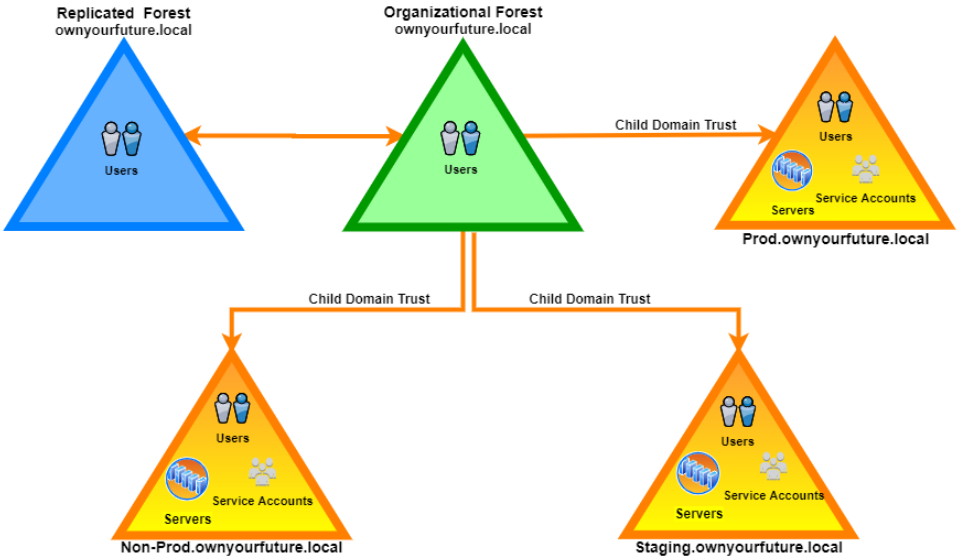


Figure 23 : High Level AD Architecture

12.2 Active Directory Forest Structure

Active Directory forest will be categorized under child domains Viz. Prod.ownyourfuture.local, Non-Prod.ownyourfuture.local & Staging. ownyourfuture.local in order to segregate the environments to provide better security by minimizing the blast radius in case of any eventuality.

The child domains will be further divided into user groups to cater various user personas Viz. Developer, Admin, Testers etc.

The access levels of various user personas will be defined / controlled at each root child domain and the same will be inherited by sub-domains.

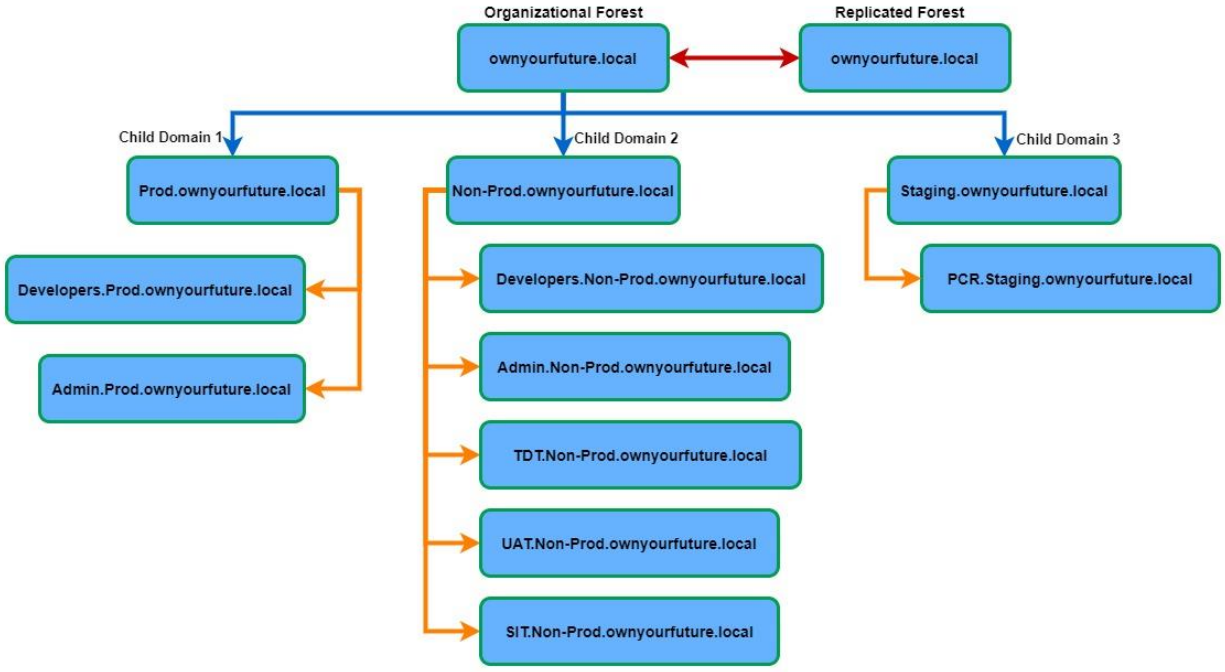


Figure 24 : AD Forest Structure

12.3 Active Directory Setup in ME

Active Directory will be setup in the Shared Services Account in AWS ME.

The Primary and the three child domains will be deployed at Primary region in US-East-1a. For high availability in the Primary Region, the same setup be deployed as a replication process in MS-AD in US-East-1b availability zone.

For DR purpose, the same AD structure as in Primary region will be setup in US-West-2a and US-West-2b and by leveraging replication feature of MS-AD , the consistency of user access levels will be maintained across the environment.

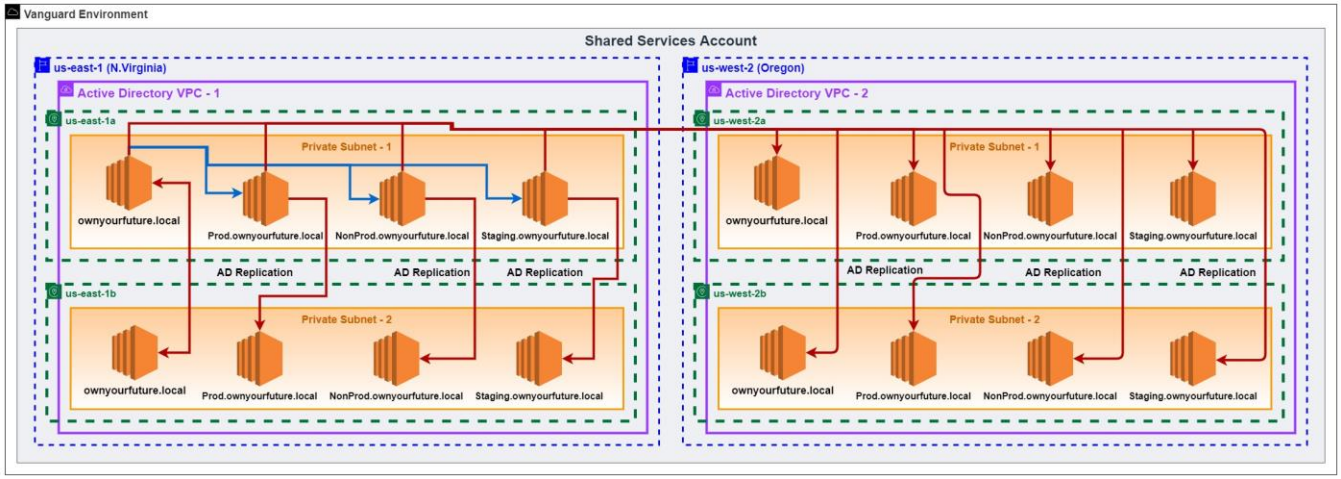


Figure 25 : AD setup in AWS ME

Appendix 1. List of Config Rules for AWS Resources

Sr.No.	Service Name	Config Rule Name	Description	Trigger type	Required Parameters	Parameter Value	Required (Y/N/TBD)
1	EC2	approved-amis-by-id	Checks whether running instances are using specified AMIs. Specify a list of approved AMI IDs. Running instances with AMIs that are not on this list are NON_COMPLIANT.	Configuration changes	amiIds The AMI IDs (comma-separated list of up to 10)		
2	EC2	approved-amis-by-tag	Checks whether running instances are using specified AMIs. Specify the tags that identify the AMIs. Running instances with AMIs that don't have at least one of the specified tags are NON_COMPLIANT.	Configuration changes	amisByTagKeyAndValue The AMIs by tag (comma-separated list up to 10; for example, "tag-key:tag-value").		
3	EC2	autoscaling-group-elb-healthcheck-required	Checks whether your Auto Scaling groups that are associated with a load balancer are using Elastic Load Balancing health checks.	Configuration changes	None		
4	EC2	desired-instance-tenancy	Checks instances for specified tenancy. Specify AMI IDs to check instances that are launched from those AMIs or specify host IDs to check whether instances are launched on those Dedicated Hosts. Separate multiple ID values with commas.	Configuration changes	tenancy The desired tenancy of the instances. Valid values are DEDICATED, HOST, and DEFAULT. imageId The rule evaluates instances launched only from the AMI with the specified ID. Separate multiple AMI IDs with commas. hostId The ID of the Amazon EC2 Dedicated Host on which the instances are meant to be launched. Separate multiple host IDs with commas.		

Sr.No.	Service Name	Config Rule Name	Description	Trigger type	Required Parameters	Parameter Value	Required (Y/N/TBD)
5	EC2	desired-instance-type	Checks whether your EC2 instances are of the specified instance types.	Configuration changes	instanceType Comma-separated list of EC2 instance types (for example, "t2.small, m4.large, i2.xlarge").		
6	EC2	ebs-optimized-instance	Checks whether EBS optimization is enabled for your EC2 instances that can be EBS-optimized.	Configuration changes	None		
7	EC2	ec2-stopped-instance	Checks whether there are instances stopped for more than the allowed number of days. The instance is NON_COMPLIANT if the state of the ec2 instance has been stopped for longer than the allowed number of days.	Periodic	allowedDays (Optional) The number of days an ec2 instance can be stopped before it is NON_COMPLIANT. The default number of days is 30.		
8	EC2	ec2-instance-detailed-monitoring-enabled	Checks whether detailed monitoring is enabled for EC2 instances.	Configuration changes	None		
9	EC2	ec2-instance-managed-by-systems-manager	Checks whether the Amazon EC2 instances in your account are managed by AWS Systems Manager.	Configuration changes	None		
10	EC2	ec2-instance-no-public-ip	Checks whether Amazon Elastic Compute Cloud (Amazon EC2) instances have a public IP association. The rule is NON_COMPLIANT if the publicIp field is present in the Amazon EC2 instance configuration item. This rule applies only to IPv4.	Configuration changes	None		
11	EC2	ec2-instances-in-vpc	Checks whether your EC2 instances belong to a virtual private cloud (VPC). Optionally, you can specify the VPC ID to associate with your instances.	Configuration changes	vpcId The ID of the VPC that contains these instances.		

Sr.No.	Service Name	Config Rule Name	Description	Trigger type	Required Parameters	Parameter Value	Required (Y/N/TBD)
12	EC2	ec2-managedinstance-applications-blacklisted	Checks that none of the specified applications are installed on the instance. Optionally, specify the application version. Newer versions of the application will not be blacklisted. You can also specify the platform to apply the rule only to instances running that platform.	Configuration changes	applicationNames Comma-separated list of application names. Optionally, specify versions appended with ":" (for example, "Chrome:0.5.3, FireFox").Note The application names must be an exact match. For example, use firefox on Linux or firefox-compat on Amazon Linux. In addition, AWS Config does not currently support wildcards for the applicationNames parameter (for example, firefox*). platformType The platform type (for example, "Linux" or "Windows").		

Sr.No.	Service Name	Config Rule Name	Description	Trigger type	Required Parameters	Parameter Value	Required (Y/N/TBD)
13	EC2	ec2-managedinstance-applications-required	Checks whether all of the specified applications are installed on the instance. Optionally, specify the minimum acceptable version. You can also specify the platform to apply the rule only to instances running that platform.	Configuration changes	applicationNames Comma-separated list of application names. Optionally, specify versions appended with ":" (for example, "Chrome:0.5.3, FireFox").Note The application names must be an exact match. For example, use firefox on Linux or firefox-compat on Amazon Linux. In addition, AWS Config does not currently support wildcards for the applicationNames parameter (for example, firefox*). PlatformType The platform type (for example, "Linux" or "Windows").		
14	EC2	ec2-managedinstance-association-compliance-status-check	Checks whether the compliance status of the Amazon EC2 Systems Manager association compliance is COMPLIANT or NON_COMPLIANT after the association execution on the instance. The rule is COMPLIANT if the field status is COMPLIANT.	Configuration changes	None		
15	EC2	ec2-managedinstance-inventory-blacklisted	Checks whether instances managed by AWS Systems Manager are configured to collect blacklisted inventory types.	Configuration changes	inventoryNames Comma-separated list of Systems Manager inventory types (for example, "AWS:Network, AWS:WindowsUpdate"). platformType Platform type (for example, “Linux”).		

Sr.No.	Service Name	Config Rule Name	Description	Trigger type	Required Parameters	Parameter Value	Required (Y/N/TBD)
16	EC2	ec2-managedinstance-patch-compliance-status-check	Checks whether the compliance status of the Amazon EC2 Systems Manager patch compliance is COMPLIANT or NON_COMPLIANT after the patch installation on the instance. The rule is COMPLIANT if the field status is COMPLIANT.	Configuration changes	None		
17	EC2	ec2-managedinstance-platform-check	Checks whether EC2 managed instances have the desired configurations.	Configuration changes	agentVersion The version of the agent (for example, "2.0.433.0"). platformType The platform type (for example, "Linux" or "Windows"). platformVersion The version of the platform (for example, "2016.09").		
18	EC2	ec2-security-group-attached-to-eni	Checks that security groups are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or to an elastic network interface. The rule returns NON_COMPLIANT if the security group is not associated with an Amazon EC2 instance or an elastic network interface.	Configuration changes	None		
19	EC2	ec2-volume-inuse-check	Checks whether EBS volumes are attached to EC2 instances. Optionally checks if EBS volumes are marked for deletion when an instance is terminated.	Configuration changes	deleteOnTermination EBS volumes are marked for deletion when an instance is terminated.		
20	EC2	eip-attached	Checks whether all Elastic IP addresses that are allocated to a VPC are attached to EC2 instances or in-use elastic network interfaces (ENIs).Results might take up to 6 hours to become available after an evaluation occurs.	Configuration changes	None		

Sr.No.	Service Name	Config Rule Name	Description	Trigger type	Required Parameters	Parameter Value	Required (Y/N/TBD)
21	ELB	elb-acm-certificate-required	Checks whether the Classic Load Balancers use SSL certificates provided by AWS Certificate Manager. To use this rule, use an SSL or HTTPS listener with your Classic Load Balancer. This rule is only applicable to Classic Load Balancers. This rule does not check Application Load Balancers and Network Load Balancers.	Configuration changes	None		
22	ELB	elb-custom-security-policy-ssl-check	Checks whether your Classic Load Balancer SSL listeners are using a custom policy. The rule is only applicable if there are SSL listeners for the Classic Load Balancer.	Configuration changes	ssl-protocols-and-ciphers Comma-separated list of ciphers and protocol.		
23	ELB	elb-logging-enabled	Checks whether the Application Load Balancers and the Classic Load Balancers have logging enabled. The rule is NON_COMPLIANT if the access_logs.s3.enabled is false or access_logs.S3.bucket is not equal to the s3BucketName that you provided.	Configuration changes	s3BucketNames (optional) Comma-separated list of Amazon S3 bucket names for Elastic Load Balancing to deliver the log files.		
24	ELB	elb-predefined-security-policy-ssl-check	Checks whether your Classic Load Balancer SSL listeners are using a predefined policy. The rule is only applicable if there are SSL listeners for the Classic Load Balancer.	Configuration changes	predefined-policy-name Name of the predefined policy.		
25	EBS	encrypted-volumes	Checks whether the EBS volumes that are in an attached state are encrypted. If you specify the ID of a KMS key for encryption using the kmsId parameter, the rule checks if the EBS volumes in an attached state are encrypted with that KMS key.	Configuration changes	kmsId ID or ARN of the KMS key that is used to encrypt the volume.		

Sr.No.	Service Name	Config Rule Name	Description	Trigger type	Required Parameters	Parameter Value	Required (Y/N/TBD)
26	Lambda	lambda-concurrency-check	Checks whether the AWS Lambda function is configured with function-level concurrent execution limit. The rule is NON_COMPLIANT if the Lambda function is not configured with function-level concurrent execution limit.	Configuration changes	ConcurrencyLimitLow (Optional) Minimum concurrency execution limit ConcurrencyLimitHigh (Optional) Maximum concurrency execution limit		
27	Lambda	lambda-dlq-check	Checks whether an AWS Lambda function is configured with a dead-letter queue. The rule is NON_COMPLIANT if the Lambda function is not configured with a dead-letter queue.	Configuration changes	dlqArns (Optional) Comma-separated list of Amazon SQS and Amazon SNS ARNs that must be configured as the Lambda function dead-letter queue target.		
28	Lambda	lambda-function-settings-check	Checks that the lambda function settings for runtime, role, timeout, and memory size match the expected values.	Configuration changes	runtime Comma-separated list of runtime values. role IAM role. timeout Timeout in seconds. memorySize Memory size in MB.		
29	Lambda	lambda-function-public-access-prohibited*	Checks whether the AWS Lambda function policy attached to the Lambda resource prohibits public access. If the Lambda function policy allows public access it is NON_COMPLIANT.	Configuration changes	None		
30	Lambda	lambda-inside-vpc	Checks whether an AWS Lambda function is in an Amazon Virtual Private Cloud. The rule is NON_COMPLIANT if the Lambda function is not in a VPC.	Configuration changes	subnetId (Optional) Comma-separated list of subnet IDs that Lambda functions must be associated with.		

Sr.No.	Service Name	Config Rule Name	Description	Trigger type	Required Parameters	Parameter Value	Required (Y/N/TBD)
31	SSH traffic	restricted-common-ports	Checks whether the incoming SSH traffic for the security groups is accessible to the specified ports. The rule is COMPLIANT when the IP addresses of the incoming SSH traffic in the security group are restricted to the specified ports. This rule applies only to IPv4.	Configuration changes	blockedPort1 Blocked TCP port number. blockedPort2 Blocked TCP port number. blockedPort3 Blocked TCP port number. blockedPort4 Blocked TCP port number. blockedPort5 Blocked TCP port number.		
32	SSH traffic	restricted-ssh	Checks whether the incoming SSH traffic for the security groups is accessible. The rule is COMPLIANT when the IP addresses of the incoming SSH traffic in the security groups are restricted. This rule applies only to IPv4.	Configuration changes	None		
33	Cloudformation-stack	cloudformation-stack-drift-detection-check	Checks whether an AWS CloudFormation stack's actual configuration differs, or has drifted, from it's expected configuration. A stack is considered to have drifted if one or more of its resources differ from their expected configuration. The rule and the stack are COMPLIANT when the stack drift status is IN_SYNC. The rule and the stack are NON_COMPLIANT when the stack drift status is DRIFTED.	Configuration changes and periodic	cloudformationRoleArn The AWS CloudFormation role ARN with IAM policy permissions to detect drift for AWS CloudFormation stacks.		

Sr.No.	Service Name	Config Rule Name	Description	Trigger type	Required Parameters	Parameter Value	Required (Y/N/TBD)
34	Cloudformation-stack	cloudformation-stack-notification-check	Checks whether your CloudFormation stacks are sending event notifications to an SNS topic. Optionally checks whether specified SNS topics are used.	Configuration changes	snsTopic1 SNS Topic ARN. snsTopic2 SNS Topic ARN. snsTopic3 SNS Topic ARN. snsTopic4 SNS Topic ARN. snsTopic5 SNS Topic ARN.		
35	CloudTrail	cloud-trail-cloud-watch-logs-enabled	Checks whether AWS CloudTrail trails are configured to send logs to Amazon CloudWatch Logs. The trail is NON_COMPLIANT if the CloudWatchLogsLogGroupArn property of the trail is empty.	Periodic	None		
36	CloudTrail	cloudtrail-enabled	Checks whether AWS CloudTrail is enabled in your AWS account. Optionally, you can specify which S3 bucket, SNS topic, and Amazon CloudWatch Logs ARN to use.	Periodic	s3BucketName The name of the S3 bucket for AWS CloudTrail to deliver log files to. snsTopicArn The ARN of the SNS topic for AWS CloudTrail to use for notifications. cloudWatchLogsLogGroupArn The ARN of the Amazon CloudWatch log group for AWS CloudTrail to send data to.		

Sr.No.	Service Name	Config Rule Name	Description	Trigger type	Required Parameters	Parameter Value	Required (Y/N/TBD)
37	CloudTrail	cloud-trail-encryption-enabled	Checks whether AWS CloudTrail is configured to use the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master key (CMK) encryption. The rule is COMPLIANT if the KmsKeyId is defined.	Periodic	None		
38	CloudTrail	cloud-trail-log-file-validation-enabled	Checks whether AWS CloudTrail creates a signed digest file with logs. AWS recommends that the file validation must be enabled on all trails. The rule is NON_COMPLIANT if the validation is not enabled.	Periodic	None		
39	CloudTrail	cloudtrail-s3-dataevents-enabled	Checks whether at least one AWS CloudTrail trail is logging Amazon S3 data events for all S3 buckets. The rule is NON_COMPLIANT if trails that log data events for S3 buckets are not configured.	Configuration changes	S3BucketNames (Optional) Comma-separated list of S3 bucket names for which data events logging should be enabled. Default behavior checks for all S3 buckets.		

Sr.No.	Service Name	Config Rule Name	Description	Trigger type	Required Parameters	Parameter Value	Required (Y/N/TBD)
40	CloudWatch	cloudwatch-alarm-action-check	Checks whether CloudWatch alarms have at least one alarm action, one INSUFFICIENT_DATA action, or one OK action enabled. Optionally, checks whether any of the actions matches one of the specified ARNs.	Configuration changes	alarmActionRequired Alarms have at least one action. The default value is true. insufficientDataActionRequired Alarms have at least one action when the alarm transitions to the INSUFFICIENT_DATA state from any other state. The default value is true. okActionRequired Alarms have at least one action when the alarm transitions to an OK state from any other state. The default value is false. action1 The action to execute, specified as an ARN. action2 The action to execute, specified as an ARN. action3 The action to execute, specified as an ARN. action4 The action to execute, specified as an ARN. action5 The action to execute, specified as an ARN.		

Sr.No.	Service Name	Config Rule Name	Description	Trigger type	Required Parameters	Parameter Value	Required (Y/N/TBD)
41	CloudWatch	cloudwatch-alarm-resource-check	Checks whether the specified resource type has a CloudWatch alarm for the specified metric. For resource type, you can specify EBS volumes, EC2 instances, RDS clusters, or S3 buckets.	Periodic	resourceType AWS resource type. The value can be one of the following: AWS::EC2::Volume AWS::EC2::Instance AWS::S3::Bucket metricName The name of the metric associated with the alarm (for example, "CPUUtilization" for EC2 instances).		

Sr.No.	Service Name	Config Rule Name	Description	Trigger type	Required Parameters	Parameter Value	Required (Y/N/TBD)
42	CloudWatch	cloudwatch-alarm-settings-check	Checks whether CloudWatch alarms with the given metric name have the specified settings.	Configuration changes	metricName The name for the metric associated with the alarm. threshold The value against which the specified statistic is compared. evaluationPeriod The number of periods in which data is compared to the specified threshold. period The period, in seconds, during which the specified statistic is applied. The default value is 300 seconds. comparisonOperator The operation for comparing the specified statistic and threshold (for example, "GreaterThanThreshold"). statistic The statistic for the metric associated with the alarm (for example, "Average" or "Sum").		
43	CloudWatch	cloudwatch-log-group-encrypted	Checks whether a log group in Amazon CloudWatch Logs is encrypted. The rule is NON_COMPLIANT if CloudWatch Logs has a log group without encryption enabled.	Periodic	KmsKeyId (Optional) Amazon Resource Name (ARN) of an AWS Key Management Service (KMS) key that is used to encrypt the CloudWatch Logs log group.		
44	Codebuild	codebuild-project-envvar-awscred-check	Checks whether the project contains environment variables AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY. The rule is NON_COMPLIANT when the project environment variables contains plaintext credentials.	Configuration changes	None		

Sr.No.	Service Name	Config Rule Name	Description	Trigger type	Required Parameters	Parameter Value	Required (Y/N/TBD)
45	Codebuild	codebuild-project-source-repo-url-check	Checks whether the GitHub or Bitbucket source repository URL contains either personal access tokens or user name and password. The rule is COMPLIANT with the usage of OAuth to grant authorization for accessing GitHub or Bitbucket repositories.	Configuration changes	None		
46	CodePipeline	codepipeline-deployment-count-check	Checks whether the first deployment stage of the AWS CodePipeline performs more than one deployment. Optionally, checks if each of the subsequent remaining stages deploy to more than the specified number of deployments (deploymentLimit). The rule is NON_COMPLIANT if the first stage in the AWS CodePipeline deploys to more than one region and the AWS CodePipeline deploys to more than the number specified in the deploymentLimit.	Configuration changes	deploymentLimit The maximum number of deployments each stage can perform.		

Sr.No.	Service Name	Config Rule Name	Description	Trigger type	Required Parameters	Parameter Value	Required (Y/N/TBD)
47	CodePipeline	codepipeline-region-fanout-check	Checks whether each stage in the AWS CodePipeline deploys to more than N times the number of the regions the AWS CodePipeline has deployed in all the previous combined stages, where N is the region fanout number. The first deployment stage can deploy to a maximum of one region and the second deployment stage can deploy to a maximum number specified in the regionFanoutFactor. If you do not provide a regionFanoutFactor, by default the value is three. For example: If 1st deployment stage deploys to one region and 2nd deployment stage deploys to three regions, 3rd deployment stage can deploy to 12 regions, that is, sum of previous stages multiplied by the region fanout (three) number. The rule is NON_COMPLIANT if the deployment is in more than one region in 1st stage or three regions in 2nd stage or 12 regions in 3rd stage.	Configuration changes	regionFanoutFactor The number of regions the AWS CodePipeline has deployed to in all previous stages is the acceptable number of regions any stage can deploy to.		

Sr.No.	Service Name	Config Rule Name	Description	Trigger type	Required Parameters	Parameter Value	Required (Y/N/TBD)
48	CloudTrail	multi-region-cloud-trail-enabled	Checks that there is at least one multi-region AWS CloudTrail. The rule is NON_COMPLIANT if the trails do not match inputs parameters.	Periodic	s3BucketName Name of Amazon S3 bucket for AWS CloudTrail to deliver log files to. snsTopicArn Amazon SNS topic ARN for AWS CloudTrail to use for notifications. cloudWatchLogsLogGroupArn Amazon CloudWatch log group ARN for AWS CloudTrail to send data to. includeManagementEvents Event selector to include management events for the AWS CloudTrail. readWriteType Type of events to record. Valid values are ReadOnly, WriteOnly and ALL.		
49	Tags	required-tags	Checks whether your resources have the tags that you specify. For example, you can check whether your EC2 instances have the 'CostCenter' tag. Separate multiple values with commas.	Configuration changes	tag1Key Key of the required tag. tag1Value Optional value of the required tag. Separate multiple values with commas.		
50	ALB	alb-http-to-https-redirection-check	Checks whether HTTP to HTTPS redirection is configured on all HTTP listeners of Application Load Balancers. The rule is NON_COMPLIANT if one or more HTTP listeners of Application Load Balancers do not have HTTP to HTTPS redirection configured.	Periodic	None		

Sr.No.	Service Name	Config Rule Name	Description	Trigger type	Required Parameters	Parameter Value	Required (Y/N/TBD)
51	APIGateway	api-gw-execution-logging-enabled	Checks that all methods in Amazon API Gateway stage has logging enabled. The rule is NON_COMPLIANT if logging is not enabled. The rule is NON_COMPLIANT if loggingLevel is neither ERROR nor INFO.	Configuration changes	loggingLevel (Optional) Comma-separated list of specific logging levels (for example, ERROR, INFO or ERROR,INFO).		
52	APIGateway	api-gw-cache-enabled-and-encrypted	Checks that all methods in Amazon API Gateway stages have caching enabled and encrypted. The rule is NON_COMPLIANT if any method in an API Gateway stage is not configured for caching or the cache is not encrypted.	Configuration changes	None		
53	APIGateway	api-gw-endpoint-type-check	Checks that Amazon API Gateway APIs are of the type specified in the rule parameter endpointConfigurationType. The rule returns NON_COMPLIANT if the REST API does not match the endpoint type configured in the rule parameter.	Configuration changes	endpointConfigurationType (Required) Comma-separated list of allowed endpoint types. Allowed values are REGIONAL, PRIVATE and EDGE.		
54	Cloudfront	cloudfront-viewer-policy-https	Checks whether your Amazon CloudFront distributions use HTTPS (directly or via a redirection). The rule is NON_COMPLIANT if the value of ViewerProtocolPolicy is set to allow-all for defaultCacheBehavior or for cacheBehaviors. This means that the rule is non compliant when viewers can use HTTP or HTTPS.	Configuration changes	None		
55	IG	internet-gateway-authorized-vpc-only	Checks that Internet gateways (IGWs) are only attached to an authorized Amazon Virtual Private Cloud (VPCs). The rule is NON_COMPLIANT if IGWs are not attached to an authorized VPC.	Configuration changes	authorizedVpcIds Comma-separated list of the authorized VPC IDs with attached IGWs. If parameter is not provided all attached IGWs will be NON_COMPLIANT.		

Sr.No.	Service Name	Config Rule Name	Description	Trigger type	Required Parameters	Parameter Value	Required (Y/N/TBD)
56	VPC Endpoint	service-vpc-endpoint-enabled	Checks whether Service Endpoint for the service provided in rule parameter is created for each Amazon VPC. The rule returns NON_COMPLIANT if an Amazon VPC doesn't have a VPC endpoint created for the service.	Periodic	serviceName (Optional) The short name or suffix for the service. To get a list of available service names or valid suffix list, use DescribeVpcEndpointServices.		
57	VPC	vpc-default-security-group-closed	Checks that the default security group of any Amazon Virtual Private Cloud (VPC) does not allow inbound or outbound traffic. The rule returns NOT_APPLICABLE if the security group is not default. The rule is NON_COMPLIANT if the default security group has one or more inbound or outbound traffic.	Configuration changes	None		
58	VPC	vpc-flow-logs-enabled	Checks whether Amazon Virtual Private Cloud flow logs are found and enabled for Amazon VPC.	Periodic	trafficType The valid trafficType values are ACCEPT, REJECT, or ALL.		
59	VPC	vpc-sg-open-only-to-authorized-ports	Checks whether the security group with 0.0.0.0/0 of any Amazon Virtual Private Cloud (Amazon VPC) allows only specific inbound TCP or UDP traffic. The rule and any security group with inbound 0.0.0.0/0. are NON_COMPLIANT if you do not provide any ports in the parameters	Configuration changes	authorizedTcpPorts (Optional) Comma-separated list of TCP ports authorized to be open to 0.0.0.0/0. Ranges are defined by a dash; for example, "443,1020-1025". authorizedUdpPorts (Optional) Comma-separated list of UDP ports authorized to be open to 0.0.0.0/0. Ranges are defined by a dash; for example, "500,1020-1025".		
60	VPC	vpc-vpn-2-tunnels-up	Checks that both AWS Virtual Private Network tunnels provided by AWS Site-to-Site VPN are in UP status. The rule returns NON_COMPLIANT if one or both tunnels are in DOWN status.	Configuration changes	None		

Sr.No.	Service Name	Config Rule Name	Description	Trigger type	Required Parameters	Parameter Value	Required (Y/N/TBD)
61	Access Keys	access-keys-rotated	Checks whether the active access keys are rotated within the number of days specified in maxAccessKeyAge. The rule is NON_COMPLIANT if the access keys have not been rotated for more than maxAccessKeyAge number of days.	Periodic	maxAccessKeyAge Maximum number of days within which the access keys must be rotated. The default value is 90 days.		
62	ACM	acm-certificate-expiration-check	Checks whether ACM Certificates in your account are marked for expiration within the specified number of days. Certificates provided by ACM are automatically renewed. ACM does not automatically renew certificates that you import.	Configuration changes and periodic	daysToExpiration Specify the number of days before the rule flags the ACM Certificate as NON_COMPLIANT.		
63	CMK	cmk-backing-key-rotation-enabled	Checks that key rotation is enabled for each customer master key (CMK). The rule is COMPLIANT, if the key rotation is enabled for specific key object. The rule is not applicable to CMKs that have imported key material.	Periodic	None		

Sr.No.	Service Name	Config Rule Name	Description	Trigger type	Required Parameters	Parameter Value	Required (Y/N/TBD)
64	Firewall Manager	fms-security-group-audit-policy-check	Checks whether the security groups associated inScope resources are compliant with the master security groups at each rule level based on allowSecurityGroup and denySecurityGroup flag.	Configuration changes	masterSecurityGroupsIds (mandatory) Comma-separated list of master security groups IDs. The rule will check if security groups associated inScope resources are compliant with the master security groups at each rule level. resourceTags (mandatory) The resource tags associated with the rule (for example, { "tagKey1" : ["tagValue1"], "tagKey2" : ["tagValue2", "tagValue3"] }"). inScope (mandatory) If true, the AWS Config rule owner is in Firewall Manager security group audit policy scope. excludeResourceTags (mandatory) If true, exclude resources that match resourceTags. resourceTypes (mandatory) The resource types such as Amazon EC2 instance or elastic network interface or security group supported by this rule. fmsRemediationEnabled (mandatory) If true, AWS Firewall Manager will update NON_COMPLIANT resources according to FMS policy. AWS Config ignores this parameter when you create this rule. allowSecurityGroup (mandatory) If true, the rule will check to ensure that all inScope security groups are within the reference security group's inbound/outbound rules.		

Sr.No.	Service Name	Config Rule Name	Description	Trigger type	Required Parameters	Parameter Value	Required (Y/N/TBD)
65	Firewall Manager	fms-security-group-content-check	Checks whether AWS Firewall Manager created security groups content is the same as the master security groups. The rule is NON_COMPLIANT if the content does not match.	Configuration changes	vpcIds (mandatory) Comma-separated list of VPC IDs in the account. securityGroupsIds (mandatory) Comma-separated list of security groups IDs created by Firewall Manager in every Amazon VPC in an account. They are sorted by VPC IDs. fmsRemediationEnabled (mandatory) If true, AWS Firewall Manager will update NON_COMPLIANT resources according to FMS policy. AWS Config ignores this parameter when you create this rule. revertManualSecurityGroupChangesFlag (mandatory) If true, AWS Firewall Manager will check the security groups in the securityGroupsIds parameter. allowSecurityGroup (mandatory) If true, the rule will check to ensure that all inScope security groups are within the reference security group's inbound/outbound rules. masterSecurityGroupsIds (optional) This parameter only applies to AWS Firewall Manager admin account. Comma-separated list of master security groups ID in Firewall Manager admin account.		

Sr.No.	Service Name	Config Rule Name	Description	Trigger type	Required Parameters	Parameter Value	Required (Y/N/TBD)
66	Firewall Manager	fms-security-group-resource-association-check	Checks whether Amazon EC2 or an elastic network interface is associated with AWS Firewall Manager security groups. The rule is NON_COMPLIANT if the resources are not associated with FMS security groups.	Configuration changes	vpcIds (mandatory) Comma-separated list of VPC IDs in the account. securityGroupsIds (mandatory) Comma-separated list of security groups IDs created by Firewall Manager in every Amazon VPC in an account. They are sorted by VPC IDs. resourceTags (mandatory) The resource tags such as Amazon EC2 instance or elastic network interface associated with the rule (for example, { "tagKey1" : ["tagValue1"], "tagKey2" : ["tagValue2", "tagValue3"] }"). excludeResourceTags (mandatory) If true, exclude resources that match resourceTags. resourceTypes (mandatory) The resource types such as Amazon EC2 instance or elastic network interface or security group supported by this rule. fmsRemediationEnabled (mandatory) If true, AWS Firewall Manager will update NON_COMPLIANT resources according to FMS policy. AWS Config ignores this parameter when you create this rule. exclusiveResourceSecurityGroupManagementFlag (mandatory If true, only allows AWS Firewall Manager created security groups associated with resource.		

Sr.No.	Service Name	Config Rule Name	Description	Trigger type	Required Parameters	Parameter Value	Required (Y/N/TBD)
67	Firewall Manager	fms-shield-resource-policy-check	Checks whether an Application Load Balancer, Amazon CloudFront distributions, Elastic Load Balancer or Elastic IP has AWS Shield protection. This rule also checks if they have web ACL associated for Application Load Balancer and Amazon CloudFront distributions.	Configuration changes	webACLId The WebACLId of the web ACL. resourceTags The resource tags associated with the rule (for example, { "tagKey1" : ["tagValue1"], "tagKey2" : ["tagValue2", "tagValue3"] }"). excludeResourceTags If true, exclude the resources that match the resourceTags. If false, include all the resources that match the resourceTags. fmsManagedToken A token generated by AWS Firewall Manager when creating the rule in your account. AWS Config ignores this parameter when you create this rule. fmsRemediationEnabled If true, AWS Firewall Manager will update NON_COMPLIANT resources according to FMS policy. AWS Config ignores this parameter when you create this rule.		

Sr.No.	Service Name	Config Rule Name	Description	Trigger type	Required Parameters	Parameter Value	Required (Y/N/TBD)
68	Firewall Manager	fms-webacl-resource-policy-check	Checks whether the web ACL is associated with an Application Load Balancer, API Gateway stage, or Amazon CloudFront distributions. When AWS Firewall Manager creates this rule, the FMS policy owner specifies the WebACLId in the FMS policy and can optionally enable remediation.	Configuration changes	Checks whether the web ACL is associated with an Application Load Balancer, API Gateway stage, or Amazon CloudFront distributions. When AWS Firewall Manager creates this rule, the FMS policy owner specifies the WebACLId in the FMS policy and can optionally enable remediation.		
69	Firewall Manager	fms-webacl-rulegroup-association-check	Checks that the rule groups associate with the web ACL at the correct priority. The correct priority is decided by the rank of the rule groups in the ruleGroups parameter. When AWS Firewall Manager creates this rule, it assigns the highest priority 0 followed by 1, 2, and so on. The FMS policy owner specifies the ruleGroups rank in the FMS policy and can optionally enable remediation.	Configuration changes	ruleGroups Comma-separated list of RuleGroupIds and WafOverrideAction pairs (for example, RuleGroupId-1:NONE, RuleGroupId-2:COUNT). For this example, RuleGroupId-1 receives the highest priority 0 and RuleGroupId-2 receives priority 1. fmsManagedToken A token generated by AWS Firewall Manager when creating the rule in your account. AWS Config ignores this parameter when you create this rule. fmsRemediationEnabled If true, AWS Firewall Manager will update NON_COMPLIANT resources according to FMS policy. AWS Config ignores this parameter when you create this rule.		

Sr.No.	Service Name	Config Rule Name	Description	Trigger type	Required Parameters	Parameter Value	Required (Y/N/TBD)
70	Guardduty	guardduty-non-archived-findings	Checks whether the Amazon GuardDuty has findings that are non archived. The rule is NON_COMPLIANT if Amazon GuardDuty has non archived low/medium/high severity findings older than the specified number in the daysLowSev/daysMediumSev/daysHighSev parameter.	Configuration changes	daysLowSev The number of days Amazon GuardDuty low severity findings are allowed to stay non archived. The default is 30 days. daysMediumSev The number of days the Amazon GuardDuty medium severity findings are allowed to stay non archived. The default is 7 days. daysHighSev The number of days Amazon GuardDuty high severity findings are allowed to stay non archived. The default is 1 day.		
71	Guardduty	guardduty-enabled-centralized	Checks whether Amazon GuardDuty is enabled in your AWS account and region. If you provide an AWS account for centralization, the rule evaluates the Amazon GuardDuty results in the centralized account. The rule is COMPLIANT when Amazon GuardDuty is enabled.	Configuration changes	CentralMonitoringAccount (optional) Specify 12-digit AWS Account for centralization of Amazon GuardDuty results.		
72	IAM	iam-group-has-users-check	Checks whether IAM groups have at least one IAM user.	Configuration changes	None		

Sr.No.	Service Name	Config Rule Name	Description	Trigger type	Required Parameters	Parameter Value	Required (Y/N/TBD)
73	IAM	iam-password-policy	Checks whether the account password policy for IAM users meets the specified requirements.	Periodic	RequireUppercaseCharacters Require at least one uppercase character in password. RequireLowercaseCharacters Require at least one lowercase character in password. RequireSymbols Require at least one symbol in password. RequireNumbers Require at least one number in password. MinimumPasswordLength Password minimum length. PasswordReusePrevention Number of passwords before allowing reuse. MaxPasswordAge Number of days before password expiration.		
74	IAM	iam-policy-blacklisted-check	Checks whether for each IAM resource, a policy ARN in the input parameter is attached to the IAM resource. The rule is NON_COMPLIANT if the policy ARN is attached to the IAM resource. AWS Config marks the resource as COMPLIANT if the IAM resource is part of the exceptionList parameter irrespective of the presence of the policy ARN.	Configuration changes	policyArns Comma-separated list of policy ARNs. exceptionList Comma-separated list IAM users, groups, or roles that are exempt from this rule. For example, users:[user1;user2], groups:[group1;group2], roles:[role1;role2;role3].		

Sr.No.	Service Name	Config Rule Name	Description	Trigger type	Required Parameters	Parameter Value	Required (Y/N/TBD)
75	IAM	iam-policy-in-use	Checks whether the IAM policy ARN is attached to an IAM user, or an IAM group with one or more IAM users, or an IAM role with one or more trusted entity.	Periodic	policyArn (mandatory) An IAM policy Amazon Resource Name (ARN) to be checked policyUsageType (optional) Specify the policy to be attached as an IAM user, IAM group, or IAM role. Valid values are IAM_USER, IAM_GROUP, IAM_ROLE, or ANY. Default value is ANY.		
76	IAM	iam-policy-no-statements-with-admin-access	Checks the IAM policies that you create, such as identity-based or resource-based policies, for Allow statements that grant permissions to all actions on all resources. The rule is NON_COMPLIANT if any policy statement includes "Effect": "Allow" with "Action": "*" over "Resource": "*".This rule checks only the IAM policies that you create. It does not check IAM Managed Policies. When you enable the rule, this rule checks all of the customer managed policies in your account, and all new policies that you create.	Configuration changes	None		
77	IAM	iam-role-managed-policy-check	Checks that AWS Identity and Access Management (IAM) policies in a list of policies are attached to all AWS roles. The rule is NON_COMPLIANT if the IAM managed policy is not attached to the IAM role	Configuration changes	managedPolicyNames Comma-separated list of AWS managed policy ARNs.		
78	IAM	iam-root-access-key-check	Checks whether the root user access key is available. The rule is COMPLIANT if the user access key does not exist.	Periodic	None		
79	IAM	iam-user-group-membership-check	Checks whether IAM users are members of at least one IAM group.	Configuration changes	groupName Comma-separated list of IAM groups in which IAM users must be members.		

Sr.No.	Service Name	Config Rule Name	Description	Trigger type	Required Parameters	Parameter Value	Required (Y/N/TBD)
80	IAM	iam-user-mfa-enabled	Checks whether the AWS Identity and Access Management users have multi-factor authentication (MFA) enabled.	Periodic	None		
81	IAM	iam-user-no-policies-check	Checks that none of your IAM users have policies attached. IAM users must inherit permissions from IAM groups or roles.	Configuration changes	None		
82	IAM	iam-user-unused-credentials-check	Checks whether your AWS Identity and Access Management (IAM) users have passwords or active access keys that have not been used within the specified number of days you provided. Re-evaluating this rule within 4 hours of the first evaluation will have no effect on the results.	Periodic	maxCredentialUsageAge Maximum number of days within which a credential must be used. The default value is 90 days.		
83	MFA	mfa-enabled-for-iam-console-access	Checks whether AWS Multi-Factor Authentication (MFA) is enabled for all AWS Identity and Access Management (IAM) users that use a console password. The rule is COMPLIANT if MFA is enabled.	Periodic	None		
84	MFA	root-account-hardware-mfa-enabled	Checks whether your AWS account is enabled to use multi-factor authentication (MFA) hardware device to sign in with root credentials. The rule is NON_COMPLIANT if any virtual MFA devices are permitted for signing in with root credentials.	Periodic	None		
85	MFA	root-account-mfa-enabled	Checks whether users of your AWS account require a multi-factor authentication (MFA) device to sign in with root credentials.	Periodic	None		
86	AWS Shield	shield-advanced-enabled-autorenew	Checks whether AWS Shield Advanced is enabled in your AWS account and this subscription is set to automatically renew.The API endpoint of AWS Shield Advanced is only available in us-east-1. This rule should only be scheduled to run in the us-east-1 Region.	Periodic	None		

Sr.No.	Service Name	Config Rule Name	Description	Trigger type	Required Parameters	Parameter Value	Required (Y/N/TBD)
87	AWS Shield	shield-drt-access	Verify that DDoS response team (DRT) can access AWS account. The rule is NON_COMPLIANT if AWS Shield Advanced is enabled but the role for DRT access is not configured.Only available in US East (N. Virginia) region	Periodic	None		
88	EBS	ebs-snapshot-public-restorable-check	Checks whether Amazon Elastic Block Store snapshots are not publicly restorable. The rule is NON_COMPLIANT if one or more snapshots with the RestorableByUserIds field is set to all. If this field is set to all, then Amazon EBS snapshots are public.	Periodic	None		
89	EFS	efs-encrypted-check	Checks whether Amazon Elastic File System (Amazon EFS) is configured to encrypt the file data using AWS Key Management Service (AWS KMS). The rule is NON_COMPLIANT if the encrypted key is set to false on DescribeFileSystems or if the KmsKeyId key on DescribeFileSystems does not match the KmsKeyId parameter.	Periodic	kmskeyid (optional) Amazon Resource Name (ARN) of the AWS KMS key that is used to encrypt the Amazon EFS file system.		
90	ELB	elb-deletion-protection-enabled	Checks whether Elastic Load Balancing has deletion protection enabled. The rule is NON_COMPLIANT if deletion_protection.enabled is false.	Configuration changes	None		
91	EMR	emr-master-no-public-ip	Checks whether Amazon Elastic MapReduce (EMR) clusters' master nodes have public IPs. The rule is NON_COMPLIANT if the master node has a public IP. This rule checks clusters that are in RUNNING or WAITING state.	Periodic	None		

Sr.No.	Service Name	Config Rule Name	Description	Trigger type	Required Parameters	Parameter Value	Required (Y/N/TBD)
92	EMR	emr-kerberos-enabled	Checks that Amazon EMR clusters have Kerberos enabled. The rule is NON_COMPLIANT if a security configuration is not attached to the cluster or the security configuration does not satisfy the specified rule parameters.	Periodic	ticketLifetimeInHours (optional) Period for which Kerberos ticket issued by cluster's KDC is valid. realm (optional) Kereberos realm name of the other realm in the trust relationship. domain (optional) Domain name of the other realm in the trust relationship. adminServer (optional) Fully qualified domain of the admin server in the other realm of the trust relationship. kdcServer (optional) Fully qualified domain of the KDC server in the other realm of the trust relationship.		

Sr.No.	Service Name	Config Rule Name	Description	Trigger type	Required Parameters	Parameter Value	Required (Y/N/TBD)
93	S3	s3-account-level-public-access-blocks	Checks whether the required public access block settings are configured from account level. The rule is only NON_COMPLIANT when the fields set below do not match the corresponding fields in the configuration item.	Configuration changes	ignorePublicAcls (Optional) Either enforced (True) or not (False). The default is True. blockPublicPolicy (Optional) Either enforced (True) or not (False). The default is True. blockPublicAcls (Optional) Either enforced (True) or not (False). The default is True. restrictPublicBuckets (Optional) Either enforced (True) or not (False). The default is True.		
94	S3	s3-bucket-blacklisted-actions-prohibited*	Checks that the Amazon Simple Storage Service bucket policy does not allow blacklisted bucket-level and object-level actions on resources in the bucket for principals from other AWS accounts. For example, the rule checks that the Amazon S3 bucket policy does not allow another AWS account to perform any s3:GetBucket* actions and s3:DeleteObject on any object in the bucket. The rule is NON_COMPLIANT if any blacklisted actions are allowed by the Amazon S3 bucket policy.	Configuration changes	blacklistedactionpatterns Comma-separated list of blacklisted action patterns, for example, s3:GetBucket* and s3:DeleteObject.		
95	S3	s3-bucket-logging-enabled	Checks whether logging is enabled for your S3 buckets.	Configuration changes	targetBucket Target S3 bucket for storing server access logs. targetPrefix Prefix of the target S3 bucket for storing server access logs.		

Sr.No.	Service Name	Config Rule Name	Description	Trigger type	Required Parameters	Parameter Value	Required (Y/N/TBD)
96	S3	s3-bucket-policy-grantee-check*	Checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or VPCs that you provide. The rule is COMPLIANT if a bucket policy is not present.	Configuration changes	awsPrincipals Comma-separated list of principals such as IAM User ARNs, IAM Role ARNs and AWS accounts, for example 'arn:aws:iam::111122223333:user/Alice, arn:aws:iam::444455556666:role/Bob, 123456789012'. servicePrincipals Comma-separated list of service principals, for example 'cloudtrail.amazonaws.com, lambda.amazonaws.com'. federatedUsers Comma-separated list of identity providers for web identity federation such as Amazon Cognito and SAML identity providers. For example, you can provide as parameter 'cognito-identity.amazonaws.com, arn:aws:iam::111122223333:saml-provider/my-provider'. ipAddresses Comma-separated list of CIDR formatted IP addresses, for example '10.0.0.1, 192.168.1.0/24, 2001:db8::/32'. vpcIds Comma-separated list of Amazon Virtual Private Cloud (Amazon VPC) IDs, for example 'vpc-1234abc0, vpc-ab1234c0'.		

Sr.No.	Service Name	Config Rule Name	Description	Trigger type	Required Parameters	Parameter Value	Required (Y/N/TBD)
97	S3	s3-bucket-policy-not-more-permissive*	Verifies that your Amazon Simple Storage Service bucket policies do not allow other inter-account permissions than the control Amazon S3 bucket policy that you provide.	Configuration changes	controlPolicy Amazon S3 bucket policy that defines an upper bound on the permissions of your S3 buckets. The policy can be a maximum of 1024 characters long.		
98	S3	s3-bucket-public-read-prohibited*	Checks that your Amazon S3 buckets do not allow public read access. The rule checks the Block Public Access settings, the bucket policy, and the bucket access control list (ACL).	Configuration changes	None		
99	S3	s3-bucket-public-write-prohibited*	Checks that your Amazon S3 buckets do not allow public write access. The rule checks the Block Public Access settings, the bucket policy, and the bucket access control list (ACL).	Configuration changes	None		
100	S3	s3-bucket-replication-enabled	Checks whether S3 buckets have cross-region replication enabled.	Configuration changes	None		
101	S3	s3-bucket-server-side-encryption-enabled*	Checks that your Amazon S3 bucket either has Amazon S3 default encryption enabled or that the S3 bucket policy explicitly denies put-object requests without server side encryption.	Configuration changes	None		
102	S3	s3-bucket-ssl-requests-only*	Checks whether S3 buckets have policies that require requests to use Secure Socket Layer (SSL).	Configuration changes	None		
103	S3	s3-bucket-versioning-enabled	Checks whether versioning is enabled for your S3 buckets. Optionally, the rule checks if MFA delete is enabled for your S3 buckets.	Configuration changes	isMfaDeleteEnabled MFA delete is enabled for your S3 buckets.		

Sr.No.	Service Name	Config Rule Name	Description	Trigger type	Required Parameters	Parameter Value	Required (Y/N/TBD)
104	RDS	db-instance-backup-enabled	Checks whether RDS DB instances have backups enabled. Optionally, the rule checks the backup retention period and the backup window.	Configuration changes	backupRetentionPeriod Retention period for backups. preferredBackupWindow Time range in which backups are created. checkReadReplicas Checks whether RDS DB instances have backups enabled for read replicas.		
105	DynamonDB	dynamodb-autoscaling-enabled	Checks whether Auto Scaling or On-Demand is enabled on your DynamoDB tables and/or global secondary indexes. Optionally you can set the read and write capacity units for the table or global secondary index.	Periodic	minProvisionedReadCapacity The minimum number of units that should be provisioned with read capacity in the Auto Scaling group. minProvisionedWriteCapacity The minimum number of units that should be provisioned with write capacity in the Auto Scaling group. maxProvisionedReadCapacity The maximum number of units that should be provisioned with read capacity in the Auto Scaling group. maxProvisionedWriteCapacity The maximum number of units that should be provisioned with write capacity in the Auto Scaling group. targetReadUtilization The target utilization percentage for read capacity. Target utilization is		

Sr.No.	Service Name	Config Rule Name	Description	Trigger type	Required Parameters	Parameter Value	Required (Y/N/TBD)
					expressed in terms of the ratio of consumed capacity to provisioned capacity. targetWriteUtilization The target utilization percentage for write capacity. Target utilization is expressed in terms of the ratio of consumed capacity to provisioned capacity.		
106	DynamonDB	dynamodb-table-encryption-enabled	Checks whether the Amazon DynamoDB tables are encrypted and checks their status. The rule is COMPLIANT if the status is enabled or enabling.	Configuration changes	None		

Sr.No.	Service Name	Config Rule Name	Description	Trigger type	Required Parameters	Parameter Value	Required (Y/N/TBD)
107	DynamonDB	dynamodb-throughput-limit-check	Checks whether provisioned DynamoDB throughput is approaching the maximum limit for your account. By default, the rule checks if provisioned throughput exceeds a threshold of 80% of your account limits.	Periodic	accountRCUThresholdPercentage Percentage of provisioned read capacity units for your account. When this value is reached, the rule is marked as NON_COMPLIANT. accountWCUThresholdPercentage Percentage of provisioned write capacity units for your account. When this value is reached, the rule is marked as NON_COMPLIANT.		
108	RDS	rds-enhanced-monitoring-enabled	Checks whether enhanced monitoring is enabled for Amazon Relational Database Service (Amazon RDS) instances.	Configuration changes	monitoringInterval (Optional) An integer value in seconds between points when enhanced monitoring metrics are collected for the database instance. The valid values are 1, 5, 10, 15, 30, and 60.		
109	RDS	rds-instance-public-access-check	Check whether the Amazon Relational Database Service instances are not publicly accessible. The rule is NON_COMPLIANT if the publiclyAccessible field is true in the instance configuration item.	Configuration changes	None		
110	RDS	rds-multi-az-support	Checks whether high availability is enabled for your RDS DB instances.	Configuration changes	None		
111	RDS	rds-snapshots-public-prohibited	Checks if Amazon Relational Database Service (Amazon RDS) snapshots are public. The rule is NON_COMPLIANT if any existing and new Amazon RDS snapshots are public.	Configuration changes	None		
112	RDS	rds-storage-encrypted	Checks whether storage encryption is enabled for your RDS DB instances.	Configuration changes	kmsKeyId KMS key ID or ARN used to encrypt the storage.		

Sr.No.	Service Name	Config Rule Name	Description	Trigger type	Required Parameters	Parameter Value	Required (Y/N/TBD)
113	Redshift	redshift-cluster-configuration-check	Checks whether Amazon Redshift clusters have the specified settings.	Configuration changes	clusterDbEncrypted Database encryption is enabled. nodeTypes Specify node type. loggingEnabled Audit logging is enabled.		
114	Redshift	redshift-cluster-maintenancesettings-check	Checks whether Amazon Redshift clusters have the specified maintenance settings.	Configuration changes	allowVersionUpgrade Allow version upgrade is enabled. preferredMaintenanceWindow Scheduled maintenance window for clusters (for example, Mon:09:30-Mon:10:00). automatedSnapshotRetentionPeriod Number of days to retain automated snapshots.		
115	Redshift	redshift-cluster-public-access-check	Checks whether Amazon Redshift clusters are not publicly accessible. The rule is NON_COMPLIANT if the publiclyAccessible field is true in the cluster configuration item.	Configuration changes	None		
116	Machine Learning	sagemaker-endpoint-configuration-kms-key-configured	Checks whether AWS Key Management Service (KMS) key is configured for an Amazon SageMaker endpoint configuration. The rule is NON_COMPLIANT if KmsKeyId is not specified for the Amazon SageMaker endpoint configuration.	Periodic	kmsKeyArns (Optional) Comma-separated list of specific AWS KMS key ARNs allowed for an Amazon SageMaker endpoint configuration.		
117	Machine Learning	sagemaker-notebook-no-direct-internet-access	Checks whether direct internet access is disabled for an Amazon SageMaker notebook instance. The rule is NON_COMPLIANT if Amazon SageMaker notebook instances are internet-enabled.	Periodic	None		

Sr.No.	Service Name	Config Rule Name	Description	Trigger type	Required Parameters	Parameter Value	Required (Y/N/TBD)
118	Machine Learning	sagemaker-notebook-kms-configured	Check whether an AWS Key Management Service (KMS) key is configured for Amazon SageMaker notebook instance. The rule is not NON_COMPLIANT if kmsKeyId is not specified for the Amazon SageMaker notebook instance.	Periodic	keyArns (optional) Comma-separated list of allowed AWS KMS key IDs allowed for Amazon SageMaker notebook instance.		
119	Analytics	elasticache-redis-cluster-automatic-backup-check	Check if the Amazon ElastiCache Redis clusters have automatic backup turned on. The rule is NON_COMPLIANT if the SnapshotRetentionLimit for Redis cluster is less than the SnapshotRetentionPeriod parameter. For example: If the parameter is 15 then the rule is non-compliant if the snapshotRetentionPeriod is between 0-15.	Periodic	snapshotRetentionPeriod (Optional) Minimum snapshot retention period in days for Redis cluster. The default is 15 days.		
120	Analytics	elasticsearch-encrypted-at-rest	Checks whether Amazon Elasticsearch Service (Amazon ES) domains have encryption at rest configuration enabled. The rule is NON_COMPLIANT if the EncryptionAtRestOptions field is not enabled.	Periodic	None		
121	Analytics	elasticsearch-in-vpc-only	Checks whether Amazon Elasticsearch Service (Amazon ES) domains are in Amazon Virtual Private Cloud (Amazon VPC). The rule is NON_COMPLIANT if the Amazon ES domain endpoint is public.	Periodic	None		
122	DMS	dms-replication-not-public	Checks whether AWS Database Migration Service replication instances are public. The rule is NON_COMPLIANT if PubliclyAccessible field is true.	Periodic	None		

Appendix 2. CloudWatch Metrics List

Sr No	Metric Type	CloudWatch Metric List
1	**Elastic Compute Cloud (EC2)**	
		CPU Utilization %
		Disk ReadBytes (Bytes)
		Disk WriteBytes (Bytes)
		NetworkIn (Bytes)
		NetworkOut (Bytes)
		Disk Space Utilization
		Memory Utilization
		Service Health & Schedule Event by Region
		Instance State Check
		System state Check
2	**ELB**	Active connection count
		ConsumedLCUs
		HTTPCode_ELB_3XX_Count
		HTTPCode_ELB_4XX_Count
		HTTPCode_ELB_5XX_Count
		NewConnectionCount
		RejectedConnectionCount
		SurgeQueueLength
		SpilloverCount
		HealthyHostCount
		UnHealthyHostCount
		NonStickyRequestCount
		RequestCountPerTarget
		TargetConnectionErrorCount
		TargetResponseTime
3	**AutoScaling**	GroupMinSize
		GroupMaxSize
		GroupDesiredCapacity
		GroupInServiceInstances
		GroupPendingInstances
		GroupStandbyInstances
		GroupTerminatingInstances
		GroupTotalInstances
4	**Lambda**	Duration (Elaspsed Time)
		Errors
		Invocations
		Dead-letter errors

Sr No	Metric Type	CloudWatch Metric List
		Concurrent executions
		Throttles
5	EBS	VolumeStatus
		IOPerformance (only for io1 type)
		VolumeReadBytes
		VolumeWriteBytes
		VolumeReadOps
		VolumeWriteOps
		VolumeIdleTime
		VolumeQueueLength
		VolumeThroughputPercentage (only for io1 type)
6	RDS	ReadIOPS
		WriteIOPS
		DiskQueueDepth
		ReadLatency
		WriteLatency
		Read Throughput
		Write Throughput
		CPUUtilization
		DatabaseConnections
		ReplicaLag
7	DynamoDB	SuccessfulRequest-Latency
		ProvisionedReadCapacityUnits
		ProvisionedWriteCapacityUnits
		ReadThrottleEvents
		WriteThrottleEvents
		ConsumedReadCapacityUnits
		ConsumedWriteCapacityUnits
		SystemErrors
		UserErrors
8	EFS	BurstCreditBalance
		ClientConnections
		DataReadIOBytes
		DataWriteIOBytes
		MetadataIOBytes
		PercentIOLimit
		PermittedThroughput
		TotalIOBytes
9	S3	BucketSizeBytes
		NumberOfObjects
		AllRequests
		BytesDownloaded

Sr No	Metric Type	CloudWatch Metric List
		BytesUploaded
		4xxErrors
		5xxErrors
		FirstByteLatency
		TotalRequestLatency
		ReplicationLatency