Enterprise Landing Zone: Colombia Customer Stories

Francisco Moreno

OCI 11x (4 Pro), AWS 4x (Trainer and 2 Pro), GCP 1x, Huawei 1x, Terraform

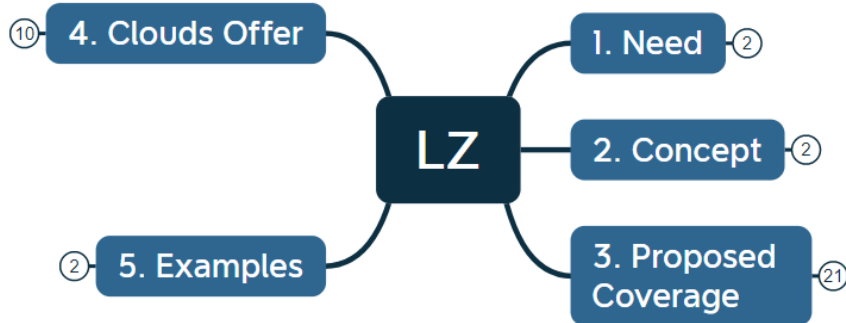Lead System Engineer, EPAM

Carlos Ribón

AWS Assoc, Terraform, CCNP

ScrumMaster, CCNP

Sr, Engineer Consultant, Oracle

fmorenod81/devopscustomerstories2023 (github.com)

JULY 2023

Agenda

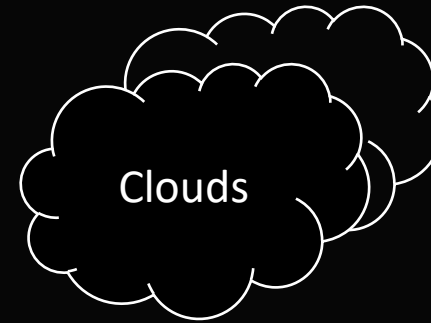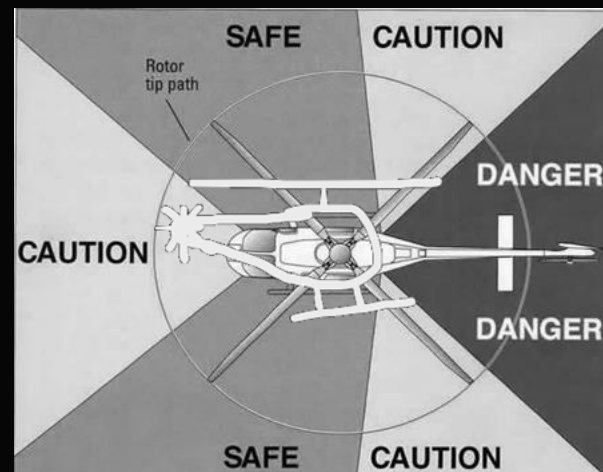|	
11:10 – 11:12	Need of a Landing Zone (LZ)
11:12 – 11:14	Concept
11:15 – 11:20	Proposed Coverage
11:25 – 11:35	Clouds Offer: AWS and Oracle Cloud
11:35 – 11:50	Colombia Cases: Telco and Banking Holding
11:50 – 11:55	Q&A

Need

Viewpoints involved
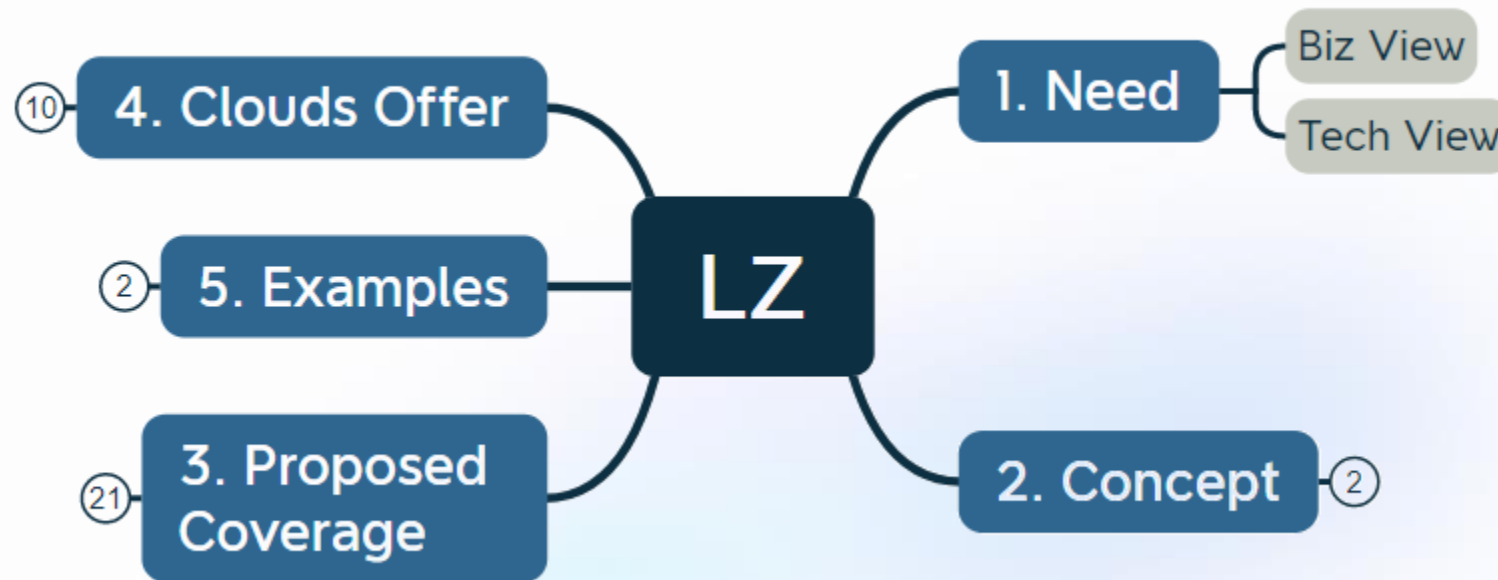
Viewpoints

Clouds

Business View

Landing Zone (LZ)

Technology View

LZ: Template for migrating or creating cloud resources fulfilling company' requirements

Business View

Current status

Enabler: Improvement?

Policies   Procedures

- The Landing Zone will show current organization structure: People, procedures, compliance standards, artifacts >> Company, Areas, Teams, Squads, Roles

- Business approved additional efforts to modify only if it add value or simplify operation.

Escalation Matrix — Networking Services

Issue: Customer can not export files to the desired format.

	Role	Time	Response	Escalation
Level 1	Customer Support Representative	10-15 min	• Live support to solve the problem	• Unable to resolve • Request to speak to manager
Level 2	Customer Support Manager	15-60 min	• Live support with support team working on resolution • Get customer details for ticket logging and follow-up	• Unable to resolve • Need skills beyond support team capabilities
Level 3	Account Manager	1-2 hours	• Review issue • Assign immediate task delegation • Attempt resolution • Document issue and attempted hot fixes in detail	• Unable to resolve • Customer threatens to leave • Customer threatens bad review
Level 4	Product Manager	Half a business day	• Review issue • Offer incentives to customer • Document conversation	• Unable to resolve • Customer requests to speak to higher level management • Customer initiates process of closing account
Level 5	Director of Product	1-2 business days	• Review issue • Apologize to customer and ensure their issue is not taken lightly • Request and document feedback • Determine if any immediate resolution is possible regarding customer account status	• Customer proceeds with closing account • Alternative to keep account is agreed upon
Level 6	Stakeholder	1-3 business days	• Review issue • Apologize to customer • Formulate improvements to product that directly prevents the issue from arising again • Finalize account cancellation • Create a timeline to keep customer in the loop about future product upgrades	• Formal approval from senior management needed
Level 7	Senior Management	Immediate resolution	• Review issue • Sign off on course o... • Consider hirin... solve issu...	

Example of a Procedure:

- Roles
- Permissions
- Period to call

Technology View

Services
Templates
Best Practices

- ➢ CSP provides service and templates based on industry best practices.

- ➢ The Cloud Architect' mind has focus on experience on common projects, but he doesn't think in special cases (exceptions), therefore it is a difficult on the coverage.

- ➢ It points a simple operations on self-Service or automated toolset.

Methodology

Evolve and
tune workload
templates

Start a
Foundational
Landing Zone

Understand the
enterprise
structure: Roles,
Artifacts &
Procedures
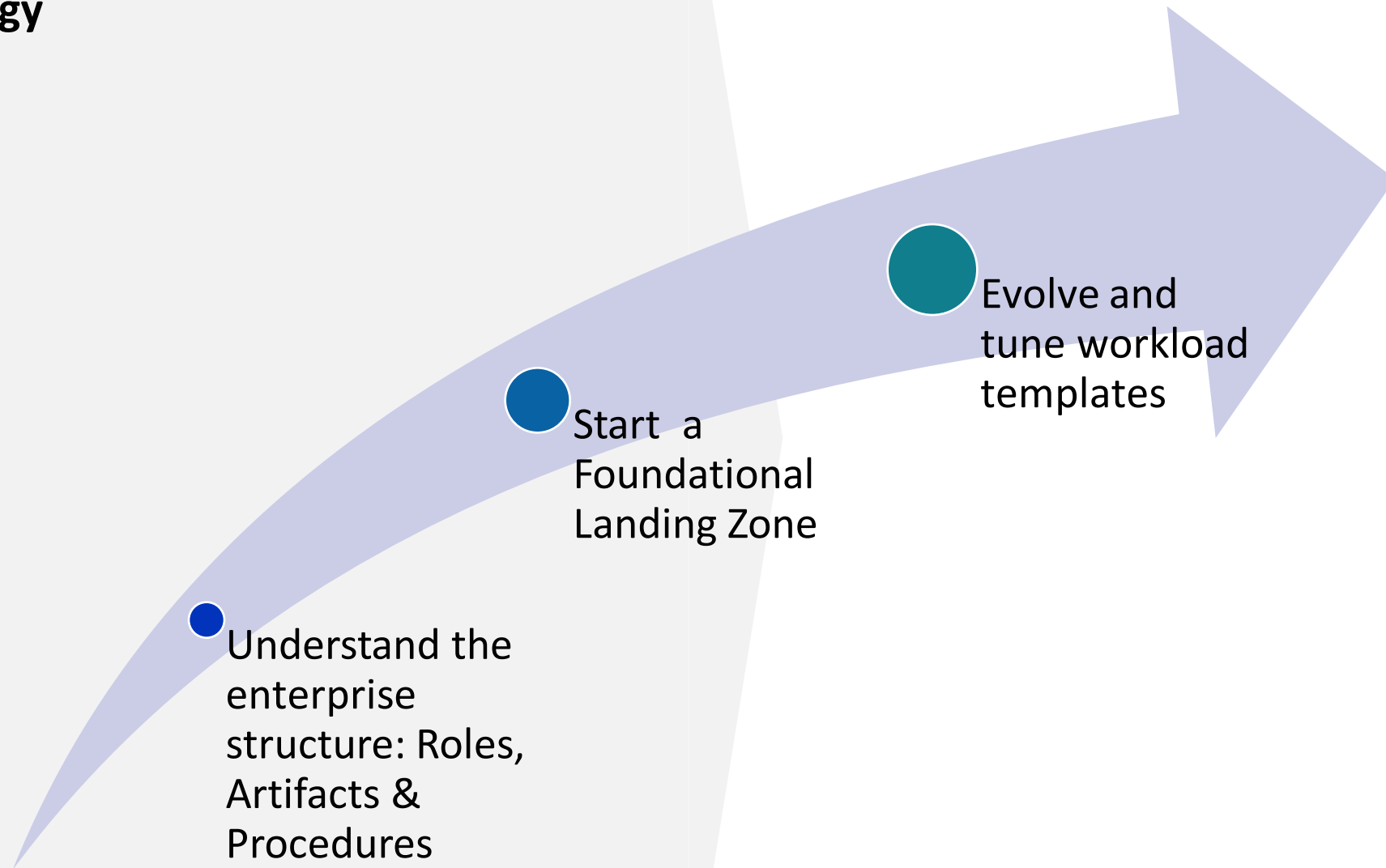
Concept

Define the scope

My own definition

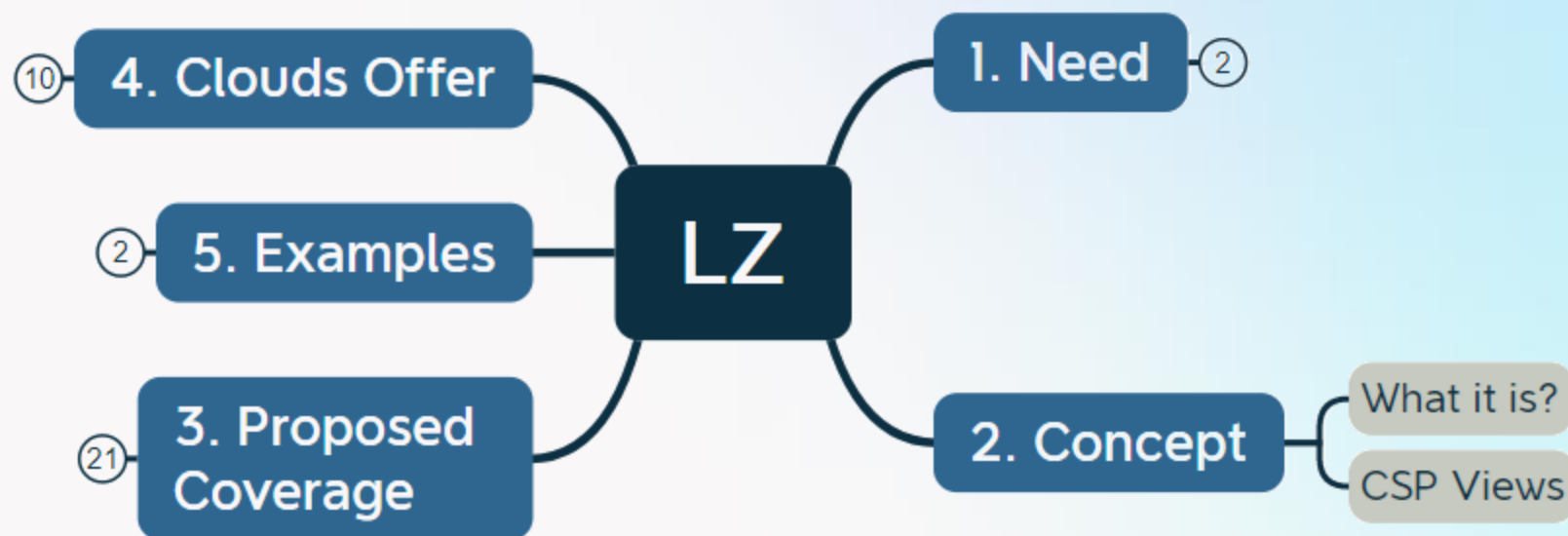Purpose-Built Cloud setup offering security, automation, controlled and scalable resources, and architectural framework at enterprise level.

a well-architected, multi-account AWS environment that is scalable and secure.

is a secured, deployment-ready cloud environment.

(…) provides baseline architecture and best practices for you to deploy new projects and workloads quickly and securely in OCI

is an environment that follows key design principles across eight design areas. These design principles accommodate all application portfolios and enable application migration, modernization, and innovation at scale.

(..) help your enterprise deploy, use, and scale Google Cloud services more securely. (…) are dynamic and grow as your enterprise adopts more cloud-based workloads over time.

Principles on a framework (CAF*)

Enterprise: Wide, Reliable

Quick/Scalable: Availability

Secure: Compliance & DR

03

Coverage

Areas to cover
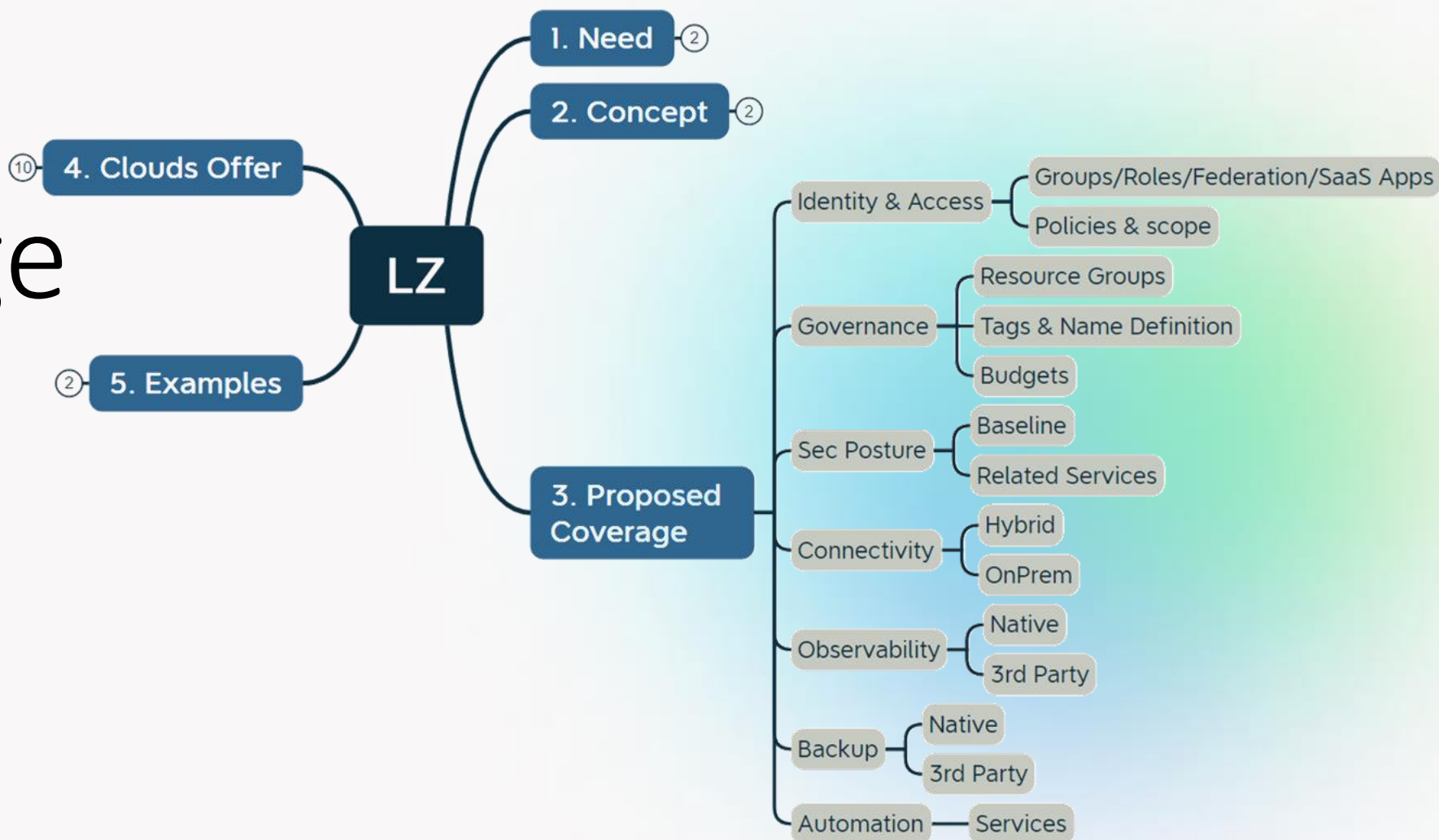
Identity & Access

IAM:
AutN & AutZ
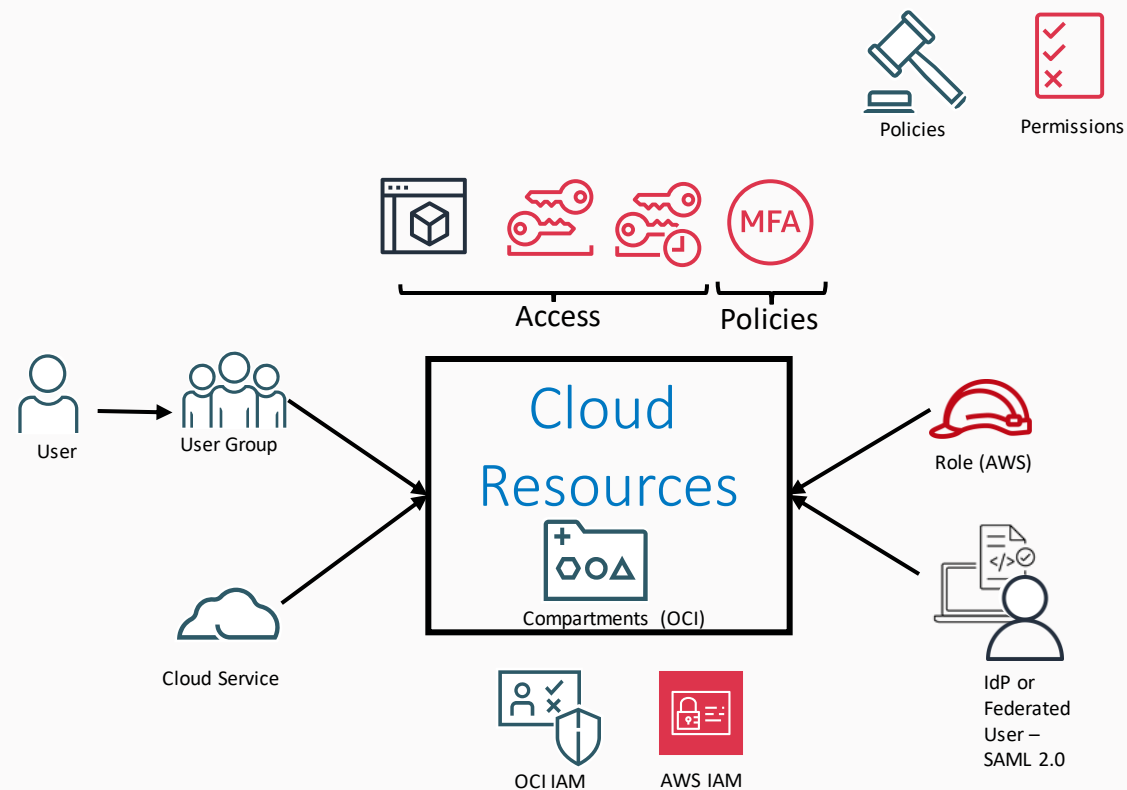
- Cloud Resources

- Principals/Entities: Identity Domains (OCI) and Federation.

- Policies and Access of Principals

- Relation between both: Permissions

Governance

Resources Groups

Reflects org chart of the company based on companies, areas and they match on Role-based Policies.

Usually common/transversal services are separated: networking, databases, security, etc.
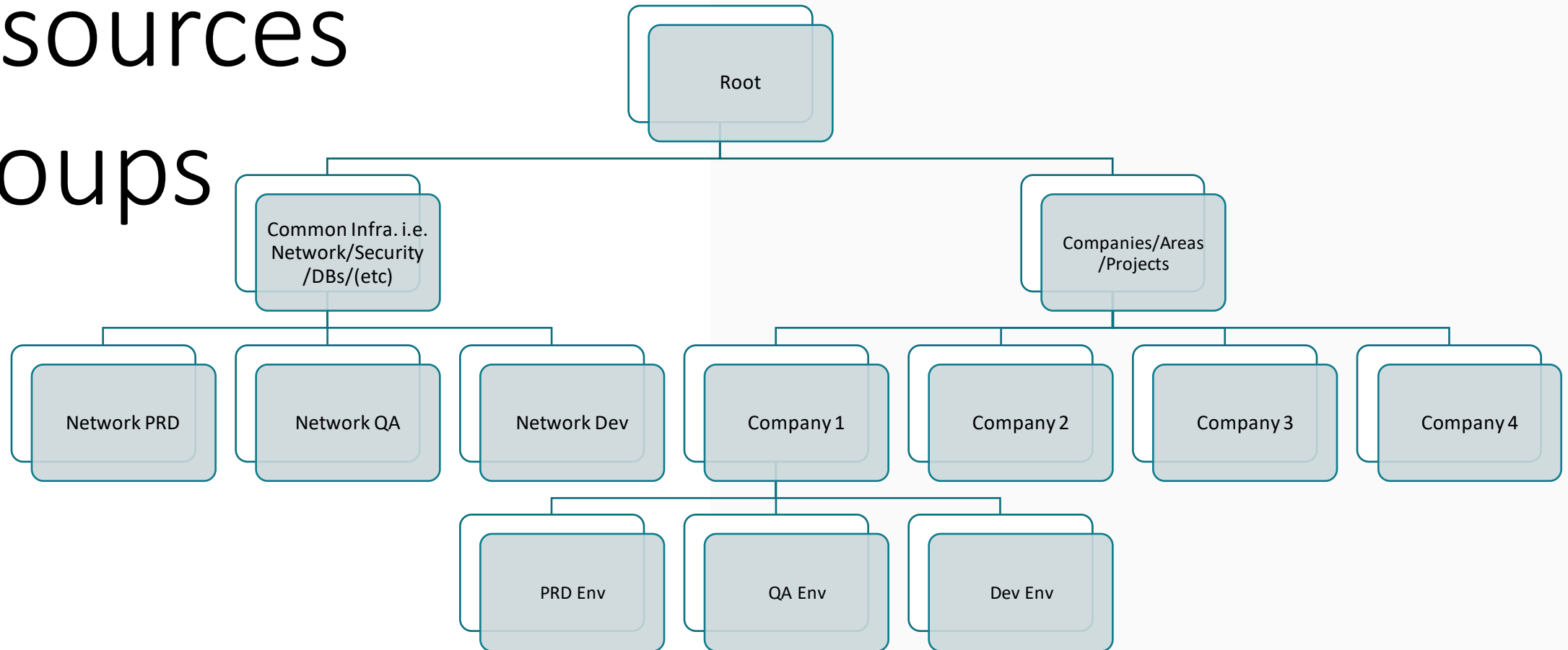
Identity & Access
Policies Scope

Governance
Rules (OCI)

Service Control
Policies (AWS)   Organization   AWS Organizations

Account Policies:

- Identity-Based Policies
- Resource-Based Policies (AWS)
- Permission Boundary (AWS)

Multiaccount Policies:

- Service Control Policies (AWS)
  Governance Rules (OCI)
- Resource-Based Policies (AWS)

Account 2

Account 1

Attach to Principal

Identity-Based Policy

OCI IAM   AWS IAM   **Resource on Statement**

Identities
(Who requests)

Permissions
(what is requested by the Identity)

Resource-Based Policy

Compartments

Policies

Groups   Instance

Resources

Users

Governance

Tags

A Tag Namespace is a container for tag keys with tag key definitions

Tag key definition specifies its key (environment) and what types of values are allowed (string, number, text, date, enumerations, etc.)

Example:

Namespace Definition: Operations

Key Definition: Environment

➡

Tag
Operations.Environment = "Production"

Namespace   Key   Value
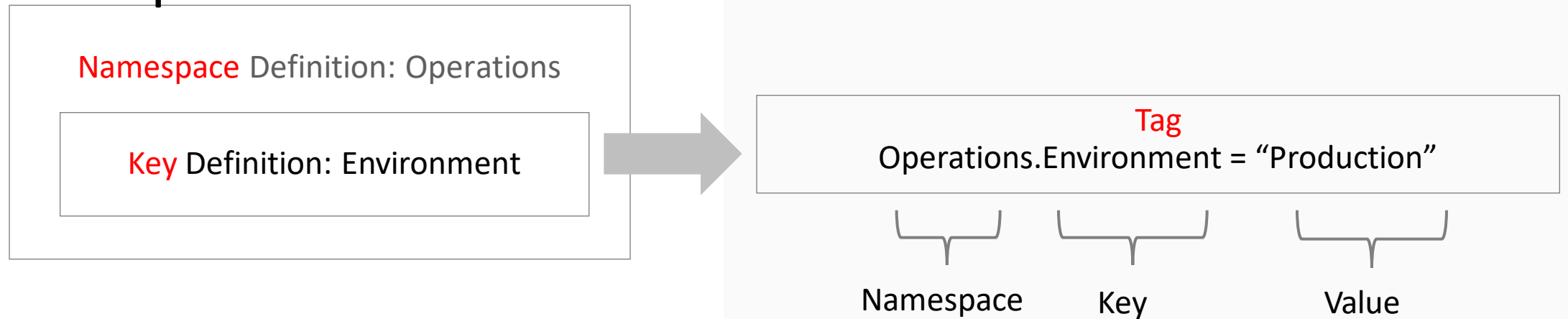
Governance

Tags and Name Definition

Can extend to:

- Operations Control, i.e. In GCP, the tags are used for Firewall Rules.

- Country: CO, EC, US, AU → 2 letters, opt.

- Cloud Region: us-east-1 → 3 letters: ASH or E01

- Resource Group: SHS, NET, SEC, WKL → 3 letters

- Serial Number: By Project or Scaling Group

- Environment: 7 env → 3 letters: DEV, QAT, UAT, PRD

- Services: End → OBJ, ADB, LB, INS

- **Security**
  - Exposition
    - *Public – Private*
  - Impact
    - *Critical – Non-critical*

- **Usage**
  - Environment
    - *Dev –Test - Prd*
  - Application
    - *App1, App2*

- **Cost**
  - Cost Center
    - *40001, 40002*
  - Running
    - *7X24, 8X5, 5X12*

Server: ASHWKL###DEVINS001

Governance

Budgets

Its means Cost control or Cost Explorer.

A tag model can provide reports in near-real-time.

A Proof-of-Concept and Sandbox budget s can be useful on startups or Dev Areas.

AWS Budgets

AWS Cost & Usage Report

AWS Cost Explorer

Monitoring

Alarms

Tagging

Cloud Advisor

Security Posture

Audit

Auditing

AWS
CloudTrail

CloudTrail Lake

Any API calls (any source) are logged and made available to customers.

API for listing audit events: Unique ID for principal, involved cloud resource, status change, timestamp and parameters (request/ response).

New events available in short time (i.e., 15 mins in OCI)

X days of history by default and configurable retention period (i.e., 90 days on OCI and up to 1 year)

Coverage for all regions using **centralized repository** (i.e., AWS)

Searchable via the Console or using another tools (AWS CloudTrail Lake)

Security Posture

Baseline

Identity & Security

Maximum Security Zone | Threat Intelligence | Cloud Guard | Vulnerability Scanning | Threat Defense | Cloud Advisor
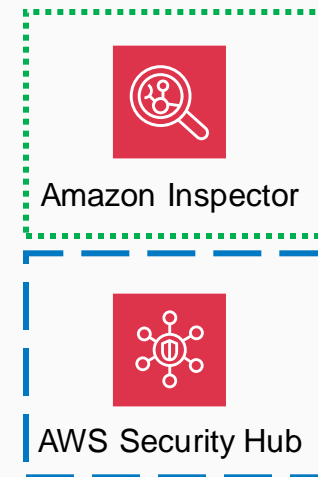
CSP Focus on Security

Several Layers for networking, development lifecycle, security posture, etc.

Centralized Repository on an account for logging

Category	Service	OCI	Info	AWS
Security	Risk and Compliance Management	- OCI **Cloud Guard** Free	Service to assess risk and compliance with regulations and industry standards based on resource usage.	- AWS Audit Manager
Security	Security Monitoring, Assessment, and Advice	- Access Governance - **Cloud Guard** Free - Security Advisor	Managed service to monitor, identify, achieve, and maintain a strong security posture. Service examines resources for security weaknesses and operators and users for risky activities. Service	- Amazon Security Lake - Amazon Detective - AWS Security Hub

Amazon GuardDuty

Amazon Inspector

Security, Identity, & Compliance
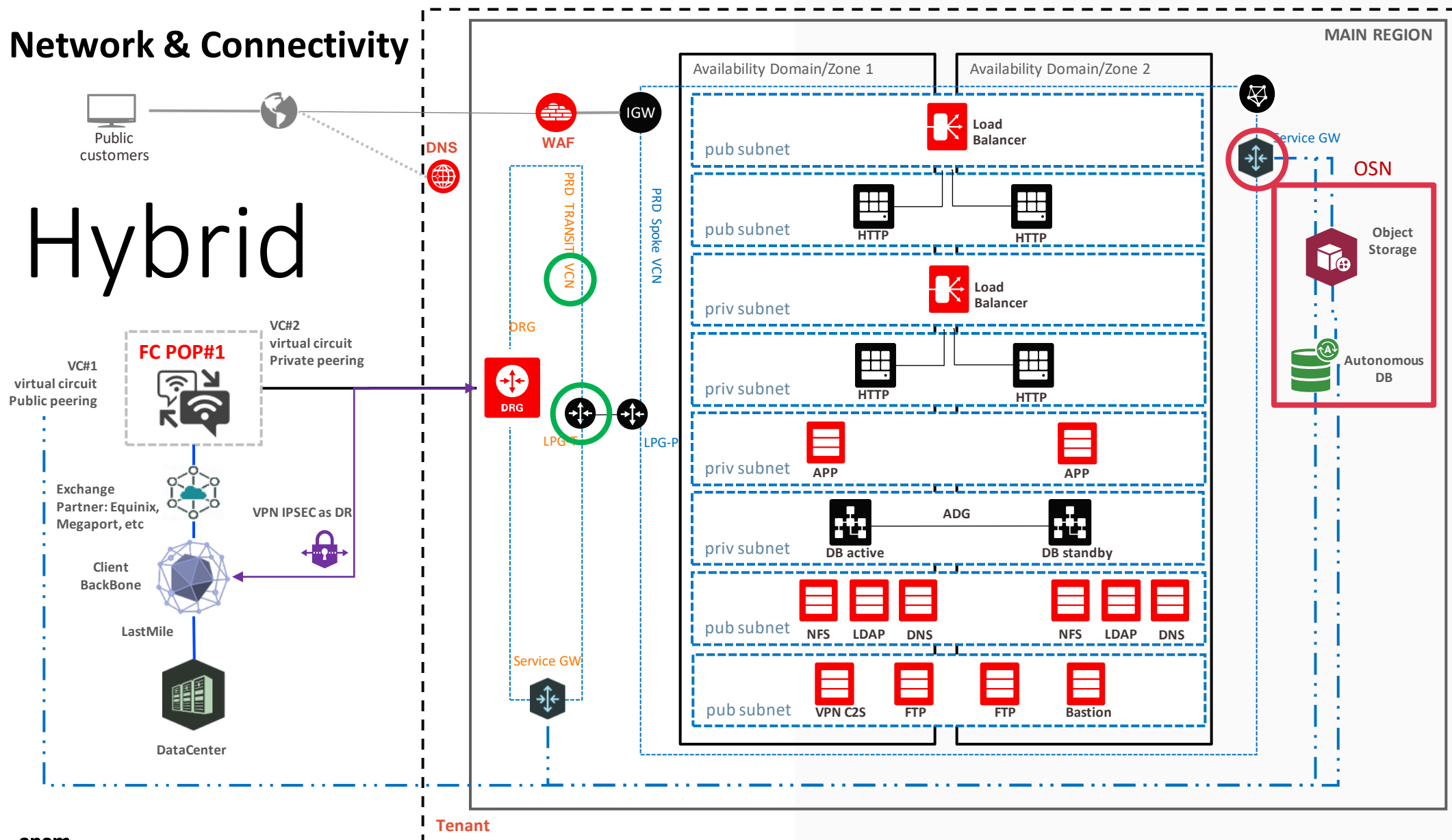
Amazon Detective

AWS Security Hub

AWS Audit Manager

Management & Governance

AWS Config

AWS Systems Manager

AWS Organizations

Network & Connectivity

Multicloud

Options:

- Native Services for Comms, i.e., Azure Interconnect

- IPSec VPN over Internet

- IPSec VPN over Dedicated Connections (No Native), i.e. Megaport between AWS & OCI

and Equinix between AWS & OCI

Region 1 (with Azure Interconnect)

VCN CD/CI

VCN Dev

VCN Test

VCN Prod

VCN Transit

Region 2

VCN CD/CI

VCN Cont

VCN Transit

Fast Connect 1 VC 1 / 2

Fast Connect 1 VC3

Fast Connect 2 VC1 / 2

VPN Site to Site 1 (Unmanaged)

VPN Site to Site 2 (Managed)

Microsoft Azure

MPLS Network

PRIMARY

GTM
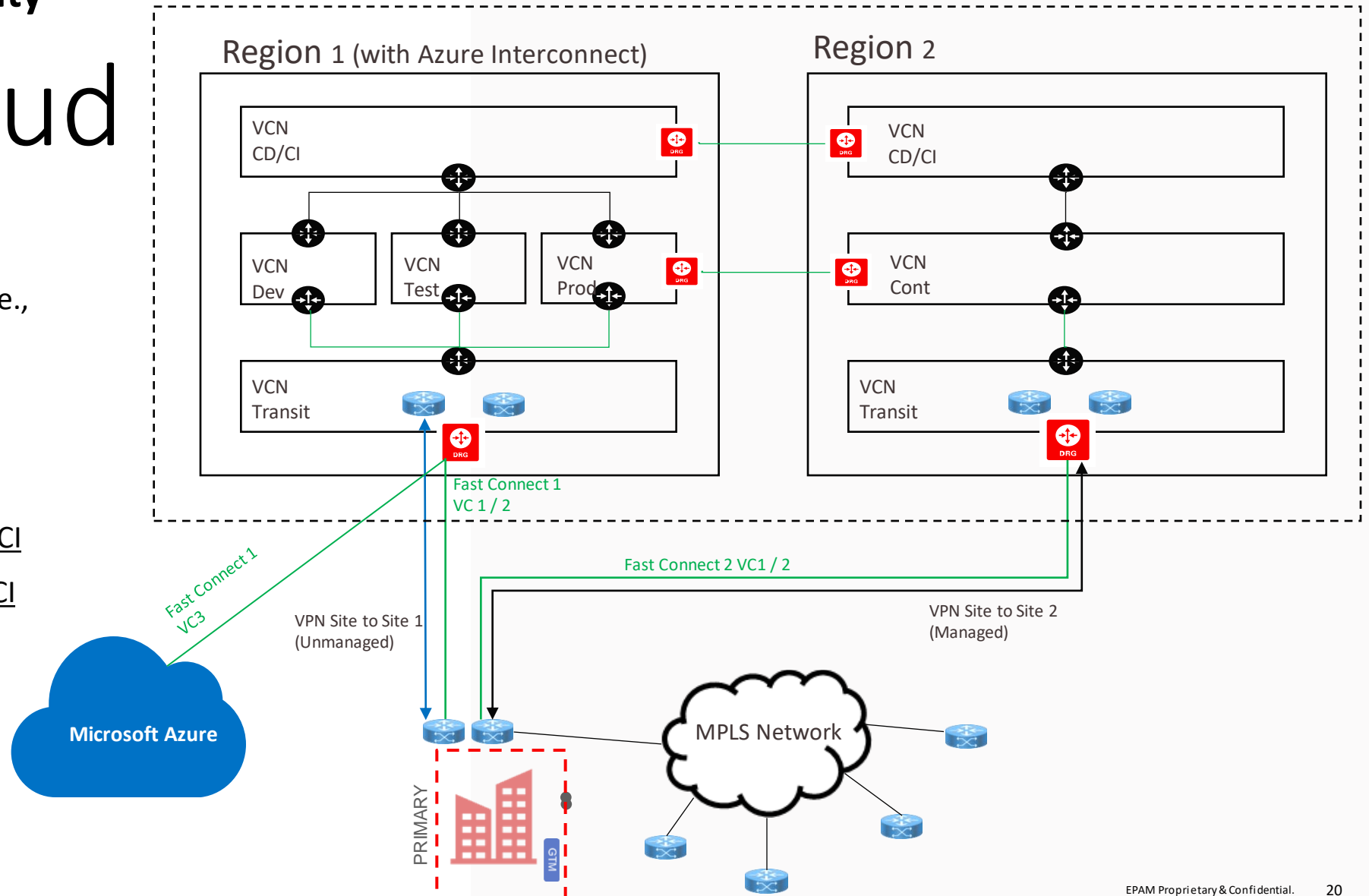
Observability

Native & 3rd Party

Native

Collection (fluentd or special agent/distro),

Aggregation (Prometheus and OpenSearch),

Visualization (Grafana and OpenSearch)

3rd Party

Standard Formats: i.e. JSON & OpenTelemetry

External Communications to 3rd Party (i.e. Splunk):

AWS

Cloudwatch Metrics Stream, Kinesis and/or Lambda.

OCI

OCI Service Connector Hub, OCI Streams

Amazon CloudWatch

AWS X-Ray

Amazon Managed Grafana

Amazon Managed Service
for Prometheus

Application
Performance
Monitoring
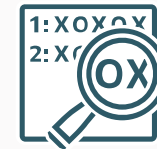
Logging

Search

Monitoring

Logging
Analytics

Backup

Native & 3rd Party

Native

Usually, CSP started with many tools specific to storage: snapshots for EBS/BV, rsync on EFS, replication and cloning for DB, etc.

There are another interesting actions: Cloning and Replication.

3rd Party:

Virtual Machine from the Marketplace and access to infrastructure: agent and agentless, i.e. Commvault.

Backup/ Restore

Block Storage Cloning

File Storage Snapshots

AWS Backup

Automation

Pipelines

Self-Service Portal for New workloads.

Customized Modules for IaC (Terraform, CloudFormation, CDK, Pulumi).

Customized Pipelines using Native Services (AWS Code Suite, OCI DevOps Services), Open Source (Jenkins) and Commercial Solutions (i.e. Github Actions, CircleCI, etc).

New Request
- IAM: Roles
- Prototype
- Tags

Container
- Code Repo
- IaC

Software
- Credentials
- Pipelines
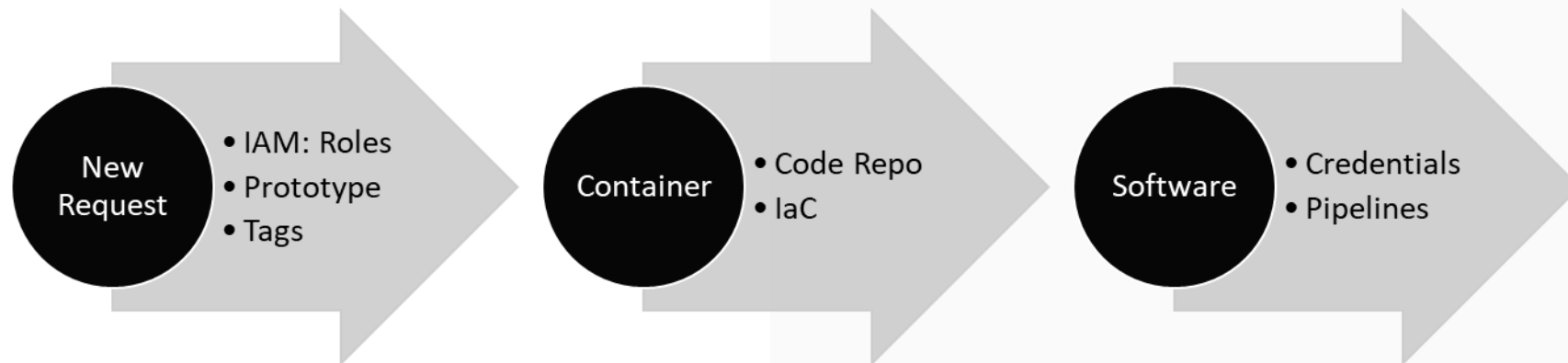
Cloud Offers

CSP Approach
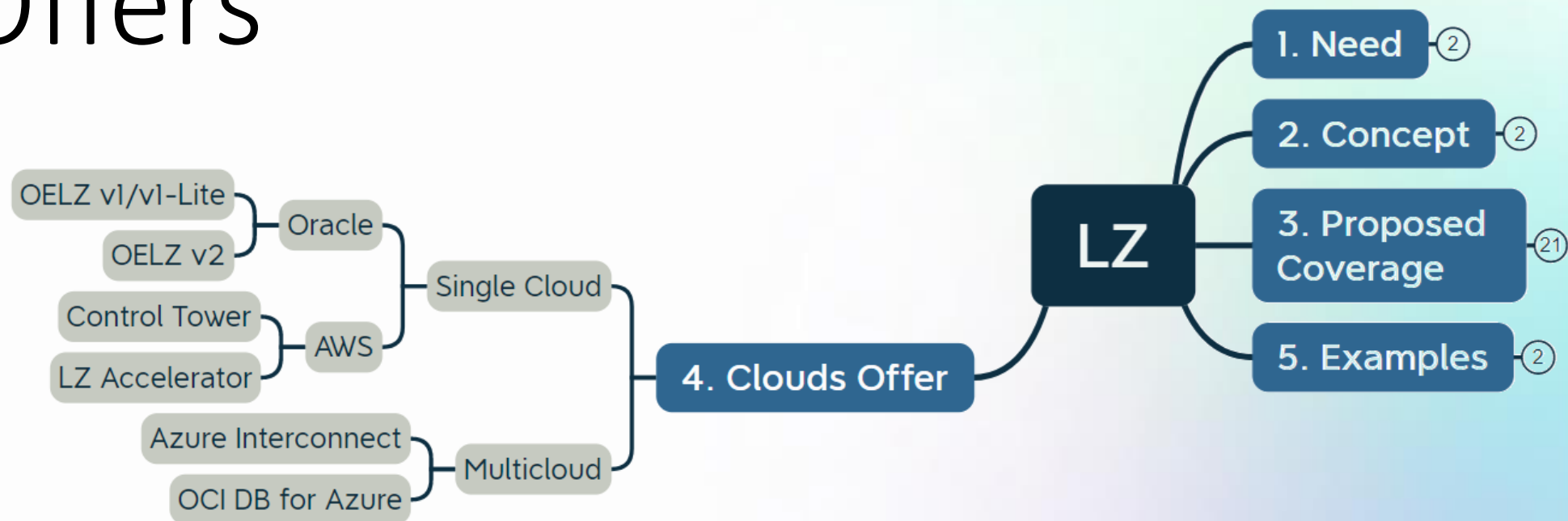
Oracle Enterprise Landing Zone v1 – IAM

2 Terraform Templates:

- Baseline LZ (Core Infrastructure Components)
- Workload Expansion

For Authentication:

- IAM Groups and Policies
- Federated with MS Active Directory (Optional)
- Break-Glass Users (Recommended)
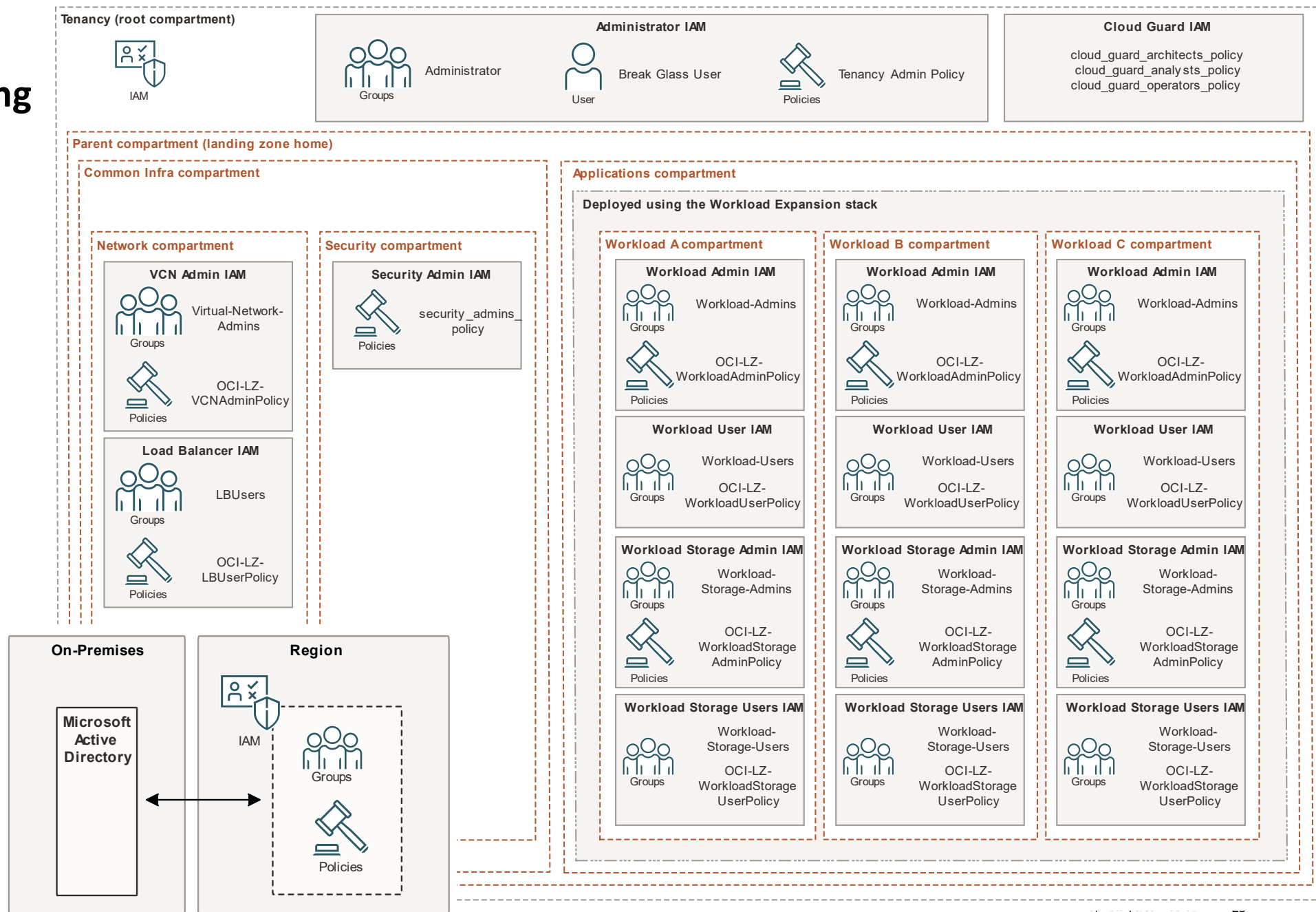
Oracle Enterprise Landing Zone v1 – Security Posture

Take account of:

- Security Lists/Network Security Groups

- Routing Table for IGW, NAT GW and Service GW

- 2 subnets for Workloads: App & DB

- DRG: FastConnect or VPN

- Bastion Services to access to servers temporary.

- Centralized actions on Sec compartment: Cloud Guard, Audit, VCN Flow Logs, Archive with User-managed Key. Connector with Native and 3rd Party Services: Logs & SIEM.

- Cloud Guard.

- Vulnerability Scanning: Scan vulnerabilities on agent & agent-less schemas: OVAL, NVD & CIS.

Tenancy (root compartment – level 0)

Cloud Guard Recipes (Oracle-managed)
- Configuration Detector Recipe
- Activity Detector Recipe
- Responder Recipe

Cloud Guard

IAM
- User
- Group
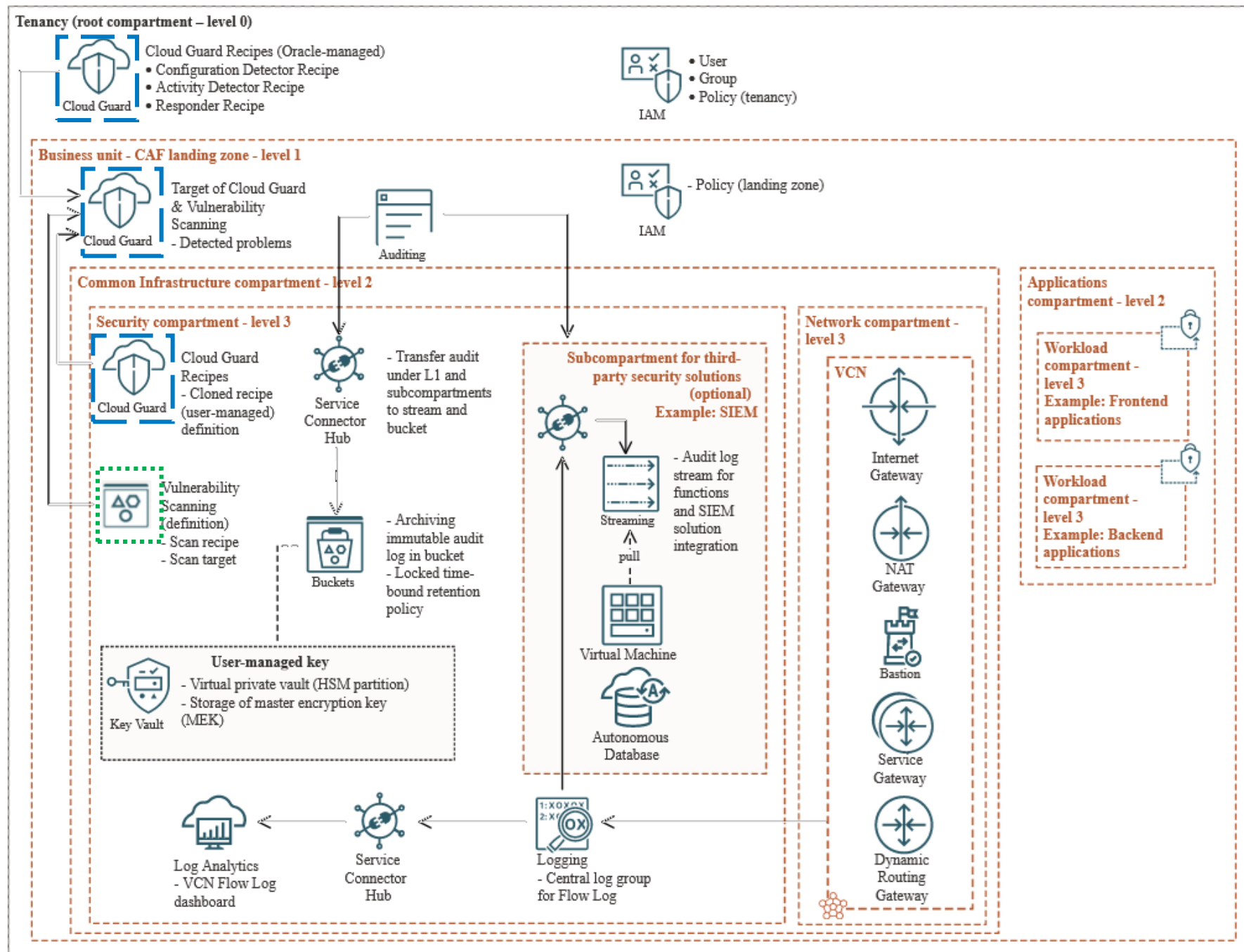- Policy (tenancy)

Business unit - CAF landing zone - level 1

Cloud Guard
Target of Cloud Guard & Vulnerability Scanning
- Detected problems

Auditing

IAM
- Policy (landing zone)

Common Infrastructure compartment - level 2

Security compartment - level 3

Cloud Guard
Cloud Guard Recipes
- Cloned recipe (user-managed) definition

Service Connector Hub
- Transfer audit under L1 and subcompartments to stream and bucket

Vulnerability Scanning (definition)
- Scan recipe
- Scan target

Buckets
- Archiving immutable audit log in bucket
- Locked time-bound retention policy

User-managed key
- Virtual private vault (HSM partition)
- Storage of master encryption key (MEK)

Key Vault

Subcompartment for third-party security solutions (optional)
Example: SIEM

Streaming
- Audit log stream for functions and SIEM solution integration

pull

Virtual Machine

Autonomous Database

Network compartment - level 3

VCN
- Internet Gateway
- NAT Gateway
- Bastion
- Service Gateway
- Dynamic Routing Gateway

Applications compartment - level 2

Workload compartment - level 3
Example: Frontend applications

Workload compartment - level 3
Example: Backend applications

Log Analytics
- VCN Flow Log dashboard

Service Connector Hub

Logging
- Central log group for Flow Log

‹epam›

Oracle Enterprise Landing Zone v2

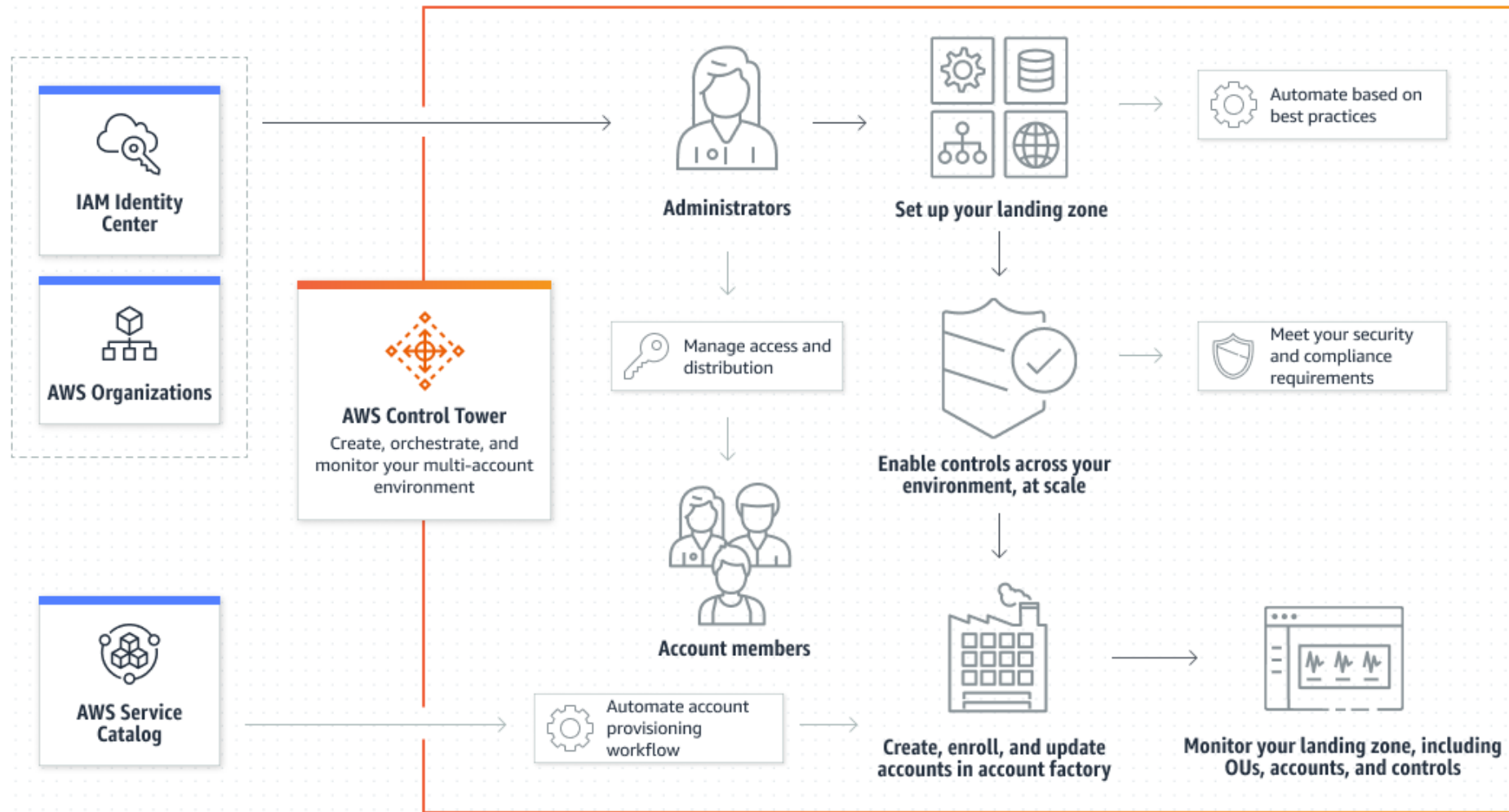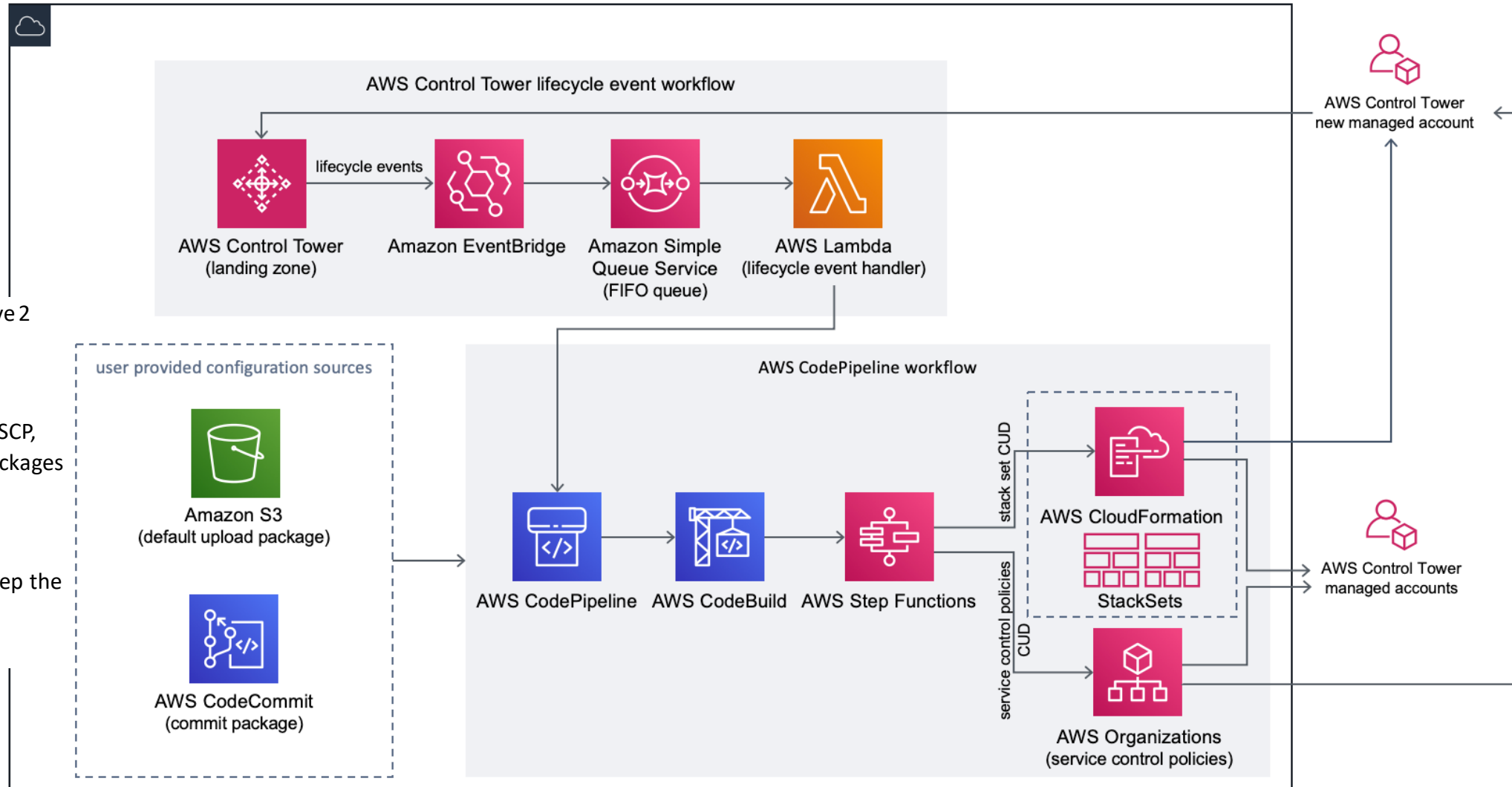| OELZ v2 Features and Services	Associated Service	Description
Multi-Environment	Compartments	Provides a new stack that offers compartment designs for Prod, Dev/Test/UAT. This allows customers to have isolated environments.
Hub & Spoke Networking	Networking	Allows users to segment their environment on a network layer by having one-to-many relationships between the hub and spoke networks.
Identity Domains	Identity, Compartments	Separates production and non-production environments on an Identity layer allowing customers to isolate different user personas.
CIS Benchmarks 1.2	Security	Is compliant with CIS Benchmark 1.2 Level 1.
Modular Design	All	Makes it easier to customize, deploy in modular chunks.
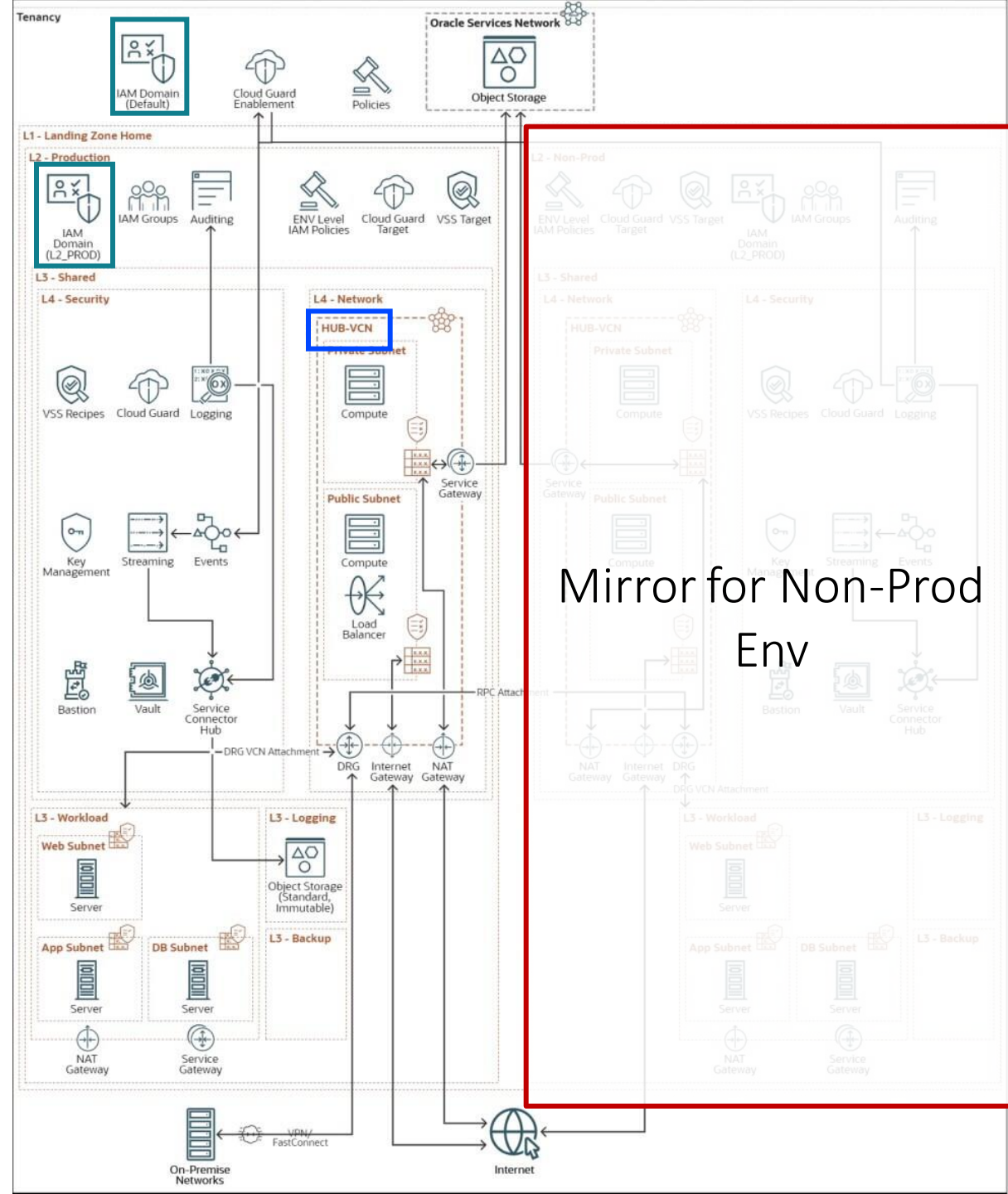
AWS Control Tower

- Extend options from AWS Organizations (for Multi-account environments). If there a previous accounts, you need to register on Control Tower.

- Integrate with AWS multiaccount services/procedures, i.e., Account Factory.

- Guardrails the deviation from security best practices.

IAM Identity Center

AWS Organizations

AWS Service Catalog

AWS Control Tower
Create, orchestrate, and monitor your multi-account environment

Administrators

Manage access and distribution

Account members

Automate account provisioning workflow

Set up your landing zone

Enable controls across your environment, at scale

Create, enroll, and update accounts in account factory

Automate based on best practices

Meet your security and compliance requirements

Monitor your landing zone, including OUs, accounts, and controls

Customizations for AWS Control Tower

On AWS Solutions Library, you have 2 main customizations:

- Existing accounts to add it.

- Configuration sources: Update SCP, StackSets and Configuration Packages to the accounts on the LZ.

>>

AWS Codepipeline workflow to keep the policies running.

AWS Control Tower lifecycle event workflow

AWS Control Tower (landing zone) — lifecycle events → Amazon EventBridge → Amazon Simple Queue Service (FIFO queue) → AWS Lambda (lifecycle event handler)

user provided configuration sources

Amazon S3 (default upload package)

AWS CodeCommit (commit package)

AWS CodePipeline workflow

AWS CodePipeline → AWS CodeBuild → AWS Step Functions

stack set CUD → AWS CloudFormation StackSets

service control policies CUD → AWS Organizations (service control policies)

AWS Control Tower new managed account

AWS Control Tower managed accounts

Landing Zone Accelerator

Cloud foundational (not strict compliant), with complements for industries: Aerospace, Education, Taxes, Healthcare, Elections and Other Gov. requirements.

Code created from CDK to CloudFormation

10 Steps so.....
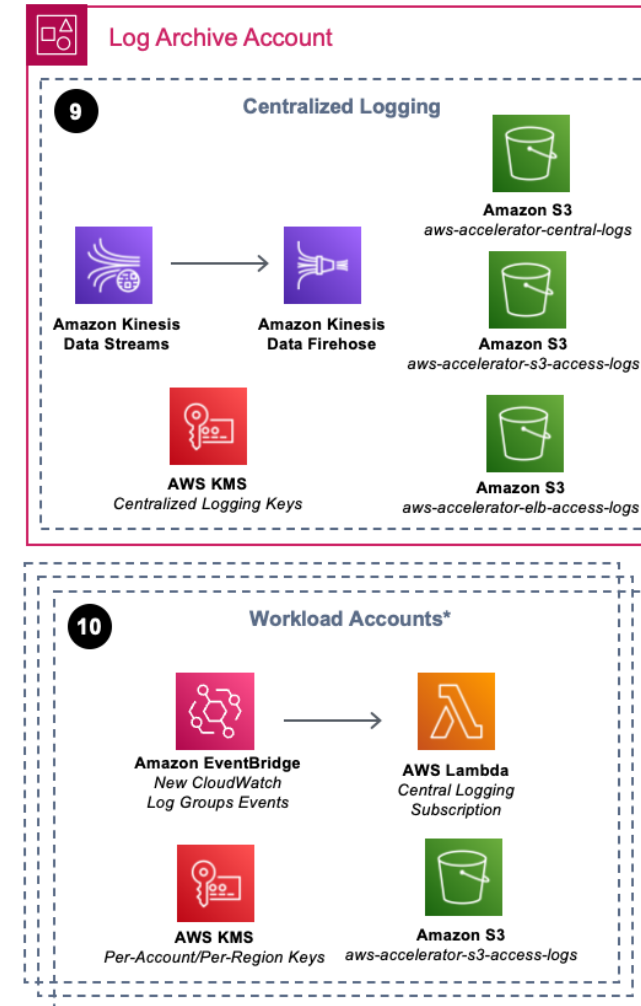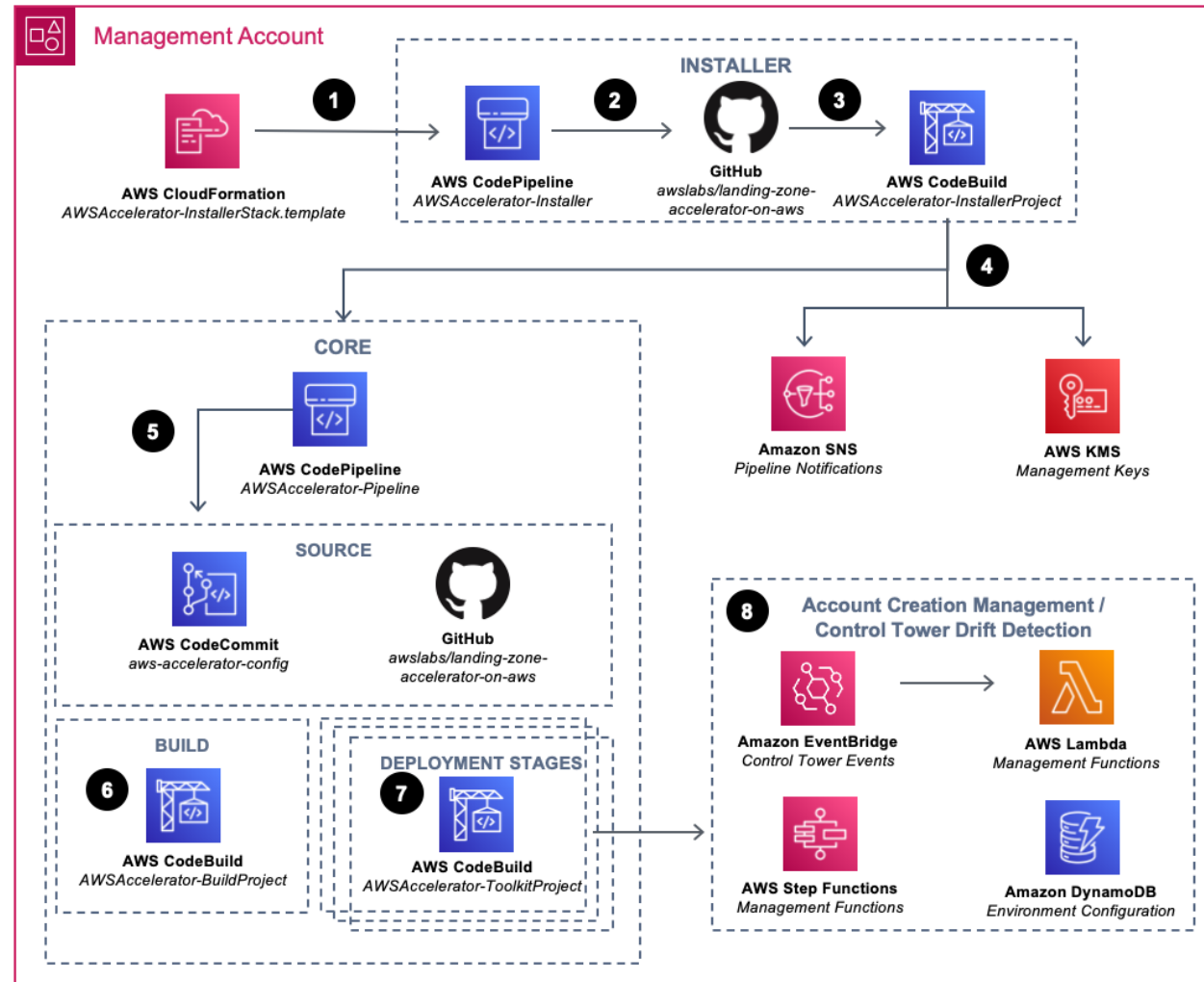
Azure Interconnect Parternship

1. Technology integration

- Private interconnect with FastConnect and ExpressRoute
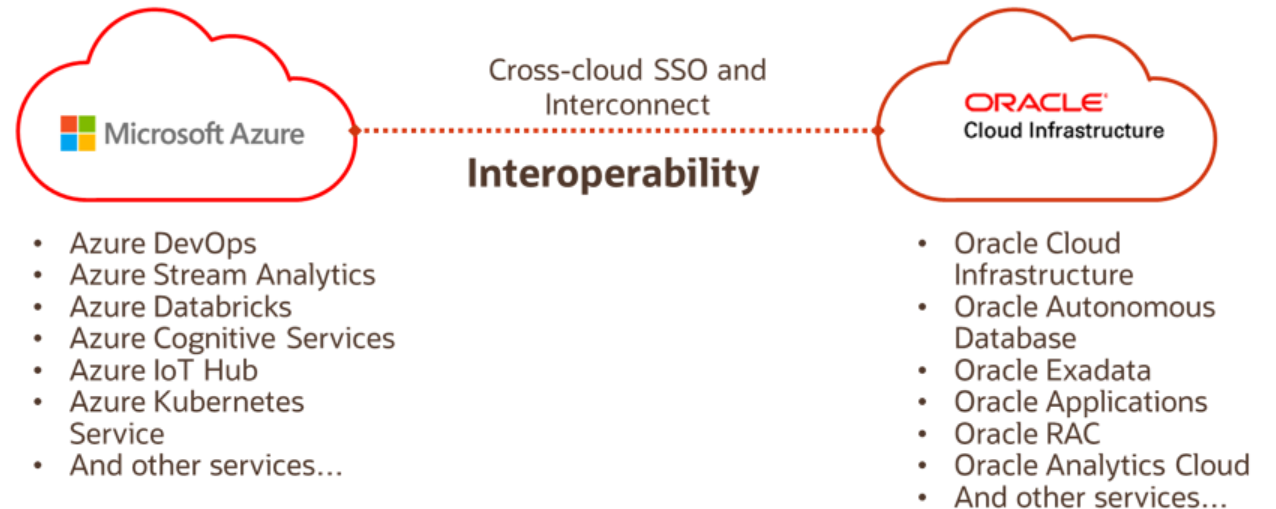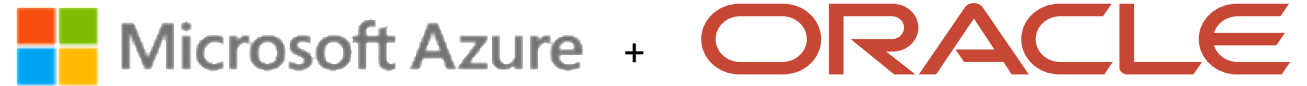- Unified identity and access management

2. Application interoperability

- Tested, validated, and supported application deployments
- Innovate across clouds
- Large choice of services
- Leverage existing investments: Maximize ROI for Licenses. No charge by traffic.

3. Collaborative support model

Joint, collaborative, standard support model

- Seamless issue resolution

Microsoft Azure + ORACLE

Cross-cloud SSO and Interconnect

Interoperability

Microsoft Azure

ORACLE Cloud Infrastructure

- Azure DevOps
- Azure Stream Analytics
- Azure Databricks
- Azure Cognitive Services
- Azure IoT Hub
- Azure Kubernetes Service
- And other services...

- Oracle Cloud Infrastructure
- Oracle Autonomous Database
- Oracle Exadata
- Oracle Applications
- Oracle RAC
- Oracle Analytics Cloud
- And other services...

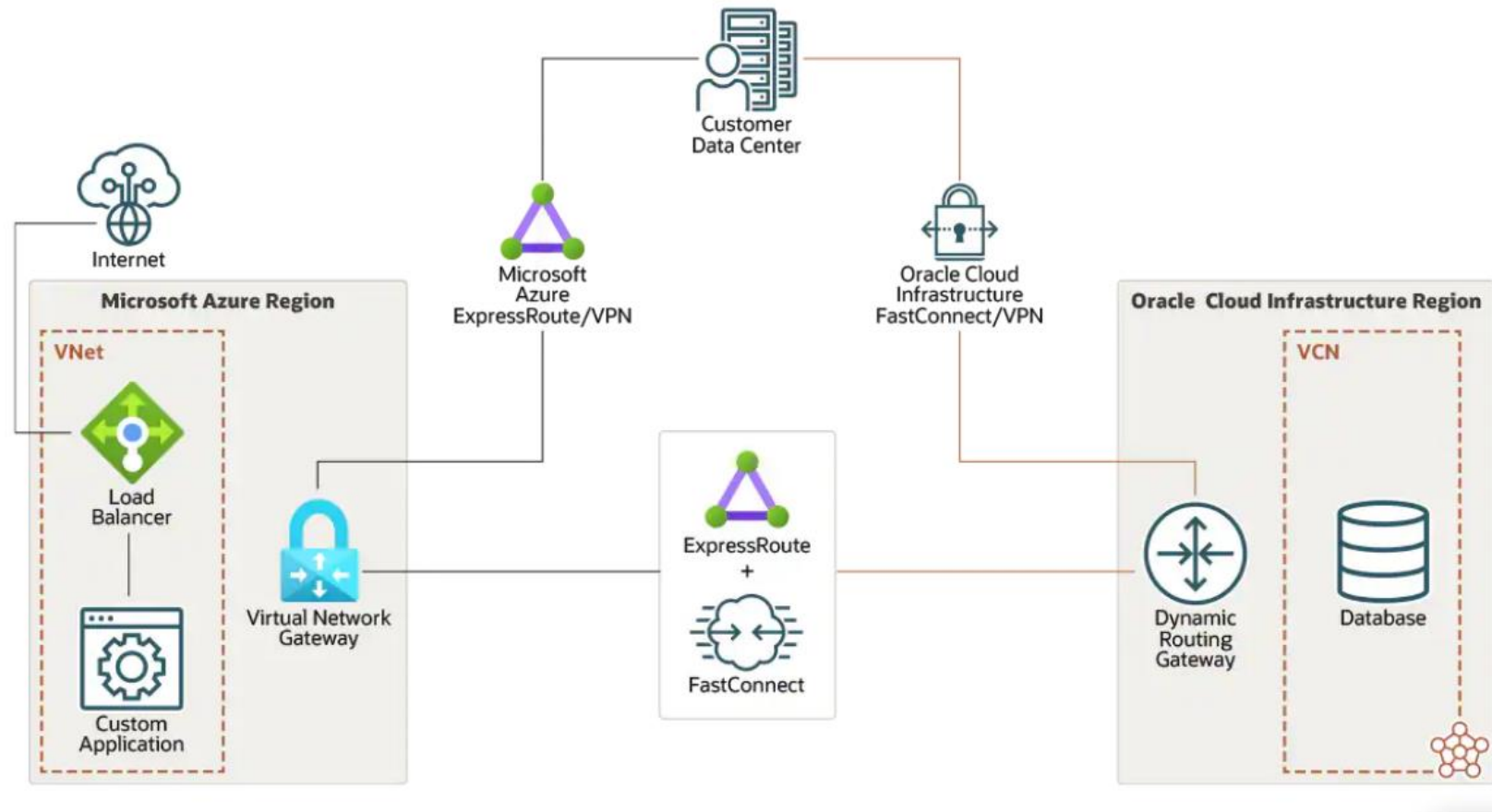# Azure Interconnect

FastConnect and ExpressRoute

- No intermediate service provider required for setup
- No bandwidth charges in either direction

Performance and Security

- Lowest multi cloud latency
  - Average latency across interconnect: ~1.2ms to ~2.1ms
- High bandwidth with a private connection

Simplified implementation

- Terraform scripts to automate provisioning and deployment

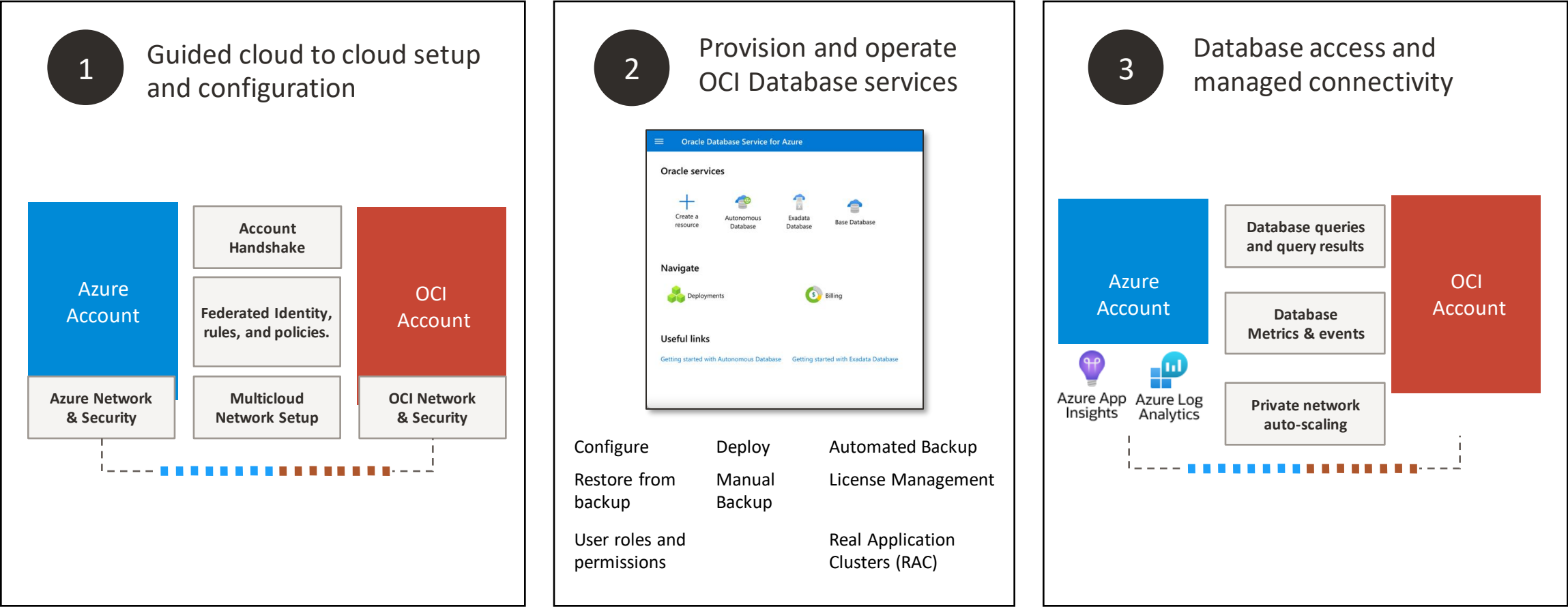*Note: Latency is a function of the service not a function of the interconnect*

Oracle Database Service for Azure (ODSA)

An Oracle managed service that enables customers to easily provision and manage Oracle databases running on OCI using an Azure-native API and console experience.
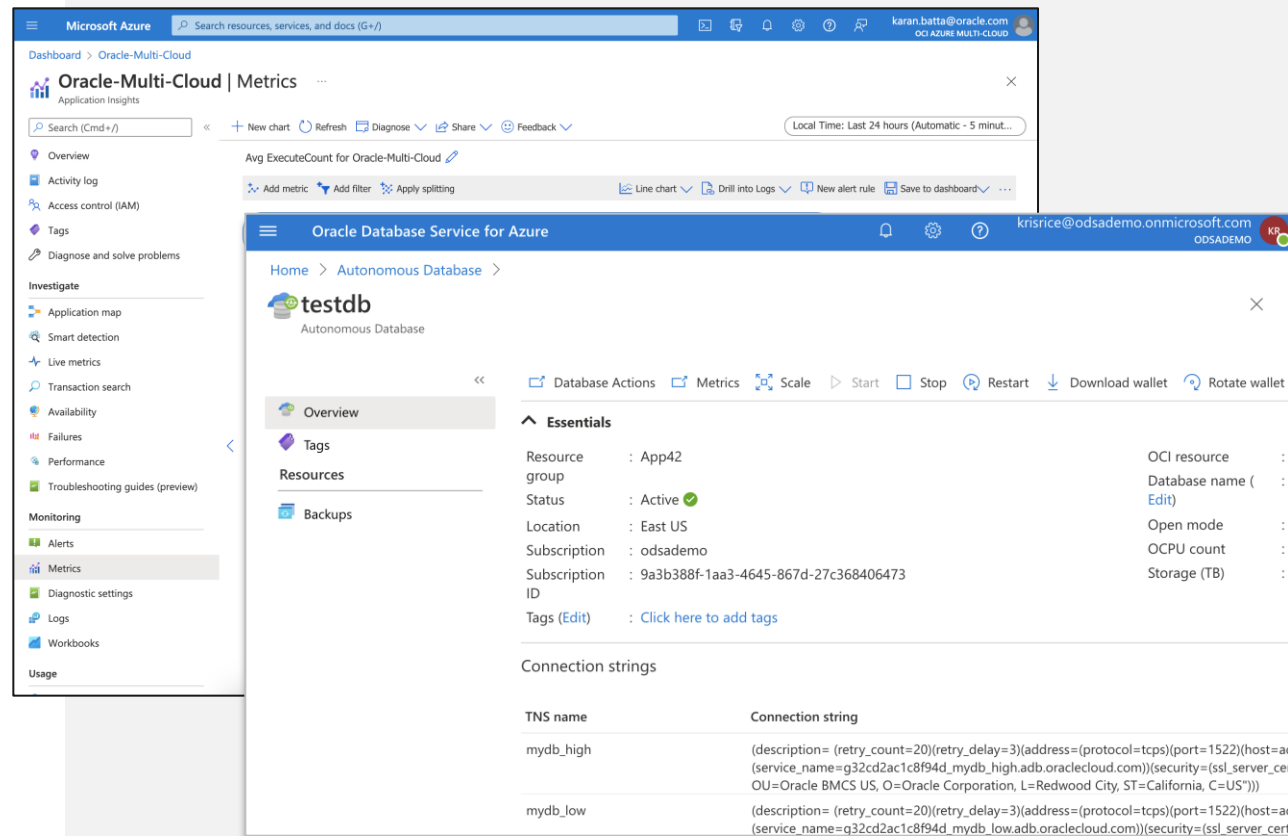
1. Connect Azure and OCI

2. Provision OCI databases

3. Use your OCI database like an Azure resource

4. OCI manages Azure-to-OCI networking

How does the ODSA work ?

1 Guided cloud to cloud setup and configuration

Azure Account	Account Handshake	OCI Account
	Federated Identity, rules, and policies.	
Azure Network & Security	Multicloud Network Setup	OCI Network & Security

2 Provision and operate OCI Database services

Oracle Database Service for Azure

Oracle services

Create a resource · Autonomous Database · Exadata Database · Base Database

Navigate

Deployments · Billing

Useful links

Getting started with Autonomous Database · Getting started with Exadata Database

Configure	Deploy	Automated Backup
Restore from backup	Manual Backup	License Management
User roles and permissions		Real Application Clusters (RAC)

3 Database access and managed connectivity

| Azure Account	Database queries and query results	OCI Account
Azure App Insights · Azure Log Analytics	Database Metrics & events	
	Private network auto-scaling	

05

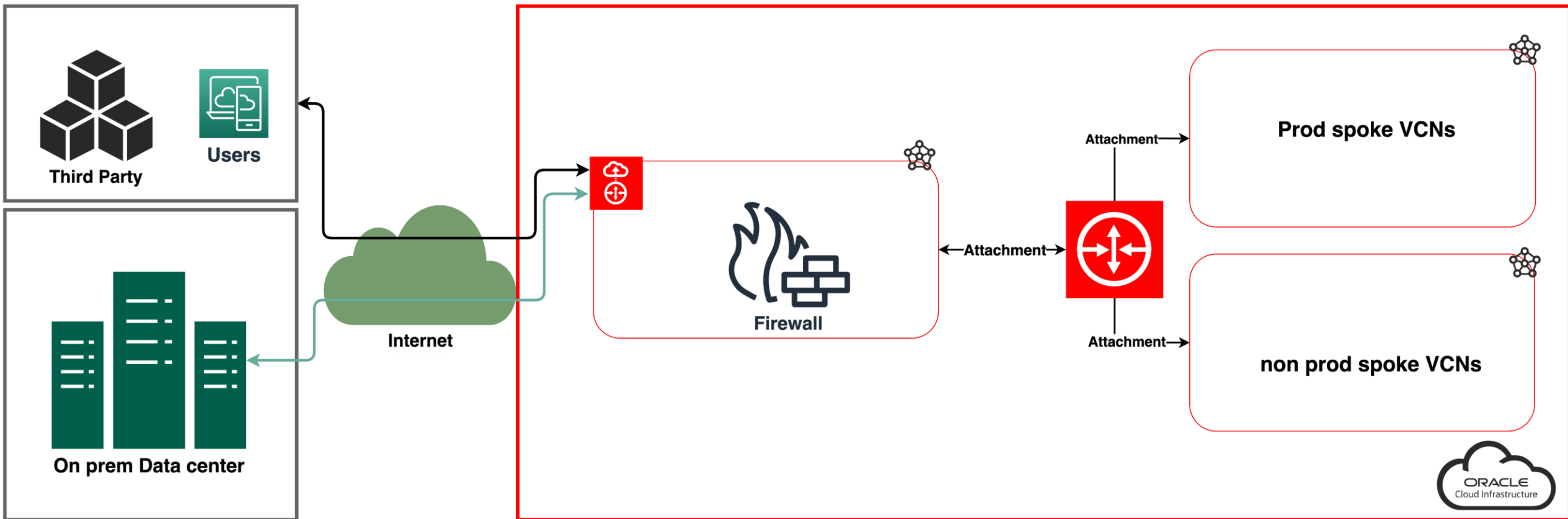# Examples

LZ Deployments in Colombia
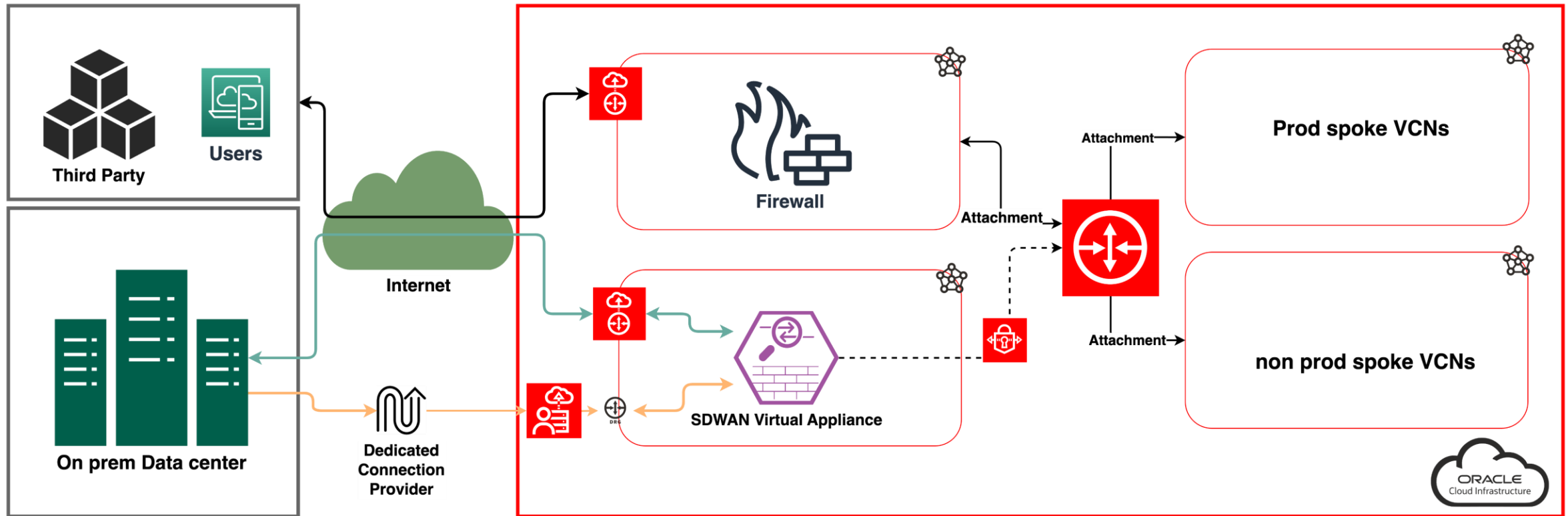
Common functional and quality requirements

- A centralized firewall that inspects traffic in east-west and north-south directions.

- To separate the traffic of the production environments from the traffic of the non-productive environments (to fulfil PCI-DSS Compliance).

- Enable high availability and redundancy in connections, as well as the implementation of traffic engineering policies.

- To centralize the management of users and groups.

- Centralize key and secret management

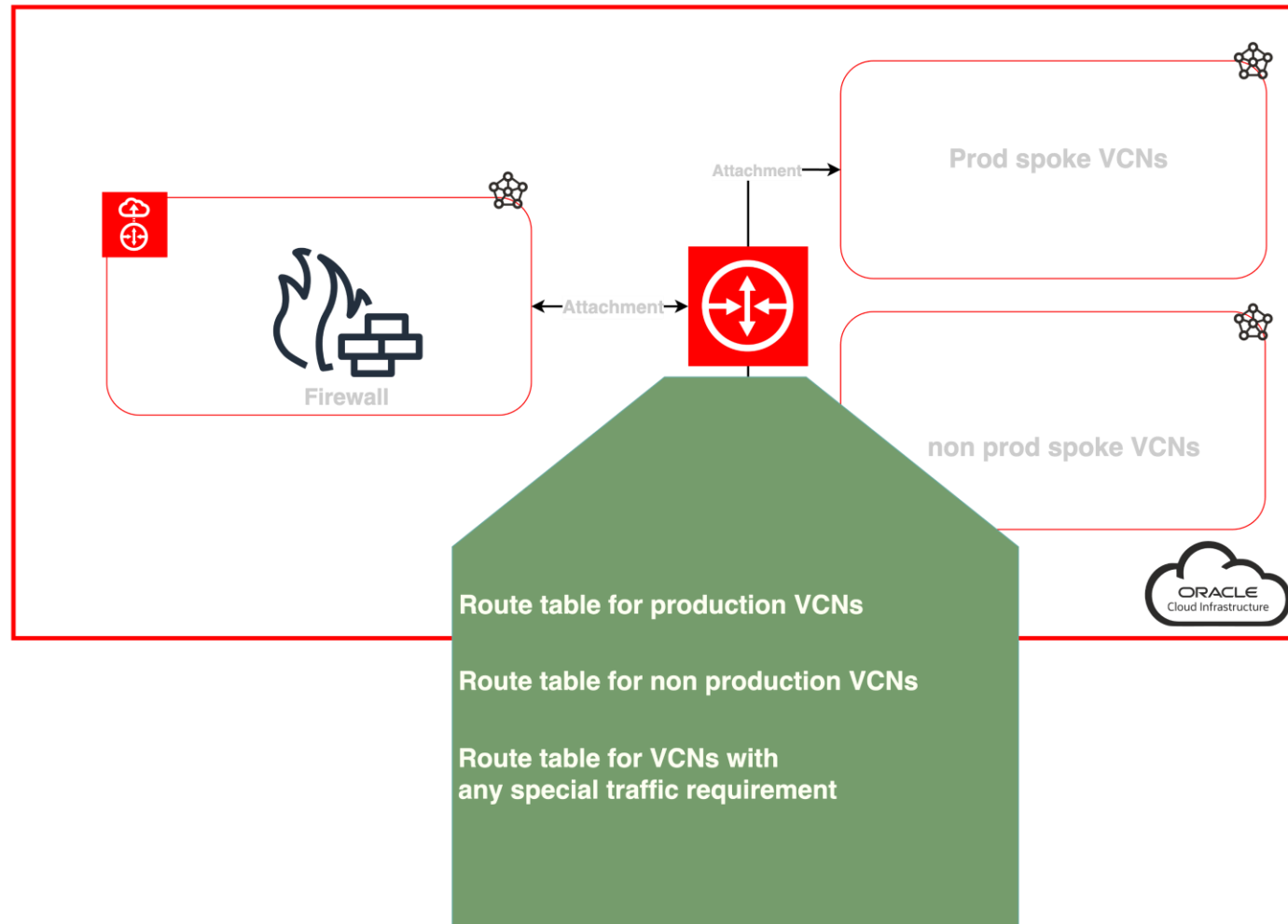- Enable Monitoring, Vulnerability Scanners, Update management.
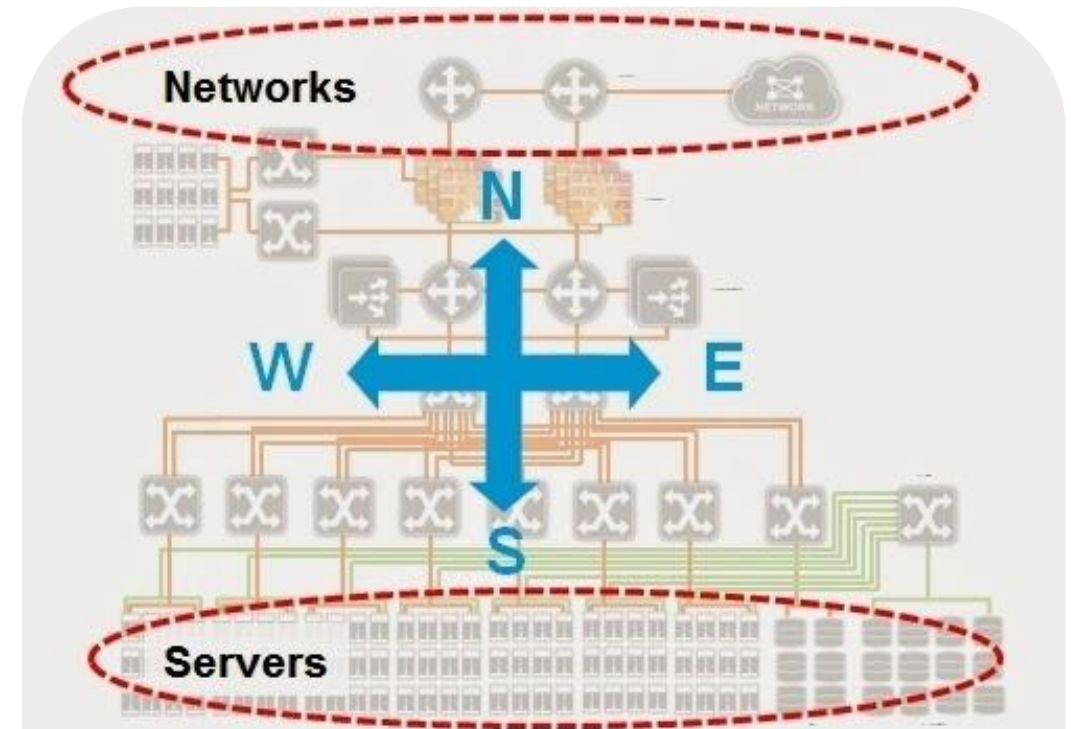
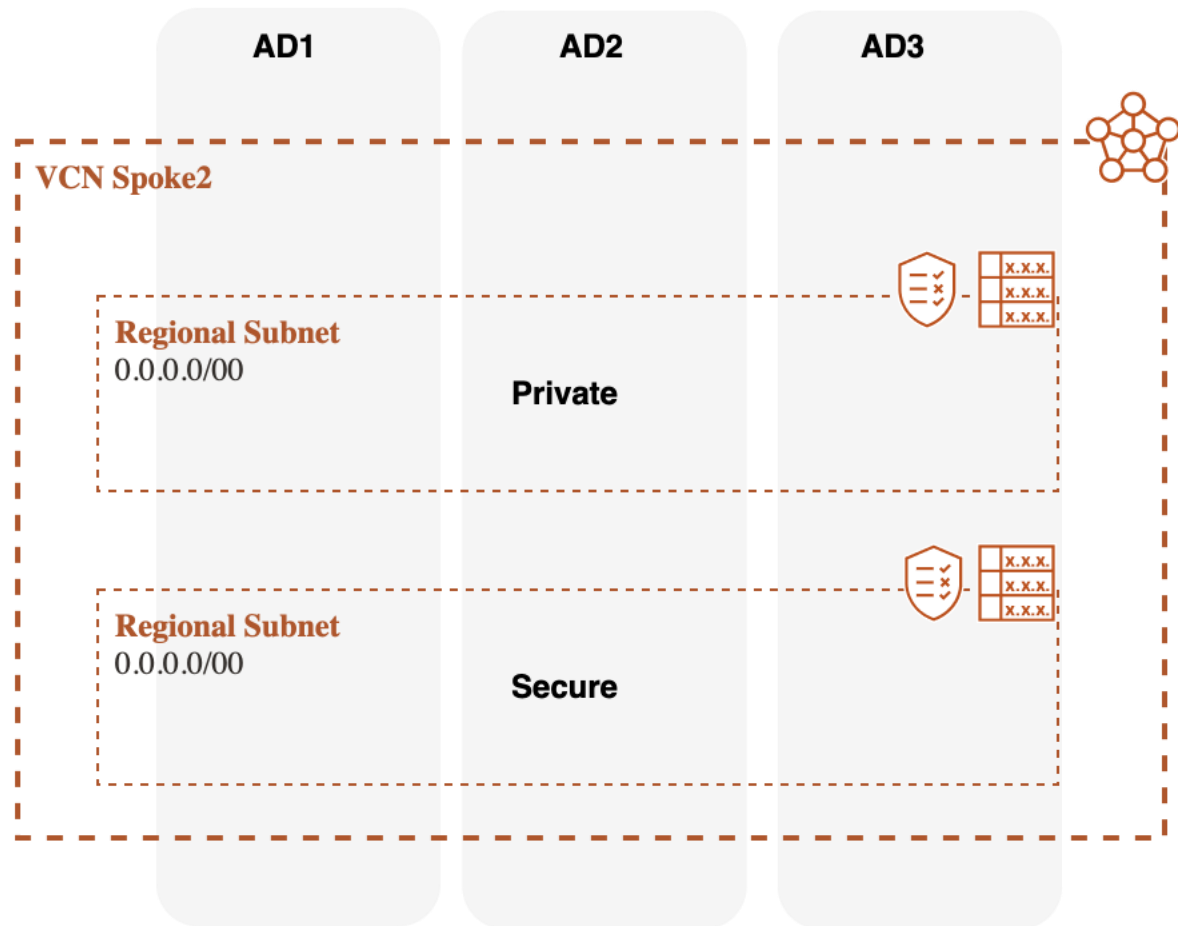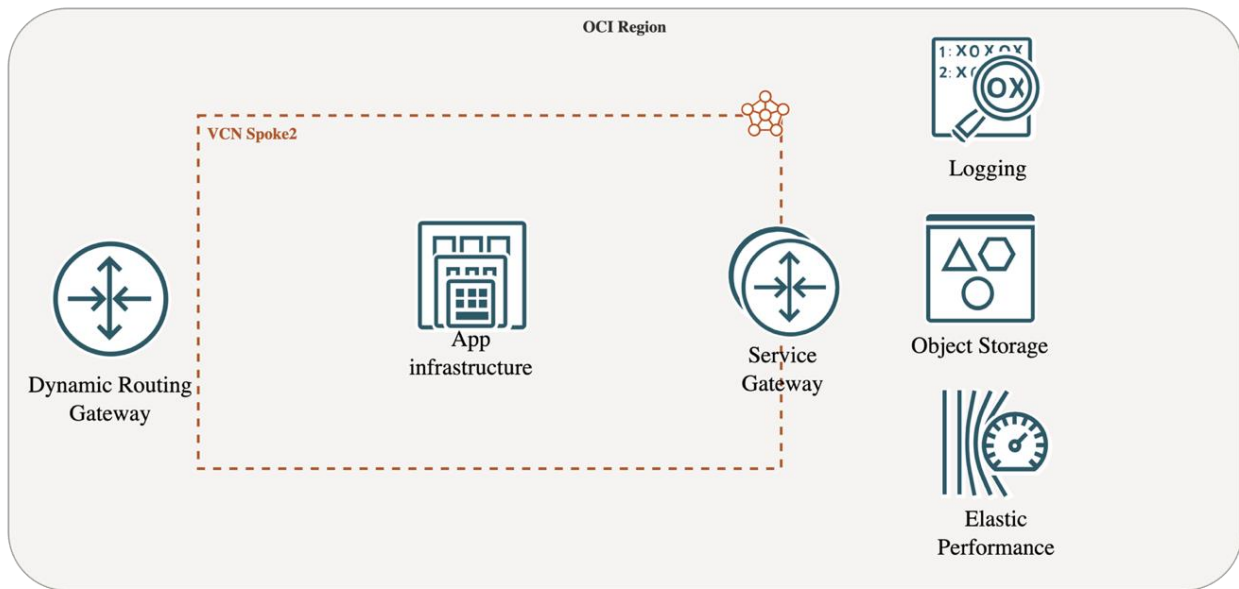# Telecommunications company: Solution using one unique HUB VCN

Financial holding: Solution using two HUB VCNs

Environment separation and traffic engineering

Attachment

Prod spoke VCNs

Attachment

Firewall

Attachment

non prod spoke VCNs

ORACLE
Cloud Infrastructure

Route table for production VCNs

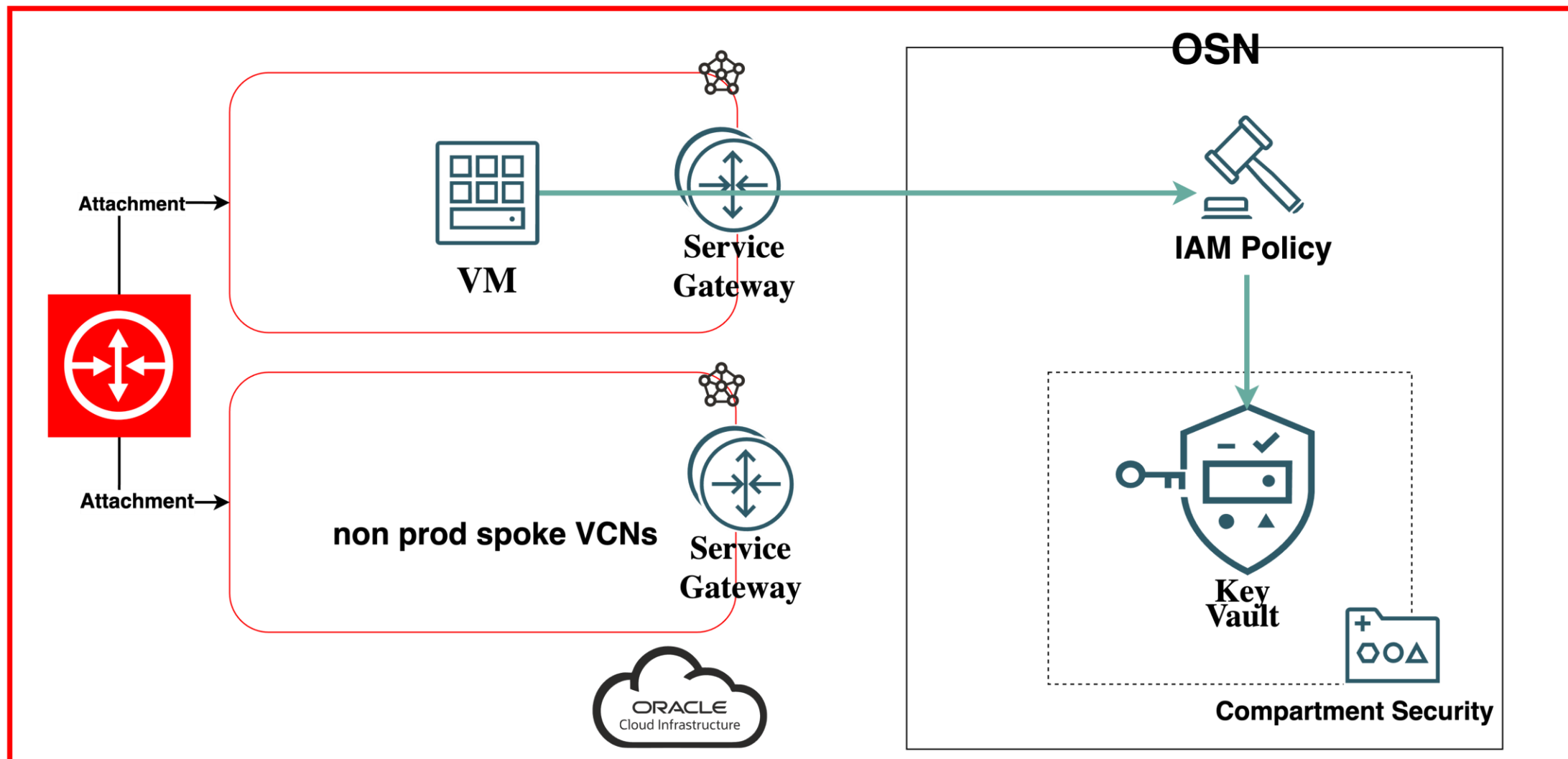**Route table for non production VCNs**

**Route table for VCNs with
any special traffic requirement**

Applications deployment

Communication with regional services
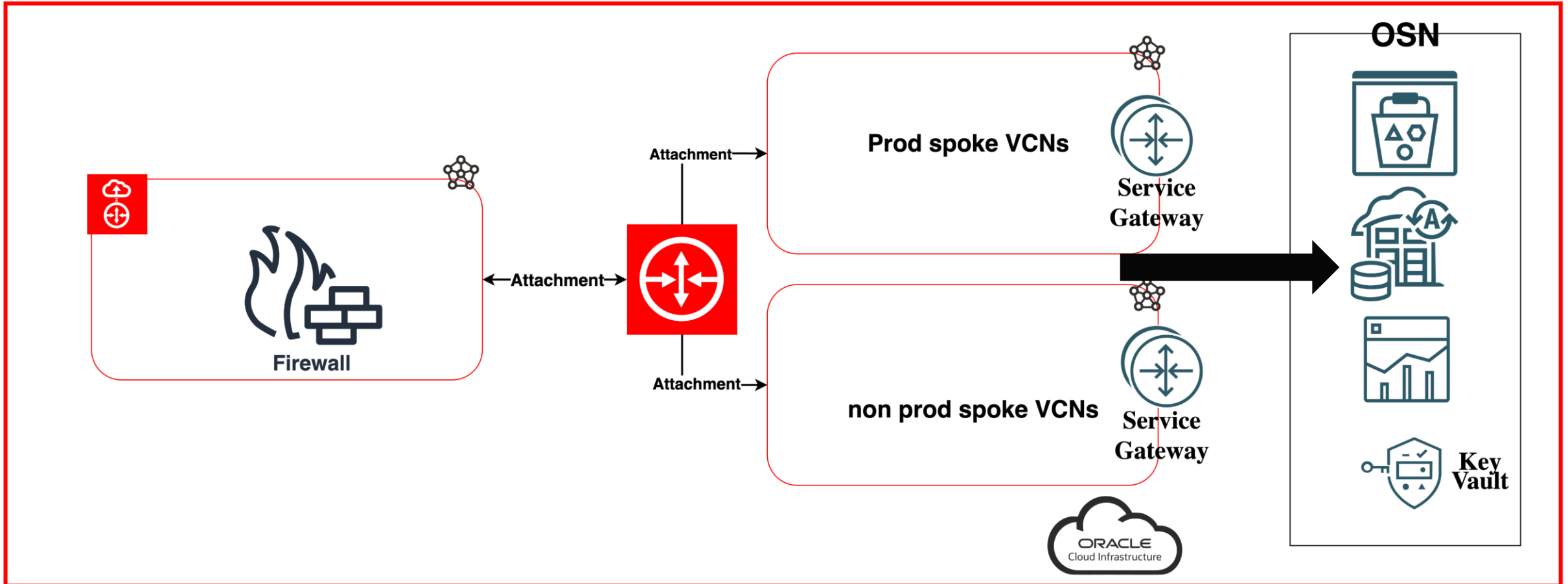
Keys and secrets management

Differences between organizations

- Similar requirements to save Personal Security Info (PSI) and Personal Identifier Info (PII)

- Similar security layers to control access and avoid external attacks.

- Less restrictive access control policies.
- Some environments can be directly exposed to internet.
- not all applications require to be deployed with high availability

- Very restrictive access control policies.
- Multiple instances of each deployment.
- High performance and auto scalability on transversal infrastructures.
- Stringent RTO and RPO.

Q&A Section

This presentation file is hosted

On

[fmorenod81/devopscustomerstories2023 (github.com)](fmorenod81/devopscustomerstories2023)

Francisco Moreno

Lead System Engineer IV

francisco_moreno@epam.com

‹epam›