ACME
EBS Migration to OCI

Solution Definition

9 May 2024 | Version 1.2

CONTENTS

DOCUMENT CONTROL

Guide:

The first chapter of the document describes the metadata for the document. Such as versioning and team members.

1.1 Version Control

Version	Authors	Date	Comments
1.0	Madhusri Bhattacharya	June 2023	First version of EBS Starter Pack in New SD Format
1.1	Madhusri Bhattacharya	October 2023	Edited EBS Starter Pack as per latest SD template
1.2	Madhusri Bhattacharya	April 2024	Edited EBS Starter Pack as per latest SD template

1.2 Team

Guide:

A section describing the Oracle team.

Example:

Name	Email	Role	Company
Name Surname	name.name@example.com	Tech Solution Specialist	Oracle
Ada lovelace	ada@example.com	Account Cloud Engineer	Oracle

1.3 Document Purpose

Guide:

Describe the purpose of this document and the Oracle-specific terminology, specifically around 'Workload'.

Example:

This document provides a high-level solution definition for the Oracle solution and aims at describing the current state, and to-be state as well as a potential high-level project scope and timeline for <Service Provider>.

The document may refer to a 'Workload', which summarizes the full technical solution for a customer (You) during a single engagement. The Workload is described in the chapter Workload Requirements and Architecture.

This is a living document, additional sections will be added as the engagement progresses resulting in a final Document to be handed over to the <Service Provider>.

BUSINESS CONTEXT

Guide:

Describe the customer's business and background. What is the context of the customer's industry and LoB? What are the business needs and goals which this Workload is an enabler for? How does this technical solution impact and support the customer's business goals? Does this solution support a specific customer strategy, or maybe certain customer values? How does this solution help our customers to either generate more revenue or save costs?

2.1 Executive Summary

Guide:

A section describing the background of the Customer and the context of the Workload migration

Example:

- Brief history of the Customer
- Current Solution and Rationale for moving to Oracle Cloud Infrastructure (OCI)

2.2 Workload Business Value

Guide:

A section describing the business value of the Application on OCI

Example:

Organizations use on-premises deployments of E-Business Suite(EBS) for a wide range of functionalities, including Financials, Order Management, Procurement, Manufacturing and Logistics. These implementations are often customized to seamlessly integrate with other applications to meet business requirements. So it’s counterproductive to re-architect software from scratch. OCI has the flexibility to support everything Organizations are currently doing with E-Business Suite.

Most On-Premises EBS deployments can be migrated to run on Oracle Cloud Infrastructure (OCI) without requiring significant configuration, integration, or business process changes, and result in an implementation that is more flexible, more reliable, higher performance, and lower cost than either On-Premises or other Cloud vendors. Running EBS on Oracle Cloud enables you to:

- Increase business agility
- Better manage growth
- Reduce time and cost for new projects
- Track and Manage Usage and Cost
- Maximise the productivity of your IT staff

OCI Database service offers Autonomous and Co-managed (Base Database, Exadata Database on Dedicated Infrastructure and Exadata Database on Cloud@Customer). EBS customers can run their mission-critical business applications with unprecedented performance, scalability, and availability. This is accomplished by leveraging the **best database platforms** available in OCI discussed above. Further note that most EBS systems currently running on OCI host the Database on either Base Database (Oracle Database Cloud Services on Virtual Machines), or on Oracle Exadata Database on Dedicated Infrastructure.

Another key EBS investment unique to OCI is the time-saving automation capability delivered by **Oracle EBS Cloud Manager**, which has been designed specifically to support EBS customers running on OCI and associated database services. EBS Cloud Manager and its associated tools can help you reduce cost, reduce risk, and increase agility by automating essential operations such as:

Environment deployment: - Lift and shift of an on-premises environment to Oracle Cloud - One-click provisioning of demo environments - Advanced provisioning, of either a fresh installation or from a backup Lifecycle management: - Backup and restore - Scaling - Optimized cloning

Additionally, all the activities mentioned within the scope will ensure the deployment of workload as per Oracle's best practices. As a tried and tested methodology by many customers 'Oracle Lift' brings speed of deployment resulting in successful project without any setbacks; thus bring value to the overall project provisioning for the Application workload.

WORKLOAD REQUIREMENTS AND ARCHITECTURE

3.1 Overview

Guide:

A section describing the Current EBS workload of the Customer. Describe the Workload: What applications and environments are part of this Workload, specify their names and details. The implementation will be scoped later and is typically a subset of the Workload. For example, a Workload could exist of two applications, but the implementer would only include one environment of one application. The workload chapter is about the whole Workload and the implementation scope will be described late in the chapter. Scope.

Example:

Currently Customer's EBS workload is a multi node deployment of EBS release 12.2. The Application tier is connected to a 19C Oracle Real Application Cluster (RAC) Database. The application tier is sub divided into the following components:

- Two nodes EBS farm (Deployed to WebLogic Clusters of Managed Servers) hosting web, forms and concurrent managers and
- A single external facing node hosting web functionality to support iSupplier portal.

Two client connection routes, internal via a WAN and externally via the internet. Both routes employ https which is terminated on a load-balancer. The internal farm employs a shared application tier home.

The reporting elements of the solution are provided using Oracle Business Intelligence Enterprise Edition 'X' together with Oracle Apex 'X' for access to archived legacy data.

Oracle Data Integrator (ODI) provides the hub for both inbound and outbound interfaces through the system.

Customer's EBS workload also has a Demilitarized Zone (DMZ) for external access to the application.

3.2 Non-Functional Requirements

Guide:

Describe the high-level technical requirements for the Workload. Consider all sub-chapters, but decide and choose which Non-Functional Requirements are necessary for your engagement. You might not need to capture all requirements for all sub-chapters.

3.2.1 Regulations and Compliances Requirements

Guide:

This section captures specific regulatory or compliance requirements for the Workload. These may limit the types of technologies that can be used and may drive some architectural decisions.

The Oracle Cloud Infrastructure Compliance Documents service lets you view and download compliance documents: https://docs.oracle.com/en-us/iaas/Content/ComplianceDocuments/Concepts/compliancedocsoverview.htm

If there are none, then please state it. Leave the second sentence as a default in the document.

Example:

At the time of this document creation, no Regulatory and Compliance requirements have been specified.

In addition to these requirements, the CIS Oracle Cloud Infrastructure Foundation Benchmark, v1.2 will be applied to the Customer tenancy.

3.2.2 Environments

Guide:

A section describing the Current EBS workload of the Customer: Environment details

Example:

Current EBS workload has four environments:

Current EBS workload has four environments:

- **Production**
  - EBS Application Version: **12.2**

  - Oracle Database Version: **19c**
  - Number of Application Node: 2 Application Nodes (with shared Oracle Application Binary) including web, Forms and Concurrent Managers Instances
    - 1 Single Instance of EBS is running on DMZ zone, catering for external end-users
  - Number of Database Node: 2 Nodes Oracle RAC
- **Pre-Production**
  - EBS Application Version: **12.2**
  - Oracle Database Version: **19c**
  - Number of Application Node: 2 Application Nodes (with shared Oracle Application Binary) including Web, Forms and Concurrent Managers Instances
    - 1 Single Instance of EBS is running on DMZ zone, catering for external end-users
  - Number of Database Node: 2 Nodes Oracle RAC (Real Application Cluster)
- **Development**
  - EBS Application Version: **12.2**
  - Oracle Database Version: **19c**
  - Number of Application Node: Single Application Node including Web, Forms and Concurrent Managers Instances
    - 1 Single Instance of EBS is running on DMZ zone, catering for external end-users
  - Number of Database Node: Single node Oracle Restart
- **Disaster Recovery (DR)**
  - This is a copy of Production environment which is kept in synch with Production environment using following synchronization methods:
    - EBS application tier are kept in synch with Production using rsync job scheduled via crontab
    - The E-Business database repository is synchronized with DR using Oracle Data Guard Solution

3.2.2.1 Environment Sizing

Guide:

A section describing the Current EBS workload of the Customer: Sizing Details, Current On-Premise BoM

Example:

Implementation Partner will capture the current EBS workload sizing here.

3.2.3 High Availability and Disaster Recovery Requirements

Guide:

This section captures the resilience and recovery requirements for the Workload. Note that these may be different from the current system.

The Recovery Point Objective (RPO) and Recovery Time Objective (RTO) requirement of each environment should be captured in the environments section above, and wherever possible.

- *What are the RTO and RPO requirements of the Application?*
- *What are the SLAs of the application?*
- *What are the backup requirements*

Example:

The recovery time objective (downtime tolerance) and recovery point objective (data loss tolerance) details are very important considerations for the Customer. The overall DR requirement is a cross region DR strategy with the goal of minimizing RTO.

3.2.3.1 Backup and Recovery Practices

Guide:

A section describing the Current EBS workload of the Customer: Backup and Recovery- RTO and RPO

Example:

Current high level backup and recovery practices are described below:

- File system and Database backups are retained for 30 days for production and at least 7 days for non-production.
- Oracle Recovery Manager (RMAN) is the standard backup tools which handles for all EBS workload Databases.
- Backup of the Oracle Databases uses the standard file system agent which backs up the Oracle RMAN disk based backup to tape.
- Backup frequency standards are:
  - Weekly full,
  - Daily incremental backup, which includes the archive log backups. *Example:*

3.2.4 Security Requirements

Guide:

Capture the Non-Functional Requirements for security-related topics. Security is a mandatory subsection that is to be reviewed by the x-workload security team. The requirements can be separated into:

- *Identity and Access Management*
- *Data Security*

Other security topics, such as network security, application security, or others can be added if needed.

Example:

The foundation of security is access control, which refers to how the system is being accessed and by whom. User security consists of three principal components: authentication, authorization and an audit trail. All current browser-based password login screens send the password as a parameter in the HTTP form submission. Using an HTTPS connection will encrypt this information. The best practice is therefore to use HTTPS for all web-based access. The requirement is to take extra steps to ensure security is not compromised either from the Infrastructure side or from the Application endpoints.

At the time of this document creation, no Security requirements have been specified.

3.2.5 Workload Access Requirement

Guide:

A section describing the Current EBS workload of the Customer: How Customer access their Application

Example:

The Customer wants to access the EBS workload, once they move to OCI, in the same way as they currently do On-Premises. They also need to secure their external internet-facing endpoints from internet threats.

The Customer has both internal and external endpoints of their EBS workload.

Internal Users:

Users access EBS using the URL https:// `<Internal LB URL:port>`. The connection flows via the external/internal firewall to the Load Balancer in DMZ. Load Balancer terminates the Secure Socket Layer (SSL) and passes the request on port 8010 to EBS internal servers. The internal EBS servers communicate with EBS RAC Database on Linux VMs using Database listener port 1531 and validate the user request.

External Users:

External users access EBS using the URL https:// `<External LB URL:port>`. The connection flows via the external/internal firewall to the Load Balancer in DMZ. Load Balancer terminates the SSL and passes the request on port 8010 to EBS external server.

3.2.6 Workload Monitoring

Guide:

A section describing the Current EBS workload of the Customer: Monitoring of the Workload (like OEM or any other monitoring tools)

Example:

Currently Oracle Enterprise Manager is used as Customer's On-Premises management platform, providing a single pane of glass for management of Oracle E-Business Suite environments.

3.2.7 Management and Monitoring (OCI)

Guide:

This subsection helps you capture any requirements for customer management and monitoring needs - e.g. system monitoring, systems management, log analysis, etc.

When you move or start an OCI project, you have a choice to use the tools you are familiar with (should they support modern application architectures), replace them with OCI native Observability services, or use a combination to improve your visibility. When contemplating how to proceed, here are some general questions that will guide you:

- *Does the tool manage across hybrid and multi-cloud environments?*
- *What is the cost of integrating the existing tool with OCI?*
- *Is my current monitor tool enabling you to prevent issues versus reacting to them?*
- *Does the tool tell you how much impact there has been on users or just that there was an impact like something is down or unavailable?*
- *Does the tool provide the full vision of applications and their infrastructure or just a piece of them or specific technology?*

Example:

Task	Target	Location	New	Notes
Application Monitoring	All targets	On-Prem and OCI	No	
Monitoring	All targets	OCI (Migration)	No	
Log Management	All targets	OCI (Migration)	No	
Insight	All Oracle DBs	OCI (Migration)	No	

3.3 Future State Architecture

Guide:

The Workload Future State Architecture can be described in various forms. In the easiest case, we describe a Logical Architecture, possibly with a System Context Diagram. A high-level physical architecture is mandatory as a description of your solution.

Additional architectures, in the subsections, can be used to describe needs for specific workloads.

3.3.1 Mandatory Security Best Practices

Guide:

Use this text for every engagement. Do not change. Aligned with the Cloud Adoption Framework

The safety of the ACME's Oracle Cloud Infrastructure (OCI) environment and data is the ACME's priority.

The following table of OCI Security Best Practices lists the recommended topics to provide a secure foundation for every OCI implementation. It applies to new and existing tenancies and should be implemented before the Workload defined in this document will be implemented.

Workload-related security requirements and settings like tenancy structure, groups, and permissions are defined in the respective chapters.

Any deviations from these recommendations needed for the scope of this document will be documented in the chapters below. They must be approved by ACME.

ACME is responsible for implementing, managing, and maintaining all listed topics.

CATEGORY	TOPIC	DETAILS
User Management	IAM Default Domain	Multi-factor Authentication (MFA) should be enabled and enforced for every non-federated OCI user account. • For configuration details see Managing Multi-Factor Authentication. In addition to enforcing MFA for local users, Adaptive Security will be enabled to track the Risk Score of each user of the Default Domain. • For configuration details see Managing Adaptive Security and Risk Providers.
	OCI Emergency Users	A maximum of **three** non-federated OCI user accounts should be present with the following requirements: • Username does not match any username in the Customer's Enterprise Identity Management System • Are real humans. • Have a recovery email address that differs from the primary email address. • User capabilities have Local Password enabled only. • Has MFA enabled and enforced (see IAM Default Domain).
	OCI Administrators	Daily business OCI Administrators are managed by the Customer's Enterprise Identity Management System. This system is federated with the IAM Default Domain following these configuration steps: • Federation Setup • User Provisioning • For configuration guidance for major Identity Providers see the OCI IAM Identity Domain tutorials.
	Application Users	Application users like OS users, Database users, or PaaS users are not managed in the IAM Default Domain but either directly or in dedicated identity domains. These identity domains and users are covered in the Workload design. For additional information see Design Guidance for IAM Security Structure.
Cloud Posture Management	OCI Cloud Guard	OCI Cloud Guard will be enabled at the root compartment of the tenancy home region. This way it covers all future extensions, like new regions or new compartments, of your tenancy automatically. It will use the Oracle Managed Detector and Responder recipes at the beginning and can be customized by the Customer to fulfill the Customer's security requirements. • For configuration details see Getting Started with Cloud Guard. Customization of the Cloud Guard Detector and Responder recipes to fit the Customer's requirements is highly recommended. This step requires thorough planning and decisions to make. • For configuration details see Customizing Cloud Guard Configuration
	OCI Vulnerability Scanning Service	In addition to OCI Cloud Guard, the OCI Vulnerability Scanning Service will be enabled at the root compartment in the home region. This service provides vulnerability scanning of all Compute instances once they are created. • For configuration details see Vulnerability Scanning.
Monitoring	SIEM Integration	Continuous monitoring of OCI resources is key for maintaining the required security level (see Regulations and Compliance for specific requirements). See Design Guidance for SIEM Integration to implement integration with the existing SIEM system.
Additional Services	Budget Control	OCI Budget Control provides an easy-to-use and quick notification on changes in the tenancy's budget consumption. It will be configured to quickly identify unexpected usage of the tenancy. • For configuration details see Managing Budgets

3.3.2 Naming Conventions

Guide:

This chapter describes naming convention best practices and usually does not require any changes. If changes are required please refer to Landing Zone GitHub. The naming convention zone needs to be described in the Solution Design by *the service provider.*

Use this template ONLY for new cloud deployments and remove it for brownfield deployments.

A naming convention is an important part of any deployment to ensure consistency, governance, and security within your tenancy. Find here Oracle's recommended best practices.

3.3.3 OCI Landing Zone Solution Definition

Guide:

This chapter describes landing zone best practices and usually does not require any changes. If changes are required please refer to Landing Zone GitHub. The full landing zone needs to be described in the Solution Design by the service provider.

Use this template ONLY for new cloud deployments and remove it for brownfield deployments.

An OCI Landing Zone sets the foundations for a secure tenancy, providing design best practices and operational control over OCI resources. A Landing Zone also simplifies the onboarding of workloads and teams, with clear patterns for network isolation and segregation of duties in the organization, which sets the cloud operating model for day-to-day operations.

Oracle highly recommends the use of an OCI Landing Zone for any deployment. Use these guidelines to set up your OCI Landing Zone, including design considerations, approaches, and solutions to use.

Note that all workloads in a tenancy should sit on top of a Landing Zone, meaning that the workload architecture defined in the next section can be subject to adjustments (e.g., network structure) towards the landing zone model, along with other future workloads.

3.3.4 Physical Architecture

Guide:

A section describing the Deployment Design and its associated Components in OCI

Example:

The Tenancy of Customer will be managed by 'X' as a Managed Service Provider. The design plan which has been decided is to create One Tenancy where Virtual Cloud Network (VCN) will be provisioned for both the Customer as well as for Managed Service provider. Traffic for Each VCN will be terminated at their respected Dynamic Routing Gateways (DRG).

In the **following sections** we are describing the **Deployment Design Diagrams** as well as all the relevant components present in the Design diagram.*

The Oracle Cloud Notation, OCI Architecture Diagram Toolkits

Reference:

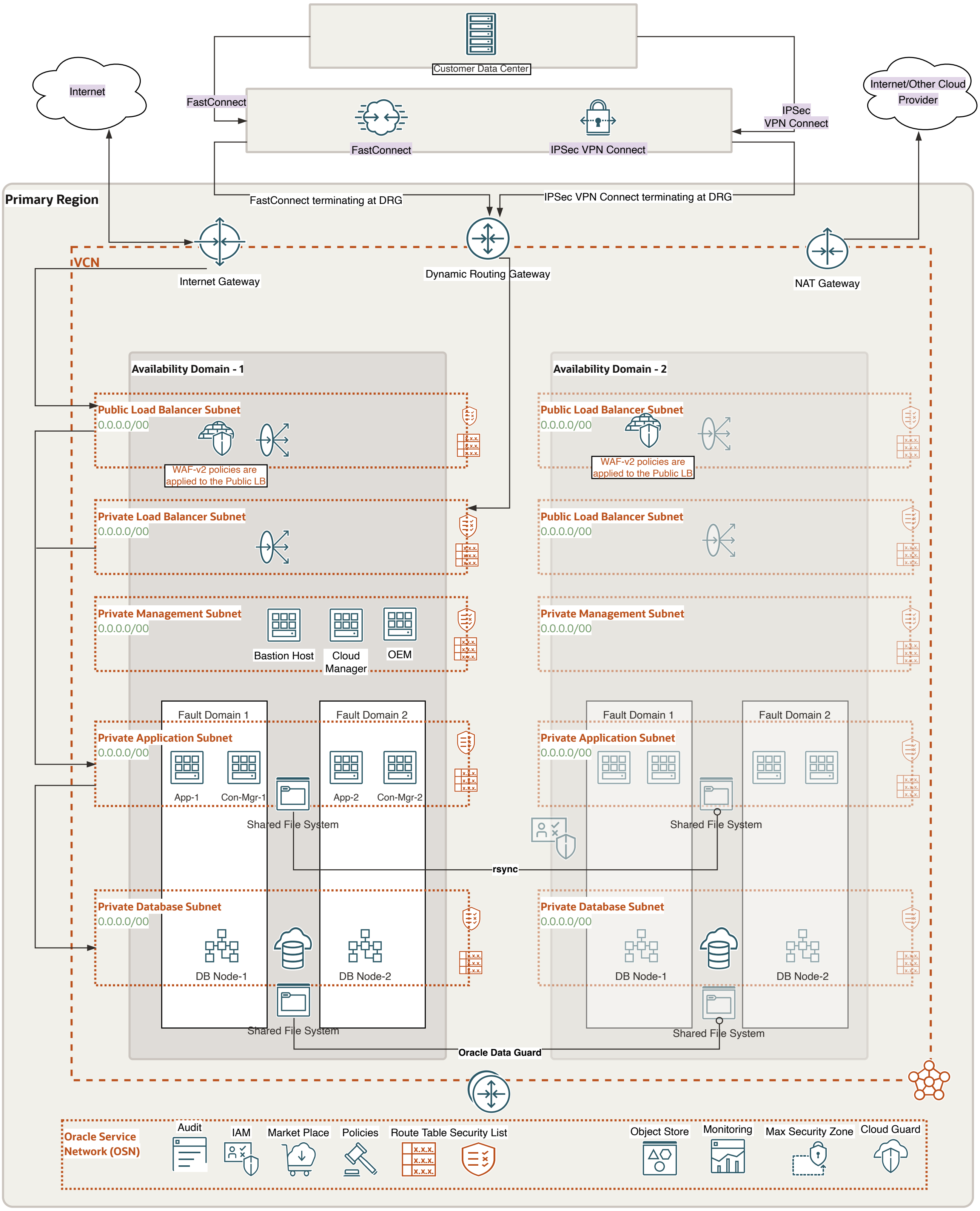


Figure 1: Future State Deployment Diagram - EBS Workload Multi-AD, DR Design Diagram

Deployment architecture for the 'X' environment of the Customers EBS Workload, in OCI, is illustrated below:

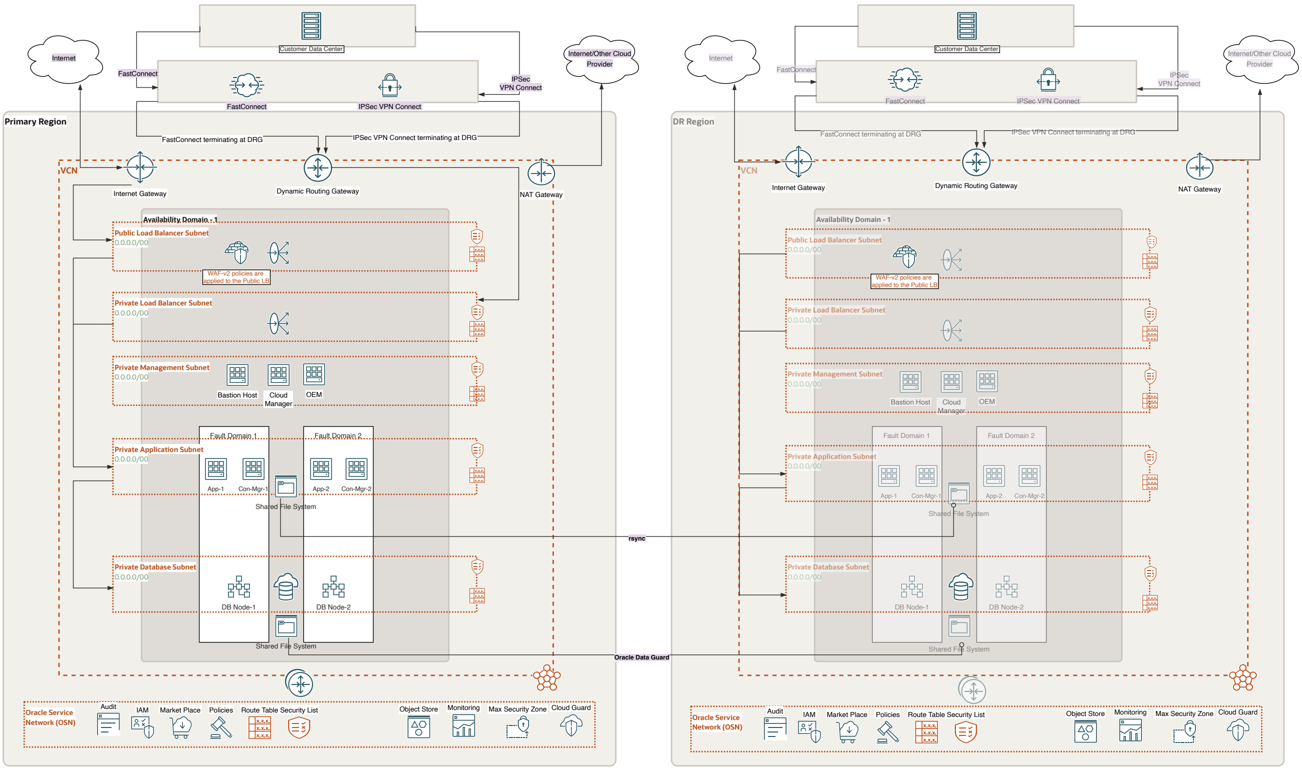


Figure 2: Future State Deployment Diagram - EBS Workload Single AD, DR Design Diagram

Deployment architecture for the Production environment of the Customers EBS Workload, in OCI, is illustrated below:

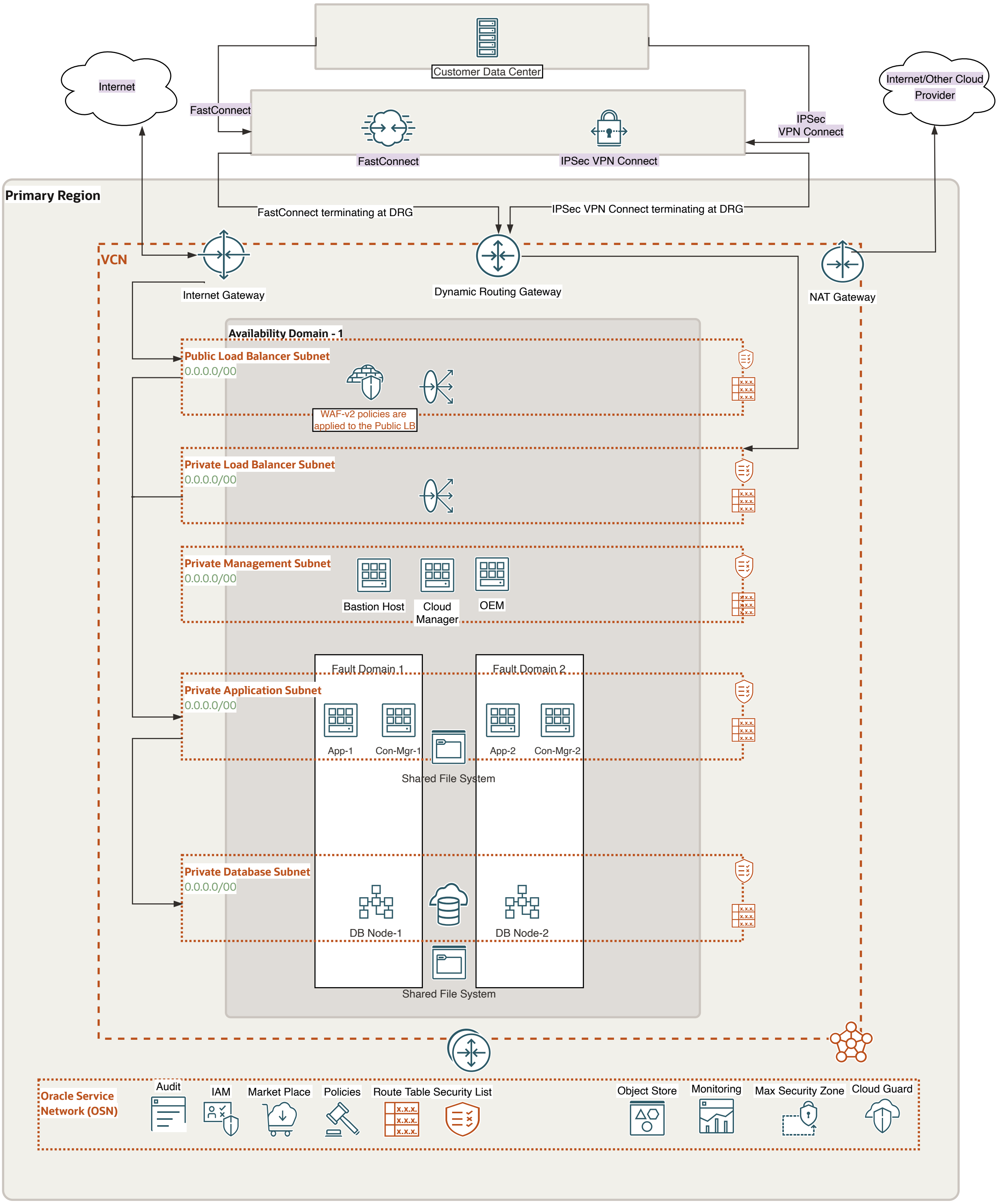


Figure 3: Future State Deployment Diagram - EBS Workload Single AD, Production Design Diagram

Deployment architecture for the Development environment of the Customers EBS Workload, in OCI, is illustrated below:

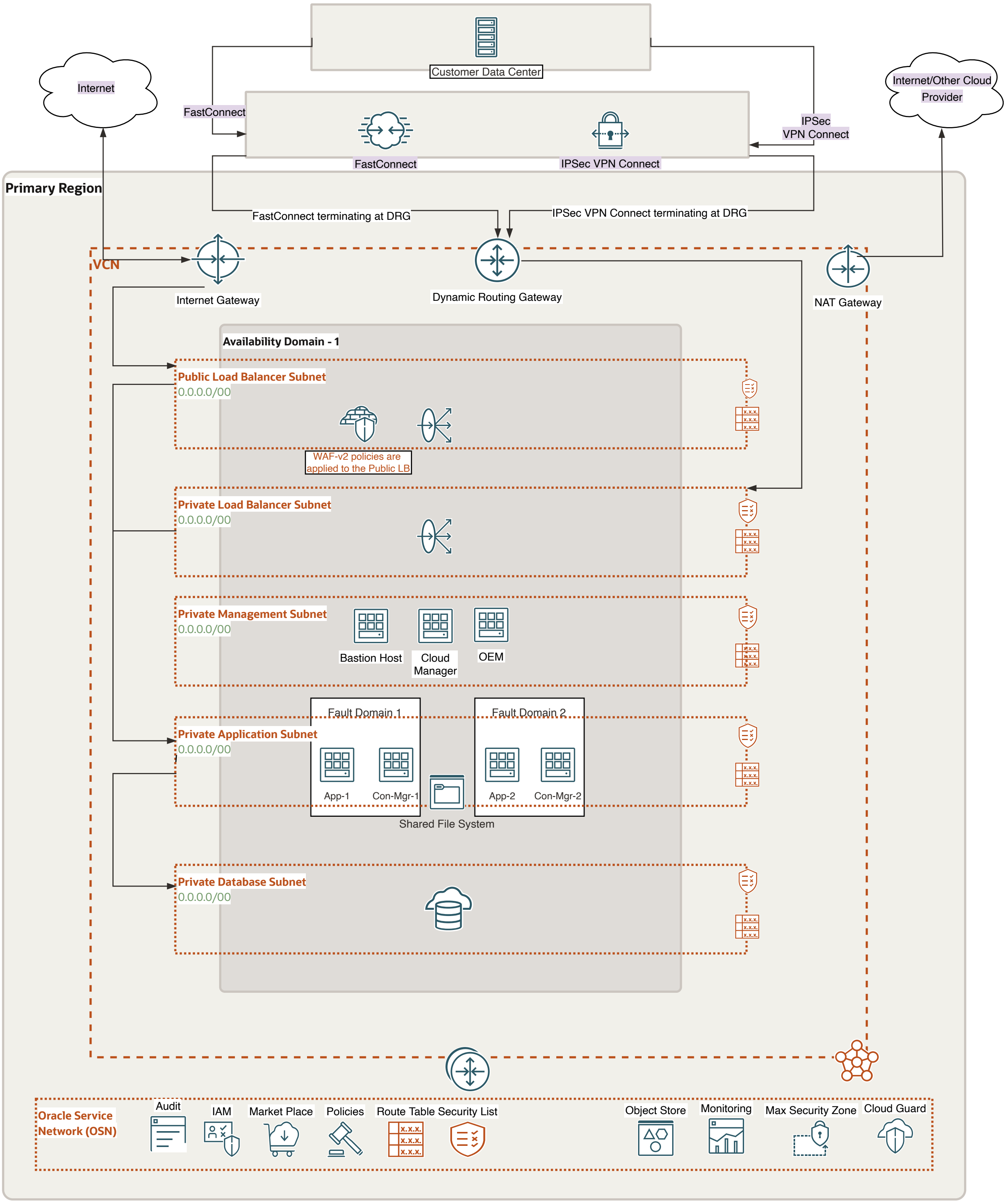


Figure 4: Future State Deployment Diagram - EBS Workload Single AD, Development Design Diagram

Deployment architecture for the 'Hub and Spoke Topology' is illustrated below:

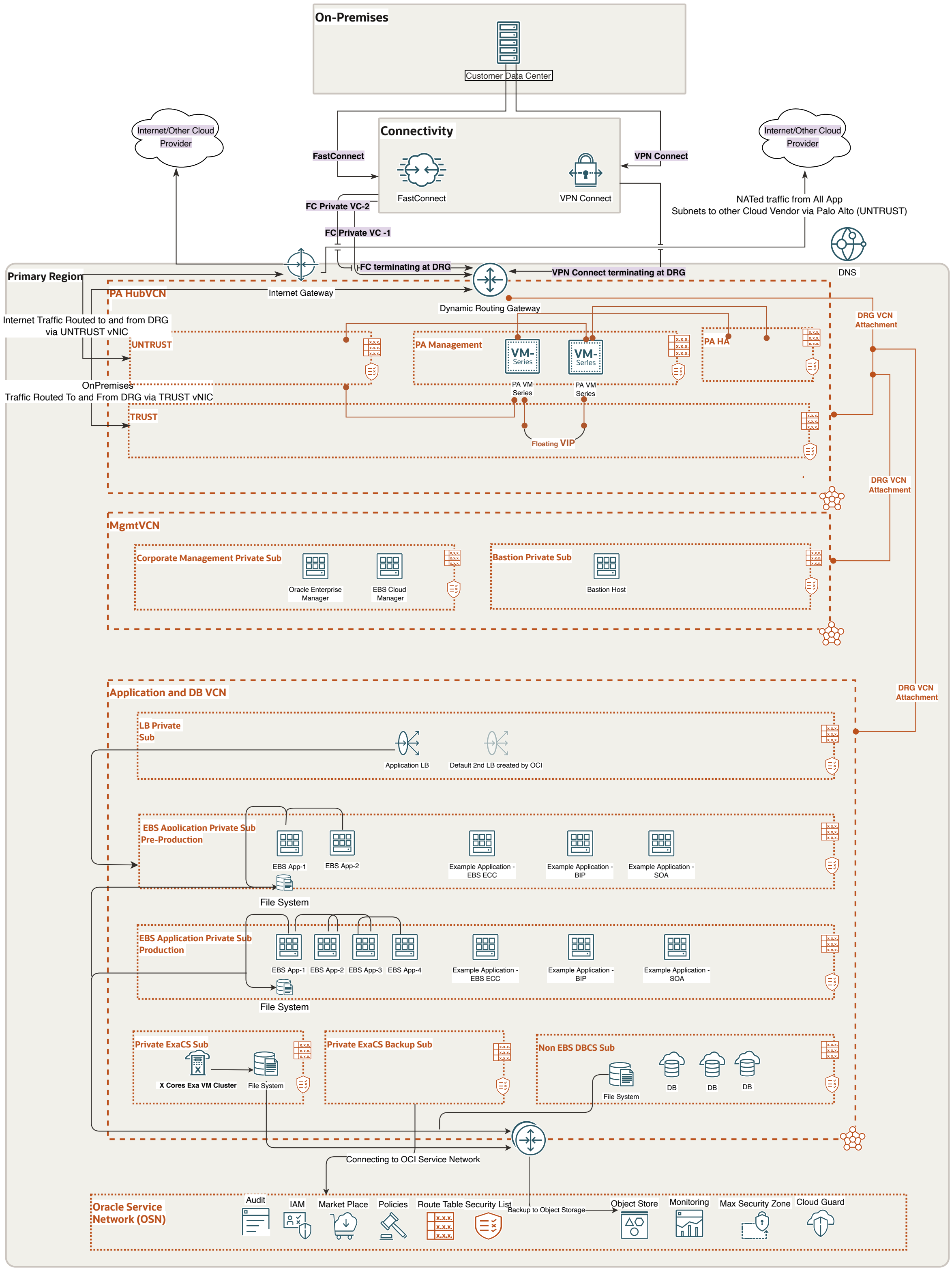


Figure 5: Future State Deployment Diagram - EBS Workload Hub and Spoke with Palo Alto Design Diagram

Deployment architecture including two tenancies:'Tenancy - A' and Tenancy - B' are illustrated in the design below:

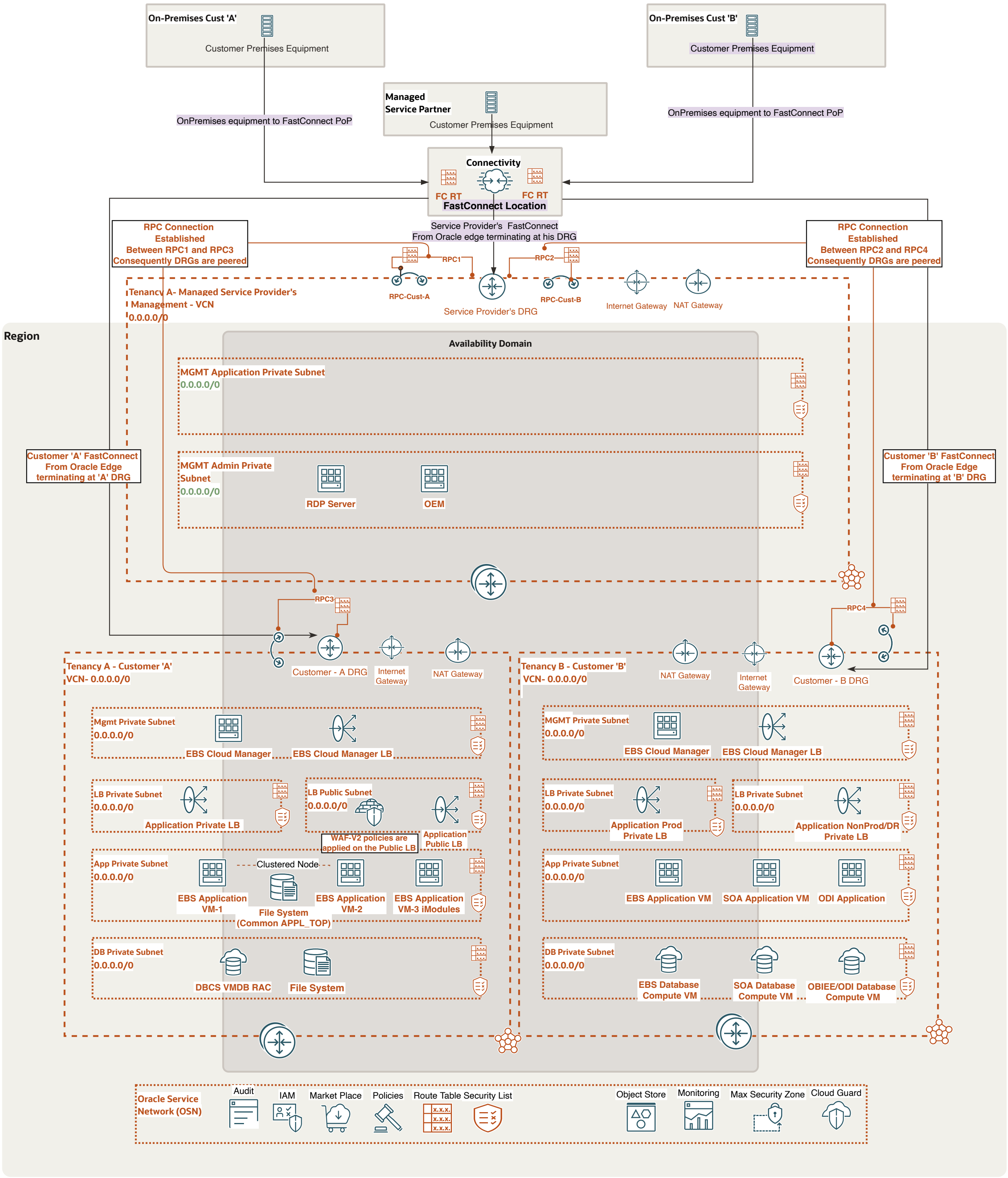

On-Premises Cust 'A'
Customer Premises Equipment
On-Premises Cust 'B'
Customer Premises Equipment
Managed Service Partner
Customer Premises Equipment
OnPremises equipment to FastConnect PoP
OnPremises equipment to FastConnect PoP
Connectivity
FC RT
FC RT
FastConnect Location
Service Provider's FastConnect From Oracle edge terminating at his DRG
RPC Connection Established Between RPC1 and RPC3 Consequently DRGs are peered
RPC Connection Established Between RPC2 and RPC4 Consequently DRGs are peered
RPC1
RPC2
RPC-Cust-A
RPC-Cust-B
Service Provider's DRG
Internet Gateway
NAT Gateway
Tenancy A- Managed Service Provider's Management - VCN 0.0.0.0/0
Region
Availability Domain
MGMT Application Private Subnet 0.0.0.0/0
MGMT Admin Private Subnet 0.0.0.0/0
RDP Server
OEM
Customer 'A' FastConnect From Oracle Edge terminating at 'A' DRG
Customer 'B' FastConnect From Oracle Edge terminating at 'B' DRG
RPC3
RPC4
Customer - A DRG
Internet Gateway
NAT Gateway
NAT Gateway
Internet Gateway
Customer - B DRG
Tenancy A - Customer 'A' VCN- 0.0.0.0/0
Tenancy B - Customer 'B' VCN- 0.0.0.0/0
Mgmt Private Subnet 0.0.0.0/0
EBS Cloud Manager
EBS Cloud Manager LB
LB Private Subnet 0.0.0.0/0
Application Private LB
LB Public Subnet 0.0.0.0/0
WAF-V2 policies are applied on the Public LB
Application Public LB
App Private Subnet 0.0.0.0/0
Clustered Node
EBS Application VM-1
File System (Common APPL_TOP)
EBS Application VM-2
EBS Application VM-3 iModules
DB Private Subnet 0.0.0.0/0
DBCS VMDB RAC
File System
MGMT Private Subnet 0.0.0.0/0
EBS Cloud Manager
EBS Cloud Manager LB
LB Private Subnet 0.0.0.0/0
Application Prod Private LB
LB Private Subnet 0.0.0.0/0
Application NonProd/DR Private LB
App Private Subnet 0.0.0.0/0
EBS Application VM
SOA Application VM
ODI Application
DB Private Subnet 0.0.0.0/0
EBS Database Compute VM
SOA Database Compute VM
OBIEE/ODI Database Compute VM
Oracle Service Network (OSN)
Audit
IAM
Market Place
Policies
Route Table
Security List
Object Store
Monitoring
Max Security Zone
Cloud Guard

Figure 6: Future State Deployment Diagram - EBS Workload Multiple tenancies with RPC Design Diagram

For official copy of the Multi-Tenancy diagram, please see the **OCI Architecture Center Reference Architecture**

3.4 Solutions Considerations

Guide:

A section describing the Future EBS workload of the Customer in OCI Describe certain aspects of your solution in detail. What are the security, resilience, networking, and operations decisions you have taken that are important for your customer?

Example:

Proposed plan is to move EBS Application server (_12.2) in the compute VM shapes on the latest OS and kernel version (which is supported). On-Premises RAC Database (**19c**) will be migrated to a VM-DB RAC system based on a multitenant architecture.

Oracle Cloud Infrastructure Web Application Firewall (WAF) helps you make your endpoints more secure by monitoring and filtering out potentially malicious traffic. It is a cloud-based, Payment Card Industry (PCI) compliant, global security service that protects applications from malicious and unwanted internet traffic.

3.4.1 High Availability and Disaster Recovery

Guide:

Please describe the Oracle MAA in the context of EBS.

Example:

Oracle Maximum Availability Architecture (MAA) is Oracle's best practice blueprint based on proven Oracle high availability technologies and recommendations. The goal of MAA is to achieve the optimal high-availability architecture at the lowest cost and complexity. Papers are published on the Oracle Technology Network OTN.

To achieve maximum Oracle E-Business Suite database availability, Oracle recommends deploying EBS on an Oracle Database MAA foundation that includes the following technologies: - Oracle Real Application Clusters (RAC) - Oracle Data Guard - Oracle Flashback Database - Oracle Automatic Storage Management - Oracle Recovery Manager and Oracle Secure Backup - Oracle Online Upgrade Using Edition-Based Redefinition

Please refer to the following reference paper for detail.

Reference:

HA Reference for EBS

3.4.1.1 Backup and Recovery

Guide:

A section describing the 'Backup and Recovery' practices of the Customer in OCI

Example:

We will follow the current Backup and Recovery strategy and practices of the Customer. Customer has the following Recovery Time Objective (RTO) and Recovery Point Objective (RPO) requirements which will be achieved with the proposed architecture:

- Official RTO practices: less than 24 hrs
- Official RPO practices: 4 hours

3.4.2 Security

Guide:

A section describing the Security in OCI in the context of the EBS Application

Example:

The objective of the security architecture is to enable you to maintain your security posture when running E-Business Suite and associated applications in the Oracle Cloud.

Oracle has designed security into every aspect of our infrastructure to help our customers achieve better protection, isolation and control. We started by taking a unique design approach, separating the network and server environments. This way, if an attack occurs on a VM, we can contain that threat and prevent it from moving to other servers, resulting in better protection and lower risk for customers.

We also hyper-segment our physical network and backend infrastructure for secure isolation between customer instances and backend hosts. Additionally, we've implemented hardware-based root of trust, making sure each server is pristine each and every time it is provisioned.

The below diagram shows the security posture of EBS in OCI.

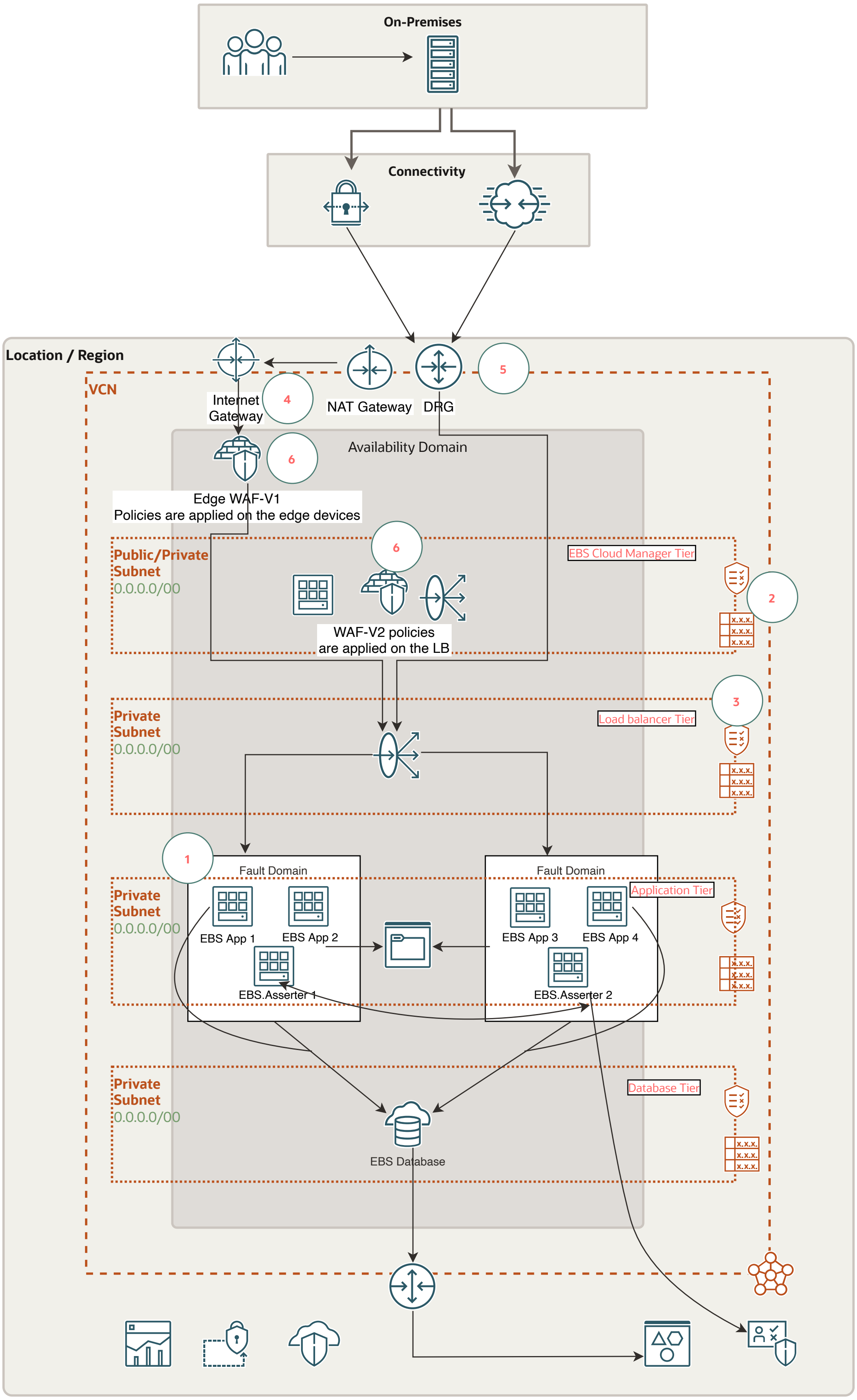


Figure 7: EBS Network Security

For each customer’s VCN there is a range of defense in depth protections available spanning across **layers 3-7**.

VCN (1): A VCN provides isolation for your workload from any other workload on Oracle Cloud Infrastructure, including your other workloads in a different VCN.

Internal Firewalls (2): Implement virtual firewalls at the subnet level using VCN security lists.

Load Balancing Traffic Securely (3): TLS 1.2 is supported by default to securely balance traffic within the implementation and from external connections.

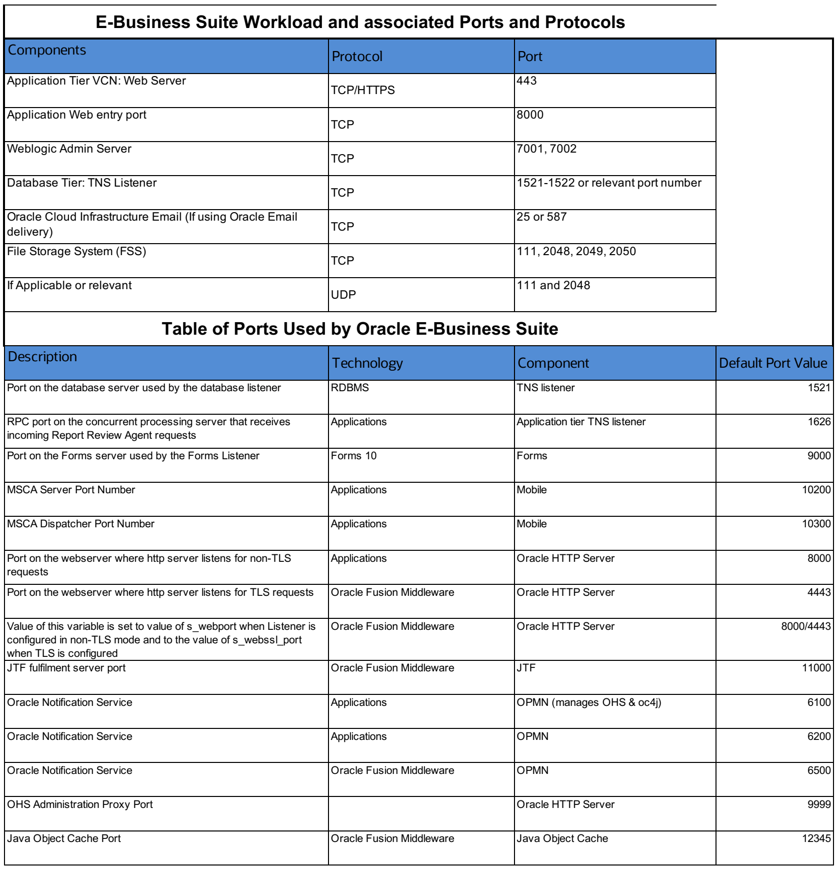
Secure Traffic Between ADs and Regions: Communications between ADs are encrypted with Media Access Control security (MACsec) to prevent layer 2 security threats such as wiretapping, DDoS, intrusion, man-in-the-middle and playback attacks. VCN traffic that travel between regions are either sent over private links or are encrypted.

Secure Connectivity to Public Internet (4): For security, a VCN has no internet connectivity by default. Therefore, internet bound traffic to / from a VCN must pass through an IGW. Virtual routing tables can be implemented with private IP addresses for use with NAT and 3rd party firewall devices for additional security.

Secure Connectivity Between Your VCN and Data Center (5): Traffic can be routed through a DRG for private traffic. It is used with an IPSec VPN or FastConnect connection to establish private connectivity between a VCN and an On-Premises or other cloud network.

Protect Internet-Facing Applications (6): Oracle Cloud Infrastructure Web Application Firewall is a regional-based and edge enforcement service that is attached to an enforcement point, such as a load balancer or a web application domain name. WAF protects applications from malicious and unwanted internet traffic. WAF can protect any internet facing endpoint, providing consistent rule enforcement across a customer's applications. It also inspects any request going from the web application server to the end user. Additionally, Oracle’s optional global 'anycast' DNS service also takes advantage of DNS-based DDoS protections providing resiliency at the DNS layers.

- Specific to some use cases: Route details for a specific use case like Hub and Spoke
- Application authentication and authorization details (If applicable how Application users are going to access the Application and associated privilege control mechanism(for example role based access control), federation with other IdP like Microsoft/Azure AD)
- Specific to some use cases: Using any specific security services available in OCI like Security Zone, Security Advisor
- Specific to some use cases: Customer from specific Industry (Financial) might require PCI compliant services like WAF
- Oracle E-Business Suite requires policies with the following ports and protocol to be open



E-Business Suite Workload and associated Ports and Protocols

Components	Protocol	Port
Application Tier VCN: Web Server	TCP/HTTPS	443
Application Web entry port	TCP	8000
Weblogic Admin Server	TCP	7001, 7002
Database Tier: TNS Listener	TCP	1521-1522 or relevant port number
Oracle Cloud Infrastructure Email (If using Oracle Email delivery)	TCP	25 or 587
File Storage System (FSS)	TCP	111, 2048, 2049, 2050
If Applicable or relevant	UDP	111 and 2048

Table of Ports Used by Oracle E-Business Suite

Description	Technology	Component	Default Port Value
Port on the database server used by the database listener	RDBMS	TNS listener	1521
RPC port on the concurrent processing server that receives incoming Report Review Agent requests	Applications	Application tier TNS listener	1626
Port on the Forms server used by the Forms Listener	Forms 10	Forms	9000
MSCA Server Port Number	Applications	Mobile	10200
MSCA Dispatcher Port Number	Applications	Mobile	10300
Port on the webserver where http server listens for non-TLS requests	Applications	Oracle HTTP Server	8000
Port on the webserver where http server listens for TLS requests	Oracle Fusion Middleware	Oracle HTTP Server	4443
Value of this variable is set to value of s_webport when Listener is configured in non-TLS mode and to the value of s_webssl_port when TLS is configured	Oracle Fusion Middleware	Oracle HTTP Server	8000/4443
JTF fulfilment server port	Oracle Fusion Middleware	JTF	11000
Oracle Notification Service	Applications	OPMN (manages OHS & oc4j)	6100
Oracle Notification Service	Applications	OPMN	6200
Oracle Notification Service	Oracle Fusion Middleware	OPMN	6500
OHS Administration Proxy Port		Oracle HTTP Server	9999
Java Object Cache Port	Oracle Fusion Middleware	Java Object Cache	12345

Figure 8: Port and Protocol Requirement for EBS Workload

__Note:__Please see generic OCI security guidelines in the Annex.

3.4.3 Workload Access

Guide:

A section describing how Customer will access their Application in OCI

Example:

Customer will access the EBS workload internally over the OCI FastConnect connectivity solution and EBS external end-points will be secured by OCI Web Application Firewall (WAF). FastConnect is a private, dedicated connectivity that improves security, it supports bandwidths from 1Gbps to 10Gbps. An alternative option to FastConnect is Virtual Private Network (VPN). VPN could also be a backup configuration if FastConnect is down.

3.4.4 Workload Monitoring

Guide:

A section describing how Customer will monitor their Application in OCI

Example:

Customer will use OEM to monitor their EBS workload. Customer can also leverage OCI Stack Monitoring for EBS. For detail please check the below blog article specified in the reference section.

Reference:

OCI Stack Monitoring for EBS

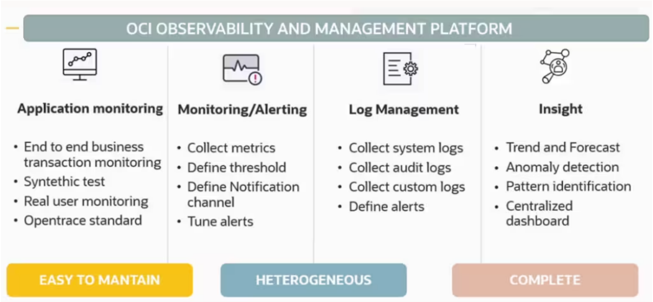
3.4.5 Manageability and Observability (OCI)

Example:

Observability is a technology advancement focused on getting insights from a vast array of data, logs, and events generated within an IT environment. By implementing an Observability strategy, organizations gain the capability to anticipate system disruptions, prevent resource overconsumption, and enhance the overall application user satisfaction. That means being proactive, which is a must, especially in a distributed environment.

Gone are the days when the IT landscape remained a mysterious black box. The company's digitalization and the Cloud model compel C-level executives to gain comprehensive insights into asset utilization. The efficient allocation of resources directly influences budgetary considerations.

Observability helps organizations examine how well their infrastructure is working, predict future needs, and help take proactive steps to improve efficiency and protect investments. Therefore, Observability tools are needed to cover these important areas.



OCI OBSERVABILITY AND MANAGEMENT PLATFORM

Application monitoring

- End to end business transaction monitoring
- Syntethic test
- Real user monitoring
- Opentrace standard

Monitoring/Alerting

- Collect metrics
- Define threshold
- Define Notification channel
- Tune alerts

Log Management

- Collect system logs
- Collect audit logs
- Collect custom logs
- Define alerts

Insight

- Trend and Forecast
- Anomaly detection
- Pattern identification
- Centralized dashboard

EASY TO MANTAIN

HETEROGENEOUS

COMPLETE

Figure 9: Observability and Manageability

3.4.5.1 Observability Architecture

The basic monitoring OCI services collect the data and send logs and metrics to OCI Monitoring and Logging services. If you want to apply machine-learning capabilities and perform analysis, you can send the data to the Logging Analytics service. If you want to use OCI Logging Analytics to collect logs coming from both on-premises and cloud sources to analyze them for auditing, security purposes, or to integrate data with an external SIEM solution, the Connector Hub serves as the solution.

It's advisable to plan your monitoring strategy by considering both the O&M (Observability and Management) native service of OCI and its integration with third-party tools, as O&M is flexible and a highly customizable solution.

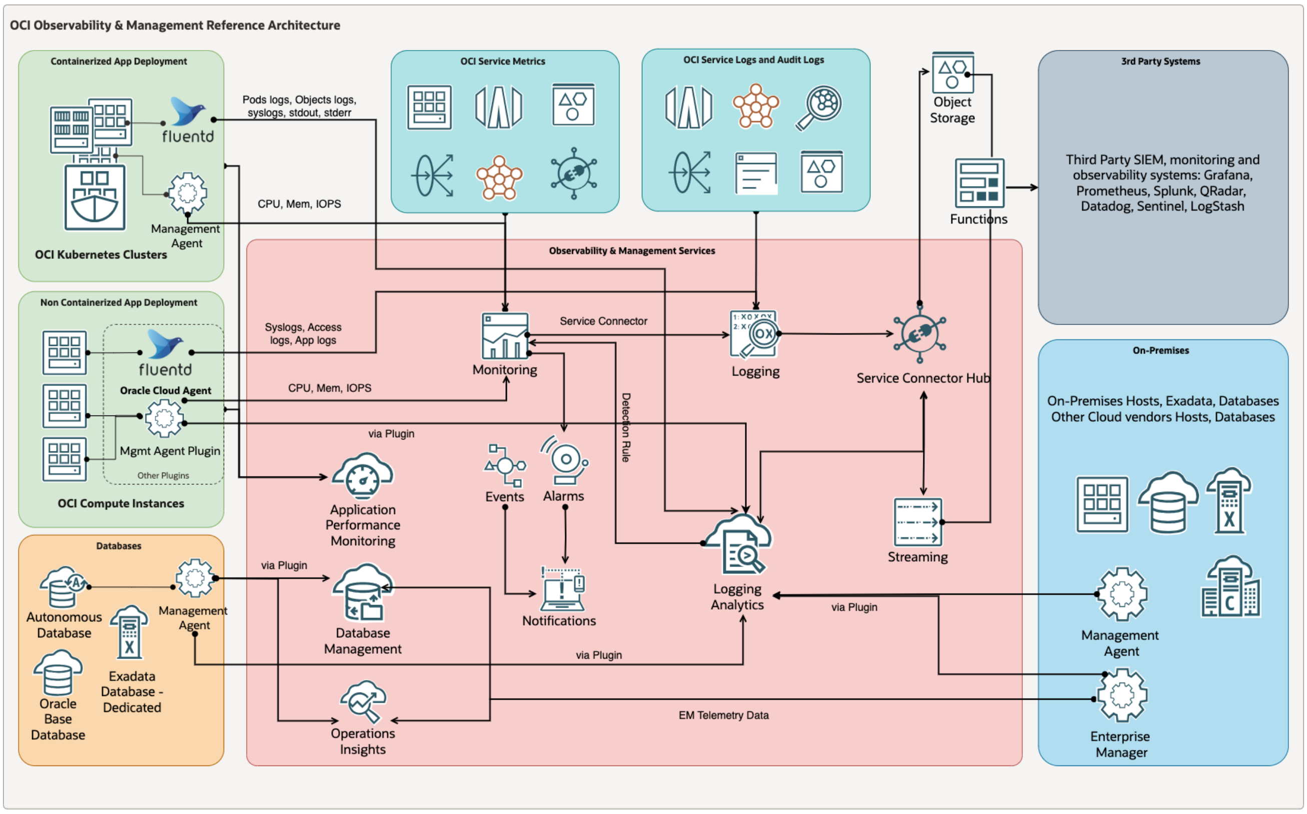


Figure 10: OCI Architecture

3.4.5.2 Real-Time Monitoring

Real-time monitoring is the delivery of continuously updated data about systems, processes, or events. Such monitoring provides information streaming at zero or low latency, so there is minimal delay between data collection and analysis. It enables quick detection of anomalies, performance issues, and critical events.

Please find all references for this chapter in the Annex.

3.4.5.3 Performance and Tuning

Performance tuning is the improvement of system performance. It can be done proactively to prevent issues or reactively in response to increased workload, which is crucial for avoiding system outages.

Please find all references for this chapter in the Annex.

3.4.5.4 Administration

Administrator tasks involve upholding a data management policy and ensuring essential equipment functionality, such as instance management, backup & restore operations, key management, and allocating resources from the database to the storage.

Please find all references for this chapter in the Annex.

3.4.5.5 Troubleshooting

Issues can happen on several levels. To identify the root cause, it is important to be able to correlate resources, drill down into the issues, and analyze trends in the systems. It's crucial to consider that the application itself might be the root cause of the issue. Therefore, it's essential to gather information about the application's behavior and performance to fully understand the problem and resolve it effectively. Troubleshooting also allows you to avoid an outage which is why it is important to notice issues as early as possible.

Please find all references for this chapter in the Annex.

3.4.5.6 Cost Control and Chargeback

Cost control is the practice of identifying and reducing business expenses to increase profits. It starts with the budgeting process. Cost control is an important factor in maintaining and growing profitability.

IT chargeback can provide greater visibility into the costs of IT services and infrastructure usage. It enables organizations to identify opportunities for cost optimization and reduce wasteful spending.

Cost control and chargeback are critical concerns, especially for companies transitioning to the cloud, presenting new financial operational challenges (FinOps). In this context, reducing consumption directly impacts the company's business.

Please find all references for this chapter in the Annex.

3.4.6 Regulations and Compliances

Guide:

A section describing any Customer-specific 'Regulation and Compliance if any' in OCI

Example:

None has been discussed at the time of Migration.

3.4.7 Cloud Manger - EBS Automation Tool

Guide:

A section describing the Cloud Manager Tooling for EBS Workload

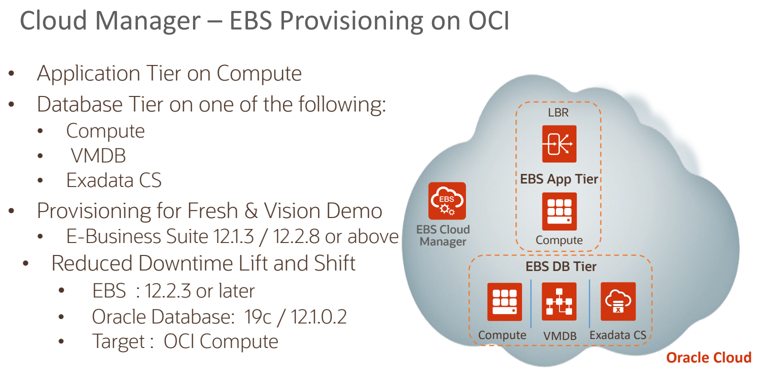
Example:

3.4.7.1 What is EBS CM

- Oracle EBS CM is a key component of the Oracle EBS automation for OCI.
- Oracle EBS CM is a web-based application that drives all the principal automation flows for Oracle E-Business Suite on Oracle Cloud Infrastructure, including provisioning new environments, performing lifecycle management activities on those environments, and restoring environments from on-premises.
- This is Oracle’s recommended way to deploy EBS on OCI.

3.4.7.2 High level Deployment steps using EBS CM

Using CM, one can provision a new environment or can perform a 'lift-and-shift' as depicted in the diagram below:

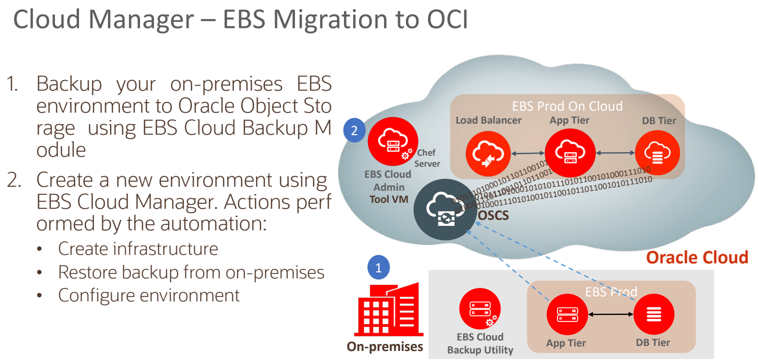


Cloud Manager – EBS Provisioning on OCI

- Application Tier on Compute
- Database Tier on one of the following:
  - Compute
  - VMDB
  - Exadata CS
- Provisioning for Fresh & Vision Demo
  - E-Business Suite 12.1.3 / 12.2.8 or above
- Reduced Downtime Lift and Shift
  - EBS : 12.2.3 or later
  - Oracle Database: 19c / 12.1.0.2
  - Target : OCI Compute

Figure 11: EBS CM Provisioning Diagram

How EBS CM can help to migrate EBS workload to OCI is depicted in the diagram below:



Cloud Manager – EBS Migration to OCI

1. Backup your on-premises EBS environment to Oracle Object Storage using EBS Cloud Backup Module
2. Create a new environment using EBS Cloud Manager. Actions performed by the automation:
   - Create infrastructure
   - Restore backup from on-premises
   - Configure environment

Figure 12: EBS CM MIgration Diagram

- If the Customer EBS estate is not compatible with CM, then we have to go for other migration options like manual Implementation.
- Another scenario could be to move Customer Workload and/or other Solution components 'as-is' to OCI using Rackware or similar tool.

3.4.7.3 Options for Automated EBS Lift & Shift from On-Premises

Automation is provided for a selection of deployment and management scenarios. These automation capabilities are continually being extended and enhanced. Details about the below table can be obtained from the My Oracle Support Doc Id: **2517025.1**

EBS Release	Apps Tier	Database Release	Target DB Tier
* 12.2.3 or later	* OCI Compute VMs	- 19c (19.3 and later)	* OCI Compute VM
* 12.1.3		- 12.1.0.2	* 1-Node VM DB System
		- 11.2.0.4	* 2-Node VM DB System (Oracle RAC)
			* Exadata DB System

3.4.8 OCI Networking

Guide:

A section describing OCI networking capabilities and features

Example:

Oracle Cloud Infrastructure (OCI) networking and connectivity products and services enable customers to manage and scale their networks. Please refer to the following article for a better understanding of OCI networking capabilities and how they can be leveraged for Customer advantage.

Reference:

- Oracle's Networking capabilities
- OCI Networking Best Practices
- Best practices for hybrid and multicloud OCI networking design

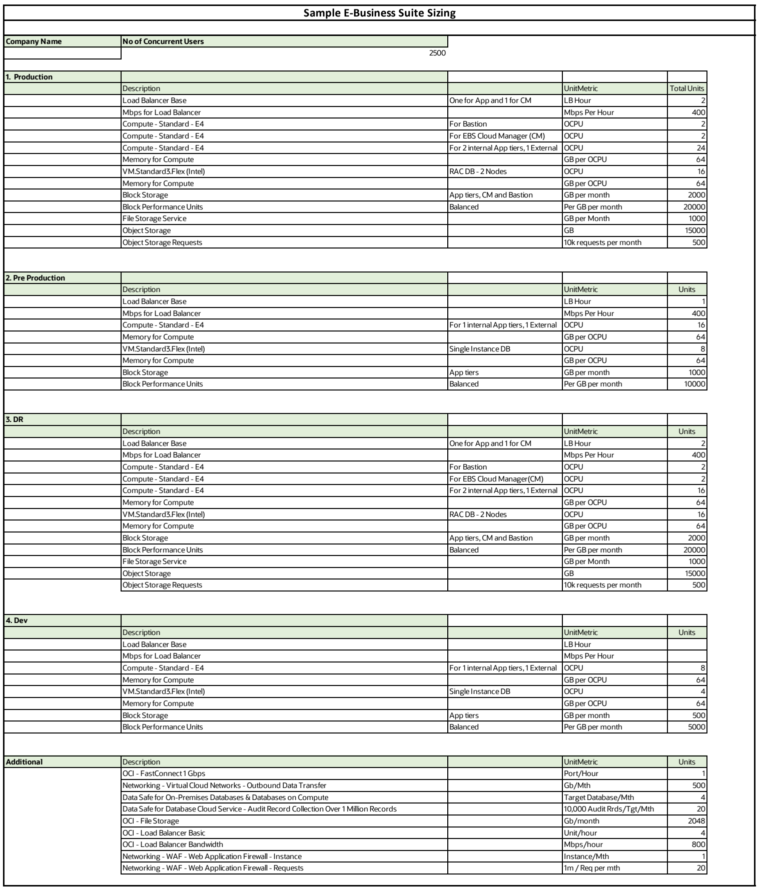
3.5 Sizing and Bill of Materials

Guide:

A section describing the Future EBS workload sizing in OCI

Example:

A sample sizing of the EBS workload is reflected in the diagram below for reference purposes:



Sample E-Business Suite Sizing

Company Name	**No of Concurrent Users**			
	2500			
1. Production				
	Description		UnitMetric	Total Units
	Load Balancer Base	One for App and 1 for CM	LB Hour	2
	Mbps for Load Balancer		Mbps Per Hour	400
	Compute - Standard - E4	For Bastion	OCPU	2
	Compute - Standard - E4	For EBS Cloud Manager (CM)	OCPU	2
	Compute - Standard - E4	For 2 internal App tiers, 1 External	OCPU	24
	Memory for Compute		GB per OCPU	64
	VM.Standard3.Flex (Intel)	RAC DB - 2 Nodes	OCPU	16
	Memory for Compute		GB per OCPU	64
	Block Storage	App tiers, CM and Bastion	GB per month	2000
	Block Performance Units	Balanced	Per GB per month	20000
	File Storage Service		GB per Month	1000
	Object Storage		GB	15000
	Object Storage Requests		10k requests per month	500
2. Pre Production				
	Description		UnitMetric	Units
	Load Balancer Base		LB Hour	1
	Mbps for Load Balancer		Mbps Per Hour	400
	Compute - Standard - E4	For 1 internal App tiers, 1 External	OCPU	16
	Memory for Compute		GB per OCPU	64
	VM.Standard3.Flex (Intel)	Single Instance DB	OCPU	8
	Memory for Compute		GB per OCPU	64
	Block Storage	App tiers	GB per month	1000
	Block Performance Units	Balanced	Per GB per month	10000
3. DR				
	Description		UnitMetric	Units
	Load Balancer Base	One for App and 1 for CM	LB Hour	2
	Mbps for Load Balancer		Mbps Per Hour	400
	Compute - Standard - E4	For Bastion	OCPU	2
	Compute - Standard - E4	For EBS Cloud Manager(CM)	OCPU	2
	Compute - Standard - E4	For 2 internal App tiers, 1 External	OCPU	16
	Memory for Compute		GB per OCPU	64
	VM.Standard3.Flex (Intel)	RAC DB - 2 Nodes	OCPU	16
	Memory for Compute		GB per OCPU	64
	Block Storage	App tiers, CM and Bastion	GB per month	2000
	Block Performance Units	Balanced	Per GB per month	20000
	File Storage Service		GB per Month	1000
	Object Storage		GB	15000
	Object Storage Requests		10k requests per month	500
4. Dev				
	Description		UnitMetric	Units
	Load Balancer Base		LB Hour	
	Mbps for Load Balancer		Mbps Per Hour	
	Compute - Standard - E4	For 1 internal App tiers, 1 External	OCPU	8
	Memory for Compute		GB per OCPU	64
	VM.Standard3.Flex (Intel)	Single Instance DB	OCPU	4
	Memory for Compute		GB per OCPU	64
	Block Storage	App tiers	GB per month	500
	Block Performance Units	Balanced	Per GB per month	5000
Additional	Description		UnitMetric	Units
	OCI - FastConnect 1 Gbps		Port/Hour	1
	Networking - Virtual Cloud Networks - Outbound Data Transfer		Gb/Mth	500
	Data Safe for On-Premises Databases & Databases on Compute		Target Database/Mth	4
	Data Safe for Database Cloud Service - Audit Record Collection Over 1 Million Records		10,000 Audit Rrds/Tgt/Mth	20
	OCI - File Storage		Gb/month	2048
	OCI - Load Balancer Basic		Unit/hour	4
	OCI - Load Balancer Bandwidth		Mbps/hour	800
	Networking - WAF - Web Application Firewall - Instance		Instance/Mth	1
	Networking - WAF - Web Application Firewall - Requests		1m / Req per mth	20

Figure 13: OCI - Bill of Materials

ANNEX

4.1 Security Guidelines

4.1.1 Oracle Security, Identity, and Compliance

Oracle Cloud Infrastructure (OCI) is designed to protect customer workloads with a security-first approach across compute, network, and storage – down to the hardware. It's complemented by essential security services to provide the required levels of security for your most business-critical workloads.

- Security Strategy – To create a successful security strategy and architecture for your deployments on OCI, it's helpful to understand Oracle's security principles and the OCI security services landscape.
- The security pillar capabilities reflect fundamental security principles for architecture, deployment, and mainte-

nance. The best practices in the security pillar, help your organization to define a secure cloud architecture, identify and implement the right security controls, and monitor and prevent issues such as configuration drift.

4.1.2 References

- The Best Practices Framework for OCI provides architectural guidance about how to build OCI services in a secure fashion, based on recommendations in the Best practices framework for Oracle Cloud Infrastructure.
- Learn more about Oracle Cloud Security Practices.
- For detailed information about security responsibilities in Oracle Cloud Infrastructure, see the Oracle Cloud Infrastructure Security Guide.

4.1.3 Compliance and Regulations

Cloud computing is fundamentally different from traditional on-premises computing. In the traditional model, organizations are typically in full control of their technology infrastructure located on-premises (e.g., physical control of the hardware, and full control over the technology stack in production). In the cloud, organizations leverage resources and practices that are under the control of the cloud service provider, while still retaining some control and responsibility over other components of their IT solution. As a result, managing security and privacy in the cloud is often a shared responsibility between the cloud customer and the cloud service provider. The distribution of responsibilities between the cloud service provider and the customer also varies based on the nature of the cloud service (IaaS, PaaS, SaaS).

4.1.4 Additional Resources

- Oracle Cloud Compliance – Oracle is committed to helping customers operate globally in a fast-changing business environment and address the challenges of an evermore complex regulatory environment. This site is a primary reference for customers on the Shared Management Model with Attestations and Advisories.
- Oracle Security Practices – Oracle's security practices are multidimensional, encompassing how the company develops and manages enterprise systems, and cloud and on-premises products and services.
- Oracle Cloud Security Practices documents.
- Contract Documents for Oracle Cloud Services.
- OCI Shared Security Model
- OCI Cloud Adoption Framework Security Strategy
- OCI Security Guide
- OCI Cloud Adoption Framework Security chapter

4.2 Networking Requirement Considerations

The below questions help to identify networking requirements.

4.2.1 Application Connectivity

- Does your application need to be exposed to the internet?
- Does your solution on DC (on-prem) need to be connected 24x7 to OCI in a Hybrid model?
  - Site-to-Site IPSEC (Y/N)
  - Dedicated Lines (FC) (Y/N)
- Are there any specific network security requirements for your application? (No internet, encryption, etc, etc)
- Will your application require connectivity to other cloud providers?
  - Site-to-Site IPSEC (Y/N)
  - Dedicated Lines (FC) (Y/N)
- Will your application require inter-region connectivity?
- Are you planning to reuse IP addresses from your on-premises environment in OCI?
- If yes, what steps have you taken to ensure IP address compatibility and avoid conflicts?
- How will you handle network address translation (NAT) for IP reuse in OCI?
- Will you bring your own public IPs to OCI?

4.2.2 DR and Business Continuity

- Does your organization need a Business Continuity/DR Plan to address potential disruptions?
  - Network Requirements (min latency, bandwidth, etc)
  - RPO/RTO values
- What are your requirements regarding Data Replication and Geo-Redundancy (different regions, restrictions, etc.)?
- Are you planning to distribute incoming traffic across multiple instances or regions to achieve business continuity?
- What strategies do you require to guarantee minimal downtime and data loss, and to swiftly recover from any unforeseen incidents?

4.2.3 High Availability and Scalability

- Does your application require load balancing for high availability and scalability? (y/n)
  - Does your application span around the globe or is regionally located?
  - How do you intend to ensure seamless user experiences and consistent connections in your application (session persistence, affinity, etc.)?
  - What are the network Security requirements for traffic management (SSL offloading, X509 certificates management, etc.)?
  - Does your application use name resolutions and traffic steering across multiple regions (Public DNS steering)?

4.2.4 Security and Access Control

- Some of the below questions help you to adopt the right sizing and deployment model of the network firewall.
  - Does the customer need to protect traffic from VCN to VCN?
  - Does the customer need to protect traffic from subnet to subnet in the same VCN?
  - When deploying an OCI Network Firewall in a dedicated HUB or secure VCN, do you want to protect inter-VCN traffic and/or inter-subnet traffic from within the same VCN?
  - Does the customer need to protect incoming or egressing traffic to the internet?
  - Does the customer need to protect internal traffic (including on-premises via IPSEC/FC)?
  - Is the network performance critical?
  - Does the customer have any requirement on network isolation (i.e., internet traffic never traverses or is mixed with internal traffic)?
- Have you considered the importance of protecting your web applications from potential cyber threats using a Web Application Firewall (WAF)?

4.2.5 Monitoring and Troubleshooting

- How do you plan to monitor your application's network performance in OCI?
- How can you proactively address and resolve any potential network connectivity challenges your company might face?
- How do you plan to troubleshoot your network connectivity?

4.3 Networking Solutions

4.3.1 OCI Network Firewall

Oracle Cloud Infrastructure Network Firewall is a next-generation managed network firewall and intrusion detection and prevention service for your Oracle Cloud Infrastructure VCN, powered by Palo Alto Networks®.

- Overview
- OCI Network Firewall

4.3.2 OCI Load Balancer

The Load Balancer service provides automated traffic distribution from one entry point to multiple servers reachable from your virtual cloud network (VCN). The service offers a load balancer with your choice of a public or private IP address and provisioned bandwidth.

- Load Balancing
- Overview
- Concept Overview

4.3.3 OCI DNS Traffic Management

Traffic Management helps you guide traffic to endpoints based on various conditions, including endpoint health and the geographic origins of DNS requests.

- Concept Overview
- DNS

4.3.4 OCI WAF

Protect applications from malicious and unwanted internet traffic with a cloud-based, PCI-compliant, global web application firewall service.

- Cloud Security Web Application Firewall
- Add WAF to a load balancer

4.3.5 OCI IGW

An internet gateway is an optional virtual router that connects the edge of the VCN with the internet. To use the gateway, the hosts on both ends of the connection must have public IP addresses for routing

- Managing IGW

4.3.6 OCI Site-to-Site VPN

Site-to-site VPN provides a site-to-site IPSec connection between your on-premises network and your virtual cloud network (VCN). The IPSec protocol suite encrypts IP traffic before the packets are transferred from the source to the destination and decrypts the traffic when it arrives. Site-to-Site VPN was previously referred to as VPN Connect and IPSec VPN.

- Overview IPSec
- Setup IPSec

4.3.7 OCI Fast Connect

FastConnect allows customers to connect directly to their Oracle Cloud Infrastructure (OCI) virtual cloud network via dedicated, private, high-bandwidth connections.

- FastConnect
- Concept Overview

4.3.8 OCI VTAP

A Virtual Test Access Point (VTAP) provides a way to mirror traffic from a designated source to a selected target to facilitate troubleshooting, security analysis, and data monitoring

- VTAP
- Network VTAP Wireshark

4.3.9 OCI NPA

Network Path Analyzer (NPA) provides a unified and intuitive capability you can use to identify virtual network configuration issues that impact connectivity. NPA collects and analyzes the network configuration to determine how the paths between the source and the destination function or fail.

- Path Analyzer

4.3.10 OCI DRG (Connectivity Options)

A DRG acts as a virtual router, providing a path for traffic between your on-premises networks and VCNs, and can also be used to route traffic between VCNs. Using different types of attachments, custom network topologies can be constructed using components in different regions and tenancies.

- Managing DRGs
- OCI Pilot Light DR
- Peering VCNs in different regions through a DRG

4.3.11 OCI Oracle Cloud Infrastructure Certificates

Easily create, deploy, and manage Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates available in Oracle Cloud. In a flexible Certificate Authority (CA) hierarchy, Oracle Cloud Infrastructure Certificates help create private CAs to provide granular security controls for each CA.

- SSL TLS Certificates

4.3.12 OCI Monitoring

You can monitor the health, capacity, and performance of your Oracle Cloud Infrastructure resources by using metrics, alarms, and notifications. For more information, see Monitoring and Notifications.

- Networking Metrics

4.4 Manageability

OCI offers a full set of services to cover all Observability and Monitoring requirements.

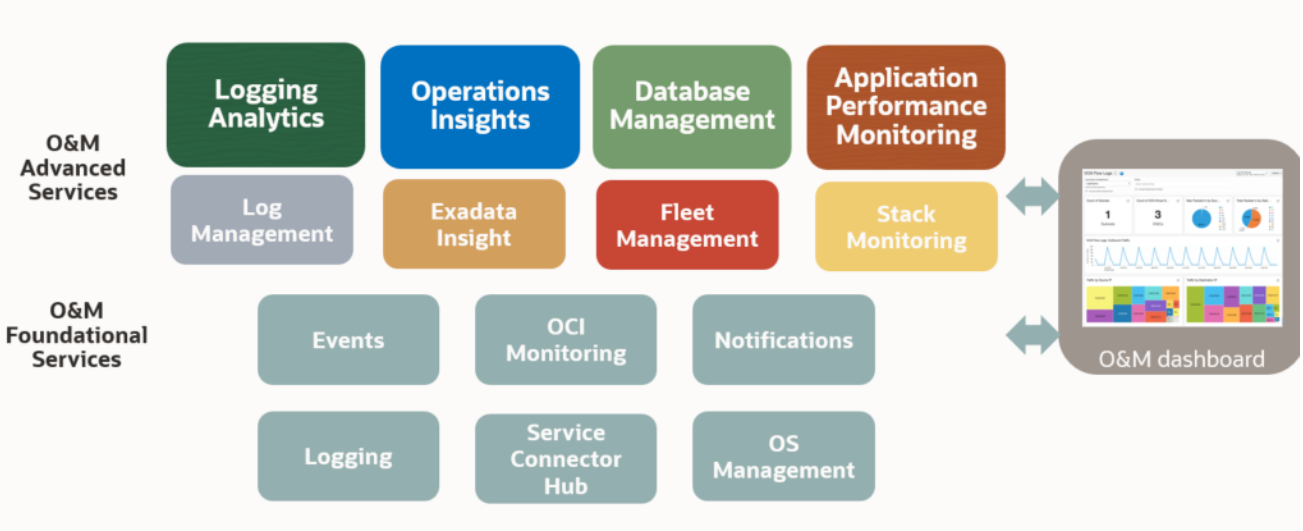


Figure 14: OCI Observability

Thanks to AI algorithms the OCI O&M (Observability and Management) solutions offer valuable insights into system status, requirements, and trends. Furthermore, it identifies SQL performance issues. This proactive approach empowers proactive measures to prevent future issues.

4.4.1 OCI O&M Services List

The observability and management services include the following services:

Application Performance Monitoring offers in-depth insight into application performance and facilitates rapid diagnostics to ensure a reliable level of service. This includes monitoring various components and application logic spread across clients, third-party services, and backend computing tiers, whether on-premises or in the cloud.

Database Management provides comprehensive database performance diagnostics and management capabilities to monitor and manage Oracle databases.

Logging lets you enable, view, and manage all the logs in your tenancy and provides access to logs from Oracle Cloud Infrastructure resources. These logs include critical diagnostic information that describes how resources are performing and being accessed.

Logging Analytics is a unified, integrated cloud solution that enables users to monitor, aggregate, index, analyze, search, explore, and correlate all log data from their applications and system infrastructure.

OCI Monitoring enables you to query metrics and manage alarms. Metrics and alarms help monitor the health, capacity, and performance of your cloud resources.

Ops Insights provides a 360-degree insight into the resource utilization and capacity of Oracle Autonomous Databases. You can easily analyze CPU and storage resources, forecast capacity issues, and proactively identify SQL performance issues across a fleet of Autonomous Databases.

Service Connector Hub is a cloud message bus platform that offers a single pane of glass for describing, running, and monitoring interactions for data moving between Oracle Cloud Infrastructure services.

Stack Monitoring enables proactive monitoring of applications and their underlying stack, including application servers and databases. By discovering all components of an application, including the application topology, Stack Monitoring automatically collects status, load, response, error, and utilization metrics for all application components. Each component of the application stack is referred to as a resource.

4.4.2 Real-Time Monitoring Annex

Service/Product Name	Description	Collateral
Monitoring	OCI Monitoring collects PaaS and IaaS OCI services metrics. It is enabled by default for all the OCI services.	List of metrics collected by default
OCI Application Performance Monitor	APM is a Distributed Tracing System as a Service. It enables DevOps teams to follow every step of every task. It uses open standards such as OpenTelemetry to monitor various programming languages. Plus, it includes a dedicated Java agent to track older J2EE applications, ensuring complete transaction tracing even in mixed environments.	OCI Application Performance Monitoring
OCI Console	The Service Console offers a list of visual representations and basic information about critical metrics like CPU, memory, and storage.	OCI Console Resource Usage Tracking
OCI Database Management (opt to OEM)	It is an OCI-managed service that simplifies database operations and enhances efficiency. It offers advanced monitoring and diagnostic capabilities, enabling proactive management and optimization of database performance.	List of metrics collected by OCI Database Management
Stack Monitoring	Stack Monitoring lets you proactively monitor an application and its underlying application stack, including application servers and databases.	Stack Monitoring for Oracle Database
Third-Party Tools - Service Connector Hub	OCI provides complete O&M capabilities. However, for customers who prefer to use their own tools, OCI allows seamless integration through the Service Connect Hub.	OCI Connector Hub Third-Party Tools Use Cases

4.4.3 Performance and Tuning Annex

Service/Product Name	Description	Collateral
OCI Logging	The OCI Logging service is a highly scalable and fully managed single pane of glass for all the logs in your tenancy. Logging provides access to logs from Oracle Cloud Infrastructure resources. These logs include critical diagnostic information that describes how resources are performing and being accessed.	OCI Logging
OCI Monitoring	Use the Oracle Cloud Infrastructure Monitoring service to actively and passively monitor cloud resources using the Metrics and Alarms features. Metric data posted to the Monitoring service is only presented to you or consumed by the Oracle Cloud Infrastructure features that you enable to use metric data.	OCI Monitoring
OCI Dashboard	The Console Dashboards service allows you to create custom dashboards in the Oracle Cloud Infrastructure Console to monitor resources, diagnostics, and key metrics for your tenancy.	OCI Dashboard
OCI Logging Analytics	OCI Logging Analytics empowers users to analyze log data from diverse sources across their infrastructure. It provides insights into system performance, identifies trends, and enables proactive resource optimization by correlating data from multiple layers of the infrastructure.	OCI Logging Analytics
OCI Application Performance Monitor	APM allows to drill down from user sessions till the single DB query or external call to identify performance bottleneck.	OCI Application Performance Monitoring
OCI Database Management - PerfHub	Is an OCI-managed service that offers performance and tuning capabilities. It provides the same performance and tuning features as the Oracle Enterprise Manager (OEM) Performance and Tuning Pack but in a managed solution.	Database Management Performance Hub
Ops Insights Sql Warehouse and Capacity Planning	OCI Ops Insights allows for the tracking of metrics charts and data collection. It allows for the correlation of resources across various infrastructure layers. Additionally, it predicts high resource utilization for computing and database instances.	OCI Operations Insight SQL Warehouse OCI Operations Insight Capacity planning

4.4.4 Administration Annex

Service/Product Name	Description	Collateral
OCI Console	The OCI Console is embedded in all cloud services. It allows basic tasks such as listing, starting, stopping, or termination of ressources.	OCI Console
OCI Database Management	This OCI-managed service allows you to manage your databases. It provides a subset of functionalities offered by the OEM.	Database Management
OCI Organization Management	The OCI Console has several tenancy management features. You can use Organization Management to centrally manage your multi-tenancy environment.	Organization Management

4.4.5 Troubleshooting Annex

Service/Product Name	Description	Collateral
Logging Analytics	OCI Logging Analytics can handle log events generated by all software applications and infrastructure on the cloud or on-premises. For Oracle software logs, a predefined severity pre-classification exists based on Oracle experience.	OCI Logging Analytics OCI Logging Analytics for Exa
OCI Application Performance Monitor	APM allows to drill down from user sessions till the application logs to find the root cause.	OCI Application Performance Monitoring
OCI Database Management	OCI-managed service that allows you to drill down and correlate metrics and data from different layers. it provides built-in links that allow you to connect to other O&M services (ex. Ops Insights).	Database Management
Ops Insights	OCI Ops Insights allows tracking of metrics charts and data collection. It allows for the correlation of resources from different infrastructure layers.	OCI Operations Insight OCI ExaInsight

4.4.6 Cost Control and Chargeback Annex

Service/Product Name	Description	Collateral
Ops Insights Capacity Planning	This OCI-managed service allows one to predict the resource consumption for a year. With tags, you can associate the forecast and the consumption to a specific department.	Operations Insight Capacity Planning
Cost Analysis	Cost Analysis is an easy-to-use visualization tool to help you track and optimize your Oracle Cloud Infrastructure spending. It allows for the generation of charts and the download of accurate and reliable tabular reports of aggregated cost data. With tags, you can associate the forecast and the consumption to a specific department.	OCI Cost Analysis
Usage RestAPI	OCI offers various RestAPI's to manage services, including the one for cost management.	OCI Usage RestAPI