

Solution Definition

Copyright © 2023, Oracle and/or its affiliates

ACME

JDE Migration to OCI

6th of May 2024 | Version 2.5

Contents

[Document Control 5](#_Toc165894099)

[1.1 Version Control 5](#_Toc165894100)

[1.2 Team 5](#_Toc165894101)

[1.3 Document Purpose 5](#_Toc165894102)

[Business Context 6](#_Toc165894103)

[2.1 Executive Summary 6](#_Toc165894104)

[2.2 Workload Business Value 6](#_Toc165894105)

[Workload Requirements and Architecture 7](#_Toc165894106)

[3.1 Overview 7](#_Toc165894107)

[3.2 Non-Functional Requirements 7](#_Toc165894108)

[3.2.1 Regulations and Compliances Requirements 8](#_Toc165894109)

[3.2.2 Environments 8](#_Toc165894110)

[3.2.3 High Availability and Disaster Recovery Requirements 10](#_Toc165894111)

[3.2.4 Security Requirements 10](#_Toc165894112)

[3.2.5 Networking Requirements 11](#_Toc165894113)

[3.2.6 Management and Monitoring 11](#_Toc165894114)

[3.3 Future State Architecture 12](#_Toc165894115)

[3.3.1 Mandatory Security Best Practices 12](#_Toc165894116)

[3.3.2 Naming Conventions 13](#_Toc165894117)

[3.3.3 OCI Landing Zone Solution Definition 14](#_Toc165894118)

[3.3.4 Logical Architecture 14](#_Toc165894119)

[3.3.5 Physical Architecture 14](#_Toc165894120)

[3.4 Solution Considerations 22](#_Toc165894121)

[3.4.1 High Availability and Disaster Recovery 22](#_Toc165894122)

[3.4.2 Security 23](#_Toc165894123)

[3.4.3 Networking 24](#_Toc165894124)

[3.4.4 Manageability and Observability 24](#_Toc165894125)

[3.5 Sizing and Bill of Materials 27](#_Toc165894126)

[Project Implementation (Only for Oracle Implementations!) 29](#_Toc165894127)

[4.1 Solution Scope 29](#_Toc165894128)

[4.1.1 Disclaimer 29](#_Toc165894129)

[4.1.2 Overview 29](#_Toc165894130)

[4.1.3 Business Value 29](#_Toc165894131)

[4.1.4 Success Criteria 30](#_Toc165894132)

[4.2 Workplan 30](#_Toc165894133)

[4.2.1 Deliverables 30](#_Toc165894134)

[4.2.2 Included Activities 30](#_Toc165894135)

[4.2.3 Recommended Activities 31](#_Toc165894136)

[4.2.4 Timeline 32](#_Toc165894137)

[4.2.5 Implementation RACI 32](#_Toc165894138)

[4.2.6 Assumptions 33](#_Toc165894139)

[4.2.7 Obligations 34](#_Toc165894140)

[4.2.8 Transition Plan 34](#_Toc165894141)

[Annex 36](#_Toc165894142)

[5.1 Security Guidelines 36](#_Toc165894143)

[5.1.1 Oracle Security, Identity, and Compliance 36](#_Toc165894144)

[5.1.2 Compliance and Regulations 36](#_Toc165894145)

[5.1.3 Additional Resources 36](#_Toc165894146)

[5.2 Networking Requirement Considerations 36](#_Toc165894147)

[5.2.1 Application Connectivity 37](#_Toc165894148)

[5.2.2 DR and Business Continuity 37](#_Toc165894149)

[5.2.3 High Availability and Scalability 37](#_Toc165894150)

[5.2.4 Security and Access Control 37](#_Toc165894151)

[5.2.5 Monitoring and Troubleshooting 37](#_Toc165894152)

[5.3 Networking Solutions 37](#_Toc165894153)

[5.3.1 OCI Network Firewall 37](#_Toc165894154)

[5.3.2 OCI Load Balancer 38](#_Toc165894155)

[5.3.3 OCI DNS Traffic Management 38](#_Toc165894156)

[5.3.4 OCI WAF 38](#_Toc165894157)

[5.3.5 OCI IGW 38](#_Toc165894158)

[5.3.6 OCI Site-to-Site VPN 38](#_Toc165894159)

[5.3.7 OCI Fast Connect 38](#_Toc165894160)

[5.3.8 OCI VTAP 39](#_Toc165894161)

[5.3.9 OCI NPA 39](#_Toc165894162)

[5.3.10 OCI DRG (Connectivity Options) 39](#_Toc165894163)

[5.3.11 OCI Oracle Cloud Infrastructure Certificates 39](#_Toc165894164)

[5.3.12 OCI Monitoring 39](#_Toc165894165)

[5.4 Manageability 39](#_Toc165894166)

[5.4.1 OCI O&M Services List 40](#_Toc165894167)

[5.4.2 Real-Time Monitoring Annex 41](#_Toc165894168)

[5.4.3 Performance and Tuning Annex 41](#_Toc165894169)

[5.4.4 Administration Annex 42](#_Toc165894170)

[5.4.5 Troubleshooting Annex 42](#_Toc165894171)

[5.4.6 Cost Control and Chargeback Annex 42](#_Toc165894172)

*Guide:*

*Author Responsibility*

* *Chapter 1-3: Sales Consultant*
* *Chapter 4: Implementer*

# Document Control

*Guide:*

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

## Version Control

*Guide:*

*A section describing the versions of this document and its changes.*

*Example:*

| Version | Author | Date | Comment |
| --- | --- | --- | --- |
| 0.1  2.1  2.5 | Bart Eygenraam  Manish Palaparthy  Manish Palaparthy | July, 2023  October, 2023  May, 2024 | Initial Draft Sol Def V0.1  Updated the document to be in line with version 2.1 template  Updated the document to be in line with version 2.5 template |
|  |  |  |  |

## Team

*Guide:*

*A section describing the Oracle team.*

*Example:*

| Name | Email | Role | Company |
| --- | --- | --- | --- |
| Name Surname | name@example.com | Solution Architect | example |
| Name Surname | name@lexample.com | Account Cloud Engineer | example |

## 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, current state requirements, and to-be state.

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](#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 that 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?*

## 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)

## Workload Business Value

*Guide:*

*A section describing the business value of the Application on OCI*

*Example:*

Organizations use on-premises deployments of JD Edwards ( JDE) for a wide range of functionalities, including Financial Management, Order Management, Project Management, Agribusiness, Supply Magement, Manufacturing, Logistics etc. 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 JD Edwards.

Most On-Premises JDE deployments can be migrated to run on 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 JDE 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
* Maximize 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). JDE 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 JDE 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. Additional JDE Database can also run on Aotonomous, both Shared as Dedicated Autonomous Database System.

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 the speed of deployment resulting in a successful project without any setbacks; thus bringing value to the overall project provisioning for the Application workload.

# Workload Requirements and Architecture

## Overview

*Guide:*

*A section describing the Current JDE 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 multiple 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*](#scope)*.*

*Example Architecture for Deploying JD Edwards EnterpriseOne in a Single Region:*

One can deploy JD Edwards EnterpriseOne in a single availability domain while ensuring high availability.

You can achieve high availability by placing the application instances inside multiple fault domains. Use this architecture when you want to ensure that your application is available even when an application instance goes down in one fault domain. The other available application instances inside the other fault domain continue to process the requests. You can deploy JD Edwards EnterpriseOne manually or by using the JD Edwards EnterpriseOne automation tools on Oracle Cloud Infrastructure.

The referenced architecture shows that redundant instances are deployed in the presentation tier and middle tier in an availability domain to ensure high availability within the availability domain. All instances in the availability domain are active. This high availability of an application within an availability domain can be achieved by placing application instances in separate fault domains. Fault domains let you distribute your instances so that they are not on the same physical hardware within a single availability domain. A hardware failure or Oracle Cloud Infrastructure Compute hardware maintenance that affects one fault domain does not affect instances in other fault domains. If an instance fails, then the traffic is diverted to other instances in the availability domain that continue to process the requests. However, if your connection to the availability domain fails or the entire availability domain goes down, then the instances are not available to process the requests.

The referenced architecture consists of a virtual cloud network (VCN) with the bastion host, load balancer tier, presentation tier, middle tier, administration tier, and database tier. The tiers are placed in a single subnet of the VCN in a single availability domain.

In the referenced architecture diagram, the bastion host is deployed in a public subnet, and all the other instances are placed in private subnets. Depending on your business requirements, you can place instances in public or private subnets. You can access the instances that are in private subnets over port 22 through the bastion host or the dynamic routing gateway (DRG). To enable communication between the DRG and the customer on-premises equipment, use IPSec VPN or Oracle Cloud Infrastructure FastConnect.

The Server Manager in the Administration tier communicates with Presentation tier, Middle tier, and Database tier to provide code deployment, configuration management, runtime metrics access, and log access. The Deployment Server in the Administration tier communicates with the Middle tier and the Database tier to build and deploy code. The Development Client communicates with the Middle tier and the Database tier. Application Development Framework (ADF) and Oracle Business Intelligence Publisher communicate with the HTML server in the Presentation tier.

## 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.*

### 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](https://www.cisecurity.org/benchmark/Oracle_Cloud) will be applied to the Customer tenancy.

### Environments

*Guide:*

*A section describing the Current JD Edwards workload of a Customer Example Environment details*

*Example:*

**Bastion host:** The bastion host is an optional component that can be used as a jump server to access instances in the private subnet. A bastion host is an Oracle Cloud Infrastructure Compute instance that uses Linux as its operating system. Place the bastion host in a public subnet and assign it a public IP address to access it from the Internet.

To provide an additional level of security, you can set up security lists to access the bastion host only from the public IP address of your on-premises network. You can access Oracle Cloud Infrastructure instances in the private subnet through the bastion host. To do this, enable ssh-agent forwarding, which allows you to connect to the bastion host, and then access the next server by forwarding the credentials from your computer. You can also access the instances in the private subnet by using dynamic SSH tunneling. SSH tunneling is a way to access a web application or other listening service. The dynamic tunnel provides a SOCKS proxy on the local port, but the connections originate from the remote host.

**Load Balancer tier:** The load balancer tier contains the Oracle Cloud Infrastructure Load Balancing instances that load balances the traffic to all instances in the presentation tier. The load balancer receives requests from users, and then routes these requests to instances in the presentation tier.

Use Oracle Cloud Infrastructure Load Balancing to distribute traffic to your application instances within a VCN. This service provides a primary and a standby instance of the load balancer to ensure that if the primary load balancer becomes unavailable, the standby load balancer forwards the requests. The load balancer ensures that requests are routed to the healthy application instances. If a problem occurs within an application instance, then the load balancer will route requests to the remaining healthy application instances. Based on your requirements, you can place load balancers in a public or private subnet.

For internal endpoints, that aren’t accessible from the Internet, use a private load balancer. A private load balancer has a private IP address, and it isn’t accessible from the Internet. Both the primary and the standby instances of a load balancer reside in the same private subnet. You can access private load balancers in the VCN or in your data center over the IPSec VPN through a DRG. The private load balancer accepts traffic from your data center, and distributes the traffic to underlying application instances.

For Internet-facing endpoints, use a public load balancer. A public load balancer has a public IP address, and it’s accessible from the Internet. You can access the public load balancers from the Internet through the Internet gateway.

For accessing internal endpoints and Internet-facing endpoints, set up private load balancers and public load balancers. Set up private load balancers to serve the internal traffic, and set up public load balancers to serve the traffic from the Internet.

Register the public or private IP address of Oracle Cloud Infrastructure Load Balancing instances in your on-premises or public domain name server (DNS) for domain resolution of your application endpoint.

The ports provided in the architecture diagram are only an example. You can use any port that’s available.

**Administration tier:** The administration tier contains a single instance of the following servers. You don’t require a redundant instance of these servers to ensure high availability.

**Provisioning server:** Use this server to automate end-to-end deployment of JD Edwards EnterpriseOne components on Oracle Cloud Infrastructure. It communicates with all the instances in the other tiers, including the instances in the database tier, over port 22. It hosts the JD Edwards EnterpriseOne One-Click Provisioning Console and JD Edwards EnterpriseOne Server Manager Console.

**Deployment Server:** During the installation process, this server acts as the central repository of all the required files and installation packages. The software is distributed or deployed to all other servers and clients from this server.

**Development client:** The JD Edwards EnterpriseOne Development client contains components that run as standard Microsoft Windows applications (for example, Active Console, Forms Design Aid (FDA), and Report Design Aid (RDA)) and components that run in a web browser.

**Application Development Framework (ADF) server:** JD Edwards EnterpriseOne ADF server is a web application that is deployed on an Oracle WebLogic server with ADF runtime. It is used to run JD Edwards EnterpriseOne applications developed with Oracle ADF. Oracle Business Intelligence Publisher: Oracle Business Intelligence Publisher presents the data collected by JD Edwards EnterpriseOne in the form of reports. Use Oracle Business Intelligence Publisher to present reports using different templates based on your business requirements. You can design and control how the report outputs are presented by using template files.

**Presentation tier:** The presentation tier contains redundant instances of Application Interface Services and Java Application Servers to provide high availability. These servers communicate with servers in the middle tier. All instances are active and they receive traffic from the load balancer. Each instance is associated with a block storage volume. This tier also contains components that you can use to create integration between JD Edwards EnterpriseOne and an external system. Your implementation can include one or more of these components.

This tier contains the following servers:

**Application Interface Services (AIS) Server:** Application Interface Service server provides the communication interface between JD Edwards EnterpriseOne mobile enterprise applications and JD Edwards EnterpriseOne.

**Standard Java Application Servers (Standard JAS):** It receives requests from the load balancer and executes simple business logic. For tasks that require complicated business logic, Standard JAS passes the requests to the logic server. It also passes requests to the AIS server in some cases. However, it's not configured with the AIS server for the AIS runtime. Dedicated Java Application Servers (Dedicated JAS): It receives requests from the AIS Server. It passes requests to the logic server to execute tasks that require complicated business logic. It is configured with the AIS server for the AIS runtime.

To ensure high availability within an availability domain, deploy redundant instances of every component. All instances are active and they receive traffic from the load balancer and middle tier.

**Middle Tier:** The middle tier contains logic servers and batch servers. They are not directly load balanced but they have one-to-one mapping with servers in presentation tier. You can host the logic server and the batch server on the same enterprise server instance. However, it is recommended that you set up the logic server and the batch server on separate enterprise server instances.

The middle tier receives requests from the presentation tier. After processing the requests, it forwards the requests to the database servers. All instances of the servers are active and process requests.

This tier contains the following servers:

Logic servers or enterprise servers: These servers contain the business logic or business functions.

Batch servers: These servers are used for batch processing.

**Database tier:** The database tier contains JD Edwards EnterpriseOne database server instances. For high availability requirements, Oracle recommends that you use two-node, Oracle Real Application Clusters (Oracle RAC) database systems or an Oracle Database Exadata Cloud Service system in Oracle Cloud Infrastructure to set up JD Edwards EnterpriseOne database server instances.

You can set up redundant database instances to provide high availability. For Oracle RAC and Oracle Database Exadata Cloud Service database systems, requests that are received from the application subnet are load balanced across the database servers. If one database instance becomes unavailable, the other database instance processes the requests. You can use Oracle Cloud Infrastructure Object Storage to back up the JD Edwards EnterpriseOne database by using Oracle Recovery Manager (RMAN). To back up or patch the JD Edwards EnterpriseOne database to Oracle Cloud Infrastructure Object Storage, the DB system's VCN must be configured with either a service gateway or an Internet gateway. It is recommended that you use a service gateway rather than an Internet gateway for backup and patching.

Use security lists to restrict access to the database servers only from the bastion host, application tier, and on-premises servers. You can set up security lists to ensure that communication occurs only over port 22, through the bastion host, and over port 1521. Also ensure that the database systems can’t be accessed over the Internet.

### 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.

### 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.

### Networking Requirements

*Guide*

*Capture the Non-Functional Requirements for networking-related topics. You can use the networking questions in the* [*Annex*](#networking-requirement-considerations)

*Example:*

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

### Management and Monitoring

*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 |  |

## 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.*

### Mandatory Security Best Practices

*Guide:*

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

*Example:*

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

<Customer Name> 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](https://docs.oracle.com/en-us/iaas/Content/Identity/mfa/understand-multi-factor-authentication.htm).   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](https://docs.oracle.com/en-us/iaas/Content/Identity/adaptivesecurity/overview.htm). |
|  | 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](https://docs.oracle.com/en-us/iaas/Content/cloud-adoption-framework/iam-security-structure.htm). |
| 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](https://docs.oracle.com/en-us/iaas/cloud-guard/using/part-start.htm). 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](https://docs.oracle.com/en-us/iaas/cloud-guard/using/part-customize.htm) |
|  | 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](https://docs.oracle.com/en-us/iaas/scanning/home.htm). |
| Monitoring | SIEM Integration | Continuous monitoring of OCI resources is key for maintaining the required security level (see [Regulations and Compliance](#regulations-and-compliances-requirements) for specific requirements). See [Design Guidance for SIEM Integration](https://docs.oracle.com/en-us/iaas/Content/cloud-adoption-framework/siem-integration.htm) 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](https://docs.oracle.com/en-us/iaas/Content/Billing/Tasks/managingbudgets.htm) |

### 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*](https://github.com/oracle-devrel/technology-engineering/tree/main/landing-zones)*. 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](https://github.com/oracle-devrel/technology-engineering/blob/main/landing-zones/commons/resource_naming_conventions.md) Oracle's recommended best practices.

### 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*](https://github.com/oracle-devrel/technology-engineering/tree/main/landing-zones)*. 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 two operations.

Oracle highly recommends the use of an OCI Landing Zone for any deployment. Use these [guidelines](https://github.com/oracle-devrel/technology-engineering/blob/main/landing-zones/commons/lz_solution_definition.md) 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.

### Logical Architecture

*Guide:*

*Provide a high-level logical Oracle solution for the complete Workload. Indicate Oracle products as abstract groups, and not as physical detailed instances. Create an architecture diagram following the latest notation and describe the solution.*

*To implement a solution the Physical Architecture is needed in the next chapter. The physical notation can show individual components with physical attributes such as IP addresses, hostnames, or sizes.*

[*The Oracle Cloud Notation, OCI Architecture Diagram Toolkits*](https://docs.oracle.com/en-us/iaas/Content/General/Reference/graphicsfordiagrams.htm)

### Physical Architecture

*Guide:*

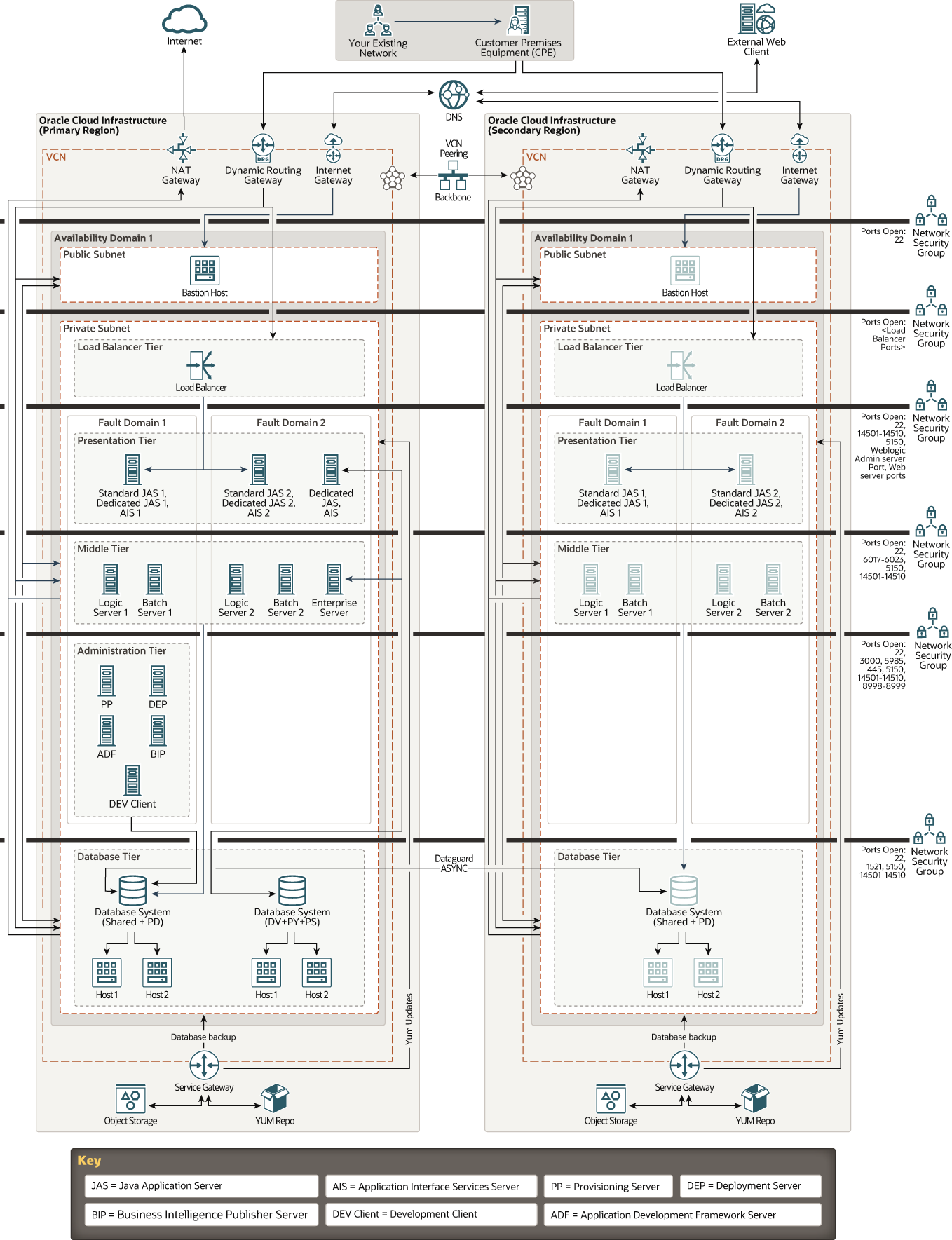
*A section describing the Deployment Design and its associated Components in OCI*

*Example:*

The Tenancy of Customer will be managed by 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).

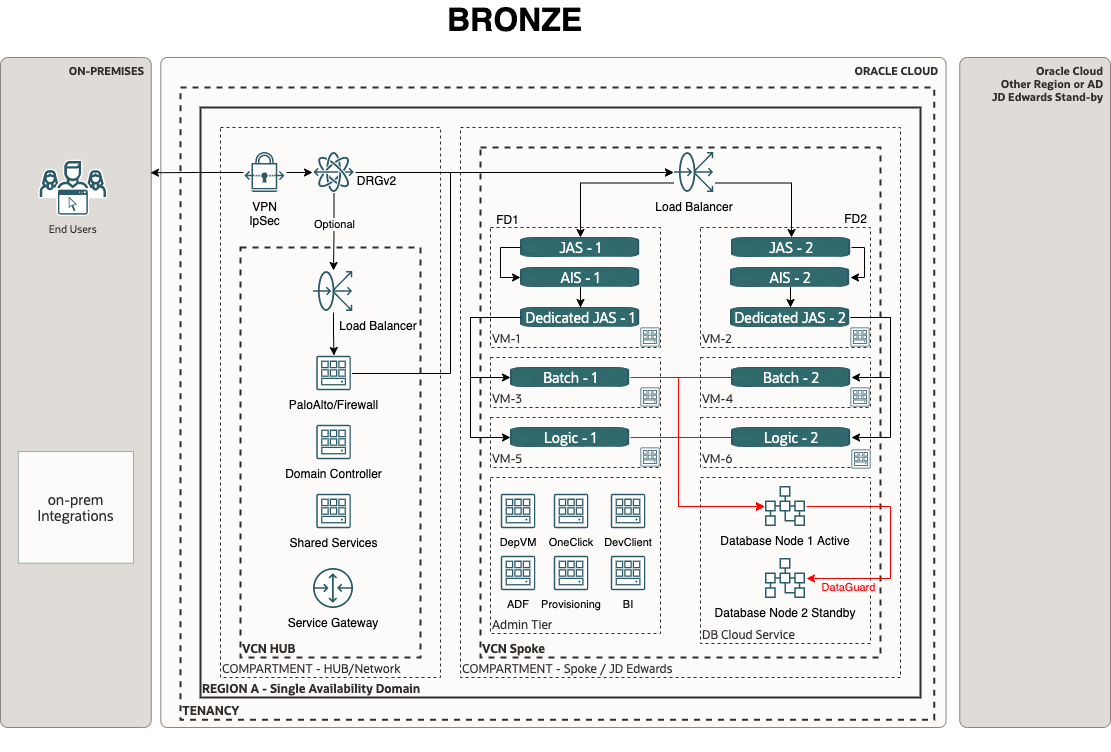
In the **following sections** we are describing the **Deployment Design Diagrams** as well as all the relevant components present in the Design diagram.\*

Deployment architecture for the 'JDE-X' environment of the Customers JD Edwards Workload, in OCI - Multi AD DR design diagram, is illustrated below:



Future State Deployment Diagram - JD Edwards Workload Multi-AD, DR Design Diagram

Deployment architecture for the 'JDE-X' environment of the Customers JD Edwards Workload, in OCI - Max Availability Architecture, Single AD design diagram, with Standby Database Node, BRONZE, is illustrated below:



Future State Deployment Diagram - JD Edwards Workload - MAA - Single AD, Bronze

Deployment architecture for the 'JDE-X' environment of the Customers JD Edwards Workload, in OCI - Max Availability Architecture, Single AD design diagram, with RAC enabled Database Nodes, SILVER, is illustrated below:



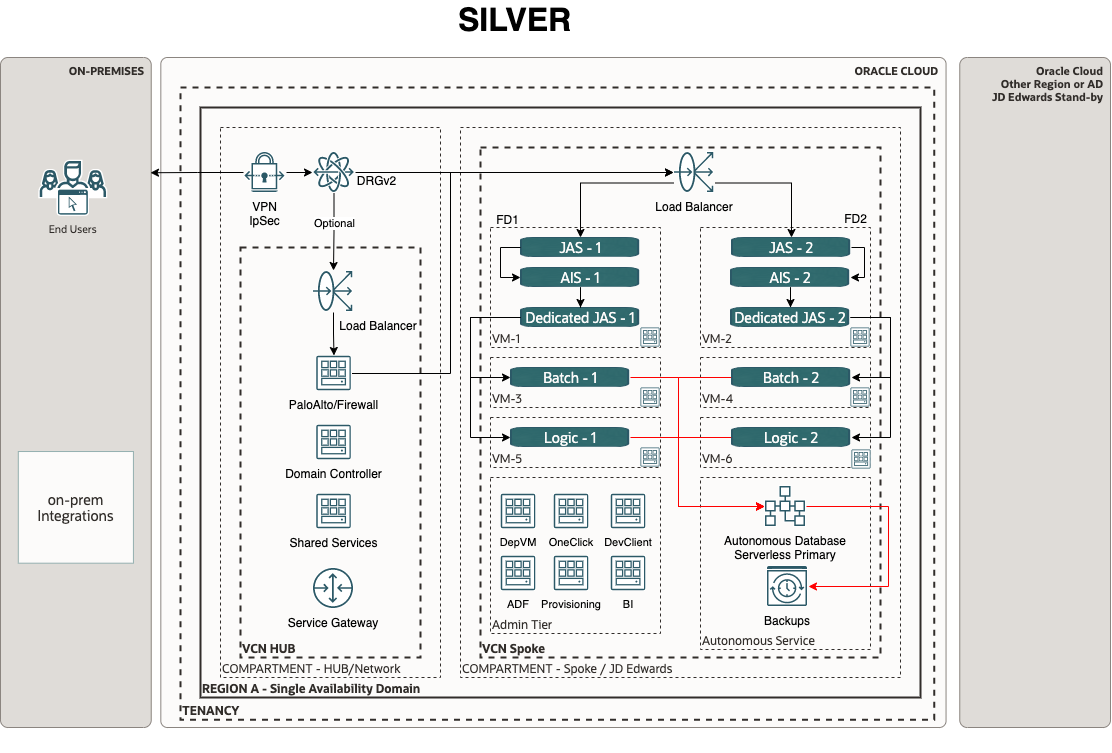
Future State Deployment Diagram - JD Edwards Workload - MAA - Single AD, Silver

Deployment architecture for the 'JDE-X' environment of the Customers JD Edwards Workload, in OCI - Max Availability Architecture, Multy AD design diagram, with RAC enabled Database Nodes, and remote Standby, GOLD, is illustrated below:

|  |
| --- |
|  |

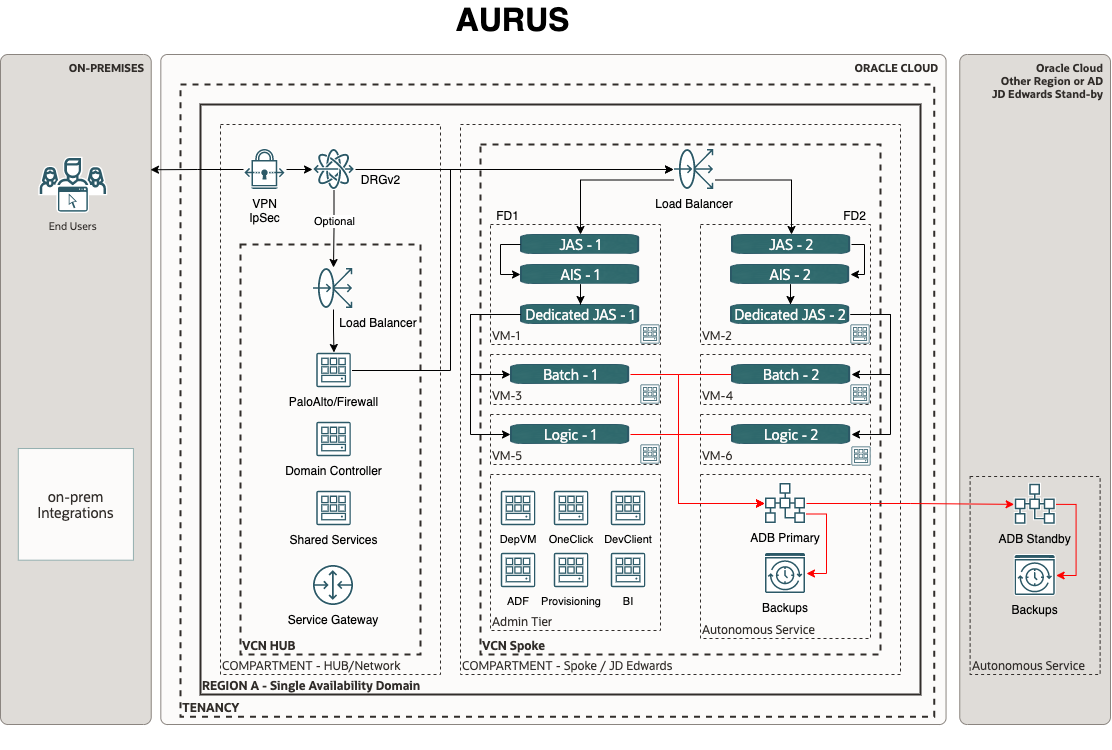
Future State Deployment Diagram - JD Edwards Workload - MAA - Single AD, Gold

Deployment architecture for the 'JDE-X' environment of the Customers JD Edwards Workload, in OCI - Max Availability Architecture - ADB , Single AD design diagram, with ADB Database Nodes, SILVER, is illustrated below:



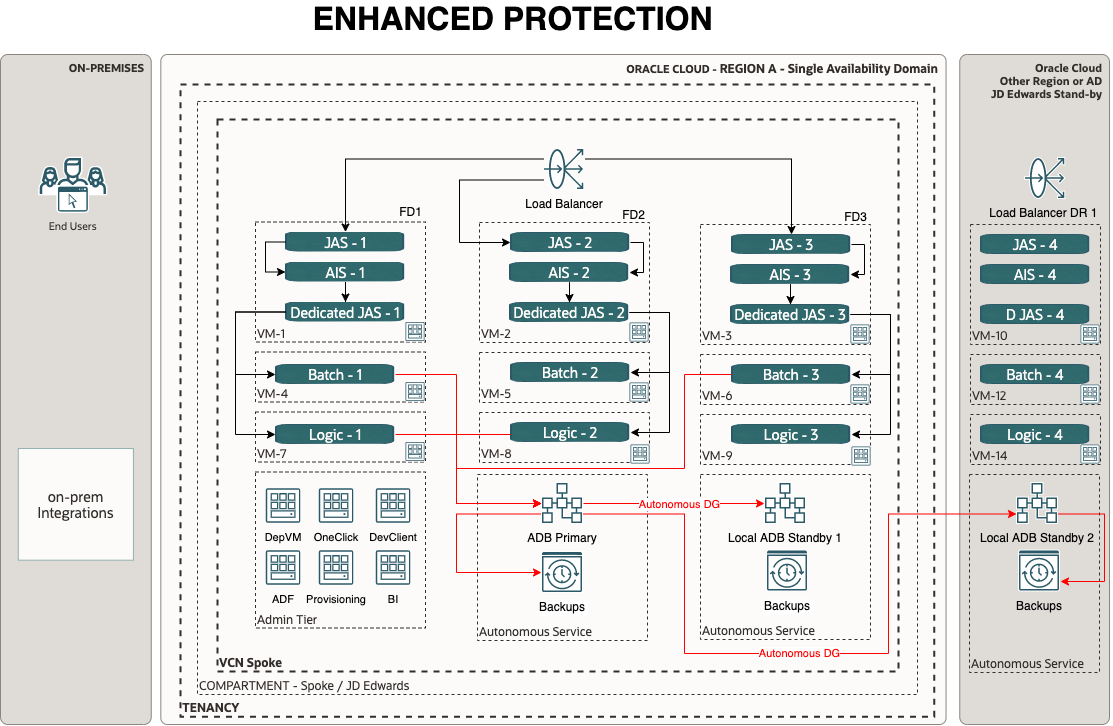
Future State Deployment Diagram - JD Edwards Workload - MAA - Single AD, Silver

Deployment architecture for the 'JDE-X' environment of the Customers JD Edwards Workload, in OCI - Max Availability Architecture - ADB, Single AD design diagram, with remote standby ADB Database Node, AURUS, is illustrated below:



Future State Deployment Diagram - JD Edwards Workload - MAA - Single AD, Aurus

Deployment architecture for the 'JDE-X' environment of the Customers JD Edwards Workload, in OCI - Max Availability Architecture - ADB, Single AD design diagram, with remote standby ADB Database Node and Apps nodes, Enhanced Protection diagram, is illustrated below:



Future State Deployment Diagram - JD Edwards Workload - MAA - Single AD, Enh. Prot.

*Reference:*

[*The Oracle Cloud Notation, OCI Architecture Diagram Toolkits*](https://docs.oracle.com/en-us/iaas/Content/General/Reference/graphicsfordiagrams.htm)

## Solution Considerations

*Guide:*

*A section describing the Future JD Edwards 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:*

The proposed plan is to migrate JDE Application servers 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 JD Edwards has a long-term roadmap to support the key capabilities of Oracle Autonomous Database that provide significant benefit to our customers. Oracle Autonomous Database is available through two deployment options: Dedicated Exadata Infrastructure and Shared Exadata Infrastructure. Oracle JD Edwards customers can leverage the capabilities of the Oracle Autonomous Database and reap significant benefits from it.

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.

### High Availability and Disaster Recovery

*Guide:*

*Please describe the Oracle MAA in the context of JDE.*

*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](http://www.oracle.com/goto/maa). To achieve maximum Oracle JKD Edwards database availability, Oracle recommends deploying JDE 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:*

[JD Edwards EnterpriseOne High Availability Architecture](https://www.oracle.com/webfolder/technetwork/tutorials/jdedwards/White%20Papers/HighAvailabilityArchitectureJDE_VER000FU.pdf)

### Security

*Guide:*

*A section describing the Security in OCI in the context of the JDE Application*

*Example:*

The objective of the security architecture is to enable you to maintain your security posture when running JDE 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 a hardware-based root of trust, making sure each server is pristine each and every time it is provisioned.

|  |
| --- |
| **Port and Protocol Requirement for JDE Workload** |

Port and Protocol Requirement for JDE Workload

**Note:** Please see generic OCI security guidelines in the [Annex](#security-guidelines).

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 travels between regions is either sent over private links or is 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 industries (Financial) might require PCI-compliant services like WAF
* Oracle JD Edwards requires policies with the following ports and protocols to be open

|  |
| --- |
| Port and Protocol Requirement for JDE Workload |

Port and Protocol Requirement for JDE Workload

**Note:\_\_**Please see generic OCI security guidelines in the [Annex](#security-guidelines).

### Networking

*Guide:*

*If your customers have any or one of the needs described in the guide of the* [*Network Requirements*](#networking-requirements)*, then the OCI Network Firewall (OCI NFW) is the cloud native solution that provides all of it. It is based on the industry-leading Nextgen firewall solution by Palo Alto (VM-Series). Refer to the Annex for more best practices around deployment models.*

*Reference:*

*A list of possible Oracle solutions can be found in the* [*Annex*](#networking-solutions)*.*

*Example:*

The OCI Network Firewall can be deployed as a Distributed Network Firewall Model or Transit Network Firewall Model, where the firewall is hosted in the Hub VCN. In general, the OCI Network Firewall can be used to protect North-South traffic (Internet traffic) and/or East-West traffic (internal traffic). As a best practice, we do recommend using one dedicated OCI Network Firewall instance per type of traffic (North-South and East-West) in separated VCNs. This way performance will be maximized as well as ensuring the network isolation between the types of traffic.

For more information please follow [this link.](https://docs.oracle.com/en/solutions/oci-network-firewall/index.html#GUID-875E911C-8D7D-4205-952B-5E8FAAD6C6D3)

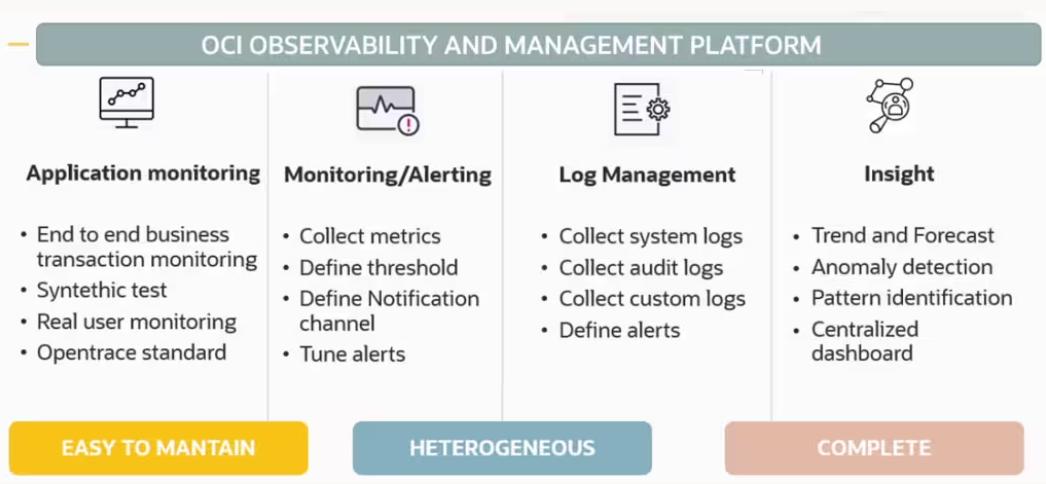
### Manageability and Observability

*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.

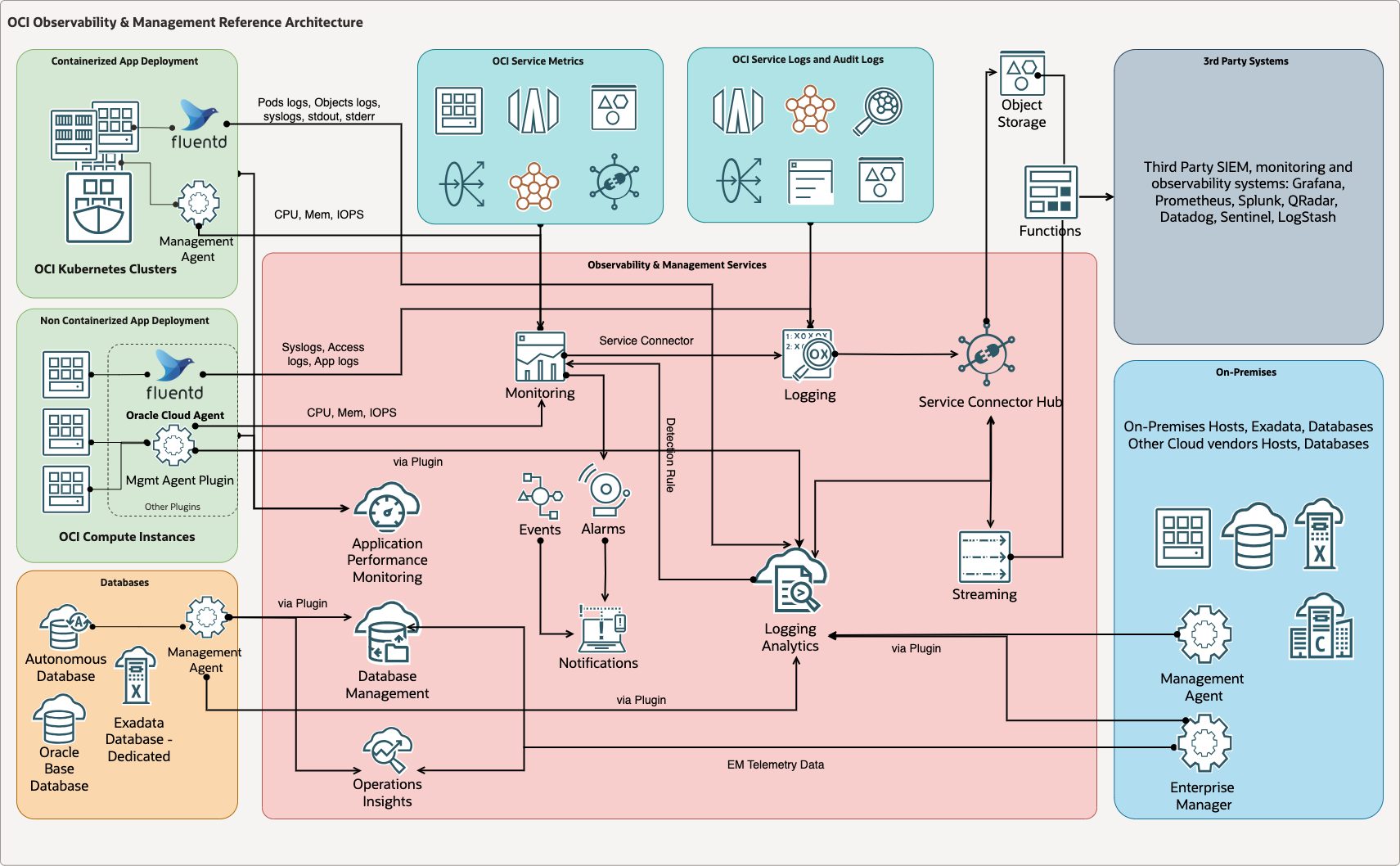


Observability and Manageability

#### 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.



OCI Architecture

#### 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](#real-time-monitoring-annex).

#### 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](#performance-and-tuning-annex).

#### 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](#administration-annex).

#### 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](#troubleshooting-annex).

#### 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](#cost-control-and-chargeback-annex).

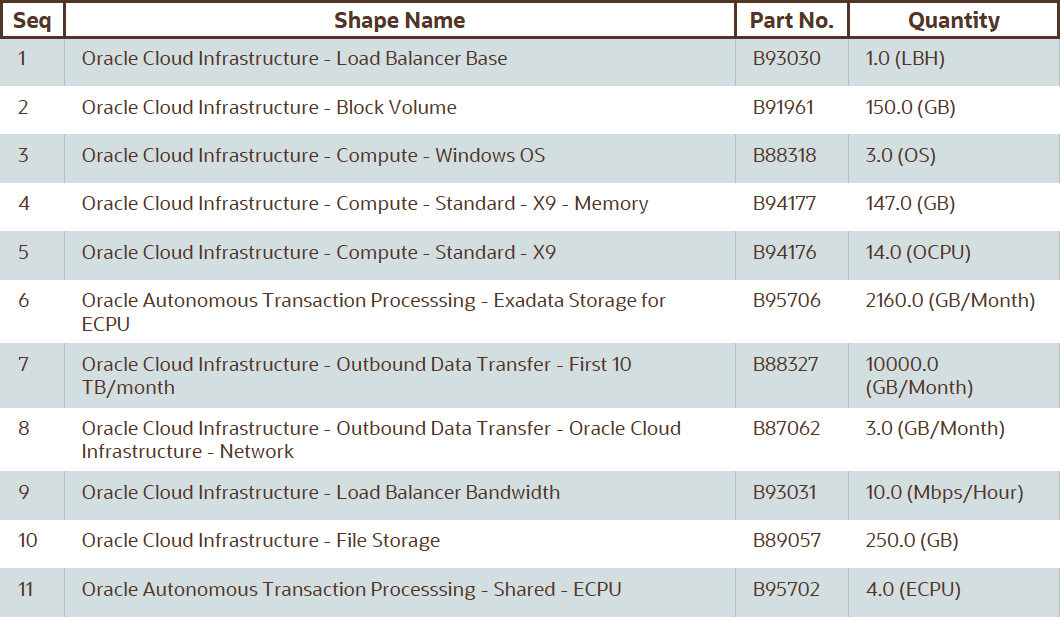
## Sizing and Bill of Materials

*Guide:*

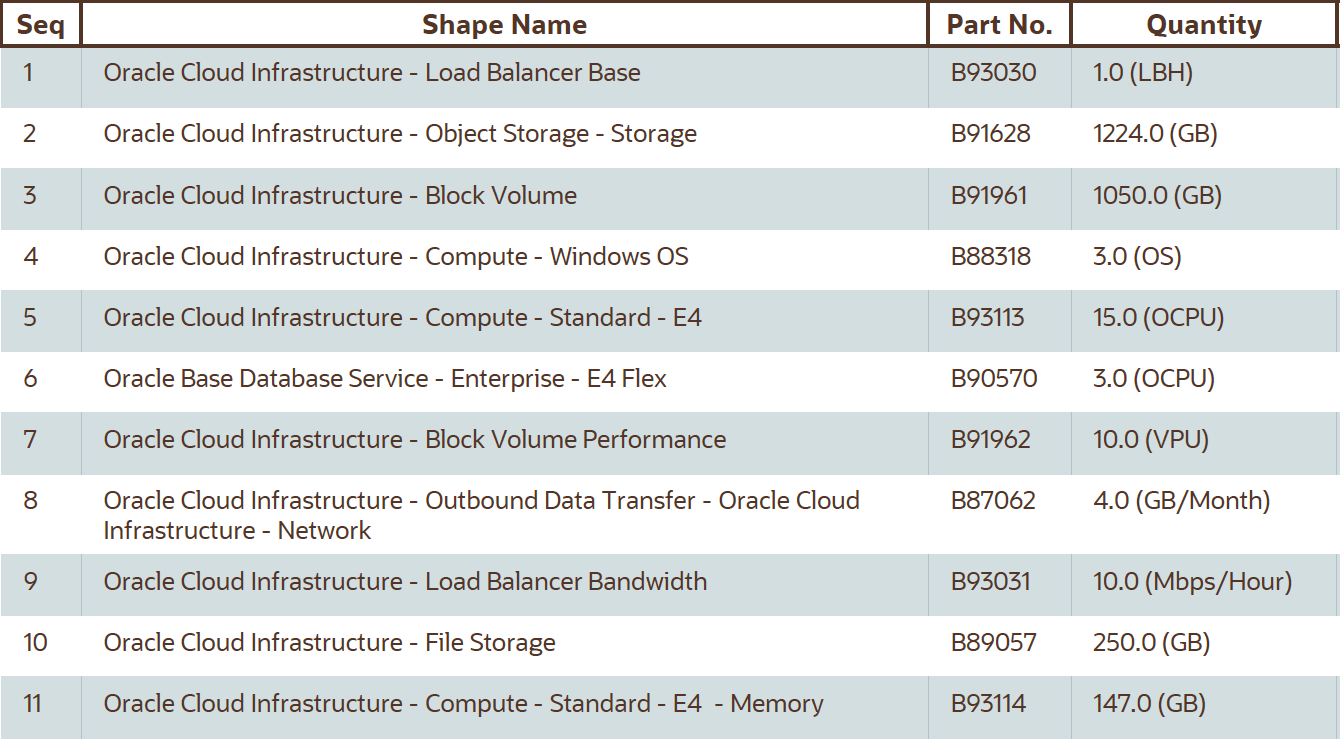
*A section describing the Future JDE workload sizing in OCI*

*Example:*

A sample BoM of the JDE workload is reflected in the table below for Intel shapes for 100 users:

**

A sample BoM of the JDE workload is reflected in the table below for AMD shapes for 100 users:

**

*Guide:*

*Estimate and size the physically needed resources of the Workload. The information can be collected and is based upon previously gathered capacities, business user numbers, integration points, or translated existing on-premises resources. The sizing is possibly done with or even without a Physical Architecture. It is okay to make assumptions and to clearly state them!*

*Clarify with sales your assumptions and your sizing. Get your sales to finalize the BoM with discounts or other sales calculations. Review the final BoM and ensure the sales are using the correct product SKUs / Part Number.*

*Even if the BoM and sizing were done with the help of Excel between the different teams, ensure that this chapter includes or links to the final BoM as well.*

*WIP*

* *Revision of existing discovery templates*
* *Consolidated data gathering sheet (sizing focused)*
* *Workload-specific sizing process/methodology*

# Project Implementation (Only for Oracle Implementations!)

## Solution Scope

### Disclaimer

*Guide:*

*A scope disclaimer should limit scope changes and create awareness that a change of scope needs to be agreed upon by both parties.*

*Example:*

As part of the Oracle <Service Provider> Project, any scope needs to be agreed upon by both the customer and Oracle. A scope can change but must be confirmed again by both parties. Oracle can reject scope changes for any reason and may only design and implement a previously agreed scope. A change of scope can change any previously agreed milestone and needs to be technically feasible.

All items not explicitly stated to be within the scope of the <Service Provider> project will be considered out of scope. Oracle recommends the use of professional services to implement extensions or customizations beyond the original scope, as well as to operate the solution, with an Oracle-certified partner.

### Overview

*Guide:*

*Describe the scope of the implementation as a sub-set of the Workload scope. For example one environment from one application.*

*Example:*

* Design and configure “least privilege” access controls and enable user access using OCI IAM compartments, groups, and policies.
* Design and provide a secure, scalable OCI network architecture.

### Business Value

*Guide:*

*What's the value for the customer to do an Oracle implementation? For example, speed of deployment and the resulting impact on time to market, and free service. Do not describe Oracle's value or consumption.*

*Example:*

The Oracle <Service Provider> service brings several benefits to this project. 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 <Service Provider> brings the speed of deployment resulting in successful projects without any setbacks. Oracle <Service Provider> services will bring value to the overall project provisioning OCI environments for the application workload.

Oracle Cloud <Service Provider> services provide guidance from cloud engineers and project managers on planning, project management, architecting, deploying, and managing cloud migrations.

### Success Criteria

*Guide:*

*Technical success criteria for the implementation. As always be S.M.A.R.T: Specific, Measurable, Achievable, Relevant, Timebound. Example: 'Deployment of all OCI resources for the scoped environments in 3 months'.*

*Example:*

The below-listed success criteria are for the <Service Provider> implementation only. Partner activities and success criteria are not listed in this documentation.

* Finish provisioning of all OCI resources
* Establish all required network connectivity
* Successfully pass all test cases
* Finished handover with documentation
* Complete the Implementation Security Checklist

## Workplan

### Deliverables

*Guide:*

*Describe deliverables within the implementation scope. Including this documentation as Solution Definition and the later following Solution Design. This should be a generic reusable text, provided by the implementers.*

### Included Activities

*Guide:*

*Describe the implementation activities in detail. It does not need to include a list of cloud services or OCI capabilities, but rather includes activities such as 'Provisioning of Infrastructure Components'. Include scope boundaries in terms of the number of environments, resource count to be provisioned, data volume to be migrated, etc.*

*Example:* The implementation scope of work includes the following activities:

**OCI Foundation & Network**

* OCI Foundation Setup - 1 Region (REGION NAME)
* OCI Networking configuration
  + Creation of VCN for up to 3 environments (up to 12 VCNs total)
  + DRG and inter-VCN routing
  + Deployment of standard Security lists and NSG in VCN
  + Deployment of Route Tables in VCNs
* Configure one site-to-site IPSec VPN between OCI & on-premises
* Configure Web Application Firewall to route the incoming internet traffic to Load Balancers and configure recommended rules
* Configure bastion service to allow admin users to connect to the tenancy through the internet access

**Security**

* Enable Cloud Guard
* Enable Datasafe and Register the Databases in scope
* Enable VSS
* Configure OCI IAM Domains

**Database**

* Migrate one non-prod database with one iteration
* Migrate one prod database with two iterations

### Recommended Activities

*Guide:*

*All activities not stated in the* [*Included Activities*](#included-activities) *are out of scope, as described in the* [*Disclaimer*](#disclaimer)*. We do not provide a list of excluded activities to not create expectations based on a grey area between included and excluded activities. Here we only recommend further activities that happen to not be included but are not a full list of excluded activities.*

*Example:*

All items not explicitly stated to be within the scope of the implementation project will be considered out of scope. Oracle recommends the use of professional services to implement extensions or customizations beyond the original scope, or to operate the solution with any of Oracle's certified partners. As a part of this engagement, the below activities are considered to be out of implementation scope.

* Any activities at customer on-premises or existing data center e.g. patching & backups required for migration
* Any integration with other products than in scope
* Any backup and recovery strategy implementation including third-party backup tool implementation
* Application upgrade of any Oracle or other vendor or open source software.
* SSL certificate management and configuration
* Any form of testing and validations, including but not limited to performance testing, load testing, HA testing, DR testing, and tuning of any component in the solution
* Any vulnerability assessment and penetration testing including server hardening, audit certification implementation
* Any functional testing is to be conducted by the customer and/or third party involved
* Any third-party firewall implementation, security tools, monitoring tools implementation
* Troubleshooting existing open issues, including the performance of the application
* Training on deployed products and OCI services
* Run and maintain the support of the environment and end-user training

### Timeline

*Guide:*

*Provide a high-level implementation plan. Use phases to communicate an iterative implementation if needed. Include prerequisites in the plan.*

#### Phase 1:

#### Phase n:

### Implementation RACI

*Guide:*

*Describe for all activities the RACI (Responsible, Accountable, Consultant, Informed) matrix*

*Example:*

| Num | Activity | Oracle | Customer |
| --- | --- | --- | --- |
| 1 | Conduct Project Kickoff | AR | C |
| 2 | Provide access to the source environment, including all the relevant ports opened | I | AR |
| 3 | Provide VPN credentials for Oracle team, OCI console access details | I | AR |
| 4 | Prepare Source System, apply required patches on source environments for migration, and take source environment backup to OCI | I | AR |
| 5 | Backup of source Database | C | AR |
| 6 | Provision Landing Zone with related Network and policies in scope | AR | C |
| 7 | Configure site-to-site VPN between onPrem and OCI tenancy | AR | C |
| 8 | Migrate non-Prod database in scope | AR | C |
| 9 | Perform Pre and Post functional migration tasks | I | AR |
| 10 | Perform functional/customization/integration testing and Validation of application within the project timeline | I | AR |
| 11 | Provide OCI technical support during validation | AR | C |
| 12 | Prepare production runbook and perform Production Cutover | C | AR |
| 13 | Provide timely support for HW, OS, network related issues at source | I | AR |
| 14 | Procure of SSL Certificates | C | AR |
| 15 | Provide access to My Oracle Support required for product support along with CSI number | I | AR |

**R- Responsible, A- Accountable, C- Consulted, I- Informed**

### Assumptions

*Guide:*

*List any assumptions, if any, which could impact the solution architecture or the implementation.*

*Example:*

**Generic assumptions**

* It is assumed that all required contractual agreements between Oracle and the Customer are in place to ensure uninterrupted execution of the project.
* It is assumed that all work will be done remotely and within either central European time or India Standard Time normal office working hours.
* It is assumed that upgrades are excluded from the scope of work and no production systems/production cutover is part of the scope of work undertaken by the Oracle Service
* It is assumed that all required Oracle cloud technical resources are available for use during the duration of the project and that engineers involved have been granted the appropriate access to those technical resources by the customer before the start of the project.
* It is assumed that all required customer resources, and if applicable third-party resources, are available during the duration of the project to work openly and collaboratively to realize the project goals uninterruptedly.
* It is assumed that all required customer resources, and if applicable third-party resources are aware of all technical and non-technical details of the as-is and to-be components. All resources are committed to technical work as far as is needed for the execution of the project.
* It is assumed that all required documentation, system details, and access needed for the execution of the project can be given/granted to parties involved when and where deemed needed for the success of the project.
* It is assumed that the customer will have adequate licenses for all the products that may/will be used during the project and that appropriate support contracts for those products are in place where the customer will take the responsibility of managing any potential service request towards a support organization to seek resolution of a problem.
* It is assumed the customer will provide the appropriate level of information and guidance on rules and regulations which can directly and/or indirectly influence the project or the resulting deliverables. This includes, however not limited to, customer-specific naming conventions, security implementation requirements, internal SLA requirements as well as details for legal and regulatory compliance. It will be the responsibility of the customer to ensure that the solution will adhere to this.
* It is assumed that under the customer's responsibility, the customer will ensure and validate that the solution will be placed under the proper controls for ensuring business continuity, system availability, recoverability, security control, and monitoring and management as part of a post-project task.
* It is assumed that the customer will take responsibility for testing all functional and non-functional parts of the solution within the provided timeline and ensure a proper test report will be shared with the full team (including customer, Oracle, and if applicable third party).
* It is assumed that any requirement, deliverable, or expectation that is not clearly defined as in-scope of the project will not be handled as part of the project and is placed under the responsibility of the customer to be handled outside of the project.

**Project-specific assumptions**

* It is assumed that sufficient network bandwidth (greater than 200 GB) is available between OCI and Customer onPremise for any data transfer.
* It is assumed that the customer, or a partner of your choice, will own the control, access, management, and further development of your OCI environment following the deployment of your solution.

### Obligations

*Guide:*

*List any obligations required by the customer to perform or have available, if any, which could impact the architecture or the implementation. Please always include this chapter to capture the obligation that we have admin access to the customer's tenancy.*

*Example:*

* You will have purchased the appropriate Universal Credits for the services required for the project.
* The implementation team will have admin access to the customer's tenancy for implementation.
* You will ensure the appropriate product training has been obtained to maintain and support the implementation
* Your business team will be available for the Testing phase, which will be completed within the agreed testing window.
* You will provide project management for the project and will manage any third-party suppliers or vendors.
* You will provide the implementation team with appropriate access to your tenancy & relevant on-premises applications/database to perform implementation activities. We recommend the least-privilege access principle.
* You will revoke implementor access on production goLive or after project completion.
* You will take consistent and restorable backups of your existing data and application before implementation.

### Transition Plan

*Guide:*

*The Transition Plan describes the handover of the project, after the implementation. Please ensure the accepting transition party is filled out.*

#### Introduction

Following the deployment of the solution to Oracle Cloud Infrastructure by the <Service Provider> team, it is important to ensure a smooth handover to a technical team, or a partner. <Service Provider> values the continuation of the cloud journey and we focus our efforts to ensure you start with the best possible foundation, to set you up for success in OCI.

When <Service Provider> completes the deliverables as described in the [Workplan](#workplan) section of this document, <Service Provider> will hand over the controls of the new OCI environment.

<Customer Name>, or a partner of your choice, will assume the ownership of the OCI tenancy and responsibility for further development of the OCI environment. From that moment forward, having completed the [Solution Scope](#solution-scope), <Service Provider> will disengage. For post-implementation support, Oracle provides you with three distinct resources:

1. Oracle Account Cloud Engineer (ACE) – This is your first point of contact and will provide technical leadership and support for Oracle cloud technologies and your cloud transformation.
2. Cloud Adoption Manager (CAM) - Introduces and plans operation monitoring and optimization advisory activities, and continues working with you on the next milestones. Please contact your ACE for further information.
3. [My Oracle Support](https://support.oracle.com/portal/)

#### Transition Acceptance

When <Service Provider> completes the deliverables as specified in the [Workplan](#workplan) section of this document, a closure session will be scheduled within 1-2 weeks to recap the project and to hand it over to the accepting party. In the case of this project, the accepting party is <Customer Name>. <Customer Name> is now responsible for the OCI tenancy.

From this moment forward, the Oracle <Service Provider> team will fully remove their access from your OCI tenancy and provide the access credentials to the accepting party. This marks the completion of the <Service Provider> project. There is no sign-off signature required.

# Annex

## Security Guidelines

### 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](https://docs.oracle.com/en-us/iaas/Content/cloud-adoption-framework/security-strategy.htm) – 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](https://docs.oracle.com/en-us/iaas/Content/cloud-adoption-framework/security.htm#capabilities) reflect fundamental security principles for architecture, deployment, and maintenance. 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.

#### 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](https://docs.oracle.com/en/solutions/oci-best-practices).
* Learn more about [Oracle Cloud Security Practices](https://www.oracle.com/corporate/security-practices/cloud/).
* For detailed information about security responsibilities in Oracle Cloud Infrastructure, see the [Oracle Cloud Infrastructure Security Guide](https://docs.oracle.com/iaas/Content/Security/Concepts/security_guide.htm).

### Compliance and Regulations

Cloud computing is fundamentally different from traditionally 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).

### Additional Resources

* [Oracle Cloud Compliance](https://www.oracle.com/corporate/cloud-compliance/) – Oracle is committed to helping customers operate globally in a fast-changing business environment and address the challenges of an ever more complex regulatory environment. This site is a primary reference for customers on the Shared Management Model with Attestations and Advisories.
* [Oracle Security Practices](https://www.oracle.com/corporate/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](https://www.oracle.com/corporate/security-practices/cloud/) documents.
* [Contract Documents](https://www.oracle.com/contracts/cloud-services/#online) for Oracle Cloud Services.
* [OCI Shared Security Model](https://docs.oracle.com/en-us/iaas/Content/cloud-adoption-framework/security.htm#shared-security-model)
* [OCI Cloud Adoption Framework Security Strategy](https://docs.oracle.com/en-us/iaas/Content/cloud-adoption-framework/security-strategy.htm)
* [OCI Security Guide](https://docs.oracle.com/en-us/iaas/Content/Security/Concepts/security_guide.htm)
* [OCI Cloud Adoption Framework Security chapter](https://docs.oracle.com/en-us/iaas/Content/cloud-adoption-framework/security.htm)

## Networking Requirement Considerations

The below questions help to identify networking requirements.

### 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?

### 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?

### 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)?

### Security and Access Control

* Are you familiar with the concept of Next-Generation Firewalls (NGFW) and their benefits over traditional firewalls?
* Have you considered the importance of protecting your web applications from potential cyber threats using a Web Application Firewall (WAF)?

### 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?

## Networking Solutions

### 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](https://docs.oracle.com/en-us/iaas/Content/network-firewall/overview.htm)
* [OCI Network Firewall](https://docs.oracle.com/en/solutions/oci-network-firewall/index.html#GUID-875E911C-8D7D-4205-952B-5E8FAAD6C6D3)

### 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](https://www.oracle.com/es/cloud/networking/load-balancing/)
* [Overview](https://docs.oracle.com/en-us/iaas/Content/NetworkLoadBalancer/overview.htm)
* [Concept Overview](https://docs.oracle.com/en-us/iaas/Content/Balance/Concepts/balanceoverview.htm)

### 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](https://docs.oracle.com/en-us/iaas/Content/TrafficManagement/Concepts/overview.htm)
* [DNS](https://docs.oracle.com/en-us/iaas/Content/DNS/home.htm)

### 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](https://www.oracle.com/security/cloud-security/web-application-firewall/)
* [Add WAF to a load balancer](https://docs.oracle.com/en/learn/oci-waf-flex-lbaas/index.html#add-oracle-cloud-infrastructure-web-application-firewall-protection-to-a-flexible-load-balancer)

### 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](https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/managingIGs.htm)

### 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](https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/overviewIPsec.htm)
* [Setup IPSec](https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/settingupIPsec.htm)

### 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](https://www.oracle.com/cloud/networking/fastconnect/)
* [Concept Overview](https://docs.public.oneportal.content.oci.oraclecloud.com/en-us/iaas/Content/Network/Concepts/fastconnect.htm)

### 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](https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/vtap.htm)
* [Network VTAP Wireshark](https://docs.oracle.com/en/solutions/oci-network-vtap-wireshark/index.html#GUID-3196621D-12EB-470A-982C-4F7F6F3723EC)

### 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](https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/path_analyzer.htm)

### 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](https://docs.oracle.com/es-ww/iaas/Content/Network/Tasks/managingDRGs.htm)
* [OCI Pilot Light DR](https://docs.oracle.com/en/solutions/oci-pilot-light-dr/index.html#GUID-3C1F7B6B-0195-4166-A38C-8B7AD53F0B79)
* [Peering VCNs in different regions through a DRG](https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/scenario_e.htm)

### 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](https://www.oracle.com/security/cloud-security/ssl-tls-certificates/)

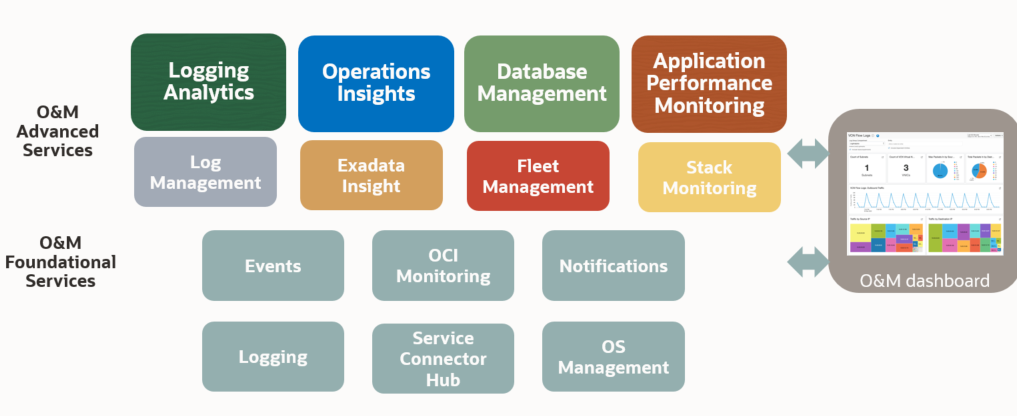
### OCI Monitoring

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](https://docs.oracle.com/iaas/Content/Monitoring/home.htm) and [Notifications](https://docs.oracle.com/en-us/iaas/Content/Notification/home.htm#top).

* [Networking Metrics](https://docs.oracle.com/en-us/iaas/Content/Network/Reference/networkmetrics.htm)

## Manageability

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



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.

### OCI O&M Services List

The observability and management services include the following services:

[Application Performance Monitoring](https://docs.oracle.com/en-us/iaas/Content/connector-hub/overview.htm) 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](https://docs.oracle.com/en-us/iaas/database-management/index.html) provides comprehensive database performance diagnostics and management capabilities to monitor and manage Oracle databases.

[Logging](https://docs.oracle.com/en-us/iaas/Content/Logging/home.htm) 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](https://docs.oracle.com/en-us/iaas/logging-analytics/home.htm) 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](https://docs.oracle.com/en-us/iaas/Content/Monitoring/home.htm) enables you to query [metrics](https://docs.oracle.com/en-us/iaas/Content/Monitoring/Concepts/monitoringoverview.htm#SupportedServices) and manage [alarms](https://docs.oracle.com/en-us/iaas/Content/Monitoring/Tasks/managingalarms.htm). Metrics and alarms help monitor the health, capacity, and performance of your cloud resources.

[Ops Insights](https://docs.oracle.com/en-us/iaas/operations-insights/index.html) 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](https://docs.oracle.com/en-us/iaas/Content/connector-hub/overview.htm) 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](https://docs.oracle.com/en-us/iaas/stack-monitoring/index.html) 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.

### 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](https://docs.oracle.com/en-us/iaas/Content/Monitoring/Concepts/monitoringoverview.htm#SupportedServices) |
| **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](https://docs.oracle.com/en-us/iaas/Content/connector-hub/overview.htm) |
| **OCI Console** | The Service Console offers a list of visual representations and basic information about critical metrics like CPU, memory, and storage. | [OCI Console](https://docs.oracle.com/en-us/iaas/Content/GSG/Concepts/console.htm) [Resource Usage Tracking](https://docs.oracle.com/en-us/iaas/Content/General/Concepts/resourcemonitoring.htm) |
| **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](https://docs.oracle.com/en-us/iaas/database-management/doc/database-management-metrics.html) |
| **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](https://docs.oracle.com/en-us/iaas/stack-monitoring/doc/promotion-and-discovery.html#GUID-633470D8-9FC3-4FD7-A34A-2A7208586AD6) |
| **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](https://docs.oracle.com/en-us/iaas/Content/connector-hub/overview.htm) [Third-Party Tools Use Cases](https://github.com/oracle-devrel/technology-engineering/tree/main/manageability-and-operations/observability-and-manageability) |

### 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](https://docs.oracle.com/en-us/iaas/Content/Logging/home.htm) |
| **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](https://docs.oracle.com/en-us/iaas/Content/Monitoring/home.htm) |
| **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](https://docs.oracle.com/en-us/iaas/Content/Dashboards/home.htm) |
| **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](https://docs.oracle.com/en-us/iaas/logging-analytics/home.htm) |
| **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](https://docs.oracle.com/en-us/iaas/Content/connector-hub/overview.htm) |
| **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](https://docs.oracle.com/en-us/iaas/performance-hub/index.html) |
| **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](https://docs.oracle.com/en-us/iaas/operations-insights/doc/operations-insights.html#GUID-9F401CEC-8B90-4B0C-AF2B-6780BA3E799D) [OCI Operations Insight Capacity planning](https://docs.oracle.com/en-us/iaas/operations-insights/doc/operations-insights.html#GUID-B2A3E104-494B-46A5-9F3E-8E3977C9328F) |

### 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](https://docs.oracle.com/en-us/iaas/database-tools/doc/using-oracle-cloud-infrastructure-console.html) |
| **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](https://www.oracle.com/it/manageability/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](https://docs.oracle.com/en-us/iaas/Content/General/Concepts/organization_management_overview.htm) |

### 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](https://github.com/oracle-quickstart/terraform-oci-open-lz/blob/master/design/OCI_Open_LZ.pdf) [OCI Logging Analytics for Exa](https://github.com/oracle-quickstart/terraform-oci-open-lz/blob/master/design/OCI_Open_LZ.pdf) |
| **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](https://docs.oracle.com/en-us/iaas/Content/connector-hub/overview.htm) |
| **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](https://www.oracle.com/it/manageability/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](https://docs.oracle.com/en-us/iaas/operations-insights/doc/operations-insights.html) [OCI ExaInsight](https://blogs.oracle.com/cloud-infrastructure/post/available-now-exadata-insights-in-oracle-cloud-infrastructure-operations-insights) |

### 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](https://docs.oracle.com/en-us/iaas/operations-insights/doc/operations-insights.html#GUID-B2A3E104-494B-46A5-9F3E-8E3977C9328F) |
| **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](https://docs.oracle.com/en-us/iaas/Content/Billing/Concepts/costanalysisoverview.htm) |
| **Usage RestAPI** | OCI offers various RestAPI’s to manage services, including the one for cost management. | [OCI Usage RestAPI](https://docs.oracle.com/en-us/iaas/Content/Billing/Concepts/costanalysisoverview.htm#cost_analysis_using_the_api) |