MS SQL Server Always ON
An architecture example in OCI

Solution Definition

31th of May 2024 | Version 2.5

Contents

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

1.1 Version Control

Guide:

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

Example:

Version	Authors	Date	Comments
1.0	Base Template	1st June 2023	Created a new Solution Definition document. To be used for iterative review and improvement.
2.0	Base Template	15th November 2023	Updated to MS Windows Server 2022 and SQL Server 2022
2.5	Base Template	31th May 2024	Updated to latest Sol. Def. Doc. Template

1.2 Team

Guide:

A section describing the team.

Example:

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

1.3 Document Purpose

Guide:

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

Example:

This document provides a high-level solution definition for the Oracle solution and aims at describing the current state, and to-be state as well as an example of physical implementable solution.

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

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

We will, specifically, consider an OCI architecture whose purpose is deploying Microsoft SQL Server Always On availability groups on Oracle Cloud Infrastructure to take advantage of the built-in redundancy and resiliency features of Oracle Cloud.

Business Context

Guide:

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

2.1 Executive Summary

Guide:

A section describing the Oracle differentiator and key values of the solution of our solution for the customer, allowing the customer to make decisions quickly.

2.2 Workload Business Value

Guide:

A clear statement of specific business value as part of the full workload scope. Try to keep it SMART: Specific, Measurable, Assignable, Realistic, and Time-Related - Agree on the business value with the customer. Keep it business-focused, and speak the language of the LoB which benefits from this Workload: "Increase Customer Retention by 3% in the next year" or "Grow Customer Base with Executive Decision-Making from our Sales and Support Data". Avoid technical success criteria such as "Migrate App X to Oracle Cloud" or "Provision 5 Compute Instances". Avoid Oracle success criteria and language "Get Workload Consuming on OCI".

Workload Requirements and Architecture

3.1 Overview

Guide:

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

ACME Corp. is a fantasy telecommunication company that focuses on empowering each individual customer by providing the most convenient and cost-effective way to communicate all over the world.

In this document we want to briefly describe how to implement the Microsoft SQL Server Always On Availability Group, that is an advanced enterprise level feature to provide high availability to SQL Server. All this harnessing the power of the OCI infrastructure.

3.2 Non-Functional Requirements

Guide:

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

This chapter is for describing customer-specific requirements (needs), not to explain Oracle solutions or capabilities.

3.2.1 Regulations and Compliances Requirements

Guide:

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

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

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

Example:

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

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

3.2.2 Environments

Guide:

A diagram or list detailing all the required environments (e.g. development, text, live, production, etc.).

If you like to describe a current state, you can use or add the chapter 'Current Sate Architecture' before the 'Future State Architecture'.

Example:

Name	Size of Prod	Location	DR	Scope
Production	100%	Malaga	Yes	Not in Scope / On-prem
DR	50%	Sevilla	No	Workload

Name	Size of Prod	Location	DR	Scope
Dev & Test	25%	Sevilla	No	Workload - <Service Provider>

3.2.3 High Availability and Disaster Recovery Requirements

Guide:

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

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

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

Note that if needed, this section may also include an overview of the proposed backup and disaster recovery proposed architectures.

This chapter is mandatory, while there could be no requirements on HA/DR, please mention that in a short single sentence.

Example:

At the time of this document creation, no Resilience or Recovery requirements have been specified.

3.2.4 Security Requirements

Guide:

Capture the Non-Functional Requirements for security-related topics. The requirements can be (but don't have to be) separated into:

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

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

Example:

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

3.2.5 Networking Requirements

Guide

Capture the Non-Functional Requirements for networking-related topics. You can use the networking questions in the Annex

As businesses increasingly rely on Cloud Infrastructure to store, process, and transmit sensitive data, the need for comprehensive security solutions has never been more important. Potential customers evaluating network security solutions typically prioritize the following requirements: Some of the broader category considerations are below.

- *Data Protection: Safeguarding sensitive information against unauthorized access, theft, or modification is a primary concern for any organization and industry today.*
  - *Threat Prevention: Advanced capabilities like IDPS and malware detection for blocking threats.*
  - *Data Loss Prevention (DLP): Monitoring and controlling sensitive data transmission.*
  - *Encryption and Decryption: Inspecting encrypted traffic without compromising privacy.*
- *Threat Prevention: Proactively identifying and mitigating security threats is essential for maintaining the integrity of network infrastructure.*
  - *Intrusion Detection and Prevention: Monitoring for suspicious or malicious activity.*

  - *Application Control: Granular control over specific applications or services.*
  - *URL Filtering: Controlling access to permitted URLs.*
- *Security compliance: Does your organization have network security requirements based on industry or organization compliance? For example - SAMA (Saudi Arabia Monetary Authority), HIPAA (Health Insurance Portability and Accountability Act), GDPR (General Data Protection Regulation), SWIFT, etc.*

Example:

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

3.2.6 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	

3.3 Future State Architecture

Guide:

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

This should be the final architecture as part of the pre-sales solution, not an intermediate or draft version

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

3.3.1 Mandatory Security Best Practices

Guide:

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

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

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

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

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

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

CATEGORY	TOPIC	DETAILS
		• For configuration details see Vulnerability Scanning.
Monitoring	SIEM Integration	Continuous monitoring of OCI resources is key for maintaining the required security level (see Regulations and Compliance for specific requirements). See Design Guidance for SIEM Integration to implement integration with the existing SIEM system.
Additional Services	Budget Control	OCI Budget Control provides an easy-to-use and quick notification on changes in the tenancy's budget consumption. It will be configured to quickly identify unexpected usage of the tenancy. • For configuration details see Managing Budgets

3.3.2 Naming Conventions

Guide:

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

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

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

3.3.3 OCI Landing Zone Solution Definition

Guide:

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

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

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

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

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

3.3.4 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

3.3.5 Physical Architecture

Guide:

The Workload Architecture is typically described in a physical form. This should include all solution components. You do not have to provide solution build or deployment details such as IP addresses.

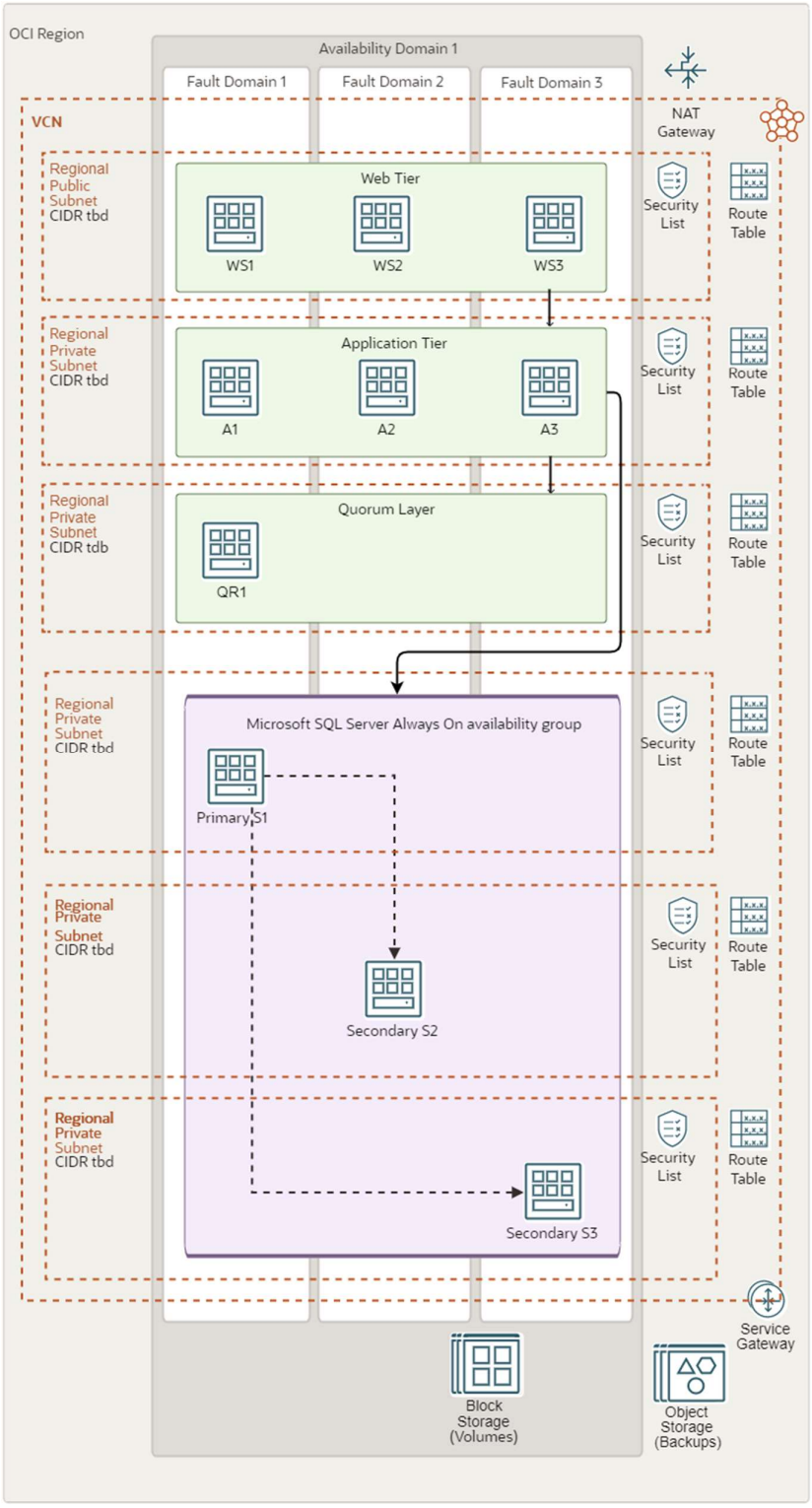
Please describe the solution with an architecture image plus a written text. If you have certain specifics you like to explain, you can also use the Solution Consideration chapter to describe the details there.

The Oracle Cloud Notation, OCI Architecture Diagram Toolkits

Reference:

StarterPacks (use the search)

Example:



Future State MS SQL Always ON Diagram

3.4 Solution Considerations

Guide:

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?

The architecture has the following components:

- Region

An Oracle Cloud Infrastructure region is a localized geographic area that contains one or more data centers, called availability domains. Regions are independent of other regions, and vast distances can separate them (across countries or even continents).

- Availability domain

Availability domains are standalone, independent data centers within a region. The physical resources in each availability domain are isolated from the resources in the other availability domains, which provides fault tolerance. Availability domains don't share infrastructure such as power or cooling, or the internal availability domain network. So, a failure at one availability domain is unlikely to affect the other availability domains in the region.

- Fault domain

A fault domain is a grouping of hardware and infrastructure within an availability domain. Each availability domain has three fault domains with independent power and hardware. When you distribute resources across multiple fault domains, your applications can tolerate physical server failure, system maintenance, and power failures inside a fault domain.

- Virtual cloud network (VCN) and subnets

A VCN is a customizable, private network that you set up in an Oracle Cloud Infrastructure region. Like traditional data center networks, VCNs give you complete control over your network environment. You can segment VCNs into subnets, which can be scoped to a region or to an availability domain. Both regional subnets and availability domain-specific subnets can coexist in the same VCN. A subnet can be public or private.

This architecture uses different subnets to host the web servers hosts, application servers, quorum witness server, and database servers.

- Route table

Virtual route tables contain rules to route traffic from subnets to destinations outside a VCN, typically through gateways.

- Security lists

For each subnet, you can create security rules that specify the source, destination, and type of traffic that must be allowed in and out of the subnet.

This architecture needs ingress and egress rules in the security lists attached to the web servers, application servers, quorum witness server, and database server subnets. These rules must be added to enable features such as remote desktop connectivity, access to the SQL Server database, and access for the Always On availability groups endpoints.

- NAT gateway

The NAT gateway allows internal generated outbound only traffic between the subnets in a VCN and the public internet.

- Block volume

With block storage volumes, you can create, attach, connect, and move storage volumes, and change volume performance to meet your storage, performance, and application requirements. After you attach and connect a volume to an instance, you can use the volume like a regular hard drive. You can also disconnect a volume and attach it to another instance without losing data.

- Object storage

Object storage provides quick access to large amounts of structured and unstructured data of any content type, including database backups, analytic data, and rich content such as images and videos. Use standard storage for "hot" storage that you need to access quickly, immediately, and frequently. Use archive storage for "cold" storage that you retain for long periods of time and seldom or rarely access.

3.4.1 High Availability and Disaster Recovery

Reference:

- Resilliance on OCI
- Workload Related Content

3.4.2 Security

Guide:

Please describe your solution from a security point of view. Generic security guidelines are in the Annex chapter.

Example:

Please see our security guidelines in the Annex.

3.4.3 Networking

Guide:

If your customers have any or one of the needs described in the guide of the Network 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.

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.

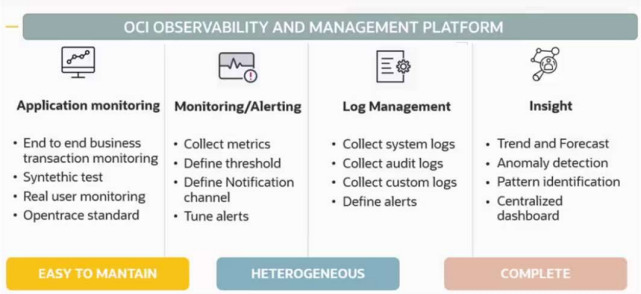
3.4.4 Manageability and Observability

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.

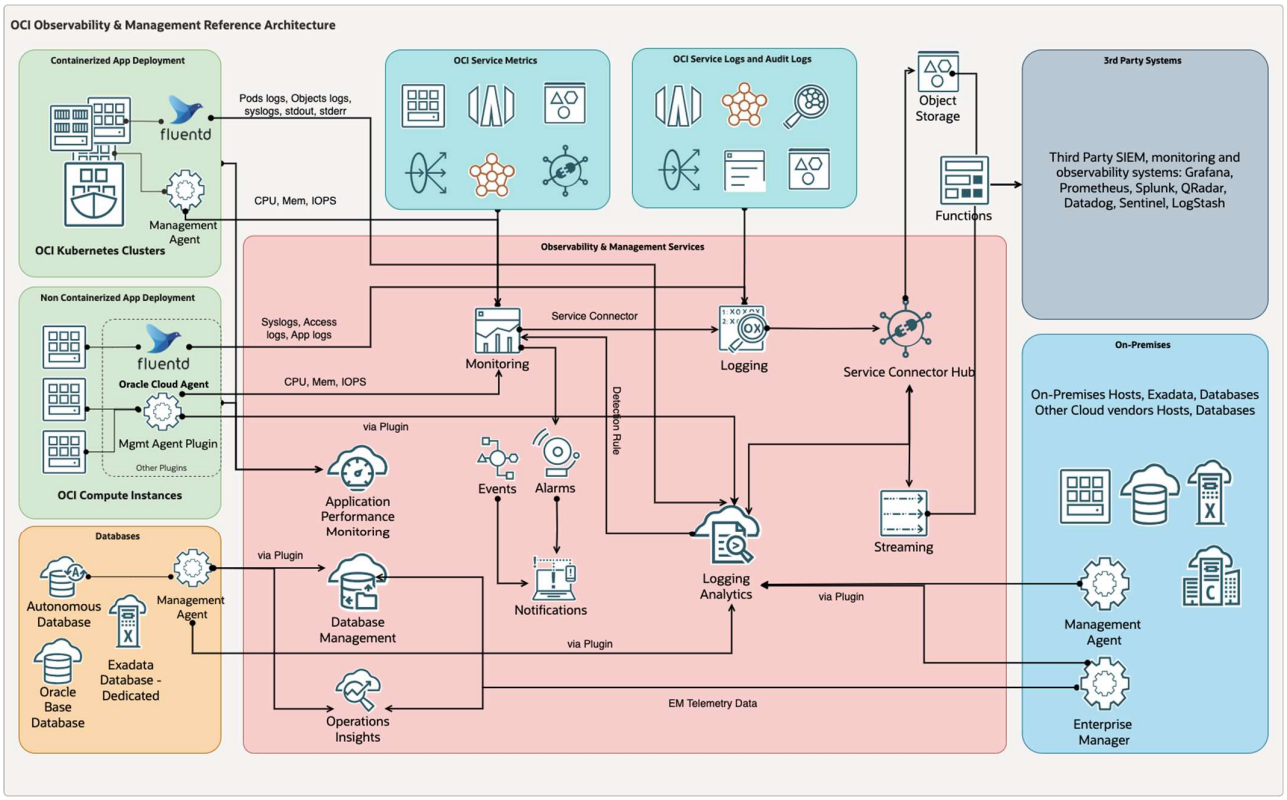


Observability and Manageability

3.4.4.1 Observability Architecture

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

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



OCI Architecture

3.4.4.2 Real-Time Monitoring

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

Please find all references for this chapter in the Annex.

3.4.4.3 Performance and Tuning

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

Please find all references for this chapter in the Annex.

3.4.4.4 Administration

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

Please find all references for this chapter in the Annex.

3.4.4.5 Troubleshooting

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

Please find all references for this chapter in the Annex.

3.4.4.6 Cost Control and Chargeback

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

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

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

Please find all references for this chapter in the Annex.

3.5 Sizing and Bill of Materials

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 ok 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*

Server Role	OCI Component	Quantity	SHAPE	OCPU	RAM (GB)	Operating System
Quorum witness server	Compute	1 VMs	VM.Standard.2.2	2	30	Windows Server 2012
SQL Server Always ON Servers	Compute	3 VMs	VM.Standard.2.2	2	30	Windows Server 2012
Load Balancer Base	Networking	1 LB				

Project Implementation (Only for Oracle Implementations!)

4.1 Solution Scope

4.1.1 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.

4.1.2 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.

4.1.3 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.

4.1.4 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

4.2 Workplan

4.2.1 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.

4.2.2 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

4.2.3 Recommended Activities

Guide:

All activities not stated in the Included Activities are out of scope, as described in the 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

4.2.4 Timeline

Guide:

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

4.2.4.1 Phase 1:

4.2.4.2 Phase n:

4.2.5 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

Num	Activity	Oracle	Customer
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

4.2.6 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.

4.2.7 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.

Add for EBS migration

- Your on-premise source non-prod environment would be a fresh clone from the production environment for easy simulation of issues.
- You would be responsible for applying and testing all migration-related patches on the on-premise source environment.
- You will ensure that the relevant pre-requisite patches have been applied on the on-premise source environment as per MOS DocID 2517025.1: Getting Started with Oracle E-Business Suite on Oracle Cloud Infrastructure:
  - Table 5 - Source Environment Requirements with Target Database Tier on Oracle Cloud Infrastructure Compute VM (Under 4.2.2 section) and
  - Section 4.5.5 Applying the Latest Critical Patch Updates (CPU) and Security Fixes

4.2.8 Transition Plan

Guide:

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

4.2.8.1 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 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, <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

4.2.8.2 Transition Acceptance

When <Service Provider> completes the deliverables as specified in the 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

5.1 Security Guidelines

5.1.1 Oracle Security, Identity, and Compliance

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

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

5.1.2 References

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

5.1.3 Compliance and Regulations

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

5.1.4 Additional Resources

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

- Contract Documents for Oracle Cloud Services.
- OCI Shared Security Model
- OCI Cloud Adoption Framework Security Strategy
- OCI Security Guide
- OCI Cloud Adoption Framework Security chapter

5.2 Networking Requirement Considerations

The below questions help to identify networking requirements.

5.2.1 Application Connectivity

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

5.2.2 DR and Business Continuity

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

5.2.3 High Availability and Scalability

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

5.2.4 Security and Access Control

- Some of the below questions help you to adopt the right sizing and deployment model of the network firewall.
  - Does the customer need to protect traffic from VCN to VCN?
  - Does the customer need to protect traffic from subnet to subnet in the same VCN?
  - When deploying an OCI Network Firewall in a dedicated HUB or secure VCN, do you want to protect inter-VCN traffic and/or inter-subnet traffic from within the same VCN?

  - Does the customer need to protect incoming or egressing traffic to the internet?
  - Does the customer need to protect internal traffic (including on-premises via IPSEC/FC)?
  - Is the network performance critical?
  - Does the customer have any requirement on network isolation (i.e., internet traffic never traverses or is mixed with internal traffic)?
- Have you considered the importance of protecting your web applications from potential cyber threats using a Web Application Firewall (WAF)?

5.2.5 Monitoring and Troubleshooting

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

5.3 Networking Solutions

5.3.1 OCI Network Firewall

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

- Overview
- OCI Network Firewall

5.3.2 OCI Load Balancer

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

- Load Balancing
- Overview
- Concept Overview

5.3.3 OCI DNS Traffic Management

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

- Concept Overview
- DNS

5.3.4 OCI WAF

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

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

5.3.5 OCI IGW

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

- Managing IGW

5.3.6 OCI Site-to-Site VPN

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

- Overview IPSec
- Setup IPSec

5.3.7 OCI Fast Connect

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

- FastConnect
- Concept Overview

5.3.8 OCI VTAP

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

- VTAP
- Network VTAP Wireshark

5.3.9 OCI NPA

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

- Path Analyzer

5.3.10 OCI DRG (Connectivity Options)

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

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

5.3.11 OCI Oracle Cloud Infrastructure Certificates

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

- SSL TLS Certificates

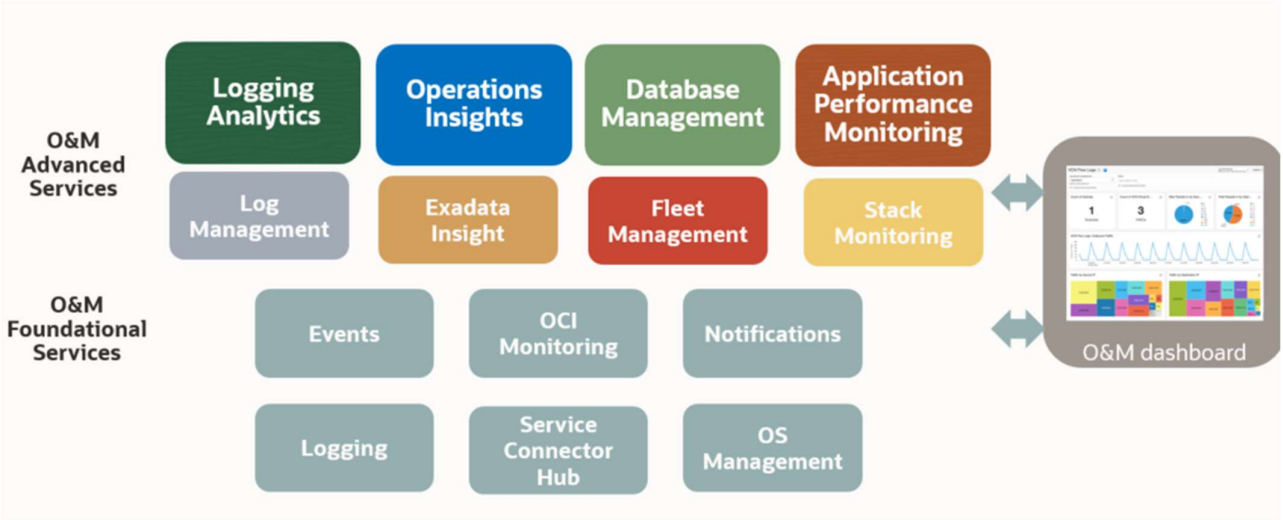
5.3.12 OCI Monitoring

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

- Networking Metrics

5.4 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.

5.4.1 OCI O&M Services List

The observability and management services include the following services:

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

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

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

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

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

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

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

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

5.4.2 Real-Time Monitoring Annex

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

5.4.3 Performance and Tuning Annex

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

5.4.4 Administration Annex

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

5.4.5 Troubleshooting Annex

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

5.4.6 Cost Control and Chargeback Annex

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