A Company Making Everything Autonomous DB ML Project Oracle Machine Learning

Workload Architecture Document
Solution Definition and Design

24 July 2023 | Version 1.3

CONTENTS

DOCUMENT CONTROL

1.1 Version Control

Version	Authors	Date	Comments
1.0	ACE	13 October 2022	Initial version
1.1	Ismael Hassane	12 January 2023	Version update Removed reference to OCI Data Science
1.2	Ismael Hassane	17 February 2023	adding the Network Firewall
1.3	Ismael Hassane	24 July 2023	adding more use-cases and details on OML

1.2 Team

Name	Email	Role	Company
Ismael Hassane	ismael.hassane@oracle.com	Cloud Solution Specialist - Analytics & Lakehouse	Oracle
ACE	ace@oracle.com	Account Cloud Engineer	Oracle

1.3 Table of Acronyms

Term	Meaning
AD	Availability Domain
ADB	Autonomous Database including ATP, ADW, AJD, etc.
ADW	Autonomous Data Warehouse
ATP	Autonomous Transaction Processing
DEV	Development Environment
DI	Data Integration
DLH	Data Lakehouse
DRG	Dynamic Routing Gateway
DWH	Data Warehouse
ELT	Extract-Load-Transform
ETA	Estimated Time of Arrival
IaaS	Infrastructure as a Service
LB	Load Balancer
NSG	Network Security Group
OCI	Oracle Cloud Infrastructure
PROD	Production Environment
SLA	Service Level Agreement
UAT	User Acceptance Test Environment
VCN	Virtual Cloud Network

1.4 Document Purpose

This document provides a high-level solution definition for the Oracle solution and aims at describing the current state, to-be state as well as a potential implementation project scope and timeline. The implementation project will be described as a physical implementable solution. The intended purpose is to provide all parties involved a clear and well-defined insight into the scope of work and intention of the project.

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 chapter Workload Requirements and Architecture.

BUSINESS CONTEXT

2.1 Executive Summary

2.2 Workload Business Value

The client is developing a new line of business where they will provide credit financing to importers and exporters. The approval process for the credit solution will be quicker than with banks. At the time of booking a consignment, the booking agent can offer it in real-time, saving a great deal of time on paperwork and approval procedures.

A precise credit risk scoring algorithm is crucial for this new service. Machine learning and data science can use historical trade information and make classifications and predictions about importer or exporter credit worthiness. Machine learning models will use 3rd party data and Fusion ERP data since this data is based on factual audited trade information that provides high confidence in data quality.

WORKLOAD REQUIREMENTS AND ARCHITECTURE

3.1 Overview

3.2 Machine Learning Model steps

The below schema lists the necessary tasks in the lifecycle of a machine learning model ranging from data collection to model retraining when performance decays.

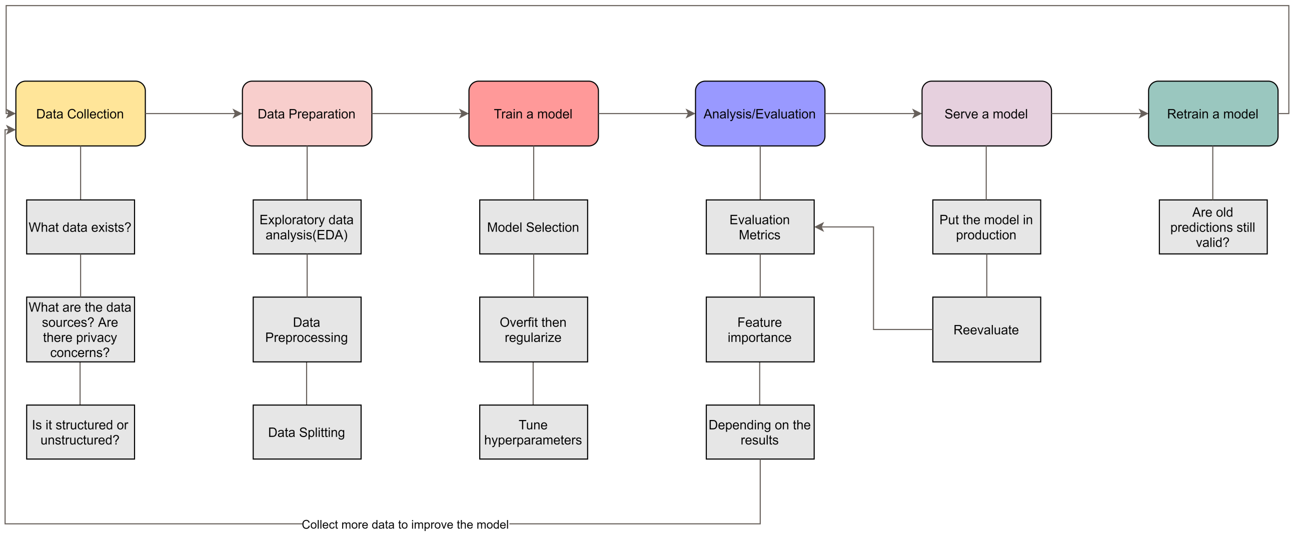

Figure 1: Ml Lifecycle

3.3 Functional Requirements

In-database machine learning refers to the integration of machine learning algorithms and models directly into a database system. This approach offers several advantages, including reduced data movement, faster predictions, and enhanced security. Here are some use cases for in-database machine learning:

3.3.1 Use Cases

3.3.1.1 Real-time Credit Risk Assessment

Credit scoring is a crucial process in the banking industry that assesses the creditworthiness of individuals or businesses applying for loans or credit. In-database machine learning can significantly improve the efficiency and accuracy of credit scoring models.

When customers apply for credit, banks need to make quick and informed decisions about their creditworthiness. Traditional credit scoring models may involve transferring large volumes of data to external systems for analysis, leading to delays in processing applications and potential security risks. In-database machine learning can address these challenges by building credit scoring models directly within the banking database.

By integrating machine learning algorithms into the database, banks can analyze a customer's historical financial data, credit history, transaction behavior, and other relevant factors in real-time. This enables immediate credit risk assessment and decision-making during the application process. In-database machine learning models can quickly evaluate a customer's credit risk profile and provide an instant credit score, facilitating faster approvals for credit products like loans, credit cards, and overdrafts.

Moreover, in-database machine learning allows banks to continuously update and fine-tune their credit scoring models as new data becomes available, ensuring that the models stay relevant and accurate over time. This adaptability is especially important in the dynamic and ever-changing financial landscape.

By leveraging in-database machine learning for credit scoring, banks can streamline their lending processes, improve customer experiences, and mitigate credit risks effectively. Additionally, it helps in maintaining data privacy and security, as sensitive customer information remains within the secure confines of the database.

3.3.1.2 Fraud Detection

In the financial industry, fraud detection is a critical application. By leveraging in-database machine learning, financial institutions can develop and deploy fraud detection models directly within their databases. This enables real-time analysis of transactions and customer behavior, reducing the time between data collection and prediction. With in-database machine learning, suspicious activities can be quickly flagged and appropriate actions taken to prevent fraudulent transactions, leading to enhanced security and reduced financial losses.

3.3.1.3 Customer Churn Prediction

For businesses with large customer bases, understanding and predicting customer churn (i.e., when customers stop using their services) is vital. By employing in-database machine learning, companies can build churn prediction models directly within their databases. These models can analyze historical customer data, such as transaction history, customer interactions, and usage patterns, to identify potential churners. The in-database approach allows businesses to make real-time predictions and take proactive measures, such as personalized retention offers, to retain valuable customers.

3.3.1.4 Personalized Recommendations

E-commerce platforms and content providers often rely on recommendation systems to offer personalized suggestions to their users. In-database machine learning can be used to develop recommendation models within the database itself. By analyzing user behavior, purchase history, and preferences in real-time, the database can generate personalized recommendations without the need to transfer vast amounts of data to external systems. This not only ensures faster response times but also protects the privacy and security of user data.

In all these use cases, the integration of machine learning directly within the database optimizes data processing, minimizes data movement, and enhances overall system performance. It also simplifies model deployment and maintenance, making it an attractive solution for various data-intensive applications.

3.3.2 Data Dictionary

3.3.3 Data Flow

Element	Description
Use Case 1	Preparing near real-time Credit Risk solution by using AutoML in Autonomous Data Warehouse
Stakeholder	Customer name
Use Case Overview	This use case will create a new business line for the company.
Precondition 1	Business requirements will be defined by the customer
Trigger	Whenever there is new data in the 3rd party application database, it will be loaded into Autonomous Data Warehouse by OCI GG. Fusion ERP data will be integrated daily.
Basic Flow	The data from 3rd party applications and Fusion ERP will be integrated to Autonomous Data Warehouse daily and AutoML will provide the best ML model over historical data. Applications will access the results through OML Services and the Business users will access through Oracle Analytics Cloud.

Element	Description
Alternative Flow 1	If the customer would like to use Jupyter Environment and they can also use OCI Data Science Cloud
Alternative Flow 2	If the customer would like to integrate new data sources, they can be integrated with OCI Data Integration

3.3.4 Functional Capabilities

3.3.5 Requirement Matrix

Requirements	OAC[1]	ADW	OCI DI	OCI GG
Access report and advanced visualization	Y			
Self-Service reporting and advanced visualization	Y			
Profile and analyze data and KPIs	Y	Y		
Data loading			Y	Y
Data processing			Y	
Data persistence (storage)		Y		

3.4 Non Functional Requirements

3.4.1 Integration and Interfaces

Name	Source	Target	Mode	Function
OCI Data Integration	Oracle Fusion Maintenance Cloud	ADW	Batch	Batch extraction
OCI Golden Gate	3rd party Application DB	ADW	realtime	Change data capture

3.4.2 Regulations and Compliances

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

3.4.3 Environments

Name	Size of Prod	Location	MAA	Scope
Production	100%	Madrid	Gold	Not in Scope / On-prem
Disaster Recovery	50%	Marseille	None	Implementation Partner
Dev & Test	25%	Madrid	None	Lift Project

3.4.4 System Configuration Control Lifecycle

[1] **OAC**:Oracle Analytics Cloud, **ADW**: Autonomous Data Warehouse, **OCI DI**: OCI Data Integration, **OCI GG**: OCI Golden Gate

3.4.5 Resilience and Recovery

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

Workload resilience is achieved by the intrinsic capabilities of ExaCS and OAC and providing Service Level Objectives as described in ”Oracle PaaS and IaaS Public Cloud Services Pillar Document”.

Recovery can be achieved by leveraging:

- **OAC** :
  - **OAC system-generated backups :** Oracle regularly do system-generated backups (daily, and also when a change is done on the data model and keep them for 30 days) of the entire Oracle Analytics Cloud environment, including system configuration and user content. Oracle Support Services use these system-generated backups to restore an environment that becomes corrupt, but these system-generated backups aren't accessible to customers and they’re not intended to provide customer-requested recovery points. Customer must use the snapshot feature (described below) to back up and restore user content.
  - **OAC Snapshots** : Customer should regularly back up the content that users create to a file called a snapshot. User content includes catalog content such as reports, dashboards, data visualization workbooks, and pixel perfect reports, datasets, data flows, data models, security roles, service settings, and so on. If something goes wrong with your content or service, you can revert to the content you saved in a snapshot. Snapshots are also useful if there is a requirement to move or share content from one service to another. Oracle Analytics Cloud Snapshot is described here

    Oracle recommends to take snapshots at significant checkpoints, for example, before making a major change to the content or environment. In addition, Oracle recommends taking regular weekly snapshots or at defined frequency based on the rate of change of the environment and rollback requirements. These Snapshots are can be downloaded to in order to store them locally.
  - To implement a disaster recovery, a well-architected business continuity plan should be designed in order to recover as quickly as possible and continue to provide services to Oracle Analytics Cloud users. Oracle recommends to do snapshots regularly and restore the content to a redundant Oracle Analytics Cloud environment (that can be only powered on during restore process) in another region if possible to mitigate the risk of region-wide events.
- **OCI DI** :
  - **Applications in ODI Data Integration** : In order to achieve disaster recovery, version upgrade and cross environment code promotion, we use the notion of Applications in OCI Data Integration. An Application in Data Integration is a container at the workspace level that holds runtime objects such as published tasks and task runs. You have the flexibility to create a new Application from scratch or make a copy of an existing one. Disaster Recovery will be achieve by automating backup creation and trigger restauration in the event of a disaster.
- **ADW** :
  - **ADW automated backups** : that have a retention period of 60 days and that allow to restore and recover the ADW database to any point-in-time in this retention period. Manual backups can also be performed and stored in an Object Storage bucket, if needed, for instance to have a higher retention period.
  - **Oracle Database Autonomous Recovery Service** You can select Recovery Service as the backup destination for automatic backups.
  - **Autonomous Data Guard** you can add an Autonomous Data Guard standby database, the system creates a standby database that continuously gets updated with the changes from the primary database
  - **OML** backup and recovery are also immediate as part of ADW.

3.4.6 Management and Monitoring

Type	Tool	Task	Target	Location	Notes
Monitoring	OAC console	monitor user sessions and cache status	OAC	OCI	
Monitoring	Performance Hub	monitor performance, CPU utilization, consumed storage, running SQL statements and sessions amongst other metrics exposed	ADW	OCI	
Management	Identity Domain console	manage users and perform role assignment for those users	Identity Domain	OCI	
Management	OCI Console	database management tasks for Autonomous Databases	ADW	OCI	
Management	Using the API	database management tasks for Autonomous Databases	ADW	OCI	
Management	OAC console	manage OAC settings, create and restore snapshots	OAC	OCI	

3.4.7 Security

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

3.4.7.1 Identity and Access Management

The proposed solution consists of ADW, Oracle Analytics Cloud (OAC) and OCI Golden Gate which are fully managed by Oracle (OCI PaaS), and therefore have very small attack surface. Authentication and authorization of users is done with the enterprise-grade Identity and Access Management (IAM) services of OCI.

3.4.7.2 Data Security

3.5 Constraints and Risks

Name	Description	Type	Impact	Mitigation Approach
OCI skills	Limited OCI skills in customers organization	Risk	No Operating Model	Involve Ops partner, for example Oracle ACS

Name	Description	Type	Impact	Mitigation Approach
Team Availability	A certain person is only available on Friday CET time zone	Constraint		Arrange meetings to fit that persons availability
Access Restriction	We are not allowed to access a certain tenancy without customer presence	Constraint		Invite customer key person to implementation sessions

3.6 Current State Architecture

3.7 Future State Architecture

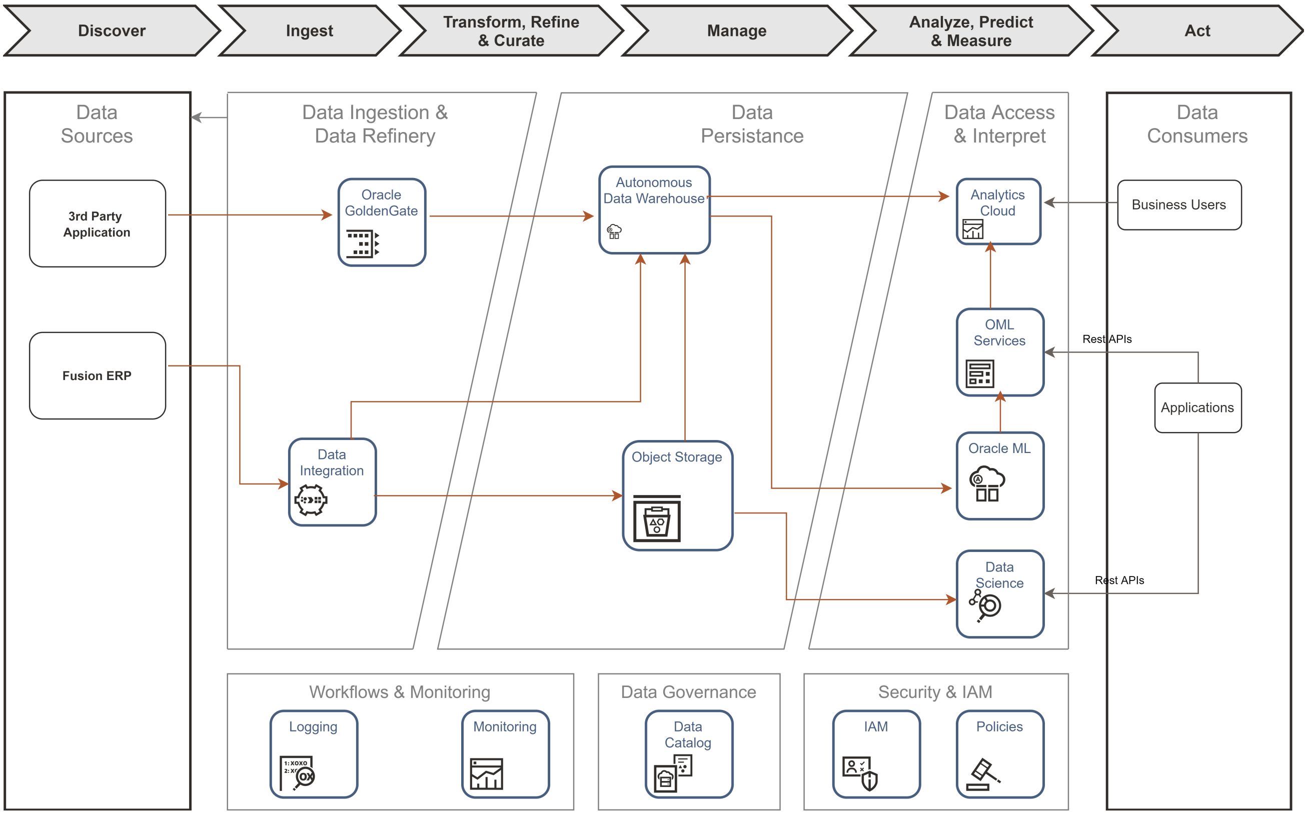

Figure 2: Future State Architecture

Main Components:

3.7.1 Data Ingestion & Data Refinery

- **Oracle Cloud Infrastructure Data Integration** will be used to process and transform data that is coming from Fusion ERP and ingest it into Autonomous Database.
- **OCI Golden Gate** will be used to replicate the data from the database of 3rd Party Application Database to Autonomous Database.

3.7.2 Serving/Data Persistance

- **Oracle Autonomous Data Warehouse** will serve as the source of the curated data that will be used to create the AutoML data preparation and feature engineering. By leveraging Autonomous Oracle Database and the power of Exadata in the cloud, data preparation over historical data will perform better.
- **Object Storage** - is an internet-scale, high-performance storage platform that offers reliable and cost-efficient data durability. Object Storage can also be used as a cold storage layer for the Autonomous Databases by storing data that is used infrequently and then joining it seamlessly with the most recent data by using hybrid tables in the Oracle Database.

3.7.3 Data Access & Interpretation

Data Science & Machine Learning

- **Predict**

Oracle Machine Learning Services extend Oracle Machine Learning (OML) functionality to support model deployment and model lifecycle management for both in-database Oracle Machine Learning models and third-party Open Neural Networks Exchange (**ONNX**) machine learning models via REST APIs. Oracle Machine Learning Services supports real-time and small-batch scoring for applications and dashboards.

The REST API for Oracle Machine Learning Services provides REST endpoints with authentication via Autonomous Data Warehouse. These endpoints enable the storage and management of machine learning models and their metadata. These endpoints also allow for the creation of scoring endpoints for models.

Oracle Machine Learning Services supports third-party classification or regression models that can be built using packages like Scikit-learn and TensorFlow, among others and then exported in ONNX format. Oracle Machine Learning Services supports integrated cognitive text analytics for topic discovery, keywords, summary, sentiment, and similarity. Oracle Machine Learning Services also supports image classification via third-party ONNX format model deployment, and supports scoring using images or tensors.

Users can also predict directly in the database using in-database models from SQL, R, and Python for singleton, small batch, and large-scale batch scoring. Users can leverage OML4Py embedded Python execution to invoke user-defined Python function with models produced from third-party packages and make predictions from Python and REST interfaces.

- **Learn**

Oracle Machine Learning **Notebooks** provide a collaborative user interface for data scientists and business and data analysts to work with SQL and Python interpreters while also performing machine learning in Oracle Autonomous Database—which includes Autonomous Data Warehouse (ADW), Autonomous Transaction Processing (ATP), and Autonomous JSON Database (AJD). Oracle Machine Learning Notebooks enable the broader data science team (data scientists, citizen data scientists, data analysts, data engineers, DBAs) to work together to explore their data visually and to develop analytical methodologies using OML4SQL and OML4Py. The Notebooks interface provides access to Oracle's high-performance, parallel, and scalable in-database implementations of machine learning algorithms via Python, SQL, and PL/SQL. In-database functionality can also be accessed through connection to Autonomous Database via external interfaces, such as SQL Developer, open source notebook environments, and third-party IDEs.

OML4Py also provides a Python API for automated machine learning (AutoML) for automated algorithm and feature selection, and for automated model tuning and selection.

Oracle Machine Learning **AutoML** User Interface (OML AutoML UI) is a no-code user interface that provides automated machine learning with ease of deployment to Oracle Machine Learning Services. Business users without extensive data science background can use OML AutoML UI to create and deploy machine learning models as well as generate an OML notebook containing the corresponding OML4Py code to rebuild the model and score data programmatically.

Expert data scientists may use OML AutoML UI as a productivity accelerator for faster model exploration, for ease of deployment, and for starter notebook generation.

Visualize and Learn

Oracle Analytics Cloud Business users will have access to the customer's final data/variables and the evaluation of their credit score results in Oracle Analytics Dashboards. It is scalable and secure public self-service & enterprise Visualization service that provides a full set of capabilities to explore and perform collaborative analytics.

OAC supports **Oracle Machine Learning** models deployments along with OCI AI services such as **OCI Vision** for image detection.

Governance

- **OCI Data Catalog** - is a crucial component in governing the data and information landscape providing visibility to where technical assets such as metadata and respective attributes reside as well as offering the ability to maintain a business glossary that is mapped to that technical metadata. Data Catalog can also serve metadata to be consumed by ADB in order to facilitate external tables creation in those autonomous databases.
- **Data Safe** - is a unified control center for Oracle Databases which helps you understand the sensitivity of your data, evaluate risks to data, mask sensitive data, implement and monitor security controls, assess user security, monitor user activity, and address data security compliance requirements. Data Safe will be used to 1) audit and implement security controls namely on the production database as well as 2) sensitive data discovery and masking of non prod environments that might originate from production copies/replicas.

CI/CD

- **OCI DevOps Service** Oracle Cloud Infrastructure DevOps service is a complete continuous integration/continuous delivery (CI/CD) platform for developers to simplify and automate their software development lifecycle. The OCI DevOps service enables developers and operators to collaboratively develop, build, test, and deploy software. Developers and operators get visibility across the full development lifecycle with a history of source commit through build, test, and deploy phases.

Security & IAM

- **IAM** - OCI Identity and Access Management allows controlling who has access to cloud resources.

  OCI IAM provides identity and access management features such as authentication, single sign-on (SSO), and identity lifecycle management for Oracle Cloud as well as Oracle and non-Oracle applications, whether SaaS, cloud-hosted, or on-premises. Employees, business partners, and customers can access applications at any time, from anywhere, and on any device in a secure manner.

  IAM integrates with existing identity stores, external identity providers, and applications across cloud and on-premises to facilitate easy access for end users. It provides the security platform for Oracle Cloud, which allows users to securely and easily access, develop, and deploy business applications such as Oracle Human Capital Management (HCM) and Oracle Sales Cloud, and platform services such as Oracle Java Cloud Service, Oracle Analytics Cloud, and others.

  It can control what type of access a group of users have and to which specific cloud resources. It is a key component of segregating resources and restricting access only to authorised groups and users. OCI IAM, and in fact, OCI as a whole implements a Zero Trust Security model of which one of the guiding principles is least privilege access; in fact, a user by default doesn't have access to any resources and policies need to be created explicitly to grant groups of users access to cloud resources.

3.7.4 Physical Architecture

This section's physical future state architecture serves as the first iteration of the Credit Risk system that might be provisioned in OCI. As a result, the physical future state architecture will be refined in accordance with the customer's low level requirements, and those refinements and the final solution will be detailed in WAD in the future.

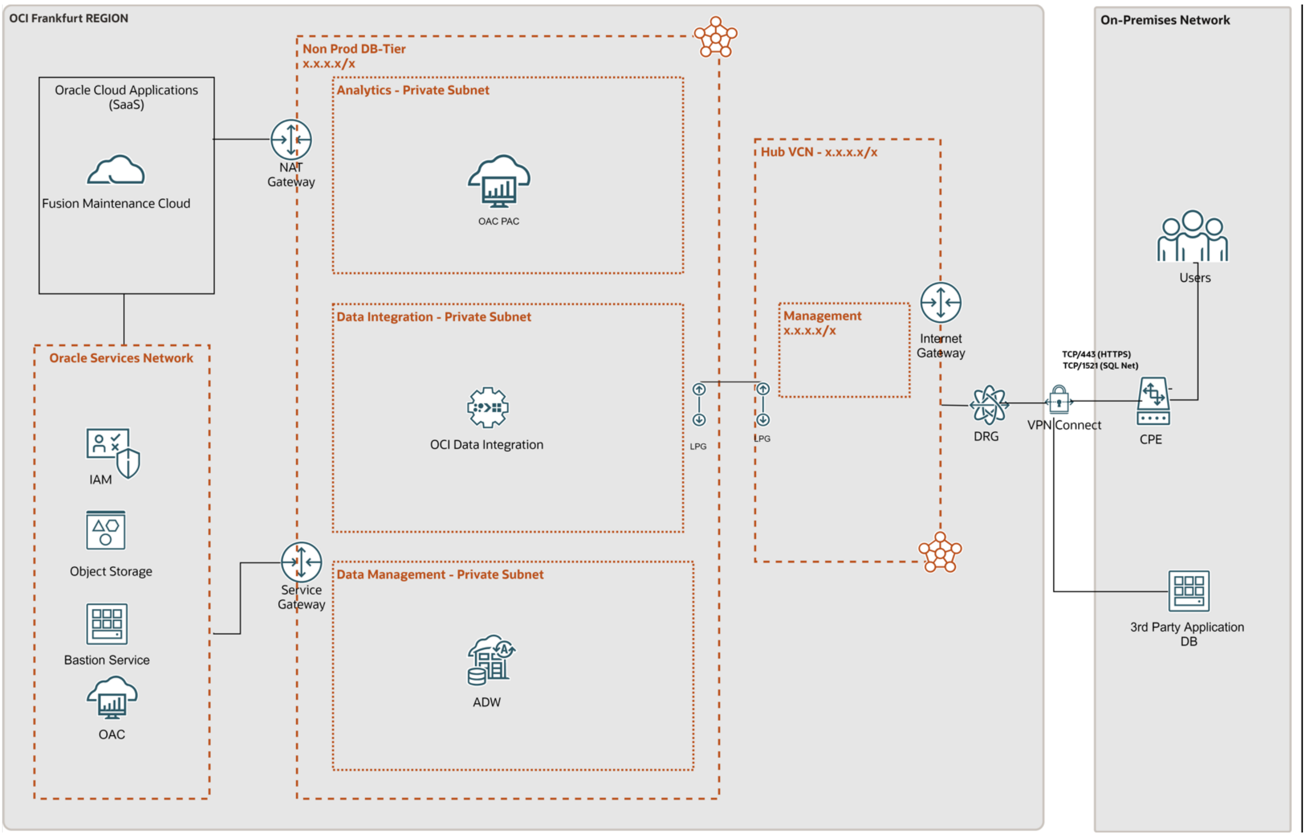

Figure 3: Physical Architecture

- **Oracle Analytics Cloud (OAC)** will be provisioned in a private subnet.
- **Oracle Cloud Analytics Private Access Channel (OAC PAC)** will be used to connect the OAC to the ADW residing in the private subnet.
- **ADW** will be provisioned in the private subnet.
- **OCI Data integration** will be prepared in the private subnet.
- **Data Catalog** will be ready to use when the tenancy is created.
- **Object storage** will be ready to use when the tenancy is created.
- **Monitoring/Logging** tools ready to use to monitor OCI Services and related Logs.
- **OCI IAM Identity Domains** is automatically provided and ready to use at the tenancy level.
- **OCI VCN and Subnets** Lift team will check the existing VCN and subnets and create new ones if needed.
- **Bastion Service** will be used by the Oracle Lift team to have external access to VCNs
- **NAT Gateway** -A NAT gateway enables private resources in a VCN to access hosts on the internet, without exposing those resources to incoming internet connections. It will be used for OCI Data integration and BICC.
- **Dynamic Routing Gateway (DRG)** is the virtual router that secures and manages traffic between on-premises networks and Virtual Cloud Networks (VCN) in Oracle Cloud.
- **Service Gateways** allow private access to Oracle managed services with public IP addresses from on-premises and from VCNs, without exposing the traffic to the public Internet.
- **Virtual Cloud Networks (VCN) and Subnets** will contain private resources like computing instances, database systems, and private endpoints for Oracle managed resources like Autonomous Data Warehouse and Oracle Analytics Cloud.

3.7.4.1 Network Firewall

Optionally a managed Network Firewall can be leveraged to increase security posture of the workload.

OCI Network Firewall is a next-generation managed network firewall and intrusion detection and prevention service for VCNs, powered by Palo Alto Networks. The Network Firewall service offers simple setup and deployment and gives visibility into traffic entering the cloud environment (North-south network traffic) as well traffic between subnets (East-west network traffic).

Use network firewall and its advanced features together with other Oracle Cloud Infrastructure security services to create a layered network security solution.

A network firewall is a highly available and scalable instance that you create in the subnet of your choice. The firewall applies business logic to traffic that is specified in an attached firewall policy. Routing in the VCN is used to direct network traffic to and from the firewall.

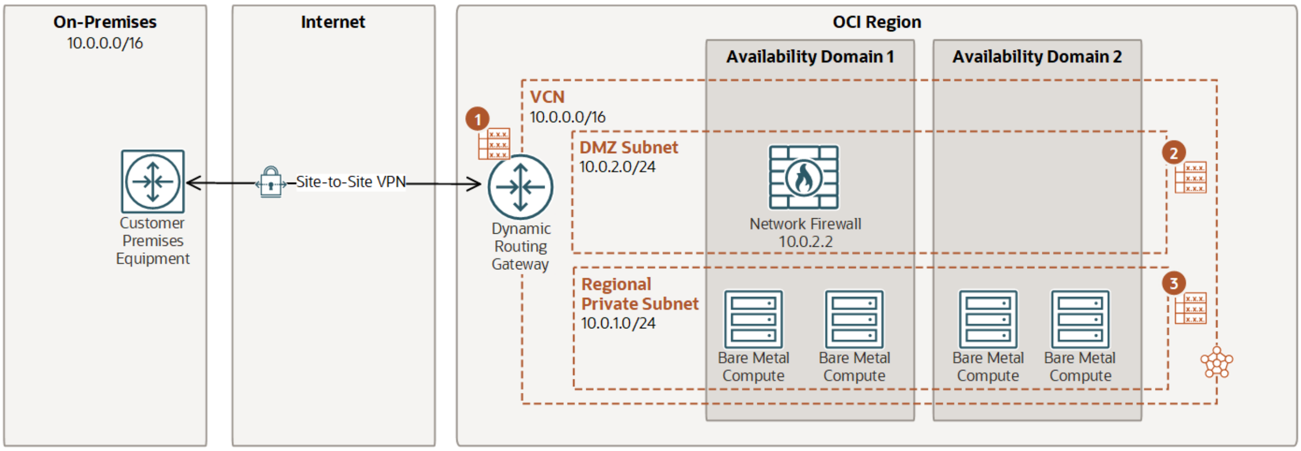

Figure 4: Network Firewall deployment example

Above a simple example is presented where a Network Firewall is deployed in a DMZ subnet and for which all incoming traffic via the DRG as well as all the outgoing traffic from the private subnet is routed to the Network Firewall so that policies are enforced to secure traffic.

3.8 OCI Cloud Landing Zone Architecture

The design considerations for an OCI Cloud Landing Zone have to do with OCI and industry architecture best practices, along with customer specific architecture requirements that reflect the Cloud Strategy (hybrid, multi-cloud, etc). An OCI Cloud Landing zone involves a variety of fundamental aspects that have a broad level of sophistication. A good summary of a Cloud Landing Zone has been published by Cap Gemini.

3.8.1 Resource Naming Convention

Oracle recommends the following Resource Naming Convention:

- The name segments are separated by “-“
- Within a name segment avoid using and “.”
- Where possible intuitive/standard abbreviations should be considered (e.g. “shared“ compared to ”shared.cloud.team”)
- When referring to the compartment full path, use “:” as separator, e.g. cmp-shared:cmp-security

Some examples of naming are given below:

- cmp-shared
- cmp-<workload>
- cmp-networking

The patterns used are these:

- <resource-type>-<environment>-<location>-<purpose>
- <resource-type>-<environment>-<source-location>-<destination-location>-<purpose>
- <resource-type>-<entity/sub-entity>-<environment>-<function/department>-<project>-<custom>
- <resource-type>-<environment>-<location>-<purpose>

Abbreviation per resource type are listed below. This list may not be complete.

Resource type	Abbreviation	Example
Bastion Service	bst	bst-<location>-<network>
Block Volume	blk	blk-<location>-<project>-<purpose>
Compartment	cmp	cmp-shared, cmp-shared-security
Customer Premise Equipment	cpe	cpe-<location>-<destination>
DNS Endpoint Forwarder	dnsepf	dnsepf-<location>
DNS Endpoint Listener	dnsepl	dnsepl-<location>
Dynamic Group	dgp	dpg-security-functions
Dynamic Routing Gateway	drg	drg-prod-<location>
Dynamic Routing Gateway Attachment	drgatt	drgatt-prod-<location>-<source_vcn>-<destination_vcn>
Fast Connect	fc# <# := 1…n>	fc0-<location>-<destination>
File Storage	fss	fss-prod-<location>-<project>
Internet Gateway	igw	igw-dev-<location>-<project>
Jump Server	js	js-<location>-xxxxx
Load Balancer	lb	lb-prod-<location>-<project>
Local Peering Gateway	lpg	lpg-prod-<source_vcn>-<destination_vcn>
NAT Gateway	nat	nat-prod-<location>-<project>
Network Security Group	nsg	nsg-prod-<location>-waf
Managed key	key	key-prod-<location>-<project>-database01
OCI Function Application	fn	fn-security-logs
Object Storage Bucket	bkt	bkt-audit-logs
Policy	pcy	pcy-services, pcy-tc-security-administration
Region Code, Location	xxx	fra, ams, zch # three letter region code
Routing Table	rt	rt-prod-<location>-network
Secret	sec	sec-prod-wls-admin
Security List	sl	sl-<location>
Service Connector Hub	sch	sch-<location>
Service Gateway	sgw	sgw-<location>
Subnet	sn	sn-<location>
Tenancy	tc	tc
Vault	vlt	vlt-<location>
Virtual Cloud Network	vcn	vcn-<location>
Virtual Machine	vm	vm-xxxx

Note: Resource names are limited to 100 characters.

3.8.1.1 Group Names

OCI Group Names should follow the naming scheme of the Enterprise Identity Management system for Groups or Roles.

Examples for global groups are:

- <prefix>-<purpose>-admins
- <prefix>-<purpose>-users

For departmental groups:

- <prefix>-<compartment>-<purpose>-admins
- <prefix>-<compartment>-<purpose>-users

The value for <prefix> or the full names **must be agreed** with customer.

3.8.2 Security and Identity Management

This chapter covers the Security and Identity Management definitions and resources which will be implemented for customer.

3.8.2.1 Universal Security and Identity and Access Management Principles

- Groups will be configured at the tenancy level and access will be governed by policies configured in OCI.
- Any new project deployment in OCI will start with the creation of a new compartment. Compartments follow a hierarchy, and the compartment structure will be decided as per the application requirements.
- It is also proposed to keep any shared resources, such as Object Storage, Networks etc. in a shared services compartment. This will allow the various resources in different compartments to access and use the resources deployed in the shared services compartment and user access can be controlled by policies related to specific resource types and user roles.
- Policies will be configured in OCI to maintain the level of access / control that should exist between resources in different compartments. These will also control user access to the various resources deployed in the tenancy.
- The tenancy will include a pre-provisioned Identity Cloud Service (IDCS) instance (the primary IDCS instance) or, where applicable, the Default Identity Domain. Both provide access management across all Oracle cloud services for IaaS, PaaS and SaaS cloud offerings.
- The primary IDCS or the Default Identity Domain will be used as the access management system for all users administrating (OCI Administrators) the OCI tenant.

3.8.2.2 Authentication and Authorization for OCI

Provisioning of respective OCI administration users will be handled by the customer.

3.8.2.2.1 User Management

Only OCI Administrators are granted access to the OCI Infrastructure. As a good practice, these users are managed within the pre-provisioned and pre-integrated Oracle Identity Cloud Service (primary IDCS) or, where applicable, the OCI Default Identity Domain, of OCI tenancy. These users are members of groups. IDCS Groups can be mapped to OCI groups while Identity Domains groups do not require any mapping. Each mapped group membership will be considered during login.

Local Users

The usage of OCI Local Users is not recommended for the majority of users and is restricted to a few users only. These users include the initial OCI Administrator created during the tenancy setup, and additional emergency administrators.

Local Users are considered as Emergency Administrators and should not be used for daily administration activities!

No additional users are to be, nor should be, configured as local users.

The customer is responsible to manage and maintain local users for emergency use cases.

Federated Users

Unlike Local Users, Federated Users are managed in the Federated or Enterprise User Management system. In the OCI User list Federated Users may be distinguished by a prefix which consists of the name of the federated service in lower case, a '/' character followed by the user name of the federated user, for example:

```
oracleidentityservicecloud/user@example.com
```

In order to provide the same attributes (OCI API Keys, Auth Tokens, Customer Secret Keys, OAuth 2.0 Client Credentials, and SMTP Credentials) for Local and *Federated Users* federation with third-party Identity Providers should only be done in the pre-configured primary IDCS or the Default Identity Domain where applicable.

All users have the same OCI-specific attributes (OCI API Keys, Auth Tokens, Customer Secret Keys, OAuth 2.0 Client Credentials, and SMTP Credentials).

OCI Administration user should only be configured in the pre-configured primary IDCS or the Default Identity Domain where applicable.

Note: Any federated user can be a member of 100 groups only. The OCI Console limits the number of groups in a SAML assertion to 100 groups. User Management in the Enterprise Identity Management system will be handled by the customer.

Authorization

In general, policies hold permissions granted to groups. Policy and Group naming follows the Resource Naming Conventions.

Tenant Level Authorization

The policies and groups defined at the tenant level will provide access to administrators and authorized users, to manage or view resources across the entire tenancy. Tenant level authorization will be granted to tenant administrators only.

These policies follow the recommendations of the CIS Oracle Cloud Infrastructure Foundations Benchmark v1.1.0, recommendations 1.1, 1.2, 1.3.

Service Policy

A Service Policy is used to enable services at the tenancy level. It is not assigned to any group.

Shared Compartment Authorization

Compartment level authorization for the cmp-shared compartment structure uses the following specific policies and groups.

Apart from tenant level authorization, authorization for the cmp-shared compartment provides specific policies and groups. In general, policies will be designed that lower-level compartments are not able to modify resources of higher-level compartments.

Policies for the cmp-shared compartment follow the recommendations of the CIS Oracle Cloud Infrastructure Foundations Benchmark v1.1.0, recommendations 1.1, 1.2, 1.3.

Compartment Level Authorization

Apart from tenant level authorization, compartment level authorization provides compartment structure specific policies and groups. In general, policies will be designed that lower-level compartments are not able to modify resources of higher-level compartments.

Authentication and Authorization for Applications and Databases

Application (including Compute Instances) and Database User management is completely separate of and done outside of the primary IDCS or Default Identity Domain. The management of these users is the sole responsibility of the customer using the application, compute instance and database specific authorization.

3.8.2.3 Security Posture Management

Oracle Cloud Guard

Oracle Cloud Guard Service will be enabled using the pcy-service policy and with the following default configuration. Customization of the Detector and Responder Recipes will result in clones of the default (Oracle Managed) recipes.

Cloud Guard default configuration provides a number of good settings. It is expected that these settings may not match with the customer's requirements.

Targets

In accordance with the CIS Oracle Cloud Infrastructure Foundations Benchmark, v1.1.0, Chapter 3.15, Cloud Guard will be enabled in the root compartment.

Detectors

The Oracle Default Configuration Detector Recipes and Oracle Default Activity Detector Recipes are implemented. To better meet the requirements, the default detectors must be cloned and configured by the customer.

Responder Rules

The default Cloud Guard Responders will be implemented. To better meet the requirements, the default detectors must be cloned and configured by the customer.

Vulnerability Scanning Service

In accordance with the CIS Oracle Cloud Infrastructure Foundations Benchmark, v1.1.0, OCI Vulnerability Scanning will be enabled using the pcy-service policy.

Compute instances which should be scanned *must* implement the *Oracle Cloud Agent* and enable the *Vulnerability Scanning plugin*.

OCI OS Management Service

Required policy statements for OCI OS Management Service are included in the pcy-service policy.

By default, the *OS Management Service Agent plugin* of the *Oracle Cloud Agent* is enabled and running on current Oracle Linux 6 and Oracle Linux 7 platform images.

3.8.2.4 Monitoring, Auditing and Logging

In accordance with the CIS Oracle Cloud Infrastructure Foundations Benchmark, v1.1.0, Chapter 3 Logging and Monitoring the following configurations will be made:

- OCI Audit log retention period set to 365 days. See CIS Oracle Cloud Infrastructure Foundations Benchmark, v1.1.0, Chapter 3.1
- At least one notification topic and subscription to receive monitoring alerts. See CIS Oracle Cloud Infrastructure Foundations Benchmark, v1.1.0, Chapter 3.3
- Notification for Identity Provider changes. See CIS Oracle Cloud Infrastructure Foundations Benchmark, v1.1.0, Chapter 3.4
- Notification for IdP group mapping changes. See CIS Oracle Cloud Infrastructure Foundations Benchmark, v1.1.0, Chapter 3.5
- Notification for IAM policy changes. See CIS Oracle Cloud Infrastructure Foundations Benchmark, v1.1.0, Chapter 3.6
- Notification for IAM group changes. See CIS Oracle Cloud Infrastructure Foundations Benchmark, v1.1.0, Chapter 3.7
- Notification for user changes. See CIS Oracle Cloud Infrastructure Foundations Benchmark, v1.1.0, Chapter 3.8
- Notification for VCN changes. See CIS Oracle Cloud Infrastructure Foundations Benchmark, v1.1.0, Chapter 3.9
- Notification for changes to route tables. See CIS Oracle Cloud Infrastructure Foundations Benchmark, v1.1.0, Chapter 3.10
- Notification for security list changes. See CIS Oracle Cloud Infrastructure Foundations Benchmark, v1.1.0, Chapter 3.11
- Notification for network security group changes. See CIS Oracle Cloud Infrastructure Foundations Benchmark, v1.1.0, Chapter 3.12
- Notification for changes to network gateways. See CIS Oracle Cloud Infrastructure Foundations Benchmark, v1.1.0, Chapter 3.13
- VCN flow logging for all subnets. See CIS Oracle Cloud Infrastructure Foundations Benchmark, v1.1.0, Chapter 3.14
- Write level logging for all Object Storage Buckets. See CIS Oracle Cloud Infrastructure Foundations Benchmark, v1.1.0, Chapter 3.17
- Notification for Cloud Guard detected problems.
- Notification for Cloud Guard remedied problems.

For IDCS or OCI Identity Domain Auditing events, the respective Auditing API can be used to retrieve all required information.

3.8.2.5 Data Encryption

All data will be encrypted at rest and in transit. Encryption keys can be managed by Oracle or the customer and will be implemented for identified resources.

3.8.2.5.1 Key Management

All keys for **OCI Block Volume**, **OCI Container Engine for Kubernetes**, **OCI Database**, **OCI File Storage**, **OCI Object Storage**, and **OCI Streaming** are centrally managed in a shared or a private virtual vault will be implemented and placed in the compartment cmp-security.

Object Storage Security

For Object Storage security the following guidelines are considered.

- **Access to Buckets** -- Assign least privileged access for IAM users and groups to resource types in the object-family (Object Storage Buckets & Object)
- **Encryption at rest** -- All data in the Object Storage is encrypted at rest using AES-256 and is on by default. This cannot be turned off and objects are encrypted with a master encryption key.

Data Residency

It is expected that data will be held in the respective region and additional steps will be taken when exporting the data to other regions to comply with the applicable laws and regulations. This should be review for every project onboard into the tenancy.

3.8.2.6 Operational Security

Security Zones

Whenever possible OCI Security Zones will be used to implement a security compartment for Compute instances or Database resources. For more information on Security Zones refer to the in the *Oracle Cloud Infrastructure User Guide* chapter on Security Zones.

Remote Access to Compute Instances or Private Database Endpoints

To allow remote access to Compute Instances or Private Database Endpoints, the OCI Bastion will be implemented for defined compartments.

To be able to use OCI services to for OS management, Vulnerability Scanning, Bastion Service, etc. it is highly recommended to implement the Oracle Cloud Agent as documented in the *Oracle Cloud Infrastructure User Guide* chapter Managing Plugins with Oracle Cloud Agent.

3.8.2.7 Network Time Protocol Configuration for Compute Instance

Synchronized clocks are a necessity for securely operating environments. OCI provides a Network Time Protocol (NTP) server using the OCI global IP number 169.254.169.254. All compute instances should be configured to use this NTP service.

3.8.2.8 Regulations and Compliance

The customer is responsible for setting the access rules to services and environments that require stakeholders' integration to the tenancy to comply with all applicable regulations. Oracle will support in accomplishing this task.

3.9 Operations

This chapter provides an introduction and collection of useful resources, to relevant topics to operate the solution on Oracle Infrastructure Cloud.

Cloud Operations Topic	Short Summary	References
Cloud Shared Responsibility Model	The shared responsibility model conveys how a cloud service provider is responsible for managing the security of the public cloud while the subscriber of the service is responsible for securing what is in the cloud.	Shared Services Link
Oracle Support Portal	Search Oracle knowledge base and engage communities to learn about products, services, and to find help resolving issues.	Oracle Support Link
Support Management API	Use the Support Management API to manage support requests	API Documentation Link and Other OCI Support Link
OCI Status	Use this link to check the global status of all OCI Cloud Services in all Regions and Availability Domains.	OCI Status Link
Oracle Incident Response	Reflecting the recommended practices in prevalent security standards issued by the International Organization for Standardization (ISO), the United States National Institute of Standards and Technology (NIST), and other industry sources, Oracle has implemented a wide variety of preventive, detective, and corrective security controls with the objective of protecting information assets.	Oracle Incident Response Link
Oracle Cloud Hosting and Delivery Policies	Describe the Oracle Cloud hosting and delivery policies in terms of security, continuity, SLAs, change management, support, and termination.	Oracle Cloud Hosting and Delivery Policies
OCI SLAs	Mission-critical workloads require consistent performance, and the ability to manage, monitor, and modify resources running in the cloud at any time. Only Oracle offers end-to-end SLAs covering performance, availability, manageability of services. This document applies to Oracle PaaS and IaaS Public Cloud Services purchased, and supplements the Oracle Cloud Hosting and Delivery Policies	OCI SLA's and PDF Link

3.10 Roadmap

3.11 Sizing and Bill of Materials

3.11.1 Sizing

The benefit of Oracle Cloud Infrastructure is that services can be set up with a small footprint and can be easily scaled as more use cases and workloads are migrated over to the new architecture. The following represents a Bill of Materials with an OCPU sizing estimates :

Phase	OCI Service	Feature Set	Size	Comment
PROD	Autonomous Data Warehouse	**License Included**	**TBD**	
PROD	Autonomous Data Warehouse-Exadata Storage		**TBD**	
PROD	Oracle Analytics Cloud-Enterprise	**License Included**	**TBD**	

Phase	OCI Service	Feature Set	Size	Comment
PROD	OCI Data Integration - Pipeline Operator Execution		**TBD**	
PROD	OCI Data Integration - GB of Data processed per hour		**TBD**	
PROD	OCI Golden Gate	**License Included**	**TBD**	
PROD	Network Firewall (optional) - B95403		**TBD**	

The sizing defined above is the recommended sizing from Oracle team to accommodate the expected volume of data and meet the scalability of the predicted data processing; since the OCI services can be scaled up and scaled down the customer can always revisit this sizing in the future and adjust it as needed.

- (1) With Autoscaling enabled, ADW will automatically scale to 3x time of base OCPUs. With 1 OCPU, it can scale up to 3 OCPUs. We recommend enabling Autoscaling for production workloads.
- (2) For OAC, 1 OCPU is recommended for Trials only. OAC instances with 1 OCPU are restricted in how many rows they may return (see https://docs.oracle.com/en-us/iaas/analytics-cloud/doc/create-services.html for details.

3.11.2 Bill of Material

3.12 Deployment Build

3.12.1 Phase 1:

3.12.1.1 Compartments

Name	Region	Parent Compartment	Description	Tags
Network			Compartment for all network resources	
Production			Compartment for production application and database tier	

3.12.1.2 Policies

Name	Statements	Region	Compartment	Description	Tags
Network_Admins_Policy	Allow group Network_Admins to manage virtual-network-family in tenancy		Policy for Network_Admins		
Compute_Admins_Policy	Allow group Compute_Admins to manage instance-family in tenancy		Policy for Compute_Admins		
Allow group Compute_Admins to manage compute-management-family in tenancy					
Allow group Compute_Admins to use volume-family in tenancy					
Database_Admins_Policy	Allow group Database_Admins to manage database-family in tenancy		Policy for Database_Admins		

Name	Statements	Region	Compartment	Description	Tags
Allow group Database_Admins to manage buckets in tenancy					
Allow group Database_Admins to use virtual-network-family in tenancy					

3.12.1.3 Groups

Name	Matching Rule	Region	Authentication	Description	Tags
AdminGroup		Frankfurt	IAM	Users that have admin access to network, DB, WLS, user management	

3.12.1.4 Dynamic Group Policies

Name	Policy	Region	Description	Tags
examplepolicy	Allow dynamic-group examplegroup to inspect autonomous-database-family in compartment Production			

3.12.1.5 Tags

Tag Namespace	Namespace Description	Tag Keys	Tag Description	Cost Tracking	Tag Values	Region
Application	Inventory	Environment	Environments Identification	Yes	Production Development Test	Region

3.12.1.6 Users

Name	Email	Group	Description

3.12.1.7 Virtual Cloud Networks

Compartment	VCN Name	CIDR Block	DNS Label	IGW	DRG	NGW	SGW	Region	Tags
Network	examplevcn	10.0.1.0/24	examplevcn					Region	

3.12.1.8 Virtual Cloud Network Information

Property	Value
onprem_destinations	10.0.0.0/16
ngw_destination	0.0.0.0/0
igw_destination	0.0.0.0/0
subnet_name_attach_cidr	n

3.12.1.9 Subnets

Compartment	VCN Name	Subnet Name	CIDR Block	Subnet Span	Type	Security List Name	Route Table Name	Region	Tags
Network	examplevcn	appsubnet	10.0.1.0/25	Regional	Private			Region	
Network	examplevcn	bastionsubnet	10.0.1.128/25	AD1	Public			Region	

3.12.2 Phase 2:

3.12.2.1 DNS Zones

Zone Name	Compartment	Region	Zone Type	Domain	TTL	IP Address	View Name	Tags
PrivateZone	anand.as.singh	zurich	private/public	example.com	300	10.0.0.0/32	privateview	

3.12.2.2 DNS Endpoint

Name	Subnet	Endpoint Type	NSG	IPAddress (Listner/Forwarder)
privateforwarder	subnetname	Listening/Fowarding	nsg	ipaddress

3.12.2.3 Dynamic Routing Gateways Attachment

Name	VCN	Compartment	IPSEC/ Virtual Circuit	Region	Tags
exampledrg	examplevcn	examplecompartment	examplevpn	Region	

3.12.2.4 Route Tables

Name	Table Compartment	Destination CIDR	Target Type	Target Compartment	Target	Region	Description	Tags	VCN Name
exampleroute	Networks	0.0.0.0/0	NAT	Networks	examplenat	Region			

3.12.2.5 Network Security Groups

Name	VCN	Compartment	Region	Description	Tags
examplensg	examplevcn	examplecompartment	Region		

3.12.2.6 NSG Rules (Egress)

NSG Name	Egress Type	Destination	Protocol	Source Port	Dest. Port	Region	Description	Tags
examplensg	Stateful/CIDR	0.0.0.0/0	TCP	all	443	Region		

3.12.2.7 NSG Rules (Ingress)

NSG Name	Ingress Type	Source	Protocol	Source Port	Dest. Port	Region	Description	Tags
examplensg	Stateful/CIDR	0.0.0.0/0	TCP	443	all	Region		

3.12.2.8 Security Lists (Egress)

Name	Compartment	Egress Type	Destination	Protocol	Source Port	Dest. Port	VCN Name	Region	Description	Tags
examplelist	compartment	Stateful/ CIDR	0.0.0.0/0	TCP	all	all		Region		

3.12.2.9 Security Lists (Ingress)

Name	Compartment	Ingress Type	Source	Protocol	Source Port	Dest. Port	VCN Name	Region	Description	Tags
examplelist	compartment	Stateful/ CIDR	0.0.0.0/0	TCP	all	all		Region		

3.12.2.10 Local Peering Gateways

Name	LPG Compartment	Source VCN	Target VCN	Region	Description	Tags
examplelpg	Networks	examplevcn	examplevcn2	Region		
examplelpg2	Networks	examplevcn2	examplevcn	Region		

3.12.2.11 Compute Instances

Compartment	Availability Domain	Name	Fault Domain	Subnet	OS Image	Shape	Backup Policy	Region	NSG	Tags
Production	AD1	ebsinstance	FD1	appsubnet	Oracle Linux 7.9	VM.Standard2		Region		
Development	AD2	bastion	FD3	bastionsubnet	Oracle Linux 7.9	VM.Standard. E3.Flex::2		Region		

3.12.2.12 Block Volumes

Compartment	Name	Size (in GB)	Availability Domain	Attached to Instance	Backup Policy	Region	Tags
Production	ebsinstance-blkvol01	500	AD1	ebsinstance	Gold	Region	

Compartment	Name	Size (in GB)	Availability Domain	Attached to Instance	Backup Policy	Region	Tags
Development	bastion-blkvol01	100	AD2	bastion	None	Region	

3.12.2.13 Object Storage Buckets

Compartment	Bucket	Visibility	Region	Description	Tags
Development	devebsbucket	Private	Region		

3.12.2.14 File Storage

Compartment	Availability Domain	Mount Target Name	Mount Target Subnet	FSS Name	Path	IP Whitelist	Region	NSG	Tags
Production	AD1	prdebsmt	appsubnet	prodebsfss	/prodebsfss	10.0.1.0/25	Region		

3.12.2.15 Load Balancers

Compartment	LB Name	Shape	Subnet	Visibility	Hostnames	NSG	Region	Tags
Network	prdebslb	100Mbps	appsubnet	Private	www.example.co ebs.application.c	Region		

3.12.2.15.1 Backend Sets

LB Name	Backend Set Name	Backend Server Port	Backend Policy	SSL	Region	Tags	HC Protocol	HC Port
prdebslb	prdebsbs	ebsinstance1:800 ebsinstance2:8005	Round Robin	No	Region			

3.12.2.15.2 Listeners

LB Name	Backend Set Name	Hostname	SSL	Listener Name	Protocol	Port	Region
prdebslb	prdebsbs	ebs.application.com	Yes	Listener1	HTTP	443	Region

3.12.2.16 Databases

3.12.2.16.1 DBSystem Info

Region	Compartment	Display Name	Shape	Total Node Count	DB Software Edition	DB Size (TB)	DB Disk Redundancy	Tags
amsterdam	network	devdb	VMStandard/ BMStandard/ Exa	1	Enterprise Edition	256	Normal/ High	

3.12.2.16.2 DBSystem Network

Display Name	Hostname Prefix	Subnet Name	Availability Domain	License Type	Time Zone
devdb	dbhost	db-sl	AD1	License Included/ Bring your own license	UTC

3.12.2.16.3 Database

Display Name	PDB Name	Workload Type	Database Name	Database Version	Character Set	ncharacter Set
devdb		OLTP/DSS	Testdb	19c		

3.12.2.17 Autonomous Databases

3.12.2.17.1 Autonomous Database Information

Compartment	Display Name	DB Name	Workload Type	Infra. Type	DB Version	OCPU Count	Storage (TB)	Region	Tags
compartment	dbsystem	db	ADW/ ATP	Shared/ Dedicated	19c	2	1	Region	Tags

3.12.2.17.2 Automation Database Network

Display Name	Auto Scaling	Network Access	Access Control Rules	Subnet Name	License Type	NSG
dbsystem	Yes/ No	Shared only	Shared/ Secure Access only	Shared only	network	BYOL/ Included

3.12.2.18 Key Management System Vaults

Compartment	Name	Type	Region	Description	Tags
A	B	Virtual private	Region		
A	B	Non virtual private	Region		

3.12.2.19 Key Management System Keys

Compartment	Protection Mode	Name	Key Algorithm	Key Length
A	Software	X	AES	128 bits
B	HSM	C	RSA	256 bits

GLOSSARY

You can learn about Oracle Cloud Infrastructure terms and concepts in this glossary. Further terms, product names or concepts are described below in each subsection.

4.1 2-Factor Authentication

A second verification factor is required each time that a user signs in. Users can't sign in using just their user name and password.

For more information please visit our documentation for Administering Oracle identity Cloud.

4.2 Other

~~~~
~~~~