Document Control

Version Control

Version	Author	Date	Comment

Team

Name	eMail	Role	Company

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 'Oracle Lift' project scope and timeline. The Lift parts 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 as it will be done as part of the Oracle Lift service.

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. In some cases Oracle offers a free implementation service called 'Oracle Lift', which has its own dedicated scope and is typically a subset of the initial Workload. The Lift project, architecture and implementation details are documented in chapter Oracle Lift Project and Architecture and in chapter Oracle Lift Implementation.

Business Context

Executive Summary

XYZ has chosen Oracle as their preferred partner to support their technology and cloud journey in order to support overall smart city objectives.

Workload Business Value

XYZ is looking at running the Outsystem in Oracle Infrastructure Cloud (OCI) that would allow :

- Being able to run the application environment in a data center within the country to comply with the regulations

- Cost effectiveness of the solution on OCI to run and expand when the load and the requirements change
- protect the application environment through OCI-provided Web Application Firewall capability

Workload Requirements and Architecture

Overview

XYZ would like to host the application in OCI in XYZ region to comply with the regulations.

Non Functional Requirements

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

Regulations and Compliances

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

Environments

Name	Size of Prod	Location	MAA	Scope
Production	100%	XYZ	Gold	Workload - Lift
Lifetime	N/A	XYZ	Gold	Workload - Lift
Test	N/A	XYZ	Gold	Workload - Lift
Dev	N/A	XYZ	Gold	Workload - Lift

Resilience and Recovery

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

Security

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

Logical Future State Architecture

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

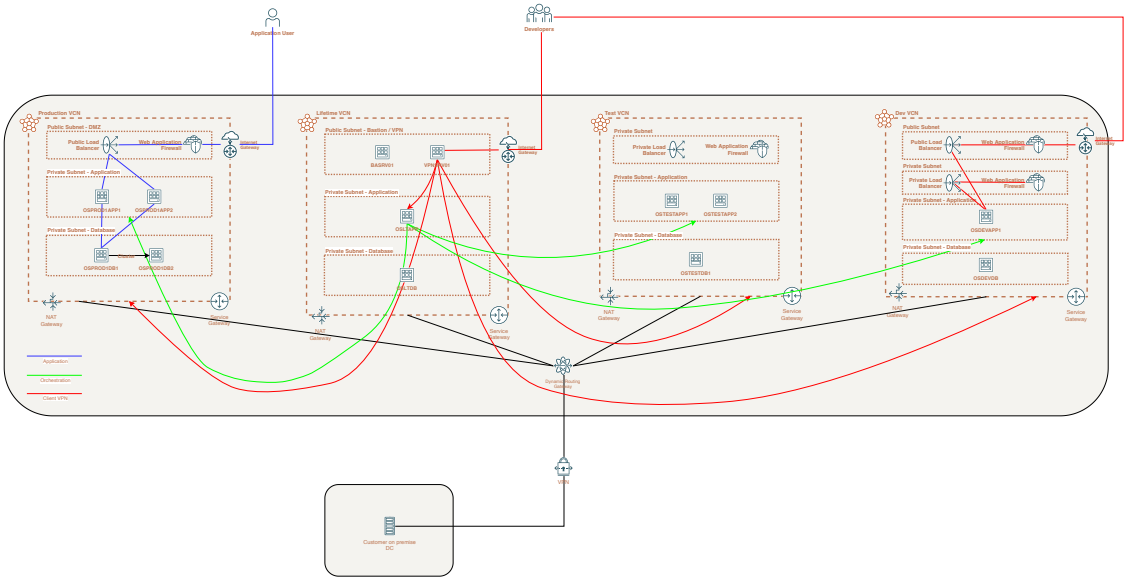

Figure 1: Future State Architecture

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.

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>

Resource type	Abbreviation	Example
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.

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.

Security and Identity Management

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

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.

Authentication and Authorization for OCI Provisioning of respective OCI administration users will be handled by the customer.

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.

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.

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.

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.

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.

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.

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.

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.

Sizing and Bill of Materials

Sizing

Environment	Server	OCPU	Memory	Disk	Operating System	Application
Production	OS-PROD1APP1	2	8 GB	350 GB	Microsoft Windows Server 2019 Standard	Microsoft Internet Information Services
Production	OS-PROD1APP2	2	8 GB	350 GB	Microsoft Windows Server 2019 Standard	Microsoft Internet Information Services
Production	OS-PROD1DB1	2	16 GB	TBD GB	Microsoft Windows Server 2019 Standard	Microsoft SQL Server 2019 Enterprise
Production	OS-PROD1DB2	2	16 GB	TBD GB	Microsoft Windows Server 2019 Standard	Microsoft SQL Server 2019 Enterprise

Environment	Server	OCPU	Memory	Disk	Operating System	Application
Lifetime	BASRV01	2	8 GB	150 GB	Microsoft Windows Server 2019 Standard	Terminal Server
Lifetime	VPN-SRV01	1	15 GB	50 GB	OpenVPN Access Server (Linux)	OpenVPN Marketplace Image
Lifetime	OSLTAPP	2	12 GB	150 GB	Microsoft Windows Server 2019 Standard	Microsoft Internet Information Services
Lifetime	OSLTDB	2	8 GB	TBD GB	Microsoft Windows Server 2019 Standard	Microsoft SQL Server 2019 Standard
Test	OS-TESTAPP1	2	8 GB	500 GB	Microsoft Windows Server 2019 Standard	Microsoft Internet Information Services
Test	OS-TESTAPP2	2	8 GB	500 GB	Microsoft Windows Server 2019 Standard	Microsoft Internet Information Services
Test	OS-TESTDB1	2	16 GB	TBD GB	Microsoft Windows Server 2019 Standard	Microsoft SQL Server 2019 Standard
Dev	OSDE-VAPP1	4	12 GB	250 GB	Microsoft Windows Server 2019 Standard	Microsoft Internet Information Services
Dev	OSDE-VDB	2	8 GB	TBD GB	Microsoft Windows Server 2019 Standard	Microsoft SQL Server 2019 Standard

Bill of Materials