

Solution Definition

Copyright © 2023, Oracle and/or its affiliates

ACME

Siebel to OCI

4th of September 2023 | Version 2

Contents

[1 Document Control 4](#_Toc145323605)

[1.1 Version Control 4](#_Toc145323606)

[1.2 Team 4](#_Toc145323607)

[1.3 Document Purpose 4](#_Toc145323608)

[2 Business Context 5](#_Toc145323609)

[2.1 Executive Summary 5](#_Toc145323610)

[2.2 Workload Business Value 5](#_Toc145323611)

[3 Workload Requirements and Architecture 6](#_Toc145323612)

[3.1 Overview 6](#_Toc145323613)

[3.2 Non-Functional Requirements 6](#_Toc145323614)

[3.2.1 Regulations and Compliances Requirements 7](#_Toc145323615)

[3.2.2 Environments 7](#_Toc145323616)

[3.2.3 High Availability and Disaster Recovery Requirements 7](#_Toc145323617)

[3.2.4 Security Requirements 8](#_Toc145323618)

[3.2.5 Networking Requirements 8](#_Toc145323619)

[3.3 Current State Architecture 9](#_Toc145323620)

[3.4 Future State Architecture 11](#_Toc145323621)

[3.4.1 Mandatory Security Best Practices 11](#_Toc145323622)

[3.4.2 OCI Secure Landing Zone Architecture 13](#_Toc145323623)

[3.4.3 Physical Architecture 19](#_Toc145323624)

[3.5 Solution Considerations 24](#_Toc145323625)

[3.5.1 High Availability and Disaster Recovery 24](#_Toc145323626)

[3.5.2 Security 24](#_Toc145323627)

[3.5.3 Networking 24](#_Toc145323628)

[3.6 Sizing and Bill of Materials 25](#_Toc145323629)

[3.7 Siebel Migration and Upgrade 25](#_Toc145323630)

[4 Annex 27](#_Toc145323631)

[4.1 Security Guidelines 27](#_Toc145323632)

[4.1.1 Oracle Security, Identity, and Compliance 27](#_Toc145323633)

[4.1.2 Compliance and Regulations 27](#_Toc145323634)

[4.2 Additional Resources 27](#_Toc145323635)

[4.3 Networking Requirement Considerations 27](#_Toc145323636)

[4.3.1 Application Connectivity 28](#_Toc145323637)

[4.3.2 DR and Business Continuity 28](#_Toc145323638)

[4.3.3 High Availability and Scalability 28](#_Toc145323639)

[4.3.4 Security and Access Control 28](#_Toc145323640)

[4.3.5 Monitoring and Troubleshooting 28](#_Toc145323641)

[4.4 Networking Solutions 29](#_Toc145323642)

[4.4.1 OCI Network Firewall 29](#_Toc145323643)

[4.4.2 OCI Load Balancer 29](#_Toc145323644)

[4.4.3 OCI DNS Traffic Management 29](#_Toc145323645)

[4.4.4 OCI WAF 29](#_Toc145323646)

[4.4.5 OCI IGW 29](#_Toc145323647)

[4.4.6 OCI Site-to-Site VPN 29](#_Toc145323648)

[4.4.7 OCI Fast Connect 29](#_Toc145323649)

[4.4.8 OCI VTAP 30](#_Toc145323650)

[4.4.9 OCI NPA 30](#_Toc145323651)

[4.4.10 OCI DRG (Connectivity Options) 30](#_Toc145323652)

[4.4.11 OCI Oracle Cloud Infrastructure Certificates 30](#_Toc145323653)

[4.4.12 OCI Monitoring 30](#_Toc145323654)

*Guide:*

*Author Responsibility*

* *Chapter 1-3: Sales Consultant*

# Document Control

*Guide:*

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

## Version Control

*Guide:*

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

*Example:*

| Version | Authors | Date | Comments |
| --- | --- | --- | --- |
| 1.0 | Name Surname | 1st June 2023 | Created a new Solution Definition document. To be used for iterative review and improvement. |
| 1.1 | Name Surname | 1st July 2023 | Update Template per feedback. Added security-templated texts and annex. |

## 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 |

## Document Purpose

*Guide:*

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

*Example:*

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

The document may refer to a ‘Workload’, which summarizes the full technical solution for a customer (You) during a single engagement. The Workload is described in the chapter [Workload Requirements and Architecture](#workload-requirements-and-architecture).

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

# Business Context

*Guide:*

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

<Customer Name> is a <Industry Name> company operating in <Country Name> and on the international markets, providing services to consumers, businesses and the public sector.

Oracle Siebel is the strategic platform for B2B/B2C sales and marketing activities called "XYZ". Siebel implementation has performance issues with the Remote Product Configurator. Assessment has been done by ACS to perform some configuration changes.

## 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.*

Oracle Cloud Infrastructure (OCI) was designed specifically to support workloads like Siebel. By further migrating <Customer Name> Siebel workload to more OCI services it will allow them to enjoy improved efficiency, cost savings, and performance gains compared to on-premises deployments and other Cloud vendors, along with the elasticity and agility of the Cloud.

## 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".*

The workload addresses the following key concerns:

1. Improve Siebel Performance and response time leveraging a modern cloud infrastructure.
2. Ensure that the Siebel application can scale up to the real time transaction processing volume.
3. Leverage OCI capabilities such as auto-scaling & enhance infrastructure availability, security and resilience.
4. Environment consistency/availability and rapid in-place technology refreshes, patching and updates.

There is an opportunity for the Oracle Cloud Infrastructure to help assist and support this transition to a new environment by providing additional deployment options. The advantages of using the Oracle Cloud include:

* Resolution of performance issues on existing on-premise deployment.
* Considerable reduction in the time it takes to provision new environments on the existing infrastructure.
* Potential cost savings in moving to the Oracle Cloud.
* Ability to utilize existing Oracle Cloud Credits.
* Availability of multiple different compute shapes that can be used to provide maximum performance at the lowest cost.
* Option to fine tune consumption e.g. by shutting-down non-production environments when not needed such as evenings and weekends.

More business value Examples:

* Siebel database tier will be using a long term supported database and might even leverage Autonomous Database
* Siebel application tier will benefit from the "pay as you go" UCM model
* Siebel application will benefit from the Siebel architecture on OCI leveraging the Siebel Cloud Manager and docker containers
* Automation may be put in place for environments creation, Siebel updates and DevOps
* OCI cost monitoring will be available for use for the complete Siebel environment
* Moving Siebel to OCI may be conducive to broader data centre exit initiatives

The success implementation of this project is to:

1. Deliver Oracle Siebel CRM running on OCI in the specified architecture for the "Stress Testing Environment".
2. Deliver the specified environments in such a way that <Customer Name> on-premise applications and other third party systems can be successfully and integrated.
3. Deliver the To-Be architecture with the Terraform scripts to be used for other environments.

# Workload Requirements and Architecture

## Overview

*Guide:*

*Describe the Workload: What applications and environments are part of this Workload migration or new implementation project, and what are their names? The implementation will be scoped later and can be a subset of the Solution Definition and proposed overall solution. 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 later in a dedicated chapter*

The SIEBEL workload described in this document documents an Oracle Cloud Infrastructure (OCI) solution which replicates <Customer Name> existing on-premises Oracle Siebel implementation.

describe other features of the customer workload - example areas:

* Customization complexity, java, siebel tools...etc.
* Application modules - Siebel Loyalty, Siebel Smart Answers etc.
* Connectivity - on-premises, Internet
* Disaster Recovery

## 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.*

### Regulations and Compliances Requirements

*Guide:*

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

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

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

*Example:*

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

In addition to these requirements, the [CIS Oracle Cloud Infrastructure Foundation Benchmark, v1.2](https://www.cisecurity.org/benchmark/Oracle_Cloud) will be applied to the Customer tenancy.

### Environments

*Guide:*

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

<Customer Name> Siebel version environments, Example:

| Name | Size of Prod | Location | DR | Scope |
| --- | --- | --- | --- | --- |
| Production | 100% | Malaga | Yes | Not in Scope / On-prem |
| DR | 50% | Sevilla | No | Workload |
| Dev & Test | 25% | Sevilla | No | Workload - <Service Provider> |

### 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.

### 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.

### Networking Requirements

*Guide*

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

*Example:*

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

## Current State Architecture

*Guide:*

*Provide a high-level logical description of the Workload current state. Stay in the Workload scope, show potential integrations, but do not try to create a full customer landscape. Use architecture diagrams to visualize the current state. We recommend not putting lists of technical resources or dependencies here. Refer to attachments instead.*

* Logical representation of the current Siebel estate architecture in the scope of business needs and current IT estate. Usually showing business flows and capabilities with high-level data flows and user interactions
* Include a diagram using the logical architecture notation or any on-premises architecture artifacts provided by Customer

A diagram of a server

Description automatically generated

* Include any available diagrams such as current networking architecture.
* Current Siebel environment details (current Production and non-Production environments)

Description of the current Siebel environment

* Integration (with SaaS, other 3rd party applications like Genesys, Billing, core banking)
* Authentication (SSO, interface with Oracle Access Manager, LDAP like OID or Microsoft AD etc)
* Shared File System with other environments if any (with other non-production environment or 3rd party applications)

A red line on a white sheet

Description automatically generated

The following information should have been collected via the Discovery Questionnaire. Example:

Database Tier:

* Database Version: 12.1.0.2.0
* Source Operating System Version and Release: Oracle Linux Server release 7.9
* Database size (in GB): 280
* DB Character set on source: AL32UTF8
* Oracle RAC configured: No
* Disaster recover plan/solution in place? No

Siebel Application Tier:

* Oracle Siebel Version: IP15
* Source Operating System Version and Release: Oracle Linux Server release 7.9
* Number of application nodes: Single Node
* What languages other than English are installed on Siebel, if any? None
* Load balancer implemented ? Yes, F5
* DMZ setup or any external tiers: No
* Single Sign On implemented: No
* SSL implemented: Yes, terminated at F5 load balancer
* Siebel is integrated with any other Oracle Products like OBIEE/SOA/IDM...etc.

## 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.*

A diagram of a computer

Description automatically generated

### 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.

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

### OCI Secure Landing Zone Architecture

*Guide:*

*This chapter describes landing zone best practices and usually does not require any changes. If changes are required please refer to* [*Landing Zone GitHub*](https://github.com/oracle-devrel/technology-engineering/tree/main/landing-zones)*. The full landing zone needs to be described in the Solution Design by the service provider.*

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

The design considerations for an OCI Cloud Landing Zone have to do with OCI and industry architecture best practices, along with <Customer Name> 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 in the [OCI User Guide](https://docs.oracle.com/en-us/iaas/Content/cloud-adoption-framework/landing-zone.htm).

#### Naming Convention

A naming convention is an important part of any deployment to ensure consistency as well as security within your tenancy. Hence we jointly agree on a naming convention, that matches Oracle's best practices and <Customer Name> requirements.

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 a 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>

Abbreviations 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 |

#### Security and Identity Management

This chapter covers the Security and Identity Management definitions and resources that will be implemented for <Customer Name>.

##### 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

The provisioning of respective OCI administration users will be handled by <Customer Name>.

###### 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 Emergency Administrators and should not be used for daily administration activities!**

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

**<Customer Name> 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 that 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

Providing 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 users 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 <Customer Name>.

**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. The tenant-level authorization will be granted to tenant administrators only.

These policies follow the recommendations of the [CIS Oracle Cloud Infrastructure Foundations Benchmark v1.2.0, recommendations 1.1, 1.2, 1.3](https://www.cisecurity.org/cis-benchmarks).

**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 so that lower-level compartments are not able to modify the resources of higher-level compartments.

Policies for the cmp-shared compartment follow the recommendations of the [CIS Oracle Cloud Infrastructure Foundations Benchmark v1.2.0, recommendations 1.1, 1.2, 1.3](https://www.cisecurity.org/cis-benchmarks).

**Compartment Level Authorization**

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

**Authentication and Authorization for Applications and Databases**

Application (including Compute Instances) and Database User management are completely separate and done outside of the primary IDCS or Default Identity Domain. The management of these users is the sole responsibility of <Customer Name> 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 <Customer Name>'s requirements.

**Targets**

In accordance with the [CIS Oracle Cloud Infrastructure Foundations Benchmark, v1.2.0, Chapter 3.15](https://www.cisecurity.org/cis-benchmarks), 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 <Customer Name>.

**Responder Rules**

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

**Vulnerability Scanning Service**

In accordance with the [CIS Oracle Cloud Infrastructure Foundations Benchmark, v1.2.0, OCI Vulnerability Scanning](https://www.cisecurity.org/cis-benchmarks) will be enabled using the pcy-service policy.

Compute instances that 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, 7, 8, and 9 platform images.

##### Monitoring, Auditing, and Logging

In accordance with the [CIS Oracle Cloud Infrastructure Foundations Benchmark, v1.2.0, Chapter 3 Logging and Monitoring](https://www.cisecurity.org/cis-benchmarks) the following configurations will be made:

* OCI Audit log retention period set to 365 days.
* At least one notification topic and subscription to receive monitoring alerts.
* Notification for Identity Provider changes.
* Notification for IdP group mapping changes.
* Notification for IAM policy changes.
* Notification for IAM group changes.
* Notification for user changes.
* Notification for VCN changes.
* Notification for changes to route tables.
* Notification for security list changes.
* Notification for network security group changes.
* Notification for changes to network gateways.
* VCN flow logging for all subnets.
* Write level logging for all Object Storage Buckets.
* 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 reviewed 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 *Oracle Cloud Infrastructure User Guide* chapter on [Security Zones](https://docs.oracle.com/en-us/iaas/security-zone/using/security-zones.htm).

**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 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](https://docs.oracle.com/en-us/iaas/Content/Compute/Tasks/manage-plugins.htm).

##### 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

<Customer Name> is responsible for setting the access rules to services and environments that require stakeholders’ integration into the tenancy to comply with all applicable regulations. Oracle will support in accomplishing this task.

### 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 as 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*](https://docs.oracle.com/en-us/iaas/Content/General/Reference/graphicsfordiagrams.htm)

*Reference:*

[StarterPacks (use the search)](https://github.com/oracle-devrel/technology-engineering/)

*Example:*

A screenshot of a computer

Description automatically generated

A diagram of a diagram

Description automatically generated

Physical Architecture Siebel on OCI (IP16 or earlier)

A diagram of a computer

Description automatically generated

Physical Architecture Siebel on OCI HA (IP16 or earlier)

A diagram of a computer

Description automatically generated

Physical Architecture Siebel on OCI (IP17 or later)

A screenshot of a diagram

Description automatically generated

Physical Architecture Siebel on OCI DR (IP17 or later)

A diagram of a computer program

Description automatically generated

Physical Architecture Siebel on OCI HADR (IP17 or later)

## 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?*

### High Availability and Disaster Recovery

*Reference:* [Learn about deploying Siebel CRM on Oracle Cloud Infrastructure](https://docs.oracle.com/en/solutions/learn-architecture-deploy-siebel/index.html#GUID-B1AF5BE2-7BB9-402A-A57C-5E9AE752244D)

### 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](#security-guidelines).

### Networking

*Reference:*

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

## 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 okay to make assumptions and to clearly state them!*

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

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

A screenshot of a computer screen

Description automatically generated

|  |  |  |
| --- | --- | --- |
| Component | Qty | Note |
| Virtual Cloud Network | 3 | Stress Testing Environment |
| Subnets | 6 | 1 x Siebel Tools, 1 regional x LBaaS, 1 x web tier, 1 x Application/GW tier, 1 x DB tier , 1 Palo Alto VM Series |
| Bastion Service | 1 | 1 x Bastion Service for remote access |
| Load Balancer | 1 x Siebel LBaaS | 400 Mbps SSL Offloading/Termination |
| Service Gateway | 1 | Connect to object storage for backups |
| NAT gateway | 1 | Outbound WWW connectivity |
| Exadata Cloud Services | 2 | RAC |
| Web servers | 4 | VM.Standard.E4.Flex |
| Gateway server | 1 | VM.Standard.E4.Flex |
| Application Servers | 9 | VM.Standard.E4.Flex |

## Siebel Migration and Upgrade

**Use Case 1: Customers on Siebel CRM IP2017 onwards**

1. Target Upgrade update is Siebel Siebel 23.x
2. Neither an Incremental Repository Merge nor a Database Upgrade is required for Siebel CRM 17.0 or later)
3. Quick Provisioning (available now on Oracle Marketplace).
4. Lift and Shift tooling:
   1. Clone existing instances to the Oracle Cloud
   2. Install "Monthly updates" to the cloned copy.
   3. Test changes, etc.
   4. Apply changes to Non-Production.

**Use Case 2: Customers on Siebel CRM IP2015 or IP2016**

1. Target Upgrade update is Siebel 23.x
2. Quick Provisioning (available now on Oracle Marketplace)
3. Lift and Shift tooling:
   1. Clone existing instances to the Oracle Cloud
   2. Use Siebel IRM to apply customer changes to cloned copy (**two Step migration**: IP17 and then Siebel 21)
   3. Test changes, etc.
   4. Apply changes to Production

**Use Case 3: Customers on Sustaining or Extended support release (7.5, 7.7, 7.8, 8.0, 8.1, 8.1)**

1. Option 1: Migrate your application into Partner/Oracle Managed Cloud Service (OMCS) Hosting
2. Option 2: Upgrade to Siebel 20.x using Partner/OMCS upgrade services
   1. Target Upgrade update is Siebel Siebel 23.x
   2. New or Migration installation of Siebel 23.x
   3. Single-Step or Two-Step Repository Upgrade based on the current version
   4. Full Database Upgrade or IRM based on the current version

The following decision tree covers upgrade procedures for all Siebel versions.

A diagram of a flowchart

Description automatically generated

# Annex

## Security Guidelines

### Oracle Security, Identity, and Compliance

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

* [Security Strategy](https://docs.oracle.com/en-us/iaas/Content/cloud-adoption-framework/security-strategy.htm) – To create a successful security strategy and architecture for your deployments on OCI, it's helpful to understand Oracle's security principles and the OCI security services landscape.
* The [security pillar capabilities](https://docs.oracle.com/en-us/iaas/Content/cloud-adoption-framework/security.htm#capabilities) reflect fundamental security principles for architecture, deployment, and maintenance. The best practices in the security pillar, help your organization to define a secure cloud architecture, identify and implement the right security controls, and monitor and prevent issues such as configuration drift.

#### References

* The Best Practices Framework for OCI provides architectural guidance about how to build OCI services in a secure fashion, based on recommendations in the [Best practices framework for Oracle Cloud Infrastructure](https://docs.oracle.com/en/solutions/oci-best-practices).
* Learn more about [Oracle Cloud Security Practices](https://www.oracle.com/corporate/security-practices/cloud/).
* For detailed information about security responsibilities in Oracle Cloud Infrastructure, see the [Oracle Cloud Infrastructure Security Guide](https://docs.oracle.com/iaas/Content/Security/Concepts/security_guide.htm).

### Compliance and Regulations

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

## Additional Resources

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

## Networking Requirement Considerations

The below questions help to identify networking requirements.

### Application Connectivity

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

### DR and Business Continuity

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

### High Availability and Scalability

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

### Security and Access Control

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

### Monitoring and Troubleshooting

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

## Networking Solutions

### OCI Network Firewall

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

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

### OCI Load Balancer

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

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

### OCI DNS Traffic Management

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

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

### OCI WAF

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

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

### OCI IGW

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

* [Managing IGW](https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/managingIGs.htm)

### OCI Site-to-Site VPN

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

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

### OCI Fast Connect

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

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

### OCI VTAP

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

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

### OCI NPA

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

* [Path Analyzer](https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/path_analyzer.htm)

### OCI DRG (Connectivity Options)

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

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

### OCI Oracle Cloud Infrastructure Certificates

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

* [SSL TLS Certificates](https://www.oracle.com/security/cloud-security/ssl-tls-certificates/)

### OCI Monitoring

You can monitor the health, capacity, and performance of your Oracle Cloud Infrastructure resources by using metrics, alarms, and notifications. For more information, see [Monitoring](https://docs.oracle.com/iaas/Content/Monitoring/home.htm) and [Notifications](https://docs.oracle.com/en-us/iaas/Content/Notification/home.htm#top).

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