ORACLE

# MS SQL Server Always ON
# An architecture example in OCI

Solution Definition

9 August 2023 | Version 1.0

# Contents

# Document Control

*Guide:*

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

## 1.1 Version Control

*Guide:*

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

*Example:*

| Version | Authors | Date | Comments |
|---|---|---|---|
| 1.0 | Alessandro Volpi | 27 July 2023 | Document Creation |

## 1.2 Team

*Guide:*

*A section describing the Oracle team.*

*Example:*

| Name | Role | Company |
|---|---|---|
| Name Surname | Job title | Company |

### 1.3 Abbreviations and Acronyms (Optional)

*Guide:*

*If needed, maintain a list of:*

- *Abbreviation: a shortened form of a word or phrase.*
- *Acronyms: an abbreviation formed from the initial letters of other words and pronounced as a word (e.g. ASCII, NASA ).*

*Example:*

| Term | Meaning |
|---|---|
| AD | Availability Domain |
| Dev | Development |
| DRG | Dynamic Routing Gateway |
| DWH | Data Warehouse |
| IaaS | Infrastructure as a Service |
| LB | Load Balancer |
| NSG | Network Security Group |
| OCI | Oracle Cloud Infrastructure |
| VCN | Virtual Cloud Network |

### 1.4 Document Purpose

*Guide:*

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

*Example:*

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

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

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

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

## Business Context

*Guide:*

*Describe the customer's business and background. What is the context of the customer's industry and LoB? What are the business needs and goals which this Workload is an enabler for? How does this technical solution impact and support the*

*customer's business goals? Does this solution support a specific customer strategy, or maybe certain customer values? How does this solution help our customers to either generate more revenue or save costs?*

## 2.1 Executive Summary

*Guide:*

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

## 2.2 Workload Business Value

*Guide:*

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

# Workload Requirements and Architecture

## 3.1 Overview

*Guide:*

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

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

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

## 3.2 Functional Requirements (Optional)

*Guide:*

*Provide a brief overview of the functional requirements, the functional area they belong to, the impacted business processes, etc.*

*Provide a formal description of the requirements as 1. a set of Use Cases or 2. a description of Functional Capabilities or 3. a Requirement Matrix. The three descriptions are not mutually exclusive.*

*Some Workload teams, especially the Analytics and Merging Tech teams, will create new applications based on functional requirements, some Workload teams will not touch the functional requirements at all and just change the platform under an application. But it is important to understand who is using the system and for what reason.*

### 3.2.1 Use Cases (Optional)

*Guide:*

*A Use Case (UC) can be represented in a table as the following one. See https://www.visual-paradigm.com/guide/use-case/what-is-use-case-specification/ for a quick introduction to the concept of UC. See https://www.usability.gov/how-to-and-tools/methods/use-cases.html for more examples and detailed instructions.*

*Example:*

| Element | Description |
|---|---|
| Use Case 1 | Housekeeper does laundry |
| Stakeholder | Owner |
| Actor | Housekeeper |
| Use Case Overview | It is Wednesday and there is laundry in the laundry room. The housekeeper sorts it, then proceeds to launder each load. The housekeeper folds the dry laundry as he/she removes it from the dryer. The housekeeper irons those items that need ironing. |
| Precondition 1 | It is Wednesday |
| Precondition 2 | There is laundry in the laundry room. |
| Trigger | Dirty laundry is transported to the laundry room on Wednesday. |

| Element | Description |
|---|---|
| Basic Flow | On Wednesdays, the housekeeper reports to the laundry room. The housekeeper sorts the laundry that is there. Then he/she washes each load. The housekeeper dries each load. He/She folds the items that need folding. He/She irons and hangs the wrinkled items. The housekeeper throws away any laundry item that is irrevocably shrunken, soiled, or scorched. |
| Alternative Flow 1 | If he/she notices that something is wrinkled, he/she irons it and then hangs it on a hanger. |
| Alternative Flow 2 | If he/she notices that something is still dirty, he/she rewashes it. |
| Alternative Flow 3 | If he/she notices that something shrank, he/she throws it out. |

#### 3.2.2 Functional Capabilities (Optional)

*Guide:*

*In specific cases, a set of Functional Capabilities can be represented in a functional decomposition diagram. This is typical of functional analysis in the System Engineering domain. For more information on Functional Analysis see, e.g. https://spacese.spacegrant.org/functional-analysis/.*

#### 3.2.3 Requirement Matrix (Optional)

*Guide:*

*A Requirement Matrix can be used when the solution will be based on software capabilities already available in existing components (either custom or vendor provided). The Requirements Matrix is a matrix that is used to capture client requirements for software selection and to evaluate the initial functional "fit" of a vendor's software solution to the business needs of the client.*

*Example:*

For example, rows can list required functional capabilities and columns can list available software components. Cells can contain a simple Y/N or provide more detail. The Requirements Matrix also is used to identify initial functional gaps or special software enhancements needed to enable each vendor's software to fulfill the client's desired system capabilities.

### 3.3 Non-Functional Requirements

*Guide:*

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

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

#### 3.3.1 Regulations and Compliances Requirements

*Guide:*

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

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

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

*Example:*

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

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

### 3.3.2 Environments

*Guide:*

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

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> |

### 3.3.3 High Availability and Disaster Recovery Requirements

*Guide:*

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

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

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

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

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

*Example:*

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

#### 3.3.3.1 High Availability (Optional)

*Guide:*

*A subsubsection, if cleaner separation of Resilience and Recovery into HA, DR, and Backup & Restore is needed.*

*Example:*

| Service Name | KPI | Unit | Value |
|---|---|---|---|
| DB | Uptime | percent | 99.98 |
| Web Application | Max Interruption | minutes | 20 |

#### 3.3.3.2 Disaster Recovery (Optional)

*Guide:*

*A subsubsection, if cleaner separation of Resilience and Recovery into HA, DR, and Backup & Restore is needed.*

*Example:*

| Service Name | KPI | Unit | Value |
|---|---|---|---|
| Web Application | RTO | minutes | 120 |
| Web Application | RPO | minutes | 10 |

#### 3.3.3.3 Backup and Restore (Optional)

*Guide:*

*A subsubsection, if cleaner separation of Resilience and Recovery into HA, DR, and Backup & Restore is needed.*

*Example:*

| Service Name | KPI | Unit | Value |
|---|---|---|---|
| DWH | Frequency | /day | 2 |
| DWH | BckpTime (F) | hours | 4 |
| DWH | BckpTime (I) | hours | 1 |

### 3.3.4 Security Requirements

*Guide:*

*Capture the Non-Functional Requirements for security-related topics. Security is a mandatory subsection that is to be reviewed by the x-workload security team. The requirements can be separated into:*

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

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

*Example:*

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

#### 3.3.4.1 Identity and Access Management (Optional)

*Guide:*

*The requirements for identity and access control. This section describes any requirements for authentication, identity management, single-sign-on, and necessary integrations to retained customer systems (e.g. corporate directories).*

- *Is there any Single Sign On or Active Directory Integration Requirement?*
- *Is the OS hardened if so please share the hardening guideline.*

#### 3.3.4.2 Data Security (Optional)

*Guide:*

*Capture any specific or special requirements for data security. This section should also describe any additional constraints such as a requirement for data to be held in a specific location or for data export restrictions.*

### 3.3.5 Integration and Interfaces (Optional)

*Guide:*

*A list of all the interfaces into and out of the defined Workload. The list should detail the type of integration, the type of connectivity required (e.g. VPN, VPC, etc) the volumes, and the frequency.*

- *list of integrations*
- *list of user interfaces*

*Example:*

| Name | Source | Target | Protocol | Function |
|---|---|---|---|---|
| IOT | Field Sensor | MQTT Server | MQTT | Data collection |
| ELT | ODI | EBS DB | SQL Net | Data extraction |
| General Ledger Integration | EBS | ERP Cloud | Batch | Batch extraction |
| Mobile API | Mobile User | HR Cloud | Rest API | Via API Cloud |

### 3.3.6 System Configuration Control Lifecycle (Optional)

*Guide:*

*This section should detail the requirements for the development and deployment lifecycle across the Workload. This details how code will be deployed and how consistency across the environments will be maintained over future software deployment. This may include a need for CI/CD.*

- *Will a CI/CD tool need access to deploy to the target environment*
- *Does the customer require software to be delivered to a repository*
- *How will configuration and software be promoted through the environments*

### 3.3.7 Operating Model (Optional)

*Guide:*

*This section captures requirements on how the system will be managed after implementation and migration. In the vast majority of cases, the solution will be handed back to the customer (or the customer's SI/partner), but in some cases, Oracle may also take on some sustaining responsibilities through ACS or OC.*

*Also, capture requirements for tools to monitor and manage the solution.*

### 3.3.8 Management and Monitoring (Optional)

*Guide:*

*This subsection captures any requirements for integrations into the customer's existing management and monitoring systems - e.g. system monitoring, systems management, etc. Also, if the customer requires new management or monitor capabilities, these should be recorded.*

*Example:*

| Tool | Task | Target | Location | New | Notes |
|---|---|---|---|---|---|
| Splunk | Log Data Consolidation | All targets | On-Prem | No | |
| Enterprise Manager | Manage DB Instances | All Oracle DBs | OCI (Migration) | No | |

### 3.3.9 Performance (Optional)

*Guide:*

*The performance requirements cover all aspects related to the time required to perform a given operation. They can be measured in different ways, for example: (1) AvrgTime: average response time that can be accepted for a given online or real interaction (data retrieve, data insert, etc.) (2) MaxTime: maximum response time for the same operations defined for AvrgRtime The operations can be online (user interactions), offline (batch execution) or (near)realtime (messaging).*

*Example:*

| Type | Operation | KPI | Unit | Value | Notes |
|---|---|---|---|---|---|
| Online | Retrieve customer data | MaxTime | sec | 3 | |
| Online | Retrieve customer data | AvrgTime | sec | 0.2 | |
| Realtime | | Receive MQTT message | AvrgTime | msec | 100 |

#### 3.3.10 Capacity (Optional)

*Guide:*

*Capacity is a measure of the total workload the system can bear without affecting performance. There are many KPIs to measure capacity, depending on the system's functionalities. Some of the most relevant KPIs are:*

- *MaxVol: maximum volume of data that can be stored in the system (can be different for different types of data, e.g. relational and file): 800-900GB current database size (probably with a significant waste of space)*
- *MaxFlow: maximum data flow (input/output) that can be managed by the system (can be two different numbers for each major system interface and/or operation): the current value has not been measured but is expected to be at most a few GB.*
- *MaxUser: maximum number of concurrent users (can be differentiated by user profile): up to 10 (number of registered users).*

*Example:*

| System | Capacity | KPI | Unit | Value | Notes |
|---|---|---|---|---|---|
| DB server | DB size | MaxVol | GB | 2000 | |
| ETL Server | Data processed nightly | MaxFlow | GB/h | 100 | |
| OAC Server | Simultaneous users | MaxUsers | - | 10 | |

## 3.4 Constraints and Risks (Optional)

*Guide:*

*Constraints are limitations that will impact the resulting project or Solution Architecture. It is a technology- or project-related condition or event that prevents the project from fully delivering the ideal solution to customers and end-users. Constraints can be identified on our customer, partner, or even Oracle's side.*

*A project risk is an uncertain event that may or may not occur during a project.*

*Describe constraints and risks affecting the Workload and possible Logical Solution Architecture. These can be technical, but might also be non-technical. Consider budgets, timing, preferred technologies, skills in the customer organization, location, etc.*

*Example:*

| 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 person's availability |
| Access Restriction | We are not allowed to access a certain tenancy without customer presence | Constraint | | Invite customer key person to implementation sessions |

## 3.5 Current State Architecture (Optional)

*Guide:*

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

## 3.6 Future State Architecture

*Guide:*

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

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

### 3.6.1 Mandatory Security Best Practices

The safety of the ACME's Oracle Cloud Infrastructure (OCI) environment and data is the ACME'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 chapters below. They must be approved by ACME.

ACME 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.<br>• For configuration details see Managing Multi-Factor Authentication.<br>In addition to enforce MFA for local users, Adaptive Security will be enabled to track the Risk Score of each user of the Default Domain.<br>• For configuration details see Managing Adaptive Security and Risk Providers. |
| | OCI Emergency Users | A maximum of **three** non-federated OCI user accounts should be present with the following requirements: |

| CATEGORY | TOPIC | DETAILS |
|---|---|---|
| | | • Username does not match any username in the Customer's Enterprise Identity Management System<br>• Are real humans.<br>• Have a recovery email address that differs from the primary email address.<br>• User capabilities has Local Password enabled only.<br>• 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:<br>• Federation Setup<br>• User Provisioning<br>• For configuration guidance for major Identity Providers see the OCI IAM Identity Domain tutorials. |
| | Application Users | Application users like OS users, Database users, or PaaS users are not managed in the IAM Default Domain but either directly or in dedicated identity domains. These identity domains and users are covered in the Workload design. For additional information see Design Guidance for IAM Security Structure. |
| Cloud Posture Management | OCI Cloud Guard | OCI Cloud Guard will be enabled at the root compartment of the tenancy home region. This way it covers all future extensions, like new regions or new compartments, of your tenancy automatically. It will use the Oracle Managed Detector and Responder recipes at the beginning and can be customized by the Customer to fulfil the Customer's security requirements.<br>• For configuration details see Getting Started with Cloud Guard. Customization of the Cloud Guard Detector and Responder recipes to fit with the Customer's requirements is highly recommended. This step requires thorough planning and decisions to make.<br>• For configuration details see Customizing Cloud Guard Configuration |
| | OCI Vulnerability Scanning Service | In addition to OCI Cloud Guard, the OCI Vulnerability Scanning Service will be enabled at the root compartment in the home region. This service provides vulnerability scanning of all Compute instances once they are created.<br>• For configuration details see Vulnerability Scanning. |
| Monitoring | SIEM Integration | Continuous monitoring of OCI resources is key for maintaining the required security level (see Regulations and Compliance for specific requirements). See Design Guidance for SIEM Integration to implement integration with the existing SIEM system. |
| Additional Services | Budget Control | OCI Budget Control provides an easy to use and quick notification on changes of the tenancy's budget consumption. It will be configured to quickly identify unexpected usage of the tenancy.<br>• For configuration details see Managing Budgets |

### 3.6.2 OCI Secure Landing Zone Architecture

The design considerations for an OCI Cloud Landing Zone have to do with OCI and industry architecture best practices, along with ACME 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.

#### 3.6.2.1 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, matching Oracle's best practices and ACME 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 |

| Resource Type | Abbreviation | Example |
|---|---|---|
| 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 |

#### 3.6.2.2 Security and Identity Management

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

##### 3.6.2.2.1 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.

##### 3.6.2.2.2 Authentication and Authorization for OCI

The provisioning of respective OCI administration users will be handled by ACME.

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

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

**ACME 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 ACME.

**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.

**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.

**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 ACME using the application, compute instance, and database-specific authorization.

#### 3.6.2.2.3 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 ACME's requirements.

**Targets**

In accordance with the CIS Oracle Cloud Infrastructure Foundations Benchmark, v1.2.0, 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 ACME.

**Responder Rules**

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

**Vulnerability Scanning Service**

In accordance with the CIS Oracle Cloud Infrastructure Foundations Benchmark, v1.2.0, OCI Vulnerability Scanning 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.

#### 3.6.2.2.4 Monitoring, Auditing, and Logging

In accordance with the CIS Oracle Cloud Infrastructure Foundations Benchmark, v1.2.0, Chapter 3 Logging and Monitoring 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.

#### 3.6.2.2.5 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.

##### 3.6.2.2.5.1 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 reviewed for every project onboard into the tenancy.

#### 3.6.2.2.6 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 *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 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.

#### 3.6.2.2.7 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.

#### 3.6.2.2.8 Regulations and Compliance

ACME 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.

### 3.6.3 Functional Architecture (Optional)

*Guide:*

*Provide a brief description of the functional architecture, split into two main areas: application capabilities and data.*

### 3.6.4 Logical Architecture (Optional)

*Guide:*

*Use System Context Diagram to show integration for the Workload solution.*

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

*The Oracle Cloud Notation, OCI Architecture Diagram Toolkits*

### 3.6.5 Physical Architecture

*Guide:*

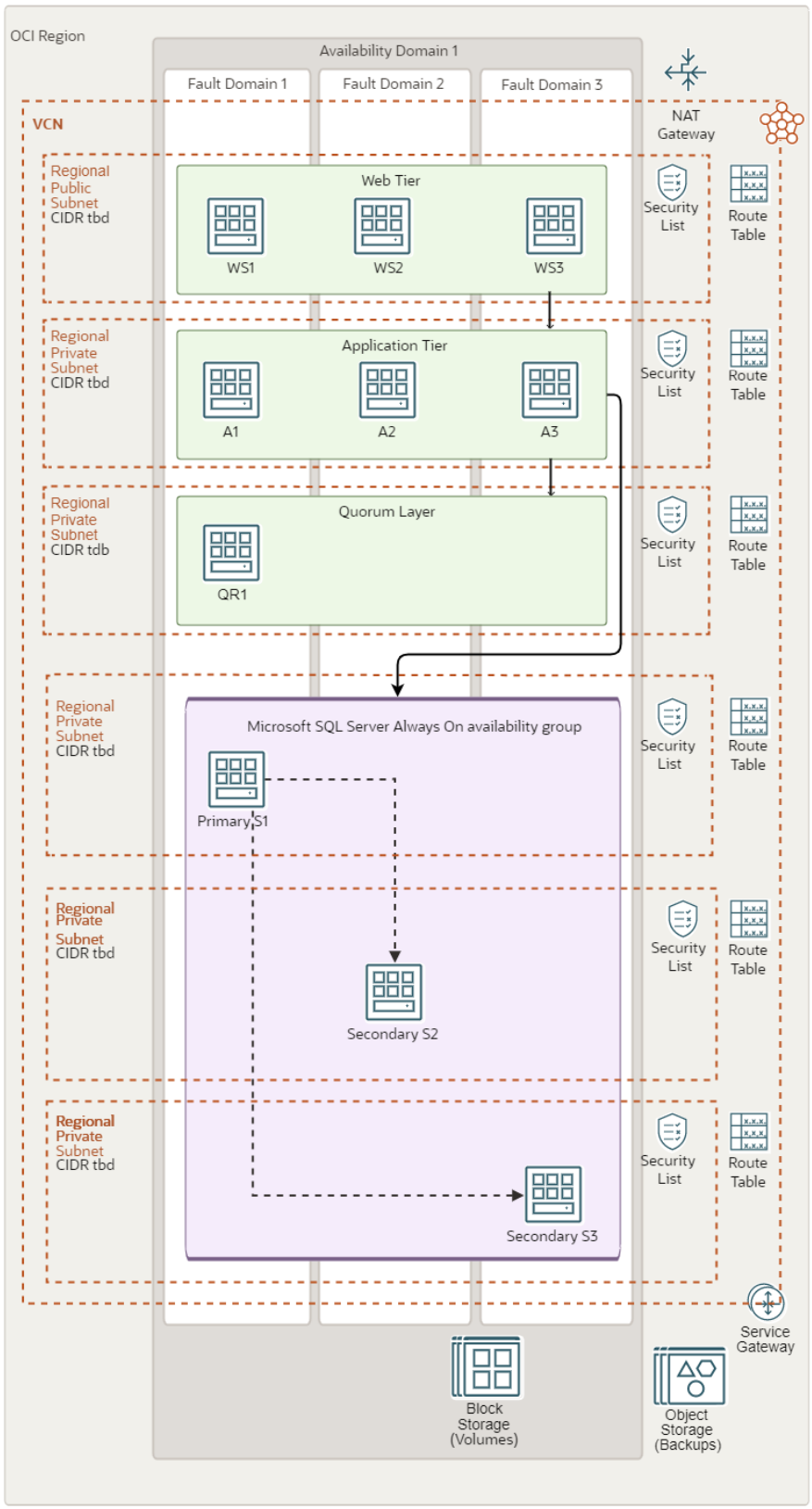
*The Workload Architecture is typically described in a physical form. This should include all solution components. You do not have to provide solution build or deployment details such as IP addresses.*

*The Oracle Cloud Notation, OCI Architecture Diagram Toolkits*

*Reference:*

StarterPacks

*Example:*




*Future State MS SQL Always ON Diagram*

The architecture has the following components:

- Region

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

- Availability domain

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

- Fault domain

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

- Virtual cloud network (VCN) and subnets

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

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

- Route table

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

- Security lists

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

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

- NAT gateway

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

- Block volume

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

- Object storage

Object storage provides quick access to large amounts of structured and unstructured data of any content type, including database backups, analytic data, and rich content such as images and videos. Use standard storage for "hot" storage that you

need to access quickly, immediately, and frequently. Use archive storage for "cold" storage that you retain for long periods of time and seldom or rarely access.

#### 3.6.6 Data Architecture (Optional)

*Guide:*

*Show how data is acquired, transported, stored, queried, and secured as in the scope of this Workload. This could include Data Ecosystem Reference Architectures, Master Data Management models, or any other data-centric model.*

#### 3.6.7 Architecture Decisions (Optional)

*Guide:*

*List the architecture decisions for the previous future state architecture(s). The decisions can be based upon the previously defined requirements or can be based on common architecture best practices or architecture design patterns.*

##### 3.6.7.1 Requirements Evaluation (Optional)

*Guide:*

*List architecture decisions and how they impact previous functional, non-function, or other requirements. Do a realist evaluation and also highlight lowlights where an architecture decision might not fully comply with a previous requirement. Discuss with your customer and get feedback from your colleagues if some requirements are not fully satisfied.*

##### 3.6.7.2 Architecture Best Practices (Optional)

*Guide:*

*Refer to or cite architecture best practices or design patterns. Explain how they are reflected in your architecture and how they improve the solution.*

### 3.7 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?*

#### 3.7.1 High Availability and Disaster Recovery

*Reference:*

#### 3.7.2 Security

*Guide:*

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

*Example:*

Please see our security guidelines in the Annex.

#### 3.7.3 Networking

*Reference:*

Networking Confluence

#### 3.7.4 Operations (Optional)

*Guide:*

*In this chapter, we provide a high-level introduction to various operations-related topics around OCI. We do not design, plan or execute any detailed operations for our customers. We can provide some best practices and workload-specific recommendations.*

*Please visit our Operations Catalogue for more information, best practices, and examples: https://confluence.oraclecorp.com/confluence/pages/viewpage.action?pageId=3403322163*

*The below example text represents the first asset from this catalog PCO#01. Please consider including other assets as well. You can find MD text snippets within each asset.*

*Example:*

This chapter provides an introduction and collection of useful resources, on 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, and 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 the performance, availability, and 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 SLAs and PDF Link |

## 3.8 Roadmap (Optional)

*Guide:*

*Explain a high-level roadmap for this Workload. Include a few easy high-level steps to success (See Business Context). Include implementation services (if possible) as a first fast step. Add other implementation partners and their work as part of your roadmap as well. Do not include details about the implementation scope or timeline. This is not about product roadmaps.*

### 3.9 Sizing and Bill of Materials

*Guide:*

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

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

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

*WIP*

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

| Server Role | OCI Component | Quantity | SHAPE | OCPU | RAM (GB) | Operating System |
|---|---|---|---|---|---|---|
| Quorum witness server | Compute | 1 VMs | VM.Standard.2.2 | 2 | 30 | Windows Server 2016 |
| SQL Server Always ON Servers | Compute | 3 VMs | VM.Standard.2.2 | 2 | 30 | Windows Server 2016 |
| Load Balancer Base | Networking | 1 LB | | | | |

## Glossary (Optional)

*Guide:*

*A chapter for Product, Technology, or Concept descriptions*

*Please avoid describing products, and linking to product documentation at the first occurrence of a product.*

*Example:*

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

*Example:*

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

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

### 4.2 Other

# Annex

## 5.1 Security Guidelines

#### 5.1.1 Oracle Security, Identity, and Compliance

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

- Security Strategy – To create a successful security strategy and architecture for your deployments on OCI, it's helpful to understand Oracle's security principles and the OCI security services landscape.
- The security pillar capabilities pillar capabilities reflect fundamental security principles for architecture, deployment, and maintenance. The best practices in the security pillar help your organization to define a secure cloud architecture, identify and implement the right security controls, and monitor and prevent issues such as configuration drift.

##### 5.1.1.1 References

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

#### 5.1.2 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 customer also varies based on the nature of the cloud service (IaaS, PaaS, SaaS).

## 5.2 Additional Resources

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