

# OCI CIS Landing Zone Configuration

---

## Sample Quick Start Scenario

November 2023, Version 0.8  
Copyright © 2023, Oracle and/or its affiliates  
Public

## Table of contents

---

<b>Version Control</b>	<b>3</b>
<b>Introduction</b>	<b>4</b>
Purpose	4
Scope	4
<b>Landing Zone Setup</b>	<b>5</b>
Solution Details	5
Solution Configuration	5
1. Summary	5
2. Scenario	5
3. ORM Stack Creation	6

## Version Control

VERSION	AUTHOR	DATE	COMMENTS
1.0	<author>	<date>	

## Introduction

### Purpose

This document identifies the landing zone solution and key setup decision for deployment.

### Scope

This document reflects a standard deployment scenario, using available pre-defined configurations for the solution.

## Landing Zone Setup

### Solution Details

Proposed Solution	OCI CIS Landing Zone
Version Used	2.4.2
Deployment Interface	<a href="#">Oracle Resource Manager</a>
Documentation	<a href="#">Solution Overview</a>
	<a href="#">Deployment Guide</a>
	<a href="#">Release Notes</a>
	<a href="#">Terraform Modules</a>
	<a href="#">Compliance Script</a>
	<a href="#">Universal Permissive License (UPL)</a>
	<a href="#">FAQ</a>

### Solution Configuration

#### 1. Summary

This document presents the Oracle Resource Manager steps with associated input and support for decision. The flow is composed of a wizard guided setup. The values for each screen and the respective sections are specified in the next chapters.

#### 2. Scenario

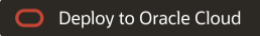
This Default scenario includes:

- Default IAM groups/dynamic groups and policies.
- A compartment holding the landing zone, deployed under the root that will contain four child compartments (<prefix>-network-cmp, <prefix>-security-cmp, <prefix>-appdev-cmp and <prefix>-database-cmp).
- Standard three-tier network architecture within one Virtual Cloud Network (VCN).
  - One public subnet for load balancers and bastion servers.
  - Two private subnets: one for the application tier and one for the database tier.
- Cloud Guard Service enabled with a default configuration.
- Vulnerability Scanning Service enabled with a customized configuration.
- Internet Gateway.
- NAT Gateway.
- Service Gateway.
- Events and Notifications.

### 3. ORM Stack Creation

For easier navigation and reference, the names of the sub chapters match the labels used in OCI Resource Manager wizard screens.

#### 2.1 Landing Zone Download

1. Log into the OCI Console for <tenancy> with Administrator permissions.
2. Point the browser to <https://github.com/oracle-quickstart/oci-cis-landingzone-quickstart>
3. Click on 

#### 2.2 Stack Information Screen

#	INPUT FIELD	OPTIONAL INPUT	VALUE	OBSERVATIONS
1	I have reviewed and accept the Oracle Terms of Use.		Check	You have to accept the Terms of Use to continue.
2	Working Directory		oci-cis-landingzone-quickstart-main/config	Use default value.
3	Name		<modify default stack name>	Use a meaningful name.
4	Create in Compartment		<include root compartment name>	Use <b>root compartment</b> for all stacks.
5	Terraform Version		1.1.x or later	Use proposed value.

#### 2.3 Configure Variables Screen

For easier navigation, the names of the sub chapters match the labels used in OCI Resource Manager wizard screens.

##### 2.3.1 Environment

#	PRIMARY INPUT	OPTIONAL INPUT	VALUE	OBSERVATIONS
1	Region		<region name>	Select home region.
2	Service Label		<include desired service label>	Use a meaningful name. This label will be used as a prefix for naming resources.
3	CIS Level		1 or 2	CIS Level 1 is for basic security, whereas CIS Level 2 is for stronger security.
4	Use an enclosing compartment?		Check	The default scenario will mainly be used for test purposes. In this case we recommend use an enclosing compartment.
4.1		Existing enclosing compartment	Leave blank or specify name of existing compartment	<ul style="list-style-type: none"><li>▪ Select a pre-created LZ parent compartment.</li><li>▪ If this variable is left blank a default enclosing compartment, called <i>"ServiceLabel-top-cmp"</i>, will be created under the root compartment.</li></ul>

5	Advanced Options		Uncheck	The Landing Zone provisions groups and dynamic groups, policies according to best practices. For standard configuration we recommend not to change this value.
---	------------------	--	---------	--

### 2.3.2 Networking – Generic VCNs

#	PRIMARY INPUT	OPTIONAL INPUT	VALUE	OBSERVATIONS
1	VCNs CIDR Blocks		<include desired CIDR>	Provide the desired value.  If left blank, no network will be created and will affect all other network settings.
2	Advanced Options		Uncheck	For standard configuration we recommend not to change this value.

### 2.3.3 Networking – Exadata Cloud Service VCNs

This is optional and required for Exadata Services only.

#	PRIMARY INPUT	OPTIONAL INPUT	VALUE	OBSERVATIONS
1	Exadata CIDR Blocks		Leave blank	Standard option does not include EXADATA workloads.
2	Advanced Options		Uncheck	For standard configuration we recommend not to change this value.

### 2.3.4 Networking – Hub / Spoke

#	PRIMARY INPUT	OPTIONAL INPUT	VALUE	OBSERVATIONS
1	Deploy Hub/Spoke Architecture?		Uncheck	For standard configuration we recommend not to change this value.
2	Advanced Options		Uncheck	For standard configuration we recommend not to change this value.

### 2.3.5 Networking – Public Connectivity

#	PRIMARY INPUT	OPTIONAL INPUT	VALUE	OBSERVATIONS
1	Block Internet Access?		Uncheck	If left unchecked, an Internet Gateway and NAT Gateway are created for Internet connectivity
2		Bastion Inbound SSH and RPD CIDR Blocks	Leave blank	For standard configuration we recommend not to change this value.

3		<b>Load Balancer Inbound HTTPS CIDR Blocks</b>	Leave blank	For standard configuration we recommend not to change this value.
4		<b>NAT Outbound HTTPS CIDR Blocks</b>	Leave blank	For standard configuration we recommend not to change this value.

### 2.3.6 Networking – Connectivity to On-premises

#	PRIMARY INPUT	OPTIONAL INPUT	VALUE	OBSERVATIONS
1	<b>Connect Landing Zone VNC(s) to on-premises network?</b>		Uncheck	For standard configuration we recommend not to change this value.  On-premises connectivity is an advanced option.

### 2.3.7 Networking – DRG (Dynamic Routing Gateway)

#	PRIMARY INPUT		VALUE	OBSERVATIONS
1	<b>Existing DRG OCID</b>		Leave blank	For standard configuration we recommend not to change this value.  Will be used with Hub / Spoke topology and for on-premises connectivity.

### 2.3.8 Events and Notifications

#	PRIMARY INPUT	OPTIONAL INPUT	VALUE	OBSERVATIONS
1	<b>Network Admin Email Endpoints</b>		<include desired email>	
2	<b>Security Admin Email Endpoints</b>		<include desired email>	
3	<b>Additional Notification Endpoints</b>		Uncheck	For standard configuration we recommend not to change this value.  Check if Cost Management is required.

### 2.3.9 Object Storage

#	PRIMARY INPUT	OPTIONAL INPUT	VALUE	OBSERVATIONS
---	---------------	----------------	-------	--------------



1	Enable Object Storage		Uncheck	For standard configuration we recommend not to change this value.
---	-----------------------	--	---------	---

### 2.3.10 Cloud Guard

#	PRIMARY INPUT	OPTIONAL INPUT	VALUE	OBSERVATIONS
1	Cloud Guard Configuration Status		ENABLE	Leave default value. Cloud Guard is always enabled.
2	Minimum Risk Level Threshold		HIGH	Leave default value. Determines the minimum risk level that will trigger an event and send information about the problem to the Cloud Guard Email Endpoints. E.g. a minimum risk level of High will include problems with High or Critical risk levels.
3	Cloud Guard Admin Email Endpoints		Leave blank	

### 2.3.11 Security Zones

#	PRIMARY INPUT	OPTIONAL INPUT	VALUE	OBSERVATIONS
1	Enable Security Zones		Uncheck	For standard configuration we recommend not to change this value. Security Zones are an advanced option.

### 2.3.12 Logging Consolidation: Service Connector Hub

#	PRIMARY INPUT	OPTIONAL INPUT	VALUE	OBSERVATIONS
1	Enable Service Connector Hub?		Uncheck	For standard configuration we recommend not to change this value. Service Connector Hub is an advanced option.

### 2.3.13 Vulnerability Scanning

#	PRIMARY INPUT	OPTIONAL INPUT	VALUE	OBSERVATIONS
1	Enable Vulnerability Scanning		Check	We recommend enabling Vulnerability Scanning.
2		Scanning Schedule	DAILY	Default value is WEEKLY. We recommend change this to DAILY
3		Scanning Day	N/A	Available for <b>WEEKLY</b> scans only.
4		Port Scan Level	STANDARD	Leave default value.
5		Agent CIS Benchmark Settings Scan Level	MEDIUM or STRICT	Depends on the value of 2.3.1 <i>Environment, number 3</i> : Use <b>MEDIUM</b> for CIS Level 1 Use <b>STRICT</b> for CIS Level 2
6		Enable File Scanning?	Uncheck	For standard configuration we recommend not to change this value.  This is an advanced option.

#### 2.3.14 Cost Management

#	PRIMARY INPUT	OPTIONAL INPUT	VALUE	OBSERVATIONS
1	Create a default budget?		Uncheck	For standard configuration we recommend not to change this value.