ORACLE

OCI CIS Landing Zone Configuration

Sample Production Scenario

November 2023, Version 0.2

Public

Table of contents

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	Oracle Resource Manager
Documentation	Solution Overview
	Deployment Guide
	Release Notes
	Terraform Modules
	Compliance Script
	Universal Permissive License (UPL)
	FAQ

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:

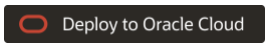
- Default IAM groups/dynamic groups and policies.
- These four compartments will be deploy under the root compartment:

  (<prefix>-network-cmp, <prefix>-security-cmp, <prefix>-appdev-cmp and <prefix>-database-cmp).
- Hub&Spoke network topology with ‘n’ VCN.
- Standard three-tier network architecture for each 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.
- Bastion Service.
- Internet Gateway.
- NAT Gateway.
- Service Gateway.
- Cloud Guard Service enabled with a default configuration.
- Vulnerability Scanning Service enabled with a customized configuration.
- 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 **root compartment** 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	For **basic security** use CIS Level 1. For **stronger security** use CIS Level 2. We recommend using CIS Level 2.
4	**Use an enclosing compartment?**		Uncheck	Uncheck to deploy LZ under the root compartment.
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 CIDRs>	List of CIDR blocks for the VCNs in CIDR notation. Each CIDR block corresponds to one VCN. When *Deploy Hub/Spoke Architecture?* is selected under *Advanced Options*, these VCNs are turned into spoke VCNs.
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?**		Check	Hub/Spoke network architecture will be deployed. Allows for inter-spoke routing through a DRG. If checked, either a new DRG is deployed or an existing DRG can be reused if you provide its OCID in *Existing DRG OCID* field below. You must click the check box for the field to appear.
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 Inboud SSH and RPD CIDR Blocks**	<Include comma separated list of CIDR blocks>	List of external IP ranges in CIDR notation allowed to make SSH and RDP inbound connections to bastion servers that are eventually deployed in public subnets. 0.0.0.0/0 is not allowed in the list. (Type the name and hit enter to enter multiple values). This setting does **not** impact the creation of bastion services!
3		**Load Balancer Inbound HTTPS CIDR Blocks**	<Include comma separated list of CIDR blocks>	List of external IP ranges in CIDR notation allowed to make HTTPS inbound connections to a Load Balancer that is eventually deployed. (Type the name and hit enter to enter multiple values.)
4		**NAT Outbound HTTPS CIDR Blocks**	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	**Connect Landing Zone VNC(s) to on-premises network?**		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	**Existing DRG OCID**		<set to existing DRG OCID or leave blank>	Can be used with Hub / Spoke topology or for on-premises connectivity. Provide a value of a pre-created DRG. If you leave this value blank the Landing Zone will deploy a DRG.

2.3.8 Events and Notifications

#	PRIMARY INPUT	OPTIONAL INPUT	VALUE	OBSERVATIONS
1	**Network Admin Email Endpoints**		<comma separated list of email recipients>	List of email addresses for all network related notifications. (Type an email address and hit enter to enter multiple values.)
2	**Security Admin Email Endpoints**		<comma separated list of email recipients>	List of email addresses for all security related notifications. (Type an email address and hit enter to enter multiple values.)
3	**Additional Notification Endpoints**		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. For example, 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 **WEEKLY** 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 Environment, number 3:* Use **MEDIUM** for CIS Level **1** Use **STRICT** 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.