

ASSET ID	ASSETNAME	CIS Landing Zone v2 ORM Execution Guide	ASSET VERSION	0.10 11.07.2023
ASSET OBJECTIVE	Support the configuration with key setup decisions on input required and deployment topologies. Provide deployment execution guidelines for deploying the CIS Landing Zone v2 with Oracle Resource Manager.			
ASSET CONTENTS	[1. BEFORE YOU START] [2. DEPLOYMENT - HOW TO DEPLOY CIS Landing Zone v2 USING ORM] [3. INPUT VALUES & DEPLOYMENT SCENARIOS] [3.1 ENCLOSING COMPARTMENT] [3.2 IAM] [3.3 HUB & SPOKE] [3.4 NETWORK APPLIANCE VCN] [3.5 EXADATA VCN] [3.6 BLOCK INTERNET ACCESS] [3.7 NOTIFICATIONS] [3.8 OBJECT STORAGE] [3.9 CLOUD GUARD] [3.10 SECURITY ZONES] [3.11 LOGGING CONSOLIDATION] [3.12 VULNERABILITY SCANNING] [3.13 COST MANAGEMENT] [3.14 MULTIPLE WORKLOADS] [3.15 OTHER SCENARIOS] [4. EXECUTE TERRAFORM PLAN] [5. EXECUTETERRAFORM APPLY] [6. POST-DEPLOYMENT ACTIONS] [6.1 SETUP MULTIPLE WORKLOADS] [6.2. CONFIRM CIS COMPLIANCE] [6.3. DESTROY THE STACK RESOURCES] [7. KNOWN ISSUES] [7.1 OCITIMEOUT ISSUE] [7.2 OCI COMPARTMENT DELETION ISSUE] [7.3 OCI VAULT DELETION ISSUE] [7.4 TOO MANY REQUESTS]			

1. BEFORE YOU START

Before you start make sure you have reviewed the **ORM Configuration decisions** that you will have to take throughout this guide.

In order to execute this guide, you will need the following:

- A paid tenancy, the always-free account is not supported.
- An OCI account with sufficient privileges to deploy the landing zone. (admin of your tenancy).
- Terraform >= 0.13.x

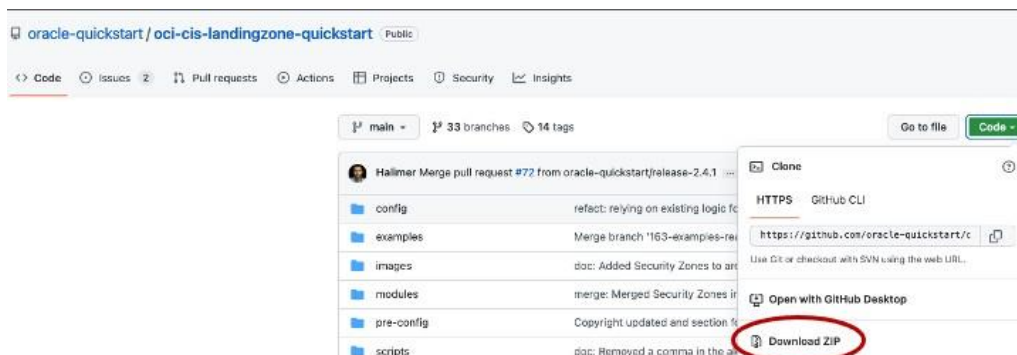
2. DEPLOYMENT - HOW TO DEPLOY CIS Landing Zone v2 USING ORM

2.1 CREATE A NEW ORM STACK

Go to the [GitHub](#) repository and select the option **Deploy to Oracle Cloud** to luncn the CIS stack



As an alternative, you can also download the ORM stack code and import it like a zip.



In the OCI console go to:

Developed Services > Resource Manager > Stacks > Create Stack

Overview

Stacks

Jobs

Private templates

Configuration source providers

Private endpoints

A stack is a Terraform configuration that you can use to provision and manage your OCI resources. To provision the resources defined in your stack, [apply the configuration](#).

Create stack

Select **My configuration** and add the zip downloaded in the previous step.

A stack is a Terraform configuration that you can use to provision and manage your OCI resources. To provision the resources defined in your stack, you must create a stack.

Choose the origin of the Terraform configuration. The Terraform configuration outlines the cloud resources to provision for this stack. [Learn more](#)

☒ My configuration

Upload Terraform configuration file

☐ Template

Select an Oracle-provided template or private template.

☐ Source code control system

Select a Terraform configuration from GitHub, GitLab, or DevOps.

☐ Existing compartment

Create a stack that captures resources from the selected compartment (resource discovery).

Stack configuration ⓘ

Terraform configuration source

☐ Folder

☐ Object Storage bucket

☒ .Zip file

Drop a .zip file [Browse](#)

oci-cis-landingzone-quickstart-main (1).zip

Stack information



OCI Secure Landing Zone Quick Start Configuration

A stack to deploy a set of CIS (Center for Internet Security) compliant resources in an OCI tenancy. The Secure Landing Zone is the combination of CIS Foundations Benchmark for OCI with OCI architecture best practices.

Working directory

oci-cis-landingzone-quickstart-main/config

The file path to the directory from which to run Terraform

Custom providers



Use custom Terraform providers

[Store custom Terraform providers in a bucket.](#)

Name *Optional*

oci-cis-landingzone-quickstart-main (1)-20220930161521

Description *Optional*

A stack to deploy a set of CIS (Center for Internet Security) compliant resources in an OCI tenancy. The Secure Landing Zone is the combination of CIS Foundations Benchmark for OCI with OCI architecture best practices.

Create in compartment

PJUAREZ_ES

oci4cca (/root/CCA_Basic_Compartment/PJUAREZ_ES)

Terraform version

1.1.x



0.11.x is no longer supported. [What Terraform versions are supported by Resource Manager?](#)

Tags

Add tags to organize your resources. [What can I do with tagging?](#)

Tag namespace

None (add a free-form tag)

Tag key

Tag value

Add tag

3. INPUT VALUES & DEPLOYMENT SCENARIOS

Now that you have the Secure CIS stack, you need to provide the values for all the required attributes.

3.1 ENCLOSING COMPARTMENT

Do you want to deploy the LZ under the root compartment or under a specific compartment?

- If it's your first deployment of a CIS LZ, and you want to do some tests, we recommend as a best practice deploying the LZ under a specific compartment. Select the option **Use an enclosing compartment** and select your predefined compartment or leave it blank (in this case a default enclosing compartment under the root compartment will be created called "CISLZ-top-cmp").
- If you are deploying the production LZ for the customer the recommendation is to deploy the LZ compartments under the root compartment

In this section, you need to add the value of the Service Label attribute. This label will be used to define the name of all the stack resources that will be created.

Environment

Region

eu-frankfurt-1

The region for resources deployment.

Service Label

CISLZ

A unique label that gets prepended to all resources created by the Landing Zone.

CIS Level

2

Determines CIS OCI Benchmark Level of services deployed by the CIS Landing Zone in the tenancy will be configured. Level 1 is be practical and prudent. Level 2 is intended for environments where security is more critical than manageability and usability. More info: [CIS OCI Benchmark](#).

☒ Use an enclosing compartment?

Whether the Landing Zone compartments are created within an enclosing compartment. If unchecked, the Landing Zone compartments are created in the Root compartment, in which case you must have the required permissions.

Existing enclosing compartment *Optional*

Choose...

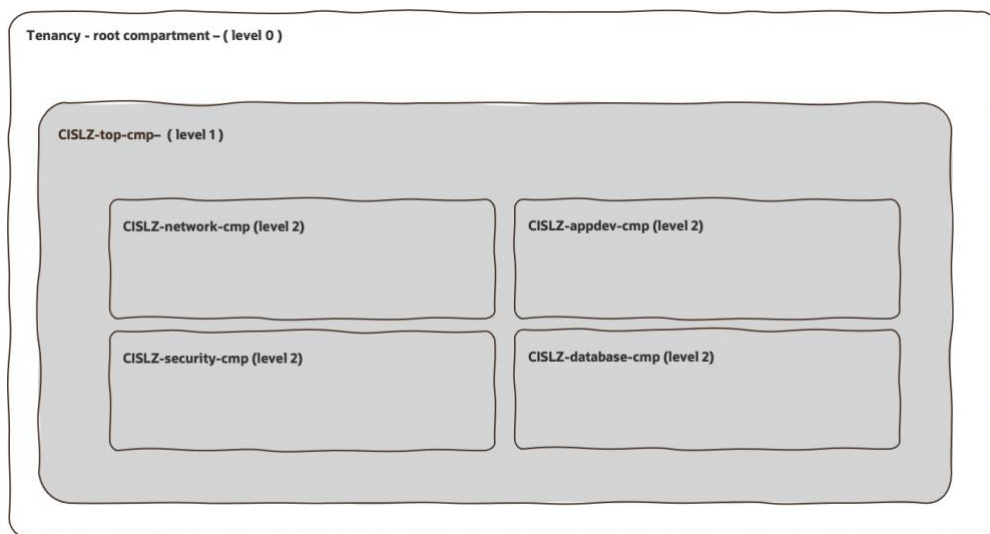
The enclosing compartment where Landing Zone compartments will be created. If not provided and "Use enclosing compartment?" is checked, an enclosing compartment is created under the Root compartment.

☐ Advanced Options

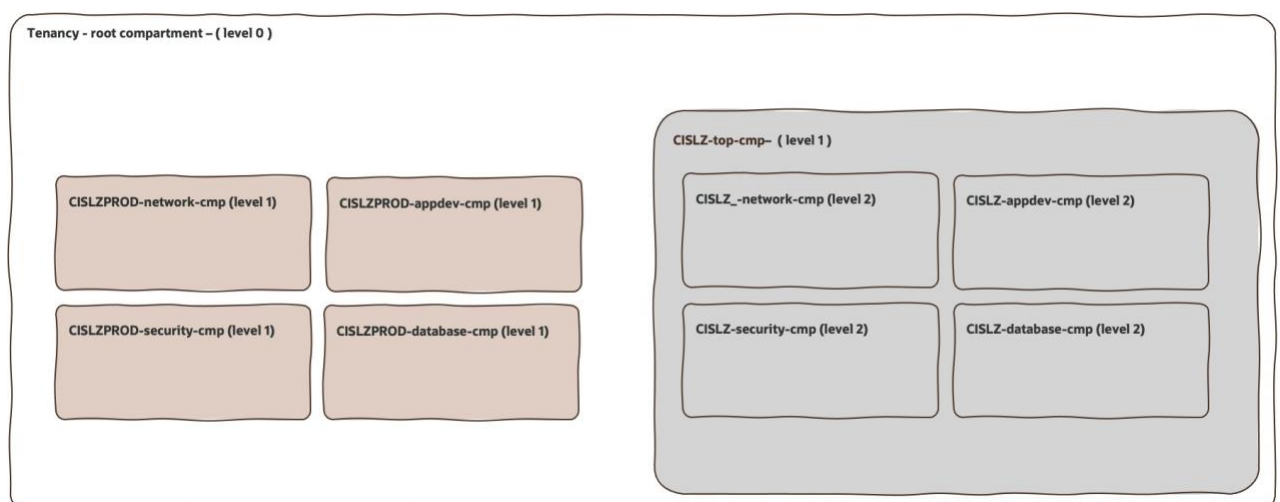
Advanced options for IAM. For details please see [VARIABLES.md](#).

This is the compartment design that will be deployed in the first LZ deployment (for test purposes).

- **Network compartment:** for all networking resources.
- **Security compartment:** for all logging, key management, scanning, and notifications resources.
- **Application Development compartment:** for application development-related services, including Compute, Storage, Functions, Streams, Kubernetes, API Gateway, etc.
- **Database compartment:** for all database resources.



After a mature level, the recommendation will be to deploy another LZ for Production purposes under the root compartment.





3.2 IAM

Do you want to deploy groups included in the CIS LZ v2 stack or do you want to reuse your own groups?

By default, the Landing Zone provisions groups and dynamic groups. These groups are assigned various grants in Landing Zone policies.

In order to deploy these groups and policies leave the default values for the environment stack attributes. (Do not select the **advanced Option**)

However, some circumstances may require the reuse of existing groups and dynamic groups, such as:

- customers who already have defined their groups
- customers who work with federated groups, like Federation with [Microsoft Azure Active Directory](#) or [Microsoft Active Directory](#).

In this case, select the **Advanced Option** and fill the desired groups with your own pre-created groups. You can see some of them in the next image.

Existing IAM admin group name *Optional*

Select an option

Existing group to which IAM management policies will be granted to.

Existing credentials admin group name *Optional*

Select an option

Existing group to which credentials management policies will be granted to.

Existing security admin group name *Optional*

Select an option

Existing group to which security management policies will be granted to.

Existing network admin group name *Optional*

Select an option

Existing group to which network management policies will be granted to.

Existing application development admin group name *Optional*

Select an option

Existing group to which application development management policies will be granted to.

Existing database admin group name *Optional*

Select an option

Existing group to which database management policies will be granted to.

3.3 HUB & SPOKE

Do you want to deploy a Hub & Spoke Network configuration?

- A hub-and-spoke network (often called star topology) has a central component (the hub) that's connected to multiple networks around it, like a wheel. Implementing this topology in the traditional data center can be costly. But in the Oracle Cloud, there's no extra cost.
- CIS LZ v2 covers different network topologies.

If your answer is **NO**.

Define your VCN CIDR and do not click the **Advanced Option**.

Networking - Generic VCNs

VCNs CIDR Blocks *Optional*

10.0.0.0/20 x

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. (Type the name and hit enter to enter multiple values, up to a maximum of 9)

☐ Advanced Options

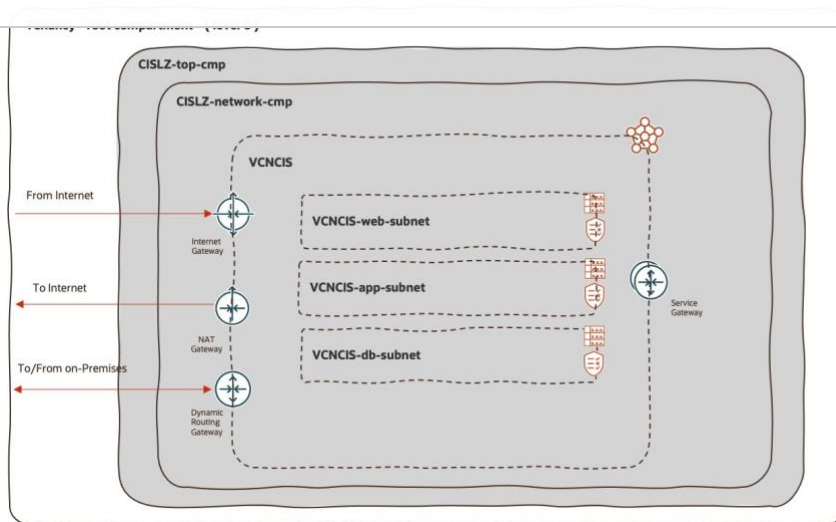
Advanced options for Networking. For details please see [VARIABLES.md](#)

This will be your network configuration after deploying de CIS LZ v2 (CIS) stack.

The stack provisions a standard three-tier network architecture within one Virtual Cloud Network (VCN).

The three tiers are divided into:

- One public subnet for load balancers and bastion servers;
- Two private subnets: one for the application tier and one for the database tier.



deployment

If you want a scenario that enables the communication between an on-premises network and one VCN in the same region over a single FastConnect private virtual circuit or Site-to-Site VPN and uses a DRG as the hub, go to step directly to step 3.5 and skip the next questions.

If your answer to the section question is **YES**, and you want a HUB&SPOKE network design, continue with the next question.

3.4 NETWORK APPLIANCE VCN

Do you want to deploy a Hub VCN for network appliance purposes?

Note: If you configure this option all traffic will be routed through this Hub VCN (also known as DMZ VCN)

In the ORM stack select the option **Deploy Hub/Spoke Architecture** and the option **Advanced Options**.

Select **Use DMZ VCN for 3rd-Party Firewalls** if a 3rd-party firewall will be deployed in the Hub VCN.

When deploying the Landing Zone with the intent of deploying network firewalls later, DRG attachments are not created for any of the VCNs because this is done by the security partner.

Their configuration will create the DRG attachments for the VCNs and route the traffic through the firewall appliance, creating a choke point. The only routing the Landing Zone will do is the spoke VCN routing. This choke point will be used to monitor traffic in and out of OCI as well as between VCN spokes.

Each partner requires a different number of subnets in the Hub VCN. Use the below chart to determine how many subnets you will need in your Hub VCN:

Security Partner	Number of Subnets
Check Point	2
Cisco	5
Fortinet	4
Palo Alto Networks	4

Networking - Hub/Spoke

☒ Deploy Hub/Spoke Architecture?

Determines if Hub/Spoke network architecture is to 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) With Hub/Spoke, all VCNs (generic and ExaCS) are peered through the DRG.

☒ Advanced Options

Advanced options for Hub/Spoke. It allows for creating a DMZ VCN. For details please see [VARIABLES.md](#).

DMZ VCN CIDR Block *Optional*

172.16.0.0/24

IP range for the DMZ VCN in CIDR notation. DMZ VCNs are commonly used for network appliance deployments. All traffic will be routed through the DMZ VCN.

☒ Use DMZ VCN for 3rd-Party Firewalls

Determines if a 3rd party firewall will be deployed in the DMZ VCN.

Number of Subnets in the DMZ VCN *Optional*

2

The number of subnets to be created in the DMZ VCN. If using the DMZ VCN for a network appliance deployment, please see the vendor's documentation or OCI reference architecture to determine the number of subnets required.

Size of the DMZ Subnet CIDRs *Optional*

4

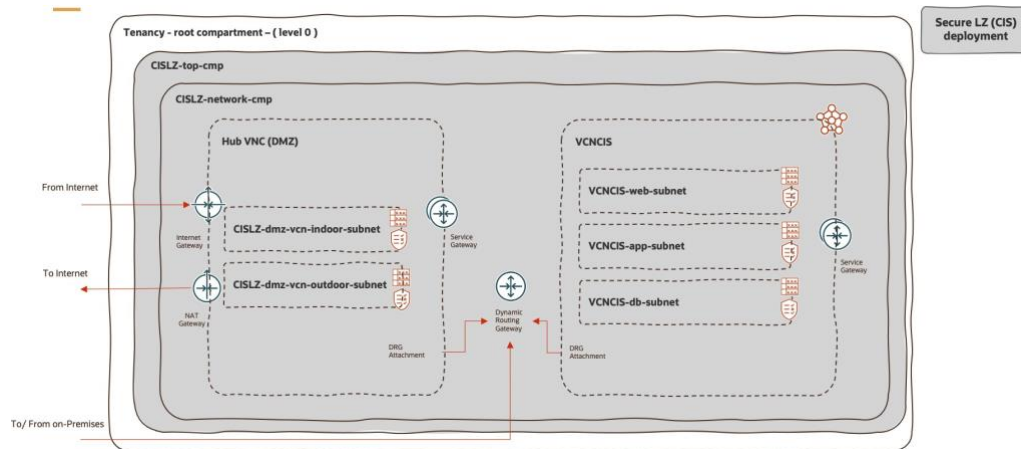
The number of additional bits with which to extend the DMZ VCN CIDR prefix. For instance, if the prefix of 'CIDR Block for the DMZ VCN' is 20 (/20) and 'Size of the DMZ Subnets CIDRs' is 4, subnets are going to be /24.

Note: To read more information about configuring a Security Partner Network Appliance with the CIS LZ v2 stack please go to this article or check the specific link

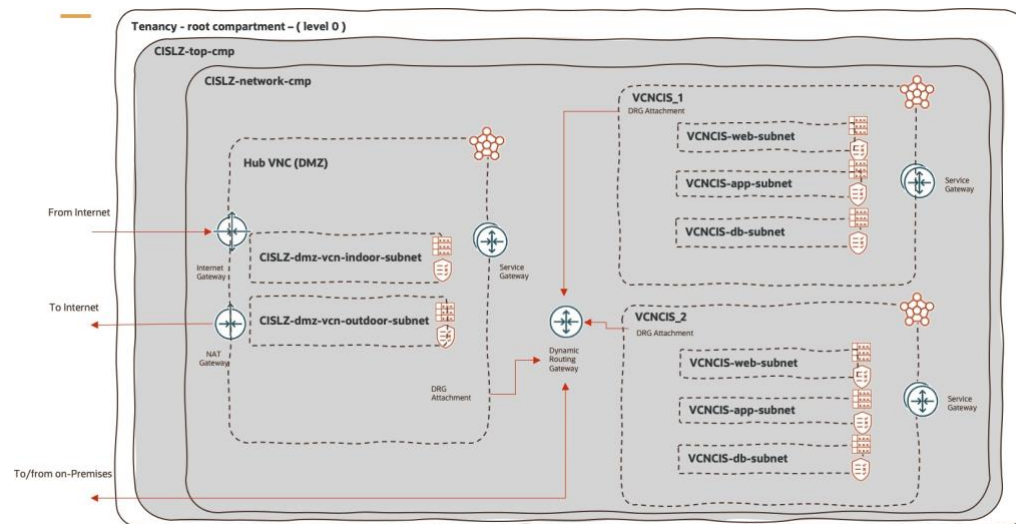
Check Point 1 for the Terraform stack to deploy the Cisco/Fortinet Firewall solution in a high-availability use case

- Cisco: Use [Terraform stack](#) to deploy Secure Firewall Threat Defense solution in an active-active use case.
- Fortinet: Use the [Terraform stack](#) to deploy the FortiGate Firewall solution in a high-availability use case.
- Palo Alto Networks: Use the [Terraform stack](#) to deploy VM-Series Firewall solution in a high-availability use case

This will be your network configuration after deploying the CIS stack. Example Hub VCN (DMZ VCN) for Check Point (2 subnets)



CIS stack support also multiple VCN deployments.



To define more than one VCN in the **Networking-Generic VCN** attributes you can define a list of CIDR blocks, each CIDR block corresponds to one VCN.

In this scenario, we have several VCNs connected to a single DRG, with all routing configured to send packets through a firewall in a hub VCN before they can be sent to another network.

For advanced or customized network deployments, go to the [CIS LZ v2 documentation](#).

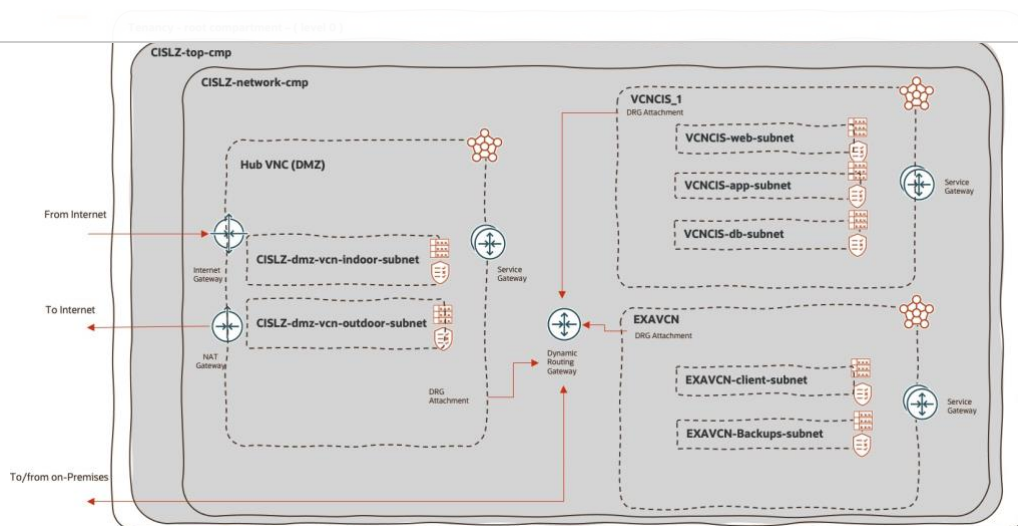
3.5 EXADATA VCN

Do you want to deploy a specific spoke VCN for Exadata deployment?

Optionally, the stack can provision one or more VCNs configured for Exadata deployments.

An EXADATA VCN is comprised of:

- One private client subnet.
- One private backup subnet.



To deploy and Spoke VCN for Exadata fill in the required values in the **Networking- Exadata Cloud Service VCNs** section.

In this case, we recommend selecting also the option **Create Compartment for Exadata Infrastructure**.

Networking - Exadata Cloud Service VCNs

Exadata VCNs CIDR Blocks (Must not overlap with 192.168.128.0/20) *Optional*

10.0.0.0/20 x

CIDR blocks for the Exadata VCNs in CIDR notation. Be mindful about Exadata "Requirements for IP Address Space" in [OCI documentation](#). (Type the name and hit enter to enter multiple values, up to a maximum of 9)

☒ **Advanced Options**
Advanced options for Exadata Cloud service infrastructure.

Exadata VCNs Custom Names *Optional*

Select a value

The Exadata VCNs custom names, overriding the default Exadata VCNs names. Each provided name relates to one and only one VCN, the 'nth' value applying to the 'nth' value in 'CIDR blocks for Exadata VCNs'. (Type the name and hit enter to enter multiple values, up to a maximum of 9)

CIDR Blocks for Exadata VCNs Client Subnets (Must not overlap with 192.168.128.0/20) *Optional*

Select a value

List of CIDR blocks for the client subnets of Exadata Cloud Service VCNs, in CIDR notation. Each provided CIDR value relates to one and only one VCN, the 'nth' value applying to the 'nth' value in 'CIDR blocks for Exadata VCNs'. (Type the CIDR and hit enter to enter multiple values, up to a maximum of 9)

CIDR Blocks for Exadata Backup Subnets (Must not overlap with 192.168.128.0/20) *Optional*

Select a value

List of CIDR blocks for the backup subnets of Exadata Cloud Service VCNs, in CIDR notation. Each provided CIDR value relates to one and only one VCN, the 'nth' value applying to the 'nth' value in 'CIDR blocks for Exadata VCNs'. (Type the CIDR and hit enter to enter multiple values, up to a maximum of 9)

☒ **Create Compartment for Exadata Infrastructure?**
Whether a compartment for Exadata infrastructure should be created. If unchecked, Exadata infrastructure should be created in the database compartment.

To review more information about how to deploy an Exadata workload using CIS LZ v2 go [here](#).

3.6 BLOCK INTERNET ACCESS

Do you want to configure connectivity or do you want to block Internet Access?

By default, the stack deploys an Internet Gateway and a NAT Gateway. If you want to include a Bastion Service please provide the values of the next attributes:

☐ Block Internet Access?

Determines if the VCNs are directly connected to the Internet. If left unchecked, an Internet Gateway and NAT Gateway are created for Internet connectivity. If checked, Internet Gateway and NAT Gateway are NOT created. In this case, it is recommended to check 'Connect Landing Zone VCN(s) to on-premises network?' and provide values to 'On-premises Network CIDR Blocks' in the 'Networking - Connectivity to On-Premises' section below, or your OCI network will not have any entry points.

Bastion Inbound SSH and RDP CIDR Blocks *Optional*

Select a value

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)

Load Balancer Inbound HTTPS CIDR Blocks *Optional*

Select a value

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)

NAT Outbound HTTPS CIDR Blocks *Optional*

Select a value

List of external IP ranges in CIDR notation for HTTPS outbound connections. Applies to connections made over NAT Gateway. (Type the name and hit enter to enter multiple values)

In this case, it is recommended to check **Connect Landing Zone VCN(s) to the on-premises network** and provide values to 'On-premises Network CIDR Blocks' or your OCI network will not have any entry points.

Networking - Connectivity to On-Premises

☒ Connect Landing Zone VCN(s) to on-premises network?

Whether the VCNs are connected to the on-premises network, in which case a DRG is attached to the VCNs. 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.) Required if 'Existing DRG OCID' is not provided and 'Block Internet Access?' is checked.

On-premises Network CIDR Blocks *Optional*

Select a value

List of on-premises IP ranges allowed to connect to the Landing Zone network via a DRG. The blocks are added to route rules and NSGs. If 'Block Internet Access?' is checked, it's advised to provide values here, or your OCI network will not have any entry points.

On-premises network CIDR Blocks Allowed to Connect over SSH and RDP *Optional*

Select a value

List of on-premises IP ranges allowed to make SSH and RDP inbound connections.

For more information check the detailed definition of these values [here](#).

Otherwise, if you want to block access, it is recommended to select the option **Block Internet Access** and leave the other values of the Network section blank. In this case, any Internet Gateway or NAT Gateway will be deployed.

Networking - Public Connectivity

☒ Block Internet Access?

Determines if the VCNs are directly connected to the Internet. If left unchecked, an Internet Gateway and NAT Gateway are created for Internet connectivity. If checked, Internet Gateway and NAT Gateway are NOT created. In this case, it is recommended to check 'Connect Landing Zone VCN(s) to on-premises network?' and provide values to 'On-premises Network CIDR Blocks' in the 'Networking - Connectivity to On-Premises' section below, or your OCI network will not have any entry points.

3.7 NOTIFICATIONS

Configure events and notifications

Network Admin Email Endpoints and **Secure Admin Email Endpoints** are mandatory attributes. You need to configure an email where network and security notifications will be sent.

The stack lets you configure additional Notification Endpoints in the case where needed.

Events and Notifications

Network Admin Email Endpoints

Select a value

List of email addresses for all network related notifications. (Type an email address and hit enter to enter multiple values)

 This variable is required.

Security Admin Email Endpoints

Select a value

List of email addresses for all security related notifications. (Type an email address and hit enter to enter multiple values)

 This variable is required.

☐ Additional Notification Endpoints

Allows for notifications that are not required by CIS Benchmark.

To create them with enable status you need to specify the option **Create alarms as enabled?** and **Create events as enabled?**

- ☒ **Create alarms as enabled?**
Whether a alarms should be created in an enabled state by default. If unchecked, alarms will be created but not emit alerts.
- ☒ **Create events as enabled?**
Whether events should be created in an enabled state by default. If unchecked, events will be created but not emit notifications.

3.8 OBJECT STORAGE

Do you want to deploy an Object Storage?

Whether an Object Storage bucket should be enabled.

If true, the bucket is managed in the application (AppDev) compartment.

Providing an encryption key is optional.

If a key is not provided and 'CIS Level' is set to 2, the Landing Zone will manage the key.

Object Storage

- ☐ **Enable Object Storage bucket?**
Whether an Object Storage bucket should be enabled. If true, the bucket is managed in the application (AppDev) compartment. Providing an encryption key is optional. If a key is not provided and 'CIS Level' is set to 2, the Landing Zone will manage the key.

3.9 CLOUD GUARD

Do you want to disable Cloud Guard monitoring?

- Oracle Cloud Guard is a native OCI service and is provided [free of cost](#) for OCI security posture monitoring.
- At a very high level, Cloud Guard uses Detector recipes to monitor Targets, which are OCI Compartment hierarchies, for misconfigurations and risky actions by users and emits findings known as Problems.
- OCI Landing Zone enables Cloud Guard monitoring in a tenancy by default.
- You can leave the default values or you can customize the CIS LZ v2 Cloud Guard deployment.

Cloud Guard

Cloud Guard Configuration Status

ENABLE

Determines whether a Cloud Guard target should be created for the Root compartment. If 'ENABLE', Cloud Guard is enabled and a target is created for the Root compartment. Make sure there is no pre-existing Cloud Guard target for the Root compartment or target creation will fail. If there's a pre-existing Cloud Guard target for the Root compartment, use 'DISABLE'. In this case, any pre-existing Cloud Guard Root target is left intact. However, keep in mind that once you use 'ENABLE', the Root target becomes managed by Landing Zone. If later on you switch to 'DISABLE', Cloud Guard remains enabled but the Root target is deleted.

Minimum Risk Level Threshold

High

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.

Cloud Guard Admin Email Endpoints *Optional*

Select a value

List of email addresses for Cloud Guard related notifications. (Type an email address and hit enter to enter multiple values)

- Customers who want to consolidate Cloud Guard Problems into their preferred SIEM and SOAR systems or take actions based on them can make use of the integration capabilities provided by the [Event Service](#) or [Cloud Guard APIs](#) and OCI SDKs for their favorite programming languages. [OCI Service Connector Hub](#) also provides rich integration capabilities to achieve various integration use cases.
- To review more information about the Cloud Guard configuration included in the CIS LZ v2 go [here](#).

3.10 SECURITY ZONES

Do you want to enable Security Zones?

Determines if Security Zones are enabled in Landing Zone compartments.

To know more about secure zones go [here](#).

Security Zones

- ☐ **Enable Security Zones**
Determines if Security Zones are enabled in Landing Zone compartments.

3.11 LOGGING CONSOLIDATION

Do you need to deploy a service connector?

Whether Service Connector should be enabled.

If true, a single Service Connector is managed for all services log sources and the designated target specified in 'Service Connector Target Kind'.

The Service Connector resource is created in an INACTIVE state.

To activate, check 'Activate Service Connector?' (costs may incur).

Logging Consolidation: Service Connector Hub

☐ Enable Service Connector?

Whether Service Connector should be enabled. If true, a single Service Connector is managed for all services log sources and the designated target specified in 'Service Connector Target Kind'. The Service Connector resource is created in INACTIVE state. To activate, check 'Activate Service Connector?' (costs may incur).

3.12 VULNERABILITY SCANNING

Do you want to disable VSS?

Scanning for vulnerabilities is a must for any security-conscious organization. At a high level, VSS works by defining recipes and targets. A recipe sets the scanning parameters for a resource, including what to scan and how often.

As VSS is a free service, Landing Zone enables it by default, creating a default recipe and four scanning targets, one for each Landing Zone compartment. The default recipe is set to execute weekly on Sundays, which can be easily changed when provisioning the Landing Zone.

Vulnerability Scanning

☒ Enable Vulnerability Scanning?

Whether Vulnerability Scanning should be enabled. If checked, a scanning recipe is enabled and scanning targets are enabled for each Landing Zone compartment.

Scanning Schedule *Optional*

WEEKLY

When to scan. WEEKLY or DAILY.

Scanning Day *Optional*

SUNDAY

The day when to scan. Applies to weekly scans only.

Port Scan Level *Optional*

STANDARD

Checks for open ports using a network mapper that searches your public IP addresses. STANDARD checks the 1000 most common port numbers. LIGHT checks the 100 most common port numbers. NONE does not check for open ports.

Agent Scan Level *Optional*

STANDARD

Checks for open ports on both public and private IP addresses, OS vulnerabilities, compliance with industry benchmarks, vulnerabilities in third-party application files (for application files scanning, check 'Enable File Scanning' below).

Agent CIS Benchmark Settings Scan Level *Optional*

MEDIUM

Checks targets for compliance with industry-standard benchmarks published by the Center for Internet Security (CIS)

☐ Enable File Scanning?

Whether file scanning is enabled.

To review more information about the VSS configuration included in the CIS LZ v2 go [here](#).

3.13 COST MANAGEMENT

Do you want to deploy a Cost Management Budget?

If checked, a budget will be created at the enclosing compartment based on forecast spending.

Cost Management

☐ Create a default budget?

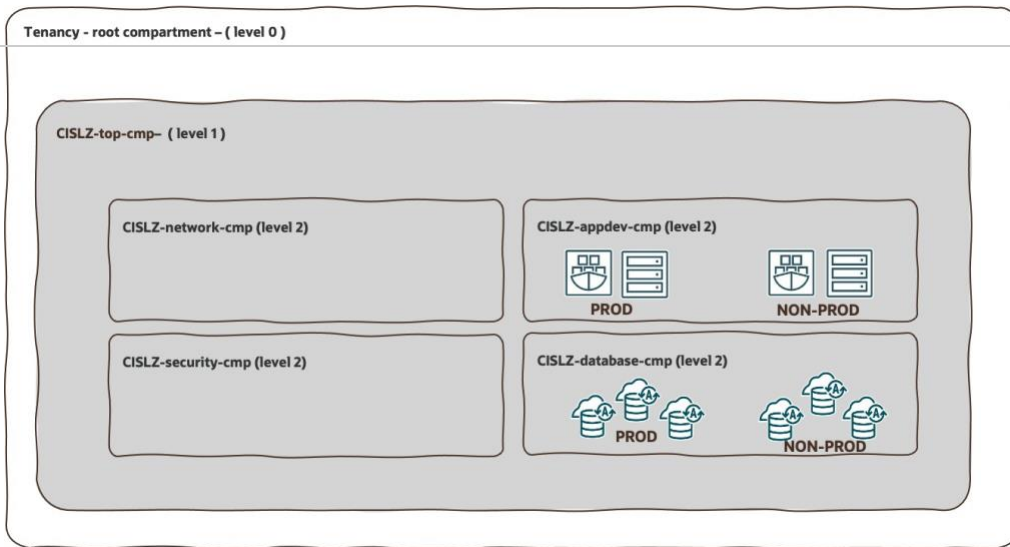
If checked, a budget will be created at the root or enclosing compartment and based on forecast spend.

3.14 MULTIPLE WORKLOADS

For this scenario, there are some proposed recommendations that will improve security and manageability.

SCENARIO A. Leave CIS LZ v2 default values.

If you deploy multiple databases and apps in an LZ deployed using the default values for the CIS LZ v2 configuration, they can have network isolation at the spoke level and will share the same compartments. You will be also sharing groups and policies.



SCENARIO B. Create additional compartments

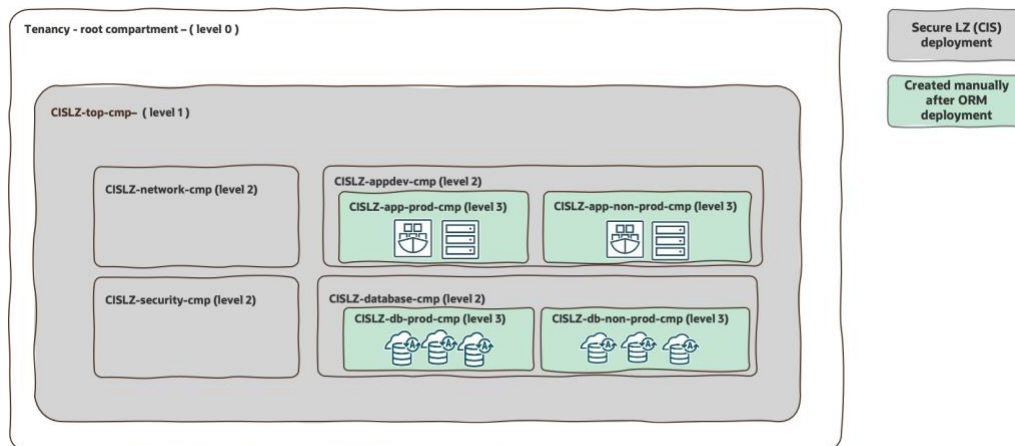
- To improve manageability and security we recommend you create specific compartments for PROD and NON-PROD workloads. On a deeper level, if it is a customer requirement, you can create even one compartment per workload.
- The default CIS LZ v2 policies and permissions will be inherited for managing the workloads in the created child compartments, meaning that it's going to be the same groups with permissions across all compartments.
- The compartment and security design will depend on the customer's organization and requirements.

Here we show you some examples:

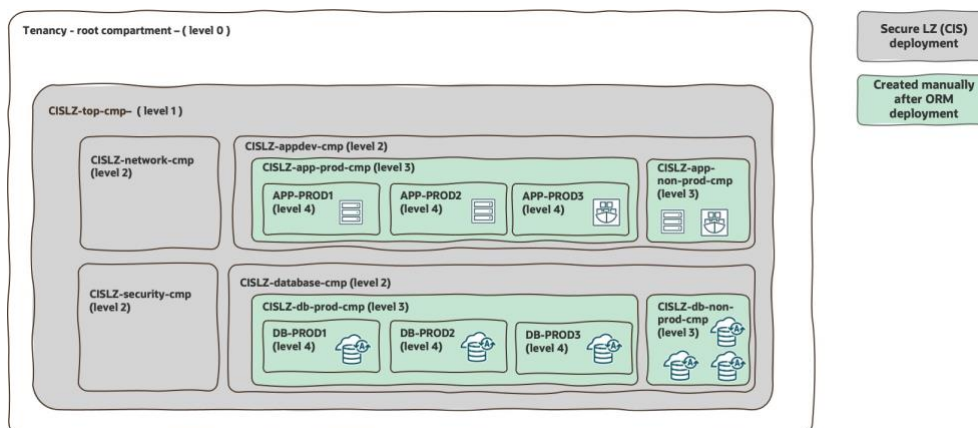
"Green" compartments have to be created manually after deploying the CIS LZ v2 stack.

Note: Remember there is a limitation, you can create subcompartments in compartments to create hierarchies that are six levels deep maximum.

B1) Layer-Driven Organization with Prod/Non-Prod segregation

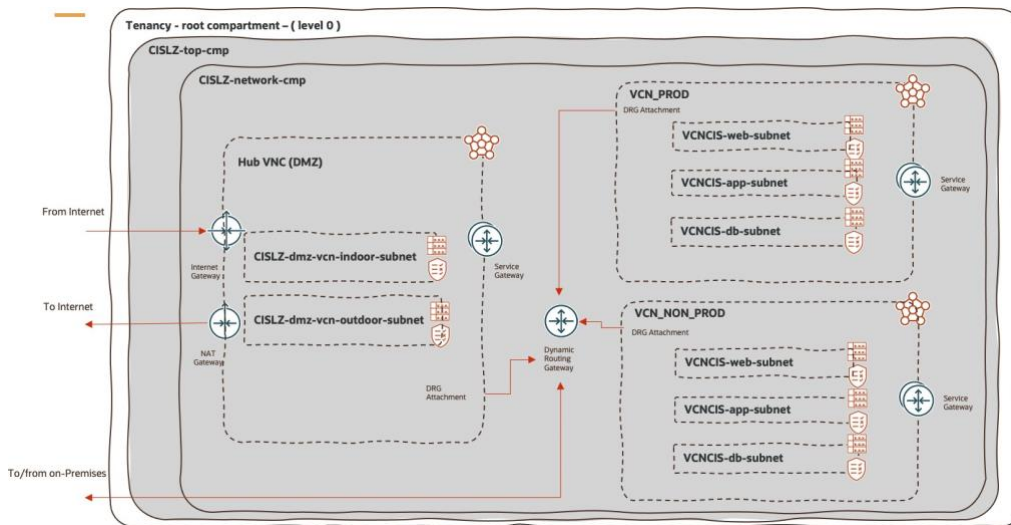


B2) Layer-Driven Organization with Prod/Non-Prod and Application Segregation



Another way to improve security is by defining a Hub&Spoke network design. (Review step 3.3 HUB & SPOKE)

In this example we have one spoke for PROD workloads and another for NON-PROD workloads. The Hub&Spoke design will depend on the customer's organization and requirements.



SCENARIO D. Hub & Spoke and Different Compartments

Include both improvements, create additional compartments to have a compartment hierarchy design, and deploy a Hub&Spoke network.

If you design a specific compartment architecture workload distribution, it will be important to include also network segregation for these workloads (Hub& Spoke).

		COMPARTMENT HIERARCHY	HUB&SPOKE
SCENARIO D		●	●
SCENARIO C			●
SCENARIO B		●	
SCENARIO A	●		

Improve security and manageability

→

3.15 OTHER SCENARIOS

For any other advanced scenario or customized issue not included in this asset go to the [CIS LZ v2 documentation](#).

4. EXECUTE TERRAFORM PLAN

After completing the previous steps, create the new stack.

Create stack

1 Stack information

2 Configure variables

3 Review

Verify your configuration variables, and then create your stack. Due to limited space, we show only variables without default values or that you edited.

Stack information

Name

oci-cis-landingzone-quickstart

Description

...fices. Show Copy

Compartment

...mhakaa Show Copy

Terraform version

1.1.x

Environment

Region

eu-frankfurt-1

Service Label

CISLZ

Use an enclosing compartment?

true

Existing enclosing compartment

...mhakaa Show Copy

Previous

Create

Cancel

The new ORM stack will appear in the OCI Console.

Resource Manager • Stacks • Stack details

RMS

ACTIVE

oci-cis-landingzone-quickstart-Customer

Edit

Plan

Apply

Destroy

More actions

Stack information

Tags

Description: A stack to deploy a set of CIS (Center for Internet Security) compliant resources in an OCI tenancy. The Secure Landing Zone is the combination of CIS Foundations Benchmark for OCI with OCI architecture best practices.

Compartment: oci4oca (root)

OCID: ...2fk3jq Show Copy

Terraform configuration: Upload Download

Working directory: oci-cis-landingzone-quickstart-main/config

Created: Thu, Oct 6, 2022, 07:30:04 UTC

Terraform version: 1.1.x

Jobs

A job is created when you run a Terraform action on a stack. Use these Terraform actions to plan, provision, and destroy your OCI resources according to your configuration. You can also import state files.

Name	Type	State	Start time	End time	State file
No items					

We choose "Plan" to start the Terraform Plan job.

Resource Manager • Stacks • Stack details

RMS

ACTIVE

oci-cis-landingzone-quickstart-Customer

Edit

Plan

Apply

Destroy

More actions

Stack information

Tags

Description: A stack to deploy a set of CIS (Center for Internet Security) compliant resources in an OCI tenancy. The Secure Landing Zone is the combination of CIS Foundations Benchmark for OCI with OCI architecture best practices.

OCID: ...2fk3jq Show Copy

Working directory: oci-cis-landingzone-quickstart-main/config

Terraform version: 1.1.x


Plan

[Help](#)

Name *Optional*

plan-job-20220916154135

Show advanced options



ACTIVE

oci-cis-landingzone-quickstart-Customer

Edit Plan Apply **Destroy** More actions

Stack information Tags

Description: A stack to deploy a set of CIS (Center for Internet Security) compliant resources in an OCI tenancy. The Secure Landing Zone is the combination of CIS Foundations Benchmark for OCI with OCI architecture best practices.

Compartment: oci4cca (root)

OCID: ...2fx3jq [Show](#) [Copy](#)

Terraform configuration: [Upload](#) [Download](#)

Working directory: oci-cis-landingzone-quickstart-main/config

Created: Thu, Oct 6, 2022, 07:30:04 UTC

Terraform version: 1.1.x

Resources

Jobs

A [job](#) is created when you run a Terraform action on a [stack](#). Use these Terraform actions to [plan](#), [provision](#), and [destroy](#) your OCI resources according to your configuration. You can also

Name	Type	State	Start time	End time
plan-job-20221006093034	Plan	Succeeded	Thu, Oct 6, 2022, 07:32:36 UTC	Thu, Oct 6, 2022, 07:33:03 UTC

When the plan phase job ends we can review and confirm all the resources that will be created.


Note: The number of resources created will depend on the selected configuration.

```
Plan: 98 to add, 0 to change, 0 to destroy.
```

5. EXECUTE TERRAFORM APPLY

When all results of the previous steps align with expectations, you can move to the final step to deploy all resources in the tenancy.

Choose "Apply" to start the job that created all the landing zone resources in your tenancy.



ACTIVE

oci-cis-landingzone-quickstart-Customer

Edit Plan **Apply** **Destroy** More actions

Stack information Tags

Description: A stack to deploy a set of CIS (Center for Internet Security) compliant resources in an OCI tenancy. The Secure Landing Zone is the combination of CIS Foundations Benchmark for OCI with OCI architecture best practices.

OCID: ...2fx3jq [Show](#) [Copy](#)

Working directory: oci-cis-landingzone-quickstart-main/config

Terraform version: 1.1.x

Apply

[Help](#)

Name *Optional*

apply-job-20220916154607

Apply job plan resolution

Automatically approve

Choose either automatic approval or the latest successful plan job

Resources defined by this stack will be deployed immediately. If you want to remove these resources later, you can run the destroy job for this stack.

[Show advanced options](#)


You can review the progress of the **apply** phase job by checking the log.

Logs

```
Download logs Show timestamps

module.workload.random_id.suffix: Creation complete after 0s [id=0-609001Fs]
random_id.suffix: Creating...
random_id.suffix: Creation complete after 0s [id=8tcmhucrg]
module.budget-topics.oc1_notifications_topic.budget_topics: Creating...
module.workload.module.groups[0].oci_identity_group.workload_admins_group: Creating...
module.workload.module.groups[0].oci_identity_group.workload_storage_users_group: Creating...
module.workload.module.groups[0].oci_identity_group.workload_users_group: Creating...
module.workload.module.groups[0].oci_identity_group.workload_storage_admins_group: Creating...
module.parent-compartment.oc1_identity_compartment.parent_compartment: Creating...
module.budget-topics.oc1_notifications_topic.budget_topics: Creation complete after 1s [id=ocid1.onstopic.oc1.eu-frankfurt-1.aaaaaaaht2bl7c3d712ukkbvas7pjtftyg61dhdzml16vjronlswa]
module.budget-notifications.oc1_events_rule.budget_notification: Creating...
module.budget-notifications.oc1_events_rule.budget_notification: Creation complete after 1s [id=ocid1.eventrule.oc1.eu-frankfurt-1.abtheljrfjxb4j1l7moj4qnmrnns75w6at1krm2g4pxsaoe7ydl1hbta]
module.workload.module.groups[0].oci_identity_group.workload_storage_users_group: Creation complete after 3s [id=ocid1.group.oc1..aaaaaaaavzdoae6sgjy84ruj6xjcgdewpdjybvryx664k642rosiaq]
module.workload.module.groups[0].oci_identity_group.workload_admins_group: Creation complete after 3s [id=ocid1.group.oc1..aaaaaaaah4yuef6wrgjrtkxtpoc15fdicq9wqz5ygrlnezh1r1geaq]
module.workload.module.groups[0].oci_identity_group.workload_admins_group: Creation complete after 3s [id=ocid1.group.oc1..aaaaaaaq8zqgdj3i4ebax7jshic2wqjzmn1ff3dp246jssroexwpj6a]
module.workload.module.groups[0].oci_identity_group.workload_users_group: Creation complete after 3s [id=ocid1.group.oc1..aaaaaaaepqwnkfh7b3fzabvhyj32x74m3j15iv4ou5gqkpd14v16x1lta]
module.parent-compartment.oc1_identity_compartment.parent_compartment: Still creating... [10s elapsed]
module.parent-compartment.oc1_identity_compartment.parent_compartment: Still creating... [20s elapsed]
module.parent-compartment.oc1_identity_compartment.parent_compartment: Still creating... [20s elapsed]
module.parent-compartment.oc1_identity_compartment.parent_compartment: Still creating... [40s elapsed]
module.parent-compartment.oc1_identity_compartment.parent_compartment: Creation complete after 44s [id=ocid1.compartment.oc1..aaaaaaaecqbpeilxafcdckpuf4mryywcqz46aphda52bz3v3bduts4jsnq]
module.parent-compartment.time_sleep.wait_90_seconds: Creating...
module.parent-compartment.time_sleep.wait_90_seconds: Still creating... [10s elapsed]
module.parent-compartment.time_sleep.wait_90_seconds: Still creating... [20s elapsed]
module.parent-compartment.time_sleep.wait_90_seconds: Still creating... [40s elapsed]
module.parent-compartment.time_sleep.wait_90_seconds: Still creating... [40s elapsed]
module.parent-compartment.time_sleep.wait_90_seconds: Still creating... [40s elapsed]
```

You can confirm how the job ends successfully or if there are any errors.



oci-cis-landingzone-quickstart-Customer

Edit Plan Apply Destroy More actions

Stack information Tags

Description: A stack to deploy a set of CIS (Center for Internet Security) compliant resources in an OCI tenancy. The Secure Landing Zone is the combination of CIS Foundations Benchmark for OCI with OCI architecture best practices.

OCID: ...2fx3jq [Show](#) [Copy](#)

Working directory: oci-cis-landingzone-quickstart-main/config

Terraform version: 1.1.x

Compartment: oc14cca (root)


Terraform configuration: [Upload](#) [Download](#)

Created: Thu, Oct 6, 2022, 07:30:04 UTC

Jobs

A [job](#) is created when you run a Terraform action on a [stack](#). Use these Terraform actions to [plan](#), [provision](#), and [destroy](#) your OCI resources according to your configuration. You can also [import](#) state files.

Name	Type	State	Start time	End time
apply-job-20221006093515	Apply	In progress	Thu, Oct 6, 2022, 07:35:17 UTC	-
plan-job-20221006093234	Plan	Succeeded	Thu, Oct 6, 2022, 07:32:36 UTC	Thu, Oct 6, 2022, 07:33:03 UTC



Baseline landing zone sandbox-customer

Edit Plan Apply **Destroy** More actions

Stack information Tags

Description: Landing zone sandbox developed by OCI

OCID: ...w43rky [Show](#) [Copy](#)

Created: Fri, Sep 16, 2022, 13:39:32 UTC

Compartment: oc14cca (root)

Terraform configuration: [Download](#)

Terraform version: 1.0.x

Jobs

A [job](#) is created when you run a Terraform action on a [stack](#). Use these Terraform actions to [plan](#), [provision](#), and [destroy](#) your OCI resources according to your configuration. You can also [import](#) state files.

Name	Type	State	Start time	End time
apply-job-2022091614607	Apply	Succeeded	Fri, Sep 16, 2022, 13:51:11 UTC	Fri, Sep 16, 2022, 13:59:38 UTC
plan-job-2022091614135	Plan	Succeeded	Fri, Sep 16, 2022, 13:41:44 UTC	Fri, Sep 16, 2022, 13:42:15 UTC

```
Apply complete! Resources: 65 added, 0 changed, 0 destroyed.

Outputs:

compartments_map = {
  "Applications" = "ocid1.compartment.oc1..aaaaaaa03ojx46n3azr147zsoecnjz16354ymxb64holastunxq3vkrfea"
  "Common-Infra" = "ocid1.compartment.oc1..aaaaaaaahdtqy7cj35ndnjaloup24ehpyioemcnz43cyd8eqah31345q"
  "Network" = "ocid1.compartment.oc1..aaaaaaaasooyohrwfbhknulcjewtajv6gpjt4o4cca5fuan7654qarvzrtq"
  "Security" = "ocid1.compartment.oc1..aaaaaaa47wn2edlnqtfjswjtgqbtfgupcjovqz2ndzy7zowvb4c3jwicqa"
  "baseline_lz_sandbox" = "ocid1.compartment.oc1..aaaaaaaecqbpeilxafcdckpuf4mryywcqz46aphda52bz3v3bduts4jsnq"
}
more_info_url = "https://github.com/oracle-quickstart/oci-enterprise-scale-baseline-landing-zone"
subnet_map = {}
vcn_ocid = "ocid1.vcn.oc1.eu-frankfurt-1.aaaaaattkvkka2zaxo7hiyqoymp715ddsqcpj22whepyygfuf6yt3asuua"
```

Under **Resource Manager > Stacks > Stack details > Job details** (of your apply phase job) you can check all the resources created.

Resources			
Logs	Name	Type	Attributes
Variables	ArchitectureCenter/cis-oci-landing-zone-quickstart-CISLZ	oci_identity_tag_namespace	10 attributes Show Copy
Job resources	CISLZ-0-app-subnet	oci_core_subnet	23 attributes Show Copy
Outputs	CISLZ-0-app-subnet-flow-log	oci_logging_log	15 attributes Show Copy
View state	CISLZ-0-app-subnet-rtable	oci_core_route_table	10 attributes Show Copy
	CISLZ-0-app-subnet-security-list	oci_core_security_list	11 attributes Show Copy
	CISLZ-0-db-subnet	oci_core_subnet	23 attributes Show Copy
	CISLZ-0-db-subnet-flow-log	oci_logging_log	15 attributes Show Copy
	CISLZ-0-db-subnet-rtable	oci_core_route_table	10 attributes Show Copy
	CISLZ-0-db-subnet-security-list	oci_core_security_list	11 attributes Show Copy
	CISLZ-0-vcn	oci_core_vcn	21 attributes Show Copy
	CISLZ-0-vcn-app-nsg	oci_core_network_security_group	9 attributes Show Copy
	CISLZ-0-vcn-bastion-nsg	oci_core_network_security_group	9 attributes Show Copy
	CISLZ-0-vcn-db-nsg	oci_core_network_security_group	9 attributes Show Copy
	CISLZ-0-vcn-igw	oci_core_internet_gateway	11 attributes Show Copy
	CISLZ-0-vcn-lbr-nsg	oci_core_network_security_group	9 attributes Show Copy
	CISLZ-0-vcn-natgw	oci_core_nat_gateway	13 attributes Show Copy
	CISLZ-0-vcn-sgw	oci_core_service_gateway	12 attributes Show Copy
	CISLZ-0-web-subnet	oci_core_subnet	23 attributes Show Copy

6. POST-DEPLOYMENT ACTIONS

After successful deployment, you might still need to perform some actions, like validations of add-on customization. All these actions are optional and you can find below some examples.

6.1 SETUP MULTIPLE WORKLOADS

If you need to deploy multiple workloads and you have chosen scenario B, C, or D during step 3.14, create manually your compartments in this step.

6.2. CONFIRM CIS COMPLIANCE

After the CIS LZ v2 deployment, do you want to confirm your CIS compliance?

In the CIS [GitHub](#) repository, there is a Python script that performs compliance checks for most of the CIS OCI Foundations Benchmark recommendations. The script is completely independent of the Terraform code and can be used against any existing tenancy.

For more information, we recommend you check this [documentation](#).

6.3. DESTROY THE STACK RESOURCES

- Remove all the resources created manually after deploying the CIS Landing Zone v2.
- Run the destroy phase in the ORM stack

Resource Manager
Stack
Compartment

Overview
Stacks
Jobs
Private templates
Configuration source providers
Private endpoints
List scope
Compartment


Templates are now available for creating stacks. Use a template to deploy cloud resources from a provided Terraform configuration.

A stack is a [Terraform configuration](#) that you can use to provision and manage your OCI resources. To provision the resources defined in your stack, [copy the configuration](#).

Create stack

Name	Description	State	Created
oci-cis-landingzone-quickstart-Customer	A stack to deploy a set of CIS (Center for Internet Security) compliant resources in an OCI tenancy. The Secure Landing Zone is the combination of CIS Foundations Benchmark for OCI with OCI architecture best practices.	Active	Thu, Oct 6, 2022, 07:30:04 UTC

Resource Manager > Stacks > Stack details



ACTIVE

oci-cis-landingzone-quickstart-Customer

Edit
Plan
Apply
Destroy
More actions

Stack information
Tags

Description: A stack to deploy a set of CIS (Center for Internet Security) compliant resources in an OCI tenancy. The Secure Landing Zone is the combination of CIS Foundations Benchmark for OCI with OCI architecture best practices.

OCID: ...2fx3jq [Show](#) [Copy](#)

Working directory: oci-cis-landingzone-quickstart-main/config

Terraform version: 1.1.x

Review KNOWN ISSUES if you have any errors during the destroy phase. OCI COMPARTMENT DELETION ISSUE is a common issue.

- Delete the stack.

Create stack				
Name	Description	State	Created	
oci-cis-landingzone-jumpstart-Customer	A stack to deploy a set of CIS (Center for Internet Security) compliant resources in an OCI tenancy. The Secure Landing Zone is the combination of CIS Foundations Benchmark for OCI with OCI architecture best practices.	Active	Thu, Oct 6, 2022, 07:30:04 UTC	View stack details
Baseline landing zone sandbox-0220928154521	Landing zone sandbox developed by OCI	Active	Wed, Sep 28, 2022, 13:45:24 UTC	Edit
Baseline landing zone sandbox-0220911154943	Landing zone sandbox developed by OCI	Active	Wed, Sep 14, 2022, 13:49:49 UTC	Open support request
				Delete

7. KNOWN ISSUES

7.1 OCI TIMEOUT ISSUE

Description

Error: timeout while waiting for state to become 'DELETED' (last state: 'DELETING', timeout: 1h30m0s), you may need to increase the Terraform Operation timeouts for your resource to continue polling for longer

Analysis

This is a Terraform Provider error.

Error: Operation Timeout Provider version: <provider_version>, released on <release_date>. This provider is <n> updates behind to current. Service: <service> Error Message: timeout while waiting for state to become 'SUCCEEDED, FAILED, CANCELED' (last state: 'IN_PROGRESS', timeout: 15m)

Specified OCI service is indicating that the resource has not yet reached the expected state after polling for some time.

Workaround

You may need to increase the operation timeout for your resource to continue polling for longer. See [Operation Timeouts](#) for details on how to do this.

https://docs.oracle.com/en-us/iaas/Content/API/SDKDocs/terraformtroubleshooting.htm#common_issues

Note: The operation timeout can not be increased in an ORM stack.

Check Job Resources (in the **stack destroy job**) to see the resources that remain after the destroy phase. The most common situation is that the only remaining resources are compartments.

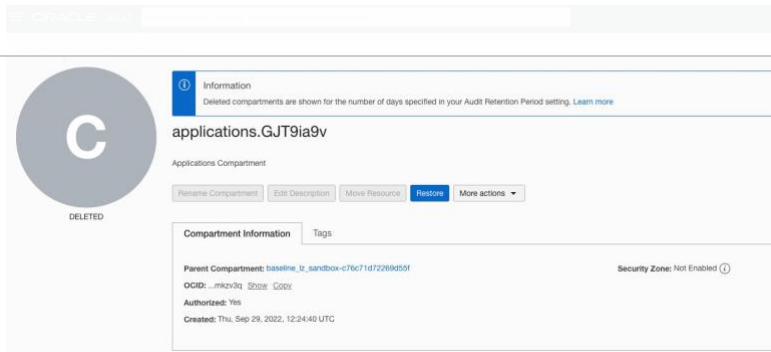
Resources	
Logs	
Variables	
Job resources	
Outputs	
View state	

Resources	
Name	Type
Applications	oci_identity_compartment
Common-Infra	oci_identity_compartment
Network	oci_identity_compartment
Security	oci_identity_compartment
baseline_lz_sandbox-c76c71d72269d55f	oci_identity_compartment
managed.random_id.suffix.0	random_id
managed.time_sleep.wait_90_seconds.0	time_sleep

You can confirm if the compartment appears but is in a DELETED state.

Resources	
Logs	
Variables	
Job resources	
Outputs	
View state	

Resources	
Name	Type
Applications	oci_identity_compartment
Common-Infra	oci_identity_compartment
Network	oci_identity_compartment
Security	oci_identity_compartment
baseline_lz_sandbox-c76c71d72269d55f	oci_identity_compartment
managed.random_id.suffix.0	random_id
managed.time_sleep.wait_90_seconds.0	time_sleep



In this case, you can proceed and delete the stack.

If the only remaining resources are compartments, remove the compartments, and later remove the stack.

7.2 OCI COMPARTMENT DELETION ISSUE

Description

Destroys phase does not remove compartment resources.

Analysis

By design, OCI compartments are not deleted upon Terraform destroy by default.

For more information about deleting compartments in OCI via Terraform, check [OCI Terraform provider documentation](#).

In some cases, not deleting compartments is ok if you plan on reusing them.

Note: Deletion can be enabled in CIS Landing Zone v2 by setting `enable_cmp_delete` variable to true in locals.file. In our case, we are deploying using ORM and we can not enable this change.

Workaround

Remove the compartments manually.

7.3 OCI VAULT DELETION ISSUE

Description

You have deployed CIS Landing Zone v2 and a Vault resource has been created due scenario chosen. The destroys phase is failing with an error.

Analysis

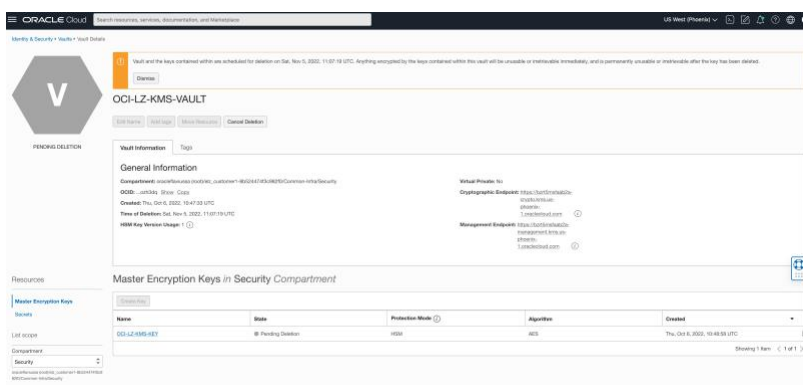
By design, OCI vaults and keys are not deleted immediately upon Terraform destroy, but scheduled for deletion. The Destroy job fails because the vault and the key created by the stack can not be deleted immediately. There is a cool-down period in which the Vault and Key are in a PendingDelete state. Because of this, the security compartment can't be deleted.

Workaround.

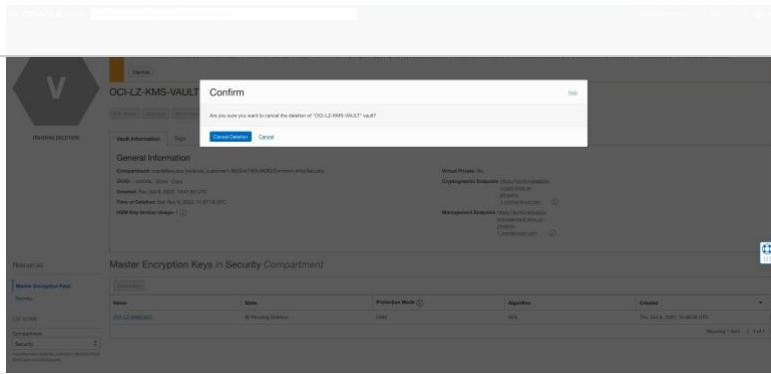
The workaround for this is to cancel deletion for the vault and move the vault and the key to a different compartment (outside the landing zone) and restart the destroy job. After the successful execution of the destroy job, the Vault (and Key) can be deleted manually.

Step by Step example.

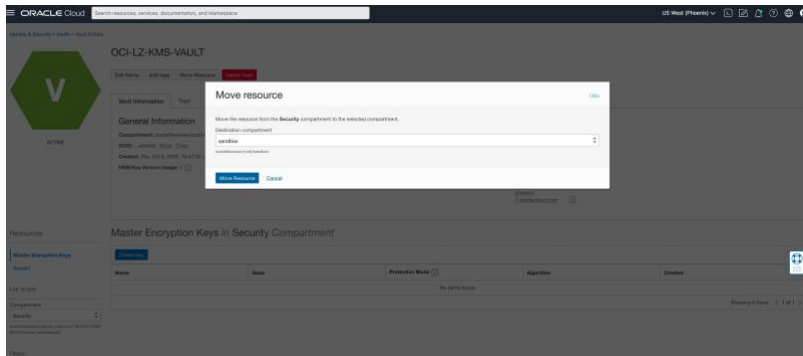
The vault is created by default in the Security compartment



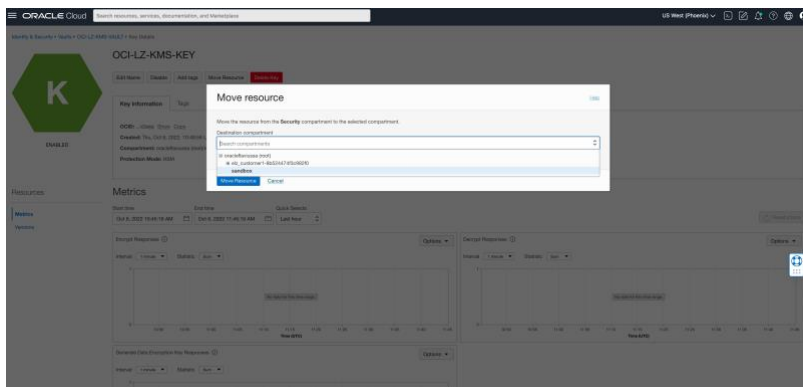
Click on **Cancel Deletion** button to cancel the deletion of the Vault resource. This action will restore the Master Key created as well.



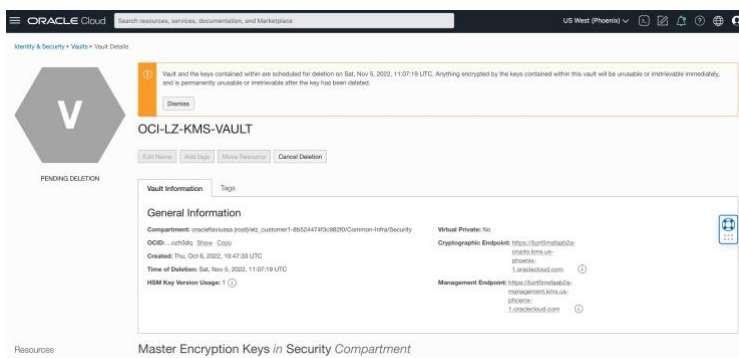
Move the Vault to a different compartment, outside the landing zone. In this example, the compartment is named "sandbox"



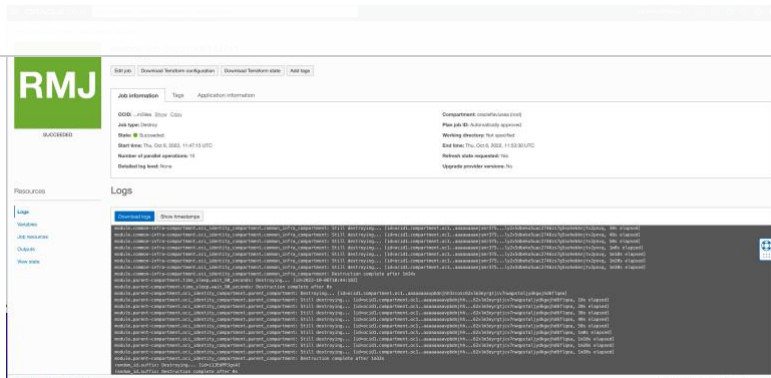
Move the master key to the same "sandbox" compartment



Delete the Vault, now in the "sandbox" compartment. This will delete the master key as well.



Run again the **Destroy** job and this time will finish successfully.



7.4 TOO MANY REQUESTS

Description

You run are running an apply or destroy job with ORM.

```
Error: 429-TooManyRequests
Provider version: 4.70.0, released on 2022-04-07. This provider is 25 Update(s) behind to current.
Service: Identity Tag
```

Error Message: Tenant has been throttled. Too Many Requests

Analysis

This is normal behavior.

Oracle Cloud Infrastructure applies **throttling** to many API requests to prevent accidental or abusive use of resources.

429 - Too Many Requests: System busy or Too many requests or User rate-limit exceeded - Oracle Cloud Infrastructure Anomaly Detection (Doc ID 2788403.1)

Workaround.

Wait some minutes and re-run the stack job.

To check more Know Issues go to the Internal CIS LZ v2 [Know Issues](#) documentation page.