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

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:

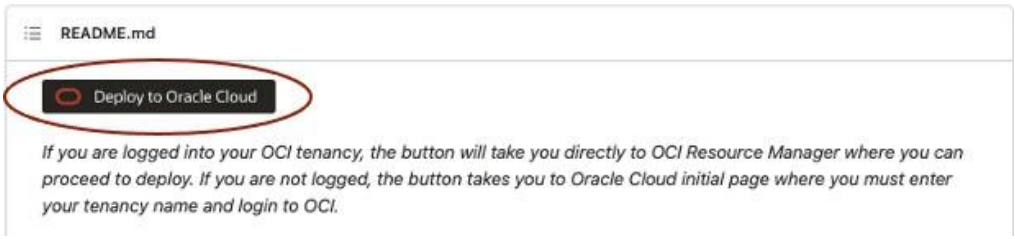
- A paid tenancy, the always-free account is not supported.
- An OCI account with sufficient privileges to deploy the landing zone. (admin of your tenancy).
- Terraform >= 0.13.x

---

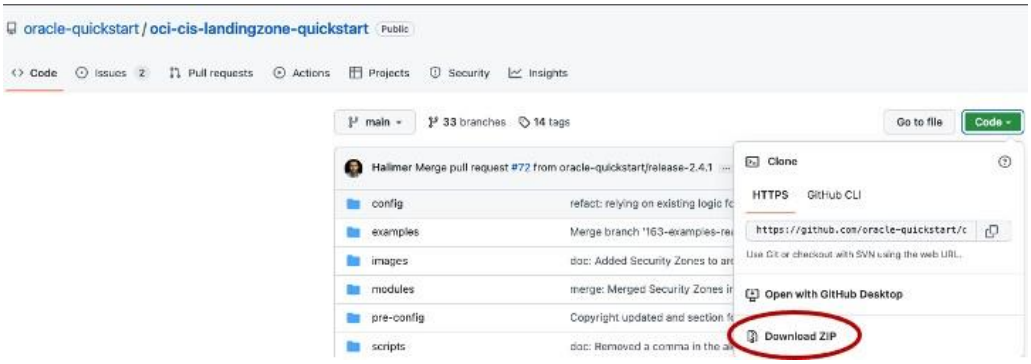
2. DEPLOYMENT - HOW TO DEPLOY CIS Landing Zone v2 USING ORM

2.1 CREATE A NEW ORM STACK

Go to the GitHub repository and select the option **Deploy to Oracle Cloud** to lunch the CIS stack



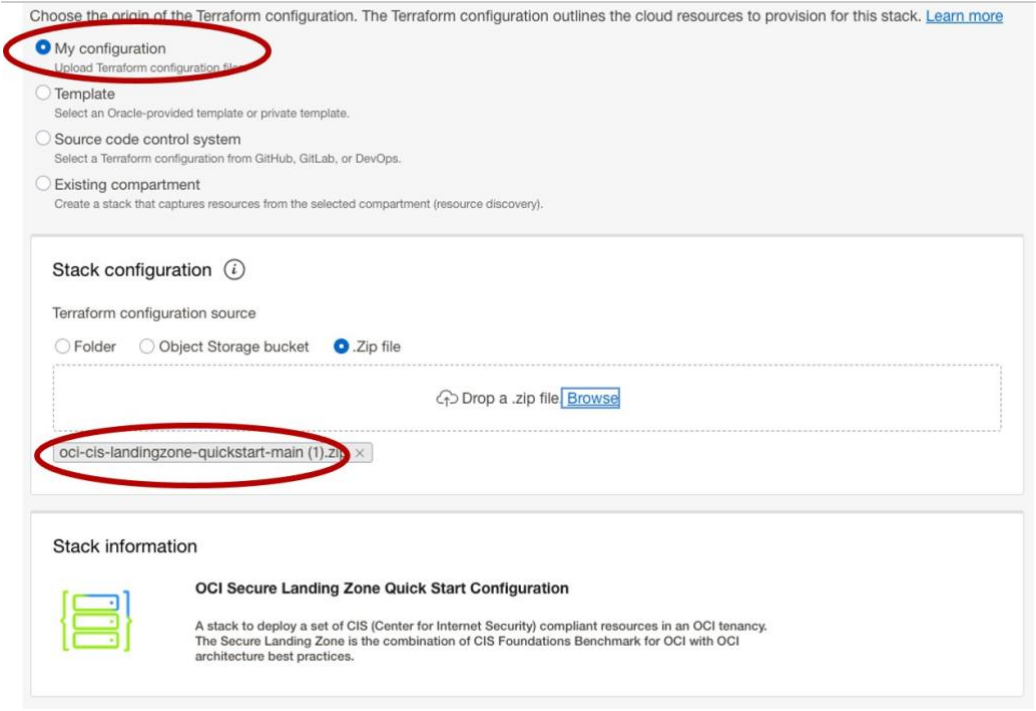
As an alternative, you can also download the ORM stack code and import it like a zip.

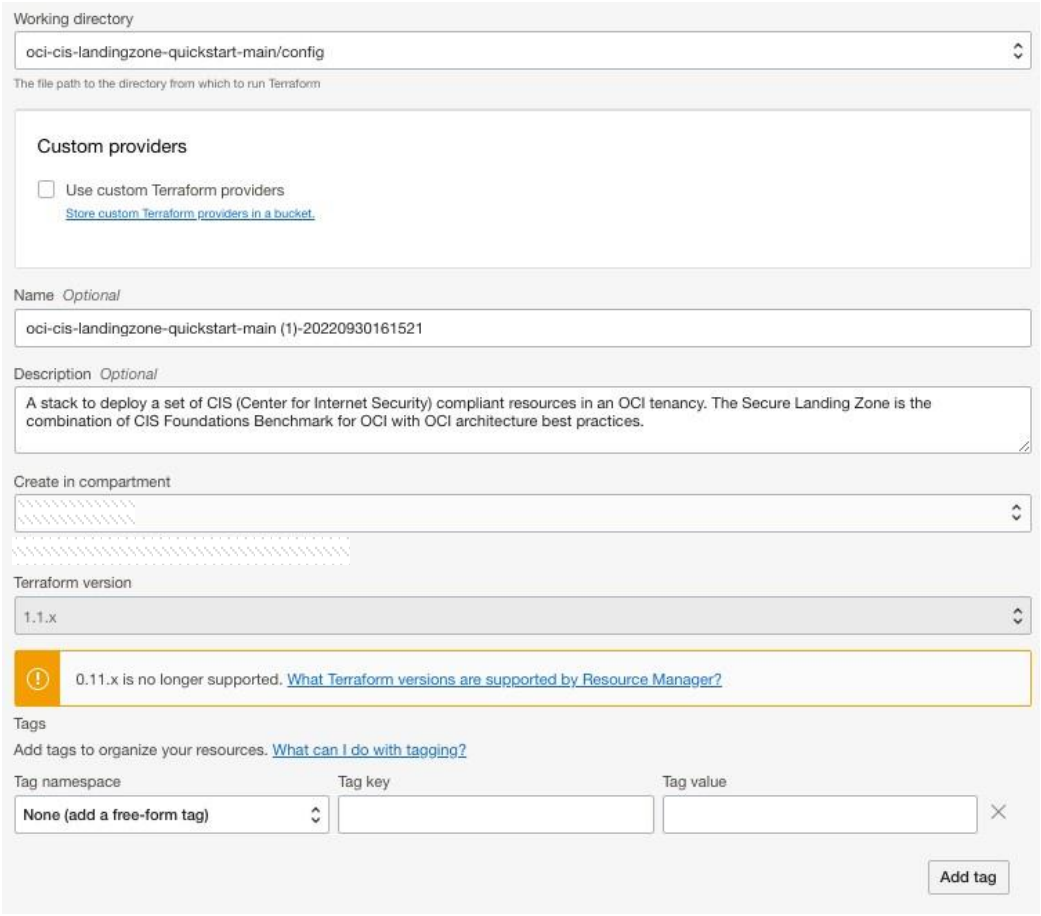


In the OCI console go to:

Developed Services > Resource Manager > Stacks > Create Stack

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





3. INPUT VALUES & DEPLOYMENT SCENARIOS

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

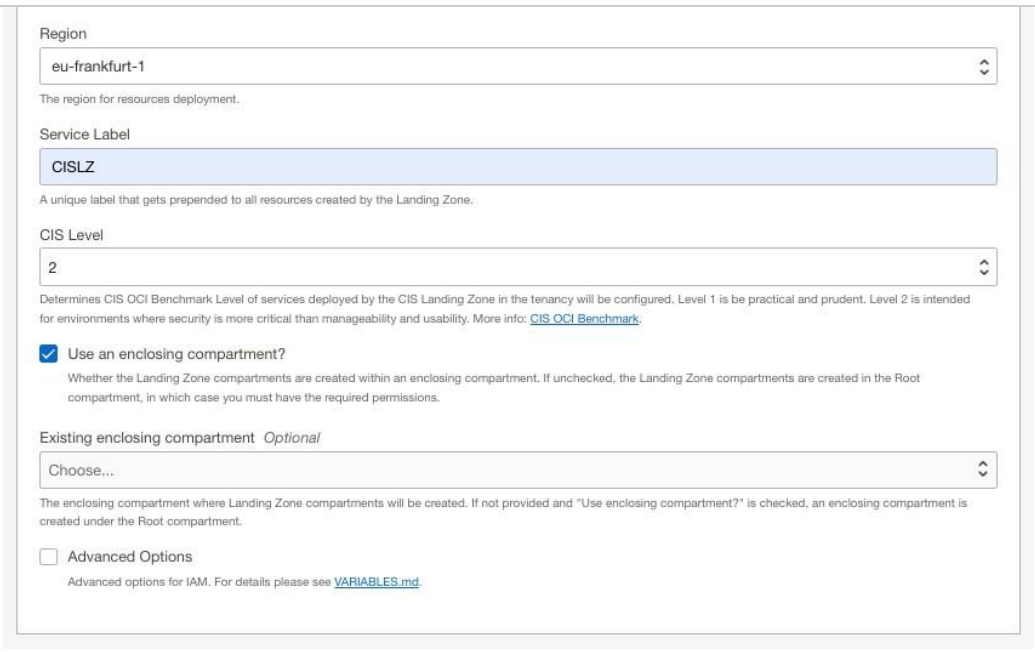
3.1 ENCLOSING COMPARTMENT

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 the recommendation is to deploy the LZ compartments under the root compartment

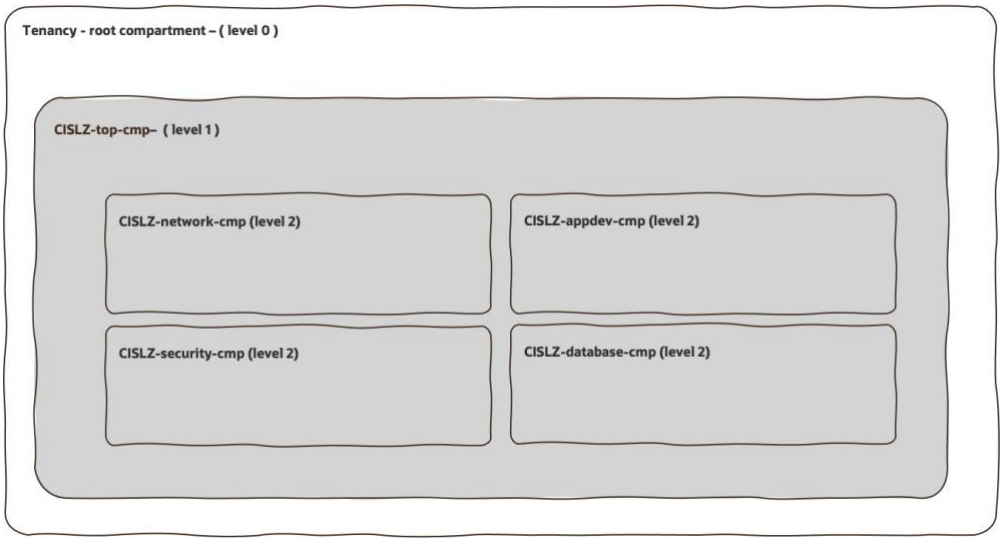
In this section, you need to add the value of the **Service Label** attribute. This label will be used to define the name of all the stack resources that will be created.

Environment

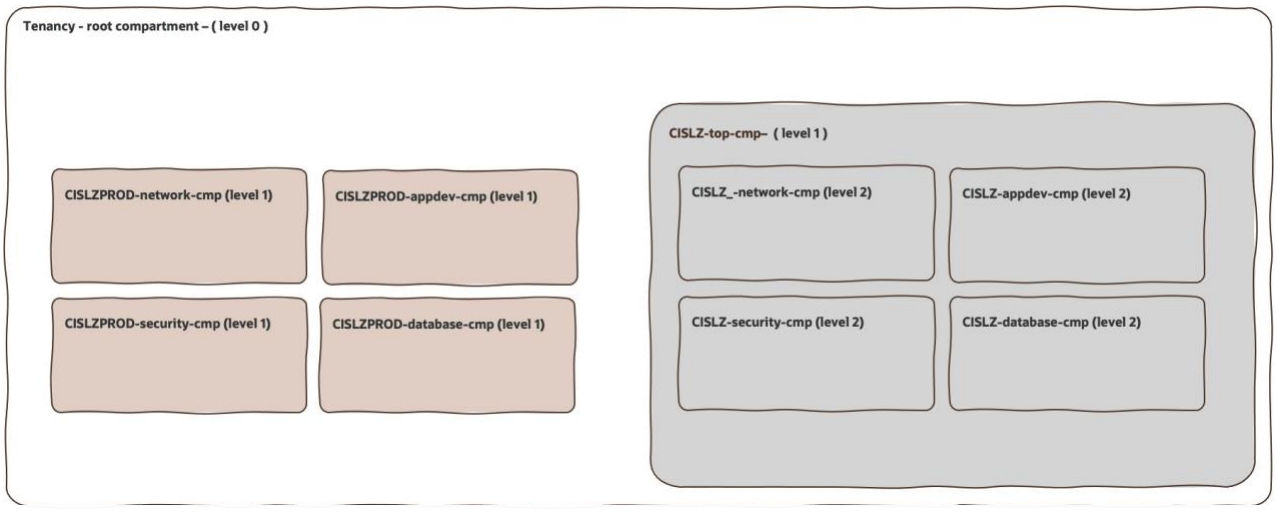


This is the compartment design that will be deployed in the first LZ deployment (for test purposes).

- **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.

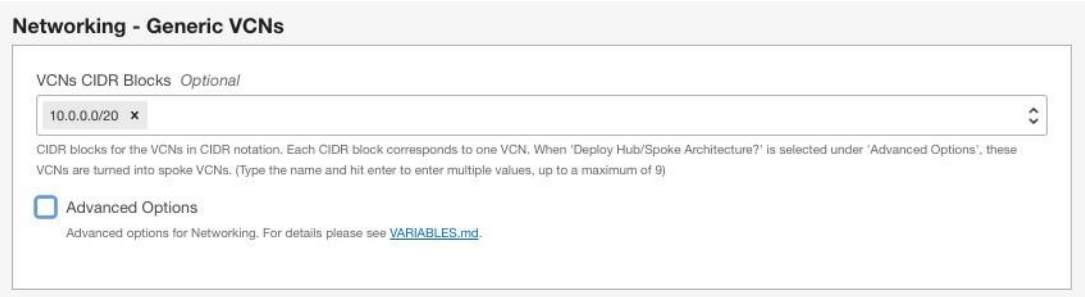
3.3 HUB & SPOKE

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.**

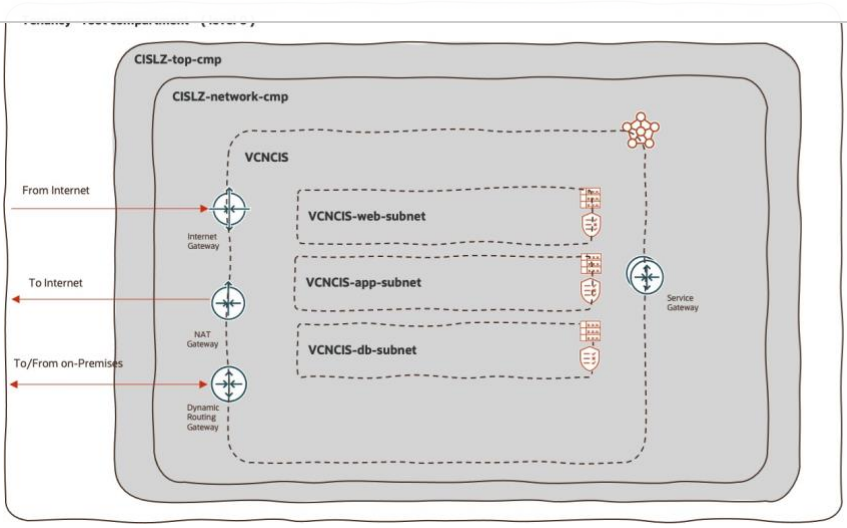


This will be your network configuration after deploying de CIS LZ v2 (CIS) stack.

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.



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.**

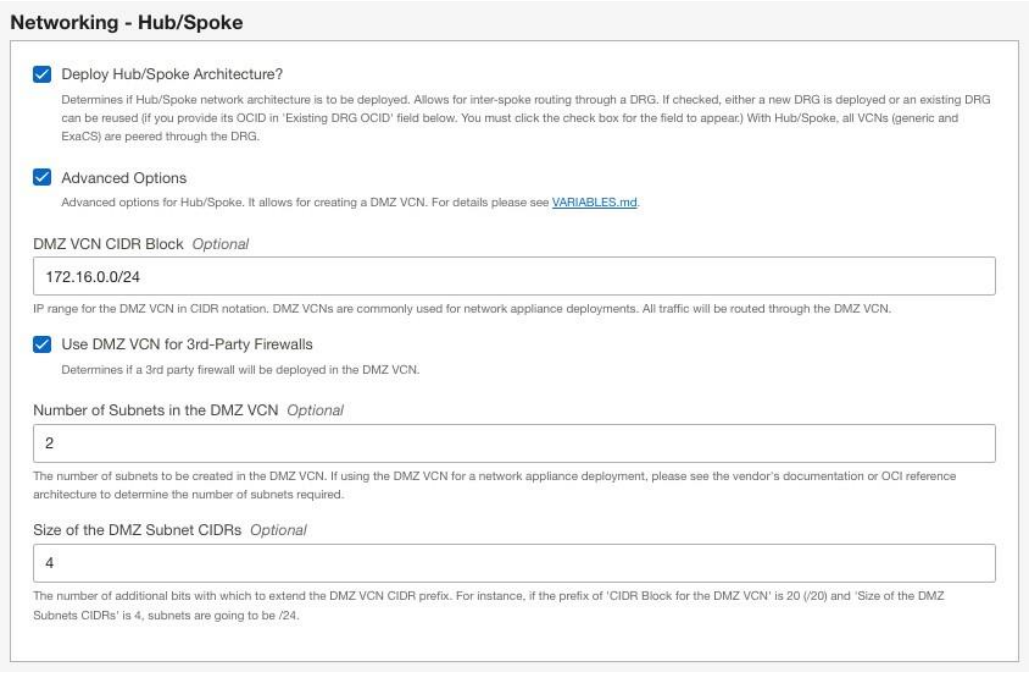
Select **Use DMZ VCN for 3rd-Party Firewalls** if a 3rd-party firewall will be deployed in the Hub VCN.

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

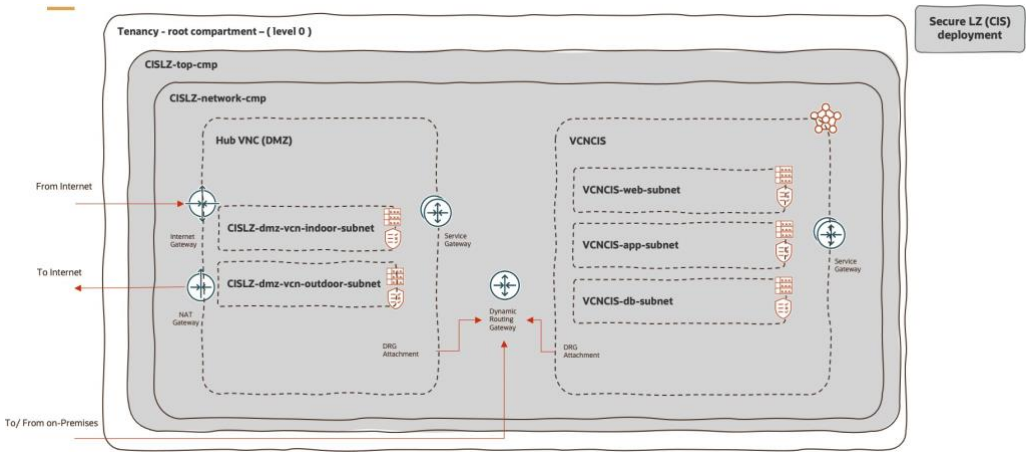


Note: To read more information about configuring a Security Partner Network Appliance with the CIS LZ v2 stack please go to this article or check the specific link:

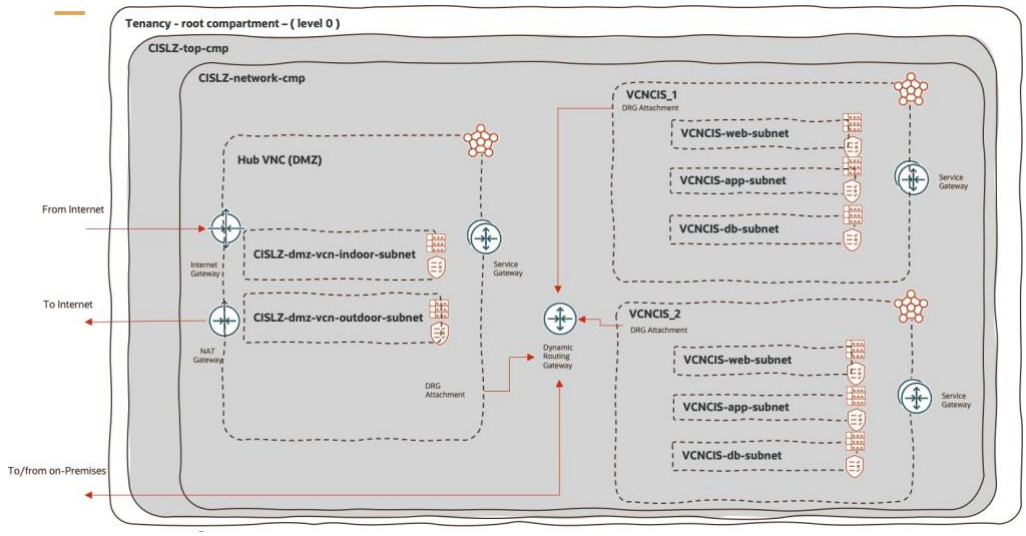
Check Point: Use the Terraform stack to deploy the CloudGuard Firewall solution in a high-availability use case.

- 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 de CIS stack. Example Hub VCN (DMZ VNC) 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.

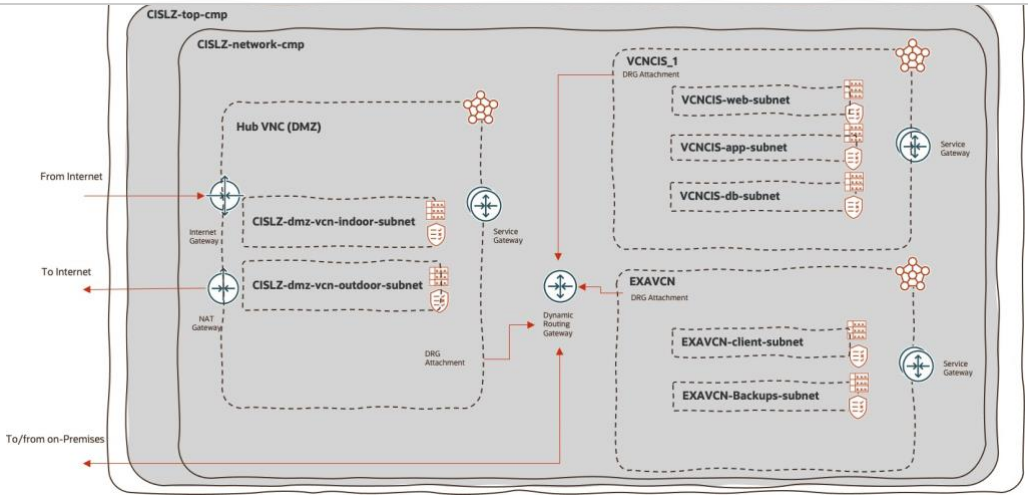
3.5 EXADATA VCN

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.

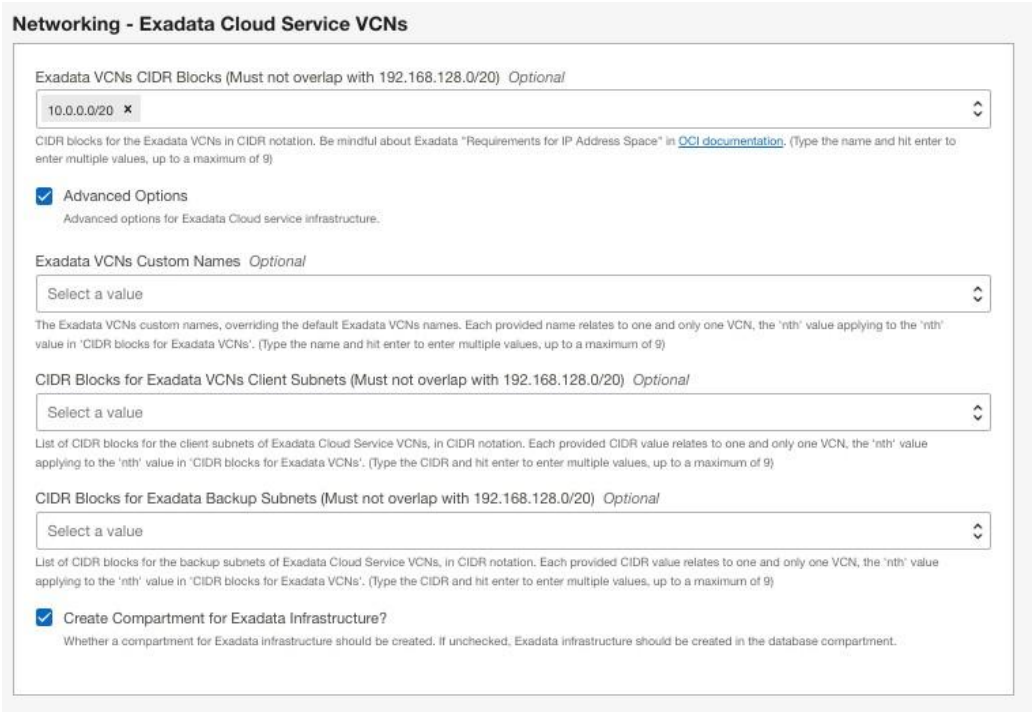
An EXADATA VCN is comprised of:

- 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.**

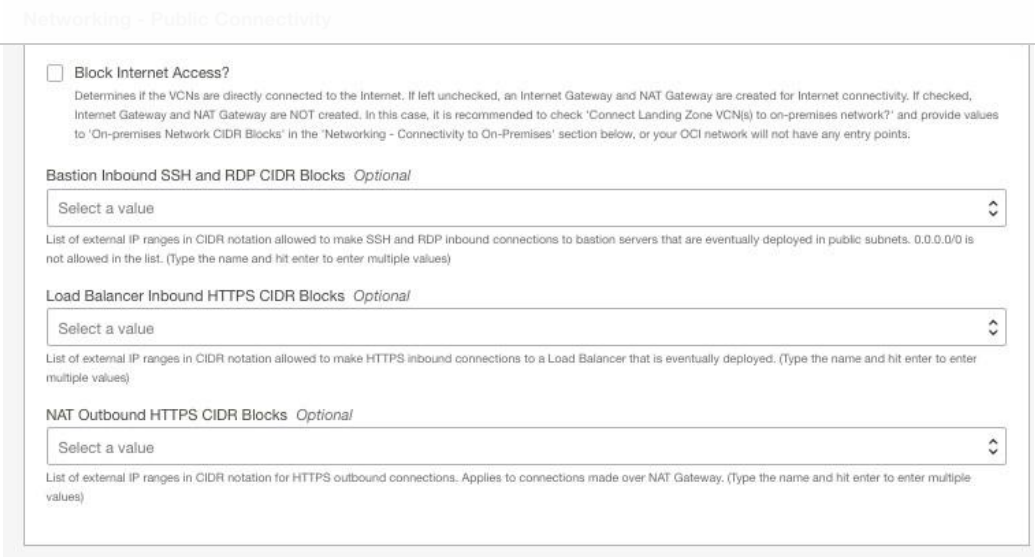


To review more information about how to deploy an Exadata workload using CIS LZ v2 go here.

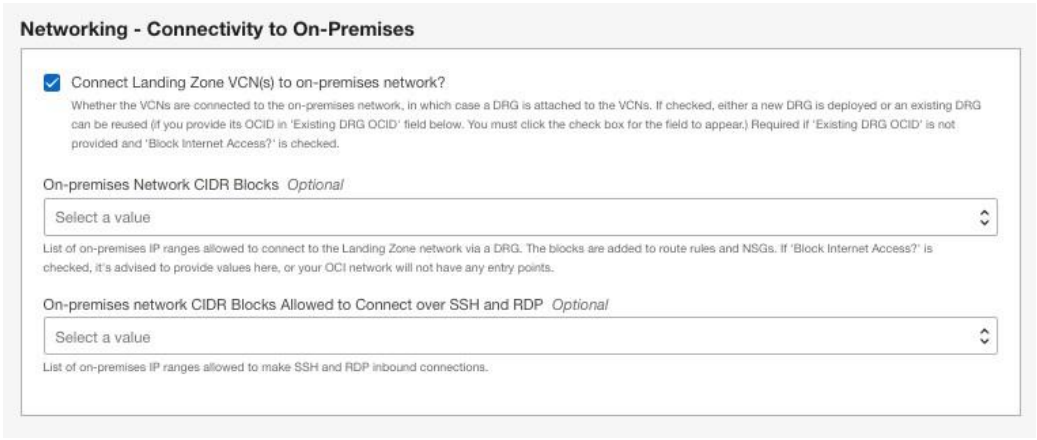
3.6 BLOCK INTERNET ACCESS

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:



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.



For more information check the detailed definition of these values here.

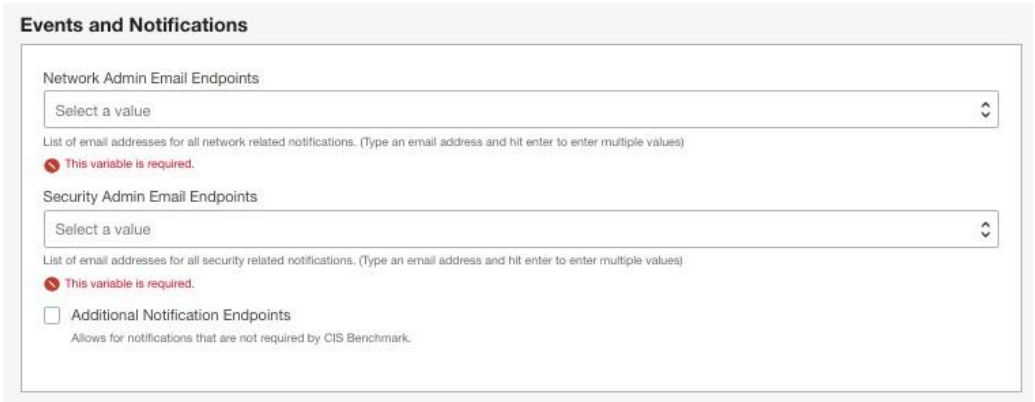
Otherwise, if you want to block access, it is recommended to select the option **Block Internet Access** and leave the other values of the Network section blank. In this case, any Internet Gateway or NAT Gateway will be deployed.

3.7 NOTIFICATIONS

Configure events and notifications

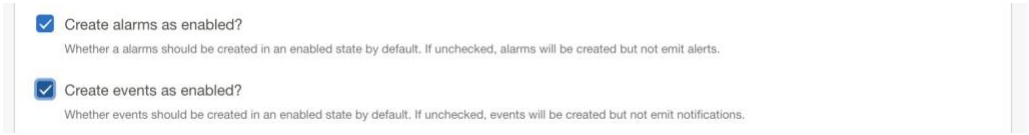
Network Admin Email Endpoints and **Secure Admin Email Endpoints** are mandatory attributes. You need to configure an email where network and security notifications will be sent.

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



By default, events and alarms are created but not enabled.

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



3.8 OBJECT STORAGE

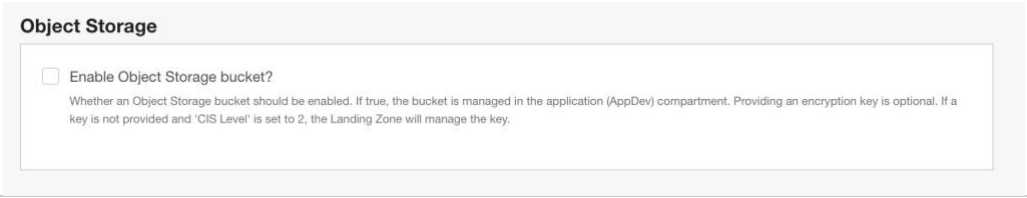
Do you want to deploy an Object Storage?

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.

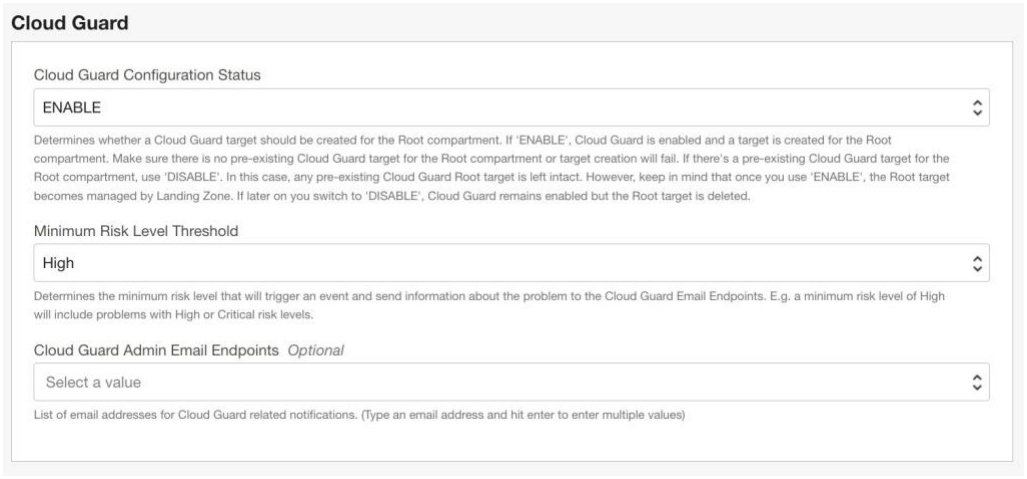
If a key is not provided and 'CIS Level' is set to 2, the Landing Zone will manage the key.



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.



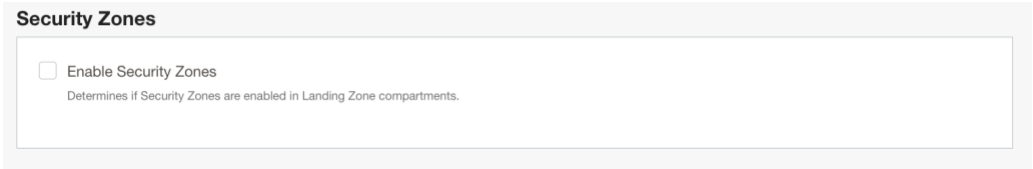
- Customers who want to consolidate Cloud Guard Problems into their preferred SIEM and SOAR systems or take actions based on them can make use of the integration capabilities provided by the Event Service or Cloud Guard APIs and OCI SDKs for their favorite programming languages. OCI Service Connector 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.



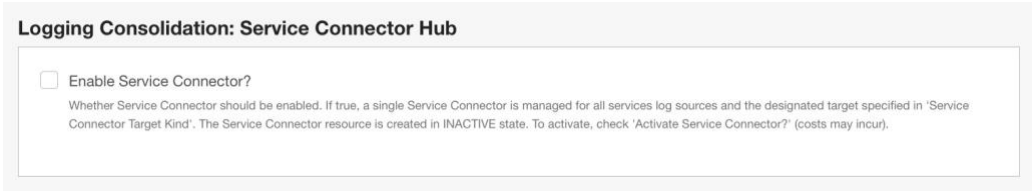
3.11 LOGGING CONSOLIDATION

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).

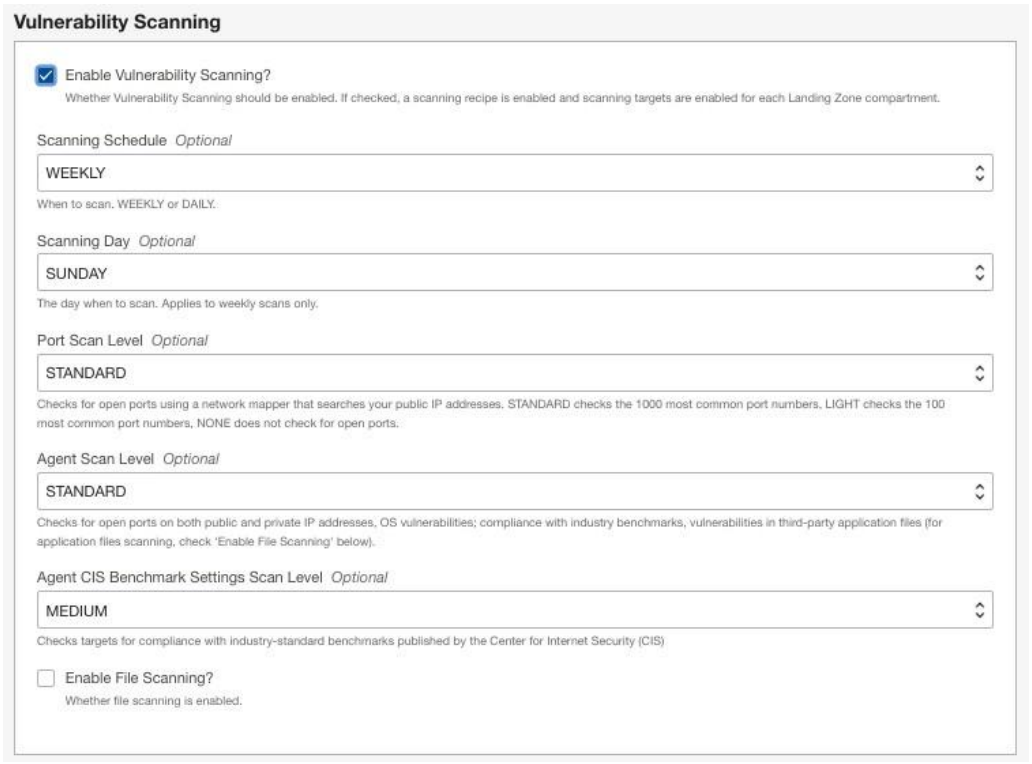


3.12 VULNERABILITY SCANNING

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.

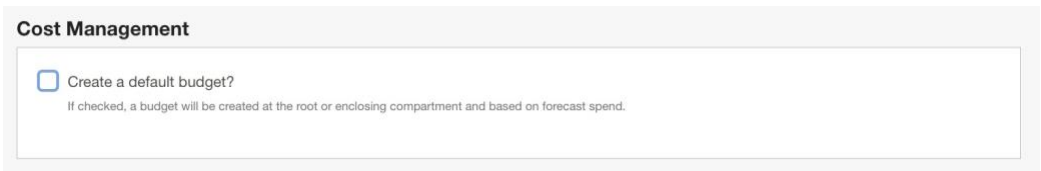


To review more information about the VSS configuration included in the CIS LZ v2 go here.

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.

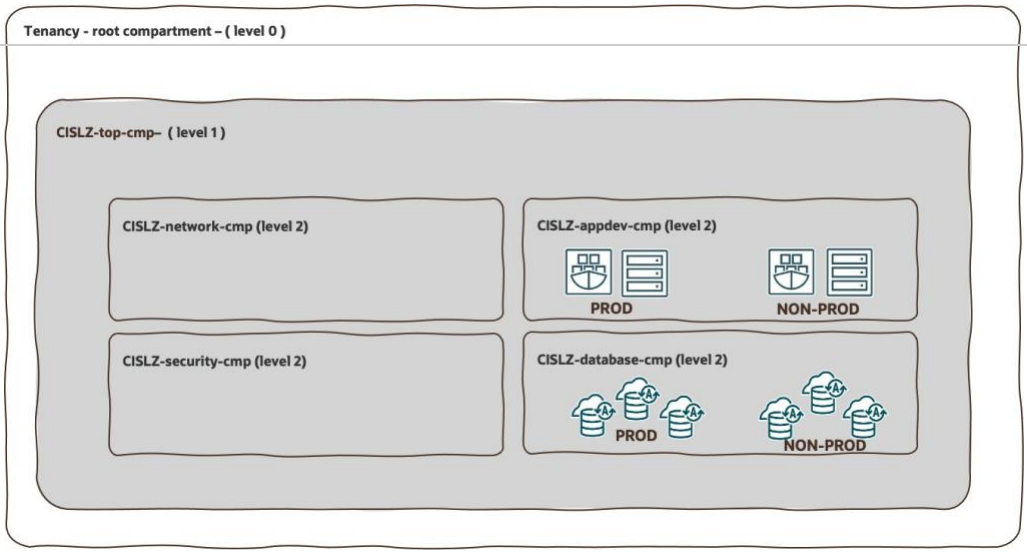


3.14 MULTIPLE WORKLOADS

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

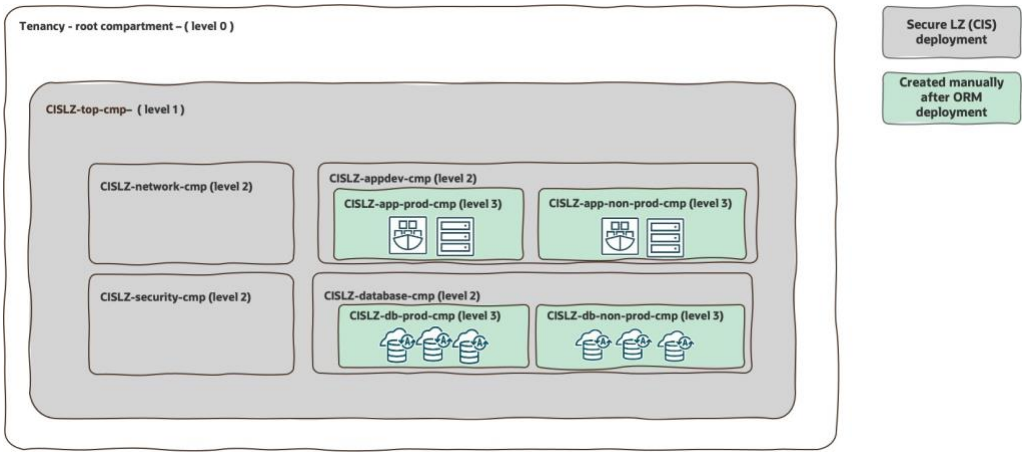
- To improve manageability and security we recommend you create specific compartments for PROD and NON-PROD workloads. On a deeper level, if it is a customer requirement, you can create even one compartment per workload.
- The default CIS LZ v2 policies and permissions will be inherited for managing 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:

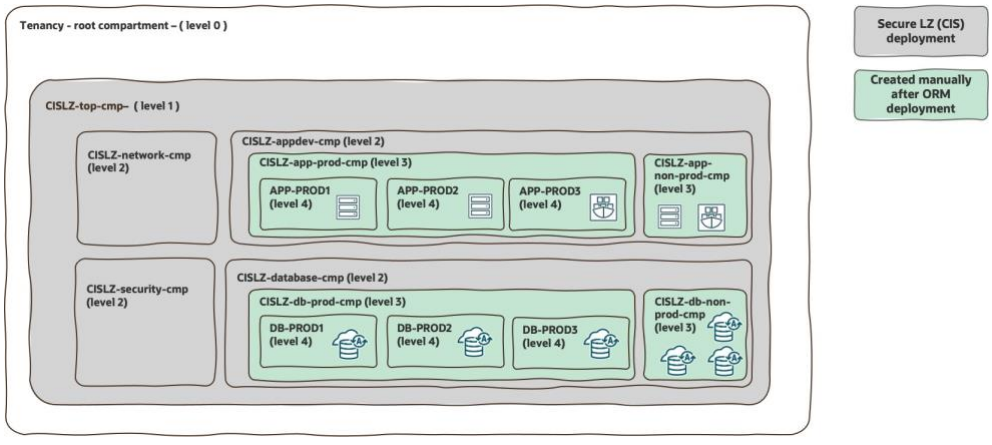
"Green" compartments have to be created manually after deploying the CIS LZ v2 stack.

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



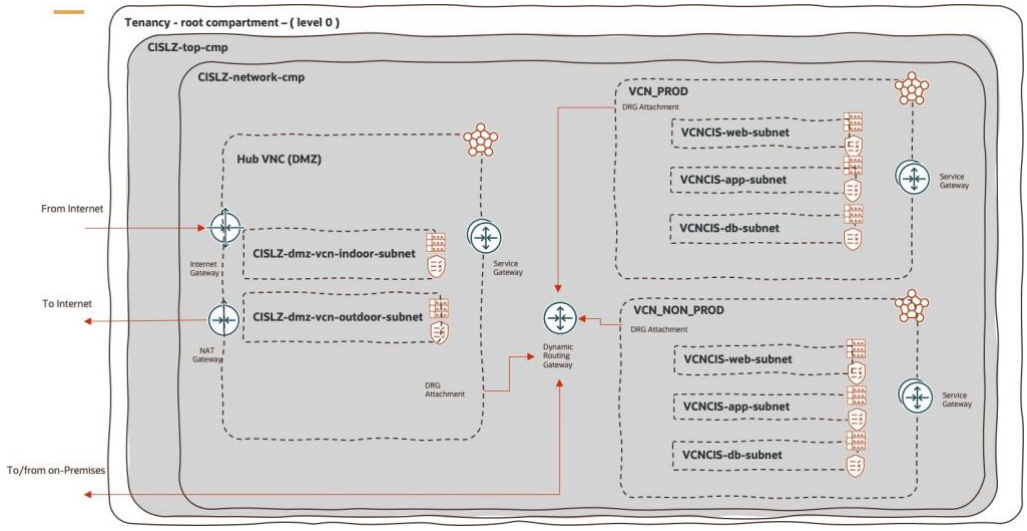
B2) Layer-Driven Organization with Prod/Non-Prod and Application Segregation



SCENARIO C. Use a Hub & Spoke network design.

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

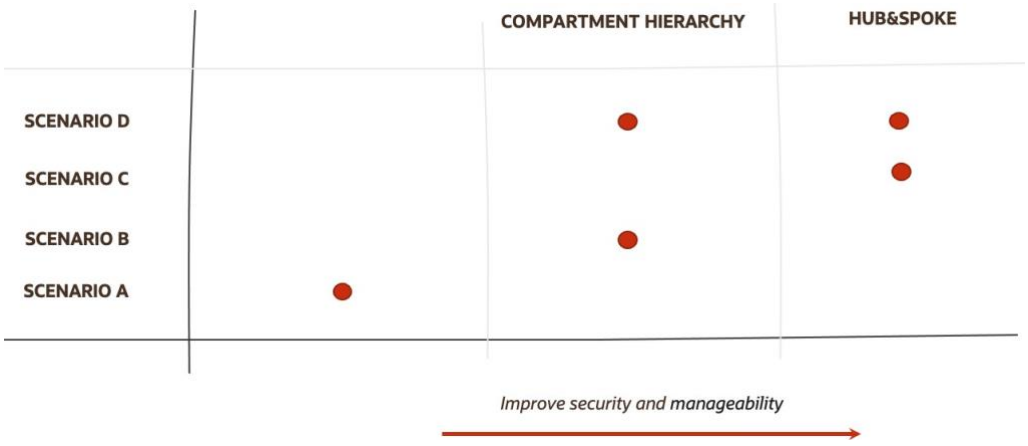
In this example we have one spoke for PROD workloads and another for NON-PROD workloads. The Hub & Spoke design will depend on the customer's organization andrequirements.



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 also include network segregation for these workloads (Hub& Spoke).

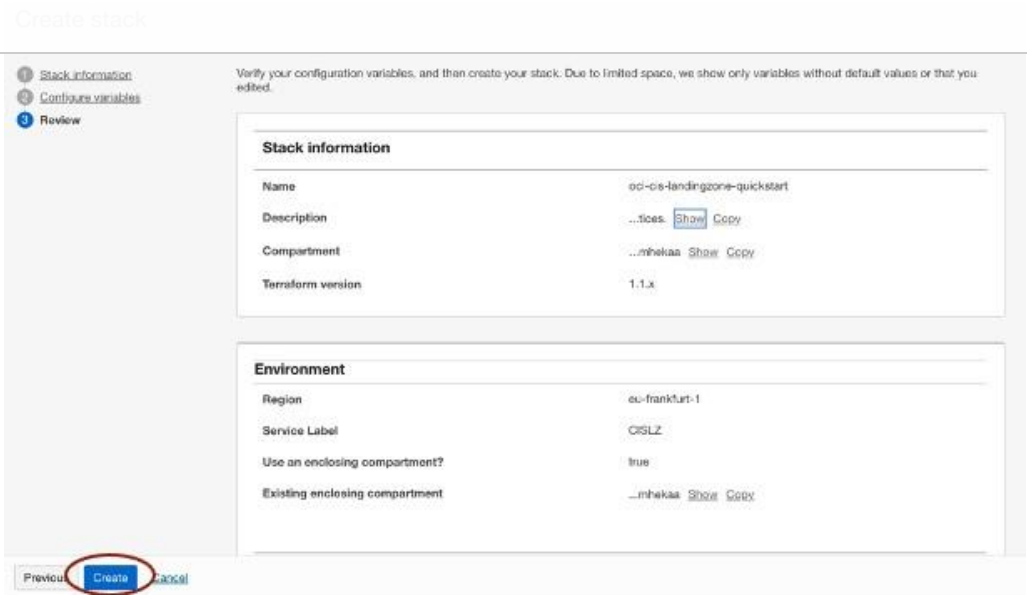


3.15 OTHER SCENARIOS

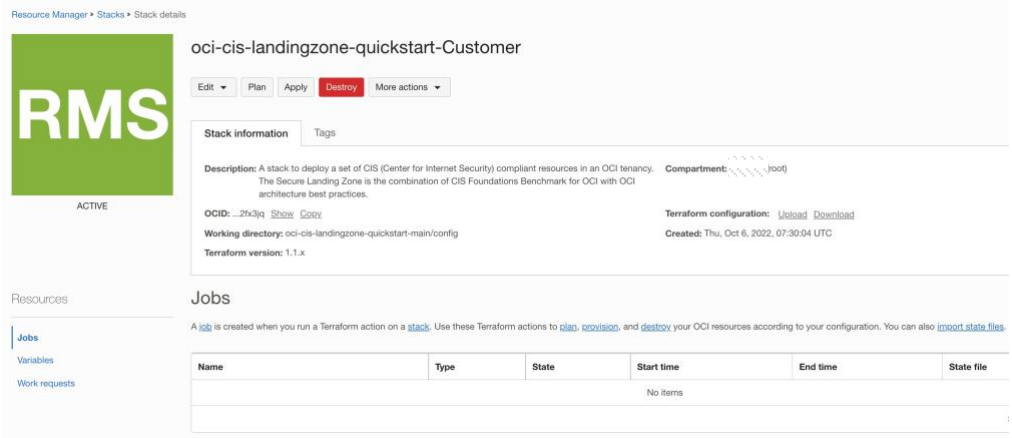
For any other advanced scenario or customized issue not included in this asset go to the CIS LZ v2 documentation.

4. EXECUTE TERRAFORM PLAN

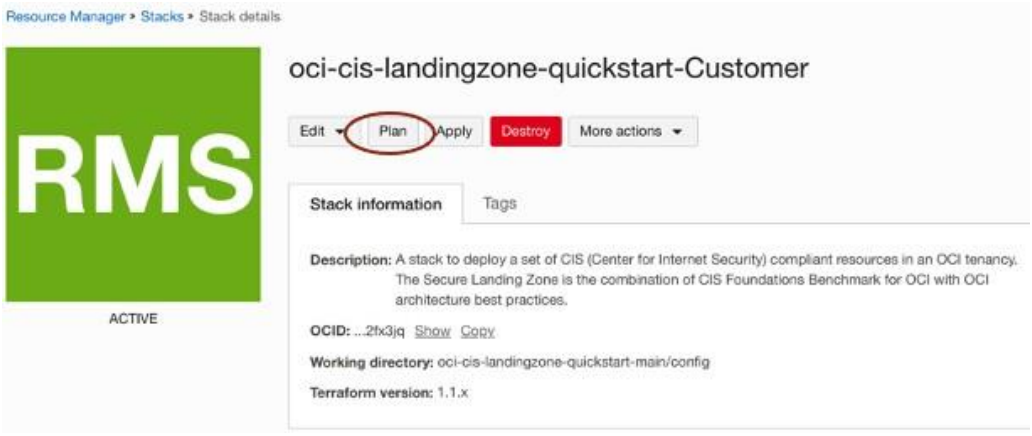
After completing the previous steps, create the new stack.

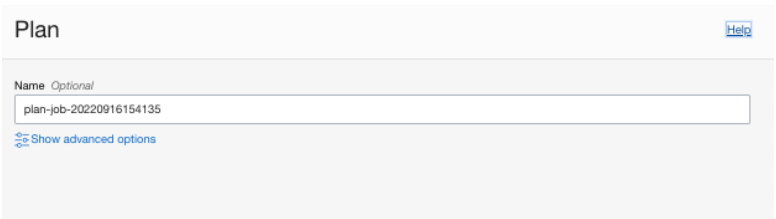


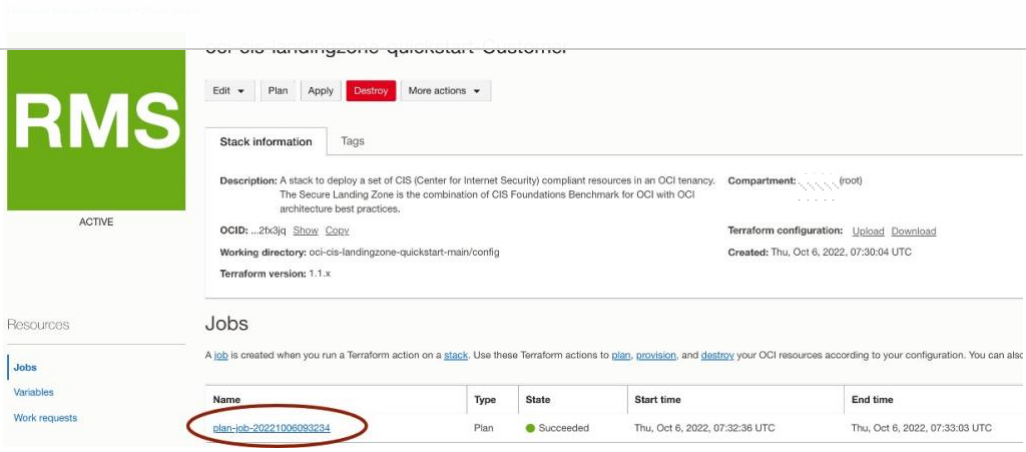
The new ORM stack will appear in the OCI Console.



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







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

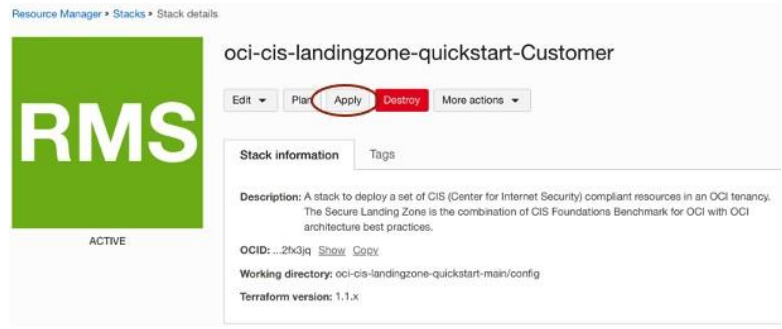
Note: The number of resources created will depend on the selected configuration.

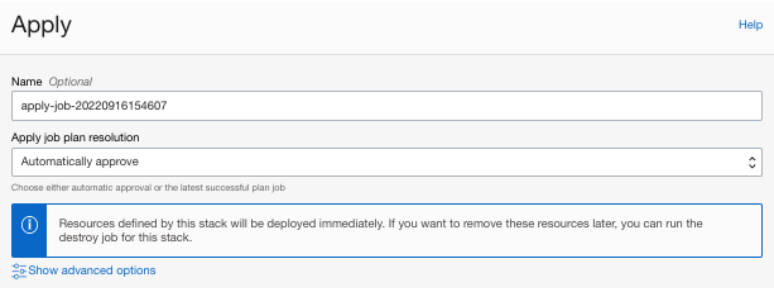
```
Plan: 98 to add, 0 to change, 0 to destroy.
```

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.

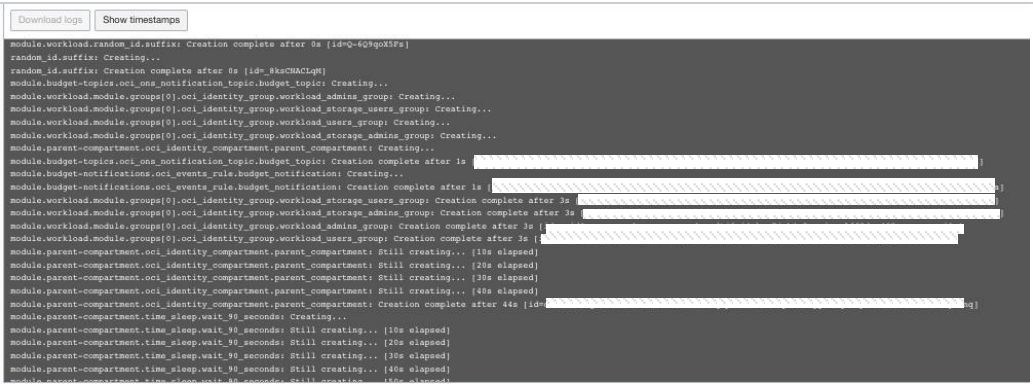
Choose "Apply" to start the job that created all the landing zone resources in your tenancy.



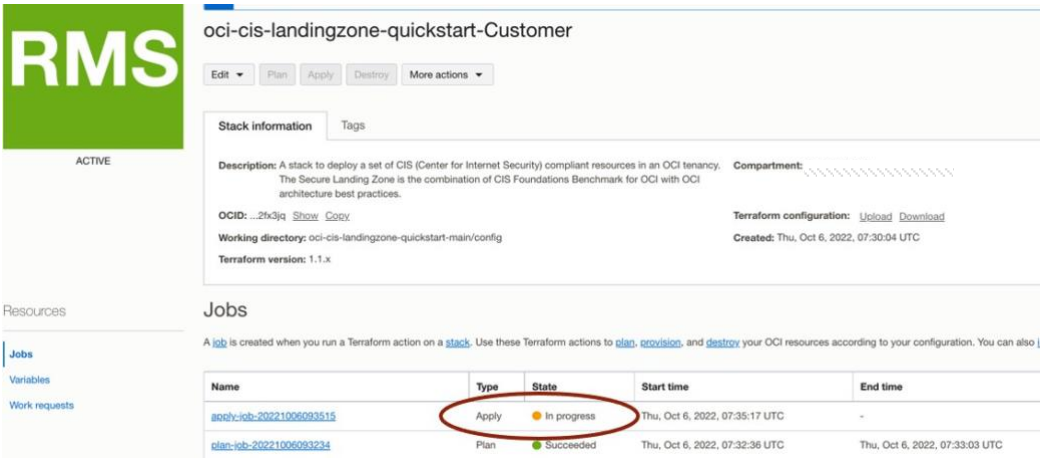


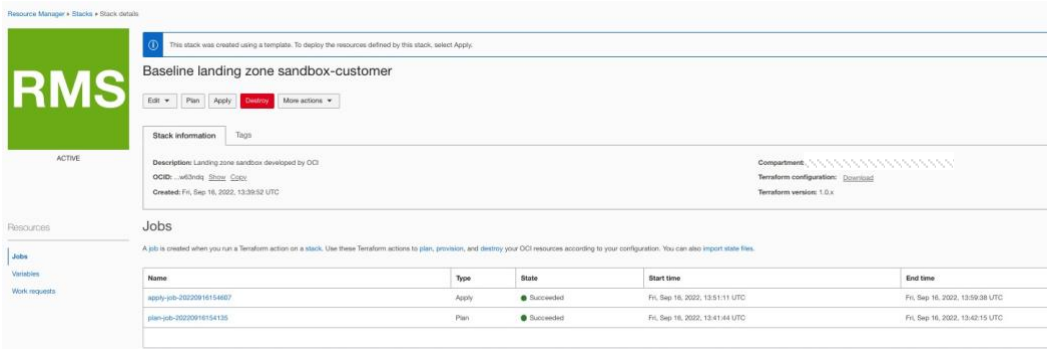
You can review the progress of the **apply** phase job by checking the log.

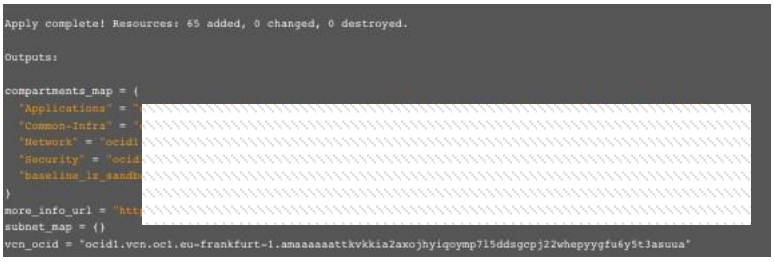
Logs



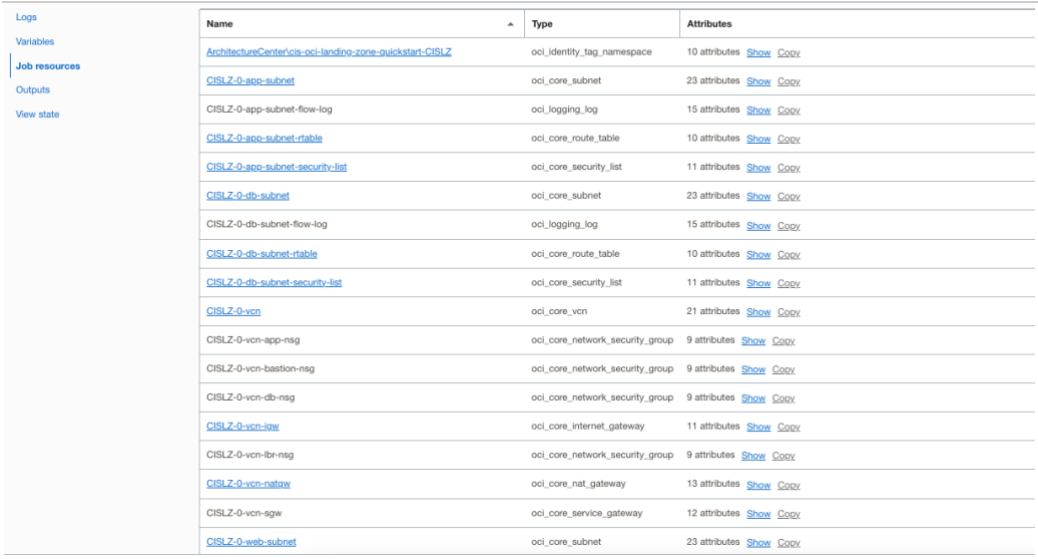
You can confirm how the job ends successfully or if there are any errors.







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



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

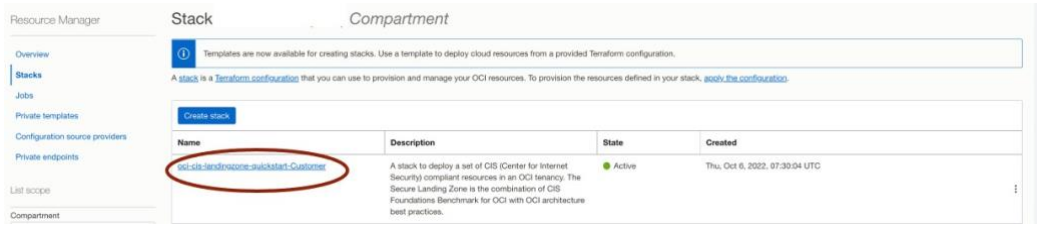
After the CIS LZ v2 deployment, do you want to confirm your CIS compliance?

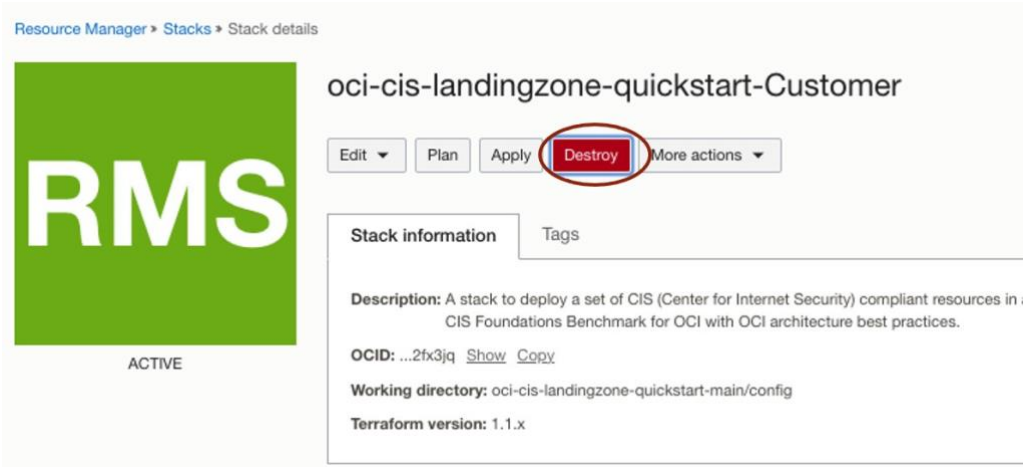
In the CIS GitHub repository, there is a Python script that performs compliance checks for most of the CIS OCI Foundations Benchmark recommendations. The script is completely independent of the Terraform code and can be used against any existing tenancy.

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





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

- Delete the stack.

---

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.

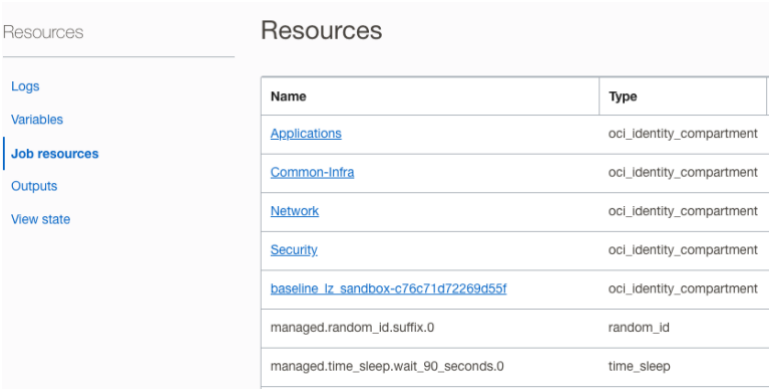
Workaround

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.

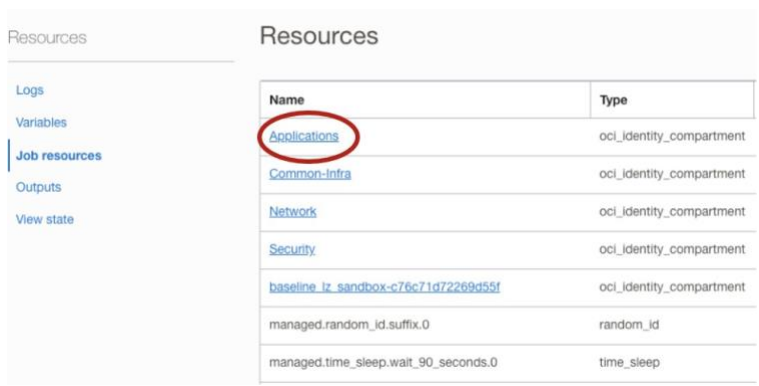
https://docs.oracle.com/en-us/iaas/Content/API/SDKDocs/terraformtroubleshooting.htm#common_issues

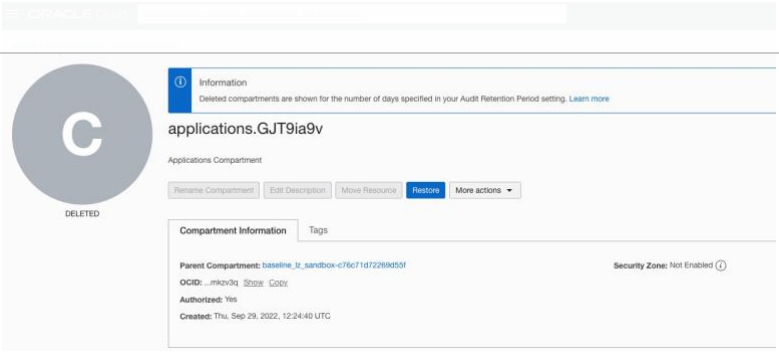
Note: The operation timeout cannot be increased in an ORM stack.

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.



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





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

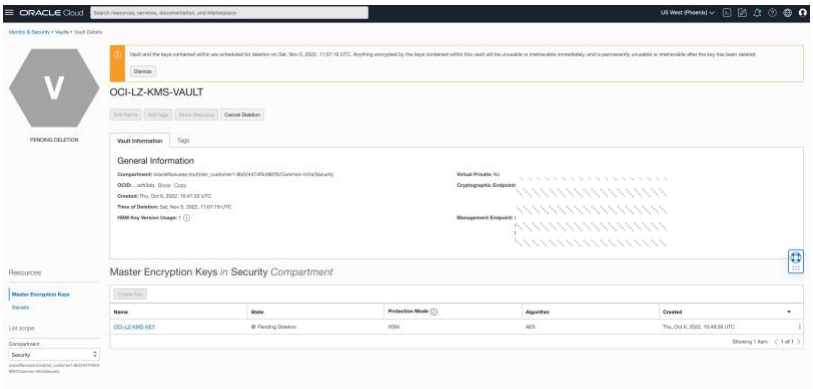
By design, OCI vaults and keys are not deleted immediately upon Terraform destroy, but scheduled for deletion. The Destroy job fails because the vault and the key created by the stack can not be deleted immediately. There is a cool-down period in which the Vault and Key are in a PendingDelete state.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

Workaround.

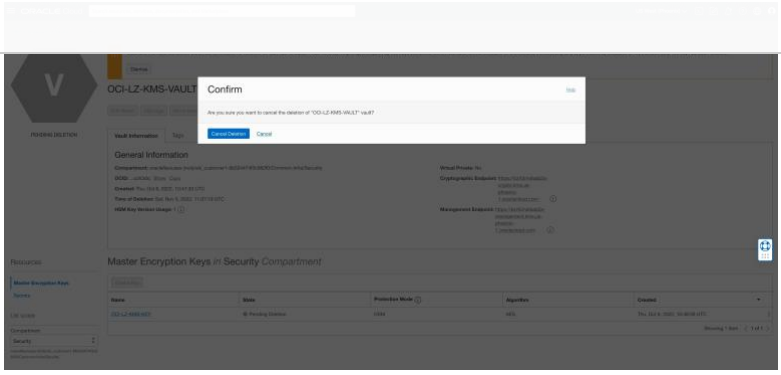
The workaround for this is to cancel deletion for the vault and move the vault and the key to a different compartment (outside the landing zone) and restart the destroy job. After the successful execution of the destroy job, the Vault (and Key) can be deleted manually.

Step by Step example.

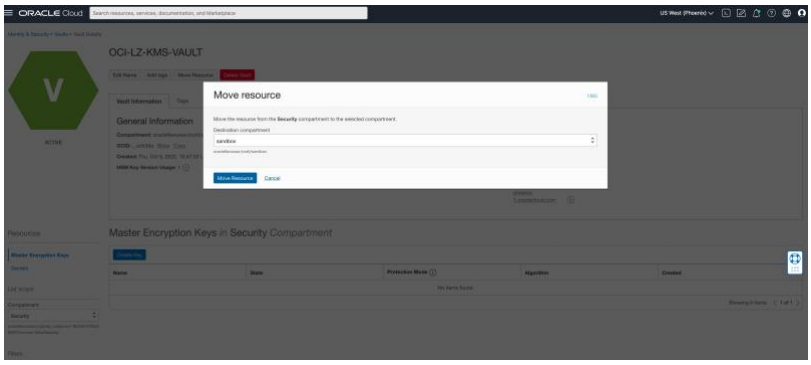
The vault is created by default in the Security compartment



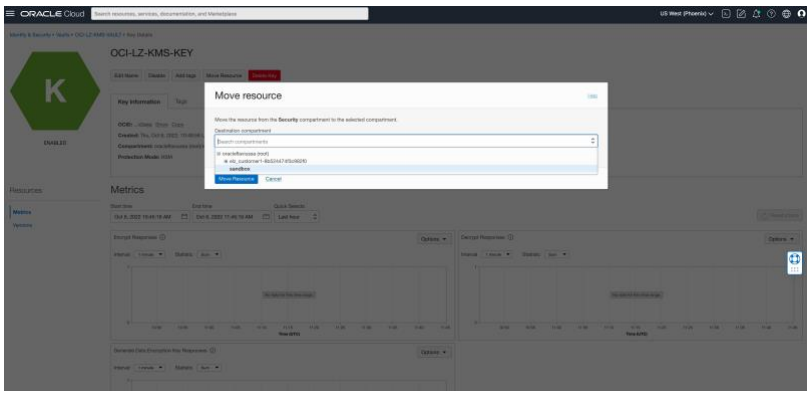
Click on **Cancel Deletion** button to cancel the deletion of the Vault resource. This action will restore the Master Key created as well.



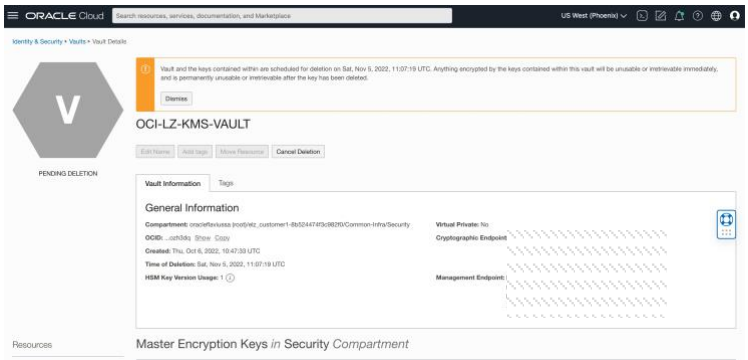
Move the Vault to a different compartment, outside the landing zone. In this example, the compartment is named "sandbox"



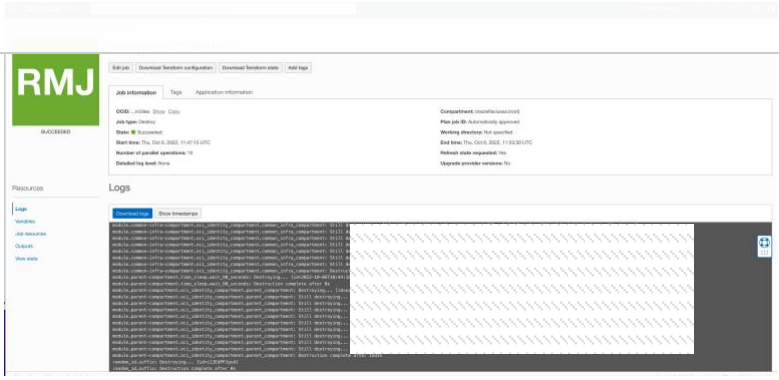
Move the master key to the same "sandbox" compartment



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.