

# 10 Steps to Launch a Secure Cloud Computing Architecture (SCCA) Landing Zone

How to deploy Oracle's Cloud Native SCCA Landing Zone

January, 2024, Version [1.0] Copyright © 2024, Oracle and/or its affiliates Public

### **Purpose statement**

This document provides 10 simple steps to configure your Oracle Cloud Native SCCA Landing Zone.

### Disclaimer

This document is for informational purposes only and is intended solely to assist you in planning for the implementation and upgrade of the product features described. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle. This document may reference products/services or security controls that currently are in the process of obtaining DISA Impact Level 5 provisional authorization. Due to the nature of the document, it may not be possible to include all features described in this document. For additional information specific to certain Oracle Cloud Services with DISA Impact Level 5 authorization, please refer to this informational website, located at: <u>Oracle Cloud US Federal Cloud with DISA Impact Level 5 Authorization</u>.

### **Table of Contents**

Step 1 Get Started	4
Step 2 Stack Configuration	5
Step 3 Configure Variables	6
Step 4 Compartment Configuration	7
Step 5 Identity and Access Management (IAM)	7
Step 6 Monitoring Variables	8
Step 7 Security Variables	8
Step 8 Network Variables	9
Step 9 Workload Variables	9
Step 10 Confirmation	10
GitHub Deployment	11

### **Step 1 Get Started**

Log in to Oracle Cloud Console.

Select the Navigation Menu and select Developer Services, then Stacks under the Resource Manager heading.

Compute Compute Storage Networking Oracle Database Databases Analytics & Al Developer Services Identity & Security Observability & Management Hybrid Migration Billing & Cost Management Governance & Administration Marketplace	Kubernetes Clusters (OKE) Container Registry Artifact Registry Functions Applications Pre-Built Functions APEX Application Development APEX Instances APIX Instances API Management Gateways APIs Application Integration Integration Notifications Email Delivery	Visual Builder Studio Visual Builder DevOps Overview Projects Resource Manager Overview Stacks Jobs Private Templates Configuration Source Providers Private Endpoints	SDK CLI PowerShell Terraform Ansible Docs Content Management Overview Instances	Compute VMware Solution Autonomous Database Oracle NoSQL Database Logging Streaming Connector Hub <b>Heip</b> OCI Developer Guide OCI Developer Tutonals Set up CLI REST APIs Developer Community Developer Live
--	---	---	---	---

Select your **Compartment** for deployment on the left dropdown menu.

#### Click Create Stack.

E ORACLE Cloud stack	ε			US DoD East (Ashburn) 🗸 🕢 🗇 🤀
Resource Manager	Stacks in pse	devoc3 (root) Compartme	ent	
Overview	(i) Templates are not	w available for creating stacks. Use a template to c	leploy cloud resources from a provic	led Terraform configuration.
Stacks Jobs	A stack is a Terraform cont	fig <u>uration</u> that you can use to provision and manag	e your OCI resources. To provision t	he resources defined in your stack, apply the configuration.
Private templates	Create stack			
Configuration source providers	Name	Description	State	Created
Private endpoints			No items	
ist scope				Showing 0 stacks 🛛 < Page 1 >
compartment				
psedevoc3 (root)				
ag filters add I clear				
o tag filters applied				

# **Step 2 Stack Configuration**

Select the **Template** radio button. Click *Select Template*. Select the **Architecture** tab. Select **OCI Cloud Native SCCA Landing Zone**.

E ORACLE Cloud	stack	US DoD East (Ashburn) 🗸	⊡ ↓ ? ⊕ 9
Create stack			Help
<ul> <li>Stack information</li> <li>Configure variables</li> <li>Review</li> </ul>	A stack is a Terratorm configuration that you can use to provision and manage your OCI resources. To provision the resour stack, apply the configuration. Choose the origin of the Terraform configuration. The Terraform configuration outlines the cloud resources to provision for the Vy configuration Upload Terraform configuration files. Implate Select an Chale-provided template or private template. Select an Chale-provided template or private template. Select an Chale-provided template or private template. Select an Chale-provide template or private template. Select an Chale-provided template or private template. Select an Chale-provident from Bitacket Cloud, Bitbucket Server, DevOps, GitHub, or GitLab. Stisting compartment Create a stack that captures resources from the selected compartment (resource discovery). Stack configuration @ Terraform configuration source Select = Object Storage bucketip file Corp a folder. Browsee	ces defined in your this stack. <u>Learn more</u>	
	Custom providers		
Next <u>Cancel</u>			
Terms of Use and Privacy Cookie Pret	ferences	Copyright © 2024, Oracle and	or its affiliates. All rights reserved.

ORACLE Clor	UC Search resources, services, and	Marketplace	US DoD East (Ashburn) 🗸	☑ ♫ ② ⊕ (
Create stack		Browse templates		
<ol> <li>Stack information</li> <li><u>Configure variables</u></li> <li><u>Review</u></li> </ol>	Select a Terraform configuration from I Existing compartment Create a stack that captures resources Stack configuration (i)	Quickstarts Service	Architecture Private a Terraform configuration using multiple cloud services.	
		Template name D	escription	
	Custom providers	OCI Cloud Native C SCCA Landing Zone	CI Cloud Native SCCA Landing Zone	~
	Use custom Terraform pro	Oracle Enterprise C Landing Zone v2 - Workload Expansion	racle Enterprise Landing Zone v2 - Workload Expansion	~
	Name Optional	Oracle Enterprise C Landing Zone v2	racle Enterprise Landing Zone v2	~
Next <u>Cancel</u>		Select template Cancel		
rms of Use and Privacy Cookie	Preferences		Copyright © 2024, Oracle a	nd/or its affiliates. All rights reserve

# **Step 3 Configure Variables**

Update the optional variables such as **Stack Name**, then click **Next**.

<b>ORACLE</b> Clo	Ud Search resources, services, and Marketplace	US DoD East (Ashburn) 🗸 🗔 🎊 🛞 🜐
Create stack		Hel
1 Stack information	Stack configuration (i)	
2 <u>Configure variables</u> 3 <u>Review</u>	ORACLE         OCI Cloud Native SCCA Landing Zone           SCCA         Landing         OCI Cloud Native SCCA Landing Zone           Zone         OCI Cloud Native SCCA Landing Zone	Change template
	Working directory	
	Use Terraform configuration files in the root folder	\$
	The file path to the directory from which to run Terraform	
	Custom providers Use custom Terraform providers Store custom Terraform providers in a bucket.	
Next <u>Cancel</u>		
rms of Use and Privacy Cookie	Preferences	Copyright © 2024, Oracle and/or its affiliates. All rights reserv

Configure the **Provider Variables** as needed. The **Secondary Region** field is required.

Create stack		Help
Stack information	Api Fingerprint Optional	
Configure variables	Value not required in Oracle Resource Manager.	
Kan Takan	The fingerprint of API	
	Api Private Key Path Optional	
	Value not required in Oracle Resource Manager.	
	The local path to the API private key	
	Region	
	us-gov-ashburn-1	
	the OCI region LZ is deployed to.	
	Secondary Region	
	us-phoenix-1	
	the OCI region for data backup.	
	Tenancy OCID Optional	
	ocid 1. ten ancy. oc 3aaaaaaaaa aaa ax pn sqzs in u 57 yv h kvc 4 tb ox qmu bq tq bp w 6 bq tn d k 2 w s l h c sz j c q a s a s a s a s a s a s a s a s a s a	
	The OCID of tenancy	
	Current User OCID Optional	
	ocid1.user.oc3aaaaaaaawtgfsjszfoujolm32gxjzw2qigv47u44sfcnb6vi57wt4hdd6beq	
	OCID of the current user	
Previous Next Cancel		

### **Step 4 Compartment Configuration**

Configure your Landing Zone **Compartments** and choose whether to enable a separate compartment for logging.

Ompartment Variables           Home Compartment Name           OCI-SCCA-LZ-Home           Name of the top level / home compartment. Maximum 100 characters, including letters, numbers, periods, hyphens, underscores, and is unique within the tenancy.           VDMS Compartment Name         OCI-SCCA-LZ-VDMS           Name of the VDMS compartment. Maximum 100 characters, including letters, numbers, periods, hyphens, underscores, and is unique within its parent compartment.           VDSS Compartment Name         OCI-SCCA-LZ-VDMS			
Home Compartment Name OCI-SCCA-LZ-Home Name of the top level / home compartment. Maximum 100 characters, including letters, numbers, periods, hyphens, underscores, and is unique within the tenancy: VDMS Compartment Name OCI-SCCA-LZ-VDMS Name of the VDMS compartment. Maximum 100 characters, including letters, numbers, periods, hyphens, underscores, and is unique within its parent compartment. VDSS Compartment Name			
OCI-SCCA-LZ-Home           Name of the top level / home compartment. Maximum 100 characters, including letters, numbers, periods, hyphens, underscores, and is unique within the tenancy.           VDMS Compartment Name           OCI-SCCA-LZ-VDMS           Name of the VDMS compartment. Maximum 100 characters, including letters, numbers, periods, hyphens, underscores, and is unique within its parent compartment.           VDSS Compartment. Maximum 100 characters, including letters, numbers, periods, hyphens, underscores, and is unique within its parent compartment.           VDSS Compartment Name			
Name of the top level / home compartment. Maximum 100 characters, including letters, numbers, periods, hyphens, underscores, and is unique within the tenancy. VDMS Compartment Name OCI-SCCA-LZ-VDMS Name of the VDMS compartment. Maximum 100 characters, including letters, numbers, periods, hyphens, underscores, and is unique within its parent compartment. VDSS Compartment Name			
OCI-SCCA-LZ-VDMS Name of the VDMS compartment. Maximum 100 characters, including letters, numbers, periods, hyphens, underscores, and is unique within its parent compartment. VDSS Compartment Name			
Name of the VDMS compartment. Maximum 100 characters, including letters, numbers, periods, hyphens, underscores, and is unique within its parent compartment. VDSS Compartment Name			
OCI-SCCA-LZ-VDSS			
Name of the VDSS compartment. Maximum 100 characters, including letters, numbers, periods, hyphens, underscores, and is unique within its parent compartment. Backup Compartment Name			
OCI-SCCA-LZ-IAC-TF-Configbackup			
Name of the Backup compartment, used to store terratorm state backups. Maximum 100 characters, including letters, numbers, periods, hyphens, underscores, and is unique within its parent compartment.  resource_label			
test			
Short label to append to global resource names to prevent name collisions.			
enable_logging_compartment     Cat to true to excelle loading compartment. To faire if uncull bis loading to relation builders to contents			
	Name of the VDSS compartment. Maximum 100 characters, including letters, numbers, periods, hyphens, underscores, and is unique within its parent compartment. Backup Compartment Name OCLSCCA-LZ-IAC-TF-Configbackup Name of the Backup compartment, used to store ternatorm state backups. Maximum 100 characters, including letters, numbers, periods, hyphens, underscores, and is unique within its parent compartment. resource_label test Short label to append to global resource names to prevent name collisions. every enable_logging_compartment. Every enable_logging_compartment Contents to namethin longing assessmentement. Its felter, if uses will be foreign to a celeting husterior is another to memory.	Name of the VDSS compartment. Maximum 100 characters, including letters, numbers, periods, hyphens, underscores, and is unique within its parent compartment.  Backup Compartment Name OCL-SCCA-L2-IAC-TF-Configbackup Name of the Backup compartment, used to store terratorm state backups. Maximum 100 characters, including letters, numbers, periods, hyphens, underscores, and is unique within its parent compartment, used to store terratorm state backups. Maximum 100 characters, including letters, numbers, periods, hyphens, underscores, and is unique within its parent compartment.  resource_label test Short label to taplend to global resource names to prevent name collisions.  e enable_logging_compartment Content. In the new biole backup is the future of times and the backups hundrate is exective terratore.	In ane of the VDSS compartment. Maximum 100 characters, including letters, numbers, periods, hyphens, underscores, and is unique within its parent compartment.  Backup Compartment Name OCLSCCA-LZ-IAC-TF-ConfigBackup Name of the Backup compartment, used to store terratorm state backups. Maximum 100 characters, including letters, numbers, periods, hyphens, underscores, and is unique within its parent compartment.  resource_label Intel Short label to append to global resource names to prevent name collisions.  e enable_logging_compartment Context.  A with the Interve to available Intervent name collisions.  e enable_logging_compartment

# **Step 5 Identity and Access Management (IAM)**

#### Configure Identity Variables:

- Realm Key
  - 1 for OC1 (Commercial)
  - o 2 for OC2 (US Government Realm)
  - 3 for OC3 (US Defense Cloud)
- Choose whether to enable Identity replication.

<b>ORACLE</b> Cloud	stacks	US DoD East (Ashburn) 🗸 🕢 💮 💭 🧕
Create stack		Help
Stack information     Stack information     Configure variables     Beview	Identity Variables  realm_key  1  OCI Realm L2 will be deployed in Available options are: 1 for OC1 (commercial), 2 for OC2 (Government), and 3 for OC3 (Government)  enable_domain_replication  Enable to replicate domain to secondary region.	÷
	Monitoring Variables VDMS Critical Notification Recipient Email List Optional Select a value List of email addresses for VDMS Critical notifications. VDMS Warning Notification Recipient Email List Optional Select a value List of email addresses for VDMS warning notifications. VDSS Critical Notification Recipient Email List Optional Select a value List of ended thereas for VDMS critical notifications.	•
Previous Next Cancel Terms of Use and Privacy Cookie Pret	erences	Copyright © 2024, Oracle and/or its affiliates. All rights reserved.

# **Step 6 Monitoring Variables**

Configure your **Monitoring Variables.** The initial Email list options are optional.

Stack information     Configure variables     Review	List of email addresses for VDSS Critical notifications. VDSS Warning Notification Recipient Email List Optional Select a value List of email addresses for VDSS Warning notifications.  enable_vdss_warning_alarm Enable withing alarms in VDSS compartment enable_vdss_critical_alarm Enable critical alarms in VDMS compartment enable_vdms_critical_alarm Enable_vdms_critical_alarm Enable_vdms_critical_alarm Enable_vdms_critical_alarm Enable_vdms_critical_alarm	\$
	onboard_log_analytics Set to true ONLY if your tenancy has NOT been onboarded onto log analytics (fails otherwise). Verify by visiting log analytics in the console.	
	Security Variables	
	backup_bucket_name Optional	
	OCLSCCA.J.Z.JAC.Backup	

### **Step 7 Security Variables**

Configure your **Security Variables**, many are optional.

Stack information	Security Variables		
Configure variables			
Review	backup_bucket_name Optional		
	OCI-SCCA-LZ-IAC-Backup		
	Name for bucket to store terraform state backups.		
	central_vault_name Optional		
	OCI-SCCA-LZ-Central-Vault		
	Name for Vault for Key storage.		
	central vault tune. Ontional		
		^	
		~	
	Type of vault. Set value to DEFAULT for testing purpose. Production deployments should be VIRTUAL_PRIVATE		
	enable_vault_replication		
	Enable to replicate vault to secondary region. Can only be enabled when vault type is VIRTUAL_PRIVATE		
	master_encryption_key_name Optional		
	OCI-SCCA-LZ-MSK		
	Name of Master Encryption Key		
	cloud guard target tenancy		
	Should Cloud Guard monitor entire tenancy? (If false, it just monitors the Landing Zone compartment tree)		



### **Step 8 Network Variables**

Configure your **Network Variables**.

Create stack		Help
1 <u>Stack information</u>	Network Variables	
3 Review	vdss_vcn_cidr_block	
	192.168.0.0/24	
	CIDR block for VDSS Network	
	firewall_subnet_cidr_block	
	192.168.0.0/25	
	CIDR block for VDSS Firewall Subnet. Must be within VDSS Network CIDR block.	
	lb_subnet_cidr_block	
	192.168.0.128/25	
	CIDR block for VDSS Loadbalancer Subnet. Must be within VDSS Network CIDR block	
	vdms_vcn_cidr_block	
	192.168.1.0/24	
	CIDR block for VDMS Network	
	vdms_subnet_cidr_block	
	192.168.1.0/24	
	CIDR block for VDMS Subnet. Must be within VDMS Network CIDR block	
	is_vdms_vtap_enabled	
	Add VTAP infrastructure for VDMS Network?	
Previous Next Cancel		

### **Step 9 Workload Variables**

Configure your Workload Variables, then click Next.

reate stack		Help
Stack information	Workload Variables	
Configure variables	mission_owner_key	
3 <u>Review</u>	test	
	Short prefix added to workload name to group workload resources.	
	workload_name	
	test	
	Name for initial example workload. Each workload within a Landing Zone should have a unique name.	
	workload_vcn_cidr_block	
	192.168.2.0/24	
	CIDR block for Workload Application Network	
	workload_subnet_cidr_block	
	192.168.2.0/24	
	CIDR block for Workload Application Subnet. Must be within Workload Network CIDR block	
	workload_db_vcn_cidr_block	
	192.168.3.0/24	
	CIDR block for Workload DB Network	
	workload_db_subnet_cidr_block	
	192.168.3.0/24	
revious Next <u>Cancel</u>		
ns of Use and Privacy Cookie Pre	arannas	Convright @ 2024. Oracle and/or its affiliates. All rights reserved

# **Step 10 Confirmation**

Validate all of your variable configuration entries.

Stack information				
Configure variables	Security Variables			
Review	central_vault_type	VIRTUAL_PRIVATE		
	enable_vault_replication	true		
	Bastion Client CIDR Block Allow List	192.168.0.0/16		
	Workload Variables			
	mission_owner_key	test		
	workload_name	test		
	Workload Critical Notification Recipient Email List			
	Workload Warning Notification Recipient Email List			
	Run apply on the created stack?			
	Immediately provision the resources defined in the Terra	form configuration by running the apply action on the new stack		

Once you have verified all of the sections, select **Create** to deploy the Landing Zone, which may take 10-15 minutes.

# **GitHub Deployment**

You can find more information on the <u>SCCA Landing Zone on GitHub</u>.

☆ m · · · · · · · · · · · · · · · · · ·	C
i≣ readme.md	
Deploy Using Oracle Resource Manager	
1. Click to deploy the stack	
C Deploy to Oracle Cloud	
If you aren't already signed in, when prompted, enter the tenancy and user credentials. Review an	
2. Select the region where you want to deploy the stack.	
3. Follow the on-screen prompts and instructions to create the stack.	
4. After creating the stack, click Terraform Actions, and select Plan.	
5. Wait for the job to be completed, and review the plan.	
<ol><li>To make any changes, return to the Stack Details page, click Edit Stack, and make the required changes. Then, run the Plan action again.</li></ol>	
<ol> <li>If no further changes are necessary, return to the Stack Details page, click Terraform Actions, and select Apply.</li> </ol>	
	<ul> <li>i github.com</li> <li>ii github.com</li> <li>iii readme.md</li> <li>Deploy Using Oracle Resource Manager</li> <li>1. Click to deploy the stack</li> <li>iii Deploy to Oracle Cloud</li> <li>If you aren't already signed in, when prompted, enter the tenancy and user credentials. Review an</li> <li>2. Select the region where you want to deploy the stack.</li> <li>3. Follow the on-screen prompts and instructions to create the stack.</li> <li>4. After creating the stack, click Terraform Actions, and select Plan.</li> <li>5. Wait for the job to be completed, and review the plan.</li> <li>6. To make any changes, return to the Stack Details page, click Edit Stack, and make the required changes. Then, run the Plan action again.</li> <li>7. If no further changes are necessary, return to the Stack Details page, click Terraform Actions, and select Plan Plan.</li> </ul>

Alternatively, you can clone the Zip file from GitHub and use the Command Line Interface (CLI) to deploy the Landing Zone.

Prerequisites         Create a terraform.tfvars file and populate with the required variables or override existing variables.         Note: An example tfvars file is included for reference. Using this file is the preferred way to run the stack from the CLI, because of the large number of variables to manage.         To use this file just copy the example tfvars file and save it in the outermost directory. Next, rename the file to terraform.tfvars. You can override the example values set in this file.         Clone the Module         Clone the source code from suing the following command:         git clone ADD_URL_HERE         cd repository_name	Deploy Using the Terraform CLI	
Create a terraform.tfvars file and populate with the required variables or override existing variables. Note: An example tfvars file is included for reference. Using this file is the preferred way to run the stack from the CLI, because of the large number of variables to manage. To use this file just copy the example tfvars file and save it in the outermost directory. Next, rename the file to terraform.tfvars. You can override the example values set in this file. <b>Clone the Module</b> Clone the source code from suing the following command: git clone ADD_URL_HERE cd repository_name	Prerequisites	
Note: An example tfvars file is included for reference. Using this file is the preferred way to run the stack from the CLI, because of the large number of variables to manage. To use this file just copy the example tfvars file and save it in the outermost directory. Next, rename the file to terraform.tfvars. You can override the example values set in this file. Clone the Module Clone the source code from suing the following command: git clone ADD_URL_HERE cd repository_name	Create a terraform.tfvars file and populate with the required variables or override existing variables.	
To use this file just copy the example tfvars file and save it in the outermost directory. Next, rename the file to terraform.tfvars. You can override the example values set in this file. Clone the Module Clone the source code from suing the following command: git clone ADD_URL_HERE cd repository_name	Note: An example tfvars file is included for reference. Using this file is the preferred way to run the stack from the CLI, because of the large number of variables to manage.	
Clone the Module Clone the source code from suing the following command: git clone ADD_URL_HERE cd repository_name	To use this file just copy the example tfvars file and save it in the outermost directory. Next, rename the file to terraform.tfvars. You can override the example values set in this file.	
Clone the source code from suing the following command: git clone ADD_URL_HERE cd repository_name	Clone the Module	
git clone ADD_URL_HERE cd repository_name	Clone the source code from suing the following command:	
	git clone ADD_URL_HERE cd repository_name	



#### **Connect with us**

Call +1.800.ORACLE1 or visit oracle.com. Outside North America, find your local office at: oracle.com/contact.

B blogs.oracle.com

facebook.com/oracle

twitter.com/oracle

Copyright © 2024, Oracle and/or its affiliates. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle, Java, and MySQL are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

12 10 Steps to Launch a Secure Cloud Computing Architecture (SCCA) Landing Zone / Version [1.0]

Copyright © 2024, Oracle and/or its affiliates / Public