

OCI Container Engine for Kubernetes Specialist

Student Guide
S1106087GC10



Copyright © 2024, Oracle and/or its affiliates.

Disclaimer

This document contains proprietary information and is protected by copyright and other intellectual property laws. The document may not be modified or altered in any way. Except where your use constitutes "fair use" under copyright law, you may not use, share, download, upload, copy, print, display, perform, reproduce, publish, license, post, transmit, or distribute this document in whole or in part without the express authorization of Oracle.

The information contained in this document is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

Restricted Rights Notice

If this documentation is delivered to the United States Government or anyone using the documentation on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

Trademark Notice

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

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

Third-Party Content, Products, and Services Disclaimer

This documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

1003072024

Table of Contents

Module 01: Containerization Overview	19
Course Overview	19
Course Description	20
For whom is this learning path intended?	22
Prerequisites	23
Learning Outcomes	24
Take the Skill Checks to Test Your Knowledge	27
Explore Limitless Possibilities with OCI's Official Documentation	28
Earn your OKE Specialist badge	29
Get the Answers You Need: <input type="checkbox"/> Use our "Ask Your Instructor" Form or Join the OU Community.....	30
Let's get started!	31
Module 1: Learning Objectives	32
Containerization Overview	33
What is Containerization?	34
How is it Different from Virtualization?	35
Benefits of Containerization	36
Docker Components	37
Docker Components	38
Virtual Machines Versus Containers	39
Basic Docker Commands	40
Demo: Docker Basic Commands	41
Working with Docker Images	42
Dockerfile	43
Basic Docker Commands	44
Demo: Working with Docker Images	45

Demo: Working with Docker Images and Repository	46
Module 02: Container Registry	47
Module 2: Learning Objectives	47
Oracle Cloud Infrastructure Registry OCIR: Introduction	48
What is OCIR	49
Key Benefits	50
Container Registry Concepts	51
Terminology: Summary	52
Managing Oracle Cloud Infrastructure Registry (OCIR)	54
Managing OCIR	55
Managing Repository	56
Managing Images	57
Managing Security	60
Preparing for Container Registry	62
Demo: Managing OCIR	63
OCIR Images Concepts	64
Open Container Initiative (OCI)	65
OCI Image Layout	68
Anatomy of an Image	69
Viewing Image Layers in OCIR	71
Putting It All Together	72
Demo: Managing OCIR (Repository Management) - I	73
Tasks	74
Demo: Managing OCIR (Push and Pull images)- II	75
Demo: Managing OCIR (Image Management) - III	76
Tasks	77
Module 03: Kubernetes Basics	78

Module 3: Learning Objectives	78
Introduction to Kubernetes	79
Container Engine for Kubernetes (OKE): Overview	80
Container Engine for Kubernetes: When and Why	81
Components of a Cluster	82
Node Pools	83
Supported Shapes and Operating Systems	84
Supported Kubernetes Versions	85
Version Drift in Control Plane Nodes and Worker Nodes	86
Kubernetes: Architecture and Main Components	87
Kubernetes Architecture: Overview	88
Kubernetes: Main Components	89
Kubernetes: Architecture and Features	97
Kubernetes Architecture: Components	98
Kubernetes: Features	99
Kubernetes Basic Commands I	100
Cluster Management	101
Basic Kubectl Commands	102
Managing Pods	103
Managing Deployments	104
Working with Services	105
Kubernetes Basic Commands II	106
Editing Pods and Deployments	107
Configuring and Debugging	108
Deleting Resources	109
Node operations	110
kubectl bash alias	111
Module 04: Introduction to OKE and working with Managed nodes	112

Module 4: Learning Objectives	112
Introduction to OKE	113
Container Engine for Kubernetes (OKE): Overview	114
Components of an OKE Cluster	117
Container Engine for Kubernetes: When and Why	118
Basic Clusters and Enhanced Clusters Overview	119
Types of OKE Clusters	120
Features Supported by Enhanced Clusters	121
Notable Features Not Supported	122
Creating Basic and Enhanced Clusters	123
Serverless Kubernetes with virtual nodes	124
Managed Nodes	128
Virtual Nodes	129
Virtual Nodes Overview	130
Supported Images and Shapes for Worker Nodes	131
Customize the worker nodes in an OKE cluster	132
Supported Images for Managed Nodes	134
Shapes for Managed Nodes	138
Shapes for Virtual Nodes	139
<input type="checkbox"/> Prerequisite to Create an OKE Cluster	140
Prerequisite to Create an OKE Cluster	141
Policy Configuration for Cluster Creation and Deployment	148
Policy Configuration for Cluster Creation and Deployment	149
Required IAM Policies	150
Policies to create and configure associated new network resources when creating new clusters in the 'Quick Create' workflow	151
Optional Policies for working with OKE Service	152
Creating Kubernetes Clusters Using Console Workflows	153
Ways to create an OKE Cluster	154

Quick Create Workflow	155
Custom Create workflow	156
Ways to create an OKE Cluster	157
Network Resource Configuration for Custom Cluster Creation and Deployment	158
Network Resource Configuration □for Custom OKE.....	159
Understanding network connectivity for pods running on worker nodes	168
Container Network Interface (CNI) specification for network resource management	169
Using the flannel CNI plugin for pod networking	171
CIDR blocks when using the flannel CNI plugin for pod networking	172
Using the OCI VCN-Native Pod Networking CNI plugin for pod networking	173
CIDR blocks when using the OCI VCN-Native Pod Networking CNI plugin for pod networking	174
Key considerations when using the OCI VCN-Native Pod Networking CNI plugin	175
Updating the OCI VCN-Native Pod Networking CNI plugin	176
Examples-Network Resource Configuration for Cluster Creation and Deployment	177
Example 01: Cluster with Flannel CNI Plugin, Private Kubernetes API Endpoint, Private Worker Nodes, and Public Load Balancers	178
Example 02: Cluster with Flannel CNI Plugin, Private Kubernetes API Endpoint, Private Worker Nodes, and Public Load Balancers	179
Example 03: Cluster with OCI VCN-Native Pod Networking CNI Plugin, Public Kubernetes API Endpoint, Private Worker Nodes, and Public Load Balancers	180
Example 04: Cluster with OCI VCN-Native Pod Networking CNI Plugin, Private Kubernetes API Endpoint, Private Worker Nodes, and Public Load Balancers	181
Demo: Create Cluster using default settings in the 'Quick Create' workflow- Managed Nodes	182
Demo: Create Cluster with Explicitly Defined Settings in the 'Custom Create' workflow- Managed Nodes	183
Example : Cluster with Flannel CNI Plugin, Private Kubernetes API Endpoint, Private Worker Nodes, and Public Load Balancers	184
Module 05: Setting up OKE cluster access	185
Module 5: Learning Objectives	185
Accessing a Cluster Using Kubectl I	186
Accessing a Cluster Using Kubectl	187
Kubeconfig Files	188

Accessing a Cluster Using Cloud Shell and Local Terminal	193
Setting Up Cloud Shell Access to Clusters	194
Setting Up Local Access to Clusters	195
Set up the kubeconfig file	196
Setting Up Local Access to Clusters	197
Demo: Setting Up Cloud Shell Access to OKE Clusters	198
Demo: Setting Up Local Access to OKE Clusters	199
Setting Up Local Access to Clusters	200
Connecting to Managed Nodes Using SSH	201
Accessing Worker Nodes	202
Connecting to Managed Nodes Using SSH	203
SSH to Managed Node in Public Subnet from UNIX Machine	204
Demo: Connecting to Managed Nodes in Public Subnets Using SSH	209
Setting Up a Bastion for Cluster Access	210
Accessing OKE cluster planes	211
OCI Bastion Overview	212
Setting up bastions and bastion sessions	213
Example cluster configuration with a bastion providing secure access to a cluster's Kubernetes API endpoint and worker nodes.	214
Bastion IAM policies	215
Setting up a bastion to access the Kubernetes API endpoint	216
Steps to have SSH access to Kubernetes API endpoint	217
Setting up IAM policies to limit the use of bastions	219
Steps to have SSH access to Kubernetes API endpoint	220
Steps to have SSH access to managed nodes	221
Demo: Setting up a bastion to access the Kubernetes API endpoint	224
Demo: Setting up a bastion to provide SSH access to managed nodes	225
Module 06: Working with OKE Virtual Nodes	226

Module 6: Learning Objectives	226
Comparing Virtual Nodes with Managed Nodes	227
Management	228
Resource Allocation	229
Load Balancing	230
Pod Networking	231
Scaling Kubernetes Clusters and Node Pools	232
Pricing	233
Prerequisite to configure Cluster with Virtual Nodes	234
Required IAM Policies for Using Virtual Nodes	235
Virtual Node and Node Pool Management and Resource Allocation	244
Virtual Node Pool Management	245
Virtual Node Management	250
Resources Allocated to Pods Provisioned by Virtual Nodes	251
CPU and memory limits and requests specified in the pod spec for containers	252
Resources Allocated to Pods Provisioned by Virtual Nodes	253
Demo: Create Cluster using default settings in the 'Quick Create' workflow- Virtual Nodes	254
Demo: Managing Virtual Nodes and Virtual Node Pools in a New Cluster	255
Module 07: Working with Self-Managed Nodes	256
Module 7: Learning Objectives	256
OKE Self-Managed Nodes Overview and Prerequisite	257
OKE Self-Managed Nodes Overview	258
OKE Self-Managed Nodes Usage	260
Prerequisites for Self-Managed Node Creation	261
Demo: Creating Self-Managed Nodes	264
Creating a Self-Managed Node for OKE Cluster	265
Key points	275

Module 08: Managing Kubernetes Deployments	276
Module 8: Learning Objectives	276
Demo: Deploying a Multi-Tier App on a OKE Cluster Using Kubectl	277
Demo: Guestbook Architecture	278
Pulling Images from Registry During Deployment	279
Pulling Images from Container Registry	280
Pull Images That Reside in <input type="checkbox"/> Oracle Cloud Infrastructure Registry	281
Create a Docker Registry Secret	283
Edit the Application Manifest	284
Demo: Pulling Images from Registry during Deployment	285
Supported Labels for Different Usecase	286
Supported Labels	287
OCI Architecture	288
Cloud Regions, Hybrid Cloud, Multi-Cloud	289
Availability Domains	290
Fault Domains	291
Supported Labels	292
topology.kubernetes.io/zone	293
Supported Labels	294
oci.oraclecloud.com/fault-domain	295
Supported Labels	297
node.kubernetes.io/exclude-from-external-load-balancers	298
OCI Service Operator for Kubernetes	300
OCI Service Operator for Kubernetes	301
Integration with Oracle Cloud Infrastructure Services	303
Demo: Adding OCI Service Operator for Kubernetes to Clusters	304
Demo: Deploy Oracle MySQL DB System Service from Kubernetes	305

Defining Kubernetes Services of Type LoadBalancer	306
Container Engine for Kubernetes Implements the Service of Type LoadBalancer	307
Specifying the Annotation for an OCI Load Balancer	309
Terminating SSL/TLS at the Load Balancer	310
Create a Self-Signed Certificate	311
Defining Kubernetes Services of Type LoadBalancer	312
Specifying Alternative Load Balancer Shapes	313
Specifying Flexible Load Balancer Shapes	315
Specifying Load Balancer Connection Timeout	317
Specifying Listener Protocols	319
Specifying the Annotation for an OCI Network Load Balancer	321
Specifying Network Security Groups	322
Specifying the Back-End Set Policy	326
Specifying Reserved Public IP Addresses	327
Specifying Health Check Parameters	329
Note that if you do not explicitly specify health check parameter values, the following defaults are used:	332
Key Points to Remember	333
Managing Ingress Controllers	334
Ingress Controllers: Overview	335
Setting Up Ingress Controller in OKE	336
Working with OCI Native Ingress Controller	337
Steps to Set Up the OCI Native Ingress Controller	338
Key Points to Note	340
Running Applications on Arm-Based Nodes	341
Running Applications on Arm-Based Nodes	342
Defining a Pod to Run <input type="checkbox"/> Only on Arm-Based Nodes.....	343
Running Applications on Arm-Based Nodes	346
Demo: Running Applications on ARM-Based Nodes	347

Running Applications on GPU Nodes	348
Running Applications on GPU Nodes	349
Defining a Pod to Run Only on Nodes That Have a GPU	351
GPU Shapes Supported by Container Engine for Kubernetes	352
Demo: Running Applications on GPU Nodes	353
Module 09: Setting Up Storage for Kubernetes Clusters within OKE	354
Module 9: Learning Objectives	354
Setting Up Storage for Kubernetes Clusters	355
Storage for Kubernetes Clusters	356
Storage for Kubernetes Clusters	357
Provisioning Persistent Volume Claims	358
Provisioning PVCs on the Block Volume Service	359
Provisioning PVCs on the Block Volume Service	360
Creating a PVC on a Block Volume Using the CSI Volume Plugin	362
Demo: Provisioning PVCs on the Block Volume Service	364
Expanding a Block Volume	365
Expanding a Block Volume	366
Key Points	369
Demo: Expanding a Block Volume	370
Specifying Block Volume Performance	371
Specifying Block Volume Performance	372
Key Points	377
Demo: Specifying Block Volume Performance	378
Specifying File System Types for Block Volumes	379
File System Types for Block Volumes	380
Specifying File System Types for Block Volumes	383
Key Points	387

Provisioning PVCs on the File Storage Service	388
File Storage Service to Provision Persistent Volume Claims (PVCs)	389
Key Points	393
Provisioning a PVC on a New File System	394
Provisioning a PVC on a New File System Using the CSI Volume Plugin	395
Provisioning a PVC on an Existing File System	410
Provisioning a PVC on an Existing File System	411
Module 10: Administering and Managing OKE Clusters	413
Module 10: Learning Objectives	413
Accessing the OKE Dashboard	414
Kubernetes Dashboard	415
Deploying Kubernetes Dashboard	416
Accessing a Cluster using the Kubernetes Dashboard	422
Using the OKE Dashboard: Considerations	425
Demo: Accessing the OKE Dashboard	426
Modifying Kubernetes Cluster Properties	427
Parameters That You Can Change	428
Managing Node Pools	429
Node Pool Management	430
Creating a Node Pool	431
Listing Node Pools	432
Getting a Node Pool's Details	433
Updating a Node Pool	434
Deleting a Node Pool	435
Deleting a Node Pool (Advanced Options)	436
Demo: Managing Node Pool	437
Modifying Node Pool and Worker Node Properties	438

Properties That You Can Change	439
Tips and Considerations	440
Managing a Worker Node	441
Tips and Considerations	442
Configuring IMDS for Kubernetes Clusters	443
Using the CLI to Disable the IMDSv1 Endpoint	444
Confirming the IMDSv1 Endpoint Is Disabled	446
Managing Worker Node Capacity Types	447
Managing Worker Node Capacity Types	448
Reserved Capacity	449
Pre-emptible Capacity	450
Required IAM Policies for Using Capacity Reservations	451
Demo: Using Capacity Reservations to Provision Managed Nodes	452
Using Custom cloud-init Initialization Scripts to Set Up Managed Nodes	453
Custom cloud-init Initialization Scripts	454
Example Use Cases for Custom cloud-init Scripts	457
Demo: Creating a Custom cloud-init Script	458
Scaling Kubernetes Clusters and Node Pools	459
Scaling Clusters with Managed Node Pools	460
Scaling Clusters with Virtual Node Pools	461
Scaling Node Pools	462
Autoscaling Kubernetes Node Pools and Pods	463
Autoscaling Kubernetes Node Pools	464
Ways to deploy the Kubernetes Cluster Autoscaler	465
Recommendations When Using the Kubernetes Cluster Autoscaler in Production Environments	466
Tips and Considerations	467
Demo: Working with the Cluster Autoscaler Add-on	468
Working with the Cluster Autoscaler	469

Kubernetes Metrics Server Overview	470
Kubernetes Metrics Server Overview	471
Kubernetes Metrics Server Overview	472
Demo: Deploying the Kubernetes Metrics Server on a Cluster by Using Kubectl	473
Deploying the Kubernetes Metrics Server on a Cluster Using Kubectl	474
Kubernetes Horizontal Pod Autoscaler	477
Using the Kubernetes Horizontal Pod Autoscaler	478
Demo: Working with the Horizontal Pod Autoscaler	479
Working with the Horizontal Pod Autoscaler	480
Kubernetes Vertical Pod Autoscaler	481
Using the Kubernetes Vertical Pod Autoscaler	482
Upgrading Clusters to Newer Kubernetes Versions	483
Kubernetes Versions and OKE	484
Upgrading Control Plane Nodes	486
Demo: Upgrading Clusters to Newer Kubernetes Versions	487
Upgrading the Kubernetes Version on Worker Nodes in a Cluster	488
Upgrading Worker Nodes	489
Managed Node Upgrade	490
Self-Managed Node Upgrade	491
Virtual Node Upgrade	492
Upgrading Clusters Keypoints	493
Demo: Upgrading the Kubernetes Version on Worker Nodes in a Cluster	494
Configuring DNS Servers for Kubernetes Clusters	495
Configuring DNS Servers for Kubernetes Clusters	496
Configuring Built-in DNS Servers	497
Configuring ExternalDNS	503
Observing Kubernetes Clusters I	504

Observing Kubernetes <input type="checkbox"/> Clusters.....	505
Monitoring Clusters	506
Observing Kubernetes Clusters II	509
Observing Kubernetes <input type="checkbox"/> Clusters.....	510
Viewing Work Requests	511
Observing Kubernetes Clusters III	513
Observing Kubernetes <input type="checkbox"/> Clusters.....	514
Viewing OKE Service Logs	515
Observing Kubernetes Clusters IV	516
Observing Kubernetes <input type="checkbox"/> Clusters.....	517
Viewing Kubernetes API Server Audit Logs	518
Observing Kubernetes Clusters V	519
Viewing Application Logs on Virtual Nodes	520
Observing Kubernetes <input type="checkbox"/> Clusters.....	521
Viewing Application Logs on Managed Nodes and Self-Managed Nodes	522
Viewing Application Logs on Virtual Nodes	523
Viewing Application Logs on Virtual Nodes	524
Observing Kubernetes Clusters VI	525
Observing Kubernetes <input type="checkbox"/> Clusters.....	526
Container Engine for Kubernetes Metrics	527
Module 11: Container Engine for Kubernetes Security	531
Module 11: Learning Objectives	531
Adding a Service Account Authentication Token to a Kubeconfig File	532
Adding a Service Account Authentication Token to a Kubeconfig File	533
Demo: Adding a Service Account Authentication Token to a Kubeconfig File	535
Access Control and Container Engine for Kubernetes	536
IAM for Access Control in OKE	537

Demo: Granting the Kubernetes RBAC <code>cluster-admin</code> ClusterRole	539
Demo: Creating a Kubernetes Role and Rolebinding to Enable a Non-administrator User to Read Pods in a Cluster	540
Demo: Creating a Kubernetes Role and Rolebinding to Enable a Group to Read Pods in a Cluster	541
Demo: Creating a Kubernetes ClusterRole and clusterrolebinding to enable Users and Groups to List Secrets in a Cluster	542
Managing Secrets for Kubernetes Clusters	543
Managing Secrets for Kubernetes Clusters	544
OKE: Container Image Security	548
Container images must have the following characteristics:	549
Security First	550
Container images must have the following characteristics:	551
Unaltered Integrity	552
Container images must have the following characteristics:	553
Trusted Sources	554
Demo: Scanning Container Image for Vulnerabilities	555
Demo: Sign and Verify Container Image for Security	557
Enforcing the Use of Signed Images from OCIR	559
Enforcing the Use of Signed Images from OCIR	560
IAM Policies for Enforcing the Use of Signed Images from OCIR	565
Demo: Enforcing the Use of Signed Images from OCIR	567
Encrypting Data at Rest and Data in Transit with the Block Volume Service	568
Data Encryption in Oracle Cloud Infrastructure Block Volume Service	569
Block Volume Encryption Options in Kubernetes	570
Block Volume Encryption Settings Interaction	571
Configuring a Storage Class to Enable At-Rest and In-Transit Encryption Using the Default Oracle-Managed Key	572
Configuring a Storage Class to Enable At-Rest and In-Transit Encryption Using a Key that You Manage	573
Encrypting Data at Rest and Data in Transit with the File Storage Service I	574
Encrypting Data at Rest and Data in Transit with the File Storage Service	575
Encrypting Data at Rest on a New File System using Oracle-Managed Keys	576

Encrypting Data at Rest on a New File System using Own Master Encryption Keys	577
Encrypting Data at Rest and Data in Transit with the File Storage Service II	578
Encrypting Data at Rest with the File Storage Service	579
Encrypting Data at Rest and Data in Transit with the File Storage Service III	582
Encrypting Data in Transit with the File Storage Service	583
Encrypting Data in Transit on a New File System	584
Encrypting Data in Transit with the File Storage Service	585
Encrypting Data in Transit on an Existing File System	586