ORACLE
PRESS

Oracle Cloud Infrastructure

A Guide to Building Cloud Native Applications

Jeevan Gheevarghese Joseph
Adao Oliveira Junior
Mickey Boxell

ORACLE

Oracle Cloud Infrastructure: A Guide to Building Cloud Native Applications

Oracle Cloud Infrastructure - A Guide to Building Cloud Native Applications

Table of Contents

Cover

Half Title

Title Page

Copyright Page

Contents

Contents at a Glance

1 Introduction to Oracle Cloud Infrastructure

- Realms, Regions, and Availability Domains
- Tenancies and Compartments
- Controlling Access to Resources
- Cloud Guard and Security Zones
- Service Limits and Cost Management
- Getting Started with Your Tenancy
  - Setting Up Users and Groups
  - Setting Up API Keys and Auth Tokens
- Planning How Your Teams Will Use OCI
- Summary
- References

2 Infrastructure Automation and Management

- One Set of APIs, Different Ways to Call Them
- A Quick Terraform Primer

Table of Contents

- A Basic Introduction to the Terraform Language
- Terraform State Tracking

The OCI Terraform Provider

- Setting Up the OCI Terraform Provider
- Managing OCI Resources with Terraform

Simplifying Infrastructure Management with the Resource Manager Service

- Helm and Kubernetes Providers
- Generating Resource Manager Stacks
- Resource Discovery
- Drift Detection
- Generating a User Interface from Terraform Configurations with a Custom Schema
- Publishing Your Stacks with Deploy Buttons

Managing Multiregion and Multicloud Configurations

Summary

References

3 Cloud Native Services on Oracle Cloud Infrastructure

Oracle Container Image Registry

Working with OCIR

- Image Signing
- Image Scanning

Creating Containers from Images

Compute Instances

Container Instances

Container Engine for Kubernetes

Service Mesh

Serverless Functions

Table of Contents

API Gateways

Components of an API Gateway

Working with the API Gateway Service

Messaging Systems

Streaming

Understanding the Streaming Service

Working with the OCI Streaming Service

OCI Events Service

Summary

References

4 Understanding Container Engine for Kubernetes

Monoliths and Microservices

Containers

Container Orchestration and Kubernetes

Oracle Container Engine for Kubernetes

OCI-Managed Components and Customer-Managed Components

Control Plane

Data Plane

Billable Components

Kubernetes Concepts

Cloud Controller Manager

Nodes and Node Pools

Node Pool Properties

Worker Node Images and Shapes

Kubernetes Labels

SSH Keys

Tagging Your Resources

Creating a Cluster

Table of Contents

Quick Create Cluster Workflow

Custom Create Cluster Workflow

Using the OCI Command-Line Interface

Using the Terraform Provider and Modules

Automation and Terraform Code Generation

Asynchronous Cluster Creation

Cluster Topology Considerations

Using Multiple Node Pools

Scheduling Workloads on Specific Nodes

Kubernetes Networking

Container Network Interface (CNI)

OCI VCN-Native Pod Networking CNI

Flannel CNI

Kubernetes Storage

StorageClass: Flex Volume and CSI Plug-ins

Updating the Default Storage Class

File System Storage

Kubernetes Load Balancer Support

Working with the OCI Load Balancer Service

SSL Termination with OCI Load Balancer

Working with the OCI Network Load Balancer Service

Specifying Reserved Public IP Addresses

Commonly Used Annotations

Understanding Security List Management Modes

Using Node Label Selectors

Security Considerations for Your Cluster

Cluster Topology and Configuration Security Considerations

Authorization Using Workload Identity and Instance Principils

Securing Access to the Cluster

Pearson

Table of Contents

OCI IAM and Kubernetes RBAC

Federation with an IDP

Summary

References

5 Container Engine for Kubernetes in Practice

Kubernetes Version Support

Upgrading the Control Plane

Upgrading the Data Plane

Upgrading an Existing Node Pool

Upgrading by Adding a Node Pool

Alternative Host OS (Not Kubernetes Version) Upgrade Options

Scaling a Cluster

Manual Scaling

Autoscaling

Scaling Workloads and Infrastructure Together

Autoscaler Best Practices

Cluster Access and Token Generation

Service Account Authentication

Configuring DNS

Configuring Node Local DNS Cache

Configuring ExternalDNS

Cluster Add-ons

Configuring Add-ons

Disabling Add-ons

Observability: Prometheus and Grafana

Monitoring Stack Components

Installing the kube-prometheus-stack

Operators and OCI Service Operator for Kubernetes

Table of Contents

    - Getting Started with Operators on OKE
    - Operators for OCI, Oracle Database, and Oracle WebLogic
  - Troubleshooting Nodes with Node Doctor
  - Configuring SR-IOV Interfaces for Pods on OKE Using Multus
    - Using Bare Metal Nodes
    - Using Virtual Machine Nodes
  - Summary
  - References
- 6 Securing Your Workloads and Infrastructure
  - Kubernetes Security Challenges
  - Concepts of Kubernetes Security
  - 4Cs of Kubernetes Security
  - Securing Oracle Cloud Infrastructure Container Engine for Kubernetes (OKE)
    - Private Clusters
    - Kubernetes Role-Based Access Control (RBAC) with OCI IAM Groups
    - Data Encryption and Key Management Service
    - Audit Logging
    - Security Zones
    - Network Security Groups (NSGs)
    - Web Application Firewall (WAF)
    - Network Firewall
    - Allowed Registries
    - Cloud Guard
  - Hardening Containers and OKE Worker Nodes
    - Container Scanning
    - Container Image Signing
    - Center for Internet Security (CIS) Kubernetes Benchmarks

Table of Contents

Using SELinux with OKE

Worker Nodes Limited Access

Securing Your Workloads

Security Context

syscalls and seccomp

Open Policy Agent (OPA)

OPA Gatekeeper

Open Web Application Security Project (OWASP)

Supporting Tools

External Container Scanning Tools

CIS-CAT Pro Assessor

Kube-bench

AppArmor

Falco

Tracee

Trivy

National Institute of Standards and Technology (NIST) Kubernetes Benchmarks

NIST Kubernetes Benchmarks

National Checklist Program Repository

National Vulnerability Database

NIST SP 800-190 Application Container Security Guide

Summary

References

7 Serverless Platforms and Applications

Container Instances

Architecture

Using Container Instances

Serverless Functions

Table of Contents

OCI Functions

Using OCI Functions

Building Your First Function

Adding an API Gateway

Function Logs and Distributed Tracing

Service Mesh

Using the Service Mesh

Adding a Service Mesh to an Application

Summary

References

8 Observability

OCI Monitoring

Alarms

OCI Logging

Service Logs

Custom Logs

Audit Logs

Auditing OKE Activity

Advanced Observability in OCI

Logging Analytics

Enabling and Using Logging Analytics

Prometheus and Grafana with OKE

Using the OCI DataSource Plug-ins for Grafana

eBPF-Based Monitoring with Tetragon on OKE

Tetragon: eBPF-Based Security Observability and Enforcement

Running Tetragon on Oracle Container Engine for Kubernetes (OKE)

Summary

References

Table of Contents

9 DevOps and Deployment Automation

- OCI DevOps Service
  - Code Repositories
  - Triggers
  - Build Pipelines
  - Artifacts
  - Environments
  - Deployment Pipelines
- Elastically Scaling Jenkins on Kubernetes
  - Setting Up Jenkins on OKE
- GitOps with ArgoCD
  - Setting Up Argo CD on OKE
- Summary
- References

10 Bringing It Together: MuShop

- Architecture
- Source Code Structure
- Services
  - Storefront
  - API
  - Catalog
  - Carts
  - User
  - Orders
  - Fulfillment
  - Payment
  - Assets
  - DBTools

Pearson

Table of Contents

Edge Router

Events

Newsletter Subscription

Load

Building the Services

Infrastructure Automation

Helm Charts

Utilities and Supporting Components

Deploying MuShop

Summary

References

Index

Pearson