Table of Contents

Preface

Section 1: Basic CI/CD and Policy as Code

1

CI/CD Using AWS CodeStar

Technical requirements 4

Introduction to CI/CD, along with a branching strategy 4

CI 4

CD 6

Branching strategy (Gitflow) 11

Creating a project in AWS CodeStar 18

Introduction to AWS CodeStar 18

Getting ready 19

Creating feature and development branches, as well as an environment 32

Creating feature and develop branches 32

Creating a development environment and pipeline 33

Validating PRs/MRs into the develop branch from the feature branch via CodeBuild and AWS Lambda 45

Adding a production stage and environment 56

Modifying the pipeline 56

Summary 66

2

Enforcing Policy as Code on CloudFormation and Terraform

Technical requirements 68

Implementing policy and governance as code on infrastructure code 68

Policy as code 68

Why use policy as code? 69

Policy as code in CI/CD 70

Using CloudFormation Guard to enforce compliance rules on CloudFormation templates 72

CloudFormation Guard 72

Installation 72

Template validation 73

Writing CloudFormation Guard rules 73

Using AWS Service Catalog across teams with access controls and constraints 82

AWS Service Catalog 82

Integrating Terraform Cloud with GitHub 92

Terraform Cloud 92

VCS-driven workflow (GitHub) 94

Running a Terraform template in Terraform Cloud 97

Writing Sentinel policies to enforce rules on Terraform templates 99

HashiCorp Sentinel 100

Summary 106

3

CI/CD Using AWS Proton and an Introduction to AWS CodeGuru

Technical requirements 108

Introduction to the AWS Proton service 108

What is AWS Proton? 109

Creating the environment template bundle 112

Writing an environment template 112

Creating the service template bundle 123

Writing the service template 123

Deploying the containerized application by creating a service instance in Proton 127

Creating a source connection (GitHub) 128

Deploying the application by creating a service instance 131

Introduction to Amazon CodeGuru 137

Integrating CodeGuru with AWS CodeCommit and analyzing the pull request report 139

Summary 143

Section 2: Chaos Engineering and EKS Clusters

4
Working with AWS EKS and App Mesh

Technical requirements 148

Deep diving into AWS EKS 148

Kubernetes components 148

Deploying an EKS cluster 153

Introducing AWS App Mesh 156

Are microservices any good? 156

AWS App Mesh 159

Deploying an application (Product Catalog) on EKS 164

Implementing traffic management 168

Installing the App Mesh controller 169

Getting observability using X-Ray 177

Enabling mTLS authentication between services 180

Summary 187

5
Securing Private EKS Cluster for Production

Technical requirements 190

Planning your fully private EKS cluster 190

Creating your EKS cluster 192

VPC, subnet, and endpoint creation 192

Bastion server 203

Creating a cluster 205

Verifying the cluster access 209

Deploying add-ons 210

Creating copies of container images in ECR 210

IAM roles for service accounts 212

Cluster Autoscaler 214

The Amazon EBS CSI driver 220

Enabling the App Mesh sidecar injector 226

Kubernetes hardening guidance using Kubescape 228

Policy and governance using OPA Gatekeeper 231

Deploying a stateful application using Helm 235

Backup and restore using Velero 240

How does Velero work? 241

Summary 246

6

Chaos Engineering with AWS Fault Injection Simulator

Technical requirements 248

The concept of, and need for, chaos engineering 248

Principles of chaos engineering 249

AWS FIS 249

Chaos engineering in CI/CD 250

Experimenting with AWS FIS on multiple EC2 instances with a terminate action 251

Experimenting with AWS FIS on EC2 instances with a CPU stress action 265

Experimenting with AWS FIS on RDS with a reboot and failover action 272

Experimenting with AWS FIS on an EKS cluster worker node 286

Summary 295

Section 3: DevSecOps and AIOps

7

Infrastructure Security Automation Using Security Hub and Systems Manager

Technical requirements 300

Introduction to AWS Security Hub 300

Deny execution of non-compliant images on EKS using AWS Security Hub and ECR 304

Importing an AWS Config rules evaluation as a finding in Security Hub 312

Integrating AWS Systems Manager with Security Hub to detect issues, create an incident, and remediate automatically 317

Summary 332

8

DevSecOps Using AWS Native Services

Technical requirements 334

Strategy and planning for a CI/CD pipeline 334

Monorepos versus polyrepos 335

Feature branch 337

Develop branch 340

Staging branch 341

Master branch 342

Creating a CodeCommit repository for microservices 349

Creating PR CodeBuild stages with CodeGuru Reviewer 351

Creating a development CodePipeline project with image scanning and an EKS cluster 359

Creating a staging CodePipeline project with mesh deployment and chaos testing with AWS FIS 368

Creating a production CodePipeline project with canary deployment and its analysis using Grafana 382

- Canary deployment using Flagger 388
- Updating a new version of the service 396

Summary 401

9

DevSecOps Pipeline with AWS Services and Tools Popular Industry-Wide

Technical requirements 404

DevSecOps in CI/CD and some terminology 404

- Why DevSecOps? 405

Introduction to and concepts of some security tools 407

- Snyk – Security advisory for source code vulnerabilities in real time 407
- Talisman – Pre-commit secrets check 407
- Anchore inline scanning and ECR scanning – SCA and SAST 407
- Open Web Application Security Project-Zed Attack Proxy (OWASP ZAP) – DAST 408
- Falco – RASP 408

Planning for a DevSecOps pipeline 409

Using a security advisory plugin and a pre-commit hook 412

Prerequisites for a DevSecOps pipeline 418

Installation of DAST and RASP tools 422

- Installing OWASP ZAP 423
- Installing Falco 426

Integration with DevOps Guru 431

Creating a CI/CD pipeline using CloudFormation 432

Testing and validating SAST, DAST, Chaos Simulation, Deployment, and RASP 435

Summary 445

10
AIOps with Amazon DevOps Guru and Systems Manager OpsCenter

Technical requirements 448

AIOps and how it helps in IT operations 448

AIOps using Amazon DevOps Guru 453

Enabling DevOps Guru on EKS cluster resources 455

Injecting a failure and then reviewing the insights 461

Deploying a serverless application and enabling DevOps Guru 468

Integrating DevOps Guru with Systems Manager OpsCenter 473

Injecting a failure and then reviewing the insights 474

Summary 484

Index

Other Books You May Enjoy