



LEARNING AMAZON WEB SERVICES (AWS)

A Hands-On Guide to the Fundamentals of AWS Cloud



MARK WILKINS

Learning Amazon Web Services (AWS)

Learning Amazon Web Services (AWS): A Hands-On Guide to the Fundamentals of AWS Cloud

Table of Contents

Cover

Title Page

Copyright Page

Contents at a Glance

Table of Contents

Preface

About the Author

Acknowledgments

1 Learning AWS

 About This Book

 Trying to Define the Cloud

 Moving to AWS

 Infrastructure as a Service

 Platform as a Service

 Essential Characteristics of AWS Cloud Computing

 Operational Benefits of AWS

 Cloud Provider Limitations

 Data Security at AWS

 Network Security at AWS

Table of Contents

Application Security at AWS

Compliance in the AWS Cloud

Playing in the AWS Sandbox

Whats the Problem That Needs to Be Solved?

Migrating Applications

The Well-Architected Framework

The Well-Architected Tool

In Conclusion

2 Designing with AWS Global Services

Considering Location

AWS Regions

Region Isolation

Availability Zones

Availability Zone Distribution

Multiple Availability Zones

Whats the AWS Service-Level Agreement?

Everything Fails

Global Edge Services

Services Located at the Edge

Choosing a Region

Compliance

AWS and Compliance

HIPAA

NIST

GovCloud

Latency Concerns

Services Offered at Each Region

Table of Contents

Calculating Costs

Management Service Costs

Management Tools Pricing: AWS Config

AWS Compute Costs

Storage Costs

Data Transfer Costs

Understand Tiered Costs at AWS

Optimizing Costs at AWS

Optimizing Compute Costs

Tools for Analyzing Costs at AWS

Trusted Advisor

AWS Simple Monthly Calculator

Total Cost of Ownership (TCO) Calculator

In Conclusion

Top 10 Big-Picture Discussion Points: Compliance, Governance,
Latency, and Failover Considerations

3 AWS Networking Services

VPC Networking

Partnering with AWS

Whats Behind the Networking Curtain?

Its All About Packet Flow

Creating Your First VPC

How Many VPCs?

Creating the VPC CIDR Block

Planning Your Primary VPC CIDR Block

The Default VPC

Revisiting Availability Zones

Table of Contents

Creating Subnets

NAT Services

Working with Route Tables

The Main Route Table

Private IPV4 Addresses

Elastic IP Addresses

Traffic Charges

Bring Your Own IP (BYOIP)

The BYOIP Process

IPv6 Addresses

Security Groups

Custom Security Groups

Network ACLs

Network ACL Implementation Details

Understanding Ephemeral Ports

VPC Flow Logs

Peering VPCs

Establishing a Peering Connection

Gateway VPC Endpoints

Interface VPC Endpoints

VPC Connectivity

Internet Gateway: The Public Door

VPN Connections

Virtual Private Gateway

VPN Connections

VPN CloudHub

Understanding Route Propagation

Table of Contents

Direct Connect

Route 53

- Route 53 Routing Options

- Route 53 Health Checks

Using DNS with a VPC: Private DNS Zones

- DNS Hostnames

In Conclusion

Top 10 Discussion Points: Considerations for Security, Failover, and Connectivity

4 Compute Services: AWS EC2 Instances

A Short History of EC2 Virtualization

The Nitro System

EC2 Instances

Instance Families

Whats a vCPU?

EC2 Instance Choices

- General-Purpose Instances

Instances Designed to Burst

- Compute-Optimized Instances

- Memory-Optimized Instances

- Accelerated Computing (GPU)

- Storage-Optimized Instances

- Bare-Metal Instances

- Dedicated Hosts

- Dedicated Instances

EC2 Network Performance

Amazon Machine Images (AMIs)

Table of Contents

Choosing an AMI

- AWS Linux AMIs

- Linux AMI Virtualization Types

- Windows AMIs

- AWS Marketplace

Creating a Custom AMI

Custom Instance Store AMIs

Proper AMI Design

- AMI Build Considerations

- AMI Best Practices

- Adopting a Best Practice: Tags

- Using Launch Templates

- Changing the Current Instance Type

EC2 Pricing

Reserved Instances (RI)

- Reserved Instance Limits

- Reserved EC2 Instances Types

- Scheduled Reserved EC2 Instances

- Spot Instance

Spot Fleet

- Spot Capacity Pools

EC2 Fleet

EC2 Instance Storage Options

- Local Instance StorageSSD or Magnetic Disk

EC2 Auto Recovery

Ordering an Instance

Migrating to AWS

- Migration Big-Picture Steps

Table of Contents

AWS Migration Hub

AWS Server Migration Services

Server Migration Big Steps

Importing and Exporting Virtual Resources

Other Ways to Host Workloads at AWS

Containers

Amazon Elastic Container Service (ECS)

AWS Fargate

AWS ECS for Kubernetes (EKS)

Amazon LightSail

Lambda

AWS Firecracker

In Conclusion

Top 10 Big-Picture Discussion Points: Migration and Planning
Considerations

5 Planning for Scale and Resiliency

The Concept of Monitoring

What Is CloudWatch?

Monitoring

Logging

Collecting Data with the CloudWatch Agent

CloudWatch Agent Install Steps

Planning for Monitoring

CloudWatch Integration

CloudWatch Terminology

Using the Dashboard

Creating a CloudWatch Alarm

Additional Alarm and Action Settings

Table of Contents

Actions

Monitoring EC2 Instances

Automatically Reboot or Recover Instances

Elastic Load Balancing Services

Redundancy by Design

EC2 Health Checks

Additional ELB Features

Application Load Balancer (ALB)

Big-Picture Steps: ALB Creation

Rule Choices

HTTPS Listener Security Settings

Target Group Routing

Maintaining User Sessions

Sticky Session Support

Configuring Health Checks

Monitoring Load Balancer Operation

Network Load Balancer

Scaling Applications

EC2 Auto Scaling

EC2 Auto Scaling Components

Launch Configuration

Launch Templates

Auto Scaling Groups (ASGs)

Scaling Options for Auto Scaling Groups

Lifecycle Hooks

AWS Auto Scaling

In Conclusion

Top 10 Big-Picture Discussion Points: Scale, Availability, and

Table of Contents

Monitoring Decisions

6 Cloud Storage

Cloud Storage

Which Storage Matches Your Workload?

EBS Block Storage

EBS Volume Types

General-Purpose SSD (gp2)

Elastic EBS Volumes

Attaching an EBS Volume

EBS Volume Encryption

EBS Snapshots

Tagging EBS Volumes and Snapshots

EBS Best Practices

S3 Storage

Buckets, Objects, and Keys

S3 Data Consistency

S3 Storage Classes

S3 Management

Versioning

S3 Bucket Security

Amazon S3 Glacier Archive Storage

S3 Glacier Vaults and Archives

Shared File Systems at AWS

Elastic File System (EFS)

EFS Performance Modes

EFS Throughput Modes

EFS Security

Storage Performance Compared

Table of Contents

Amazon FSx for Windows File Server

Relational Database Service (RDS)

- RDS Database Instances

- High Availability for RDS

Big-Picture RDS Installation Steps

- Monitoring Database Performance

- Best Practices for RDS

Aurora

- Aurora Storage

- Communicating with Aurora

DynamoDB

- Database Design 101

DynamoDB Tables

- Provisioning Table Capacity

- Adaptive Capacity

- Data Consistency

- ACID and DynamoDB

- Global Tables

- DynamoDB Accelerator (DAX)

- Backup and Restore

ElastiCache

AWS Data Transfer Options

The Snow Family

AWS Storage Gateway Family

In Conclusion

Top 10 Big-Picture Discussion Points: Storage Options and
Considerations

7 Security Services

Table of Contents

Identity and Access Management

- IAM Policy Defined
- IAM Authentication
- Requesting Access to AWS Resources
- The Authorization Process
- Actions

IAM Users

- The Root User
- The IAM User

Creating an IAM User

- IAM User Access keys
- IAM Groups
- Signing In as an IAM User
- IAM Account Details
- IAM User Account Summary
- Creating a Password Policy
- Rotating Access Keys

Using Multifactor Authentication (MFA)

IAM Policy Types

- Identity-Based Policies
- Resource-Based Policies
- In-Line Policies

IAM Policy Creation

- Policy Elements

Reading a Simple JSON Policy

Policy Actions

- Additional Policy Control Options

Reviewing the Policy Permissions Applied

Table of Contents

IAM Policy Versions

Using Conditional Elements

Using Tags with IAM Identities

IAM Roles

When to Use Roles

Cross-Account Access to AWS Resources

The AWS Security Token Service (STS)

Identity Federation

IAM Best Practices

IAM Security Tools

Creating a CloudWatch Trail Event

Other AWS Security Services

AWS Organizations

Resource Access Manager (AWS RAM)

Secrets Manager

GuardDuty

AWS Inspector

In Conclusion

Top 10 Big-Picture Discussion Points

8 Automating AWS Infrastructure

Automating with AWS

From Manual to Automated Infrastructure with CloudFormation

CloudFormation Components

CloudFormation Templates

Stacks

Creating an EC2 Instance with EIP

Updating with Change Sets

Table of Contents

Working with CloudFormation Stack Sets

AWS Service Catalog

The 12-Factor Methodology

Rule 1. CodebaseOne Codebase That Is Tracked with Version Control
Allows Many Deploys

AWS CodeCommit

Rule 2. DependenciesExplicitly Declare and Isolate Dependencies

Rule 3. ConfigStore Config in the Environment

Rule 4. Backing ServicesTreat Backing Services as Attached Resources

Rule 5. Build, Release, RunSeparate, Build, and Run Stages

Rule 6. ProcessExecute the App as One or More Stateless Processes

Rule 7. Port BindingExport Services via Port Binding

Rule 8. ConcurrencyScale Out via the Process Model

Rule 9. DisposabilityMaximize Robustness with Fast Startup and
Graceful Shutdown

Rule 10. Dev/Prod ParityKeep Development, Staging, and Production as
Similar as Possible

Rule 11. LogsTreat Logs as Event Streams

Rule 12. Admin ProcessesRun Admin/Management Tasks as One-Off
Processes

Elastic Beanstalk

Updating Elastic Beanstalk Applications

CodePipeline

AWS CodeDeploy

Serviceless Computing with Lambda

API Gateway

Building a Serverless Web App

Create a Static Website

User Authentication

Table of Contents

Serverless Back-End Components

Set Up the API Gateway

In Conclusion

Top 10 Big-Picture Discussion Points: Moving Toward Stateless
Design

Index