AWS Cloud Automation

In-depth guide to automation using Terraform infrastructure as code solutions

Oluyemi James Odeyinka

www.bpbonline.com

First published: 2024

Published by BPB Online
WeWork
119 Marylebone Road
London NW1 5PU

UK | UAE | INDIA | SINGAPORE

ISBN 978-93-55516-534

www.bpbonline.com

Dedicated to

My beloved wife,

Memunat

&

My daughter ***Ayobola*** *& my son* ***Damola***

About the Author

Oluyemi James Odeyinka has over a decade of experience serving as a cloud solution architect and cybersecurity leader. Throughout his career, he has played pivotal roles in numerous cloud projects, demonstrating both leadership and hands-on engineering expertise. His project delivery encompasses the deployment of resources for major companies, employing Infrastructure as Code methodologies. Notably, he has achieved success with high-profile projects in the United States.

Currently holding the position of Senior Solution Architect at Walgreens and serving as the Founder and President of Cloudall Technologies, Odeyinka is a multifaceted professional. His academic background includes the attainment of a postgraduate MBA degree in Analysis, coupled with in-depth knowledge of Agile Methods.

As an accomplished information technology leader, Odeyinka has amassed significant experience in Cyber Security, Hybrid Cloud, Product Management, Data Analytics, Governance, IoT, and Data Protection and Data Management. He has actively contributed to the field by authoring and leading numerous cloud and cybersecurity training sessions on a global scale.

A sought-after speaker, Odeyinka has addressed audiences at various conferences, such as IoT World in 2020 & 2021, Edge Computing 2021, Embedded Devices 2022, and the latest Infosec World 2022. His expertise is further solidified by his CISSP certification and proud membership in ISC2, a leading IT Security organization. In recognition of his substantial contributions to technical communities worldwide, he was also honored with the Outstanding Leadership Award at the 2022 Internet 2.0 Conference.

About the Reviewers

- **Divit Gupta**, a seasoned IT professional with 20 years of industry expertise, excels in driving strategic architecture initiatives and providing leadership in multi-pillar sales cycles. With a global impact, he spearheads technical partnerships, defines team vision, and champions new strategic endeavors.

  As the host of popular podcasts like 'Tech Talk with Divit,' 'Live Labs with Divit,' and 'Cloud Bites with Divit,' he showcases technological initiatives and leadership.

  In 2022-23, he served as Oracle TV's correspondent for Cloud World. A recognized expert, Divit presented on Oracle Database technology at Oracle Cloud World FY 2023.

  His passion for knowledge sharing extends to international conference talks, technical blogs, and multiple books on emerging technologies. Divit has been featured in several prominent newspapers and technology magazines worldwide.

  Holding over 40 certifications from Microsoft, Oracle, AWS, and Databricks, he remains at the forefront of technology.

- **Mariano Geuzi Karaian** is a seasoned technical delivery leader with expertise in Architecture, Networking, and Security, complemented by a deep passion for Cloud technologies. He leverages AWS and Azure to assist companies in migrating their technology stack to the cloud and developing cloud-native solutions, prioritizing automation, throughout the process. Additionally, he possesses experience in multi-cloud environments and is adept at formulating resilient multi-cloud strategies.

Acknowledgement

I wish to convey my heartfelt appreciation to my family for their constant support and encouragement during the creation of this book, with special mention to my wife, Memunat, and my two children, Ayobola, my daughter, and Damola, my son.

I want to also express my gratitude to BPB Publications for their invaluable guidance and expertise in the successful completion of this book. The process of revising the manuscript was a lengthy journey, enriched by the valuable contributions and collaborative efforts of reviewers, technical experts, and editors.

I would also want to express my gratitude for the significant contributions made by my colleagues and co-workers throughout the years in the tech industry. Their wealth of knowledge and constructive feedback have been instrumental in my professional growth.

Finally, I would like to express my gratitude to every reader who has shown interest in my book and supported its realization. Your encouragement has been immensely valuable.

Preface

In the relentless pursuit of technological advancement, the landscape of managing and deploying cloud infrastructure has undergone a profound transformation. This metamorphosis is not merely a shift in methodology but a revolution in the way we conceive, build, and maintain the digital foundations of our interconnected world.

As we stand on the precipice of a new era in computing, this book embarks on a journey into the heart of AWS IaC—a paradigm that transcends traditional boundaries and challenges the very fabric of conventional infrastructure management. In these pages, we will explore the profound impact of treating infrastructure not as a static set of hardware and software components but as dynamic, version-controlled code.

The genesis of this book lies in the realization that AWS IaC is not just a buzzword or a fleeting trend. It is a fundamental shift that empowers engineers, architects, and organizations to sculpt their digital landscapes with unprecedented precision and agility. Gone are the days of manual, error-prone configurations and the labyrinthine processes of provisioning and scaling infrastructure. In their place emerges a landscape where AWS infrastructure is expressed as code, a language understood by both machines and humans.

Our exploration will traverse the foundational principles of IaC, delving into the core philosophies that underpin its effectiveness. We will demystify the orchestration tools and platforms that breathe life into code, orchestrating intricate symphonies of servers, networks, and services with the precision of a maestro.

The chapters that follow are not just a compilation of technical insights but a narrative that unfolds the stories of pioneers who have harnessed the power of IaC to reshape industries, break barriers, and fuel innovation. From the streamlined efficiency of continuous delivery pipelines to the resilience of infrastructure that adapts to the ever-changing demands of modern applications, each page is a testament to the transformative potential that IaC holds.

As you embark on this journey, whether you are a seasoned AWS engineer seeking to deepen your understanding or a newcomer eager to grasp the AWS fundamentals, I invite you to immerse yourself in the philosophy, practices, and promises of Infrastructure as Code. Let this book be your guide through the intricate tapestry of AWS code-driven infrastructure, where the future unfolds with every line written and every deployment executed. May it inspire you to not only embrace the tools and techniques but to forge a

mindset that embraces change, values collaboration, and champions the evolution of our digital world.

Chapter 1: AWS DevOps and Automation Tools Set – This chapter explains the skills to set up AWS CLI, AWS CDK, AWS CloudFormation, and CodeCommit. Additionally, the reader will gain proficiency in configuring CodeBuild, CodeDeploy, CodePipeline, and CodeArtifact to automate AWS builds. Lastly, the reader will understand the process of creating an S3 Bucket using CloudFormation.

Chapter 2: AWS Terraform Setup – This chapter presents an introduction to Infrastructure as Code (IaC), elucidating its significance in contemporary software development and operations. It offers an overview of Terraform, highlighting its merits as an IaC tool. The chapter subsequently presents a detailed, step-by-step guide on initiating work with Terraform, encompassing aspects like installation, configuration, infrastructure deployment, and management. Furthermore, the chapter addresses common challenges and considerations inherent in the utilization of Terraform, including constraints, security aspects, and the scalability of infrastructure. By doing so, it aims to equip readers with a comprehensive understanding of both the advantages and potential pitfalls associated with implementing Terraform in the realm of Infrastructure as Code.

Chapter 3: IAM, Governance and Policies Administration – This chapter covers AWS Identity and Access Management (IAM), governance, and policy is presented to provide readers with essential knowledge and skills for proficiently overseeing access control, establishing a governance framework, and enforcing security measures within their AWS infrastructure. Readers will gain insight into the core elements of AWS IAM, such as users, groups, roles, and policies, and grasp the importance of governance in the AWS environment. The chapter guides readers in creating account structures and implementing Identity lifecycle management through Terraform Infrastructure as Code (IaC). This chapter introduces readers to the implementation of role-based access control (RBAC), adherence to least privilege principles, resource-level permissions, and the adoption of a zero-trust approach.

Chapter 4: Automating AWS Storage Deployment and Configuration – This chapter aims to offer a thorough insight into the automation of deployment and configuration processes for different Amazon storage services through the use of Terraform. Upon completing this chapter, readers will have acquired the expertise and hands-on proficiency required to define, provision, and oversee storage deployment in a streamlined and reliable manner using Terraform. The content of this chapter will provide readers with a comprehensive understanding of employing Terraform Infrastructure as Code (IaC) to deploy Amazon S3, EBS volumes, and EFS file systems. Practical examples and hands-on exercises will be

woven throughout the chapter, guiding readers in the practical application of Terraform for automating various AWS storage services.

Chapter 5: VPC and Network Security Tools Automation – This chapter explores the complex domain of AWS Virtual Private Cloud (VPC) to provide readers with a deep comprehension of its structure, elements, and functionalities. This chapter guide readers through the intricacies of automating the creation, setup, and administration of VPCs, enabling them to proficiently design isolated network environments, establish secure communication between resources, and seamlessly integrate with various AWS services. By demystifying the intricacies of VPC security, connectivity choices, and advanced configurations, it aims to cultivate expertise in leveraging the full potential of AWS VPC for crafting robust, scalable, and flexible cloud infrastructures.

Chapter 6: Automating EC2 Deployment of various Workloads – This chapter explore the domain of EC2 deployment automation using the robust infrastructure-as-code tool. Emphasizing efficiency and reproducibility, navigating through contemporary cloud deployment practices, illustrating how Terraform adeptly orchestrates the provisioning and management of Amazon EC2 instances. By the conclusion of this chapter, readers will acquire a comprehensive grasp of both the essential principles of Terraform and EC2, as well as the strategic approaches to automate and enhance their infrastructure deployment workflows. Through practical examples, best practices, and real-world insights, the chapter empower readers to leverage the capabilities of Terraform, enabling them to establish a sturdy foundation for deploying EC2 instances while embracing the agility and reliability that automation brings to cloud environments.

Chapter 7: Automating ELB Deployment and Configurations – This chapter explains Elastic Load Balancer (ELB) foundational service provided by Amazon Web Services (AWS), leading the way in load balancing solutions. Amazon ELB serves as a versatile tool, empowering developers and system administrators to efficiently distribute incoming traffic across multiple instances, ensuring seamless and dependable user experiences. As reader progress through this chapter, the reader will not only gain a solid understanding of Amazon ELB but also the confidence to design and deploy resilient, scalable, and fault-tolerant applications utilizing this potent AWS service.

Chapter 8: AWS Route53 Policy and Routing Automation – This chapter is dedicated to AWS Route 53 Policy and Routing Automation seeks to optimize and automate the management of domains and traffic routing within the Amazon Web Services (AWS) ecosystem. Its primary goal is to streamline domain name management, enabling efficient traffic routing and improved application performance. By employing automated policies, this service ensures that domain requests adhere to defined rules and conditions, directing

them to the appropriate resources. Furthermore, the reader learn how to use AWS Route 53 service to facilitates rapid failover and disaster recovery by automating the redirection of traffic away from unhealthy endpoints. This ensures uninterrupted service delivery and minimal downtime during system failures or maintenance activities. Ultimately, the goal is to provide a resilient and high-performance DNS management solution that contributes to an optimal end-user experience.

Chapter 9: AWS EKS and Fargate Deployments – This chapter is dedicated to Amazon Elastic Kubernetes Service (EKS) and AWS Fargate. It covers essential concepts, deployment strategies, and provides hands-on experience to equip readers with the knowledge and skills needed for efficient management of containerized applications in a cloud-native environment. AWS EKS, also known as Elastic Kubernetes Service, is a fully managed Kubernetes service designed to streamline the deployment, management, and scaling of containerized applications using Kubernetes on the Amazon Web Services platform. The key goal of AWS EKS is to furnish users with a dependable, highly available, and secure Kubernetes environment, facilitating seamless orchestration and management of containerized workloads. By eliminating the need for manual setup and management of Kubernetes clusters, EKS allows organizations to focus on their applications and business logic, with AWS handling the Kubernetes infrastructure.

Chapter 10: Databases and Backup Services Automation – This chapter this chapter is to explore the fundamental concepts underlying AWS database services, comprehending their distinctive features, applications, and advantages. Reader will learn how these services contribute to optimizing organizational data architecture, ensuring data integrity, achieving cost-effectiveness, and fostering innovation through insights derived from data. Furthermore, the chapter delves deeply into the intricacies of AWS Backup Services, a robust and versatile suite of tools crafted to ensure the resilience and recoverability of your invaluable data.

Chapter 11: Automating and Bootstrapping Monitoring Service – This chapter is dedicated to AWS Monitoring Service and reliability for applications and infrastructure hosted on the Amazon Web Services (AWS) platform. Monitoring plays a crucial role in proactively identifying and addressing issues, preventing potential downtimes, and improving overall operational efficiency. By continuously monitoring aspects such as resource utilization, application performance, and system health, the AWS Monitoring Service aims to provide actionable insights and data-driven decisions for efficient resource allocation and management. The monitoring tools and services within AWS enable organizations to analyze trends, forecast growth, and make informed decisions about resource provisioning. This ensures that applications and services can seamlessly handle increased workloads while maintaining optimal performance.

Code Bundle and Coloured Images

Please follow the link to download the
Code Bundle and the ***Coloured Images*** of the book:

https://rebrand.ly/8wyxaqf

The code bundle for the book is also hosted on GitHub at
https://github.com/bpbpublications/AWS-Cloud-Automation.
In case there's an update to the code, it will be updated on the existing GitHub repository.

We have code bundles from our rich catalogue of books and videos available at **https://github.com/bpbpublications**. Check them out!

Errata

We take immense pride in our work at BPB Publications and follow best practices to ensure the accuracy of our content to provide with an indulging reading experience to our subscribers. Our readers are our mirrors, and we use their inputs to reflect and improve upon human errors, if any, that may have occurred during the publishing processes involved. To let us maintain the quality and help us reach out to any readers who might be having difficulties due to any unforeseen errors, please write to us at :

errata@bpbonline.com

Your support, suggestions and feedbacks are highly appreciated by the BPB Publications' Family.

Piracy

If you come across any illegal copies of our works in any form on the internet, we would be grateful if you would provide us with the location address or website name. Please contact us at **business@bpbonline.com** with a link to the material.

If you are interested in becoming an author

If there is a topic that you have expertise in, and you are interested in either writing or contributing to a book, please visit **www.bpbonline.com**. We have worked with thousands of developers and tech professionals, just like you, to help them share their insights with the global tech community. You can make a general application, apply for a specific hot topic that we are recruiting an author for, or submit your own idea.

Reviews

Please leave a review. Once you have read and used this book, why not leave a review on the site that you purchased it from? Potential readers can then see and use your unbiased opinion to make purchase decisions. We at BPB can understand what you think about our products, and our authors can see your feedback on their book. Thank you!

For more information about BPB, please visit **www.bpbonline.com**.

Join our book's Discord space

Join the book's Discord Workspace for Latest updates, Offers, Tech happenings around the world, New Release and Sessions with the Authors:

https://discord.bpbonline.com

Table of Contents

Chapter 1
AWS DevOps and Automation Tools Set

Introduction

Amazon Web Services (AWS- **https://aws.amazon.com/what-is-aws/**) DevOps is a set of practices and tools that are used by AWS to automate and orchestrate the process of cloud infrastructure deployment and software development. DevOps stands for Development and Operations, and it is a software deployment and development methodology that combines the best practices of software development with the best practices of IT operations. The main purpose of DevOps is to improve the speed and quality of software delivery by creating a culture of collaboration between development teams and operations teams.

AWS provides a wide range of services and automation tools that are designed to help businesses automate various tasks, from deployment to monitoring and management. In the context of tools set, businesses can use automation tools like AWS CodeCommit, AWS CodePipeline, AWS CodeBuild, AWS OpsWorks, and AWS CodeDeploy. AWS CodeStart enables you to quickly develop, build, and deploy applications on AWS.

Finally, it should be noted that **Site Reliability Engineering (SRE)** is now replacing the operation part of DevOps. SRE is a methodology for managing large-scale software systems that prioritizes reliability, availability, and automation to reduce the risk of downtime or other issues.

Structure

In this chapter, we will go through the following topics:

- Overview of Amazon Web services automation tool set
- AWS CloudDevelopment Kit
- End-to-End view of AWS deployment tools

Objectives

In this chapter, you will learn how to setup AWS CLI, AWS CDK, AWS CloudFormation, and CodeCommit. You will also learn how to configure CodeBuild, CodeDeploy, CodePipeline, and Code Artifact for automating AWS builds. And lastly, you will learn how to create S3 Bucket using CloudFormation.

Overview of Amazon Web Services tool set

The emergence of digital economy has drastically changed how Companies deliver software. DevOps and Automation have championed the transformation journey, and there is no way to mention DevOps without mentioning its twin assistant, known as Automation, and vice versa. **Amazon Web Services** (**AWS**) has a wide range of automation tool sets, some of which can be easily adapted for **Infrastructure as Code** (**IaC**) while others are used for software development codes. This chapter introduces you to the tool set available within the AWS ecosystem, but before we look at this toolset in detail, let us understand what this toolset is primarily used to accomplish:

- **Deployments:** Includes pre-provisioning and post-provisioning definitions
- **Provisioning**: Includes definition of desired state settings and goals
- **Configuration**: Includes set of standards in parameterized format
- **Orchestration**: Zero-touch deployment or zero-manual intervention from users

The principle behind IaC is to treat infrastructure deployment the same way the developers treat software code. The list of AWS tools set below will be used to make our automation journey effective, smoother, and efficient to deliver enterprise-grade IaC and software automation.

Lists of AWS automation tool set

Following is the list of AWS automation tool set:

- AWS CodeCommit
- AWS CodeBuild

- AWS CodeArtifact
- AWS Code Deploy
- AWS CodeStar
- AWS CodePipeline
- AWS CloudFormation
- **AWS Cloud Development Kit (AWS CDK)**
- AWS Cloud Development Kit for Kubernetes
- AWS Device Farm

Before we dive into the details of the toolset and its configuration, let us divide the above list into three segments with details.

Infrastructure as code

AWS **`CodeCommit`** is a private or managed GitHub version of AWS; it is a private source control service within AWS eco-system that hosts your git repositories. **`CodeCommit`** allows you to host your IaC code within AWS services. You can still use GitHub with **`CodeCommit`** if you choose to, you can migrate your existing code to **`CodeCommit`**, and you can still collaborate with developers across the globe.

How to setup CodeCommit repository

AWS CodeCommit can be setup through AWS Management Console or AWS CLI, we are going to use AWS CLI to setup our repository and Open CMD if you are using Windows or Terminal if you are using Linux or MAC OS.

TIP: It is assumed you already have AWS Account, you already installed GIT, AWS CLI, and you already configured AWS CLI to connect to your AWS Account with the existing IAM user. Please use this link if you need help setting up CodeCommit https://docs.aws.amazon.com/codecommit/latest/userguide/setting-up.html.

AWS CloudFormation

Follow these steps:

1. Check **`CodeCommit`** help feature:

   ```
   Policy $ aws codecommit help
   ```

   If everything is setup right, you should get the following output:

   ```
       codecommit
   ^^^^^^^^^^
   ```

```
Description
***********
This is the *AWS CodeCommit API Reference* . This reference provides
descriptions of the operations and data types for AWS CodeCommit API
along with usage examples.
```

You can use the AWS CodeCommit API to work with the following objects.

2. Create your first **CodeCommit** repository:

```
$ aws codecommit create-repository --repository-name awsca-chapter1-
repo --repository-description "This is chapter1 demo repo"
```

3. Verify the repository that was actually created:

```
$ aws codecommit list-repositories
```

Output:

```
        {
    "repositories": [
        {
            "repositoryName": "aws-cloud-automation",
            "repositoryId": "dbd5e1f2-860e-4c32-9f4d-7a56229730fa"
        }
    ]
}
```

4. Now clone the repository you just created:

```
$ git clone https://git-codecommit.us-east-2.amazonaws.com/v1/repos/
awsca-chapter1-repo
```

5. Now check your cloned repository:

```
ls
```

Output:

```
awsca-chapter1-repo/
```

You have now finished setting up your CodeCommit repository, we will use this repo later to hold all **chapter1** codes including our CLI commands we have used so far.

AWS CloudFormation is a service that provides developers and system administrator an automated way to create, deploy, provision, and manage AWS cloud resources in a consistent and predictable manner. CloudFormation templates are written in JSON or YAML to describe the standard of AWS stack.

AWS CloudFormation template anatomy

Following is the AWS CloudFormation template anatomy:

- Template Format Version
- Description
- Metadata
- Parameters
- Mappings
- Conditions
- Transform
- Resources
- Outputs

AWS CloudFormation which is used to create a new **`CodeCommit`**:

```
AWSTemplateFormatVersion: "2010-09-09"
Description: "This is codecommit repository created with cloud formation"
Resources:
  CodeCommitRepository:
    Type: "AWS::CodeCommit::Repository"
    Properties:
      RepositoryName: "awsca-chapter1-cloudFormation-repo"
Parameters: {}
Metadata: {}
Conditions: {}
```

Verify if the repository was created:

```
$ aws codecommit list-repositories
{
    "repositories": [
        {
            "repositoryName": "aws-cloud-automation",
            "repositoryId": "dbd5e1f2-860e-4c32-9f4d-7a56229730fa"
        }
    ]
}
```