AWS All-in-One Security Guide

Design, Build, Monitor, and Manage a Fortified Application Ecosystem on AWS

Adrin Mukherjee

www.bpbonline.com

FIRST EDITION 2022

ISBN: 978-93-55510-327

LIMITS OF LIABILITY AND DISCLAIMER OF WARRANTY

The information contained in this book is true to correct and the best of author's and publisher's knowledge. The author has made every effort to ensure the accuracy of these publications, but publisher cannot be held responsible for any loss or damage arising from any information in this book.

All trademarks referred to in the book are acknowledged as properties of their respective owners but BPB Publications cannot guarantee the accuracy of this information.

Distributors:

BPB PUBLICATIONS
20, Ansari Road, Darya Ganj
New Delhi-110002
Ph: 23254990/23254991

DECCAN AGENCIES
4-3-329, Bank Street,
Hyderabad-500195
Ph: 24756967/24756400

MICRO MEDIA
Shop No. 5, Mahendra Chambers,
150 DN Rd. Next to Capital Cinema,
V.T. (C.S.T.) Station, MUMBAI-400 001
Ph: 22078296/22078297

BPB BOOK CENTRE
376 Old Lajpat Rai Market,
Delhi-110006
Ph: 23861747

Published by Manish Jain for BPB Publications, 20 Ansari Road, Darya Ganj, New Delhi-110002 and Printed by him at Repro India Ltd, Mumbai

In loving memory of

Anindya Kanti Roy

- a maverick philosopher, mentor, and techie.

About the Author

Adrin Mukherjee is an experienced solutions architect who has taken up several challenging roles throughout his career, building distributed applications and high-performance systems. He enjoys helping customers in their digital transformation journeys, especially migrating applications to the cloud and creating highly scalable, secure, and resilient cloud-native platforms.

He is a certified AWS and Google Cloud solutions architect and security engineer. His interests include serverless computing, containerization, cloud security, and machine learning.

When not dabbling at the keyboard, he loves to trek, listens to hard rock, and enjoys spending time with his family.

LinkedIn: **https://www.linkedin.com/in/adrinmukherjee**

Blog: **https://adrin-mukherjee.medium.com**

About the Reviewer

Javid Ur Rahman is a distinguished database product manager and enterprise solution architect and has been actively involved in productizing and promoting cross-ecosystem collaboration in the Cloud Infrastructure, Edge & Analytics Platform space for over half a decade. He's focused on research and development of blockchain-based database algorithm designs and cloud-native-run engine development.

In his current role, he's taken the Enterprise Architect role in Fourth Square Inc, US Based Product, and Consulting Firm to new geographies.

LinkedIn: **https://www.linkedin.com/in/jrahaman7/**

Acknowledgement

First and foremost, thanks to my better half, Sakuntala, for giving me the initial nudge to take up this project and putting up with me while I was engrossed in writing this book over many weekends- I could not have finished this without her continuous support.

I am eternally grateful to my mother, who has been a pillar of strength and the one I have always turned for comfort during difficult times.

To my son Arik, who happens to be the source of my laughter and immense joy- I can't imagine a life without his childish pranks and exhibitions of newly acquired antics.

To Choco, my best friend and canine companion, who was equally enthusiastic and ignorant of my work- Thanks for keeping me company during the writing of this book, even in the ungodly hours.

My heartfelt gratitude towards my colleagues and friends who believed in me and have shown interest in my work. Special thanks to Binson Paul, Ratnadeep Bardhan Roy, Angshuman Mukherjee, Arijit Mazumdar and Animesh Das.

Finally, sincere thanks to the team at BPB Publications for providing me with this exciting opportunity of writing my first book for them.

Preface

With enterprises moving their workloads and assets to public clouds, securing application ecosystems and resources on multi-tenanted public cloud providers like Amazon Web Services (AWS) is a primary concern. In AWS, security is considered “job-zero” as such, the customers can leverage AWS’s highly secure global infrastructure and various infrastructure and abstract services. However, in the public cloud, the customers also have their share of responsibility towards securing applications and workloads.

The goal of this book is to provide in-depth information on various security-focused AWS services and features that can be leveraged to design and implement a fortified application ecosystem on AWS. The book takes a layered approach to security which introduces multiple security controls across the cloud environment. Each layer has to be secured independently with a chosen set of security controls and guardrails. This ensures that a gap or flaw in one layer can be countered by controls and measures in another layer. This book dedicates individual chapters to each such layer and introduces specific security measures and AWS services that can help to establish the necessary security fences.

In the course of seven chapters, the readers will learn the following:

Chapter 1 introduces the shared responsibility model of security on AWS and various service offerings that can help secure applications and workloads on AWS.

Chapter 2 discusses the fundamental service in AWS- Identity and Access Management (IAM). The chapter shows how to create IAM policies to secure AWS resources with the help of multiple examples. It also introduces the commonly used access management strategies like delegation and federation. Finally, the chapter explains various AWS tools available for easy creation, management, and governance of access policies.

Chapter 3 moves through the various AWS features, services, and strategies available to secure cloud infrastructure. These include security of Virtual Private Cloud, patch management for EC2 instances, privileged session management, etc. The chapter also covers Distributed Denial of Service (DDoS) attacks, mitigation steps and introduces AWS Shield- a managed service that can help fight such attacks.

Chapter 4 is related to the security of data in the AWS cloud. The chapter introduces AWS Key Management Service (KMS) and AWS CloudHSM, which are at the core of data protection on AWS. It also visits the data security features of popular services like S3, EBS, DynamoDB, and RDS. Lastly, it introduces Amazon Macie, a fully managed service for data loss prevention.

Chapter 5 focuses on how AWS can help in securing the application layer. The chapter takes a deeper look into securing APIs deployed on AWS API Gateway, leveraging Amazon Cognito to design authentication and authorization schemes, securing web applications hosted on Amazon S3 and Amazon CloudFront, etc. The chapter emphasizes using AWS Secrets Manager and AWS Systems Manager-Parameter Store services to externalize various application-level secrets and configuration parameters. It also takes a closer look at using AWS Web Application Firewall (WAF) to safeguard applications from Layer-7 attacks and how appropriate use of Elastic Load Balancers (ELBs) can go a long way in securing applications deployed on AWS.

Chapter 6 focuses on essential logging, monitoring, and auditing services like Amazon CloudWatch, AWS CloudTrail, AWS Config, etc. The chapter briefly introduces advanced monitoring services like Amazon GuardDuty, AWS Security Hub, Amazon Detective, etc.

Chapter 7 is all about security best practices recommended to be followed in the AWS cloud to improve the security posture of the application ecosystem. The best practices have been grouped into the following layers- IAM, infrastructure, data, application, logging, and monitoring.

Code Bundle and Coloured Images

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

https://rebrand.ly/db7792

The code bundle for the book is also hosted on GitHub at **https://github.com/bpbpublications/AWS-All-in-One-Security-Guide**. 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.

Table of Contents

CHAPTER 1
Introduction to Security in AWS

Introduction

As the enterprises and businesses move their workloads into the public cloud, security has become the most talked about subject in cloud migration and cloud adoption journeys. Design for security is pervasive throughout the Amazon's infrastructure and is built into every service offered by **Amazon Web Services** (**AWS**). However, security on the public cloud is different in many respects from security on-premises, and thus, it must be seen from different angles. As such, there is a shared responsibility model of security on the AWS cloud. While AWS is responsible for the "Security of the cloud", the customers are responsible for the "*Security in the cloud*."

Structure

In this chapter, we will cover the following topics:

- Shared responsibility model
- Important AWS security service offerings
- Security guidance offered by AWS
- Quick note on AWS Management Console

Objectives

In this chapter, we will gather the basic understanding of the security in the AWS cloud, which primarily revolves around the concept of the shared responsibility model. We will also identify some of the critical AWS security service offerings. We will cover some security guidance tools, documentation, and other resources that are provided by AWS and **AWS Partner Network** (**APN**) partners. These can help us create highly secure and resilient workloads and applications hosted on the AWS cloud.

Shared responsibility model

Security of the workloads and applications on the AWS cloud is a shared responsibility. This responsibility is shared between AWS and the customer. AWS is responsible for securing the global infrastructure and hardware that supports the cloud. The customer, on the other hand, is responsible for anything that they put on the cloud. This model can essentially improve the security posture of the customer and increase operational efficiency. The key goal is to create highly secure and resilient applications and workloads on the AWS cloud. *Figure 1.1* explains the responsibilities shared by AWS and customers as follows:

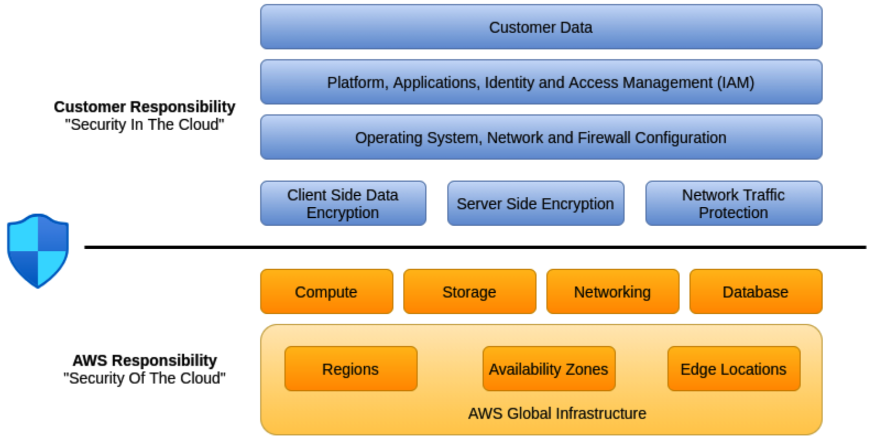

Figure 1.1: *Shared responsibility in AWS cloud*

In the subsequent sections, we will dive deeper into understanding the responsibilities pertaining to each player.

Security of the cloud – AWS responsibility

AWS is responsible for protecting the global infrastructure that runs all the services offered in the AWS Cloud. This infrastructure is composed of hardware, software, networking, and facilities/data centers that run the AWS Cloud services. Securing this infrastructure is AWS's utmost priority, and as such, the infrastructure undergoes regular audits to meet the required security and compliance standards. These audit reports are made available to the AWS customers digitally. AWS is also responsible for the security of the basic essential infrastructure services like compute, storage, networking, and database (managed database services like Amazon RDS or Amazon DynamoDB, etc.).

The *figure 1.2* provides an overview of AWS's slice pertaining to the shared responsibility model as follows:

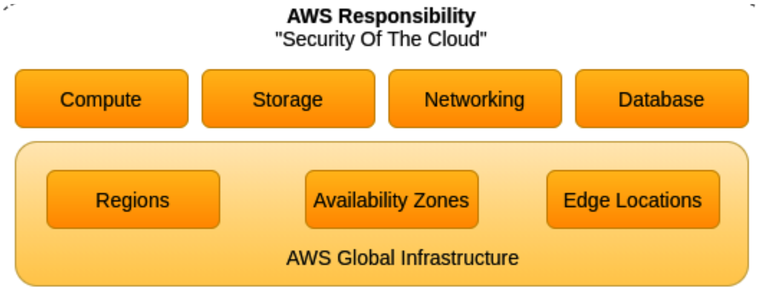

Figure 1.2: *Security of the cloud*

For pure infrastructure services like Amazon EC2, Amazon EBS, Amazon VPC, etc., AWS is responsible for the security of the underlying global infrastructure and the other infrastructure-related services, including the hypervisor layer (wherever applicable).

For the managed or abstracted services like Amazon RDS, Amazon DynamoDB, Amazon S3, in addition to the security of the infrastructure and related infrastructure services, AWS also handles the fundamental security tasks like guest OS patching, database patching, firewall configurations, and disaster recovery.

Security in the cloud – customer responsibility

Customer responsibility is determined by the AWS Cloud services that a customer uses. The AWS services that fall clearly into the category of **Infrastructure-as-a-Service** (**IaaS**) – such as Amazon EC2, Amazon VPC, etc. – are entirely under the customer's control, and the customers are expected to perform all of the necessary security configuration and management tasks. For example, for Amazon EC2 instances, the customer is responsible for the guest OS updates and patches, any application software or utilities installed on these instances, and the configuration of AWS firewall (called **security groups**) on each instance.

In the case of managed or abstracted services like Amazon S3, Amazon DynamoDB, or Amazon RDS, the customer is relieved of the burden of launching and maintaining the underlying instances, patching the guest OS or database, etc. AWS handles the infrastructure layer, operating system, and the platforms on behalf of the customer.

However, the customer still needs to access the service endpoints to store and retrieve the data, setup necessary permissions, and access control policies, etc. The customer also needs to decide on the classification of the data and security of the data at rest and in motion and apply the appropriate encryption options. Auditing and tracking of the API/user activity need to be performed by the customer.

The *figure 1.3* gives the basic set of responsibilities that needs to be managed by the customers who have deployed their applications and workloads on the AWS cloud as follows:

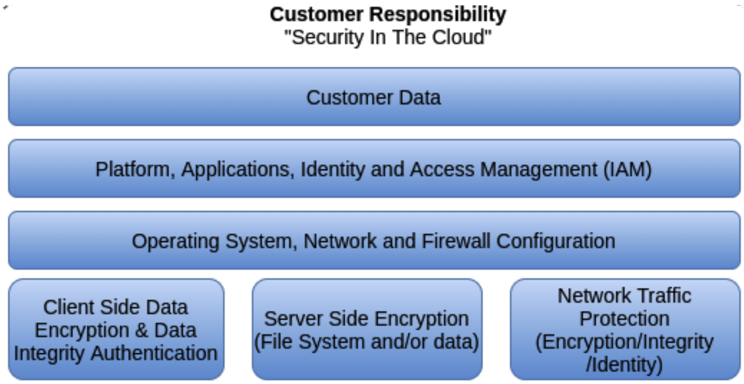
Customer Responsibility
"Security In The Cloud"
Customer Data
Platform, Applications, Identity and Access Management (IAM)
Operating System, Network and Firewall Configuration
Client Side Data Encryption & Data Integrity Authentication
Server Side Encryption (File System and/or data)
Network Traffic Protection (Encryption/Integrity /Identity)

Figure 1.3: *Security in the cloud*

Controls in shared responsibility model

In this section, we will look into "who is responsible for what" in the context of Shared Responsibility Model and IT controls in the AWS cloud. The IT controls can be differentiated into the following three categories:

Inherited controls

These controls are inherited by the customers from AWS. Some examples are as follows:

- **Physical and environmental controls**: This includes the physical access to the AWS facilities and involves various strict and controlled access to the facilities, professional security staff at ingress points, video surveillance, intrusion detection systems, multi-factor authentication, decommissioning physical storage devices, etc. The environmental controls like fire detection and suppression, power, climate, and temperature controls also fall under this category.

- **Controls For Business Continuity Management**: The AWS data centers are always built in clusters in various geographical regions to offer greater availability. The core applications are load-balanced and deployed in the N+1 configurations, so that the architecture can handle the data center failures. **Availability Zones** (**AZs**) are engineered to be physically separated within a metropolitan region and are located in the lower-risk flood plains. To reduce the single point of failure, in addition to the **uninterruptable power supply** (**UPS**) and the on-site backup generation facilities, AZs are also fed via different power grids from the independent sources.

- **Network Security Controls**: AWS has state-of-the-art, high bandwidth, fault-tolerant network infrastructure that is strictly monitored and managed. The boundary devices and other network devices manage the rulesets and traffic flow policies that are approved by Amazon Information Security. AWS has a limited number of access points to the cloud placed strategically that offer comprehensive ingress and egress traffic monitoring. These are called API endpoints, and they allow the HTTPS traffic only.

Shared controls

These controls apply to both the infrastructure and the customer layers. Here, AWS provides the requirements specific to the infrastructure, and the customers provide their own implementation of the controls within the context of their use of the AWS services. Some common examples are as follows:

- **Patch management**: AWS is responsible for patching and fixing the issues within the infrastructure, including network, hypervisor, host OS, etc. The customers are responsible for patching their guest OS and applications hosted on top of the infrastructure. AWS does provide services like AWS Systems Manager-Patch Manager that can be used by the customers to facilitate the patching process.

- **Configuration management**: AWS maintains and manages the configuration of its infrastructure devices, and the customers are responsible for configuring their own guest OS, databases, and applications.

- **Awareness and training**: While AWS train the AWS employees with the knowledge about the security controls in place, the customers are responsible for training and educating the internal cloud employees.

Fully controlled by the customer

These controls are solely the responsibility of the customers, based on the nature of the workload or the application deployed within the AWS services. Here's an example:

- **Service and communications protection/zone security:** The customers may require routing or zoning the data within the specific security environments.

Important AWS security service offerings

AWS has a plethora of related security services which can help the customer to create a highly secured platform or application on the AWS cloud. The following section provides with the introductory notes on some of the essential and vital services that can be leveraged.

AWS Identity and Access Management (IAM)

AWS Identity and Access Management (**IAM**) enables the customers to control and manage the access to the AWS services and resources securely. AWS IAM can be leveraged to create the human identities and/or machine identities and provide the fine-grained permission and access control to these identities. It supports the complex conditions to control the access, like originating IP address, whether SSL is used, or whether the user has been authenticated with Multi-Factor Authentication (MFA) device, etc. AWS IAM also helps to integrate the users with the existing corporate identity providers, like Microsoft Active Directory, or with the web identity providers, like Google, Facebook, etc., through Identity Federation.

Amazon Virtual Private Cloud (VPC)

Amazon Virtual Private Cloud, or VPC for short, is a foundational regional service that allows us to launch or instantiate the AWS resources in a logically isolated virtual network that we define. A VPC is a **software-defined network** (**SDN**) optimized for moving massive amounts of network packets from the source to the destination. It gives us complete control over the virtual networking environment which includes, selection of the IP ranges (or classless inter-domain routing/CIDR ranges), creation of the subnets, configuration of the route tables, network gateways (like Internet Gateways), etc. Support for both the IPv4 and the IPv6 is available for most resources in the VPC. Amazon VPC supports multiple layers of security that includes security groups and **Network Access Control Lists** (**NACLs**). In essence, VPC is our own chunk of AWS cloud that creates a network fabric, abstracting the inherent complexities of the routers, switches, and other networking devices.

VPC Flow Logs

VPC Flow Logs is a feature that enables us to capture information about the IP traffic going to and from the network interfaces in the VPC. Flow log data can be published to the Amazon CloudWatch Logs or Amazon S3. VPC Flow Logs can be enabled at the VPC level, subnet level, or network interface level.

Amazon CloudWatch

Amazon CloudWatch is the primary logging and monitoring service available in the AWS service arsenal. CloudWatch collects the monitoring and operational data from the AWS resources, applications, and services in the form of logs, metrics, and events, thereby providing a unified view with actionable insights.

AWS CloudTrail

AWS CloudTrail helps with the governance, compliance, and operational/risk auditing of the AWS accounts. Actions taken by a user, role, or an AWS service are recorded as events in CloudTrail. The events include actions taken in the AWS Management Console, AWS Command Line Interface, and AWS SDKs and APIs. This event history helps in the compliance auditing, operational analysis, security analysis, resource change tracking, and other troubleshooting.

AWS Config

AWS Config is a regional service that helps us to continuously keep track of the configuration changes made to the AWS resources. We can evaluate and audit the recorded configurations against the desired state of the resources, thereby simplifying the compliance auditing, security/forensic analysis, change management, operational troubleshooting, and enterprise-wide compliance monitoring. As part of the tracking, AWS Config sends the updated configuration details to a specified Amazon S3 bucket. For each resource type that AWS Config records, it sends a configuration history file (in JSON format) every six hours. Each configuration history file contains the details about the resources that changed in that period of six hours. AWS Config can also deliver the configuration snapshots to an Amazon S3 bucket, on demand. AWS Config can also be configured to send the configuration change notifications to a specified Amazon Simple Notification Service (SNS) topic. AWS Config supports several resource types.

Amazon Inspector

Amazon Inspector is an automated security assessment service. It can perform the assessments based on the pre-defined templates and produce a detailed list of security findings that are prioritized by severity. Amazon Inspector primarily supports two types of assessments – host assessment and network assessment. For the host assessment, an agent, also known as inspector agent, is required to be installed in the EC2 instances (also known as **assessment targets**). However, for the network assessment, an inspector agent is optional. The following pre-defined assessment templates are supported:

- Common Vulnerabilities and Exposures (CVE)

- CIS Operating System Security Configuration Benchmarks
- Network Reachability
- Security Best Practices

Amazon GuardDuty

Amazon GuardDuty is an intelligent threat detection service that can continuously monitor for malicious activity and unauthorized behavior to protect the AWS accounts and workloads. The service uses machine learning, anomaly detection, and integrated threat intelligence to identify the potential threats. GuardDuty can detect activities like crypto-currency mining, credential compromise behavior, unauthorized and unusual data access, API calls from known malicious IPs, etc. GuardDuty actively monitors the following three types of resources and can generate comprehensive findings along with severities:

- CloudTrail events
- VPC Flow Logs
- Route53 DNS Logs

AWS Shield

AWS Shield is a managed service for protection against the **Open Systems Interconnection** (**OSI**) layers 3 & 4 and **Distributed Denial of Service** (**DDoS**) attacks. AWS Shield provides the always-on detection and automatic inline mitigation that essentially minimize the application downtime and latency due to the DDoS attacks. There are two tiers of AWS Shield service, which are as follows:

- The **standard tier** provides protection against the most common network and transport layer DDoS attacks.
- The **advanced tier** protects against the large and sophisticated DDoS attacks with near real-time visibility. It also provides 24x7 access to AWS **DDoS Response Team** (**DRT**) and cost protection. The cost protection is provided by AWS in terms of credits to services like Amazon Route53, **Elastic Load Balancer** (**ELB**), Amazon CloudFront, etc.

AWS WAF

AWS WAF is a web application firewall that helps protect the web applications and/or APIs against the common OSI layer-7 attacks like SQL injection, **Cross-Site Scripting** (**XSS**), etc., by filtering out the malicious traffic patterns using managed rules. These managed rules can be used to address well-known issues like **Open Web Application Security Project** (**OWASP**) Top 10 security risks. AWS WAF can be deployed on the following AWS services:

- Amazon CloudFront
- Application Load Balancer
- Amazon API Gateway (to protect RESTful APIs)
- AWS AppSync (to protect GraphQL APIs)

Amazon Macie

Amazon Macie is a fully managed, Machine Learning powered, sensitive data discovery and classification service that helps to implement the Data Loss Prevention (DLP) solutions. It can continuously evaluate the Amazon S3 environment, which includes buckets, bucket contents, and relevant access controls, and can automatically discover and classify sensitive data like **personally identifiable information** (**PII**). It can additionally generate findings that could be sent to CloudWatch Events for further action and remediation.

AWS Security Hub

AWS Security Hub is a regional service that provides a comprehensive and aggregated view of the high-priority security alerts and compliance status across multiple AWS accounts, thus, providing a single source of truth for the security audits. AWS Security Hub can aggregate, organize, and prioritize the security findings from multiple AWS Services. The following services are supported out-of-the-box:

- Amazon GuardDuty
- Amazon Macie
- Amazon Inspector
- AWS Systems Manager
- AWS Firewall Manager
- AWS IAM Access Analyzer

AWS Security Hub also provides integrations with other third-party security solution providers like AlertLogic, Twistlock, Symantec, Barracuda, etc. AWS Security Hub can significantly improve the security posture with aggregated findings and automated checks.

AWS Key Management Service (KMS)

AWS Key Management Service (**KMS**) is a fully managed service that helps to create and manage the cryptographic keys. AWS KMS is highly secure and resilient, and leverages **hardware security modules** (**HSM**) to protect the keys. It provides centralized key management and helps to define the consistent policies around the ownership and access of the keys.

AWS Secrets Manager

AWS Secrets Manager is a fully managed service that can securely store and manage the lifecycle of the secrets like database credentials, API-keys, security tokens, etc. AWS Secrets Manager supports the versioning of these sensitive pieces of information and could be used for rotating these secrets as well. Essentially, AWS Secrets Manager can help the application developers to eliminate the need to hardcode sensitive information in the code or configuration files.

AWS Systems Manager

AWS Systems Manager is a suite of services that gives better visibility and control over our infrastructure on AWS. It supports the grouping of resources like Amazon EC2 instances, Amazon S3 buckets, Amazon RDS instances, etc., by application. Some of the crucial services under AWS Systems Manager are as follows:

- **Parameter Store** is a centralized store to manage the application configuration data. It can also act as a cost-effective alternative to AWS Secrets Manager for storing the secrets in the form of **`SecureString`**, provided automatic rotation requirements are not being considered for such secrets.
- **Sessions Manager** helps to start a session on the EC2 instance with an SSM agent installed and get access into the instance from the browser-based shell (and execute shell commands) or through AWS CLI without having to explicitly open any inbound SSH port (22) or setup any VPN.
- **Patch Manager** automates the process of patching managed instances. It can be used to scan for missing patches using the Patch baseline service.

AWS Artifact

AWS Artifact is the central resource for compliance-related information on AWS. It gives on-demand access to AWS security and compliance audit reports like **Payment Card Industry** (**PCI**) reports, **Service Organization Control** (**SOC**) reports, etc.

Security Guidance

AWS provides the customers with guidance and expertise through online tools, resources, support, and professional services provided by AWS and its partners. This guidance helps the customer to create and deploy the applications and manage the workloads following the AWS security best practices. Here is a list of some of the commonly used security guidance tools and resources.

AWS Trusted Advisor

AWS Trusted Advisor is an online tool that provides real-time guidance and helps us in provisioning the AWS resources following the AWS best practices. AWS Trusted Advisor analyzes the AWS environment and provides recommendations that fall under the following five distinct categories:

- Security
- Cost optimization
- Performance
- Fault tolerance
- Service limits

Under **`AWS Basic Support and Developer Support`**, we can get access to security checks like S3 bucket permissions that are open/insecure, improper IAM usage, **Multi-Factor Authentication** (**MFA**) on root account, public **Amazon Elastic Block Storage** (**EBS**), and **Amazon Relational Database Service** (**RDS**) snapshots. With AWS Business Support and AWS Enterprise Support, a lot more security checks can be accessed.

AWS Account Teams

Account Teams provide the first point of contact. This team can guide the customers through their deployments and implementations and point them to the right resources to resolve the security issues that they may encounter.

AWS Enterprise Support

AWS Enterprise Support provides a 15-minute response time and is available 24×7 over the phone, chat, or email, along with a dedicated Technical Account Manager. This is a concierge service that ensures that the customers' issues are addressed as quickly as possible.

AWS Partner Network

AWS Partner Network offers hundreds of industry-leading products that are equivalent, identical to, or integrated with the existing controls in your on-premises environments. These products complement the existing AWS services to enable you to deploy a comprehensive security architecture and a more seamless experience across your cloud and on-premises environments, as well as hundreds of certified AWS Consulting Partners worldwide to help with your security and compliance needs.

AWS Professional Services

AWS professional services has a security, risk, and compliance specialty practice to help the customers develop confidence and technical capability when migrating the sensitive workloads to the AWS Cloud. AWS Professional Services helps the customers develop security policies and practices based on the well-proven designs and helps ensure that the customers' security design meets the internal and external compliance requirements.

AWS Marketplace

AWS marketplace is a digital marketplace with thousands of software listings from the independent software vendors that make it easier to find, test, buy, and deploy the software that runs on AWS. AWS Marketplace Security products complement the existing AWS services to enable the customers to deploy a comprehensive security architecture and a more seamless experience across the cloud and on-premises environments.

AWS Security Bulletins

AWS security bulletins provide security bulletins around current vulnerabilities and threats and enables the customers to work with the AWS security experts to address various concerns like reporting abuse, vulnerabilities, and penetration testing.

AWS Security Documentation

AWS security documentation shows how to configure the AWS services to meet the security and compliance objectives. The AWS customers benefit from a data center and network architecture that are built to meet the requirements of the security-sensitive organizations. AWS provides a security blog with posts covering a wide range of security topics that include, but are not limited to, security best practices, advanced security patterns, threat modeling, data masking, etc.

Click on the following link to access the security blogs from AWS: https://aws.amazon.com/blogs/security/

AWS Well-Architected Framework

AWS Well-Architected Framework helps the cloud architects to build secure, high-performing, resilient, and efficient infrastructure for their applications. The framework includes a security pillar that focuses on protecting the information and systems. The customers can use the AWS Well-Architected Tool from the AWS Management Console or engage the services of one of the **AWS Partner Network (APN)** partners to assist them in conducting an automated review of the security posture of their AWS hosted applications and workloads.

AWS Well-architected Tool

AWS well-architected tool helps the customers to review the state of their workloads and compares them to the latest AWS architectural best practices. This is a free tool and is available in the AWS Management Console. The customers are required to answer a set of questions regarding the operational excellence, security, reliability, performance efficiency, and cost optimization. The AWS well-architected tool then provides a plan on how to architect for the cloud using the established best practices.

Quick Note on AWS Management Console

There are quite a few ways to interact with the AWS services and resources. AWS Management Console, AWS **Command Line Interface** (**CLI**), and AWS **Software Development Kit** (**SDK**) are the commonly used options. Throughout this book, we will use AWS Management Console and AWS CLI interchangeably to work with the AWS services and their features.

AWS Management Console is a friendly web-based portal to search and configure the AWS services, build new cloud-based applications, manage AWS account, and much more. Once an AWS account has been created and we have successfully logged in, the easiest way to explore all the available AWS services is to click on the **`Services`** menu on the top-left corner of the landing page, as shown in *figure 1.4* as follows:

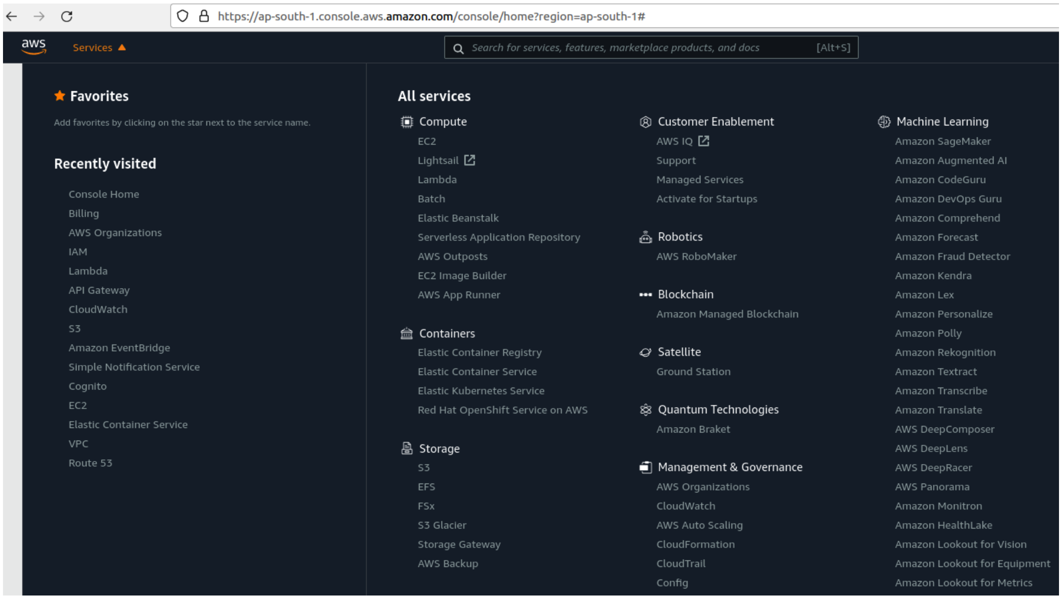

Figure 1.4: *Exploring AWS services from AWS Management Console*