Module 6

AWS Identity and Access Management (IAM)

With IAM, you can manage access to AWS services and resources securely. IAM enables you to configure access based on your company’s specific operational and security needs. IAM users are identities that you create in AWS, representing the person or application that interacts with AWS services and resources. IAM policies are documents that allow or deny permissions to AWS services and resources. IAM groups are collections of IAM users, and you can assign IAM policies to groups to grant permissions.

IAM users:

An IAM user is an identity that you create in AWS. It represents the person or application that interacts with AWS services and resources. It consist of a name and credentials.

IAM policies:

An IAM policy is document that allows or denies permissions to AWS services and resources.

IAM groups:

An IAM groups is a collection of IAM users. When you assign an IAM policy to a group, all users in the group are granted permissions specified by the policy.

Multi factor authentication:

In IAM multi-factor authentication provides an extra layer of security for your AWS account.

AWS Organizations:

We use AWS organizations to consolidate and manage multiple AWS accounts within a central location.

AWS Artifact:

It is a service that provides on-demand access to AWS security and compliance reports and select online agreements.

AWS artifact consists of two main sections: AWS artifact agreements and AWS artifact reports

AWS Artifact Agreements:

In AWS Artifact agreements, you can review, accept and manage agreements for an individual account and for all your accounts in AWS organizations.

Different types of agreements are offered to address that needs of customers who are subject to specific regulations

AWS Artifact Reports:

AWS Artifact Reports provide compliance reports from third-party auditors. These auditors have tested and verified that AWS is compliant with a variety of global, regional, and industry-specific security standards and regulations.

Customer Compliance Center:

It contains resources to help you learn more about AWS compliance.

In the Customer Compliance Center, you can read customer compliance stories to discover how companies in regulated industries have solved various compliance, governance, and audit challenges.

Denial-of-service attacks:

A Denial of service attacks is a deliberate attempt to make a website or application unavailable to users.

AWS Shield:

It is a service that protects applications against DDoS attacks. It provides two level of protection: Standard and Advanced

AWS Shield Standard:

AWS Shield Standard automatically protects all AWS customers at no cost. It protects your AWS resources from the most common, frequently occuring types of DDoS attacks.

It uses a variety of analysis techniques to detect malicious traffic in real time and automatically mitigates it.

AWS Shield Advanced:

It is a paid service that provides detailed attack diagnostics and the ability to detect and mitigate sophisticated DDoS attacks.

AWS WAF

It is a web application firewall that lets you monitor network requests that come into your web applications.

WS WAF works together with Amazon CloudFront and an Application Load Balancer. Recall the network access control lists that you learned about in an earlier module. AWS WAF works in a similar way to block or allow traffic.

Amazon Guard Duty:

It is a service that provides intelligent threat detection for your AWS infrastructure and resources.

Amazon Inspector

Amazon Inspector helps to improve the security and compliance of applications by running automated security assessments. It identifies security issues and deviations from best practices, and provides recommendations on how to fix them.

AWS Key Management Service (KMS)

AWS KMS is a managed service that makes it easy for you to create and control the encryption keys used to encrypt your data. It integrates with other AWS services to protect your data at rest and in transit.

Security Threats on AWS

There are a variety of security threats that can impact your data on AWS, including denial-of-service attacks (DDoS), data breaches, and unauthorized access. AWS Shield is a service that protects applications against DDoS attacks with two levels of protection: Standard and Advanced. AWS WAF is a web application firewall that lets you monitor network requests that come into your web applications. Amazon GuardDuty is a service that provides intelligent threat detection for your AWS infrastructure and resources.

It is important to take steps to protect your data on AWS, including using strong passwords, encrypting data at rest and in transit, and monitoring for potential security threats. AWS provides a range of security options to help you protect your data and resources on the platform.

AWS CloudTrail:

AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. It provides a record of actions taken by a user, role, or an AWS service in AWS Management Console, AWS Command Line Interface (CLI), and AWS SDKs and APIs.

AWS Config:

AWS Config is a service that enables you to assess, audit, and evaluate the configuration of your AWS resources. It provides a detailed view of the configuration of AWS resources in your account.

AWS Security Hub:

AWS Security Hub is a service that provides a comprehensive view of your security alerts and compliance status across your AWS accounts. It provides automated compliance checks, security alerts, and security findings from various security services.

AWS Firewall Manager:

AWS Firewall Manager is a service that provides centralized management of AWS WAF rules across multiple AWS accounts and resources.

Amazon Macie:

Amazon Macie is a service that helps you discover, classify, and protect sensitive data in AWS. It uses machine learning to automatically discover and classify data stored in Amazon S3.

AWS Secrets Manager:

AWS Secrets Manager is a service that enables you to manage secrets, such as database credentials, API keys, and other sensitive data.

AWS Certificate Manager:

AWS Certificate Manager is a service that provides SSL/TLS certificates for your domain names. It simplifies the process of requesting, deploying, and managing SSL/TLS certificates.