AWS Cloud security checklist (Cloud Security)

By: Piyush Kumawat

Note: This document is not created by a professional content writer so any mistake and error is a part of great design

Disclaimer

This document is generated by VIEH Group and if there is any contribution or or credit, it's mentioned on the first page. The information provided herein is for educational purposes only and does not constitute legal or professional advice. While we have made every effort to ensure the accuracy and reliability of the information presented, VIEH Group disclaims any warranties or representations, express or implied, regarding the completeness, accuracy, or usefulness of this document. Any reliance you place on the information contained in this document is strictly at your own risk. VIEH Group shall not be liable for any damages arising from the use of or reliance on this document. also we highly appreciate the source person for this document.

Happy reading !

Content Credit: Piyush Kumawat (Securitycipher)

Introduction

Here, you can access a security checklist tailored for the AWS cloud environment. This checklist encompasses a wide range of services, including IAM (Identity and Access Management), EC2 (Elastic Compute Cloud), EBS (Elastic Blob Storage), ELBv2 (Elastic Load Balancer V2), VPC (Virtual Private Cloud), S3 (Simple Storage Service), RDS (Relational Database Service), and numerous others.

IAM (Identity and Access Management)

MFA is not enabled for Root Account — Ensure Multi-Factor Authentication (MFA) is enabled for the AWS root account.

MFA is not enabled for IAM Users — Ensure Multi-Factor Authentication (MFA) is enabled for all AWS IAM users with AWS Console access.

Multiple Access Keys exists for IAM Users — Detects when a canary token access key has been used

Cross-Account Access Lacks External ID and MFA — Ensure cross-account IAM roles use either MFA or external IDs to secure the access to AWS resources.

Lack of Access Key Rotation — Ensure AWS IAM access keys are rotated on a periodic basis as a security best practice (90 Days).

Password Expiration is Disabled — Ensure AWS Identity and Access Management (IAM) user passwords are reset before expiration (90 Days).

Weak Password Policy (AWS Default password policy) is set for the AWS account — Ensure AWS account has an IAM strong password policy in use

Weak IAM Server Certificate in use — Ensure that all your SSL/TLS certificates are using either 2048 or 4096 bit RSA keys instead of 1024-bit keys.

IAM Role Policy are Too Permissive — Ensure AWS IAM policies attached to IAM roles are not too permissive.

IAM Access Analyzer is not Enabled — Ensure that IAM Access Analyzer feature is enabled to maintain access security to your AWS resources.

Pre-Heartbleed Server Certificates — Ensure that your server certificates are not vulnerable to Heartbleed security bug.

Root Account Access Keys Present — Ensure that your AWS account (root) is not using access keys as a security best practice.

Lack of SSH Public Keys Rotation — Ensure IAM SSH public keys are rotated on a periodic basis to adhere to AWS security best practices.

SSL/TLS Certificate is about to Expire — Ensure SSL/TLS certificates are renewed before their expiration.

Security Challenge Question not Enabled — Ensure security challenge questions are enabled and configured to improve the security of your AWS account.

Security Contact Information is not Registered — Ensure alternate contacts are set to improve the security of your AWS account.

AWS Multi-Account are managed centrally via Identity Federation or AWS Organization — Set up, organize and manage your AWS accounts for optimal security and manageability.

Root Account Recently Used — Ensure root account credentials have not been used recently to access your AWS account.

Elastic Compute Cloud (EC2) , Elastic Blob Storage (EBS), Elastic Load Balancer V2 (ELBv2)

Overbroad Ingress Rules for Security Groups — Ensure no EC2 security group allows unrestricted inbound access to any uncommon ports.

EC2 Instance Termination Protection is not Enabled — Ensure the Termination Protection feature is enabled for EC2 instances that are not part of ASGs.

AMIs are Publicly Shared — Ensure your Amazon Machine Images (AMIs) are not accessible to all AWS accounts.

Golden/Approved AMIs not in Use — Ensure all AWS EC2 instances are launched from approved AMIs.

Amazon EBS Snapshots are Publicly Accessible — Ensure that your Amazon EBS volume snapshots are not accessible to all AWS accounts.

Amazon EBS Volumes Encryption is not enabled — Ensure that existing Elastic Block Store (EBS) attached volumes are encrypted to meet security and compliance requirements.

Amazon EBS Snapshots Encryption is not enabled — Ensure Amazon EBS snapshots are encrypted to meet security and compliance requirements.

KMS Customer Master Keys is not used for EBS Volume Encryption — Ensure EBS volumes are encrypted with KMS CMKs in order to have full control over data encryption and decryption.

Weak Cryptographic Controls for ELB — Ensure AWS Application Load Balancers (ALBs) are using the latest predefined security policy.

Load Balancer is not Integrated with AWS WAF — Ensure that WAF ACL is integrated with Elastic Load Balancer

ELB uses In-secure protocols — Ensure that your Application Load Balancer (ALB) listeners are using a secure protocol such as HTTPS.

ELB Deletion Protection Disabled — Ensure the Deletion Protection feature is enabled for your AWS load balancers to follow security best practices.

Access logging disabled for ELB — Ensure access logging is enabled for your AWS ALBs to follow security best practices.

Virtual Private Cloud(VPC)

VPC Flow Logs Disabled — Ensure Virtual Private Cloud (VPC) Flow Logs feature is enabled in all applicable AWS regions.

Simple Storage Service (S3)

Overbroad S3 Access Control — Ensure that your AWS S3 buckets are not publicly exposed to the Internet.

Cross-Account Access for S3 Buckets — Ensure Amazon S3 buckets do not allow unknown cross account access via bucket policies.

Server-Side Encryption is not Enabled for S3 — Ensure AWS S3 buckets enforce Server-Side Encryption (SSE)

KMS Customer Master Keys is not used for S3 Buckets Encryption — Ensure that Amazon S3 buckets are encrypted with customer-provided AWS KMS CMKs

Versioning and Multi-Factor Delete is not Enabled on S3 buckets — Ensure AWS S3 buckets have the MFA Delete feature enabled.Ensure AWS S3 object versioning is enabled for an additional level of data protection.

Access Logging Disabled for S3 — Ensure AWS S3 buckets have server access logging enabled to track access requests.

Secure Transport is Not Enabled on S3 — Ensure AWS S3 buckets enforce SSL to secure data in transit

Cloud Trail

CloudTrail Log Encryption Disabled — Ensure your AWS CloudTrail logs are encrypted using AWS KMS–Managed Keys (SSE-KMS).

KMS Customer Master Keys is not used for CloudTrail Encryption — Ensure that KMS master keys are used for CloudTrail Encryption

CloudTrail Log File Validation is Disabled — Ensure your AWS CloudTrail trails have log file integrity validation enabled.

CloudTrail is not integrated with CloudWatch — Ensure CloudTrail event monitoring with CloudWatch is enabled.

CloudWatch

No Security Incident Alarm exist for AWS Services — Ensure that Security Incident Alarms are created in CloudWatch

Relational Database Service (RDS)

RDS Database instance are Publicly accessible — Ensure RDS database instances are not publicly accessible and prone to security risks.

Deletion protection is not Enabled for RDS Instance — Ensure Deletion Protection feature is enabled for your AWS RDS database instances.

RDS Automated Backup is not enabled — Ensure that Automated Backups are created for the RDS Instances

RDS Instance Encryption is not Enabled — Ensure AWS RDS instances are encrypted to meet security and compliance requirements.

KMS Customer Master Keys is not used for RDS Instance Encryption — Ensure RDS instances are encrypted with KMS CMKs in order to have full control over data encryption and decryption.

RDS Snapshots Encryption is not Enabled — Ensure that AWS RDS snapshots are encrypted to meet security and compliance requirements.

RDS Snapshots Publicly accessible — Ensure that your Amazon RDS database snapshots are not accessible to all AWS accounts.

RDS Log Exports is not Enabled (RDS MySQL, Aurora and MariaDB) — Ensure Log Exports feature is enabled for your AWS RDS MySQL, Aurora and MariaDB database instances.

IAM Database Authentication is not Enabled for RDS Instances — Ensure IAM Database Authentication feature is enabled for your AWS RDS MySQL and PostgreSQL database instances.

RDS Auto Minor Version Upgrade Not Enabled — Ensure AWS RDS instances have the Auto Minor Version Upgrade feature enabled.

RDS Database Instance not updated — Ensure that the RDS Instance is Updated

RDS Automated Backup is not enabled — Ensure AWS RDS instances have Automated Backups feature enabled.

RDS Secure Transport is not Enabled (SQL Server, PostgreSQL) — Ensure AWS RDS SQL Server instances have Transport Encryption feature enabled.

RDS Backup Retention Period is not enough — Ensure AWS RDS instances have sufficient backup retention period for compliance purposes.

SSL/TLS Certificates Already Expired for RDS — Ensure that RDS Instance is using the updated SSL Certificate

RDS not using Multi-AZ deployment — Ensure AWS RDS clusters have the Multi-AZ feature enabled.

Simple Notification Service (SNS)

Cross-Account Access for SNS Topics — Ensure Amazon SNS topics do not allow unknown cross account access.

SNS Topics Exposed to Everyone — Ensure that AWS Simple Notification Service (SNS) topics are not exposed to everyone.

Server-Side Encryption is Not Enabled for AWS SNS Topics — Ensure that Amazon SNS topics enforce Server-Side Encryption (SSE).

KMS Customer Master Keys is not used for SNS Topics Encryption — Ensure that Amazon SNS topics are encrypted with KMS Customer Master Keys (CMKs).

Key Management Service (KMS)

Lack of KMS Key Rotation — Ensure KMS key rotation feature is enabled for all your Customer Master Keys (CMK).

AWS Keys Exposed to Everyone — Ensure Amazon KMS master keys are not exposed to everyone.

Cross-Account Access for KMS Service — Ensure Amazon KMS master keys do not allow unknown cross account access.

Lambda

Code Signing is not Enabled for Lambda Functions — Ensure that Code Signing is enabled for your Amazon Lambda functions.

Lambda Runtime Environment Version is not Latest — Ensure that the latest version of the runtime environment is used for your AWS Lambda functions.

Cross-Account Access for Lambda Functions Queues — Ensure AWS Lambda functions do not allow unknown cross account access via permission policies.

Lambda Function Exposed to Everyone — Ensure that your Amazon Lambda functions are not exposed to everyone.

Lambda Environment Variables are not Encrypted — Ensure encryption is enabled for the AWS Lambda environment variables that store sensitive information.

KMS Customer Master Keys is not used for Lambda Environment Variables Encryption — Ensure Lambda environment variables are encrypted with KMS Customer Master Keys (CMKs) to gain full control over data encryption and decryption.

AWS Config

AWS Config Not Used — Ensure AWS Config is enabled in all regions to get the optimal visibility of the activity on your account.

Validate AWS Config Rules — Validate the AWS Config Rules and check for NonCompliant Rules

AWS GuardDuty

AWS GuardDuty Not Used — Ensure Amazon GuardDuty is enabled to help you protect your AWS accounts and workloads against security threats.

Validate the AWS GuardDuty Findings — Always validate the findings that are reported by GuardDuty

Route 53

Route 53 Domain Transfer Lock is not Enabled — Ensure your domain names have the Transfer Lock feature enabled in order to keep them secure.

SPF Record not Present — Ensure there is an SPF record set for each MX DNS record in order to stop spammers from spoofing your domains.

Route53 Domains Already Expired — Ensure expired AWS Route 53 domains names are restored.

Route53 Domains are about to Expire — Ensure AWS Route 53 domain names are renewed before their expiration (90 days before expiration).

DNSSEC Signing for Route 53 Hosted Zones is not Enabled — Ensure that DNSSEC signing is enabled for your Amazon Route 53 Hosted Zones.

Elastic Kubernetes Service (EKS)

EKS Secret Encryption is not Enabled — Ensure that envelope encryption of Kubernetes secrets using Amazon KMS is enabled.

Kubernetes Cluster Logging is not Enabled — Ensure that EKS control plane logging is enabled for your Amazon EKS clusters.

Kubernetes Cluster Version is not Updated — Ensure that the latest version of Kubernetes is installed on your Amazon EKS clusters.

Cluster Endpoints are Publicly accessible — Ensure that AWS EKS cluster endpoint access is not public and prone to security risks.

Simple Queue Service (SQS)

Server-Side Encryption is not Enabled for SQS Queues — Ensure Amazon SQS queues enforce Server-Side Encryption (SSE).

KMS Customer Master Keys is not used for SQS Queue Encryption — Ensure SQS queues are encrypted with KMS CMKs to gain full control over data encryption and decryption.

SQS Queue Exposed to Everyone — Ensure that AWS Simple Queue Service (SQS) queues are not exposed to everyone.

Cross-Account Access for SQS Queues — Ensure AWS Simple Queue Service (SQS) queues do not allow unknown cross account access.

DynamoDB

Continuous Backup is Not Enabled for DynamoDB — Ensure that continuous backup is enabled for all the DynamoDB

KMS Customer Master Keys are not used for DynamoDB Table Encryption — Ensure that all the DynamoDB tables are using KMS Customers Master Keys for encryption

AWS Backups

AWS Backup Vault is Not Prevented from Accidental Deletion — Ensure that Accidental Deletion is enabled for AWS Backup Vault

RedShift

Redshift Cluster is publicly accessible — Ensure that Redshift Cluster is not publicly accessible

WorkSpaces

Workspaces Volume Encryption is not Enabled — Ensure that the volume encryption is enabled for all the Workspaces

ElastiCache

Older Version of ElastiCache Engine in Use — Ensure that you are not using an older version of Elasticache and use the latest version that is available

ElastiCache Redis cluster In-Transit and At-rest Encryption not enabled — Ensure that Redis clusters data In-transit and At-rest encryptions are enabled

CloudFront

Access logging is disabled for CloudFront — Ensure that access logging is enabled for Cloudfront

WAF is Not Enabled in CloudFront — Ensure that WAF is enabled for all the available Cloudfront

TLSv1.0 Supported by CloudFront Distribution — Ensure that you are using the latest TLS version for all Cloudfront

Thanks for reading