AWS CLOUD SECURITY CHECKLIST

AWS CLOUD SECURITY CHECKLIST

SERVICES NAME	FINDINGS NAME	DESCRIPTION
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).

SERVICES NAME	FINDINGS NAME	DESCRIPTION
	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.

SERVICES NAME	FINDINGS NAME	DESCRIPTION
	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.

SERVICES NAME	FINDINGS NAME	DESCRIPTION
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 TERMINATION PROTECTION FEATURE IS ENABLED FOR EC2 INSTANCES THAT ARE NOT PART OF ASGS.
	AMIS ARE PUBLICALY 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.

SERVICES NAME	FINDINGS NAME	DESCRIPTION
	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 DELETION PROTECTION FEATURE IS ENABLED FOR YOUR AWS LOAD BALANCERS TO FOLLOW SECURITY BEST PRACTICES.

SERVICES NAME	FINDINGS NAME	DESCRIPTION
	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

SERVICES NAME	FINDINGS NAME	DESCRIPTION
	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.

SERVICES NAME	FINDINGS NAME	DESCRIPTION
	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.

SERVICES NAME	FINDINGS NAME	DESCRIPTION
	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.

SERVICES NAME	FINDINGS NAME	DESCRIPTION
	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.

SERVICES NAME	FINDINGS NAME	DESCRIPTION
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.

SERVICES NAME	FINDINGS NAME	DESCRIPTION
	CROSS-ACCOUNT ACCESS FOR KMS SERVICE	CROSS-ACCOUNT ACCESS FOR KMS SERVICE
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.

SERVICES NAME	FINDINGS NAME	DESCRIPTION
	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.

SERVICES NAME	FINDINGS NAME	DESCRIPTION
	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.

SERVICES NAME	FINDINGS NAME	DESCRIPTION
	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.

SERVICES NAME	FINDINGS NAME	DESCRIPTION
DYNAMODB	CONTINUOUS BACKUP IS NOT ENABLED FOR DYNAMODB	ENSURE THAT CONTINOUS BACKUP IS ENABLD FOR ALL THE DYNAMODB
	KMS CUSTOMER MASTER KEYS IS NOT USED FOR DYNAMODB TABLE ENCRYPTION	ENSURE THAT FOR 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

SERVICES NAME	FINDINGS NAME	DESCRIPTION
	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 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 LATEST TLS VERSION FOR ALL CLOUDFRONT

Note: The above content is taken from securitycipher.com, special thanks to Piyush Kumawat