CLOUD
BY PALO ALTO NETWORKS

# PCI DSS v3.2.1 Compliance Report

## Prepared for Palo Alto Networks (TEST ACCT) - 7907678726403151297

Generated On: Jan 19, 2023 at 16:57 GMT

From: Jan 28, 2020 at 22:00 GMT

To: Jan 19, 2023 at 16:52 GMT

Cloud Account(s):
AWS Prod

Cloud Region(s):

# Table of Contents

Executive Summary

1. Install and maintain a firewall configuration to protect cardholder data

2. Do not use vendor-supplied defaults for system passwords and other security parameters

3. Protect stored cardholder data

4. Encrypt transmission of cardholder data across open, public networks

6. Develop and maintain secure systems and applications

7. Restrict access to cardholder data by business need to know

8. Identify and authenticate access to system components

10. Track and monitor all access to network resources and cardholder data

A3. Designated Entities Supplemental Validation (DESV)

# Executive Summary

| Resources Monitored | Accounts Monitored | Pass | Fail |
| --- | --- | --- | --- |
| 532 | 1 | 286 | 246 |

Severity: High Medium Low

## 1. Install and maintain a firewall configuration to protect cardholder data

| Section Number | Policy Name | Resource(s) Passed | Resource(s) Failed | Overall Status |
|---|---|---|---|---|
| 1.2.1 | Instances exposed to network traffic from the internet | 0 | 5 | ⚠ |
| 1.2.1 | AWS Elastic Load Balancer v2 (ELBv2) load balancer with invalid security groups | 0 | 0 | ✓ |
| 1.2.1 | AWS Security Group allows all traffic on SSH port (22) | 30 | 4 | ⚠ |
| 1.2.1 | AWS RDS event subscription disabled for DB security groups | 0 | 0 | ✓ |
| 1.2.1 | AWS Security Group allows all traffic on RDP port (3389) | 33 | 1 | ⚠ |
| 1.2.1 | AWS EKS cluster control plane assigned multiple security groups | 0 | 0 | ✓ |
| 1.2.1 | AWS EKS cluster security group overly permissive to all traffic | 60 | 0 | ✓ |
| 1.2.1 | AWS route table with VPC peering overly permissive to all traffic | 27 | 0 | ✓ |
| 1.2.1 | AWS Default Security Group does not restrict all traffic | 13 | 21 | ⚠ |
| 1.2.1 | AWS Elasticsearch IAM policy overly permissive to all traffic | 31 | 0 | ✓ |
| 1.2.1 | AWS Elastic Load Balancer (ELB) has security group with no inbound rules | 32 | 0 | ✓ |
| 1.2.1 | AWS SageMaker notebook instance IAM policy overly permissive to all traffic | 31 | 0 | ✓ |
| 1.3 | AWS VPC subnets should not allow automatic public IP assignment | 7 | 57 | ⚠ |
| 1.3 | AWS CloudTrail bucket is publicly accessible | 13 | 0 | ✓ |
| 1.3 | AWS S3 Bucket Policy allows public access to CloudTrail logs | 13 | 0 | ✓ |
| 1.3 | AWS Route53 Public Zone with Private Records | 0 | 0 | ✓ |
| 1.3 | AWS Private ECR repository policy is overly permissive | 2 | 0 | ✓ |
| 1.3 | AWS RDS database instance is publicly accessible | 1 | 1 | ⚠ |
| 1.3 | AWS Classic Load Balancer is in use for internet-facing applications | 0 | 0 | ✓ |
| 1.3 | AWS SageMaker notebook instance configured with direct internet access feature | 0 | 0 | ✓ |
| 1.3 | AWS S3 bucket publicly writable | 12 | 0 | ✓ |
| 1.3 | AWS EKS cluster endpoint access publicly enabled | 0 | 0 | ✓ |
| 1.3 | AWS MQ is publicly accessible | 0 | 0 | ✓ |
| 1.3 | AWS Amazon Machine Image (AMI) is publicly accessible | 8 | 0 | ✓ |
| 1.3 | AWS CloudFormation template contains globally open resources | 27 | 1 | ⚠ |
| 1.3 | AWS Elasticsearch domain publicly accessible | 1 | 0 | ✓ |
| 1.3 | AWS S3 bucket publicly readable | 12 | 0 | ✓ |
| 1.3.1 | AWS Elastic Load Balancer (ELB) has security group with no outbound rules | 32 | 0 | ✓ |
| 1.3.5 | Instances exposed to network traffic from the internet | 0 | 5 | ⚠ |
| 1.3.6 | AWS ElastiCache cluster not associated with VPC | 1 | 0 | ✓ |
| 1.3.6 | AWS SageMaker notebook instance is not placed in VPC | 0 | 0 | ✓ |
| 1.3.6 | AWS VPC allows unauthorized peering | 29 | 0 | ✓ |

| Section Number | Policy Name | Resource(s) Passed | Resource(s) Failed | Overall Status |
|---|---|---|---|---|
| 1.3.7 | AWS RDS instance not in private subnet | 28 | 0 | ✓ |

Severity: High Medium Low

## 2. Do not use vendor-supplied defaults for system passwords and other security parameters

| Section Number | Policy Name | Resource(s) Passed | Resource(s) Failed | Overall Status |
|---|---|---|---|---|
| 2.1 | AWS EKS cluster using the default VPC | 20 | 0 | ✓ |
| 2.1 | AWS NAT Gateways are not being utilized for the default route | 27 | 0 | ✓ |
| 2.1 | AWS CloudFront web distribution using insecure TLS version | 2 | 0 | ✓ |
| 2.1 | AWS CloudFront web distribution with default SSL certificate | 0 | 2 | ⚠ |
| 2.1 | AWS Elastic Load Balancer v2 (ELBv2) listener that allow connection requests over HTTP | 0 | 0 | ✓ |
| 2.3 | AWS CloudFront origin protocol policy does not enforce HTTPS-only | 2 | 0 | ✓ |
| 2.3 | AWS Glue connection do not have SSL configured | 0 | 0 | ✓ |
| 2.3 | AWS Elastic Load Balancer v2 (ELBv2) SSL negotiation policy configured with weak ciphers | 0 | 0 | ✓ |
| 2.3 | AWS Elastic Load Balancer (Classic) SSL negotiation policy configured with vulnerable SSL protocol | 0 | 0 | ✓ |
| 2.3 | AWS S3 bucket not configured with secure data transport policy | 12 | 0 | ✓ |
| 2.3 | AWS CloudFront distribution is using insecure SSL protocols for HTTPS communication | 2 | 0 | ✓ |
| 2.3 | AWS Database Migration Service endpoint do not have SSL configured | 0 | 0 | ✓ |
| 2.3 | AWS Elastic Load Balancer with listener TLS/SSL is not configured | 0 | 0 | ✓ |
| 2.3 | AWS Redshift does not have require_ssl configured | 0 | 0 | ✓ |
| 2.3 | AWS Elastic Load Balancer (Classic) SSL negotiation policy configured with insecure ciphers | 0 | 0 | ✓ |

Severity: High Medium Low

## 3. Protect stored cardholder data

| Section Number | Policy Name | Resource(s) Passed | Resource(s) Failed | Overall Status |
|---|---|---|---|---|
| 3.1 | AWS RDS instance without Automatic Backup setting | 2 | 0 | ✓ |
| 3.1 | AWS RDS retention policy less than 7 days | 0 | 2 | ⚠ |
| 3.4.1 | AWS RDS instance is not encrypted | 0 | 2 | ⚠ |
| 3.4.1 | AWS Redshift instances are not encrypted | 0 | 0 | ✓ |
| 3.4.1 | AWS Elastic File System (EFS) with encryption for data at rest is disabled | 0 | 0 | ✓ |
| 3.4.1 | AWS EMR cluster is not enabled with local disk encryption using Custom key provider | 0 | 0 | ✓ |
| 3.4.1 | AWS RDS DB snapshot is not encrypted | 3 | 5 | ⚠ |
| 3.4.1 | AWS Kinesis streams encryption using default KMS keys instead of Customer's Managed Master Keys | 3 | 0 | ✓ |
| 3.4.1 | AWS SageMaker notebook instance not configured with data encryption at rest using KMS key | 0 | 0 | ✓ |
| 3.4.1 | AWS EMR cluster is not configured with CSE CMK for data at rest encryption (Amazon S3 with EMRFS) | 0 | 0 | ✓ |
| 3.4.1 | AWS RDS DB cluster encryption is disabled | 0 | 1 | ⚠ |
| 3.4.1 | AWS EMR cluster is not enabled with data encryption at rest | 0 | 0 | ✓ |
| 3.4.1 | AWS Kinesis streams are not encrypted using Server Side Encryption | 0 | 0 | ✓ |
| 3.4.1 | AWS SSM Parameter is not encrypted | 0 | 2 | ⚠ |
| 3.4.1 | AWS CloudTrail logs are not encrypted using Customer Master Keys (CMKs) | 0 | 2 | ⚠ |
| 3.4.1 | AWS Redshift Cluster not encrypted using Customer Managed Key | 3 | 0 | ✓ |
| 3.4.1 | AWS S3 buckets do not have server side encryption | 4 | 8 | ⚠ |
| 3.4.1 | AWS DynamoDB encrypted using AWS owned CMK instead of AWS managed CMK | 0 | 4 | ⚠ |
| 3.4.1 | AWS SQS queue encryption using default KMS key instead of CMK | 0 | 0 | ✓ |
| 3.4.1 | AWS ElastiCache Redis cluster with encryption for data at rest disabled | 0 | 0 | ✓ |
| 3.4.1 | AWS EMR cluster is not configured with SSE KMS for data at rest encryption (Amazon S3 with EMRFS) | 0 | 0 | ✓ |
| 3.4.1 | AWS EMR cluster is not enabled with local disk encryption | 0 | 0 | ✓ |
| 3.4.1 | AWS Elastic File System (EFS) not encrypted using Customer Managed Key | 3 | 0 | ✓ |
| 3.4.1 | AWS SageMaker notebook instance not encrypted using Customer Managed Key | 0 | 0 | ✓ |
| 3.4.1 | AWS RDS database not encrypted using Customer Managed Key | 5 | 0 | ✓ |
| 3.4.1 | AWS Elasticsearch domain Encryption for data at rest is disabled | 0 | 1 | ⚠ |
| 3.4.1 | AWS RDS DB cluster is encrypted using default KMS key instead of CMK | 4 | 0 | ✓ |
| 3.4.1 | AWS EBS volume region with encryption is disabled | 0 | 17 | ⚠ |

| Section Number | Policy Name | Resource(s) Passed | Resource(s) Failed | Overall Status |
|---|---|---|---|---|
| 3.6.4 | AWS Customer Master Key (CMK) rotation is not enabled | 1 | 2 | ⚠ |
| 3.6.4 | AWS Elastic Load Balancer (ELB) with IAM certificate expiring in 90 days | 0 | 0 | ✓ |
| 3.6.4 | AWS KMS Key scheduled for deletion | 3 | 0 | ✓ |
| 3.6.4 | AWS KMS customer managed external key expiring in 30 days or less | 3 | 0 | ✓ |
| 3.6.4 | AWS Certificate Manager (ACM) has certificates expiring in 30 days or less | 0 | 0 | ✓ |
| 3.6.4 | AWS IAM has expired SSL/TLS certificates | 0 | 0 | ✓ |
| 3.6.4 | AWS Database Migration Service (DMS) has expired certificates | 0 | 0 | ✓ |
| 3.6.4 | AWS Elastic Load Balancer (ELB) with ACM certificate expired or expiring in 90 days | 0 | 0 | ✓ |
| 3.6.4 | AWS Certificate Manager (ACM) has expired certificates | 0 | 0 | ✓ |
| 3.6.4 | AWS KMS Key policy overly permissive | 3 | 0 | ✓ |

Severity: High Medium Low

## 4. Encrypt transmission of cardholder data across open, public networks

| Section Number | Policy Name | Resource(s) Passed | Resource(s) Failed | Overall Status |
|---|---|---|---|---|
| 4.1 | Internet connectivity via TCP over insecure port | 0 | 3 | ⚠ |
| 4.1 | AWS CloudFront origin protocol policy does not enforce HTTPS-only | 2 | 0 | ✓ |
| 4.1 | AWS ElastiCache Redis cluster with in-transit encryption disabled (Replication group) | 0 | 0 | ✓ |
| 4.1 | AWS Kinesis streams encryption using default KMS keys instead of Customer's Managed Master Keys | 3 | 0 | ✓ |
| 4.1 | AWS SageMaker notebook instance not configured with data encryption at rest using KMS key | 0 | 0 | ✓ |
| 4.1 | AWS Glue connection do not have SSL configured | 0 | 0 | ✓ |
| 4.1 | AWS EMR cluster is not configured with CSE CMK for data at rest encryption (Amazon S3 with EMRFS) | 0 | 0 | ✓ |
| 4.1 | AWS Elastic Load Balancer v2 (ELBv2) SSL negotiation policy configured with weak ciphers | 0 | 0 | ✓ |
| 4.1 | AWS EMR cluster is not enabled with data encryption at rest | 0 | 0 | ✓ |
| 4.1 | AWS Elastic Load Balancer (Classic) SSL negotiation policy configured with vulnerable SSL protocol | 0 | 0 | ✓ |
| 4.1 | AWS Kinesis streams are not encrypted using Server Side Encryption | 0 | 0 | ✓ |
| 4.1 | AWS CloudFront distribution is using insecure SSL protocols for HTTPS communication | 2 | 0 | ✓ |
| 4.1 | AWS CloudTrail logs are not encrypted using Customer Master Keys (CMKs) | 0 | 2 | ⚠ |
| 4.1 | AWS Redshift Cluster not encrypted using Customer Managed Key | 3 | 0 | ✓ |
| 4.1 | AWS DynamoDB encrypted using AWS owned CMK instead of AWS managed CMK | 0 | 4 | ⚠ |
| 4.1 | AWS SQS queue encryption using default KMS key instead of CMK | 0 | 0 | ✓ |
| 4.1 | AWS EMR cluster is not configured with SSE KMS for data at rest encryption (Amazon S3 with EMRFS) | 0 | 0 | ✓ |
| 4.1 | AWS Database Migration Service endpoint do not have SSL configured | 0 | 0 | ✓ |
| 4.1 | AWS access keys are not rotated for 90 days | 11 | 4 | ⚠ |
| 4.1 | AWS EMR cluster is not enabled with data encryption in transit | 0 | 0 | ✓ |
| 4.1 | AWS Elastic File System (EFS) not encrypted using Customer Managed Key | 3 | 0 | ✓ |
| 4.1 | AWS SageMaker notebook instance not encrypted using Customer Managed Key | 0 | 0 | ✓ |
| 4.1 | AWS IAM SSH keys for AWS CodeCommit have aged more than 90 days without being rotated | 0 | 0 | ✓ |
| 4.1 | AWS Elastic Load Balancer with listener TLS/SSL is not configured | 0 | 0 | ✓ |
| 4.1 | AWS RDS database not encrypted using Customer Managed Key | 5 | 0 | ✓ |
| 4.1 | AWS Elasticsearch domain Encryption for data at rest is disabled | 0 | 1 | ⚠ |
| 4.1 | AWS Redshift does not have require_ssl configured | 0 | 0 | ✓ |

| Section Number | Policy Name | Resource(s) Passed | Resource(s) Failed | Overall Status |
|---|---|---|---|---|
| 4.1 | AWS RDS DB cluster is encrypted using default KMS key instead of CMK | 4 | 0 | ✓ |
| 4.1 | AWS Elastic Load Balancer (Classic) SSL negotiation policy configured with insecure ciphers | 0 | 0 | ✓ |
| 4.1 | AWS EMR cluster is not enabled with local disk encryption using Custom key provider | 0 | 0 | ✓ |
| 4.1.1 | AWS ElastiCache Redis cluster with in-transit encryption disabled (Replication group) | 0 | 0 | ✓ |
| 4.1.1 | AWS EMR cluster is not enabled with data encryption in transit | 0 | 0 | ✓ |

Severity: High Medium Low

## 6. Develop and maintain secure systems and applications

| Section Number | Policy Name | Resource(s) Passed | Resource(s) Failed | Overall Status |
|---|---|---|---|---|
| 6.3 | AWS Elastic Load Balancer (Classic) with cross-zone load balancing disabled | 0 | 0 | ✓ |
| 6.3 | AWS Certificate Manager (ACM) has invalid or failed certificate | 0 | 0 | ✓ |
| 6.3 | AWS ECS/ Fargate task definition root user found | 0 | 0 | ✓ |
| 6.3 | AWS CloudTrail log validation is not enabled in all regions | 2 | 0 | ✓ |
| 6.3 | AWS API gateway request parameter is not validated | 0 | 30 | ⚠ |
| 6.3 | AWS access keys not used for more than 90 days | 12 | 3 | ⚠ |
| 6.3 | AWS CloudTrail S3 buckets have not enabled MFA Delete | 12 | 1 | ⚠ |
| 6.3 | AWS root account configured with Virtual MFA | 0 | 1 | ⚠ |
| 6.3 | AWS API gateway request authorisation is not set | 19 | 11 | ⚠ |
| 6.3 | AWS VPC not in use | 82 | 0 | ✓ |
| 6.3 | AWS Elastic Load Balancer (ELB) not in use | 0 | 0 | ✓ |
| 6.3 | AWS RDS minor upgrades not enabled | 2 | 0 | ✓ |
| 6.3 | AWS API Gateway endpoints without client certificate authentication | 0 | 2 | ⚠ |
| 6.3 | AWS EBS Snapshot with access for unmonitored cloud accounts | 0 | 0 | ✓ |
| 6.3 | AWS Elasticsearch domain has Dedicated master set to disabled | 0 | 1 | ⚠ |
| 6.3 | AWS RDS instance with copy tags to snapshots disabled | 1 | 1 | ⚠ |
| 6.3 | AWS S3 bucket is not configured with MFA Delete | 11 | 1 | ⚠ |
| 6.3 | AWS Lambda nearing availability code storage limit | 5 | 0 | ✓ |
| 6.3 | AWS RDS Snapshot with access for unmonitored cloud accounts | 5 | 0 | ✓ |
| 6.3 | AWS ACM Certificate with wildcard domain name | 0 | 0 | ✓ |
| 6.3 | AWS S3 Object Versioning is disabled | 1 | 11 | ⚠ |
| 6.3 | AWS RDS instance with Multi-Availability Zone disabled | 0 | 2 | ⚠ |
| 6.3 | AWS Elasticsearch domain has Zone Awareness set to disabled | 0 | 1 | ⚠ |
| 6.3 | AWS ElastiCache Redis cluster with Multi-AZ Automatic Failover feature set to disabled | 0 | 0 | ✓ |
| 6.3 | AWS Certificate Manager (ACM) contains certificate pending validation | 0 | 0 | ✓ |
| 6.3 | AWS regions nearing VPC Private Gateway limit | 0 | 0 | ✓ |
| 6.3 | AWS EMR cluster is not configured with security configuration | 0 | 0 | ✓ |
| 6.3 | AWS S3 bucket accessible to unmonitored cloud accounts | 12 | 0 | ✓ |
| 6.3 | S3 buckets with configurations set to host websites | 10 | 2 | ⚠ |
| 6.3 | AWS Network Load Balancer (NLB) is not using the latest predefined security policy | 0 | 0 | ✓ |
| 6.3 | AWS CloudFront web distribution with AWS Web Application Firewall (AWS WAF) service disabled | 0 | 2 | ⚠ |

| Section Number | Policy Name | Resource(s) Passed | Resource(s) Failed | Overall Status |
|---|---|---|---|---|
| 6.3 | AWS CloudFront web distribution with geo restriction disabled | 0 | 2 | ⚠ |
| 6.3 | AWS regions nearing VPC Private Gateway IPSec Limit | 0 | 0 | ✓ |
| 6.3 | AWS Application Load Balancer (ALB) is not using the latest predefined security policy | 0 | 0 | ✓ |
| 6.3 | AWS Cloudfront Distribution with S3 have Origin Access set to disabled | 2 | 0 | ✓ |

Severity: High Medium Low

## 7. Restrict access to cardholder data by business need to know

| Section Number | Policy Name | Resource(s) Passed | Resource(s) Failed | Overall Status |
|---|---|---|---|---|
| 7.1 | AWS EBS snapshots are accessible to public | 0 | 0 | ✓ |
| 7.1 | AWS RDS snapshots are accessible to public | 5 | 0 | ✓ |
| 7.1 | AWS S3 buckets are accessible to public | 12 | 0 | ✓ |
| 7.1 | AWS S3 bucket has global view ACL permissions enabled | 12 | 0 | ✓ |
| 7.1 | AWS VPC subnets should not allow automatic public IP assignment | 7 | 57 | ⚠ |
| 7.1 | AWS CloudTrail bucket is publicly accessible | 13 | 0 | ✓ |
| 7.1 | AWS S3 Bucket Policy allows public access to CloudTrail logs | 13 | 0 | ✓ |
| 7.1 | AWS Route53 Public Zone with Private Records | 0 | 0 | ✓ |
| 7.1 | AWS IAM user has two active Access Keys | 14 | 1 | ⚠ |
| 7.1 | AWS IAM user has both Console access and Access Keys | 15 | 0 | ✓ |
| 7.1 | AWS EC2 Instance IAM Role not enabled | 5 | 7 | ⚠ |
| 7.1 | AWS Private ECR repository policy is overly permissive | 2 | 0 | ✓ |
| 7.1 | AWS RDS database instance is publicly accessible | 1 | 1 | ⚠ |
| 7.1 | AWS IAM policy attached to users | 3 | 11 | ⚠ |
| 7.1 | AWS Classic Load Balancer is in use for internet-facing applications | 0 | 0 | ✓ |
| 7.1 | AWS SageMaker notebook instance configured with direct internet access feature | 0 | 0 | ✓ |
| 7.1 | AWS SageMaker notebook instance with root access enabled | 0 | 0 | ✓ |
| 7.1 | AWS S3 bucket publicly writable | 12 | 0 | ✓ |
| 7.1 | AWS S3 bucket having policy overly permissive to VPC endpoints | 12 | 0 | ✓ |
| 7.1 | AWS IAM policy allows assume role permission across all services | 31 | 0 | ✓ |
| 7.1 | AWS IAM deprecated managed policies in use by User | 14 | 0 | ✓ |
| 7.1 | AWS IAM support access policy is not associated to any role | 31 | 0 | ✓ |
| 7.1 | AWS EKS cluster endpoint access publicly enabled | 0 | 0 | ✓ |
| 7.1 | AWS MQ is publicly accessible | 0 | 0 | ✓ |
| 7.1 | AWS Amazon Machine Image (AMI) is publicly accessible | 8 | 0 | ✓ |
| 7.1 | AWS SQS queue access policy is overly permissive | 0 | 0 | ✓ |
| 7.1 | AWS CloudFormation template contains globally open resources | 27 | 1 | ⚠ |
| 7.1 | AWS IAM Roles with Administrator Access Permissions | 88 | 5 | ⚠ |
| 7.1 | AWS Elasticsearch domain publicly accessible | 1 | 0 | ✓ |
| 7.1 | AWS S3 bucket publicly readable | 12 | 0 | ✓ |
| 7.1 | AWS IAM policy allows full administrative privileges | 31 | 0 | ✓ |
| 7.1 | AWS ECS task definition elevated privileges enabled | 0 | 0 | ✓ |

| Section Number | Policy Name | Resource(s) Passed | Resource(s) Failed | Overall Status |
|---|---|---|---|---|
| 7.1 | AWS IAM role/user with unused CloudTrail delete or full permission | 80 | 0 | ✓ |
| 7.1.2 | AWS S3 bucket has global view ACL permissions enabled | 12 | 0 | ✓ |
| 7.1.2 | AWS IAM user has two active Access Keys | 14 | 1 | ⚠ |
| 7.1.2 | AWS IAM user has both Console access and Access Keys | 15 | 0 | ✓ |
| 7.1.2 | AWS EC2 Instance IAM Role not enabled | 5 | 7 | ⚠ |
| 7.1.2 | AWS IAM policy attached to users | 3 | 11 | ⚠ |
| 7.1.2 | AWS SageMaker notebook instance with root access enabled | 0 | 0 | ✓ |
| 7.1.2 | AWS S3 bucket having policy overly permissive to VPC endpoints | 12 | 0 | ✓ |
| 7.1.2 | AWS IAM policy allows assume role permission across all services | 31 | 0 | ✓ |
| 7.1.2 | AWS IAM deprecated managed policies in use by User | 14 | 0 | ✓ |
| 7.1.2 | AWS IAM support access policy is not associated to any role | 31 | 0 | ✓ |
| 7.1.2 | AWS SQS queue access policy is overly permissive | 0 | 0 | ✓ |
| 7.1.2 | AWS IAM Roles with Administrator Access Permissions | 88 | 5 | ⚠ |
| 7.1.2 | AWS IAM policy allows full administrative privileges | 31 | 0 | ✓ |
| 7.1.2 | AWS ECS task definition elevated privileges enabled | 0 | 0 | ✓ |
| 7.1.2 | AWS IAM role/user with unused CloudTrail delete or full permission | 80 | 0 | ✓ |

Severity: High Medium Low

## 8. Identify and authenticate access to system components

| Section Number | Policy Name | Resource(s) Passed | Resource(s) Failed | Overall Status |
|---|---|---|---|---|
| 8.2 | AWS EMR cluster is not configured with Kerberos Authentication | 0 | 0 | ✓ |
| 8.2 | AWS IAM Password policy is unsecure | 1 | 0 | ✓ |
| 8.2 | AWS ElastiCache Redis cluster with Redis AUTH feature disabled | 0 | 0 | ✓ |
| 8.2.3 | AWS IAM password policy does not have a minimum of 14 characters | 1 | 0 | ✓ |
| 8.2.3 | AWS IAM password policy does not have a lowercase character | 1 | 0 | ✓ |
| 8.2.3 | AWS IAM password policy does not have a number | 1 | 0 | ✓ |
| 8.2.3 | AWS IAM password policy does not have a symbol | 1 | 0 | ✓ |
| 8.2.3 | AWS IAM password policy does not have an uppercase character | 1 | 0 | ✓ |
| 8.2.4 | AWS IAM password policy does not expire in 90 days | 1 | 0 | ✓ |
| 8.2.4 | AWS IAM password policy does not have password expiration period | 1 | 0 | ✓ |
| 8.2.5 | AWS IAM password policy allows password reuse | 1 | 0 | ✓ |
| 8.3 | AWS MFA is not enabled on Root account | 15 | 0 | ✓ |
| 8.3 | AWS MFA not enabled for IAM users | 15 | 0 | ✓ |
| 8.3 | AWS Inactive users for more than 30 days | 2 | 13 | ⚠ |
| 8.3 | AWS Access key enabled on root account | 1 | 0 | ✓ |

Severity: High Medium Low

## 10. Track and monitor all access to network resources and cardholder data

| Section Number | Policy Name | Resource(s) Passed | Resource(s) Failed | Overall Status |
|---|---|---|---|---|
| 10.1 | AWS CloudTrail is not enabled on the account | 21 | 0 | ✓ |
| 10.1 | AWS Access logging not enabled on S3 buckets | 0 | 12 | ⚠ |
| 10.1 | AWS S3 buckets are accessible to public | 12 | 0 | ✓ |
| 10.1 | AWS S3 buckets are accessible to any authenticated user | 12 | 0 | ✓ |
| 10.1 | AWS CloudTrail is not enabled with multi trail and not capturing all management events | 3 | 0 | ✓ |
| 10.2.3 | AWS Access logging not enabled on S3 buckets | 0 | 12 | ⚠ |
| 10.2.3 | AWS Redshift database does not have audit logging enabled | 0 | 0 | ✓ |
| 10.2.3 | AWS Elasticsearch domain has Index slow logs set to disabled | 0 | 1 | ⚠ |
| 10.2.3 | AWS Config fails to deliver log files | 5 | 0 | ✓ |
| 10.2.3 | AWS Config must record all possible resources | 5 | 0 | ✓ |
| 10.2.3 | AWS CloudTrail logging is disabled | 3 | 0 | ✓ |
| 10.2.3 | AWS EKS control plane logging disabled | 0 | 0 | ✓ |
| 10.2.3 | AWS VPC Flow Logs not enabled | 8 | 17 | ⚠ |
| 10.2.3 | AWS CloudTrail logs should integrate with CloudWatch for all regions | 3 | 0 | ✓ |
| 10.2.3 | AWS Certificate Manager (ACM) has certificates with Certificate Transparency Logging disabled | 0 | 0 | ✓ |
| 10.2.3 | AWS S3 CloudTrail bucket for which access logging is disabled | 12 | 1 | ⚠ |
| 10.2.3 | AWS RDS Event subscription All event categories and All instances disabled for DB instance | 0 | 0 | ✓ |
| 10.2.3 | AWS Elasticsearch domain has Search slow logs set to disabled | 0 | 1 | ⚠ |
| 10.2.3 | CloudTrail trail is not integrated with CloudWatch Log | 1 | 1 | ⚠ |
| 10.2.3 | AWS Elastic Load Balancer v2 (ELBv2) with access log disabled | 0 | 0 | ✓ |
| 10.2.3 | AWS Elastic Load Balancer (Classic) with access log disabled | 0 | 0 | ✓ |
| 10.2.3 | AWS CloudFront distribution with access logging disabled | 0 | 2 | ⚠ |
| 10.2.3 | AWS Config Recording is disabled | 11 | 19 | ⚠ |
| 10.6 | AWS Redshift database does not have audit logging enabled | 0 | 0 | ✓ |
| 10.6 | AWS EC2 Instance Scheduled Events | 12 | 0 | ✓ |
| 10.6 | AWS Elasticsearch domain has Index slow logs set to disabled | 0 | 1 | ⚠ |
| 10.6 | AWS Config fails to deliver log files | 5 | 0 | ✓ |
| 10.6 | AWS Config must record all possible resources | 5 | 0 | ✓ |
| 10.6 | AWS CloudTrail logging is disabled | 3 | 0 | ✓ |
| 10.6 | AWS EKS control plane logging disabled | 0 | 0 | ✓ |
| 10.6 | AWS VPC Flow Logs not enabled | 8 | 17 | ⚠ |

| Section Number | Policy Name | Resource(s) Passed | Resource(s) Failed | Overall Status |
|---|---|---|---|---|
| 10.6 | AWS CloudTrail logs should integrate with CloudWatch for all regions | 3 | 0 | ✓ |
| 10.6 | AWS Certificate Manager (ACM) has certificates with Certificate Transparency Logging disabled | 0 | 0 | ✓ |
| 10.6 | AWS S3 CloudTrail bucket for which access logging is disabled | 12 | 1 | ⚠ |
| 10.6 | AWS RDS Event subscription All event categories and All instances disabled for DB instance | 0 | 0 | ✓ |
| 10.6 | AWS Elasticsearch domain has Search slow logs set to disabled | 0 | 1 | ⚠ |
| 10.6 | CloudTrail trail is not integrated with CloudWatch Log | 1 | 1 | ⚠ |
| 10.6 | AWS Elastic Load Balancer v2 (ELBv2) with access log disabled | 0 | 0 | ✓ |
| 10.6 | AWS Elastic Load Balancer (Classic) with access log disabled | 0 | 0 | ✓ |
| 10.6 | AWS CloudFront distribution with access logging disabled | 0 | 2 | ⚠ |
| 10.6 | AWS Config Recording is disabled | 11 | 19 | ⚠ |

Severity: High Medium Low

## A3. Designated Entities Supplemental Validation (DESV)

| Section Number | Policy Name | Resource(s) Passed | Resource(s) Failed | Overall Status |
|---|---|---|---|---|
| A3.3.1 | AWS EC2 Instance Scheduled Events | 12 | 0 | ✓ |
| A3.3.1 | AWS Log metric filter and alarm does not exist for Network gateways changes | 21 | 1 | ⚠ |
| A3.3.1 | AWS Log metric filter and alarm does not exist for AWS management console authentication failures | 21 | 1 | ⚠ |
| A3.3.1 | AWS Log metric filter and alarm does not exist for CloudTrail configuration changes | 21 | 1 | ⚠ |
| A3.3.1 | AWS Log metric filter and alarm does not exist for S3 bucket policy changes | 21 | 1 | ⚠ |
| A3.3.1 | AWS Log metric filter and alarm does not exist for Network Access Control Lists (NACL) changes | 21 | 1 | ⚠ |
| A3.3.1 | AWS Log metric filter and alarm does not exist for VPC changes | 21 | 1 | ⚠ |
| A3.3.1 | AWS Log metric filter and alarm does not exist for Route table changes | 21 | 1 | ⚠ |
| A3.3.1 | AWS Log metric filter and alarm does not exist for unauthorized API calls | 21 | 1 | ⚠ |
| A3.3.1 | AWS Log metric filter and alarm does not exist for disabling or scheduled deletion of customer created CMKs | 21 | 1 | ⚠ |
| A3.3.1 | AWS Log metric filter and alarm does not exist for IAM policy changes | 21 | 1 | ⚠ |
| A3.3.1 | AWS Log metric filter and alarm does not exist for AWS Config configuration changes | 21 | 1 | ⚠ |

# 1. Install and maintain a firewall configuration to protect cardholder data

1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.

## Instances exposed to network traffic from the internet

| | |
|---|---|
| Compliance Section: 1.2.1 | First Seen: N/A |
| Resource(s) Failed: 5 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies network traffic coming from the internet to sensitive cloud workloads. Cloud workloads should have appropriate Security Groups and ACLs in place so that only external facing workloads such as load balancers, web servers, bastion hosts are exposed to the internet. Cloud workloads with internet exposure are vulnerable to external threats. Note: This policy alerts AWS and GCP workloads correctly and for Azure, it may trigger alerts for NAT Gateway configured resources also.

### Resource(s) Failed:

PANW-WindowsBastionServer-awsjamconfig, eni-08ed2d71b4d68332d, PANW-WebServer-awsjamconfig, eni-00ba3b413a9e8a932, LinuxBastion

### Recommendations:

1. Log in to the Cloud Console
2. Search for the resource reported in the alert
3. Check if the Security Group/Firewall Rule of the resource indeed allows connections from the internet
4. Assign another Security Group/Firewall Rule to the resource that has a more restrictive ACL, which does not permit connection from the internet

# 1. Install and maintain a firewall configuration to protect cardholder data

1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.

## AWS Elastic Load Balancer v2 (ELBv2) load balancer with invalid security groups

| | |
|---|---|
| Compliance Section: 1.2.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies Elastic Load Balancer v2 (ELBv2) load balancers that do not have security groups with a valid inbound or outbound rule. A security group with no inbound/outbound rule will deny all incoming/outgoing requests. ELBv2 security groups should have at least one inbound and outbound rule, ELBv2 with no inbound/outbound permissions will deny all traffic incoming/outgoing to/from any resources configured behind that ELBv2; in other words, the ELBv2 is useless without inbound and outbound permissions.

### Recommendations:

1. Log in to the AWS console
2. In the console, select the specific region from the region drop-down on the top right corner, for which the alert is generated
3. Navigate to EC2 Dashboard
4. Click on 'Load Balancers', choose the reported load balancer
5. Click on the 'Description' tab, click on each security group, it will open Security Group properties in a new tab in your browser.
6. For to check the Inbound rule, Click on the 'Inbound Rules'
7. If there are no rules, click on 'Edit rules', add an inbound rule according to your ELBv2 functional requirement.
8. For to check the Outbound rule, Click on the 'Outbound Rules'
9. If there are no rules, click on 'Edit rules', add an outbound rule according to your ELBv2 functional requirement.
10. Click on 'Save'

# 1. Install and maintain a firewall configuration to protect cardholder data

1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.

## AWS Security Group allows all traffic on SSH port (22)

| | |
|---|---|
| Compliance Section: 1.2.1 | First Seen: N/A |
| Resource(s) Failed: 4 | Resource Type: Other |
| Resource(s) Passed: 30 | |

### Description:

This policy identifies Security groups that allow all traffic on SSH port 22. Doing so, may allow a bad actor to brute force their way into the system and potentially get access to the entire network. Review your list of security group rules to ensure that your resources are not exposed. As a best practice, restrict SSH solely to known static IP addresses. Limit the access list to include known hosts, services, or specific employees only.

### Resource(s) Failed:

awsjamconfig-WebServerSecurityGroup-19OM44VWRYX15, guarddutytester-BastionSecurityGroup-1JVTQIA1OFP3Q, jenkins, launch-wizard-1

### Recommendations:

Before making any changes, please check the impact to your applications/services. If the Security Group reported indeed need to restrict all traffic, follow the instructions below:

1. Log in to the AWS Console
2. Navigate to the 'VPC' service
3. Select the 'Security Group' reported in the alert
4. Click on the 'Inbound Rule'
5. Remove the rule which has 'Source' value as 0.0.0.0/0 or ::/0 and 'Port Range' value as 22 (or range containing 22)

# 1. Install and maintain a firewall configuration to protect cardholder data

1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.

## AWS RDS event subscription disabled for DB security groups

| | |
|---|---|
| Compliance Section: 1.2.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies RDS event subscriptions for which DB security groups event subscription is disabled. You can create an Amazon RDS event notification subscription so that you can be notified when an event occurs for given DB security groups.

### Recommendations:

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to Amazon RDS Dashboard
4. Click on 'Event subscriptions' (Left Panel)
5. Choose the reported Event subscription
6. Click on 'Edit'
7. On 'Edit event subscription' page, Under 'Details' section; Select 'Yes' for 'Enabled' and Make sure you have subscribed your DB to 'All instances' and 'All event categories'
8. Click on 'Edit'

# 1. Install and maintain a firewall configuration to protect cardholder data

1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.

## AWS Security Group allows all traffic on RDP port (3389)

| | |
|---|---|
| Compliance Section: 1.2.1 | First Seen: N/A |
| Resource(s) Failed: 1 | Resource Type: Other |
| Resource(s) Passed: 33 | |

### Description:

This policy identifies Security groups that allow all traffic on RDP port 3389. Doing so, may allow a bad actor to brute force their way into the system and potentially get access to the entire network. Review your list of security group rules to ensure that your resources are not exposed. As a best practice, restrict RDP solely to known static IP addresses. Limit the access list to include known hosts, services, or specific employees only.

### Resource(s) Failed:

awsjamconfig-WindowsBastionSecurityGroup-OB0NJ4ZUWO8Q

### Recommendations:

Before making any changes, please check the impact to your applications/services. If the Security Group reported indeed need to restrict all traffic, follow the instructions below:

1. Log in to the AWS Console
2. Navigate to the 'VPC' service
3. Select the 'Security Group' reported in the alert
4. Click on the 'Inbound Rule'
5. Remove the rule which has 'Source' value as 0.0.0.0/0 or ::/0 and 'Port Range' value as 3389 (or range containing 3389)

# 1. Install and maintain a firewall configuration to protect cardholder data

1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.

## AWS EKS cluster control plane assigned multiple security groups

| | |
|---|---|
| Compliance Section: 1.2.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

Amazon EKS strongly recommends that you use a dedicated security group for each cluster control plane (one per cluster). This policy checks the number of security groups assigned to your cluster's control plane and alerts if there are more than one.

### Recommendations:

Create a single dedicated VPC security group for your EKS cluster control plane.
From the AWS console a security group cannot be added to, nor removed from, a Kubernetes cluster once it is created. To resolve this alert, create a new cluster with a single dedicated security group as per your requirements, then migrate all required cluster data from the reported cluster to this newly created cluster and delete the reported Kubernetes cluster.
1. Open the Amazon EKS dashboard.
2. Choose Create cluster.
3. On the Create cluster page, fill in the following fields:
- Cluster name
- Kubernetes version
- Role name
- VPC
- Subnets
- Security Groups - Choose your new dedicated control plane security group.
- Endpoint private access
- Endpoint public access
- Logging
4. Choose Create.

# 1. Install and maintain a firewall configuration to protect cardholder data

1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.

## AWS EKS cluster security group overly permissive to all traffic

| | |
|---|---|
| Compliance Section: 1.2.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 60 | |

### Description:

This policy identifies EKS cluster Security groups that are overly permissive to all traffic. Doing so, may allow a bad actor to brute force their way into the system and potentially get access to the entire network. Review your list of security group rules to ensure that your resources are not exposed. As a best practice, restrict traffic solely from known static IP addresses. Limit the access list to include known hosts, services, or specific employees only.

### Recommendations:

Before making any changes, please check the impact on your applications/services. If the Security Group reported indeed need to restrict all traffic, follow the instructions below:

1. Log in to the AWS console
2. Navigate to the 'VPC' service
3. Select the 'Security Group' reported in the alert
4. Click on 'Inbound Rules'
5. Remove the rule which has the 'Source' value as 0.0.0.0/0 or ::/0

# 1. Install and maintain a firewall configuration to protect cardholder data

1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.

## AWS route table with VPC peering overly permissive to all traffic

| | |
|---|---|
| Compliance Section: 1.2.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 27 | |

### Description:

This policy identifies VPC route tables with VPC peering connection which are overly permissive to all traffic. Being highly selective in peering routing tables is a very effective way of minimizing the impact of breach as resources outside of these routes are inaccessible to the peered VPC.

### Recommendations:

1. Log in to the AWS Console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated.
3. Navigate to 'VPC' dashboard from 'Services' dropdown
4. From left menu, select 'Route Tables'
5. Click on the alerted route table
6. From top click on 'Action' button
7. From the Action menu dropdown, select 'Edit routes'
8. From the list of destination remove the extra permissive destination by clicking the cross symbol available for that destination
9. Add a destination with 'least access'
10. Click on 'Save Routes'.

# 1. Install and maintain a firewall configuration to protect cardholder data

1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.

## AWS Default Security Group does not restrict all traffic

| | |
|---|---|
| Compliance Section: 1.2.1 | First Seen: N/A |
| Resource(s) Failed: 21 | Resource Type: Other |
| Resource(s) Passed: 13 | |

### Description:

This policy identifies the default security groups which does not restrict inbound and outbound traffic. A VPC comes with a default security group whose initial configuration denies all inbound traffic and allow all outbound traffic. If you do not specify a security group when you launch an instance, the instance is automatically assigned to this default security group. As a result, the instance may accidentally send outbound traffic. It is recommended that to remove any inbound and outbound rules in the default security group and not to attach the default security group to any resources.

### Resource(s) Failed:

default ...and 11 more

### Recommendations:

Before making any changes, please check the impact on your applications/services.
For Resources associated with the alerted security group:
1. Identify AWS resources that exist within the default security group
2. Create a set of least privilege security groups for those resources
3. Place the resources in those security groups
4. Remove the associated resources from the default security group
For alerted Security Groups:
1. Log in to the AWS console
2. In the console, select the specific region from the 'Region' drop-down on the top right corner, for which the alert is generated
3. Navigate to the 'VPC' service
4. For each region, Click on 'Security Groups' specific to the alert
5. On section 'Inbound rules', Click on 'Edit Inbound Rules' and remove the existing rule, click on 'Save'
6. On section 'Outbound rules', Click on 'Edit Outbound Rules' and remove the existing rule, click on 'Save'

# 1. Install and maintain a firewall configuration to protect cardholder data

1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.

## AWS Elasticsearch IAM policy overly permissive to all traffic

| | |
|---|---|
| Compliance Section: 1.2.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 31 | |

### Description:

This policy identifies Elasticsearch IAM policies that are overly permissive to all traffic. Amazon Elasticsearch service makes it easy to deploy and manage Elasticsearch. Customers can create a domain where the service is accessible. The domain should be granted access restrictions so that only authorized users and applications have access to the service.

### Recommendations:

1. Log in to AWS console
2. Goto the IAM Services
3. Click on 'Policies' in the left-hand panel
4. Search for the Policy for which the Alert is generated and click on it
5. Under the Permissions tab, click on Edit policy
6. Under the Visual editor, for each of the 'Elasticsearch Service', click to expand and perform following.
6.a. Click to expand 'Request conditions'
6.b. Under the 'Source IP', remove the row with the entry '0.0.0.0/0' or '::/0'. Add condition with restrictive IP ranges.
7. Click on Review policy and Save changes.

# 1. Install and maintain a firewall configuration to protect cardholder data

1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.

## AWS Elastic Load Balancer (ELB) has security group with no inbound rules

| | |
|---|---|
| Compliance Section: 1.2.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 32 | |

### Description:

This policy identifies Elastic Load Balancers (ELB) which have security group with no inbound rules. A security group with no inbound rule will deny all incoming requests. ELB security groups should have at least one inbound rule, ELB with no inbound permissions will deny all traffic incoming to ELB; in other words, the ELB is useless without inbound permissions.

### Recommendations:

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to EC2 Dashboard
4. Click on 'Load Balancers', choose the reported load balancer
5. Click on the 'Description' tab, click on the security group, it will open Security Group properties in a new tab in your browser
6. Click on the 'Inbound Rules'
7. If there are no rules, click on 'Edit rules', add an inbound rule according to your ELB functional requirement
8. Click on 'Save'

# 1. Install and maintain a firewall configuration to protect cardholder data

1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.

## AWS SageMaker notebook instance IAM policy overly permissive to all traffic

| | |
|---|---|
| Compliance Section: 1.2.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 31 | |

### Description:

This policy identifies SageMaker notebook instances IAM policies that are overly permissive to all traffic. It is recommended that the SageMaker notebook instances should be granted access restrictions so that only authorized users and applications have access to the service. For more details: https://docs.aws.amazon.com/sagemaker/latest/dg/security_iam_id-based-policy-examples.html

### Recommendations:

1. Login to AWS console
2. Goto IAM Services
3. Click on 'Policies' in left hand panel
4. Search for the Policy for which the Alert is generated and click on it
5. Under Permissions tab, click on Edit policy
6. Under the Visual editor, for each of the 'SageMaker' Service, click to expand and perform following.
6.a. Click to expand 'Request conditions'
6.b. Under the 'Source IP', remove the row with the entry '0.0.0.0/0' or '::/0'. Add condition with restrictive IP ranges.
7. Click on Review policy and Save changes.

# 1. Install and maintain a firewall configuration to protect cardholder data

1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.

## AWS VPC subnets should not allow automatic public IP assignment

| | |
|---|---|
| Compliance Section: 1.3 | First Seen: N/A |
| Resource(s) Failed: 57 | Resource Type: Subnet |
| Resource(s) Passed: 7 | |

### Description:

This policy identifies VPC subnets which allow automatic public IP assignment. VPC subnet is a part of the VPC having its own rules for traffic. Assigning the Public IP to the subnet automatically (on launch) can accidentally expose the instances within this subnet to internet and should be edited to 'No' post creation of the Subnet.

### Resource(s) Failed:

subnet-14ad5472, subnet-4e4e6b12, subnet-81fc4ce7, subnet-e219f2ae, subnet-765a6d1f, subnet-bab57e91, subnet-aacee2e2, subnet-66f6e848, subnet-a1410fda, subnet-415f4208 ...and 47 more

### Recommendations:

1. Sign into the AWS console.
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated.
3. Navigate to the 'VPC' service.
4. In the navigation pane, click on 'Subnets'.
5. Select the identified Subnet and choose the option 'Modify auto-assign IP settings' under the Subnet Actions.
6. Disable the 'Auto-Assign IP' option and save it.

# 1. Install and maintain a firewall configuration to protect cardholder data

1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.

## AWS CloudTrail bucket is publicly accessible

| | |
|---|---|
| Compliance Section: 1.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 13 | |

### Description:

This policy identifies publicly accessible S3 buckets that store CloudTrail data. These buckets contains sensitive audit data and only authorized users and applications should have access.

### Recommendations:

1. Login to the AWS Console
2. Navigate to the 'S3' service
3. Click on the 'S3' resource reported in the alert
4. Click on the 'Permissions'
5. If Access Control List' is set to 'Public' follow below steps
a. Under 'Access Control List', Click on 'Everyone' and uncheck all items
b. Click on Save
6. If 'Bucket Policy' is set to public follow below steps
a. Under 'Bucket Policy', modify the policy to remove public access
b. Click on Save
c. If 'Bucket Policy' is not required delete the existing 'Bucket Policy'.
Note: Make sure updating 'Access Control List' or 'Bucket Policy' does not affect S3 bucket data access.

# 1. Install and maintain a firewall configuration to protect cardholder data

1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.

## AWS S3 Bucket Policy allows public access to CloudTrail logs

| | |
|---|---|
| Compliance Section: 1.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 13 | |

### Description:

This policy scans your bucket policy that is applied to the S3 bucket to prevent public access to the CloudTrail logs. CloudTrail logs a record of every API call made in your AWS account. These logs file are stored in an S3 bucket. Bucket policy or the access control list (ACL) applied to the S3 bucket does not prevent public access to the CloudTrail logs. It is recommended that the bucket policy or access control list (ACL) applied to the S3 bucket that stores CloudTrail logs prevents public access. Allowing public access to CloudTrail log content may aid an adversary in identifying weaknesses in the affected account's use or configuration.

### Recommendations:

1. Sign in to the AWS Console
2. Goto S3
3. Choose the reported S3 bucket and click Properties
4. In the Properties pane, click the Permissions tab.
5. If the Edit bucket policy button is present, select it.
6. Remove any statement having an effect Set to 'Allow' and a principal set to '*'.

Note: We recommend that you do not configure CloudTrail to write into an S3 bucket that resides in a different AWS account.

# 1. Install and maintain a firewall configuration to protect cardholder data

1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.

## AWS Route53 Public Zone with Private Records

| | |
|---|---|
| Compliance Section: 1.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

A hosted zone is a container for records (An object in a hosted zone that you use to define how you want to route traffic for the domain or a subdomain), which include information about how you want to route traffic for a domain (such as example.com) and all of its subdomains (such as www.example.com, retail.example.com, and seattle.accounting.example.com). A hosted zone has the same name as the corresponding domain. A public hosted zone is a container that holds information about how you want to route traffic on the internet for a specific domain.It is best practice to avoid AWS Route 53 Public Hosted Zones containing DNS records for private IPs or resources within your AWS account to overcome information leakage of your internal network and resources.

### Recommendations:

You can not convert a public hosted zone into a private hosted zone. So, it is recommended to create and configure a Private Hosted Zone to manage private IPs within your Virtual Private Cloud (VPC) as Amazon Route 53 service will only return your private DNS records when queried from within the associated VPC, and delete the associated public hosted zone once the Private hosted zone is configured with all the records.
To create a private hosted zone using the Route 53 console:
1.For each VPC that you want to associate with the Route 53 hosted zone, change the following VPC settings to true:
'enableDnsHostnames'
'enableDnsSupport'
For more information, see Updating DNS Support (http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-dns.html#vpc-dns-updating) for Your VPC in the Amazon VPC User Guide.
2. Sign in to the AWS console
3. Go to Route 53 console
4. If you are new to Route 53, choose Get Started Now under DNS Management. If you are already using Route 53, choose Hosted Zones in the navigation pane.
5. Choose 'Create Hosted Zone'
6. In the Create Private Hosted Zone pane, enter a domain name and, optionally, a comment.
For information about how to specify characters other than a-z, 0-9, and - (hyphen) and how to specify internationalized domain names, see DNS Domain Name Format (https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/DomainNameFormat.html).
7. In the Type list, choose Private Hosted Zone for Amazon VPC
8. In the VPC ID list, choose the VPC that you want to associate with the hosted zone. If you want to associate more than one VPC with the hosted zone, you can add VPCs after you create the hosted zone.
Note: If the console displays the following message, you are trying to associate a VPC with this hosted zone that has already been associated with another hosted zone that has an overlapping namespace, such as example.com and retail.example.com:
'A conflicting domain is already associated with the given VPC or Delegation Set.'
9. Choose Create
10. To associate more VPCs with the new hosted zone, perform the following steps:
a. Choose Back to Hosted Zones.
b. Choose the radio button for the hosted zone.
c. In the right pane, in VPC ID, choose another VPC that you want to associate with the hosted zone.
d. Choose Associate New VPC.
e. Repeat steps c and d until you have associated all of the VPCs that you want to with the hosted zone.
For More Information : https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/hosted-zone-private-creating.html
To delete a public hosted zone using the Route 53 console:
1. Sign into the AWS console

2. Go Route53 console
3. Confirm that the hosted zone that you want to delete contains only an NS and an SOA record. If it contains additional records, delete them:
a. Choose the name of the hosted zone that you want to delete.
b. On the Record Sets page, if the list of records includes any records for which the value of the Type column is something other than NS or SOA, choose the row, and choose Delete Record Set. To select multiple, consecutive records, choose the first row, press and hold the Shift key, and choose the last row. To select multiple, non-consecutive records, choose the first row, press and hold the Ctrl key, and choose the remaining rows.
Note: If you created any NS records for subdomains in the hosted zone, delete those records, too.
c. Choose Back to Hosted Zones
4. On the Hosted Zones page, choose the row for the hosted zone that you want to delete.
5. Choose Delete Hosted Zone.
6. Choose OK to confirm.
7. If you want to make the domain unavailable on the internet, we recommend that you transfer DNS service to a free DNS service and then delete the Route 53 hosted zone. This prevents future DNS queries from possibly being misrouted. If the domain is registered with Route 53, see Adding or Changing Name Servers and Glue Records for a Domain (https://docs.aws.amazon.com/Route53/latest DeveloperGuide/domain-name-servers-glue-records.html) for information about how to replace Route 53 nameservers with name servers for the new DNS service. If the domain is registered with another registrar, use the method provided by the registrar to change name servers for the domain.
For More Information : https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/DeleteHostedZone.html

# 1. Install and maintain a firewall configuration to protect cardholder data

1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.

## AWS Private ECR repository policy is overly permissive

| | |
|---|---|
| Compliance Section: 1.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 2 | |

### Description:

This policy identifies AWS Private ECR repositories that have overly permissive registry policies. An ECR(Elastic Container Registry) repository is a collection of Docker images available on the AWS cloud. These images might contain sensitive information which should be restricted to unauthorized users.

### Recommendations:

1. Log in to the AWS Console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated.
3. Navigate to 'ECR' dashboard from 'Services' dropdown
4. Go to 'Repository', from the left panel
5. Select the repository for which alert is being generated
6. Select the 'Permissions' option from left menu below 'repositores'
7. Click on 'Edit policy JSON' to modify the JSON so that Principal is restrictive
8. After modifications, click on 'Save'.

# 1. Install and maintain a firewall configuration to protect cardholder data

1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.

## AWS RDS database instance is publicly accessible

| | |
|---|---|
| Compliance Section: 1.3 | First Seen: N/A |
| Resource(s) Failed: 1 | Resource Type: Other |
| Resource(s) Passed: 1 | |

### Description:

This policy identifies RDS database instances which are publicly accessible. DB instances should not be publicly accessible to protect the integrity of data. Public accessibility of DB instances can be modified by turning on or off the Public accessibility parameter.

### Resource(s) Failed:

ad1r2yeh915nzgo

### Recommendations:

1. Sign into the AWS console.
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to the 'RDS' service.
4. Select the RDS instance reported in the alert, Click on 'Modify'
5. Under 'Network and Security', update the value of 'public accessibility' to 'No' and Click on 'Continue'
6. Select required 'Scheduling of modifications' option and click on 'Modify DB Instance'

# 1. Install and maintain a firewall configuration to protect cardholder data

1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.

AWS Classic Load Balancer is in use for internet-facing applications

| | |
|---|---|
| Compliance Section: 1.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

## Description:

This policy identifies Classic Load Balancers that are being used for internet-facing HTTP/HTTPS applications. Classic Load Balancer should be used when you have an existing application running in the EC2-Classic network. Application Load Balancers (ALB) is recommended for internet-facing HTTP/HTTPS web applications. For more details: https://docs.aws.amazon.com/elasticloadbalancing/latest/application/create-application-load-balancer.html

## Recommendations:

To create Application Load Balancer (ALB) refer,
https://docs.aws.amazon.com/elasticloadbalancing/latest/application/create-application-load-balancer.html
Once Application Load Balancer created, you can delete the reported Classic Load Balancer by,

1. Log in to the AWS console
2. In the console, select the specific region from the region drop-down on the top right corner, for which the alert is generated
3. Navigate to EC2 Dashboard
4. Click on 'Load Balancers', choose the reported load balancer
5. Click on the 'Actions' and from the drop-down click on 'Delete'
6. Click on the 'Yes, Delete'

# 1. Install and maintain a firewall configuration to protect cardholder data

1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.

## AWS SageMaker notebook instance configured with direct internet access feature

| | |
|---|---|
| Compliance Section: 1.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies SageMaker notebook instances that are configured with direct internet access feature. If AWS SageMaker notebook instances are configured with direct internet access feature, any machine outside the VPC can establish a connection to these instances, which provides an additional avenue for unauthorized access to data and the opportunity for malicious activity. For more details: https://docs.aws.amazon.com/sagemaker/latest/dg/appendix-notebook-and-internet-access.html

### Recommendations:

AWS SageMaker notebook instance direct internet access feature can not be disabled; once it is created. You need to create a new notebook instance with disabled direct internet access feature; and migrate all required data from the reported notebook instance to the newly created notebook instance before you delete the reported notebook instance.
To create a New AWS SageMaker notebook instance,
1. Log in to AWS console
2. Navigate to the AWS SageMaker dashboard
3. Choose Notebook instances and then choose 'Create notebook instance'
4. On the Create notebook instance page, within the 'Network' section,
From 'VPC – optional' dropdown list, select the VPC where you want to deploy a new SageMaker notebook instance.
5. Select the 'Disable - Access the internet through a VPC' button under the 'Direct internet access' to disable direct internet access for the new notebook instance.
6. Choose other parameters as per your requirement and Click on the 'Create notebook instance' button
To delete reported notebook instance,
1. Log in to AWS console
2. Navigate to the AWS SageMaker dashboard
3. Choose Notebook instances and Choose the reported notebook instance
4. Click on the 'Actions' dropdown menu, select the 'Stop' option, and when instance stops, select the 'Delete' option.
5. Within Delete <notebook-instance-name> dialog box, click the Delete button to confirm the action.

# 1. Install and maintain a firewall configuration to protect cardholder data

1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.

## AWS S3 bucket publicly writable

| | |
|---|---|
| Compliance Section: 1.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 12 | |

### Description:

This policy identifies the S3 buckets that are publicly writable by Put/Create/Update/Replicate/Write/Delete bucket operations. These permissions permit anyone, malicious or not, to Put/Create/Update/Replicate/Write/Delete bucket operations on your S3 bucket if they can guess the namespace. S3 service does not protect the namespace if ACLs and Bucket policy is not handled properly, with this configuration you may be at risk of compromise of critical data by leaving S3 public. For more details: https://docs.aws.amazon.com/AmazonS3/latest/user-guide/set-permissions.html https://docs.aws.amazon.com/AmazonS3/latest/dev/about-object-ownership.html#ensure-object-ownership

### Recommendations:

1. Log in to the AWS Console
2. Navigate to the 'S3' service
3. Click on the S3 resource reported in the alert
4. Click on the 'Permissions' tab
5. If Access Control List is set to 'Public' follow the below steps
a. Under 'Access Control List', Click on 'Everyone' and uncheck all items
b. Click on Save changes
6. If 'Bucket Policy' is set to public follow the below steps
a. Under 'Bucket Policy', Select 'Edit Bucket Policy' and consider defining what explicit 'Principal' should have the ability to PUT/CREATE/REPLICATE/DELETE objects in your S3 bucket. You may also want to specifically limit the 'Principal' ability to perform specific PUT/CREATE/REPLICATE/DELETE functions, without the wild card.
If 'Bucket Policy' is not required delete the existing 'Bucket Policy'.
b. Click on Save changes
Note: Make sure updating 'Access Control List' or 'Bucket Policy' does not affect S3 bucket data access.

# 1. Install and maintain a firewall configuration to protect cardholder data

1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.

## AWS EKS cluster endpoint access publicly enabled

| | |
|---|---|
| Compliance Section: 1.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

When you create a new cluster, Amazon EKS creates an endpoint for the managed Kubernetes API server that you use to communicate with your cluster (using Kubernetes management tools such as kubectl). By default, this API server endpoint is public to the internet, and access to the API server is secured using a combination of AWS Identity and Access Management (IAM) and native Kubernetes Role Based Access Control (RBAC). This policy checks your Kubernetes cluster endpoint access and triggers an alert if publicly enabled.

### Recommendations:

Enable private access to the Kubernetes API server so that all communication between your worker nodes and the API server stays within your VPC. Disable public access to your API server so that it's not accessible from the internet.

1. Login to AWS Console
2. Navigate to the Amazon EKS dashboard
3. Choose the name of the cluster to display your cluster information
4. Under Networking, choose 'Manage networking'
5. Select 'Private' radio button
6. Click on 'Save changes'

# 1. Install and maintain a firewall configuration to protect cardholder data

1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.

## AWS MQ is publicly accessible

| | |
|---|---|
| Compliance Section: 1.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies the AWS MQ brokers which are publicly accessible. It is advisable to use MQ brokers privately only from within your AWS Virtual Private Cloud (VPC). Ensure that the AWS MQ brokers provisioned in your AWS account are not publicly accessible from the Internet to avoid sensitive data exposure and minimize security risks.

### Recommendations:

Note: MQ broker configuration for public access cannot be modified. In case we need to update the MQ not to be public we need to recreate it.
1. Go to AWS console
2. Navigate to service 'Amazon MQ' from the 'Services' Menu
3. From the list of 'Brokers' select the reported MQ broker
4. From 'Details' section, copy all the configuration information.
5. Within 'Users' section, locate and copy the ActiveMQ Web Console access credentials.
6. Click on 'Brokers' from left panel, click on 'Create broker'
7. Provide an unique name in field 'Broker name'
8. In 'Advanced settings' section, select 'No' for 'Public accessibility'
9. Set the new broker configuration parameters using the information copied at step no. 4
10. Set the existing ActiveMQ Web Console access credentials copied at step no. 5
11. Click on 'Create broker'
12. Once the new broker is created, you can replace the broker endpoints within your applications
To delete the publicly accessible broker,
1. select the alerted from the list of 'Brokers'
2. Click on 'Delete' button
3. When a dialog box pops up, enter the broker name to confirm and click on 'delete' button

# 1. Install and maintain a firewall configuration to protect cardholder data

1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.

## AWS Amazon Machine Image (AMI) is publicly accessible

| | |
|---|---|
| Compliance Section: 1.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: VM Image |
| Resource(s) Passed: 8 | |

### Description:

This policy identifies AWS AMIs which are owned by the AWS account and are accessible to the public. Amazon Machine Image (AMI) provides information to launch an instance in the cloud. The AMIs may contain proprietary customer information and should be accessible only to authorized internal users.

### Recommendations:

1. Login to the AWS Console and navigate to 'EC2' service.
2. In the navigation pane, choose AMIs.
3. Select your AMI from the list, and then choose Actions, Modify Image Permissions.
4. Choose Private and choose Save.

# 1. Install and maintain a firewall configuration to protect cardholder data

1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.

## AWS CloudFormation template contains globally open resources

| | |
|---|---|
| Compliance Section: 1.3 | First Seen: N/A |
| Resource(s) Failed: 1 | Resource Type: Other |
| Resource(s) Passed: 27 | |

### Description:

This alert triggers if a CloudFormation template that when launched will result in resources allowing global network access. Below are three common causes: - Security Group with a {0.0.0.0/0, ::/0} rule - Network Access Control List with a {0.0.0.0/0, ::/0} rule - Network Access Control List with -1 IpProtocol

### Resource(s) Failed:

awsjamconfig

### Recommendations:

Prisma Cloud encourages you to review the template and ensure this is the intended behavior.
1. Goto the AWS CloudFormation dashboard.
2. Click on the Stack you want to modify.
3. Select the Template tab and then View in Designer.
4. Make your template modifications.
5. Check for syntax errors in your template by choosing Validate template near the top of the page.
6. Select Save from the file (icon) menu.
7. Choose Amazon S3 bucket, name your template and Save.
8. Copy the bucket URL and click OK.
9. Select Close to close Designer.
10. Click on the Stack you want to modify.
11. From the Actions pull down menu, select Update stack
12. Choose Replace current template and paste the URL from Designer into the Amazon S3 URL field. Then click on Next.
13. Specify stack details, then click on Next.
14. Configure stack options, then click on Next.
15. Review, then select Update stack near the bottom of the page.

# 1. Install and maintain a firewall configuration to protect cardholder data

1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.

## AWS Elasticsearch domain publicly accessible

| | |
|---|---|
| Compliance Section: 1.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 1 | |

### Description:

This policy identifies Elasticsearch domains which are publicly accessible. Enabling VPCs for Elasticsearch domains provides flexibility and control over the clusters access with an extra layer of security than Elasticsearch domains that use public endpoints. It also keeps all traffic between your VPC and Elasticsearch domains within the AWS network instead of going over the public Internet.

### Recommendations:

VPC for AWS Elasticsearch domain can be set only at the time of the creation of domain. So to resolve this alert, create a new domain with VPC, then migrate all required Elasticsearch domain data from the reported Elasticsearch domain to this newly created domain and delete reported Elasticsearch domain.
To set up the new ES domain with VPC, refer the following URL:
https://docs.aws.amazon.com/elasticsearch-service/latest/developerguide/es-createupdatedomains.html
To create Elasticsearch domain within VPC, In Network configuration choose VPC access instead of Public access.
To delete reported ES domain, refer the following URL:
https://docs.aws.amazon.com/elasticsearch-service/latest/developerguide/es-gsg-deleting.html

# 1. Install and maintain a firewall configuration to protect cardholder data

1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.

## AWS S3 bucket publicly readable

| | |
|---|---|
| Compliance Section: 1.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 12 | |

### Description:

This policy identifies the S3 buckets that are publicly readable by Get/Read/List bucket operations. These permissions permit anyone, malicious or not, to Get/Read/List bucket operations on your S3 bucket if they can guess the namespace. S3 service does not protect the namespace if ACLs and Bucket policy is not handled properly, with this configuration you may be at risk of compromise of critical data by leaving S3 public. For more details: https://docs.aws.amazon.com/AmazonS3/latest/user-guide/set-permissions.html https://docs.aws.amazon.com/AmazonS3/latest/dev/about-object-ownership.html#ensure-object-ownership

### Recommendations:

1. Log in to the AWS Console
2. Navigate to the 'S3' service
3. Click on the S3 resource reported in the alert
4. Click on the 'Permissions' tab
5. If Access Control List is set to 'Public' follow the below steps
a. Under 'Access Control List', Click on 'Everyone' and uncheck all items
b. Click on Save changes
6. If 'Bucket Policy' is set to public follow the below steps
a. Under 'Bucket Policy', Select 'Edit Bucket Policy' and consider defining what explicit 'Principal' should have the ability to GET/LIST objects in your S3 bucket. You may also want to specifically limit the 'Principal' ability to perform specific GET/LIST functions, without the wild card.
If 'Bucket Policy' is not required delete the existing 'Bucket Policy'.
b. Click on Save changes
Note: Make sure updating 'Access Control List' or 'Bucket Policy' does not affect S3 bucket data access.

# 1. Install and maintain a firewall configuration to protect cardholder data

1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.

## AWS Elastic Load Balancer (ELB) has security group with no outbound rules

| | |
|---|---|
| Compliance Section: 1.3.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 32 | |

### Description:

This policy identifies Elastic Load Balancers (ELB) which have security group with no outbound rules. A security group with no outbound rule will deny all outgoing requests. ELB security groups should have at least one outbound rule, ELB with no outbound permissions will deny all traffic going to any EC2 instances or resources configured behind that ELB; in other words, the ELB is useless without outbound permissions.

### Recommendations:

1. Log in to the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to EC2 Dashboard
4. Click on 'Load Balancers', choose the reported load balancer
5. Click on the 'Description' tab, click on the security group, it will open Security Group properties in a new tab in your browser
6. Click on the 'Outbound Rules'
7. If there are no rules, click on 'Edit rules', add an outbound rule according to your ELB functional requirement
8. Click on 'Save'

# 1. Install and maintain a firewall configuration to protect cardholder data

1.3.5 Permit only “established” connections into the network.

## Instances exposed to network traffic from the internet

| | |
|---|---|
| Compliance Section: 1.3.5 | First Seen: N/A |
| Resource(s) Failed: 5 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies network traffic coming from the internet to sensitive cloud workloads. Cloud workloads should have appropriate Security Groups and ACLs in place so that only external facing workloads such as load balancers, web servers, bastion hosts are exposed to the internet. Cloud workloads with internet exposure are vulnerable to external threats. Note: This policy alerts AWS and GCP workloads correctly and for Azure, it may trigger alerts for NAT Gateway configured resources also.

### Resource(s) Failed:

PANW-WindowsBastionServer-awsjamconfig, eni-08ed2d71b4d68332d, PANW-WebServer-awsjamconfig, eni-00ba3b413a9e8a932, LinuxBastion

### Recommendations:

1. Log in to the Cloud Console
2. Search for the resource reported in the alert
3. Check if the Security Group/Firewall Rule of the resource indeed allows connections from the internet
4. Assign another Security Group/Firewall Rule to the resource that has a more restrictive ACL, which does not permit connection from the internet

# 1. Install and maintain a firewall configuration to protect cardholder data

1.3.6 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.

## AWS ElastiCache cluster not associated with VPC

| | |
|---|---|
| Compliance Section: 1.3.6 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 1 | |

### Description:

This policy identifies ElastiCache Clusters which are not associated with VPC. It is highly recommended to associate ElastiCache with VPC, as provides virtual network in your own logically isolated area and features such as selecting IP address range, creating subnets, and configuring route tables, network gateways, and security settings. NOTE: If you created your AWS account before 2013-12-04, you might have support for the EC2-Classic platform in some regions. AWS has deprecated the use of Amazon EC2-Classic for launching ElastiCache clusters. All current generation nodes are launched in Amazon Virtual Private Cloud only. So this policy only applies legacy ElastiCache clusters which are created using EC2-Classic.

### Recommendations:

AWS ElastiCache cluster VPC association can be done only at the time of the creation of the cluster. So to fix this alert, create a new cluster with VPC, then migrate all required ElastiCache cluster data from the reported ElastiCache cluster to this newly created cluster and delete reported ElastiCache cluster.

To create new ElastiCache cluster with at-rest encryption set, perform the following:

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to ElastiCache Dashboard
4. Click on Redis or Memcached based on your requirement
5. Choose cluster parameters as per your requirement
6. Click on 'Advanced Redis settings' to expand the cluster advanced settings panel
7. Select desired VPC for 'Subnet group' along with other parameters

NOTE: If you don't specify a subnet when you launch a cluster, the cluster launches into your default Amazon VPC.

8. Click on 'Create' button to launch your new ElastiCache cluster

To delete reported ElastiCache cluster, perform the following:

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to ElastiCache Dashboard
4. Select reported cluster
5. Click on 'Delete' button
6. In the 'Delete Cluster' dialog box, if you want a backup for your cluster select 'Yes' from the 'Create final backup' dropdown menu, provide a name for the cluster backup, then click on 'Delete'.

# 1. Install and maintain a firewall configuration to protect cardholder data

1.3.6 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.

## AWS SageMaker notebook instance is not placed in VPC

| | |
|---|---|
| Compliance Section: 1.3.6 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies SageMaker notebook instances that are not placed inside a VPC. It is recommended to place your SageMaker inside VPC so that VPC-only resources able to access your SageMaker data, which cannot be accessed outside a VPC network. For more details: https://docs.aws.amazon.com/sagemaker/latest/dg/process-vpc.html

### Recommendations:

AWS SageMaker notebook instance can be not placed in VPC once it is created. You need to create a new notebook instance placing it in VPC; migrate all required data from the reported notebook instance to the newly created notebook instance before you delete the reported notebook instance.
To create a New AWS SageMaker notebook instance,
1. Log in to AWS console
2. Navigate to the AWS SageMaker dashboard
3. Choose Notebook instances and then choose 'Create notebook instance'
4. On the Create notebook instance page, within the 'Network' section,
From the 'VPC – optional' dropdown list, select the VPC where you want to deploy a new SageMaker notebook instance.
5. Choose other parameters as per your requirement and click on the 'Create notebook instance' button
To delete reported notebook instance,
1. Log in to AWS console
2. Navigate to the AWS SageMaker dashboard
3. Choose Notebook instances and Choose the reported notebook instance
4. Click on the 'Actions' dropdown menu, select the 'Stop' option, and when instance stops, select the 'Delete' option.
5. Within Delete <notebook-instance-name> dialog box, click the Delete button to confirm the action.

# 1. Install and maintain a firewall configuration to protect cardholder data

1.3.6 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.

## AWS VPC allows unauthorized peering

| | |
|---|---|
| Compliance Section: 1.3.6 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 29 | |

### Description:

This policy identifies the VPCs which have unauthorized peering. The recommended best practice is to disallow VPC peering between two VPCs from different AWS accounts, as this potentially enables unauthorized access to private resources.

### Recommendations:

1. Sign in to the AWS Console
2. Go to AWS VPC console at https://console.aws.amazon.com/vpc/
3. In the left navigation panel, select Peering Connection
4. Choose the reported Peering Connection
5. Click on Actions and select 'Delete VPC Peering Connection'
6. click on Yes, Delete

# 1. Install and maintain a firewall configuration to protect cardholder data

1.3.7 Do not disclose private IP addresses and routing information to unauthorized parties.

## AWS RDS instance not in private subnet

| | |
|---|---|
| Compliance Section: 1.3.7 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 28 | |

### Description:

This policy identifies AWS RDS instance which are not in a private subnet. RDS should not be deployed in a public subnet, production databases should be located behind a DMZ in a private subnet with limited access in most scenarios.

### Recommendations:

To resolve this alert, you should redeploy RDS into a private RDS Subnet group.
Note: You can not move an existing RDS instance from one subnet to another.
Create a RDS Subnet group:
A DB subnet group is a collection of subnets (typically private) that you create for a VPC and that you then designate for your DB instances.
1. Open the Amazon RDS console
2. In the navigation pane, choose 'Subnet groups'
3. Choose 'Create DB Subnet Group'
4. Type the 'Name' of your DB subnet group
5. Add a 'Description' for your DB subnet group
6. Choose your 'VPC'
7. Choose 'Availability Zones'
8. In the Add subnets section, add your Private subnets related to this VPC
9. Choose Create
When creating your RDS DB, under Configure advanced settings, choose the Subnet group created above.

# 2. Do not use vendor-supplied defaults for system passwords and other security parameters

2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.).

## AWS EKS cluster using the default VPC

| | |
|---|---|
| Compliance Section: 2.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 20 | |

### Description:

This policy identifies AWS EKS clusters which are configured with the default VPC. It is recommended to use a VPC configuration based on your security and networking requirements. You should create your own EKS VPC instead of using the default, so that you can have full control over the cluster network.

### Recommendations:

An AWS EKS cluster VPC cannot be changed once it is created. To resolve this alert, create a new cluster with the custom VPC as per your requirements, then migrate all required cluster data from the reported cluster to this newly created cluster and delete the reported Kubernetes cluster.

1. Open the Amazon EKS dashboard.
2. Choose Create cluster.
3. On the Create cluster page, fill in the following fields:
- Cluster name
- Kubernetes version
- Role name
- VPC - Choose your new custom VPC.
- Subnets
- Security Groups
- Endpoint private access
- Endpoint public access
- Logging
4. Choose Create.

# 2. Do not use vendor-supplied defaults for system passwords and other security parameters

2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.).

## AWS NAT Gateways are not being utilized for the default route

| | |
|---|---|
| Compliance Section: 2.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 27 | |

### Description:

This policy identifies Route Tables which have NAT instances for the default route instead of NAT gateways. It is recommended to use NAT gateways as the AWS managed NAT Gateway provides a scalable and resilient method for allowing outbound internet traffic from your private VPC subnets.

### Recommendations:

To create a NAT gateway:
1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to VPC Dashboard
4. In the navigation pane, choose 'NAT Gateways'
5. Click on 'Create NAT Gateway', Specify the subnet in which to create the NAT gateway, and select the allocation ID of an Elastic IP address to associate with the NAT gateway. When you're done, Click on 'Create a NAT Gateway'. The NAT gateway displays in the console. After a few moments, its status changes to Available, after which it's ready for you to use.

To update Route Table:
After you've created your NAT gateway, you must update your route tables for your private subnets to point internet traffic to the NAT gateway. We use the most specific route that matches the traffic to determine how to route the traffic.
1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to VPC Dashboard
4. In the navigation pane, choose 'Route Tables'
5. Select the reported route table associated with your private subnet
6. Choose 'Routes' and Click on 'Edit routes'
7. Replace the current route that points to the NAT instance with a route to the NAT gateway
8. Click on 'Save routes'

# 2. Do not use vendor-supplied defaults for system passwords and other security parameters

2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.).

## AWS CloudFront web distribution using insecure TLS version

| | |
|---|---|
| Compliance Section: 2.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 2 | |

### Description:

This policy identifies AWS CloudFront web distributions which are configured with TLS versions for HTTPS communication between viewers and CloudFront. As a best practice, use recommended TLSv1.2_2021 as the minimum protocol version in your CloudFront distribution security policies.

### Recommendations:

1. Sign in to the AWS console
2. Navigate to CloudFront Distributions Dashboard
3. Click on the reported distribution
4. On 'General' tab, Click on 'Edit' button under 'Settings'
5. On 'Edit Distribution' page, Set 'Security Policy' to TLSv1.2_2021
6. Click on 'Save changes'

# 2. Do not use vendor-supplied defaults for system passwords and other security parameters

2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.).

## AWS CloudFront web distribution with default SSL certificate

| | |
|---|---|
| Compliance Section: 2.1 | First Seen: N/A |
| Resource(s) Failed: 2 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies CloudFront web distributions which have a default SSL certificate to access CloudFront content. It is a best practice to use custom SSL Certificate to access CloudFront content. It gives you full control over the content data. custom SSL certificates also allow your users to access your content by using an alternate domain name. You can use a certificate stored in AWS Certificate Manager (ACM) or you can use a certificate stored in IAM.

### Resource(s) Failed:

d2rwvuyjsg9kf7.cloudfront.net, d2u45drmoykiua.cloudfront.net

### Recommendations:

1. Sign in to the AWS console
2. Select the region, from the region drop-down, in which the alert is generated
3. Navigate to CloudFront Distributions Dashboard
4. Click on the reported distribution
5. On the 'General' tab, Click on the 'Edit' button
6. On 'Edit Distribution' page set 'SSL Certificate' to 'Custom SSL Certificate (example.com):', Select a certificate or type your certificate ARN in the field and other parameters as per your requirement.
7. Click on 'Yes, Edit'

# 2. Do not use vendor-supplied defaults for system passwords and other security parameters

2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.).

## AWS Elastic Load Balancer v2 (ELBv2) listener that allow connection requests over HTTP

| | |
|---|---|
| Compliance Section: 2.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies Elastic Load Balancers v2 (ELBv2) listener that are configured to accept connection requests over HTTP instead of HTTPS. As a best practice, use the HTTPS protocol to encrypt the communication between the application clients and the application load balancer.

### Recommendations:

1. Sign in to the AWS console
2. Select the region, from the region drop-down, in which the alert is generated
3. Navigate to EC2 dashboard
4. Click on 'Load Balancers' (Left Panel)
5. Select the reported ELB
6. Click on 'Listeners' tab
7.'Edit' the 'Listener ID' rule that uses HTTP
8. Select 'HTTPS' in the 'Protocol : port' section, Choose appropriate Default action, Security policy and Default SSL certificate parameters as per your requirement.
9. Click on 'Update'

# 2. Do not use vendor-supplied defaults for system passwords and other security parameters

2.3 Encrypt all non-console administrative access using strong cryptography.

## AWS CloudFront origin protocol policy does not enforce HTTPS-only

| | |
|---|---|
| Compliance Section: 2.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 2 | |

### Description:

This policy identifies AWS CloudFront which has an origin protocol policy that does not enforce HTTPS-only. Enforcing HTTPS protocol policy between origin and CloudFront will encrypt all communication and will be more secure. As a security best practice, enforce HTTPS-only traffic between a CloudFront distribution and the origin.

### Recommendations:

Communication between CloudFront and your Custom Origin should enforce HTTPS-only traffic. Modify the CloudFront Origin's Origin Protocol Policy to HTTPS only.

1. Go to the AWS console CloudFront dashboard.
2. Select your distribution Id.
3. Select the 'Origins' tab.
4. Check the origin you want to modify then select Edit.
5. Change the Origin Protocol Policy to 'https-only.'
6. Select 'Yes, Edit.'

# 2. Do not use vendor-supplied defaults for system passwords and other security parameters

2.3 Encrypt all non-console administrative access using strong cryptography.

## AWS Glue connection do not have SSL configured

| | |
|---|---|
| Compliance Section: 2.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies the Glue connections that are not configured with SSL to encrypt connections. It is recommended to use an SSL connection with hostname matching is enforced for the DB connection on the client; enforcing SSL connections help protect against 'man in the middle' attacks by encrypting the data stream between connections.

### Recommendations:

1. Log in to the AWS Console
2. In the console, select the specific region from the region drop-down on the top right corner, for which the alert is generated
3. Navigate to AWS Glue service
4. Click on 'Connections', Click on the reported Connection
5. Click on 'Edit'
6. On the 'Edit connection' page, Select 'Require SSL connection'
7. Click on 'Next'
8. Click on 'Finish'

# 2. Do not use vendor-supplied defaults for system passwords and other security parameters

2.3 Encrypt all non-console administrative access using strong cryptography.

## AWS Elastic Load Balancer v2 (ELBv2) SSL negotiation policy configured with weak ciphers

| | |
|---|---|
| Compliance Section: 2.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies Elastic Load Balancers v2 (ELBv2) which are configured with SSL negotiation policy containing weak ciphers. An SSL cipher is an encryption algorithm that uses encryption keys to create a coded message. SSL protocols use several SSL ciphers to encrypt data over the Internet. As many of the other ciphers are not secure/weak, it is recommended to use only the ciphers recommended in the following AWS link: https://docs.aws.amazon.com/elasticloadbalancing/latest/application/create-https-listener.html

### Recommendations:

1. Log in to the AWS console
2. In the console, select the specific region from the region drop-down on the top right corner, for which the alert is generated
3. Go to the EC2 Dashboard, and select 'Load Balancers'
4. Click on the reported Load Balancer
5. On the 'Listeners' tab, Choose the 'HTTPS' or 'SSL' rule; Click on 'Edit', Change 'Security policy' to other than 'ELBSecurityPolicy-TLS-1-0-2015-04' as it contains DES-CBC3-SHA cipher, which is a weak cipher.
6. Click on 'Update' to save your changes.

# 2. Do not use vendor-supplied defaults for system passwords and other security parameters

2.3 Encrypt all non-console administrative access using strong cryptography.

## AWS Elastic Load Balancer (Classic) SSL negotiation policy configured with vulnerable SSL protocol

| | |
|---|---|
| Compliance Section: 2.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies Elastic Load Balancers (Classic) which are configured with SSL negotiation policy containing vulnerable SSL protocol. The SSL protocol establishes a secure connection between a client and a server and ensures that all the data passed between the client and your load balancer is private. As a security best practice, it is recommended to use the latest version SSL protocol.

### Recommendations:

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to EC2 Dashboard
4. Click on 'Load Balancers' (Left Panel)
5. Click on the reported Load Balancer
6. On 'Listeners' tab, Click on 'Edit' button
7. On 'Edit Listeners' popup for rule 'HTTPS/SSL',
- If your cipher is 'Predefined Security Policy', change 'Cipher' to 'ELBSecurityPolicy-TLS-1-2-2017-01 or latest'
OR
- If your cipher is 'Custom Security Policy', Choose 'Protocol-TLSv1.2' only on 'SSL Protocols' section
8. Click on 'Save'

# 2. Do not use vendor-supplied defaults for system passwords and other security parameters

2.3 Encrypt all non-console administrative access using strong cryptography.

## AWS S3 bucket not configured with secure data transport policy

| | |
|---|---|
| Compliance Section: 2.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 12 | |

### Description:

This policy identifies S3 buckets which are not configured with secure data transport policy. AWS S3 buckets should enforce encryption of data over the network using Secure Sockets Layer (SSL). It is recommended to add a bucket policy that explicitly denies (Effect: Deny) all access (Action: s3:*) from anybody who browses (Principal: *) to Amazon S3 objects within an Amazon S3 bucket if they are not accessed through HTTPS (aws:SecureTransport: false).

### Recommendations:

1. Sign into the AWS console
2. Navigate to Amazon S3 Dashboard
3. Click on 'Buckets' (Left Panel)
4. Choose the reported S3 bucket
5. On 'Permissions' tab, Click on 'Bucket Policy'
6. Add a bucket policy that explicitly denies (Effect: Deny) all access (Action: s3:) from anybody who browses (Principal: ) to Amazon S3 objects within an Amazon S3 bucket if they are not accessed through HTTPS (aws:SecureTransport: false). Below is the sample policy:

```
{
"Sid": "ForceSSLOnlyAccess",
"Effect": "Deny",
"Principal": "*",
"Action": "s3:GetObject",
"Resource": "arn:aws:s3:::bucket_name/*",
"Condition": {
"Bool": {
"aws:SecureTransport": "false"
}
}
}
```

# 2. Do not use vendor-supplied defaults for system passwords and other security parameters

2.3 Encrypt all non-console administrative access using strong cryptography.

## AWS CloudFront distribution is using insecure SSL protocols for HTTPS communication

| | |
|---|---|
| Compliance Section: 2.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 2 | |

### Description:

CloudFront, a content delivery network (CDN) offered by AWS, is not using a secure cipher for distribution. It is a best security practice to enforce the use of secure ciphers TLSv1.0, TLSv1.1, and/or TLSv1.2 in a CloudFront Distribution's certificate configuration. This policy scans for any deviations from this practice and returns the results.

### Recommendations:

Communication between CloudFront and your Custom Origin should enforce the use of secure ciphers. Modify the CloudFront Origin's Origin SSL Protocol to include TLSv1.0, TLSv1.1, and/or TLSv1.2.

1. Go to the AWS console CloudFront dashboard.
2. Select your distribution Id.
3. Select the 'Origins' tab.
4. Check the origin you want to modify then select Edit.
5. Remove (uncheck) 'SSLv3' from Origin SSL Protocols.
6. Select 'Yes, Edit.'

# 2. Do not use vendor-supplied defaults for system passwords and other security parameters

2.3 Encrypt all non-console administrative access using strong cryptography.

## AWS Database Migration Service endpoint do not have SSL configured

| | |
|---|---|
| Compliance Section: 2.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies Database Migration Service (DMS) endpoints that are not configured with SSL to encrypt connections for source and target endpoints. It is recommended to use SSL connection for source and target endpoints; enforcing SSL connections help protect against 'man in the middle' attacks by encrypting the data stream between endpoint connections. NOTE: Not all databases use SSL in the same way. An Amazon Redshift endpoint already uses an SSL connection and does not require an SSL connection set up by AWS DMS. So there are some exlcusions included in policy RQL to report only those endpoints which can be configured using DMS SSL feature. For more details: https://docs.aws.amazon.com/dms/latest/userguide/CHAP_Security.html#CHAP_Security.SSL

### Recommendations:

1. Log in to the AWS Console
2. Navigate to the AWS DMS dashboard
3. In the navigation pane, choose 'Endpoints'
4. Select the reported DMS endpoint
5. Under 'Actions', choose 'Modify'
6. In the 'Endpoint configuration' section, select the 'Secure Socket Layer (SSL) mode' from the dropdown list select suitable SSL mode according to your requirement other than 'none'.
7. Click on 'Save'

NOTE: Before modifying the SSL setting, you should be configured with the proper certificate you want to use for SSL connection under the DMS 'Certificate' service.

# 2. Do not use vendor-supplied defaults for system passwords and other security parameters

2.3 Encrypt all non-console administrative access using strong cryptography.

## AWS Elastic Load Balancer with listener TLS/SSL is not configured

| | |
|---|---|
| Compliance Section: 2.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Managed Load Balancer |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies AWS Elastic Load Balancers which have non-secure listeners. As Load Balancers will be handling all incoming requests and routing the traffic accordingly. The listeners on the load balancers should always receive traffic over secure channel with a valid SSL certificate configured.

### Recommendations:

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to EC2 dashboard
4. Click on 'Load Balancers' (Left Panel)
5. Select the reported ELB
6. On the Listeners tab, Click the 'Edit' button under the available listeners
7. In the Load Balancer Protocol, Select 'HTTPS (Secure HTTP)' or 'SSL (Secure TCP)'
8. In the SSL Certificate column, click 'Change'
9. On 'Select Certificate' popup dialog, Choose a certificate from ACM or IAM or upload a new certificate based on requirement and Click on 'Save'
10. Back to the 'Edit listeners' dialog box, review the secure listeners configuration, then click on 'Save'

# 2. Do not use vendor-supplied defaults for system passwords and other security parameters

2.3 Encrypt all non-console administrative access using strong cryptography.

## AWS Redshift does not have require_ssl configured

| | |
|---|---|
| Compliance Section: 2.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Managed Database |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies Redshift databases in which data connection to and from is occurring on an insecure channel. SSL connections ensures the security of the data in transit.

### Recommendations:

1. Login to the AWS and navigate to the 'Amazon Redshift' service.
2. Expand the identified 'Redshift' cluster and make a note of the 'Cluster Parameter Group'
3. In the navigation panel, click on the 'Parameter group'.
4. Select the identified 'Parameter Group' and click on 'Edit Parameters'.
5. Review the require_ssl flag. Update the parameter 'require_ssl' to true and save it.

Note: If the current parameter group is a Default parameter group, it cannot be edited. You will need to create a new parameter group and point it to an affected cluster.

# 2. Do not use vendor-supplied defaults for system passwords and other security parameters

2.3 Encrypt all non-console administrative access using strong cryptography.

## AWS Elastic Load Balancer (Classic) SSL negotiation policy configured with insecure ciphers

| | |
|---|---|
| Compliance Section: 2.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies Elastic Load Balancers (Classic) which are configured with SSL negotiation policy containing insecure ciphers. An SSL cipher is an encryption algorithm that uses encryption keys to create a coded message. SSL protocols use several SSL ciphers to encrypt data over the Internet. As many of the other ciphers are not secure, it is recommended to use only the ciphers recommended in the following AWS link: https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-ssl-security-policy.html.

### Recommendations:

1. Sign in to the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Go to the EC2 Dashboard, and select 'Load Balancers'
4. Click on the reported Load Balancer
5. On 'Listeners' tab, Change the cipher for the 'HTTPS/SSL' rule
For a 'Predefined Security Policy', change 'Cipher' to 'ELBSecurityPolicy-TLS-1-2-2017-01' or latest
For a 'Custom Security Policy', select from the secure ciphers as recommended in the below AWS link:
https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-ssl-security-policy.html
6. 'Save' your changes

# 3. Protect stored cardholder data

3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes.

## AWS RDS instance without Automatic Backup setting

| | |
|---|---|
| Compliance Section: 3.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 2 | |

### Description:

This policy identifies RDS instances which are not set with the Automatic Backup setting. If Automatic Backup is set, RDS creates a storage volume snapshot of your DB instance, backing up the entire DB instance and not just individual databases which provide for point-in-time recovery. The automatic backup will happen during the specified backup window time and keeps the backups for a limited period of time as defined in the retention period. It is recommended to set Automatic backups for your critical RDS servers that will help in the data restoration process.

### Recommendations:

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to Amazon RDS console
4. Choose Instances, and then select the reported DB instance
5. On 'Instance Actions' drop-down list, choose 'Modify'
6. In 'Backup' section,
a. From the 'Backup Retention Period' drop-down list, select the number of days you want RDS should retain automatic backups of this DB instance
b. Choose 'Start Time' and 'Duration' in 'Backup window' which is the daily time range (in UTC) during which automated backups created
7. Click on 'Continue'
8. On the confirmation page, choose 'Modify DB Instance' to save your changes

# 3. Protect stored cardholder data

3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes.

## AWS RDS retention policy less than 7 days

| | |
|---|---|
| Compliance Section: 3.1 | First Seen: N/A |
| Resource(s) Failed: 2 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

RDS Retention Policies for Backups are an important part of your DR/BCP strategy. Recovering data from catastrophic failures, malicious attacks, or corruption often requires a several day window of potentially good backup material to leverage. As such, the best practice is to ensure your RDS clusters are retaining at least 7 days of backups, if not more (up to a maximum of 35).

### Resource(s) Failed:

ad1r2yeh915nzgo, bookstoreneptunedb-bhpb9s1h0ck7

### Recommendations:

Configure your RDS backup retention policy to at least 7 days.
1. Go to the AWS console RDS dashboard.
2. In the navigation pane, choose Instances.
3. Select the database instance you wish to configure.
4. Click on 'Modify'.
5. Scroll down to Additional Configuration and set the retention period to at least 7 days under 'Backup retention period'.
6. Click Continue.
7. Under 'Scheduling of modifications' choose 'When to apply modifications'
8. On the confirmation page, Review the changes and Click on 'Modify DB Instance' to save your changes.

# 3. Protect stored cardholder data

3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.

## AWS RDS instance is not encrypted

| | |
|---|---|
| Compliance Section: 3.4.1 | First Seen: N/A |
| Resource(s) Failed: 2 | Resource Type: Managed Database |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies AWS RDS instances which are not encrypted. Amazon Relational Database Service (Amazon RDS) is a web service that makes it easier to set up and manage databases. Amazon allows customers to turn on encryption for RDS which is recommended for compliance and security reasons.

### Resource(s) Failed:

ad1r2yeh915nzgo, bookstoreneptunedb-bhpb9s1h0ck7

### Recommendations:

Amazon RDS instance can only be encrypted at the time of DB instance creation. So to resolve this alert, create a new DB instance with encryption and then migrate all required DB instance data from the reported DB instance to this newly created DB instance.
To create RDS DB instance with encryption, follow the instructions mentioned in below reference link based on your Database vendor:
http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html

# 3. Protect stored cardholder data

3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.

## AWS Redshift instances are not encrypted

| | |
|---|---|
| Compliance Section: 3.4.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Managed Database |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies AWS Redshift instances which are not encrypted. These instances should be encrypted for clusters to help protect data at rest which otherwise can result in a data breach.

### Recommendations:

To enable encryption on your Redshift cluster follow the steps mentioned in below URL:
https://docs.aws.amazon.com/redshift/latest/mgmt/changing-cluster-encryption.html

# 3. Protect stored cardholder data

3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.

## AWS Elastic File System (EFS) with encryption for data at rest is disabled

| | |
|---|---|
| Compliance Section: 3.4.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies Elastic File Systems (EFSs) for which encryption for data at rest is disabled. It is highly recommended to implement at-rest encryption in order to prevent unauthorized users from reading sensitive data saved to EFSs.

### Recommendations:

AWS EFS Encryption of data at rest can only be enabled during file system creation. So to resolve this alert, create a new EFS with encryption enabled, then migrate all required file data from the reported EFS to this newly created EFS and delete reported EFS.
To create a new EFS with encryption enabled, perform the following:
1. Sign in to the AWS console
2. In the console, select the specific region from the region drop-down on the top right corner, for which the alert is generated
3. Navigate to the EFS dashboard
4. Click on 'File systems' (Left Panel)
5. Click on the 'Create file system' button
6. On the 'Create file system' pop-up window,
7. Click on 'Customize' button to replicate the configurations of alerted file system as required
8. Ensure 'Enable encryption of data at rest' is selected
9. On the 'Review and create' step, Review all your setting and click on the 'Create' button
To delete reported EFS which does not has encryption, perform the following:
1. Sign in to the AWS console
2. In the console, select the specific region from the region drop-down on the top right corner, for which the alert is generated
3. Navigate to the EFS dashboard
4. Click on 'File systems' (Left Panel)
5. Select the reported file system
6. Click on 'Delete' button
7. In the 'Delete file system' popup box, To confirm the deletion enter the file system's ID and Click on 'Confirm'

# 3. Protect stored cardholder data

3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.

## AWS EMR cluster is not enabled with local disk encryption using Custom key provider

| | |
|---|---|
| Compliance Section: 3.4.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies AWS EMR clusters that are not enabled with local disk encryption using Custom key provider. Applications using the local file system on each cluster instance for intermediate data throughout workloads, where data could be spilled to disk when it overflows memory. With Local disk encryption at place, data at rest can be protected.

### Recommendations:

1. Login to the AWS Console.
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated.
3. Navigate to 'EMR' dashboard from 'Services' dropdown.
4. Go to 'Security configurations', click 'Create'.
5. On the Create security configuration window,
6. In 'Name' box, provide a name for the new EMR security configuration.
7. Under 'Local disk encryption', check the box 'Enable at-rest encryption for local disks'.
8. Select 'Custom' Key provider type from the 'Key provider type' dropdown list.
9. Follow the below link for creating the custom key,
https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-data-encryption-options.html
10. Click on 'Create' button.
11. On the left menu of EMR dashboard Click 'Clusters'.
12. Select the EMR cluster for which the alert has been generated and click on the 'Clone' button from the top menu.
13. In the Cloning popup, choose 'Yes' and Click 'Clone'.
14. On the Create Cluster page, in the Security Options section, click on 'security configuration'.
15. From the 'Security configuration' drop down select the name of the security configuration created at step 4 to step 8, click 'Create Cluster'.
16. Once the new cluster is set up verify its working and terminate the source cluster.
17. On the left menu of EMR dashboard Click 'Clusters', from the list of clusters select the source cluster which is alerted.
18. Click on the 'Terminate' button from the top menu.
19. On the 'Terminate clusters' pop-up, click 'Terminate'.

# 3. Protect stored cardholder data

3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.

## AWS RDS DB snapshot is not encrypted

| | |
|---|---|
| Compliance Section: 3.4.1 | First Seen: N/A |
| Resource(s) Failed: 5 | Resource Type: Other |
| Resource(s) Passed: 3 | |

### Description:

This policy identifies AWS RDS DB (Relational Database Service Database) cluster snapshots which are not encrypted. It is highly recommended to implement encryption at rest when you are working with production data that have sensitive information, to protect from unauthorized access.

### Resource(s) Failed:

jamconfig-snapshot-dbinstance-17osfvyiwgxml, rds:ad1r2yeh915nzgo-2023-01-18-06-15, rds:ad1r2yeh915nzgo-2023-01-17-06-15, rds:ad1r2yeh915nzgo-2023-01-19-06-15, jamconfig-snapshot-dbinstance-1ds57t6h47se4

### Recommendations:

You can encrypt a copy of an unencrypted snapshot. This way, you can quickly add encryption to a previously unencrypted DB instance.
Follow below steps to encrypt a copy of an unencrypted snapshot:
1. Log in to the AWS Console.
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated.
3. Navigate to 'RDS' dashboard from 'Services' dropdown.
4. Click on 'Snapshot' from left menu.
5. Select the alerted snapshot
6. From 'Action' dropdown, select 'Copy Snapshot'
7. In 'Settings' section, from 'Destination Region' select a region,
8. Provide an identifier for the new snapshot in field 'New DB Snapshot Identifier'
9.In 'Encryption' section, select 'Enable Encryption'
10. Select a master key for encryption from the dropdown 'Master key'.
11. Click on 'Copy Snapshot'.
The source snapshot needs to be removed once the copy is available.
Note: If you delete a source snapshot before the target snapshot becomes available, the snapshot copy may fail. Verify that the target snapshot has a status of AVAILABLE before you delete a source snapshot.

# 3. Protect stored cardholder data

3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.

## AWS Kinesis streams encryption using default KMS keys instead of Customer's Managed Master Keys

| | |
|---|---|
| Compliance Section: 3.4.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 3 | |

### Description:

This policy identifies the AWS Kinesis streams which are encrypted with default KMS keys and not with Master Keys managed by Customer. It is a best practice to use customer managed Master Keys to encrypt your Amazon Kinesis streams data. It gives you full control over the encrypted data.

### Recommendations:

1. Sign in to the AWS Console
2. Go to Kinesis Service
3. Select the reported Kinesis data stream for the corresponding region
4. Under Server-side encryption, Click on Edit
5. Choose Enabled
6. Under KMS master key, You can choose any KMS other than the default (Default) aws/kinesis
7. Click Save

# 3. Protect stored cardholder data

3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.

## AWS SageMaker notebook instance not configured with data encryption at rest using KMS key

| | |
|---|---|
| Compliance Section: 3.4.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies SageMaker notebook instances that are not configured with data encryption at rest using the AWS managed KMS key. It is recommended to implement encryption at rest in order to protect data from unauthorized entities. For more details: https://docs.aws.amazon.com/sagemaker/latest/dg/encryption-at-rest.html

### Recommendations:

AWS SageMaker notebook instance can not be configured with data encryption at rest once it is created. You need to create a new notebook instance with encryption at rest using the KMS key; migrate all required data from the reported notebook instance to the newly created notebook instance before you delete the reported notebook instance.

To create a New AWS SageMaker notebook instance,

1. Log in to AWS console
2. Navigate to the AWS SageMaker dashboard
3. Choose Notebook instances and then choose 'Create notebook instance'
4. On the Create notebook instance page, From the 'Permissions and encryption' section,
select the KMS key from the 'Encryption key - optional' dropdown list. If no KMS keys already, you have to create a KMS key first.
5. Choose other parameters as per your requirement and click on the 'Create notebook instance' button

To delete reported notebook instance,

1. Log in to AWS console
2. Navigate to the AWS SageMaker dashboard
3. Choose Notebook instances and Choose the reported notebook instance
4. Click on the 'Actions' dropdown menu and, select the 'Stop' option, and when instance stops, select the 'Delete' option.
5. Within Delete <notebook-instance-name> dialog box, click the Delete button to confirm the action.

# 3. Protect stored cardholder data

3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.

## AWS EMR cluster is not configured with CSE CMK for data at rest encryption (Amazon S3 with EMRFS)

| | |
|---|---|
| Compliance Section: 3.4.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies EMR clusters which are not configured with Client Side Encryption with Customer Master Keys(CSE CMK) for data at rest encryption of Amazon S3 with EMRFS. As a best practice, use Customer Master Keys (CMK) to encrypt the data in your EMR cluster and ensure full control over your data.

### Recommendations:

1. Log in to the AWS Console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to 'EMR' dashboard from 'Services' dropdown
4. Go to 'Security configurations', click 'Create'
5. On the Create security configuration window,
6. In 'Name' box, provide a name for the new EMR security configuration.
7. For encryption At Rest click the checkbox for 'Enable at-rest encryption for EMRFS data in Amazon S3'.
8. From the dropdown 'Default encryption mode' select 'CSE-Custom'. Follow below link for configuration steps.
https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-encryption-enable.html
9. Click on 'Create' button
10. On the left menu of EMR dashboard Click 'Clusters'
11. Select the EMR cluster for which the alert has been generated and click on the 'Clone' button from the top menu
12. In the Cloning popup, choose 'Yes' and Click 'Clone'.
13. On the Create Cluster page, in the Security Options section, click on 'security configuration'
14. From the 'Security configuration' drop down select the name of the security configuration created at step 4 to step 8, click 'Create Cluster'
15. Once you the new cluster is set up verify its working and terminate the source cluster in order to stop incurring charges for it.
16. On the left menu of EMR dashboard Click 'Clusters', from the list of clusters select the source cluster which is alerted
17. Click on the 'Terminate' button from the top menu.
18. On the 'Terminate clusters' pop-up, click 'Terminate'.

# 3. Protect stored cardholder data

3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.

## AWS RDS DB cluster encryption is disabled

| | |
|---|---|
| Compliance Section: 3.4.1 | First Seen: N/A |
| Resource(s) Failed: 1 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies RDS DB clusters for which encryption is disabled. Amazon Aurora encrypted DB clusters provide an additional layer of data protection by securing your data from unauthorized access to the underlying storage. You can use Amazon Aurora encryption to increase data protection of your applications deployed in the cloud, and to fulfill compliance requirements for data-at-rest encryption. NOTE: This policy is applicable only for Aurora DB clusters. https://docs.aws.amazon.com/cli/latest/reference/rds/describe-db-clusters.html

### Resource(s) Failed:

bookstoreneptunecluster-ufqa59y5zpaz

### Recommendations:

AWS DB clusters can be encrypted only while creating the database cluster. You can't convert an unencrypted DB cluster to an encrypted one. However, you can restore an unencrypted Aurora DB cluster snapshot to an encrypted Aurora DB cluster. To do this, specify a KMS encryption key when you restore from the unencrypted DB cluster snapshot.
For AWS RDS,
1. To create a 'Snapshot' of the unencrypted DB cluster, follow the instruction mentioned in below link:
RDS Link: https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/USER_CreateSnapshotCluster.html
NOTE: As you can't restore from a DB cluster snapshot to an existing DB cluster; a new DB cluster is created when you restore. Once the Snapshot status is 'Available', delete the unencrypted DB cluster before restoring from the DB cluster Snapshot by following below steps for AWS RDS,
a. Sign to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/
b. In the navigation pane, choose 'Databases'.
c. In the list of DB instances, choose a writer instance for the DB cluster.
d. Choose 'Actions', and then choose 'Delete'.
2. To restoring the Cluster from a DB Cluster Snapshot, follow the instruction mentioned in below link:
RDS Link: https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/USER_RestoreFromSnapshot.html
For AWS Document DB,
1. To create a 'Snapshot' of the unencrypted DB cluster, follow the instruction mentioned in below link:
Document DB Link: https://docs.aws.amazon.com/documentdb/latest/developerguide/backup_restore-create_manual_cluster_snapshot.html
NOTE: As you can't restore from a DB cluster snapshot to an existing DB cluster; a new DB cluster is created when you restore. Once the Snapshot status is 'Available', delete the unencrypted DB cluster before restoring from the DB cluster Snapshot by following below steps for AWS Document DB,
a. Sign to the AWS Management Console and open the Amazon DocumentDB console at https://console.aws.amazon.com/docdb/
b. In the navigation pane, choose 'Clusters'.
c. Select the cluster from the list which needs to be deleted
d. Choose 'Actions', and then choose 'Delete'.
2. To restoring the Cluster from a DB Cluster Snapshot, follow the instruction mentioned in below link:
Document DB Link: https://docs.aws.amazon.com/documentdb/latest/developerguide/backup_restore-restore_from_snapshot.html

# 3. Protect stored cardholder data

3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.

## AWS EMR cluster is not enabled with data encryption at rest

| | |
|---|---|
| Compliance Section: 3.4.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies AWS EMR clusters for which data encryption at rest is not enabled. Encryption of data at rest is required to prevent unauthorized users from accessing the sensitive information available on your EMR clusters and associated storage systems.

### Recommendations:

1. Login to the AWS Console.
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated.
3. Navigate to 'EMR' dashboard from 'Services' dropdown.
4. Go to 'Security configurations', click 'Create'.
5. On the Create security configuration window,
6. In 'Name' box, provide a name for the new EMR security configuration.
7. For encryption At Rest select the required encryption type ('S3 encryption'/'Local disk encryption'/both) and follow below link for enabling the same.
8. https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-encryption-enable.html
9. Click on 'Create' button.
10. On the left menu of EMR dashboard Click 'Clusters'.
11. Select the EMR cluster for which the alert has been generated and click on the 'Clone' button from the top menu.
12. In the Cloning popup, choose 'Yes' and Click 'Clone'.
13. On the Create Cluster page, in the Security Options section, click on 'security configuration'.
14. From the 'Security configuration' drop down select the name of the security configuration created at step 4 to step 8, click 'Create Cluster'.
15. Once you the new cluster is set up verify its working and terminate the source cluster in order to stop incurring charges for it.
16. On the left menu of EMR dashboard Click 'Clusters', from the list of clusters select the source cluster which is alerted.
17. Click on the 'Terminate' button from the top menu.
18. On the 'Terminate clusters' pop-up, click 'Terminate'.

# 3. Protect stored cardholder data

3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.

## AWS Kinesis streams are not encrypted using Server Side Encryption

| | |
|---|---|
| Compliance Section: 3.4.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This Policy identifies the AWS Kinesis streams which are not encrypted using Server Side Encryption. Server Side Encryption is used to encrypt your sensitive data before it is written to the Kinesis stream storage layer and decrypted after it is retrieved from storage.

### Recommendations:

1. Sign in to the AWS Console
2. Go to Kinesis Service
3. Select the reported Kinesis data stream for the corresponding region
4. Under Server-side encryption, Click on Edit
5. Choose Enabled
6. Under KMS master key, You can choose any KMS other than the default (Default) aws/kinesis
7. Click Save

# 3. Protect stored cardholder data

3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.

## AWS SSM Parameter is not encrypted

| | |
|---|---|
| Compliance Section: 3.4.1 | First Seen: N/A |
| Resource(s) Failed: 2 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies the AWS SSM Parameters which are not encrypted. AWS Systems Manager (SSM) parameters that store sensitive data, for example, passwords, database strings, and permit codes are encrypted so as to meet security and compliance prerequisites. An encrypted SSM parameter is any sensitive information that should be kept and referenced in a protected way.

### Resource(s) Failed:

AgentInstallLocation, AgentActivationKey

### Recommendations:

1. Sign in to the AWS Console
2. Go to System Manager
3. In the navigation panel, Click on 'Parameter Store'
4. Choose the reported parameter and port it to a new parameter with Type 'SecureString'
5. Delete the reported parameter by clicking on 'Delete'
6. Click on 'Delete parameters'

# 3. Protect stored cardholder data

3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.

## AWS CloudTrail logs are not encrypted using Customer Master Keys (CMKs)

| | |
|---|---|
| Compliance Section: 3.4.1 | First Seen: N/A |
| Resource(s) Failed: 2 | Resource Type: CloudTrail Setting |
| Resource(s) Passed: 0 | |

### Description:

Checks to ensure that CloudTrail logs are encrypted. AWS CloudTrail is a service that enables governance, compliance, operational & risk auditing of the AWS account. It is a compliance and security best practice to encrypt the CloudTrail data since it may contain sensitive information.

### Resource(s) Failed:

aws-controltower-BaselineCloudTrail, cloud-trail-demo

### Recommendations:

1. Login to AWS Console and navigate to the 'CloudTrail' service.
2. For each trail, under Configuration > Storage Location, select 'Yes' to 'Encrypt log files' setting
3.Choose and existing KMS key or create a new one to encrypt the logs with.

# 3. Protect stored cardholder data

3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.

## AWS Redshift Cluster not encrypted using Customer Managed Key

| | |
|---|---|
| Compliance Section: 3.4.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 3 | |

### Description:

This policy identifies Redshift Clusters which are encrypted with default KMS keys and not with Keys managed by Customer. It is a best practice to use customer managed KMS Keys to encrypt your Redshift databases data. Customer-managed CMKs give you more flexibility, including the ability to create, rotate, disable, define access control for, and audit the encryption keys used to help protect your data.

### Recommendations:

To enable encryption with Customer Managed Key on your Redshift cluster follow the steps mentioned in below URL:
https://docs.aws.amazon.com/redshift/latest/mgmt/changing-cluster-encryption.html

# 3. Protect stored cardholder data

3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.

## AWS S3 buckets do not have server side encryption

| | |
|---|---|
| Compliance Section: 3.4.1 | First Seen: N/A |
| Resource(s) Failed: 8 | Resource Type: Other |
| Resource(s) Passed: 4 | |

### Description:

Customers can protect the data in S3 buckets using the AWS server-side encryption. If the server-side encryption is not turned on for S3 buckets with sensitive data, in the event of a data breach, malicious users can gain access to the data. NOTE: Do NOT enable this policy if you are using 'Server-Side Encryption with Customer-Provided Encryption Keys (SSE-C).'

### Resource(s) Failed:

aws-cloudtrail-logs-795462528824-317b0c26, mygoalsapp-pipelineartifactsbucket-1es78l9rtorl1, s3-production-for-pp-ctf, photos.cats.ctf, mybookstore-assetsbucket-h49w4uta9ws4, mygoalsapp-assetsbucket-1jvraqv1lbf1z, mybookstore-pipelineartifactsbucket-1ov8q9nvordkf, agentbucket-795462528824

### Recommendations:

1. Login to the AWS Console and navigate to the 'S3' service
2. Click on the reported S3 bucket
3. Click on the 'Properties' tab
4. Under the 'Default encryption' section, choose encryption option either AES-256 or AWS-KMS based on your requirement.

For more information about Server-side encryption,
Default encryption:
https://docs.aws.amazon.com/AmazonS3/latest/dev/bucket-encryption.html
Policy based encryption:
https://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html

# 3. Protect stored cardholder data

3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.

## AWS DynamoDB encrypted using AWS owned CMK instead of AWS managed CMK

| | |
|---|---|
| Compliance Section: 3.4.1 | First Seen: N/A |
| Resource(s) Failed: 4 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies the DynamoDB tables that use AWS owned CMK (default ) instead of AWS managed CMK (KMS ) to encrypt data. AWS managed CMK provide additional features such as the ability to view the CMK and key policy, and audit the encryption and decryption of DynamoDB tables.

### Resource(s) Failed:

mybookstore-Books, mybookstore-Cart, mybookstore-Orders, goalsapp

### Recommendations:

1. Sign in to AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated.
3. Navigate to 'DynamoDB' dashboard
4. Select the reported table from the list of DynamoDB tables
5. In 'Overview' tab, go to 'Table Details' section
6. Click on the 'Manage Encryption' link available for 'Encryption Type'
7. On 'Manage Encryption' pop up window, Select 'KMS' as the encryption type.

# 3. Protect stored cardholder data

3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.

## AWS SQS queue encryption using default KMS key instead of CMK

| | |
|---|---|
| Compliance Section: 3.4.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies SQS queues which are encrypted with default KMS keys and not with Customer Master Keys(CMKs). It is a best practice to use customer managed Master Keys to encrypt your SQS queue messages. It gives you full control over the encrypted messages data.

### Recommendations:

1. Sign in to the AWS console
2. Select the region, from the region drop-down, in which the alert is generated
3. Navigate to Simple Queue Service (SQS) dashboard
4. Choose the reported Simple Queue Service (SQS)
5. Click on 'Queue Actions' and Choose 'Configure Queue' from the dropdown
6. On 'Configure' popup, Under 'Server-Side Encryption (SSE) Settings' section; Choose an 'AWS KMS Customer Master Key (CMK)' from the drop-down list or copy existing key ARN instead of (Default) alias/aws/sqs key.
7. Click on 'Save Changes'

# 3. Protect stored cardholder data

3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.

## AWS ElastiCache Redis cluster with encryption for data at rest disabled

| | |
|---|---|
| Compliance Section: 3.4.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies ElastiCache Redis clusters which have encryption for data at rest(at-rest) is disabled. It is highly recommended to implement at-rest encryption in order to prevent unauthorized users from reading sensitive data saved to persistent media available on your Redis clusters and their associated cache storage systems.

### Recommendations:

AWS ElastiCache Redis cluster at-rest encryption can be set only at the time of the creation of the cluster. So to fix this alert, create a new cluster with at-rest encryption, then migrate all required ElastiCache Redis cluster data from the reported ElastiCache Redis cluster to this newly created cluster and delete reported ElastiCache Redis cluster.
To create new ElastiCache Redis cluster with at-rest encryption set, perform the following:
1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to ElastiCache Dashboard
4. Click on Redis
5. Click on 'Create' button
6. On the 'Create your Amazon ElastiCache cluster' page,
a. Select 'Redis' cache engine type.
b. Enter a name for the new cache cluster
c. Select Redis engine version from 'Engine version compatibility' dropdown list.
Note: As of July 2018, In-transit encryption can be enabled only for AWS ElastiCache clusters with Redis engine version 3.2.6 and 4.0.10.
d. Click on 'Advanced Redis settings' to expand the cluster advanced settings panel
e. Select 'Encryption at-rest' checkbox to enable encryption along with other necessary parameters
7. Click on 'Create' button to launch your new ElastiCache Redis cluster
To delete reported ElastiCache Redis cluster, perform the following:
1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to ElastiCache Dashboard
4. Click on Redis
5. Select reported Redis cluster
6. Click on 'Delete' button
7. In the 'Delete Cluster' dialog box, if you want a backup for your cluster select 'Yes' from the 'Create final backup' dropdown menu, provide a name for the cluster backup, then click on 'Delete'.

# 3. Protect stored cardholder data

3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.

## AWS EMR cluster is not configured with SSE KMS for data at rest encryption (Amazon S3 with EMRFS)

| | |
|---|---|
| Compliance Section: 3.4.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies EMR clusters which are not configured with Server Side Encryption(SSE KMS) for data at rest encryption of Amazon S3 with EMRFS. As a best practice, use SSE-KMS for server side encryption to encrypt the data in your EMR cluster and ensure full control over your data.

### Recommendations:

1. Log in to the AWS Console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to 'EMR' dashboard from 'Services' dropdown
4. Go to 'Security configurations', click 'Create'
5. On the Create security configuration window,
6. In 'Name' box, provide a name for the new EMR security configuration
7. For encryption At Rest click the checkbox for 'Enable at-rest encryption for EMRFS data in Amazon S3'
8. From the dropdown 'Default encryption mode' select 'SSE-KMS'. Follow below link for configuration steps.
https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-encryption-enable.html
9. Click on 'Create' button.
10. On the left menu of EMR dashboard Click 'Clusters'.
11. Select the EMR cluster for which the alert has been generated and click on the 'Clone' button from the top menu.
12. In the Cloning popup, choose 'Yes' and Click 'Clone'.
13. On the Create Cluster page, in the Security Options section, click on 'security configuration'.
14. From the 'Security configuration' drop down select the name of the security configuration created at step 4 to step 8, click 'Create Cluster'
15. Once you the new cluster is set up verify its working and terminate the source cluster in order to stop incurring charges for it.
16. On the left menu of EMR dashboard Click 'Clusters', from the list of clusters select the source cluster which is alerted
17. Click on the 'Terminate' button from the top menu
18. On the 'Terminate clusters' pop-up, click 'Terminate'.

# 3. Protect stored cardholder data

3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.

## AWS EMR cluster is not enabled with local disk encryption

| | |
|---|---|
| Compliance Section: 3.4.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies AWS EMR clusters that are not enabled with local disk encryption. Applications using the local file system on each cluster instance for intermediate data throughout workloads, where data could be spilled to disk when it overflows memory. With Local disk encryption at place, data at rest can be protected.

### Recommendations:

1. Login to the AWS Console.
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated.
3. Navigate to 'EMR' dashboard from 'Services' dropdown.
4. Go to 'Security configurations', click 'Create'.
5. On the Create security configuration window,
6. In 'Name' box, provide a name for the new EMR security configuration.
7. Under 'Local disk encryption', check the box 'Enable at-rest encryption for local disks'.
8. Select the appropriate Key provider type from the 'Key provider type' dropdown list.
9. Click on 'Create' button.
10. On the left menu of EMR dashboard Click 'Clusters'.
11. Select the EMR cluster for which the alert has been generated and click on the 'Clone' button from the top menu.
12. In the Cloning popup, choose 'Yes' and Click 'Clone'.
13. On the Create Cluster page, in the Security Options section, click on 'security configuration'.
14. From the 'Security configuration' drop down select the name of the security configuration created at step 4 to step 8, click 'Create Cluster'.
15. Once the new cluster is set up verify its working and terminate the source cluster.
16. On the left menu of EMR dashboard Click 'Clusters', from the list of clusters select the source cluster which is alerted.
17. Click on the 'Terminate' button from the top menu.
18. On the 'Terminate clusters' pop-up, click 'Terminate'.

# 3. Protect stored cardholder data

3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.

## AWS Elastic File System (EFS) not encrypted using Customer Managed Key

| | |
|---|---|
| Compliance Section: 3.4.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 3 | |

### Description:

This policy identifies Elastic File Systems (EFSs) which are encrypted with default KMS keys and not with Keys managed by Customer. It is a best practice to use customer managed KMS Keys to encrypt your EFS data. It gives you full control over the encrypted data.

### Recommendations:

AWS EFS Encryption of data at rest can only be enabled during file system creation. So to resolve this alert, create a new EFS with encryption enabled with the customer-managed key, then migrate all required data from the reported EFS to this newly created EFS and delete reported EFS.
To create new EFS with encryption enabled, perform the following:
1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to EFS dashboard
4. Click on 'File systems' (Left Panel)
5. Click on 'Create file system' button
6. On the 'Configure file system access' step, specify EFS details as per your requirements and Click on 'Next Step'
7. On the 'Configure optional settings' step, Under 'Enable encryption' Choose 'Enable encryption of data at rest' and Select customer managed key [i.e. Other than (default)aws/elasticfilesystem] from 'Select KMS master key' dropdown list along with other parameters and Click on 'Next Step'
8. On the 'Review and create' step, Review all your setting and Click on 'Create File System' button
To delete reported EFS which does not has encryption, perform the following:
1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to EFS dashboard
4. Click on 'File systems' (Left Panel)
5. Select the reported file system
6. Click on 'Actions' drop-down
7. Click on 'Delete file system'
8. In the 'Permanently delete file system' popup box, To confirm the deletion enter the file system's ID and Click on 'Delete File System'

# 3. Protect stored cardholder data

3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.

## AWS SageMaker notebook instance not encrypted using Customer Managed Key

| | |
|---|---|
| Compliance Section: 3.4.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies SageMaker notebook instances that are not encrypted using Customer Managed Key. SageMaker notebook instances should be encrypted with Amazon KMS Customer Master Keys (CMKs) instead of AWS managed-keys in order to have more granular control over the data-at-rest encryption/decryption process and meet compliance requirements. For more details:
https://docs.aws.amazon.com/sagemaker/latest/dg/encryption-at-rest.html

### Recommendations:

AWS SageMaker notebook instance encryption can not be modified once it is created. You need to create a new notebook instance with encryption using a custom KMS key; migrate all required data from the reported notebook instance to the newly created notebook instance before you delete the reported notebook instance.
To create a New AWS SageMaker notebook instance,
1. Log in to AWS console
2. Navigate to the AWS SageMaker dashboard
3. Choose Notebook instances and then choose 'Create notebook instance'
4. On the Create notebook instance page, within the 'Permissions and encryption' section,
From the 'Encryption key - optional' dropdown list, choose a custom KMS key for the new SageMaker notebook instance.
5. Choose other parameters as per your requirement and click on the 'Create notebook instance' button
To delete reported notebook instance,
1. Log in to AWS console
2. Navigate to the AWS SageMaker dashboard
3. Choose Notebook instances and Choose the reported notebook instance
4. Click on the 'Actions' dropdown menu, select the 'Stop' option, and when instance stops, select the 'Delete' option.
5. Within Delete <notebook-instance-name> dialog box, click the Delete button to confirm the action.

# 3. Protect stored cardholder data

3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.

## AWS RDS database not encrypted using Customer Managed Key

| | |
|---|---|
| Compliance Section: 3.4.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 5 | |

### Description:

This policy identifies RDS databases that are encrypted with default KMS keys and not with customer managed keys. As a best practice, use customer managed keys to encrypt the data on your RDS databases and maintain control of your keys and data on sensitive workloads.

### Recommendations:

Because you can set AWS RDS database encryption only during database creation, the process for resolving this alert requires you to create a new RDS database with a customer managed key for encryption, migrate the data from the reported database to this newly created database, and delete the RDS database identified in the alert.
To create a new RDS database with encryption using a customer managed key:
1. Log in to the AWS console.
2. Select the region for which the alert was generated.
3. Navigate to the Amazon RDS Dashboard.
4. Select 'Create database'.
5. On the 'Select engine' page, select 'Engine options' and 'Next'.
6. On the 'Choose use case' page, select 'Use case' of database and 'Next'.
7. On the 'Specify DB details' page, specify the database details you need and click 'Next'.
Note: Amazon RDS encryption has some limitation on region and type instances. For Availability of Amazon RDS Encryption refer to:
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html#Overview.Encryption.Availability
8. On the 'Configure advanced settings' page, Under 'Encryption', select 'Enable encryption' and select the customer managed key [i.e. Other than (default)aws/rds] from 'Master key' dropdown list].
9. Select 'Create database'.
To delete the RDS database that uses the default KMS keys, which triggered the alert:
1. Log in to the AWS console
2. Select the region for which the alert was generated.
3. Navigate to the Amazon RDS Dashboard.
4. Click on Instances, and select the reported RDS database.
5. Select the 'Instance actions' drop-down and click 'Delete'.
7. In the 'Delete' dialog, select the 'Create final snapshot?' checkbox, if you want a backup. Provide a name for the final snapshot, confirm deletion and select 'Delete'.

# 3. Protect stored cardholder data

3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.

## AWS Elasticsearch domain Encryption for data at rest is disabled

| | |
|---|---|
| Compliance Section: 3.4.1 | First Seen: N/A |
| Resource(s) Failed: 1 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies Elasticsearch domains for which encryption is disabled. Encryption of data at rest is required to prevent unauthorized users from accessing the sensitive information available on your Elasticsearch domains components. This may include all data of file systems, primary and replica indices, log files, memory swap files and automated snapshots. The Elasticsearch uses AWS KMS service to store and manage the encryption keys. It is highly recommended to implement encryption at rest when you are working with production data that have sensitive information, to protect from unauthorized access.

### Resource(s) Failed:

mybookstore-domain

### Recommendations:

Enabling the encryption feature on existing domains requires Elasticsearch 6.7 or later. If your Elasticsearch 6.7 or later, follow below steps to enable encryption on existing Elasticsearch domain:

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to Elasticsearch Service Dashboard
4. Choose reported Elasticsearch domain
5. Click on 'Actions' button, from drop-down select 'Modify encryptions'
6.In Modify encryptions page, Select the 'Enable encryption of data at rest' checkbox and Choose KMS key as per your requirement. It is recommended to choose KMS CMKs instead of default KMS [Default(aws/es)]; to get more grannular control on your Elasticsearch domain data.
7. Click on 'Submit'.

If your Elasticsearch is less than 6.7 version, then AWS Elasticsearch Domain encryption can be set only at the time of the creation of domain. So to fix this alert, create a new domain with encryption using KMS Keys and then migrate all required Elasticsearch domain data from the reported Elasticsearch domain to this newly created domain.

To set up the new Elasticsearch domain with encryption using KMS Key, refer the following URL:
https://docs.aws.amazon.com/elasticsearch-service/latest/developerguide/es-createupdatedomains.html

To delete reported ES domain, refer the following URL:
https://docs.aws.amazon.com/elasticsearch-service/latest/developerguide/es-gsg-deleting.html

# 3. Protect stored cardholder data

3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.

## AWS RDS DB cluster is encrypted using default KMS key instead of CMK

| | |
|---|---|
| Compliance Section: 3.4.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 4 | |

### Description:

This policy identifies RDS DB(Relational Database Service Database) clusters which are encrypted using default KMS key instead of CMK (Customer Master Key). As a security best practice CMK should be used instead of default KMS key for encryption to gain the ability to rotate the key according to your own policies, delete the key, and control access to the key via KMS policies and IAM policies.

### Recommendations:

RDS DB clusters can be encrypted only while creating the database cluster. You can't convert an unencrypted DB cluster to an encrypted one. However, you can restore an unencrypted Aurora DB cluster snapshot to an encrypted Aurora DB cluster. To do this, specify a KMS encryption key when you restore from the unencrypted DB cluster snapshot.
Step 1: To create a 'Snapshot' of the unencrypted DB cluster,
https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/USER_CreateSnapshotCluster.html
NOTE: As you can't restore from a DB cluster snapshot to an existing DB cluster; a new DB cluster is created when you restore. Once the Snapshot status is 'Available'.
Step 2: Follow the below link to restoring the Cluster from a DB Cluster Snapshot,
https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/USER_RestoreFromSnapshot.html
Once the DB cluster is restored and verified, follow below steps to delete the reported DB cluster,
1. Log in to the AWS Management Console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated.
3. Navigate to 'RDS' dashboard from 'Services' dropdown
4. In the navigation pane, choose ‘Databases’
5. In the list of DB instances, choose a writer instance for the DB cluster
6. Choose 'Actions', and then choose 'Delete'
FMI:
1. While deleting a RDS DB cluster, customer has to disable 'Enable deletion protection' otherwise instance cannot be deleted
2. While deleting RDS DB instance , AWS application will ask the end user to take Final snapshot
3. If a RDS DB cluster has a writer role instance, then User has to delete the write instance to delete the main cluster (Delete option won’t be enabled for main RDS DB cluster)

# 3. Protect stored cardholder data

3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.

## AWS EBS volume region with encryption is disabled

| | |
|---|---|
| Compliance Section: 3.4.1 | First Seen: N/A |
| Resource(s) Failed: 17 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies AWS regions in which new EBS volumes are getting created without any encryption. Encrypting data at rest reduces unintentional exposure of data stored in EBS volumes. It is recommended to configure EBS volume at the regional level so that every new EBS volume created in that region will be enabled with encryption by using a provided encryption key.

### Resource(s) Failed:

795462528824:EBS:eu-west-3, 795462528824:EBS:us-east-2, 795462528824:EBS:us-east-1, 795462528824:EBS:ap-northeast-3, 795462528824:EBS:ca-central-1, 795462528824:EBS:us-west-2, 795462528824:EBS:eu-west-1, 795462528824:EBS:eu-central-1, 795462528824:EBS:eu-west-2, 795462528824:EBS:ap-northeast-1 ...and 7 more

### Recommendations:

To enable encryption at region level by default, follow below URL:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html#encryption-by-default
Additional Information:
To detect existing EBS volumes that are not encrypted ; refer Saved Search:
AWS EBS volumes are not encrypted_RL
To detect existing EBS volumes that are not encrypted with CMK, refer Saved Search:
AWS EBS volume not encrypted using Customer Managed Key_RL

# 3. Protect stored cardholder data

3.6.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).

## AWS Customer Master Key (CMK) rotation is not enabled

| | |
|---|---|
| Compliance Section: 3.6.4 | First Seen: N/A |
| Resource(s) Failed: 2 | Resource Type: Managed Key Rotation Status |
| Resource(s) Passed: 1 | |

### Description:

This policy identifies Customer Master Keys (CMKs) that are not enabled with key rotation. AWS KMS (Key Management Service) allows customers to create master keys to encrypt sensitive data in different services. As a security best practice, it is important to rotate the keys periodically so that if the keys are compromised, the data in the underlying service is still secure with the new keys.

### Resource(s) Failed:

prisma-duty, 0ef3f1ee-e8da-4366-ba8a-0731c04ef0cd

### Recommendations:

1. Log in to the AWS console
2. In the console, select the specific region from region drop-down on the top right corner, for which the alert is generated
3. Navigate to Key Management Service (KMS)
4. Click on 'Customer managed keys' (Left Panel)
5. Select reported KMS Customer managed key
6. Under the 'Key Rotation' tab, Enable 'Automatically rotate this CMK every year'
7. Click on Save

# 3. Protect stored cardholder data

3.6.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).

## AWS Elastic Load Balancer (ELB) with IAM certificate expiring in 90 days

| | |
|---|---|
| Compliance Section: 3.6.4 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies Elastic Load Balancers (ELB) which are using IAM certificates expiring in 90 days or using expired certificates. Removing expired IAM certificates eliminates the risk and prevents the damage of credibility of the application/website behind the ELB. As a best practice, it is recommended to reimport expiring certificates while preserving the ELB associations of the original certificate.

### Recommendations:

Removing invalid certificates via AWS Management Console is not currently supported. To delete/upload SSL/TLS certificates stored in IAM via the AWS API use the Command Line Interface (CLI).
Remediation CLI:
1. Run describe-load-balancers command to make sure that the expiring server certificate is not currently used by any active load balancer.
aws elb describe-load-balancers --region <COMPUTE_REGION> --load-balancer-names <ELB_NAME> --query 'LoadBalancerDescriptions[*].ListenerDescriptions[*].Listener.SSLCertificateId'
This command output will return the Amazon Resource Name (ARN) for the SSL certificate currently used by the selected ELB:
[
[
\"arn:aws:iam::1234567890:server-certificate/MyCertificate\"
]
]
2. Create new AWS IAM certificate with your desired parameters value
3. To upload new IAM Certificate:
aws iam upload-server-certificate --server-certificate-name <NEW_CERTIFICATE_NAME> --certificate-body file://Certificate.pem --certificate-chain file://CertificateChain.pem --private-key file://PrivateKey.pem
4. To replaces the existing SSL certificate for the specified HTTPS load balancer:
aws elb set-load-balancer-listener-ssl-certificate --load-balancer-name <ELB_NAME> --load-balancer-port 443 --ssl-certificate-id arn:aws:iam::1234567890:server-certificate/<NEW_CERTIFICATE_NAME>
5. Now that is safe to remove the expiring SSL/TLS certificate from AWS IAM, To delete it run:
aws iam delete-server-certificate --server-certificate-name <CERTIFICATE_NAME>

# 3. Protect stored cardholder data

3.6.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).

## AWS KMS Key scheduled for deletion

| | |
|---|---|
| Compliance Section: 3.6.4 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 3 | |

### Description:

This policy identifies KMS Keys which are scheduled for deletion. Deleting keys in AWS KMS is destructive and potentially dangerous. It deletes the key material and all metadata associated with it and is irreversible. After a key is deleted, you can no longer decrypt the data that was encrypted under that key, which means that data becomes unrecoverable. You should delete a key only when you are sure that you don't need to use it anymore. If you are not sure, It is recommended that to disable the key instead of deleting it.

### Recommendations:

You should delete a KMS key only when you are sure that you don't need to use it anymore. To fix this alert, If you sure you no longer need a reported KMS key; dismiss the alert. If you are not sure, consider disabling the KMS key instead of deleting it.
To enable KMS CMKs which are scheduled for deletion, perform the following:
1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to Key Management Service (KMS)
4. Click on 'Customer managed keys' (Left Panel)
5. Select reported KMS Customer managed key
6. Click on 'Key actions' dropdown
7. Click on 'Cancel key deletion'
8. Click on 'Enable'

# 3. Protect stored cardholder data

3.6.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).

## AWS KMS customer managed external key expiring in 30 days or less

| | |
|---|---|
| Compliance Section: 3.6.4 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 3 | |

### Description:

This policy identifies KMS customer managed external keys which are expiring in 30 days or less. As a best practice, it is recommended to reimport the same key material and specifying a new expiration date. If the key material expires, AWS KMS deletes the key material and the customer managed external key becomes unusable.

### Recommendations:

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to Key Management Service (KMS) Dashboard
4. Click on Customer managed keys (Left Panel)
5. Click on reported KMS Customer managed key
6. Under 'Key material' section, Delete the existing key material before you reimport the key material by clicking on 'Delete key material'
7. Click on 'Upload key material'
8. Under 'Encrypted key material and import token' section, Reimport same encrypted key material and import token
9. Under 'Expiration option', Select 'Key material expires' and choose new expiration date in 'Key material expires at' date box
10. Click on 'Upload key material' button

NOTE: Deleting key material makes all data encrypted under the customer master key (CMK) unrecoverable unless you later import the same key material into the CMK. The CMK is not affected by this operation.

# 3. Protect stored cardholder data

3.6.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).

## AWS Certificate Manager (ACM) has certificates expiring in 30 days or less

| | |
|---|---|
| Compliance Section: 3.6.4 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies ACM certificates expiring in 30 days or less, which are in the AWS Certificate Manager. If SSL/TLS certificates are not renewed prior to their expiration date, they will become invalid and the communication between the client and the AWS resource that implements the certificates is no longer secure. As a best practice, it is recommended to renew certificates before their validity period ends. AWS Certificate Manager automatically renews certificates issued by the service that is used with other AWS resources. However, the ACM service does not renew automatically certificates that are not in use or not associated anymore with other AWS resources. So the renewal process must be done manually before these certificates become invalid. NOTE: If you wanted to be notified other than before or less than 30 days; you can clone this policy and replace '30' in RQL with your desired days value. For example, 15 days OR 7 days which will alert certificates expiring in 15 days or less OR 7 days or less respectively.

### Recommendations:

1. Log in to the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Go to the Certificate Manager(ACM) service
4. Choose the reported certificate
5. Verify that the 'Status' column shows 'Issued' for the reported certificate
6. Under 'Actions' drop-down select 'Reimport certificate' option
7. On the Import a certificate page, perform the following actions:

7a. In 'Certificate body*' box, paste the PEM-encoded certificate to import, purchased from your SSL certificate provider.
7b. In 'Certificate private key*' box, paste the PEM-encoded, unencrypted private key that matches the SSL/TLS certificate public key.
7c.(Optional) In 'Certificate chain' box, paste the PEM-encoded certificate chain delivered with the certificate body specified at step 7a.

8. Click on 'Review and import' button
9. On the Review and import page, review the imported certificate details then click on 'Import'

# 3. Protect stored cardholder data

3.6.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).

## AWS IAM has expired SSL/TLS certificates

| | |
|---|---|
| Compliance Section: 3.6.4 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies expired SSL/TLS certificates. To enable HTTPS connections to your website or application in AWS, you need an SSL/TLS server certificate. You can use ACM or IAM to store and deploy server certificates. Removing expired SSL/TLS certificates eliminates the risk that an invalid certificate will be deployed accidentally to a resource such as AWS Elastic Load Balancer (ELB), which can damage the credibility of the application/website behind the ELB. This policy generates alerts if there are any expired SSL/TLS certificates stored in AWS IAM. As a best practice, it is recommended to delete expired certificates.

### Recommendations:

Removing invalid certificates via AWS Management Console is not currently supported. To delete SSL/TLS certificates stored in IAM via the AWS API use the Command Line Interface (CLI).
Remediation CLI:
1. Run describe-load-balancers command to make sure that the expired server certificate is not currently used by any active load balancer.
aws elb describe-load-balancers --region <COMPUTE_REGION> --load-balancer-names <ELB_NAME> --query 'LoadBalancerDescriptions[*].ListenerDescriptions[*].Listener.SSLCertificateId'
This command output will return the Amazon Resource Name (ARN) for the SSL certificate currently used by the selected ELB:
[
[
"arn:aws:iam::1234567890:server-certificate/MyCertificate"
]
]
2. If the load balancer listener using the reported expired certificate is not removed before the certificate, the ELB may continue to use the same certificate and work improperly. To delete the ELB listener that is using the expired SSL certificate, run following command:
aws elb delete-load-balancer-listeners --region <COMPUTE_REGION> --load-balancer-name <ELB_NAME> --load-balancer-ports 443
3. Now that is safe to remove the expired SSL/TLS certificate from AWS IAM, To delete it run:
aws iam delete-server-certificate --server-certificate-name <CERTIFICATE_NAME>

# 3. Protect stored cardholder data

3.6.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).

## AWS Database Migration Service (DMS) has expired certificates

| | |
|---|---|
| Compliance Section: 3.6.4 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies expired certificates that are in AWS Database Migration Service (DMS). AWS Database Migration Service (DMS) Certificate service is the preferred tool to provision, manage, and deploy your DMS endpoint certificates. As a best practice, it is recommended to delete expired certificates. For more details:
https://docs.aws.amazon.com/dms/latest/userguide/CHAP_Security.html#CHAP_Security.SSL.ManagingCerts

### Recommendations:

1. Log in to the AWS Console
2. In the console, select the specific region from the region drop-down on the top right corner, for which the alert is generated
3. Navigate to 'AWS DMS' service
4. Click on 'Certificates', Choose the reported certificate
5. Make sure the reported certificate is already out of date from the 'Valid to' field
6. Click on 'Delete', to delete the expired certificate.

# 3. Protect stored cardholder data

3.6.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).

## AWS Elastic Load Balancer (ELB) with ACM certificate expired or expiring in 90 days

| | |
|---|---|
| Compliance Section: 3.6.4 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies Elastic Load Balancers (ELB) which are using ACM certificates expired or expiring in 90 days. AWS Certificate Manager (ACM) is the preferred tool to provision, manage, and deploy your server certificates. With ACM you can request a certificate or deploy an existing ACM or external certificate to AWS resources. As a best practice, it is recommended to reimport expiring/expired certificates while preserving the ELB associations of the original certificate.

### Recommendations:

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Go to Certificate Manager(ACM) service
4. Choose the reported certificate
5. Under 'Actions' drop-down click on 'Reimport certificate'
6. On the 'Import a certificate' page:

6a. For 'Certificate body*', paste the PEM-encoded certificate to import
6b. For 'Certificate private key*', paste the PEM-encoded, unencrypted private key that matches the SSL/TLS certificate public key
6c. (Optional) For 'Certificate chain', paste the PEM-encoded certificate chain delivered
6d. Click Review and import button to continue the process

7. On the 'Review and import' page, review the imported certificate details then click on 'Import'

# 3. Protect stored cardholder data

3.6.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).

## AWS Certificate Manager (ACM) has expired certificates

| | |
|---|---|
| Compliance Section: 3.6.4 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies expired certificates which are in AWS Certificate Manager. AWS Certificate Manager (ACM) is the preferred tool to provision, manage, and deploy your server certificates. With ACM you can request a certificate or deploy an existing ACM or external certificate to AWS resources. This policy generates alerts if there are any expired ACM managed certificates. As a best practice, it is recommended to delete expired certificates.

### Recommendations:

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Go to Certificate Manager(ACM) service
4. Choose the reported certificate
5. Verify that the 'Status' column shows 'Expired' for the reported certificate
6. Under 'Actions' drop-down click on 'Delete'

# 3. Protect stored cardholder data

3.6.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).

## AWS KMS Key policy overly permissive

| | |
|---|---|
| Compliance Section: 3.6.4 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 3 | |

### Description:

This policy identifies KMS Keys that have a key policy overly permissive. Key policies are the primary way to control access to customer master keys (CMKs) in AWS KMS. It is recommended to follow the principle of least privilege ensuring that KMS key policy does not have all the permissions to be able to complete a malicious action. For more details: https://docs.aws.amazon.com/kms/latest/developerguide/control-access-overview.html#overview-policy-elements

### Recommendations:

1. Log in to the AWS console
2. In the console, select the specific region from region drop-down on the top right corner, for which the alert is generated
3. Navigate to Key Management Service (KMS)
4. Click on 'Customer managed keys' (Left Panel)
5. Select reported KMS Customer managed key
6. Click on the 'Key policy' tab
7. Click on 'Edit',

Replace the 'Everyone' grantee (i.e. '*') from the Principal element value with an AWS account ID or an AWS account ARN.
OR
Add a Condition clause to the existing policy statement so that the KMS key is restricted.

8. Click on 'Save Changes'

# 4. Encrypt transmission of cardholder data across open, public networks

4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: - Only trusted keys and certificates are accepted. - The protocol in use only supports secure versions or configurations. - The encryption strength is appropriate for the encryption methodology in use.

## Internet connectivity via TCP over insecure port

| | |
|---|---|
| Compliance Section: 4.1 | First Seen: N/A |
| Resource(s) Failed: 3 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies network traffic coming from the internet which is plain text FTP, Telnet, or HTTP. It is recommended to have Security Group/Firewall Rule for the resource that has a more restrictive ACL, which does not permit connection from the internet. Note: This policy alerts AWS workloads correctly and for Azure and GCP this policy could also trigger alerts for NAT Gateway configured resources.

### Resource(s) Failed:

eni-08ed2d71b4d68332d, PANW-WebServer-awsjamconfig, eni-00ba3b413a9e8a932

### Recommendations:

1. Log in to the Cloud Console
2. Search for the resource reported in the alert
3. Check if the Security Group/Firewall Rule of the resource indeed allows connections from the internet
4. Assign another Security Group/Firewall Rule to the resource that has a more restrictive ACL, which does not permit connection from the internet

# 4. Encrypt transmission of cardholder data across open, public networks

4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: - Only trusted keys and certificates are accepted. - The protocol in use only supports secure versions or configurations. - The encryption strength is appropriate for the encryption methodology in use.

## AWS CloudFront origin protocol policy does not enforce HTTPS-only

| | |
|---|---|
| Compliance Section: 4.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 2 | |

### Description:

This policy identifies AWS CloudFront which has an origin protocol policy that does not enforce HTTPS-only. Enforcing HTTPS protocol policy between origin and CloudFront will encrypt all communication and will be more secure. As a security best practice, enforce HTTPS-only traffic between a CloudFront distribution and the origin.

### Recommendations:

Communication between CloudFront and your Custom Origin should enforce HTTPS-only traffic. Modify the CloudFront Origin's Origin Protocol Policy to HTTPS only.

1. Go to the AWS console CloudFront dashboard.
2. Select your distribution Id.
3. Select the 'Origins' tab.
4. Check the origin you want to modify then select Edit.
5. Change the Origin Protocol Policy to 'https-only.'
6. Select 'Yes, Edit.'

# 4. Encrypt transmission of cardholder data across open, public networks

4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: - Only trusted keys and certificates are accepted. - The protocol in use only supports secure versions or configurations. - The encryption strength is appropriate for the encryption methodology in use.

## AWS ElastiCache Redis cluster with in-transit encryption disabled (Replication group)

| | |
|---|---|
| Compliance Section: 4.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies ElastiCache Redis clusters that are replication groups and have in-transit encryption disabled. It is highly recommended to implement in-transit encryption in order to protect data from unauthorized access as it travels through the network, between clients and cache servers. Enabling data encryption in-transit helps prevent unauthorized users from reading sensitive data between your Redis clusters and their associated cache storage systems.

### Recommendations:

AWS ElastiCache Redis cluster in-transit encryption can be set, only at the time of creation of the cluster. So to resolve this alert, create a new cluster with in-transit encryption enabled, then migrate all required ElastiCache Redis cluster data from the reported ElastiCache Redis cluster to this newly created cluster and delete reported ElastiCache Redis cluster.
To create new ElastiCache Redis cluster with In-transit encryption set, perform the following:
1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to ElastiCache Dashboard
4. Click on Redis
5. Click on 'Create' button
6. On the 'Create your Amazon ElastiCache cluster' page,
a. Select 'Redis' cache engine type.
b. Enter a name for the new cache cluster
c. Select Redis engine version from 'Engine version compatibility' dropdown list.
Note: As of July 2018, In-transit encryption can be enabled only for AWS ElastiCache clusters with Redis engine version 3.2.6 and 4.0.10.
d. Click on 'Advanced Redis settings' to expand the cluster advanced settings panel
e. Select 'Encryption in-transit' checkbox to enable encryption along with other necessary parameters
7. Click on 'Create' button to launch your new ElastiCache Redis cluster
To delete reported ElastiCache Redis cluster, perform the following:
1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to ElastiCache Dashboard
4. Click on Redis
5. Select reported Redis cluster
6. Click on 'Delete' button
7. In the 'Delete Cluster' dialog box, if you want a backup for your cluster select 'Yes' from the 'Create final backup' dropdown menu, provide a name for the cluster backup, then click on 'Delete'.

# 4. Encrypt transmission of cardholder data across open, public networks

4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: - Only trusted keys and certificates are accepted. - The protocol in use only supports secure versions or configurations. - The encryption strength is appropriate for the encryption methodology in use.

## AWS Kinesis streams encryption using default KMS keys instead of Customer's Managed Master Keys

| | |
|---|---|
| Compliance Section: 4.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 3 | |

### Description:

This policy identifies the AWS Kinesis streams which are encrypted with default KMS keys and not with Master Keys managed by Customer. It is a best practice to use customer managed Master Keys to encrypt your Amazon Kinesis streams data. It gives you full control over the encrypted data.

### Recommendations:

1. Sign in to the AWS Console
2. Go to Kinesis Service
3. Select the reported Kinesis data stream for the corresponding region
4. Under Server-side encryption, Click on Edit
5. Choose Enabled
6. Under KMS master key, You can choose any KMS other than the default (Default) aws/kinesis
7. Click Save

# 4. Encrypt transmission of cardholder data across open, public networks

4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: - Only trusted keys and certificates are accepted. - The protocol in use only supports secure versions or configurations. - The encryption strength is appropriate for the encryption methodology in use.

## AWS SageMaker notebook instance not configured with data encryption at rest using KMS key

| | |
|---|---|
| Compliance Section: 4.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies SageMaker notebook instances that are not configured with data encryption at rest using the AWS managed KMS key. It is recommended to implement encryption at rest in order to protect data from unauthorized entities. For more details: https://docs.aws.amazon.com/sagemaker/latest/dg/encryption-at-rest.html

### Recommendations:

AWS SageMaker notebook instance can not be configured with data encryption at rest once it is created. You need to create a new notebook instance with encryption at rest using the KMS key; migrate all required data from the reported notebook instance to the newly created notebook instance before you delete the reported notebook instance.

To create a New AWS SageMaker notebook instance,

1. Log in to AWS console
2. Navigate to the AWS SageMaker dashboard
3. Choose Notebook instances and then choose 'Create notebook instance'
4. On the Create notebook instance page, From the 'Permissions and encryption' section,
select the KMS key from the 'Encryption key - optional' dropdown list. If no KMS keys already, you have to create a KMS key first.
5. Choose other parameters as per your requirement and click on the 'Create notebook instance' button

To delete reported notebook instance,

1. Log in to AWS console
2. Navigate to the AWS SageMaker dashboard
3. Choose Notebook instances and Choose the reported notebook instance
4. Click on the 'Actions' dropdown menu and, select the 'Stop' option, and when instance stops, select the 'Delete' option.
5. Within Delete <notebook-instance-name> dialog box, click the Delete button to confirm the action.

# 4. Encrypt transmission of cardholder data across open, public networks

4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: - Only trusted keys and certificates are accepted. - The protocol in use only supports secure versions or configurations. - The encryption strength is appropriate for the encryption methodology in use.

## AWS Glue connection do not have SSL configured

| | |
|---|---|
| Compliance Section: 4.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies the Glue connections that are not configured with SSL to encrypt connections. It is recommended to use an SSL connection with hostname matching is enforced for the DB connection on the client; enforcing SSL connections help protect against 'man in the middle' attacks by encrypting the data stream between connections.

### Recommendations:

1. Log in to the AWS Console
2. In the console, select the specific region from the region drop-down on the top right corner, for which the alert is generated
3. Navigate to AWS Glue service
4. Click on 'Connections', Click on the reported Connection
5. Click on 'Edit'
6. On the 'Edit connection' page, Select 'Require SSL connection'
7. Click on 'Next'
8. Click on 'Finish'

# 4. Encrypt transmission of cardholder data across open, public networks

4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: - Only trusted keys and certificates are accepted. - The protocol in use only supports secure versions or configurations. - The encryption strength is appropriate for the encryption methodology in use.

## AWS EMR cluster is not configured with CSE CMK for data at rest encryption (Amazon S3 with EMRFS)

| | |
|---|---|
| Compliance Section: 4.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies EMR clusters which are not configured with Client Side Encryption with Customer Master Keys(CSE CMK) for data at rest encryption of Amazon S3 with EMRFS. As a best practice, use Customer Master Keys (CMK) to encrypt the data in your EMR cluster and ensure full control over your data.

### Recommendations:

1. Log in to the AWS Console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to 'EMR' dashboard from 'Services' dropdown
4. Go to 'Security configurations', click 'Create'
5. On the Create security configuration window,
6. In 'Name' box, provide a name for the new EMR security configuration.
7. For encryption At Rest click the checkbox for 'Enable at-rest encryption for EMRFS data in Amazon S3'.
8. From the dropdown 'Default encryption mode' select 'CSE-Custom'. Follow below link for configuration steps.
https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-encryption-enable.html
9. Click on 'Create' button
10. On the left menu of EMR dashboard Click 'Clusters'
11. Select the EMR cluster for which the alert has been generated and click on the 'Clone' button from the top menu
12. In the Cloning popup, choose 'Yes' and Click 'Clone'.
13. On the Create Cluster page, in the Security Options section, click on 'security configuration'
14. From the 'Security configuration' drop down select the name of the security configuration created at step 4 to step 8, click 'Create Cluster'
15. Once you the new cluster is set up verify its working and terminate the source cluster in order to stop incurring charges for it.
16. On the left menu of EMR dashboard Click 'Clusters', from the list of clusters select the source cluster which is alerted
17. Click on the 'Terminate' button from the top menu.
18. On the 'Terminate clusters' pop-up, click 'Terminate'.

# 4. Encrypt transmission of cardholder data across open, public networks

4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: - Only trusted keys and certificates are accepted. - The protocol in use only supports secure versions or configurations. - The encryption strength is appropriate for the encryption methodology in use.

## AWS Elastic Load Balancer v2 (ELBv2) SSL negotiation policy configured with weak ciphers

| | |
|---|---|
| Compliance Section: 4.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies Elastic Load Balancers v2 (ELBv2) which are configured with SSL negotiation policy containing weak ciphers. An SSL cipher is an encryption algorithm that uses encryption keys to create a coded message. SSL protocols use several SSL ciphers to encrypt data over the Internet. As many of the other ciphers are not secure/weak, it is recommended to use only the ciphers recommended in the following AWS link: https://docs.aws.amazon.com/elasticloadbalancing/latest/application/create-https-listener.html

### Recommendations:

1. Log in to the AWS console
2. In the console, select the specific region from the region drop-down on the top right corner, for which the alert is generated
3. Go to the EC2 Dashboard, and select 'Load Balancers'
4. Click on the reported Load Balancer
5. On the 'Listeners' tab, Choose the 'HTTPS' or 'SSL' rule; Click on 'Edit', Change 'Security policy' to other than 'ELBSecurityPolicy-TLS-1-0-2015-04' as it contains DES-CBC3-SHA cipher, which is a weak cipher.
6. Click on 'Update' to save your changes.

# 4. Encrypt transmission of cardholder data across open, public networks

4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: - Only trusted keys and certificates are accepted. - The protocol in use only supports secure versions or configurations. - The encryption strength is appropriate for the encryption methodology in use.

## AWS EMR cluster is not enabled with data encryption at rest

| | |
|---|---|
| Compliance Section: 4.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies AWS EMR clusters for which data encryption at rest is not enabled. Encryption of data at rest is required to prevent unauthorized users from accessing the sensitive information available on your EMR clusters and associated storage systems.

### Recommendations:

1. Login to the AWS Console.
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated.
3. Navigate to 'EMR' dashboard from 'Services' dropdown.
4. Go to 'Security configurations', click 'Create'.
5. On the Create security configuration window,
6. In 'Name' box, provide a name for the new EMR security configuration.
7. For encryption At Rest select the required encryption type ('S3 encryption'/'Local disk encryption'/both) and follow below link for enabling the same.
8. https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-encryption-enable.html
9. Click on 'Create' button.
10. On the left menu of EMR dashboard Click 'Clusters'.
11. Select the EMR cluster for which the alert has been generated and click on the 'Clone' button from the top menu.
12. In the Cloning popup, choose 'Yes' and Click 'Clone'.
13. On the Create Cluster page, in the Security Options section, click on 'security configuration'.
14. From the 'Security configuration' drop down select the name of the security configuration created at step 4 to step 8, click 'Create Cluster'.
15. Once you the new cluster is set up verify its working and terminate the source cluster in order to stop incurring charges for it.
16. On the left menu of EMR dashboard Click 'Clusters', from the list of clusters select the source cluster which is alerted.
17. Click on the 'Terminate' button from the top menu.
18. On the 'Terminate clusters' pop-up, click 'Terminate'.

# 4. Encrypt transmission of cardholder data across open, public networks

4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: - Only trusted keys and certificates are accepted. - The protocol in use only supports secure versions or configurations. - The encryption strength is appropriate for the encryption methodology in use.

## AWS Elastic Load Balancer (Classic) SSL negotiation policy configured with vulnerable SSL protocol

| | |
|---|---|
| Compliance Section: 4.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies Elastic Load Balancers (Classic) which are configured with SSL negotiation policy containing vulnerable SSL protocol. The SSL protocol establishes a secure connection between a client and a server and ensures that all the data passed between the client and your load balancer is private. As a security best practice, it is recommended to use the latest version SSL protocol.

### Recommendations:

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to EC2 Dashboard
4. Click on 'Load Balancers' (Left Panel)
5. Click on the reported Load Balancer
6. On 'Listeners' tab, Click on 'Edit' button
7. On 'Edit Listeners' popup for rule 'HTTPS/SSL',
- If your cipher is 'Predefined Security Policy', change 'Cipher' to 'ELBSecurityPolicy-TLS-1-2-2017-01 or latest'
OR
- If your cipher is 'Custom Security Policy', Choose 'Protocol-TLSv1.2' only on 'SSL Protocols' section
8. Click on 'Save'

# 4. Encrypt transmission of cardholder data across open, public networks

4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: - Only trusted keys and certificates are accepted. - The protocol in use only supports secure versions or configurations. - The encryption strength is appropriate for the encryption methodology in use.

## AWS Kinesis streams are not encrypted using Server Side Encryption

| | |
|---|---|
| Compliance Section: 4.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This Policy identifies the AWS Kinesis streams which are not encrypted using Server Side Encryption. Server Side Encryption is used to encrypt your sensitive data before it is written to the Kinesis stream storage layer and decrypted after it is retrieved from storage.

### Recommendations:

1. Sign in to the AWS Console
2. Go to Kinesis Service
3. Select the reported Kinesis data stream for the corresponding region
4. Under Server-side encryption, Click on Edit
5. Choose Enabled
6. Under KMS master key, You can choose any KMS other than the default (Default) aws/kinesis
7. Click Save

# 4. Encrypt transmission of cardholder data across open, public networks

4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: - Only trusted keys and certificates are accepted. - The protocol in use only supports secure versions or configurations. - The encryption strength is appropriate for the encryption methodology in use.

## AWS CloudFront distribution is using insecure SSL protocols for HTTPS communication

| | |
|---|---|
| Compliance Section: 4.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 2 | |

### Description:

CloudFront, a content delivery network (CDN) offered by AWS, is not using a secure cipher for distribution. It is a best security practice to enforce the use of secure ciphers TLSv1.0, TLSv1.1, and/or TLSv1.2 in a CloudFront Distribution's certificate configuration. This policy scans for any deviations from this practice and returns the results.

### Recommendations:

Communication between CloudFront and your Custom Origin should enforce the use of secure ciphers. Modify the CloudFront Origin's Origin SSL Protocol to include TLSv1.0, TLSv1.1, and/or TLSv1.2.

1. Go to the AWS console CloudFront dashboard.
2. Select your distribution Id.
3. Select the 'Origins' tab.
4. Check the origin you want to modify then select Edit.
5. Remove (uncheck) 'SSLv3' from Origin SSL Protocols.
6. Select 'Yes, Edit.'

# 4. Encrypt transmission of cardholder data across open, public networks

4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: - Only trusted keys and certificates are accepted. - The protocol in use only supports secure versions or configurations. - The encryption strength is appropriate for the encryption methodology in use.

## AWS CloudTrail logs are not encrypted using Customer Master Keys (CMKs)

| | |
|---|---|
| Compliance Section: 4.1 | First Seen: N/A |
| Resource(s) Failed: 2 | Resource Type: CloudTrail Setting |
| Resource(s) Passed: 0 | |

### Description:

Checks to ensure that CloudTrail logs are encrypted. AWS CloudTrail is a service that enables governance, compliance, operational & risk auditing of the AWS account. It is a compliance and security best practice to encrypt the CloudTrail data since it may contain sensitive information.

### Resource(s) Failed:

aws-controltower-BaselineCloudTrail, cloud-trail-demo

### Recommendations:

1. Login to AWS Console and navigate to the 'CloudTrail' service.
2. For each trail, under Configuration > Storage Location, select 'Yes' to 'Encrypt log files' setting
3.Choose and existing KMS key or create a new one to encrypt the logs with.

# 4. Encrypt transmission of cardholder data across open, public networks

4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: - Only trusted keys and certificates are accepted. - The protocol in use only supports secure versions or configurations. - The encryption strength is appropriate for the encryption methodology in use.

## AWS Redshift Cluster not encrypted using Customer Managed Key

| | |
|---|---|
| Compliance Section: 4.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 3 | |

### Description:

This policy identifies Redshift Clusters which are encrypted with default KMS keys and not with Keys managed by Customer. It is a best practice to use customer managed KMS Keys to encrypt your Redshift databases data. Customer-managed CMKs give you more flexibility, including the ability to create, rotate, disable, define access control for, and audit the encryption keys used to help protect your data.

### Recommendations:

To enable encryption with Customer Managed Key on your Redshift cluster follow the steps mentioned in below URL: https://docs.aws.amazon.com/redshift/latest/mgmt/changing-cluster-encryption.html

# 4. Encrypt transmission of cardholder data across open, public networks

4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: - Only trusted keys and certificates are accepted. - The protocol in use only supports secure versions or configurations. - The encryption strength is appropriate for the encryption methodology in use.

## AWS DynamoDB encrypted using AWS owned CMK instead of AWS managed CMK

| | |
|---|---|
| Compliance Section: 4.1 | First Seen: N/A |
| Resource(s) Failed: 4 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies the DynamoDB tables that use AWS owned CMK (default ) instead of AWS managed CMK (KMS ) to encrypt data. AWS managed CMK provide additional features such as the ability to view the CMK and key policy, and audit the encryption and decryption of DynamoDB tables.

### Resource(s) Failed:

mybookstore-Books, mybookstore-Cart, mybookstore-Orders, goalsapp

### Recommendations:

1. Sign in to AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated.
3. Navigate to 'DynamoDB' dashboard
4. Select the reported table from the list of DynamoDB tables
5. In 'Overview' tab, go to 'Table Details' section
6. Click on the 'Manage Encryption' link available for 'Encryption Type'
7. On 'Manage Encryption' pop up window, Select 'KMS' as the encryption type.

# 4. Encrypt transmission of cardholder data across open, public networks

4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: - Only trusted keys and certificates are accepted. - The protocol in use only supports secure versions or configurations. - The encryption strength is appropriate for the encryption methodology in use.

## AWS SQS queue encryption using default KMS key instead of CMK

| | |
|---|---|
| Compliance Section: 4.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies SQS queues which are encrypted with default KMS keys and not with Customer Master Keys(CMKs). It is a best practice to use customer managed Master Keys to encrypt your SQS queue messages. It gives you full control over the encrypted messages data.

### Recommendations:

1. Sign in to the AWS console
2. Select the region, from the region drop-down, in which the alert is generated
3. Navigate to Simple Queue Service (SQS) dashboard
4. Choose the reported Simple Queue Service (SQS)
5. Click on 'Queue Actions' and Choose 'Configure Queue' from the dropdown
6. On 'Configure' popup, Under 'Server-Side Encryption (SSE) Settings' section; Choose an 'AWS KMS Customer Master Key (CMK)' from the drop-down list or copy existing key ARN instead of (Default) alias/aws/sqs key.
7. Click on 'Save Changes'

# 4. Encrypt transmission of cardholder data across open, public networks

4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: - Only trusted keys and certificates are accepted. - The protocol in use only supports secure versions or configurations. - The encryption strength is appropriate for the encryption methodology in use.

## AWS EMR cluster is not configured with SSE KMS for data at rest encryption (Amazon S3 with EMRFS)

| | |
|---|---|
| Compliance Section: 4.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies EMR clusters which are not configured with Server Side Encryption(SSE KMS) for data at rest encryption of Amazon S3 with EMRFS. As a best practice, use SSE-KMS for server side encryption to encrypt the data in your EMR cluster and ensure full control over your data.

### Recommendations:

1. Log in to the AWS Console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to 'EMR' dashboard from 'Services' dropdown
4. Go to 'Security configurations', click 'Create'
5. On the Create security configuration window,
6. In 'Name' box, provide a name for the new EMR security configuration
7. For encryption At Rest click the checkbox for 'Enable at-rest encryption for EMRFS data in Amazon S3'
8. From the dropdown 'Default encryption mode' select 'SSE-KMS'. Follow below link for configuration steps.
https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-encryption-enable.html
9. Click on 'Create' button.
10. On the left menu of EMR dashboard Click 'Clusters'.
11. Select the EMR cluster for which the alert has been generated and click on the 'Clone' button from the top menu.
12. In the Cloning popup, choose 'Yes' and Click 'Clone'.
13. On the Create Cluster page, in the Security Options section, click on 'security configuration'.
14. From the 'Security configuration' drop down select the name of the security configuration created at step 4 to step 8, click 'Create Cluster'
15. Once you the new cluster is set up verify its working and terminate the source cluster in order to stop incurring charges for it.
16. On the left menu of EMR dashboard Click 'Clusters', from the list of clusters select the source cluster which is alerted
17. Click on the 'Terminate' button from the top menu
18. On the 'Terminate clusters' pop-up, click 'Terminate'.

# 4. Encrypt transmission of cardholder data across open, public networks

4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: - Only trusted keys and certificates are accepted. - The protocol in use only supports secure versions or configurations. - The encryption strength is appropriate for the encryption methodology in use.

## AWS Database Migration Service endpoint do not have SSL configured

| | |
|---|---|
| Compliance Section: 4.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies Database Migration Service (DMS) endpoints that are not configured with SSL to encrypt connections for source and target endpoints. It is recommended to use SSL connection for source and target endpoints; enforcing SSL connections help protect against 'man in the middle' attacks by encrypting the data stream between endpoint connections. NOTE: Not all databases use SSL in the same way. An Amazon Redshift endpoint already uses an SSL connection and does not require an SSL connection set up by AWS DMS. So there are some exlcusions included in policy RQL to report only those endpoints which can be configured using DMS SSL feature. For more details: https://docs.aws.amazon.com/dms/latest/userguide/CHAP_Security.html#CHAP_Security.SSL

### Recommendations:

1. Log in to the AWS Console
2. Navigate to the AWS DMS dashboard
3. In the navigation pane, choose 'Endpoints'
4. Select the reported DMS endpoint
5. Under 'Actions', choose 'Modify'
6. In the 'Endpoint configuration' section, select the 'Secure Socket Layer (SSL) mode' from the dropdown list select suitable SSL mode according to your requirement other than 'none'.
7. Click on 'Save'

NOTE: Before modifying the SSL setting, you should be configured with the proper certificate you want to use for SSL connection under the DMS 'Certificate' service.

# 4. Encrypt transmission of cardholder data across open, public networks

4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: - Only trusted keys and certificates are accepted. - The protocol in use only supports secure versions or configurations. - The encryption strength is appropriate for the encryption methodology in use.

## AWS access keys are not rotated for 90 days

| | |
|---|---|
| Compliance Section: 4.1 | First Seen: N/A |
| Resource(s) Failed: 4 | Resource Type: Other |
| Resource(s) Passed: 11 | |

### Description:

This policy identifies IAM users for which access keys are not rotated for 90 days. Access keys are used to sign API requests to AWS. As a security best practice, it is recommended that all access keys are regularly rotated to make sure that in the event of key compromise, unauthorized users are not able to gain access to your AWS services.

### Resource(s) Failed:

PrismaCloudCompute, CTF_ADMIN_VM, CTF_ADMIN, rsingh1@paloaltonetworks.com

### Recommendations:

1. Sign in to the AWS console and navigate to the 'IAM' service.
2. Click on the user that was reported in the alert.
3. Click on 'Security Credentials' and for each 'Access Key'.
4. Follow the instructions below to rotate the Access Keys that are older than 90 days.

https://aws.amazon.com/blogs/security/how-to-rotate-access-keys-for-iam-users/

# 4. Encrypt transmission of cardholder data across open, public networks

4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: - Only trusted keys and certificates are accepted. - The protocol in use only supports secure versions or configurations. - The encryption strength is appropriate for the encryption methodology in use.

## AWS EMR cluster is not enabled with data encryption in transit

| | |
|---|---|
| Compliance Section: 4.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies AWS EMR clusters which are not enabled with data encryption in transit. It is highly recommended to implement in-transit encryption in order to protect data from unauthorized access as it travels through the network, between clients and storage server. Enabling data encryption in-transit helps prevent unauthorized users from reading sensitive data between your EMR clusters and their associated storage systems.

### Recommendations:

1.Login to the AWS Console.
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated.
3. Navigate to 'EMR' dashboard from 'Services' dropdown
4. Go to 'Security configurations', click 'Create'.
5. On the Create security configuration window,
6. In 'Name' box, provide a name for the new EMR security configuration.
7. Under 'Data in transit encryption', check the box 'Enable in-transit encryption'.
8. From the dropdown of 'TLS certificate provider' select the appropriate certificate provider type and follow below link to create them.
Reference: https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-encryption-enable.html
9. Click on 'Create' button.
10. On the left menu of EMR dashboard Click 'Clusters'.
11. Select the EMR cluster for which the alert has been generated and click on the 'Clone' button from the top menu.
12. In the Cloning popup, choose 'Yes' and Click 'Clone'.
13. On the Create Cluster page, in the Security Options section, click on 'security configuration'.
14. From the 'Security configuration' drop down select the name of the security configuration created at step 4 to step 8, click 'Create Cluster'.
15. Once you the new cluster is set up verify its working and terminate the source cluster in order to stop incurring charges for it.
16. On the left menu of EMR dashboard Click 'Clusters', from the list of clusters select the source cluster which is alerted.
17. Click on the 'Terminate' button from the top menu.
18. On the 'Terminate clusters' pop-up, click 'Terminate'.

# 4. Encrypt transmission of cardholder data across open, public networks

4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: - Only trusted keys and certificates are accepted. - The protocol in use only supports secure versions or configurations. - The encryption strength is appropriate for the encryption methodology in use.

## AWS Elastic File System (EFS) not encrypted using Customer Managed Key

| | |
|---|---|
| Compliance Section: 4.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 3 | |

### Description:

This policy identifies Elastic File Systems (EFSs) which are encrypted with default KMS keys and not with Keys managed by Customer. It is a best practice to use customer managed KMS Keys to encrypt your EFS data. It gives you full control over the encrypted data.

### Recommendations:

AWS EFS Encryption of data at rest can only be enabled during file system creation. So to resolve this alert, create a new EFS with encryption enabled with the customer-managed key, then migrate all required data from the reported EFS to this newly created EFS and delete reported EFS.
To create new EFS with encryption enabled, perform the following:
1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to EFS dashboard
4. Click on 'File systems' (Left Panel)
5. Click on 'Create file system' button
6. On the 'Configure file system access' step, specify EFS details as per your requirements and Click on 'Next Step'
7. On the 'Configure optional settings' step, Under 'Enable encryption' Choose 'Enable encryption of data at rest' and Select customer managed key [i.e. Other than (default)aws/elasticfilesystem] from 'Select KMS master key' dropdown list along with other parameters and Click on 'Next Step'
8. On the 'Review and create' step, Review all your setting and Click on 'Create File System' button
To delete reported EFS which does not has encryption, perform the following:
1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to EFS dashboard
4. Click on 'File systems' (Left Panel)
5. Select the reported file system
6. Click on 'Actions' drop-down
7. Click on 'Delete file system'
8. In the 'Permanently delete file system' popup box, To confirm the deletion enter the file system's ID and Click on 'Delete File System'

# 4. Encrypt transmission of cardholder data across open, public networks

4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: - Only trusted keys and certificates are accepted. - The protocol in use only supports secure versions or configurations. - The encryption strength is appropriate for the encryption methodology in use.

## AWS SageMaker notebook instance not encrypted using Customer Managed Key

| | |
|---|---|
| Compliance Section: 4.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies SageMaker notebook instances that are not encrypted using Customer Managed Key. SageMaker notebook instances should be encrypted with Amazon KMS Customer Master Keys (CMKs) instead of AWS managed-keys in order to have more granular control over the data-at-rest encryption/decryption process and meet compliance requirements. For more details: https://docs.aws.amazon.com/sagemaker/latest/dg/encryption-at-rest.html

### Recommendations:

AWS SageMaker notebook instance encryption can not be modified once it is created. You need to create a new notebook instance with encryption using a custom KMS key; migrate all required data from the reported notebook instance to the newly created notebook instance before you delete the reported notebook instance.

To create a New AWS SageMaker notebook instance,

1. Log in to AWS console
2. Navigate to the AWS SageMaker dashboard
3. Choose Notebook instances and then choose 'Create notebook instance'
4. On the Create notebook instance page, within the 'Permissions and encryption' section,

From the 'Encryption key - optional' dropdown list, choose a custom KMS key for the new SageMaker notebook instance.

5. Choose other parameters as per your requirement and click on the 'Create notebook instance' button

To delete reported notebook instance,

1. Log in to AWS console
2. Navigate to the AWS SageMaker dashboard
3. Choose Notebook instances and Choose the reported notebook instance
4. Click on the 'Actions' dropdown menu, select the 'Stop' option, and when instance stops, select the 'Delete' option.
5. Within Delete <notebook-instance-name> dialog box, click the Delete button to confirm the action.

# 4. Encrypt transmission of cardholder data across open, public networks

4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: - Only trusted keys and certificates are accepted. - The protocol in use only supports secure versions or configurations. - The encryption strength is appropriate for the encryption methodology in use.

## AWS IAM SSH keys for AWS CodeCommit have aged more than 90 days without being rotated

| | |
|---|---|
| Compliance Section: 4.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies all of your IAM SSH public keys which haven't been rotated in the past 90 days. It is recommended to verify that they are rotated on a regular basis in order to protect your AWS CodeCommit repositories.

### Recommendations:

1. Login to AWS Console
2. Goto IAM and select Users
3. Choose the reported user
4. Goto Security Credential
5. Delete the SSH Key ID and upload a new SSH Key

Key creation steps: https://docs.aws.amazon.com/codecommit/latest/userguide/setting-up-ssh-unixes.html

# 4. Encrypt transmission of cardholder data across open, public networks

4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: - Only trusted keys and certificates are accepted. - The protocol in use only supports secure versions or configurations. - The encryption strength is appropriate for the encryption methodology in use.

## AWS Elastic Load Balancer with listener TLS/SSL is not configured

| | |
|---|---|
| Compliance Section: 4.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Managed Load Balancer |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies AWS Elastic Load Balancers which have non-secure listeners. As Load Balancers will be handling all incoming requests and routing the traffic accordingly. The listeners on the load balancers should always receive traffic over secure channel with a valid SSL certificate configured.

### Recommendations:

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to EC2 dashboard
4. Click on 'Load Balancers' (Left Panel)
5. Select the reported ELB
6. On the Listeners tab, Click the 'Edit' button under the available listeners
7. In the Load Balancer Protocol, Select 'HTTPS (Secure HTTP)' or 'SSL (Secure TCP)'
8. In the SSL Certificate column, click 'Change'
9. On 'Select Certificate' popup dialog, Choose a certificate from ACM or IAM or upload a new certificate based on requirement and Click on 'Save'
10. Back to the 'Edit listeners' dialog box, review the secure listeners configuration, then click on 'Save'

# 4. Encrypt transmission of cardholder data across open, public networks

4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: - Only trusted keys and certificates are accepted. - The protocol in use only supports secure versions or configurations. - The encryption strength is appropriate for the encryption methodology in use.

## AWS RDS database not encrypted using Customer Managed Key

| | |
|---|---|
| Compliance Section: 4.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 5 | |

### Description:

This policy identifies RDS databases that are encrypted with default KMS keys and not with customer managed keys. As a best practice, use customer managed keys to encrypt the data on your RDS databases and maintain control of your keys and data on sensitive workloads.

### Recommendations:

Because you can set AWS RDS database encryption only during database creation, the process for resolving this alert requires you to create a new RDS database with a customer managed key for encryption, migrate the data from the reported database to this newly created database, and delete the RDS database identified in the alert.
To create a new RDS database with encryption using a customer managed key:
1. Log in to the AWS console.
2. Select the region for which the alert was generated.
3. Navigate to the Amazon RDS Dashboard.
4. Select 'Create database'.
5. On the 'Select engine' page, select 'Engine options' and 'Next'.
6. On the 'Choose use case' page, select 'Use case' of database and 'Next'.
7. On the 'Specify DB details' page, specify the database details you need and click 'Next'.
Note: Amazon RDS encryption has some limitation on region and type instances. For Availability of Amazon RDS Encryption refer to: https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html#Overview.Encryption.Availability
8. On the 'Configure advanced settings' page, Under 'Encryption', select 'Enable encryption' and select the customer managed key [i.e. Other than (default)aws/rds] from 'Master key' dropdown list].
9. Select 'Create database'.
To delete the RDS database that uses the default KMS keys, which triggered the alert:
1. Log in to the AWS console
2. Select the region for which the alert was generated.
3. Navigate to the Amazon RDS Dashboard.
4. Click on Instances, and select the reported RDS database.
5. Select the 'Instance actions' drop-down and click 'Delete'.
7. In the 'Delete' dialog, select the 'Create final snapshot?' checkbox, if you want a backup. Provide a name for the final snapshot, confirm deletion and select 'Delete'.

# 4. Encrypt transmission of cardholder data across open, public networks

4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: - Only trusted keys and certificates are accepted. - The protocol in use only supports secure versions or configurations. - The encryption strength is appropriate for the encryption methodology in use.

## AWS Elasticsearch domain Encryption for data at rest is disabled

| | |
|---|---|
| Compliance Section: 4.1 | First Seen: N/A |
| Resource(s) Failed: 1 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies Elasticsearch domains for which encryption is disabled. Encryption of data at rest is required to prevent unauthorized users from accessing the sensitive information available on your Elasticsearch domains components. This may include all data of file systems, primary and replica indices, log files, memory swap files and automated snapshots. The Elasticsearch uses AWS KMS service to store and manage the encryption keys. It is highly recommended to implement encryption at rest when you are working with production data that have sensitive information, to protect from unauthorized access.

### Resource(s) Failed:

mybookstore-domain

### Recommendations:

Enabling the encryption feature on existing domains requires Elasticsearch 6.7 or later. If your Elasticsearch 6.7 or later, follow below steps to enable encryption on existing Elasticsearch domain:

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to Elasticsearch Service Dashboard
4. Choose reported Elasticsearch domain
5. Click on 'Actions' button, from drop-down select 'Modify encryptions'
6.In Modify encryptions page, Select the 'Enable encryption of data at rest' checkbox and Choose KMS key as per your requirement. It is recommended to choose KMS CMKs instead of default KMS [Default(aws/es)]; to get more grannular control on your Elasticsearch domain data.
7. Click on 'Submit'.

If your Elasticsearch is less than 6.7 version, then AWS Elasticsearch Domain encryption can be set only at the time of the creation of domain. So to fix this alert, create a new domain with encryption using KMS Keys and then migrate all required Elasticsearch domain data from the reported Elasticsearch domain to this newly created domain.

To set up the new Elasticsearch domain with encryption using KMS Key, refer the following URL:
https://docs.aws.amazon.com/elasticsearch-service/latest/developerguide/es-createupdatedomains.html

To delete reported ES domain, refer the following URL:
https://docs.aws.amazon.com/elasticsearch-service/latest/developerguide/es-gsg-deleting.html

# 4. Encrypt transmission of cardholder data across open, public networks

4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: - Only trusted keys and certificates are accepted. - The protocol in use only supports secure versions or configurations. - The encryption strength is appropriate for the encryption methodology in use.

## AWS Redshift does not have require_ssl configured

| | |
|---|---|
| Compliance Section: 4.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Managed Database |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies Redshift databases in which data connection to and from is occurring on an insecure channel. SSL connections ensures the security of the data in transit.

### Recommendations:

1. Login to the AWS and navigate to the 'Amazon Redshift' service.
2. Expand the identified 'Redshift' cluster and make a note of the 'Cluster Parameter Group'
3. In the navigation panel, click on the 'Parameter group'.
4. Select the identified 'Parameter Group' and click on 'Edit Parameters'.
5. Review the require_ssl flag. Update the parameter 'require_ssl' to true and save it.

Note: If the current parameter group is a Default parameter group, it cannot be edited. You will need to create a new parameter group and point it to an affected cluster.

# 4. Encrypt transmission of cardholder data across open, public networks

4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: - Only trusted keys and certificates are accepted. - The protocol in use only supports secure versions or configurations. - The encryption strength is appropriate for the encryption methodology in use.

## AWS RDS DB cluster is encrypted using default KMS key instead of CMK

| | |
|---|---|
| Compliance Section: 4.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 4 | |

### Description:

This policy identifies RDS DB(Relational Database Service Database) clusters which are encrypted using default KMS key instead of CMK (Customer Master Key). As a security best practice CMK should be used instead of default KMS key for encryption to gain the ability to rotate the key according to your own policies, delete the key, and control access to the key via KMS policies and IAM policies.

### Recommendations:

RDS DB clusters can be encrypted only while creating the database cluster. You can't convert an unencrypted DB cluster to an encrypted one. However, you can restore an unencrypted Aurora DB cluster snapshot to an encrypted Aurora DB cluster. To do this, specify a KMS encryption key when you restore from the unencrypted DB cluster snapshot.
Step 1: To create a 'Snapshot' of the unencrypted DB cluster,
https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/USER_CreateSnapshotCluster.html
NOTE: As you can't restore from a DB cluster snapshot to an existing DB cluster; a new DB cluster is created when you restore. Once the Snapshot status is 'Available'.
Step 2: Follow the below link to restoring the Cluster from a DB Cluster Snapshot,
https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/USER_RestoreFromSnapshot.html
Once the DB cluster is restored and verified, follow below steps to delete the reported DB cluster,
1. Log in to the AWS Management Console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated.
3. Navigate to 'RDS' dashboard from 'Services' dropdown
4. In the navigation pane, choose ‘Databases’
5. In the list of DB instances, choose a writer instance for the DB cluster
6. Choose 'Actions', and then choose 'Delete'
FMI:
1. While deleting a RDS DB cluster, customer has to disable 'Enable deletion protection' otherwise instance cannot be deleted
2. While deleting RDS DB instance , AWS application will ask the end user to take Final snapshot
3. If a RDS DB cluster has a writer role instance, then User has to delete the write instance to delete the main cluster (Delete option won’t be enabled for main RDS DB cluster)

# 4. Encrypt transmission of cardholder data across open, public networks

4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: - Only trusted keys and certificates are accepted. - The protocol in use only supports secure versions or configurations. - The encryption strength is appropriate for the encryption methodology in use.

## AWS Elastic Load Balancer (Classic) SSL negotiation policy configured with insecure ciphers

| | |
|---|---|
| Compliance Section: 4.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies Elastic Load Balancers (Classic) which are configured with SSL negotiation policy containing insecure ciphers. An SSL cipher is an encryption algorithm that uses encryption keys to create a coded message. SSL protocols use several SSL ciphers to encrypt data over the Internet. As many of the other ciphers are not secure, it is recommended to use only the ciphers recommended in the following AWS link: https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-ssl-security-policy.html.

### Recommendations:

1. Sign in to the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Go to the EC2 Dashboard, and select 'Load Balancers'
4. Click on the reported Load Balancer
5. On 'Listeners' tab, Change the cipher for the 'HTTPS/SSL' rule
For a 'Predefined Security Policy', change 'Cipher' to 'ELBSecurityPolicy-TLS-1-2-2017-01' or latest
For a 'Custom Security Policy', select from the secure ciphers as recommended in the below AWS link:
https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-ssl-security-policy.html
6. 'Save' your changes

# 4. Encrypt transmission of cardholder data across open, public networks

4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: - Only trusted keys and certificates are accepted. - The protocol in use only supports secure versions or configurations. - The encryption strength is appropriate for the encryption methodology in use.

## AWS EMR cluster is not enabled with local disk encryption using Custom key provider

| | |
|---|---|
| Compliance Section: 4.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies AWS EMR clusters that are not enabled with local disk encryption using Custom key provider. Applications using the local file system on each cluster instance for intermediate data throughout workloads, where data could be spilled to disk when it overflows memory. With Local disk encryption at place, data at rest can be protected.

### Recommendations:

1. Login to the AWS Console.
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated.
3. Navigate to 'EMR' dashboard from 'Services' dropdown.
4. Go to 'Security configurations', click 'Create'.
5. On the Create security configuration window,
6. In 'Name' box, provide a name for the new EMR security configuration.
7. Under 'Local disk encryption', check the box 'Enable at-rest encryption for local disks'.
8. Select 'Custom' Key provider type from the 'Key provider type' dropdown list.
9. Follow the below link for creating the custom key,
https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-data-encryption-options.html
10. Click on 'Create' button.
11. On the left menu of EMR dashboard Click 'Clusters'.
12. Select the EMR cluster for which the alert has been generated and click on the 'Clone' button from the top menu.
13. In the Cloning popup, choose 'Yes' and Click 'Clone'.
14. On the Create Cluster page, in the Security Options section, click on 'security configuration'.
15. From the 'Security configuration' drop down select the name of the security configuration created at step 4 to step 8, click 'Create Cluster'.
16. Once the new cluster is set up verify its working and terminate the source cluster.
17. On the left menu of EMR dashboard Click 'Clusters', from the list of clusters select the source cluster which is alerted.
18. Click on the 'Terminate' button from the top menu.
19. On the 'Terminate clusters' pop-up, click 'Terminate'.

# 4. Encrypt transmission of cardholder data across open, public networks

4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission.

## AWS ElastiCache Redis cluster with in-transit encryption disabled (Replication group)

| | |
|---|---|
| Compliance Section: 4.1.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies ElastiCache Redis clusters that are replication groups and have in-transit encryption disabled. It is highly recommended to implement in-transit encryption in order to protect data from unauthorized access as it travels through the network, between clients and cache servers. Enabling data encryption in-transit helps prevent unauthorized users from reading sensitive data between your Redis clusters and their associated cache storage systems.

### Recommendations:

AWS ElastiCache Redis cluster in-transit encryption can be set, only at the time of creation of the cluster. So to resolve this alert, create a new cluster with in-transit encryption enabled, then migrate all required ElastiCache Redis cluster data from the reported ElastiCache Redis cluster to this newly created cluster and delete reported ElastiCache Redis cluster.

To create new ElastiCache Redis cluster with In-transit encryption set, perform the following:

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to ElastiCache Dashboard
4. Click on Redis
5. Click on 'Create' button
6. On the 'Create your Amazon ElastiCache cluster' page,

a. Select 'Redis' cache engine type.
b. Enter a name for the new cache cluster
c. Select Redis engine version from 'Engine version compatibility' dropdown list.

Note: As of July 2018, In-transit encryption can be enabled only for AWS ElastiCache clusters with Redis engine version 3.2.6 and 4.0.10.

d. Click on 'Advanced Redis settings' to expand the cluster advanced settings panel
e. Select 'Encryption in-transit' checkbox to enable encryption along with other necessary parameters

7. Click on 'Create' button to launch your new ElastiCache Redis cluster

To delete reported ElastiCache Redis cluster, perform the following:

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to ElastiCache Dashboard
4. Click on Redis
5. Select reported Redis cluster
6. Click on 'Delete' button
7. In the 'Delete Cluster' dialog box, if you want a backup for your cluster select 'Yes' from the 'Create final backup' dropdown menu, provide a name for the cluster backup, then click on 'Delete'.

# 4. Encrypt transmission of cardholder data across open, public networks

4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission.

## AWS EMR cluster is not enabled with data encryption in transit

| | |
|---|---|
| Compliance Section: 4.1.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies AWS EMR clusters which are not enabled with data encryption in transit. It is highly recommended to implement in-transit encryption in order to protect data from unauthorized access as it travels through the network, between clients and storage server. Enabling data encryption in-transit helps prevent unauthorized users from reading sensitive data between your EMR clusters and their associated storage systems.

### Recommendations:

1.Login to the AWS Console.
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated.
3. Navigate to 'EMR' dashboard from 'Services' dropdown
4. Go to 'Security configurations', click 'Create'.
5. On the Create security configuration window,
6. In 'Name' box, provide a name for the new EMR security configuration.
7. Under 'Data in transit encryption', check the box 'Enable in-transit encryption'.
8. From the dropdown of 'TLS certificate provider' select the appropriate certificate provider type and follow below link to create them.
Reference: https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-encryption-enable.html
9. Click on 'Create' button.
10. On the left menu of EMR dashboard Click 'Clusters'.
11. Select the EMR cluster for which the alert has been generated and click on the 'Clone' button from the top menu.
12. In the Cloning popup, choose 'Yes' and Click 'Clone'.
13. On the Create Cluster page, in the Security Options section, click on 'security configuration'.
14. From the 'Security configuration' drop down select the name of the security configuration created at step 4 to step 8, click 'Create Cluster'.
15. Once you the new cluster is set up verify its working and terminate the source cluster in order to stop incurring charges for it.
16. On the left menu of EMR dashboard Click 'Clusters', from the list of clusters select the source cluster which is alerted.
17. Click on the 'Terminate' button from the top menu.
18. On the 'Terminate clusters' pop-up, click 'Terminate'.

# 6. Develop and maintain secure systems and applications

6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: - In accordance with PCI DSS (for example, secure authentication and logging) - Based on industry standards and/or best practices. - Incorporating information security throughout the software-development life cycle

## AWS Elastic Load Balancer (Classic) with cross-zone load balancing disabled

| | |
|---|---|
| Compliance Section: 6.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies Classic Elastic Load Balancers which have cross-zone load balancing disabled. When Cross-zone load balancing enabled, classic load balancer distributes requests evenly across the registered instances in all enabled Availability Zones. Cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled Availability Zone, and improves your application's ability to handle the loss of one or more instances.

### Recommendations:

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to EC2 dashboard
4. Click on 'Load Balancers' (Left Panel)
5. Select the reported ELB
6. On the Description tab, choose 'Change cross-zone load balancing setting'
7. On the 'Configure Cross-Zone Load Balancing' popup dialog, select 'Enable'
8. Click on 'Save'

# 6. Develop and maintain secure systems and applications

6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: - In accordance with PCI DSS (for example, secure authentication and logging) - Based on industry standards and/or best practices. - Incorporating information security throughout the software-development life cycle

## AWS Certificate Manager (ACM) has invalid or failed certificate

| | |
|---|---|
| Compliance Section: 6.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies certificates in ACM which are either in Invalid or Failed state. If the ACM certificate is not validated within 72 hours, it becomes Invalid. An ACM certificate fails when, - the certificate is requested for invalid public domains - the certificate is requested for domains which are not allowed missing contact information - typographical errors In such cases (Invalid or Failed certificate), you will have to request for a new certificate. It is strongly recommended to delete the certificates which are in failed or invalid state.

### Recommendations:

To delete Certificates:

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Go to Certificate Manager(ACM) service
4. Choose the reported certificate
5. Under 'Actions' drop-down click on 'Delete'

# 6. Develop and maintain secure systems and applications

6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: - In accordance with PCI DSS (for example, secure authentication and logging) - Based on industry standards and/or best practices. - Incorporating information security throughout the software-development life cycle

## AWS ECS/ Fargate task definition root user found

| | |
|---|---|
| Compliance Section: 6.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

The user name to use inside the container should not be root. This policy generates an alert if root user is found in your container definition. The User parameter maps to User in the Create a container section of the Docker Remote API and the --user option to docker run Note: This parameter is not supported for Windows containers.

### Recommendations:

Create a task definition revision.

1. Open the Amazon ECS console.
2. From the navigation bar, choose the region that contains your task definition.
3. In the navigation pane, choose Task Definitions.
4. On the Task Definitions page, select the box to the left of the task definition to revise and choose Create new revision.
5. On the Create new revision of Task Definition page, change the existing Container Definitions.
6. Under Security, remove root from the User field.
7. Verify the information and choose Update, then Create.
8. If your task definition is used in a service, update your service with the updated task definition.
9. Deactivate previous task definition

# 6. Develop and maintain secure systems and applications

6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: - In accordance with PCI DSS (for example, secure authentication and logging) - Based on industry standards and/or best practices. - Incorporating information security throughout the software-development life cycle

## AWS CloudTrail log validation is not enabled in all regions

| | |
|---|---|
| Compliance Section: 6.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: CloudTrail Setting |
| Resource(s) Passed: 2 | |

### Description:

This policy identifies AWS CloudTrails in which log validation is not enabled in all regions. CloudTrail log file validation creates a digitally signed digest file containing a hash of each log that CloudTrail writes to S3. These digest files can be used to determine whether a log file was modified after CloudTrail delivered the log. It is recommended that file validation be enabled on all CloudTrails.

### Recommendations:

1. Sign in to the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Access the 'CloudTrail' service.
4. For each trail reported, under Configuration > Storage Location, make sure 'Enable log file validation' is set to 'Yes'.

# 6. Develop and maintain secure systems and applications

6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: - In accordance with PCI DSS (for example, secure authentication and logging) - Based on industry standards and/or best practices. - Incorporating information security throughout the software-development life cycle

## AWS API gateway request parameter is not validated

| | |
|---|---|
| Compliance Section: 6.3 | First Seen: N/A |
| Resource(s) Failed: 30 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies the AWS API gateways for which the request parameters are not validated. When the validation fails, API Gateway fails the request, returns a 400 error response to the caller, and publishes the validation results in CloudWatch Logs. It is recommended to perform basic validation of an API request before proceeding with the integration request to block unvalidated calls to the backend.

### Resource(s) Failed:

uyqi9kdzjc_6pjosh_{id}_OPTIONS, ewpdec3fy2_uexgyv_search_OPTIONS, uyqi9kdzjc_8gi5vu_goals_GET, ewpdec3fy2_0om6hr_bestsellers_GET, ewpdec3fy2_am9nbk_cart_PUT, ewpdec3fy2_myub8s_{id}_OPTIONS, ewpdec3fy2_u1g5xw_books_GET, ewpdec3fy2_fq4hbp_recommendations_OPTIONS, uyqi9kdzjc_6pjosh_{id}_GET, uyqi9kdzjc_6pjosh_{id}_DELETE ...and 20 more

### Recommendations:

1. Login to AWS management console
2. Navigate to 'API Gateway' service
3. Select the region for which the API gateway is reported.
4. Find the alerted API by the API gateway ID which is the first part of reported resource and click on it
5. Navigate to the reported method
6. Click on the clickable link of 'Method Request'
7. Under section ‘Settings' ,click on the pencil symbol for 'Request Validator' field
8. From the dropdown, Select the type of Request Validator as per the requirement
9. Click on the tick symbol next to it to save the changes

# 6. Develop and maintain secure systems and applications

6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: - In accordance with PCI DSS (for example, secure authentication and logging) - Based on industry standards and/or best practices. - Incorporating information security throughout the software-development life cycle

## AWS access keys not used for more than 90 days

| | |
|---|---|
| Compliance Section: 6.3 | First Seen: N/A |
| Resource(s) Failed: 3 | Resource Type: IAM Credentials Report |
| Resource(s) Passed: 12 | |

### Description:

This policy identifies IAM users for which access keys are not used for more than 90 days. Access keys allow users programmatic access to resources. However, if any access key has not been used in the past 90 days, then that access key needs to be deleted (even though the access key is inactive).

### Resource(s) Failed:

CTF_ADMIN_VM, CTF_ADMIN, rsingh1@paloaltonetworks.com

### Recommendations:

To delete the reported AWS User access key follow below mentioned URL:
https://aws.amazon.com/premiumsupport/knowledge-center/delete-access-key/

# 6. Develop and maintain secure systems and applications

6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: - In accordance with PCI DSS (for example, secure authentication and logging) - Based on industry standards and/or best practices. - Incorporating information security throughout the software-development life cycle

## AWS CloudTrail S3 buckets have not enabled MFA Delete

| | |
|---|---|
| Compliance Section: 6.3 | First Seen: N/A |
| Resource(s) Failed: 1 | Resource Type: Other |
| Resource(s) Passed: 12 | |

### Description:

This policy identifies the S3 buckets which do not have Multi-Factor Authentication enabled for CloudTrails. For encryption of log files, CloudTrail defaults to use of S3 server-side encryption (SSE). We recommend adding an additional layer of security by adding MFA Delete to your S3 bucket. This will help to prevent deletion of CloudTrail logs without your explicit authorization. We also encourage you to use a bucket policy that places restrictions on which of your identity access management (IAM) users are allowed to delete S3 objects.

### Resource(s) Failed:

aws-cloudtrail-logs-795462528824-317b0c26

### Recommendations:

Enable MFA Delete on the bucket(s) you have configured to receive CloudTrail log files.
Note: We recommend that you do not configure CloudTrail to write into an S3 bucket that resides in a different AWS account.
Additional information on how to do this can be found here:
http://docs.aws.amazon.com/AmazonS3/latest/dev/Versioning.html#MultiFactorAuthenticationDelete

# 6. Develop and maintain secure systems and applications

6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: - In accordance with PCI DSS (for example, secure authentication and logging) - Based on industry standards and/or best practices. - Incorporating information security throughout the software-development life cycle

## AWS root account configured with Virtual MFA

| | |
|---|---|
| Compliance Section: 6.3 | First Seen: N/A |
| Resource(s) Failed: 1 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies AWS root accounts which are configured with Virtual MFA. Root is an important role in your account and root accounts must be configured with hardware MFA. Hardware MFA adds extra security because it requires users to type a unique authentication code from an approved authentication device when they access AWS websites or services.

### Resource(s) Failed:

arn:aws:iam::795462528824:mfa/root-account-mfa-device

### Recommendations:

To manage MFA devices for your AWS account, you must use your root user credentials to sign in to AWS. You cannot manage MFA devices for the root user while signed in with other credentials.
1. Sign in to the AWS Management Console with your root user credentials
2. Go to IAM
3. Do one of the following:
Option 1: Choose Dashboard, and under Security Status, expand Activate MFA on your root account.
Option 2: On the right side of the navigation bar, select your account name, and then choose My Security Credentials. If necessary, choose Continue to Security Credentials. Then expand the Multi-Factor Authentication (MFA) section on the page.
4. Choose Manage MFA or Activate MFA, depending on which option you chose in the preceding step.
5. In the wizard, choose A hardware MFA device and then choose Next Step.
6. If you have U2F security key as hardware MFA device, choose U2F security key and click on Continue. Next plug the USB U2F security key, when setup is complete click on Close.
If you have any other hardware MFA device, choose Other hardware MFA device option
a. In the Serial Number box, type the serial number that is found on the back of the MFA device.
b. In the Authentication Code 1 box, type the six-digit number displayed by the MFA device. You might need to press the button on the front of the device to display the number.
c. Wait 30 seconds while the device refreshes the code, and then type the next six-digit number into the Authentication Code 2 box. You might need to press the button on the front of the device again to display the second number.
d. Choose Next Step. The MFA device is now associated with the AWS account.
Important:
Submit your request immediately after generating the authentication codes. If you generate the codes and then wait too long to submit the request, the MFA device successfully associates with the user but the MFA device becomes out of sync. This happens because time-based one-time passwords (TOTP) expire after a short period of time. If this happens, you can resync the device.

# 6. Develop and maintain secure systems and applications

6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: - In accordance with PCI DSS (for example, secure authentication and logging) - Based on industry standards and/or best practices. - Incorporating information security throughout the software-development life cycle

## AWS API gateway request authorisation is not set

| | |
|---|---|
| Compliance Section: 6.3 | First Seen: N/A |
| Resource(s) Failed: 11 | Resource Type: Other |
| Resource(s) Passed: 19 | |

### Description:

This policy identifies AWS API Gateways of protocol type REST for which the request authorisation is not set. The method request for API gateways takes the client input that is passed to the back end through the integration request. It is recommended to add authorization type to each of the method to add a layer of protection.

### Resource(s) Failed:

uyqi9kdzjc_6pjosh_{id}_OPTIONS, ewpdec3fy2_uexgyv_search_OPTIONS, ewpdec3fy2_fwiiom_{bookId}_OPTIONS, ewpdec3fy2_dvheqp_orders_OPTIONS, uyqi9kdzjc_8gi5vu_goals_OPTIONS, ewpdec3fy2_am9nbk_cart_OPTIONS, ewpdec3fy2_0om6hr_bestsellers_OPTIONS, ewpdec3fy2_myub8s_{id}_OPTIONS, ewpdec3fy2_fq4hbp_recommendations_OPTIONS, ewpdec3fy2_cafmp8_{bookId}_OPTIONS ...and 1 more

### Recommendations:

1. Login to AWS management console
2. Navigate to 'API Gateway' service
3. Select the region for which the API gateway is reported.
4. Find the alerted API by the API gateway ID which is the first part of reported resource and click on it
5. Navigate to the reported method
6. Click on the clickable link of 'Method Request'
7. Under section 'Settings', click on the pencil symbol for 'Authorization' field
8. From the dropdown, Select the type of Authorization as per the requirement
9. Click on the tick symbol next to it to save the changes

# 6. Develop and maintain secure systems and applications

6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: - In accordance with PCI DSS (for example, secure authentication and logging) - Based on industry standards and/or best practices. - Incorporating information security throughout the software-development life cycle

## AWS VPC not in use

| | |
|---|---|
| Compliance Section: 6.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 82 | |

### Description:

This policy identifies VPCs which are not in use. These VPC resources might be unintentionally launched and AWS also imposes a limit to the number of VPCs allowed per region. So it is recommended to either delete or use effectively such VPCs that do not have resources attached to them.

### Recommendations:

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to VPC Dashboard
4. Click on 'Your VPCs' and Choose the reported VPC
5. If you want use reported VPC, Associate subnets to VPC or If you want to delete VPC, Click on 'Actions' and Choose 'Delete VPC' from the dropdown

# 6. Develop and maintain secure systems and applications

6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: - In accordance with PCI DSS (for example, secure authentication and logging) - Based on industry standards and/or best practices. - Incorporating information security throughout the software-development life cycle

## AWS Elastic Load Balancer (ELB) not in use

| | |
|---|---|
| Compliance Section: 6.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies unused Elastic Load Balancers (ELBs) in your AWS account. Any Elastic Load Balancer in your AWS account is adding charges to your monthly bill, although it is not used by any resources. As a best practice, it is recommended to remove ELBs that are not associated with any instances, it will also help you avoid unexpected charges on your bill.

### Recommendations:

To check and remove ELB that has no registered instances, perform the following:

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to EC2 dashboard
4. In the navigation pane, under 'LOAD BALANCING', click on 'Load Balancers'
5. Select reported Elastic Load Balancer
6. Select the 'Description' tab from the bottom panel
7. In 'Basic Configuration' section, see If the selected load balancer 'Status' is '0 of 0 instances in service'.

It means that there are no registered instances and the ELB can be safely removed.

8. Click the 'Actions' dropdown from the ELB dashboard top menu
9. Select Delete
10. In the 'Delete Load Balancer' pop-up dialog, confirm the action to delete on clicking 'Yes, Delete' button

# 6. Develop and maintain secure systems and applications

6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: - In accordance with PCI DSS (for example, secure authentication and logging) - Based on industry standards and/or best practices. - Incorporating information security throughout the software-development life cycle

## AWS RDS minor upgrades not enabled

| | |
|---|---|
| Compliance Section: 6.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 2 | |

### Description:

When Amazon Relational Database Service (Amazon RDS) supports a new version of a database engine, you can upgrade your DB instances to the new version. There are two kinds of upgrades: major version upgrades and minor version upgrades. Minor upgrades helps maintain a secure and stable RDS with minimal impact on the application. For this reason, we recommend that your automatic minor upgrade is enabled. Minor version upgrades only occur automatically if a minor upgrade replaces an unsafe version, such as a minor upgrade that contains bug fixes for a previous version.

### Recommendations:

Enable RDS auto minor version upgrades.

1. Go to the AWS console RDS dashboard.
2. In the navigation pane, choose Instances.
3. Select the database instance you wish to configure.
4. From the 'Instance actions' menu, select Modify.
5. Under the Maintenance section, choose Yes for Auto minor version upgrade.
6. Select Continue and then Modify DB Instance.

# 6. Develop and maintain secure systems and applications

6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: - In accordance with PCI DSS (for example, secure authentication and logging) - Based on industry standards and/or best practices. - Incorporating information security throughout the software-development life cycle

## AWS API Gateway endpoints without client certificate authentication

| | |
|---|---|
| Compliance Section: 6.3 | First Seen: N/A |
| Resource(s) Failed: 2 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

API Gateway can generate an SSL certificate and use its public key in the backend to verify that HTTP requests to your backend system are from API Gateway. This allows your HTTP backend to control and accept only requests originating from Amazon API Gateway, even if the backend is publicly accessible. Note: Some backend servers may not support SSL client authentication as API Gateway does and could return an SSL certificate error. For a list of incompatible backend servers, see Known Issues. https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-known-issues.html

### Resource(s) Failed:

prod

### Recommendations:

These instructions assume you already completed Generate a Client Certificate Using the API Gateway Console. If not please generate a client certificate by following below steps and then Configure an API to Use SSL Certificates.
Steps to Generate a Client Certificate Using the API Gateway Console:
1. Login to AWS Console
2. Go to API Gateway console
3. In the main navigation pane (Left Panel), choose Client Certificates.
4. From the Client Certificates pane, choose Generate Client Certificate.
5. Optionally, for Edit, choose to add a descriptive title for the generated certificate and choose Save to save the description. API Gateway generates a new certificate and returns the new certificate GUID, along with the PEM-encoded public key.
Steps to Configure an API to Use SSL Certificates:
1. Login to AWS Console
2. Go to API Gateway console
3. In the API Gateway console, create or open an API for which you want to use the client certificate. Make sure the API has been deployed to a stage (Left Panel).
4. Choose Stages under the selected API and then choose a stage (Left Panel).
5. In the Stage Editor panel, select a certificate under the Client Certificate section.
6. Click Save Changes

# 6. Develop and maintain secure systems and applications

6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: - In accordance with PCI DSS (for example, secure authentication and logging) - Based on industry standards and/or best practices. - Incorporating information security throughout the software-development life cycle

## AWS EBS Snapshot with access for unmonitored cloud accounts

| | |
|---|---|
| Compliance Section: 6.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies EBS Snapshot with access for unmonitored cloud accounts.The EBS Snapshots which have either the read / write permission opened up for Cloud Accounts which are NOT part of Cloud Accounts monitored by Prisma Cloud. These accounts with read / write privileges should be reviewed and confirmed that these are valid accounts of your organisation (or authorised by your organisation) and are not active under Prisma Cloud monitoring.

### Recommendations:

1. Sign in to the AWS console.
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated.
3. Access the EC2 service, navigate to 'Snapshots' under 'Elastic Block Store' in left hand menu.
4. Select the identified 'EBS Snapshot' and select the tab 'Permissions'.
5. Review and delete the AWS Accounts which should not have read access.

# 6. Develop and maintain secure systems and applications

6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: - In accordance with PCI DSS (for example, secure authentication and logging) - Based on industry standards and/or best practices. - Incorporating information security throughout the software-development life cycle

## AWS Elasticsearch domain has Dedicated master set to disabled

| | |
|---|---|
| Compliance Section: 6.3 | First Seen: N/A |
| Resource(s) Failed: 1 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies Elasticsearch domains for which Dedicated master is disabled in your AWS account. If dedicated master nodes are provided those handle the management tasks and cluster nodes can easily manage index and search requests from different types of workload and make them more resilient in production. Dedicated master nodes improve environmental stability by freeing all the management tasks from the cluster data nodes.

### Resource(s) Failed:

mybookstore-domain

### Recommendations:

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to Elasticsearch Service Dashboard
4. Choose reported Elasticsearch domain
5. Click on 'Edit Domain'
6. On the 'Edit domain' page,
a. Check 'Enable dedicated master' checkbox to enable dedicated master nodes for the current cluster.
b. Select the 'Instance type' based on your ES cluster requirements from the dropdown list.
Note: As dedicated master nodes do not hold any data nor process any search and query requests, the instance node for this role typically does not require a large amount of CPU/RAM memory.
c. Select the 'Number of master nodes' from dropdown list to allocate dedicated master nodes.
7. Click on 'Submit'

# 6. Develop and maintain secure systems and applications

6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: - In accordance with PCI DSS (for example, secure authentication and logging) - Based on industry standards and/or best practices. - Incorporating information security throughout the software-development life cycle

## AWS RDS instance with copy tags to snapshots disabled

| | |
|---|---|
| Compliance Section: 6.3 | First Seen: N/A |
| Resource(s) Failed: 1 | Resource Type: Other |
| Resource(s) Passed: 1 | |

### Description:

This policy identifies RDS instances that have copy tags to snapshots disabled. Copy tags to snapshots copies all the user-defined tags from the DB instance to snapshots. Copying tags allow you to add metadata and apply access policies to your Amazon RDS resources. NOTE: Setting Copy tags to snapshots for an Aurora DB instance has no effect on the DB setting. So Aurora DB instances are excluded from policy check.

### Resource(s) Failed:

ad1r2yeh915nzgo

### Recommendations:

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to Amazon RDS console
4. Choose DB Instances, and then select the reported DB instance
5. Click on 'Modify'
6. In 'Additional Configuration' section, In 'Backup' sub-section select the 'Copy tags to snapshots'
7. Click on 'Continue'
8. On the 'Summary of Modifications' panel, review the configuration changes. From 'Scheduling of Modifications' section, select whether changes to 'Apply immediately' or 'Apply during the next scheduled maintenance window'.
9. On the confirmation page, Review the changes and Click on 'Modify DB Instance' to save your changes.

# 6. Develop and maintain secure systems and applications

6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: - In accordance with PCI DSS (for example, secure authentication and logging) - Based on industry standards and/or best practices. - Incorporating information security throughout the software-development life cycle

## AWS S3 bucket is not configured with MFA Delete

| | |
|---|---|
| Compliance Section: 6.3 | First Seen: N/A |
| Resource(s) Failed: 1 | Resource Type: Other |
| Resource(s) Passed: 11 | |

### Description:

This policy identifies the S3 buckets which do not have Multi-Factor Authentication(MFA) enabled to delete S3 object version. Enabling MFA Delete on a versioned bucket adds another layer of protection. In order to permanently delete an object version or suspend or reactivate versioning on the bucket valid code from the account's MFA device required. Note: MFA Delete only works for CLI or API interaction, not in the AWS Management Console. Also, you cannot make version DELETE actions with MFA using IAM user credentials. You must use your root AWS account.

### Resource(s) Failed:

s3-production-for-pp-ctf

### Recommendations:

Using console you can enable versioning on the bucket but you cannot enable MFA delete.
You can do it via only with the AWS CLI:
aws s3api put-bucket-versioning --bucket <BUCKET_NAME> --versioning-configuration Status=Enabled,MFADelete=Enabled --mfa " <MFA_SERIAL_NUMBER> <MFA_CODE>"
NOTE: The bucket owner, the AWS account that created the bucket (root account), and all authorized IAM users can enable versioning, but only the bucket owner (root account) can enable MFA Delete. Successful execution will enable the S3 bucket versioning and MFA delete on the bucket.

# 6. Develop and maintain secure systems and applications

6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: - In accordance with PCI DSS (for example, secure authentication and logging) - Based on industry standards and/or best practices. - Incorporating information security throughout the software-development life cycle

## AWS Lambda nearing availability code storage limit

| | |
|---|---|
| Compliance Section: 6.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 5 | |

### Description:

This policy identifies Lambda nearing availability code storage limit per region. AWS provides a reasonable starting amount of compute and storage resources that you can use to run and store functions. As a best practice, it is recommended to either remove the functions that you no longer in use or reduce the code size of the functions that you do not want to remove. It will also help you avoid unexpected charges on your bill. NOTE: As per https://docs.aws.amazon.com/lambda/latest/dg/limits.html. On the date, Lambda account limit per region is 75 GB. This policy will trigger an alert if Lambda account limit per region reached to 90% (i.e. 67500000 KB) of resource availability limit allocated. If you need more Lambda account code storage size per region, You can contact AWS for a service limit increase.

### Recommendations:

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to the AWS Lambda Dashboard
4. Click on 'Functions', choose each the lambda function
5. Either remove the function that you no longer use or deduce the code size of the function that if you do not want to remove.

# 6. Develop and maintain secure systems and applications

6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: - In accordance with PCI DSS (for example, secure authentication and logging) - Based on industry standards and/or best practices. - Incorporating information security throughout the software-development life cycle

## AWS RDS Snapshot with access for unmonitored cloud accounts

| | |
|---|---|
| Compliance Section: 6.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 5 | |

### Description:

This policy identifies RDS snapshots with access for unmonitored cloud accounts. The RDS Snapshot which have either the read / write permission opened up for Cloud Accounts which are NOT part of Cloud Accounts monitored by Prisma Cloud. These accounts with read / write privileges should be reviewed and confirmed that these are valid accounts of your organisation (or authorised by your organisation) and are not active under Prisma Cloud monitoring.

### Recommendations:

1. Sign into the AWS console.
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to the RDS service.
4. Select the identified 'RDS Snapshot' under the 'Snapshots' in the left hand menu.
5. Under the tab 'Snapshot Actions', selection the option 'Share Snapshot'.
6. Review and delete the AWS Accounts which should not have read access.

# 6. Develop and maintain secure systems and applications

6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: - In accordance with PCI DSS (for example, secure authentication and logging) - Based on industry standards and/or best practices. - Incorporating information security throughout the software-development life cycle

## AWS ACM Certificate with wildcard domain name

| | |
|---|---|
| Compliance Section: 6.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies ACM Certificates which are using wildcard certificates for wildcard domain name instead of single domain name certificates. ACM allows you to use an asterisk (*) in the domain name to create an ACM Certificate containing a wildcard name that can protect several sites in the same domain. For example, a wildcard certificate issued for *.prismacloud.io can match both www.prismacloud.io and images.prismacloud.io. When you use wildcard certificates, if the private key of a certificate is compromised, then all domain and subdomains that use the compromised certificate are potentially impacted. So it is recommended to use single domain name certificates instead of wildcard certificates to reduce the associated risks with a compromised domain or subdomain.

### Recommendations:

To resolve this alert, you have to replace the reported wildcard certificate with single domain name certificate for all the first-level subdomains resulted from the domain name of the website secured with the wildcard certificate and delete the reported wildcard domain certificate.
To create a new certificate with a single domain:
1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to Certificate Manager
4. In 'Request a certificate' page,
a. On Step 1: 'Add domain names' page, in the 'Domain name' box, type the fully qualified domain name. Click on 'Next'
b. On Step 2: 'Select validation method' page, Select the validation method. Click on 'Review'
c. On Step 3: 'Review' page, review the domain name and validation method details. click on 'Confirm'
d. On Step 4: 'Validation' page, validate the certificate request based on the validation method selected. then click on 'Continue'
The certificate status should change from 'Pending validation' to 'Issued'. Now access your application's web server configuration and replace the wildcard certificate with the newly issued single domain name certificate.
To delete wildcard certificate:
1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Go to Certificate Manager(ACM) service
4. Choose the reported certificate
5. Under 'Actions' drop-down click on 'Delete'
6. On 'Delete certificate' popup windows, Click on 'Delete' button

# 6. Develop and maintain secure systems and applications

6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: - In accordance with PCI DSS (for example, secure authentication and logging) - Based on industry standards and/or best practices. - Incorporating information security throughout the software-development life cycle

## AWS S3 Object Versioning is disabled

| | |
|---|---|
| Compliance Section: 6.3 | First Seen: N/A |
| Resource(s) Failed: 11 | Resource Type: Other |
| Resource(s) Passed: 1 | |

### Description:

This policy identifies the S3 buckets which have Object Versioning disabled. S3 Object Versioning is an important capability in protecting your data within a bucket. Once you enable Object Versioning, you cannot remove it; you can suspend Object Versioning at any time on a bucket if you do not wish for it to persist. It is recommended to enable Object Versioning on S3.

### Resource(s) Failed:

aws-cloudtrail-logs-795462528824-317b0c26, mygoalsapp-pipelineartifactsbucket-1es78l9rtorl1, prisma-guardduty-findings, photos.cats.ctf, mybookstore-assetsbucket-h49w4uta9ws4, cf-templates-cnh9x6netk1b-us-west-1, mygoalsapp-assetsbucket-1jvraqv1lbf1z, mybookstore-pipelineartifactsbucket-1ov8q9nvordkf, cf-templates-cnh9x6netk1b-us-east-1, agentbucket-795462528824 ...and 1 more

### Recommendations:

1. Log into your AWS Console and select the S3 service.
2. Choose the reported S3 bucket and click the Properties tab in the upper right frame.
3. Expand the Versioning option
4. Click Enable Versioning
5. Click Save

# 6. Develop and maintain secure systems and applications

6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: - In accordance with PCI DSS (for example, secure authentication and logging) - Based on industry standards and/or best practices. - Incorporating information security throughout the software-development life cycle

## AWS RDS instance with Multi-Availability Zone disabled

| | |
|---|---|
| Compliance Section: 6.3 | First Seen: N/A |
| Resource(s) Failed: 2 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies RDS instances which have Multi-Availability Zone(Multi-AZ) disabled. When RDS DB instance is enabled with Multi-AZ, RDS automatically creates a primary DB Instance and synchronously replicates the data to a standby instance in a different availability zone. These Multi-AZ deployments will improve primary node reachability by providing read replica in case of network connectivity loss or loss of availability in the primary’s availability zone for read/write operations, so by making them the best fit for production database workloads.

### Resource(s) Failed:

ad1r2yeh915nzgo, bookstoreneptunedb-bhpb9s1h0ck7

### Recommendations:

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to Amazon RDS console
4. Choose Instances, and then select the reported DB instance
5. Click on 'Modify'
6. In 'Availability & durability' section for the 'Multi-AZ Deployment', select 'Create a standby instance'
7. Click on 'Continue'
8. Under 'Scheduling of modifications' choose 'When to apply modifications'
9. On the confirmation page, Review the changes and Click on 'Modify DB Instance' to save your changes.

# 6. Develop and maintain secure systems and applications

6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: - In accordance with PCI DSS (for example, secure authentication and logging) - Based on industry standards and/or best practices. - Incorporating information security throughout the software-development life cycle

## AWS Elasticsearch domain has Zone Awareness set to disabled

| | |
|---|---|
| Compliance Section: 6.3 | First Seen: N/A |
| Resource(s) Failed: 1 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies Elasticsearch domains for which Zone Awareness is disabled in your AWS account. Enabling Zone Awareness (cross-zone replication) increases the availability by distributing your Elasticsearch data nodes across two availability zones available in the same AWS region. It also prevents data loss and minimizes downtime in the event of node or availability zone failure.

### Resource(s) Failed:

mybookstore-domain

### Recommendations:

To enable Zone Awareness feature on existing Elasticsearch, following CLI can be used:
aws es update-elasticsearch-domain-config --domain-name <DOMAINNAME> --region <REGION> --elasticsearch-cluster-config ZoneAwarenessEnabled=true, ZoneAwarenessConfig={AvailabilityZoneCount=<COUNT>}
For more refer:
https://docs.aws.amazon.com/elasticsearch-service/latest/developerguide/es-managedomains-multiaz.html

# 6. Develop and maintain secure systems and applications

6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: - In accordance with PCI DSS (for example, secure authentication and logging) - Based on industry standards and/or best practices. - Incorporating information security throughout the software-development life cycle

## AWS ElastiCache Redis cluster with Multi-AZ Automatic Failover feature set to disabled

| | |
|---|---|
| Compliance Section: 6.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies ElastiCache Redis clusters which have Multi-AZ Automatic Failover feature set to disabled. It is recommended to enable the Multi-AZ Automatic Failover feature for your Redis Cache cluster, which will improve primary node reachability by providing read replica in case of network connectivity loss or loss of availability in the primary's availability zone for read/write operations. Note: Redis cluster Multi-AZ with automatic failover does not support T1 and T2 cache node types and is only available if the cluster has at least one read replica.

### Recommendations:

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to ElastiCache Dashboard
4. Click on Redis
5. Select reported Redis cluster
6. Click on 'Modify' button
7. In the 'Modify Cluster' dialog box,

a. Set 'Multi-AZ' to 'Yes'

b. Select 'Apply Immediately' checkbox, to apply the configuration changes immediately. If Apply Immediately is not selected, the changes will be processed during the next maintenance window.

c. Click on 'Modify'

# 6. Develop and maintain secure systems and applications

6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: - In accordance with PCI DSS (for example, secure authentication and logging) - Based on industry standards and/or best practices. - Incorporating information security throughout the software-development life cycle

## AWS Certificate Manager (ACM) contains certificate pending validation

| | |
|---|---|
| Compliance Section: 6.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies invalid certificates which are in AWS Certificate Manager. When your Amazon ACM certificates are not validated within 72 hours after the request is made, those certificates become invalid and you will have to request new certificates, which could cause interruption to your applications or services. Though AWS Certificate Manager automatically renews certificates issued by the service that is used with other AWS resources. However, the ACM service does not automatically renew certificates that are not currently in use or not associated anymore with other AWS resources. So the renewal process including validation must be done manually before these certificates become invalid.

### Recommendations:

To validate Certificates:
1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Go to Certificate Manager(ACM) service
4. Choose the reported certificate
5. Validate your certificate for your domain using either Email or DNS validation, depending upon your certificate validation method.

OR

If the certificate is not required you can delete that certificate. To delete invalid Certificates:
1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Go to Certificate Manager(ACM) service
4. Choose the reported certificate
5. Under 'Actions' drop-down click on 'Delete'

Note: This alert will get auto-resolved, as the certificate becomes invalid in 72 hours. It is recommended to either delete or validate the certificate within the timeframe.

# 6. Develop and maintain secure systems and applications

6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: - In accordance with PCI DSS (for example, secure authentication and logging) - Based on industry standards and/or best practices. - Incorporating information security throughout the software-development life cycle

## AWS regions nearing VPC Private Gateway limit

| | |
|---|---|
| Compliance Section: 6.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies if your account is near the private gateway limitation per VPC per Region. AWS provides a reasonable starting limitation for the maximum number of Virtual private gateways you can assign in each VPC. If you approach the limit in a particular VPC, this alert indicates that you have nearly exhausted your allocation. NOTE: As per http://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html Virtual private gateway per region limit is 5. This policy will trigger an alert if Virtual private gateway per region reached 80% (i.e. 4) of resource availability limit allocated.

### Recommendations:

1. Sign in to the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to VPC Dashboard
4. Click on 'Virtual Private Gateways' (Left Panel)
5. Choose the Virtual Private Gateway you want to delete, which is not used or required
6. Click on 'Actions' dropdown
7. Click on 'Delete Virtual Private Gateway'NOTE: If Virtual Private Gateway is already in use it can not be deleted. Make sure gateways unassociated before going to deleting it.
8. On 'Delete Virtual Private Gateway' popup dialog, Click on 'Yes, Delete'NOTE: If existing Virtual Private Gateways are properly associated and exhausted your VPC Virtual Private Gateway limit allocation, you can contact AWS for a service limit increase.

# 6. Develop and maintain secure systems and applications

6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: - In accordance with PCI DSS (for example, secure authentication and logging) - Based on industry standards and/or best practices. - Incorporating information security throughout the software-development life cycle

## AWS EMR cluster is not configured with security configuration

| | |
|---|---|
| Compliance Section: 6.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies EMR clusters which are not configured with security configuration. With Amazon EMR release version 4.8.0 or later, you can use security configurations to configure data encryption, Kerberos authentication, and Amazon S3 authorization for EMRFS.

### Recommendations:

1. Log in to the AWS Console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated.
3. Navigate to 'EMR' dashboard from 'Services' dropdown
4. Go to 'Security configurations', click 'Create'
5. On the Create security configuration window,
6. In 'Name' box, provide a name for the new EMR security configuration
7. Follow below link to configure a security configuration
https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-create-security-configuration.html
8. Click on 'Create' button
9. On the left menu of EMR dashboard Click 'Clusters'
10. Select the EMR cluster for which the alert has been generated and click on the 'Clone' button from the top menu.
11. In the Cloning popup, choose 'Yes' and Click 'Clone'
12. On the Create Cluster page, in the Security Options section, click on 'security configuration'
13. From the 'Security configuration' drop down select the name of the security configuration created at step 4 to step 8, click 'Create Cluster'.
14. Once you the new cluster is set up verify its working and terminate the source cluster in order to stop incurring charges for it
15. On the left menu of EMR dashboard Click 'Clusters', from the list of clusters select the source cluster which is alerted
16. Click on the 'Terminate' button from the top menu
17. On the 'Terminate clusters' pop-up, click 'Terminate'

# 6. Develop and maintain secure systems and applications

6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: - In accordance with PCI DSS (for example, secure authentication and logging) - Based on industry standards and/or best practices. - Incorporating information security throughout the software-development life cycle

## AWS S3 bucket accessible to unmonitored cloud accounts

| | |
|---|---|
| Compliance Section: 6.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 12 | |

### Description:

This policy identifies those S3 buckets which have either the read/write permission opened up for Cloud Accounts which are NOT part of Cloud Accounts monitored by Prisma Cloud. These accounts with read/write privileges should be reviewed and confirmed that these are valid accounts of your organization (or authorised by your organization) and are not active under Prisma Cloud monitoring.

### Recommendations:

1. Log in to the AWS Console
2. Navigate to the 'S3' service
3. Click on the reported S3 bucket
4. Click on the 'Permissions' tab
5. Navigate to the 'Access control list (ACL)' section and Click on the 'Edit'
6. Under 'Access for other AWS accounts', Add the Cloud Accounts that are monitored by Prisma Cloud
7. Click on 'Save changes'

# 6. Develop and maintain secure systems and applications

6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: - In accordance with PCI DSS (for example, secure authentication and logging) - Based on industry standards and/or best practices. - Incorporating information security throughout the software-development life cycle

## S3 buckets with configurations set to host websites

| | |
|---|---|
| Compliance Section: 6.3 | First Seen: N/A |
| Resource(s) Failed: 2 | Resource Type: Other |
| Resource(s) Passed: 10 | |

### Description:

To host a website on AWS S3 you should configure a bucket as a website. This policy identifies all the S3 buckets that are configured to host websites. By frequently surveying these S3 buckets you can ensure that only authorized buckets are enabled to host websites. Make sure to disable static website hosting for unauthorized S3 buckets.

### Resource(s) Failed:

mybookstore-assetsbucket-h49w4uta9ws4, mygoalsapp-assetsbucket-1jvraqv1lbf1z

### Recommendations:

1. Login to AWS Console
2. Goto S3 under Services
3. Choose the reported bucket
4. Goto Properties tab
5. Click on Static website hosting
6. Click on Disable website hosting
7. Click on Save

# 6. Develop and maintain secure systems and applications

6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: - In accordance with PCI DSS (for example, secure authentication and logging) - Based on industry standards and/or best practices. - Incorporating information security throughout the software-development life cycle

## AWS Network Load Balancer (NLB) is not using the latest predefined security policy

| | |
|---|---|
| Compliance Section: 6.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies Network Load Balancers (NLBs) which are not using the latest predefined security policy. A security policy is a combination of protocols and ciphers. The protocol establishes a secure connection between a client and a server and ensures that all data passed between the client and your load balancer is private. A cipher is an encryption algorithm that uses encryption keys to create a coded message. So it is recommended to use the latest predefined security policy which uses only secured protocol and ciphers. For more details: https://docs.aws.amazon.com/elasticloadbalancing/latest/network/create-tls-listener.html#describe-ssl-policies

### Recommendations:

1. Log in to the AWS console
2. In the console, select the specific region from the region drop-down on the top right corner, for which the alert is generated
3. Go to the EC2 Dashboard, and select 'Load Balancers'
4. Click on the reported Load Balancer
5. On the 'Listeners' tab, Choose the 'TLS' rule
6. Click on 'Edit', Change 'Security policy' to 'ELBSecurityPolicy-TLS13-1-2-2021-06'
7. Click on 'Update' to save your changes

# 6. Develop and maintain secure systems and applications

6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: - In accordance with PCI DSS (for example, secure authentication and logging) - Based on industry standards and/or best practices. - Incorporating information security throughout the software-development life cycle

## AWS CloudFront web distribution with AWS Web Application Firewall (AWS WAF) service disabled

| | |
|---|---|
| Compliance Section: 6.3 | First Seen: N/A |
| Resource(s) Failed: 2 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies Amazon CloudFront web distributions which have the AWS Web Application Firewall (AWS WAF) service disabled. As a best practice, enable the AWS WAF service on CloudFront web distributions to protect against application layer attacks. To block malicious requests to your Cloudfront Content Delivery Network, define the block criteria in the WAF web access control list (web ACL).

### Resource(s) Failed:

d2rwvuyjsg9kf7.cloudfront.net, d2u45drmoykiua.cloudfront.net

### Recommendations:

1. Sign in to the AWS console
2. Go to the CloudFront Distributions Dashboard
3. Click on the reported web distribution
4. On 'General' tab, Click on 'Edit' button
5. On 'Edit Distribution' page, Choose a 'AWS WAF Web ACL' from dropdown.
6. Click on 'Yes, Edit'

# 6. Develop and maintain secure systems and applications

6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: - In accordance with PCI DSS (for example, secure authentication and logging) - Based on industry standards and/or best practices. - Incorporating information security throughout the software-development life cycle

## AWS CloudFront web distribution with geo restriction disabled

| | |
|---|---|
| Compliance Section: 6.3 | First Seen: N/A |
| Resource(s) Failed: 2 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies CloudFront web distributions which have geo restriction feature disabled. Geo Restriction has the ability to block IP addresses based on Geo IP by allowlist or denylist a country in order to allow or restrict users in specific locations from accessing web application content.

### Resource(s) Failed:

d2rwvuyjsg9kf7.cloudfront.net, d2u45drmoykiua.cloudfront.net

### Recommendations:

1. Sign in to the AWS console
2. Select the region, from the region drop-down, in which the alert is generated
3. Navigate to CloudFront Distributions Dashboard
4. Click on the reported distribution
5. On 'Restrictions' tab, Click on the 'Edit' button
6. On 'Edit Geo-Restrictions' page, Set 'Enable Geo-Restriction' to 'Yes' and allowlist/denylist countries as per your requirement.
7. Click on 'Yes, Edit'

# 6. Develop and maintain secure systems and applications

6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: - In accordance with PCI DSS (for example, secure authentication and logging) - Based on industry standards and/or best practices. - Incorporating information security throughout the software-development life cycle

## AWS regions nearing VPC Private Gateway IPSec Limit

| | |
|---|---|
| Compliance Section: 6.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies if your account is near the private gateway IPSec limitation per VPC per Region. AWS provides a reasonable starting limitation for the maximum number of VPC Private Gateway IPSec connections you can assign in each VPC. If you approach the limit in a particular VPC, this alert indicates that you have nearly exhausted your allocation.

### Recommendations:

1. Sign in to the AWS console.
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated.
3. Navigate to VPC Dashboard
4. Click on 'Site-to-Site VPN Connections' (Left Panel)
5. Choose the VPN connection you want to delete, which more used or required
6. Click on 'Actions' dropdown
7. Click on 'Delete'
8. On 'Delete' popup dialog, Click on 'Delete'

NOTE: If existing VPN Connection is properly associated and exhausted your VPC Site-to-Site VPN Connections limit allocation, you can contact AWS for a service limit increase.

# 6. Develop and maintain secure systems and applications

6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: - In accordance with PCI DSS (for example, secure authentication and logging) - Based on industry standards and/or best practices. - Incorporating information security throughout the software-development life cycle

## AWS Application Load Balancer (ALB) is not using the latest predefined security policy

| | |
|---|---|
| Compliance Section: 6.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies Application Load Balancers (ALBs) are not using the latest predefined security policy. A security policy is a combination of protocols and ciphers. The protocol establishes a secure connection between a client and a server and ensures that all data passed between the client and your load balancer is private. A cipher is an encryption algorithm that uses encryption keys to create a coded message. So it is recommended to use the latest predefined security policy which uses only secured protocol and ciphers. We recommend using ELBSecurityPolicy-FS-1-2-Res-2020-10 policy if you require Forward Secrecy (FS) and use ELBSecurityPolicy-TLS-1-2-Ext-2018-06 policy to meet compliance and security standards that require disabling certain TLS protocol versions or to support legacy clients that require deprecated ciphers. For more details: https://docs.aws.amazon.com/elasticloadbalancing/latest/application/create-https-listener.html#describe-ssl-policies

### Recommendations:

1. Log in to the AWS console
2. In the console, select the specific region from the region drop-down on the top right corner, for which the alert is generated
3. Go to the EC2 Dashboard, and select 'Load Balancers'
4. Click on the reported Load Balancer
5. On the 'Listeners' tab, Choose the 'HTTPS' or 'SSL' rule
6.Click on 'Edit', Change 'Security policy' to 'ELBSecurityPolicy-FS-1-2-Res-2020-10' policy if you require Forward Secrecy (FS) and use 'ELBSecurityPolicy-TLS-1-2-Ext-2018-06' policy to meet compliance and security standards that require disabling certain TLS protocol versions or to support legacy clients that require deprecated ciphers.
7. Click on 'Update' to save your changes

# 6. Develop and maintain secure systems and applications

6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: - In accordance with PCI DSS (for example, secure authentication and logging) - Based on industry standards and/or best practices. - Incorporating information security throughout the software-development life cycle

## AWS Cloudfront Distribution with S3 have Origin Access set to disabled

| | |
|---|---|
| Compliance Section: 6.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 2 | |

### Description:

This policy identifies the AWS CloudFront distributions which are utilizing S3 bucket and have Origin Access Disabled. The origin access identity feature should be enabled for all your AWS CloudFront CDN distributions in order to restrict any direct access to your objects through Amazon S3 URLs.

### Recommendations:

1. Sign in to the AWS Console
2. Go to CloudFront
3. Choose the reported Distribution
4. Click on Distribution Settings
5. Click on 'Origins and Origin Groups
6. Select the S3 bucket and click on Edit
7. On the 'Restrict Bucket Access', Select Yes
8. Click on 'Yes, Edit'

# 7. Restrict access to cardholder data by business need to know

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.

## AWS EBS snapshots are accessible to public

| | |
|---|---|
| Compliance Section: 7.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Snapshot Settings |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies EC2 EBS snapshots which are accessible to public. Amazon Elastic Block Store (Amazon EBS) provides persistent block storage volumes for use with Amazon EC2 instances in the AWS Cloud. If EBS snapshots are inadvertently shared to public, any unauthorized user with AWS console access can gain access to the snapshots and gain access to sensitive data.

### Recommendations:

1. Log in to the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to 'EC2' service.
4. Under the 'Elastic Block Storage', click on the 'Snapshots'.
5. For the specific Snapshots, change the value of field 'Property' to 'Private'.
6. Under the section 'Encryption Details', set the value of 'Encryption Enabled' to 'Yes'.

# 7. Restrict access to cardholder data by business need to know

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.

## AWS RDS snapshots are accessible to public

| | |
|---|---|
| Compliance Section: 7.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Managed Database Snapshot |
| Resource(s) Passed: 5 | |

### Description:

This policy identifies AWS RDS snapshots which are accessible to public. Amazon Relational Database Service (Amazon RDS) is a web service that makes it easier to setup and manage databases. If RDS snapshots are inadvertently shared to public, any unauthorized user with AWS console access can gain access to the snapshots and gain access to sensitive data.

### Recommendations:

1. Sign in to the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to the 'RDS' service.
4. For the RDS instance reported in the alert, change 'Publicly Accessible' setting to 'No'.

# 7. Restrict access to cardholder data by business need to know

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.

## AWS S3 buckets are accessible to public

| | |
|---|---|
| Compliance Section: 7.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 12 | |

### Description:

This policy identifies S3 buckets which are publicly accessible. Amazon S3 allows customers to store or retrieve any type of content from anywhere in the web. Often, customers have legitimate reasons to expose the S3 bucket to public, for example, to host website content. However, these buckets often contain highly sensitive enterprise data which if left open to public may result in sensitive data leaks.

### Recommendations:

1. Login to the AWS Console
2. Navigate to the 'S3' service
3. Click on the 'S3' resource reported in the alert
4. Click on the 'Permissions'
5. If Access Control List' is set to 'Public' follow below steps
a. Under 'Access Control List', Click on 'Everyone' and uncheck all items
b. Click on Save
6. If 'Bucket Policy' is set to public follow below steps
a. Under 'Bucket Policy', modify the policy to remove public access
b. Click on Save
c. If 'Bucket Policy' is not required delete the existing 'Bucket Policy'.
Note: Make sure updating 'Access Control List' or 'Bucket Policy' does not affect S3 bucket data access.

# 7. Restrict access to cardholder data by business need to know

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.

## AWS S3 bucket has global view ACL permissions enabled

| | |
|---|---|
| Compliance Section: 7.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 12 | |

### Description:

This policy determines if any S3 bucket(s) has Global View ACL permissions enabled for the All Users group. These permissions allow external resources to see the permission settings associated to the object.

### Recommendations:

1. Go to the AWS console S3 dashboard.
2. Select your bucket by clicking on the bucket name.
3. Select the Permissions tab and 'Access Control List.'
4. Under Public Access, select Everyone.
5. In the popup window, under Access to this bucket's ACL, uncheck 'Read bucket permissions' and Save.

# 7. Restrict access to cardholder data by business need to know

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.

## AWS VPC subnets should not allow automatic public IP assignment

| | |
|---|---|
| Compliance Section: 7.1 | First Seen: N/A |
| Resource(s) Failed: 57 | Resource Type: Subnet |
| Resource(s) Passed: 7 | |

### Description:

This policy identifies VPC subnets which allow automatic public IP assignment. VPC subnet is a part of the VPC having its own rules for traffic. Assigning the Public IP to the subnet automatically (on launch) can accidentally expose the instances within this subnet to internet and should be edited to 'No' post creation of the Subnet.

### Resource(s) Failed:

subnet-14ad5472, subnet-4e4e6b12, subnet-81fc4ce7, subnet-e219f2ae, subnet-765a6d1f, subnet-bab57e91, subnet-aacee2e2, subnet-66f6e848, subnet-a1410fda, subnet-415f4208 ...and 47 more

### Recommendations:

1. Sign into the AWS console.
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated.
3. Navigate to the 'VPC' service.
4. In the navigation pane, click on 'Subnets'.
5. Select the identified Subnet and choose the option 'Modify auto-assign IP settings' under the Subnet Actions.
6. Disable the 'Auto-Assign IP' option and save it.

# 7. Restrict access to cardholder data by business need to know

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.

## AWS CloudTrail bucket is publicly accessible

| | |
|---|---|
| Compliance Section: 7.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 13 | |

### Description:

This policy identifies publicly accessible S3 buckets that store CloudTrail data. These buckets contains sensitive audit data and only authorized users and applications should have access.

### Recommendations:

1. Login to the AWS Console
2. Navigate to the 'S3' service
3. Click on the 'S3' resource reported in the alert
4. Click on the 'Permissions'
5. If Access Control List' is set to 'Public' follow below steps
a. Under 'Access Control List', Click on 'Everyone' and uncheck all items
b. Click on Save
6. If 'Bucket Policy' is set to public follow below steps
a. Under 'Bucket Policy', modify the policy to remove public access
b. Click on Save
c. If 'Bucket Policy' is not required delete the existing 'Bucket Policy'.
Note: Make sure updating 'Access Control List' or 'Bucket Policy' does not affect S3 bucket data access.

# 7. Restrict access to cardholder data by business need to know

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.

## AWS S3 Bucket Policy allows public access to CloudTrail logs

| | |
|---|---|
| Compliance Section: 7.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 13 | |

### Description:

This policy scans your bucket policy that is applied to the S3 bucket to prevent public access to the CloudTrail logs. CloudTrail logs a record of every API call made in your AWS account. These logs file are stored in an S3 bucket. Bucket policy or the access control list (ACL) applied to the S3 bucket does not prevent public access to the CloudTrail logs. It is recommended that the bucket policy or access control list (ACL) applied to the S3 bucket that stores CloudTrail logs prevents public access. Allowing public access to CloudTrail log content may aid an adversary in identifying weaknesses in the affected account's use or configuration.

### Recommendations:

1. Sign in to the AWS Console
2. Goto S3
3. Choose the reported S3 bucket and click Properties
4. In the Properties pane, click the Permissions tab.
5. If the Edit bucket policy button is present, select it.
6. Remove any statement having an effect Set to 'Allow' and a principal set to '*'.

Note: We recommend that you do not configure CloudTrail to write into an S3 bucket that resides in a different AWS account.

# 7. Restrict access to cardholder data by business need to know

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.

## AWS Route53 Public Zone with Private Records

| | |
|---|---|
| Compliance Section: 7.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

A hosted zone is a container for records (An object in a hosted zone that you use to define how you want to route traffic for the domain or a subdomain), which include information about how you want to route traffic for a domain (such as example.com) and all of its subdomains (such as www.example.com, retail.example.com, and seattle.accounting.example.com). A hosted zone has the same name as the corresponding domain. A public hosted zone is a container that holds information about how you want to route traffic on the internet for a specific domain.It is best practice to avoid AWS Route 53 Public Hosted Zones containing DNS records for private IPs or resources within your AWS account to overcome information leakage of your internal network and resources.

### Recommendations:

You can not convert a public hosted zone into a private hosted zone. So, it is recommended to create and configure a Private Hosted Zone to manage private IPs within your Virtual Private Cloud (VPC) as Amazon Route 53 service will only return your private DNS records when queried from within the associated VPC, and delete the associated public hosted zone once the Private hosted zone is configured with all the records.
To create a private hosted zone using the Route 53 console:
1.For each VPC that you want to associate with the Route 53 hosted zone, change the following VPC settings to true:
'enableDnsHostnames'
'enableDnsSupport'
For more information, see Updating DNS Support (http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-dns.html#vpc-dns-updating) for Your VPC in the Amazon VPC User Guide.
2. Sign in to the AWS console
3. Go to Route 53 console
4. If you are new to Route 53, choose Get Started Now under DNS Management. If you are already using Route 53, choose Hosted Zones in the navigation pane.
5. Choose 'Create Hosted Zone'
6. In the Create Private Hosted Zone pane, enter a domain name and, optionally, a comment.
For information about how to specify characters other than a-z, 0-9, and - (hyphen) and how to specify internationalized domain names, see DNS Domain Name Format (https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/DomainNameFormat.html).
7. In the Type list, choose Private Hosted Zone for Amazon VPC
8. In the VPC ID list, choose the VPC that you want to associate with the hosted zone. If you want to associate more than one VPC with the hosted zone, you can add VPCs after you create the hosted zone.
Note: If the console displays the following message, you are trying to associate a VPC with this hosted zone that has already been associated with another hosted zone that has an overlapping namespace, such as example.com and retail.example.com:
'A conflicting domain is already associated with the given VPC or Delegation Set.'
9. Choose Create
10. To associate more VPCs with the new hosted zone, perform the following steps:
a. Choose Back to Hosted Zones.
b. Choose the radio button for the hosted zone.
c. In the right pane, in VPC ID, choose another VPC that you want to associate with the hosted zone.
d. Choose Associate New VPC.
e. Repeat steps c and d until you have associated all of the VPCs that you want to with the hosted zone.
For More Information : https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/hosted-zone-private-creating.html
To delete a public hosted zone using the Route 53 console:
1. Sign into the AWS console

2. Go Route53 console
3. Confirm that the hosted zone that you want to delete contains only an NS and an SOA record. If it contains additional records, delete them:
a. Choose the name of the hosted zone that you want to delete.
b. On the Record Sets page, if the list of records includes any records for which the value of the Type column is something other than NS or SOA, choose the row, and choose Delete Record Set. To select multiple, consecutive records, choose the first row, press and hold the Shift key, and choose the last row. To select multiple, non-consecutive records, choose the first row, press and hold the Ctrl key, and choose the remaining rows.
Note: If you created any NS records for subdomains in the hosted zone, delete those records, too.
c. Choose Back to Hosted Zones
4. On the Hosted Zones page, choose the row for the hosted zone that you want to delete.
5. Choose Delete Hosted Zone.
6. Choose OK to confirm.
7. If you want to make the domain unavailable on the internet, we recommend that you transfer DNS service to a free DNS service and then delete the Route 53 hosted zone. This prevents future DNS queries from possibly being misrouted. If the domain is registered with Route 53, see Adding or Changing Name Servers and Glue Records for a Domain (https://docs.aws.amazon.com/Route53/latest DeveloperGuide/domain-name-servers-glue-records.html) for information about how to replace Route 53 nameservers with name servers for the new DNS service. If the domain is registered with another registrar, use the method provided by the registrar to change name servers for the domain.
For More Information : https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/DeleteHostedZone.html

# 7. Restrict access to cardholder data by business need to know

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.

## AWS IAM user has two active Access Keys

| | |
|---|---|
| Compliance Section: 7.1 | First Seen: N/A |
| Resource(s) Failed: 1 | Resource Type: IAM Credentials Report |
| Resource(s) Passed: 14 | |

### Description:

This policy identifies IAM users who have two active Access Keys. Each IAM user can have up to two Access Keys, having two Keys instead of one can lead to increased chances of accidental exposure. So it needs to be ensured that unused Access Keys are deleted.

### Resource(s) Failed:

PrismaCloudCompute

### Recommendations:

1. Sign in to the AWS Console and navigate to the 'IAM' service.
2. Click on Users in the navigation pane.
3. For the identified IAM user which has two active Access Keys, based on policies of your company, take appropriate action.
4. Create another IAM user with the specific objective performed by the 2nd Access Key.
5. Delete one of the unused Access Keys.

# 7. Restrict access to cardholder data by business need to know

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.

## AWS IAM user has both Console access and Access Keys

| | |
|---|---|
| Compliance Section: 7.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: IAM Credentials Report |
| Resource(s) Passed: 15 | |

### Description:

This policy identifies IAM users who have both Console access and Access Keys. When an IAM user is created, the Administrator can assign either Console access or Access Keys or both. Ideally the Console access should be assigned to Users and Access Keys for system / API applications, but not both to the same IAM user.

### Recommendations:

1. Sign in to the AWS console and navigate to the 'IAM' service.
2. Identify the reported IAM user.
3. In 'Security credentials' tab check for presence of Access Keys.
4. Based on the requirement and company policy, either delete the Access Keys or remove the Console access for this IAM user.

# 7. Restrict access to cardholder data by business need to know

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.

## AWS EC2 Instance IAM Role not enabled

| | |
|---|---|
| Compliance Section: 7.1 | First Seen: N/A |
| Resource(s) Failed: 7 | Resource Type: Other |
| Resource(s) Passed: 5 | |

### Description:

AWS provides Identity Access Management (IAM) roles to securely access AWS services and resources. The role is an identity with permission policies that define what the identity can and cannot do in AWS. As a best practice, create IAM roles and attach the role to manage EC2 instance permissions securely instead of distributing or sharing keys or passwords.

### Resource(s) Failed:

Jenkins, BasicWindowsTarget, CTF_ADMIN_VM, i-0e5bac92212240efd, i-0fa5de28b835f969b, i-0698bcb22d1feb644, i-0112554313a2717e2

### Recommendations:

The most common setup is the AWS default that allows for EC2 access to AWS Services. For most, this is a great way to realize flexible, yet secure, EC2 access enabled for your instances. Select this when you launch EC2 instances to automatically inherit these permissions.

IAM

1. Go to the AWS console IAM dashboard.
2. In the navigation pane, choose Roles, Create new role.
3. Under 'Choose the service that will use this role' select EC2, then 'Next:Permissions.'
4. On the Attach permissions policies page, select an AWS managed policy that grants your instance access to the resources that they need, then 'Next:Tags.'
5. Add tags (optional), the select 'Next:Review.'
6. On the Create role and Review page, type a name for the role and choose Create role.

EC2

1. Go to the AWS console EC2 dashboard.
2. Select Running Instances.
3. Check the instance you want to modify.
4. From the Actions pull down menu, select Instance Settings and Attach/Replace IAM Role.
5. On the Attach/Replace IAM Role page, under the IAM role pull down menu, choose the role created in the IAM steps above.

# 7. Restrict access to cardholder data by business need to know

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.

## AWS Private ECR repository policy is overly permissive

| | |
|---|---|
| Compliance Section: 7.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 2 | |

### Description:

This policy identifies AWS Private ECR repositories that have overly permissive registry policies. An ECR(Elastic Container Registry) repository is a collection of Docker images available on the AWS cloud. These images might contain sensitive information which should be restricted to unauthorized users.

### Recommendations:

1. Log in to the AWS Console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated.
3. Navigate to 'ECR' dashboard from 'Services' dropdown
4. Go to 'Repository', from the left panel
5. Select the repository for which alert is being generated
6. Select the 'Permissions' option from left menu below 'repositores'
7. Click on 'Edit policy JSON' to modify the JSON so that Principal is restrictive
8. After modifications, click on 'Save'.

# 7. Restrict access to cardholder data by business need to know

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.

## AWS RDS database instance is publicly accessible

| | |
|---|---|
| Compliance Section: 7.1 | First Seen: N/A |
| Resource(s) Failed: 1 | Resource Type: Other |
| Resource(s) Passed: 1 | |

### Description:

This policy identifies RDS database instances which are publicly accessible. DB instances should not be publicly accessible to protect the integrity of data. Public accessibility of DB instances can be modified by turning on or off the Public accessibility parameter.

### Resource(s) Failed:

ad1r2yeh915nzgo

### Recommendations:

1. Sign into the AWS console.
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to the 'RDS' service.
4. Select the RDS instance reported in the alert, Click on 'Modify'
5. Under 'Network and Security', update the value of 'public accessibility' to 'No' and Click on 'Continue'
6. Select required 'Scheduling of modifications' option and click on 'Modify DB Instance'

# 7. Restrict access to cardholder data by business need to know

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.

## AWS IAM policy attached to users

| | |
|---|---|
| Compliance Section: 7.1 | First Seen: N/A |
| Resource(s) Failed: 11 | Resource Type: IAM User Managed Policies |
| Resource(s) Passed: 3 | |

### Description:

This policy identifies IAM policies attached to user. By default, IAM users, groups, and roles have no access to AWS resources. IAM policies are the means by which privileges are granted to users, groups, or roles. It is recommended that IAM policies be applied directly to groups but not users.

### Resource(s) Failed:

Adam, PrismaCloudCompute, Michaele, suhas, CTF_ADMIN_VM, CTF_ADMIN, flau, Randy, Cindy, Jim ...and 1 more

### Recommendations:

1. Sign in to the AWS Console
2. Navigate to the 'IAM' service.
3. Identify the users that were specifically assigned to the reported IAM policy.
4. If a group with a similar policy already exists, put the user into that group. If such a group does not exist, create a new group with relevant policy and assign the user to the group.

# 7. Restrict access to cardholder data by business need to know

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.

## AWS Classic Load Balancer is in use for internet-facing applications

| | |
|---|---|
| Compliance Section: 7.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies Classic Load Balancers that are being used for internet-facing HTTP/HTTPS applications. Classic Load Balancer should be used when you have an existing application running in the EC2-Classic network. Application Load Balancers (ALB) is recommended for internet-facing HTTP/HTTPS web applications. For more details: https://docs.aws.amazon.com/elasticloadbalancing/latest/application/create-application-load-balancer.html

### Recommendations:

To create Application Load Balancer (ALB) refer,
https://docs.aws.amazon.com/elasticloadbalancing/latest/application/create-application-load-balancer.html
Once Application Load Balancer created, you can delete the reported Classic Load Balancer by,

1. Log in to the AWS console
2. In the console, select the specific region from the region drop-down on the top right corner, for which the alert is generated
3. Navigate to EC2 Dashboard
4. Click on 'Load Balancers', choose the reported load balancer
5. Click on the 'Actions' and from the drop-down click on 'Delete'
6. Click on the 'Yes, Delete'

# 7. Restrict access to cardholder data by business need to know

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.

## AWS SageMaker notebook instance configured with direct internet access feature

| | |
|---|---|
| Compliance Section: 7.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies SageMaker notebook instances that are configured with direct internet access feature. If AWS SageMaker notebook instances are configured with direct internet access feature, any machine outside the VPC can establish a connection to these instances, which provides an additional avenue for unauthorized access to data and the opportunity for malicious activity. For more details: https://docs.aws.amazon.com/sagemaker/latest/dg/appendix-notebook-and-internet-access.html

### Recommendations:

AWS SageMaker notebook instance direct internet access feature can not be disabled; once it is created. You need to create a new notebook instance with disabled direct internet access feature; and migrate all required data from the reported notebook instance to the newly created notebook instance before you delete the reported notebook instance.
To create a New AWS SageMaker notebook instance,
1. Log in to AWS console
2. Navigate to the AWS SageMaker dashboard
3. Choose Notebook instances and then choose 'Create notebook instance'
4. On the Create notebook instance page, within the 'Network' section,
From 'VPC – optional' dropdown list, select the VPC where you want to deploy a new SageMaker notebook instance.
5. Select the 'Disable - Access the internet through a VPC' button under the 'Direct internet access' to disable direct internet access for the new notebook instance.
6. Choose other parameters as per your requirement and Click on the 'Create notebook instance' button
To delete reported notebook instance,
1. Log in to AWS console
2. Navigate to the AWS SageMaker dashboard
3. Choose Notebook instances and Choose the reported notebook instance
4. Click on the 'Actions' dropdown menu, select the 'Stop' option, and when instance stops, select the 'Delete' option.
5. Within Delete <notebook-instance-name> dialog box, click the Delete button to confirm the action.

# 7. Restrict access to cardholder data by business need to know

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.

## AWS SageMaker notebook instance with root access enabled

| | |
|---|---|
| Compliance Section: 7.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies the SageMaker notebook instances which are enabled with root access. Root access means having administrator privileges, users with root access can access and edit all files on the compute instance, including system-critical files. Removing root access prevents notebook users from deleting system-level software, installing new software, and modifying essential environment components. NOTE: Lifecycle configurations need root access to be able to set up a notebook instance. Because of this, lifecycle configurations associated with a notebook instance always run with root access even if you disable root access for users. For more details: https://docs.aws.amazon.com/sagemaker/latest/dg/nbi-root-access.html

### Recommendations:

1. Log in to AWS console
2. Navigate to the AWS SageMaker dashboard
3. Choose Notebook instances (Left panel)
4. Click on the reported SageMaker notebook instance

Note: To update root access for SageMaker notebook instances; Instances need to be stopped. So stop running instance before editing.

5. In the 'Notebook instance settings' section, click on 'Edit'
6. On the Edit notebook instance page, within the 'Permissions and encryption' section,

From the 'Root access - optional' options, select 'Disable - Don't give users root access to the notebook'

7. Click on the 'Update notebook instance'

# 7. Restrict access to cardholder data by business need to know

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.

## AWS S3 bucket publicly writable

| | |
|---|---|
| Compliance Section: 7.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 12 | |

### Description:

This policy identifies the S3 buckets that are publicly writable by Put/Create/Update/Replicate/Write/Delete bucket operations. These permissions permit anyone, malicious or not, to Put/Create/Update/Replicate/Write/Delete bucket operations on your S3 bucket if they can guess the namespace. S3 service does not protect the namespace if ACLs and Bucket policy is not handled properly, with this configuration you may be at risk of compromise of critical data by leaving S3 public. For more details: https://docs.aws.amazon.com/AmazonS3/latest/user-guide/set-permissions.html https://docs.aws.amazon.com/AmazonS3/latest/dev/about-object-ownership.html#ensure-object-ownership

### Recommendations:

1. Log in to the AWS Console
2. Navigate to the 'S3' service
3. Click on the S3 resource reported in the alert
4. Click on the 'Permissions' tab
5. If Access Control List is set to 'Public' follow the below steps
a. Under 'Access Control List', Click on 'Everyone' and uncheck all items
b. Click on Save changes
6. If 'Bucket Policy' is set to public follow the below steps
a. Under 'Bucket Policy', Select 'Edit Bucket Policy' and consider defining what explicit 'Principal' should have the ability to PUT/CREATE/REPLICATE/DELETE objects in your S3 bucket. You may also want to specifically limit the 'Principal' ability to perform specific PUT/CREATE/REPLICATE/DELETE functions, without the wild card.
If 'Bucket Policy' is not required delete the existing 'Bucket Policy'.
b. Click on Save changes
Note: Make sure updating 'Access Control List' or 'Bucket Policy' does not affect S3 bucket data access.

# 7. Restrict access to cardholder data by business need to know

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.

## AWS S3 bucket having policy overly permissive to VPC endpoints

| | |
|---|---|
| Compliance Section: 7.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 12 | |

### Description:

This policy identifies S3 buckets that have the bucket policy overly permissive to VPC endpoints. It is recommended to follow the principle of least privileges ensuring that the VPC endpoints have only necessary permissions instead of full permission on S3 operations. NOTE: When applying the Amazon S3 bucket policies for VPC endpoints described in this section, you might block your access to the bucket without intending to do so. Bucket permissions that are intended to specifically limit bucket access to connections originating from your VPC endpoint can block all connections to the bucket. The policy might disable console access to the specified bucket because console requests don't originate from the specified VPC endpoint. So remediation should be done very carefully. For details refer https://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies-vpc-endpoint.html

### Recommendations:

1. Log in to the AWS console
2. Navigate to the S3 dashboard
3. Choose the reported S3 bucket
4. In the 'Permissions' tab, click on the 'Bucket Policy'
5. Update the S3 bucket policy for the VPC endpoint so that it has only required permissions instead of full S3 permission.

Refer for example: https://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies-vpc-endpoint.html

# 7. Restrict access to cardholder data by business need to know

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.

## AWS IAM policy allows assume role permission across all services

| | |
|---|---|
| Compliance Section: 7.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: IAM Policy |
| Resource(s) Passed: 31 | |

### Description:

This policy identifies AWS IAM policy which allows assume role permission across all services. Typically, AssumeRole is used if you have multiple accounts and need to access resources from each account then you can create long term credentials in one account and then use temporary security credentials to access all the other accounts by assuming roles in those accounts.

### Recommendations:

1. Log in to the AWS Console
2. Navigate to the 'IAM' service.
3. Identify the reported policy
4. Change the Service element of the policy document to be more restrictive so that it only allows AssumeRole permission on select services.

# 7. Restrict access to cardholder data by business need to know

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.

## AWS IAM deprecated managed policies in use by User

| | |
|---|---|
| Compliance Section: 7.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 14 | |

### Description:

This policy checks for any usage of deprecated AWS IAM managed policies and returns an alert if it finds one in your cloud resources. When AWS deprecate an IAM managed policy, a new alternative is released with improved access restrictions. Existing IAM users and roles can continue to use the previous policy without interruption, however new IAM users and roles will use the new replacement policy. Before you migrate any user or role to the new replacement policy, we recommend you review their differences in the Policy section of AWS IAM console. If you require one or more of the removed permissions, please add them separately to any user or role. List of deprecated AWS IAM managed policies: AmazonElasticTranscoderFullAccess (replaced by AmazonElasticTranscoder_FullAccess)

### Recommendations:

1. Go to the AWS console IAM dashboard.
2. Click Policies on the left navigation menu.
3. Enter the deprecated IAM policy name into the filter.
4. Click on the policy name.
5. Select the Policy usage tab.
6. Check all attached users, make note of them, then select Detach.
7. Click Policies on the left navigation menu.
8. Enter the new IAM policy name into the filter.
9. Click on the policy name.
10. Select the Policy usage tab.
11. Select Attach and check all the users you made a note of.
12. Click Attach policy.

# 7. Restrict access to cardholder data by business need to know

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.

## AWS IAM support access policy is not associated to any role

| | |
|---|---|
| Compliance Section: 7.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 31 | |

### Description:

This policy identifies IAM policies with support role access which are not attached to any role for an account. AWS provides a support centre that can be used for incident notification and response, as well as technical support and customer services.

### Recommendations:

1. Log in to AWS console
2.Go to service IAM under Services panel.
3.From left panel click on 'Policies'
4.Search for the existence of a support policy 'AWSSupportAccess'
5.Create a IAM role
6.Attach 'AWSSupportAccess' managed policy to the created IAM role

# 7. Restrict access to cardholder data by business need to know

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.

## AWS EKS cluster endpoint access publicly enabled

| | |
|---|---|
| Compliance Section: 7.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

When you create a new cluster, Amazon EKS creates an endpoint for the managed Kubernetes API server that you use to communicate with your cluster (using Kubernetes management tools such as kubectl). By default, this API server endpoint is public to the internet, and access to the API server is secured using a combination of AWS Identity and Access Management (IAM) and native Kubernetes Role Based Access Control (RBAC). This policy checks your Kubernetes cluster endpoint access and triggers an alert if publicly enabled.

### Recommendations:

Enable private access to the Kubernetes API server so that all communication between your worker nodes and the API server stays within your VPC. Disable public access to your API server so that it's not accessible from the internet.

1. Login to AWS Console
2. Navigate to the Amazon EKS dashboard
3. Choose the name of the cluster to display your cluster information
4. Under Networking, choose 'Manage networking'
5. Select 'Private' radio button
6. Click on 'Save changes'

# 7. Restrict access to cardholder data by business need to know

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.

## AWS MQ is publicly accessible

| | |
|---|---|
| Compliance Section: 7.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies the AWS MQ brokers which are publicly accessible. It is advisable to use MQ brokers privately only from within your AWS Virtual Private Cloud (VPC). Ensure that the AWS MQ brokers provisioned in your AWS account are not publicly accessible from the Internet to avoid sensitive data exposure and minimize security risks.

### Recommendations:

Note: MQ broker configuration for public access cannot be modified. In case we need to update the MQ not to be public we need to recreate it.
1. Go to AWS console
2. Navigate to service 'Amazon MQ' from the 'Services' Menu
3. From the list of 'Brokers' select the reported MQ broker
4. From 'Details' section, copy all the configuration information.
5. Within 'Users' section, locate and copy the ActiveMQ Web Console access credentials.
6. Click on 'Brokers' from left panel, click on 'Create broker'
7. Provide an unique name in field 'Broker name'
8. In 'Advanced settings' section, select 'No' for 'Public accessibility'
9. Set the new broker configuration parameters using the information copied at step no. 4
10. Set the existing ActiveMQ Web Console access credentials copied at step no. 5
11. Click on 'Create broker'
12. Once the new broker is created, you can replace the broker endpoints within your applications

To delete the publicly accessible broker,
1. select the alerted from the list of 'Brokers'
2. Click on 'Delete' button
3. When a dialog box pops up, enter the broker name to confirm and click on 'delete' button

# 7. Restrict access to cardholder data by business need to know

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.

## AWS Amazon Machine Image (AMI) is publicly accessible

| | |
|---|---|
| Compliance Section: 7.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: VM Image |
| Resource(s) Passed: 8 | |

### Description:

This policy identifies AWS AMIs which are owned by the AWS account and are accessible to the public. Amazon Machine Image (AMI) provides information to launch an instance in the cloud. The AMIs may contain proprietary customer information and should be accessible only to authorized internal users.

### Recommendations:

1. Login to the AWS Console and navigate to 'EC2' service.
2. In the navigation pane, choose AMIs.
3. Select your AMI from the list, and then choose Actions, Modify Image Permissions.
4. Choose Private and choose Save.

# 7. Restrict access to cardholder data by business need to know

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.

## AWS SQS queue access policy is overly permissive

| | |
|---|---|
| Compliance Section: 7.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies Simple Queue Service (SQS) queues that have an overly permissive access policy. It is highly recommended to have the least privileged access policy to protect the SQS queue from data leakage and unauthorized access. For more details: https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-basic-examples-of-sqs-policies.html

### Recommendations:

1. Log in to the AWS console
2. Select the region, from the region drop-down, in which the alert is generated
3. Navigate to Simple Queue Service (SQS) dashboard
4. Choose the reported Simple Queue Service (SQS) and choose 'Edit'
5. Scroll to the 'Access policy' section
6. Edit the access policy statements in the input box, Make sure the 'Principal' is not set to '*', which makes your SQS queues accessible to any anonymous users.
7. When you finish configuring the access policy, choose 'Save'.

# 7. Restrict access to cardholder data by business need to know

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.

## AWS CloudFormation template contains globally open resources

| | |
|---|---|
| Compliance Section: 7.1 | First Seen: N/A |
| Resource(s) Failed: 1 | Resource Type: Other |
| Resource(s) Passed: 27 | |

### Description:

This alert triggers if a CloudFormation template that when launched will result in resources allowing global network access. Below are three common causes: - Security Group with a {0.0.0.0/0, ::/0} rule - Network Access Control List with a {0.0.0.0/0, ::/0} rule - Network Access Control List with -1 IpProtocol

### Resource(s) Failed:

awsjamconfig

### Recommendations:

Prisma Cloud encourages you to review the template and ensure this is the intended behavior.

1. Goto the AWS CloudFormation dashboard.
2. Click on the Stack you want to modify.
3. Select the Template tab and then View in Designer.
4. Make your template modifications.
5. Check for syntax errors in your template by choosing Validate template near the top of the page.
6. Select Save from the file (icon) menu.
7. Choose Amazon S3 bucket, name your template and Save.
8. Copy the bucket URL and click OK.
9. Select Close to close Designer.
10. Click on the Stack you want to modify.
11. From the Actions pull down menu, select Update stack
12. Choose Replace current template and paste the URL from Designer into the Amazon S3 URL field. Then click on Next.
13. Specify stack details, then click on Next.
14. Configure stack options, then click on Next.
15. Review, then select Update stack near the bottom of the page.

# 7. Restrict access to cardholder data by business need to know

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.

## AWS IAM Roles with Administrator Access Permissions

| | |
|---|---|
| Compliance Section: 7.1 | First Seen: N/A |
| Resource(s) Failed: 5 | Resource Type: Other |
| Resource(s) Passed: 88 | |

### Description:

This policy identifies AWS IAM roles which has administrator access permission set. This would allow all users who assume this role to have administrative privileges. As a security best practice, it is recommended to grant least privilege access like granting only the permissions required to perform a task, instead of providing excessive permissions.

### Resource(s) Failed:

AWSControlTowerExecution, AWSReservedSSO_AWSAdministratorAccess_fb576f420364742d, OrganizationAccountAccessRole, aws-controltower-AdministratorExecutionRole, stacksets-exec-86bfe566cedf709ff3051abaab72473e

### Recommendations:

1. Log in to AWS console
2. Navigate to IAM service
3. Click on Roles
4. Click on reported IAM role
5. Under 'Permissions policies' click on 'X' to detach or remove the policy having excessive permissions and assign a limited permission policy as required for a particular role.

# 7. Restrict access to cardholder data by business need to know

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.

## AWS Elasticsearch domain publicly accessible

| | |
|---|---|
| Compliance Section: 7.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 1 | |

### Description:

This policy identifies Elasticsearch domains which are publicly accessible. Enabling VPCs for Elasticsearch domains provides flexibility and control over the clusters access with an extra layer of security than Elasticsearch domains that use public endpoints. It also keeps all traffic between your VPC and Elasticsearch domains within the AWS network instead of going over the public Internet.

### Recommendations:

VPC for AWS Elasticsearch domain can be set only at the time of the creation of domain. So to resolve this alert, create a new domain with VPC, then migrate all required Elasticsearch domain data from the reported Elasticsearch domain to this newly created domain and delete reported Elasticsearch domain.
To set up the new ES domain with VPC, refer the following URL:
https://docs.aws.amazon.com/elasticsearch-service/latest/developerguide/es-createupdatedomains.html
To create Elasticsearch domain within VPC, In Network configuration choose VPC access instead of Public access.
To delete reported ES domain, refer the following URL:
https://docs.aws.amazon.com/elasticsearch-service/latest/developerguide/es-gsg-deleting.html

# 7. Restrict access to cardholder data by business need to know

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.

## AWS S3 bucket publicly readable

| | |
|---|---|
| Compliance Section: 7.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 12 | |

### Description:

This policy identifies the S3 buckets that are publicly readable by Get/Read/List bucket operations. These permissions permit anyone, malicious or not, to Get/Read/List bucket operations on your S3 bucket if they can guess the namespace. S3 service does not protect the namespace if ACLs and Bucket policy is not handled properly, with this configuration you may be at risk of compromise of critical data by leaving S3 public. For more details: https://docs.aws.amazon.com/AmazonS3/latest/user-guide/set-permissions.html https://docs.aws.amazon.com/AmazonS3/latest/dev/about-object-ownership.html#ensure-object-ownership

### Recommendations:

1. Log in to the AWS Console
2. Navigate to the 'S3' service
3. Click on the S3 resource reported in the alert
4. Click on the 'Permissions' tab
5. If Access Control List is set to 'Public' follow the below steps
a. Under 'Access Control List', Click on 'Everyone' and uncheck all items
b. Click on Save changes
6. If 'Bucket Policy' is set to public follow the below steps
a. Under 'Bucket Policy', Select 'Edit Bucket Policy' and consider defining what explicit 'Principal' should have the ability to GET/LIST objects in your S3 bucket. You may also want to specifically limit the 'Principal' ability to perform specific GET/LIST functions, without the wild card.
If 'Bucket Policy' is not required delete the existing 'Bucket Policy'.
b. Click on Save changes
Note: Make sure updating 'Access Control List' or 'Bucket Policy' does not affect S3 bucket data access.

# 7. Restrict access to cardholder data by business need to know

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.

## AWS IAM policy allows full administrative privileges

| | |
|---|---|
| Compliance Section: 7.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 31 | |

### Description:

This policy identifies IAM policies with full administrative privileges. IAM policies are the means by which privileges are granted to users, groups, or roles. It is recommended and considered a standard security advice to grant least privilege like granting only the permissions required to perform a task. Determine what users need to do and then craft policies for them that let the users perform only those tasks, instead of allowing full administrative privileges.

### Recommendations:

1. Log in to the AWS Console
2. Navigate to the IAM dashboard
3. In the navigation pane, click on Policies and then search for the policy name reported
4. Select the policy, click on the 'Policy actions', select 'Detach'
5. Select all Users, Groups, Roles that have this policy attached, Click on 'Detach policy'

# 7. Restrict access to cardholder data by business need to know

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.

## AWS ECS task definition elevated privileges enabled

| | |
|---|---|
| Compliance Section: 7.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies the ECS containers that are having elevated privileges on the host container instance. When the Privileged parameter is true, the container is given elevated privileges on the host container instance (similar to the root user). Note: This parameter is not supported for Windows containers or tasks using the Fargate launch type.

### Recommendations:

Create a task definition revision.

1. Open the Amazon ECS console.
2. From the navigation bar, choose the region that contains your task definition.
3. In the navigation pane, choose Task Definitions.
4. On the Task Definitions page, select the box to the left of the task definition to revise and choose Create new revision.
5. On the Create new revision of Task Definition page, change the existing Container Definitions.
6. Under Security, uncheck the Privileged box.
7. Verify the information and choose Update, then Create.
8. If your task definition is used in a service, update your service with the updated task definition.
9. Deactivate previous task definition

# 7. Restrict access to cardholder data by business need to know

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.

## AWS IAM role/user with unused CloudTrail delete or full permission

| | |
|---|---|
| Compliance Section: 7.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 80 | |

### Description:

This policy identifies IAM roles/users that have unused CloudTrail delete permission or CloudTrail full permissions. As a security best practice, it is recommended to grant the least privilege access like granting only the permissions required to perform a task, instead of providing excessive permissions to a particular role/user. It helps to reduce the potential improper or unintended access to your critical CloudTrail infrastructure.

### Recommendations:

If Roles with unused CloudTrail delete permission,
1. Log in to AWS console
2. Navigate IAM service
3. Click on Roles
4. Click on reported IAM role
5. In the Permissions tab, Under the 'Permissions policies' section, Remove the policies which have CloudTrail permissions or Delete role if is not required.

If Users with unused CloudTrail delete permission,
1. Log in to AWS console
2. Navigate IAM service
3. Click on Users
4. Click on reported IAM user
5. In the Permissions tab, Under the 'Permissions policies' section, Remove the policies which have CloudTrail permissions or Delete user if is not required.

# 7. Restrict access to cardholder data by business need to know

7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.

## AWS S3 bucket has global view ACL permissions enabled

| | |
|---|---|
| Compliance Section: 7.1.2 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 12 | |

### Description:

This policy determines if any S3 bucket(s) has Global View ACL permissions enabled for the All Users group. These permissions allow external resources to see the permission settings associated to the object.

### Recommendations:

1. Go to the AWS console S3 dashboard.
2. Select your bucket by clicking on the bucket name.
3. Select the Permissions tab and 'Access Control List.'
4. Under Public Access, select Everyone.
5. In the popup window, under Access to this bucket's ACL, uncheck 'Read bucket permissions' and Save.

# 7. Restrict access to cardholder data by business need to know

7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.

## AWS IAM user has two active Access Keys

| | |
|---|---|
| Compliance Section: 7.1.2 | First Seen: N/A |
| Resource(s) Failed: 1 | Resource Type: IAM Credentials Report |
| Resource(s) Passed: 14 | |

### Description:

This policy identifies IAM users who have two active Access Keys. Each IAM user can have up to two Access Keys, having two Keys instead of one can lead to increased chances of accidental exposure. So it needs to be ensured that unused Access Keys are deleted.

### Resource(s) Failed:

PrismaCloudCompute

### Recommendations:

1. Sign in to the AWS Console and navigate to the 'IAM' service.
2. Click on Users in the navigation pane.
3. For the identified IAM user which has two active Access Keys, based on policies of your company, take appropriate action.
4. Create another IAM user with the specific objective performed by the 2nd Access Key.
5. Delete one of the unused Access Keys.

# 7. Restrict access to cardholder data by business need to know

7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.

## AWS IAM user has both Console access and Access Keys

| | |
|---|---|
| Compliance Section: 7.1.2 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: IAM Credentials Report |
| Resource(s) Passed: 15 | |

### Description:

This policy identifies IAM users who have both Console access and Access Keys. When an IAM user is created, the Administrator can assign either Console access or Access Keys or both. Ideally the Console access should be assigned to Users and Access Keys for system / API applications, but not both to the same IAM user.

### Recommendations:

1. Sign in to the AWS console and navigate to the 'IAM' service.
2. Identify the reported IAM user.
3. In 'Security credentials' tab check for presence of Access Keys.
4. Based on the requirement and company policy, either delete the Access Keys or remove the Console access for this IAM user.

# 7. Restrict access to cardholder data by business need to know

7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.

## AWS EC2 Instance IAM Role not enabled

| | |
|---|---|
| Compliance Section: 7.1.2 | First Seen: N/A |
| Resource(s) Failed: 7 | Resource Type: Other |
| Resource(s) Passed: 5 | |

### Description:

AWS provides Identity Access Management (IAM) roles to securely access AWS services and resources. The role is an identity with permission policies that define what the identity can and cannot do in AWS. As a best practice, create IAM roles and attach the role to manage EC2 instance permissions securely instead of distributing or sharing keys or passwords.

### Resource(s) Failed:

Jenkins, BasicWindowsTarget, CTF_ADMIN_VM, i-0e5bac92212240efd, i-0fa5de28b835f969b, i-0698bcb22d1feb644, i-0112554313a2717e2

### Recommendations:

The most common setup is the AWS default that allows for EC2 access to AWS Services. For most, this is a great way to realize flexible, yet secure, EC2 access enabled for your instances. Select this when you launch EC2 instances to automatically inherit these permissions.

IAM

1. Go to the AWS console IAM dashboard.
2. In the navigation pane, choose Roles, Create new role.
3. Under 'Choose the service that will use this role' select EC2, then 'Next:Permissions.'
4. On the Attach permissions policies page, select an AWS managed policy that grants your instance access to the resources that they need, then 'Next:Tags.'
5. Add tags (optional), the select 'Next:Review.'
6. On the Create role and Review page, type a name for the role and choose Create role.

EC2

1. Go to the AWS console EC2 dashboard.
2. Select Running Instances.
3. Check the instance you want to modify.
4. From the Actions pull down menu, select Instance Settings and Attach/Replace IAM Role.
5. On the Attach/Replace IAM Role page, under the IAM role pull down menu, choose the role created in the IAM steps above.

# 7. Restrict access to cardholder data by business need to know

7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.

## AWS IAM policy attached to users

| | |
|---|---|
| Compliance Section: 7.1.2 | First Seen: N/A |
| Resource(s) Failed: 11 | Resource Type: IAM User Managed Policies |
| Resource(s) Passed: 3 | |

### Description:

This policy identifies IAM policies attached to user. By default, IAM users, groups, and roles have no access to AWS resources. IAM policies are the means by which privileges are granted to users, groups, or roles. It is recommended that IAM policies be applied directly to groups but not users.

### Resource(s) Failed:

Adam, PrismaCloudCompute, Michaele, suhas, CTF_ADMIN_VM, CTF_ADMIN, flau, Randy, Cindy, Jim ...and 1 more

### Recommendations:

1. Sign in to the AWS Console
2. Navigate to the 'IAM' service.
3. Identify the users that were specifically assigned to the reported IAM policy.
4. If a group with a similar policy already exists, put the user into that group. If such a group does not exist, create a new group with relevant policy and assign the user to the group.

# 7. Restrict access to cardholder data by business need to know

7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.

## AWS SageMaker notebook instance with root access enabled

| | |
|---|---|
| Compliance Section: 7.1.2 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies the SageMaker notebook instances which are enabled with root access. Root access means having administrator privileges, users with root access can access and edit all files on the compute instance, including system-critical files. Removing root access prevents notebook users from deleting system-level software, installing new software, and modifying essential environment components. NOTE: Lifecycle configurations need root access to be able to set up a notebook instance. Because of this, lifecycle configurations associated with a notebook instance always run with root access even if you disable root access for users. For more details: https://docs.aws.amazon.com/sagemaker/latest/dg/nbi-root-access.html

### Recommendations:

1. Log in to AWS console
2. Navigate to the AWS SageMaker dashboard
3. Choose Notebook instances (Left panel)
4. Click on the reported SageMaker notebook instance

Note: To update root access for SageMaker notebook instances; Instances need to be stopped. So stop running instance before editing.

5. In the 'Notebook instance settings' section, click on 'Edit'
6. On the Edit notebook instance page, within the 'Permissions and encryption' section,

From the 'Root access - optional' options, select 'Disable - Don't give users root access to the notebook'

7. Click on the 'Update notebook instance'

# 7. Restrict access to cardholder data by business need to know

7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.

## AWS S3 bucket having policy overly permissive to VPC endpoints

| | |
|---|---|
| Compliance Section: 7.1.2 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 12 | |

### Description:

This policy identifies S3 buckets that have the bucket policy overly permissive to VPC endpoints. It is recommended to follow the principle of least privileges ensuring that the VPC endpoints have only necessary permissions instead of full permission on S3 operations. NOTE: When applying the Amazon S3 bucket policies for VPC endpoints described in this section, you might block your access to the bucket without intending to do so. Bucket permissions that are intended to specifically limit bucket access to connections originating from your VPC endpoint can block all connections to the bucket. The policy might disable console access to the specified bucket because console requests don't originate from the specified VPC endpoint. So remediation should be done very carefully. For details refer https://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies-vpc-endpoint.html

### Recommendations:

1. Log in to the AWS console
2. Navigate to the S3 dashboard
3. Choose the reported S3 bucket
4. In the 'Permissions' tab, click on the 'Bucket Policy'
5. Update the S3 bucket policy for the VPC endpoint so that it has only required permissions instead of full S3 permission.

Refer for example: https://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies-vpc-endpoint.html

# 7. Restrict access to cardholder data by business need to know

7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.

## AWS IAM policy allows assume role permission across all services

| | |
|---|---|
| Compliance Section: 7.1.2 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: IAM Policy |
| Resource(s) Passed: 31 | |

### Description:

This policy identifies AWS IAM policy which allows assume role permission across all services. Typically, AssumeRole is used if you have multiple accounts and need to access resources from each account then you can create long term credentials in one account and then use temporary security credentials to access all the other accounts by assuming roles in those accounts.

### Recommendations:

1. Log in to the AWS Console
2. Navigate to the 'IAM' service.
3. Identify the reported policy
4. Change the Service element of the policy document to be more restrictive so that it only allows AssumeRole permission on select services.

# 7. Restrict access to cardholder data by business need to know

7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.

## AWS IAM deprecated managed policies in use by User

| | |
|---|---|
| Compliance Section: 7.1.2 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 14 | |

### Description:

This policy checks for any usage of deprecated AWS IAM managed policies and returns an alert if it finds one in your cloud resources. When AWS deprecate an IAM managed policy, a new alternative is released with improved access restrictions. Existing IAM users and roles can continue to use the previous policy without interruption, however new IAM users and roles will use the new replacement policy. Before you migrate any user or role to the new replacement policy, we recommend you review their differences in the Policy section of AWS IAM console. If you require one or more of the removed permissions, please add them separately to any user or role. List of deprecated AWS IAM managed policies: AmazonElasticTranscoderFullAccess (replaced by AmazonElasticTranscoder_FullAccess)

### Recommendations:

1. Go to the AWS console IAM dashboard.
2. Click Policies on the left navigation menu.
3. Enter the deprecated IAM policy name into the filter.
4. Click on the policy name.
5. Select the Policy usage tab.
6. Check all attached users, make note of them, then select Detach.
7. Click Policies on the left navigation menu.
8. Enter the new IAM policy name into the filter.
9. Click on the policy name.
10. Select the Policy usage tab.
11. Select Attach and check all the users you made a note of.
12. Click Attach policy.

# 7. Restrict access to cardholder data by business need to know

7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.

## AWS IAM support access policy is not associated to any role

| | |
|---|---|
| Compliance Section: 7.1.2 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 31 | |

### Description:

This policy identifies IAM policies with support role access which are not attached to any role for an account. AWS provides a support centre that can be used for incident notification and response, as well as technical support and customer services.

### Recommendations:

1. Log in to AWS console
2.Go to service IAM under Services panel.
3.From left panel click on 'Policies'
4.Search for the existence of a support policy 'AWSSupportAccess'
5.Create a IAM role
6.Attach 'AWSSupportAccess' managed policy to the created IAM role

# 7. Restrict access to cardholder data by business need to know

7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.

## AWS SQS queue access policy is overly permissive

| | |
|---|---|
| Compliance Section: 7.1.2 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies Simple Queue Service (SQS) queues that have an overly permissive access policy. It is highly recommended to have the least privileged access policy to protect the SQS queue from data leakage and unauthorized access. For more details: https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-basic-examples-of-sqs-policies.html

### Recommendations:

1. Log in to the AWS console
2. Select the region, from the region drop-down, in which the alert is generated
3. Navigate to Simple Queue Service (SQS) dashboard
4. Choose the reported Simple Queue Service (SQS) and choose 'Edit'
5. Scroll to the 'Access policy' section
6. Edit the access policy statements in the input box, Make sure the 'Principal' is not set to '*', which makes your SQS queues accessible to any anonymous users.
7. When you finish configuring the access policy, choose 'Save'.

# 7. Restrict access to cardholder data by business need to know

7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.

## AWS IAM Roles with Administrator Access Permissions

| | |
|---|---|
| Compliance Section: 7.1.2 | First Seen: N/A |
| Resource(s) Failed: 5 | Resource Type: Other |
| Resource(s) Passed: 88 | |

### Description:

This policy identifies AWS IAM roles which has administrator access permission set. This would allow all users who assume this role to have administrative privileges. As a security best practice, it is recommended to grant least privilege access like granting only the permissions required to perform a task, instead of providing excessive permissions.

### Resource(s) Failed:

AWSControlTowerExecution, AWSReservedSSO_AWSAdministratorAccess_fb576f420364742d, OrganizationAccountAccessRole, aws-controltower-AdministratorExecutionRole, stacksets-exec-86bfe566cedf709ff3051abaab72473e

### Recommendations:

1. Log in to AWS console
2. Navigate to IAM service
3. Click on Roles
4. Click on reported IAM role
5. Under 'Permissions policies' click on 'X' to detach or remove the policy having excessive permissions and assign a limited permission policy as required for a particular role.

# 7. Restrict access to cardholder data by business need to know

7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.

AWS IAM policy allows full administrative privileges

| | |
|---|---|
| Compliance Section: 7.1.2 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 31 | |

## Description:

This policy identifies IAM policies with full administrative privileges. IAM policies are the means by which privileges are granted to users, groups, or roles. It is recommended and considered a standard security advice to grant least privilege like granting only the permissions required to perform a task. Determine what users need to do and then craft policies for them that let the users perform only those tasks, instead of allowing full administrative privileges.

## Recommendations:

1. Log in to the AWS Console
2. Navigate to the IAM dashboard
3. In the navigation pane, click on Policies and then search for the policy name reported
4. Select the policy, click on the 'Policy actions', select 'Detach'
5. Select all Users, Groups, Roles that have this policy attached, Click on 'Detach policy'

# 7. Restrict access to cardholder data by business need to know

7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.

## AWS ECS task definition elevated privileges enabled

| | |
|---|---|
| Compliance Section: 7.1.2 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies the ECS containers that are having elevated privileges on the host container instance. When the Privileged parameter is true, the container is given elevated privileges on the host container instance (similar to the root user). Note: This parameter is not supported for Windows containers or tasks using the Fargate launch type.

### Recommendations:

Create a task definition revision.

1. Open the Amazon ECS console.
2. From the navigation bar, choose the region that contains your task definition.
3. In the navigation pane, choose Task Definitions.
4. On the Task Definitions page, select the box to the left of the task definition to revise and choose Create new revision.
5. On the Create new revision of Task Definition page, change the existing Container Definitions.
6. Under Security, uncheck the Privileged box.
7. Verify the information and choose Update, then Create.
8. If your task definition is used in a service, update your service with the updated task definition.
9. Deactivate previous task definition

# 7. Restrict access to cardholder data by business need to know

7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.

AWS IAM role/user with unused CloudTrail delete or full permission

| | |
|---|---|
| Compliance Section: 7.1.2 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 80 | |

## Description:

This policy identifies IAM roles/users that have unused CloudTrail delete permission or CloudTrail full permissions. As a security best practice, it is recommended to grant the least privilege access like granting only the permissions required to perform a task, instead of providing excessive permissions to a particular role/user. It helps to reduce the potential improper or unintended access to your critical CloudTrail infrastructure.

## Recommendations:

If Roles with unused CloudTrail delete permission,
1. Log in to AWS console
2. Navigate IAM service
3. Click on Roles
4. Click on reported IAM role
5. In the Permissions tab, Under the 'Permissions policies' section, Remove the policies which have CloudTrail permissions or Delete role if is not required.

If Users with unused CloudTrail delete permission,
1. Log in to AWS console
2. Navigate IAM service
3. Click on Users
4. Click on reported IAM user
5. In the Permissions tab, Under the 'Permissions policies' section, Remove the policies which have CloudTrail permissions or Delete user if is not required.

# 8. Identify and authenticate access to system components

8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users - Something you know, such as a password or passphrase - Something you have, such as a token device or smart card- Something you are, such as a biometric.

## AWS EMR cluster is not configured with Kerberos Authentication

| | |
|---|---|
| Compliance Section: 8.2 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies EMR clusters which are not configured with Kerberos Authentication. Kerberos uses secret-key cryptography to provide strong authentication so that passwords or other credentials aren't sent over the network in an unencrypted format.

### Recommendations:

1. Log in to the AWS Console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to 'EMR' dashboard from 'Services' dropdown
4. Go to 'Security configurations', click 'Create'
5. On the Create security configuration window,
6. In 'Name' box, provide a name for the new EMR security configuration
7. Under the section 'Enable Kerberos authentication' select the check box
8. Follow below link for configuration steps,
https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-kerberos.html
9. Click on 'Create' button
10. On the left menu of EMR dashboard Click 'Clusters'
11. Select the EMR cluster for which the alert has been generated and click on the 'Clone' button from the top menu
12. In the Cloning popup, choose 'Yes' and Click 'Clone'
13. On the Create Cluster page, in the Security Options section, click on 'security configuration'.
14. From the 'Security configuration' drop down select the name of the security configuration created at step 4 to step 8, click 'Create Cluster'
15. Once you the new cluster is set up verify its working and terminate the source cluster in order to stop incurring charges for it.
16. On the left menu of EMR dashboard Click 'Clusters', from the list of clusters select the source cluster which is alerted
17. Click on the 'Terminate' button from the top menu
18. On the 'Terminate clusters' pop-up, click 'Terminate'.

# 8. Identify and authenticate access to system components

8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users - Something you know, such as a password or passphrase - Something you have, such as a token device or smart card- Something you are, such as a biometric.

## AWS IAM Password policy is unsecure

| | |
|---|---|
| Compliance Section: 8.2 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 1 | |

### Description:

Checks to ensure that IAM password policy is in place for the cloud accounts. As a security best practice, customers must have strong password policies in place. This policy ensures password policies are set with all following options: - Minimum Password Length - At least one Uppercase letter - At least one Lowercase letter - At least one Number - At least one Symbol/non-alphanumeric character - Users have permission to change their own password - Password expiration period - Password reuse - Password expiration requires administrator reset

### Recommendations:

1. Login to AWS Console and navigate to the 'IAM' Service
2. Click on 'Account Settings'
3. Under 'Password Policy', select and set all the options
4. Click on 'Apply password policy'

# 8. Identify and authenticate access to system components

8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users - Something you know, such as a password or passphrase - Something you have, such as a token device or smart card- Something you are, such as a biometric.

## AWS ElastiCache Redis cluster with Redis AUTH feature disabled

| | |
|---|---|
| Compliance Section: 8.2 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies ElastiCache Redis clusters which have Redis AUTH feature disabled. Redis AUTH can improve data security by requiring the user to enter a password before they are granted permission to execute Redis commands on a password protected Redis server.

### Recommendations:

AWS ElastiCache Redis cluster Redis AUTH password can be set, only at the time of creation of the cluster. So to resolve this alert, create a new cluster with Redis AUTH feature enabled, then migrate all required ElastiCache Redis cluster data from the reported ElastiCache Redis cluster to this newly created cluster and delete the reported ElastiCache Redis cluster.
To create new ElastiCache Redis cluster with Redis AUTH password set, perform the following:
1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to ElastiCache Dashboard
4. Click on Redis
5. Click on 'Create' button
6. On the 'Create your Amazon ElastiCache cluster' page,
a. Select 'Redis' cache engine type.
b. Enter a name for the new cache cluster
c. Select Redis engine version from 'Engine version compatibility' dropdown list.
Note: As of July 2018, In-transit encryption can be enabled only for AWS ElastiCache clusters with Redis engine version 3.2.6 and 4.0.10.
d. Click on 'Advanced Redis settings' to expand the cluster advanced settings panel
e. Select 'Encryption in-transit' checkbox to enable encryption
Note: Redis AUTH can only be enabled when creating clusters where in-transit encryption is enabled.
f. Select 'Redis AUTH' checkbox to enable to enable AuthToken password
g. Type password you want enforce on 'Redis AUTH Token' textbox.
Choosen password should meet 'Passwords must be at least 16 and a maximum of 128 printable characters. At least 16 characters, and maximum 128 characters, restricted to any printable ASCII character except ' ', "", '/' and '@' signs' criteria. Set the new Redis cluster other parameters which are same as of reported Redis cluster configuration details.
Note: The password set at cluster creation cannot be changed.
7. Click on 'Create' button to launch your new ElastiCache Redis cluster
To delete reported ElastiCache Redis cluster, perform the following:
1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to ElastiCache Dashboard
4. Click on Redis
5. Select reported Redis cluster
6. Click on 'Delete' button

7. In the 'Delete Cluster' dialog box, if you want back for you cluster select 'Yes' from the 'Create final backup' dropdown menu, provide a name for the cluster backup, then click on 'Delete'.

# 8. Identify and authenticate access to system components

8.2.3 Passwords/passphrases must meet the following: - Require a minimum length of at least seven characters. - Contain both numeric and alphabetic characters. Alternatively, the passwords/ passphrases must have complexity and strength at least equivalent to the parameters specified above.

> AWS IAM password policy does not have a minimum of 14 characters

| | |
|---|---|
| Compliance Section: 8.2.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Password Policy |
| Resource(s) Passed: 1 | |

### Description:

Checks to ensure that IAM password policy requires minimum of 14 characters. AWS IAM (Identity & Access Management) allows customers to secure AWS console access. As a security best practice, customers must have strong password policies in place.

### Recommendations:

1. Login to the AWS console and navigate to the 'IAM' service.
2. On the left navigation panel, Click on 'Account Settings'
3. In the 'Minimum password length' field, put 14 or more (As per preference).
4. Click on 'Apply password policy'

# 8. Identify and authenticate access to system components

8.2.3 Passwords/passphrases must meet the following: - Require a minimum length of at least seven characters. - Contain both numeric and alphabetic characters. Alternatively, the passwords/ passphrases must have complexity and strength at least equivalent to the parameters specified above.

## AWS IAM password policy does not have a lowercase character

| | |
|---|---|
| Compliance Section: 8.2.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Password Policy |
| Resource(s) Passed: 1 | |

### Description:

Checks to ensure that IAM password policy requires a lowercase character. AWS IAM (Identity & Access Management) allows customers to secure AWS console access. As a security best practice, customers must have strong password policies in place.

### Recommendations:

1. Login to the AWS console and navigate to the 'IAM' service.
2. On the left navigation panel, Click on 'Account Settings'
3. check 'Require at least one lowercase letter'.
4. Click on 'Apply password policy'

# 8. Identify and authenticate access to system components

8.2.3 Passwords/passphrases must meet the following: - Require a minimum length of at least seven characters. - Contain both numeric and alphabetic characters. Alternatively, the passwords/ passphrases must have complexity and strength at least equivalent to the parameters specified above.

## AWS IAM password policy does not have a number

| | |
|---|---|
| Compliance Section: 8.2.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Password Policy |
| Resource(s) Passed: 1 | |

### Description:

Checks to ensure that IAM password policy requires a number. AWS IAM (Identity & Access Management) allows customers to secure AWS console access. As a security best practice, customers must have strong password policies in place.

### Recommendations:

1. Login to the AWS console and navigate to the 'IAM' service.
2. On the left navigation panel, Click on 'Account Settings'
3. check 'Require at least one number'.
4. Click on 'Apply password policy'

# 8. Identify and authenticate access to system components

8.2.3 Passwords/passphrases must meet the following: - Require a minimum length of at least seven characters. - Contain both numeric and alphabetic characters. Alternatively, the passwords/ passphrases must have complexity and strength at least equivalent to the parameters specified above.

## AWS IAM password policy does not have a symbol

| | |
|---|---|
| Compliance Section: 8.2.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Password Policy |
| Resource(s) Passed: 1 | |

### Description:

Checks to ensure that IAM password policy requires a symbol. AWS IAM (Identity & Access Management) allows customers to secure AWS console access. As a security best practice, customers must have strong password policies in place.

### Recommendations:

1. Login to the AWS console and navigate to the 'IAM' service.
2. On the left navigation panel, Click on 'Account Settings'
3. check 'Require at least one non-alphanumeric character'.
4. Click on 'Apply password policy'

# 8. Identify and authenticate access to system components

8.2.3 Passwords/passphrases must meet the following: - Require a minimum length of at least seven characters. - Contain both numeric and alphabetic characters. Alternatively, the passwords/ passphrases must have complexity and strength at least equivalent to the parameters specified above.

## AWS IAM password policy does not have an uppercase character

| | |
|---|---|
| Compliance Section: 8.2.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Password Policy |
| Resource(s) Passed: 1 | |

### Description:

This policy identifies AWS accounts in which IAM password policy does not have an uppercase character. AWS IAM (Identity & Access Management) allows customers to secure AWS console access. As a security best practice, customers must have strong password policies in place.

### Recommendations:

1. Login to the AWS console and navigate to the 'IAM' service.
2. On the left navigation panel, Click on 'Account Settings'
3. check 'Require at least one uppercase letter'.
4. Click on 'Apply password policy'

# 8. Identify and authenticate access to system components

8.2.4 Change user passwords/passphrases at least once every 90 days.

AWS IAM password policy does not expire in 90 days

| | |
|---|---|
| Compliance Section: 8.2.4 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Password Policy |
| Resource(s) Passed: 1 | |

## Description:

This policy identifies the IAM policies which does not have password expiration set to 90 days. AWS IAM (Identity & Access Management) allows customers to secure AWS console access. As a security best practice, customers must have strong password policies in place.

## Recommendations:

1. Login to the AWS console and navigate to the 'IAM' service.
2. On the left navigation panel, Click on 'Account Settings'
3. check 'Enable password expiration' and enter a password expiration period.
4. Click on 'Apply password policy'

# 8. Identify and authenticate access to system components

8.2.4 Change user passwords/passphrases at least once every 90 days.

AWS IAM password policy does not have password expiration period

| | |
|---|---|
| Compliance Section: 8.2.4 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Password Policy |
| Resource(s) Passed: 1 | |

## Description:

Checks to ensure that IAM password policy has an expiration period. AWS IAM (Identity & Access Management) allows customers to secure AWS console access. As a security best practice, customers must have strong password policies in place.

## Recommendations:

1. Login to the AWS console and navigate to the 'IAM' service.
2. On the left navigation panel, Click on 'Account Settings'
3. check 'Enable password expiration' and enter a password expiration period.
4. Click on 'Apply password policy'

# 8. Identify and authenticate access to system components

8.2.5 Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used.

> AWS IAM password policy allows password reuse

| | |
|---|---|
| Compliance Section: 8.2.5 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Password Policy |
| Resource(s) Passed: 1 | |

### Description:

This policy identifies IAM policies which allow password reuse . AWS IAM (Identity & Access Management) allows customers to secure AWS console access. As a security best practice, customers must have strong password policies in place.

### Recommendations:

1. Sign in to the AWS console and navigate to the 'IAM' service.
2. Click on 'Account Settings', check 'Prevent password reuse'.

# 8. Identify and authenticate access to system components

8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.

## AWS MFA is not enabled on Root account

| | |
|---|---|
| Compliance Section: 8.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: IAM Account Summary |
| Resource(s) Passed: 15 | |

### Description:

This policy identifies root account which has MFA enabled. Root accounts have privileged access to all AWS services. Without MFA, if the root credentials are compromised, unauthorized users will get full access to your account. NOTE: This policy does not apply to AWS GovCloud Accounts. As you cannot enable an MFA device for AWS GovCloud (US) account root user. For more details refer: https://docs.aws.amazon.com/govcloud-us/latest/UserGuide/govcloud-console.html

### Recommendations:

1. Sign in to the 'AWS Console' using Root credentials.
2. Navigate to the 'IAM' service.
3. On the dashboard, click on 'Activate MFA on your root account', click on 'Manage MFA' and follow the steps to configure MFA for the root account.

# 8. Identify and authenticate access to system components

8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.

## AWS MFA not enabled for IAM users

| | |
|---|---|
| Compliance Section: 8.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: IAM Credentials Report |
| Resource(s) Passed: 15 | |

### Description:

This policy identifies AWS IAM users for whom MFA is not enabled. AWS Multi-Factor Authentication (MFA) is a simple best practice that adds an extra layer of protection on top of your user name and password. Multiple factors provide increased security for your AWS account settings and resources.

### Recommendations:

1. Sign in to the AWS and navigate to the 'IAM' service.
2. Navigate to the user that was reported in the alert.
3. Under 'Security Credentials', check "Assigned MFA Device" and follow the instructions to enable MFA for the user.

# 8. Identify and authenticate access to system components

8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.

## AWS Inactive users for more than 30 days

| | |
|---|---|
| Compliance Section: 8.3 | First Seen: N/A |
| Resource(s) Failed: 13 | Resource Type: IAM Credentials Report |
| Resource(s) Passed: 2 | |

### Description:

This policy identifies users who are inactive for more than 30 days. Inactive user accounts are an easy target for attacker because any activity on the account will largely get unnoticed. NOTE: Exception to this policy is, it is not valid for SSO login users and Root users

### Resource(s) Failed:

Ann, Adam, Michaele, suhas, Randy, flau, CTF_ADMIN, awsjamconfig-PANWLabUser-XU1LWGL7AKS7, Cindy, rsingh1@paloaltonetworks.com ...and 3 more

### Recommendations:

1.Sign in to AWS console and navigate to IAM.
2.Identify the user reported and Make sure that the user has legitimate reason to be inactive for such an extended period.
3. Delete the user account, if the user no longer needs access to the console or no longer exists.

# 8. Identify and authenticate access to system components

8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.

## AWS Access key enabled on root account

| | |
|---|---|
| Compliance Section: 8.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: IAM Account Summary |
| Resource(s) Passed: 1 | |

### Description:

This policy identifies root accounts for which access keys are enabled. Access keys are used to sign API requests to AWS. Root accounts have complete access to all your AWS services. If the access key for a root account is compromised, an unauthorized users will have complete access to your AWS account.

### Recommendations:

1. Sign in to AWS Console as the root user.
2. Click root account name and on the top right select 'Security Credentials' from the dropdown.
3. For each key in 'Access Keys', click on "X" to delete the keys.

# 10. Track and monitor all access to network resources and cardholder data

10.1 Implement audit trails to link all access to system components to each individual user.

AWS CloudTrail is not enabled on the account

| | |
|---|---|
| Compliance Section: 10.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 21 | |

Description:

Checks to ensure that CloudTrail is enabled on the account. AWS CloudTrail is a service that enables governance, compliance, operational & risk auditing of the AWS account. It is a compliance and security best practice to turn on CloudTrail to get a complete audit trail of activities across various services.

Recommendations:

1. Login to the AWS Console and navigate to the 'CloudTrail' service.
2. Follow the instructions below to enable CloudTrail on the account.

http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-create-and-update-a-trail.html

# 10. Track and monitor all access to network resources and cardholder data

10.1 Implement audit trails to link all access to system components to each individual user.

## AWS Access logging not enabled on S3 buckets

| | |
|---|---|
| Compliance Section: 10.1 | First Seen: N/A |
| Resource(s) Failed: 12 | Resource Type: Bucket Logging Config |
| Resource(s) Passed: 0 | |

### Description:

Checks for S3 buckets without access logging turned on. Access logging allows customers to view complete audit trail on sensitive workloads such as S3 buckets. It is recommended that Access logging is turned on for all S3 buckets to meet audit & compliance requirement

### Resource(s) Failed:

aws-cloudtrail-logs-795462528824-317b0c26, mygoalsapp-pipelineartifactsbucket-1es78l9rtorl1, s3-production-for-pp-ctf, prisma-guardduty-findings, mybookstore-assetsbucket-h49w4uta9ws4, cf-templates-cnh9x6netk1b-us-west-1, mygoalsapp-assetsbucket-1jvraqv1lbf1z, mybookstore-pipelineartifactsbucket-1ov8q9nvordkf, cf-templates-cnh9x6netk1b-us-east-1, agentbucket-795462528824 ...and 2 more

### Recommendations:

1. Login to the AWS Console and navigate to the 'S3' service.
2. Click on the the S3 bucket that was reported.
3. Click on the 'Properties' tab.
4. Under the 'Server access logging' section, select 'Enable logging' option.

# 10. Track and monitor all access to network resources and cardholder data

10.1 Implement audit trails to link all access to system components to each individual user.

## AWS S3 buckets are accessible to public

| | |
|---|---|
| Compliance Section: 10.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 12 | |

### Description:

This policy identifies S3 buckets which are publicly accessible. Amazon S3 allows customers to store or retrieve any type of content from anywhere in the web. Often, customers have legitimate reasons to expose the S3 bucket to public, for example, to host website content. However, these buckets often contain highly sensitive enterprise data which if left open to public may result in sensitive data leaks.

### Recommendations:

1. Login to the AWS Console
2. Navigate to the 'S3' service
3. Click on the 'S3' resource reported in the alert
4. Click on the 'Permissions'
5. If Access Control List' is set to 'Public' follow below steps
a. Under 'Access Control List', Click on 'Everyone' and uncheck all items
b. Click on Save
6. If 'Bucket Policy' is set to public follow below steps
a. Under 'Bucket Policy', modify the policy to remove public access
b. Click on Save
c. If 'Bucket Policy' is not required delete the existing 'Bucket Policy'.
Note: Make sure updating 'Access Control List' or 'Bucket Policy' does not affect S3 bucket data access.

# 10. Track and monitor all access to network resources and cardholder data

10.1 Implement audit trails to link all access to system components to each individual user.

## AWS S3 buckets are accessible to any authenticated user

| | |
|---|---|
| Compliance Section: 10.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 12 | |

### Description:

This policy identifies S3 buckets accessible to any authenticated AWS users. Amazon S3 allows customer to store and retrieve any type of content from anywhere in the web. Often, customers have legitimate reasons to expose the S3 bucket to public, for example to host website content. However, these buckets often contain highly sensitive enterprise data which if left accessible to anyone with valid AWS credentials, may result in sensitive data leaks.

### Recommendations:

1. Login to the AWS Console
2. Navigate to the 'S3' service
3. Click on the 'S3' resource reported in the alert
4. Click on the 'Permissions'
5. Under 'Public access', Click on 'Any AWS user' and uncheck all items
6. Click on Save

# 10. Track and monitor all access to network resources and cardholder data

10.1 Implement audit trails to link all access to system components to each individual user.

AWS CloudTrail is not enabled with multi trail and not capturing all management events

| | |
|---|---|
| Compliance Section: 10.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: CloudTrail Setting |
| Resource(s) Passed: 3 | |

### Description:

This policy identifies the AWS accounts which do not have a CloudTrail with multi trail enabled and capturing all management events. AWS CloudTrail is a service that enables governance, compliance, operational & risk auditing of the AWS account. It is a compliance and security best practice to turn on CloudTrail across different regions to get a complete audit trail of activities across various services. NOTE: If you have Organization Trail enabled in your account, this policy can be disabled, or alerts generated for this policy on such an account can be ignored; as Organization Trail by default enables trail log for all accounts under that organization.

### Recommendations:

Refer to the following link to create/update the trail:
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-create-and-update-a-trail.html

# 10. Track and monitor all access to network resources and cardholder data

10.2.3 Access to all audit trails.

## AWS Access logging not enabled on S3 buckets

| | |
|---|---|
| Compliance Section: 10.2.3 | First Seen: N/A |
| Resource(s) Failed: 12 | Resource Type: Bucket Logging Config |
| Resource(s) Passed: 0 | |

### Description:

Checks for S3 buckets without access logging turned on. Access logging allows customers to view complete audit trail on sensitive workloads such as S3 buckets. It is recommended that Access logging is turned on for all S3 buckets to meet audit & compliance requirement

### Resource(s) Failed:

aws-cloudtrail-logs-795462528824-317b0c26, mygoalsapp-pipelineartifactsbucket-1es78l9rtorl1, s3-production-for-pp-ctf, prisma-guardduty-findings, mybookstore-assetsbucket-h49w4uta9ws4, cf-templates-cnh9x6netk1b-us-west-1, mygoalsapp-assetsbucket-1jvraqv1lbf1z, mybookstore-pipelineartifactsbucket-1ov8q9nvordkf, cf-templates-cnh9x6netk1b-us-east-1, agentbucket-795462528824 ...and 2 more

### Recommendations:

1. Login to the AWS Console and navigate to the 'S3' service.
2. Click on the the S3 bucket that was reported.
3. Click on the 'Properties' tab.
4. Under the 'Server access logging' section, select 'Enable logging' option.

# 10. Track and monitor all access to network resources and cardholder data

10.2.3 Access to all audit trails.

## AWS Redshift database does not have audit logging enabled

| | |
|---|---|
| Compliance Section: 10.2.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Managed Database |
| Resource(s) Passed: 0 | |

### Description:

Audit logging is not enabled by default in Amazon Redshift. When you enable logging on your cluster, Amazon Redshift creates and uploads logs to Amazon S3 that capture data from the creation of the cluster to the present time.

### Recommendations:

1. Login to AWS Console.
2. Goto Amazon Redshift service
3. On left navigation panel, click on Clusters
4. Click on the reported cluster
5. Click on Database tab and choose 'Configure Audit Logging'
6. On Enable Audit Logging, choose 'Yes'
7. Create a new s3 bucket or use an existing bucket
8. click Save

# 10. Track and monitor all access to network resources and cardholder data

10.2.3 Access to all audit trails.

## AWS Elasticsearch domain has Index slow logs set to disabled

| | |
|---|---|
| Compliance Section: 10.2.3 | First Seen: N/A |
| Resource(s) Failed: 1 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies Elasticsearch domains for which Index slow logs is disabled in your AWS account. Enabling support for publishing indexing slow logs to AWS CloudWatch Logs enables you have full insight into the performance of indexing operations performed on your Elasticsearch clusters. This will help you in identifying performance issues caused by specific queries or due to changes in cluster usage, so that you can optimize your index configuration to address the problem.

### Resource(s) Failed:

mybookstore-domain

### Recommendations:

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to Elasticsearch Service Dashboard
4. Choose reported Elasticsearch domain
5. Select the 'Logs' tab
6. In 'Set up Index slow logs' section,

a. click on 'Setup'
b. In 'Select CloudWatch Logs log group' setting, Create/Use existing CloudWatch Logs log group as per your requirement
c. In 'Specify CloudWatch access policy', Create new/Select an existing policy as per your requirement
d. Click on 'Enable'

The Index slow logs setting 'Status' should change now to 'Enabled'.

# 10. Track and monitor all access to network resources and cardholder data

10.2.3 Access to all audit trails.

## AWS Config fails to deliver log files

| | |
|---|---|
| Compliance Section: 10.2.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 5 | |

### Description:

This policy identifies AWS Configs which are failing to deliver its log files to the specified S3 bucket. It happens when it doesn't have sufficient permissions to complete the operation. To deliver information to S3 bucket, AWS Config needs to assume an IAM role that manages the permissions required to access the designated S3 bucket.

### Recommendations:

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to the AWS Config Dashboard
4. Go to 'Settings' (Left Pane)
5. In 'AWS Config role' section, 'Choose a role from your account' option and provide a unique name for new IAM role for the 'Role name' box; which does have permission to access S3 bucket.
6. Click Save

# 10. Track and monitor all access to network resources and cardholder data

10.2.3 Access to all audit trails.

## AWS Config must record all possible resources

| | |
|---|---|
| Compliance Section: 10.2.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Config Service Recorder |
| Resource(s) Passed: 5 | |

### Description:

This policy identifies resources for which AWS Config recording is enabled but recording for all possible resources are disabled. AWS Config provides an inventory of your AWS resources and a history of configuration changes to these resources. You can use AWS Config to define rules that evaluate these configurations for compliance. Hence, it is important to enable this feature.

### Recommendations:

1. Login to the AWS and navigate to the 'Config' service
2. Change to the respective region and in the navigation pane, click on 'Settings'
3. Review the 'All resources' and Check the 2 options (3.a and 3.b)

3.a Record all resources supported in this region

3.b Include global resources (e.g., AWS IAM resources)

# 10. Track and monitor all access to network resources and cardholder data

10.2.3 Access to all audit trails.

## AWS CloudTrail logging is disabled

| | |
|---|---|
| Compliance Section: 10.2.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 3 | |

### Description:

This policy identifies the CloudTrails in which logging is disabled. AWS CloudTrail is a service that enables governance, compliance, operational & risk auditing of the AWS account. It is a compliance and security best practice to turn on logging for CloudTrail across different regions to get a complete audit trail of activities across various services. NOTE: This policy will be triggered only when you have CloudTrail configured in your AWS account and logging is disabled.

### Recommendations:

1. Sign in to AWS Console
2. Navigate to CloudTrail dashboard
3. Click on 'Trails' (Left panel)
4. Click on reported CloudTrail
5. Enable 'Logging' by hovering logging button to 'ON'

OR

If CLoudTrail is not required you can delete by clicking on the delete icon below the logging hover button.

# 10. Track and monitor all access to network resources and cardholder data

10.2.3 Access to all audit trails.

## AWS EKS control plane logging disabled

| | |
|---|---|
| Compliance Section: 10.2.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

Amazon EKS control plane logging provides audit and diagnostic logs directly from the Amazon EKS control plane to CloudWatch Logs in your account. These logs make it easy for you to secure and run your clusters. You can select the exact log types you need, and logs are sent as log streams to a group for each Amazon EKS cluster in CloudWatch. This policy generates an alert if control plane logging is disabled.

### Recommendations:

To enable control plane logs:
1. Login to AWS Console
2. Navigate to the Amazon EKS dashboard
3. Choose the name of the cluster to display your cluster information
4. Under Logging, choose 'Manage logging'
5. For each individual log type, choose Enabled
6. Click on 'Save changes'

# 10. Track and monitor all access to network resources and cardholder data

10.2.3 Access to all audit trails.

## AWS VPC Flow Logs not enabled

| | |
|---|---|
| Compliance Section: 10.2.3 | First Seen: N/A |
| Resource(s) Failed: 17 | Resource Type: Other |
| Resource(s) Passed: 8 | |

### Description:

This policy identifies VPCs which have flow logs disabled. VPC Flow logs capture information about IP traffic going to and from network interfaces in your VPC. Flow logs are used as a security tool to monitor the traffic that is reaching your instances. Without the flow logs turned on, it is not possible to get any visibility into network traffic.

### Resource(s) Failed:

Jenkins, vpc-60c2d707, vpc-0f271f68, vpc-e045df89, vpc-f085549b, vpc-d9581cb1, vpc-84def2fe, vpc-aabf7ec1, vpc-86fd1eff, vpc-2cd6d14b ...and 7 more

### Recommendations:

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to VPC Dashboard
4. Click on 'Your VPCs' and Choose the reported VPC
5. Click on the 'Flow logs' tab and follow the instructions as in link below to enable Flow Logs for the VPC:
https://aws.amazon.com/blogs/aws/vpc-flow-logs-log-and-view-network-traffic-flows/

# 10. Track and monitor all access to network resources and cardholder data

10.2.3 Access to all audit trails.

## AWS CloudTrail logs should integrate with CloudWatch for all regions

| | |
|---|---|
| Compliance Section: 10.2.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 3 | |

### Description:

This policy identifies the Cloudtrails which is not integrated with cloudwatch for all regions. CloudTrail uses Amazon S3 for log file storage and delivery, so log files are stored durably. In addition to capturing CloudTrail logs within a specified S3 bucket for long term analysis, realtime analysis can be performed by configuring CloudTrail to send logs to CloudWatch Logs. For a trail that is enabled in all regions in an account, CloudTrail sends log files from all those regions to a CloudWatch Logs log group. It is recommended that CloudTrail logs be sent to CloudWatch Logs.

### Recommendations:

1. Sign into AWS and navigate to CloudTrail service.
2. Click on Trail in the left menu navigation and choose the reported cloudtrail.
3. Go to CloudWatch Logs section and click Configure.
4. Define a new or select an existing log group and click Continue to complete the process.

# 10. Track and monitor all access to network resources and cardholder data

10.2.3 Access to all audit trails.

## AWS Certificate Manager (ACM) has certificates with Certificate Transparency Logging disabled

| | |
|---|---|
| Compliance Section: 10.2.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies AWS Certificate Manager certificates in which Certificate Transparency Logging is disabled. AWS Certificate Manager (ACM) is the preferred tool to provision, manage, and deploy your server certificates. Certificate Transparency Logging is used to guard against SSL/TLS certificates that are issued by mistake or by a compromised CA, some browsers require that public certificates issued for your domain can also be recorded. This policy generates alerts for certificates which have transparency logging disabled. As a best practice, it is recommended to enable Transparency logging for all certificates.

### Recommendations:

You cannot currently use the console to opt out of or into transparency logging. It's recommended to use the command line utility to enable transparency logging.
Remediation CLI:
1. Use the below command to list ACM certificate
aws acm list-certificates
2. Note the 'CertificateArn' of the reported ACM certificate
3. Use the below command to ENABLE Certificate Transparency Logging
aws acm update-certificate-options --certificate-arn <certificateARN> --options CertificateTransparencyLoggingPreference=ENABLED
where 'CertificateArn' is captured in the step2

# 10. Track and monitor all access to network resources and cardholder data

10.2.3 Access to all audit trails.

## AWS S3 CloudTrail bucket for which access logging is disabled

| | |
|---|---|
| Compliance Section: 10.2.3 | First Seen: N/A |
| Resource(s) Failed: 1 | Resource Type: Other |
| Resource(s) Passed: 12 | |

### Description:

This policy identifies S3 CloudTrail buckets for which access is disabled. S3 Bucket access logging generates access records for each request made to your S3 bucket. An access log record contains information such as the request type, the resources specified in the request worked, and the time and date the request was processed. It is recommended that bucket access logging be enabled on the CloudTrail S3 bucket.

### Resource(s) Failed:

aws-cloudtrail-logs-795462528824-317b0c26

### Recommendations:

1. Login to the AWS Console and navigate to the 'S3' service.
2. Click on the the S3 bucket that was reported.
3. Click on the 'Properties' tab.
4. Under the 'Server access logging' section, select 'Enable' option and provide s3 bucket of your choice in the 'Target bucket'
5. Click on 'Save Changes'

# 10. Track and monitor all access to network resources and cardholder data

10.2.3 Access to all audit trails.

## AWS RDS Event subscription All event categories and All instances disabled for DB instance

| | |
|---|---|
| Compliance Section: 10.2.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies AWS RDS event subscriptions for DB instance which has 'All event categories' and 'All instances' is disabled. As a best practice enabling 'All event categories' for 'All instances' helps to get notified when an event occurs for a DB instance.

### Recommendations:

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to Amazon RDS Dashboard
4. Click on 'Event subscriptions' (Left Panel)
5. Choose the reported Event subscription
6. Click on 'Edit'
7. On 'Edit event subscription' page, Under 'Details' section; Select 'Yes' for 'Enabled' and Make sure you have subscribed your DB to 'All instances' and 'All event categories'
8. Click on 'Edit'

# 10. Track and monitor all access to network resources and cardholder data

10.2.3 Access to all audit trails.

## AWS Elasticsearch domain has Search slow logs set to disabled

| | |
|---|---|
| Compliance Section: 10.2.3 | First Seen: N/A |
| Resource(s) Failed: 1 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies Elasticsearch domains for which Search slow logs is disabled in your AWS account. Enabling support for publishing Search slow logs to AWS CloudWatch Logs enables you to have full insight into the performance of search operations performed on your Elasticsearch clusters. This will help you in identifying performance issues caused by specific search queries so that you can optimize your queries to address the problem.

### Resource(s) Failed:

mybookstore-domain

### Recommendations:

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to Elasticsearch Service Dashboard
4. Choose reported Elasticsearch domain
5. Select the 'Logs' tab
6. In 'Set up Search slow logs' section,

a. click on 'Setup'
b. In 'Select CloudWatch Logs log group' setting, Create/Use existing CloudWatch Logs log group as per your requirement
c. In 'Specify CloudWatch access policy', Create new/Select an existing policy as per your requirement
d. Click on 'Enable'

The search slow logs setting 'Status' should change now to 'Enabled'.

# 10. Track and monitor all access to network resources and cardholder data

10.2.3 Access to all audit trails.

## CloudTrail trail is not integrated with CloudWatch Log

| | |
|---|---|
| Compliance Section: 10.2.3 | First Seen: N/A |
| Resource(s) Failed: 1 | Resource Type: CloudTrail Setting |
| Resource(s) Passed: 1 | |

### Description:

Enabling the CloudTrail trail logs integrated with CloudWatch Logs will enable the real-time as well as historic activity logging. This will further effective monitoring and alarm capability.

### Resource(s) Failed:

cloud-trail-demo

### Recommendations:

1. Login to the AWS Admin Console and access the CloudTrail service.
2. Click on the Trails in the left hand menu.
3. Click on the identified CloudTrail and navigate to the 'CloudWatch Logs' section.
4. Click on 'Configure' tab and provide required
5. Provide a log group name in field 'New or existing log group'
6. Click on 'Continue'
7. In the next page from 'IAM role' dropdown select an IAM role with required access or select the 'Create a new IAM role'
8. Click on 'Allow'

# 10. Track and monitor all access to network resources and cardholder data

10.2.3 Access to all audit trails.

## AWS Elastic Load Balancer v2 (ELBv2) with access log disabled

| | |
|---|---|
| Compliance Section: 10.2.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies Elastic Load Balancers v2 (ELBv2) which have access log disabled. Access logs capture detailed information about requests sent to your load balancer and each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. You can use these access logs to analyze traffic patterns and troubleshoot issues.

### Recommendations:

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to EC2 dashboard
4. Click on 'Load Balancers' (Left Panel)
5. Select the reported ELB
6. Click on 'Actions' drop-down
7. Click on 'Edit attributes'
8. In the 'Edit load balancer attributes' popup box, Choose 'Enable' for 'Access logs' and configure S3 location where you want to store ELB logs.
9. Click on 'Save'

# 10. Track and monitor all access to network resources and cardholder data

10.2.3 Access to all audit trails.

## AWS Elastic Load Balancer (Classic) with access log disabled

| | |
|---|---|
| Compliance Section: 10.2.3 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies Classic Elastic Load Balancers which have access log disabled. When Access log enabled, Classic load balancer captures detailed information about requests sent to your load balancer. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. You can use these access logs to analyze traffic patterns and to troubleshoot issues.

### Recommendations:

To enable access logging for Elastic Load Balancer (Classic), follow below mentioned URL:
https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/enable-access-logs.html

# 10. Track and monitor all access to network resources and cardholder data

10.2.3 Access to all audit trails.

## AWS CloudFront distribution with access logging disabled

| | |
|---|---|
| Compliance Section: 10.2.3 | First Seen: N/A |
| Resource(s) Failed: 2 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies CloudFront distributions which have access logging disabled. Enabling access log on distributions creates log files that contain detailed information about every user request that CloudFront receives. Access logs are available for web distributions. If you enable logging, you can also specify the Amazon S3 bucket that you want CloudFront to save files in.

### Resource(s) Failed:

d2rwvuyjsg9kf7.cloudfront.net, d2u45drmoykiua.cloudfront.net

### Recommendations:

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to CloudFront Distributions Dashboard
4. Click on the reported distribution
5. On 'General' tab, Click on 'Edit' button
6. On 'Edit Distribution' page, Set 'Logging' to 'On', choose a 'Bucket for Logs' and 'Log Prefix' as desired
7. Click on 'Yes, Edit'

# 10. Track and monitor all access to network resources and cardholder data

10.2.3 Access to all audit trails.

## AWS Config Recording is disabled

| | |
|---|---|
| Compliance Section: 10.2.3 | First Seen: N/A |
| Resource(s) Failed: 19 | Resource Type: Other |
| Resource(s) Passed: 11 | |

### Description:

AWS Config is a web service that performs configuration management of supported AWS resources within your account and delivers log files to you. AWS config uses configuration recorder to detect changes in your resource configurations and capture these changes as configuration items. It continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. This policy generates alerts when AWS Config recorder is not enabled.

### Resource(s) Failed:

795462528824:AWS California, 795462528824:AWS Paris, 795462528824:AWS Jakarta, 795462528824:AWS Seoul, 795462528824:AWS Singapore, 795462528824:AWS Osaka, 795462528824:AWS Cape Town, 795462528824:AWS Hong Kong, 795462528824:AWS Tokyo, 795462528824:AWS Canada ...and 9 more

### Recommendations:

1. Sign in to the AWS Management Console
2. Select the specific region from the top down, for which the alert is generated
3. Navigate to service 'Config' from the 'Services' dropdown.

If AWS Config set up exists,

a. Go to Settings
b. Click on 'Turn On' button under 'Recording is Off' section,
c. provide required information for bucket and role with proper permission

If AWS Config set up doesn't exist

a. Click on 'Get Started'
b. For Step 1, Tick the check box for 'Record all resources supported in this region' under section 'Resource types to record'
c. Under section 'Amazon S3 bucket', select bucket with permission to Config services
d. Under section 'AWS Config role', select a role with permission to Config services
e. Click on 'Next'
f. For Step 2, Select required rule and click on 'Next' otherwise click on 'Skip'
g. For Step 3, Review the created 'Settings' and click on 'Confirm'

# 10. Track and monitor all access to network resources and cardholder data

10.6 Review logs and security events for all system components to identify anomalies or suspicious activity.

## AWS Redshift database does not have audit logging enabled

| | |
|---|---|
| Compliance Section: 10.6 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Managed Database |
| Resource(s) Passed: 0 | |

### Description:

Audit logging is not enabled by default in Amazon Redshift. When you enable logging on your cluster, Amazon Redshift creates and uploads logs to Amazon S3 that capture data from the creation of the cluster to the present time.

### Recommendations:

1. Login to AWS Console.
2. Goto Amazon Redshift service
3. On left navigation panel, click on Clusters
4. Click on the reported cluster
5. Click on Database tab and choose 'Configure Audit Logging'
6. On Enable Audit Logging, choose 'Yes'
7. Create a new s3 bucket or use an existing bucket
8. click Save

# 10. Track and monitor all access to network resources and cardholder data

10.6 Review logs and security events for all system components to identify anomalies or suspicious activity.

## AWS EC2 Instance Scheduled Events

| | |
|---|---|
| Compliance Section: 10.6 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 12 | |

### Description:

This policy identifies your Amazon EC2 instances which have a scheduled event. AWS can schedule events for your instances, such as a reboot, stop/start, or retirement. These events do not occur frequently. If one of your instances will be affected by a scheduled event, AWS sends an email to the email address that's associated with your AWS account prior to the scheduled event, with details about the event, including the start and end date. Depending on the event, you might be able to take action to control the timing of the event. If AWS scheduled event is planned for within 7 days, this signature triggers an alert.

### Recommendations:

To remediate this alert, review and follow the steps at AWS: Scheduled Events for Your Instances as needed.
For more info: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/monitoring-instances-status-check_sched.html

# 10. Track and monitor all access to network resources and cardholder data

10.6 Review logs and security events for all system components to identify anomalies or suspicious activity.

## AWS Elasticsearch domain has Index slow logs set to disabled

| | |
|---|---|
| Compliance Section: 10.6 | First Seen: N/A |
| Resource(s) Failed: 1 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies Elasticsearch domains for which Index slow logs is disabled in your AWS account. Enabling support for publishing indexing slow logs to AWS CloudWatch Logs enables you have full insight into the performance of indexing operations performed on your Elasticsearch clusters. This will help you in identifying performance issues caused by specific queries or due to changes in cluster usage, so that you can optimize your index configuration to address the problem.

### Resource(s) Failed:

mybookstore-domain

### Recommendations:

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to Elasticsearch Service Dashboard
4. Choose reported Elasticsearch domain
5. Select the 'Logs' tab
6. In 'Set up Index slow logs' section,

a. click on 'Setup'
b. In 'Select CloudWatch Logs log group' setting, Create/Use existing CloudWatch Logs log group as per your requirement
c. In 'Specify CloudWatch access policy', Create new/Select an existing policy as per your requirement
d. Click on 'Enable'

The Index slow logs setting 'Status' should change now to 'Enabled'.

# 10. Track and monitor all access to network resources and cardholder data

10.6 Review logs and security events for all system components to identify anomalies or suspicious activity.

## AWS Config fails to deliver log files

| | |
|---|---|
| Compliance Section: 10.6 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 5 | |

### Description:

This policy identifies AWS Configs which are failing to deliver its log files to the specified S3 bucket. It happens when it doesn't have sufficient permissions to complete the operation. To deliver information to S3 bucket, AWS Config needs to assume an IAM role that manages the permissions required to access the designated S3 bucket.

### Recommendations:

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to the AWS Config Dashboard
4. Go to 'Settings' (Left Pane)
5. In 'AWS Config role' section, 'Choose a role from your account' option and provide a unique name for new IAM role for the 'Role name' box; which does have permission to access S3 bucket.
6. Click Save

# 10. Track and monitor all access to network resources and cardholder data

10.6 Review logs and security events for all system components to identify anomalies or suspicious activity.

## AWS Config must record all possible resources

| | |
|---|---|
| Compliance Section: 10.6 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Config Service Recorder |
| Resource(s) Passed: 5 | |

### Description:

This policy identifies resources for which AWS Config recording is enabled but recording for all possible resources are disabled. AWS Config provides an inventory of your AWS resources and a history of configuration changes to these resources. You can use AWS Config to define rules that evaluate these configurations for compliance. Hence, it is important to enable this feature.

### Recommendations:

1. Login to the AWS and navigate to the 'Config' service
2. Change to the respective region and in the navigation pane, click on 'Settings'
3. Review the 'All resources' and Check the 2 options (3.a and 3.b)

3.a Record all resources supported in this region

3.b Include global resources (e.g., AWS IAM resources)

# 10. Track and monitor all access to network resources and cardholder data

10.6 Review logs and security events for all system components to identify anomalies or suspicious activity.

## AWS CloudTrail logging is disabled

| | |
|---|---|
| Compliance Section: 10.6 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 3 | |

### Description:

This policy identifies the CloudTrails in which logging is disabled. AWS CloudTrail is a service that enables governance, compliance, operational & risk auditing of the AWS account. It is a compliance and security best practice to turn on logging for CloudTrail across different regions to get a complete audit trail of activities across various services. NOTE: This policy will be triggered only when you have CloudTrail configured in your AWS account and logging is disabled.

### Recommendations:

1. Sign in to AWS Console
2. Navigate to CloudTrail dashboard
3. Click on 'Trails' (Left panel)
4. Click on reported CloudTrail
5. Enable 'Logging' by hovering logging button to 'ON'

OR

If CLoudTrail is not required you can delete by clicking on the delete icon below the logging hover button.

# 10. Track and monitor all access to network resources and cardholder data

10.6 Review logs and security events for all system components to identify anomalies or suspicious activity.

## AWS EKS control plane logging disabled

| | |
|---|---|
| Compliance Section: 10.6 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

Amazon EKS control plane logging provides audit and diagnostic logs directly from the Amazon EKS control plane to CloudWatch Logs in your account. These logs make it easy for you to secure and run your clusters. You can select the exact log types you need, and logs are sent as log streams to a group for each Amazon EKS cluster in CloudWatch. This policy generates an alert if control plane logging is disabled.

### Recommendations:

To enable control plane logs:
1. Login to AWS Console
2. Navigate to the Amazon EKS dashboard
3. Choose the name of the cluster to display your cluster information
4. Under Logging, choose 'Manage logging'
5. For each individual log type, choose Enabled
6. Click on 'Save changes'

# 10. Track and monitor all access to network resources and cardholder data

10.6 Review logs and security events for all system components to identify anomalies or suspicious activity.

## AWS VPC Flow Logs not enabled

| | |
|---|---|
| Compliance Section: 10.6 | First Seen: N/A |
| Resource(s) Failed: 17 | Resource Type: Other |
| Resource(s) Passed: 8 | |

### Description:

This policy identifies VPCs which have flow logs disabled. VPC Flow logs capture information about IP traffic going to and from network interfaces in your VPC. Flow logs are used as a security tool to monitor the traffic that is reaching your instances. Without the flow logs turned on, it is not possible to get any visibility into network traffic.

### Resource(s) Failed:

Jenkins, vpc-60c2d707, vpc-0f271f68, vpc-e045df89, vpc-f085549b, vpc-d9581cb1, vpc-84def2fe, vpc-aabf7ec1, vpc-86fd1eff, vpc-2cd6d14b ...and 7 more

### Recommendations:

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to VPC Dashboard
4. Click on 'Your VPCs' and Choose the reported VPC
5. Click on the 'Flow logs' tab and follow the instructions as in link below to enable Flow Logs for the VPC:
https://aws.amazon.com/blogs/aws/vpc-flow-logs-log-and-view-network-traffic-flows/

# 10. Track and monitor all access to network resources and cardholder data

10.6 Review logs and security events for all system components to identify anomalies or suspicious activity.

## AWS CloudTrail logs should integrate with CloudWatch for all regions

| | |
|---|---|
| Compliance Section: 10.6 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 3 | |

### Description:

This policy identifies the Cloudtrails which is not integrated with cloudwatch for all regions. CloudTrail uses Amazon S3 for log file storage and delivery, so log files are stored durably. In addition to capturing CloudTrail logs within a specified S3 bucket for long term analysis, realtime analysis can be performed by configuring CloudTrail to send logs to CloudWatch Logs. For a trail that is enabled in all regions in an account, CloudTrail sends log files from all those regions to a CloudWatch Logs log group. It is recommended that CloudTrail logs be sent to CloudWatch Logs.

### Recommendations:

1. Sign into AWS and navigate to CloudTrail service.
2. Click on Trail in the left menu navigation and choose the reported cloudtrail.
3. Go to CloudWatch Logs section and click Configure.
4. Define a new or select an existing log group and click Continue to complete the process.

# 10. Track and monitor all access to network resources and cardholder data

10.6 Review logs and security events for all system components to identify anomalies or suspicious activity.

## AWS Certificate Manager (ACM) has certificates with Certificate Transparency Logging disabled

| | |
|---|---|
| Compliance Section: 10.6 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies AWS Certificate Manager certificates in which Certificate Transparency Logging is disabled. AWS Certificate Manager (ACM) is the preferred tool to provision, manage, and deploy your server certificates. Certificate Transparency Logging is used to guard against SSL/TLS certificates that are issued by mistake or by a compromised CA, some browsers require that public certificates issued for your domain can also be recorded. This policy generates alerts for certificates which have transparency logging disabled. As a best practice, it is recommended to enable Transparency logging for all certificates.

### Recommendations:

You cannot currently use the console to opt out of or into transparency logging. It's recommended to use the command line utility to enable transparency logging.
Remediation CLI:
1. Use the below command to list ACM certificate
aws acm list-certificates
2. Note the 'CertificateArn' of the reported ACM certificate
3. Use the below command to ENABLE Certificate Transparency Logging
aws acm update-certificate-options --certificate-arn <certificateARN> --options CertificateTransparencyLoggingPreference=ENABLED
where 'CertificateArn' is captured in the step2

# 10. Track and monitor all access to network resources and cardholder data

10.6 Review logs and security events for all system components to identify anomalies or suspicious activity.

## AWS S3 CloudTrail bucket for which access logging is disabled

| | |
|---|---|
| Compliance Section: 10.6 | First Seen: N/A |
| Resource(s) Failed: 1 | Resource Type: Other |
| Resource(s) Passed: 12 | |

### Description:

This policy identifies S3 CloudTrail buckets for which access is disabled. S3 Bucket access logging generates access records for each request made to your S3 bucket. An access log record contains information such as the request type, the resources specified in the request worked, and the time and date the request was processed. It is recommended that bucket access logging be enabled on the CloudTrail S3 bucket.

### Resource(s) Failed:

aws-cloudtrail-logs-795462528824-317b0c26

### Recommendations:

1. Login to the AWS Console and navigate to the 'S3' service.
2. Click on the the S3 bucket that was reported.
3. Click on the 'Properties' tab.
4. Under the 'Server access logging' section, select 'Enable' option and provide s3 bucket of your choice in the 'Target bucket'
5. Click on 'Save Changes'

# 10. Track and monitor all access to network resources and cardholder data

10.6 Review logs and security events for all system components to identify anomalies or suspicious activity.

## AWS RDS Event subscription All event categories and All instances disabled for DB instance

| | |
|---|---|
| Compliance Section: 10.6 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies AWS RDS event subscriptions for DB instance which has 'All event categories' and 'All instances' is disabled. As a best practice enabling 'All event categories' for 'All instances' helps to get notified when an event occurs for a DB instance.

### Recommendations:

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to Amazon RDS Dashboard
4. Click on 'Event subscriptions' (Left Panel)
5. Choose the reported Event subscription
6. Click on 'Edit'
7. On 'Edit event subscription' page, Under 'Details' section; Select 'Yes' for 'Enabled' and Make sure you have subscribed your DB to 'All instances' and 'All event categories'
8. Click on 'Edit'

# 10. Track and monitor all access to network resources and cardholder data

10.6 Review logs and security events for all system components to identify anomalies or suspicious activity.

## AWS Elasticsearch domain has Search slow logs set to disabled

| | |
|---|---|
| Compliance Section: 10.6 | First Seen: N/A |
| Resource(s) Failed: 1 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies Elasticsearch domains for which Search slow logs is disabled in your AWS account. Enabling support for publishing Search slow logs to AWS CloudWatch Logs enables you to have full insight into the performance of search operations performed on your Elasticsearch clusters. This will help you in identifying performance issues caused by specific search queries so that you can optimize your queries to address the problem.

### Resource(s) Failed:

mybookstore-domain

### Recommendations:

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to Elasticsearch Service Dashboard
4. Choose reported Elasticsearch domain
5. Select the 'Logs' tab
6. In 'Set up Search slow logs' section,

a. click on 'Setup'
b. In 'Select CloudWatch Logs log group' setting, Create/Use existing CloudWatch Logs log group as per your requirement
c. In 'Specify CloudWatch access policy', Create new/Select an existing policy as per your requirement
d. Click on 'Enable'

The search slow logs setting 'Status' should change now to 'Enabled'.

# 10. Track and monitor all access to network resources and cardholder data

10.6 Review logs and security events for all system components to identify anomalies or suspicious activity.

## CloudTrail trail is not integrated with CloudWatch Log

| | |
|---|---|
| Compliance Section: 10.6 | First Seen: N/A |
| Resource(s) Failed: 1 | Resource Type: CloudTrail Setting |
| Resource(s) Passed: 1 | |

### Description:

Enabling the CloudTrail trail logs integrated with CloudWatch Logs will enable the real-time as well as historic activity logging. This will further effective monitoring and alarm capability.

### Resource(s) Failed:

cloud-trail-demo

### Recommendations:

1. Login to the AWS Admin Console and access the CloudTrail service.
2. Click on the Trails in the left hand menu.
3. Click on the identified CloudTrail and navigate to the 'CloudWatch Logs' section.
4. Click on 'Configure' tab and provide required
5. Provide a log group name in field 'New or existing log group'
6. Click on 'Continue'
7. In the next page from 'IAM role' dropdown select an IAM role with required access or select the 'Create a new IAM role'
8. Click on 'Allow'

# 10. Track and monitor all access to network resources and cardholder data

10.6 Review logs and security events for all system components to identify anomalies or suspicious activity.

## AWS Elastic Load Balancer v2 (ELBv2) with access log disabled

| | |
|---|---|
| Compliance Section: 10.6 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies Elastic Load Balancers v2 (ELBv2) which have access log disabled. Access logs capture detailed information about requests sent to your load balancer and each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. You can use these access logs to analyze traffic patterns and troubleshoot issues.

### Recommendations:

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to EC2 dashboard
4. Click on 'Load Balancers' (Left Panel)
5. Select the reported ELB
6. Click on 'Actions' drop-down
7. Click on 'Edit attributes'
8. In the 'Edit load balancer attributes' popup box, Choose 'Enable' for 'Access logs' and configure S3 location where you want to store ELB logs.
9. Click on 'Save'

# 10. Track and monitor all access to network resources and cardholder data

10.6 Review logs and security events for all system components to identify anomalies or suspicious activity.

## AWS Elastic Load Balancer (Classic) with access log disabled

| | |
|---|---|
| Compliance Section: 10.6 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies Classic Elastic Load Balancers which have access log disabled. When Access log enabled, Classic load balancer captures detailed information about requests sent to your load balancer. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. You can use these access logs to analyze traffic patterns and to troubleshoot issues.

### Recommendations:

To enable access logging for Elastic Load Balancer (Classic), follow below mentioned URL:
https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/enable-access-logs.html

# 10. Track and monitor all access to network resources and cardholder data

10.6 Review logs and security events for all system components to identify anomalies or suspicious activity.

## AWS CloudFront distribution with access logging disabled

| | |
|---|---|
| Compliance Section: 10.6 | First Seen: N/A |
| Resource(s) Failed: 2 | Resource Type: Other |
| Resource(s) Passed: 0 | |

### Description:

This policy identifies CloudFront distributions which have access logging disabled. Enabling access log on distributions creates log files that contain detailed information about every user request that CloudFront receives. Access logs are available for web distributions. If you enable logging, you can also specify the Amazon S3 bucket that you want CloudFront to save files in.

### Resource(s) Failed:

d2rwvuyjsg9kf7.cloudfront.net, d2u45drmoykiua.cloudfront.net

### Recommendations:

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to CloudFront Distributions Dashboard
4. Click on the reported distribution
5. On 'General' tab, Click on 'Edit' button
6. On 'Edit Distribution' page, Set 'Logging' to 'On', choose a 'Bucket for Logs' and 'Log Prefix' as desired
7. Click on 'Yes, Edit'

# 10. Track and monitor all access to network resources and cardholder data

10.6 Review logs and security events for all system components to identify anomalies or suspicious activity.

## AWS Config Recording is disabled

| | |
|---|---|
| Compliance Section: 10.6 | First Seen: N/A |
| Resource(s) Failed: 19 | Resource Type: Other |
| Resource(s) Passed: 11 | |

### Description:

AWS Config is a web service that performs configuration management of supported AWS resources within your account and delivers log files to you. AWS config uses configuration recorder to detect changes in your resource configurations and capture these changes as configuration items. It continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. This policy generates alerts when AWS Config recorder is not enabled.

### Resource(s) Failed:

795462528824:AWS California, 795462528824:AWS Paris, 795462528824:AWS Jakarta, 795462528824:AWS Seoul, 795462528824:AWS Singapore, 795462528824:AWS Osaka, 795462528824:AWS Cape Town, 795462528824:AWS Hong Kong, 795462528824:AWS Tokyo, 795462528824:AWS Canada ...and 9 more

### Recommendations:

1. Sign in to the AWS Management Console
2. Select the specific region from the top down, for which the alert is generated
3. Navigate to service 'Config' from the 'Services' dropdown.

If AWS Config set up exists,

a. Go to Settings
b. Click on 'Turn On' button under 'Recording is Off' section,
c. provide required information for bucket and role with proper permission

If AWS Config set up doesn't exist

a. Click on 'Get Started'
b. For Step 1, Tick the check box for 'Record all resources supported in this region' under section 'Resource types to record'
c. Under section 'Amazon S3 bucket', select bucket with permission to Config services
d. Under section 'AWS Config role', select a role with permission to Config services
e. Click on 'Next'
f. For Step 2, Select required rule and click on 'Next' otherwise click on 'Skip'
g. For Step 3, Review the created 'Settings' and click on 'Confirm'

# A3. Designated Entities Supplemental Validation (DESV)

A3.3.1 Implement a process to immediately detect and alert on critical security control failures. Examples of critical security controls include, but are not limited to Firewalls, IDS/IPS, FIM, Anti-virus, Physical access controls, Logical access controls, Audit logging mechanisms, Segmentation controls (if used).

## AWS EC2 Instance Scheduled Events

| | |
|---|---|
| Compliance Section: A3.3.1 | First Seen: N/A |
| Resource(s) Failed: 0 | Resource Type: Other |
| Resource(s) Passed: 12 | |

### Description:

This policy identifies your Amazon EC2 instances which have a scheduled event. AWS can schedule events for your instances, such as a reboot, stop/start, or retirement. These events do not occur frequently. If one of your instances will be affected by a scheduled event, AWS sends an email to the email address that's associated with your AWS account prior to the scheduled event, with details about the event, including the start and end date. Depending on the event, you might be able to take action to control the timing of the event. If AWS scheduled event is planned for within 7 days, this signature triggers an alert.

### Recommendations:

To remediate this alert, review and follow the steps at AWS: Scheduled Events for Your Instances as needed.
For more info: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/monitoring-instances-status-check_sched.html

# A3. Designated Entities Supplemental Validation (DESV)

A3.3.1 Implement a process to immediately detect and alert on critical security control failures. Examples of critical security controls include, but are not limited to Firewalls, IDS/IPS, FIM, Anti-virus, Physical access controls, Logical access controls, Audit logging mechanisms, Segmentation controls (if used).

## AWS Log metric filter and alarm does not exist for Network gateways changes

| | |
|---|---|
| Compliance Section: A3.3.1 | First Seen: N/A |
| Resource(s) Failed: 1 | Resource Type: Other |
| Resource(s) Passed: 21 | |

### Description:

This policy identifies the AWS regions which do not have a log metric filter and alarm for Network gateways changes. Monitoring changes to network gateways will help ensure that all ingress/egress traffic traverses the VPC border via a controlled path. It is recommended that a metric filter and alarm be established for changes to network gateways. NOTE: This policy will trigger alert if you have at least one Cloudtrail with the multi trial is enabled, Logs all management events in your account and is not set with specific log metric filter and alarm.

### Resource(s) Failed:

795462528824

### Recommendations:

1. Sign in to AWS Console
2. Navigate to CloudWatch dashboard
3. Click on 'Log groups' in the 'Logs' section (Left panel)
4. Select the log group created for your CloudTrail trail event logs (CloudTrail should be multi trail enabled with all management events captured) and click 'Create Metric Filter' button.
5. In 'Define Logs Metric Filter' page, add 'Filter pattern' value as
{ ($.eventName = CreateCustomerGateway) || ($.eventName = DeleteCustomerGateway) || ($.eventName = AttachInternetGateway) || ($.eventName = CreateInternetGateway) || ($.eventName = DeleteInternetGateway) || ($.eventName = DetachInternetGateway) }
and Click on 'Assign Metric'
6. In 'Create Metric Filter and Assign a Metric' page, Choose Filter Name, Metric Details parameter according to your requirement and click on 'Create Filter'
7. Click on 'Create Alarm',
- In Step 1 specify metric details and conditions details as required and click on 'Next'
- In Step 2 Select an SNS topic either by creating a new topic or use existing SNS topic/ARN and click on 'Next'
- In Step 3 Select name and description to alarm and click on 'Next'
- In Step 4 Preview your data entered and click on 'Create Alarm'

# A3. Designated Entities Supplemental Validation (DESV)

A3.3.1 Implement a process to immediately detect and alert on critical security control failures. Examples of critical security controls include, but are not limited to Firewalls, IDS/IPS, FIM, Anti-virus, Physical access controls, Logical access controls, Audit logging mechanisms, Segmentation controls (if used).

## AWS Log metric filter and alarm does not exist for AWS management console authentication failures

| | |
|---|---|
| Compliance Section: A3.3.1 | First Seen: N/A |
| Resource(s) Failed: 1 | Resource Type: Other |
| Resource(s) Passed: 21 | |

### Description:

This policy identifies the AWS accounts which do not have a log metric filter and alarm for AWS management console authentication failures. Monitoring failed console logins may decrease lead time to detect an attempt to brute force a credential, which may provide an indicator, such as source IP, that can be used in other event correlation. It is recommended that a metric filter and alarm be established for failed console authentication attempts. NOTE: This policy will trigger alert if you have at least one Cloudtrail with the multi trial is enabled, Logs all management events and is not set with specific log metric filter and alarm in your account.

### Resource(s) Failed:

795462528824

### Recommendations:

1. Sign in to AWS Console
2. Navigate to CloudWatch dashboard
3. Click on 'Log groups' in the 'Logs' section (Left panel)
4. Select the log group created for your CloudTrail trail event logs (Cloudtrail should be multi trail enabled with all Management Events captured) and click 'Create Metric Filter' button.
5. In 'Define Logs Metric Filter' page, add 'Filter pattern' value as
{ ($.eventName = ConsoleLogin) && ($.errorMessage = "Failed authentication") }
and Click on 'Assign Metric'
6. In 'Create Metric Filter and Assign a Metric' page, Choose Filter Name, Metric Details parameter according to your requirement and click on 'Create Filter'
7. Click on 'Create Alarm',
- In Step 1, specify metric details and conditions details as required and click on 'Next'
- In Step 2, Select an SNS topic either by creating a new topic or use existing SNS topic/ARN and click on 'Next'
- In Step 3, Select name and description to alarm and click on 'Next'
- In Step 4, Preview your data entered and click on 'Create Alarm'

# A3. Designated Entities Supplemental Validation (DESV)

A3.3.1 Implement a process to immediately detect and alert on critical security control failures. Examples of critical security controls include, but are not limited to Firewalls, IDS/IPS, FIM, Anti-virus, Physical access controls, Logical access controls, Audit logging mechanisms, Segmentation controls (if used).

## AWS Log metric filter and alarm does not exist for CloudTrail configuration changes

| | |
|---|---|
| Compliance Section: A3.3.1 | First Seen: N/A |
| Resource(s) Failed: 1 | Resource Type: Other |
| Resource(s) Passed: 21 | |

### Description:

This policy identifies the AWS regions which do not have a log metric filter and alarm for CloudTrail configuration changes. Monitoring changes to CloudTrail's configuration will help ensure sustained visibility to activities performed in the AWS account. It is recommended that a metric filter and alarm be established for detecting changes to CloudTrail's configurations. NOTE: This policy will trigger alert if you have at least one Cloudtrail with the multi trial is enabled, Logs all management events in your account and is not set with specific log metric filter and alarm.

### Resource(s) Failed:

795462528824

### Recommendations:

1. Sign in to AWS Console
2. Navigate to CloudWatch dashboard
3. Click on 'Log groups' in the 'Logs' section (Left panel)
4. Select the log group created for your CloudTrail trail event logs (CloudTrail should be multi trail enabled with all management events captured) and click 'Create Metric Filter' button.
5. In 'Define Logs Metric Filter' page, add 'Filter pattern' value as
{ ($.eventName = CreateTrail) || ($.eventName = UpdateTrail) || ($.eventName = DeleteTrail) || ($.eventName = StartLogging) || ($.eventName = StopLogging) }
and Click on 'Assign Metric'
6. In 'Create Metric Filter and Assign a Metric' page, Choose Filter Name, Metric Details parameter according to your requirement and click on 'Create Filter'
7. Click on 'Create Alarm',
- In Step 1 specify metric details and conditions details as required and click on 'Next'
- In Step 2 Select an SNS topic either by creating a new topic or use existing SNS topic/ARN and click on 'Next'
- In Step 3 Select name and description to alarm and click on 'Next'
- In Step 4 Preview your data entered and click on 'Create Alarm'

# A3. Designated Entities Supplemental Validation (DESV)

A3.3.1 Implement a process to immediately detect and alert on critical security control failures. Examples of critical security controls include, but are not limited to Firewalls, IDS/IPS, FIM, Anti-virus, Physical access controls, Logical access controls, Audit logging mechanisms, Segmentation controls (if used).

## AWS Log metric filter and alarm does not exist for S3 bucket policy changes

| | |
|---|---|
| Compliance Section: A3.3.1 | First Seen: N/A |
| Resource(s) Failed: 1 | Resource Type: Other |
| Resource(s) Passed: 21 | |

### Description:

This policy identifies the AWS regions which do not have a log metric filter and alarm for S3 bucket policy changes. Monitoring changes to S3 bucket policies may reduce time to detect and correct permissive policies on sensitive S3 buckets. It is recommended that a metric filter and alarm be established for changes to S3 bucket policies. NOTE: This policy will trigger alert if you have at least one Cloudtrail with the multi trial is enabled, Logs all management events in your account and is not set with specific log metric filter and alarm.

### Resource(s) Failed:

795462528824

### Recommendations:

1. Sign in to AWS Console
2. Navigate to CloudWatch dashboard
3. Click on 'Log groups' in the 'Logs' section (Left panel)
4. Select the log group created for your CloudTrail trail event logs (CloudTrail should be multi trail enabled with all management events captured) and click 'Create Metric Filter' button.
5. In 'Define Logs Metric Filter' page, add 'Filter pattern' value as
{ ($.eventSource = s3.amazonaws.com) && (($.eventName = PutBucketAcl) || ($.eventName = PutBucketPolicy) || ($.eventName = PutBucketCors) || ($.eventName = PutBucketLifecycle) || ($.eventName = PutBucketReplication) || ($.eventName = DeleteBucketPolicy) || ($.eventName = DeleteBucketCors) || ($.eventName = DeleteBucketLifecycle) || ($.eventName = DeleteBucketReplication)) }
and Click on 'Assign Metric'
6. In 'Create Metric Filter and Assign a Metric' page, Choose Filter Name, Metric Details parameter according to your requirement and click on 'Create Filter'
7. Click on 'Create Alarm',
- In Step 1 specify metric details and conditions details as required and click on 'Next'
- In Step 2 Select an SNS topic either by creating a new topic or use existing SNS topic/ARN and click on 'Next'
- In Step 3 Select name and description to alarm and click on 'Next'
- In Step 4 Preview your data entered and click on 'Create Alarm'

# A3. Designated Entities Supplemental Validation (DESV)

A3.3.1 Implement a process to immediately detect and alert on critical security control failures. Examples of critical security controls include, but are not limited to Firewalls, IDS/IPS, FIM, Anti-virus, Physical access controls, Logical access controls, Audit logging mechanisms, Segmentation controls (if used).

## AWS Log metric filter and alarm does not exist for Network Access Control Lists (NACL) changes

| | |
|---|---|
| Compliance Section: A3.3.1 | First Seen: N/A |
| Resource(s) Failed: 1 | Resource Type: Other |
| Resource(s) Passed: 21 | |

### Description:

This policy identifies the AWS regions which do not have a log metric filter and alarm for Network Access Control Lists (NACL) changes. Monitoring changes to NACLs will help ensure that AWS resources and services are not unintentionally exposed. It is recommended that a metric filter and alarm be established for changes made to NACLs. NOTE: This policy will trigger alert if you have at least one Cloudtrail with the multi trial is enabled, Logs all management events in your account and is not set with specific log metric filter and alarm.

### Resource(s) Failed:

795462528824

### Recommendations:

1. Sign in to AWS Console
2. Navigate to CloudWatch dashboard
3. Click on 'Log groups' in the 'Logs' section (Left panel)
4. Select the log group created for your CloudTrail trail event logs (CloudTrail should be multi trail enabled with all management events captured) and click 'Create Metric Filter' button.
5. In 'Define Logs Metric Filter' page, add 'Filter pattern' value as
{ ($.eventName = CreateNetworkAcl) || ($.eventName = CreateNetworkAclEntry) || ($.eventName = DeleteNetworkAcl) || ($.eventName = DeleteNetworkAclEntry) || ($.eventName = ReplaceNetworkAclEntry) || ($.eventName = ReplaceNetworkAclAssociation) }
and Click on 'Assign Metric'
6. In 'Create Metric Filter and Assign a Metric' page, Choose Filter Name, Metric Details parameter according to your requirement and click on 'Create Filter'
7. Click on 'Create Alarm',
- In Step 1 specify metric details and conditions details as required and click on 'Next'
- In Step 2 Select an SNS topic either by creating a new topic or use existing SNS topic/ARN and click on 'Next'
- In Step 3 Select name and description to alarm and click on 'Next'
- In Step 4 Preview your data entered and click on 'Create Alarm'

# A3. Designated Entities Supplemental Validation (DESV)

A3.3.1 Implement a process to immediately detect and alert on critical security control failures. Examples of critical security controls include, but are not limited to Firewalls, IDS/IPS, FIM, Anti-virus, Physical access controls, Logical access controls, Audit logging mechanisms, Segmentation controls (if used).

## AWS Log metric filter and alarm does not exist for VPC changes

| | |
|---|---|
| Compliance Section: A3.3.1 | First Seen: N/A |
| Resource(s) Failed: 1 | Resource Type: Other |
| Resource(s) Passed: 21 | |

### Description:

This policy identifies the AWS regions which do not have a log metric filter and alarm for VPC changes. Monitoring changes to VPC will help ensure that resources and services are not unintentionally exposed. It is recommended that a metric filter and alarm be established for changes made to VPCs. NOTE: This policy will trigger alert if you have at least one Cloudtrail with the multi trial is enabled, Logs all management events in your account and is not set with specific log metric filter and alarm.

### Resource(s) Failed:

795462528824

### Recommendations:

1. Sign in to AWS Console
2. Navigate to CloudWatch dashboard
3. Click on 'Log groups' in the 'Logs' section (Left panel)
4. Select the log group created for your CloudTrail trail event logs (CloudTrail should be multi trail enabled with all management events captured) and click 'Create Metric Filter' button.
5. In 'Define Logs Metric Filter' page, add 'Filter pattern' value as
{ ($.eventName = CreateVpc) || ($.eventName = DeleteVpc) || ($.eventName = ModifyVpcAttribute) || ($.eventName = AcceptVpcPeeringConnection) || ($.eventName = CreateVpcPeeringConnection) || ($.eventName = DeleteVpcPeeringConnection) || ($.eventName = RejectVpcPeeringConnection) || ($.eventName = AttachClassicLinkVpc) || ($.eventName = DetachClassicLinkVpc) || ($.eventName = DisableVpcClassicLink) || ($.eventName = EnableVpcClassicLink) }
and Click on 'Assign Metric'
6. In 'Create Metric Filter and Assign a Metric' page, Choose Filter Name, Metric Details parameter according to your requirement and click on 'Create Filter'
7. Click on 'Create Alarm',
- In Step 1 specify metric details and conditions details as required and click on 'Next'
- In Step 2 Select an SNS topic either by creating a new topic or use existing SNS topic/ARN and click on 'Next'
- In Step 3 Select name and description to alarm and click on 'Next'
- In Step 4 Preview your data entered and click on 'Create Alarm'

# A3. Designated Entities Supplemental Validation (DESV)

A3.3.1 Implement a process to immediately detect and alert on critical security control failures. Examples of critical security controls include, but are not limited to Firewalls, IDS/IPS, FIM, Anti-virus, Physical access controls, Logical access controls, Audit logging mechanisms, Segmentation controls (if used).

## AWS Log metric filter and alarm does not exist for Route table changes

| | |
|---|---|
| Compliance Section: A3.3.1 | First Seen: N/A |
| Resource(s) Failed: 1 | Resource Type: Other |
| Resource(s) Passed: 21 | |

### Description:

This policy identifies the AWS regions which do not have a log metric filter and alarm for Route table changes. Monitoring changes to route tables will help ensure that all VPC traffic flows through an expected path. It is recommended that a metric filter and alarm be established for changes to route tables. NOTE: This policy will trigger alert if you have at least one Cloudtrail with the multi trial is enabled, Logs all management events in your account and is not set with specific log metric filter and alarm.

### Resource(s) Failed:

795462528824

### Recommendations:

1. Sign in to AWS Console
2. Navigate to CloudWatch dashboard
3. Click on 'Log groups' in the 'Logs' section (Left panel)
4. Select the log group created for your CloudTrail trail event logs (CloudTrail should be multi trail enabled with all management events captured) and click 'Create Metric Filter' button.
5. In 'Define Logs Metric Filter' page, add 'Filter pattern' value as
{ ($.eventName = CreateRoute) || ($.eventName = CreateRouteTable) || ($.eventName = ReplaceRoute) || ($.eventName = ReplaceRouteTableAssociation) || ($.eventName = DeleteRouteTable) || ($.eventName = DeleteRoute) || ($.eventName = DisassociateRouteTable) }
and Click on 'Assign Metric'
6. In 'Create Metric Filter and Assign a Metric' page, Choose Filter Name, Metric Details parameter according to your requirement and click on 'Create Filter'
7. Click on 'Create Alarm',
- In Step 1 specify metric details and conditions details as required and click on 'Next'
- In Step 2 Select an SNS topic either by creating a new topic or use existing SNS topic/ARN and click on 'Next'
- In Step 3 Select name and description to alarm and click on 'Next'
- In Step 4 Preview your data entered and click on 'Create Alarm'

# A3. Designated Entities Supplemental Validation (DESV)

A3.3.1 Implement a process to immediately detect and alert on critical security control failures. Examples of critical security controls include, but are not limited to Firewalls, IDS/IPS, FIM, Anti-virus, Physical access controls, Logical access controls, Audit logging mechanisms, Segmentation controls (if used).

## AWS Log metric filter and alarm does not exist for unauthorized API calls

| | |
|---|---|
| Compliance Section: A3.3.1 | First Seen: N/A |
| Resource(s) Failed: 1 | Resource Type: Other |
| Resource(s) Passed: 21 | |

### Description:

This policy identifies the AWS regions which do not have a log metric filter and alarm for unauthorized API calls. Monitoring unauthorized API calls will help reveal application errors and may reduce the time to detect malicious activity. It is recommended that a metric filter and alarm be established for unauthorized API calls. NOTE: This policy will trigger alert if you have at least one Cloudtrail with the multi trial is enabled, Logs all management events in your account and is not set with specific log metric filter and alarm.

### Resource(s) Failed:

795462528824

### Recommendations:

1. Sign in to AWS Console
2. Navigate to CloudWatch dashboard
3. Click on 'Log groups' in the 'Logs' section (Left panel)
4. Select the log group created for your CloudTrail trail event logs (CloudTrail should be multi trail enabled with all management events captured) and click 'Create Metric Filter' button.
5. In 'Define Logs Metric Filter' page, add 'Filter pattern' value as
{ ($.errorCode = "*UnauthorizedOperation") || ($.errorCode = "AccessDenied*") }
and Click on 'Assign Metric'
6. In 'Create Metric Filter and Assign a Metric' page, Choose Filter Name, Metric Details parameter according to your requirement and click on 'Create Filter'
7. Click on 'Create Alarm',
- In Step 1 specify metric details and conditions details as required and click on 'Next'
- In Step 2 Select an SNS topic either by creating a new topic or use existing SNS topic/ARN and click on 'Next'
- In Step 3 Select name and description to alarm and click on 'Next'
- In Step 4 Preview your data entered and click on 'Create Alarm'

# A3. Designated Entities Supplemental Validation (DESV)

A3.3.1 Implement a process to immediately detect and alert on critical security control failures. Examples of critical security controls include, but are not limited to Firewalls, IDS/IPS, FIM, Anti-virus, Physical access controls, Logical access controls, Audit logging mechanisms, Segmentation controls (if used).

## AWS Log metric filter and alarm does not exist for disabling or scheduled deletion of customer created CMKs

| | |
|---|---|
| Compliance Section: A3.3.1 | First Seen: N/A |
| Resource(s) Failed: 1 | Resource Type: Other |
| Resource(s) Passed: 21 | |

### Description:

This policy identifies the AWS regions which do not have a log metric filter and alarm for disabling or scheduled deletion of customer created CMKs. Data encrypted with disabled or deleted keys will no longer be accessible. It is recommended that a metric filter and alarm be established for customer created CMKs which have changed state to disabled or scheduled deletion. NOTE: This policy will trigger alert if you have at least one Cloudtrail with the multi trial is enabled, Logs all management events in your account and is not set with specific log metric filter and alarm.

### Resource(s) Failed:

795462528824

### Recommendations:

1. Sign in to AWS Console
2. Navigate to CloudWatch dashboard
3. Click on 'Log groups' in the 'Logs' section (Left panel)
4. Select the log group created for your CloudTrail trail event logs (CloudTrail should be multi trail enabled with all management events captured) and click 'Create Metric Filter' button.
5. In 'Define Logs Metric Filter' page, add 'Filter pattern' value as
{ ($.eventSource = kms.amazonaws.com) && (($.eventName=DisableKey)||($.eventName=ScheduleKeyDeletion)) }
and Click on 'Assign Metric'
6. In 'Create Metric Filter and Assign a Metric' page, Choose Filter Name, Metric Details parameter according to your requirement and click on 'Create Filter'
7. Click on 'Create Alarm',
- In Step 1 specify metric details and conditions details as required and click on 'Next'
- In Step 2 Select an SNS topic either by creating a new topic or use existing SNS topic/ARN and click on 'Next'
- In Step 3 Select name and description to alarm and click on 'Next'
- In Step 4 Preview your data entered and click on 'Create Alarm'

# A3. Designated Entities Supplemental Validation (DESV)

A3.3.1 Implement a process to immediately detect and alert on critical security control failures. Examples of critical security controls include, but are not limited to Firewalls, IDS/IPS, FIM, Anti-virus, Physical access controls, Logical access controls, Audit logging mechanisms, Segmentation controls (if used).

## AWS Log metric filter and alarm does not exist for IAM policy changes

| | |
|---|---|
| Compliance Section: A3.3.1 | First Seen: N/A |
| Resource(s) Failed: 1 | Resource Type: Other |
| Resource(s) Passed: 21 | |

### Description:

This policy identifies the AWS regions which do not have a log metric filter and alarm for IAM policy changes. Monitoring changes to IAM policies will help ensure authentication and authorization controls remain intact. It is recommended that a metric filter and alarm be established changes made to Identity and Access Management (IAM) policies. NOTE: This policy will trigger alert if you have at least one Cloudtrail with the multi trial is enabled, Logs all management events in your account and is not set with specific log metric filter and alarm.

### Resource(s) Failed:

795462528824

### Recommendations:

1. Sign in to AWS Console
2. Navigate to CloudWatch dashboard
3. Click on 'Log groups' in the 'Logs' section (Left panel)
4. Select the log group created for your CloudTrail trail event logs (CloudTrail should be multi trail enabled with all management events captured) and click 'Create Metric Filter' button.
5. In 'Define Logs Metric Filter' page, add 'Filter pattern' value as
{ ($.eventName=DeleteGroupPolicy)||($.eventName=DeleteRolePolicy)||($.eventName=DeleteUserPolicy)||($.eventName=PutGroupPolicy)||($.eventName=PutRolePolicy)||($.eventName=PutUserPolicy)||($.eventName=CreatePolicy)||($.eventName=DeletePolicy)||($.eventName=CreatePolicyVersion)||($.eventName=DeletePolicyVersion)||($.eventName=AttachRolePolicy)||($.eventName=DetachRolePolicy)||($.eventName=AttachUserPolicy)||($.eventName=DetachUserPolicy)||($.eventName=AttachGroupPolicy)||($.eventName=DetachGroupPolicy) }
and Click on 'Assign Metric'
6. In 'Create Metric Filter and Assign a Metric' page, Choose Filter Name, Metric Details parameter according to your requirement and click on 'Create Filter'
7. Click on 'Create Alarm',
- In Step 1 specify metric details and conditions details as required and click on 'Next'
- In Step 2 Select an SNS topic either by creating a new topic or use existing SNS topic/ARN and click on 'Next'
- In Step 3 Select name and description to alarm and click on 'Next'
- In Step 4 Preview your data entered and click on 'Create Alarm'

# A3. Designated Entities Supplemental Validation (DESV)

A3.3.1 Implement a process to immediately detect and alert on critical security control failures. Examples of critical security controls include, but are not limited to Firewalls, IDS/IPS, FIM, Anti-virus, Physical access controls, Logical access controls, Audit logging mechanisms, Segmentation controls (if used).

## AWS Log metric filter and alarm does not exist for AWS Config configuration changes

| | |
|---|---|
| Compliance Section: A3.3.1 | First Seen: N/A |
| Resource(s) Failed: 1 | Resource Type: Other |
| Resource(s) Passed: 21 | |

### Description:

This policy identifies the AWS regions which do not have a log metric filter and alarm for AWS Config configuration changes. Monitoring changes to AWS Config configuration will help ensure sustained visibility of configuration items within the AWS account. It is recommended that a metric filter and alarm be established for detecting changes to AWS Config's configurations. NOTE: This policy will trigger alert if you have at least one Cloudtrail with the multi trial is enabled, Logs all management events in your account and is not set with specific log metric filter and alarm.

### Resource(s) Failed:

795462528824

### Recommendations:

1. Sign in to AWS Console
2. Navigate to CloudWatch dashboard
3. Click on 'Log groups' in the 'Logs' section (Left panel)
4. Select the log group created for your CloudTrail trail event logs (CloudTrail should be multi trail enabled with all management events captured) and click 'Create Metric Filter' button.
5. In 'Define Logs Metric Filter' page, add 'Filter pattern' value as
{ ($.eventSource = config.amazonaws.com) && (($.eventName=StopConfigurationRecorder)||($.eventName=DeleteDeliveryChannel)||($.eventName=PutDeliveryChannel)||($.eventName=PutConfigurationRecorder)) }
and Click on 'Assign Metric'
6. In 'Create Metric Filter and Assign a Metric' page, Choose Filter Name, Metric Details parameter according to your requirement and click on 'Create Filter'
7. Click on 'Create Alarm',
- In Step 1 specify metric details and conditions details as required and click on 'Next'
- In Step 2 Select an SNS topic either by creating a new topic or use existing SNS topic/ARN and click on 'Next'
- In Step 3 Select name and description to alarm and click on 'Next'
- In Step 4 Preview your data entered and click on 'Create Alarm'