Networkology

AWS NIST SP 800-53
Detailed Report

Compliance Report

Created For:
Acme Corporation

Created On:
Aug 24, 2020 at 05:36 AM

Cloud Account:
c3m-aws-prod

Powered by C3M

About Report

Disclaimer

The report generated for the compliance assessment is indicative and based on the assessment period, mapped controls, and does not in any way indicate complete compliance with a specific standard or regulation. C3M does not certify your compliance against any particular standard since all of them involve some level of MANUAL checks which must be completed outside of our system.

Table of contents

Brief Summary

Current Score
70%

Policies

Total Policies	Passed Policies	Failed Policies
180	126	54

Critical	8
High	36
Medium	9
Low	1

Resources

Total Resources	Passed Resources	Failed Resources
103	23	80

Controls Summary

Control	Compliance
AC-1 Access Control Policy and Procedures	8/17
AC-2 Account Management	14/32
AC-3 Access Enforcement	23/31
AC-4 Information Flow Enforcement	65/74
AC-5 Separation of duties	1/1
AC-6 Least Privilege	9/21
AC-17 Remote Access	11/12
AU-2 Audit Events	6/7
AU-3 Content of Audit Records	5/6
AU-5 Response to Audit Processing Failures	0/1
AU-7 Audit Reduction and Report Generation	1/1
AU-8 Time Stamps	1/1
AU-9 Protection of Audit Information	2/3
AU-10 Non-Repudiation	5/6

Controls Summary

Control	Compliance
AU-12 Audit Generation	5/6
CM-5 Access Restrictions For Change	6/18
CM-6 Configuration Settings	2/13
CM-7 Least Functionality	64/72
CP-7 Alternate Processing Site	1/1
IA-2 Identification and Authentication	0/3
IA-5 Authenticator Management	3/9
SC-7 Boundary Protection	83/95
SC-8 Transmission Confidentiality and Integrity	5/5
SC-12 Cryptographic Key Establishment and Management	5/5
SC-13 Cryptographic Protection	12/18
SC-23 Session Authenticity	5/5
SC-28 Protection of Information at Rest	9/15

Evaluation Summary

AC-1 Access Control Policy and Procedures 8/17

Policy Name	Compliance	Passed	Failed
Ensure credentials unused for 90 days or greater are disabled	✗	1	6
Ensure IAM user access keys are rotated within 90 days or less	✗	2	5
Do not set up access keys during initial user setup for all IAM users that have a console password	✓	7	0
Ensure IAM user is not directly attached to policies	✗	2	5
Avoid the use of the "root" account	✓	1	0
Ensure IAM group always have at least one or more users	✓	2	0
Ensure MFA is enabled for the "root" account	✗	0	1
Ensure IAM roles allowing cross-account access are configured with either external-ID or MFA	✗	11	2
Ensure IAM password policy prevents password reuse	✓	1	0
IAM users with Administrative Access	✗	2	5
Ensure no IAM group exists without any permissions	✓	2	0
Ensure IAM policies that allow full "*:*" administrative privileges are not created	✓	6	0
Ensure no IAM user exists without any permissions	✓	7	0

Evaluation Summary

AC-1 Access Control Policy and Procedures 8/17

Policy Name	Compliance	Passed	Failed
Ensure IAM user with console access should have MFA enabled	✗	4	3
IAM user with more than one active access keys	✗	5	2
Ensure no root account access key exists	✓	1	0
Ensure IAM password policy is enabled	✗	0	1

Evaluation Summary

AC-2 Account Management 14/32

Policy Name	Compliance	Passed	Failed
Ensure a log metric filter and alarm exist for changes to network gateways	✗	0	1
Ensure SNS topics do not grant wildcard (*) access	✗	0	2
Ensure a log metric filter and alarm exist for route table changes	✗	0	1
Ensure a log metric filter and alarm exist for changes to Network Access Control Lists (NACL)	✗	0	1
Ensure S3 buckets enable server access logging	✗	0	1
Ensure Lambda functions are not granted Admin access	✓	0	0
Ensure a log metric filter and alarm exist for security group changes	✗	0	1
Ensure a log metric filter and alarm exist for unauthorized API calls	✗	0	1
Ensure IAM user is not directly attached to policies	✗	2	5
Ensure Redshift clusters enable audit logging	✓	0	0
Ensure Lambda functions enable active tracing	✓	0	0
Ensure IAM group always have at least one or more users	✓	2	0
Ensure no IAM group exists without any permissions	✓	2	0

Evaluation Summary

AC-2 Account Management 14/32

Policy Name	Compliance	Passed	Failed
IAM users with Administrative Access	✗	2	5
Ensure a log metric filter and alarm exist for Management Console sign-in without MFA	✗	0	1
Ensure a log metric filter and alarm exist for usage of "root" account	✗	0	1
Ensure EKS Cluster enables Logging	✓	0	0
Ensure CloudTrail log file validation is enabled	✓	1	0
Ensure a log metric filter and alarm exist for disabling or scheduled deletion of customer created CMKs	✗	0	1
Ensure no IAM user exists without any permissions	✓	7	0
Ensure a log metric filter and alarm exist for IAM policy changes	✗	0	1
Ensure to enable Cloudwatch Container Insights	✓	0	0
Ensure a log metric filter and alarm exist for AWS Management Console authentication failures	✗	0	1
Ensure CloudTrail is enabled in all regions	✓	1	0
Ensure a log metric filter and alarm exist for VPC changes	✗	0	1
Ensure IAM policies that allow full "*:*" administrative privileges are not created	✓	6	0

Evaluation Summary

AC-2 Account Management 14/32

Policy Name	Compliance	Passed	Failed
Ensure Elasticsearch domains do not grant wildcard (*) access	✓	0	0
Ensure a log metric filter and alarm exist for CloudTrail configuration changes	✗	0	1
Ensure no root account access key exists	✓	1	0
Ensure Elasticsearch domains are configured with VPC access	✓	0	0
Ensure a log metric filter and alarm exist for S3 bucket policy changes	✗	0	1
Ensure a log metric filter and alarm exist for AWS Config configuration changes	✗	0	1

Evaluation Summary

AC-3 Access Enforcement 23/31

Policy Name	Compliance	Passed	Failed
Ensure ECR repositories are not exposed to Public	✓	0	0
Ensure S3 Bucket ACLs do not grant public WRITE_ACP access to all Authenticated Users	✓	1	0
Ensure no RDS instance allows traffic from 0.0.0.0/0	✓	0	0
Ensure Lambda functions are not granted Admin access	✓	0	0
Ensure S3 Bucket ACLs do not grant public WRITE access	✓	1	0
Ensure S3 bucket Public access setting "Block new public ACLs and uploading public objects" is enabled at an account level	✗	0	1
Ensure no EBS Snapshot is Publicly accessible	✓	1	0
Ensure S3 Bucket ACLs do not grant public WRITE_ACP access	✓	1	0
Ensure S3 Bucket ACLs do not grant public READ_ACP access to all Authenticated Users	✓	1	0
Ensure S3 Bucket Policies do not allow any action from all principals	✓	1	0
Ensure AMIs are not Publicly Accessible	✓	0	0
Ensure IAM user is not directly attached to policies	✗	2	5
Ensure S3 bucket Public access setting "Block new public bucket policies" is enabled at an account level	✗	0	1

Evaluation Summary

AC-3 Access Enforcement 23/31

Policy Name	Compliance	Passed	Failed
Ensure S3 bucket Public access setting "Remove public access granted through public ACLs" is enabled at an account level	✗	0	1
Ensure Redshift clusters are not publicly accessible	✓	0	0
Ensure SNS topics do not grant wildcard (*) access	✗	0	2
Ensure SNS topics do not allow everyone to Subscribe	✗	0	2
Ensure S3 bucket ACLs do not grant public FULL_CONTROL access	✓	1	0
Ensure S3 bucket Public access setting "Block public and cross-account access to buckets that have public policies" is enabled at an account level	✗	0	1
Ensure SQS queues not exposed to Everyone	✓	0	0
Ensure S3 Bucket ACLs do not grant public READ access	✓	1	0
Ensure S3 Bucket ACLs do not grant public READ access to all Authenticated Users	✓	1	0
Ensure S3 Bucket ACLs do not grant public FULL_CONTROL access to all Authenticated Users	✓	1	0
Ensure S3 Bucket Policies do not grant public access on all actions	✓	1	0
Ensure S3 Bucket ACLs do not grant public READ_ACP access	✓	1	0
Ensure S3 Bucket ACLs do not grant public WRITE access to all Authenticated Users	✓	1	0

Evaluation Summary

AC-3 Access Enforcement 23/31

Policy Name	Compliance	Passed	Failed
Ensure SNS topics do not allow everyone to Publish	✗	0	2
Ensure Lambda functions do not share the same execution role	✓	0	0
Ensure IAM policies that allow full "*:*" administrative privileges are not created	✓	6	0
Ensure Elasticsearch domains do not grant wildcard (*) access	✓	0	0
Ensure CMKs (Customer Master Keys) are not exposed to everyone	✓	0	0

Evaluation Summary

AC-4 Information Flow Enforcement 65/74

Policy Name	Compliance	Passed	Failed
Ensure no ELBs allow ingress from 0.0.0.0/0 to FTP port 20	✓	0	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to Oracle DB port 1521	✓	0	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to Cassandra client port 9042	✓	0	0
Ensure no EC2 Instance allows Public access on LDAP port 389	✓	4	0
Ensure no EC2 Instance allows Public access on Elastic search port 9200	✓	4	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to remote desktop port 3389	✓	0	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to LDAP SSL port 636	✓	0	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to FTP port 21	✓	0	0
Ensure no EC2 Instance allows Public access on Cassandra Monitoring port 7199	✓	4	0
Ensure no EC2 Instance allows Public access on Cassandra Client port 9042	✓	4	0
Ensure no EC2 Instance allows Public access on RDP port 3389	✓	4	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to Cassandra Thrift port 9160	✓	0	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to Oracle DB port 2483	✓	0	0

Evaluation Summary

AC-4 Information Flow Enforcement 65/74

Policy Name	Compliance	Passed	Failed
Ensure no EC2 Instance allows Public access on PostgreSQL port 5432	✓	4	0
Ensure no EC2 Instance allows Public access on RPC port 135	✓	4	0
Ensure no EC2 Instance allows Public access on Redis port 6379	✓	4	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to TELNET port 23	✓	0	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to LDAP port 389	✓	0	0
Ensure no EC2 Instance allows Public access on Oracle DB port 2483	✓	4	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to PostgreSQL port 5432	✓	0	0
Ensure no EC2 Instance allows Public access on DNS port 53	✓	4	0
Ensure no EC2 Instance allows Public access on SSH port 22	✓	4	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to NetBIOS port 137	✓	0	0
Ensure no EC2 Instance allows Public access on Cassandra Thrift port 9160	✓	4	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to MySQL port 3306	✓	0	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to MSSQL port 1434	✓	0	0

Evaluation Summary

AC-4 Information Flow Enforcement 65/74

Policy Name	Compliance	Passed	Failed
Ensure no ELBs allow ingress from 0.0.0.0/0 to mongod (with shardsvr option) default port 27018	✓	0	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to Memcached port 11211	✓	0	0
Ensure no EC2 Instance allows Public access on LDAP SSL port 636	✓	4	0
Ensure Elasticsearch domains are configured with VPC access	✓	0	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to Cassandra Monitoring port 7199	✓	0	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to SMTP port 25	✓	0	0
Public EC2 Instances	✗	3	1
Ensure no EC2 Instance allows Public access on mongod (with shardsvr option) default port 27018	✓	4	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to NetBIOS port 139	✓	0	0
Ensure no Security Groups allow ingress from any IPv4 address to ALL ports	✗	6	18
Ensure no EC2 Instance allows Public access on MSSQL Monitor port 1434	✓	4	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to MSSQL port 1433	✓	0	0
Ensure Lambda functions are allowed to access only VPC resources	✓	0	0

Evaluation Summary

AC-4 Information Flow Enforcement 65/74

Policy Name	Compliance	Passed	Failed
Ensure no EC2 Instance allows Public access on NetBIOS port 139	✓	4	0
Ensure no Security Groups allow egress to external IPv4 addresses on ALL ports	✗	23	1
Ensure no RDS instance allows traffic from 0.0.0.0/0	✓	0	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to DNS port 53	✓	0	0
Ensure no EC2 Instance allows Public access on FTP port 21	✓	4	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to mongod (with configsvr option) default port 27019	✓	0	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to RPC port 135	✓	0	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to SMB port 445	✓	0	0
Ensure no EC2 Instance allows Public access on TELNET port 23	✓	4	0
Ensure no EC2 Instance allows Public access on Cassandra Internode Communication port 7000	✓	4	0
Ensure no EC2 Instance allows Public access on NetBIOS port 137	✓	4	0
Ensure no EC2 Instance allows Public access on SMTP port 25	✓	4	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to NetBIOS port 138	✓	0	0

Evaluation Summary

AC-4 Information Flow Enforcement 65/74

Policy Name	Compliance	Passed	Failed
Ensure no EC2 Instance allows Public access on mongod default port 27017	✓	4	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to Redis port 6379	✓	0	0
Ensure no network ACLs allow ingress access from 0.0.0.0/0 to ALL ports	✗	1	18
Ensure no EC2 Instance allows Public access on Memcached port 11211	✓	4	0
Ensure no EC2 Instance allows Public access on MySQL port 3306	✓	4	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to Elastic search port 9200	✓	0	0
Ensure no EC2 Instance is associated with Security Groups allowing traffic from 0.0.0.0/0	✗	1	3
Ensure no EC2 Instance allows Public access on Oracle port 1521	✓	4	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to Cassandra Internode Communication port 7000	✓	0	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to SSH port 22	✓	0	0
Ensure no network ACLs allow egress access to 0.0.0.0/0 on ALL ports	✗	0	19
Ensure no EC2 Instance allows Public access on NetBIOS port 138	✓	4	0
Ensure no EC2 Instance allows Public access on mongod (with configsvr option) default port 27019	✓	4	0

Evaluation Summary

AC-4 Information Flow Enforcement 65/74

Policy Name	Compliance	Passed	Failed
Ensure no ELBs allow ingress from 0.0.0.0/0 to MongoDB port 27017	✓	0	0
Ensure no EC2 instances exist in default VPC	✗	1	3
Ensure no EC2 Instance allows Public access on SMB port 445	✓	4	0
Ensure no Security Groups allow egress to 0.0.0.0/0	✗	23	1
Ensure no EC2 Instance allows Public access on MSSQL port 1433	✓	4	0
Ensure no EC2 Instance allows Public access on FTP port 20	✓	4	0
Ensure no EC2 Instance allows Public access on Elastic search port 9300	✓	4	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to Elastic search port 9300	✓	0	0
Ensure no Security Groups allow ingress from 0.0.0.0/0	✗	22	2

Evaluation Summary

AC-5 Separation of duties 1/1

Policy Name	Compliance	Passed	Failed
Ensure Lambda functions do not share the same execution role	✓	0	0

Evaluation Summary

AC-6 Least Privilege 9/21

Policy Name	Compliance	Passed	Failed
Ensure a log metric filter and alarm exist for AWS Config configuration changes	✗	0	1
Ensure a log metric filter and alarm exist for S3 bucket policy changes	✗	0	1
Ensure no IAM user exists without any permissions	✓	7	0
Ensure a log metric filter and alarm exist for disabling or scheduled deletion of customer created CMKs	✗	0	1
Ensure CloudTrail is enabled in all regions	✓	1	0
Ensure a log metric filter and alarm exist for IAM policy changes	✗	0	1
Ensure Elasticsearch domains do not grant wildcard (*) access	✓	0	0
Ensure a log metric filter and alarm exist for usage of "root" account	✗	0	1
Ensure Redshift clusters enable audit logging	✓	0	0
Ensure a log metric filter and alarm exist for changes to network gateways	✗	0	1
Ensure SNS topics do not grant wildcard (*) access	✗	0	2
Ensure a log metric filter and alarm exist for changes to Network Access Control Lists (NACL)	✗	0	1
Avoid the use of the "root" account	✓	1	0

Evaluation Summary

AC-6 Least Privilege 9/21

Policy Name	Compliance	Passed	Failed
Ensure IAM group always have at least one or more users	✓	2	0
Ensure a log metric filter and alarm exist for CloudTrail configuration changes	✗	0	1
Ensure a log metric filter and alarm exist for VPC changes	✗	0	1
Ensure Lambda functions are not granted Admin access	✓	0	0
Ensure a log metric filter and alarm exist for route table changes	✗	0	1
Ensure a log metric filter and alarm exist for security group changes	✗	0	1
Ensure no IAM group exists without any permissions	✓	2	0
Ensure IAM policies that allow full "*:*" administrative privileges are not created	✓	6	0

Evaluation Summary

AC-17 Remote Access 11/12

Policy Name	Compliance	Passed	Failed
Ensure Elasticsearch domains enable node-to-node encryption	✓	0	0
Ensure Elasticsearch domains enable HTTPS	✓	0	0
Ensure to enable Cloudwatch Container Insights	✓	0	0
Ensure ELBs enable access logging	✓	0	0
Ensure Redshift clusters enable audit logging	✓	0	0
Ensure CloudTrail is enabled in all regions	✓	1	0
Ensure Redshift clusters enable SSL for all connections	✓	0	0
Ensure EKS Cluster enables Logging	✓	0	0
Ensure S3 buckets enable server access logging	✗	0	1
Ensure Application Load Balancers do not support TLS 1.0	✓	0	0
Ensure Application Load Balancers are configured to use HTTPS	✓	0	0
Ensure Lambda functions enable active tracing	✓	0	0

Evaluation Summary

AU-2 Audit Events 6/7

Policy Name	Compliance	Passed	Failed
Ensure Lambda functions enable active tracing	✓	0	0
Ensure CloudTrail is enabled in all regions	✓	1	0
Ensure ELBs enable access logging	✓	0	0
Ensure to enable Cloudwatch Container Insights	✓	0	0
Ensure Redshift clusters enable audit logging	✓	0	0
Ensure S3 buckets enable server access logging	✗	0	1
Ensure EKS Cluster enables Logging	✓	0	0

Evaluation Summary

AU-3 Content of Audit Records 5/6

Policy Name	Compliance	Passed	Failed
Ensure Lambda functions enable active tracing	✓	0	0
Ensure ELBs enable access logging	✓	0	0
Ensure Redshift clusters enable audit logging	✓	0	0
Ensure S3 buckets enable server access logging	✗	0	1
Ensure EKS Cluster enables Logging	✓	0	0
Ensure CloudTrail is enabled in all regions	✓	1	0

Evaluation Summary

AU-5 Response to Audit Processing Failures 0/1

Policy Name	Compliance	Passed	Failed
Ensure a log metric filter and alarm exist for CloudTrail configuration changes	✗	0	1

Evaluation Summary

AU-7 Audit Reduction and Report Generation 1/1

Policy Name	Compliance	Passed	Failed
Ensure CloudTrail log file validation is enabled	✓	1	0

Evaluation Summary

AU-8 Time Stamps 1/1

Policy Name	Compliance	Passed	Failed
Ensure CloudTrail is enabled in all regions	✓	1	0

Evaluation Summary

AU-9 Protection of Audit Information 2/3

Policy Name	Compliance	Passed	Failed
Ensure CloudTrail logs are pushed to S3 bucket that is not public	✓	1	0
Ensure CloudTrail log file validation is enabled	✓	1	0
Ensure cloud trails logs are encrypted at rest using AWS KMS customer master keys (CMKs)	✗	0	1

Evaluation Summary

AU-10 Non-Repudiation 5/6

Policy Name	Compliance	Passed	Failed
Ensure Lambda functions enable active tracing	✓	0	0
Ensure ELBs enable access logging	✓	0	0
Ensure Redshift clusters enable audit logging	✓	0	0
Ensure S3 buckets enable server access logging	✗	0	1
Ensure EKS Cluster enables Logging	✓	0	0
Ensure CloudTrail is enabled in all regions	✓	1	0

Evaluation Summary

AU-12 Audit Generation 5/6

Policy Name	Compliance	Passed	Failed
Ensure Lambda functions enable active tracing	✓	0	0
Ensure ELBs enable access logging	✓	0	0
Ensure Redshift clusters enable audit logging	✓	0	0
Ensure S3 buckets enable server access logging	✗	0	1
Ensure EKS Cluster enables Logging	✓	0	0
Ensure CloudTrail is enabled in all regions	✓	1	0

Evaluation Summary

CM-5 Access Restrictions For Change 6/18

Policy Name	Compliance	Passed	Failed
Ensure Elasticsearch domains do not grant wildcard (*) access	✓	0	0
Ensure a log metric filter and alarm exist for changes to network gateways	✗	0	1
Ensure a log metric filter and alarm exist for usage of "root" account	✗	0	1
Ensure Redshift clusters enable audit logging	✓	0	0
Ensure a log metric filter and alarm exist for IAM policy changes	✗	0	1
Ensure CloudTrail is enabled in all regions	✓	1	0
Ensure CloudTrail trails are integrated with CloudWatch Logs	✗	0	1
Ensure a log metric filter and alarm exist for changes to Network Access Control Lists (NACL)	✗	0	1
Ensure SNS topics do not grant wildcard (*) access	✗	0	2
Ensure to enable Cloudwatch Container Insights	✓	0	0
Ensure a log metric filter and alarm exist for AWS Management Console authentication failures	✗	0	1
Ensure a log metric filter and alarm exist for unauthorized API calls	✗	0	1
Ensure IAM policies that allow full "*:*" administrative privileges are not created	✓	6	0

Evaluation Summary

CM-5 Access Restrictions For Change 6/18

Policy Name	Compliance	Passed	Failed
Ensure a log metric filter and alarm exist for route table changes	✗	0	1
Ensure a log metric filter and alarm exist for security group changes	✗	0	1
Ensure a log metric filter and alarm exist for CloudTrail configuration changes	✗	0	1
Ensure Lambda functions are not granted Admin access	✓	0	0
Ensure a log metric filter and alarm exist for VPC changes	✗	0	1

Evaluation Summary

CM-6 Configuration Settings 2/13

Policy Name	Compliance	Passed	Failed
Ensure a log metric filter and alarm exist for changes to network gateways	✗	0	1
Ensure a log metric filter and alarm exist for changes to Network Access Control Lists (NACL)	✗	0	1
Ensure to enable Cloudwatch Container Insights	✓	0	0
Ensure a log metric filter and alarm exist for AWS Config configuration changes	✗	0	1
Ensure a log metric filter and alarm exist for disabling or scheduled deletion of customer created CMKs	✗	0	1
Ensure a log metric filter and alarm exist for IAM policy changes	✗	0	1
Ensure CloudTrail is enabled in all regions	✓	1	0
Ensure CloudTrail trails are integrated with CloudWatch Logs	✗	0	1
Ensure a log metric filter and alarm exist for S3 bucket policy changes	✗	0	1
Ensure a log metric filter and alarm exist for route table changes	✗	0	1
Ensure a log metric filter and alarm exist for VPC changes	✗	0	1
Ensure a log metric filter and alarm exist for CloudTrail configuration changes	✗	0	1
Ensure a log metric filter and alarm exist for security group changes	✗	0	1

Evaluation Summary

CM-7 Least Functionality 64/72

Policy Name	Compliance	Passed	Failed
Ensure no ELBs allow ingress from 0.0.0.0/0 to FTP port 20	✓	0	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to Oracle DB port 1521	✓	0	0
Ensure no EC2 Instance allows Public access on NetBIOS port 139	✓	4	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to Cassandra client port 9042	✓	0	0
Ensure no EC2 Instance allows Public access on LDAP port 389	✓	4	0
Ensure no EC2 Instance allows Public access on Elastic search port 9200	✓	4	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to remote desktop port 3389	✓	0	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to LDAP SSL port 636	✓	0	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to FTP port 21	✓	0	0
Ensure no EC2 Instance allows Public access on Cassandra Monitoring port 7199	✓	4	0
Ensure no EC2 Instance allows Public access on Cassandra Client port 9042	✓	4	0
Ensure no EC2 Instance allows Public access on RDP port 3389	✓	4	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to Cassandra Thrift port 9160	✓	0	0

Evaluation Summary

CM-7 Least Functionality 64/72

Policy Name	Compliance	Passed	Failed
Ensure no ELBs allow ingress from 0.0.0.0/0 to Oracle DB port 2483	✓	0	0
Ensure no EC2 Instance allows Public access on PostgreSQL port 5432	✓	4	0
Ensure no EC2 Instance allows Public access on RPC port 135	✓	4	0
Ensure no EC2 Instance allows Public access on Redis port 6379	✓	4	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to TELNET port 23	✓	0	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to Redis port 6379	✓	0	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to LDAP port 389	✓	0	0
Ensure no EC2 Instance allows Public access on Oracle DB port 2483	✓	4	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to PostgreSQL port 5432	✓	0	0
Ensure no EC2 Instance allows Public access on DNS port 53	✓	4	0
Ensure no EC2 Instance allows Public access on Cassandra Thrift port 9160	✓	4	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to MySQL port 3306	✓	0	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to MSSQL port 1434	✓	0	0

Evaluation Summary

CM-7 Least Functionality 64/72

Policy Name	Compliance	Passed	Failed
Ensure IAM policies that allow full "*:*" administrative privileges are not created	✓	6	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to mongod (with shardsvr option) default port 27018	✓	0	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to Memcached port 11211	✓	0	0
Ensure no EC2 Instance allows Public access on LDAP SSL port 636	✓	4	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to SMTP port 25	✓	0	0
Public EC2 Instances	✗	3	1
Ensure no EC2 Instance allows Public access on mongod (with shardsvr option) default port 27018	✓	4	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to NetBIOS port 139	✓	0	0
Ensure no Security Groups allow ingress from any IPv4 address to ALL ports	✗	6	18
Ensure no EC2 Instance allows Public access on MSSQL Monitor port 1434	✓	4	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to MSSQL port 1433	✓	0	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to DNS port 53	✓	0	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to RPC port 135	✓	0	0

Evaluation Summary

CM-7 Least Functionality — 64/72

Policy Name	Compliance	Passed	Failed
Ensure no ELBs allow ingress from 0.0.0.0/0 to SMB port 445	✓	0	0
Ensure no EC2 Instance allows Public access on TELNET port 23	✓	4	0
Ensure no EC2 Instance allows Public access on Cassandra Internode Communication port 7000	✓	4	0
Ensure no EC2 Instance allows Public access on NetBIOS port 137	✓	4	0
Ensure no EC2 Instance allows Public access on SMTP port 25	✓	4	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to NetBIOS port 138	✓	0	0
Ensure no EC2 Instance allows Public access on mongod default port 27017	✓	4	0
Ensure no network ACLs allow ingress access from 0.0.0.0/0 to ALL ports	✗	1	18
Ensure no EC2 Instance allows Public access on MySQL port 3306	✓	4	0
Ensure no EC2 Instance allows Public access on Memcached port 11211	✓	4	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to Elastic search port 9200	✓	0	0
Ensure no EC2 Instance is associated with Security Groups allowing traffic from 0.0.0.0/0	✗	1	3
Ensure no EC2 Instance allows Public access on Oracle port 1521	✓	4	0

Evaluation Summary

CM-7 Least Functionality — 64/72

Policy Name	Compliance	Passed	Failed
Ensure no ELBs allow ingress from 0.0.0.0/0 to Cassandra Internode Communication port 7000	✓	0	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to SSH port 22	✓	0	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to Cassandra Monitoring port 7199	✓	0	0
Ensure no RDS instance allows traffic from 0.0.0.0/0	✓	0	0
Ensure no Security Groups allow egress to external IPv4 addresses on ALL ports	✗	23	1
Ensure no network ACLs allow egress access to 0.0.0.0/0 on ALL ports	✗	0	19
Ensure no ELBs allow ingress from 0.0.0.0/0 to mongod (with configsvr option) default port 27019	✓	0	0
Ensure no EC2 Instance allows Public access on FTP port 21	✓	4	0
Ensure no EC2 Instance allows Public access on NetBIOS port 138	✓	4	0
Ensure no EC2 Instance allows Public access on mongod (with configsvr option) default port 27019	✓	4	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to MongoDB port 27017	✓	0	0
Ensure no EC2 Instance allows Public access on SMB port 445	✓	4	0
Ensure no Security Groups allow egress to 0.0.0.0/0	✗	23	1

Evaluation Summary

CM-7 Least Functionality 64/72

Policy Name	Compliance	Passed	Failed
Ensure no EC2 Instance allows Public access on MSSQL port 1433	✓	4	0
Ensure no EC2 Instance allows Public access on FTP port 20	✓	4	0
Ensure no EC2 Instance allows Public access on Elastic search port 9300	✓	4	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to Elastic search port 9300	✓	0	0
Ensure no Security Groups allow ingress from 0.0.0.0/0	✗	22	2
Ensure no ELBs allow ingress from 0.0.0.0/0 to NetBIOS port 137	✓	0	0
Ensure no EC2 Instance allows Public access on SSH port 22	✓	4	0

Evaluation Summary

CP-7 Alternate Processing Site 1/1

Policy Name	Compliance	Passed	Failed
Ensure Elasticsearch domains enable zone awareness		0	0

Evaluation Summary

IA-2 Identification and Authentication 0/3

Policy Name	Compliance	Passed	Failed
Ensure IAM user with console access should have MFA enabled	✗	4	3
Ensure MFA is enabled for the "root" account	✗	0	1
Ensure IAM roles allowing cross-account access are configured with either external-ID or MFA	✗	11	2

Evaluation Summary

IA-5 Authenticator Management 3/9

Policy Name	Compliance	Passed	Failed
Ensure IAM password policy require at least one lowercase letter	✗	0	1
Ensure IAM password policy requires a minimum length of 14 or greater	✓	1	0
Ensure IAM password policy prevents password reuse	✓	1	0
Ensure IAM password policy allows users to change their passwords	✗	0	1
Ensure IAM password policy requires at least one uppercase letter	✗	0	1
Ensure IAM password policy require at least one symbol	✗	0	1
Ensure IAM password policy expires passwords within 90 days or less	✓	1	0
Ensure IAM password policy require at least one number	✗	0	1
Ensure hardware MFA is enabled for the "root" account	✗	0	1

Evaluation Summary

SC-7 Boundary Protection 83/95

Policy Name	Compliance	Passed	Failed
Ensure no EC2 Instance allows Public access on Cassandra Monitoring port 7199	✓	4	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to Cassandra Thrift port 9160	✓	0	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to Oracle DB port 2483	✓	0	0
Ensure no EC2 Instance allows Public access on Cassandra Client port 9042	✓	4	0
Ensure no EBS Snapshot is Publicly accessible	✓	1	0
Ensure S3 Bucket ACLs do not grant public READ access to all Authenticated Users	✓	1	0
Ensure no EC2 Instance allows Public access on RDP port 3389	✓	4	0
Ensure S3 Bucket Policies do not allow any action from all principals	✓	1	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to Cassandra client port 9042	✓	0	0
Ensure no EC2 Instance allows Public access on LDAP port 389	✓	4	0
Ensure no EC2 Instance allows Public access on Elastic search port 9200	✓	4	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to remote desktop port 3389	✓	0	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to LDAP SSL port 636	✓	0	0

Evaluation Summary

SC-7 Boundary Protection — 83/95

Policy Name	Compliance	Passed	Failed
Ensure SNS topics do not allow everyone to Subscribe	✗	0	2
Ensure no EC2 Instance allows Public access on TELNET port 23	✓	4	0
Ensure no EC2 Instance allows Public access on NetBIOS port 137	✓	4	0
Ensure no EC2 Instance allows Public access on Cassandra Internode Communication port 7000	✓	4	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to Cassandra Internode Communication port 7000	✓	0	0
Ensure no EC2 Instance allows Public access on MSSQL port 1433	✓	4	0
Ensure S3 Bucket ACLs do not grant public WRITE_ACP access	✓	1	0
Ensure no EC2 Instance allows Public access on DNS port 53	✓	4	0
Ensure no EC2 Instance allows Public access on mongod default port 27017	✓	4	0
Ensure S3 bucket ACLs do not grant public FULL_CONTROL access	✓	1	0
Ensure no EC2 Instance allows Public access on mongod (with configsvr option) default port 27019	✓	4	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to MongoDB port 27017	✓	0	0
Ensure no EC2 Instance allows Public access on NetBIOS port 138	✓	4	0

Evaluation Summary

SC-7 Boundary Protection — 83/95

Policy Name	Compliance	Passed	Failed
Ensure no EC2 instances exist in default VPC	✗	1	3
Ensure no Security Groups allow egress to 0.0.0.0/0	✗	23	1
Ensure no EC2 Instance allows Public access on SMB port 445	✓	4	0
Ensure no EC2 Instance allows Public access on Memcached port 11211	✓	4	0
Ensure no network ACLs allow ingress access from 0.0.0.0/0 to ALL ports	✗	1	18
Ensure no EC2 Instance allows Public access on MySQL port 3306	✓	4	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to LDAP port 389	✓	0	0
Ensure no EC2 Instance allows Public access on Oracle DB port 2483	✓	4	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to PostgreSQL port 5432	✓	0	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to FTP port 20	✓	0	0
Ensure no EC2 Instance allows Public access on SSH port 22	✓	4	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to NetBIOS port 137	✓	0	0
Ensure no EC2 Instance allows Public access on Cassandra Thrift port 9160	✓	4	0

Evaluation Summary

SC-7 Boundary Protection 83/95

Policy Name	Compliance	Passed	Failed
Ensure no ELBs allow ingress from 0.0.0.0/0 to MySQL port 3306	✓	0	0
Ensure no EC2 Instance allows Public access on SMTP port 25	✓	4	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to NetBIOS port 138	✓	0	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to SMB port 445	✓	0	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to RPC port 135	✓	0	0
Ensure SQS queues not exposed to Everyone	✓	0	0
Ensure Application Load Balancers are associated with security group	✓	0	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to mongod (with shardsvr option) default port 27018	✓	0	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to MSSQL port 1434	✓	0	0
Ensure SNS topics do not allow everyone to Publish	✗	0	2
Ensure no EC2 Instance allows Public access on FTP port 20	✓	4	0
Ensure S3 Bucket ACLs do not grant public WRITE access to all Authenticated Users	✓	1	0
Ensure no EC2 Instance allows Public access on mongod (with shardsvr option) default port 27018	✓	4	0

Evaluation Summary

SC-7 Boundary Protection — 83/95

Policy Name	Compliance	Passed	Failed
Ensure no ELBs allow ingress from 0.0.0.0/0 to NetBIOS port 139	✓	0	0
Ensure no Security Groups allow ingress from any IPv4 address to ALL ports	✗	6	18
Ensure no EC2 Instance allows Public access on MSSQL Monitor port 1434	✓	4	0
Ensure no EC2 Instance allows Public access on NetBIOS port 139	✓	4	0
Ensure S3 Bucket ACLs do not grant public READ access	✓	1	0
Ensure S3 Bucket ACLs do not grant public FULL_CONTROL access to all Authenticated Users	✓	1	0
Ensure no Security Groups allow egress to external IPv4 addresses on ALL ports	✗	23	1
Ensure CMKs (Customer Master Keys) are not exposed to everyone	✓	0	0
Ensure no RDS instance allows traffic from 0.0.0.0/0	✓	0	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to SMTP port 25	✓	0	0
Public EC2 Instances	✗	3	1
Ensure no ELBs allow ingress from 0.0.0.0/0 to Elastic search port 9300	✓	0	0
Ensure no Security Groups allow ingress from 0.0.0.0/0	✗	22	2

Evaluation Summary

SC-7 Boundary Protection 83/95

Policy Name	Compliance	Passed	Failed
Ensure no EC2 Instance allows Public access on Elastic search port 9300	✓	4	0
Ensure ECR repositories are not exposed to Public	✓	0	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to DNS port 53	✓	0	0
Ensure no EC2 Instance allows Public access on LDAP SSL port 636	✓	4	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to Memcached port 11211	✓	0	0
Ensure no EC2 Instance allows Public access on RPC port 135	✓	4	0
Ensure no EC2 Instance allows Public access on Redis port 6379	✓	4	0
Ensure S3 Bucket Policies do not grant public access on all actions	✓	1	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to TELNET port 23	✓	0	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to FTP port 21	✓	0	0
Ensure Redshift clusters are not publicly accessible	✓	0	0
Ensure S3 Bucket ACLs do not grant public WRITE_ACP access to all Authenticated Users	✓	1	0
Ensure no EC2 Instance allows Public access on FTP port 21	✓	4	0

Evaluation Summary

SC-7 Boundary Protection 83/95

Policy Name	Compliance	Passed	Failed
Ensure no ELBs allow ingress from 0.0.0.0/0 to mongod (with configsvr option) default port 27019	✓	0	0
Ensure S3 Bucket ACLs do not grant public READ_ACP access to all Authenticated Users	✓	1	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to MSSQL port 1433	✓	0	0
Ensure S3 Bucket ACLs do not grant public READ_ACP access	✓	1	0
Ensure S3 Bucket ACLs do not grant public WRITE access	✓	1	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to Redis port 6379	✓	0	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to Cassandra Monitoring port 7199	✓	0	0
Ensure RDS snapshot is not public	✓	0	0
Ensure AMIs are not Publicly Accessible	✓	0	0
Ensure no network ACLs allow egress access to 0.0.0.0/0 on ALL ports	✗	0	19
Ensure no EC2 Instance allows Public access on PostgreSQL port 5432	✓	4	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to Oracle DB port 1521	✓	0	0
Ensure no ELBs allow ingress from 0.0.0.0/0 to Elastic search port 9200	✓	0	0

Evaluation Summary

SC-7 Boundary Protection — 83/95

Policy Name	Compliance	Passed	Failed
Ensure no EC2 Instance is associated with Security Groups allowing traffic from 0.0.0.0/0	✗	1	3
Ensure no EC2 Instance allows Public access on Oracle port 1521	✓	4	0
Ensure VPC Flow Logs are enabled	✗	0	18
Ensure no ELBs allow ingress from 0.0.0.0/0 to SSH port 22	✓	0	0

Evaluation Summary

SC-8 Transmission Confidentiality and Integrity 5/5

Policy Name	Compliance	Passed	Failed
Ensure Elasticsearch domains enable HTTPS	✓	0	0
Ensure Redshift clusters enable SSL for all connections	✓	0	0
Ensure Application Load Balancers are configured to use HTTPS	✓	0	0
Ensure Elasticsearch domains enable node-to-node encryption	✓	0	0
Ensure Application Load Balancers do not support TLS 1.0	✓	0	0

Evaluation Summary

SC-12 Cryptographic Key Establishment and Management 5/5

Policy Name	Compliance	Passed	Failed
ACM certificates due for renewal in 30 days	✓	0	0
Ensure rotation of keys is enabled for customer managed CMKs	✓	0	0
IAM server certificates due for renewal in 30 days	✓	0	0
Ensure expired certificates are removed from ACM	✓	0	0
Ensure expired IAM server certificates are removed	✓	0	0

Evaluation Summary

SC-13 Cryptographic Protection 12/18

Policy Name	Compliance	Passed	Failed
Ensure Elasticsearch domains enable encryption at rest	✓	0	0
Ensure RDS snapshot is encrypted	✓	0	0
Ensure cloud trails logs are encrypted at rest using AWS KMS customer master keys (CMKs)	✗	0	1
Ensure S3 buckets are encrypted	✓	1	0
Ensure EBS Volumes attached to EC2 Instance are Encrypted	✗	0	4
Ensure SNS topics are encrypted using CMKs	✗	0	2
Ensure EBS snapshots are encrypted	✗	0	1
Ensure SQS queues are encrypted using CMKs	✓	0	0
Ensure Application Load Balancers are configured to use HTTPS	✓	0	0
Ensure EFS file systems are encrypted	✓	0	0
Ensure Amazon SQS queues enable Server-Side Encryption (SSE)	✓	0	0
Ensure AMIs are encrypted	✓	0	0
Ensure SNS topics are encrypted	✗	0	2

Evaluation Summary

SC-13 Cryptographic Protection 12/18

Policy Name	Compliance	Passed	Failed
Ensure Application Load Balancers do not support TLS 1.0	✓	0	0
Ensure RDS instance is encrypted	✓	0	0
Ensure EBS volumes are encrypted	✗	0	4
Ensure Redshift clusters enable SSL for all connections	✓	0	0
Ensure Redshift clusters are encrypted	✓	0	0

Evaluation Summary

SC-23 Session Authenticity 5/5

Policy Name	Compliance	Passed	Failed
Ensure Elasticsearch domains enable HTTPS		0	0
Ensure Redshift clusters enable SSL for all connections		0	0
Ensure Application Load Balancers are configured to use HTTPS		0	0
Ensure Elasticsearch domains enable node-to-node encryption		0	0
Ensure Application Load Balancers do not support TLS 1.0		0	0

Evaluation Summary

SC-28 Protection of Information at Rest 9/15

Policy Name	Compliance	Passed	Failed
Ensure Elasticsearch domains enable encryption at rest	✓	0	0
Ensure RDS snapshot is encrypted	✓	0	0
Ensure RDS instance is encrypted	✓	0	0
Ensure EBS volumes are encrypted	✗	0	4
Ensure SNS topics are encrypted using CMKs	✗	0	2
Ensure EBS Volumes attached to EC2 Instance are Encrypted	✗	0	4
Ensure SQS queues are encrypted using CMKs	✓	0	0
Ensure EBS snapshots are encrypted	✗	0	1
Ensure Amazon SQS queues enable Server-Side Encryption (SSE)	✓	0	0
Ensure EFS file systems are encrypted	✓	0	0
Ensure Redshift clusters are encrypted	✓	0	0
Ensure cloud trails logs are encrypted at rest using AWS KMS customer master keys (CMKs)	✗	0	1
Ensure S3 buckets are encrypted	✓	1	0

Evaluation Summary

SC-28 Protection of Information at Rest 9/15

Policy Name	Compliance	Passed	Failed
Ensure AMIs are encrypted	✓	0	0
Ensure SNS topics are encrypted	✗	0	2

Policy Details

Ensure a log metric filter and alarm exist for AWS Config configuration changes

Resource(s) Evaluated : 1

Non-Compliant Resource(s) : 1

Description

Real-time monitoring of API calls can be achieved by directing CloudTrail Logs to CloudWatch Logs and establishing corresponding metric filters and alarms. It is recommended that a metric filter and alarm be established for AWS Config configuration changes

For more information visit
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, choose "cloudtrail"
2. Click on "Trails" on left navigation pane and create new, or select already existing trail which is enabled across all regions ("Region" column with value "All" and with Read/Write events "All") and integrated with cloudwatch
3. Copy the log group name under "CloudWatch Logs Log group" column
4. Go to "cloudwatch" service, click on "Logs", select the log group copied and click on "Create Metric Filter"
5. Apply the Filter Pattern "{ ($.eventSource = config.amazonaws.com) && (($.eventName = StopConfigurationRecorder) || ($.eventName = DeleteDeliveryChannel) || ($.eventName = PutDeliveryChannel) || ($.eventName = PutConfigurationRecorder)) }" and create metric filter with proper filter name, metric namespace and metric name
6. Go to "Alarm", create an alarm for the metric created in step 5 with an appropriate alarm condition and SNS topic
7. Make sure at least one user is subscribed to SNS topic selected in step 6

Non-Compliant Resource(s)

445487006798

Policy Details

Ensure a log metric filter and alarm exist for S3 bucket policy changes

Resource(s) Evaluated : 1

Non-Compliant Resource(s) : 1

Description

Real-time monitoring of API calls can be achieved by directing CloudTrail Logs to CloudWatch Logs and establishing corresponding metric filters and alarms. It is recommended that a metric filter and alarm be established for S3 bucket policy changes

For more information visit
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, choose "cloudtrail"
2. Click on "Trails" on left navigation pane and create new, or select already existing trail which is enabled across all regions ("Region" column with value "All" and with Read/Write events "All") and integrated with cloudwatch
3. Copy the log group name under "CloudWatch Logs Log group" column
4. Go to "cloudwatch" service, click on "Logs", select the log group copied and click on "Create Metric Filter"
5. Apply the Filter Pattern "{ ($.eventSource = s3.amazonaws.com) && (($.eventName = PutBucketAcl) || ($.eventName = PutBucketPolicy) || ($.eventName = PutBucketCors) || ($.eventName = PutBucketLifecycle) || ($.eventName = PutBucketReplication) || ($.eventName = DeleteBucketPolicy) || ($.eventName = DeleteBucketCors) || ($.eventName = DeleteBucketLifecycle) || ($.eventName = DeleteBucketReplication)) }" and create metric filter with proper filter name, metric namespace and metric name
6. Go to "Alarm", create an alarm for the metric created in step 5 with an appropriate alarm condition and SNS topic
7. Make sure at least one user is subscribed to SNS topic selected in step 6

Non-Compliant Resource(s)

445487006798

Policy Details

Ensure a log metric filter and alarm exist for disabling or scheduled deletion of customer created CMKs

Resource(s) Evaluated : 1

Non-Compliant Resource(s) : 1

Description

Real-time monitoring of API calls can be achieved by directing CloudTrail Logs to CloudWatch Logs and establishing corresponding metric filters and alarms. It is recommended that a metric filter and alarm be established for disabling or scheduled deletion of customer created CMKs

For more information visit
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, choose "cloudtrail"
2. Click on "Trails" on left navigation pane and create new, or select already existing trail which is enabled across all regions ("Region" column with value "All" and with Read/Write events "All") and integrated with cloudwatch
3. Copy the log group name under "CloudWatch Logs Log group" column
4. Go to "cloudwatch" service, click on "Logs", select the log group copied and click on "Create Metric Filter"
5. Apply the Filter Pattern "{ ($.eventSource = kms.amazonaws.com) && (($.eventName = DisableKey) || ($.eventName = ScheduleKeyDeletion)) }" and create metric filter with proper filter name, metric namespace and metric name
6. Go to "Alarm", create an alarm for the metric created in step 5 with an appropriate alarm condition and SNS topic
7. Make sure at least one user is subscribed to SNS topic selected in step 6

Non-Compliant Resource(s)

445487006798

Policy Details

Ensure a log metric filter and alarm exist for IAM policy changes

Resource(s) Evaluated : 1

Non-Compliant Resource(s) : 1

Description

Real-time monitoring of API calls can be achieved by directing CloudTrail Logs to CloudWatch Logs and establishing corresponding metric filters and alarms. It is recommended that a metric filter and alarm be established for IAM policy changes

For more information visit
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, choose "cloudtrail"
2. Click on "Trails" on left navigation pane and create new, or select already existing trail which is enabled across all regions ("Region" column with value "All" and with Read/Write events "All") and integrated with cloudwatch
3. Copy the log group name under "CloudWatch Logs Log group" column
4. Go to "cloudwatch" service, click on "Logs", select the log group copied and click on "Create Metric Filter"
5. Apply the Filter Pattern "{ ($.eventName = DeleteGroupPolicy) || ($.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 create metric filter with proper filter name, metric namespace and metric name
6. Go to "Alarm", create an alarm for the metric created in step 5 with an appropriate alarm condition and SNS topic
7. Make sure at least one user is subscribed to SNS topic selected in step 6

Non-Compliant Resource(s)

445487006798

Policy Details

Ensure a log metric filter and alarm exist for usage of "root" account

Resource(s) Evaluated : 1

Non-Compliant Resource(s) : 1

Description

Real-time monitoring of API calls can be achieved by directing CloudTrail Logs to CloudWatch Logs and establishing corresponding metric filters and alarms. It is recommended that a metric filter and alarm be established for usage of "root" account

For more information visit
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, choose "cloudtrail"
2. Click on "Trails" on left navigation pane and create new, or select already existing trail which is enabled across all regions ("Region" column with value "All" and with Read/Write events "All") and integrated with cloudwatch
3. Copy the log group name under "CloudWatch Logs Log group" column
4. Go to "cloudwatch" service, click on "Logs", select the log group copied and click on "Create Metric Filter"
5. Apply the Filter Pattern "{ ($.userIdentity.type = Root) && ($.userIdentity.invokedBy NOT EXISTS) && ($.eventType != AwsServiceEvent) }" and create metric filter with proper filter name, metric namespace and metric name
6. Go to "Alarm", create an alarm for the metric created in step 5 with an appropriate alarm condition and SNS topic
7. Make sure at least one user is subscribed to SNS topic selected in step 6

Non-Compliant Resource(s)

445487006798

Policy Details

Ensure a log metric filter and alarm exist for changes to network gateways

Resource(s) Evaluated : 1

Non-Compliant Resource(s) : 1

Description

Real-time monitoring of API calls can be achieved by directing CloudTrail Logs to CloudWatch Logs and establishing corresponding metric filters and alarms. It is recommended that a metric filter and alarm be established for changes to network gateways

For more information visit
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, choose "cloudtrail"
2. Click on "Trails" on left navigation pane and create new, or select already existing trail which is enabled across all regions ("Region" column with value "All" and with Read/Write events "All") and integrated with cloudwatch
3. Copy the log group name under "CloudWatch Logs Log group" column
4. Go to "cloudwatch" service, click on "Logs", select the log group copied and click on "Create Metric Filter"
5. Apply the Filter Pattern "{ ($.eventName = CreateCustomerGateway) || ($.eventName = DeleteCustomerGateway) || ($.eventName = AttachInternetGateway) || ($.eventName = CreateInternetGateway) || ($.eventName = DeleteInternetGateway) || ($.eventName = DetachInternetGateway) }" and create metric filter with proper filter name, metric namespace and metric name
6. Go to "Alarm", create an alarm for the metric created in step 5 with an appropriate alarm condition and SNS topic
7. Make sure at least one user is subscribed to SNS topic selected in step 6

Non-Compliant Resource(s)

445487006798

Policy Details

Ensure SNS topics do not grant wildcard (*) access

Resource(s) Evaluated : 2

Non-Compliant Resource(s) : 2

Description

A resource-based policy enables you to specify which AWS account and which AWS users or roles can access your SNS Topic. Allowing access to any principal (* or AWS: *) is against compliance requirements, and if appropriate conditions are not added, it might expose SNS topics to the public. As a best practice, ensure SNS topics enable access to only desired cloud accounts or IAM members.

For more information visit
https://docs.aws.amazon.com/sns/latest/dg/sns-using-identity-based-policies.html

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, Choose SNS service.
2. In the left navigation panel, select Topics.
3. Select the desired SNS topic and click the Edit button.
4. Under "Access policy" section, edit the policy statement, ensure no statement exist with a combination "Effect": "Allow", "Principal": { "AWS":"*" } and click "Save changes".

Non-Compliant Resource(s)

arn:aws:sns:us-east-1:445487006798:c3m-sns-cloudwatch, arn:aws:sns:us-east-1:445487006798:C3m_Integration

Policy Details

Ensure a log metric filter and alarm exist for changes to Network Access Control Lists (NACL)

Resource(s) Evaluated : 1

Non-Compliant Resource(s) : 1

Description

Real-time monitoring of API calls can be achieved by directing CloudTrail Logs to CloudWatch Logs and establishing corresponding metric filters and alarms. It is recommended that a metric filter and alarm be established for changes to Network Access Control Lists (NACL)

For more information visit
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, choose "cloudtrail"
2. Click on "Trails" on left navigation pane and create new, or select already existing trail which is enabled across all regions ("Region" column with value "All" and with Read/Write events "All") and integrated with cloudwatch
3. Copy the log group name under "CloudWatch Logs Log group" column
4. Go to "cloudwatch" service, click on "Logs", select the log group copied and click on "Create Metric Filter"
5. Apply the Filter Pattern "{ ($.eventName = CreateNetworkAcl) || ($.eventName = CreateNetworkAclEntry) || ($.eventName = DeleteNetworkAcl) || ($.eventName = DeleteNetworkAclEntry) || ($.eventName = ReplaceNetworkAclEntry) || ($.eventName = ReplaceNetworkAclAssociation) }" and create metric filter with proper filter name, metric namespace and metric name
6. Go to "Alarm", create an alarm for the metric created in step 5 with an appropriate alarm condition and SNS topic
7. Make sure at least one user is subscribed to SNS topic selected in step 6

Non-Compliant Resource(s)

445487006798

Policy Details

Ensure a log metric filter and alarm exist for CloudTrail configuration changes

Resource(s) Evaluated : 1

Non-Compliant Resource(s) : 1

Description

Real-time monitoring of API calls can be achieved by directing CloudTrail Logs to CloudWatch Logs and establishing corresponding metric filters and alarms. It is recommended that a metric filter and alarm be established for CloudTrail configuration changes

For more information visit
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, choose "cloudtrail"
2. Click on "Trails" on left navigation pane and create new, or select already existing trail which is enabled across all regions ("Region" column with value "All" and with Read/Write events "All") and integrated with cloudwatch
3. Copy the log group name under "CloudWatch Logs Log group" column
4. Go to "cloudwatch" service, click on "Logs", select the log group copied and click on "Create Metric Filter"
5. Apply the Filter Pattern "{ ($.eventName = CreateTrail) || ($.eventName = UpdateTrail) || ($.eventName = DeleteTrail) || ($.eventName = StartLogging) || ($.eventName = StopLogging) }" and create metric filter with proper filter name, metric namespace and metric name
6. Go to "Alarm", create an alarm for the metric created in step 5 with an appropriate alarm condition and SNS topic
7. Make sure at least one user is subscribed to SNS topic selected in step 6

Non-Compliant Resource(s)

445487006798

Policy Details

Ensure a log metric filter and alarm exist for VPC changes

Resource(s) Evaluated : 1

Non-Compliant Resource(s) : 1

Description

Real-time monitoring of API calls can be achieved by directing CloudTrail Logs to CloudWatch Logs and establishing corresponding metric filters and alarms. It is recommended that a metric filter and alarm be established for VPC changes

For more information visit
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, choose "cloudtrail"
2. Click on "Trails" on left navigation pane and create new, or select already existing trail which is enabled across all regions ("Region" column with value "All" and with Read/Write events "All") and integrated with cloudwatch
3. Copy the log group name under "CloudWatch Logs Log group" column
4. Go to "cloudwatch" service, click on "Logs", select the log group copied and click on "Create Metric Filter"
5. Apply the Filter Pattern "{ ($.eventName = CreateVpc) || ($.eventName = DeleteVpc) || ($.eventName = ModifyVpcAttribute) || ($.eventName = AcceptVpcPeeringConnection) || ($.eventName = CreateVpcPeeringConnection) || ($.eventName = DeleteVpcPeeringConnection) || ($.eventName = RejectVpcPeeringConnection) || ($.eventName = AttachClassicLinkVpc) || ($.eventName = DetachClassicLinkVpc) || ($.eventName = DisableVpcClassicLink) || ($.eventName = EnableVpcClassicLink) }" and create metric filter with proper filter name, metric namespace and metric name
6. Go to "Alarm", create an alarm for the metric created in step 5 with an appropriate alarm condition and SNS topic
7. Make sure at least one user is subscribed to SNS topic selected in step 6

Non-Compliant Resource(s)

445487006798

Policy Details

Ensure a log metric filter and alarm exist for route table changes

Resource(s) Evaluated : 1

Non-Compliant Resource(s) : 1

Description

Real-time monitoring of API calls can be achieved by directing CloudTrail Logs to CloudWatch Logs and establishing corresponding metric filters and alarms. It is recommended that a metric filter and alarm be established for route table changes

For more information visit
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, choose "cloudtrail"
2. Click on "Trails" on left navigation pane and create new, or select already existing trail which is enabled across all regions ("Region" column with value "All" and with Read/Write events "All") and integrated with cloudwatch
3. Copy the log group name under "CloudWatch Logs Log group" column
4. Go to "cloudwatch" service, click on "Logs", select the log group copied and click on "Create Metric Filter"
5. Apply the Filter Pattern "{ ($.eventName = CreateRoute) || ($.eventName = CreateRouteTable) || ($.eventName = ReplaceRoute) || ($.eventName = ReplaceRouteTableAssociation) || ($.eventName = DeleteRouteTable) || ($.eventName = DeleteRoute) || ($.eventName = DisassociateRouteTable) }" and create metric filter with proper filter name, metric namespace and metric name
6. Go to "Alarm", create an alarm for the metric created in step 5 with an appropriate alarm condition and SNS topic
7. Make sure at least one user is subscribed to SNS topic selected in step 6

Non-Compliant Resource(s)

445487006798

Policy Details

Ensure a log metric filter and alarm exist for security group changes

Resource(s) Evaluated : 1

Non-Compliant Resource(s) : 1

Description

Real-time monitoring of API calls can be achieved by directing CloudTrail Logs to CloudWatch Logs and establishing corresponding metric filters and alarms. It is recommended that a metric filter and alarm be established for security group changes

For more information visit
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, choose "cloudtrail"
2. Click on "Trails" on left navigation pane and create new, or select already existing trail which is enabled across all regions ("Region" column with value "All" and with Read/Write events "All") and integrated with cloudwatch
3. Copy the log group name under "CloudWatch Logs Log group" column
4. Go to "cloudwatch" service, click on "Logs", select the log group copied and click on "Create Metric Filter"
5. Apply the Filter Pattern "{ ($.eventName = AuthorizeSecurityGroupIngress) || ($.eventName = AuthorizeSecurityGroupEgress) || ($.eventName = RevokeSecurityGroupIngress) || ($.eventName = RevokeSecurityGroupEgress) || ($.eventName = CreateSecurityGroup) || ($.eventName = DeleteSecurityGroup) }" and create metric filter with proper filter name, metric namespace and metric name
6. Go to "Alarm", create an alarm for the metric created in step 5 with an appropriate alarm condition and SNS topic
7. Make sure at least one user is subscribed to SNS topic selected in step 6

Non-Compliant Resource(s)

445487006798

Policy Details

Ensure S3 buckets enable server access logging

Resource(s) Evaluated : 1

Non-Compliant Resource(s) : 1

Description

AWS provides an option to enable server side access logging on S3 buckets. Server side access logs provide detailed records of the requests that are made to S3 bucket. These logs are useful in security & access audits. It is a best practice to enable server side logging on S3 buckets.

For more information visit
https://docs.aws.amazon.com/AmazonS3/latest/dev/ServerLogs.html

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, Choose S3
2. Select the S3 bucket reported under violation
3. Click on "Properties" tab, select "Server access logging", select "Enable logging" and configure the required parameters

Non-Compliant Resource(s)

c3m-s3-cloudtrail

Policy Details

Ensure a log metric filter and alarm exist for unauthorized API calls

Resource(s) Evaluated : 1

Non-Compliant Resource(s) : 1

Description

Real-time monitoring of API calls can be achieved by directing CloudTrail Logs to CloudWatch Logs and establishing corresponding metric filters and alarms. It is recommended that a metric filter and alarm be established for unauthorized API calls

For more information visit
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, choose "cloudtrail"
2. Click on "Trails" on left navigation pane and create new, or select already existing trail which is enabled across all regions ("Region" column with value "All" and with Read/Write events "All") and integrated with cloudwatch
3. Copy the log group name under "CloudWatch Logs Log group" column
4. Go to "cloudwatch" service, click on "Logs" on left navigation pane
5. Select the log group copied in step 3 and click on "Create Metric Filter"
6. Apply the Filter Pattern "{ ($.errorCode = *UnauthorizedOperation) || ($.errorCode = AccessDenied*) }" and click on "Assign Metric"
7. Provide proper Filter name, Metric Namespace and Metric Name and click on "Create Filter"
8. On the confirmation page, click on "Create Alarm" link next to the Metric listed or Go to "Alarm" in the left navigation pane and click on "Create Alarm"
9. On the Create new alarm page, make sure the metric created is selected
10. Under "Alarm Details", provide a Name for alarm, and select an appropriate condition under "Whenever" section. eg: "is" >= 1, for 1 out of 1 datapoints
11. Under "Actions", select appropriate alarm condition and SNS topic, and click on "Create Alarm"
12. Make sure at least one user is subscribed to SNS topic selected in step 11

Non-Compliant Resource(s)

445487006798

Policy Details

Ensure IAM user is not directly attached to policies

Resource(s) Evaluated : 7

Non-Compliant Resource(s) : 5

Description

An IAM user gets the required permissions to access AWS resources through IAM policies. The IAM policy can be associated with users, groups, or roles. It is recommended that IAM policies be applied directly to groups and roles but not to users. Assigning privileges at the group or role level reduces the complexity of access management as the number of users grow.

For more information visit
https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#use-groups-for-permissions

Recommendation

1. Log in to the AWS Console and go to the IAM service and click on Users
2. For each user, select the user and click on the Permissions tab
3. Make sure policies are associated only under category - "Attached from group"
4. Remove policies under category - "Attached directly"

Non-Compliant Resource(s)

arn:aws:iam::445487006798:user/c3m-demo-2, arn:aws:iam::445487006798:user/c3m-demo-user-1, arn:aws:iam::445487006798:user/c3m-demo-3, arn:aws:iam::445487006798:user/c3m-demo-user-2, arn:aws:iam::445487006798:user/c3m-demo-5

Policy Details

IAM users with Administrative Access

Resource(s) Evaluated : 7

Non-Compliant Resource(s) : 5

Description

It is a security best practice to grant required Administrative access to only selected users. And as a cloud admin one should be aware of IAM users with Administrative privileges.

For more information visit
https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#grant-least-privilege

Recommendation

1. This is more of an information policy to let C3M admins know the IAM Administrators in an account
2. If every IAM Administrator user is created with proper justification you can ignore this policy

Non-Compliant Resource(s)

arn:aws:iam::445487006798:user/c3m-demo-2, arn:aws:iam::445487006798:user/c3m-demo-user-1, arn:aws:iam::445487006798:user/c3m-demo-3, arn:aws:iam::445487006798:user/c3m-demo-user-2, arn:aws:iam::445487006798:user/c3m-demo-5

Policy Details

Ensure a log metric filter and alarm exist for Management Console sign-in without MFA

Resource(s) Evaluated : 1

Non-Compliant Resource(s) : 1

Description

Real-time monitoring of API calls can be achieved by directing CloudTrail Logs to CloudWatch Logs and establishing corresponding metric filters and alarms. It is recommended that a metric filter and alarm be established for console logins that are not protected by multi-factor authentication (MFA).

For more information visit
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, choose "cloudtrail"
2. Click on "Trails" on left navigation pane and create new, or select already existing trail which is enabled across all regions ("Region" column with value "All" and with Read/Write events "All") and integrated with cloudwatch
3. Copy the log group name under "CloudWatch Logs Log group" column
4. Go to "cloudwatch" service, click on "Logs" on left navigation pane
5. Select the log group copied in step 3 and click on "Create Metric Filter"
6. Apply the Filter Pattern "{ ($.eventName = ConsoleLogin) && ($.additionalEventData.MFAUsed != Yes) }" and click on "Assign Metric"
7. Provide proper Filter name, Metric Namespace and Metric Name and click on "Create Filter"
8. On the confirmation page, click on "Create Alarm" link next to the Metric listed or Go to "Alarm" in the left navigation pane and click on "Create Alarm"
9. On the Create new alarm page, make sure the metric created is selected
10. Under "Alarm Details", provide a Name for alarm, and select an appropriate condition under "Whenever" section. eg: "is" >= 1, for 1 out of 1 datapoints
11. Under "Actions", select appropriate alarm condition and SNS topic, and click on "Create Alarm"
12. Make sure at least one user is subscribed to SNS topic selected in step 11

Non-Compliant Resource(s)

445487006798

Policy Details

Ensure a log metric filter and alarm exist for AWS Management Console authentication failures

Resource(s) Evaluated : 1

Non-Compliant Resource(s) : 1

Description

Real-time monitoring of API calls can be achieved by directing CloudTrail Logs to CloudWatch Logs and establishing corresponding metric filters and alarms. It is recommended that a metric filter and alarm be established for AWS Management Console authentication failures

For more information visit
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, choose "cloudtrail"
2. Click on "Trails" on left navigation pane and create new, or select already existing trail which is enabled across all regions ("Region" column with value "All" and with Read/Write events "All") and integrated with cloudwatch
3. Copy the log group name under "CloudWatch Logs Log group" column
4. Go to "cloudwatch" service, click on "Logs", select the log group copied and click on "Create Metric Filter"
5. Apply the Filter Pattern "{ ($.eventName = ConsoleLogin) && ($.errorMessage = "Failed authentication") }" and create metric filter with proper filter name, metric namespace and metric name
6. Go to "Alarm", create an alarm for the metric created in step 5 with an appropriate alarm condition and SNS topic
7. Make sure at least one user is subscribed to SNS topic selected in step 6

Non-Compliant Resource(s)

445487006798

Policy Details

Ensure IAM password policy require at least one lowercase letter

Resource(s) Evaluated : 1

Non-Compliant Resource(s) : 1

Description

Password policies are, in part, used to enforce password complexity requirements. IAM password policies can be used to ensure the password is comprised of different character sets. It is recommended that the password policy require at least one lower case letter.

For more information visit
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html#password-policy-details

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, Choose IAM service
2. Click on "Account settings" on the left navigation pane
3. Select "Require at least one lowercase letter"
4. Click on "Apply password policy"

Non-Compliant Resource(s)

445487006798

Policy Details

Ensure IAM password policy allows users to change their passwords

Resource(s) Evaluated : 1

Non-Compliant Resource(s) : 1

Description

Password policies are, in part, used to enforce password complexity requirements. IAM password policies can be used to ensure users have complete control on changing their passwords. It is recommended that the password policy allow users to change their passwords.

For more information visit
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html#password-policy-details

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, Choose IAM service
2. Click on "Account settings" on the left navigation pane
3. Select "Allow users to change their own password"
4. Click on "Apply password policy"

Non-Compliant Resource(s)

445487006798

Policy Details

Ensure IAM password policy requires at least one uppercase letter

Resource(s) Evaluated : 1

Non-Compliant Resource(s) : 1

Description

Password policies are, in part, used to enforce password complexity requirements. IAM password policies can be used to ensure the password is comprised of different character sets. It is recommended that the password policy require at least one uppercase letter.

For more information visit
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html#password-policy-details

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, Choose IAM service
2. Click on "Account settings" on the left navigation pane
3. Select "Require at least one uppercase letter"
4. Click on "Apply password policy"

Non-Compliant Resource(s)

445487006798

Policy Details

Ensure IAM password policy require at least one symbol

Resource(s) Evaluated : 1

Non-Compliant Resource(s) : 1

Description

Password policies are, in part, used to enforce password complexity requirements. IAM password policies can be used to ensure the password is comprised of different character sets. It is recommended that the password policy require at least one symbol.

For more information visit
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html#password-policy-details

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, Choose IAM service
2. Click on "Account settings" on the left navigation pane
3. Select "Require at least one non-alphanumeric character"
4. Click on "Apply password policy"

Non-Compliant Resource(s)

445487006798

Policy Details

Ensure IAM password policy require at least one number

Resource(s) Evaluated : 1

Non-Compliant Resource(s) : 1

Description

Password policies are, in part, used to enforce password complexity requirements. IAM password policies can be used to ensure the password is comprised of different character sets. It is recommended that the password policy require at least one number.

For more information visit
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html#password-policy-details

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, Choose IAM service
2. Click on "Account settings" on the left navigation pane
3. Select "Require at least one number"
4. Click on "Apply password policy"

Non-Compliant Resource(s)

445487006798

Policy Details

Ensure hardware MFA is enabled for the "root" account

Resource(s) Evaluated : 1	Non-Compliant Resource(s) : 1

Description

The root account is the most privileged user in an AWS account. Multi-Factor Authentication (MFA) adds an extra layer of protection on top of a username and password. A hardware MFA has a smaller attack surface than a virtual MFA. For example, a hardware MFA does not suffer the attack surface introduced by the mobile smartphone on which a virtual MFA resides. It is a best practice to at least have hardware MFA for a privileged user like root account.

For more information visit
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_enable_virtual.html

Recommendation

1. Log in to the AWS Console https://console.aws.amazon.com/ using root credentials
2. Go to "My Security Credentials" from drop-down menu next to account name on top right corner
3. If a pop-up opens select "Continue to Security Credentials"
4. On "Your Security Credentials" page select "Multi-factor authentication (MFA)"
5. Click on "Activate MFA" and Follow the instructions on "Manage MFA Device" wizard to setup "Other hardware MFA" device

Non-Compliant Resource(s)

445487006798

Policy Details

Public EC2 Instances

Resource(s) Evaluated : 4

Non-Compliant Resource(s) : 1

Description

Allowing access from all IP addresses on the Internet to EC2 instance is risky as it can lead to Brute Force or DoS attacks. To determine public access of an instance, Cloud Control checks for all the following conditions. (i) instance associated with Public IP address. (ii) instance associated with security group allowing traffic on any port from 0.0.0.0/0. (iii) instance placed in a subnet that is connected to the Internet gateway, and the subnet is associated with NACL allowing traffic from 0.0.0.0/0 on any port. As a security best practice, ensure EC2 instances are not open to the World.

For more information visit
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/authorizing-access-to-an-instance.html

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, Choose EC2 or VPC Service
2. In the Navigation pane, choose "Security Groups"
3. Select the security group to edit, click on the "Inbound" tab and click Edit
4. Replace the rule with Source as 0.0.0.0/0 with specific IP address or delete the rule

Non-Compliant Resource(s)

i-0456d0b62aa631b88

Policy Details

Ensure no Security Groups allow ingress from any IPv4 address to ALL ports

Resource(s) Evaluated : 24

Non-Compliant Resource(s) : 18

Description

Allowing Inbound traffic on ALL ports increases the attack surface of your environment. It is a best practice to follow the principle of least privilege, and grant access on only required ports.

For more information visit
https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, Choose EC2 or VPC Service
2. In the Navigation pane, choose "Security Groups"
3. Select the security group to edit, click on the "Inbound" tab and click Edit
4. Add the new rule with specific ports, and delete the rule granting access to port range 0-65535

Non-Compliant Resource(s)

sg-f2c4b498, sg-9a9a60f5, sg-977cfeff, sg-f837b597, sg-2135f055, sg-de294ab2, sg-6b6cb605, sg-4e5a9830, sg-571a332c, sg-0822a3e46f2571709, ...8 more

Policy Details

Ensure no network ACLs allow ingress access from 0.0.0.0/0 to ALL ports

Resource(s) Evaluated : 19

Non-Compliant Resource(s) : 18

Description

Network ACL acts as a firewall for controlling traffic in and out of one or more subnets in a VPC. Allowing Inbound traffic from all external IPv4 addresses - 0.0.0.0/0 to ALL ports is always a risky configuration. It can lead to attacks like DoS, Brute Force, Smurf, and reconnaissance. It is a security best practice to restrict inbound traffic to only required port(s), and that too from known IP ranges.

For more information visit
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, choose "VPC"
2. In the Navigation pane, choose "Network ACLs"
3. Select each network ACL reported as non-compliant, click on the "Inbound Rules" tab and click "Edit Inbound Rules"
4. Replace the ALLOW rules to grant access to only specific port(s) and IP range(s) combinations as required

Non-Compliant Resource(s)

acl-3cde9254, acl-25b6b34c, acl-91ea2bf8, acl-8b7dfcf2, acl-0b7f9a60, acl-2cabfe44, acl-48228823, acl-78578c1e, acl-727d5b15, acl-c611ccbb, ...8 more

Policy Details

Ensure no EC2 Instance is associated with Security Groups allowing traffic from 0.0.0.0/0

Resource(s) Evaluated : 4

Non-Compliant Resource(s) : 3

Description

Associating an EC2 instance with a security group that allows traffic from 0.0.0.0/0 can lead to potential threats like Brute Force or DoS attacks. As a security best practice, ensure EC2 instances are associated with the security group(s) that are allowing traffic from specific IP addresses.

For more information visit
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/authorizing-access-to-an-instance.html

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, Choose EC2 or VPC Service
2. In the Navigation pane, choose "Security Groups"
3. Select the security group to edit, click on the "Inbound" tab and click Edit
4. Replace the rule with Source as 0.0.0.0/0 with specific IP address or delete the rule

Non-Compliant Resource(s)

i-0456d0b62aa631b88, i-005b75a35bb7fe93f, i-0f3a2708da804e087

Policy Details

Ensure no Security Groups allow egress to external IPv4 addresses on ALL ports

Resource(s) Evaluated : 24

Non-Compliant Resource(s) : 1

Description

Allowing Outbound traffic to ALL ports can lead to internal resources accessing unwanted and untrusted resources. It is a best practice to follow the principle of least privilege, and grant access to only required ports.

For more information visit
https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, Choose EC2 or VPC Service
2. In the Navigation pane, choose "Security Groups"
3. Select the security group to edit, click on the "Outbound" tab and click Edit
4. Add the new rule with specific ports, and delete the rule granting access to port range 0-65535

Non-Compliant Resource(s)

sg-0ecad3c3d8c0c1a73

Policy Details

Ensure no network ACLs allow egress access to 0.0.0.0/0 on ALL ports

Resource(s) Evaluated : 19

Non-Compliant Resource(s) : 19

Description

Network ACL acts as a firewall for controlling traffic in and out of one or more subnets in a VPC. Allowing outbound traffic to all external IPv4 addresses - 0.0.0.0/0 on ALL ports is always a risky configuration. It leads to internal systems accessing unwanted or untrusted resources on the external network. It is a security best practice to restrict outbound traffic to only required port(s), and that too to known IP ranges.

For more information visit
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, choose "VPC"
2. In the Navigation pane, choose "Network ACLs"
3. Select each network ACL reported as non-compliant, click on the "Outbound Rules" tab and click "Edit Outbound Rules"
4. Replace the ALLOW rules to grant access to only specific port(s) and IP range(s) combinations as required

Non-Compliant Resource(s)

acl-3cde9254, acl-25b6b34c, acl-91ea2bf8, acl-8b7dfcf2, acl-0b7f9a60, acl-2cabfe44, acl-48228823, acl-78578c1e, acl-727d5b15, acl-c611ccbb, ...9 more

Policy Details

Ensure no Security Groups allow egress to 0.0.0.0/0

Resource(s) Evaluated : 24

Non-Compliant Resource(s) : 1

Description

Allowing Outbound traffic to any IPv4 address - 0.0.0.0/0 can lead to internal resources accessing unwanted and untrusted resources. If a system is compromised, an attacker can use it to exfiltrate data or conduct spam or phishing campaigns. It is a best practice to restrict outbound traffic to only required IP address(es).

For more information visit
https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, Choose EC2 or VPC Service
2. In the Navigation pane, choose "Security Groups"
3. Select the security group to edit, click on the "Outbound" tab and click Edit.
4. Replace the rule with Destination as 0.0.0.0/0 with specific IP address or delete the rule

Non-Compliant Resource(s)

sg-0ecad3c3d8c0c1a73

Policy Details

Ensure no Security Groups allow ingress from 0.0.0.0/0

Resource(s) Evaluated : 24

Non-Compliant Resource(s) : 2

Description

Allowing Inbound traffic from any IPv4 address - 0.0.0.0/0 can lead to attacks like DoS, Brute Force, Smurf, and reconnaissance. It is a best practice to restrict inbound traffic from the required source IP address(es).

For more information visit
https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, Choose EC2 or VPC Service
2. In the Navigation pane, choose "Security Groups"
3. Select the security group to edit, click on the "Inbound" tab and click Edit
4. Replace the rule with Source as 0.0.0.0/0 with specific IP address or delete the rule

Non-Compliant Resource(s)

sg-0ad1f056d4247498d, sg-0ecad3c3d8c0c1a73

Policy Details

Ensure S3 bucket Public access setting "Block new public ACLs and uploading public objects" is enabled at an account level

Resource(s) Evaluated : 1

Non-Compliant Resource(s) : 1

Description

S3 buckets can be used to store sensitive and confidential information in an organization. So it is always advised to protect them from public access to avoid any data breaches. As a best practice enable S3 bucket public access setting "Block new public ACLs and uploading public objects". This prevents any accidental exposure of S3 buckets to the public.

For more information visit
https://docs.aws.amazon.com/AmazonS3/latest/user-guide/block-public-access-account.html

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, Choose S3
2. Select "Public access settings for this account"
3. Click on "Edit" button, enable a setting option "Block new public ACLs and uploading public objects" and save the configurations

Non-Compliant Resource(s)

445487006798

Policy Details

Ensure S3 bucket Public access setting "Block new public bucket policies" is enabled at an account level

Resource(s) Evaluated : 1

Non-Compliant Resource(s) : 1

Description

S3 buckets can be used to store sensitive and confidential information in an organization. So it is always advised to protect them from public access to avoid any data breaches. As a best practice enable S3 bucket public access setting "Block new public bucket policies". This prevents any accidental exposure of S3 buckets to the public

For more information visit
https://docs.aws.amazon.com/AmazonS3/latest/user-guide/block-public-access-account.html

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, Choose S3
2. Select "Public access settings for this account"
3. Click on "Edit" button, enable a setting option "Block new public bucket policies" and save the configurations

Non-Compliant Resource(s)

445487006798

Policy Details

Ensure S3 bucket Public access setting "Remove public access granted through public ACLs" is enabled at an account level

Resource(s) Evaluated : 1

Non-Compliant Resource(s) : 1

Description

S3 buckets can be used to store sensitive and confidential information in an organization. So it is always advised to protect them from public access to avoid any data breaches. As a best practice enable S3 bucket public access setting "Remove public access granted through public ACLs". This prevents any accidental exposure of S3 buckets to the public.

For more information visit
https://docs.aws.amazon.com/AmazonS3/latest/user-guide/block-public-access-account.html

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, Choose S3
2. Select "Public access settings for this account"
3. Click on "Edit" button, enable a setting option "Remove public access granted through public ACLs" and save the configurations

Non-Compliant Resource(s)

445487006798

Policy Details

Ensure SNS topics do not allow everyone to Subscribe

Resource(s) Evaluated : 2

Non-Compliant Resource(s) : 2

Description

A resource-based policy enables you to specify which AWS account and which AWS users or roles can access your SNS Topic. Allowing "Everyone" to subscribe to the SNS topic is a security risk and can lead to data leaks. As a best practice, ensure SNS topics do not allow "Everyone" to Subscribe to topics.

For more information visit
https://docs.aws.amazon.com/sns/latest/dg/sns-using-identity-based-policies.html

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, Choose SNS service.
2. In the left navigation panel, select Topics.
3. Select the desired SNS topic and click the Edit button.
4. Under "Access policy" section, edit the policy statement, ensure no statement exist with a combination "Effect": "Allow", "Principal": { "AWS":"*" }, "Action": ["SNS:Subscribe", "SNS:Receive"] and click "Save changes".

Non-Compliant Resource(s)

arn:aws:sns:us-east-1:445487006798:c3m-sns-cloudwatch, arn:aws:sns:us-east-1:445487006798:C3m_Integration

Policy Details

Ensure S3 bucket Public access setting "Block public and cross-account access to buckets that have public policies" is enabled at an account level

Resource(s) Evaluated : 1	Non-Compliant Resource(s) : 1

Description

S3 buckets can be used to store sensitive and confidential information in an organization. So it is always advised to protect them from public access to avoid any data breaches. As a best practice enable S3 bucket public access setting "Block public and cross-account access to buckets that have public policies". This prevents any accidental exposure of S3 buckets to the public and also blocks cross-account access to the bucket

For more information visit
https://docs.aws.amazon.com/AmazonS3/latest/user-guide/block-public-access-account.html

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, Choose S3
2. Select "Public access settings for this account"
3. Click on "Edit" button, enable a setting option "Block public and cross-account access to buckets that have public policies" and save the configurations

Non-Compliant Resource(s)

445487006798

Policy Details

Ensure SNS topics do not allow everyone to Publish

Resource(s) Evaluated : 2

Non-Compliant Resource(s) : 2

Description

A resource-based policy enables you to specify which AWS account and which AWS users or roles can access your SNS Topic. Allowing "Everyone" to publish messages to SNS topic is a security risk and can lead to DoS attacks. As a best practice, ensure SNS topics do not allow "Everyone" to Publish messages.

For more information visit
https://docs.aws.amazon.com/sns/latest/dg/sns-using-identity-based-policies.html

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, Choose SNS service.
2. In the left navigation panel, select Topics.
3. Select the desired SNS topic and click the Edit button.
4. Under "Access policy" section, edit the policy statement, ensure no statement exist with a combination "Effect": "Allow", "Principal": { "AWS":"*" }, "Action": "SNS:Publish" and click "Save changes".

Non-Compliant Resource(s)

arn:aws:sns:us-east-1:445487006798:c3m-sns-cloudwatch, arn:aws:sns:us-east-1:445487006798:C3m_Integration

Policy Details

Ensure cloud trails logs are encrypted at rest using AWS KMS customer master keys (CMKs)

Resource(s) Evaluated : 1	Non-Compliant Resource(s) : 1

Description

Cloud Trail log files delivered to S3 buckets are encrypted by Amazon server-side encryption with Amazon S3-managed encrypted keys (SSE-S3) by default. Another layer of security can be provided by using server-side encryption with AWS KMSâ€“managed keys (SSE-KMS) for CloudTrail log files.

For more information visit https://docs.aws.amazon.com/awscloudtrail/latest/userguide/encrypting-cloudtrail-log-files-with-aws-kms.html

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, choose "cloudtrail"
2. Click on "Trails" on left navigation pane.
3. Click on each trail reported as non-compliant and set "Encrypt log files with SSE-KMS" to "Yes" in Storage location section. Create a new SSE-KMS key to be used for encryption or provide an existing one.

Non-Compliant Resource(s)

arn:aws:cloudtrail:us-east-1:445487006798:trail/c3m-demo-1-cloudevents

Policy Details

Ensure no EC2 instances exist in default VPC

Resource(s) Evaluated : 4

Non-Compliant Resource(s) : 3

Description

Every AWS account comes with default Virtual Private Cloud in each region. A default VPC is suitable for getting started quickly, and for launching public instances for simple websites. But, if you need to host a complex multi-tier application or add more layers of security to your infrastructure it is a best practice to create non-default VPC with public, private subnets & demilitarized (DMZ) zones. This segregates the network based on their functionality, services, and security.

For more information visit
https://aws.amazon.com/premiumsupport/knowledge-center/move-ec2-instance/

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, Choose EC2
2. Select the EC2 instance reported under violation
3. Stop the Instance, Create an AMI of the instance
4. Launch new EC2 instance using the AMI created and place it in the non-default VPC

Non-Compliant Resource(s)

i-005b75a35bb7fe93f, i-0f3a2708da804e087, i-0558928557a60f224

Policy Details

Ensure CloudTrail trails are integrated with CloudWatch Logs

Resource(s) Evaluated : 1

Non-Compliant Resource(s) : 1

Description

CloudTrail records all API calls on AWS account and delivers the log files to S3 bucket. The recorded information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the AWS service. For real-time analysis of these logs, it is advised to configure CloudTrail to send logs to CloudWatch Logs. Sending CloudTrail logs to CloudWatch Logs will facilitate historic activity logging based on user, API, resource, and IP address, and provides an opportunity to establish alarms and notifications for anomalous or sensitivity account activity

For more information visit
https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/WhatIsCloudWatchLogs.html

Recommendation

1. Log in to the AWS Management Console and go to CloudTrail https://console.aws.amazon.com/cloudtrail
2. Click Trails in the left menu
3. Click on each trail where no CloudWatch Logs log group is empty
4. Go to the CloudWatch Logs section and click on Configure to integrate CloudWatch log group

Non-Compliant Resource(s)

arn:aws:cloudtrail:us-east-1:445487006798:trail/c3m-demo-1-cloudevents

Policy Details

Ensure IAM user with console access should have MFA enabled

Resource(s) Evaluated : 7

Non-Compliant Resource(s) : 3

Description

Multi-Factor Authentication (MFA) adds an extra layer of protection on top of a username and password. Enabling MFA provides increased security for console access as it requires the authenticating principal to possess a device that emits a time-sensitive key and have knowledge of a credential

For more information visit
https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#enable-mfa-for-privileged-users

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, Choose IAM service
2. Click on "Users" and select the user reported as non-compliant
3. Click "Security credentials" tab
4. Click on "Manage" next to "Assigned MFA device" heading.
5. Follow the instructions in Manage MFA Device wizard to setup MFA of your choice

Non-Compliant Resource(s)

arn:aws:iam::445487006798:user/c3m-demo-2, arn:aws:iam::445487006798:user/c3m-demo-3, arn:aws:iam::445487006798:user/c3m-demo-5

Policy Details

Ensure MFA is enabled for the "root" account

Resource(s) Evaluated : 1

Non-Compliant Resource(s) : 1

Description

The root account is the most privileged user in an AWS account. MFA adds an extra layer of protection on top of a username and password. With MFA enabled, when a root user signs into AWS, they will be prompted for their user name and password as well as an authentication code from their AWS MFA device.

For more information visit
http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa.html

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/ using root credentials
2. Go to "My Security Credentials" from drop-down menu next to account name on top right corner
3. If a pop-up opens select "Continue to Security Credentials"
4. On "Your Security Credentials" page select "Multi-factor authentication (MFA)"
5. Click on "Activate MFA" and Follow the instructions on "Manage MFA Device" wizard to setup "Other hardware MFA" device

Non-Compliant Resource(s)

445487006798

Policy Details

Ensure IAM roles allowing cross-account access are configured with either external-ID or MFA

Resource(s) Evaluated : 13

Non-Compliant Resource(s) : 2

Description

IAM roles can be used to grant access to an organization's AWS resources to AWS account owned by thirdparty by assuming the permission granted through the role. It is a security best practice to have IAM Roles designated for cross-account access to be configured with an external ID or MFA for additional security.

For more information visit
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_third-party.html

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, Choose "IAM"
2. In the Navigation pane, choose "Roles"
3. Click on name of each role reported as violation.
4. Select "Trust Relationships" tab and click on "Edit trust relationship"
5. Update the policy statement granting cross account access with either (a) a condition checking external ID as "Condition": { "StringEquals": { "sts:ExternalId": "external-ID"} } or (b) a condition checking use of MFA "Condition": { "StringEquals": { "Bool": { "aws:MultiFactorAuthPresent": "true" } }

Non-Compliant Resource(s)

arn:aws:iam::445487006798:role/administrator, arn:aws:iam::445487006798:role/esecure-brew-organization

Policy Details

Ensure EBS Volumes attached to EC2 Instance are Encrypted

Resource(s) Evaluated : 4

Non-Compliant Resource(s) : 4

Description

It is a security best practice to attach encrypted EBS volumes to EC2 instances to ensure data at rest is always protected.

For more information visit
https://docs.amazonaws.cn/en_us/AWSEC2/latest/UserGuide/EBSEncryption.html

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, Choose EC2.
2. In the Navigation pane, choose "Volumes".
3. Select the unencrypted EBS volume that is attached to an EC2 instance, and create a snapshot of the volume.
4. Go to Snapshots, select the newly created snapshot, and create a copy of the same by choosing the "Encryption" option.
5. Select the newly created encrypted snapshot and create an EBS volume from the snapshot in the same availability zone as the EC2 Instance.
6. Go to Instances, Stop the EC2 Instance.
7. Go to Volumes, detach the unencrypted EBS volume.
8. Select the newly created encrypted volume and attach the same to an EC2 Instance. Note: Ensure to specify the appropriate "Device" name while attaching a volume. e.g., for Linux root volumes specify the "Device" as "/dev/xvda".
9. Go to Instances, Start the EC2 Instance.

Non-Compliant Resource(s)

i-0456d0b62aa631b88, i-005b75a35bb7fe93f, i-0f3a2708da804e087, i-0558928557a60f224

Policy Details

Ensure SNS topics are encrypted using CMKs

Resource(s) Evaluated : 2

Non-Compliant Resource(s) : 2

Description

Ensure SNS topics are encrypted using Customer Master Keys instead of default AWS managed keys reserved for SNS service to protect highly sensitive messages and have more control over the encryption and decryption process.

For more information visit
https://docs.aws.amazon.com/sns/latest/dg/sns-server-side-encryption.html

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, Choose SNS service.
2. In the left navigation panel, select Topics.
3. Select the desired SNS topic and click the Edit button.
4. Under Encryption section, select "Enable encryption", choose one of the listed CMK (not the (Default) alias/aws/sns) or provide the ARN of the desired key.
5. Click "Save changes".

Non-Compliant Resource(s)

arn:aws:sns:us-east-1:445487006798:c3m-sns-cloudwatch, arn:aws:sns:us-east-1:445487006798:C3m_Integration

Policy Details

Ensure EBS snapshots are encrypted

Resource(s) Evaluated : 1

Non-Compliant Resource(s) : 1

Description

Snapshots are the backups taken on the Amazon EBS Volumes. They store sensitive and confidential information about your applications stored on the EBS volumes. It is a security best practice to encrypt snapshots so that data at rest is always protected.

For more information visit https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-copy-snapshot.html#ebs-snapshot-copy

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, Choose "EC2".
2. In the Navigation pane, choose "Snapshots".
3. Select the snapshot reported as a violation, go to "Actions" and select "Copy".
4. In the "Copy Snapshot" pop-up check the "Encrypt this snapshot" option and click "Copy".
5. Once the new encrypted snapshot is created, delete the old unencrypted snapshot.

Non-Compliant Resource(s)

snap-03c68007ba7be0fa9

Policy Details

Ensure SNS topics are encrypted

Resource(s) Evaluated : 2

Non-Compliant Resource(s) : 2

Description

Ensure SNS topics are encrypted to protect sensitive messages and avoid any data leaks.

For more information visit
https://docs.aws.amazon.com/sns/latest/dg/sns-server-side-encryption.html

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, Choose SNS service.
2. In the left navigation panel, select Topics.
3. Select the desired SNS topic and click the Edit button.
4. Under Encryption section, select "Enable encryption" and click "Save changes".

Non-Compliant Resource(s)

arn:aws:sns:us-east-1:445487006798:c3m-sns-cloudwatch, arn:aws:sns:us-east-1:445487006798:C3m_Integration

Policy Details

Ensure EBS volumes are encrypted

Resource(s) Evaluated : 4

Non-Compliant Resource(s) : 4

Description

EBS Volume is a durable, block-level storage device that can be attached to a single EC2 instance. It can be used as primary storage for data that requires frequent updates, such as the system drive for an instance or storage for a database application. EBS volumes persist independently from the running life of an EC2 instance. It is a security best practice to encrypt EBS volumes so that data at rest is always protected.

For more information visit
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html#EBSEncryption_conside

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, Choose "EC2".
2. In the Navigation pane, choose "Volumes".
3. Select the unencrypted EBS volume, and create a snapshot of the volume.
4. Go to Snapshots, select the newly created snapshot, and create a copy of the same by checking the Encryption option.
5. Select the newly created encrypted snapshot and create an EBS volume from the snapshot.
6. Delete the old unencrypted volume.

Non-Compliant Resource(s)

vol-03103514016253188, vol-025183bd3cca5a294, vol-099f2c3289f126e11, vol-0362d2ed6aa219ede

Policy Details

Ensure credentials unused for 90 days or greater are disabled

Resource(s) Evaluated : 7

Non-Compliant Resource(s) : 6

Description

AWS IAM users use credentials like passwords and access keys to connect to AWS resources. It is a best practice disable any credentials unused for more than 90days. Disabling or removing unnecessary credentials will reduce the window of opportunity for credentials associated with a compromised or abandoned account to be used.

For more information visit
https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#remove-credentials

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, Choose IAM service
2. Click on "Users" and select the user reported as non-compliant
3. Click "Security credentials" tab
4. Click on "Make inactive" or Delete keys

Non-Compliant Resource(s)

arn:aws:iam::445487006798:user/c3m-demo-2, arn:aws:iam::445487006798:user/c3m-demo-3, arn:aws:iam::445487006798:user/c3m-demo-5, arn:aws:iam::445487006798:user/c3m-demo-user-1, arn:aws:iam::445487006798:user/c3m-demo-user-2, arn:aws:iam::445487006798:user/oktaApp

Policy Details

Ensure IAM user access keys are rotated within 90 days or less

Resource(s) Evaluated : 7

Non-Compliant Resource(s) : 5

Description

Access keys consist of an access key ID and secret access key, which are used to sign programmatic requests that you make to AWS. Access keys should be rotated to ensure that data cannot be accessed with an old key which might have been lost, cracked, or stolen.

For more information visit
https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#rotate-credentials

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, Choose IAM service
2. Click on "Users" and select the user reported as non-compliant
3. Click "Security credentials" tab
4. Click on "Make inactive" or Delete keys
5. Click on Create Access Key
6. Update programmatic call with new Access Key credentials

Non-Compliant Resource(s)

arn:aws:iam::445487006798:user/c3m-demo-2, arn:aws:iam::445487006798:user/c3m-demo-user-1, arn:aws:iam::445487006798:user/c3m-demo-user-2, arn:aws:iam::445487006798:user/c3m-user, arn:aws:iam::445487006798:user/oktaApp

Policy Details

IAM user with more than one active access keys

Resource(s) Evaluated : 7

Non-Compliant Resource(s) : 2

Description

IAM user access keys are mainly used for programmatic access through CLI or API calls. Each IAM user is restricted to have maximum only 2 access keys at any point of time. This is mainly to support the rotation of keys so that applications already using old access keys can gracefully update the new keys without any downtime. It is a best practice to always use one access key and create new access key only at the time of rotation.

For more information visit https://docs.aws.amazon.com/general/latest/gr/aws-sec-cred-types.html#access-keys-and-secret-access-keys

Non-Compliant Resource(s)

arn:aws:iam::445487006798:user/c3m-demo-user-1, arn:aws:iam::445487006798:user/c3m-user

Policy Details

Ensure IAM password policy is enabled

Resource(s) Evaluated : 1

Non-Compliant Resource(s) : 1

Description

Password policies are, in part, used to enforce password complexity requirements. IAM password policies can be used to ensure the password is comprised of different character sets. It is recommended that the password policy is enabled for AWS account.

For more information visit
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html#password-policy-details

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, Choose IAM service
2. Click on "Account settings" on the left navigation pane
3. Make sure all the available options are selected, and password policy is applied

Non-Compliant Resource(s)

445487006798

Policy Details

Ensure VPC Flow Logs are enabled

Resource(s) Evaluated : 18

Non-Compliant Resource(s) : 18

Description

VPC Flow Logs capture the information about the IP traffic entering in & out of the network interfaces. It can be used for troubleshooting purposes to know why the traffic is not reaching a particular instance or for security monitoring of the incoming traffic to EC2 instances. It is a security best practice to enable VPC flow logs.

For more information visit
https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html

Recommendation

1. Log in to Amazon Console https://console.aws.amazon.com/, Choose VPC Service
2. In the Navigation pane, choose "Your VPCs"
3. Select the VPC reported under violation
4. Click on the "Flow Logs" tab and click "Create flow log" button to create flow log

Non-Compliant Resource(s)

vpc-3dacc155, vpc-3315265a, vpc-1238fe7b, vpc-401d1226, vpc-cfc8faa7, vpc-bda2d7d5, vpc-47f8da20, vpc-f846bf93, vpc-325d6855, vpc-03fc9dab31959bd75, ...8 more