PRISMA® CLOUD
BY PALO ALTO NETWORKS

NIST 800-53 Rev 5 Compliance Report

February 13, 2024 at 11:25:30 AM UTC

Prepared for PrismaCloud1

Table of Contents

Table of Contents (Continued)

Executive Summary

CLOUD ACCOUNT(S)

kishwar-aws-2 - 673174758328, AWS: Demo Team Account, kfirdaus-aws-org, AWS: Demo Team Account 2, mgruner-Xploit-Demo, CNS_PM_Account, PureSec Demo Account

REGION(S)

All cloud regions

DATES

Generated on: February 13, 2024, 11:25:30 AM UTC

From: August 22, 2018, 2:46:27 AM UTC
To: February 13, 2024, 11:25:18 AM UTC

NIST 800-53 Rev 5

Executive Summary

Resources Passed	Resources Failed	Resources Monitored	Accounts Monitored
2,025	1,110	3,135	7

Compliance Coverage Breakdown

	Passed	Failed
ACCESS CONTROL **58** Policies Enabled	27	31
AUDIT AND ACCOUNTABILITY **23** Policies Enabled	6	17
ASSESSMENT, AUTHORIZATION, AND⋯ **4** Policies Enabled	2	2
CONFIGURATION MANAGEMENT **7** Policies Enabled	4	3
CONTINGENCY PLANNING **1** Policies Enabled	0	1
IDENTIFICATION AND AUTHENTICA⋯ **21** Policies Enabled	8	13

NIST 800-53 Rev 5 / Compliance Coverage Breakdown

PROGRAM MANAGEMENT

1 Policies Enabled

Passed	Failed
0	1

PERSONNEL SECURITY

1 Policies Enabled

Passed	Failed
1	0

RISK ASSESSMENT

7 Policies Enabled

Passed	Failed
1	6

SYSTEM AND COMMUNICATIONS PRO…

77 Policies Enabled

Passed	Failed
40	37

SYSTEM AND INFORMATION INTEGRI…

16 Policies Enabled

Passed	Failed
9	7

NIST 800-53 Rev 5

Requirements	Pass	Fail	Overall
SYSTEM AND COMMUNICATIONS PROTECTION	2.1K	702	Fail
SYSTEM AND INFORMATION INTEGRITY	1.1K	366	Fail
CONFIGURATION MANAGEMENT	61	331	Fail
ACCESS CONTROL	1.8K	213	Fail
RISK ASSESSMENT	46	176	Fail
ASSESSMENT, AUTHORIZATION, AND MONITORING	40	172	Fail
IDENTIFICATION AND AUTHENTICATION	207	36	Fail
AUDIT AND ACCOUNTABILITY	191	20	Fail
PROGRAM MANAGEMENT	0	2	Fail
CONTINGENCY PLANNING	4	1	Fail
INCIDENT RESPONSE	0	0	Pass
AWARENESS AND TRAINING	0	0	Pass
PERSONNEL SECURITY	0	0	Pass
PHYSICAL AND ENVIRONMENTAL PROTECTION	0	0	Pass
PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY	0	0	Pass
SYSTEM AND SERVICES ACOUISITION	0	0	Pass
SUPPLY CHAIN RISK MANAGEMENT	0	0	Pass
PLANNING	0	0	Pass
MEDIA PROTECTION	0	0	Pass
MAINTENANCE	0	0	Pass

1

ACCESS CONTROL

ACCESS CONTROL Overview

Section			Pass Rate	Failed	Passed
Account Management | Disable Accounts	AWS Inactive users for more than 30 days	Low	78%	4	15
Account Management | Automated Audit Actions	AWS Log metric filter···	Informational	14%	6	1
Account Management | Automated Audit Actions	AWS Elasticsearch do···	Informational	50%	1	1
Account Management | Automated Audit Actions	AWS Log metric filter···	Informational	14%	6	1
Account Management | Automated Audit Actions	AWS Log metric filter···	Informational	14%	6	1
Account Management | Automated Audit Actions	AWS Log metric filter···	Informational	14%	6	1
Account Management | Automated Audit Actions	AWS Elasticsearch do···	Informational	50%	1	1
Account Management | Automated Audit Actions	AWS Log metric fil···	Informational	14%	6	1
Account Management | Automated Audit Actions	AWS Log metric filter···	Informational	14%	6	1
Account Management | Automated Audit Actions	AWS Log metric filter···	Informational	14%	6	1

NIST 800-53 Rev 5 / ACCESS CONTROL

Section			Pass Rate	Failed	Passed
Account Management | Automated Audit Actions	AWS Log metric filter···	Informational	14%	6	1
Account Management | Automated Audit Actions	AWS Log metric filter···	Informational	14%	6	1
Account Management | Automated Audit Actions	AWS Log metric filter···	Informational	14%	6	1
Account Management | Automated Audit Actions	AWS Log metric filter···	Informational	14%	6	1
Access Enforcement | Role-based Access Control	AWS IAM policy allows as···	Medium	100%	0	677
Access Enforcement | Role-based Access Control	AWS EC2 Instance IAM···	Informational	59%	34	50
Least Privilege	AWS IAM support access policy is not associated to any role	Informational	100%	0	677
Least Privilege	AWS ECS Fargate task definition root user found	Medium	100%	0	1
Least Privilege	AWS IAM policy attached to users	Low	8%	11	1
Least Privilege	AWS S3 bucket has global view ACL permissions enabled	Low	97%	5	181
Least Privilege	AWS ACM Certificate with wildcard domain name	Low	75%	1	3

NIST 800-53 Rev 5 / ACCESS CONTROL

Section			Pass Rate	Failed	Passed
Least Privilege	AWS ECS task definition elevated privileges enabled	Medium	100%	0	1
Least Privilege	AWS Access key enabled on root account	High	100%	0	7
Least Privilege	AWS IAM policy allows full administrative privileges	Medium	100%	0	677
Least Privilege | Privileged Access by Non-organizational Users	AWS···	Low	8%	11	1
System Use Notification	AWS RDS database instance is publicly accessible	Medium	60%	2	3
System Use Notification	AWS RDS Snapshot with access for unmonitored cloud accounts	Low	100%	0	26
System Use Notification	AWS S3 buckets are accessible to public via ACL	Medium	91%	15	171
System Use Notification	AWS EBS snapshots are accessible to public	Medium	96%	1	29
System Use Notification	AWS Amazon Machine Image (AMI) is publicly accessible	Low	100%	0	103
System Use Notification	AWS EBS Snapshot with access for unmonitored cloud accounts	Low	100%	0	30
System Use Notification	AWS RDS snapshots are accessible to public	Medium	100%	0	26

NIST 800-53 Rev 5 / ACCESS CONTROL

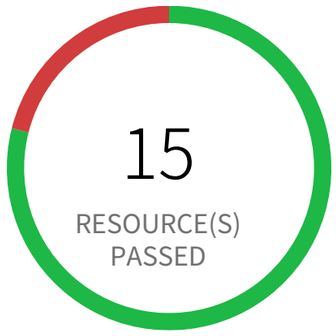
Section			Pass Rate	Failed	Passed
System Use Notification	AWS CloudTrail bucket is publicly accessible	Low	100%	0	188
System Use Notification	AWS S3 buckets are accessible to any authenticated user	Medium	99%	1	185
System Use Notification	AWS S3 bucket accessible to unmonitored cloud accounts	Low	99%	1	185
Remote Access | Protection of Confidentiality and Integrity Using Encryption		Low	100%	0	0
Remote Access | Protection of Confidentiality and Integrity Using Encryption		Low	100%	0	0
Remote Access | Protection of Confidentiality and Integrity Using Encryption		Low	0%	5	0
Remote Access | Protection of Confidentiality and Integrity Using Encryption		Low	100%	0	0
Remote Access | Protection of Confidentiality and Integrity Using Encryption		Low	100%	0	0
Remote Access | Protection of Confidentiality and Integrity Using Encryption		Informational	98%	1	82
Remote Access | Protection of Confidentiality and Integrity Using Encryption		Low	100%	0	0
Remote Access | Protection of Confidentiality and Integrity Using Encryption		Low	99%	1	369

NIST 800-53 Rev 5 / ACCESS CONTROL

Section	Pass Rate	Failed	Passed
Remote Access | Protection of Confidentiality and Integrity Using Encryption	100%	0	1
Remote Access | Protection of Confidentiality and Integrity Using Encryption	100%	0	0
Remote Access | Protection of Confidentiality and Integrity Using Encryption	14%	104	17
Remote Access | Protection of Confidentiality and Integrity Using Encryption	65%	22	42
Remote Access | Protection of Confidentiality and Integrity Using Encryption	100%	0	0
Remote Access | Protection of Confidentiality and Integrity Using Encryption	100%	0	211
Remote Access | Protection of Confidentiality and Integrity Using Encryption	100%	0	21
Remote Access | Protection of Confidentiality and Integrity Using Encryption	100%	0	1
Remote Access | Protection of Confidentiality and Integrity Using Encryption	100%	0	6
Remote Access | Protection of Confidentiality and Integrity Using Encryption	100%	0	0
Remote Access | Protection of Confidentiality and Integrity Using Encryption	100%	0	1

Section	Pass Rate	Failed	Passed
Remote Access | Protection of Confidentiality and Integrity Using Encryption — Low	0%	1	0
Remote Access | Protection of Confidentiality and Integrity Using Encryption — Informational	20%	4	1
Remote Access | Protection of Confidentiality and Integrity Using Encryption — Informational	100%	0	68
Remote Access | Protection of Confidentiality and Integrity Using Encryption — Informational	50%	1	1
Remote Access | Protection of Confidentiality and Integrity Using Encryption — Low	100%	0	0

ACCESS CONTROL / Section Account Management | Disable Accounts



4 Resource(s) Failed

pcsdemo-tenant-automation, pcsdemo-UEBA-usecase, demo-aws_resource_discovery-dmostardi, elad-okta-user1

Compliance Section: Account Management | Disable Accounts

Low

Disable accounts within [Assignment: organization-defined time period] when the accounts:
(a) Have expired;
(b) Are no longer associated with a user or individual;
(c) Are in violation of organizational policy; or
(d) Have been inactive for [Assignment: organization-defined time period].

AWS Inactive users for more than 30 days

This policy identifies users who are inactive for more than 30 days. Inactive user accounts are an easy target for attacker because any activity on the account will largely get unnoticed.

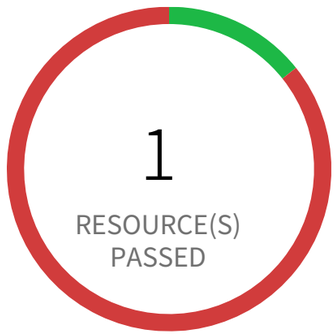
NOTE: Exception to this policy is, it is not valid for SSO login users and Root users

First Seen November 28, 2022 at 9:10:30 PM UTC | **Resource Type** IAM Credentials Report

Recommendations

1.Sign in to AWS console and navigate to IAM.
2.Identify the user reported and Make sure that the user has legitimate reason to be inactive for such an extended period.
3. Delete the user account, if the user no longer needs access to the console or no longer exists.

ACCESS CONTROL / Section Account Management | Automated Audit Actions



6 Resource(s) Failed

035297560255, 016671749923, 197802673547, 154600454722, 240075317252, 673174758328

Compliance Section: Account Management | Automated Audit Actions — Informational

Automatically audit account creation, modification, enabling, disabling, and removal actions.

AWS Log metric filter and alarm does not exist for Network Access Control Lists (NACL) changes

This policy identifies the AWS regions which do not have a log metric filter and alarm for Network Access Control Lists (NACL) changes. Monitoring changes to NACLs will help ensure that AWS resources and services are not unintentionally exposed. It is recommended that a metric filter and alarm be established for changes made to NACLs.

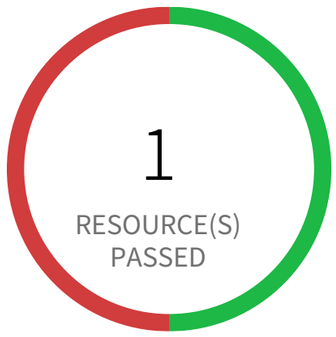
NOTE: This policy will trigger alert if you have at least one Cloudtrail with the multi trial is enabled, Logs all management events in your account and is not set with specific log metric filter and alarm.

First Seen March 18, 2021 at 11:01:09 AM UTC | **Resource Type** Other

Recommendations

1. Sign in to AWS Console
2. Navigate to CloudWatch dashboard
3. Click on 'Log groups' in the 'Logs' section (Left panel)
4. Select the log group created for your CloudTrail trail event logs (CloudTrail should be multi trail enabled with all management events captured) and click 'Create Metric Filter' button.
5. In 'Define Logs Metric Filter' page, add 'Filter pattern' value as
{ ($.eventName = CreateNetworkAcl) || ($.eventName = CreateNetworkAclEntry) || ($.eventName = DeleteNetworkAcl) || ($.eventName = DeleteNetworkAclEntry) || ($.eventName = ReplaceNetworkAclEntry) || ($.eventName = ReplaceNetworkAclAssociation) }
and Click on 'Assign Metric'
6. In 'Create Metric Filter and Assign a Metric' page, Choose Filter Name, Metric Details parameter according to your requirement and click on 'Create Filter'
7. Click on 'Create Alarm',
- In Step 1 specify metric details and conditions details as required and click on 'Next'
- In Step 2 Select an SNS topic either by creating a new topic or use existing SNS topic/ARN and click on 'Next'
- In Step 3 Select name and description to alarm and click on 'Next'
- In Step 4 Preview your data entered and click on 'Create Alarm'

ACCESS CONTROL / Section Account Management | Automated Audit Actions



1 Resource(s) Failed

eladingestsearch

Compliance Section: Account Management | Automated Audit Actions

Informational

Automatically audit account creation, modification, enabling, disabling, and removal actions.

AWS Elasticsearch domain has Index slow logs set to disabled

This policy identifies Elasticsearch domains for which Index slow logs is disabled in your AWS account. Enabling support for publishing indexing slow logs to AWS CloudWatch Logs enables you have full insight into the performance of indexing operations performed on your Elasticsearch clusters. This will help you in identifying performance issues caused by specific queries or due to changes in cluster usage, so that you can optimize your index configuration to address the problem.

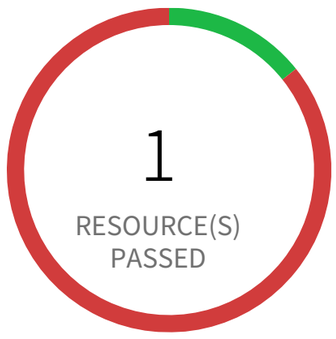
First Seen August 13, 2022 at 9:01:40 AM UTC | **Resource Type** Other

Recommendations

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to Elasticsearch Service Dashboard
4. Choose reported Elasticsearch domain
5. Select the 'Logs' tab
6. In 'Set up Index slow logs' section,
   a. click on 'Setup'
   b. In 'Select CloudWatch Logs log group' setting, Create/Use existing CloudWatch Logs log group as per your requirement
   c. In 'Specify CloudWatch access policy', Create new/Select an existing policy as per your requirement
   d. Click on 'Enable'

The Index slow logs setting 'Status' should change now to 'Enabled'.

ACCESS CONTROL / Section Account Management | Automated Audit Actions



6 Resource(s) Failed

035297560255, 016671749923, 197802673547, 154600454722, 240075317252, 673174758328

Compliance Section: Account Management | Automated Audit Actions

Informational

Automatically audit account creation, modification, enabling, disabling, and removal actions.

AWS Log metric filter and alarm does not exist for AWS management console authentication failures

This policy identifies the AWS accounts which do not have a log metric filter and alarm for AWS management console authentication failures. Monitoring failed console logins may decrease lead time to detect an attempt to brute force a credential, which may provide an indicator, such as source IP, that can be used in other event correlation. It is recommended that a metric filter and alarm be established for failed console authentication attempts.

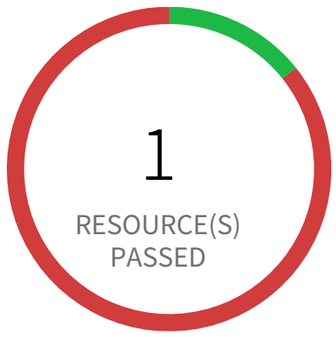
NOTE: This policy will trigger alert if you have at least one Cloudtrail with the multi trial is enabled, Logs all management events and is not set with specific log metric filter and alarm in your account.

First Seen March 18, 2021 at 11:01:09 AM UTC | **Resource Type** Other

Recommendations

1. Sign in to AWS Console
2. Navigate to CloudWatch dashboard
3. Click on 'Log groups' in the 'Logs' section (Left panel)
4. Select the log group created for your CloudTrail trail event logs (Cloudtrail should be multi trail enabled with all Management Events captured) and click 'Create Metric Filter' button.
5. In 'Define Logs Metric Filter' page, add 'Filter pattern' value as
{ ($.eventName = ConsoleLogin) && ($.errorMessage = "Failed authentication") }
and Click on 'Assign Metric'
6. In 'Create Metric Filter and Assign a Metric' page, Choose Filter Name, Metric Details parameter according to your requirement and click on 'Create Filter'
7. Click on 'Create Alarm',
- In Step 1, specify metric details and conditions details as required and click on 'Next'
- In Step 2, Select an SNS topic either by creating a new topic or use existing SNS topic/ARN and click on 'Next'
- In Step 3, Select name and description to alarm and click on 'Next'
- In Step 4, Preview your data entered and click on 'Create Alarm'

ACCESS CONTROL / Section Account Management | Automated Audit Actions



6 Resource(s) Failed

035297560255, 016671749923, 197802673547, 154600454722, 240075317252, 673174758328

Compliance Section: Account Management | Automated Audit Actions — Informational

Automatically audit account creation, modification, enabling, disabling, and removal actions.

AWS Log metric filter and alarm does not exist for CloudTrail configuration changes

This policy identifies the AWS regions which do not have a log metric filter and alarm for CloudTrail configuration changes. Monitoring changes to CloudTrail's configuration will help ensure sustained visibility to activities performed in the AWS account. It is recommended that a metric filter and alarm be established for detecting changes to CloudTrail's configurations.

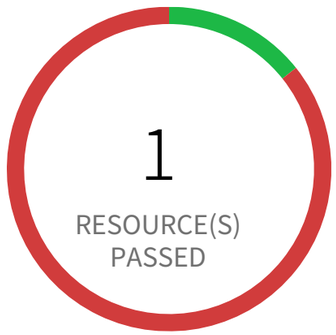
NOTE: This policy will trigger alert if you have at least one Cloudtrail with the multi trial is enabled, Logs all management events in your account and is not set with specific log metric filter and alarm.

First Seen March 18, 2021 at 11:01:09 AM UTC | **Resource Type** Other

Recommendations

1. Sign in to AWS Console
2. Navigate to CloudWatch dashboard
3. Click on 'Log groups' in the 'Logs' section (Left panel)
4. Select the log group created for your CloudTrail trail event logs (CloudTrail should be multi trail enabled with all management events captured) and click 'Create Metric Filter' button.
5. In 'Define Logs Metric Filter' page, add 'Filter pattern' value as
{ ($.eventName = CreateTrail) || ($.eventName = UpdateTrail) || ($.eventName = DeleteTrail) || ($.eventName = StartLogging) || ($.eventName = StopLogging) }
and Click on 'Assign Metric'
6. In 'Create Metric Filter and Assign a Metric' page, Choose Filter Name, Metric Details parameter according to your requirement and click on 'Create Filter'
7. Click on 'Create Alarm',
- In Step 1 specify metric details and conditions details as required and click on 'Next'
- In Step 2 Select an SNS topic either by creating a new topic or use existing SNS topic/ARN and click on 'Next'
- In Step 3 Select name and description to alarm and click on 'Next'
- In Step 4 Preview your data entered and click on 'Create Alarm'

ACCESS CONTROL / Section Account Management | Automated Audit Actions



6 Resource(s) Failed

035297560255, 016671749923, 197802673547, 154600454722, 240075317252, 673174758328

Compliance Section: Account Management | Automated Audit Actions — Informational

Automatically audit account creation, modification, enabling, disabling, and removal actions.

AWS Log metric filter and alarm does not exist for Route table changes

This policy identifies the AWS regions which do not have a log metric filter and alarm for Route table changes. Monitoring changes to route tables will help ensure that all VPC traffic flows through an expected path. It is recommended that a metric filter and alarm be established for changes to route tables.

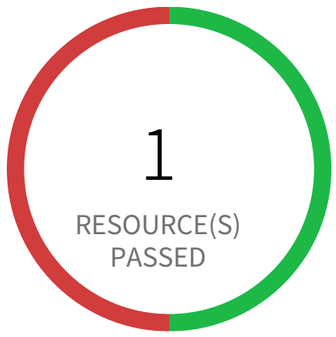
NOTE: This policy will trigger alert if you have at least one Cloudtrail with the multi trial is enabled, Logs all management events in your account and is not set with specific log metric filter and alarm.

First Seen March 18, 2021 at 11:01:09 AM UTC | **Resource Type** Other

Recommendations

1. Sign in to AWS Console
2. Navigate to CloudWatch dashboard
3. Click on 'Log groups' in the 'Logs' section (Left panel)
4. Select the log group created for your CloudTrail trail event logs (CloudTrail should be multi trail enabled with all management events captured) and click 'Create Metric Filter' button.
5. In 'Define Logs Metric Filter' page, add 'Filter pattern' value as
{ ($.eventName = CreateRoute) || ($.eventName = CreateRouteTable) || ($.eventName = ReplaceRoute) || ($.eventName = ReplaceRouteTable-Association) || ($.eventName = DeleteRouteTable) || ($.eventName = DeleteRoute) || ($.eventName = DisassociateRouteTable) }
and Click on 'Assign Metric'
6. In 'Create Metric Filter and Assign a Metric' page, Choose Filter Name, Metric Details parameter according to your requirement and click on 'Create Filter'
7. Click on 'Create Alarm',
- In Step 1 specify metric details and conditions details as required and click on 'Next'
- In Step 2 Select an SNS topic either by creating a new topic or use existing SNS topic/ARN and click on 'Next'
- In Step 3 Select name and description to alarm and click on 'Next'
- In Step 4 Preview your data entered and click on 'Create Alarm'

ACCESS CONTROL / Section Account Management | Automated Audit Actions



1 Resource(s) Failed

eladingestsearch

Compliance Section: Account Management | Automated Audit Actions

Informational

Automatically audit account creation, modification, enabling, disabling, and removal actions.

AWS Elasticsearch domain has Search slow logs set to disabled

This policy identifies Elasticsearch domains for which Search slow logs is disabled in your AWS account. Enabling support for publishing Search slow logs to AWS CloudWatch Logs enables you to have full insight into the performance of search operations performed on your Elasticsearch clusters. This will help you in identifying performance issues caused by specific search queries so that you can optimize your queries to address the problem.

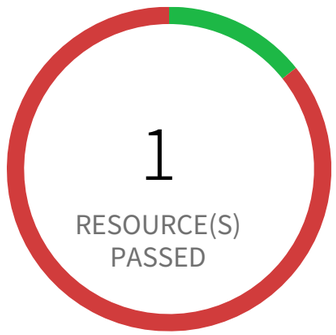
First Seen August 13, 2022 at 9:01:40 AM UTC | **Resource Type** Other

Recommendations

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to Elasticsearch Service Dashboard
4. Choose reported Elasticsearch domain
5. Select the 'Logs' tab
6. In 'Set up Search slow logs' section,
   a. click on 'Setup'
   b. In 'Select CloudWatch Logs log group' setting, Create/Use existing CloudWatch Logs log group as per your requirement
   c. In 'Specify CloudWatch access policy', Create new/Select an existing policy as per your requirement
   d. Click on 'Enable'

The search slow logs setting 'Status' should change now to 'Enabled'.

ACCESS CONTROL / Section Account Management | Automated Audit Actions



6 Resource(s) Failed

035297560255, 016671749923, 197802673547, 154600454722, 240075317252, 673174758328

Compliance Section: Account Management | Automated Audit Actions — Informational

Automatically audit account creation, modification, enabling, disabling, and removal actions.

AWS Log metric filter and alarm does not exist for disabling or scheduled deletion of customer created CMKs

This policy identifies the AWS regions which do not have a log metric filter and alarm for disabling or scheduled deletion of customer created CMKs. Data encrypted with disabled or deleted keys will no longer be accessible. It is recommended that a metric filter and alarm be established for customer created CMKs which have changed state to disabled or scheduled deletion.

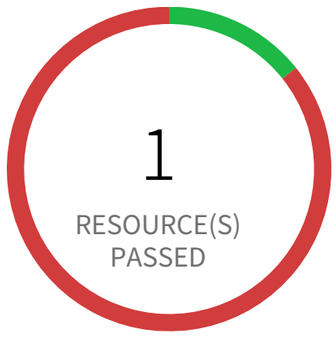
NOTE: This policy will trigger alert if you have at least one Cloudtrail with the multi trial is enabled, Logs all management events in your account and is not set with specific log metric filter and alarm.

First Seen March 18, 2021 at 11:01:09 AM UTC | **Resource Type** Other

Recommendations

1. Sign in to AWS Console
2. Navigate to CloudWatch dashboard
3. Click on 'Log groups' in the 'Logs' section (Left panel)
4. Select the log group created for your CloudTrail trail event logs (CloudTrail should be multi trail enabled with all management events captured) and click 'Create Metric Filter' button.
5. In 'Define Logs Metric Filter' page, add 'Filter pattern' value as
{ ($.eventSource = kms.amazonaws.com) && (($.eventName=DisableKey)||($.eventName=ScheduleKeyDeletion)) }
and Click on 'Assign Metric'
6. In 'Create Metric Filter and Assign a Metric' page, Choose Filter Name, Metric Details parameter according to your requirement and click on 'Create Filter'
7. Click on 'Create Alarm',
- In Step 1 specify metric details and conditions details as required and click on 'Next'
- In Step 2 Select an SNS topic either by creating a new topic or use existing SNS topic/ARN and click on 'Next'
- In Step 3 Select name and description to alarm and click on 'Next'
- In Step 4 Preview your data entered and click on 'Create Alarm'

ACCESS CONTROL / Section Account Management | Automated Audit Actions



6 Resource(s) Failed

035297560255, 016671749923, 197802673547, 154600454722, 240075317252, 673174758328

Compliance Section: Account Management | Automated Audit Actions — Informational

Automatically audit account creation, modification, enabling, disabling, and removal actions.

AWS Log metric filter and alarm does not exist for IAM policy changes

This policy identifies the AWS regions which do not have a log metric filter and alarm for IAM policy changes. Monitoring changes to IAM policies will help ensure authentication and authorization controls remain intact. It is recommended that a metric filter and alarm be established changes made to Identity and Access Management (IAM) policies.

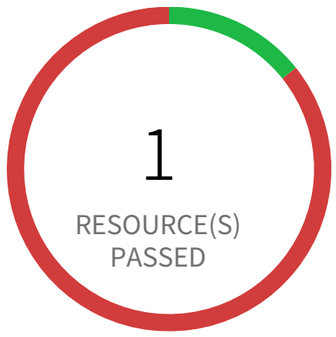
NOTE: This policy will trigger alert if you have at least one Cloudtrail with the multi trial is enabled, Logs all management events in your account and is not set with specific log metric filter and alarm.

First Seen March 18, 2021 at 11:01:00 AM UTC | **Resource Type** Other

Recommendations

1. Sign in to AWS Console
2. Navigate to CloudWatch dashboard
3. Click on 'Log groups' in the 'Logs' section (Left panel)
4. Select the log group created for your CloudTrail trail event logs (CloudTrail should be multi trail enabled with all management events captured) and click 'Create Metric Filter' button.
5. In 'Define Logs Metric Filter' page, add 'Filter pattern' value as
{
($.eventName=DeleteGroupPolicy)||($.eventName=DeleteRolePolicy)||($.eventName=DeleteUserPolicy)||($.eventName=PutGroupPolicy)||($.eventName=PutRolePolicy)||($.eventName=PutUserPolicy)||($.eventName=CreatePolicy)||($.eventName=DeletePolicy)||($.eventName=CreatePolicyVersion)||($.eventName=DeletePolicyVersion)||($.eventName=AttachRolePolicy)||($.eventName=DetachRolePolicy)||($.eventName=AttachUserPolicy)||($.eventName=DetachUserPolicy)||($.eventName=AttachGroupPolicy)||($.eventName=DetachGroupPolicy) }
and Click on 'Assign Metric'
6. In 'Create Metric Filter and Assign a Metric' page, Choose Filter Name, Metric Details parameter according to your requirement and click on 'Create Filter'
7. Click on 'Create Alarm',
- In Step 1 specify metric details and conditions details as required and click on 'Next'
- In Step 2 Select an SNS topic either by creating a new topic or use existing SNS topic/ARN and click on 'Next'
- In Step 3 Select name and description to alarm and click on 'Next'
- In Step 4 Preview your data entered and click on 'Create Alarm'

ACCESS CONTROL / Section Account Management | Automated Audit Actions



6 Resource(s) Failed

035297560255, 016671749923, 197802673547, 154600454722, 240075317252, 673174758328

Compliance Section: Account Management | Automated Audit Actions — Informational

Automatically audit account creation, modification, enabling, disabling, and removal actions.

AWS Log metric filter and alarm does not exist for unauthorized API calls

This policy identifies the AWS regions which do not have a log metric filter and alarm for unauthorized API calls. Monitoring unauthorized API calls will help reveal application errors and may reduce the time to detect malicious activity. It is recommended that a metric filter and alarm be established for unauthorized API calls.

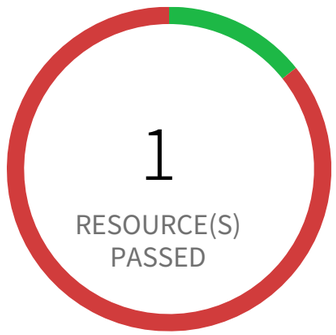
NOTE: This policy will trigger alert if you have at least one Cloudtrail with the multi trial is enabled, Logs all management events in your account and is not set with specific log metric filter and alarm.

First Seen March 18, 2021 at 11:01:09 AM UTC | **Resource Type** Other

Recommendations

1. Sign in to AWS Console
2. Navigate to CloudWatch dashboard
3. Click on 'Log groups' in the 'Logs' section (Left panel)
4. Select the log group created for your CloudTrail trail event logs (CloudTrail should be multi trail enabled with all management events captured) and click 'Create Metric Filter' button.
5. In 'Define Logs Metric Filter' page, add 'Filter pattern' value as
{ ($.errorCode = "*UnauthorizedOperation") || ($.errorCode = "AccessDenied*") }
and Click on 'Assign Metric'
6. In 'Create Metric Filter and Assign a Metric' page, Choose Filter Name, Metric Details parameter according to your requirement and click on 'Create Filter'
7. Click on 'Create Alarm',
- In Step 1 specify metric details and conditions details as required and click on 'Next'
- In Step 2 Select an SNS topic either by creating a new topic or use existing SNS topic/ARN and click on 'Next'
- In Step 3 Select name and description to alarm and click on 'Next'
- In Step 4 Preview your data entered and click on 'Create Alarm'

ACCESS CONTROL / Section Account Management | Automated Audit Actions



6 Resource(s) Failed

035297560255, 016671749923, 197802673547, 154600454722, 240075317252, 673174758328

Compliance Section: Account Management | Automated Audit Actions — Informational

Automatically audit account creation, modification, enabling, disabling, and removal actions.

AWS Log metric filter and alarm does not exist for S3 bucket policy changes

This policy identifies the AWS regions which do not have a log metric filter and alarm for S3 bucket policy changes. Monitoring changes to S3 bucket policies may reduce time to detect and correct permissive policies on sensitive S3 buckets. It is recommended that a metric filter and alarm be established for changes to S3 bucket policies.

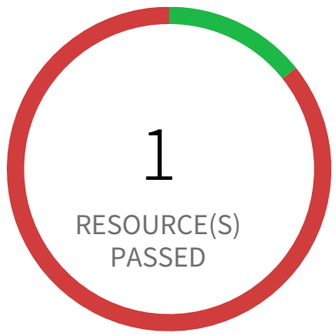
NOTE: This policy will trigger alert if you have at least one Cloudtrail with the multi trial is enabled, Logs all management events in your account and is not set with specific log metric filter and alarm.

First Seen March 18, 2021 at 11:01:09 AM UTC | **Resource Type** Other

Recommendations

1. Sign in to AWS Console
2. Navigate to CloudWatch dashboard
3. Click on 'Log groups' in the 'Logs' section (Left panel)
4. Select the log group created for your CloudTrail trail event logs (CloudTrail should be multi trail enabled with all management events captured) and click 'Create Metric Filter' button.
5. In 'Define Logs Metric Filter' page, add 'Filter pattern' value as
{ ($.eventSource = s3.amazonaws.com) && (($.eventName = PutBucketAcl) || ($.eventName = PutBucketPolicy) || ($.eventName = PutBucketCors) || ($.eventName = PutBucketLifecycle) || ($.eventName = PutBucketReplication) || ($.eventName = DeleteBucketPolicy) || ($.eventName = DeleteBucketCors) || ($.eventName = DeleteBucketLifecycle) || ($.eventName = DeleteBucketReplication)) }
and Click on 'Assign Metric'
6. In 'Create Metric Filter and Assign a Metric' page, Choose Filter Name, Metric Details parameter according to your requirement and click on 'Create Filter'
7. Click on 'Create Alarm',
- In Step 1 specify metric details and conditions details as required and click on 'Next'
- In Step 2 Select an SNS topic either by creating a new topic or use existing SNS topic/ARN and click on 'Next'
- In Step 3 Select name and description to alarm and click on 'Next'
- In Step 4 Preview your data entered and click on 'Create Alarm'

ACCESS CONTROL / Section Account Management | Automated Audit Actions



6 Resource(s) Failed

035297560255, 016671749923, 197802673547, 154600454722, 240075317252, 673174758328

Compliance Section: Account Management | Automated Audit Actions — Informational

Automatically audit account creation, modification, enabling, disabling, and removal actions.

AWS Log metric filter and alarm does not exist for Network gateways changes

This policy identifies the AWS regions which do not have a log metric filter and alarm for Network gateways changes. Monitoring changes to network gateways will help ensure that all ingress/egress traffic traverses the VPC border via a controlled path. It is recommended that a metric filter and alarm be established for changes to network gateways.

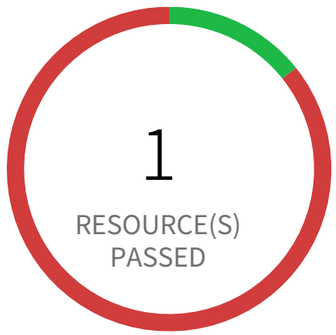
NOTE: This policy will trigger alert if you have at least one Cloudtrail with the multi trial is enabled, Logs all management events in your account and is not set with specific log metric filter and alarm.

First Seen March 18, 2021 at 11:01:09 AM UTC | **Resource Type** Other

Recommendations

1. Sign in to AWS Console
2. Navigate to CloudWatch dashboard
3. Click on 'Log groups' in the 'Logs' section (Left panel)
4. Select the log group created for your CloudTrail trail event logs (CloudTrail should be multi trail enabled with all management events captured) and click 'Create Metric Filter' button.
5. In 'Define Logs Metric Filter' page, add 'Filter pattern' value as
{ ($.eventName = CreateCustomerGateway) || ($.eventName = DeleteCustomerGateway) || ($.eventName = AttachInternetGateway) || ($.eventName = CreateInternetGateway) || ($.eventName = DeleteInternetGateway) || ($.eventName = DetachInternetGateway) }
and Click on 'Assign Metric'
6. In 'Create Metric Filter and Assign a Metric' page, Choose Filter Name, Metric Details parameter according to your requirement and click on 'Create Filter'
7. Click on 'Create Alarm',
- In Step 1 specify metric details and conditions details as required and click on 'Next'
- In Step 2 Select an SNS topic either by creating a new topic or use existing SNS topic/ARN and click on 'Next'
- In Step 3 Select name and description to alarm and click on 'Next'
- In Step 4 Preview your data entered and click on 'Create Alarm'

ACCESS CONTROL / Section Account Management | Automated Audit Actions



6 Resource(s) Failed

035297560255, 016671749923, 197802673547, 154600454722, 240075317252, 673174758328

Compliance Section: Account Management | Automated Audit Actions — Informational

Automatically audit account creation, modification, enabling, disabling, and removal actions.

AWS Log metric filter and alarm does not exist for AWS Config configuration changes

This policy identifies the AWS regions which do not have a log metric filter and alarm for AWS Config configuration changes. Monitoring changes to AWS Config configuration will help ensure sustained visibility of configuration items within the AWS account. It is recommended that a metric filter and alarm be established for detecting changes to AWS Config's configurations.

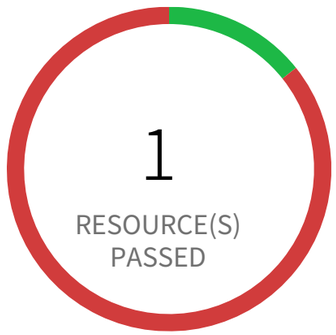
NOTE: This policy will trigger alert if you have at least one Cloudtrail with the multi trial is enabled, Logs all management events in your account and is not set with specific log metric filter and alarm.

First Seen March 18, 2021 at 11:01:09 AM UTC | **Resource Type** Other

Recommendations

1. Sign in to AWS Console
2. Navigate to CloudWatch dashboard
3. Click on 'Log groups' in the 'Logs' section (Left panel)
4. Select the log group created for your CloudTrail trail event logs (CloudTrail should be multi trail enabled with all management events captured) and click 'Create Metric Filter' button.
5. In 'Define Logs Metric Filter' page, add 'Filter pattern' value as
{ ($.eventSource = config.amazonaws.com) && (($.eventName=StopConfigurationRecorder)||($.eventName=DeleteDeliveryChannel)||($.eventName=PutDeliveryChannel)||($.eventName=PutConfigurationRecorder)) }
and Click on 'Assign Metric'
6. In 'Create Metric Filter and Assign a Metric' page, Choose Filter Name, Metric Details parameter according to your requirement and click on 'Create Filter'
7. Click on 'Create Alarm',
- In Step 1 specify metric details and conditions details as required and click on 'Next'
- In Step 2 Select an SNS topic either by creating a new topic or use existing SNS topic/ARN and click on 'Next'
- In Step 3 Select name and description to alarm and click on 'Next'
- In Step 4 Preview your data entered and click on 'Create Alarm'

ACCESS CONTROL / Section Account Management | Automated Audit Actions



6 Resource(s) Failed

035297560255, 016671749923, 197802673547, 154600454722, 240075317252, 673174758328

Compliance Section: Account Management | Automated Audit Actions — Informational

Automatically audit account creation, modification, enabling, disabling, and removal actions.

AWS Log metric filter and alarm does not exist for VPC changes

This policy identifies the AWS regions which do not have a log metric filter and alarm for VPC changes. Monitoring changes to VPC will help ensure that resources and services are not unintentionally exposed. It is recommended that a metric filter and alarm be established for changes made to VPCs.

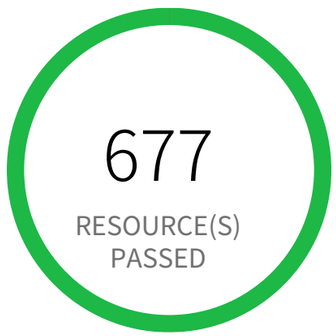
NOTE: This policy will trigger alert if you have at least one Cloudtrail with the multi trial is enabled, Logs all management events in your account and is not set with specific log metric filter and alarm.

First Seen March 18, 2021 at 11:01:09 AM UTC | **Resource Type** Other

Recommendations

1. Sign in to AWS Console
2. Navigate to CloudWatch dashboard
3. Click on 'Log groups' in the 'Logs' section (Left panel)
4. Select the log group created for your CloudTrail trail event logs (CloudTrail should be multi trail enabled with all management events captured) and click 'Create Metric Filter' button.
5. In 'Define Logs Metric Filter' page, add 'Filter pattern' value as
{ ($.eventName = CreateVpc) || ($.eventName = DeleteVpc) || ($.eventName = ModifyVpcAttribute) || ($.eventName = AcceptVpcPeeringConnection) || ($.eventName = CreateVpcPeeringConnection) || ($.eventName = DeleteVpcPeeringConnection) || ($.eventName = RejectVpcPeeringConnection) || ($.eventName = AttachClassicLinkVpc) || ($.eventName = DetachClassicLinkVpc) || ($.eventName = DisableVpcClassicLink) || ($.eventName = EnableVpcClassicLink) }
and Click on 'Assign Metric'
6. In 'Create Metric Filter and Assign a Metric' page, Choose Filter Name, Metric Details parameter according to your requirement and click on 'Create Filter'
7. Click on 'Create Alarm',
- In Step 1 specify metric details and conditions details as required and click on 'Next'
- In Step 2 Select an SNS topic either by creating a new topic or use existing SNS topic/ARN and click on 'Next'
- In Step 3 Select name and description to alarm and click on 'Next'
- In Step 4 Preview your data entered and click on 'Create Alarm'

ACCESS CONTROL / Section Access Enforcement | Role-based Access Control



0 Resource(s) Failed

Compliance Section: Access Enforcement | Role-based Access Control

Medium

Enforce a role-based access control policy over defined subjects and objects and control access based upon [Assignment: organization-defined roles and users authorized to assume such roles].

AWS IAM policy allows assume role permission across all services

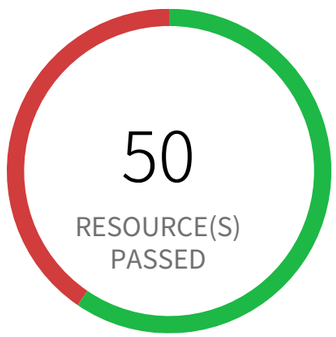
This policy identifies AWS IAM policy which allows assume role permission across all services. Typically, AssumeRole is used if you have multiple accounts and need to access resources from each account then you can create long term credentials in one account and then use temporary security credentials to access all the other accounts by assuming roles in those accounts.

First Seen N/A | **Resource Type** IAM Policy

Recommendations

1. Log in to the AWS Console
2. Navigate to the 'IAM' service.
3. Identify the reported policy
4. Change the Service element of the policy document to be more restrictive so that it only allows AssumeRole permission on select services.

ACCESS CONTROL / Section Access Enforcement | Role-based Access Control



34 Resource(s) Failed

kfirdaus-ec2, private-ec2, i-0da0289306d19adfc, i-05c9f7d4f427571a9, i-0859ea5792dcd86c4, i-055e923769104c3e1, i-03d553b23e20e382d, i-04756a64205372363, i-0aa331398f2ad7b30, i-021929ecd65f14543 & 24 more

Compliance Section: Access Enforcement | Role-based Access Control

Informational

Enforce a role-based access control policy over defined subjects and objects and control access based upon [Assignment: organization-defined roles and users authorized to assume such roles].

AWS EC2 Instance IAM Role not enabled

AWS provides Identity Access Management (IAM) roles to securely access AWS services and resources. The role is an identity with permission policies that define what the identity can and cannot do in AWS. As a best practice, create IAM roles and attach the role to manage EC2 instance permissions securely instead of distributing or sharing keys or passwords.

First Seen June 11, 2020 at 5:27:28 PM UTC | **Resource Type** Other

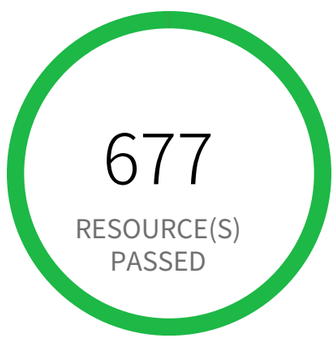
Recommendations

The most common setup is the AWS default that allows for EC2 access to AWS Services. For most, this is a great way to realize flexible, yet secure, EC2 access enabled for your instances. Select this when you launch EC2 instances to automatically inherit these permissions.

IAM
1. Go to the AWS console IAM dashboard.
2. In the navigation pane, choose Roles, Create new role.
3. Under 'Choose the service that will use this role' select EC2, then 'Next:Permissions.'
4. On the Attach permissions policies page, select an AWS managed policy that grants your instance access to the resources that they need, then 'Next:Tags.'
5. Add tags (optional), the select 'Next:Review.'
6. On the Create role and Review page, type a name for the role and choose Create role.

EC2
1. Go to the AWS console EC2 dashboard.
2. Select Running Instances.
3. Check the instance you want to modify.
4. From the Actions pull down menu, select Instance Settings and Attach/Replace IAM Role.
5. On the Attach/Replace IAM Role page, under the IAM role pull down menu, choose the role created in the IAM steps above.

ACCESS CONTROL / Section Least Privilege



0 Resource(s) Failed

Compliance Section: Least Privilege

Informational

Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

AWS IAM support access policy is not associated to any role

This policy identifies IAM policies with support role access which are not attached to any role for an account. AWS provides a support centre that can be used for incident notification and response, as well as technical support and customer services.

First Seen N/A | **Resource Type** Other

Recommendations

1. Log in to AWS console
2.Go to service IAM under Services panel.
3.From left panel click on 'Policies'
4.Search for the existence of a support policy 'AWSSupportAccess'
5.Create a IAM role
6.Attach 'AWSSupportAccess' managed policy to the created IAM role

ACCESS CONTROL / Section Least Privilege

0 Resource(s) Failed

Compliance Section: Least Privilege

Medium

Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

AWS ECS Fargate task definition root user found

This policy identifies AWS ECS Fargate task definition which has user name as root. As a best practice, the user name to use inside the container should not be root.

Note: This parameter is not supported for Windows containers.

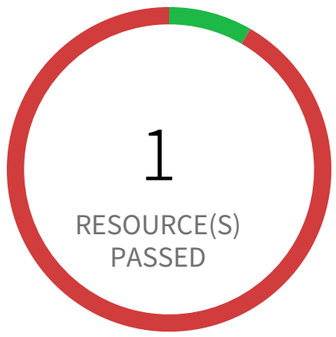
First Seen N/A | **Resource Type** Other

Recommendations

Create a task definition revision.

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

ACCESS CONTROL / Section Least Privilege



11 Resource(s) Failed

pcsdemo-tenant-automation, pcsdemo-compute-serverless-autodefend, pcsdemo-compute-ami-scanning, twistlock-se-demo-service-account, pcsdemo-provisioning-crypto-usecase, pcsdemo-UEBA-usecase, elad-azure-user1, elcohen@paloaltonetworks.com, test-iam, varun & 1 more

Compliance Section: Least Privilege

Low

Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

AWS IAM policy attached to users

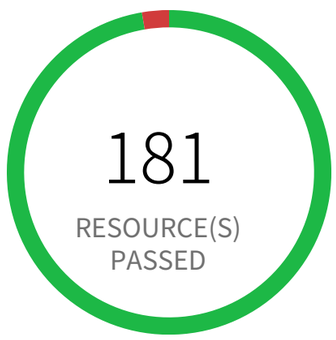
This policy identifies IAM policies attached to user. By default, IAM users, groups, and roles have no access to AWS resources. IAM policies are the means by which privileges are granted to users, groups, or roles. It is recommended that IAM policies be applied directly to groups but not users.

First Seen February 14, 2020 at 3:37:58 PM UTC | **Resource Type** IAM User Managed Policies

Recommendations

1. Sign in to the AWS Console
2. Navigate to the 'IAM' service.
3. Identify the users that were specifically assigned to the reported IAM policy.
4. If a group with a similar policy already exists, put the user into that group. If such a group does not exist, create a new group with relevant policy and assign the user to the group.

ACCESS CONTROL / Section Least Privilege



5 Resource(s) Failed

corporatemarketingcontent, human-resources-archive, productmarketingcontent, confidentialinformation, orc-public-bucket

Compliance Section: Least Privilege

Low

Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

AWS S3 bucket has global view ACL permissions enabled

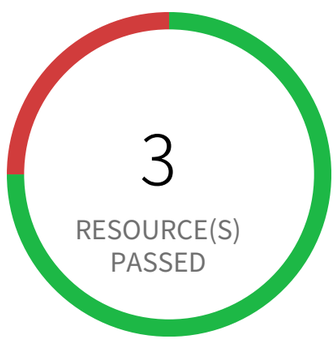
This policy determines if any S3 bucket(s) has Global View ACL permissions enabled for the All Users group. These permissions allow external resources to see the permission settings associated to the object.

First Seen January 28, 2019 at 5:26:07 PM UTC | **Resource Type** Other

Recommendations

1. Go to the AWS console S3 dashboard.
2. Select your bucket by clicking on the bucket name.
3. Select the Permissions tab and 'Access Control List.'
4. Under Public Access, select Everyone.
5. In the popup window, under Access to this bucket's ACL, uncheck 'Read bucket permissions' and Save.

ACCESS CONTROL / Section Least Privilege



1 Resource(s) Failed

*.pancloud.io

Compliance Section: Least Privilege

Low

Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

AWS ACM Certificate with wildcard domain name

This policy identifies ACM Certificates which are using wildcard certificates for wildcard domain name instead of single domain name certificates. ACM allows you to use an asterisk (*) in the domain name to create an ACM Certificate containing a wildcard name that can protect several sites in the same domain. For example, a wildcard certificate issued for *.prismacloud.io can match both www.prismacloud.io and images.prismacloud.io. When you use wildcard certificates, if the private key of a certificate is compromised, then all domain and subdomains that use the compromised certificate are potentially impacted. So it is recommended to use single domain name certificates instead of wildcard certificates to reduce the associated risks with a compromised domain or subdomain.

First Seen December 7, 2021 at 11:43:33 PM UTC | **Resource Type** Other

Recommendations

To resolve this alert, you have to replace the reported wildcard certificate with single domain name certificate for all the first-level sub-domains resulted from the domain name of the website secured with the wildcard certificate and delete the reported wildcard domain certificate.

To create a new certificate with a single domain:
1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to Certificate Manager
4. In 'Request a certificate' page,
a. On Step 1: 'Add domain names' page, in the 'Domain name' box, type the fully qualified domain name. Click on 'Next'
b. On Step 2: 'Select validation method' page, Select the validation method. Click on 'Review'
c. On Step 3: 'Review' page, review the domain name and validation method details. click on 'Confirm'
d. On Step 4: 'Validation' page, validate the certificate request based on the validation method selected. then click on 'Continue'
The certificate status should change from 'Pending validation' to 'Issued'. Now access your application's web server configuration and replace the wildcard certificate with the newly issued single domain name certificate.

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

ACCESS CONTROL / Section Least Privilege

0 Resource(s) Failed

Compliance Section: Least Privilege

Medium

Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

AWS ECS task definition elevated privileges enabled

This policy identifies the ECS containers that are having elevated privileges on the host container instance. When the Privileged parameter is true, the container is given elevated privileges on the host container instance (similar to the root user).

Note: This parameter is not supported for Windows containers or tasks using the Fargate launch type.

First Seen N/A | **Resource Type** Other

Recommendations

Create a task definition revision.

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

ACCESS CONTROL / Section Least Privilege

0 Resource(s) Failed

Compliance Section: Least Privilege

High

Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

AWS Access key enabled on root account

This policy identifies root accounts for which access keys are enabled. Access keys are used to sign API requests to AWS. Root accounts have complete access to all your AWS services. If the access key for a root account is compromised, an unauthorized users will have complete access to your AWS account.

First Seen N/A | **Resource Type** IAM Account Summary

Recommendations

1. Sign in to AWS Console as the root user.
2. Click root account name and on the top right select 'Security Credentials' from the dropdown.
3. For each key in 'Access Keys', click on "X" to delete the keys.

ACCESS CONTROL / Section Least Privilege

677
RESOURCE(S)
PASSED

0 Resource(s) Failed

Compliance Section: Least Privilege

Medium

Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

AWS IAM policy allows full administrative privileges

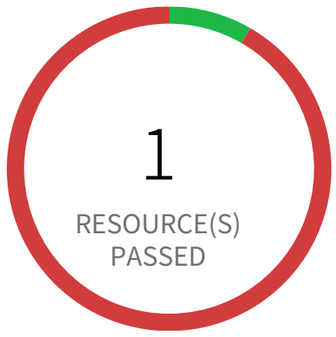
This policy identifies IAM policies with full administrative privileges. IAM policies are the means by which privileges are granted to users, groups, or roles. It is recommended and considered a standard security advice to grant least privilege like granting only the permissions required to perform a task. Determine what users need to do and then craft policies for them that let the users perform only those tasks, instead of allowing full administrative privileges.

First Seen N/A | **Resource Type** Other

Recommendations

1. Log in to the AWS Console
2. Navigate to the IAM dashboard
3. In the navigation pane, click on Policies and then search for the policy name reported
4. Select the policy, click on the 'Policy actions', select 'Detach'
5. Select all Users, Groups, Roles that have this policy attached, Click on 'Detach policy'

ACCESS CONTROL / Section Least Privilege | Privileged Access by Non-organizational Users



11 Resource(s) Failed

pcsdemo-tenant-automation, pcsdemo-compute-serverless-autodefend, pcsdemo-compute-ami-scanning, twistlock-se-demo-service-account, pcsdemo-provisioning-crypto-usecase, pcsdemo-UEBA-usecase, elad-azure-user1, elcohen@paloaltonetworks.com, test-iam, varun & 1 more

Compliance Section: Least Privilege | Privileged Access by Non-organizational Users

Low

Prohibit privileged access to the system by non-organizational users.

AWS IAM policy attached to users

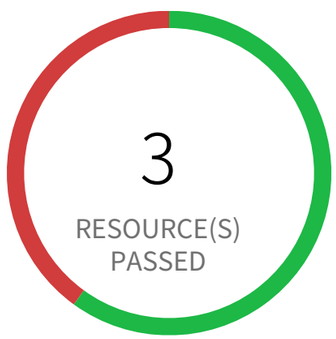
This policy identifies IAM policies attached to user. By default, IAM users, groups, and roles have no access to AWS resources. IAM policies are the means by which privileges are granted to users, groups, or roles. It is recommended that IAM policies be applied directly to groups but not users.

First Seen February 14, 2020 at 3:37:58 PM UTC | **Resource Type** IAM User Managed Policies

Recommendations

1. Sign in to the AWS Console
2. Navigate to the 'IAM' service.
3. Identify the users that were specifically assigned to the reported IAM policy.
4. If a group with a similar policy already exists, put the user into that group. If such a group does not exist, create a new group with relevant policy and assign the user to the group.

ACCESS CONTROL / Section System Use Notification



2 Resource(s) Failed

myinstance, paasdb

Compliance Section: System Use Notification

Medium

a. Display [Assignment: organization-defined system use notification message or banner] to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that:
1. Users are accessing a U.S. Government system;
2. System usage may be monitored, recorded, and subject to audit;
3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and
4. Use of the system indicates consent to monitoring and recording;
b. Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system; and
c. For publicly accessible systems:
1. Display system use information [Assignment: organization-defined conditions], before granting further access to the publicly accessible system;
2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
3. Include a description of the authorized uses of the system.

AWS RDS database instance is publicly accessible

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

First Seen October 16, 2018 at 8:02:27 PM UTC | **Resource Type** Other

Recommendations

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

ACCESS CONTROL / Section System Use Notification

0 Resource(s) Failed

Compliance Section: System Use Notification

Low

a. Display [Assignment: organization-defined system use notification message or banner] to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that:
1. Users are accessing a U.S. Government system;
2. System usage may be monitored, recorded, and subject to audit;
3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and
4. Use of the system indicates consent to monitoring and recording;
b. Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system; and
c. For publicly accessible systems:
1. Display system use information [Assignment: organization-defined conditions], before granting further access to the publicly accessible system;
2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
3. Include a description of the authorized uses of the system.

AWS RDS Snapshot with access for unmonitored cloud accounts

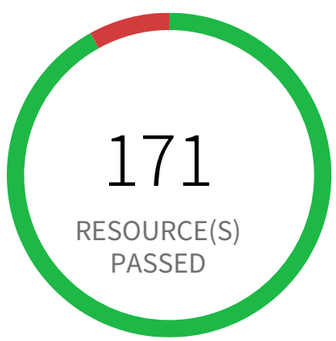
This policy identifies RDS snapshots with access for unmonitored cloud accounts. The RDS Snapshot which have either the read / write permission opened up for Cloud Accounts which are NOT part of Cloud Accounts monitored by Prisma Cloud. These accounts with read / write privileges should be reviewed and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

First Seen N/A | **Resource Type** Other

Recommendations

1. Sign into the AWS console.
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to the RDS service.
4. Select the identified 'RDS Snapshot' under the 'Snapshots' in the left hand menu.
5. Under the tab 'Snapshot Actions', selection the option 'Share Snapshot'.
6. Review and delete the AWS Accounts which should not have read access.

ACCESS CONTROL / Section System Use Notification



15 Resource(s) Failed

totalmess-s3-q4ns, corporatecontracts, corporatemarketingcontent, demo-bucket-publicly-exposed, human-resources-archive, foundry-vtt-ron-s3, productmarketingcontent, redlockpocprepdocs, confidentialinformation, orc-public-bucket & 5 more

Compliance Section: System Use Notification

Medium

a. Display [Assignment: organization-defined system use notification message or banner] to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that:
1. Users are accessing a U.S. Government system;
2. System usage may be monitored, recorded, and subject to audit;
3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and
4. Use of the system indicates consent to monitoring and recording;
b. Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system; and
c. For publicly accessible systems:
1. Display system use information [Assignment: organization-defined conditions], before granting further access to the publicly accessible system;
2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
3. Include a description of the authorized uses of the system.

AWS S3 buckets are accessible to public via ACL

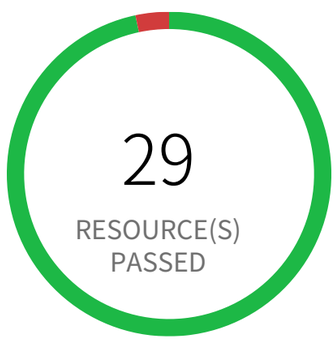
This policy identifies S3 buckets which are publicly accessible via ACL. Amazon S3 often used to store highly sensitive enterprise data and allowing public access to such S3 bucket through ACL would result in sensitive data being compromised. It is highly recommended to disable ACL configuration for all S3 buckets and use resource based policies to allow access to S3 buckets.

First Seen December 5, 2018 at 2:04:56 AM UTC | **Resource Type** Other

Recommendations

1. Login to the AWS Console
2. Navigate to the 'S3' service
3. Click on the 'S3' resource reported in the alert
4. Click on the 'Permissions'
5. If Access Control List' is set to 'Public' follow below steps
a. Under 'Access Control List', Click on 'Everyone' and uncheck all items
b. Click on Save

ACCESS CONTROL / Section System Use Notification



1 Resource(s) Failed

snap-0c77fc00f314d9a13

Compliance Section: System Use Notification

Medium

a. Display [Assignment: organization-defined system use notification message or banner] to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that:
1. Users are accessing a U.S. Government system;
2. System usage may be monitored, recorded, and subject to audit;
3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and
4. Use of the system indicates consent to monitoring and recording;
b. Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system; and
c. For publicly accessible systems:
1. Display system use information [Assignment: organization-defined conditions], before granting further access to the publicly accessible system;
2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
3. Include a description of the authorized uses of the system.

AWS EBS snapshots are accessible to public

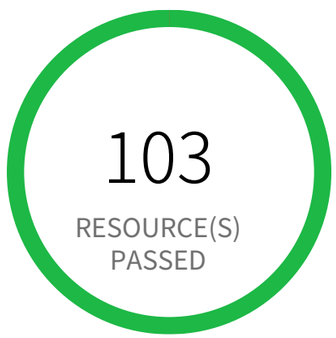
This policy identifies EC2 EBS snapshots which are accessible to public. Amazon Elastic Block Store (Amazon EBS) provides persistent block storage volumes for use with Amazon EC2 instances in the AWS Cloud. If EBS snapshots are inadvertently shared to public, any unauthorized user with AWS console access can gain access to the snapshots and gain access to sensitive data.

First Seen November 28, 2019 at 6:43:42 PM UTC | **Resource Type** Snapshot Settings

Recommendations

1. Log in to the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to 'EC2' service.
4. Under the 'Elastic Block Storage', click on the 'Snapshots'.
5. For the specific Snapshots, change the value of field 'Property' to 'Private'.
6. Under the section 'Encryption Details', set the value of 'Encryption Enabled' to 'Yes'.

ACCESS CONTROL / Section System Use Notification



0 Resource(s) Failed

Compliance Section: System Use Notification

Low

a. Display [Assignment: organization-defined system use notification message or banner] to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that:
1. Users are accessing a U.S. Government system;
2. System usage may be monitored, recorded, and subject to audit;
3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and
4. Use of the system indicates consent to monitoring and recording;
b. Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system; and
c. For publicly accessible systems:
1. Display system use information [Assignment: organization-defined conditions], before granting further access to the publicly accessible system;
2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
3. Include a description of the authorized uses of the system.

AWS Amazon Machine Image (AMI) is publicly accessible

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

First Seen N/A | **Resource Type** VM Image

Recommendations

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

ACCESS CONTROL / Section System Use Notification

0 Resource(s) Failed

Compliance Section: System Use Notification

Low

a. Display [Assignment: organization-defined system use notification message or banner] to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that:
1. Users are accessing a U.S. Government system;
2. System usage may be monitored, recorded, and subject to audit;
3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and
4. Use of the system indicates consent to monitoring and recording;
b. Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system; and
c. For publicly accessible systems:
1. Display system use information [Assignment: organization-defined conditions], before granting further access to the publicly accessible system;
2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
3. Include a description of the authorized uses of the system.

AWS EBS Snapshot with access for unmonitored cloud accounts

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

First Seen N/A | **Resource Type** Other

Recommendations

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

ACCESS CONTROL / Section System Use Notification

0 Resource(s) Failed

Compliance Section: System Use Notification

Medium

a. Display [Assignment: organization-defined system use notification message or banner] to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that:
1. Users are accessing a U.S. Government system;
2. System usage may be monitored, recorded, and subject to audit;
3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and
4. Use of the system indicates consent to monitoring and recording;
b. Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system; and
c. For publicly accessible systems:
1. Display system use information [Assignment: organization-defined conditions], before granting further access to the publicly accessible system;
2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
3. Include a description of the authorized uses of the system.

AWS RDS snapshots are accessible to public

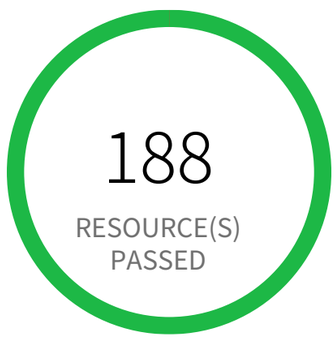
This policy identifies AWS RDS snapshots which are accessible to public. Amazon Relational Database Service (Amazon RDS) is a web service that makes it easier to setup and manage databases. If RDS snapshots are inadvertently shared to public, any unauthorized user with AWS console access can gain access to the snapshots and gain access to sensitive data.

First Seen N/A | **Resource Type** Managed Database Snapshot

Recommendations

1. Sign in to the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to the 'RDS' service.
4. For the RDS instance reported in the alert, change 'Publicly Accessible' setting to 'No'.

ACCESS CONTROL / Section System Use Notification



0 Resource(s) Failed

Compliance Section: System Use Notification

Low

a. Display [Assignment: organization-defined system use notification message or banner] to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that:
1. Users are accessing a U.S. Government system;
2. System usage may be monitored, recorded, and subject to audit;
3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and
4. Use of the system indicates consent to monitoring and recording;
b. Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system; and
c. For publicly accessible systems:
1. Display system use information [Assignment: organization-defined conditions], before granting further access to the publicly accessible system;
2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
3. Include a description of the authorized uses of the system.

AWS CloudTrail bucket is publicly accessible

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

First Seen N/A | **Resource Type** Other

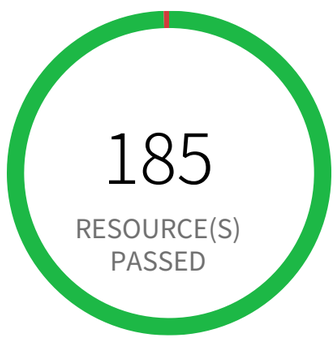
Recommendations

1. Login to the AWS Console
2. Navigate to the 'S3' service
3. Click on the 'S3' resource reported in the alert
4. Click on the 'Permissions'
5. If Access Control List' is set to 'Public' follow below steps
a. Under 'Access Control List', Click on 'Everyone' and uncheck all items
b. Click on Save
6. If 'Bucket Policy' is set to public follow below steps

a. Under 'Bucket Policy', modify the policy to remove public access
b. Click on Save
c. If 'Bucket Policy' is not required delete the existing 'Bucket Policy'.

Note: Make sure updating 'Access Control List' or 'Bucket Policy' does not affect S3 bucket data access.

ACCESS CONTROL / Section System Use Notification



1 Resource(s) Failed

demo-bucket-publicly-exposed

Compliance Section: System Use Notification

Medium

a. Display [Assignment: organization-defined system use notification message or banner] to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that:
1. Users are accessing a U.S. Government system;
2. System usage may be monitored, recorded, and subject to audit;
3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and
4. Use of the system indicates consent to monitoring and recording;
b. Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system; and
c. For publicly accessible systems:
1. Display system use information [Assignment: organization-defined conditions], before granting further access to the publicly accessible system;
2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
3. Include a description of the authorized uses of the system.

AWS S3 buckets are accessible to any authenticated user

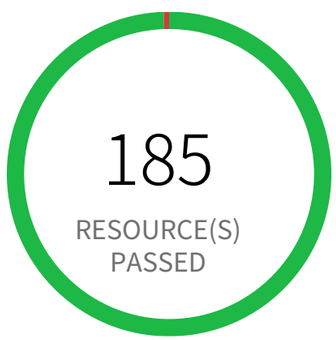
This policy identifies S3 buckets accessible to any authenticated AWS users. Amazon S3 allows customer to store and retrieve any type of content from anywhere in the web. Often, customers have legitimate reasons to expose the S3 bucket to public, for example to host website content. However, these buckets often contain highly sensitive enterprise data which if left accessible to anyone with valid AWS credentials, may result in sensitive data leaks.

First Seen November 28, 2021 at 10:35:20 PM UTC | **Resource Type** Other

Recommendations

1. Login to the AWS Console
2. Navigate to the 'S3' service
3. Click on the 'S3' resource reported in the alert
4. Click on the 'Permissions'
5. Under 'Public access', Click on 'Any AWS user' and uncheck all items
6. Click on Save

ACCESS CONTROL / Section System Use Notification



1 Resource(s) Failed

yuri-pipeline-test

Compliance Section: System Use Notification

Low

a. Display [Assignment: organization-defined system use notification message or banner] to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that:
1. Users are accessing a U.S. Government system;
2. System usage may be monitored, recorded, and subject to audit;
3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and
4. Use of the system indicates consent to monitoring and recording;
b. Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system; and
c. For publicly accessible systems:
1. Display system use information [Assignment: organization-defined conditions], before granting further access to the publicly accessible system;
2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
3. Include a description of the authorized uses of the system.

AWS S3 bucket accessible to unmonitored cloud accounts

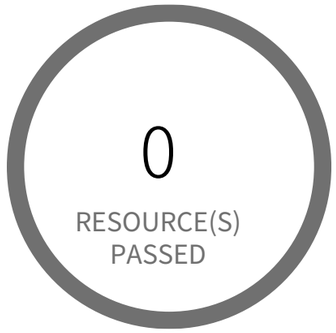
This policy identifies those S3 buckets which have either the read/write permission opened up for Cloud Accounts which are NOT part of Cloud Accounts monitored by Prisma Cloud. These accounts with read/write privileges should be reviewed and confirmed that these are valid accounts of your organization (or authorised by your organization) and are not active under Prisma Cloud monitoring.

First Seen August 2, 2023 at 9:12:30 PM UTC | **Resource Type** Other

Recommendations

1. Log in to the AWS Console
2. Navigate to the 'S3' service
3. Click on the reported S3 bucket
4. Click on the 'Permissions' tab
5. Navigate to the 'Access control list (ACL)' section and Click on the 'Edit'
6. Under 'Access for other AWS accounts', Add the Cloud Accounts that are monitored by Prisma Cloud
7. Click on 'Save changes'

ACCESS CONTROL / Section Remote Access | Protection of Confidentiality and Integrity Using Encryption



0 Resource(s) Failed

Compliance Section: Remote Access | Protection of Confidentiality and Integrity Using Encryption

Low

Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

AWS Redshift instances are not encrypted

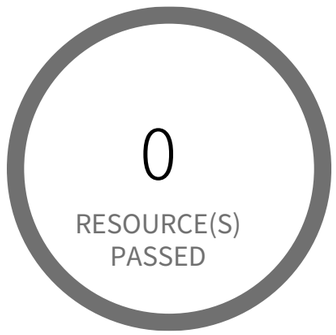
This policy identifies AWS Redshift instances which are not encrypted. These instances should be encrypted for clusters to help protect data at rest which otherwise can result in a data breach.

First Seen N/A | **Resource Type** Managed Database

Recommendations

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

ACCESS CONTROL / Section Remote Access | Protection of Confidentiality and Integrity Using Encryption



0 Resource(s) Failed

Compliance Section: Remote Access | Protection of Confidentiality and Integrity Using Encryption Low

Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

AWS EMR cluster is not enabled with local disk encryption

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

First Seen N/A | **Resource Type** Other

Recommendations

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

ACCESS CONTROL / Section Remote Access | Protection of Confidentiality and Integrity Using Encryption

5 Resource(s) Failed

myinstance, paasdb, apprds, pcsdemo-microseg-wordpress-mysql, database-1t

Compliance Section: Remote Access | Protection of Confidentiality and Integrity Using Encryption Low

Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

AWS RDS instance is not encrypted

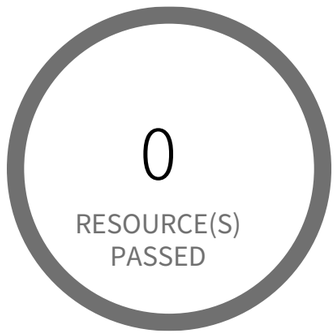
This policy identifies AWS RDS instances which are not encrypted. Amazon Relational Database Service (Amazon RDS) is a web service that makes it easier to set up and manage databases. Amazon allows customers to turn on encryption for RDS which is recommended for compliance and security reasons.

First Seen February 4, 2023 at 10:00:44 AM UTC | **Resource Type** Managed Database

Recommendations

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

ACCESS CONTROL / Section Remote Access | Protection of Confidentiality and Integrity Using Encryption



0 Resource(s) Failed

Compliance Section: Remote Access | Protection of Confidentiality and Integrity Using Encryption Low

Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

AWS EMR cluster is not enabled with data encryption at rest

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

First Seen N/A | **Resource Type** Other

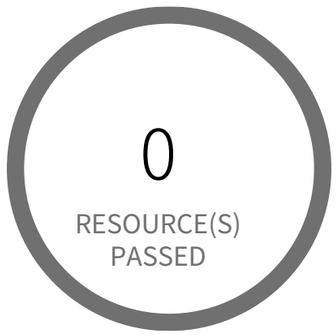
Recommendations

1. Login to the AWS Console.
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated.
3. Navigate to 'EMR' dashboard from 'Services' dropdown.
4. Go to 'Security configurations', click 'Create'.
5. On the Create security configuration window,
6. In 'Name' box, provide a name for the new EMR security configuration.
7. For encryption At Rest select the required encryption type ('S3 encryption'/'Local disk encryption'/both) and follow below link for enabling the same.
8. https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-encryption-enable.html

9. Click on 'Create' button.
10. On the left menu of EMR dashboard Click 'Clusters'.
11. Select the EMR cluster for which the alert has been generated and click on the 'Clone' button from the top menu.
12. In the Cloning popup, choose 'Yes' and Click 'Clone'.
13. On the Create Cluster page, in the Security Options section, click on 'security configuration'.
14. From the 'Security configuration' drop down select the name of the security configuration created at step 4 to step 8, click 'Create Cluster'.
15. Once you the new cluster is set up verify its working and terminate the source cluster in order to stop incurring charges for it.
16. On the left menu of EMR dashboard Click 'Clusters', from the list of clusters select the source cluster which is alerted.

17. Click on the 'Terminate' button from the top menu.
18. On the 'Terminate clusters' pop-up, click 'Terminate'.

ACCESS CONTROL / Section Remote Access | Protection of Confidentiality and Integrity Using Encryption



0 Resource(s) Failed

Compliance Section: Remote Access | Protection of Confidentiality and Integrity Using Encryption

Low

Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

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

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

First Seen N/A | **Resource Type** Other

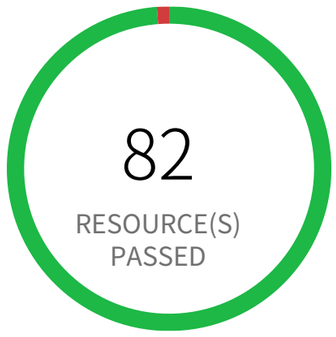
Recommendations

1. Login to the AWS Console.
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated.
3. Navigate to 'EMR' dashboard from 'Services' dropdown.
4. Go to 'Security configurations', click 'Create'.
5. On the Create security configuration window,
6. In 'Name' box, provide a name for the new EMR security configuration.
7. Under 'Local disk encryption', check the box 'Enable at-rest encryption for local disks'.
8. Select 'Custom' Key provider type from the 'Key provider type' dropdown list.
9. Follow the below link for creating the custom key,

https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-data-encryption-options.html
10. Click on 'Create' button.
11. On the left menu of EMR dashboard Click 'Clusters'.
12. Select the EMR cluster for which the alert has been generated and click on the 'Clone' button from the top menu.
13. In the Cloning popup, choose 'Yes' and Click 'Clone'.
14. On the Create Cluster page, in the Security Options section, click on 'security configuration'.
15. From the 'Security configuration' drop down select the name of the security configuration created at step 4 to step 8, click 'Create Cluster'.
16. Once the new cluster is set up verify its working and terminate the source cluster.

17. On the left menu of EMR dashboard Click 'Clusters', from the list of clusters select the source cluster which is alerted.
18. Click on the 'Terminate' button from the top menu.
19. On the 'Terminate clusters' pop-up, click 'Terminate'.

ACCESS CONTROL / Section Remote Access | Protection of Confidentiality and Integrity Using Encryption



1 Resource(s) Failed

bar-remediation-queue

Compliance Section: Remote Access | Protection of Confidentiality and Integrity Using Encryption

Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

Informational

AWS SQS queue encryption using default KMS key instead of CMK

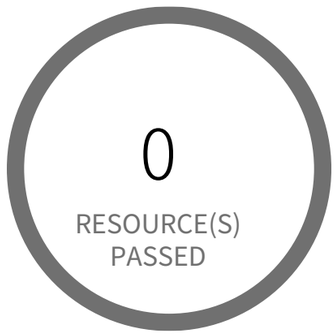
This policy identifies SQS queues which are encrypted with default KMS keys and not with Customer Master Keys(CMKs). It is a best practice to use customer managed Master Keys to encrypt your SQS queue messages. It gives you full control over the encrypted messages data.

First Seen June 29, 2021 at 3:18:58 PM UTC | **Resource Type** Other

Recommendations

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

ACCESS CONTROL / Section Remote Access | Protection of Confidentiality and Integrity Using Encryption



0 Resource(s) Failed

Compliance Section: Remote Access | Protection of Confidentiality and Integrity Using Encryption Low

Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

AWS EMR cluster is not enabled with data encryption in transit

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

First Seen N/A | **Resource Type** Other

Recommendations

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

17. Click on the 'Terminate' button from the top menu.
18. On the 'Terminate clusters' pop-up, click 'Terminate'.

ACCESS CONTROL / Section Remote Access | Protection of Confidentiality and Integrity Using Encryption

1 Resource(s) Failed

Allow All

Compliance Section: Remote Access | Protection of Confidentiality and Integrity Using Encryption

Low

Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

AWS EKS cluster security group overly permissive to all traffic

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

First Seen June 13, 2023 at 8:48:36 PM UTC | **Resource Type** Other

Recommendations

Before making any changes, please check the impact on your applications/services. If the Security Group reported indeed need to restrict all traffic, follow the instructions below:
1. Log in to the AWS console
2. Navigate to the 'VPC' service
3. Select the 'Security Group' reported in the alert
4. Click on 'Inbound Rules'
5. Remove the rule which has the 'Source' value as 0.0.0.0/0 or ::/0

ACCESS CONTROL / Section Remote Access | Protection of Confidentiality and Integrity Using Encryption

0 Resource(s) Failed

Informational

Compliance Section: Remote Access | Protection of Confidentiality and Integrity Using Encryption

Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

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

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

First Seen N/A | **Resource Type** Other

Recommendations

RDS DB clusters can be encrypted only while creating the database cluster. You can't convert an unencrypted DB cluster to an encrypted one. However, you can restore an unencrypted Aurora DB cluster snapshot to an encrypted Aurora DB cluster. To do this, specify a KMS encryption key when you restore from the unencrypted DB cluster snapshot.

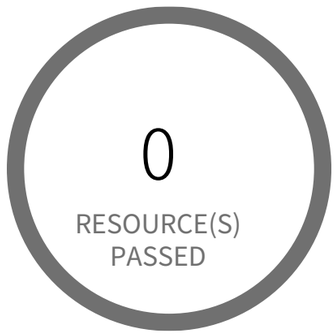
Step 1: To create a 'Snapshot' of the unencrypted DB cluster,
https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/USER_CreateSnapshotCluster.html
NOTE: As you can't restore from a DB cluster snapshot to an existing DB cluster; a new DB cluster is created when you restore. Once the Snapshot status is 'Available'.

Step 2: Follow the below link to restoring the Cluster from a DB Cluster Snapshot,
https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/USER_RestoreFromSnapshot.html

Once the DB cluster is restored and verified, follow below steps to delete the reported DB cluster,
1. Log in to the AWS Management Console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated.
3. Navigate to 'RDS' dashboard from 'Services' dropdown
4. In the navigation pane, choose ‘Databases’
5. In the list of DB instances, choose a writer instance for the DB cluster
6. Choose 'Actions', and then choose 'Delete'

FMI:
1. While deleting a RDS DB cluster, customer has to disable 'Enable deletion protection' otherwise instance cannot be deleted
2. While deleting RDS DB instance , AWS application will ask the end user to take Final snapshot
3. If a RDS DB cluster has a writer role instance, then User has to delete the write instance to delete the main cluster (Delete option won’t be enabled for main RDS DB cluster)

ACCESS CONTROL / Section Remote Access | Protection of Confidentiality and Integrity Using Encryption



0 Resource(s) Failed

Compliance Section: Remote Access | Protection of Confidentiality and Integrity Using Encryption

Low

Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

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

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

First Seen N/A | **Resource Type** Other

Recommendations

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

ACCESS CONTROL / Section Remote Access | Protection of Confidentiality and Integrity Using Encryption

104 Resource(s) Failed

035297560255:EBS:ap-southeast-1,
035297560255:EBS:ap-south-1,
035297560255:EBS:eu-west-1,
035297560255:EBS:eu-central-1,
035297560255:EBS:eu-west-2,
035297560255:EBS:us-east-2,
035297560255:EBS:eu-north-1,
035297560255:EBS:ap-northeast-1,
035297560255:EBS:ap-northeast-3,
035297560255:EBS:us-west-2 & 94 more

Compliance Section: Remote Access | Protection of Confidentiality and Integrity Using Encryption low

Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

AWS EBS volume region with encryption is disabled

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

First Seen November 2, 2021 at 9:19:13 AM UTC | **Resource Type** Other

Recommendations

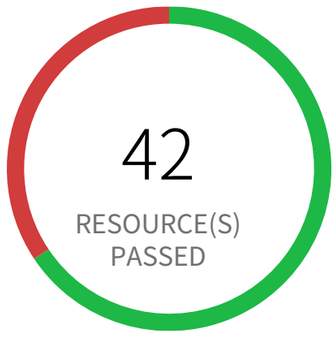
To enable encryption at region level by default, follow below URL:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html#encryption-by-default

Additional Information:

To detect existing EBS volumes that are not encrypted ; refer Saved Search:
AWS EBS volumes are not encrypted_RL

To detect existing EBS volumes that are not encrypted with CMK, refer Saved Search:
AWS EBS volume not encrypted using Customer Managed Key_RL

ACCESS CONTROL / Section Remote Access | Protection of Confidentiality and Integrity Using Encryption



22 Resource(s) Failed

rds:pcsdemo-microseg-word-press-mysql-2024-02-11-10-26,
rds:pcsdemo-microseg-word-press-mysql-2024-02-10-10-26,
rds:pcsdemo-microseg-word-press-mysql-2024-02-12-10-26,
rds:pcsdemo-microseg-word-press-mysql-2024-02-09-10-26,
rds:pcsdemo-microseg-word-press-mysql-2024-02-06-10-27,
rds:pcsdemo-microseg-word-press-mysql-2024-02-05-10-26,
rds:pcsdemo-microseg-word-press-mysql-2024-02-10-13-12,
rds:myinstance-2024-02-13-07-17,…

Compliance Section: Remote Access | Protection of Confidentiality and Integrity Using Encryption

Low

Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

AWS RDS DB snapshot is not encrypted

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

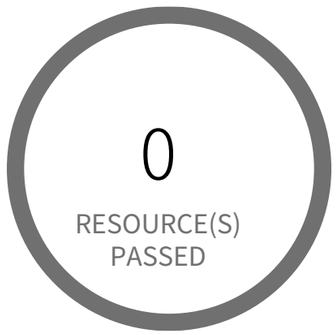
First Seen February 5, 2024 at 9:08:20 AM UTC | **Resource Type** Other

Recommendations

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

The source snapshot needs to be removed once the copy is available.
Note: If you delete a source snapshot before the target snapshot becomes available, the snapshot copy may fail. Verify that the target snapshot has a status of AVAILABLE before you delete a source snapshot.

ACCESS CONTROL / Section Remote Access | Protection of Confidentiality and Integrity Using Encryption



0 Resource(s) Failed

Compliance Section: Remote Access | Protection of Confidentiality and Integrity Using Encryption Low

Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

AWS ElastiCache Redis cluster with encryption for data at rest disabled

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

First Seen N/A | **Resource Type** Other

Recommendations

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

To create new ElastiCache Redis cluster with at-rest encryption set, perform the following:
1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to ElastiCache Dashboard
4. Click on Redis
5. Click on 'Create' button
6. On the 'Create your Amazon ElastiCache cluster' page,
a. Select 'Redis' cache engine type.
b. Enter a name for the new cache cluster
c. Select Redis engine version from 'Engine version compatibility' dropdown list.
Note: As of July 2018, In-transit encryption can be enabled only for AWS ElastiCache clusters with Redis engine version 3.2.6 and 4.0.10.
d. Click on 'Advanced Redis settings' to expand the cluster advanced settings panel
e. Select 'Encryption at-rest' checkbox to enable encryption along with other necessary parameters
7. Click on 'Create' button to launch your new ElastiCache Redis cluster

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

ACCESS CONTROL / Section Remote Access | Protection of Confidentiality and Integrity Using Encryption

0 Resource(s) Failed

Compliance Section: Remote Access | Protection of Confidentiality and Integrity Using Encryption

low

Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

AWS route table with VPC peering overly permissive to all traffic

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

First Seen N/A | **Resource Type** Other

Recommendations

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

ACCESS CONTROL / Section Remote Access | Protection of Confidentiality and Integrity Using Encryption

0 Resource(s) Failed

Compliance Section: Remote Access | Protection of Confidentiality and Integrity Using Encryption

Low

Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

AWS SSM Parameter is not encrypted

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

First Seen N/A | **Resource Type** Other

Recommendations

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

ACCESS CONTROL / Section Remote Access | Protection of Confidentiality and Integrity Using Encryption

0 Resource(s) Failed

Compliance Section: Remote Access | Protection of Confidentiality and Integrity Using Encryption

Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

Low

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

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

First Seen N/A | **Resource Type** Other

Recommendations

AWS EFS Encryption of data at rest can only be enabled during file system creation. So to resolve this alert, create a new EFS with encryption enabled, then migrate all required file data from the reported EFS to this newly created EFS and delete reported EFS.

To create a new EFS with encryption enabled, perform the following:
1. Sign in to the AWS console
2. In the console, select the specific region from the region drop-down on the top right corner, for which the alert is generated
3. Navigate to the EFS dashboard
4. Click on 'File systems' (Left Panel)
5. Click on the 'Create file system' button
6. On the 'Create file system' pop-up window,
7. Click on 'Customize' button to replicate the configurations of alerted file system as required
8. Ensure 'Enable encryption of data at rest' is selected
9. On the 'Review and create' step, Review all your setting and click on the 'Create' button

To delete reported EFS which does not has encryption, perform the following:
1. Sign in to the AWS console
2. In the console, select the specific region from the region drop-down on the top right corner, for which the alert is generated
3. Navigate to the EFS dashboard
4. Click on 'File systems' (Left Panel)
5. Select the reported file system

6. Click on 'Delete' button
7. In the 'Delete file system' popup box, To confirm the deletion enter the file system's ID and Click on 'Confirm'

ACCESS CONTROL / Section Remote Access | Protection of Confidentiality and Integrity Using Encryption

0 Resource(s) Failed

Informational

Compliance Section: Remote Access | Protection of Confidentiality and Integrity Using Encryption

Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

AWS RDS database not encrypted using Customer Managed Key

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

First Seen N/A | **Resource Type** Other

Recommendations

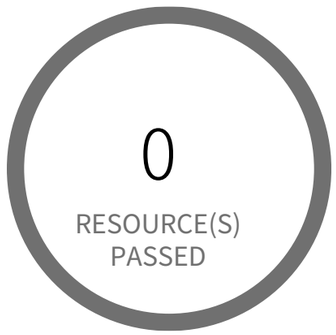
Because you can set AWS RDS database encryption only during database creation, the process for resolving this alert requires you to create a new RDS database with a customer managed key for encryption, migrate the data from the reported database to this newly created database, and delete the RDS database identified in the alert.

To create a new RDS database with encryption using a customer managed key:
1. Log in to the AWS console.
2. Select the region for which the alert was generated.
3. Navigate to the Amazon RDS Dashboard.
4. Select 'Create database'.
5. On the 'Select engine' page, select 'Engine options' and 'Next'.
6. On the 'Choose use case' page, select 'Use case' of database and 'Next'.
7. On the 'Specify DB details' page, specify the database details you need and click 'Next'.
Note: Amazon RDS encryption has some limitation on region and type instances. For Availability of Amazon RDS Encryption refer to: https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html#Overview.Encryption.Availability
8. On the 'Configure advanced settings' page, Under 'Encryption', select 'Enable encryption' and select the customer managed key [i.e. Other than (default)aws/rds] from 'Master key' dropdown list].
9. Select 'Create database'.

To delete the RDS database that uses the default KMS keys, which triggered the alert:
1. Log in to the AWS console

2. Select the region for which the alert was generated.
3. Navigate to the Amazon RDS Dashboard.
4. Click on Instances, and select the reported RDS database.
5. Select the 'Instance actions' drop-down and click 'Delete'.
7. In the 'Delete' dialog, select the 'Create final snapshot?' checkbox, if you want a backup. Provide a name for the final snapshot, confirm deletion and select 'Delete'.

ACCESS CONTROL / Section Remote Access | Protection of Confidentiality and Integrity Using Encryption



0 Resource(s) Failed

Informational

Compliance Section: Remote Access | Protection of Confidentiality and Integrity Using Encryption

Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

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

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

First Seen N/A | **Resource Type** Other

Recommendations

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

ACCESS CONTROL / Section Remote Access | Protection of Confidentiality and Integrity Using Encryption

0 Resource(s) Failed

Informational

Compliance Section: Remote Access | Protection of Confidentiality and Integrity Using Encryption

Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

AWS Redshift Cluster not encrypted using Customer Managed Key

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

First Seen N/A | **Resource Type** Other

Recommendations

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

ACCESS CONTROL / Section Remote Access | Protection of Confidentiality and Integrity Using Encryption

1 Resource(s) Failed

paasdb-cluster

Compliance Section: Remote Access | Protection of Confidentiality and Integrity Using Encryption

Low

Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

AWS RDS DB cluster encryption is disabled

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

First Seen July 17, 2022 at 12:04:20 PM UTC | **Resource Type** Other

Recommendations

AWS DB clusters can be encrypted only while creating the database cluster. You can't convert an unencrypted DB cluster to an encrypted one. However, you can restore an unencrypted Aurora DB cluster snapshot to an encrypted Aurora DB cluster. To do this, specify a KMS encryption key when you restore from the unencrypted DB cluster snapshot.

For AWS RDS,
1. To create a 'Snapshot' of the unencrypted DB cluster, follow the instruction mentioned in below link:
RDS Link: https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/USER_CreateSnapshotCluster.html

NOTE: As you can't restore from a DB cluster snapshot to an existing DB cluster; a new DB cluster is created when you restore. Once the Snapshot status is 'Available', delete the unencrypted DB cluster before restoring from the DB cluster Snapshot by following below steps for AWS RDS,
a. Sign to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/
b. In the navigation pane, choose 'Databases'.
c. In the list of DB instances, choose a writer instance for the DB cluster.
d. Choose 'Actions', and then choose 'Delete'.

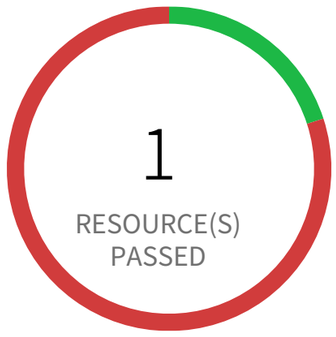
2. To restoring the Cluster from a DB Cluster Snapshot, follow the instruction mentioned in below link:
RDS Link: https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/USER_RestoreFromSnapshot.html

For AWS Document DB,
1. To create a 'Snapshot' of the unencrypted DB cluster, follow the instruction mentioned in below link:
Document DB Link: https://docs.aws.amazon.com/documentdb/latest/developerguide/backup_restore-create_manual_cluster_snapshot.html

NOTE: As you can't restore from a DB cluster snapshot to an existing DB cluster; a new DB cluster is created when you restore. Once the Snapshot status is 'Available', delete the unencrypted DB cluster before restoring from the DB cluster Snapshot by following below steps for AWS Document DB,
a. Sign to the AWS Management Console and open the Amazon DocumentDB console at https://console.aws.amazon.com/docdb/
b. In the navigation pane, choose 'Clusters'.
c. Select the cluster from the list which needs to be deleted
d. Choose 'Actions', and then choose 'Delete'.

2. To restoring the Cluster from a DB Cluster Snapshot, follow the instruction mentioned in below link:
Document DB Link: https://docs.aws.amazon.com/documentdb/latest/developerguide/backup_restore-restore_from_snapshot.html

ACCESS CONTROL / Section Remote Access | Protection of Confidentiality and Integrity Using Encryption



4 Resource(s) Failed

CorporateDynamoTable, indexed-docs, my-pool-party-users-bathers, yaron_testing_dynamo

Informational

Compliance Section: Remote Access | Protection of Confidentiality and Integrity Using Encryption

Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

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

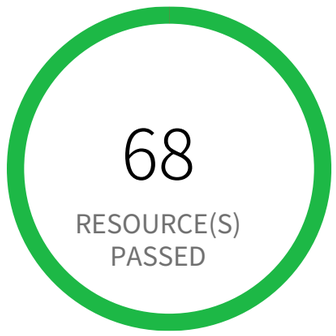
This policy identifies the DynamoDB tables that use AWS owned CMK (default) instead of AWS managed CMK (KMS) to encrypt data. AWS managed CMK provide additional features such as the ability to view the CMK and key policy, and audit the encryption and decryption of DynamoDB tables.

First Seen July 23, 2019 at 7:24:43 AM UTC | **Resource Type** Other

Recommendations

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

ACCESS CONTROL / Section Remote Access | Protection of Confidentiality and Integrity Using Encryption



0 Resource(s) Failed

Informational

Compliance Section: Remote Access | Protection of Confidentiality and Integrity Using Encryption

Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

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

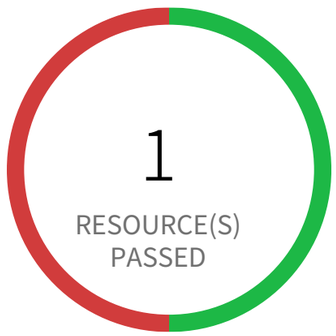
This policy identifies Elastic Load Balancers (ELB) which have security group with no inbound rules. A security group with no inbound rule will deny all incoming requests. ELB security groups should have at least one inbound rule, ELB with no inbound permissions will deny all traffic incoming to ELB;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

First Seen N/A | **Resource Type** Other

Recommendations

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

ACCESS CONTROL / Section Remote Access | Protection of Confidentiality and Integrity Using Encryption



1 Resource(s) Failed

test

Informational

Compliance Section: Remote Access | Protection of Confidentiality and Integrity Using Encryption

Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

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

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

First Seen December 8, 2023 at 6:25:54 AM UTC | **Resource Type** Other

Recommendations

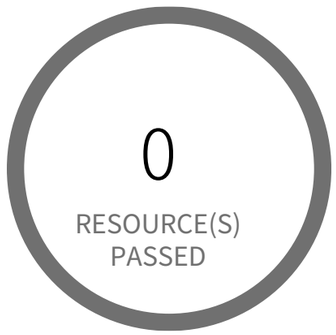
AWS EFS Encryption of data at rest can only be enabled during file system creation. So to resolve this alert, create a new EFS with encryption enabled with the customer-managed key, then migrate all required data from the reported EFS to this newly created EFS and delete reported EFS.

To create new EFS with encryption enabled, perform the following:
1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to EFS dashboard
4. Click on 'File systems' (Left Panel)
5. Click on 'Create file system' button
6. On the 'Configure file system access' step, specify EFS details as per your requirements and Click on 'Next Step'
7. On the 'Configure optional settings' step, Under 'Enable encryption' Choose 'Enable encryption of data at rest' and Select customer managed key [i.e. Other than (default)aws/elasticfilesystem] from 'Select KMS master key' dropdown list along with other parameters and Click on 'Next Step'
8. On the 'Review and create' step, Review all your setting and Click on 'Create File System' button

To delete reported EFS which does not has encryption, perform the following:
1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to EFS dashboard

4. Click on 'File systems' (Left Panel)
5. Select the reported file system
6. Click on 'Actions' drop-down
7. Click on 'Delete file system'
8. In the 'Permanently delete file system' popup box, To confirm the deletion enter the file system's ID and Click on 'Delete File System'

ACCESS CONTROL / Section Remote Access | Protection of Confidentiality and Integrity Using Encryption



0 Resource(s) Failed

Compliance Section: Remote Access | Protection of Confidentiality and Integrity Using Encryption

Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

Low

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

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

First Seen N/A | **Resource Type** Other

Recommendations

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

To create new ElastiCache Redis cluster with In-transit encryption set, perform the following:
1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to ElastiCache Dashboard
4. Click on Redis
5. Click on 'Create' button
6. On the 'Create your Amazon ElastiCache cluster' page,
a. Select 'Redis' cache engine type.
b. Enter a name for the new cache cluster
c. Select Redis engine version from 'Engine version compatibility' dropdown list.
Note: As of July 2018, In-transit encryption can be enabled only for AWS ElastiCache clusters with Redis engine version 3.2.6 and 4.0.10.
d. Click on 'Advanced Redis settings' to expand the cluster advanced settings panel
e. Select 'Encryption in-transit' checkbox to enable encryption along with other necessary parameters
7. Click on 'Create' button to launch your new ElastiCache Redis cluster

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

2

AUDIT AND ACCOUNTABILITY

AUDIT AND ACCOUNTABILITY Overview

Section			Pass Rate	Failed	Passed
Event Logging	AWS Log metric filter and alarm does not exist for Network Access Control Lists···	Informational	14%	6	1
Event Logging	AWS Log metric filter and alarm does not exist for AWS management console···	Informational	14%	6	1
Event Logging	AWS Log metric filter and alarm does not exist for CloudTrail configuration···	Informational	14%	6	1
Event Logging	AWS Log metric filter and alarm does not exist for Route table changes	Informational	14%	6	1
Event Logging	AWS Log metric filter and alarm does not exist for disabling or scheduled deletion···	Informational	14%	6	1
Event Logging	AWS Log metric filter and alarm does not exist for IAM policy changes	Informational	14%	6	1
Event Logging	AWS Redshift database does not have audit logging enabled	Informational	100%	0	0
Event Logging	AWS Log metric filter and alarm does not exist for unauthorized API calls	Informational	14%	6	1
Event Logging	AWS Log metric filter and alarm does not exist for S3 bucket policy changes	Informational	14%	6	1
Event Logging	AWS Log metric filter and alarm does not exist for Network gateways changes	Informational	14%	6	1

NIST 800-53 Rev 5 / AUDIT AND ACCOUNTABILITY

Section			Pass Rate	Failed	Passed
Event Logging	AWS Log metric filter and alarm does not exist for AWS Config configuration···	Informational	14%	6	1
Event Logging	AWS Log metric filter and alarm does not exist for VPC changes	Informational	14%	6	1
Content of Audit Records	AWS Log metric filter and alarm does not exist for Network···	Informational	14%	6	1
Content of Audit Records	AWS Log metric filter and alarm does not exist for AWS manage···	Informational	14%	6	1
Content of Audit Records	AWS Log metric filter and alarm does not exist for CloudTrail···	Informational	14%	6	1
Content of Audit Records	AWS Log metric filter and alarm does not exist for Route table···	Informational	14%	6	1
Content of Audit Records	AWS Log metric filter and alarm does not exist for disabling or···	Informational	14%	6	1
Content of Audit Records	AWS Log metric filter and alarm does not exist for IAM policy···	Informational	14%	6	1
Content of Audit Records	AWS Log metric filter and alarm does not exist for unauthorized··	Informational	14%	6	1
Content of Audit Records	AWS Log metric filter and alarm does not exist for S3 bucket···	Informational	14%	6	1
Content of Audit Records	AWS Log metric filter and alarm does not exist for Network···	Informational	14%	6	1

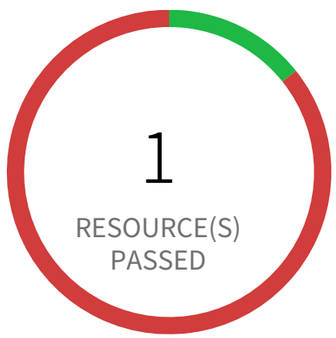
NIST 800-53 Rev 5 / AUDIT AND ACCOUNTABILITY

Section			Pass Rate	Failed	Passed
Content of Audit Records	AWS Log metric filter and alarm does not exist for AWS Config…	Informational	14%	6	1
Content of Audit Records	AWS Log metric filter and alarm does not exist for VPC changes	Informational	14%	6	1
Protection of Audit Information	AWS S3 Bucket Policy allows public access to CloudTrail logs	Low	100%	0	188
Protection of Audit Information | Cryptographic Protection	AWS Cloud…	Low	66%	4	8
Protection of Audit Information | Cryptographic Protection	AWS…	Informational	100%	0	1
Protection of Audit Information | Cryptographic Protection	AWS S3 buck…	Low	100%	0	186
Protection of Audit Information | Cryptographic Protection	AWS Kinesis…	Low	100%	0	0
Protection of Audit Information | Cryptographic Protection	AWS…	Informational	33%	8	4
Audit Record Retention	AWS RDS retention policy less than 7 days	Low	40%	3	2
Audit Record Generation | System-wide and Time-correlated Audit Trail		Low	88%	1	8
Audit Record Generation | System-wide and Time-correlated Audit Trail		Informational	25%	9	3

NIST 800-53 Rev 5 / AUDIT AND ACCOUNTABILITY

Section	Pass Rate	Failed	Passed
Audit Record Generation | System-wide and Time-correlated Audit Trail — Medium	83%	2	10
Audit Record Generation | System-wide and Time-correlated Audit Trail — Informational	100%	0	12

AUDIT AND ACCOUNTABILITY / Section Event Logging



6 Resource(s) Failed

035297560255, 016671749923, 197802673547, 154600454722, 240075317252, 673174758328

Compliance Section: Event Logging

Informational

a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging];
b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;
c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-2a.) along with the frequency of (or situation requiring) logging for each identified event type];
d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and
e. Review and update the event types selected for logging [Assignment: organization-defined frequency].

AWS Log metric filter and alarm does not exist for Network Access Control Lists (NACL) changes

This policy identifies the AWS regions which do not have a log metric filter and alarm for Network Access Control Lists (NACL) changes. Monitoring changes to NACLs will help ensure that AWS resources and services are not unintentionally exposed. It is recommended that a metric filter and alarm be established for changes made to NACLs.

NOTE: This policy will trigger alert if you have at least one Cloudtrail with the multi trial is enabled, Logs all management events in your account and is not set with specific log metric filter and alarm.

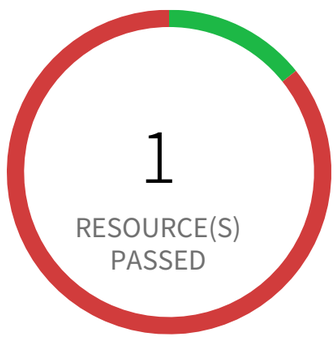
First Seen March 18, 2021 at 11:01:09 AM UTC | **Resource Type** Other

Recommendations

1. Sign in to AWS Console
2. Navigate to CloudWatch dashboard
3. Click on 'Log groups' in the 'Logs' section (Left panel)
4. Select the log group created for your CloudTrail trail event logs (CloudTrail should be multi trail enabled with all management events captured) and click 'Create Metric Filter' button.
5. In 'Define Logs Metric Filter' page, add 'Filter pattern' value as
{ ($.eventName = CreateNetworkAcl) || ($.eventName = CreateNetworkAclEntry) || ($.eventName = DeleteNetworkAcl) || ($.eventName = DeleteNetworkAclEntry) || ($.eventName = ReplaceNetworkAclEntry) || ($.eventName = ReplaceNetworkAclAssociation) }
and Click on 'Assign Metric'
6. In 'Create Metric Filter and Assign a Metric' page, Choose Filter Name, Metric Details parameter according to your requirement and click

on 'Create Filter'
7. Click on 'Create Alarm',
- In Step 1 specify metric details and conditions details as required and click on 'Next'
- In Step 2 Select an SNS topic either by creating a new topic or use existing SNS topic/ARN and click on 'Next'
- In Step 3 Select name and description to alarm and click on 'Next'
- In Step 4 Preview your data entered and click on 'Create Alarm'

AUDIT AND ACCOUNTABILITY / Section Event Logging



6 Resource(s) Failed

035297560255, 016671749923, 197802673547, 154600454722, 240075317252, 673174758328

Compliance Section: Event Logging

Informational

a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging];
b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;
c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-2a.) along with the frequency of (or situation requiring) logging for each identified event type];
d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and
e. Review and update the event types selected for logging [Assignment: organization-defined frequency].

AWS Log metric filter and alarm does not exist for AWS management console authentication failures

This policy identifies the AWS accounts which do not have a log metric filter and alarm for AWS management console authentication failures. Monitoring failed console logins may decrease lead time to detect an attempt to brute force a credential, which may provide an indicator, such as source IP, that can be used in other event correlation. It is recommended that a metric filter and alarm be established for failed console authentication attempts.

NOTE: This policy will trigger alert if you have at least one Cloudtrail with the multi trial is enabled, Logs all management events and is not set with specific log metric filter and alarm in your account.

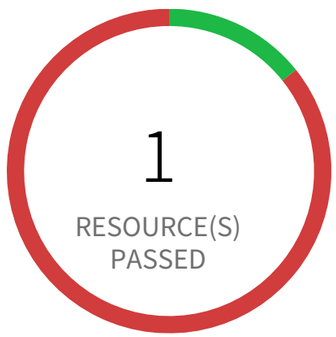
First Seen March 18, 2021 at 11:01:09 AM UTC | **Resource Type** Other

Recommendations

1. Sign in to AWS Console
2. Navigate to CloudWatch dashboard
3. Click on 'Log groups' in the 'Logs' section (Left panel)
4. Select the log group created for your CloudTrail trail event logs (Cloudtrail should be multi trail enabled with all Management Events captured) and click 'Create Metric Filter' button.
5. In 'Define Logs Metric Filter' page, add 'Filter pattern' value as
{ ($.eventName = ConsoleLogin) && ($.errorMessage = "Failed authentication") }
and Click on 'Assign Metric'
6. In 'Create Metric Filter and Assign a Metric' page, Choose Filter Name, Metric Details parameter according to your requirement and click on 'Create Filter'

7. Click on 'Create Alarm',
- In Step 1, specify metric details and conditions details as required and click on 'Next'
- In Step 2, Select an SNS topic either by creating a new topic or use existing SNS topic/ARN and click on 'Next'
- In Step 3, Select name and description to alarm and click on 'Next'
- In Step 4, Preview your data entered and click on 'Create Alarm'

AUDIT AND ACCOUNTABILITY / Section Event Logging



6 Resource(s) Failed

035297560255, 016671749923, 197802673547, 154600454722, 240075317252, 673174758328

Compliance Section: Event Logging

Informational

a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging];
b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;
c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-2a.) along with the frequency of (or situation requiring) logging for each identified event type];
d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and
e. Review and update the event types selected for logging [Assignment: organization-defined frequency].

AWS Log metric filter and alarm does not exist for CloudTrail configuration changes

This policy identifies the AWS regions which do not have a log metric filter and alarm for CloudTrail configuration changes. Monitoring changes to CloudTrail's configuration will help ensure sustained visibility to activities performed in the AWS account. It is recommended that a metric filter and alarm be established for detecting changes to CloudTrail's configurations.

NOTE: This policy will trigger alert if you have at least one Cloudtrail with the multi trial is enabled, Logs all management events in your account and is not set with specific log metric filter and alarm.

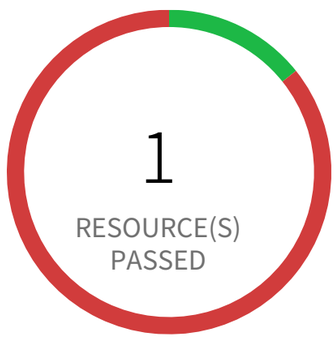
First Seen March 18, 2021 at 11:01:09 AM UTC | **Resource Type** Other

Recommendations

1. Sign in to AWS Console
2. Navigate to CloudWatch dashboard
3. Click on 'Log groups' in the 'Logs' section (Left panel)
4. Select the log group created for your CloudTrail trail event logs (CloudTrail should be multi trail enabled with all management events captured) and click 'Create Metric Filter' button.
5. In 'Define Logs Metric Filter' page, add 'Filter pattern' value as
{ ($.eventName = CreateTrail) || ($.eventName = UpdateTrail) || ($.eventName = DeleteTrail) || ($.eventName = StartLogging) || ($.eventName = StopLogging) }
and Click on 'Assign Metric'
6. In 'Create Metric Filter and Assign a Metric' page, Choose Filter Name, Metric Details parameter according to your requirement and click

on 'Create Filter'
7. Click on 'Create Alarm',
- In Step 1 specify metric details and conditions details as required and click on 'Next'
- In Step 2 Select an SNS topic either by creating a new topic or use existing SNS topic/ARN and click on 'Next'
- In Step 3 Select name and description to alarm and click on 'Next'
- In Step 4 Preview your data entered and click on 'Create Alarm'

AUDIT AND ACCOUNTABILITY / Section Event Logging



6 Resource(s) Failed

035297560255, 016671749923, 197802673547, 154600454722, 240075317252, 673174758328

Compliance Section: Event Logging

Informational

a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging];
b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;
c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-2a.) along with the frequency of (or situation requiring) logging for each identified event type];
d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and
e. Review and update the event types selected for logging [Assignment: organization-defined frequency].

AWS Log metric filter and alarm does not exist for Route table changes

This policy identifies the AWS regions which do not have a log metric filter and alarm for Route table changes. Monitoring changes to route tables will help ensure that all VPC traffic flows through an expected path. It is recommended that a metric filter and alarm be established for changes to route tables.

NOTE: This policy will trigger alert if you have at least one Cloudtrail with the multi trial is enabled, Logs all management events in your account and is not set with specific log metric filter and alarm.

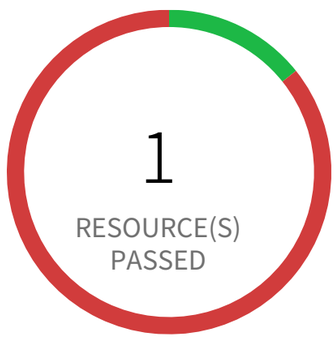
First Seen March 18, 2021 at 11:01:09 AM UTC | **Resource Type** Other

Recommendations

1. Sign in to AWS Console
2. Navigate to CloudWatch dashboard
3. Click on 'Log groups' in the 'Logs' section (Left panel)
4. Select the log group created for your CloudTrail trail event logs (CloudTrail should be multi trail enabled with all management events captured) and click 'Create Metric Filter' button.
5. In 'Define Logs Metric Filter' page, add 'Filter pattern' value as
{ ($.eventName = CreateRoute) || ($.eventName = CreateRouteTable) || ($.eventName = ReplaceRoute) || ($.eventName = ReplaceRouteTable-Association) || ($.eventName = DeleteRouteTable) || ($.eventName = DeleteRoute) || ($.eventName = DisassociateRouteTable) }
and Click on 'Assign Metric'
6. In 'Create Metric Filter and Assign a Metric' page, Choose Filter Name, Metric Details parameter according to your requirement and click

on 'Create Filter'
7. Click on 'Create Alarm',
- In Step 1 specify metric details and conditions details as required and click on 'Next'
- In Step 2 Select an SNS topic either by creating a new topic or use existing SNS topic/ARN and click on 'Next'
- In Step 3 Select name and description to alarm and click on 'Next'
- In Step 4 Preview your data entered and click on 'Create Alarm'

AUDIT AND ACCOUNTABILITY / Section Event Logging



6 Resource(s) Failed

035297560255, 016671749923, 197802673547, 154600454722, 240075317252, 673174758328

Compliance Section: Event Logging

Informational

a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging];
b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;
c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-2a.) along with the frequency of (or situation requiring) logging for each identified event type];
d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and
e. Review and update the event types selected for logging [Assignment: organization-defined frequency].

AWS Log metric filter and alarm does not exist for disabling or scheduled deletion of customer created CMKs

This policy identifies the AWS regions which do not have a log metric filter and alarm for disabling or scheduled deletion of customer created CMKs. Data encrypted with disabled or deleted keys will no longer be accessible. It is recommended that a metric filter and alarm be established for customer created CMKs which have changed state to disabled or scheduled deletion.

NOTE: This policy will trigger alert if you have at least one Cloudtrail with the multi trial is enabled, Logs all management events in your account and is not set with specific log metric filter and alarm.

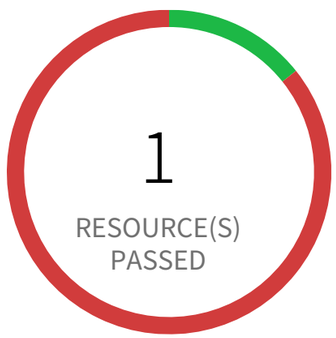
First Seen March 18, 2021 at 11:01:09 AM UTC | **Resource Type** Other

Recommendations

1. Sign in to AWS Console
2. Navigate to CloudWatch dashboard
3. Click on 'Log groups' in the 'Logs' section (Left panel)
4. Select the log group created for your CloudTrail trail event logs (CloudTrail should be multi trail enabled with all management events captured) and click 'Create Metric Filter' button.
5. In 'Define Logs Metric Filter' page, add 'Filter pattern' value as
{ ($.eventSource = kms.amazonaws.com) && (($.eventName=DisableKey)||($.eventName=ScheduleKeyDeletion)) }
and Click on 'Assign Metric'
6. In 'Create Metric Filter and Assign a Metric' page, Choose Filter Name, Metric Details parameter according to your requirement and click on 'Create Filter'

7. Click on 'Create Alarm',
- In Step 1 specify metric details and conditions details as required and click on 'Next'
- In Step 2 Select an SNS topic either by creating a new topic or use existing SNS topic/ARN and click on 'Next'
- In Step 3 Select name and description to alarm and click on 'Next'
- In Step 4 Preview your data entered and click on 'Create Alarm'

AUDIT AND ACCOUNTABILITY / Section Event Logging



6 Resource(s) Failed

035297560255, 016671749923, 197802673547, 154600454722, 240075317252, 673174758328

Compliance Section: Event Logging

Informational

a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging];
b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;
c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-2a.) along with the frequency of (or situation requiring) logging for each identified event type];
d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and
e. Review and update the event types selected for logging [Assignment: organization-defined frequency].

AWS Log metric filter and alarm does not exist for IAM policy changes

This policy identifies the AWS regions which do not have a log metric filter and alarm for IAM policy changes. Monitoring changes to IAM policies will help ensure authentication and authorization controls remain intact. It is recommended that a metric filter and alarm be established changes made to Identity and Access Management (IAM) policies.

NOTE: This policy will trigger alert if you have at least one Cloudtrail with the multi trial is enabled, Logs all management events in your account and is not set with specific log metric filter and alarm.

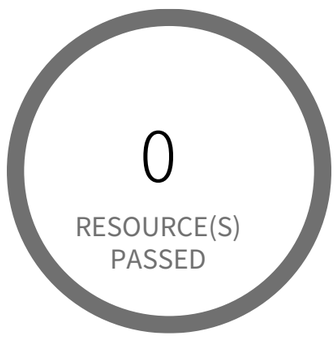
First Seen March 18, 2021 at 11:01:00 AM UTC | **Resource Type** Other

Recommendations

1. Sign in to AWS Console
2. Navigate to CloudWatch dashboard
3. Click on 'Log groups' in the 'Logs' section (Left panel)
4. Select the log group created for your CloudTrail trail event logs (CloudTrail should be multi trail enabled with all management events captured) and click 'Create Metric Filter' button.
5. In 'Define Logs Metric Filter' page, add 'Filter pattern' value as
{
($.eventName=DeleteGroupPolicy)||($.eventName=DeleteRolePolicy)||($.eventName=DeleteUserPolicy)||($.eventName=PutGroupPolicy)||($.eventName=PutRolePolicy)||($.eventName=PutUserPolicy)||($.eventName=CreatePolicy)||($.eventName=DeletePolicy)||($.eventName=CreatePolicyVersion)||($.eventName=DeletePolicyVersion)||($.eventName=AttachRolePolicy)||($.eventName=DetachRolePoli-

cy)||($.eventName=AttachUserPolicy)||($.eventName=DetachUserPolicy)||($.eventName=AttachGroupPolicy)||($.eventName=DetachGroup-Policy) }
and Click on 'Assign Metric'
6. In 'Create Metric Filter and Assign a Metric' page, Choose Filter Name, Metric Details parameter according to your requirement and click on 'Create Filter'
7. Click on 'Create Alarm',
- In Step 1 specify metric details and conditions details as required and click on 'Next'
- In Step 2 Select an SNS topic either by creating a new topic or use existing SNS topic/ARN and click on 'Next'
- In Step 3 Select name and description to alarm and click on 'Next'
- In Step 4 Preview your data entered and click on 'Create Alarm'

AUDIT AND ACCOUNTABILITY / Section Event Logging



0 Resource(s) Failed

Compliance Section: Event Logging

Informational

a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging];
b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;
c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-2a.) along with the frequency of (or situation requiring) logging for each identified event type];
d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and
e. Review and update the event types selected for logging [Assignment: organization-defined frequency].

AWS Redshift database does not have audit logging enabled

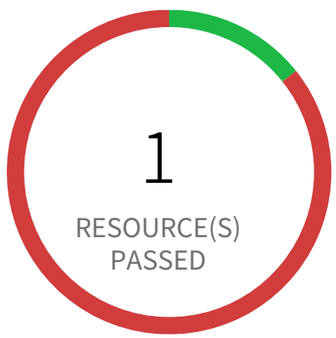
Audit logging is not enabled by default in Amazon Redshift. When you enable logging on your cluster, Amazon Redshift creates and uploads logs to Amazon S3 that capture data from the creation of the cluster to the present time.

First Seen N/A | **Resource Type** Managed Database

Recommendations

1. Login to AWS Console.
2. Goto Amazon Redshift service
3. On left navigation panel, click on Clusters
4. Click on the reported cluster
5. Click on Database tab and choose 'Configure Audit Logging'
6. On Enable Audit Logging, choose 'Yes'
7. Create a new s3 bucket or use an existing bucket
8. click Save

AUDIT AND ACCOUNTABILITY / Section Event Logging



6 Resource(s) Failed

035297560255, 016671749923, 197802673547, 154600454722, 240075317252, 673174758328

Compliance Section: Event Logging

Informational

a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging];
b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;
c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-2a.) along with the frequency of (or situation requiring) logging for each identified event type];
d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and
e. Review and update the event types selected for logging [Assignment: organization-defined frequency].

AWS Log metric filter and alarm does not exist for unauthorized API calls

This policy identifies the AWS regions which do not have a log metric filter and alarm for unauthorized API calls. Monitoring unauthorized API calls will help reveal application errors and may reduce the time to detect malicious activity. It is recommended that a metric filter and alarm be established for unauthorized API calls.

NOTE: This policy will trigger alert if you have at least one Cloudtrail with the multi trial is enabled, Logs all management events in your account and is not set with specific log metric filter and alarm.

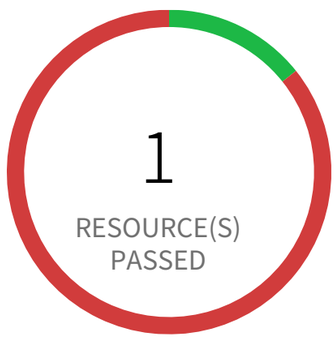
First Seen March 18, 2021 at 11:01:09 AM UTC | **Resource Type** Other

Recommendations

1. Sign in to AWS Console
2. Navigate to CloudWatch dashboard
3. Click on 'Log groups' in the 'Logs' section (Left panel)
4. Select the log group created for your CloudTrail trail event logs (CloudTrail should be multi trail enabled with all management events captured) and click 'Create Metric Filter' button.
5. In 'Define Logs Metric Filter' page, add 'Filter pattern' value as
{ ($.errorCode = "*UnauthorizedOperation") || ($.errorCode = "AccessDenied*") }
and Click on 'Assign Metric'
6. In 'Create Metric Filter and Assign a Metric' page, Choose Filter Name, Metric Details parameter according to your requirement and click on 'Create Filter'

7. Click on 'Create Alarm',
- In Step 1 specify metric details and conditions details as required and click on 'Next'
- In Step 2 Select an SNS topic either by creating a new topic or use existing SNS topic/ARN and click on 'Next'
- In Step 3 Select name and description to alarm and click on 'Next'
- In Step 4 Preview your data entered and click on 'Create Alarm'

AUDIT AND ACCOUNTABILITY / Section Event Logging



6 Resource(s) Failed

035297560255, 016671749923, 197802673547, 154600454722, 240075317252, 673174758328

Compliance Section: Event Logging

Informational

a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging];
b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;
c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-2a.) along with the frequency of (or situation requiring) logging for each identified event type];
d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and
e. Review and update the event types selected for logging [Assignment: organization-defined frequency].

AWS Log metric filter and alarm does not exist for S3 bucket policy changes

This policy identifies the AWS regions which do not have a log metric filter and alarm for S3 bucket policy changes. Monitoring changes to S3 bucket policies may reduce time to detect and correct permissive policies on sensitive S3 buckets. It is recommended that a metric filter and alarm be established for changes to S3 bucket policies.

NOTE: This policy will trigger alert if you have at least one Cloudtrail with the multi trial is enabled, Logs all management events in your account and is not set with specific log metric filter and alarm.

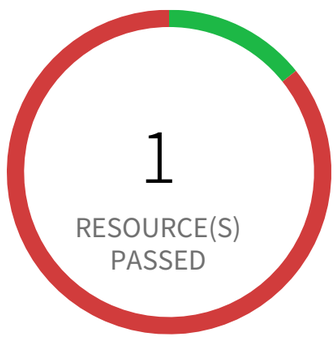
First Seen March 18, 2021 at 11:01:09 AM UTC | **Resource Type** Other

Recommendations

1. Sign in to AWS Console
2. Navigate to CloudWatch dashboard
3. Click on 'Log groups' in the 'Logs' section (Left panel)
4. Select the log group created for your CloudTrail trail event logs (CloudTrail should be multi trail enabled with all management events captured) and click 'Create Metric Filter' button.
5. In 'Define Logs Metric Filter' page, add 'Filter pattern' value as
{ ($.eventSource = s3.amazonaws.com) && (($.eventName = PutBucketAcl) || ($.eventName = PutBucketPolicy) || ($.eventName = PutBucket-Cors) || ($.eventName = PutBucketLifecycle) || ($.eventName = PutBucketReplication) || ($.eventName = DeleteBucketPolicy) || ($.eventName = DeleteBucketCors) || ($.eventName = DeleteBucketLifecycle) || ($.eventName = DeleteBucketReplication)) }
and Click on 'Assign Metric'

6. In 'Create Metric Filter and Assign a Metric' page, Choose Filter Name, Metric Details parameter according to your requirement and click on 'Create Filter'
7. Click on 'Create Alarm',
- In Step 1 specify metric details and conditions details as required and click on 'Next'
- In Step 2 Select an SNS topic either by creating a new topic or use existing SNS topic/ARN and click on 'Next'
- In Step 3 Select name and description to alarm and click on 'Next'
- In Step 4 Preview your data entered and click on 'Create Alarm'

AUDIT AND ACCOUNTABILITY / Section Event Logging



6 Resource(s) Failed

035297560255, 016671749923, 197802673547, 154600454722, 240075317252, 673174758328

Compliance Section: Event Logging Informational

a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging];
b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;
c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-2a.) along with the frequency of (or situation requiring) logging for each identified event type];
d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and
e. Review and update the event types selected for logging [Assignment: organization-defined frequency].

AWS Log metric filter and alarm does not exist for Network gateways changes

This policy identifies the AWS regions which do not have a log metric filter and alarm for Network gateways changes. Monitoring changes to network gateways will help ensure that all ingress/egress traffic traverses the VPC border via a controlled path. It is recommended that a metric filter and alarm be established for changes to network gateways.

NOTE: This policy will trigger alert if you have at least one Cloudtrail with the multi trial is enabled, Logs all management events in your account and is not set with specific log metric filter and alarm.

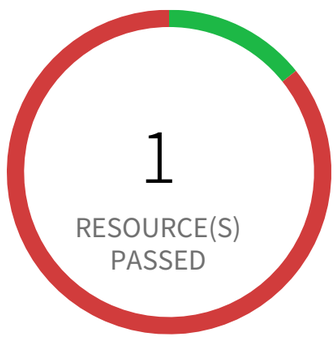
First Seen March 18, 2021 at 11:01:09 AM UTC | **Resource Type** Other

Recommendations

1. Sign in to AWS Console
2. Navigate to CloudWatch dashboard
3. Click on 'Log groups' in the 'Logs' section (Left panel)
4. Select the log group created for your CloudTrail trail event logs (CloudTrail should be multi trail enabled with all management events captured) and click 'Create Metric Filter' button.
5. In 'Define Logs Metric Filter' page, add 'Filter pattern' value as
{ ($.eventName = CreateCustomerGateway) || ($.eventName = DeleteCustomerGateway) || ($.eventName = AttachInternetGateway) || ($.eventName = CreateInternetGateway) || ($.eventName = DeleteInternetGateway) || ($.eventName = DetachInternetGateway) }
and Click on 'Assign Metric'
6. In 'Create Metric Filter and Assign a Metric' page, Choose Filter Name, Metric Details parameter according to your requirement and click

on 'Create Filter'
7. Click on 'Create Alarm',
- In Step 1 specify metric details and conditions details as required and click on 'Next'
- In Step 2 Select an SNS topic either by creating a new topic or use existing SNS topic/ARN and click on 'Next'
- In Step 3 Select name and description to alarm and click on 'Next'
- In Step 4 Preview your data entered and click on 'Create Alarm'

AUDIT AND ACCOUNTABILITY / Section Event Logging



6 Resource(s) Failed

035297560255, 016671749923, 197802673547, 154600454722, 240075317252, 673174758328

Compliance Section: Event Logging

Informational

a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging];
b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;
c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-2a.) along with the frequency of (or situation requiring) logging for each identified event type];
d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and
e. Review and update the event types selected for logging [Assignment: organization-defined frequency].

AWS Log metric filter and alarm does not exist for AWS Config configuration changes

This policy identifies the AWS regions which do not have a log metric filter and alarm for AWS Config configuration changes. Monitoring changes to AWS Config configuration will help ensure sustained visibility of configuration items within the AWS account. It is recommended that a metric filter and alarm be established for detecting changes to AWS Config's configurations.

NOTE: This policy will trigger alert if you have at least one Cloudtrail with the multi trial is enabled, Logs all management events in your account and is not set with specific log metric filter and alarm.

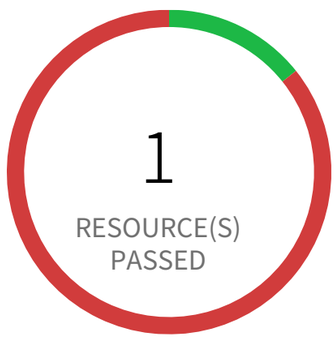
First Seen March 18, 2021 at 11:01:09 AM UTC | **Resource Type** Other

Recommendations

1. Sign in to AWS Console
2. Navigate to CloudWatch dashboard
3. Click on 'Log groups' in the 'Logs' section (Left panel)
4. Select the log group created for your CloudTrail trail event logs (CloudTrail should be multi trail enabled with all management events captured) and click 'Create Metric Filter' button.
5. In 'Define Logs Metric Filter' page, add 'Filter pattern' value as
{ ($.eventSource = config.amazonaws.com) && (($.eventName=StopConfigurationRecorder)||($.eventName=DeleteDeliveryChannel)||($.eventName=PutDeliveryChannel)||($.eventName=PutConfigurationRecorder)) }
and Click on 'Assign Metric'
6. In 'Create Metric Filter and Assign a Metric' page, Choose Filter Name, Metric Details parameter according to your requirement and click

on 'Create Filter'
7. Click on 'Create Alarm',
- In Step 1 specify metric details and conditions details as required and click on 'Next'
- In Step 2 Select an SNS topic either by creating a new topic or use existing SNS topic/ARN and click on 'Next'
- In Step 3 Select name and description to alarm and click on 'Next'
- In Step 4 Preview your data entered and click on 'Create Alarm'

AUDIT AND ACCOUNTABILITY / Section Event Logging



6 Resource(s) Failed

035297560255, 016671749923, 197802673547, 154600454722, 240075317252, 673174758328

Compliance Section: Event Logging

Informational

a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging];
b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;
c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-2a.) along with the frequency of (or situation requiring) logging for each identified event type];
d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and
e. Review and update the event types selected for logging [Assignment: organization-defined frequency].

AWS Log metric filter and alarm does not exist for VPC changes

This policy identifies the AWS regions which do not have a log metric filter and alarm for VPC changes. Monitoring changes to VPC will help ensure that resources and services are not unintentionally exposed. It is recommended that a metric filter and alarm be established for changes made to VPCs.

NOTE: This policy will trigger alert if you have at least one Cloudtrail with the multi trial is enabled, Logs all management events in your account and is not set with specific log metric filter and alarm.

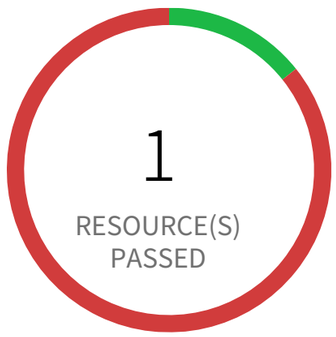
First Seen March 18, 2021 at 11:01:09 AM UTC | **Resource Type** Other

Recommendations

1. Sign in to AWS Console
2. Navigate to CloudWatch dashboard
3. Click on 'Log groups' in the 'Logs' section (Left panel)
4. Select the log group created for your CloudTrail trail event logs (CloudTrail should be multi trail enabled with all management events captured) and click 'Create Metric Filter' button.
5. In 'Define Logs Metric Filter' page, add 'Filter pattern' value as
{ ($.eventName = CreateVpc) || ($.eventName = DeleteVpc) || ($.eventName = ModifyVpcAttribute) || ($.eventName = AcceptVpcPeeringConnection) || ($.eventName = CreateVpcPeeringConnection) || ($.eventName = DeleteVpcPeeringConnection) || ($.eventName = RejectVpcPeeringConnection) || ($.eventName = AttachClassicLinkVpc) || ($.eventName = DetachClassicLinkVpc) || ($.eventName = DisableVpcClassicLink) || ($.eventName = EnableVpcClassicLink) }

and Click on 'Assign Metric'
6. In 'Create Metric Filter and Assign a Metric' page, Choose Filter Name, Metric Details parameter according to your requirement and click on 'Create Filter'
7. Click on 'Create Alarm',
- In Step 1 specify metric details and conditions details as required and click on 'Next'
- In Step 2 Select an SNS topic either by creating a new topic or use existing SNS topic/ARN and click on 'Next'
- In Step 3 Select name and description to alarm and click on 'Next'
- In Step 4 Preview your data entered and click on 'Create Alarm'

AUDIT AND ACCOUNTABILITY / Section Content of Audit Records



6 Resource(s) Failed

035297560255, 016671749923, 197802673547, 154600454722, 240075317252, 673174758328

Compliance Section: Content of Audit Records — Informational

Ensure that audit records contain information that establishes the following:
a. What type of event occurred;
b. When the event occurred;
c. Where the event occurred;
d. Source of the event;
e. Outcome of the event; and
f. Identity of any individuals, subjects, or objects/entities associated with the event.

AWS Log metric filter and alarm does not exist for Network Access Control Lists (NACL) changes

This policy identifies the AWS regions which do not have a log metric filter and alarm for Network Access Control Lists (NACL) changes. Monitoring changes to NACLs will help ensure that AWS resources and services are not unintentionally exposed. It is recommended that a metric filter and alarm be established for changes made to NACLs.

NOTE: This policy will trigger alert if you have at least one Cloudtrail with the multi trial is enabled, Logs all management events in your account and is not set with specific log metric filter and alarm.

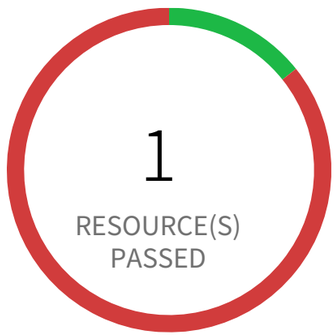
First Seen March 18, 2021 at 11:01:09 AM UTC | **Resource Type** Other

Recommendations

1. Sign in to AWS Console
2. Navigate to CloudWatch dashboard
3. Click on 'Log groups' in the 'Logs' section (Left panel)
4. Select the log group created for your CloudTrail trail event logs (CloudTrail should be multi trail enabled with all management events captured) and click 'Create Metric Filter' button.
5. In 'Define Logs Metric Filter' page, add 'Filter pattern' value as
{ ($.eventName = CreateNetworkAcl) || ($.eventName = CreateNetworkAclEntry) || ($.eventName = DeleteNetworkAcl) || ($.eventName = DeleteNetworkAclEntry) || ($.eventName = ReplaceNetworkAclEntry) || ($.eventName = ReplaceNetworkAclAssociation) }
and Click on 'Assign Metric'
6. In 'Create Metric Filter and Assign a Metric' page, Choose Filter Name, Metric Details parameter according to your requirement and click on 'Create Filter'
7. Click on 'Create Alarm',
- In Step 1 specify metric details and conditions details as required and click on 'Next'
- In Step 2 Select an SNS topic either by creating a new topic or use existing SNS topic/ARN and click on 'Next'

- In Step 3 Select name and description to alarm and click on 'Next'
- In Step 4 Preview your data entered and click on 'Create Alarm'

AUDIT AND ACCOUNTABILITY / Section Content of Audit Records



6 Resource(s) Failed

035297560255, 016671749923, 197802673547, 154600454722, 240075317252, 673174758328

Compliance Section: Content of Audit Records

Informational

Ensure that audit records contain information that establishes the following:
a. What type of event occurred;
b. When the event occurred;
c. Where the event occurred;
d. Source of the event;
e. Outcome of the event; and
f. Identity of any individuals, subjects, or objects/entities associated with the event.

AWS Log metric filter and alarm does not exist for AWS management console authentication failures

This policy identifies the AWS accounts which do not have a log metric filter and alarm for AWS management console authentication failures. Monitoring failed console logins may decrease lead time to detect an attempt to brute force a credential, which may provide an indicator, such as source IP, that can be used in other event correlation. It is recommended that a metric filter and alarm be established for failed console authentication attempts.

NOTE: This policy will trigger alert if you have at least one Cloudtrail with the multi trial is enabled, Logs all management events and is not set with specific log metric filter and alarm in your account.

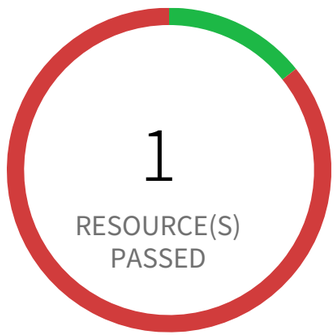
First Seen March 18, 2021 at 11:01:09 AM UTC | **Resource Type** Other

Recommendations

1. Sign in to AWS Console
2. Navigate to CloudWatch dashboard
3. Click on 'Log groups' in the 'Logs' section (Left panel)
4. Select the log group created for your CloudTrail trail event logs (Cloudtrail should be multi trail enabled with all Management Events captured) and click 'Create Metric Filter' button.
5. In 'Define Logs Metric Filter' page, add 'Filter pattern' value as
{ ($.eventName = ConsoleLogin) && ($.errorMessage = "Failed authentication") }
and Click on 'Assign Metric'
6. In 'Create Metric Filter and Assign a Metric' page, Choose Filter Name, Metric Details parameter according to your requirement and click on 'Create Filter'
7. Click on 'Create Alarm',
- In Step 1, specify metric details and conditions details as required and click on 'Next'
- In Step 2, Select an SNS topic either by creating a new topic or use existing SNS topic/ARN and click on 'Next'

- In Step 3, Select name and description to alarm and click on 'Next'
- In Step 4, Preview your data entered and click on 'Create Alarm'

AUDIT AND ACCOUNTABILITY / Section Content of Audit Records



6 Resource(s) Failed

035297560255, 016671749923, 197802673547, 154600454722, 240075317252, 673174758328

Compliance Section: Content of Audit Records

Informational

Ensure that audit records contain information that establishes the following:
a. What type of event occurred;
b. When the event occurred;
c. Where the event occurred;
d. Source of the event;
e. Outcome of the event; and
f. Identity of any individuals, subjects, or objects/entities associated with the event.

AWS Log metric filter and alarm does not exist for CloudTrail configuration changes

This policy identifies the AWS regions which do not have a log metric filter and alarm for CloudTrail configuration changes. Monitoring changes to CloudTrail's configuration will help ensure sustained visibility to activities performed in the AWS account. It is recommended that a metric filter and alarm be established for detecting changes to CloudTrail's configurations.

NOTE: This policy will trigger alert if you have at least one Cloudtrail with the multi trial is enabled, Logs all management events in your account and is not set with specific log metric filter and alarm.

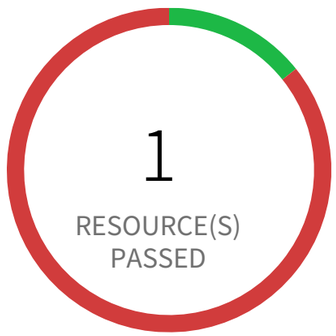
First Seen March 18, 2021 at 11:01:09 AM UTC | **Resource Type** Other

Recommendations

1. Sign in to AWS Console
2. Navigate to CloudWatch dashboard
3. Click on 'Log groups' in the 'Logs' section (Left panel)
4. Select the log group created for your CloudTrail trail event logs (CloudTrail should be multi trail enabled with all management events captured) and click 'Create Metric Filter' button.
5. In 'Define Logs Metric Filter' page, add 'Filter pattern' value as
{ ($.eventName = CreateTrail) || ($.eventName = UpdateTrail) || ($.eventName = DeleteTrail) || ($.eventName = StartLogging) || ($.eventName = StopLogging) }
and Click on 'Assign Metric'
6. In 'Create Metric Filter and Assign a Metric' page, Choose Filter Name, Metric Details parameter according to your requirement and click on 'Create Filter'
7. Click on 'Create Alarm',
- In Step 1 specify metric details and conditions details as required and click on 'Next'
- In Step 2 Select an SNS topic either by creating a new topic or use existing SNS topic/ARN and click on 'Next'

- In Step 3 Select name and description to alarm and click on 'Next'
- In Step 4 Preview your data entered and click on 'Create Alarm'

AUDIT AND ACCOUNTABILITY / Section Content of Audit Records



6 Resource(s) Failed

035297560255, 016671749923, 197802673547, 154600454722, 240075317252, 673174758328

Compliance Section: Content of Audit Records

Informational

Ensure that audit records contain information that establishes the following:
a. What type of event occurred;
b. When the event occurred;
c. Where the event occurred;
d. Source of the event;
e. Outcome of the event; and
f. Identity of any individuals, subjects, or objects/entities associated with the event.

AWS Log metric filter and alarm does not exist for Route table changes

This policy identifies the AWS regions which do not have a log metric filter and alarm for Route table changes. Monitoring changes to route tables will help ensure that all VPC traffic flows through an expected path. It is recommended that a metric filter and alarm be established for changes to route tables.

NOTE: This policy will trigger alert if you have at least one Cloudtrail with the multi trial is enabled, Logs all management events in your account and is not set with specific log metric filter and alarm.

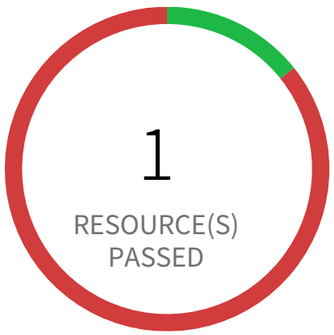
First Seen March 18, 2021 at 11:01:09 AM UTC | **Resource Type** Other

Recommendations

1. Sign in to AWS Console
2. Navigate to CloudWatch dashboard
3. Click on 'Log groups' in the 'Logs' section (Left panel)
4. Select the log group created for your CloudTrail trail event logs (CloudTrail should be multi trail enabled with all management events captured) and click 'Create Metric Filter' button.
5. In 'Define Logs Metric Filter' page, add 'Filter pattern' value as
{ ($.eventName = CreateRoute) || ($.eventName = CreateRouteTable) || ($.eventName = ReplaceRoute) || ($.eventName = ReplaceRouteTableAssociation) || ($.eventName = DeleteRouteTable) || ($.eventName = DeleteRoute) || ($.eventName = DisassociateRouteTable) }
and Click on 'Assign Metric'
6. In 'Create Metric Filter and Assign a Metric' page, Choose Filter Name, Metric Details parameter according to your requirement and click on 'Create Filter'
7. Click on 'Create Alarm',
- In Step 1 specify metric details and conditions details as required and click on 'Next'
- In Step 2 Select an SNS topic either by creating a new topic or use existing SNS topic/ARN and click on 'Next'

- In Step 3 Select name and description to alarm and click on 'Next'
- In Step 4 Preview your data entered and click on 'Create Alarm'

AUDIT AND ACCOUNTABILITY / Section Content of Audit Records



6 Resource(s) Failed

035297560255, 016671749923, 197802673547, 154600454722, 240075317252, 673174758328

Compliance Section: Content of Audit Records

Informational

Ensure that audit records contain information that establishes the following:
a. What type of event occurred;
b. When the event occurred;
c. Where the event occurred;
d. Source of the event;
e. Outcome of the event; and
f. Identity of any individuals, subjects, or objects/entities associated with the event.

AWS Log metric filter and alarm does not exist for disabling or scheduled deletion of customer created CMKs

This policy identifies the AWS regions which do not have a log metric filter and alarm for disabling or scheduled deletion of customer created CMKs. Data encrypted with disabled or deleted keys will no longer be accessible. It is recommended that a metric filter and alarm be established for customer created CMKs which have changed state to disabled or scheduled deletion.

NOTE: This policy will trigger alert if you have at least one Cloudtrail with the multi trial is enabled, Logs all management events in your account and is not set with specific log metric filter and alarm.

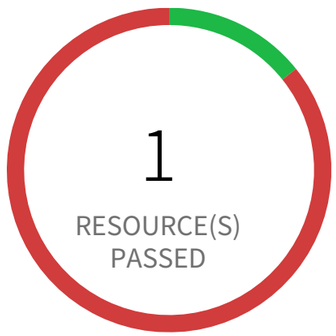
First Seen March 18, 2021 at 11:01:09 AM UTC | **Resource Type** Other

Recommendations

1. Sign in to AWS Console
2. Navigate to CloudWatch dashboard
3. Click on 'Log groups' in the 'Logs' section (Left panel)
4. Select the log group created for your CloudTrail trail event logs (CloudTrail should be multi trail enabled with all management events captured) and click 'Create Metric Filter' button.
5. In 'Define Logs Metric Filter' page, add 'Filter pattern' value as
{ ($.eventSource = kms.amazonaws.com) && (($.eventName=DisableKey)||($.eventName=ScheduleKeyDeletion)) }
and Click on 'Assign Metric'
6. In 'Create Metric Filter and Assign a Metric' page, Choose Filter Name, Metric Details parameter according to your requirement and click on 'Create Filter'
7. Click on 'Create Alarm',
- In Step 1 specify metric details and conditions details as required and click on 'Next'
- In Step 2 Select an SNS topic either by creating a new topic or use existing SNS topic/ARN and click on 'Next'

- In Step 3 Select name and description to alarm and click on 'Next'
- In Step 4 Preview your data entered and click on 'Create Alarm'

AUDIT AND ACCOUNTABILITY / Section Content of Audit Records



6 Resource(s) Failed

035297560255, 016671749923, 197802673547, 154600454722, 240075317252, 673174758328

Compliance Section: Content of Audit Records

Informational

Ensure that audit records contain information that establishes the following:
a. What type of event occurred;
b. When the event occurred;
c. Where the event occurred;
d. Source of the event;
e. Outcome of the event; and
f. Identity of any individuals, subjects, or objects/entities associated with the event.

AWS Log metric filter and alarm does not exist for IAM policy changes

This policy identifies the AWS regions which do not have a log metric filter and alarm for IAM policy changes. Monitoring changes to IAM policies will help ensure authentication and authorization controls remain intact. It is recommended that a metric filter and alarm be established changes made to Identity and Access Management (IAM) policies.

NOTE: This policy will trigger alert if you have at least one Cloudtrail with the multi trial is enabled, Logs all management events in your account and is not set with specific log metric filter and alarm.

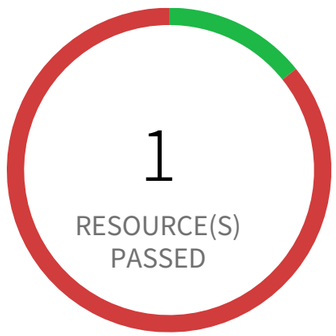
First Seen March 18, 2021 at 11:01:00 AM UTC | **Resource Type** Other

Recommendations

1. Sign in to AWS Console
2. Navigate to CloudWatch dashboard
3. Click on 'Log groups' in the 'Logs' section (Left panel)
4. Select the log group created for your CloudTrail trail event logs (CloudTrail should be multi trail enabled with all management events captured) and click 'Create Metric Filter' button.
5. In 'Define Logs Metric Filter' page, add 'Filter pattern' value as
{
($.eventName=DeleteGroupPolicy)||($.eventName=DeleteRolePolicy)||($.eventName=DeleteUserPolicy)||($.eventName=PutGroupPolicy)||($.eventName=PutRolePolicy)||($.eventName=PutUserPolicy)||($.eventName=CreatePolicy)||($.eventName=DeletePolicy)||($.eventName=CreatePolicyVersion)||($.eventName=DeletePolicyVersion)||($.eventName=AttachRolePolicy)||($.eventName=DetachRolePolicy)||($.eventName=AttachUserPolicy)||($.eventName=DetachUserPolicy)||($.eventName=AttachGroupPolicy)||($.eventName=DetachGroupPolicy) }
and Click on 'Assign Metric'
6. In 'Create Metric Filter and Assign a Metric' page, Choose Filter Name, Metric Details parameter according to your requirement and click

on 'Create Filter'
7. Click on 'Create Alarm',
- In Step 1 specify metric details and conditions details as required and click on 'Next'
- In Step 2 Select an SNS topic either by creating a new topic or use existing SNS topic/ARN and click on 'Next'
- In Step 3 Select name and description to alarm and click on 'Next'
- In Step 4 Preview your data entered and click on 'Create Alarm'

AUDIT AND ACCOUNTABILITY / Section Content of Audit Records



6 Resource(s) Failed

035297560255, 016671749923, 197802673547, 154600454722, 240075317252, 673174758328

Compliance Section: Content of Audit Records

Informational

Ensure that audit records contain information that establishes the following:
a. What type of event occurred;
b. When the event occurred;
c. Where the event occurred;
d. Source of the event;
e. Outcome of the event; and
f. Identity of any individuals, subjects, or objects/entities associated with the event.

AWS Log metric filter and alarm does not exist for unauthorized API calls

This policy identifies the AWS regions which do not have a log metric filter and alarm for unauthorized API calls. Monitoring unauthorized API calls will help reveal application errors and may reduce the time to detect malicious activity. It is recommended that a metric filter and alarm be established for unauthorized API calls.

NOTE: This policy will trigger alert if you have at least one Cloudtrail with the multi trial is enabled, Logs all management events in your account and is not set with specific log metric filter and alarm.

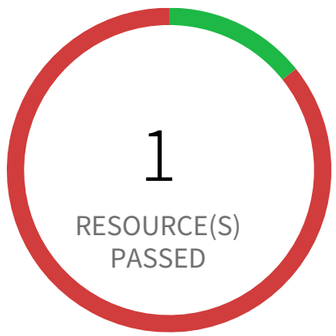
First Seen March 18, 2021 at 11:01:09 AM UTC | **Resource Type** Other

Recommendations

1. Sign in to AWS Console
2. Navigate to CloudWatch dashboard
3. Click on 'Log groups' in the 'Logs' section (Left panel)
4. Select the log group created for your CloudTrail trail event logs (CloudTrail should be multi trail enabled with all management events captured) and click 'Create Metric Filter' button.
5. In 'Define Logs Metric Filter' page, add 'Filter pattern' value as
{ ($.errorCode = "*UnauthorizedOperation") || ($.errorCode = "AccessDenied*") }
and Click on 'Assign Metric'
6. In 'Create Metric Filter and Assign a Metric' page, Choose Filter Name, Metric Details parameter according to your requirement and click on 'Create Filter'
7. Click on 'Create Alarm',
- In Step 1 specify metric details and conditions details as required and click on 'Next'
- In Step 2 Select an SNS topic either by creating a new topic or use existing SNS topic/ARN and click on 'Next'

- In Step 3 Select name and description to alarm and click on 'Next'
- In Step 4 Preview your data entered and click on 'Create Alarm'

AUDIT AND ACCOUNTABILITY / Section Content of Audit Records



6 Resource(s) Failed

035297560255, 016671749923, 197802673547, 154600454722, 240075317252, 673174758328

Compliance Section: Content of Audit Records

Informational

Ensure that audit records contain information that establishes the following:
a. What type of event occurred;
b. When the event occurred;
c. Where the event occurred;
d. Source of the event;
e. Outcome of the event; and
f. Identity of any individuals, subjects, or objects/entities associated with the event.

AWS Log metric filter and alarm does not exist for S3 bucket policy changes

This policy identifies the AWS regions which do not have a log metric filter and alarm for S3 bucket policy changes. Monitoring changes to S3 bucket policies may reduce time to detect and correct permissive policies on sensitive S3 buckets. It is recommended that a metric filter and alarm be established for changes to S3 bucket policies.

NOTE: This policy will trigger alert if you have at least one Cloudtrail with the multi trial is enabled, Logs all management events in your account and is not set with specific log metric filter and alarm.

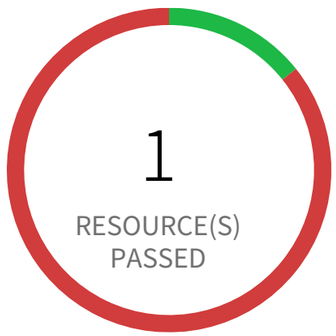
First Seen March 18, 2021 at 11:01:09 AM UTC | **Resource Type** Other

Recommendations

1. Sign in to AWS Console
2. Navigate to CloudWatch dashboard
3. Click on 'Log groups' in the 'Logs' section (Left panel)
4. Select the log group created for your CloudTrail trail event logs (CloudTrail should be multi trail enabled with all management events captured) and click 'Create Metric Filter' button.
5. In 'Define Logs Metric Filter' page, add 'Filter pattern' value as
{ ($.eventSource = s3.amazonaws.com) && (($.eventName = PutBucketAcl) || ($.eventName = PutBucketPolicy) || ($.eventName = PutBucketCors) || ($.eventName = PutBucketLifecycle) || ($.eventName = PutBucketReplication) || ($.eventName = DeleteBucketPolicy) || ($.eventName = DeleteBucketCors) || ($.eventName = DeleteBucketLifecycle) || ($.eventName = DeleteBucketReplication)) }
and Click on 'Assign Metric'
6. In 'Create Metric Filter and Assign a Metric' page, Choose Filter Name, Metric Details parameter according to your requirement and click on 'Create Filter'
7. Click on 'Create Alarm',
- In Step 1 specify metric details and conditions details as required and click on 'Next'

- In Step 2 Select an SNS topic either by creating a new topic or use existing SNS topic/ARN and click on 'Next'
- In Step 3 Select name and description to alarm and click on 'Next'
- In Step 4 Preview your data entered and click on 'Create Alarm'

AUDIT AND ACCOUNTABILITY / Section Content of Audit Records



6 Resource(s) Failed

035297560255, 016671749923, 197802673547, 154600454722, 240075317252, 673174758328

Compliance Section: Content of Audit Records

Informational

Ensure that audit records contain information that establishes the following:
a. What type of event occurred;
b. When the event occurred;
c. Where the event occurred;
d. Source of the event;
e. Outcome of the event; and
f. Identity of any individuals, subjects, or objects/entities associated with the event.

AWS Log metric filter and alarm does not exist for Network gateways changes

This policy identifies the AWS regions which do not have a log metric filter and alarm for Network gateways changes. Monitoring changes to network gateways will help ensure that all ingress/egress traffic traverses the VPC border via a controlled path. It is recommended that a metric filter and alarm be established for changes to network gateways.

NOTE: This policy will trigger alert if you have at least one Cloudtrail with the multi trial is enabled, Logs all management events in your account and is not set with specific log metric filter and alarm.

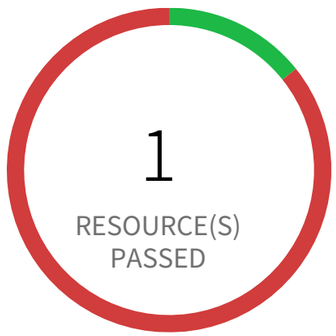
First Seen March 18, 2021 at 11:01:09 AM UTC | **Resource Type** Other

Recommendations

1. Sign in to AWS Console
2. Navigate to CloudWatch dashboard
3. Click on 'Log groups' in the 'Logs' section (Left panel)
4. Select the log group created for your CloudTrail trail event logs (CloudTrail should be multi trail enabled with all management events captured) and click 'Create Metric Filter' button.
5. In 'Define Logs Metric Filter' page, add 'Filter pattern' value as
{ ($.eventName = CreateCustomerGateway) || ($.eventName = DeleteCustomerGateway) || ($.eventName = AttachInternetGateway) || ($.eventName = CreateInternetGateway) || ($.eventName = DeleteInternetGateway) || ($.eventName = DetachInternetGateway) }
and Click on 'Assign Metric'
6. In 'Create Metric Filter and Assign a Metric' page, Choose Filter Name, Metric Details parameter according to your requirement and click on 'Create Filter'
7. Click on 'Create Alarm',
- In Step 1 specify metric details and conditions details as required and click on 'Next'
- In Step 2 Select an SNS topic either by creating a new topic or use existing SNS topic/ARN and click on 'Next'

- In Step 3 Select name and description to alarm and click on 'Next'
- In Step 4 Preview your data entered and click on 'Create Alarm'

AUDIT AND ACCOUNTABILITY / Section Content of Audit Records



6 Resource(s) Failed

035297560255, 016671749923, 197802673547, 154600454722, 240075317252, 673174758328

Compliance Section: Content of Audit Records

Informational

Ensure that audit records contain information that establishes the following:
a. What type of event occurred;
b. When the event occurred;
c. Where the event occurred;
d. Source of the event;
e. Outcome of the event; and
f. Identity of any individuals, subjects, or objects/entities associated with the event.

AWS Log metric filter and alarm does not exist for AWS Config configuration changes

This policy identifies the AWS regions which do not have a log metric filter and alarm for AWS Config configuration changes. Monitoring changes to AWS Config configuration will help ensure sustained visibility of configuration items within the AWS account. It is recommended that a metric filter and alarm be established for detecting changes to AWS Config's configurations.

NOTE: This policy will trigger alert if you have at least one Cloudtrail with the multi trial is enabled, Logs all management events in your account and is not set with specific log metric filter and alarm.

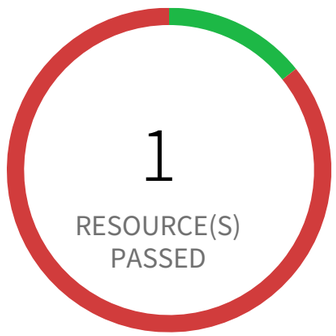
First Seen March 18, 2021 at 11:01:09 AM UTC | **Resource Type** Other

Recommendations

1. Sign in to AWS Console
2. Navigate to CloudWatch dashboard
3. Click on 'Log groups' in the 'Logs' section (Left panel)
4. Select the log group created for your CloudTrail trail event logs (CloudTrail should be multi trail enabled with all management events captured) and click 'Create Metric Filter' button.
5. In 'Define Logs Metric Filter' page, add 'Filter pattern' value as
{ ($.eventSource = config.amazonaws.com) && (($.eventName=StopConfigurationRecorder)||($.eventName=DeleteDeliveryChannel)||($.eventName=PutDeliveryChannel)||($.eventName=PutConfigurationRecorder)) }
and Click on 'Assign Metric'
6. In 'Create Metric Filter and Assign a Metric' page, Choose Filter Name, Metric Details parameter according to your requirement and click on 'Create Filter'
7. Click on 'Create Alarm',
- In Step 1 specify metric details and conditions details as required and click on 'Next'
- In Step 2 Select an SNS topic either by creating a new topic or use existing SNS topic/ARN and click on 'Next'

- In Step 3 Select name and description to alarm and click on 'Next'
- In Step 4 Preview your data entered and click on 'Create Alarm'

AUDIT AND ACCOUNTABILITY / Section Content of Audit Records



6 Resource(s) Failed

035297560255, 016671749923, 197802673547, 154600454722, 240075317252, 673174758328

Compliance Section: Content of Audit Records

Informational

Ensure that audit records contain information that establishes the following:
a. What type of event occurred;
b. When the event occurred;
c. Where the event occurred;
d. Source of the event;
e. Outcome of the event; and
f. Identity of any individuals, subjects, or objects/entities associated with the event.

AWS Log metric filter and alarm does not exist for VPC changes

This policy identifies the AWS regions which do not have a log metric filter and alarm for VPC changes. Monitoring changes to VPC will help ensure that resources and services are not unintentionally exposed. It is recommended that a metric filter and alarm be established for changes made to VPCs.

NOTE: This policy will trigger alert if you have at least one Cloudtrail with the multi trial is enabled, Logs all management events in your account and is not set with specific log metric filter and alarm.

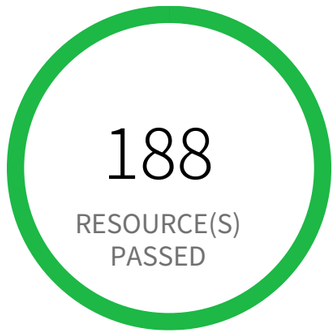
First Seen March 18, 2021 at 11:01:09 AM UTC | **Resource Type** Other

Recommendations

1. Sign in to AWS Console
2. Navigate to CloudWatch dashboard
3. Click on 'Log groups' in the 'Logs' section (Left panel)
4. Select the log group created for your CloudTrail trail event logs (CloudTrail should be multi trail enabled with all management events captured) and click 'Create Metric Filter' button.
5. In 'Define Logs Metric Filter' page, add 'Filter pattern' value as
{ ($.eventName = CreateVpc) || ($.eventName = DeleteVpc) || ($.eventName = ModifyVpcAttribute) || ($.eventName = AcceptVpcPeeringConnection) || ($.eventName = CreateVpcPeeringConnection) || ($.eventName = DeleteVpcPeeringConnection) || ($.eventName = RejectVpcPeeringConnection) || ($.eventName = AttachClassicLinkVpc) || ($.eventName = DetachClassicLinkVpc) || ($.eventName = DisableVpcClassicLink) || ($.eventName = EnableVpcClassicLink) }
and Click on 'Assign Metric'
6. In 'Create Metric Filter and Assign a Metric' page, Choose Filter Name, Metric Details parameter according to your requirement and click on 'Create Filter'
7. Click on 'Create Alarm',

- In Step 1 specify metric details and conditions details as required and click on 'Next'
- In Step 2 Select an SNS topic either by creating a new topic or use existing SNS topic/ARN and click on 'Next'
- In Step 3 Select name and description to alarm and click on 'Next'
- In Step 4 Preview your data entered and click on 'Create Alarm'

AUDIT AND ACCOUNTABILITY / Section Protection of Audit Information



0 Resource(s) Failed

Compliance Section: Protection of Audit Information

Low

a. Protect audit information and audit logging tools from unauthorized access, modification, and deletion; and b. Alert [Assignment: organization-defined personnel or roles] upon detection of unauthorized access, modification, or deletion of audit information.

AWS S3 Bucket Policy allows public access to CloudTrail logs

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

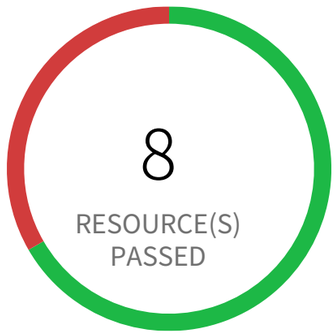
First Seen N/A | **Resource Type** Other

Recommendations

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

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

AUDIT AND ACCOUNTABILITY / Section Protection of Audit Information | Cryptographic Protection



4 Resource(s) Failed

kfirdaus-aws-cloudtrail, read-events-trail, read-event-test-cloudtrail, yuri-test-trail

Compliance Section: Protection of Audit Information | Cryptographic Protection Low

Implement cryptographic mechanisms to protect the integrity of audit information and audit tools.

AWS CloudTrail log validation is not enabled in all regions

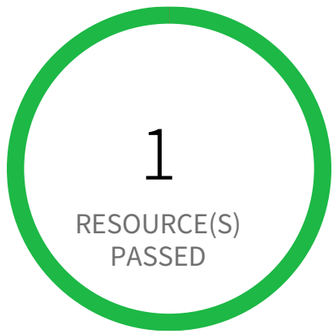
This policy identifies AWS CloudTrails in which log validation is not enabled in all regions. CloudTrail log file validation creates a digitally signed digest file containing a hash of each log that CloudTrail writes to S3. These digest files can be used to determine whether a log file was modified after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

First Seen June 29, 2021 at 3:18:58 PM UTC | **Resource Type** CloudTrail Setting

Recommendations

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

AUDIT AND ACCOUNTABILITY / Section Protection of Audit Information | Cryptographic Protection



0 Resource(s) Failed

Compliance Section: Protection of Audit Information | Cryptographic Protection

Informational

Implement cryptographic mechanisms to protect the integrity of audit information and audit tools.

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

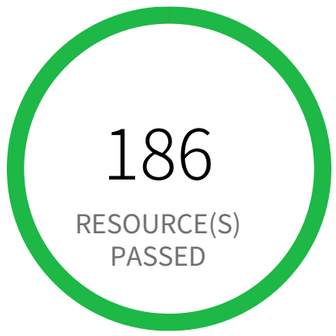
This policy identifies the AWS Kinesis streams which are encrypted with default KMS keys and not with Master Keys managed by Customer. It is a best practice to use customer managed Master Keys to encrypt your Amazon Kinesis streams data. It gives you full control over the encrypted data.

First Seen N/A | **Resource Type** Other

Recommendations

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

AUDIT AND ACCOUNTABILITY / Section Protection of Audit Information | Cryptographic Protection



0 Resource(s) Failed

Compliance Section: Protection of Audit Information | Cryptographic Protection

Low

Implement cryptographic mechanisms to protect the integrity of audit information and audit tools.

AWS S3 buckets do not have server side encryption

Customers can protect the data in S3 buckets using the AWS server-side encryption. If the server-side encryption is not turned on for S3 buckets with sensitive data, in the event of a data breach, malicious users can gain access to the data.

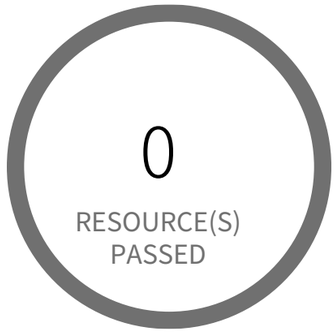
NOTE: Do NOT enable this policy if you are using 'Server-Side Encryption with Customer-Provided Encryption Keys (SSE-C).'

First Seen N/A | **Resource Type** Other

Recommendations

1. Login to the AWS Console and navigate to the 'S3' service
2. Click on the reported S3 bucket
3. Click on the 'Properties' tab
4. Under the 'Default encryption' section, choose encryption option either AES-256 or AWS-KMS based on your requirement.
For more information about Server-side encryption,
Default encryption:
https://docs.aws.amazon.com/AmazonS3/latest/dev/bucket-encryption.html
Policy based encryption:
https://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html

AUDIT AND ACCOUNTABILITY / Section Protection of Audit Information | Cryptographic Protection



0 Resource(s) Failed

Compliance Section: Protection of Audit Information | Cryptographic Protection

Low

Implement cryptographic mechanisms to protect the integrity of audit information and audit tools.

AWS Kinesis streams are not encrypted using Server Side Encryption

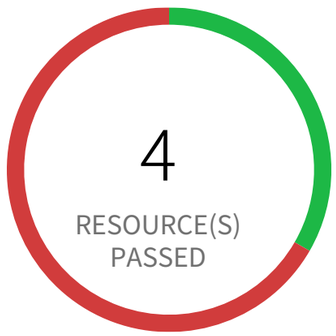
This Policy identifies the AWS Kinesis streams which are not encrypted using Server Side Encryption. Server Side Encryption is used to encrypt your sensitive data before it is written to the Kinesis stream storage layer and decrypted after it is retrieved from storage.

First Seen N/A | **Resource Type** Other

Recommendations

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

AUDIT AND ACCOUNTABILITY / Section Protection of Audit Information | Cryptographic Protection



8 Resource(s) Failed

aws-controltower-BaselineCloudTrail, kfirdaus-aws-cloudtrail, demo-pcds-sns, sedemocloudtrail, read-events-trail, yuritrail, read-event-test-cloudtrail, yuri-test-trail

Compliance Section: Protection of Audit Information | Cryptographic Protection — Informational

Implement cryptographic mechanisms to protect the integrity of audit information and audit tools.

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

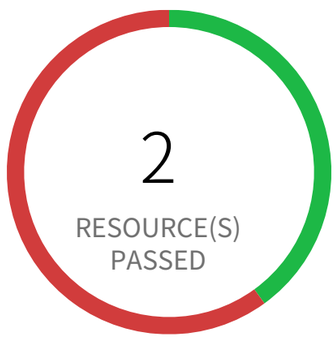
Checks to ensure that CloudTrail logs are encrypted. AWS CloudTrail is a service that enables governance, compliance, operational & risk auditing of the AWS account. It is a compliance and security best practice to encrypt the CloudTrail data since it may contain sensitive information.

First Seen August 22, 2018 at 4:44:02 AM UTC | **Resource Type** CloudTrail Setting

Recommendations

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

AUDIT AND ACCOUNTABILITY / Section Audit Record Retention



3 Resource(s) Failed

myinstance, paasdb, apprds

Compliance Section: Audit Record Retention

Low

Retain audit records for [Assignment: organization-defined time period consistent with records retention policy] to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.

AWS RDS retention policy less than 7 days

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

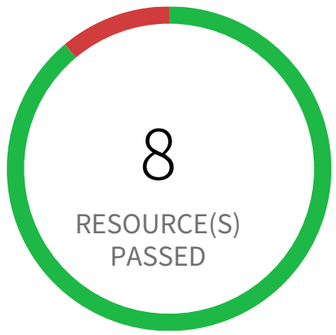
First Seen May 5, 2023 at 6:50:42 AM UTC | **Resource Type** Other

Recommendations

Configure your RDS backup retention policy to at least 7 days.

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

AUDIT AND ACCOUNTABILITY / Section Audit Record Generation | System-wide and Time-correlated Audit Trail



1 Resource(s) Failed

673174758328

Compliance Section: Audit Record Generation | System-wide and Time-correlated Audit Trail

Low

Compile audit records from [Assignment: organization-defined system components] into a system-wide (logical or physical) audit trail that is time-correlated to within [Assignment: organization-defined level of tolerance for the relationship between time stamps of individual records in the audit trail].

AWS CloudTrail is not enabled on the account

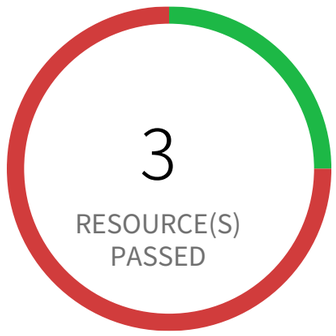
Checks to ensure that CloudTrail is enabled on the account. AWS CloudTrail is a service that enables governance, compliance, operational & risk auditing of the AWS account. It is a compliance and security best practice to turn on CloudTrail to get a complete audit trail of activities across various services.

First Seen September 6, 2023 at 9:14:30 AM UTC | **Resource Type** Other

Recommendations

1. Login to the AWS Console and navigate to the 'CloudTrail' service.
2. Follow the instructions below to enable CloudTrail on the account.
http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-create-and-update-a-trail.html

AUDIT AND ACCOUNTABILITY / Section Audit Record Generation | System-wide and Time-correlated Audit Trail



9 Resource(s) Failed

kfirdaus-aws-cloudtrail, ALL-Accounts,
demo-pcds-sns, ALL-Accounts,
read-events-trail, yuritrail,
read-event-test-cloudtrail, ALL-Accounts,
yuri-test-trail

Compliance Section: Audit Record Generation | System-wide and Time-correlated Audit Trail

Informational

Compile audit records from [Assignment: organization-defined system components] into a system-wide (logical or physical) audit trail that is time-correlated to within [Assignment: organization-defined level of tolerance for the relationship between time stamps of individual records in the audit trail].

AWS CloudTrail trail logs is not integrated with CloudWatch Log

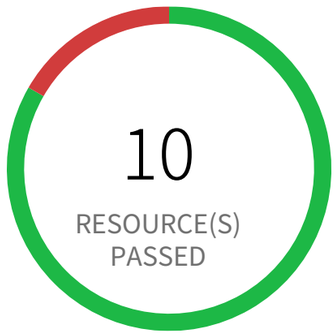
This policy identifies AWS CloudTrail which has trail logs that are not integrated with CloudWatch Log. Enabling the CloudTrail trail logs integrated with CloudWatch Logs will enable the real-time as well as historic activity logging. This will further improve monitoring and alarm capability.

First Seen January 28, 2021 at 3:01:40 AM UTC | **Resource Type** CloudTrail Setting

Recommendations

1. Login to the AWS Admin Console and access the CloudTrail service.
2. Click on the Trails in the left hand menu.
3. Click on the identified CloudTrail and navigate to the 'CloudWatch Logs' section.
4. Click on 'Configure' tab and provide required
5. Provide a log group name in field 'New or existing log group'
6. Click on 'Continue'
7. In the next page from 'IAM role' dropdown select an IAM role with required access or select the 'Create a new IAM role'
8. Click on 'Allow'

AUDIT AND ACCOUNTABILITY / Section Audit Record Generation | System-wide and Time-correlated Audit Trail



2 Resource(s) Failed

016671749923, 673174758328

Compliance Section: Audit Record Generation | System-wide and Time-correlated Audit Trail

Medium

Compile audit records from [Assignment: organization-defined system components] into a system-wide (logical or physical) audit trail that is time-correlated to within [Assignment: organization-defined level of tolerance for the relationship between time stamps of individual records in the audit trail].

AWS CloudTrail is not enabled with multi trail and not capturing all management events

This policy identifies the AWS accounts which do not have a CloudTrail with multi trail enabled and capturing all management events. AWS CloudTrail is a service that enables governance, compliance, operational & risk auditing of the AWS account. It is a compliance and security best practice to turn on CloudTrail across different regions to get a complete audit trail of activities across various services.

NOTE: If you have Organization Trail enabled in your account, this policy can be disabled, or alerts generated for this policy on such an account can be ignored; as Organization Trail by default enables trail log for all accounts under that organization.

First Seen September 6, 2023 at 8:58:29 AM UTC | **Resource Type** CloudTrail Setting

Recommendations

Refer to the following link to create/update the trail:
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-create-and-update-a-trail.html

Refer to the following link for more info on logging management events:
Logging management events - AWS CloudTrail

AUDIT AND ACCOUNTABILITY / Section Audit Record Generation | System-wide and Time-correlated Audit Trail

0 Resource(s) Failed

Compliance Section: Audit Record Generation | System-wide and Time-correlated Audit Trail

Informational

Compile audit records from [Assignment: organization-defined system components] into a system-wide (logical or physical) audit trail that is time-correlated to within [Assignment: organization-defined level of tolerance for the relationship between time stamps of individual records in the audit trail].

AWS CloudTrail logs should integrate with CloudWatch for all regions

This policy identifies the Cloudtrails which is not integrated with cloudwatch for all regions. CloudTrail uses Amazon S3 for log file storage and delivery, so log files are stored durably. In addition to capturing CloudTrail logs within a specified S3 bucket for long term analysis, realtime analysis can be performed by configuring CloudTrail to send logs to CloudWatch Logs. For a trail that is enabled in all regions in an account, CloudTrail sends log files from all those regions to a CloudWatch Logs log group. It is recommended that CloudTrail logs be sent to CloudWatch Logs.

First Seen N/A | **Resource Type** Other

Recommendations

1. Sign into AWS and navigate to CloudTrail service.
2. Click on Trail in the left menu navigation and choose the reported cloudtrail.
3. Go to CloudWatch Logs section and click Configure.
4. Define a new or select an existing log group and click Continue to complete the process.

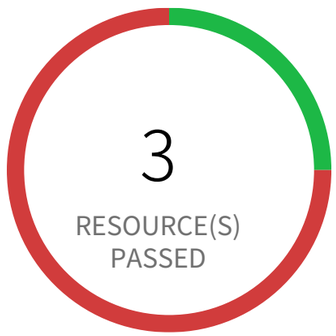
3

ASSESSMENT, AUTHORIZATION, AND MONITORING

ASSESSMENT, AUTHORIZATION, AND MONITORING Overview

Section			Pass Rate	Failed	Passed
Continuous Monitoring	AWS CloudTrail trail logs is not integrated with CloudWatch Log	Informational	25%	9	3
Continuous Monitoring	AWS Config must record all possible resources	Informational	100%	0	7
Continuous Monitoring	AWS CloudTrail logs should integrate with CloudWatch for all re…	Informational	100%	0	12
Continuous Monitoring	AWS Config Recording is disabled	Informational	15%	163	30

ASSESSMENT, AUTHORIZATION, AND MONITORING / Section Continuous Monitoring



9 Resource(s) Failed

kfirdaus-aws-cloudtrail, ALL-Accounts, demo-pcds-sns, ALL-Accounts, read-events-trail, yuritrail, read-event-test-cloudtrail, ALL-Accounts, yuri-test-trail

Compliance Section: Continuous Monitoring

Informational

Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes:
a. Establishing the following system-level metrics to be monitored: [Assignment: organization-defined system-level metrics];
b. Establishing [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessment of control effectiveness;
c. Ongoing control assessments in accordance with the continuous monitoring strategy;
d. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy;
e. Correlation and analysis of information generated by control assessments and monitoring;
f. Response actions to address results of the analysis of control assessment and monitoring information; and
g. Reporting the security and privacy status of the system to [Assignment: organization-defined personnel or roles]
[Assignment: organization-defined frequency].

AWS CloudTrail trail logs is not integrated with CloudWatch Log

This policy identifies AWS CloudTrail which has trail logs that are not integrated with CloudWatch Log. Enabling the CloudTrail trail logs integrated with CloudWatch Logs will enable the real-time as well as historic activity logging. This will further improve monitoring and alarm capability.

First Seen January 28, 2021 at 3:01:40 AM UTC | **Resource Type** CloudTrail Setting

Recommendations

1. Login to the AWS Admin Console and access the CloudTrail service.
2. Click on the Trails in the left hand menu.
3. Click on the identified CloudTrail and navigate to the 'CloudWatch Logs' section.
4. Click on 'Configure' tab and provide required
5. Provide a log group name in field 'New or existing log group'
6. Click on 'Continue'
7. In the next page from 'IAM role' dropdown select an IAM role with required access or select the 'Create a new IAM role'
8. Click on 'Allow'

ASSESSMENT, AUTHORIZATION, AND MONITORING / Section Continuous Monitoring

0 Resource(s) Failed

Compliance Section: Continuous Monitoring

Informational

Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes:
a. Establishing the following system-level metrics to be monitored: [Assignment: organization-defined system-level metrics];
b. Establishing [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessment of control effectiveness;
c. Ongoing control assessments in accordance with the continuous monitoring strategy;
d. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy;
e. Correlation and analysis of information generated by control assessments and monitoring;
f. Response actions to address results of the analysis of control assessment and monitoring information; and
g. Reporting the security and privacy status of the system to [Assignment: organization-defined personnel or roles]
[Assignment: organization-defined frequency].

AWS Config must record all possible resources

This policy identifies resources for which AWS Config recording is enabled but recording for all possible resources are disabled. AWS Config provides an inventory of your AWS resources and a history of configuration changes to these resources. You can use AWS Config to define rules that evaluate these configurations for compliance. Hence, it is important to enable this feature.

First Seen N/A | **Resource Type** Config Service Recorder

Recommendations

1. Login to the AWS and navigate to the 'Config' service
2. Change to the respective region and in the navigation pane, click on 'Settings'
3. Review the 'All resources' and Check the 2 options (3.a and 3.b)
3.a Record all resources supported in this region
3.b Include global resources (e.g., AWS IAM resources)

ASSESSMENT, AUTHORIZATION, AND MONITORING / Section Continuous Monitoring

0 Resource(s) Failed

Compliance Section: Continuous Monitoring

Informational

Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes:
a. Establishing the following system-level metrics to be monitored: [Assignment: organization-defined system-level metrics];
b. Establishing [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessment of control effectiveness;
c. Ongoing control assessments in accordance with the continuous monitoring strategy;
d. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy;
e. Correlation and analysis of information generated by control assessments and monitoring;
f. Response actions to address results of the analysis of control assessment and monitoring information; and
g. Reporting the security and privacy status of the system to [Assignment: organization-defined personnel or roles]
[Assignment: organization-defined frequency].

AWS CloudTrail logs should integrate with CloudWatch for all regions

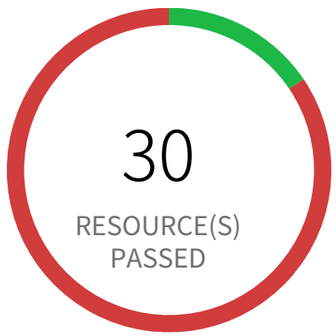
This policy identifies the Cloudtrails which is not integrated with cloudwatch for all regions. CloudTrail uses Amazon S3 for log file storage and delivery, so log files are stored durably. In addition to capturing CloudTrail logs within a specified S3 bucket for long term analysis, realtime analysis can be performed by configuring CloudTrail to send logs to CloudWatch Logs. For a trail that is enabled in all regions in an account, CloudTrail sends log files from all those regions to a CloudWatch Logs log group. It is recommended that CloudTrail logs be sent to CloudWatch Logs.

First Seen N/A | **Resource Type** Other

Recommendations

1. Sign into AWS and navigate to CloudTrail service.
2. Click on Trail in the left menu navigation and choose the reported cloudtrail.
3. Go to CloudWatch Logs section and click Configure.
4. Define a new or select an existing log group and click Continue to complete the process.

ASSESSMENT, AUTHORIZATION, AND MONITORING / Section Continuous Monitoring



163 Resource(s) Failed

035297560255:AWS Bahrain, 035297560255:AWS Mumbai, 035297560255:AWS Paris, 035297560255:AWS Melbourne, 035297560255:AWS Canada, 035297560255:AWS Milan, 035297560255:AWS Israel, 035297560255:AWS Spain, 035297560255:AWS Jakarta, 035297560255:AWS Zurich & 153 more

Compliance Section: Continuous Monitoring

Informational

Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes:
a. Establishing the following system-level metrics to be monitored: [Assignment: organization-defined system-level metrics];
b. Establishing [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessment of control effectiveness;
c. Ongoing control assessments in accordance with the continuous monitoring strategy;
d. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy;
e. Correlation and analysis of information generated by control assessments and monitoring;
f. Response actions to address results of the analysis of control assessment and monitoring information; and
g. Reporting the security and privacy status of the system to [Assignment: organization-defined personnel or roles]
[Assignment: organization-defined frequency].

AWS Config Recording is disabled

AWS Config is a web service that performs configuration management of supported AWS resources within your account and delivers log files to you. AWS config uses configuration recorder to detect changes in your resource configurations and capture these changes as configuration items. It continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. This policy generates alerts when AWS Config recorder is not enabled.

First Seen March 18, 2020 at 6:13:50 AM UTC | **Resource Type** Other

Recommendations

1. Sign in to the AWS Management Console
2. Select the specific region from the top down, for which the alert is generated
3. Navigate to service 'Config' from the 'Services' dropdown.
If AWS Config set up exists,
a. Go to Settings
b. Click on 'Turn On' button under 'Recording is Off' section,
c. provide required information for bucket and role with proper permission

If AWS Config set up doesn't exist
a. Click on 'Get Started'
b. For Step 1, Tick the check box for 'Record all resources supported in this region' under section 'Resource types to record'
c. Under section 'Amazon S3 bucket', select bucket with permission to Config services
d. Under section 'AWS Config role', select a role with permission to Config services
e. Click on 'Next'
f. For Step 2, Select required rule and click on 'Next' otherwise click on 'Skip'
g. For Step 3, Review the created 'Settings' and click on 'Confirm'

4

CONFIGURATION MANAGEMENT

CONFIGURATION MANAGEMENT Overview

Section	Pass Rate	Failed	Passed
Baseline Configuration | Automation Support for Accuracy and Currency — Informational	100%	0	7
Baseline Configuration | Automation Support for Accuracy and Currency — Informational	15%	163	30
Access Restrictions for Change | Automated Access Enforcement and Audit Records — Informational	96%	7	181
Access Restrictions for Change | Automated Access Enforcement and Audit Records — Informational	9%	168	18
Access Restrictions for Change | Automated Access Enforcement and Audit Records — Informational	100%	0	4
Access Restrictions for Change | Automated Access Enforcement and Audit Records — Informational	100%	0	0
Configuration Settings — AWS Config must record all possible resources — Informational	100%	0	7
Configuration Settings — AWS Config Recording is disabled — Informational	15%	163	30

NIST 800-53 Rev 5 / CONFIGURATION MANAGEMENT

Section	Pass Rate	Failed	Passed
Configuration Settings — AWS EMR cluster is not configured with security configuration — Informational	100%	0	0
System Component Inventory | Assessed Configurations and Approved Deviations — Informational	15%	163	30

CONFIGURATION MANAGEMENT / Section Baseline Configuration | Automation Support for Accuracy and Currency

0 Resource(s) Failed

Compliance Section: Baseline Configuration | Automation Support for Accuracy and Currency

Informational

Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using [Assignment: organization-defined automated mechanisms].

AWS Config must record all possible resources

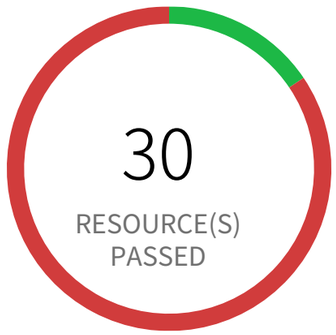
This policy identifies resources for which AWS Config recording is enabled but recording for all possible resources are disabled. AWS Config provides an inventory of your AWS resources and a history of configuration changes to these resources. You can use AWS Config to define rules that evaluate these configurations for compliance. Hence, it is important to enable this feature.

First Seen N/A | **Resource Type** Config Service Recorder

Recommendations

1. Login to the AWS and navigate to the 'Config' service
2. Change to the respective region and in the navigation pane, click on 'Settings'
3. Review the 'All resources' and Check the 2 options (3.a and 3.b)
3.a Record all resources supported in this region
3.b Include global resources (e.g., AWS IAM resources)

CONFIGURATION MANAGEMENT / Section Baseline Configuration | Automation Support for Accuracy and Currency



163 Resource(s) Failed

035297560255:AWS Bahrain, 035297560255:AWS Mumbai, 035297560255:AWS Paris, 035297560255:AWS Melbourne, 035297560255:AWS Canada, 035297560255:AWS Milan, 035297560255:AWS Israel, 035297560255:AWS Spain, 035297560255:AWS Jakarta, 035297560255:AWS Zurich & 153 more

Compliance Section: Baseline Configuration | Automation Support for Accuracy and Currency

Informational

Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using [Assignment: organization-defined automated mechanisms].

AWS Config Recording is disabled

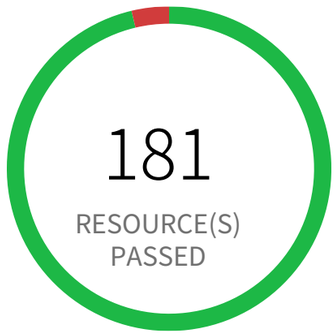
AWS Config is a web service that performs configuration management of supported AWS resources within your account and delivers log files to you. AWS config uses configuration recorder to detect changes in your resource configurations and capture these changes as configuration items. It continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. This policy generates alerts when AWS Config recorder is not enabled.

First Seen March 18, 2020 at 6:13:50 AM UTC | **Resource Type** Other

Recommendations

1. Sign in to the AWS Management Console
2. Select the specific region from the top down, for which the alert is generated
3. Navigate to service 'Config' from the 'Services' dropdown.
If AWS Config set up exists,
a. Go to Settings
b. Click on 'Turn On' button under 'Recording is Off' section,
c. provide required information for bucket and role with proper permission
If AWS Config set up doesn't exist
a. Click on 'Get Started'
b. For Step 1, Tick the check box for 'Record all resources supported in this region' under section 'Resource types to record'
c. Under section 'Amazon S3 bucket', select bucket with permission to Config services
d. Under section 'AWS Config role', select a role with permission to Config services
e. Click on 'Next'
f. For Step 2, Select required rule and click on 'Next' otherwise click on 'Skip'
g. For Step 3, Review the created 'Settings' and click on 'Confirm'

CONFIGURATION MANAGEMENT / Section Access Restrictions for Change | Automated Access Enforcement and Audit Records



7 Resource(s) Failed

kfirdaus-aws-bucket, demo-bucket-pcds-root, sedemocloudtrail, aws-cloudtrail-logs-240075317252-884b0070, read-events-test-plan-cloudtrail-s3-bucket, read-event-ct, yuricloudtrail.puresec-dev-2.puresec.io

Compliance Section: Access Restrictions for Change | Automated Access Enforcement and Audit Records

Informational

(a) Enforce access restrictions using [Assignment: organization-defined automated mechanisms]; and
(b) Automatically generate audit records of the enforcement actions.

AWS S3 CloudTrail bucket for which access logging is disabled

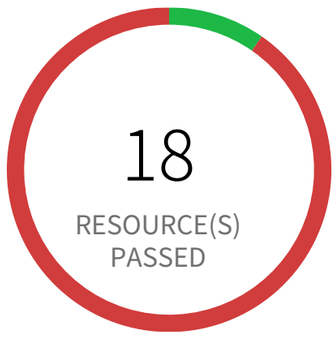
This policy identifies S3 CloudTrail buckets for which access is disabled. S3 Bucket access logging generates access records for each request made to your S3 bucket. An access log record contains information such as the request type, the resources specified in the request worked, and the time and date the request was processed. It is recommended that bucket access logging be enabled on the CloudTrail S3 bucket.

First Seen February 3, 2021 at 7:24:13 PM UTC | **Resource Type** Other

Recommendations

1. Login to the AWS Console and navigate to the 'S3' service.
2. Click on the the S3 bucket that was reported.
3. Click on the 'Properties' tab.
4. Under the 'Server access logging' section, select 'Enable' option and provide s3 bucket of your choice in the 'Target bucket'
5. Click on 'Save Changes'

CONFIGURATION MANAGEMENT / Section Access Restrictions for Change | Automated Access Enforcement and Audit Records



168 Resource(s) Failed

totalmess-s3-q4ns, kfirdaus-aws-bucket, cf-templates-1g3mmga26xna6-us-east-2, cf-templates-1g3mmga26xna6-us-east-1, cf-templates-m1lan4o379zj-us-east-2, demo-sam-deployment, pcsdemo-hyperdrive-log4j-s3bucket1, corporatecontracts, pos-payment-backup, corporatemarketingcontent & 158 more

Compliance Section: Access Restrictions for Change | Automated Access Enforcement and Audit Records

Informational

(a) Enforce access restrictions using [Assignment: organization-defined automated mechanisms]; and
(b) Automatically generate audit records of the enforcement actions.

AWS Access logging not enabled on S3 buckets

Checks for S3 buckets without access logging turned on. Access logging allows customers to view complete audit trail on sensitive workloads such as S3 buckets. It is recommended that Access logging is turned on for all S3 buckets to meet audit & compliance requirement

First Seen March 18, 2021 at 11:01:09 AM UTC | **Resource Type** Bucket Logging Config

Recommendations

1. Login to the AWS Console and navigate to the 'S3' service.
2. Click on the the S3 bucket that was reported.
3. Click on the 'Properties' tab.
4. Under the 'Server access logging' section, select 'Enable logging' option.

CONFIGURATION MANAGEMENT / Section Access Restrictions for Change | Automated Access Enforcement and Audit Records

0 Resource(s) Failed

Compliance Section: Access Restrictions for Change | Automated Access Enforcement and Audit Records

Informational

(a) Enforce access restrictions using [Assignment: organization-defined automated mechanisms]; and
(b) Automatically generate audit records of the enforcement actions.

AWS Certificate Manager (ACM) has certificates with Certificate Transparency Logging disabled

This policy identifies AWS Certificate Manager certificates in which Certificate Transparency Logging is disabled. AWS Certificate Manager (ACM) is the preferred tool to provision, manage, and deploy your server certificates. Certificate Transparency Logging is used to guard against SSL/TLS certificates that are issued by mistake or by a compromised CA, some browsers require that public certificates issued for your domain can also be recorded. This policy generates alerts for certificates which have transparency logging disabled. As a best practice, it is recommended to enable Transparency logging for all certificates.

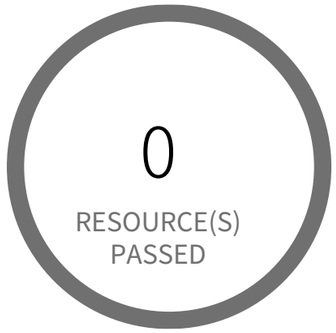
First Seen N/A | **Resource Type** Other

Recommendations

You cannot currently use the console to opt out of or into transparency logging. It's recommended to use the command line utility to enable transparency logging.

Remediation CLI:
1. Use the below command to list ACM certificate
aws acm list-certificates
2. Note the 'CertificateArn' of the reported ACM certificate
3. Use the below command to ENABLE Certificate Transparency Logging
aws acm update-certificate-options --certificate-arn <certificateARN> --options CertificateTransparencyLoggingPreference=ENABLED
where 'CertificateArn' is captured in the step2

CONFIGURATION MANAGEMENT / Section Access Restrictions for Change | Automated Access Enforcement and Audit Records



0 Resource(s) Failed

Compliance Section: Access Restrictions for Change | Automated Access Enforcement and Audit Records

Informational

(a) Enforce access restrictions using [Assignment: organization-defined automated mechanisms]; and
(b) Automatically generate audit records of the enforcement actions.

AWS Redshift database does not have audit logging enabled

Audit logging is not enabled by default in Amazon Redshift. When you enable logging on your cluster, Amazon Redshift creates and uploads logs to Amazon S3 that capture data from the creation of the cluster to the present time.

First Seen N/A | **Resource Type** Managed Database

Recommendations

1. Login to AWS Console.
2. Goto Amazon Redshift service
3. On left navigation panel, click on Clusters
4. Click on the reported cluster
5. Click on Database tab and choose 'Configure Audit Logging'
6. On Enable Audit Logging, choose 'Yes'
7. Create a new s3 bucket or use an existing bucket
8. click Save

CONFIGURATION MANAGEMENT / Section Configuration Settings

0 Resource(s) Failed

Compliance Section: Configuration Settings

Informational

a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using [Assignment: organization-defined common secure configurations];
b. Implement the configuration settings;
c. Identify, document, and approve any deviations from established configuration settings for [Assignment: organization-defined system components] based on [Assignment: organization-defined operational requirements]; and
d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

AWS Config must record all possible resources

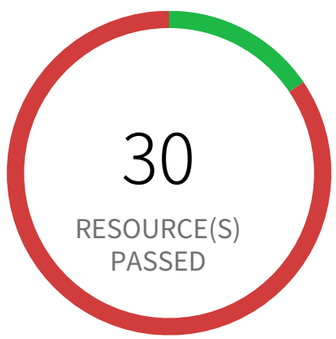
This policy identifies resources for which AWS Config recording is enabled but recording for all possible resources are disabled. AWS Config provides an inventory of your AWS resources and a history of configuration changes to these resources. You can use AWS Config to define rules that evaluate these configurations for compliance. Hence, it is important to enable this feature.

First Seen N/A | **Resource Type** Config Service Recorder

Recommendations

1. Login to the AWS and navigate to the 'Config' service
2. Change to the respective region and in the navigation pane, click on 'Settings'
3. Review the 'All resources' and Check the 2 options (3.a and 3.b)
3.a Record all resources supported in this region
3.b Include global resources (e.g., AWS IAM resources)

CONFIGURATION MANAGEMENT / Section Configuration Settings



163 Resource(s) Failed

035297560255:AWS Bahrain, 035297560255:AWS Mumbai, 035297560255:AWS Paris, 035297560255:AWS Melbourne, 035297560255:AWS Canada, 035297560255:AWS Milan, 035297560255:AWS Israel, 035297560255:AWS Spain, 035297560255:AWS Jakarta, 035297560255:AWS Zurich & 153 more

Compliance Section: Configuration Settings

Informational

a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using [Assignment: organization-defined common secure configurations];
b. Implement the configuration settings;
c. Identify, document, and approve any deviations from established configuration settings for [Assignment: organization-defined system components] based on [Assignment: organization-defined operational requirements]; and
d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

AWS Config Recording is disabled

AWS Config is a web service that performs configuration management of supported AWS resources within your account and delivers log files to you. AWS config uses configuration recorder to detect changes in your resource configurations and capture these changes as configuration items. It continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. This policy generates alerts when AWS Config recorder is not enabled.

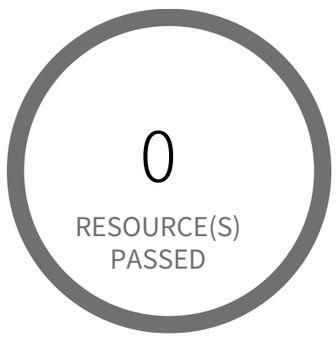
First Seen March 18, 2020 at 6:13:50 AM UTC | **Resource Type** Other

Recommendations

1. Sign in to the AWS Management Console
2. Select the specific region from the top down, for which the alert is generated
3. Navigate to service 'Config' from the 'Services' dropdown.
If AWS Config set up exists,
a. Go to Settings
b. Click on 'Turn On' button under 'Recording is Off' section,
c. provide required information for bucket and role with proper permission
If AWS Config set up doesn't exist
a. Click on 'Get Started'
b. For Step 1, Tick the check box for 'Record all resources supported in this region' under section 'Resource types to record'
c. Under section 'Amazon S3 bucket', select bucket with permission to Config services
d. Under section 'AWS Config role', select a role with permission to Config services
e. Click on 'Next'

f. For Step 2, Select required rule and click on 'Next' otherwise click on 'Skip'
g. For Step 3, Review the created 'Settings' and click on 'Confirm'

CONFIGURATION MANAGEMENT / Section Configuration Settings



0 Resource(s) Failed

Compliance Section: Configuration Settings

Informational

a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using [Assignment: organization-defined common secure configurations];
b. Implement the configuration settings;
c. Identify, document, and approve any deviations from established configuration settings for [Assignment: organization-defined system components] based on [Assignment: organization-defined operational requirements]; and
d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

AWS EMR cluster is not configured with security configuration

This policy identifies EMR clusters which are not configured with security configuration. With Amazon EMR release version 4.8.0 or later, you can use security configurations to configure data encryption, Kerberos authentication, and Amazon S3 authorization for EMRFS.

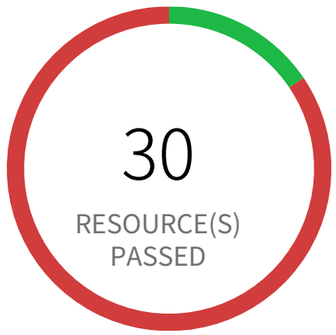
First Seen N/A | **Resource Type** Other

Recommendations

1. Log in to the AWS Console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated.
3. Navigate to 'EMR' dashboard from 'Services' dropdown
4. Go to 'Security configurations', click 'Create'
5. On the Create security configuration window,
6. In 'Name' box, provide a name for the new EMR security configuration
7. Follow below link to configure a security configuration
https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-create-security-configuration.html
8. Click on 'Create' button
9. On the left menu of EMR dashboard Click 'Clusters'
10. Select the EMR cluster for which the alert has been generated and click on the 'Clone' button from the top menu.
11. In the Cloning popup, choose 'Yes' and Click 'Clone'
12. On the Create Cluster page, in the Security Options section, click on 'security configuration'
13. From the 'Security configuration' drop down select the name of the security configuration created at step 4 to step 8, click 'Create Cluster'.

14. Once you the new cluster is set up verify its working and terminate the source cluster in order to stop incurring charges for it
15. On the left menu of EMR dashboard Click 'Clusters', from the list of clusters select the source cluster which is alerted
16. Click on the 'Terminate' button from the top menu
17. On the 'Terminate clusters' pop-up, click 'Terminate'

CONFIGURATION MANAGEMENT / System Component Inventory | Assessed Configurations and Approved Deviations



163 Resource(s) Failed

035297560255:AWS Bahrain, 035297560255:AWS Mumbai, 035297560255:AWS Paris, 035297560255:AWS Melbourne, 035297560255:AWS Canada, 035297560255:AWS Milan, 035297560255:AWS Israel, 035297560255:AWS Spain, 035297560255:AWS Jakarta, 035297560255:AWS Zurich & 153 more

Compliance Section: System Component Inventory | Assessed Configurations and Approved Deviations

Informational

Include assessed component configurations and any approved deviations to current deployed configurations in the system component inventory.

AWS Config Recording is disabled

AWS Config is a web service that performs configuration management of supported AWS resources within your account and delivers log files to you. AWS config uses configuration recorder to detect changes in your resource configurations and capture these changes as configuration items. It continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. This policy generates alerts when AWS Config recorder is not enabled.

First Seen March 18, 2020 at 6:13:50 AM UTC | **Resource Type** Other

Recommendations

1. Sign in to the AWS Management Console
2. Select the specific region from the top down, for which the alert is generated
3. Navigate to service 'Config' from the 'Services' dropdown.
If AWS Config set up exists,
a. Go to Settings
b. Click on 'Turn On' button under 'Recording is Off' section,
c. provide required information for bucket and role with proper permission
If AWS Config set up doesn't exist
a. Click on 'Get Started'
b. For Step 1, Tick the check box for 'Record all resources supported in this region' under section 'Resource types to record'
c. Under section 'Amazon S3 bucket', select bucket with permission to Config services
d. Under section 'AWS Config role', select a role with permission to Config services
e. Click on 'Next'
f. For Step 2, Select required rule and click on 'Next' otherwise click on 'Skip'
g. For Step 3, Review the created 'Settings' and click on 'Confirm'

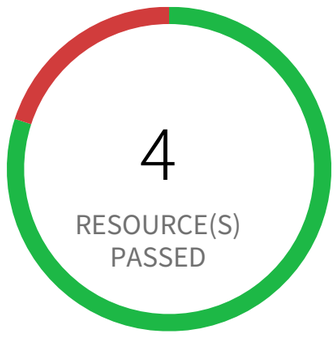
5

CONTINGENCY PLANNING

CONTINGENCY PLANNING Overview

Section			Pass Rate	Failed	Passed
System Backup	AWS RDS instance without Automatic Backup setting	•••• Low	80%	1	4

CONTINGENCY PLANNING / Section System Backup



1 Resource(s) Failed

apprds

Compliance Section: System Backup

Low

a. Conduct backups of user-level information contained in [Assignment: organization-defined system components]
[Assignment: organization-defined frequency consistent with recovery time and recovery point objectives];
b. Conduct backups of system-level information contained in the system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives];
c. Conduct backups of system documentation, including security- and privacy-related documentation [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; and
d. Protect the confidentiality, integrity, and availability of backup information.

AWS RDS instance without Automatic Backup setting

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

First Seen June 22, 2023 at 10:45:19 AM UTC | **Resource Type** Other

Recommendations

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

6

IDENTIFICATION AND AUTHENTICATION

IDENTIFICATION AND AUTHENTICATION Overview

Section	Pass Rate	Failed	Passed
Identification and Authentication (organizational Users) AWS S3 bucket is··· Low	98%	3	183
Identification and Authentication (organizational Users) AWS··· Informational	96%	7	181
Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts Medium	80%	4	16
Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts Low	100%	0	19
Identification and Authentication (organizational Users) | Multi-factor Authentication to Non-privileged Accounts Medium	80%	4	16
Identification and Authentication (organizational Users) | Multi-factor Authentication to Non-privileged Accounts Low	100%	0	19
Identification and Authentication (organizational Users) | Access to Accounts — Separate Device Medium	50%	2	2

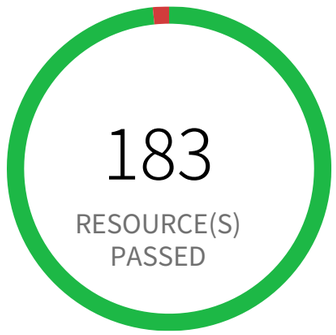
NIST 800-53 Rev 5 / IDENTIFICATION AND AUTHENTICATION

Section			Pass Rate	Failed	Passed
Identification and Authentication (organizational Users) | Access to Accounts — Separate Device		Medium	80%	4	16
Identification and Authentication (organizational Users) | Access to Accounts — Separate Device		Low	100%	0	19
Authenticator Management	AWS S3 bucket is not configured with MFA Delete	Low	98%	3	183
Authenticator Management	AWS CloudTrail S3 buckets have not enabled MFA Delete	Informational	96%	7	181
Authenticator Management | Password-based Authentication	AV	Informational	57%	3	4
Authenticator Management | Password-based Authentication	AV	Informational	57%	3	4
Authenticator Management | Password-based Authentication	AWS IAM…	Low	57%	3	4
Authenticator Management | Password-based Authentication	AV	Informational	57%	3	4
Authenticator Management | Password-based Authentication	AV	Informational	57%	3	4
Authenticator Management | Password-based Authentication	AWS IAM…	Low	100%	0	7

NIST 800-53 Rev 5 / IDENTIFICATION AND AUTHENTICATION

Section			Pass Rate	Failed	Passed
Authenticator Management | Password-based Authentication	AV	Informational	57%	3	4
Authenticator Management | Password-based Authentication	AV	Informational	57%	3	4
Authenticator Management | Password-based Authentication	AV	Informational	57%	3	4
Authenticator Management | Public Key-based Authentication	A	Informational	100%	0	4
Authenticator Management | Public Key-based Authentication	AWS···	Low	100%	0	4
Authenticator Management | Public Key-based Authentication	AWS API··	Low	15%	17	3
Authenticator Management | Public Key-based Authentication	AWS···	Low	100%	0	4
Authenticator Management | Expiration of Cached Authenticators	AWS	Low	100%	0	0
Service Identification and Authentication	AWS ElastiCache Redis cluster with Redis···	Low	100%	0	0
Service Identification and Authentication	AWS EMR cluster is not configured with Ker···	Low	100%	0	0

IDENTIFICATION AND AUTHENTICATION / Section Identification and Authentication (organizational Users)



3 Resource(s) Failed

demoappdashboard-deployments-mobile-hub-12027657, elad-bucket1, izabellatest1

Compliance Section: Identification and Authentication (organizational Users)

Low

Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

AWS S3 bucket is not configured with MFA Delete

This policy identifies the S3 buckets which do not have Multi-Factor Authentication(MFA) enabled to delete S3 object version. Enabling MFA Delete on a versioned bucket adds another layer of protection. In order to permanently delete an object version or suspend or reactivate versioning on the bucket valid code from the account's MFA device required.

Note: MFA Delete only works for CLI or API interaction, not in the AWS Management Console. Also, you cannot make version DELETE actions with MFA using IAM user credentials. You must use your root AWS account.

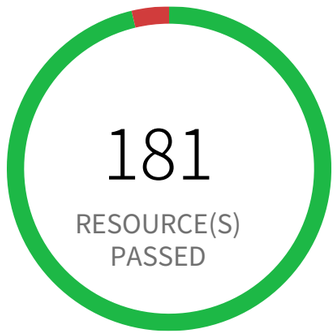
First Seen April 20, 2021 at 6:01:04 PM UTC | **Resource Type** Other

Recommendations

Using console you can enable versioning on the bucket but you cannot enable MFA delete.
You can do it via only with the AWS CLI:
aws s3api put-bucket-versioning --bucket <BUCKET_NAME> --versioning-configuration Status=Enabled,MFADelete=Enabled --mfa "<MFA_SERIAL_NUMBER> <MFA_CODE>"

NOTE: The bucket owner, the AWS account that created the bucket (root account), and all authorized IAM users can enable versioning, but only the bucket owner (root account) can enable MFA Delete. Successful execution will enable the S3 bucket versioning and MFA delete on the bucket.

IDENTIFICATION AND AUTHENTICATION / Section Identification and Authentication (organizational Users)



7 Resource(s) Failed

kfirdaus-aws-bucket, demo-bucket-pcds-root, sedemocloudtrail, aws-cloudtrail-logs-240075317252-884b0070, read-events-test-plan-cloudtrail-s3-bucket, read-event-ct, vuricloudtrail.puresec-dev-2.puresec.io

Compliance Section: Identification and Authentication (organizational Users)

Informational

Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

AWS CloudTrail S3 buckets have not enabled MFA Delete

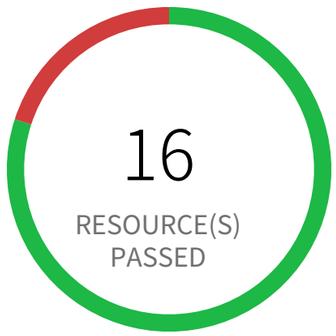
This policy identifies the S3 buckets which do not have Multi-Factor Authentication enabled for CloudTrails. For encryption of log files, CloudTrail defaults to use of S3 server-side encryption (SSE). We recommend adding an additional layer of security by adding MFA Delete to your S3 bucket. This will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

First Seen February 3, 2021 at 7:24:07 PM UTC | **Resource Type** Other

Recommendations

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

IDENTIFICATION AND AUTHENTICATION / Section Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts



4 Resource(s) Failed

<root_account>, <root_account>, <root_account>, <root_account>

Compliance Section: Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts

Medium

Implement multi-factor authentication for access to privileged accounts.

AWS MFA is not enabled on Root account

This policy identifies root account which has MFA enabled. Root accounts have privileged access to all AWS services. Without MFA, if the root credentials are compromised, unauthorized users will get full access to your account.

NOTE: This policy does not apply to AWS GovCloud Accounts. As you cannot enable an MFA device for AWS GovCloud (US) account root user. For more details refer: https://docs.aws.amazon.com/govcloud-us/latest/UserGuide/govcloud-console.html

First Seen April 20, 2023 at 11:28:40 PM UTC | **Resource Type** IAM Account Summary

Recommendations

1. Sign in to the 'AWS Console' using Root credentials.
2. Navigate to the 'IAM' service.
3. On the dashboard, click on 'Activate MFA on your root account', click on 'Manage MFA' and follow the steps to configure MFA for the root account.

IDENTIFICATION AND AUTHENTICATION / Section Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts

0 Resource(s) Failed

Compliance Section: Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts

Low

Implement multi-factor authentication for access to privileged accounts.

AWS MFA not enabled for IAM users

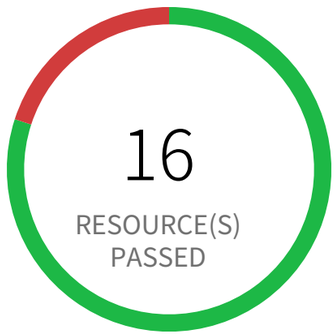
This policy identifies AWS IAM users for whom MFA is not enabled. AWS Multi-Factor Authentication (MFA) is a simple best practice that adds an extra layer of protection on top of your user name and password. Multiple factors provide increased security for your AWS account settings and resources.

First Seen N/A | **Resource Type** IAM Credentials Report

Recommendations

1. Sign in to the AWS and navigate to the 'IAM' service.
2. Navigate to the user that was reported in the alert.
3. Under 'Security Credentials', check "Assigned MFA Device" and follow the instructions to enable MFA for the user.

IDENTIFICATION AND AUTHENTICATION / Section Identification and Authentication (organizational Users) | Multi-factor Authentication to Non-privileged Accounts



4 Resource(s) Failed

<root_account>, <root_account>, <root_account>, <root_account>

Compliance Section: Identification and Authentication (organizational Users) | Multi-factor Authentication to Non-privileged Accounts

Medium

Implement multi-factor authentication for access to non-privileged accounts.

AWS MFA is not enabled on Root account

This policy identifies root account which has MFA enabled. Root accounts have privileged access to all AWS services. Without MFA, if the root credentials are compromised, unauthorized users will get full access to your account.

NOTE: This policy does not apply to AWS GovCloud Accounts. As you cannot enable an MFA device for AWS GovCloud (US) account root user. For more details refer: https://docs.aws.amazon.com/govcloud-us/latest/UserGuide/govcloud-console.html

First Seen April 20, 2023 at 11:28:40 PM UTC | **Resource Type** IAM Account Summary

Recommendations

1. Sign in to the 'AWS Console' using Root credentials.
2. Navigate to the 'IAM' service.
3. On the dashboard, click on 'Activate MFA on your root account', click on 'Manage MFA' and follow the steps to configure MFA for the root account.

IDENTIFICATION AND AUTHENTICATION / Section Identification and Authentication (organizational Users) | Multi-factor Authentication to Non-privileged Accounts

0 Resource(s) Failed

Compliance Section: Identification and Authentication (organizational Users) | Multi-factor Authentication to Non-privileged Accounts

Low

Implement multi-factor authentication for access to non-privileged accounts.

AWS MFA not enabled for IAM users

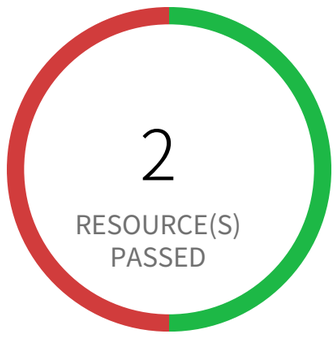
This policy identifies AWS IAM users for whom MFA is not enabled. AWS Multi-Factor Authentication (MFA) is a simple best practice that adds an extra layer of protection on top of your user name and password. Multiple factors provide increased security for your AWS account settings and resources.

First Seen N/A | **Resource Type** IAM Credentials Report

Recommendations

1. Sign in to the AWS and navigate to the 'IAM' service.
2. Navigate to the user that was reported in the alert.
3. Under 'Security Credentials', check "Assigned MFA Device" and follow the instructions to enable MFA for the user.

IDENTIFICATION AND AUTHENTICATION / Section Identification and Authentication (organizational Users) | Access to Accounts — Separate Device



2 Resource(s) Failed

arn:aws:iam::154600454722:mfa/root-account-mfa-device,
arn:aws:iam::240075317252:mfa/root-account-mfa-device

Compliance Section: Identification and Authentication (organizational Users) | Access to Accounts — Separate Device

Medium

Implement multi-factor authentication for [Selection (one or more): local; network; remote] access to [Selection (one or more): privileged accounts; non-privileged accounts] such that:
(a) One of the factors is provided by a device separate from the system gaining access; and
(b) The device meets [Assignment: organization-defined strength of mechanism requirements].

AWS root account configured with Virtual MFA

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

First Seen November 18, 2020 at 10:06:25 PM UTC | **Resource Type** Other

Recommendations

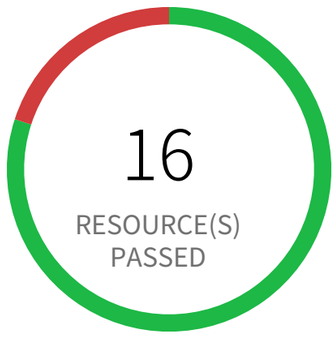
To manage MFA devices for your AWS account, you must use your root user credentials to sign in to AWS. You cannot manage MFA devices for the root user while signed in with other credentials.

1. Sign in to the AWS Management Console with your root user credentials
2. Go to IAM
3. Do one of the following:
Option 1: Choose Dashboard, and under Security Status, expand Activate MFA on your root account.
Option 2: On the right side of the navigation bar, select your account name, and then choose My Security Credentials. If necessary, choose Continue to Security Credentials. Then expand the Multi-Factor Authentication (MFA) section on the page.
4. Choose Manage MFA or Activate MFA, depending on which option you chose in the preceding step.
5. In the wizard, choose A hardware MFA device and then choose Next Step.

6. If you have U2F security key as hardware MFA device, choose U2F security key and click on Continue. Next plug the USB U2F security key, when setup is complete click on Close.
If you have any other hardware MFA device, choose Other hardware MFA device option
a. In the Serial Number box, type the serial number that is found on the back of the MFA device.
b. In the Authentication Code 1 box, type the six-digit number displayed by the MFA device. You might need to press the button on the front of the device to display the number.
c. Wait 30 seconds while the device refreshes the code, and then type the next six-digit number into the Authentication Code 2 box. You might need to press the button on the front of the device again to display the second number.
d. Choose Next Step. The MFA device is now associated with the AWS account.

Important:
Submit your request immediately after generating the authentication codes. If you generate the codes and then wait too long to submit the request, the MFA device successfully associates with the user but the MFA device becomes out of sync. This happens because time-based one-time passwords (TOTP) expire after a short period of time. If this happens, you can resync the device.

IDENTIFICATION AND AUTHENTICATION / Section Identification and Authentication (organizational Users) | Access to Accounts — Separate Device



4 Resource(s) Failed

<root_account>, <root_account>, <root_account>, <root_account>

Compliance Section: Identification and Authentication (organizational Users) | Access to Accounts — Separate Device

Medium

Implement multi-factor authentication for [Selection (one or more): local; network; remote] access to [Selection (one or more): privileged accounts; non-privileged accounts] such that:
(a) One of the factors is provided by a device separate from the system gaining access; and
(b) The device meets [Assignment: organization-defined strength of mechanism requirements].

AWS MFA is not enabled on Root account

This policy identifies root account which has MFA enabled. Root accounts have privileged access to all AWS services. Without MFA, if the root credentials are compromised, unauthorized users will get full access to your account.

NOTE: This policy does not apply to AWS GovCloud Accounts. As you cannot enable an MFA device for AWS GovCloud (US) account root user. For more details refer: https://docs.aws.amazon.com/govcloud-us/latest/UserGuide/govcloud-console.html

First Seen April 20, 2023 at 11:28:40 PM UTC | **Resource Type** IAM Account Summary

Recommendations

1. Sign in to the 'AWS Console' using Root credentials.
2. Navigate to the 'IAM' service.
3. On the dashboard, click on 'Activate MFA on your root account', click on 'Manage MFA' and follow the steps to configure MFA for the root account.

IDENTIFICATION AND AUTHENTICATION / Section Identification and Authentication (organizational Users) | Access to Accounts — Separate Device

0 Resource(s) Failed

Compliance Section: Identification and Authentication (organizational Users) | Access to Accounts — Separate Device

Low

Implement multi-factor authentication for [Selection (one or more): local; network; remote] access to [Selection (one or more): privileged accounts; non-privileged accounts] such that:
(a) One of the factors is provided by a device separate from the system gaining access; and
(b) The device meets [Assignment: organization-defined strength of mechanism requirements].

AWS MFA not enabled for IAM users

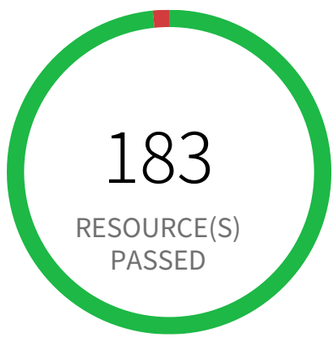
This policy identifies AWS IAM users for whom MFA is not enabled. AWS Multi-Factor Authentication (MFA) is a simple best practice that adds an extra layer of protection on top of your user name and password. Multiple factors provide increased security for your AWS account settings and resources.

First Seen N/A | **Resource Type** IAM Credentials Report

Recommendations

1. Sign in to the AWS and navigate to the 'IAM' service.
2. Navigate to the user that was reported in the alert.
3. Under 'Security Credentials', check "Assigned MFA Device" and follow the instructions to enable MFA for the user.

IDENTIFICATION AND AUTHENTICATION / Section Authenticator Management



3 Resource(s) Failed

demoappdashboard-deployments-mobile-hub-12027657, elad-bucket1, izabellatest1

Compliance Section: Authenticator Management

Low

Manage system authenticators by:
a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;
b. Establishing initial authenticator content for any authenticators issued by the organization;
c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;
e. Changing default authenticators prior to first use;
f. Changing or refreshing authenticators [Assignment: organization-defined time period by authenticator type] or when [Assignment: organization-defined events] occur;
g. Protecting authenticator content from unauthorized disclosure and modification;
h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and
i. Changing authenticators for group or role accounts when membership to those accounts changes.

AWS S3 bucket is not configured with MFA Delete

This policy identifies the S3 buckets which do not have Multi-Factor Authentication(MFA) enabled to delete S3 object version. Enabling MFA Delete on a versioned bucket adds another layer of protection. In order to permanently delete an object version or suspend or reactivate versioning on the bucket valid code from the account's MFA device required.

Note: MFA Delete only works for CLI or API interaction, not in the AWS Management Console. Also, you cannot make version DELETE actions with MFA using IAM user credentials. You must use your root AWS account.

First Seen April 20, 2021 at 6:01:04 PM UTC | **Resource Type** Other

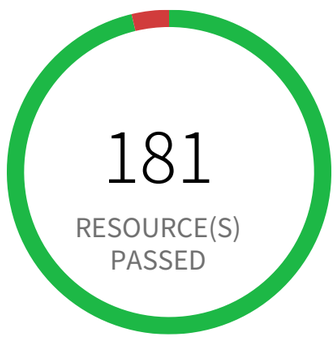
Recommendations

Using console you can enable versioning on the bucket but you cannot enable MFA delete.
You can do it via only with the AWS CLI:
aws s3api put-bucket-versioning --bucket <BUCKET_NAME> --versioning-configuration Status=Enabled,MFADelete=Enabled --mfa "<MFA_SERIAL_NUMBER> <MFA_CODE>"

NOTE: The bucket owner, the AWS account that created the bucket (root account), and all authorized IAM users can enable versioning, but

only the bucket owner (root account) can enable MFA Delete. Successful execution will enable the S3 bucket versioning and MFA delete on the bucket.

IDENTIFICATION AND AUTHENTICATION / Section Authenticator Management



7 Resource(s) Failed

kfirdaus-aws-bucket, demo-bucket-pcds-root, sedemocloudtrail, aws-cloudtrail-logs-240075317252-884b0070, read-events-test-plan-cloudtrail-s3-bucket, read-event-ct, yuricloudtrail.puresec-dev-2.puresec.io

Compliance Section: Authenticator Management

Informational

Manage system authenticators by:
a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;
b. Establishing initial authenticator content for any authenticators issued by the organization;
c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;
e. Changing default authenticators prior to first use;
f. Changing or refreshing authenticators [Assignment: organization-defined time period by authenticator type] or when [Assignment: organization-defined events] occur;
g. Protecting authenticator content from unauthorized disclosure and modification;
h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and
i. Changing authenticators for group or role accounts when membership to those accounts changes.

AWS CloudTrail S3 buckets have not enabled MFA Delete

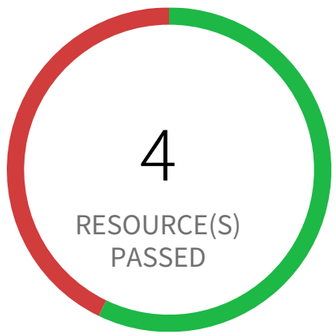
This policy identifies the S3 buckets which do not have Multi-Factor Authentication enabled for CloudTrails. For encryption of log files, CloudTrail defaults to use of S3 server-side encryption (SSE). We recommend adding an additional layer of security by adding MFA Delete to your S3 bucket. This will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

First Seen February 3, 2021 at 7:24:07 PM UTC | **Resource Type** Other

Recommendations

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

IDENTIFICATION AND AUTHENTICATION / Section Authenticator Management | Password-based Authentication



3 Resource(s) Failed

016671749923-iam-password-policy,
197802673547-iam-password-policy,
673174758328-iam-password-policy

Compliance Section: Authenticator Management | Password-based Authentication

Informational

For password-based authentication:
(a) Maintain a list of commonly-used, expected, or compromised passwords and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised directly or indirectly;
(b) Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a);
(c) Transmit passwords only over cryptographically-protected channels;
(d) Store passwords using an approved salted key derivation function, preferably using a keyed hash;
(e) Require immediate selection of a new password upon account recovery;
(f) Allow user selection of long passwords and passphrases, including spaces and all printable characters;
(g) Employ automated tools to assist the user in selecting strong password authenticators; and
(h) Enforce the following composition and complexity rules: [Assignment: organization-defined composition and complexity rules].

AWS IAM password policy does not have a minimum of 14 characters

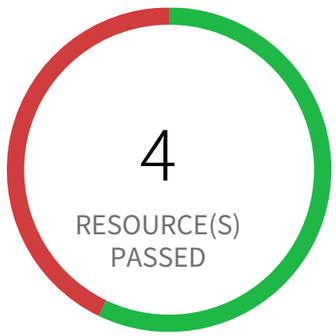
Checks to ensure that IAM password policy requires minimum of 14 characters. AWS IAM (Identity & Access Management) allows customers to secure AWS console access. As a security best practice, customers must have strong password policies in place.

First Seen April 20, 2023 at 11:28:37 PM UTC | **Resource Type** Password Policy

Recommendations

1. Login to the AWS console and navigate to the 'IAM' service.
2. On the left navigation panel, Click on 'Account Settings'
3. In the 'Minimum password length' field, put 14 or more (As per preference).
4. Click on 'Apply password policy'

IDENTIFICATION AND AUTHENTICATION / Section Authenticator Management | Password-based Authentication



3 Resource(s) Failed

016671749923-iam-password-policy,
197802673547-iam-password-policy,
673174758328-iam-password-policy

Compliance Section: Authenticator Management | Password-based Authentication

Informational

For password-based authentication:
(a) Maintain a list of commonly-used, expected, or compromised passwords and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised directly or indirectly;
(b) Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a);
(c) Transmit passwords only over cryptographically-protected channels;
(d) Store passwords using an approved salted key derivation function, preferably using a keyed hash;
(e) Require immediate selection of a new password upon account recovery;
(f) Allow user selection of long passwords and passphrases, including spaces and all printable characters;
(g) Employ automated tools to assist the user in selecting strong password authenticators; and
(h) Enforce the following composition and complexity rules: [Assignment: organization-defined composition and complexity rules].

AWS IAM password policy does not have an uppercase character

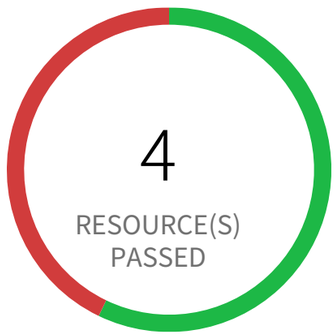
This policy identifies AWS accounts in which IAM password policy does not have an uppercase character. AWS IAM (Identity & Access Management) allows customers to secure AWS console access. As a security best practice, customers must have strong password policies in place.

First Seen April 20, 2023 at 11:28:37 PM UTC | **Resource Type** Password Policy

Recommendations

1. Login to the AWS console and navigate to the 'IAM' service.
2. On the left navigation panel, Click on 'Account Settings'
3. check 'Require at least one uppercase letter'.
4. Click on 'Apply password policy'

IDENTIFICATION AND AUTHENTICATION / Section Authenticator Management | Password-based Authentication



3 Resource(s) Failed

016671749923-iam-password-policy,
197802673547-iam-password-policy,
673174758328-iam-password-policy

Compliance Section: Authenticator Management | Password-based Authentication

Low

For password-based authentication:
(a) Maintain a list of commonly-used, expected, or compromised passwords and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised directly or indirectly;
(b) Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a);
(c) Transmit passwords only over cryptographically-protected channels;
(d) Store passwords using an approved salted key derivation function, preferably using a keyed hash;
(e) Require immediate selection of a new password upon account recovery;
(f) Allow user selection of long passwords and passphrases, including spaces and all printable characters;
(g) Employ automated tools to assist the user in selecting strong password authenticators; and
(h) Enforce the following composition and complexity rules: [Assignment: organization-defined composition and complexity rules].

AWS IAM password policy does not have a number

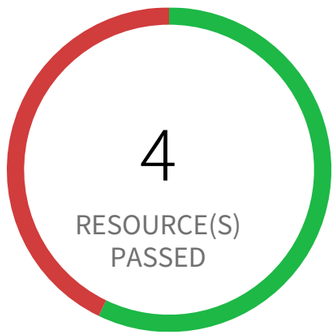
Checks to ensure that IAM password policy requires a number. AWS IAM (Identity & Access Management) allows customers to secure AWS console access. As a security best practice, customers must have strong password policies in place.

First Seen April 20, 2023 at 11:28:37 PM UTC | **Resource Type** Password Policy

Recommendations

1. Login to the AWS console and navigate to the 'IAM' service.
2. On the left navigation panel, Click on 'Account Settings'
3. check 'Require at least one number'.
4. Click on 'Apply password policy'

IDENTIFICATION AND AUTHENTICATION / Section Authenticator Management | Password-based Authentication



3 Resource(s) Failed

016671749923-iam-password-policy,
197802673547-iam-password-policy,
673174758328-iam-password-policy

Compliance Section: Authenticator Management | Password-based Authentication

Informational

For password-based authentication:
(a) Maintain a list of commonly-used, expected, or compromised passwords and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised directly or indirectly;
(b) Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a);
(c) Transmit passwords only over cryptographically-protected channels;
(d) Store passwords using an approved salted key derivation function, preferably using a keyed hash;
(e) Require immediate selection of a new password upon account recovery;
(f) Allow user selection of long passwords and passphrases, including spaces and all printable characters;
(g) Employ automated tools to assist the user in selecting strong password authenticators; and
(h) Enforce the following composition and complexity rules: [Assignment: organization-defined composition and complexity rules].

AWS IAM password policy allows password reuse

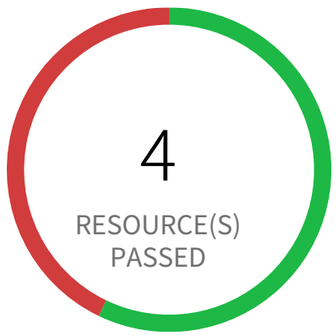
This policy identifies IAM policies which allow password reuse . AWS IAM (Identity & Access Management) allows customers to secure AWS console access. As a security best practice, customers must have strong password policies in place.

First Seen April 20, 2023 at 11:28:37 PM UTC | **Resource Type** Password Policy

Recommendations

1. Sign in to the AWS console and navigate to the 'IAM' service.
2. Click on 'Account Settings', check 'Prevent password reuse'.

IDENTIFICATION AND AUTHENTICATION / Section Authenticator Management | Password-based Authentication



3 Resource(s) Failed

016671749923-iam-password-policy,
197802673547-iam-password-policy,
673174758328-iam-password-policy

Compliance Section: Authenticator Management | Password-based Authentication

Informational

For password-based authentication:
(a) Maintain a list of commonly-used, expected, or compromised passwords and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised directly or indirectly;
(b) Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a);
(c) Transmit passwords only over cryptographically-protected channels;
(d) Store passwords using an approved salted key derivation function, preferably using a keyed hash;
(e) Require immediate selection of a new password upon account recovery;
(f) Allow user selection of long passwords and passphrases, including spaces and all printable characters;
(g) Employ automated tools to assist the user in selecting strong password authenticators; and
(h) Enforce the following composition and complexity rules: [Assignment: organization-defined composition and complexity rules].

AWS IAM password policy does not have password expiration period

Checks to ensure that IAM password policy has an expiration period. AWS IAM (Identity & Access Management) allows customers to secure AWS console access. As a security best practice, customers must have strong password policies in place.

First Seen April 20, 2023 at 11:28:37 PM UTC | **Resource Type** Password Policy

Recommendations

1. Login to the AWS console and navigate to the 'IAM' service.
2. On the left navigation panel, Click on 'Account Settings'
3. check 'Enable password expiration' and enter a password expiration period.
4. Click on 'Apply password policy'

IDENTIFICATION AND AUTHENTICATION / Section Authenticator Management | Password-based Authentication

0 Resource(s) Failed

Compliance Section: Authenticator Management | Password-based Authentication

Low

For password-based authentication:
(a) Maintain a list of commonly-used, expected, or compromised passwords and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised directly or indirectly;
(b) Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a);
(c) Transmit passwords only over cryptographically-protected channels;
(d) Store passwords using an approved salted key derivation function, preferably using a keyed hash;
(e) Require immediate selection of a new password upon account recovery;
(f) Allow user selection of long passwords and passphrases, including spaces and all printable characters;
(g) Employ automated tools to assist the user in selecting strong password authenticators; and
(h) Enforce the following composition and complexity rules: [Assignment: organization-defined composition and complexity rules].

AWS IAM Password policy is unsecure

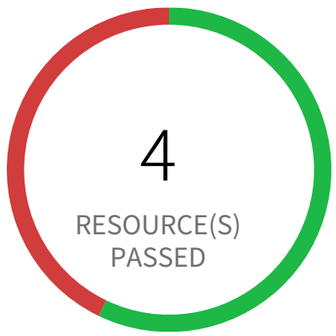
Checks to ensure that IAM password policy is in place for the cloud accounts. As a security best practice, customers must have strong password policies in place. This policy ensures password policies are set with all following options:
- Minimum Password Length
- At least one Uppercase letter
- At least one Lowercase letter
- At least one Number
- At least one Symbol/non-alphanumeric character
- Users have permission to change their own password
- Password expiration period
- Password reuse
- Password expiration requires administrator reset

First Seen N/A | **Resource Type** Other

Recommendations

1. Login to AWS Console and navigate to the 'IAM' Service
2. Click on 'Account Settings'
3. Under 'Password Policy', select and set all the options
4. Click on 'Apply password policy'

IDENTIFICATION AND AUTHENTICATION / Section Authenticator Management | Password-based Authentication



3 Resource(s) Failed

016671749923-iam-password-policy,
197802673547-iam-password-policy,
673174758328-iam-password-policy

Compliance Section: Authenticator Management | Password-based Authentication

Informational

For password-based authentication:
(a) Maintain a list of commonly-used, expected, or compromised passwords and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised directly or indirectly;
(b) Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a);
(c) Transmit passwords only over cryptographically-protected channels;
(d) Store passwords using an approved salted key derivation function, preferably using a keyed hash;
(e) Require immediate selection of a new password upon account recovery;
(f) Allow user selection of long passwords and passphrases, including spaces and all printable characters;
(g) Employ automated tools to assist the user in selecting strong password authenticators; and
(h) Enforce the following composition and complexity rules: [Assignment: organization-defined composition and complexity rules].

AWS IAM password policy does not have a lowercase character

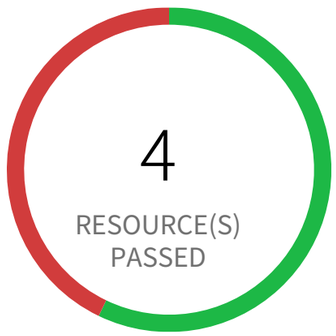
Checks to ensure that IAM password policy requires a lowercase character. AWS IAM (Identity & Access Management) allows customers to secure AWS console access. As a security best practice, customers must have strong password policies in place.

First Seen April 20, 2023 at 11:28:37 PM UTC | **Resource Type** Password Policy

Recommendations

1. Login to the AWS console and navigate to the 'IAM' service.
2. On the left navigation panel, Click on 'Account Settings'
3. check 'Require at least one lowercase letter'.
4. Click on 'Apply password policy'

IDENTIFICATION AND AUTHENTICATION / Section Authenticator Management | Password-based Authentication



3 Resource(s) Failed

016671749923-iam-password-policy,
197802673547-iam-password-policy,
673174758328-iam-password-policy

Compliance Section: Authenticator Management | Password-based Authentication

Informational

For password-based authentication:
(a) Maintain a list of commonly-used, expected, or compromised passwords and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised directly or indirectly;
(b) Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a);
(c) Transmit passwords only over cryptographically-protected channels;
(d) Store passwords using an approved salted key derivation function, preferably using a keyed hash;
(e) Require immediate selection of a new password upon account recovery;
(f) Allow user selection of long passwords and passphrases, including spaces and all printable characters;
(g) Employ automated tools to assist the user in selecting strong password authenticators; and
(h) Enforce the following composition and complexity rules: [Assignment: organization-defined composition and complexity rules].

AWS IAM password policy does not expire in 90 days

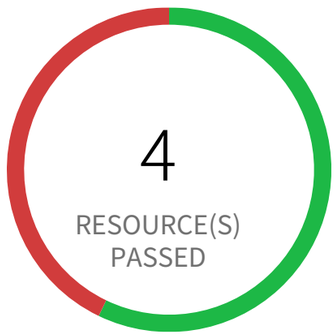
This policy identifies the IAM policies which does not have password expiration set to 90 days. AWS IAM (Identity & Access Management) allows customers to secure AWS console access. As a security best practice, customers must have strong password policies in place.

First Seen April 20, 2023 at 11:28:37 PM UTC | **Resource Type** Password Policy

Recommendations

1. Login to the AWS console and navigate to the 'IAM' service.
2. On the left navigation panel, Click on 'Account Settings'
3. check 'Enable password expiration' and enter a password expiration period.
4. Click on 'Apply password policy'

IDENTIFICATION AND AUTHENTICATION / Section Authenticator Management | Password-based Authentication



3 Resource(s) Failed

016671749923-iam-password-policy,
197802673547-iam-password-policy,
673174758328-iam-password-policy

Compliance Section: Authenticator Management | Password-based Authentication

Informational

For password-based authentication:
(a) Maintain a list of commonly-used, expected, or compromised passwords and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised directly or indirectly;
(b) Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a);
(c) Transmit passwords only over cryptographically-protected channels;
(d) Store passwords using an approved salted key derivation function, preferably using a keyed hash;
(e) Require immediate selection of a new password upon account recovery;
(f) Allow user selection of long passwords and passphrases, including spaces and all printable characters;
(g) Employ automated tools to assist the user in selecting strong password authenticators; and
(h) Enforce the following composition and complexity rules: [Assignment: organization-defined composition and complexity rules].

AWS IAM password policy does not have a symbol

Checks to ensure that IAM password policy requires a symbol. AWS IAM (Identity & Access Management) allows customers to secure AWS console access. As a security best practice, customers must have strong password policies in place.

First Seen April 20, 2023 at 11:28:37 PM UTC | **Resource Type** Password Policy

Recommendations

1. Login to the AWS console and navigate to the 'IAM' service.
2. On the left navigation panel, Click on 'Account Settings'
3. check 'Require at least one non-alphanumeric character'.
4. Click on 'Apply password policy'

IDENTIFICATION AND AUTHENTICATION / Section Authenticator Management | Public Key-based Authentication

0 Resource(s) Failed

Compliance Section: Authenticator Management | Public Key-based Authentication

Informational

(a) For public key-based authentication:
(1) Enforce authorized access to the corresponding private key; and
(2) Map the authenticated identity to the account of the individual or group; and
(b) When public key infrastructure (PKI) is used:
(1) Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and
(2) Implement a local cache of revocation data to support path discovery and validation.

AWS Certificate Manager (ACM) contains certificate pending validation

This policy identifies invalid certificates which are in AWS Certificate Manager. When your Amazon ACM certificates are not validated within 72 hours after the request is made, those certificates become invalid and you will have to request new certificates, which could cause interruption to your applications or services. Though AWS Certificate Manager automatically renews certificates issued by the service that is used with other AWS resources. However, the ACM service does not automatically renew certificates that are not currently in use or not associated anymore with other AWS resources. So the renewal process including validation must be done manually before these certificates become invalid.

First Seen N/A | **Resource Type** Other

Recommendations

To validate Certificates:
1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Go to Certificate Manager(ACM) service
4. Choose the reported certificate
5. Validate your certificate for your domain using either Email or DNS validation, depending upon your certificate validation method.

OR

If the certificate is not required you can delete that certificate. To delete invalid Certificates:

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

Note: This alert will get auto-resolved, as the certificate becomes invalid in 72 hours. It is recommended to either delete or validate the certificate within the timeframe.

IDENTIFICATION AND AUTHENTICATION / Section Authenticator Management | Public Key-based Authentication

0 Resource(s) Failed

Compliance Section: Authenticator Management | Public Key-based Authentication Low

(a) For public key-based authentication:
(1) Enforce authorized access to the corresponding private key; and
(2) Map the authenticated identity to the account of the individual or group; and
(b) When public key infrastructure (PKI) is used:
(1) Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and
(2) Implement a local cache of revocation data to support path discovery and validation.

AWS Certificate Manager (ACM) has invalid or failed certificate

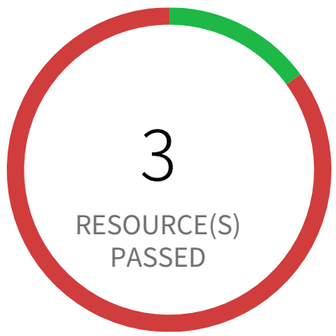
This policy identifies certificates in ACM which are either in Invalid or Failed state. If the ACM certificate is not validated within 72 hours, it becomes Invalid. An ACM certificate fails when,
- the certificate is requested for invalid public domains
- the certificate is requested for domains which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

First Seen N/A | **Resource Type** Other

Recommendations

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

IDENTIFICATION AND AUTHENTICATION / Section Authenticator Management | Public Key-based Authentication



17 Resource(s) Failed

Dev, default, dev, elad, prod, default, prod, dev, dev, prod & 7 more

Compliance Section: Authenticator Management | Public Key-based Authentication Low

(a) For public key-based authentication:
(1) Enforce authorized access to the corresponding private key; and
(2) Map the authenticated identity to the account of the individual or group; and
(b) When public key infrastructure (PKI) is used:
(1) Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and
(2) Implement a local cache of revocation data to support path discovery and validation.

AWS API Gateway endpoints without client certificate authentication

API Gateway can generate an SSL certificate and use its public key in the backend to verify that HTTP requests to your backend system are from API Gateway. This allows your HTTP backend to control and accept only requests originating from Amazon API Gateway, even if the backend is publicly accessible.

Note: Some backend servers may not support SSL client authentication as API Gateway does and could return an SSL certificate error. For a list of incompatible backend servers, see Known Issues. https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-known-issues.html

First Seen April 20, 2021 at 6:01:15 PM UTC | **Resource Type** Other

Recommendations

These instructions assume you already completed Generate a Client Certificate Using the API Gateway Console. If not please generate a client certificate by following below steps and then Configure an API to Use SSL Certificates.
Steps to Generate a Client Certificate Using the API Gateway Console:
1. Login to AWS Console
2. Go to API Gateway console
3. In the main navigation pane (Left Panel), choose Client Certificates.
4. From the Client Certificates pane, choose Generate Client Certificate.
5. Optionally, for Edit, choose to add a descriptive title for the generated certificate and choose Save to save the description. API Gateway generates a new certificate and returns the new certificate GUID, along with the PEM-encoded public key.

Steps to Configure an API to Use SSL Certificates:
1. Login to AWS Console
2. Go to API Gateway console
3. In the API Gateway console, create or open an API for which you want to use the client certificate. Make sure the API has been deployed to a stage (Left Panel).
4. Choose Stages under the selected API and then choose a stage (Left Panel).
5. In the Stage Editor panel, select a certificate under the Client Certificate section.
6. Click Save Changes

IDENTIFICATION AND AUTHENTICATION / Section Authenticator Management | Public Key-based Authentication

0 Resource(s) Failed

Compliance Section: Authenticator Management | Public Key-based Authentication Low

(a) For public key-based authentication:
(1) Enforce authorized access to the corresponding private key; and
(2) Map the authenticated identity to the account of the individual or group; and
(b) When public key infrastructure (PKI) is used:
(1) Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and
(2) Implement a local cache of revocation data to support path discovery and validation.

AWS Certificate Manager (ACM) has expired certificates

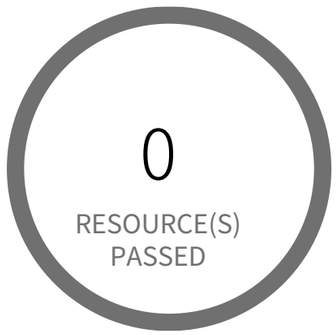
This policy identifies expired certificates which are in AWS Certificate Manager. AWS Certificate Manager (ACM) is the preferred tool to provision, manage, and deploy your server certificates. With ACM you can request a certificate or deploy an existing ACM or external certificate to AWS resources. This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

First Seen N/A | **Resource Type** Other

Recommendations

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

IDENTIFICATION AND AUTHENTICATION / Section Authenticator Management | Expiration of Cached Authenticators



0 Resource(s) Failed

Compliance Section: Authenticator Management | Expiration of Cached Authenticators

Low

Prohibit the use of cached authenticators after [Assignment: organization-defined time period].

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

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

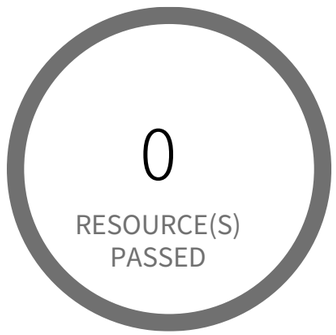
First Seen N/A | **Resource Type** Other

Recommendations

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

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

IDENTIFICATION AND AUTHENTICATION / Section Service Identification and Authentication



0 Resource(s) Failed

Compliance Section: Service Identification and Authentication

Low

Uniquely identify and authenticate [Assignment: organization-defined system services and applications] before establishing communications with devices, users, or other services or applications.

AWS ElastiCache Redis cluster with Redis AUTH feature disabled

This policy identifies ElastiCache Redis clusters which have Redis AUTH feature disabled. Redis AUTH can improve data security by requiring the user to enter a password before they are granted permission to execute Redis commands on a password protected Redis server.

First Seen N/A | **Resource Type** Other

Recommendations

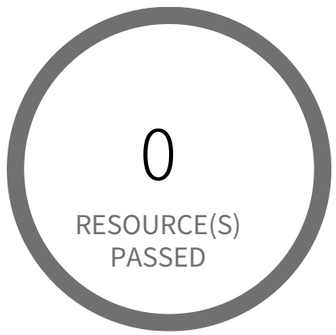
AWS ElastiCache Redis cluster Redis AUTH password can be set, only at the time of creation of the cluster. So to resolve this alert, create a new cluster with Redis AUTH feature enabled, then migrate all required ElastiCache Redis cluster data from the reported ElastiCache Redis cluster to this newly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

To create new ElastiCache Redis cluster with Redis AUTH password set, perform the following:
1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to ElastiCache Dashboard
4. Click on Redis
5. Click on 'Create' button
6. On the 'Create your Amazon ElastiCache cluster' page,
a. Select 'Redis' cache engine type.
b. Enter a name for the new cache cluster
c. Select Redis engine version from 'Engine version compatibility' dropdown list.
Note: As of July 2018, In-transit encryption can be enabled only for AWS ElastiCache clusters with Redis engine version 3.2.6 and 4.0.10.
d. Click on 'Advanced Redis settings' to expand the cluster advanced settings panel
e. Select 'Encryption in-transit' checkbox to enable encryption
Note: Redis AUTH can only be enabled when creating clusters where in-transit encryption is enabled.
f. Select 'Redis AUTH' checkbox to enable to enable AuthToken password
g. Type password you want enforce on 'Redis AUTH Token' textbox.
Choosen password should meet 'Passwords must be at least 16 and a maximum of 128 printable characters. At least 16 characters, and maximum 128 characters, restricted to any printable ASCII character except ' ', '"', '/' and '@' signs' criteria. Set the new Redis cluster other parameters which are same as of reported Redis cluster configuration details.

Note: The password set at cluster creation cannot be changed.
7. Click on 'Create' button to launch your new ElastiCache Redis cluster

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

IDENTIFICATION AND AUTHENTICATION / Section Service Identification and Authentication



0 Resource(s) Failed

Compliance Section: Service Identification and Authentication

Low

Uniquely identify and authenticate [Assignment: organization-defined system services and applications] before establishing communications with devices, users, or other services or applications.

AWS EMR cluster is not configured with Kerberos Authentication

This policy identifies EMR clusters which are not configured with Kerberos Authentication. Kerberos uses secret-key cryptography to provide strong authentication so that passwords or other credentials aren't sent over the network in an unencrypted format.

First Seen N/A | **Resource Type** Other

Recommendations

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

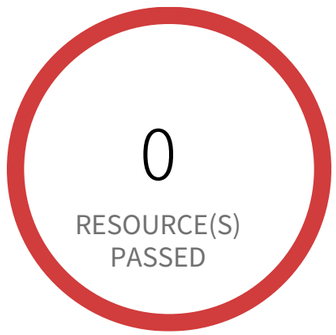
7

PROGRAM MANAGEMENT

PROGRAM MANAGEMENT Overview

Section			Pass Rate	Failed	Passed
Measures of Performance	AWS Elastic Load Balancer (Classic) with cross-zone load balancing…	•••• Low	0%	2	0

PROGRAM MANAGEMENT / Section Measures of Performance



2 Resource(s) Failed

appElb, a90cc32b132be4f9c82eb1a4891319d6

Compliance Section: Measures of Performance

Low

Develop, monitor, and report on the results of information security and privacy measures of performance.

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

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

First Seen June 19, 2019 at 6:42:05 PM UTC | **Resource Type** Other

Recommendations

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

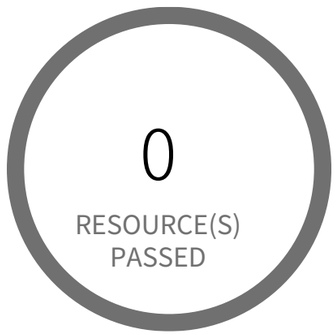
8

PERSONNEL SECURITY

PERSONNEL SECURITY Overview

Section	Pass Rate	Failed	Passed
Personnel Termination | Automated Actions AWS RDS Event subscription··· Informational	100%	0	0

PERSONNEL SECURITY / Section Personnel Termination | Automated Actions



0 Resource(s) Failed

Compliance Section: Personnel Termination | Automated Actions

Informational

Use [Assignment: organization-defined automated mechanisms] to [Selection (one or more): notify [Assignment: organization-defined personnel or roles] of individual termination actions; disable access to system resources].

AWS RDS Event subscription All event categories and All instances disabled for DB instance

This policy identifies AWS RDS event subscriptions for DB instance which has 'All event categories' and 'All instances' is disabled. As a best practice enabling 'All event categories' for 'All instances' helps to get notified when an event occurs for a DB instance.

First Seen N/A | **Resource Type** Other

Recommendations

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

9

RISK ASSESSMENT

RISK ASSESSMENT Overview

Section			Pass Rate	Failed	Passed
Vulnerability Monitoring and Scanning	AWS Config must record all possible re…	Informational	100%	0	7
Vulnerability Monitoring and Scanning	AWS Config Recording is disabled	Informational	15%	163	30
Vulnerability Monitoring and Scanning | Review Historic Audit Logs		Informational	50%	1	1
Vulnerability Monitoring and Scanning | Review Historic Audit Logs		Informational	50%	1	1
Vulnerability Monitoring and Scanning | Review Historic Audit Logs		Informational	58%	5	7
Vulnerability Monitoring and Scanning | Review Historic Audit Logs		Informational	0%	2	0
Vulnerability Monitoring and Scanning | Review Historic Audit Logs		Informational	0%	4	0

RISK ASSESSMENT / Section Vulnerability Monitoring and Scanning

0 Resource(s) Failed

Compliance Section: Vulnerability Monitoring and Scanning

Informational

a. Monitor and scan for vulnerabilities in the system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported;
b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
1. Enumerating platforms, software flaws, and improper configurations;
2. Formatting checklists and test procedures; and
3. Measuring vulnerability impact;
c. Analyze vulnerability scan reports and results from vulnerability monitoring;
d. Remediate legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk;
e. Share information obtained from the vulnerability monitoring process and control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other systems; and
f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.

AWS Config must record all possible resources

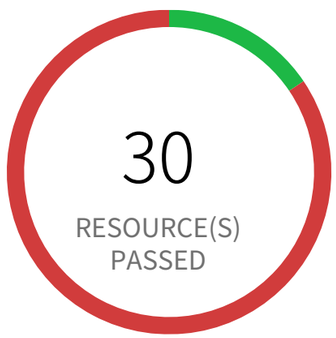
This policy identifies resources for which AWS Config recording is enabled but recording for all possible resources are disabled. AWS Config provides an inventory of your AWS resources and a history of configuration changes to these resources. You can use AWS Config to define rules that evaluate these configurations for compliance. Hence, it is important to enable this feature.

First Seen N/A | **Resource Type** Config Service Recorder

Recommendations

1. Login to the AWS and navigate to the 'Config' service
2. Change to the respective region and in the navigation pane, click on 'Settings'
3. Review the 'All resources' and Check the 2 options (3.a and 3.b)
3.a Record all resources supported in this region
3.b Include global resources (e.g., AWS IAM resources)

RISK ASSESSMENT / Section Vulnerability Monitoring and Scanning



163 Resource(s) Failed

035297560255:AWS Bahrain, 035297560255:AWS Mumbai, 035297560255:AWS Paris, 035297560255:AWS Melbourne, 035297560255:AWS Canada, 035297560255:AWS Milan, 035297560255:AWS Israel, 035297560255:AWS Spain, 035297560255:AWS Jakarta, 035297560255:AWS Zurich & 153 more

Compliance Section: Vulnerability Monitoring and Scanning

Informational

a. Monitor and scan for vulnerabilities in the system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported;
b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
1. Enumerating platforms, software flaws, and improper configurations;
2. Formatting checklists and test procedures; and
3. Measuring vulnerability impact;
c. Analyze vulnerability scan reports and results from vulnerability monitoring;
d. Remediate legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk;
e. Share information obtained from the vulnerability monitoring process and control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other systems; and
f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.

AWS Config Recording is disabled

AWS Config is a web service that performs configuration management of supported AWS resources within your account and delivers log files to you. AWS config uses configuration recorder to detect changes in your resource configurations and capture these changes as configuration items. It continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. This policy generates alerts when AWS Config recorder is not enabled.

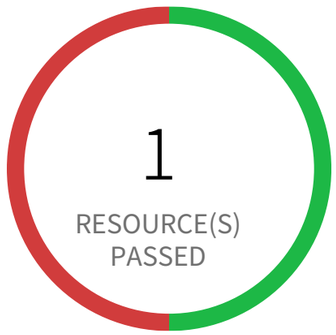
First Seen March 18, 2020 at 6:13:50 AM UTC | **Resource Type** Other

Recommendations

1. Sign in to the AWS Management Console
2. Select the specific region from the top down, for which the alert is generated
3. Navigate to service 'Config' from the 'Services' dropdown.
If AWS Config set up exists,
a. Go to Settings
b. Click on 'Turn On' button under 'Recording is Off' section,

c. provide required information for bucket and role with proper permission
If AWS Config set up doesn't exist
a. Click on 'Get Started'
b. For Step 1, Tick the check box for 'Record all resources supported in this region' under section 'Resource types to record'
c. Under section 'Amazon S3 bucket', select bucket with permission to Config services
d. Under section 'AWS Config role', select a role with permission to Config services
e. Click on 'Next'
f. For Step 2, Select required rule and click on 'Next' otherwise click on 'Skip'
g. For Step 3, Review the created 'Settings' and click on 'Confirm'

RISK ASSESSMENT / Section Vulnerability Monitoring and Scanning | Review Historic Audit Logs



1 Resource(s) Failed

EKS-cluster-1

Compliance Section: Vulnerability Monitoring and Scanning | Review Historic Audit Logs

Informational

Review historic audit logs to determine if a vulnerability identified in a [Assignment: organization-defined system] has been previously exploited within an [Assignment: organization-defined time period].

AWS EKS control plane logging disabled

Amazon EKS control plane logging provides audit and diagnostic logs directly from the Amazon EKS control plane to CloudWatch Logs in your account. These logs make it easy for you to secure and run your clusters. You can select the exact log types you need, and logs are sent as log streams to a group for each Amazon EKS cluster in CloudWatch.

This policy generates an alert if control plane logging is disabled.

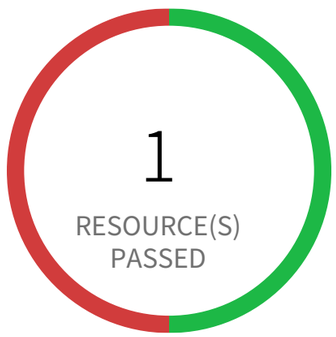
First Seen December 8, 2021 at 12:33:46 AM UTC | **Resource Type** Other

Recommendations

To enable control plane logs:

1. Login to AWS Console
2. Navigate to the Amazon EKS dashboard
3. Choose the name of the cluster to display your cluster information
4. Under Logging, choose 'Manage logging'
5. For each individual log type, choose Enabled
6. Click on 'Save changes'

RISK ASSESSMENT / Section Vulnerability Monitoring and Scanning | Review Historic Audit Logs



1 Resource(s) Failed

d1ove8b1vrwgv4.cloudfront.net

Compliance Section: Vulnerability Monitoring and Scanning | Review Historic Audit Logs

Informational

Review historic audit logs to determine if a vulnerability identified in a [Assignment: organization-defined system] has been previously exploited within an [Assignment: organization-defined time period].

AWS CloudFront distribution with access logging disabled

This policy identifies CloudFront distributions which have access logging disabled. Enabling access log on distributions creates log files that contain detailed information about every user request that CloudFront receives. Access logs are available for web distributions. If you enable logging, you can also specify the Amazon S3 bucket that you want CloudFront to save files in.

First Seen November 3, 2019 at 2:15:19 PM UTC | **Resource Type** Other

Recommendations

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to CloudFront Distributions Dashboard
4. Click on the reported distribution
5. On 'General' tab, Click on 'Edit' button
6. On 'Edit Distribution' page, Set 'Logging' to 'On', choose a 'Bucket for Logs' and 'Log Prefix' as desired
7. Click on 'Yes, Edit'

RISK ASSESSMENT / Section Vulnerability Monitoring and Scanning | Review Historic Audit Logs

5 Resource(s) Failed

demo-pcds-sns, sedemocloudtrail, read-events-trail, yuritrail, read-event-test-cloudtrail

Informational

Compliance Section: Vulnerability Monitoring and Scanning | Review Historic Audit Logs

Review historic audit logs to determine if a vulnerability identified in a [Assignment: organization-defined system] has been previously exploited within an [Assignment: organization-defined time period].

AWS CloudTrail logging is disabled

This policy identifies the CloudTrails in which logging is disabled. AWS CloudTrail is a service that enables governance, compliance, operational & risk auditing of the AWS account. It is a compliance and security best practice to turn on logging for CloudTrail across different regions to get a complete audit trail of activities across various services.

NOTE: This policy will be triggered only when you have CloudTrail configured in your AWS account and logging is disabled.

First Seen August 8, 2021 at 11:18:24 AM UTC | **Resource Type** Other

Recommendations

1. Sign in to AWS Console
2. Navigate to CloudTrail dashboard
3. Click on 'Trails' (Left panel)
4. Click on reported CloudTrail
5. Enable 'Logging' by hovering logging button to 'ON'

OR

If CLoudTrail is not required you can delete by clicking on the delete icon below the logging hover button.

RISK ASSESSMENT / Section Vulnerability Monitoring and Scanning | Review Historic Audit Logs

2 Resource(s) Failed

appElb, a90cc32b132be4f9c82eb1a4891319d6

Compliance Section: Vulnerability Monitoring and Scanning | Review Historic Audit Logs

Informational

Review historic audit logs to determine if a vulnerability identified in a [Assignment: organization-defined system] has been previously exploited within an [Assignment: organization-defined time period].

AWS Elastic Load Balancer (Classic) with access log disabled

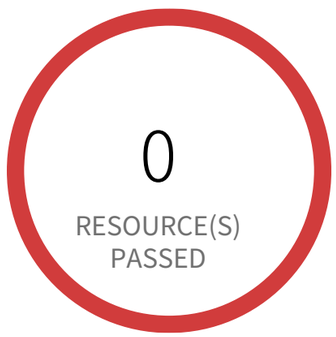
This policy identifies Classic Elastic Load Balancers which have access log disabled. When Access log enabled, Classic load balancer captures detailed information about requests sent to your load balancer. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. You can use these access logs to analyze traffic patterns and to troubleshoot issues.

First Seen June 19, 2019 at 6:42:05 PM UTC | **Resource Type** Other

Recommendations

To enable access logging for Elastic Load Balancer (Classic), follow below mentioned URL:
https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/enable-access-logs.html

RISK ASSESSMENT / Section Vulnerability Monitoring and Scanning | Review Historic Audit Logs



4 Resource(s) Failed

pcsdemo-useast1f-nlb, pscdemo-use-ast1e-nlb, elb-pcsdemo-useast2-dmostardi, awseb-AWSEB-Q2FO6T2FSEDJ

Compliance Section: Vulnerability Monitoring and Scanning | Review Historic Audit Logs

Informational

Review historic audit logs to determine if a vulnerability identified in a [Assignment: organization-defined system] has been previously exploited within an [Assignment: organization-defined time period].

AWS Elastic Load Balancer v2 (ELBv2) with access log disabled

This policy identifies Elastic Load Balancers v2 (ELBv2) which have access log disabled. Access logs capture detailed information about requests sent to your load balancer and each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. You can use these access logs to analyze traffic patterns and troubleshoot issues.

First Seen November 17, 2021 at 1:12:50 PM UTC | **Resource Type** Other

Recommendations

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to EC2 dashboard
4. Click on 'Load Balancers' (Left Panel)
5. Select the reported ELB
6. Click on 'Actions' drop-down
7. Click on 'Edit attributes'
8. In the 'Edit load balancer attributes' popup box, Choose 'Enable' for 'Access logs' and configure S3 location where you want to store ELB logs.
9. Click on 'Save'

10

SYSTEM AND COMMUNICATIONS PROTECTION

SYSTEM AND COMMUNICATIONS PROTECTION Overview

Section			Pass Rate	Failed	Passed
Boundary Protection	AWS RDS database instance is publicly accessible	Medium	60%	2	3
Boundary Protection	AWS CloudFormation template contains globally open resources	Low	97%	6	211
Boundary Protection	AWS Elasticsearch domain publicly accessible	Medium	50%	1	1
Boundary Protection	AWS RDS Snapshot with access for unmonitored cloud accounts	Low	100%	0	26
Boundary Protection	AWS S3 buckets are accessible to public via ACL	Medium	91%	15	171
Boundary Protection	AWS EBS snapshots are accessible to public	Medium	96%	1	29
Boundary Protection	AWS Amazon Machine Image (AMI) is publicly accessible	Low	100%	0	103
Boundary Protection	AWS EBS Snapshot with access for unmonitored cloud accounts	Low	100%	0	30
Boundary Protection	AWS EKS cluster endpoint access publicly enabled	Low	100%	0	2

NIST 800-53 Rev 5 / SYSTEM AND COMMUNICATIONS PROTECTION

Section			Pass Rate	Failed	Passed
Boundary Protection	AWS Private ECR repository policy is overly permissive	Medium	80%	1	4
Boundary Protection	AWS CloudFront web distribution with AWS Web Application Firewall…	Informational	50%	1	1
Boundary Protection	AWS RDS snapshots are accessible to public	Medium	100%	0	26
Boundary Protection	AWS CloudFront web distribution with geo restriction disabled	Low	50%	1	1
Boundary Protection	AWS CloudTrail bucket is publicly accessible	Low	100%	0	188
Boundary Protection	AWS S3 buckets are accessible to any authenticated user	Medium	99%	1	185
Boundary Protection	AWS S3 bucket accessible to unmonitored cloud accounts	Low	99%	1	185
Boundary Protection | External Telecommunications Services	Al	Informational	30%	90	40
Boundary Protection | External Telecommunications Services	AWS…	Low	83%	1	5
Boundary Protection | Deny by Default — Allow by Exception	AWS EKS…	Low	99%	1	369
Boundary Protection | Deny by Default — Allow by Exception	AWS route…	Low	100%	0	211

NIST 800-53 Rev 5 / SYSTEM AND COMMUNICATIONS PROTECTION

Section	Pass Rate	Failed	Passed
Boundary Protection | Deny by Default — Allow by Exception AWS Informational	100%	0	68
Boundary Protection | Restrict Incoming Communications Traffic AWS Low	99%	1	369
Boundary Protection | Restrict Incoming Communications Traffic AWS Low	100%	0	211
Boundary Protection | Restrict Incoming Communications Traffic Informational	100%	0	68
Boundary Protection | Block Communication from Non-organizationally Configured Hosts High	70%	100	239
Boundary Protection | Block Communication from Non-organizationally Configured Hosts Low	99%	1	369
Boundary Protection | Block Communication from Non-organizationally Configured Hosts High	81%	63	276
Boundary Protection | Block Communication from Non-organizationally Configured Hosts Low	100%	0	211
Boundary Protection | Block Communication from Non-organizationally Configured Hosts High	92%	25	314

NIST 800-53 Rev 5 / SYSTEM AND COMMUNICATIONS PROTECTION

Section	Pass Rate	Failed	Passed
Boundary Protection | Block Communication from Non-organizationally Configured Hosts — Informational	100%	0	677
Boundary Protection | Block Communication from Non-organizationally Configured Hosts — Informational	100%	0	68
Boundary Protection | Separate Subnets for Connecting to Different Security Domains — Low	40%	264	177
Boundary Protection | Separate Subnets for Connecting to Different Security Domains — Low	100%	0	37
Boundary Protection | Connections to Public Networks — AWS VPC subnets… — Low	40%	264	177
Boundary Protection | Connections to Public Networks — AWS VPC… — Informational	100%	0	37
Boundary Protection | Connections to Public Networks — AWS EKS… — Informational	95%	1	23
Boundary Protection | Connections to Public Networks — AWS Amazon Ma… — Low	100%	0	103
Boundary Protection | Connections to Public Networks — AWS Cloudfront Dis… — Low	50%	1	1

NIST 800-53 Rev 5 / SYSTEM AND COMMUNICATIONS PROTECTION

Section	Pass Rate	Failed	Passed
Boundary Protection | Connections to Public Networks AWS Elasti··· Informational	100%	0	0
Transmission Confidentiality and Integrity | Cryptographic Protection Low	100%	0	2
Transmission Confidentiality and Integrity | Cryptographic Protection Medium	100%	0	2
Transmission Confidentiality and Integrity | Cryptographic Protection Medium	100%	0	2
Transmission Confidentiality and Integrity | Cryptographic Protection Low	100%	0	0
Transmission Confidentiality and Integrity | Cryptographic Protection Low	50%	1	1
Transmission Confidentiality and Integrity | Cryptographic Protection Informational	98%	1	82
Transmission Confidentiality and Integrity | Cryptographic Protection Informational	100%	0	1
Transmission Confidentiality and Integrity | Cryptographic Protection Low	100%	0	0
Transmission Confidentiality and Integrity | Cryptographic Protection Medium	91%	15	171
Transmission Confidentiality and Integrity | Cryptographic Protection Medium	50%	2	2

NIST 800-53 Rev 5 / SYSTEM AND COMMUNICATIONS PROTECTION

Section		Pass Rate	Failed	Passed
Transmission Confidentiality and Integrity | Cryptographic Protection	Low	0%	2	0
Transmission Confidentiality and Integrity | Cryptographic Protection	Low	100%	0	2
Transmission Confidentiality and Integrity | Cryptographic Protection	Informational	100%	0	6
Transmission Confidentiality and Integrity | Cryptographic Protection	Informational	100%	0	0
Transmission Confidentiality and Integrity | Cryptographic Protection	Medium	100%	0	2
Transmission Confidentiality and Integrity | Cryptographic Protection	Informational	100%	0	1
Transmission Confidentiality and Integrity | Cryptographic Protection	Low	0%	4	0
Transmission Confidentiality and Integrity | Cryptographic Protection	Informational	20%	4	1
Transmission Confidentiality and Integrity | Cryptographic Protection	Informational	50%	1	1
Transmission Confidentiality and Integrity | Cryptographic Protection	Low	100%	0	2
Cryptographic Key Establishment and Management	AWS KMS cus… Informational	100%	0	100

NIST 800-53 Rev 5 / SYSTEM AND COMMUNICATIONS PROTECTION

Section			Pass Rate	Failed	Passed
Cryptographic Key Establishment and Management	BPI AWS access keys are…	High	57%	8	11
Cryptographic Key Establishment and Management	AWS Elastic Load…	Informational	100%	0	2
Cryptographic Key Establishment and Management	AWS Certificate Manager…	Low	100%	0	4
Cryptographic Key Establishment and Management	AWS EMR cluster is not en…	Low	100%	0	0
Cryptographic Key Establishment and Management	AWS SQS queue…	Informational	98%	1	82
Cryptographic Key Establishment and Management	AWS KMS Key…	Informational	100%	0	100
Cryptographic Key Establishment and Management	AWS Customer…	Informational	99%	1	99
Cryptographic Key Establishment and Management	AWS IAM has expired…	Low	100%	0	0
Cryptographic Key Establishment and Management	AWS Kinesis…	Informational	100%	0	1
Cryptographic Key Establishment and Management	AWS RDS DB clus…	Informational	100%	0	1
Cryptographic Key Establishment and Management	AWS access keys are not…	Low	57%	8	11

NIST 800-53 Rev 5 / SYSTEM AND COMMUNICATIONS PROTECTION

Section			Pass Rate	Failed	Passed
Cryptographic Key Establishment and Management	AWS access keys···	Informational	73%	5	14
Cryptographic Key Establishment and Management	AWS RDS data···	Informational	100%	0	6
Cryptographic Key Establishment and Management	AWS EMR cluster···	Informational	100%	0	0
Cryptographic Key Establishment and Management	AWS Redshift···	Informational	100%	0	1
Cryptographic Key Establishment and Management	AWS DynamoDB···	Informational	20%	4	1
Cryptographic Key Establishment and Management	AWS Elastic Load··	Informational	100%	0	2
Cryptographic Key Establishment and Management	AWS IAM user has··	Informational	73%	5	14
Cryptographic Key Establishment and Management	AWS Elastic File···	Informational	50%	1	1
Cryptographic Protection	AWS Redshift instances are not encrypted	Low	100%	0	0
Cryptographic Protection	AWS RDS instance is not encrypted	Low	0%	5	0
Cryptographic Protection	AWS EBS volume region with encryption is disabled	Low	14%	104	17

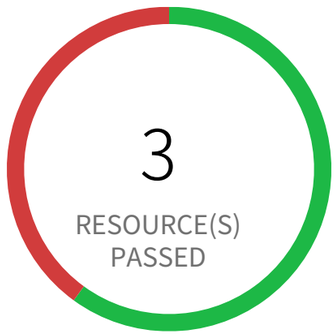
NIST 800-53 Rev 5 / SYSTEM AND COMMUNICATIONS PROTECTION

Section			Pass Rate	Failed	Passed
Public Key Infrastructure Certificates	AWS Elastic Load Balancer (ELB) with IAM···	Informational	100%	0	2
Public Key Infrastructure Certificates	AWS Certificate Manager (ACM) has certificates ex···	Low	100%	0	4
Public Key Infrastructure Certificates	AWS IAM has expired SSL/TLS certificates	Low	100%	0	0
Public Key Infrastructure Certificates	AWS Elastic Load Balancer (ELB) with ACM···	Informational	100%	0	2
Protection of Information at Rest	AWS Elasticsearch domain Encryption for data at rest is···	Low	50%	1	1
Protection of Information at Rest	AWS EMR cluster is not enabled with data encryption at···	Low	100%	0	0
Protection of Information at Rest	AWS EMR cluster is not configured with SSE KMS for data···	Low	100%	0	0
Protection of Information at Rest	AWS ElastiCache Redis cluster with encryption for data at···	Low	100%	0	0
Protection of Information at Rest	AWS Elastic File System (EFS) with encryption for data at···	Low	100%	0	1
Protection of Information at Rest | Cryptographic Protection	AWS EMR···	Low	100%	0	0
Protection of Information at Rest | Cryptographic Protection	AWS EMR···	Low	100%	0	0

NIST 800-53 Rev 5 / SYSTEM AND COMMUNICATIONS PROTECTION

Section			Pass Rate	Failed	Passed
Protection of Information at Rest | Cryptographic Protection	AWS RDS DB·	Low	65%	22	42
Protection of Information at Rest | Cryptographic Protection	AWS SSM···	Low	100%	0	21
Protection of Information at Rest | Cryptographic Protection	AWS RDS DB·	Low	0%	1	0
Protection of Information at Rest | Cryptographic Protection	AWS···	Low	100%	0	0

SYSTEM AND COMMUNICATIONS PROTEC-TION / Section Boundary Protection



2 Resource(s) Failed

myinstance, paasdb

Compliance Section: Boundary Protection

Medium

a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system;
b. Implement subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and
c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.

AWS RDS database instance is publicly accessible

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

First Seen October 16, 2018 at 8:02:27 PM UTC | **Resource Type** Other

Recommendations

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

SYSTEM AND COMMUNICATIONS PROTECTION / Section Boundary Protection

6 Resource(s) Failed

StackSet-AWSControlTowerBP-VPC-AC-COUNT-FACTO-RY-V1-f9505867-d833-4761-9182-f9c18184c064,
StackSet-AWSControlTowerBP-VPC-AC-COUNT-FACTO-RY-V1-59a176eb-2348-472b-8c1b-33a7cb87a46f,
StackSet-AWSControlTowerBP-VPC-AC-COUNT-FACTO-RY-V1-fe0caf67-ed22-4f2b-86ba-08652ceedcc7,
StackSet-AWSControlTowerBP-VPC-AC-COUNT-FACTO-RY-V1-aff1c2b5-ec40-4caf-93eb-5344cf504b63,
StackSet-AWSControlTowerBP-VPC-AC-COUNT-FACTO-RY-V1-0abca017-ea58-4c7e-94ec-5a318d13842c,·

Compliance Section: Boundary Protection

Low

a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system;
b. Implement subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and
c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.

AWS CloudFormation template contains globally open resources

This alert triggers if a CloudFormation template that when launched will result in resources allowing global network access. Below are three common causes:

- Security Group with a {0.0.0.0/0, ::/0} rule
- Network Access Control List with a {0.0.0.0/0, ::/0} rule
- Network Access Control List with -1 IpProtocol

First Seen November 17, 2021 at 1:07:27 PM UTC | **Resource Type** Other

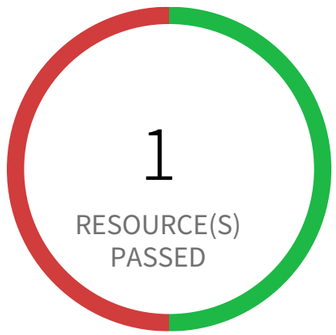
Recommendations

Prisma Cloud encourages you to review the template and ensure this is the intended behavior.

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

14. Configure stack options, then click on Next.
15. Review, then select Update stack near the bottom of the page.

SYSTEM AND COMMUNICATIONS PROTEC-TION / Section Boundary Protection



1 Resource(s) Failed

eladingestsearch

Compliance Section: Boundary Protection

Medium

a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system;
b. Implement subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and
c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.

AWS Elasticsearch domain publicly accessible

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

First Seen August 13, 2022 at 9:01:40 AM UTC | **Resource Type** Other

Recommendations

VPC for AWS Elasticsearch domain can be set only at the time of the creation of domain. So to resolve this alert, create a new domain with VPC, then migrate all required Elasticsearch domain data from the reported Elasticsearch domain to this newly created domain and delete reported Elasticsearch domain.

To set up the new ES domain with VPC, refer the following URL:
https://docs.aws.amazon.com/elasticsearch-service/latest/developerguide/es-createupdatedomains.html
To create Elasticsearch domain within VPC, In Network configuration choose VPC access instead of Public access.

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

SYSTEM AND COMMUNICATIONS PROTEC-TION / Section Boundary Protection

0 Resource(s) Failed

Compliance Section: Boundary Protection

Low

a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system;
b. Implement subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and
c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.

AWS RDS Snapshot with access for unmonitored cloud accounts

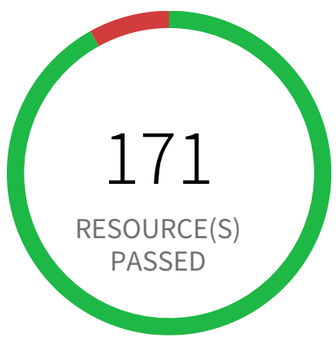
This policy identifies RDS snapshots with access for unmonitored cloud accounts. The RDS Snapshot which have either the read / write permission opened up for Cloud Accounts which are NOT part of Cloud Accounts monitored by Prisma Cloud. These accounts with read / write privileges should be reviewed and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

First Seen N/A | **Resource Type** Other

Recommendations

1. Sign into the AWS console.
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to the RDS service.
4. Select the identified 'RDS Snapshot' under the 'Snapshots' in the left hand menu.
5. Under the tab 'Snapshot Actions', selection the option 'Share Snapshot'.
6. Review and delete the AWS Accounts which should not have read access.

SYSTEM AND COMMUNICATIONS PROTECTION / Section Boundary Protection



15 Resource(s) Failed

totalmess-s3-q4ns, corporatecontracts, corporatemarketingcontent, demo-bucket-publicly-exposed, human-resources-archive, foundry-vtt-ron-s3, productmarketingcontent, redlockpocprepdocs, confidentialinformation, orc-public-bucket & 5 more

Compliance Section: Boundary Protection

Medium

a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system;
b. Implement subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and
c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.

AWS S3 buckets are accessible to public via ACL

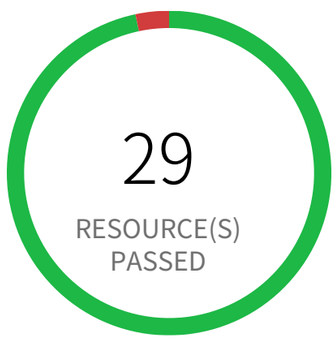
This policy identifies S3 buckets which are publicly accessible via ACL. Amazon S3 often used to store highly sensitive enterprise data and allowing public access to such S3 bucket through ACL would result in sensitive data being compromised. It is highly recommended to disable ACL configuration for all S3 buckets and use resource based policies to allow access to S3 buckets.

First Seen December 5, 2018 at 2:04:56 AM UTC | **Resource Type** Other

Recommendations

1. Login to the AWS Console
2. Navigate to the 'S3' service
3. Click on the 'S3' resource reported in the alert
4. Click on the 'Permissions'
5. If Access Control List' is set to 'Public' follow below steps
a. Under 'Access Control List', Click on 'Everyone' and uncheck all items
b. Click on Save

SYSTEM AND COMMUNICATIONS PROTEC-TION / Section Boundary Protection



1 Resource(s) Failed

snap-0c77fc00f314d9a13

Compliance Section: Boundary Protection

Medium

a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system;
b. Implement subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and
c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.

AWS EBS snapshots are accessible to public

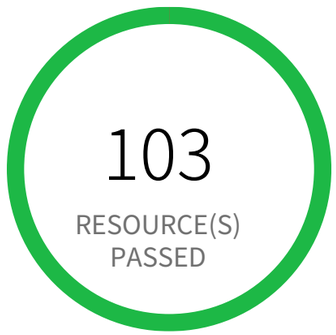
This policy identifies EC2 EBS snapshots which are accessible to public. Amazon Elastic Block Store (Amazon EBS) provides persistent block storage volumes for use with Amazon EC2 instances in the AWS Cloud. If EBS snapshots are inadvertently shared to public, any unauthorized user with AWS console access can gain access to the snapshots and gain access to sensitive data.

First Seen November 28, 2019 at 6:43:42 PM UTC | **Resource Type** Snapshot Settings

Recommendations

1. Log in to the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to 'EC2' service.
4. Under the 'Elastic Block Storage', click on the 'Snapshots'.
5. For the specific Snapshots, change the value of field 'Property' to 'Private'.
6. Under the section 'Encryption Details', set the value of 'Encryption Enabled' to 'Yes'.

SYSTEM AND COMMUNICATIONS PROTEC-TION / Section Boundary Protection



0 Resource(s) Failed

Compliance Section: Boundary Protection

Low

a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system;
b. Implement subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and
c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.

AWS Amazon Machine Image (AMI) is publicly accessible

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

First Seen N/A | **Resource Type** VM Image

Recommendations

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

SYSTEM AND COMMUNICATIONS PROTEC-TION / Section Boundary Protection

30
RESOURCE(S) PASSED

0 Resource(s) Failed

Compliance Section: Boundary Protection

Low

a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system;
b. Implement subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and
c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.

AWS EBS Snapshot with access for unmonitored cloud accounts

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

First Seen N/A | **Resource Type** Other

Recommendations

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

SYSTEM AND COMMUNICATIONS PROTEC-TION / Section Boundary Protection

0 Resource(s) Failed

Compliance Section: Boundary Protection

Low

a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system;
b. Implement subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and
c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.

AWS EKS cluster endpoint access publicly enabled

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

This policy checks your Kubernetes cluster endpoint access and triggers an alert if publicly enabled.

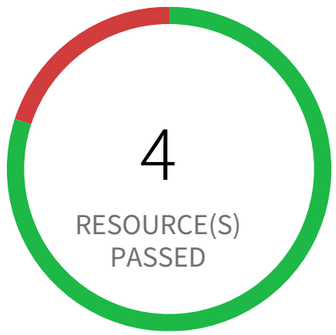
First Seen N/A | **Resource Type** Other

Recommendations

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

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

SYSTEM AND COMMUNICATIONS PROTEC-TION / Section Boundary Protection



1 Resource(s) Failed

test

Compliance Section: Boundary Protection

Medium

a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system;
b. Implement subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and
c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.

AWS Private ECR repository policy is overly permissive

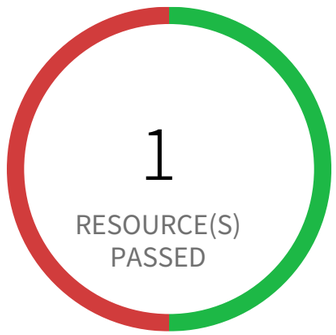
This policy identifies AWS Private ECR repositories that have overly permissive registry policies. An ECR(Elastic Container Registry) repository is a collection of Docker images available on the AWS cloud. These images might contain sensitive information which should be restricted to unauthorized users.

First Seen June 29, 2021 at 2:58:38 PM UTC | **Resource Type** Other

Recommendations

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

SYSTEM AND COMMUNICATIONS PROTEC-TION / Section Boundary Protection



1 Resource(s) Failed

d1ove8b1vrwgv4.cloudfront.net

Compliance Section: Boundary Protection

Informational

a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system;
b. Implement subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and
c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.

AWS CloudFront web distribution with AWS Web Application Firewall (AWS WAF) service disabled

This policy identifies Amazon CloudFront web distributions which have the AWS Web Application Firewall (AWS WAF) service disabled. As a best practice, enable the AWS WAF service on CloudFront web distributions to protect against application layer attacks. To block malicious requests to your Cloudfront Content Delivery Network, define the block criteria in the WAF web access control list (web ACL).

First Seen November 3, 2019 at 2:15:19 PM UTC | **Resource Type** Other

Recommendations

1. Sign in to the AWS console
2. Go to the CloudFront Distributions Dashboard
3. Click on the reported web distribution
4. On 'General' tab, Click on 'Edit' button
5. On 'Edit Distribution' page, Choose a 'AWS WAF Web ACL' from dropdown.
6. Click on 'Yes, Edit'

SYSTEM AND COMMUNICATIONS PROTEC-TION / Section Boundary Protection

0 Resource(s) Failed

Compliance Section: Boundary Protection

Medium

a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system;
b. Implement subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and
c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.

AWS RDS snapshots are accessible to public

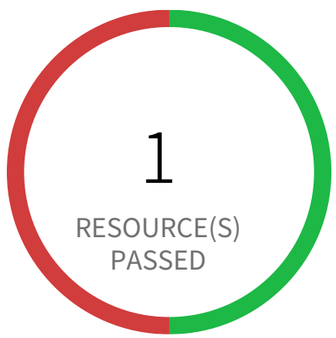
This policy identifies AWS RDS snapshots which are accessible to public. Amazon Relational Database Service (Amazon RDS) is a web service that makes it easier to setup and manage databases. If RDS snapshots are inadvertently shared to public, any unauthorized user with AWS console access can gain access to the snapshots and gain access to sensitive data.

First Seen N/A | **Resource Type** Managed Database Snapshot

Recommendations

1. Sign in to the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to the 'RDS' service.
4. For the RDS instance reported in the alert, change 'Publicly Accessible' setting to 'No'.

SYSTEM AND COMMUNICATIONS PROTEC-TION / Section Boundary Protection



1 Resource(s) Failed

d1ove8b1vrwgv4.cloudfront.net

Compliance Section: Boundary Protection

Low

a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system;
b. Implement subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and
c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.

AWS CloudFront web distribution with geo restriction disabled

This policy identifies CloudFront web distributions which have geo restriction feature disabled. Geo Restriction has the ability to block IP addresses based on Geo IP by allowlist or denylist a country in order to allow or restrict users in specific locations from accessing web application content.

First Seen November 3, 2019 at 2:15:19 PM UTC | **Resource Type** Other

Recommendations

1. Sign in to the AWS console
2. Select the region, from the region drop-down, in which the alert is generated
3. Navigate to CloudFront Distributions Dashboard
4. Click on the reported distribution
5. On 'Restrictions' tab, Click on the 'Edit' button
6. On 'Edit Geo-Restrictions' page, Set 'Enable Geo-Restriction' to 'Yes' and allowlist/denylist countries as per your requirement.
7. Click on 'Yes, Edit'

SYSTEM AND COMMUNICATIONS PROTEC-TION / Section Boundary Protection

188
RESOURCE(S) PASSED

0 Resource(s) Failed

Compliance Section: Boundary Protection

Low

a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system;
b. Implement subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and
c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.

AWS CloudTrail bucket is publicly accessible

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

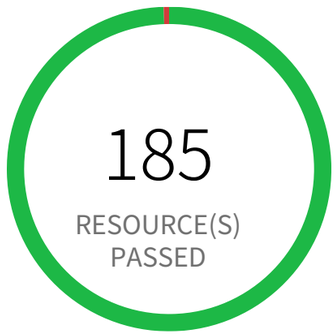
First Seen N/A | **Resource Type** Other

Recommendations

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

Note: Make sure updating 'Access Control List' or 'Bucket Policy' does not affect S3 bucket data access.

SYSTEM AND COMMUNICATIONS PROTEC-TION / Section Boundary Protection



1 Resource(s) Failed

demo-bucket-publicly-exposed

Compliance Section: Boundary Protection

Medium

a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system;
b. Implement subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and
c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.

AWS S3 buckets are accessible to any authenticated user

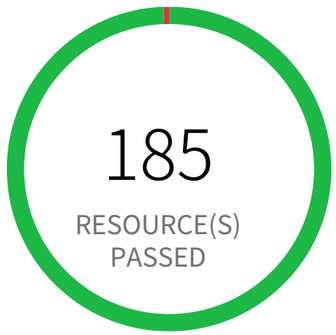
This policy identifies S3 buckets accessible to any authenticated AWS users. Amazon S3 allows customer to store and retrieve any type of content from anywhere in the web. Often, customers have legitimate reasons to expose the S3 bucket to public, for example to host website content. However, these buckets often contain highly sensitive enterprise data which if left accessible to anyone with valid AWS credentials, may result in sensitive data leaks.

First Seen November 28, 2021 at 10:35:20 PM UTC | **Resource Type** Other

Recommendations

1. Login to the AWS Console
2. Navigate to the 'S3' service
3. Click on the 'S3' resource reported in the alert
4. Click on the 'Permissions'
5. Under 'Public access', Click on 'Any AWS user' and uncheck all items
6. Click on Save

SYSTEM AND COMMUNICATIONS PROTEC-TION / Section Boundary Protection



1 Resource(s) Failed

yuri-pipeline-test

Compliance Section: Boundary Protection

Low

a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system;
b. Implement subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and
c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.

AWS S3 bucket accessible to unmonitored cloud accounts

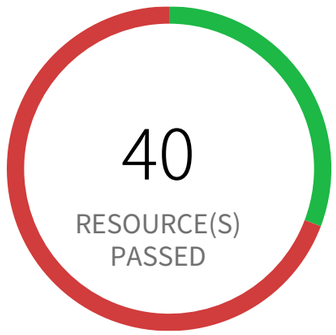
This policy identifies those S3 buckets which have either the read/write permission opened up for Cloud Accounts which are NOT part of Cloud Accounts monitored by Prisma Cloud. These accounts with read/write privileges should be reviewed and confirmed that these are valid accounts of your organization (or authorised by your organization) and are not active under Prisma Cloud monitoring.

First Seen August 2, 2023 at 9:12:30 PM UTC | **Resource Type** Other

Recommendations

1. Log in to the AWS Console
2. Navigate to the 'S3' service
3. Click on the reported S3 bucket
4. Click on the 'Permissions' tab
5. Navigate to the 'Access control list (ACL)' section and Click on the 'Edit'
6. Under 'Access for other AWS accounts', Add the Cloud Accounts that are monitored by Prisma Cloud
7. Click on 'Save changes'

SYSTEM AND COMMUNICATIONS PROTECTION / Section Boundary Protection | External Telecommunications Services



90 Resource(s) Failed

vpc-0471b3e2bb096facc,
vpc-011dc3f3696071f32,
vpc-094d28157f02ee78b,
vpc-0b6f0b71a665b77af,
vpc-05fa2ee4a0f24b7c6,
prismacloud-scan-1695743053643244271,
vpc-0cebecdf463401439,
vpc-0c9d3f27eb3596295, totalmess-vpc-q4ns,
vpc-0acb09cee29e45ce0 & 80 more

Compliance Section: Boundary Protection | External Telecommunications Services

Informational

(a) Implement a managed interface for each external telecommunication service;
(b) Establish a traffic flow policy for each managed interface;
(c) Protect the confidentiality and integrity of the information being transmitted across each interface;
(d) Document each exception to the traffic flow policy with a supporting mission or business need and duration of that need;
(e) Review exceptions to the traffic flow policy [Assignment: organization-defined frequency] and remove exceptions that are no longer supported by an explicit mission or business need;
(f) Prevent unauthorized exchange of control plane traffic with external networks;
(g) Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks; and
(h) Filter unauthorized control plane traffic from external networks.

AWS VPC Flow Logs not enabled

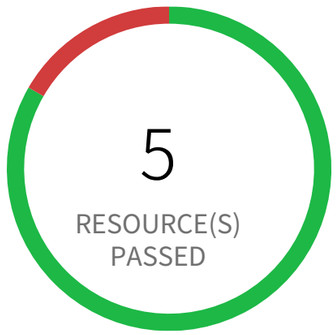
This policy identifies VPCs which have flow logs disabled. VPC Flow logs capture information about IP traffic going to and from network interfaces in your VPC. Flow logs are used as a security tool to monitor the traffic that is reaching your instances. Without the flow logs turned on, it is not possible to get any visibility into network traffic.

First Seen February 8, 2019 at 10:19:01 PM UTC | **Resource Type** Other

Recommendations

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to VPC Dashboard
4. Click on 'Your VPCs' and Choose the reported VPC
5. Click on the 'Flow logs' tab and follow the instructions as in link below to enable Flow Logs for the VPC:
https://aws.amazon.com/blogs/aws/vpc-flow-logs-log-and-view-network-traffic-flows/

SYSTEM AND COMMUNICATIONS PROTEC-TION / Section Boundary Protection | External Telecommunications Services



1 Resource(s) Failed

paloaltocloud.io.

Compliance Section: Boundary Protection | External Telecommunications Services Low

(a) Implement a managed interface for each external telecommunication service;
(b) Establish a traffic flow policy for each managed interface;
(c) Protect the confidentiality and integrity of the information being transmitted across each interface;
(d) Document each exception to the traffic flow policy with a supporting mission or business need and duration of that need;
(e) Review exceptions to the traffic flow policy [Assignment: organization-defined frequency] and remove exceptions that are no longer supported by an explicit mission or business need;
(f) Prevent unauthorized exchange of control plane traffic with external networks;
(g) Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks; and
(h) Filter unauthorized control plane traffic from external networks.

AWS Route53 Public Zone with Private Records

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

First Seen April 20, 2021 at 6:01:15 PM UTC | **Resource Type** Other

Recommendations

You can not convert a public hosted zone into a private hosted zone. So, it is recommended to create and configure a Private Hosted Zone to manage private IPs within your Virtual Private Cloud (VPC) as Amazon Route 53 service will only return your private DNS records when queried from within the associated VPC, and delete the associated public hosted zone once the Private hosted zone is configured with all the records.
To create a private hosted zone using the Route 53 console:

1.For each VPC that you want to associate with the Route 53 hosted zone, change the following VPC settings to true:
'enableDnsHostnames'
'enableDnsSupport'
For more information, see Updating DNS Support (http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-dns.html#vpc-dns-updating) for Your VPC in the Amazon VPC User Guide.
2. Sign in to the AWS console
3. Go to Route 53 console
4. If you are new to Route 53, choose Get Started Now under DNS Management. If you are already using Route 53, choose Hosted Zones in the navigation pane.
5. Choose 'Create Hosted Zone'
6. In the Create Private Hosted Zone pane, enter a domain name and, optionally, a comment.
For information about how to specify characters other than a-z, 0-9, and - (hyphen) and how to specify internationalized domain names, see DNS Domain Name Format (https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/DomainNameFormat.html).
7. In the Type list, choose Private Hosted Zone for Amazon VPC
8. In the VPC ID list, choose the VPC that you want to associate with the hosted zone. If you want to associate more than one VPC with the hosted zone, you can add VPCs after you create the hosted zone.
Note: If the console displays the following message, you are trying to associate a VPC with this hosted zone that has already been associated with another hosted zone that has an overlapping namespace, such as example.com and retail.example.com:
'A conflicting domain is already associated with the given VPC or Delegation Set.'
9. Choose Create
10. To associate more VPCs with the new hosted zone, perform the following steps:
a. Choose Back to Hosted Zones.
b. Choose the radio button for the hosted zone.
c. In the right pane, in VPC ID, choose another VPC that you want to associate with the hosted zone.
d. Choose Associate New VPC.
e. Repeat steps c and d until you have associated all of the VPCs that you want to with the hosted zone.
For More Information : https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/hosted-zone-private-creating.html

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

SYSTEM AND COMMUNICATIONS PROTECTION / Section Boundary Protection | Deny by Default — Allow by Exception

1 Resource(s) Failed

Allow All

Compliance Section: Boundary Protection | Deny by Default — Allow by Exception

Low

**Deny network communications traffic by default and allow network communications traffic by exception [Selection (one or more): at managed interfaces; for [Assignment: organization-defined systems]
].**

AWS EKS cluster security group overly permissive to all traffic

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

First Seen June 13, 2023 at 8:48:36 PM UTC | **Resource Type** Other

Recommendations

Before making any changes, please check the impact on your applications/services. If the Security Group reported indeed need to restrict all traffic, follow the instructions below:
1. Log in to the AWS console
2. Navigate to the 'VPC' service
3. Select the 'Security Group' reported in the alert
4. Click on 'Inbound Rules'
5. Remove the rule which has the 'Source' value as 0.0.0.0/0 or ::/0

SYSTEM AND COMMUNICATIONS PROTECTION / Section Boundary Protection | Deny by Default — Allow by Exception

0 Resource(s) Failed

Compliance Section: Boundary Protection | Deny by Default — Allow by Exception

Low

**Deny network communications traffic by default and allow network communications traffic by exception [Selection (one or more): at managed interfaces; for [Assignment: organization-defined systems]
].**

AWS route table with VPC peering overly permissive to all traffic

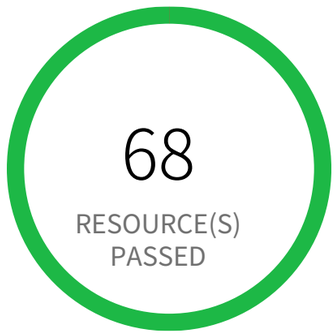
This policy identifies VPC route tables with VPC peering connection which are overly permissive to all traffic. Being highly selective in peering routing tables is a very effective way of minimizing the impact of breach as resources outside of these routes are inaccessible to the peered VPC.

First Seen N/A | **Resource Type** Other

Recommendations

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

SYSTEM AND COMMUNICATIONS PROTECTION / Section Boundary Protection | Deny by Default — Allow by Exception



0 Resource(s) Failed

Compliance Section: Boundary Protection | Deny by Default — Allow by Exception

Informational

**Deny network communications traffic by default and allow network communications traffic by exception [Selection (one or more): at managed interfaces; for [Assignment: organization-defined systems]
].**

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

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

First Seen N/A | **Resource Type** Other

Recommendations

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

SYSTEM AND COMMUNICATIONS PROTECTION / Section Boundary Protection | Restrict Incoming Communications Traffic

1 Resource(s) Failed

Allow All

Compliance Section: Boundary Protection | Restrict Incoming Communications Traffic Low

Only allow incoming communications from [Assignment: organization-defined authorized sources] to be routed to [Assignment: organization-defined authorized destinations].

AWS EKS cluster security group overly permissive to all traffic

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

First Seen June 13, 2023 at 8:48:36 PM UTC | **Resource Type** Other

Recommendations

Before making any changes, please check the impact on your applications/services. If the Security Group reported indeed need to restrict all traffic, follow the instructions below:
1. Log in to the AWS console
2. Navigate to the 'VPC' service
3. Select the 'Security Group' reported in the alert
4. Click on 'Inbound Rules'
5. Remove the rule which has the 'Source' value as 0.0.0.0/0 or ::/0

SYSTEM AND COMMUNICATIONS PROTECTION / Section Boundary Protection | Restrict Incoming Communications Traffic

211
RESOURCE(S) PASSED

0 Resource(s) Failed

Compliance Section: Boundary Protection | Restrict Incoming Communications Traffic

Low

Only allow incoming communications from [Assignment: organization-defined authorized sources] to be routed to [Assignment: organization-defined authorized destinations].

AWS route table with VPC peering overly permissive to all traffic

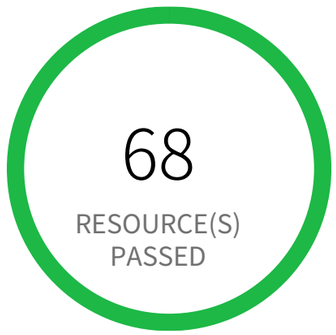
This policy identifies VPC route tables with VPC peering connection which are overly permissive to all traffic. Being highly selective in peering routing tables is a very effective way of minimizing the impact of breach as resources outside of these routes are inaccessible to the peered VPC.

First Seen N/A | **Resource Type** Other

Recommendations

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

SYSTEM AND COMMUNICATIONS PROTECTION / Section Boundary Protection | Restrict Incoming Communications Traffic



0 Resource(s) Failed

Compliance Section: Boundary Protection | Restrict Incoming Communications Traffic

Informational

Only allow incoming communications from [Assignment: organization-defined authorized sources] to be routed to [Assignment: organization-defined authorized destinations].

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

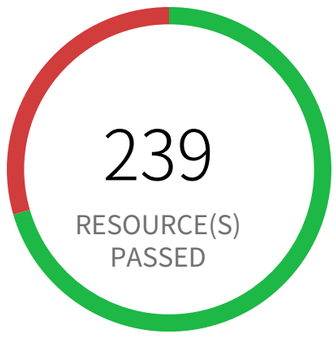
This policy identifies Elastic Load Balancers (ELB) which have security group with no inbound rules. A security group with no inbound rule will deny all incoming requests. ELB security groups should have at least one inbound rule, ELB with no inbound permissions will deny all traffic incoming to ELB;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

First Seen N/A | **Resource Type** Other

Recommendations

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

SYSTEM AND COMMUNICATIONS PROTECTION / Section Boundary Protection | Block Communication from Non-organizationally Configured Hosts



100 Resource(s) Failed

default, default, default, default, default, default, default, default, default, default & 90 more

Compliance Section: Boundary Protection | Block Communication from Non-organizationally Configured Hosts

High

Block inbound and outbound communications traffic between [Assignment: organization-defined communication clients] that are independently configured by end users and external service providers.

AWS Default Security Group does not restrict all traffic

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

First Seen August 22, 2018 at 4:44:04 AM UTC | **Resource Type** Other

Recommendations

Before making any changes, please check the impact on your applications/services.

For Resources associated with the alerted security group:
1. Identify AWS resources that exist within the default security group
2. Create a set of least privilege security groups for those resources
3. Place the resources in those security groups
4. Remove the associated resources from the default security group

For alerted Security Groups:
1. Log in to the AWS console
2. In the console, select the specific region from the 'Region' drop-down on the top right corner, for which the alert is generated

3. Navigate to the 'VPC' service
4. For each region, Click on 'Security Groups' specific to the alert
5. On section 'Inbound rules', Click on 'Edit Inbound Rules' and remove the existing rule, click on 'Save'
6. On section 'Outbound rules', Click on 'Edit Outbound Rules' and remove the existing rule, click on 'Save'

SYSTEM AND COMMUNICATIONS PROTECTION / Section Boundary Protection | Block Communication from Non-organizationally Configured Hosts

1 Resource(s) Failed

Allow All

Compliance Section: Boundary Protection | Block Communication from Non-organizationally Configured Hosts

Low

Block inbound and outbound communications traffic between [Assignment: organization-defined communication clients] that are independently configured by end users and external service providers.

AWS EKS cluster security group overly permissive to all traffic

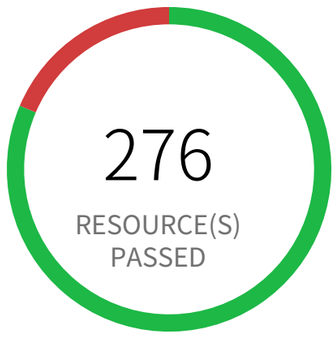
This policy identifies EKS cluster Security groups that are overly permissive to all traffic. Doing so, may allow a bad actor to brute force their way into the system and potentially get access to the entire network. Review your list of security group rules to ensure that your resources are not exposed.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

First Seen June 13, 2023 at 8:48:36 PM UTC | **Resource Type** Other

Recommendations

Before making any changes, please check the impact on your applications/services. If the Security Group reported indeed need to restrict all traffic, follow the instructions below:
1. Log in to the AWS console
2. Navigate to the 'VPC' service
3. Select the 'Security Group' reported in the alert
4. Click on 'Inbound Rules'
5. Remove the rule which has the 'Source' value as 0.0.0.0/0 or ::/0

SYSTEM AND COMMUNICATIONS PROTECTION / Section Boundary Protection | Block Communication from Non-organizationally Configured Hosts



63 Resource(s) Failed

launch-wizard-2, launch-wizard-1, launch-wizard-3, launch-wizard-1, launch-wizard-4, launch-wizard-1, launch-wizard-3, launch-wizard-2, launch-wizard-4, SSH SG & 53 more

Compliance Section: Boundary Protection | Block Communication from Non-organizationally Configured Hosts

High

Block inbound and outbound communications traffic between [Assignment: organization-defined communication clients] that are independently configured by end users and external service providers.

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

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

First Seen November 28, 2019 at 12:25:25 PM UTC | **Resource Type** Other

Recommendations

Before making any changes, please check the impact to your applications/services. If the Security Group reported indeed need to restrict all traffic, follow the instructions below:
1. Log in to the AWS Console
2. Navigate to the 'VPC' service
3. Select the 'Security Group' reported in the alert
4. Click on the 'Inbound Rule'
5. Remove the rule which has 'Source' value as 0.0.0.0/0 or ::/0 and 'Port Range' value as 22 (or range containing 22)

SYSTEM AND COMMUNICATIONS PROTECTION / Section Boundary Protection | Block Communication from Non-organizationally Configured Hosts

0 Resource(s) Failed

Compliance Section: Boundary Protection | Block Communication from Non-organizationally Configured Hosts

Low

Block inbound and outbound communications traffic between [Assignment: organization-defined communication clients] that are independently configured by end users and external service providers.

AWS route table with VPC peering overly permissive to all traffic

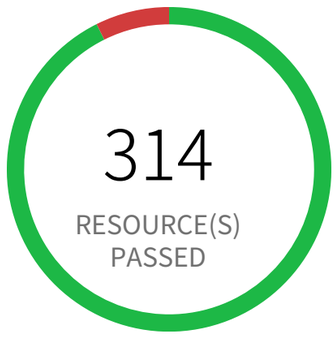
This policy identifies VPC route tables with VPC peering connection which are overly permissive to all traffic. Being highly selective in peering routing tables is a very effective way of minimizing the impact of breach as resources outside of these routes are inaccessible to the peered VPC.

First Seen N/A | **Resource Type** Other

Recommendations

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

SYSTEM AND COMMUNICATIONS PROTECTION / Section Boundary Protection | Block Communication from Non-organizationally Configured Hosts



25 Resource(s) Failed

pcsdemo-useast1-nlb-sg, Allow All_xpanse_ar_564, launch-wizard-3, Allow All_xpanse_ar_988, Allow All_xpanse_ar_605, Allow All_xpanse_ar_628, Allow All_xpanse_ar_248, Allow All_xpanse_ar_349, Allow All_xpanse_ar_588, Allow All_xpanse_ar_420 & 15 more

Compliance Section: Boundary Protection | Block Communication from Non-organizationally Configured Hosts

High

Block inbound and outbound communications traffic between [Assignment: organization-defined communication clients] that are independently configured by end users and external service providers.

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

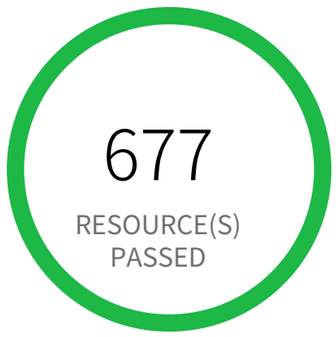
This policy identifies Security groups that allow all traffic on RDP port 3389. Doing so, may allow a bad actor to brute force their way into the system and potentially get access to the entire network. Review your list of security group rules to ensure that your resources are not exposed. As a best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

First Seen December 7, 2021 at 8:21:37 PM UTC | **Resource Type** Other

Recommendations

Before making any changes, please check the impact to your applications/services. If the Security Group reported indeed need to restrict all traffic, follow the instructions below:
1. Log in to the AWS Console
2. Navigate to the 'VPC' service
3. Select the 'Security Group' reported in the alert
4. Click on the 'Inbound Rule'
5. Remove the rule which has 'Source' value as 0.0.0.0/0 or ::/0 and 'Port Range' value as 3389 (or range containing 3389)

SYSTEM AND COMMUNICATIONS PROTECTION / Section Boundary Protection | Block Communication from Non-organizationally Configured Hosts



0 Resource(s) Failed

Compliance Section: Boundary Protection | Block Communication from Non-organizationally Configured Hosts

Informational

Block inbound and outbound communications traffic between [Assignment: organization-defined communication clients] that are independently configured by end users and external service providers.

AWS Elasticsearch IAM policy overly permissive to all traffic

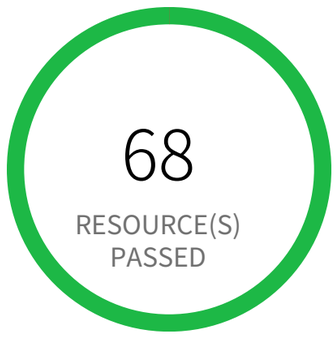
This policy identifies Elasticsearch IAM policies that are overly permissive to all traffic. Amazon Elasticsearch service makes it easy to deploy and manage Elasticsearch. Customers can create a domain where the service is accessible. The domain should be granted access restrictions so that only authorized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

First Seen N/A | **Resource Type** Other

Recommendations

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

SYSTEM AND COMMUNICATIONS PROTECTION / Section Boundary Protection | Block Communication from Non-organizationally Configured Hosts



0 Resource(s) Failed

Compliance Section: Boundary Protection | Block Communication from Non-organizationally Configured Hosts

Informational

Block inbound and outbound communications traffic between [Assignment: organization-defined communication clients] that are independently configured by end users and external service providers.

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

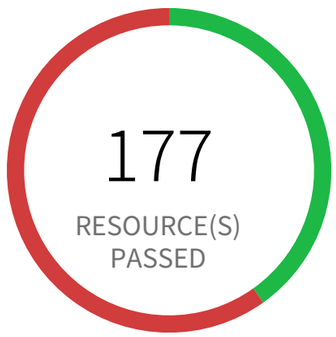
This policy identifies Elastic Load Balancers (ELB) which have security group with no inbound rules. A security group with no inbound rule will deny all incoming requests. ELB security groups should have at least one inbound rule, ELB with no inbound permissions will deny all traffic incoming to ELB;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

First Seen N/A | **Resource Type** Other

Recommendations

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

SYSTEM AND COMMUNICATIONS PROTECTION / Section Boundary Protection | Separate Subnets for Connecting to Different Security Domains



264 Resource(s) Failed

subnet-03cfc77261840b563,
subnet-09463d542833d6875,
subnet-097dbf2cb5c730dbb,
subnet-04e77351c2dc2bc64,
subnet-031a1752c34894bec,
subnet-0e04fc6277d8784b3,
subnet-0eebe8137dd18dba9,
subnet-0b734fbc89d666ffd,
subnet-066cccd20c29c7c6a,
subnet-0da5de145a30d0032 & 254 more

Compliance Section: Boundary Protection | Separate Subnets for Connecting to Different Security Domains

Low

Implement separate network addresses to connect to systems in different security domains.

AWS VPC subnets should not allow automatic public IP assignment

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

First Seen February 8, 2019 at 10:19:00 PM UTC | **Resource Type** Subnet

Recommendations

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

SYSTEM AND COMMUNICATIONS PROTECTION / Section Boundary Protection | Separate Subnets for Connecting to Different Security Domains

0 Resource(s) Failed

Compliance Section: Boundary Protection | Separate Subnets for Connecting to Different Security Domains

Low

Implement separate network addresses to connect to systems in different security domains.

AWS RDS instance not in private subnet

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

First Seen N/A | **Resource Type** Other

Recommendations

To resolve this alert, you should redeploy RDS into a private RDS Subnet group.

Note: You can not move an existing RDS instance from one subnet to another.

Create a RDS Subnet group:

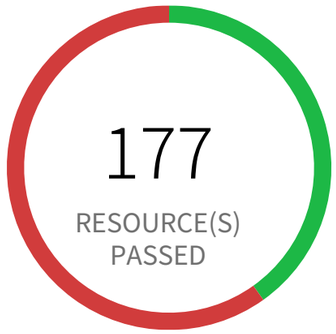
A DB subnet group is a collection of subnets (typically private) that you create for a VPC and that you then designate for your DB instances.

1. Open the Amazon RDS console
2. In the navigation pane, choose 'Subnet groups'
3. Choose 'Create DB Subnet Group'
4. Type the 'Name' of your DB subnet group
5. Add a 'Description' for your DB subnet group
6. Choose your 'VPC'
7. Choose 'Availability Zones'

8. In the Add subnets section, add your Private subnets related to this VPC
9. Choose Create

When creating your RDS DB, under Configure advanced settings, choose the Subnet group created above.

SYSTEM AND COMMUNICATIONS PROTECTION / Section Boundary Protection | Connections to Public Networks



264 Resource(s) Failed

subnet-03cfc77261840b563,
subnet-09463d542833d6875,
subnet-097dbf2cb5c730dbb,
subnet-04e77351c2dc2bc64,
subnet-031a1752c34894bec,
subnet-0e04fc6277d8784b3,
subnet-0eebe8137dd18dba9,
subnet-0b734fbc89d666ffd,
subnet-066cccd20c29c7c6a,
subnet-0da5de145a30d0032 & 254 more

Compliance Section: Boundary Protection | Connections to Public Networks Low

Prohibit the direct connection of [Assignment: organization-defined system] to a public network.

AWS VPC subnets should not allow automatic public IP assignment

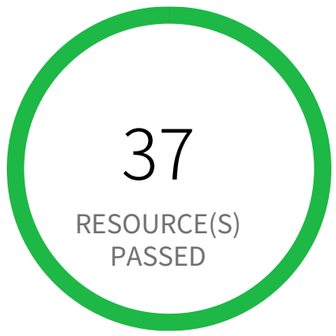
This policy identifies VPC subnets which allow automatic public IP assignment. VPC subnet is a part of the VPC having its own rules for traffic. Assigning the Public IP to the subnet automatically (on launch) can accidentally expose the instances within this subnet to internet and should be edited to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

First Seen February 8, 2019 at 10:19:00 PM UTC | **Resource Type** Subnet

Recommendations

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

SYSTEM AND COMMUNICATIONS PROTECTION / Section Boundary Protection | Connections to Public Networks



0 Resource(s) Failed

Compliance Section: Boundary Protection | Connections to Public Networks

Informational

Prohibit the direct connection of [Assignment: organization-defined system] to a public network.

AWS VPC allows unauthorized peering

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

First Seen N/A | **Resource Type** Other

Recommendations

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

SYSTEM AND COMMUNICATIONS PROTECTION / Section Boundary Protection | Connections to Public Networks

1 Resource(s) Failed

EKS-cluster-1

Compliance Section: Boundary Protection | Connections to Public Networks Informational

Prohibit the direct connection of [Assignment: organization-defined system] to a public network.

AWS EKS cluster using the default VPC

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

First Seen November 11, 2023 at 5:02:02 PM UTC | **Resource Type** Other

Recommendations

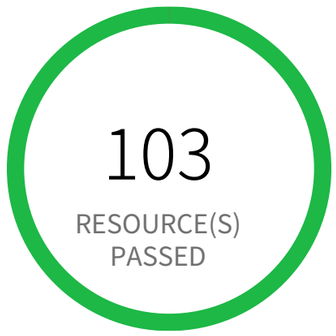
An AWS EKS cluster VPC cannot be changed once it is created. To resolve this alert, create a new cluster with the custom VPC as per your requirements, then migrate all required cluster data from the reported cluster to this newly created cluster and delete the reported Kubernetes cluster.

1. Open the Amazon EKS dashboard.
2. Choose Create cluster.
3. On the Create cluster page, fill in the following fields:

- Cluster name
- Kubernetes version
- Role name
- VPC - Choose your new custom VPC.
- Subnets
- Security Groups
- Endpoint private access
- Endpoint public access
- Logging

4. Choose Create.

SYSTEM AND COMMUNICATIONS PROTECTION / Section Boundary Protection | Connections to Public Networks



0 Resource(s) Failed

Compliance Section: Boundary Protection | Connections to Public Networks Low

Prohibit the direct connection of [Assignment: organization-defined system] to a public network.

AWS Amazon Machine Image (AMI) is publicly accessible

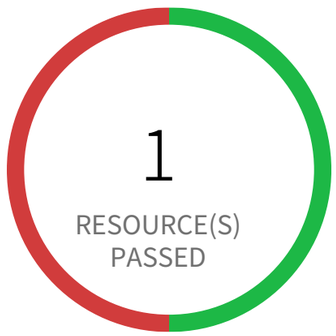
This policy identifies AWS AMIs which are owned by the AWS account and are accessible to the public. Amazon Machine Image (AMI) provides information to launch an instance in the cloud. The AMIs may contain proprietary customer information and should be accessible only to authorized internal users.

First Seen N/A | **Resource Type** VM Image

Recommendations

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

SYSTEM AND COMMUNICATIONS PROTECTION / Section Boundary Protection | Connections to Public Networks



1 Resource(s) Failed

d1ove8b1vrwgv4.cloudfront.net

Compliance Section: Boundary Protection | Connections to Public Networks Low

Prohibit the direct connection of [Assignment: organization-defined system] to a public network.

AWS Cloudfront Distribution with S3 have Origin Access set to disabled

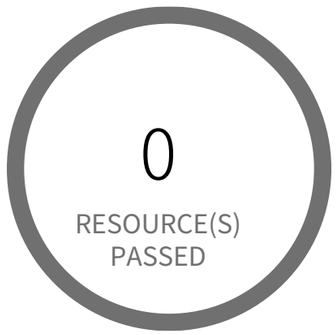
This policy identifies the AWS CloudFront distributions which are utilizing S3 bucket and have Origin Access Disabled. The origin access identity feature should be enabled for all your AWS CloudFront CDN distributions in order to restrict any direct access to your objects through Amazon S3 URLs.

First Seen November 3, 2019 at 2:15:19 PM UTC | **Resource Type** Other

Recommendations

1. Sign in to the AWS Console
2. Go to CloudFront
3. Choose the reported Distribution
4. Click on Distribution Settings
5. Click on 'Origins and Origin Groups
6. Select the S3 bucket and click on Edit
7. On the 'Restrict Bucket Access', Select Yes
8. Click on 'Yes, Edit'

SYSTEM AND COMMUNICATIONS PROTECTION / Section Boundary Protection | Connections to Public Networks



0 Resource(s) Failed

Compliance Section: Boundary Protection | Connections to Public Networks — Informational

Prohibit the direct connection of [Assignment: organization-defined system] to a public network.

AWS ElastiCache cluster not associated with VPC

This policy identifies ElastiCache Clusters which are not associated with VPC. It is highly recommended to associate ElastiCache with VPC, as provides virtual network in your own logically isolated area and features such as selecting IP address range, creating subnets, and configuring route tables, network gateways, and security settings.

NOTE: If you created your AWS account before 2013-12-04, you might have support for the EC2-Classic platform in some regions. AWS has deprecated the use of Amazon EC2-Classic for launching ElastiCache clusters. All current generation nodes are launched in Amazon Virtual Private Cloud only. So this policy only applies legacy ElastiCache clusters which are created using EC2-Classic.

First Seen N/A | **Resource Type** Other

Recommendations

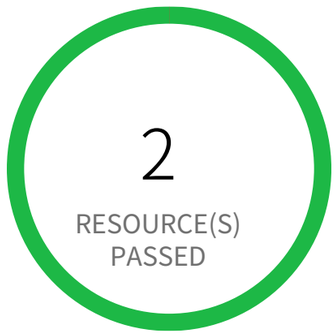
AWS ElastiCache cluster VPC association can be done only at the time of the creation of the cluster. So to fix this alert, create a new cluster with VPC, then migrate all required ElastiCache cluster data from the reported ElastiCache cluster to this newly created cluster and delete reported ElastiCache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

To create new ElastiCache cluster with at-rest encryption set, perform the following:
1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to ElastiCache Dashboard
4. Click on Redis or Memcached based on your requirement
5. Choose cluster parameters as per your requirement
6. Click on 'Advanced Redis settings' to expand the cluster advanced settings panel
7. Select desired VPC for 'Subnet group' along with other parameters
NOTE: If you don't specify a subnet when you launch a cluster, the cluster launches into your default Amazon VPC.
8. Click on 'Create' button to launch your new ElastiCache cluster

To delete reported ElastiCache cluster, perform the following:

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

SYSTEM AND COMMUNICATIONS PROTECTION / Section Transmission Confidentiality and Integrity | Cryptographic Protection



0 Resource(s) Failed

Compliance Section: Transmission Confidentiality and Integrity | Cryptographic Protection

Low

Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.

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

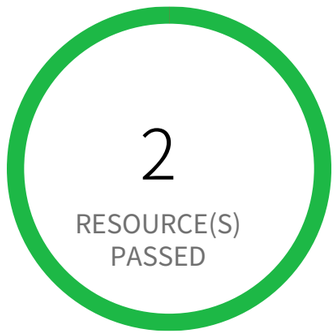
This policy identifies Elastic Load Balancers (Classic) which are configured with SSL negotiation policy containing vulnerable SSL protocol. The SSL protocol establishes a secure connection between a client and a server and ensures that all the data passed between the client and your load balancer is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

First Seen N/A | **Resource Type** Other

Recommendations

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

SYSTEM AND COMMUNICATIONS PROTECTION / Section Transmission Confidentiality and Integrity | Cryptographic Protection



0 Resource(s) Failed

Compliance Section: Transmission Confidentiality and Integrity | Cryptographic Protection

Medium

Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.

AWS CloudFront origin protocol policy does not enforce HTTPS-only

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

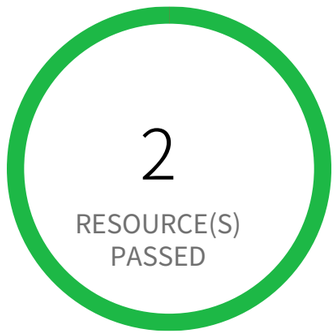
First Seen N/A | **Resource Type** Other

Recommendations

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

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

SYSTEM AND COMMUNICATIONS PROTECTION / Section Transmission Confidentiality and Integrity | Cryptographic Protection



0 Resource(s) Failed

Compliance Section: Transmission Confidentiality and Integrity | Cryptographic Protection

Medium

Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.

AWS CloudFront distribution is using insecure SSL protocols for HTTPS communication

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

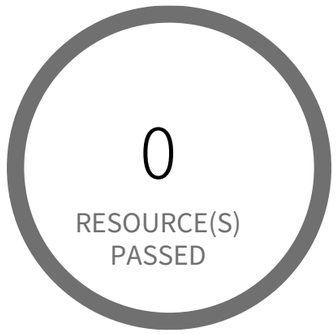
First Seen N/A | **Resource Type** Other

Recommendations

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

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

SYSTEM AND COMMUNICATIONS PROTECTION / Section Transmission Confidentiality and Integrity | Cryptographic Protection



0 Resource(s) Failed

Compliance Section: Transmission Confidentiality and Integrity | Cryptographic Protection

Low

Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.

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

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

First Seen N/A | **Resource Type** Other

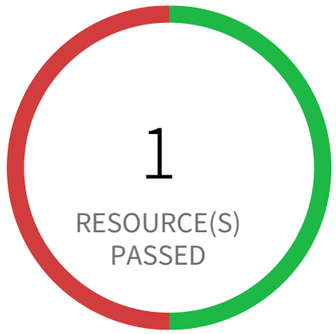
Recommendations

1. Login to the AWS Console.
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated.
3. Navigate to 'EMR' dashboard from 'Services' dropdown.
4. Go to 'Security configurations', click 'Create'.
5. On the Create security configuration window,
6. In 'Name' box, provide a name for the new EMR security configuration.
7. Under 'Local disk encryption', check the box 'Enable at-rest encryption for local disks'.
8. Select 'Custom' Key provider type from the 'Key provider type' dropdown list.
9. Follow the below link for creating the custom key,

https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-data-encryption-options.html
10. Click on 'Create' button.
11. On the left menu of EMR dashboard Click 'Clusters'.
12. Select the EMR cluster for which the alert has been generated and click on the 'Clone' button from the top menu.
13. In the Cloning popup, choose 'Yes' and Click 'Clone'.
14. On the Create Cluster page, in the Security Options section, click on 'security configuration'.
15. From the 'Security configuration' drop down select the name of the security configuration created at step 4 to step 8, click 'Create Cluster'.

16. Once the new cluster is set up verify its working and terminate the source cluster.
17. On the left menu of EMR dashboard Click 'Clusters', from the list of clusters select the source cluster which is alerted.
18. Click on the 'Terminate' button from the top menu.
19. On the 'Terminate clusters' pop-up, click 'Terminate'.

SYSTEM AND COMMUNICATIONS PROTECTION / Section Transmission Confidentiality and Integrity | Cryptographic Protection



1 Resource(s) Failed

d1ove8b1vrwgv4.cloudfront.net

Compliance Section: Transmission Confidentiality and Integrity | Cryptographic Protection

Low

Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.

AWS CloudFront web distribution using insecure TLS version

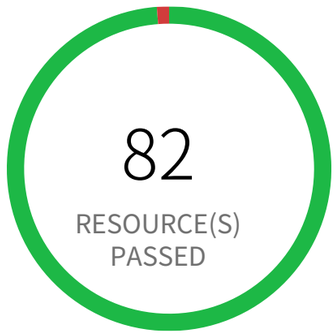
This policy identifies AWS CloudFront web distributions which are configured with TLS versions for HTTPS communication between viewers and CloudFront. As a best practice, use recommended TLSv1.2_2021 as the minimum protocol version in your CloudFront distribution security policies.

First Seen August 31, 2022 at 10:05:57 AM UTC | **Resource Type** Other

Recommendations

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

SYSTEM AND COMMUNICATIONS PROTECTION / Section Transmission Confidentiality and Integrity | Cryptographic Protection



1 Resource(s) Failed

bar-remediation-queue

Compliance Section: Transmission Confidentiality and Integrity | Cryptographic Protection Informational

Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.

AWS SQS queue encryption using default KMS key instead of CMK

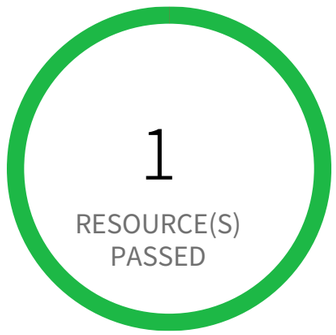
This policy identifies SQS queues which are encrypted with default KMS keys and not with Customer Master Keys(CMKs). It is a best practice to use customer managed Master Keys to encrypt your SQS queue messages. It gives you full control over the encrypted messages data.

First Seen June 29, 2021 at 3:18:58 PM UTC | **Resource Type** Other

Recommendations

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

SYSTEM AND COMMUNICATIONS PROTECTION / Section Transmission Confidentiality and Integrity | Cryptographic Protection



0 Resource(s) Failed

Compliance Section: Transmission Confidentiality and Integrity | Cryptographic Protection

Informational

Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.

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

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

First Seen N/A | **Resource Type** Other

Recommendations

RDS DB clusters can be encrypted only while creating the database cluster. You can't convert an unencrypted DB cluster to an encrypted one. However, you can restore an unencrypted Aurora DB cluster snapshot to an encrypted Aurora DB cluster. To do this, specify a KMS encryption key when you restore from the unencrypted DB cluster snapshot.

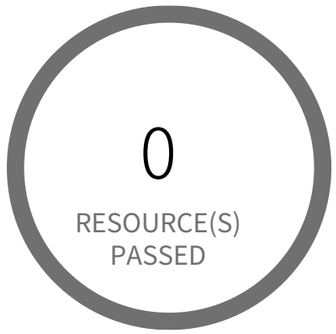
Step 1: To create a 'Snapshot' of the unencrypted DB cluster,
https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/USER_CreateSnapshotCluster.html
NOTE: As you can't restore from a DB cluster snapshot to an existing DB cluster; a new DB cluster is created when you restore. Once the Snapshot status is 'Available'.

Step 2: Follow the below link to restoring the Cluster from a DB Cluster Snapshot,
https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/USER_RestoreFromSnapshot.html

Once the DB cluster is restored and verified, follow below steps to delete the reported DB cluster,
1. Log in to the AWS Management Console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated.
3. Navigate to 'RDS' dashboard from 'Services' dropdown
4. In the navigation pane, choose ‘Databases’
5. In the list of DB instances, choose a writer instance for the DB cluster

6. Choose 'Actions', and then choose 'Delete'
FMI:
1. While deleting a RDS DB cluster, customer has to disable 'Enable deletion protection' otherwise instance cannot be deleted
2. While deleting RDS DB instance , AWS application will ask the end user to take Final snapshot
3. If a RDS DB cluster has a writer role instance, then User has to delete the write instance to delete the main cluster (Delete option won’t be enabled for main RDS DB cluster)

SYSTEM AND COMMUNICATIONS PROTECTION / Section Transmission Confidentiality and Integrity | Cryptographic Protection



0 Resource(s) Failed

Compliance Section: Transmission Confidentiality and Integrity | Cryptographic Protection

Low

Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.

AWS Redshift does not have require_ssl configured

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

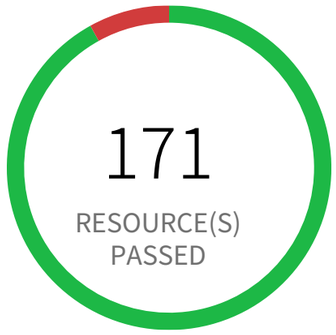
First Seen N/A | **Resource Type** Managed Database

Recommendations

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

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

SYSTEM AND COMMUNICATIONS PROTECTION / Section Transmission Confidentiality and Integrity | Cryptographic Protection



15 Resource(s) Failed

totalmess-s3-q4ns, corporatecontracts, corporatemarketingcontent, demo-bucket-publicly-exposed, human-resources-archive, foundry-vtt-ron-s3, productmarketingcontent, redlockpocprepdocs, confidentialinformation, orc-public-bucket & 5 more

Compliance Section: Transmission Confidentiality and Integrity | Cryptographic Protection

Medium

Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.

AWS S3 bucket not configured with secure data transport policy

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

First Seen February 19, 2019 at 8:45:03 PM UTC | **Resource Type** Other

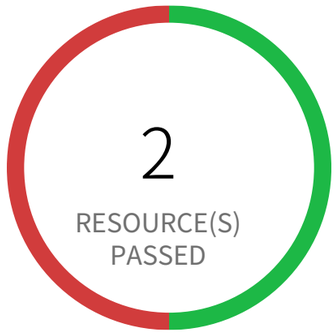
Recommendations

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

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

```
□}
}
```

SYSTEM AND COMMUNICATIONS PROTECTION / Section Transmission Confidentiality and Integrity | Cryptographic Protection



2 Resource(s) Failed

elb-pcsdemo-useast2-dmostardi, awseb-AWSEB-Q2FO6T2FSEDJ

Compliance Section: Transmission Confidentiality and Integrity | Cryptographic Protection

Medium

Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.

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

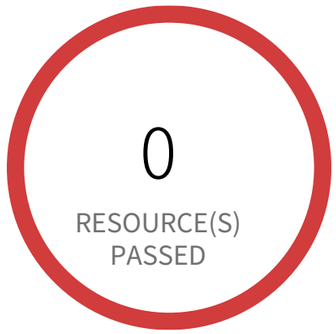
This policy identifies Elastic Load Balancers v2 (ELBv2) listener that are configured to accept connection requests over HTTP instead of HTTPS. As a best practice, use the HTTPS protocol to encrypt the communication between the application clients and the application load balancer.

First Seen November 17, 2021 at 1:12:50 PM UTC | **Resource Type** Other

Recommendations

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

SYSTEM AND COMMUNICATIONS PROTECTION / Section Transmission Confidentiality and Integrity | Cryptographic Protection



2 Resource(s) Failed

appElb, a90cc32b132be4f9c82eb1a4891319d6

Compliance Section: Transmission Confidentiality and Integrity | Cryptographic Protection

Low

Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.

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

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

First Seen July 15, 2020 at 1:54:20 AM UTC | **Resource Type** Managed Load Balancer

Recommendations

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

SYSTEM AND COMMUNICATIONS PROTECTION / Section Transmission Confidentiality and Integrity | Cryptographic Protection

0 Resource(s) Failed

Compliance Section: Transmission Confidentiality and Integrity | Cryptographic Protection

Low

Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.

AWS CloudFront web distribution with default SSL certificate

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

First Seen N/A | **Resource Type** Other

Recommendations

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

SYSTEM AND COMMUNICATIONS PROTECTION / Section Transmission Confidentiality and Integrity | Cryptographic Protection

0 Resource(s) Failed

Compliance Section: Transmission Confidentiality and Integrity | Cryptographic Protection

Informational

Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.

AWS RDS database not encrypted using Customer Managed Key

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

First Seen N/A | **Resource Type** Other

Recommendations

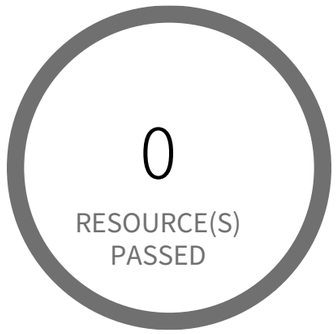
Because you can set AWS RDS database encryption only during database creation, the process for resolving this alert requires you to create a new RDS database with a customer managed key for encryption, migrate the data from the reported database to this newly created database, and delete the RDS database identified in the alert.

To create a new RDS database with encryption using a customer managed key:
1. Log in to the AWS console.
2. Select the region for which the alert was generated.
3. Navigate to the Amazon RDS Dashboard.
4. Select 'Create database'.
5. On the 'Select engine' page, select 'Engine options' and 'Next'.
6. On the 'Choose use case' page, select 'Use case' of database and 'Next'.
7. On the 'Specify DB details' page, specify the database details you need and click 'Next'.
Note: Amazon RDS encryption has some limitation on region and type instances. For Availability of Amazon RDS Encryption refer to: https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html#Overview.Encryption.Availability
8. On the 'Configure advanced settings' page, Under 'Encryption', select 'Enable encryption' and select the customer managed key [i.e. Other than (default)aws/rds] from 'Master key' dropdown list].
9. Select 'Create database'.

To delete the RDS database that uses the default KMS keys, which triggered the alert:

1. Log in to the AWS console
2. Select the region for which the alert was generated.
3. Navigate to the Amazon RDS Dashboard.
4. Click on Instances, and select the reported RDS database.
5. Select the 'Instance actions' drop-down and click 'Delete'.
7. In the 'Delete' dialog, select the 'Create final snapshot?' checkbox, if you want a backup. Provide a name for the final snapshot, confirm deletion and select 'Delete'.

SYSTEM AND COMMUNICATIONS PROTECTION / Section Transmission Confidentiality and Integrity | Cryptographic Protection



0 Resource(s) Failed

Compliance Section: Transmission Confidentiality and Integrity | Cryptographic Protection

Informational

Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.

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

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

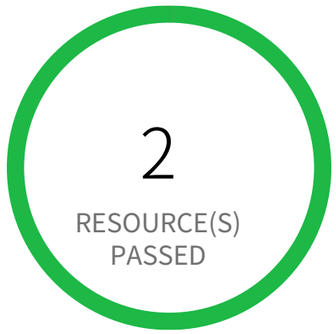
First Seen N/A | **Resource Type** Other

Recommendations

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

17. Click on the 'Terminate' button from the top menu.
18. On the 'Terminate clusters' pop-up, click 'Terminate'.

SYSTEM AND COMMUNICATIONS PROTECTION / Section Transmission Confidentiality and Integrity | Cryptographic Protection



0 Resource(s) Failed

Compliance Section: Transmission Confidentiality and Integrity | Cryptographic Protection

Medium

Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.

AWS CloudFront viewer protocol policy is not configured with HTTPS

For web distributions, you can configure CloudFront to require that viewers use HTTPS to request your objects, so connections are encrypted when CloudFront communicates with viewers.

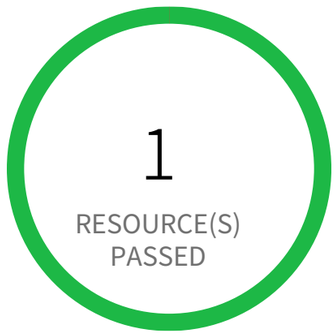
First Seen N/A | **Resource Type** Other

Recommendations

Configure CloudFront to require HTTPS between viewers and CloudFront.

1. Go to the AWS console CloudFront dashboard.
2. Select your distribution Id.
3. Select the 'Behaviors' tab.
4. Check the behavior you want to modify then select Edit.
5. Choose 'HTTPS Only' or 'Redirect HTTP to HTTPS' for Viewer Protocol Policy.
6. Select 'Yes, Edit.'

SYSTEM AND COMMUNICATIONS PROTECTION / Section Transmission Confidentiality and Integrity | Cryptographic Protection



0 Resource(s) Failed

Compliance Section: Transmission Confidentiality and Integrity | Cryptographic Protection

Informational

Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.

AWS Redshift Cluster not encrypted using Customer Managed Key

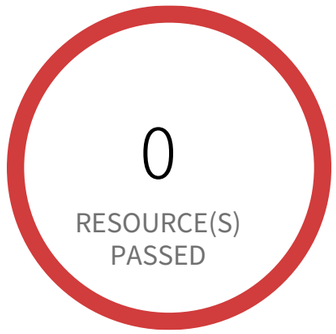
This policy identifies Redshift Clusters which are encrypted with default KMS keys and not with Keys managed by Customer. It is a best practice to use customer managed KMS Keys to encrypt your Redshift databases data. Customer-managed CMKs give you more flexibility, including the ability to create, rotate,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

First Seen N/A | **Resource Type** Other

Recommendations

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

SYSTEM AND COMMUNICATIONS PROTECTION / Section Transmission Confidentiality and Integrity | Cryptographic Protection



4 Resource(s) Failed

pcsdemo-useast1f-nlb, pscdemo-use-ast1e-nlb, elb-pcsdemo-useast2-dmostardi, awseb-AWSEB-Q2FO6T2FSEDJ

Compliance Section: Transmission Confidentiality and Integrity | Cryptographic Protection

Low

Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.

AWS Elastic Load Balancer v2 (ELBv2) with listener TLS/SSL is not configured

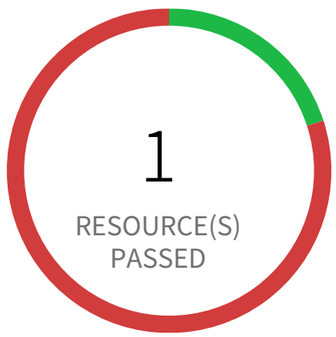
This policy identifies AWS Elastic Load Balancers v2 (ELBv2) which have non-secure listeners. As Load Balancers will be handling all incoming requests and routing the traffic accordingly. The listeners on the load balancers should always receive traffic over secure channel with a valid SSL certificate configured.

First Seen November 17, 2021 at 1:12:50 PM UTC | **Resource Type** Other

Recommendations

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

SYSTEM AND COMMUNICATIONS PROTECTION / Section Transmission Confidentiality and Integrity | Cryptographic Protection



4 Resource(s) Failed

CorporateDynamoTable, indexed-docs, my-pool-party-users-bathers, yaron_testing_dynamo

Compliance Section: Transmission Confidentiality and Integrity | Cryptographic Protection

Informational

Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.

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

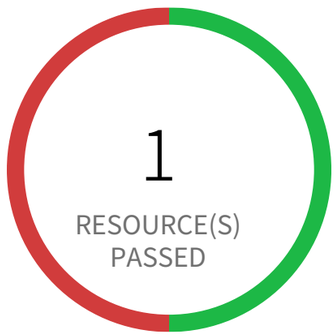
This policy identifies the DynamoDB tables that use AWS owned CMK (default) instead of AWS managed CMK (KMS) to encrypt data. AWS managed CMK provide additional features such as the ability to view the CMK and key policy, and audit the encryption and decryption of DynamoDB tables.

First Seen July 23, 2019 at 7:24:43 AM UTC | **Resource Type** Other

Recommendations

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

SYSTEM AND COMMUNICATIONS PROTECTION / Section Transmission Confidentiality and Integrity | Cryptographic Protection



1 Resource(s) Failed

test

Compliance Section: Transmission Confidentiality and Integrity | Cryptographic Protection

Informational

Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.

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

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

First Seen December 8, 2023 at 6:25:54 AM UTC | **Resource Type** Other

Recommendations

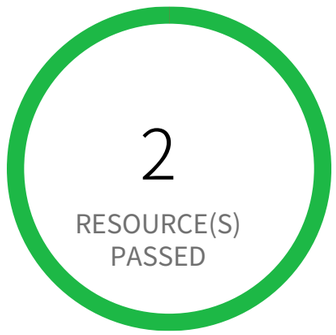
AWS EFS Encryption of data at rest can only be enabled during file system creation. So to resolve this alert, create a new EFS with encryption enabled with the customer-managed key, then migrate all required data from the reported EFS to this newly created EFS and delete reported EFS.

To create new EFS with encryption enabled, perform the following:
1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to EFS dashboard
4. Click on 'File systems' (Left Panel)
5. Click on 'Create file system' button
6. On the 'Configure file system access' step, specify EFS details as per your requirements and Click on 'Next Step'
7. On the 'Configure optional settings' step, Under 'Enable encryption' Choose 'Enable encryption of data at rest' and Select customer managed key [i.e. Other than (default)aws/elasticfilesystem] from 'Select KMS master key' dropdown list along with other parameters and Click on 'Next Step'
8. On the 'Review and create' step, Review all your setting and Click on 'Create File System' button

To delete reported EFS which does not has encryption, perform the following:
1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated

3. Navigate to EFS dashboard
4. Click on 'File systems' (Left Panel)
5. Select the reported file system
6. Click on 'Actions' drop-down
7. Click on 'Delete file system'
8. In the 'Permanently delete file system' popup box, To confirm the deletion enter the file system's ID and Click on 'Delete File System'

SYSTEM AND COMMUNICATIONS PROTECTION / Section Transmission Confidentiality and Integrity | Cryptographic Protection



0 Resource(s) Failed

Compliance Section: Transmission Confidentiality and Integrity | Cryptographic Protection

Low

Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.

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

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

First Seen N/A | **Resource Type** Other

Recommendations

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

SYSTEM AND COMMUNICATIONS PROTECTION / Section Cryptographic Key Establishment and Management

0 Resource(s) Failed

Compliance Section: Cryptographic Key Establishment and Management

Informational

Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].

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

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

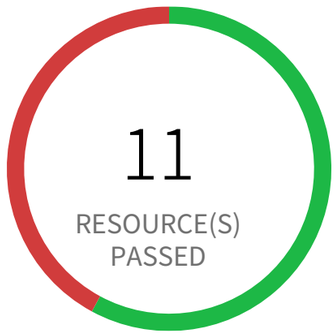
First Seen N/A | **Resource Type** Other

Recommendations

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

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

SYSTEM AND COMMUNICATIONS PROTECTION / Section Cryptographic Key Establishment and Management



8 Resource(s) Failed

pcsdemo-compute-ami-scanning, pcsdemo-compute-serverless-autodefend, twistlock-se-demo-service-account, pcsdemo-provisioning-crypto-usecase, test-iam, elcohen@paloaltonetworks.com, elad-azure-user1, varun

Compliance Section: Cryptographic Key Establishment and Management

High

Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].

BPI AWS access keys are not rotated for 60 days

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

First Seen June 23, 2022 at 5:56:01 AM UTC | **Resource Type** Other

Recommendations

1. Sign in to the AWS console and navigate to the 'IAM' service.
2. Click on the user that was reported in the alert.
3. Click on 'Security Credentials' and for each 'Access Key'.
4. Follow the instructions below to rotate the Access Keys that are older than 90 days.
https://aws.amazon.com/blogs/security/how-to-rotate-access-keys-for-iam-users/

SYSTEM AND COMMUNICATIONS PROTECTION / Section Cryptographic Key Establishment and Management

0 Resource(s) Failed

Compliance Section: Cryptographic Key Establishment and Management

Informational

Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].

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

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

First Seen N/A | **Resource Type** Other

Recommendations

Removing invalid certificates via AWS Management Console is not currently supported. To delete/upload SSL/TLS certificates stored in IAM via the AWS API use the Command Line Interface (CLI).

Remediation CLI:
1. Run describe-load-balancers command to make sure that the expiring server certificate is not currently used by any active load balancer.
aws elb describe-load-balancers --region <COMPUTE_REGION> --load-balancer-names <ELB_NAME> --query 'LoadBalancerDescriptions[*].ListenerDescriptions[*].Listener.SSLCertificateId'
This command output will return the Amazon Resource Name (ARN) for the SSL certificate currently used by the selected ELB:
[
□[
□□\"arn:aws:iam::1234567890:server-certificate/MyCertificate\"
□]
]
2. Create new AWS IAM certificate with your desired parameters value
3. To upload new IAM Certificate:
aws iam upload-server-certificate --server-certificate-name <NEW_CERTIFICATE_NAME> --certificate-body file://Certificate.pem --certificate-chain file://CertificateChain.pem --private-key file://PrivateKey.pem

4. To replaces the existing SSL certificate for the specified HTTPS load balancer:
aws elb set-load-balancer-listener-ssl-certificate --load-balancer-name <ELB_NAME> --load-balancer-port 443 --ssl-certificate-id arn:aws:iam::1234567890:server-certificate/<NEW_CERTIFICATE_NAME>
5. Now that is safe to remove the expiring SSL/TLS certificate from AWS IAM, To delete it run:
aws iam delete-server-certificate --server-certificate-name <CERTIFICATE_NAME>

SYSTEM AND COMMUNICATIONS PROTECTION / Section Cryptographic Key Establishment and Management

0 Resource(s) Failed

Compliance Section: Cryptographic Key Establishment and Management

Low

Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].

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

This policy identifies ACM certificates expiring in 30 days or less, which are in the AWS Certificate Manager. If SSL/TLS certificates are not renewed prior to their expiration date, they will become invalid and the communication between the client and the AWS resource that implements the certificates is no longer secure. As a best practice, it is recommended to renew certificates before their validity period ends. AWS Certificate Manager automatically renews certificates issued by the service that is used with other AWS resources. However, the ACM service does not renew automatically certificates that are not in use or not associated anymore with other AWS resources. So the renewal process must be done manually before these certificates become invalid.

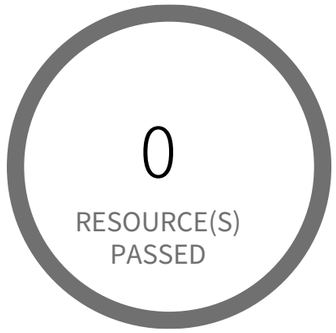
NOTE: If you wanted to be notified other than before or less than 30 days; you can clone this policy and replace '30' in RQL with your desired days value. For example, 15 days OR 7 days which will alert certificates expiring in 15 days or less OR 7 days or less respectively.

First Seen N/A | **Resource Type** Other

Recommendations

1. Log in to the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Go to the Certificate Manager(ACM) service
4. Choose the reported certificate
5. Verify that the 'Status' column shows 'Issued' for the reported certificate
6. Under 'Actions' drop-down select 'Reimport certificate' option
7. On the Import a certificate page, perform the following actions:
7a. In 'Certificate body*' box, paste the PEM-encoded certificate to import, purchased from your SSL certificate provider.
7b. In 'Certificate private key*' box, paste the PEM-encoded, unencrypted private key that matches the SSL/TLS certificate public key.
7c.(Optional) In 'Certificate chain' box, paste the PEM-encoded certificate chain delivered with the certificate body specified at step 7a.
8. Click on 'Review and import' button
9. On the Review and import page, review the imported certificate details then click on 'Import'

SYSTEM AND COMMUNICATIONS PROTECTION / Section Cryptographic Key Establishment and Management



0 Resource(s) Failed

Compliance Section: Cryptographic Key Establishment and Management

Low

Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].

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

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

First Seen N/A | **Resource Type** Other

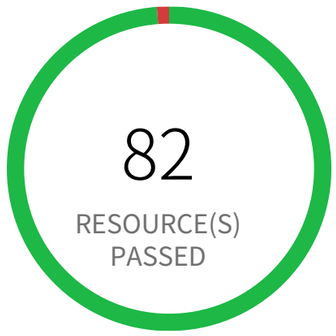
Recommendations

1. Login to the AWS Console.
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated.
3. Navigate to 'EMR' dashboard from 'Services' dropdown.
4. Go to 'Security configurations', click 'Create'.
5. On the Create security configuration window,
6. In 'Name' box, provide a name for the new EMR security configuration.
7. Under 'Local disk encryption', check the box 'Enable at-rest encryption for local disks'.
8. Select 'Custom' Key provider type from the 'Key provider type' dropdown list.
9. Follow the below link for creating the custom key,

https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-data-encryption-options.html
10. Click on 'Create' button.
11. On the left menu of EMR dashboard Click 'Clusters'.
12. Select the EMR cluster for which the alert has been generated and click on the 'Clone' button from the top menu.
13. In the Cloning popup, choose 'Yes' and Click 'Clone'.
14. On the Create Cluster page, in the Security Options section, click on 'security configuration'.
15. From the 'Security configuration' drop down select the name of the security configuration created at step 4 to step 8, click 'Create

Cluster'.
16. Once the new cluster is set up verify its working and terminate the source cluster.
17. On the left menu of EMR dashboard Click 'Clusters', from the list of clusters select the source cluster which is alerted.
18. Click on the 'Terminate' button from the top menu.
19. On the 'Terminate clusters' pop-up, click 'Terminate'.

SYSTEM AND COMMUNICATIONS PROTECTION / Section Cryptographic Key Establishment and Management



1 Resource(s) Failed

bar-remediation-queue

Compliance Section: Cryptographic Key Establishment and Management

Informational

Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].

AWS SQS queue encryption using default KMS key instead of CMK

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

First Seen June 29, 2021 at 3:18:58 PM UTC | **Resource Type** Other

Recommendations

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

SYSTEM AND COMMUNICATIONS PROTECTION / Section Cryptographic Key Establishment and Management

0 Resource(s) Failed

Compliance Section: Cryptographic Key Establishment and Management

Informational

Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].

AWS KMS Key scheduled for deletion

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

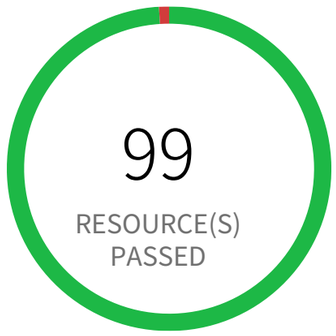
First Seen N/A | **Resource Type** Other

Recommendations

You should delete a KMS key only when you are sure that you don't need to use it anymore. To fix this alert, If you sure you no longer need a reported KMS key; dismiss the alert. If you are not sure, consider disabling the KMS key instead of deleting it.

To enable KMS CMKs which are scheduled for deletion, perform the following:
1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to Key Management Service (KMS)
4. Click on 'Customer managed keys' (Left Panel)
5. Select reported KMS Customer managed key
6. Click on 'Key actions' dropdown
7. Click on 'Cancel key deletion'
8. Click on 'Enable'

SYSTEM AND COMMUNICATIONS PROTECTION / Section Cryptographic Key Establishment and Management



1 Resource(s) Failed

test-elad-dev

Compliance Section: Cryptographic Key Establishment and Management

Informational

Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].

AWS Customer Master Key (CMK) rotation is not enabled

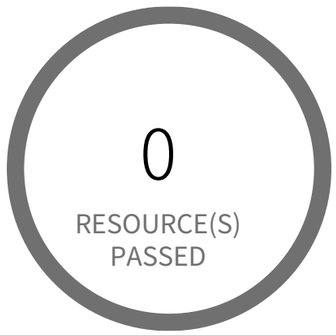
This policy identifies Customer Master Keys (CMKs) that are not enabled with key rotation. AWS KMS (Key Management Service) allows customers to create master keys to encrypt sensitive data in different services. As a security best practice, it is important to rotate the keys periodically so that if the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

First Seen June 29, 2021 at 3:18:58 PM UTC | **Resource Type** Managed Key Rotation Status

Recommendations

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

SYSTEM AND COMMUNICATIONS PROTECTION / Section Cryptographic Key Establishment and Management



0 Resource(s) Failed

Compliance Section: Cryptographic Key Establishment and Management

Low

Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].

AWS IAM has expired SSL/TLS certificates

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

First Seen N/A | **Resource Type** Other

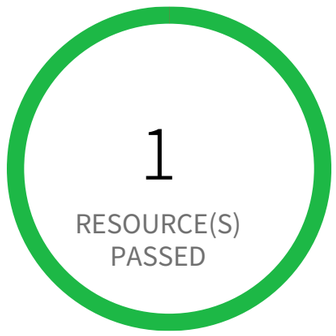
Recommendations

Removing invalid certificates via AWS Management Console is not currently supported. To delete SSL/TLS certificates stored in IAM via the AWS API use the Command Line Interface (CLI).

Remediation CLI:
1. Run describe-load-balancers command to make sure that the expired server certificate is not currently used by any active load balancer.
□aws elb describe-load-balancers --region <COMPUTE_REGION> --load-balancer-names <ELB_NAME> --query 'LoadBalancerDescriptions[*].ListenerDescriptions[*].Listener.SSLCertificateId'
This command output will return the Amazon Resource Name (ARN) for the SSL certificate currently used by the selected ELB:
□[
□□[
□□□"arn:aws:iam::1234567890:server-certificate/MyCertificate"
□□]
□]
2. If the load balancer listener using the reported expired certificate is not removed before the certificate, the ELB may continue to use the same certificate and work improperly. To delete the ELB listener that is using the expired SSL certificate, run following command:

- aws elb delete-load-balancer-listeners --region <COMPUTE_REGION> --load-balancer-name <ELB_NAME> --load-balancer-ports 443
3. Now that is safe to remove the expired SSL/TLS certificate from AWS IAM, To delete it run:
- aws iam delete-server-certificate --server-certificate-name <CERTIFICATE_NAME>

SYSTEM AND COMMUNICATIONS PROTECTION / Section Cryptographic Key Establishment and Management



0 Resource(s) Failed

Compliance Section: Cryptographic Key Establishment and Management

Informational

Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].

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

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

First Seen N/A | **Resource Type** Other

Recommendations

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

SYSTEM AND COMMUNICATIONS PROTECTION / Section Cryptographic Key Establishment and Management

0 Resource(s) Failed

Compliance Section: Cryptographic Key Establishment and Management

Informational

Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].

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

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

First Seen N/A | **Resource Type** Other

Recommendations

RDS DB clusters can be encrypted only while creating the database cluster. You can't convert an unencrypted DB cluster to an encrypted one. However, you can restore an unencrypted Aurora DB cluster snapshot to an encrypted Aurora DB cluster. To do this, specify a KMS encryption key when you restore from the unencrypted DB cluster snapshot.

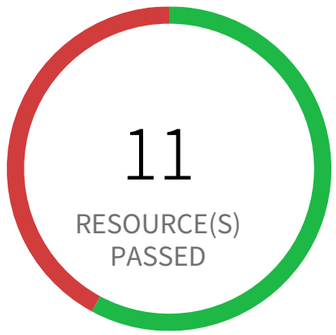
Step 1: To create a 'Snapshot' of the unencrypted DB cluster,
https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/USER_CreateSnapshotCluster.html
NOTE: As you can't restore from a DB cluster snapshot to an existing DB cluster; a new DB cluster is created when you restore. Once the Snapshot status is 'Available'.

Step 2: Follow the below link to restoring the Cluster from a DB Cluster Snapshot,
https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/USER_RestoreFromSnapshot.html

Once the DB cluster is restored and verified, follow below steps to delete the reported DB cluster,
1. Log in to the AWS Management Console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated.
3. Navigate to 'RDS' dashboard from 'Services' dropdown
4. In the navigation pane, choose ‘Databases’

5. In the list of DB instances, choose a writer instance for the DB cluster
6. Choose 'Actions', and then choose 'Delete'
FMI:
1. While deleting a RDS DB cluster, customer has to disable 'Enable deletion protection' otherwise instance cannot be deleted
2. While deleting RDS DB instance , AWS application will ask the end user to take Final snapshot
3. If a RDS DB cluster has a writer role instance, then User has to delete the write instance to delete the main cluster (Delete option won’t be enabled for main RDS DB cluster)

SYSTEM AND COMMUNICATIONS PROTECTION / Section Cryptographic Key Establishment and Management



8 Resource(s) Failed

pcsdemo-compute-ami-scanning, pcsdemo-compute-serverless-autodefend, twistlock-se-demo-service-account, pcsdemo-provisioning-crypto-usecase, test-iam, elcohen@paloaltonetworks.com, elad-azure-user1, varun

Compliance Section: Cryptographic Key Establishment and Management

Low

Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].

AWS access keys are not rotated for 90 days

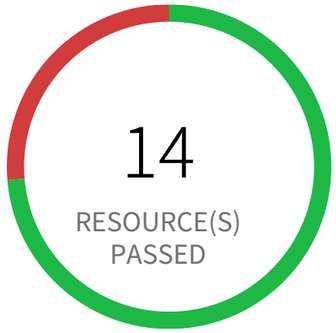
This policy identifies IAM users for which access keys are not rotated for 90 days. Access keys are used to sign API requests to AWS. As a security best practice, it is recommended that all access keys are regularly rotated to make sure that in the event of key compromise, unauthorized users are not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

First Seen June 29, 2021 at 3:18:50 PM UTC | **Resource Type** Other

Recommendations

1. Sign in to the AWS console and navigate to the 'IAM' service.
2. Click on the user that was reported in the alert.
3. Click on 'Security Credentials' and for each 'Access Key'.
4. Follow the instructions below to rotate the Access Keys that are older than 90 days.
https://aws.amazon.com/blogs/security/how-to-rotate-access-keys-for-iam-users/

SYSTEM AND COMMUNICATIONS PROTECTION / Section Cryptographic Key Establishment and Management



5 Resource(s) Failed

twistlock-se-demo-service-account, test-iam, elcohen@paloaltonetworks.com, elad-azure-user1, varun

Compliance Section: Cryptographic Key Establishment and Management

Informational

Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].

AWS access keys not used for more than 45 days

This policy identifies IAM users for which access keys are not used for more than 45 days. Access keys allow users programmatic access to resources. However, if any access key has not been used in the past 45 days, then that access key needs to be deleted (even though the access key is inactive)

First Seen September 18, 2022 at 12:36:52 PM UTC | **Resource Type** IAM Credentials Report

Recommendations

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

SYSTEM AND COMMUNICATIONS PROTECTION / Section Cryptographic Key Establishment and Management

0 Resource(s) Failed

Compliance Section: Cryptographic Key Establishment and Management

Informational

Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].

AWS RDS database not encrypted using Customer Managed Key

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

First Seen N/A | **Resource Type** Other

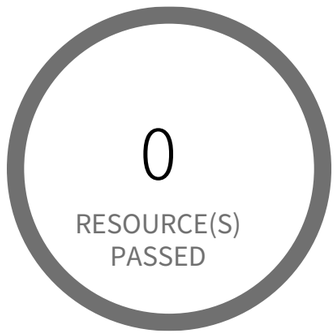
Recommendations

Because you can set AWS RDS database encryption only during database creation, the process for resolving this alert requires you to create a new RDS database with a customer managed key for encryption, migrate the data from the reported database to this newly created database, and delete the RDS database identified in the alert.

To create a new RDS database with encryption using a customer managed key:
1. Log in to the AWS console.
2. Select the region for which the alert was generated.
3. Navigate to the Amazon RDS Dashboard.
4. Select 'Create database'.
5. On the 'Select engine' page, select 'Engine options' and 'Next'.
6. On the 'Choose use case' page, select 'Use case' of database and 'Next'.
7. On the 'Specify DB details' page, specify the database details you need and click 'Next'.
Note: Amazon RDS encryption has some limitation on region and type instances. For Availability of Amazon RDS Encryption refer to: https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html#Overview.Encryption.Availability
8. On the 'Configure advanced settings' page, Under 'Encryption', select 'Enable encryption' and select the customer managed key [i.e. Other than (default)aws/rds] from 'Master key' dropdown list].
9. Select 'Create database'.

To delete the RDS database that uses the default KMS keys, which triggered the alert:
1. Log in to the AWS console
2. Select the region for which the alert was generated.
3. Navigate to the Amazon RDS Dashboard.
4. Click on Instances, and select the reported RDS database.
5. Select the 'Instance actions' drop-down and click 'Delete'.
7. In the 'Delete' dialog, select the 'Create final snapshot?' checkbox, if you want a backup. Provide a name for the final snapshot, confirm deletion and select 'Delete'.

SYSTEM AND COMMUNICATIONS PROTECTION / Section Cryptographic Key Establishment and Management



0 Resource(s) Failed

Compliance Section: Cryptographic Key Establishment and Management

Informational

Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].

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

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

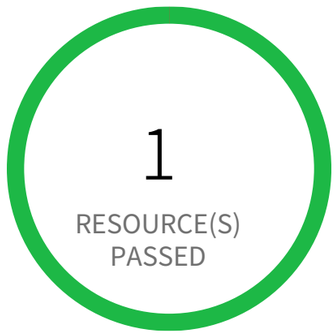
First Seen N/A | **Resource Type** Other

Recommendations

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

17. Click on the 'Terminate' button from the top menu.
18. On the 'Terminate clusters' pop-up, click 'Terminate'.

SYSTEM AND COMMUNICATIONS PROTECTION / Section Cryptographic Key Establishment and Management



0 Resource(s) Failed

Compliance Section: Cryptographic Key Establishment and Management

Informational

Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].

AWS Redshift Cluster not encrypted using Customer Managed Key

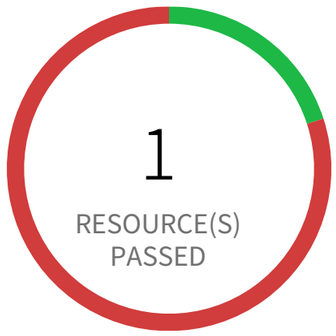
This policy identifies Redshift Clusters which are encrypted with default KMS keys and not with Keys managed by Customer. It is a best practice to use customer managed KMS Keys to encrypt your Redshift databases data. Customer-managed CMKs give you more flexibility, including the ability to create, rotate,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

First Seen N/A | **Resource Type** Other

Recommendations

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

SYSTEM AND COMMUNICATIONS PROTECTION / Section Cryptographic Key Establishment and Management



4 Resource(s) Failed

CorporateDynamoTable, indexed-docs, my-pool-party-users-bathers, yaron_testing_dynamo

Compliance Section: Cryptographic Key Establishment and Management

Informational

Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].

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

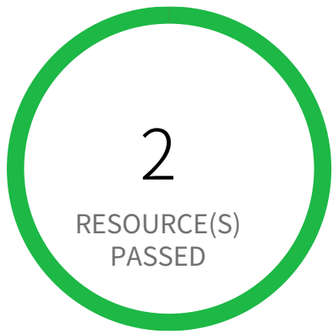
This policy identifies the DynamoDB tables that use AWS owned CMK (default) instead of AWS managed CMK (KMS) to encrypt data. AWS managed CMK provide additional features such as the ability to view the CMK and key policy, and audit the encryption and decryption of DynamoDB tables.

First Seen July 23, 2019 at 7:24:43 AM UTC | **Resource Type** Other

Recommendations

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

SYSTEM AND COMMUNICATIONS PROTECTION / Section Cryptographic Key Establishment and Management



0 Resource(s) Failed

Compliance Section: Cryptographic Key Establishment and Management

Informational

Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].

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

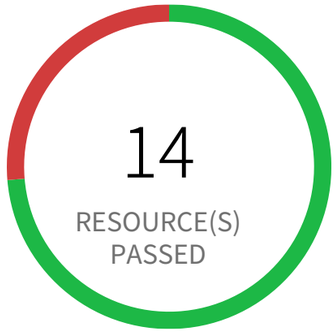
This policy identifies Elastic Load Balancers (ELB) which are using ACM certificates expired or expiring in 90 days. AWS Certificate Manager (ACM) is the preferred tool to provision, manage, and deploy your server certificates. With ACM you can request a certificate or deploy an existing ACM or external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

First Seen N/A | **Resource Type** Other

Recommendations

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Go to Certificate Manager(ACM) service
4. Choose the reported certificate
5. Under 'Actions' drop-down click on 'Reimport certificate'
6. On the 'Import a certificate' page:
6a. For 'Certificate body*', paste the PEM-encoded certificate to import
6b. For 'Certificate private key*', paste the PEM-encoded, unencrypted private key that matches the SSL/TLS certificate public key
6c. (Optional) For 'Certificate chain', paste the PEM-encoded certificate chain delivered
6d. Click Review and import button to continue the process
7. On the 'Review and import' page, review the imported certificate details then click on 'Import'

SYSTEM AND COMMUNICATIONS PROTECTION / Section Cryptographic Key Establishment and Management



5 Resource(s) Failed

twistlock-se-demo-service-account, test-iam, elcohen@paloaltonetworks.com, elad-azure-user1, varun

Compliance Section: Cryptographic Key Establishment and Management

Informational

Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].

AWS IAM user has two active Access Keys

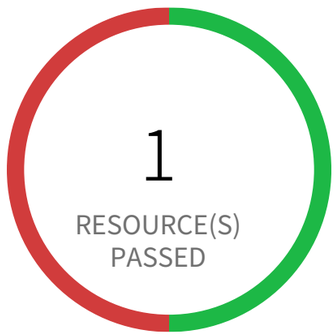
This policy identifies IAM users who have two active Access Keys. Each IAM user can have up to two Access Keys, having two Keys instead of one can lead to increased chances of accidental exposure. So it needs to be ensured that unused Access Keys are deleted.

First Seen March 27, 2022 at 7:16:58 PM UTC | **Resource Type** IAM Credentials Report

Recommendations

1. Sign in to the AWS Console and navigate to the 'IAM' service.
2. Click on Users in the navigation pane.
3. For the identified IAM user which has two active Access Keys, based on policies of your company, take appropriate action.
4. Create another IAM user with the specific objective performed by the 2nd Access Key.
5. Delete one of the unused Access Keys.

SYSTEM AND COMMUNICATIONS PROTECTION / Section Cryptographic Key Establishment and Management



1 Resource(s) Failed

test

Compliance Section: Cryptographic Key Establishment and Management

Informational

Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].

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

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

First Seen December 8, 2023 at 6:25:54 AM UTC | **Resource Type** Other

Recommendations

AWS EFS Encryption of data at rest can only be enabled during file system creation. So to resolve this alert, create a new EFS with encryption enabled with the customer-managed key, then migrate all required data from the reported EFS to this newly created EFS and delete reported EFS.

To create new EFS with encryption enabled, perform the following:
1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to EFS dashboard
4. Click on 'File systems' (Left Panel)
5. Click on 'Create file system' button
6. On the 'Configure file system access' step, specify EFS details as per your requirements and Click on 'Next Step'
7. On the 'Configure optional settings' step, Under 'Enable encryption' Choose 'Enable encryption of data at rest' and Select customer managed key [i.e. Other than (default)aws/elasticfilesystem] from 'Select KMS master key' dropdown list along with other parameters and Click on 'Next Step'
8. On the 'Review and create' step, Review all your setting and Click on 'Create File System' button

To delete reported EFS which does not has encryption, perform the following:
1. Sign into the AWS console

2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to EFS dashboard
4. Click on 'File systems' (Left Panel)
5. Select the reported file system
6. Click on 'Actions' drop-down
7. Click on 'Delete file system'
8. In the 'Permanently delete file system' popup box, To confirm the deletion enter the file system's ID and Click on 'Delete File System'

SYSTEM AND COMMUNICATIONS PROTEC-TION / Section Cryptographic Protection

0
RESOURCE(S) PASSED

0 Resource(s) Failed

Compliance Section: Cryptographic Protection

Low

a. Determine the [Assignment: organization-defined cryptographic uses]; and
b. Implement the following types of cryptography required for each specified cryptographic use: [Assignment: organization-defined types of cryptography for each specified cryptographic use].

AWS Redshift instances are not encrypted

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

First Seen N/A | **Resource Type** Managed Database

Recommendations

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

SYSTEM AND COMMUNICATIONS PROTECTION / Section Cryptographic Protection

0
RESOURCE(S) PASSED

5 Resource(s) Failed

myinstance, paasdb, apprds, pcsdemo-micro-seg-wordpress-mysql, database-1t

Compliance Section: Cryptographic Protection

Low

a. Determine the [Assignment: organization-defined cryptographic uses]; and
b. Implement the following types of cryptography required for each specified cryptographic use: [Assignment: organization-defined types of cryptography for each specified cryptographic use].

AWS RDS instance is not encrypted

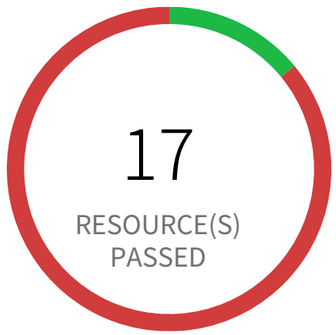
This policy identifies AWS RDS instances which are not encrypted. Amazon Relational Database Service (Amazon RDS) is a web service that makes it easier to set up and manage databases. Amazon allows customers to turn on encryption for RDS which is recommended for compliance and security reasons.

First Seen February 4, 2023 at 10:00:44 AM UTC | **Resource Type** Managed Database

Recommendations

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

SYSTEM AND COMMUNICATIONS PROTEC-TION / Section Cryptographic Protection



104 Resource(s) Failed

035297560255:EBS:ap-southeast-1,
035297560255:EBS:ap-south-1,
035297560255:EBS:eu-west-1,
035297560255:EBS:eu-central-1,
035297560255:EBS:eu-west-2,
035297560255:EBS:us-east-2,
035297560255:EBS:eu-north-1,
035297560255:EBS:ap-northeast-1,
035297560255:EBS:ap-northeast-3,
035297560255:EBS:us-west-2 & 94 more

Compliance Section: Cryptographic Protection

Low

a. Determine the [Assignment: organization-defined cryptographic uses]; and
b. Implement the following types of cryptography required for each specified cryptographic use: [Assignment: organization-defined types of cryptography for each specified cryptographic use].

AWS EBS volume region with encryption is disabled

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

First Seen November 2, 2021 at 9:19:13 AM UTC | **Resource Type** Other

Recommendations

To enable encryption at region level by default, follow below URL:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html#encryption-by-default

Additional Information:

To detect existing EBS volumes that are not encrypted ; refer Saved Search:
AWS EBS volumes are not encrypted_RL

To detect existing EBS volumes that are not encrypted with CMK, refer Saved Search:
AWS EBS volume not encrypted using Customer Managed Key_RL

SYSTEM AND COMMUNICATIONS PROTECTION / Section Public Key Infrastructure Certificates

0 Resource(s) Failed

Compliance Section: Public Key Infrastructure Certificates

Informational

a. Issue public key certificates under an [Assignment: organization-defined certificate policy] or obtain public key certificates from an approved service provider; and
b. Include only approved trust anchors in trust stores or certificate stores managed by the organization.

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

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

First Seen N/A | **Resource Type** Other

Recommendations

Removing invalid certificates via AWS Management Console is not currently supported. To delete/upload SSL/TLS certificates stored in IAM via the AWS API use the Command Line Interface (CLI).

Remediation CLI:
1. Run describe-load-balancers command to make sure that the expiring server certificate is not currently used by any active load balancer.
aws elb describe-load-balancers --region <COMPUTE_REGION> --load-balancer-names <ELB_NAME> --query 'LoadBalancerDescriptions[*].ListenerDescriptions[*].Listener.SSLCertificateId'
This command output will return the Amazon Resource Name (ARN) for the SSL certificate currently used by the selected ELB:
[
□[
□□\"arn:aws:iam::1234567890:server-certificate/MyCertificate\"
□]
]
2. Create new AWS IAM certificate with your desired parameters value
3. To upload new IAM Certificate:
aws iam upload-server-certificate --server-certificate-name <NEW_CERTIFICATE_NAME> --certificate-body file://Certificate.pem --certificate-chain file://CertificateChain.pem --private-key file://PrivateKey.pem

4. To replaces the existing SSL certificate for the specified HTTPS load balancer:
aws elb set-load-balancer-listener-ssl-certificate --load-balancer-name <ELB_NAME> --load-balancer-port 443 --ssl-certificate-id arn:aws:iam::1234567890:server-certificate/<NEW_CERTIFICATE_NAME>
5. Now that is safe to remove the expiring SSL/TLS certificate from AWS IAM, To delete it run:
aws iam delete-server-certificate --server-certificate-name <CERTIFICATE_NAME>

SYSTEM AND COMMUNICATIONS PROTECTION / Section Public Key Infrastructure Certificates

0 Resource(s) Failed

Compliance Section: Public Key Infrastructure Certificates

Low

a. Issue public key certificates under an [Assignment: organization-defined certificate policy] or obtain public key certificates from an approved service provider; and
b. Include only approved trust anchors in trust stores or certificate stores managed by the organization.

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

This policy identifies ACM certificates expiring in 30 days or less, which are in the AWS Certificate Manager. If SSL/TLS certificates are not renewed prior to their expiration date, they will become invalid and the communication between the client and the AWS resource that implements the certificates is no longer secure. As a best practice, it is recommended to renew certificates before their validity period ends. AWS Certificate Manager automatically renews certificates issued by the service that is used with other AWS resources. However, the ACM service does not renew automatically certificates that are not in use or not associated anymore with other AWS resources. So the renewal process must be done manually before these certificates become invalid.

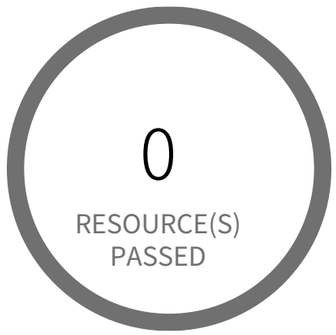
NOTE: If you wanted to be notified other than before or less than 30 days; you can clone this policy and replace '30' in RQL with your desired days value. For example, 15 days OR 7 days which will alert certificates expiring in 15 days or less OR 7 days or less respectively.

First Seen N/A | **Resource Type** Other

Recommendations

1. Log in to the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Go to the Certificate Manager(ACM) service
4. Choose the reported certificate
5. Verify that the 'Status' column shows 'Issued' for the reported certificate
6. Under 'Actions' drop-down select 'Reimport certificate' option
7. On the Import a certificate page, perform the following actions:
7a. In 'Certificate body*' box, paste the PEM-encoded certificate to import, purchased from your SSL certificate provider.
7b. In 'Certificate private key*' box, paste the PEM-encoded, unencrypted private key that matches the SSL/TLS certificate public key.
7c.(Optional) In 'Certificate chain' box, paste the PEM-encoded certificate chain delivered with the certificate body specified at step 7a.
8. Click on 'Review and import' button
9. On the Review and import page, review the imported certificate details then click on 'Import'

SYSTEM AND COMMUNICATIONS PROTECTION / Section Public Key Infrastructure Certificates



0 Resource(s) Failed

Compliance Section: Public Key Infrastructure Certificates

Low

a. Issue public key certificates under an [Assignment: organization-defined certificate policy] or obtain public key certificates from an approved service provider; and
b. Include only approved trust anchors in trust stores or certificate stores managed by the organization.

AWS IAM has expired SSL/TLS certificates

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

First Seen N/A | **Resource Type** Other

Recommendations

Removing invalid certificates via AWS Management Console is not currently supported. To delete SSL/TLS certificates stored in IAM via the AWS API use the Command Line Interface (CLI).

Remediation CLI:
1. Run describe-load-balancers command to make sure that the expired server certificate is not currently used by any active load balancer.
□aws elb describe-load-balancers --region <COMPUTE_REGION> --load-balancer-names <ELB_NAME> --query 'LoadBalancerDescriptions[*].ListenerDescriptions[*].Listener.SSLCertificateId'
This command output will return the Amazon Resource Name (ARN) for the SSL certificate currently used by the selected ELB:
□[
□□[
□□□"arn:aws:iam::1234567890:server-certificate/MyCertificate"
□□]
□]
2. If the load balancer listener using the reported expired certificate is not removed before the certificate, the ELB may continue to use the same certificate and work improperly. To delete the ELB listener that is using the expired SSL certificate, run following command:

- aws elb delete-load-balancer-listeners --region <COMPUTE_REGION> --load-balancer-name <ELB_NAME> --load-balancer-ports 443
3. Now that is safe to remove the expired SSL/TLS certificate from AWS IAM, To delete it run:
- aws iam delete-server-certificate --server-certificate-name <CERTIFICATE_NAME>

SYSTEM AND COMMUNICATIONS PROTECTION / Section Public Key Infrastructure Certificates

0 Resource(s) Failed

Compliance Section: Public Key Infrastructure Certificates

Informational

a. Issue public key certificates under an [Assignment: organization-defined certificate policy] or obtain public key certificates from an approved service provider; and
b. Include only approved trust anchors in trust stores or certificate stores managed by the organization.

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

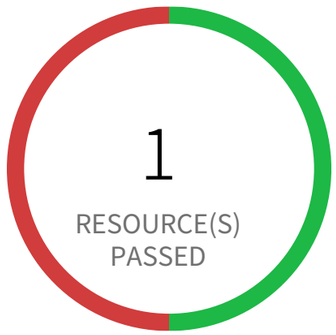
This policy identifies Elastic Load Balancers (ELB) which are using ACM certificates expired or expiring in 90 days. AWS Certificate Manager (ACM) is the preferred tool to provision, manage, and deploy your server certificates. With ACM you can request a certificate or deploy an existing ACM or external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

First Seen N/A | **Resource Type** Other

Recommendations

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Go to Certificate Manager(ACM) service
4. Choose the reported certificate
5. Under 'Actions' drop-down click on 'Reimport certificate'
6. On the 'Import a certificate' page:
6a. For 'Certificate body*', paste the PEM-encoded certificate to import
6b. For 'Certificate private key*', paste the PEM-encoded, unencrypted private key that matches the SSL/TLS certificate public key
6c. (Optional) For 'Certificate chain', paste the PEM-encoded certificate chain delivered
6d. Click Review and import button to continue the process
7. On the 'Review and import' page, review the imported certificate details then click on 'Import'

SYSTEM AND COMMUNICATIONS PROTEC-TION / Section Protection of Information at Rest



1 Resource(s) Failed

eladingestsearch

Compliance Section: Protection of Information at Rest

Low

Protect the [Selection (one or more): confidentiality; integrity] of the following information at rest: [Assignment: organization-defined information at rest].

AWS Elasticsearch domain Encryption for data at rest is disabled

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

First Seen August 13, 2022 at 9:01:40 AM UTC | **Resource Type** Other

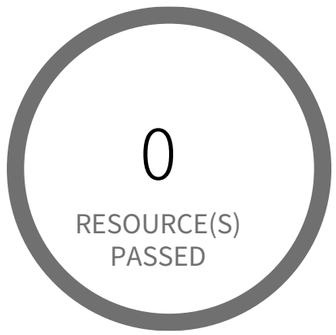
Recommendations

Enabling the encryption feature on existing domains requires Elasticsearch 6.7 or later. If your Elasticsearch 6.7 or later, follow below steps to enable encryption on existing Elasticsearch domain:
1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to Elasticsearch Service Dashboard
4. Choose reported Elasticsearch domain
5. Click on 'Actions' button, from drop-down select 'Modify encryptions'
6.In Modify encryptions page, Select the 'Enable encryption of data at rest' checkbox and Choose KMS key as per your requirement. It is recommended to choose KMS CMKs instead of default KMS [Default(aws/es)]; to get more grannular control on your Elasticsearch domain data.
7. Click on 'Submit'.

If your Elasticsearch is less than 6.7 version, then AWS Elasticsearch Domain encryption can be set only at the time of the creation of domain. So to fix this alert, create a new domain with encryption using KMS Keys and then migrate all required Elasticsearch domain data from the reported Elasticsearch domain to this newly created domain.
To set up the new Elasticsearch domain with encryption using KMS Key, refer the following URL:
https://docs.aws.amazon.com/elasticsearch-service/latest/developerguide/es-createupdatedomains.html

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

SYSTEM AND COMMUNICATIONS PROTEC-TION / Section Protection of Information at Rest



0 Resource(s) Failed

Compliance Section: Protection of Information at Rest

Low

Protect the [Selection (one or more): confidentiality; integrity] of the following information at rest: [Assignment: organization-defined information at rest].

AWS EMR cluster is not enabled with data encryption at rest

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

First Seen N/A | **Resource Type** Other

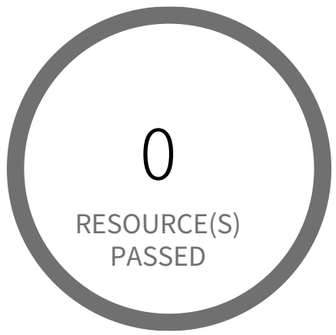
Recommendations

1. Login to the AWS Console.
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated.
3. Navigate to 'EMR' dashboard from 'Services' dropdown.
4. Go to 'Security configurations', click 'Create'.
5. On the Create security configuration window,
6. In 'Name' box, provide a name for the new EMR security configuration.
7. For encryption At Rest select the required encryption type ('S3 encryption'/'Local disk encryption'/both) and follow below link for enabling the same.
8. https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-encryption-enable.html

9. Click on 'Create' button.
10. On the left menu of EMR dashboard Click 'Clusters'.
11. Select the EMR cluster for which the alert has been generated and click on the 'Clone' button from the top menu.
12. In the Cloning popup, choose 'Yes' and Click 'Clone'.
13. On the Create Cluster page, in the Security Options section, click on 'security configuration'.
14. From the 'Security configuration' drop down select the name of the security configuration created at step 4 to step 8, click 'Create Cluster'.
15. Once you the new cluster is set up verify its working and terminate the source cluster in order to stop incurring charges for it.
16. On the left menu of EMR dashboard Click 'Clusters', from the list of clusters select the source cluster which is alerted.

17. Click on the 'Terminate' button from the top menu.
18. On the 'Terminate clusters' pop-up, click 'Terminate'.

SYSTEM AND COMMUNICATIONS PROTEC-TION / Section Protection of Information at Rest



0 Resource(s) Failed

Compliance Section: Protection of Information at Rest

Low

Protect the [Selection (one or more): confidentiality; integrity] of the following information at rest: [Assignment: organization-defined information at rest].

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

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

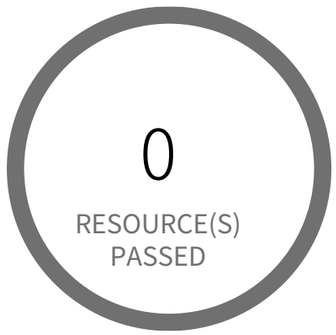
First Seen N/A | **Resource Type** Other

Recommendations

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

17. Click on the 'Terminate' button from the top menu
18. On the 'Terminate clusters' pop-up, click 'Terminate'.

SYSTEM AND COMMUNICATIONS PROTEC-TION / Section Protection of Information at Rest



0 Resource(s) Failed

Compliance Section: Protection of Information at Rest

Low

Protect the [Selection (one or more): confidentiality; integrity] of the following information at rest: [Assignment: organization-defined information at rest].

AWS ElastiCache Redis cluster with encryption for data at rest disabled

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

First Seen N/A | **Resource Type** Other

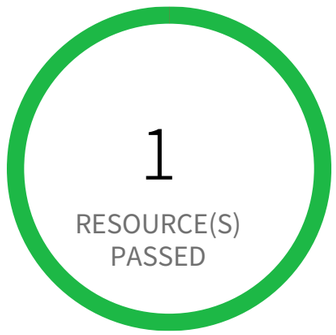
Recommendations

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

To create new ElastiCache Redis cluster with at-rest encryption set, perform the following:
1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to ElastiCache Dashboard
4. Click on Redis
5. Click on 'Create' button
6. On the 'Create your Amazon ElastiCache cluster' page,
a. Select 'Redis' cache engine type.
b. Enter a name for the new cache cluster
c. Select Redis engine version from 'Engine version compatibility' dropdown list.
Note: As of July 2018, In-transit encryption can be enabled only for AWS ElastiCache clusters with Redis engine version 3.2.6 and 4.0.10.
d. Click on 'Advanced Redis settings' to expand the cluster advanced settings panel
e. Select 'Encryption at-rest' checkbox to enable encryption along with other necessary parameters
7. Click on 'Create' button to launch your new ElastiCache Redis cluster

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

SYSTEM AND COMMUNICATIONS PROTEC-TION / Section Protection of Information at Rest



0 Resource(s) Failed

Compliance Section: Protection of Information at Rest

Low

Protect the [Selection (one or more): confidentiality; integrity] of the following information at rest: [Assignment: organization-defined information at rest].

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

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

First Seen N/A | **Resource Type** Other

Recommendations

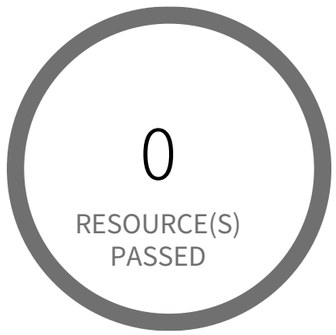
AWS EFS Encryption of data at rest can only be enabled during file system creation. So to resolve this alert, create a new EFS with encryption enabled, then migrate all required file data from the reported EFS to this newly created EFS and delete reported EFS.

To create a new EFS with encryption enabled, perform the following:
1. Sign in to the AWS console
2. In the console, select the specific region from the region drop-down on the top right corner, for which the alert is generated
3. Navigate to the EFS dashboard
4. Click on 'File systems' (Left Panel)
5. Click on the 'Create file system' button
6. On the 'Create file system' pop-up window,
7. Click on 'Customize' button to replicate the configurations of alerted file system as required
8. Ensure 'Enable encryption of data at rest' is selected
9. On the 'Review and create' step, Review all your setting and click on the 'Create' button

To delete reported EFS which does not has encryption, perform the following:
1. Sign in to the AWS console
2. In the console, select the specific region from the region drop-down on the top right corner, for which the alert is generated
3. Navigate to the EFS dashboard
4. Click on 'File systems' (Left Panel)

5. Select the reported file system
6. Click on 'Delete' button
7. In the 'Delete file system' popup box, To confirm the deletion enter the file system's ID and Click on 'Confirm'

SYSTEM AND COMMUNICATIONS PROTECTION / Section Protection of Information at Rest | Cryptographic Protection



0 Resource(s) Failed

Compliance Section: Protection of Information at Rest | Cryptographic Protection

Low

Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information].

AWS EMR cluster is not enabled with local disk encryption

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

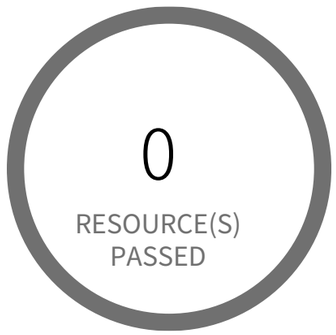
First Seen N/A | **Resource Type** Other

Recommendations

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

17. Click on the 'Terminate' button from the top menu.
18. On the 'Terminate clusters' pop-up, click 'Terminate'.

SYSTEM AND COMMUNICATIONS PROTECTION / Section Protection of Information at Rest | Cryptographic Protection



0 Resource(s) Failed

Compliance Section: Protection of Information at Rest | Cryptographic Protection

Low

Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information].

AWS EMR cluster is not enabled with data encryption in transit

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

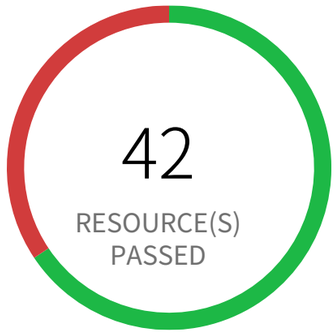
First Seen N/A | **Resource Type** Other

Recommendations

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

15. Once you the new cluster is set up verify its working and terminate the source cluster in order to stop incurring charges for it.
16. On the left menu of EMR dashboard Click 'Clusters', from the list of clusters select the source cluster which is alerted.
17. Click on the 'Terminate' button from the top menu.
18. On the 'Terminate clusters' pop-up, click 'Terminate'.

SYSTEM AND COMMUNICATIONS PROTECTION / Section Protection of Information at Rest | Cryptographic Protection



22 Resource(s) Failed

rds:pcsdemo-microseg-word-press-mysql-2024-02-11-10-26,
rds:pcsdemo-microseg-word-press-mysql-2024-02-10-10-26,
rds:pcsdemo-microseg-word-press-mysql-2024-02-12-10-26,
rds:pcsdemo-microseg-word-press-mysql-2024-02-09-10-26,
rds:pcsdemo-microseg-word-press-mysql-2024-02-06-10-27,
rds:pcsdemo-microseg-word-press-mysql-2024-02-05-10-26,
rds:pcsdemo-microseg-word-press-mysql-2024-02-10-13-12,
rds:myinstance-2024-02-13-07-17,…

Compliance Section: Protection of Information at Rest | Cryptographic Protection

Low

Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information].

AWS RDS DB snapshot is not encrypted

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

First Seen February 5, 2024 at 9:08:20 AM UTC | **Resource Type** Other

Recommendations

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

The source snapshot needs to be removed once the copy is available.
Note: If you delete a source snapshot before the target snapshot becomes available, the snapshot copy may fail. Verify that the target snapshot has a status of AVAILABLE before you delete a source snapshot.

SYSTEM AND COMMUNICATIONS PROTECTION / Section Protection of Information at Rest | Cryptographic Protection

0 Resource(s) Failed

Compliance Section: Protection of Information at Rest | Cryptographic Protection

Low

Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information].

AWS SSM Parameter is not encrypted

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

First Seen N/A | **Resource Type** Other

Recommendations

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

SYSTEM AND COMMUNICATIONS PROTECTION / Section Protection of Information at Rest | Cryptographic Protection

1 Resource(s) Failed

paasdb-cluster

Compliance Section: Protection of Information at Rest | Cryptographic Protection

Low

Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information].

AWS RDS DB cluster encryption is disabled

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

First Seen July 17, 2022 at 12:04:20 PM UTC | **Resource Type** Other

Recommendations

AWS DB clusters can be encrypted only while creating the database cluster. You can't convert an unencrypted DB cluster to an encrypted one. However, you can restore an unencrypted Aurora DB cluster snapshot to an encrypted Aurora DB cluster. To do this, specify a KMS encryption key when you restore from the unencrypted DB cluster snapshot.

For AWS RDS,
1. To create a 'Snapshot' of the unencrypted DB cluster, follow the instruction mentioned in below link:
RDS Link: https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/USER_CreateSnapshotCluster.html

NOTE: As you can't restore from a DB cluster snapshot to an existing DB cluster; a new DB cluster is created when you restore. Once the Snapshot status is 'Available', delete the unencrypted DB cluster before restoring from the DB cluster Snapshot by following below steps for AWS RDS,
a. Sign to the AWS Management Console and open the Amazon RDS console at https://console.aws.amazon.com/rds/
b. In the navigation pane, choose 'Databases'.
c. In the list of DB instances, choose a writer instance for the DB cluster.
d. Choose 'Actions', and then choose 'Delete'.

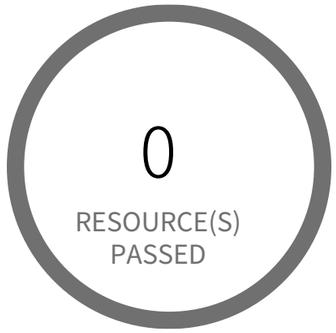
2. To restoring the Cluster from a DB Cluster Snapshot, follow the instruction mentioned in below link:
RDS Link: https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/USER_RestoreFromSnapshot.html

For AWS Document DB,
1. To create a 'Snapshot' of the unencrypted DB cluster, follow the instruction mentioned in below link:
Document DB Link: https://docs.aws.amazon.com/documentdb/latest/developerguide/backup_restore-create_manual_cluster_snapshot.html

NOTE: As you can't restore from a DB cluster snapshot to an existing DB cluster; a new DB cluster is created when you restore. Once the Snapshot status is 'Available', delete the unencrypted DB cluster before restoring from the DB cluster Snapshot by following below steps for AWS Document DB,
a. Sign to the AWS Management Console and open the Amazon DocumentDB console at https://console.aws.amazon.com/docdb/
b. In the navigation pane, choose 'Clusters'.
c. Select the cluster from the list which needs to be deleted
d. Choose 'Actions', and then choose 'Delete'.

2. To restoring the Cluster from a DB Cluster Snapshot, follow the instruction mentioned in below link:
Document DB Link: https://docs.aws.amazon.com/documentdb/latest/developerguide/backup_restore-restore_from_snapshot.html

SYSTEM AND COMMUNICATIONS PROTECTION / Section Protection of Information at Rest | Cryptographic Protection



0 Resource(s) Failed

Compliance Section: Protection of Information at Rest | Cryptographic Protection

Low

Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information].

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

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

First Seen N/A | **Resource Type** Other

Recommendations

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

To create new ElastiCache Redis cluster with In-transit encryption set, perform the following:
1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to ElastiCache Dashboard
4. Click on Redis
5. Click on 'Create' button
6. On the 'Create your Amazon ElastiCache cluster' page,
a. Select 'Redis' cache engine type.
b. Enter a name for the new cache cluster
c. Select Redis engine version from 'Engine version compatibility' dropdown list.
Note: As of July 2018, In-transit encryption can be enabled only for AWS ElastiCache clusters with Redis engine version 3.2.6 and 4.0.10.
d. Click on 'Advanced Redis settings' to expand the cluster advanced settings panel

e. Select 'Encryption in-transit' checkbox to enable encryption along with other necessary parameters
7. Click on 'Create' button to launch your new ElastiCache Redis cluster

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

11

SYSTEM AND INFORMATION INTEGRITY

SYSTEM AND INFORMATION INTEGRITY Overview

Section	Pass Rate	Failed	Passed
Flaw Remediation | Removal of Previous Versions of Software and Firmware — Low	100%	0	5
System Monitoring | System-wide Intrusion Detection System — Informational	30%	90	40
System Monitoring | Inbound and Outbound Communications Traffic — High	70%	100	239
System Monitoring | Inbound and Outbound Communications Traffic — Low	99%	1	369
System Monitoring | Inbound and Outbound Communications Traffic — High	81%	63	276
System Monitoring | Inbound and Outbound Communications Traffic — Low	100%	0	211
System Monitoring | Inbound and Outbound Communications Traffic — High	92%	25	314
System Monitoring | Inbound and Outbound Communications Traffic — Informational	100%	0	68
System Monitoring | Inbound and Outbound Communications Traffic — Informational	100%	0	677

NIST 800-53 Rev 5 / SYSTEM AND INFORMATION INTEGRITY

Section	Pass Rate	Failed	Passed
System Monitoring | Inbound and Outbound Communications Traffic — Informational	100%	0	68
System Monitoring | Analyze Communications Traffic Anomalies — Informational	30%	90	40
System Monitoring | Analyze Traffic and Event Patterns — AWS VPC··· — Informational	30%	90	40
Software, Firmware, and Information Integrity | Automated Notifications of Integrity Violations — Informational	100%	0	0
Software, Firmware, and Information Integrity | Cryptographic Protection — Low	100%	0	0
Software, Firmware, and Information Integrity | Cryptographic Protection — Low	0%	5	0
Software, Firmware, and Information Integrity | Cryptographic Protection — Low	14%	104	17
Software, Firmware, and Information Integrity | Auditing Capability for Significant Events — Informational	100%	0	0
Predictable Failure Prevention | Failover Capability — AWS ElastiCache··· — Informational	100%	0	0

SYSTEM AND INFORMATION INTEGRITY / Section Flaw Remediation | Removal of Previous Versions of Software and Firmware

0 Resource(s) Failed

Compliance Section: Flaw Remediation | Removal of Previous Versions of Software and Firmware Low

Remove previous versions of [Assignment: organization-defined software and firmware components] after updated versions have been installed.

AWS RDS minor upgrades not enabled

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

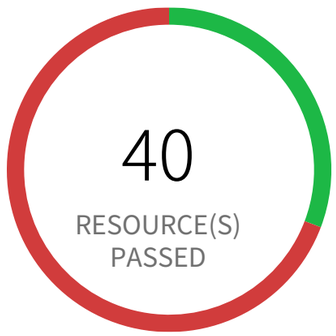
First Seen N/A | **Resource Type** Other

Recommendations

Enable RDS auto minor version upgrades.

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

SYSTEM AND INFORMATION INTEGRITY / Section System Monitoring | System-wide Intrusion Detection System



90 Resource(s) Failed

vpc-0471b3e2bb096facc,
vpc-011dc3f3696071f32,
vpc-094d28157f02ee78b,
vpc-0b6f0b71a665b77af,
vpc-05fa2ee4a0f24b7c6,
prismacloud-scan-1695743053643244271,
vpc-0cebecdf463401439,
vpc-0c9d3f27eb3596295, totalmess-vpc-q4ns,
vpc-0acb09cee29e45ce0 & 80 more

Compliance Section: System Monitoring | System-wide Intrusion Detection System — Informational

Connect and configure individual intrusion detection tools into a system-wide intrusion detection system.

AWS VPC Flow Logs not enabled

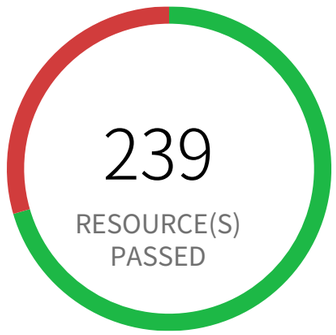
This policy identifies VPCs which have flow logs disabled. VPC Flow logs capture information about IP traffic going to and from network interfaces in your VPC. Flow logs are used as a security tool to monitor the traffic that is reaching your instances. Without the flow logs turned on, it is not possible to get any visibility into network traffic.

First Seen February 8, 2019 at 10:19:01 PM UTC | **Resource Type** Other

Recommendations

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to VPC Dashboard
4. Click on 'Your VPCs' and Choose the reported VPC
5. Click on the 'Flow logs' tab and follow the instructions as in link below to enable Flow Logs for the VPC:
https://aws.amazon.com/blogs/aws/vpc-flow-logs-log-and-view-network-traffic-flows/

SYSTEM AND INFORMATION INTEGRITY / Section System Monitoring | Inbound and Outbound Communications Traffic



100 Resource(s) Failed

default, default, default, default, default, default, default, default, default, default & 90 more

Compliance Section: System Monitoring | Inbound and Outbound Communications Traffic High

(a) Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic;
(b) Monitor inbound and outbound communications traffic [Assignment: organization-defined frequency] for [Assignment: organization-defined unusual or unauthorized activities or conditions].

AWS Default Security Group does not restrict all traffic

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

First Seen August 22, 2018 at 4:44:04 AM UTC | **Resource Type** Other

Recommendations

Before making any changes, please check the impact on your applications/services.

For Resources associated with the alerted security group:
1. Identify AWS resources that exist within the default security group
2. Create a set of least privilege security groups for those resources
3. Place the resources in those security groups
4. Remove the associated resources from the default security group

For alerted Security Groups:
1. Log in to the AWS console
2. In the console, select the specific region from the 'Region' drop-down on the top right corner, for which the alert is generated
3. Navigate to the 'VPC' service
4. For each region, Click on 'Security Groups' specific to the alert

5. On section 'Inbound rules', Click on 'Edit Inbound Rules' and remove the existing rule, click on 'Save'
6. On section 'Outbound rules', Click on 'Edit Outbound Rules' and remove the existing rule, click on 'Save'

SYSTEM AND INFORMATION INTEGRITY / Section System Monitoring | Inbound and Outbound Communications Traffic

1 Resource(s) Failed

Allow All

Compliance Section: System Monitoring | Inbound and Outbound Communications Traffic

Low

(a) Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic;
(b) Monitor inbound and outbound communications traffic [Assignment: organization-defined frequency] for [Assignment: organization-defined unusual or unauthorized activities or conditions].

AWS EKS cluster security group overly permissive to all traffic

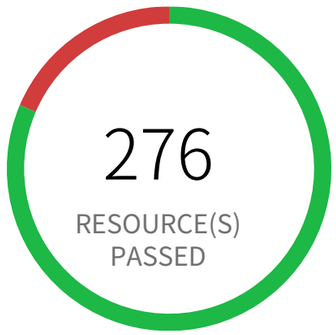
This policy identifies EKS cluster Security groups that are overly permissive to all traffic. Doing so, may allow a bad actor to brute force their way into the system and potentially get access to the entire network. Review your list of security group rules to ensure that your resources are not exposed.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

First Seen June 13, 2023 at 8:48:36 PM UTC | **Resource Type** Other

Recommendations

Before making any changes, please check the impact on your applications/services. If the Security Group reported indeed need to restrict all traffic, follow the instructions below:
1. Log in to the AWS console
2. Navigate to the 'VPC' service
3. Select the 'Security Group' reported in the alert
4. Click on 'Inbound Rules'
5. Remove the rule which has the 'Source' value as 0.0.0.0/0 or ::/0

SYSTEM AND INFORMATION INTEGRITY / Section System Monitoring | Inbound and Outbound Communications Traffic



63 Resource(s) Failed

launch-wizard-2, launch-wizard-1, launch-wizard-3, launch-wizard-1, launch-wizard-4, launch-wizard-1, launch-wizard-3, launch-wizard-2, launch-wizard-4, SSH SG & 53 more

Compliance Section: System Monitoring | Inbound and Outbound Communications Traffic High

(a) Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic;
(b) Monitor inbound and outbound communications traffic [Assignment: organization-defined frequency] for [Assignment: organization-defined unusual or unauthorized activities or conditions].

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

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

First Seen November 28, 2019 at 12:25:25 PM UTC | **Resource Type** Other

Recommendations

Before making any changes, please check the impact to your applications/services. If the Security Group reported indeed need to restrict all traffic, follow the instructions below:
1. Log in to the AWS Console
2. Navigate to the 'VPC' service
3. Select the 'Security Group' reported in the alert
4. Click on the 'Inbound Rule'
5. Remove the rule which has 'Source' value as 0.0.0.0/0 or ::/0 and 'Port Range' value as 22 (or range containing 22)

SYSTEM AND INFORMATION INTEGRITY / Section System Monitoring | Inbound and Outbound Communications Traffic

0 Resource(s) Failed

Compliance Section: System Monitoring | Inbound and Outbound Communications Traffic

Low

(a) Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic;
(b) Monitor inbound and outbound communications traffic [Assignment: organization-defined frequency] for [Assignment: organization-defined unusual or unauthorized activities or conditions].

AWS route table with VPC peering overly permissive to all traffic

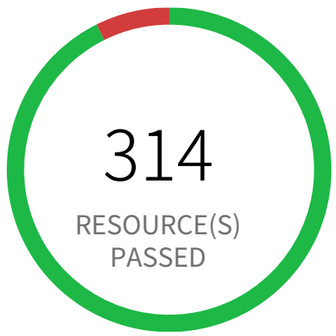
This policy identifies VPC route tables with VPC peering connection which are overly permissive to all traffic. Being highly selective in peering routing tables is a very effective way of minimizing the impact of breach as resources outside of these routes are inaccessible to the peered VPC.

First Seen N/A | **Resource Type** Other

Recommendations

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

SYSTEM AND INFORMATION INTEGRITY / Section System Monitoring | Inbound and Outbound Communications Traffic



25 Resource(s) Failed

pcsdemo-useast1-nlb-sg, Allow All_xpanse_ar_564, launch-wizard-3, Allow All_xpanse_ar_988, Allow All_xpanse_ar_605, Allow All_xpanse_ar_628, Allow All_xpanse_ar_248, Allow All_xpanse_ar_349, Allow All_xpanse_ar_588, Allow All_xpanse_ar_420 & 15 more

Compliance Section: System Monitoring | Inbound and Outbound Communications Traffic High

(a) Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic;
(b) Monitor inbound and outbound communications traffic [Assignment: organization-defined frequency] for [Assignment: organization-defined unusual or unauthorized activities or conditions].

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

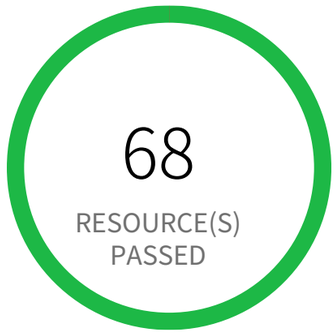
This policy identifies Security groups that allow all traffic on RDP port 3389. Doing so, may allow a bad actor to brute force their way into the system and potentially get access to the entire network. Review your list of security group rules to ensure that your resources are not exposed. As a best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

First Seen December 7, 2021 at 8:21:37 PM UTC | **Resource Type** Other

Recommendations

Before making any changes, please check the impact to your applications/services. If the Security Group reported indeed need to restrict all traffic, follow the instructions below:
1. Log in to the AWS Console
2. Navigate to the 'VPC' service
3. Select the 'Security Group' reported in the alert
4. Click on the 'Inbound Rule'
5. Remove the rule which has 'Source' value as 0.0.0.0/0 or ::/0 and 'Port Range' value as 3389 (or range containing 3389)

SYSTEM AND INFORMATION INTEGRITY / Section System Monitoring | Inbound and Outbound Communications Traffic



0 Resource(s) Failed

Compliance Section: System Monitoring | Inbound and Outbound Communications Traffic

Informational

(a) Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic;
(b) Monitor inbound and outbound communications traffic [Assignment: organization-defined frequency] for [Assignment: organization-defined unusual or unauthorized activities or conditions].

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

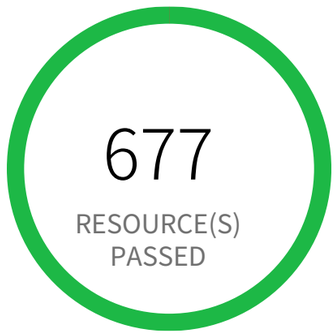
This policy identifies Elastic Load Balancers (ELB) which have security group with no outbound rules. A security group with no outbound rule will deny all outgoing requests. ELB security groups should have at least one outbound rule, ELB with no outbound permissions will deny all traffic going to any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

First Seen N/A | **Resource Type** Other

Recommendations

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

SYSTEM AND INFORMATION INTEGRITY / Section System Monitoring | Inbound and Outbound Communications Traffic



0 Resource(s) Failed

Compliance Section: System Monitoring | Inbound and Outbound Communications Traffic

Informational

(a) Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic;
(b) Monitor inbound and outbound communications traffic [Assignment: organization-defined frequency] for [Assignment: organization-defined unusual or unauthorized activities or conditions].

AWS Elasticsearch IAM policy overly permissive to all traffic

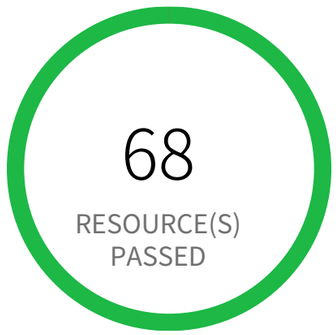
This policy identifies Elasticsearch IAM policies that are overly permissive to all traffic. Amazon Elasticsearch service makes it easy to deploy and manage Elasticsearch. Customers can create a domain where the service is accessible. The domain should be granted access restrictions so that only authorized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

First Seen N/A | **Resource Type** Other

Recommendations

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

SYSTEM AND INFORMATION INTEGRITY / Section System Monitoring | Inbound and Outbound Communications Traffic



0 Resource(s) Failed

Compliance Section: System Monitoring | Inbound and Outbound Communications Traffic

Informational

(a) Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic;
(b) Monitor inbound and outbound communications traffic [Assignment: organization-defined frequency] for [Assignment: organization-defined unusual or unauthorized activities or conditions].

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

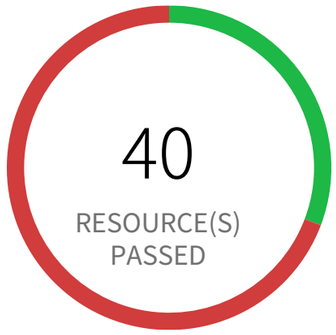
This policy identifies Elastic Load Balancers (ELB) which have security group with no inbound rules. A security group with no inbound rule will deny all incoming requests. ELB security groups should have at least one inbound rule, ELB with no inbound permissions will deny all traffic incoming to ELB;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

First Seen N/A | **Resource Type** Other

Recommendations

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

SYSTEM AND INFORMATION INTEGRITY / Section System Monitoring | Analyze Communications Traffic Anomalies



90 Resource(s) Failed

vpc-0471b3e2bb096facc,
vpc-011dc3f3696071f32,
vpc-094d28157f02ee78b,
vpc-0b6f0b71a665b77af,
vpc-05fa2ee4a0f24b7c6,
prismacloud-scan-1695743053643244271,
vpc-0cebecdf463401439,
vpc-0c9d3f27eb3596295, totalmess-vpc-q4ns,
vpc-0acb09cee29e45ce0 & 80 more

Compliance Section: System Monitoring | Analyze Communications Traffic Anomalies

Informational

Analyze outbound communications traffic at the external interfaces to the system and selected [Assignment: organization-defined interior points within the system] to discover anomalies.

AWS VPC Flow Logs not enabled

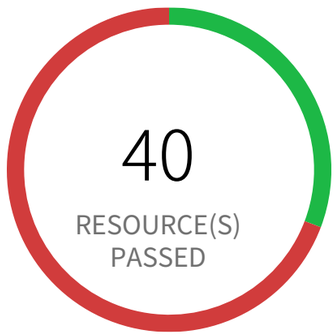
This policy identifies VPCs which have flow logs disabled. VPC Flow logs capture information about IP traffic going to and from network interfaces in your VPC. Flow logs are used as a security tool to monitor the traffic that is reaching your instances. Without the flow logs turned on, it is not possible to get any visibility into network traffic.

First Seen February 8, 2019 at 10:19:01 PM UTC | **Resource Type** Other

Recommendations

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to VPC Dashboard
4. Click on 'Your VPCs' and Choose the reported VPC
5. Click on the 'Flow logs' tab and follow the instructions as in link below to enable Flow Logs for the VPC:
https://aws.amazon.com/blogs/aws/vpc-flow-logs-log-and-view-network-traffic-flows/

SYSTEM AND INFORMATION INTEGRITY / Section System Monitoring | Analyze Traffic and Event Patterns



90 Resource(s) Failed

vpc-0471b3e2bb096facc,
vpc-011dc3f3696071f32,
vpc-094d28157f02ee78b,
vpc-0b6f0b71a665b77af,
vpc-05fa2ee4a0f24b7c6,
prismacloud-scan-1695743053643244271,
vpc-0cebecdf463401439,
vpc-0c9d3f27eb3596295, totalmess-vpc-q4ns,
vpc-0acb09cee29e45ce0 & 80 more

Compliance Section: System Monitoring | Analyze Traffic and Event Patterns — Informational

(a) Analyze communications traffic and event patterns for the system;
(b) Develop profiles representing common traffic and event patterns; and
(c) Use the traffic and event profiles in tuning system-monitoring devices.

AWS VPC Flow Logs not enabled

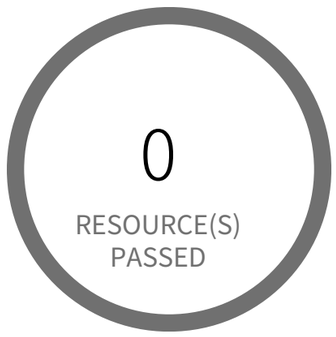
This policy identifies VPCs which have flow logs disabled. VPC Flow logs capture information about IP traffic going to and from network interfaces in your VPC. Flow logs are used as a security tool to monitor the traffic that is reaching your instances. Without the flow logs turned on, it is not possible to get any visibility into network traffic.

First Seen February 8, 2019 at 10:19:01 PM UTC | **Resource Type** Other

Recommendations

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to VPC Dashboard
4. Click on 'Your VPCs' and Choose the reported VPC
5. Click on the 'Flow logs' tab and follow the instructions as in link below to enable Flow Logs for the VPC:
https://aws.amazon.com/blogs/aws/vpc-flow-logs-log-and-view-network-traffic-flows/

SYSTEM AND INFORMATION INTEGRITY / Section Software, Firmware, and Information Integrity | Automated Notifications of Integrity Violations



0 Resource(s) Failed

Compliance Section: Software, Firmware, and Information Integrity | Automated Notifications of Integrity Violations

Informational

Employ automated tools that provide notification to [Assignment: organization-defined personnel or roles] upon discovering discrepancies during integrity verification.

AWS RDS event subscription disabled for DB security groups

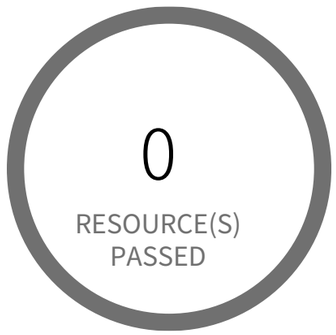
This policy identifies RDS event subscriptions for which DB security groups event subscription is disabled. You can create an Amazon RDS event notification subscription so that you can be notified when an event occurs for given DB security groups.

First Seen N/A | **Resource Type** Other

Recommendations

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

SYSTEM AND INFORMATION INTEGRITY / Section Software, Firmware, and Information Integrity | Cryptographic Protection



0 Resource(s) Failed

Compliance Section: Software, Firmware, and Information Integrity | Cryptographic Protection

Low

Implement cryptographic mechanisms to detect unauthorized changes to software, firmware, and information.

AWS Redshift instances are not encrypted

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

First Seen N/A | **Resource Type** Managed Database

Recommendations

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

SYSTEM AND INFORMATION INTEGRITY / Section Software, Firmware, and Information Integrity | Cryptographic Protection

5 Resource(s) Failed

myinstance, paasdb, apprds, pcsdemo-microseg-wordpress-mysql, database-1t

Compliance Section: Software, Firmware, and Information Integrity | Cryptographic Protection Low

Implement cryptographic mechanisms to detect unauthorized changes to software, firmware, and information.

AWS RDS instance is not encrypted

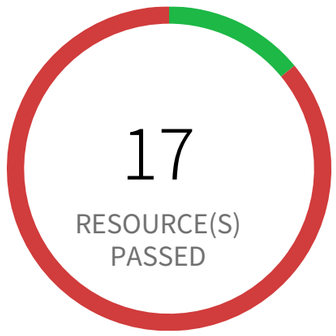
This policy identifies AWS RDS instances which are not encrypted. Amazon Relational Database Service (Amazon RDS) is a web service that makes it easier to set up and manage databases. Amazon allows customers to turn on encryption for RDS which is recommended for compliance and security reasons.

First Seen February 4, 2023 at 10:00:44 AM UTC | **Resource Type** Managed Database

Recommendations

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

SYSTEM AND INFORMATION INTEGRITY / Section Software, Firmware, and Information Integrity | Cryptographic Protection



104 Resource(s) Failed

035297560255:EBS:ap-southeast-1,
035297560255:EBS:ap-south-1,
035297560255:EBS:eu-west-1,
035297560255:EBS:eu-central-1,
035297560255:EBS:eu-west-2,
035297560255:EBS:us-east-2,
035297560255:EBS:eu-north-1,
035297560255:EBS:ap-northeast-1,
035297560255:EBS:ap-northeast-3,
035297560255:EBS:us-west-2 & 94 more

Compliance Section: Software, Firmware, and Information Integrity | Cryptographic Protection Low

Implement cryptographic mechanisms to detect unauthorized changes to software, firmware, and information.

AWS EBS volume region with encryption is disabled

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

First Seen November 2, 2021 at 9:19:13 AM UTC | **Resource Type** Other

Recommendations

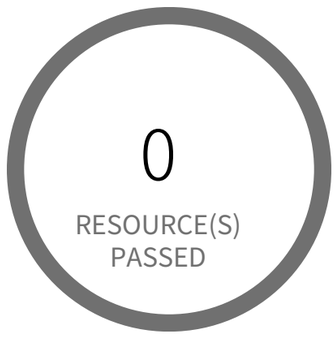
To enable encryption at region level by default, follow below URL:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html#encryption-by-default

Additional Information:

To detect existing EBS volumes that are not encrypted ; refer Saved Search:
AWS EBS volumes are not encrypted_RL

To detect existing EBS volumes that are not encrypted with CMK, refer Saved Search:
AWS EBS volume not encrypted using Customer Managed Key_RL

SYSTEM AND INFORMATION INTEGRITY / Section Software, Firmware, and Information Integrity | Auditing Capability for Significant Events



0 Resource(s) Failed

Compliance Section: Software, Firmware, and Information Integrity | Auditing Capability for Significant Events

Informational

Upon detection of a potential integrity violation, provide the capability to audit the event and initiate the following actions: [Selection (one or more): generate an audit record; alert current user; alert [Assignment: organization-defined personnel or roles]
;
[Assignment: organization-defined other actions]
].

AWS Redshift database does not have audit logging enabled

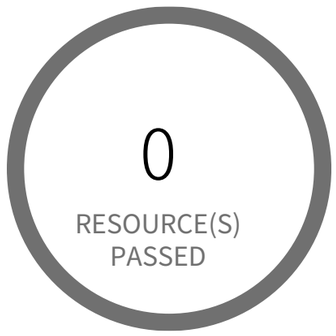
Audit logging is not enabled by default in Amazon Redshift. When you enable logging on your cluster, Amazon Redshift creates and uploads logs to Amazon S3 that capture data from the creation of the cluster to the present time.

First Seen N/A | **Resource Type** Managed Database

Recommendations

1. Login to AWS Console.
2. Goto Amazon Redshift service
3. On left navigation panel, click on Clusters
4. Click on the reported cluster
5. Click on Database tab and choose 'Configure Audit Logging'
6. On Enable Audit Logging, choose 'Yes'
7. Create a new s3 bucket or use an existing bucket
8. click Save

SYSTEM AND INFORMATION INTEGRITY / Section Predictable Failure Prevention | Failover Capability



0 Resource(s) Failed

Compliance Section: Predictable Failure Prevention | Failover Capability — Informational

**Provide [Selection: real-time; near real-time]
[Assignment: organization-defined failover capability] for the system.**

AWS ElastiCache Redis cluster with Multi-AZ Automatic Failover feature set to disabled

This policy identifies ElastiCache Redis clusters which have Multi-AZ Automatic Failover feature set to disabled. It is recommended to enable the Multi-AZ Automatic Failover feature for your Redis Cache cluster, which will improve primary node reachability by providing read replica in case of network connectivity loss or loss of availability in the primary's availability zone for read/write operations.
Note: Redis cluster Multi-AZ with automatic failover does not support T1 and T2 cache node types and is only available if the cluster has at least one read replica.

First Seen N/A | **Resource Type** Other

Recommendations

1. Sign into the AWS console
2. In the console, select the specific region from region drop down on the top right corner, for which the alert is generated
3. Navigate to ElastiCache Dashboard
4. Click on Redis
5. Select reported Redis cluster
6. Click on 'Modify' button
7. In the 'Modify Cluster' dialog box,
a. Set 'Multi-AZ' to 'Yes'
b. Select 'Apply Immediately' checkbox, to apply the configuration changes immediately. If Apply Immediately is not selected, the changes will be processed during the next maintenance window.
c. Click on 'Modify'