AWS Security Audit Findings Remediation Runbook

Last updated: 10 September 2020

Version: 1.0



**Document Control**

|  |  |  |  |
| --- | --- | --- | --- |
| Document Title | Version | Author | Summary |
| Security Findings Remediation Setup | 1 | AWS Professional Services | Runbook on launching the AWS CloudFormation template that will set up Access Key auto-rotation. |

Table of Contents

[Summary 4](#_Toc57639712)

[Section 1: Remediation CloudFormation Template 5](#_Toc57639713)

[Section 2: IAM Auto Key Rotation 7](#_Toc57639714)

[Section 2.1: IAM Key Auto-Rotation Architecture 7](#_Toc57639715)

[Section 2.2: Sample Email for Notification of IAM Auto Key Rotation Enforcement 8](#_Toc57639716)

[Section 3: Automated End User Emailing Tool 9](#_Toc57639717)

[Section 3.1: Automated End User Emailing Tool Architecture 9](#_Toc57639718)

[Section 3.2: One-Time Setup Steps for End User Emailing Tool 9](#_Toc57639719)

# Summary

This runbook will walk you through the AWS CloudFormation template setup. This template will create a mechanism to scan daily, and automatically rotate your AWS IAM user Access Keys every 90 days and store the new Access Keys in a secret inside AWS Secrets Manager. An AWS SNS notification will be sent to alert of the rotation. 10 days later, the old Access Keys will be disabled. And 10 days after that, deleted. This gives the user time to implement the new Access Keys in their applications.

This document covers Config Rules for the following Security Audit Findings:

* 'Lack of Key Rotation (Active)'

# Section 1: Remediation CloudFormation Template

This CloudFormation Template will deploy all remediation artifacts discussed in this runbook.

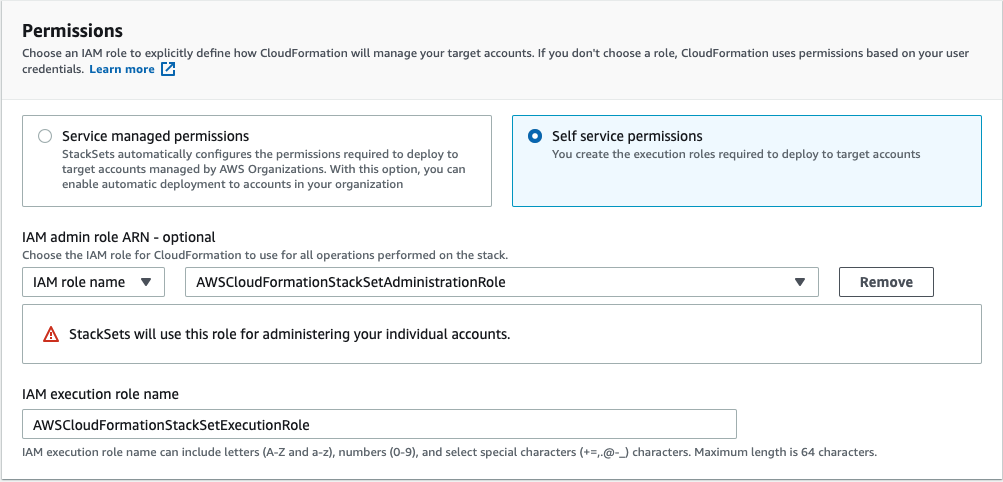
* Upload all files to an S3 bucket of your choosing. Make sure all files are at the root of the bucket.
* Log into the **AWS Management Console**, and select **S3** from the **Services** menu.



* Choose a bucket, and upload the project zip files (Make sure the bucket allows all accounts in your OUs to perform s3:GetObject\*.)
* Still in the console, choose **CloudFormation** from the **Services** menu.



* In the left-hand pane, choose **StackSets**. (If you’ve never created a CloudFormation stack before, choose **Get Started**.)
* Click on **Create StackSet**.
* Choose **Upload a template file**.
* Click on **Choose file** and select the file named **iam-key-auto-rotation-and-notifier-.yml**.
* Click **Next**.
* Give the **StackSet** a name. I used **SecurityFindingsRemediationStackSet**.
* Fill in all parameter fields required.
* Click **Next**.
* For **Permissions**, select **Self services permissions** and select the AWS IAM Role **AWSCloudFormationStackSetAdministrativeRole**. (If you created a different Role for this operation, choose this instead.)



* Click **Next**.
* Select **Deploy stacks in organizational units** and enter all **OUs** in the text field separated by a comma.
* For regions, choose the same region the S3 bucket lives in that you used to upload the zip files..
* Leave all other defaults and click **Next**.
* After reviewing the information, click the checkbox next to **I acknowledge that AWS CloudFormation might create IAM resources**.
* Click **Submit**.

# Section 2: IAM Auto Key Rotation

This section covers a mechanism used to scan daily, and automatically rotate your AWS IAM user Access Keys every 90 days and store the new Access Keys in a secret inside AWS Secrets Manager. An AWS SNS notification will be sent to alert of the rotation. 10 days later, the old Access Keys will be disabled. And 10 days after that, deleted. This gives the user time to implement the new Access Keys in their applications.

## Section 2.1: IAM Key Auto-Rotation Architecture



1. The CloudWatch Event will trigger once every 24 hours the Lambda Function.
2. The Lambda Function will scan every IAM user in the account’s Access Keys, checking for creation date.
3. If there are Access Keys newer than 90 days old, or no Access Keys exist, the function exits.
4. If there are Access Keys that need rotation, it will create a new Access Key pair and either create a new Secret named after the user (in the event it’s the first time for rotation), or update the Secret with the new Access Key pair.
5. It will attach an IAM policy to the user allowing access to the secret (if it’s the first time, if not, it will be ignored).
6. It will attach a resource policy to the secret, allowing only the specific user access (if it’s the first time, if not, it will be ignored).
7. Upon creation of new access keys, the Lambda will trigger the SNS Topic.
8. SNS will then trigger a different Lambda function that will reach out to S3 to pull an email template, and DynamoDB to pull the user’s account email address.
9. Using the information gathered, it will then send a custom email to the user’s email address via SES.

## Section 2.2: Sample Email for Notification of IAM Auto Key Rotation Enforcement

*Below is a draft you can use for your company-wide email to inform end users of the new 90-day AWS IAM user Access Key rotation policy (Risk level: High).*

To all application owners,

Security is the top-most priority of any organization. To ensure continued success in our drive to design and architect a secure infrastructure, we are implementing a 90-day automatic rotation of all AWS IAM User Access Keys. This will begin on DATE HERE.

Why is this important and how does fixing this help you?

Rotating Identity and Access Management (IAM) credentials periodically will significantly reduce the chances that a compromised set of access keys can be used without your knowledge to access certain components within your AWS account.

What this means for you:

You will need to update your applications every 90-days with the new Access Key pair. These can be found in AWS Secrets Manager in a secret accessible by your application’s AWS IAM User only. You will have a grace period of 10 days after rotation before old Access Keys are disabled. There will be another 10-day grace period before old Access Keys are deleted. Until they are disabled, old Access Keys can be used to programmatically retrieve the new Access Keys from AWS Secrets Manager.

Enabling this setting will also help you align with the following compliance standards:

* The Center of Internet Security AWS Foundations Benchmark
* APRA
* MAS
* National Institute of Standards and Technology (NIST)
* AWS Well-Architected Framework

Should you have any questions, please reach out to EMAIL ADDRESS HERE. As always, thank you for continuing to strive for a secure work environment.

Sincerely,

INFO HERE

# Section 3: Automated End User Emailing Tool

This section covers the automated end user emailing tool. After deploying the tool’s AWS resources via the CloudFormation template you will need to preform 2 manual actions:

* Upload the accountemailmapping-commercial.csv or accountemailmapping-govcloud.csv file to the S3 Import-to-DynamoDB Bucket (*note: you will give this a custom name in the CTF*).

## Section 3.1: Automated End User Emailing Tool Architecture



## Section 3.2: One-Time Setup Steps for End User Emailing Tool

1. Move the Amazon Simple Email Service (SES) service out of sandbox mode
   1. <https://docs.aws.amazon.com/ses/latest/DeveloperGuide/request-production-access.html>
   2. *Note: There is about a 24 hour wait for approval*
2. While in Amazon Simple Email Service (SES), verify the senders address or the sender domain that you will use as the email source.
   1. This is the email that will be in the ‘Sender’ section of the email sent to your end users.
3. The AWS resources needed for this tool will deploy with the main CloudFormation template.
4. Once the template is fully deployed, you will need to upload the following CSV files into the new S3 bucket created for importing into DynamoDB. By uploading the file, it will kick off the import script.
   1. **csv-to-s3-account-emails.csv**
5. You can validate import was successful by going to:
   1. <https://console.aws.amazon.com/dynamodb/>
   2. ‘Tables’ on the left side menu
   3. Clicking on the table name ‘aws-account-emails’
   4. Clicking on the ‘Items’ tab
6. Upload email templates
7. To monitor the EmailerTool, you can review the logs in CloudWatch under
   1. **/aws/lambda/Direct-to-End-User-Emailing-Tool**
8. All config rules are setup to send SNS notifications to this Lambda for processing and emailing to end users.