



# AWS IAM Key Rotation Runbook

Last updated: 10 September 2020  
Version: 2.0

**Laura Seletos**, CISSP  
*Senior Security Consultant*  
AWS WWPS Professional Services  
E: [lseleto@amazon.com](mailto:lseleto@amazon.com) | M: +1.727.271.3205



## Table of Contents

<b>Document Control</b>	<b>3</b>
<b>1.0 Introduction</b>	<b>3</b>
<b>2.0 Architecture</b>	<b>4</b>
<b>3.0 Required Files</b>	<b>7</b>
<b>4.0 Deployment</b>	<b>7</b>
4.1 Step 1: Upload Project Files to S3 Bucket	7
4.2 Step 2: Deploy IAM Assumed Roles CloudFormation Template as a StackSet	8
4.3 Step 3: Deploy the main IAM Key Rotation Solution as a CloudFormation Stack	12
<b>5.0 Validating Deployment &amp; Manual Tests</b>	<b>16</b>
5.1 Manually Test: Daily Schedule via ASA-Account-Inventory Lambda Function	16
5.2 Manually Test: ASA-IAM-Access-Key-Rotation-Function Lambda Function	17
5.3 Manually Test: ASA-Notifier Lambda Function	17
<b>6.0 Troubleshooting</b>	<b>18</b>
6.1 ClientError: An error occurred (AccessDenied) when calling the AssumeRole operation	18
6.2 MessageRejected: Email address is not verified.	18



## Document Control

Author	Version	Date	Update Notes
Laura Seletos	1	04/06/2021	Initial document version
Laura Seletos	2	11/04/2021	Updated document for version 2 (new diagrams, troubleshooting, and unit testing). Version 2 was re-architected for scale, centralizing all main resources into a single, centralized account with assumed roles allowing for cross-account access.

## 1.0 Introduction

This document is the runbook on how to deploy, configured, validate, and troubleshoot the Automated AWS IAM Key Rotation solution.

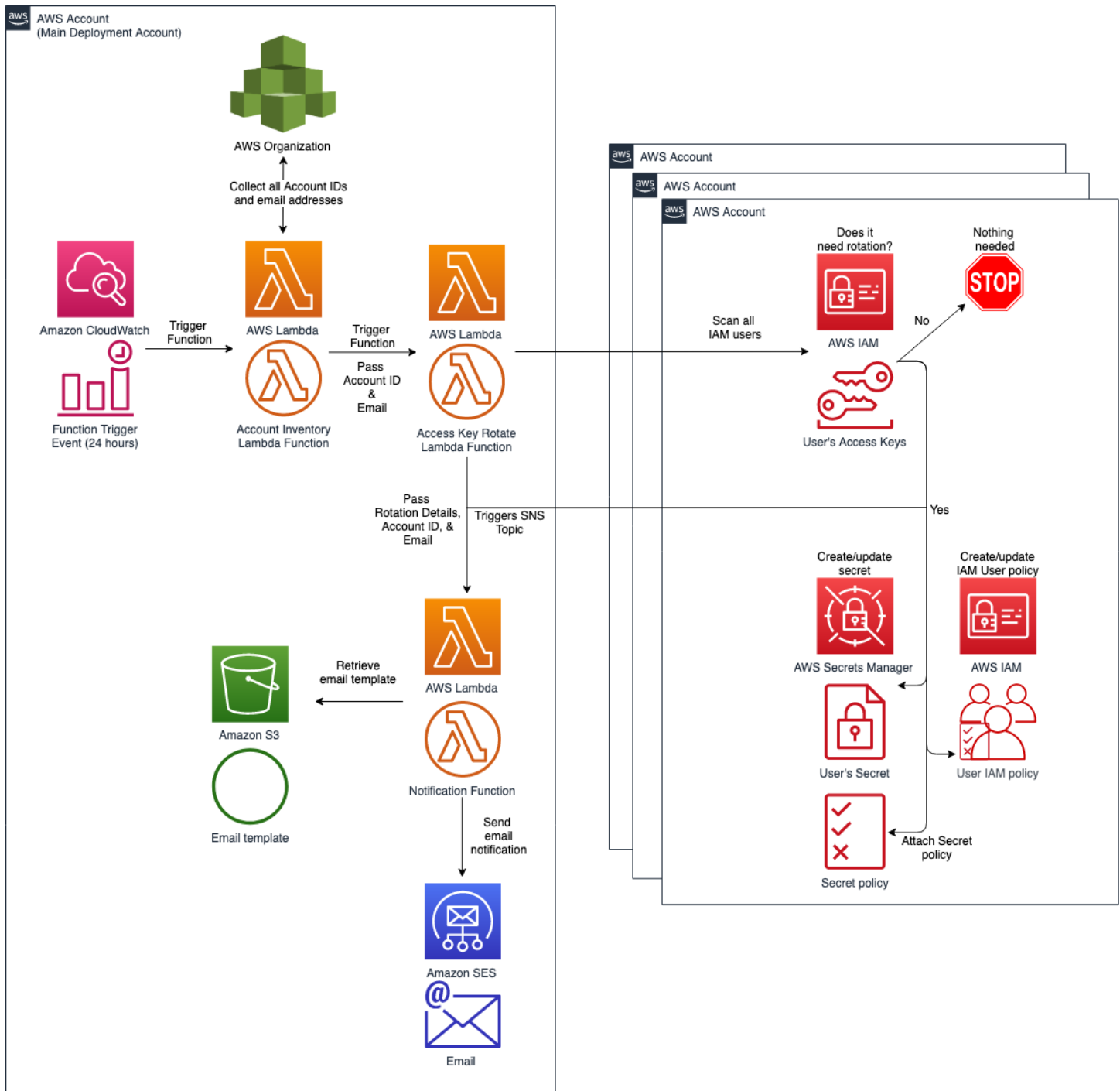
This runbook will walk you through the AWS CloudFormation template setup. This template will create a mechanism to scan daily, and automatically rotate your AWS IAM user Access Keys every 90 days and store the new Access Keys in a secret inside AWS Secrets Manager. An AWS SES notification will be sent 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)'

## 2.0 Architecture

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.





**Note:** The Lambda Function in the 'Main Deployment Account' assumes a local role, in the individual AWS Account(s), that allows it to facilitate localized IAM key rotation actions (i.e. violation detection, rotation, secret creation, etc.).

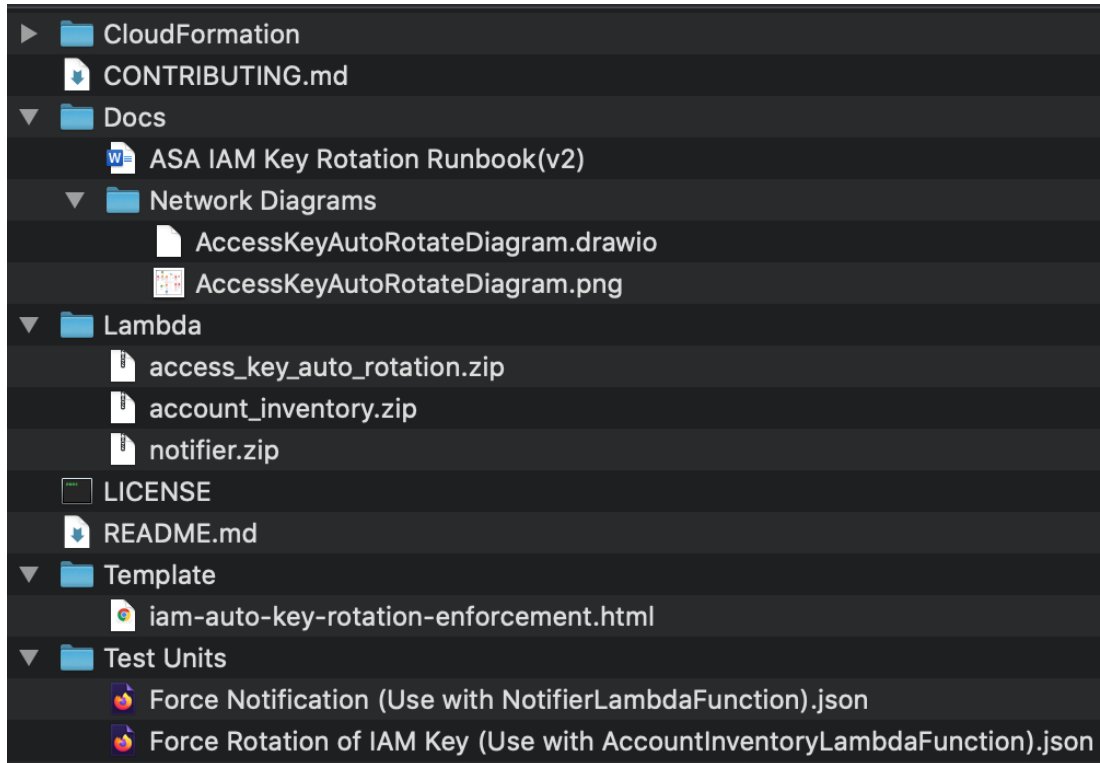
1. Once every 24 hours, the CloudWatch Event will trigger the 'ASA-Account-Inventory' Lambda Function.
2. The 'ASA-Account-Inventory' Lambda Function will list all AWS Account within AWS Organizations, capturing Account ID and Account Email.
3. For each Account ID, the Lambda 'ASA-IAM-Access-Key-Rotation-Function' executes and assumes a role in the target account, scanning every IAM user in the account's Access Keys, checking for creation date.
  - The following are supported key actions:
    - UNUSED\_EXPIRED\_KEY = 'Expired key has never been used.'
    - EXPIRED\_ACTIVE\_KEY = 'Active key has expired.'
    - FORCED\_ROTATION = 'Forced active key rotation.'
    - EXPIRED\_ACTIVE\_KEY\_CONFLICT\_LRU = 'Expired active key with conflict, least recently used.'
    - EXPIRED\_INACTIVE\_KEY\_CONFLICT = 'Expired key with conflict, already inactive.'
    - FORCED\_ROTATION\_CONFLICT\_LRU = 'Forced active key rotation with conflict, least recently used.'
    - FORCED\_INACTIVE\_KEY\_CONFLICT = 'Forced rotation with conflict, already inactive.'
    - INSTALL\_GRACE\_PERIOD\_END = 'Installation grace period has ended.'
    - RECOVER\_GRACE\_PERIOD\_END = 'Recovery grace period has ended.'
    - KEY\_PENDING\_ROTATION = 'Key will be rotated soon.'
    - KEY\_PENDING\_DEACTIVATION = 'Key will be deactivated soon, please install new key.'
    - KEY\_PENDING\_DELETION = 'Key will be permanently deleted soon, please validate new key.'
    - KEY\_PENDING\_EXPIRATION\_CONFLICT = 'Key will expire soon, cannot be rotated due to presence of other key.'
    - KEY\_PENDING\_DELETION\_CONFLICT = 'Key will be permanently deleted soon, due to conflict.'
    - UNUSED\_KEY\_PENDING\_DELETION = 'Key will be permanently deleted soon, key is about to expire and has never been used.'
4. If there are IAM users in the IAM group 'IAMKeyRotationExemptionGroup', those users will not be evaluated.
5. If there are Access Keys, outside of the exemption IAM group, newer than 90 days old, or no Access Keys exist, the function exits.
6. If there are Access Keys, outside of the exemption IAM group, that need rotation, the function 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.
7. It will then attach an IAM policy to the user allowing access to the secret (*if it's the first time, if not, it will be ignored*).
8. 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).
9. Upon any creation, deactivation, deletion actions on an IAM access key, the 'ASA-IAM-Access-Key-Rotation-Function' Lambda will trigger the 'ASA-Notifier' Lambda Function.



10. The 'ASA-Notifier' Lambda Function will reach out to the S3 Bucket to pull the customizable email template and facilitate sending an email, via Amazon Simple Email Service (SES), to the email associate to the AWS Organization's Account ID.

### 3.0 Required Files

Project files included in the zip:



### 4.0 Deployment

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

#### 4.1 Step 1: Upload Project Files to S3 Bucket

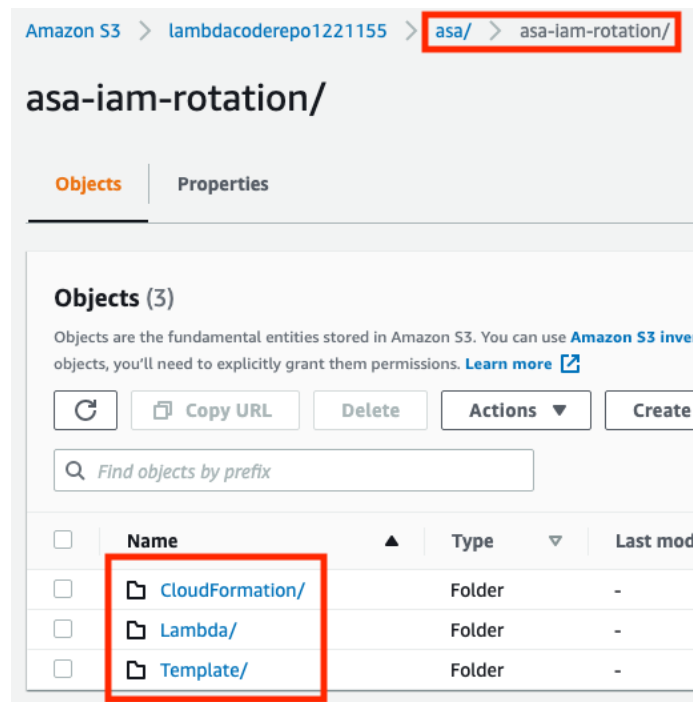
**Step 1:** Unzip the project files.

**Step 2:** Log into the **AWS Management Console**, and select **S3** from the **Services** menu.



**Step 3:** Drag & Drop the ASA folder into your S3 Bucket.

- **IMPORTANT:** Make sure all files are in the 'asa/asa-iam-rotation' folder structure.
- The 3 main folders from you need from the zip file are:
  - 'CloudFormation/', 'Template/', and 'Lambda/' as shown below:



**IMPORTANT NOTE:** Ensure the account where you are deploying CloudFormation Stacks and StackSets from has access to this S3 Bucket.

## 4.2 Step 2: Deploy IAM Assumed Roles CloudFormation Template as a StackSet

**IMPORTANT NOTE:** The 'list\_accounts' API operation can only be called from the organization's management account or by a member account that is a delegated administrator for an AWS service.

Reference:

[https://boto3.amazonaws.com/v1/documentation/api/latest/reference/services/organizations.html#Organizations.Client.list\\_accounts](https://boto3.amazonaws.com/v1/documentation/api/latest/reference/services/organizations.html#Organizations.Client.list_accounts)

**Step 1:** Still in the AWS console, choose **CloudFormation** from the **Services** menu.



**Step 2:** In the left-hand pane, choose **StackSets**. (If you've never created a CloudFormation stack before, choose **Get Started**.)

**Step 3:** Click on **Create StackSet**.





**Step 4:** Copy the Object URL of the “*ASA-iam-key-auto-rotation-iam-assumed-roles.yaml*” template you uploaded to the S3 Bucket.

**Step 2:** Go to CloudFormation service and select StackSets. Paste the copied Object URL into the ‘Template Source’ and click ‘Next’.

**Step 3:** Fill in the StackSet name (ex: ‘IAM-Auto-Key-Rotation-Assumed-Roles’).

- You can leave ‘*Assumed IAM Role Name*’ and ‘*IAM Execution Role Name*’ and ‘*IAMKeyRotationExemptionGroup*’ as default or you can customize them.



- You will need to enter the 'Primary AWS Account ID' and 'AWS Organization ID'.
  - This Account ID is where you will be deploying the ASA-iam-key-auto-rotation-and-notifier-solution.yaml CloudFormation template to.
  - The Organization ID is to help further lock down the deployed IAM assumed roles.
- Click the 'Next' button.

**Parameters (4)**  
Parameters are defined in your template and allow you to input custom values when you create or update a stack.

**ASA IAM Role Configurations**

**Assumed IAM Role Name**  
Enter the name of IAM Role that the main ASA-iam-key-auto-rotation-and-notifier-solution.yaml CloudFormation template will assume.

asa-iam-key-rotation-lambda-assumed-role

**IAM Execution Role Name**  
Enter the name of IAM Execution Role that will assume the sub-account role for Lambda Execution.

asa-iam-key-rotation-lambda-execution-role

**Primary AWS Account ID**  
Enter the primary AWS Account ID that will you will be deploying the ASA-iam-key-auto-rotation-and-notifier-solution.yaml CloudFormation template to.

066429\*\*\*\*\*

**IAM Exemption Group**  
Manage IAM Key Rotation exemptions via an IAM Group. Enter the IAM Group name being used to facilitate IAM accounts excluded from auto-key rotation.

IAMKeyRotationExemptionGroup

○

**Step 4:** Select 'Service-managed permissions', and then 'Next'. Under 'Set deployment options', you can select either 'Deploy to organization' or 'Deploy to organizational units (OUs)'.

- You may leave 'Automatic deployment' and 'Account removal behavior' as defaults. Under 'Specify regions' select a region (*since IAM is a global service, the stack will be deployed within 1 region but the IAM role will be global for that account*). You can also leave 'Deployment options' default.

**Permissions**  
Choose an IAM role to explicitly define how CloudFormation will manage your target accounts. If you don't choose a role, CloudFormation uses permissions based on your user credentials. [Learn more](#)

☐ Service managed permissions  
StackSets automatically configures the permissions required to deploy to target accounts managed by AWS Organizations. With this option, you can enable automatic deployment to accounts in your organization

☒ Self service permissions  
You create the execution roles required to deploy to target accounts

**IAM admin role ARN - optional**  
Choose the IAM role for CloudFormation to use for all operations performed on the stack.

IAM role name: AWSCloudFormationStackSetAdministrationRole Remove

⚠ StackSets will use this role for administering your individual accounts.

**IAM execution role name**

AWSCloudFormationStackSetExecutionRole

IAM execution role name can include letters (A-Z and a-z), numbers (0-9), and select special characters (+, =, @, -, \_) characters. Maximum length is 64 characters.

•




**IMPORTANT NOTE:** If you selected more than 1 region per account you will get an error message similar to:

ResourceLogicalId:ASAIAMAssumedRole, ResourceType:AWS::IAM::Role, ResourceStatusReason:asa-iam-key-rotation-lambda-assumed-role already exists.

This is due to IAM being a global service, once it's deployed in 1 region it will be there for all regions.

**Step 5:** On the final screen, make sure to check off the 'I acknowledge that AWS CloudFormation might create IAM resources with custom names' Option under 'Capabilities'. Then click 'Submit'.

### Capabilities

**The following resource(s) require capabilities: [AWS::IAM::Role]**

This template contains Identity and Access Management (IAM) resources. Check that you want to create each of these resources and that they have the minimum required permissions. In addition, they have custom names. Check that the custom names are unique within your AWS account. [Learn more](#)

☒ I acknowledge that AWS CloudFormation might create IAM resources with custom names.

**Step 6:** After launching the StackSet, you will have to wait for it to deploy the IAM role to all sub-accounts. You can track progress via the 'Stack instances' tab.





CloudFormation > StackSets > ASA-IAM-Assumed-Roles: StackSet details

Actions

StackSet infoStack instancesOperationsParametersTemplate

Stack instances (2)  
For details of a stack instance, log into the stack instance's account, navigate to the appropriate region, and then select the desired stack by name.

Search

AWS account	AWS region	Stack ID	Status	Status Reason	Drift status	Last drift check time
048795182642	us-west-2	arn:aws:cloudformation:us-west-2:048795182642:stack/StackSet-ASA-IAM-Assumed-Roles-93a38caa-e21f-46b3-9211-4b3a6e0d6999/aa60b350-973f-11eb-8a78-0653a4b84513	 CURRENT	-	 NOT_CHECKED	-
662608458177	us-west-2	arn:aws:cloudformation:us-west-2:662608458177:stack/StackSet-ASA-IAM-Assumed-Roles-6d208dba-8f62-4044-9a91-26fbd151fb6b/bbc16680-973f-11eb-b68c-0a14a5ae98bb	 CURRENT	-	 NOT_CHECKED	-



### 4.3 Step 3: Deploy the main IAM Key Rotation Solution as a CloudFormation Stack

**Step 1:** Copy the Object URL of the “*ASA-iam-key-auto-rotation-and-notifier-solution.yaml*” template you uploaded to the S3 Bucket.

Amazon S3 > lambdacoderepo1221155 > asa/ > asa-iam-rotation/ > CloudFormation/ > ASA-iam-key-auto-rotation-and-notifier-solution.yaml

ASA-iam-key-auto-rotation-and-notifier-solution.yaml

Copy S3 URI Object actions

Properties Permissions Versions

**Object overview**

Owner  
lselecto

AWS Region  
US West (Oregon) us-west-2

Last modified  
April 6, 2021, 21:00:48 (UTC-04:00)

Size  
11.9 KB

Type  
yaml

Key  
asa/asa-iam-rotation/CloudFormation/ASA-iam-key-auto-rotation-and-notifier-solution.yaml

S3 URI  
s3://lambdacoderepo1221155/asa/asa-iam-rotation/CloudFormation/ASA-iam-key-auto-rotation-and-notifier-solution.yaml

Amazon Resource Name (ARN)  
arn:aws:s3::lambdacoderepo1221155/asa/asa-iam-rotation/CloudFormation/ASA-iam-key-auto-rotation-and-notifier-solution.yaml

Entity tag (Etag)  
1a6901ed2644bdbc4dea0ca7abb90ac5

Object URL Copied

https://lambdacoderepo1221155.s3-us-west-2.amazonaws.com/asa/asa-iam-rotation/CloudFormation/ASA-iam-key-auto-rotation-and-notifier-solution.yaml

**Step 2:** Go to CloudFormation service and select Stacks. Paste the copied Object URL into the ‘Template Source’ and click ‘Next’.

*Note: Make sure the Account ID you are deploying this stack from matches the ‘Primary AWS Account ID’ from ‘4.2 Deploy IAM Assumed Roles CloudFormation Template as a StackSet’.*

CloudFormation > Stacks > Create stack

Step 1  
Specify template

Step 2  
Specify stack details

Step 3  
Configure stack options

Step 4  
Review

**Create stack**

**Prerequisite - Prepare template**

Prepare template  
Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

☒ Template is ready ☐ Use a sample template ☐ Create template in Designer

**Specify template**  
A template is a JSON or YAML file that describes your stack's resources and properties.

Template source  
Selecting a template generates an Amazon S3 URL where it will be stored.

☒ Amazon S3 URL ☐ Upload a template file

Amazon S3 URL  
https://lambdacoderepo1221155.s3-us-west-2.amazonaws.com/asa/asa-iam-rotation/CloudFormation/ASA-iam-key-auto-rotation-and-notifier-solution.yaml

Amazon S3 template URL

S3 URL: https://lambdacoderepo1221155.s3-us-west-2.amazonaws.com/asa/asa-iam-rotation/CloudFormation/ASA-iam-key-auto-rotation-and-notifier-solution.yaml

View in Designer

Cancel Next



### Step 3: Specify stack details

- Fill in the Stack name (ex: 'IAM-Auto-Key-Rotation-Solution').

**Specify stack details**

**Stack name**

Stack name

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

- Enter the S3 Bucket name you uploaded all your files to in step '4.1 Upload Project Files to S3 Bucket' into 'CloudFormation S3 Bucket Name'.
- 'CloudFormation S3 Bucket Prefix' should match the folder structure of what you uploaded in the S3 Bucket (ex: 'asa/asa-iam-rotation').
- You can leave 'Assumed IAM Role Name' and 'IAM Execution Role Name' as default or you can customize them.
- The 'Dry Run Flag' will allow you to simulate the AWS IAM Rotation Solution without actually rotating end user's keys. This is a great way to notify users or test the solution.
  - *Note: You can easily toggle between 'True' or 'False' values by updating the already deployed CloudFormation stack.*

**Parameters**

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

**Deployment Configurations**

**CloudFormation S3 Bucket Name**  
S3 Bucket Name where code is located.

**CloudFormation S3 Bucket Prefix**  
The prefix or directory where resources will be stored.

**Assumed IAM Role Name**  
Enter the name of IAM Role that the main ASA-iam-key-auto-rotation-and-notifier-solution.yaml CloudFormation template will assume.

**IAM Execution Role Name**  
Enter the name of IAM Execution Role that will assume the sub-account role for Lambda Execution.

**Dry Run Flag (Audit Mode)**  
Enables/Disables key rotation functionality. 'True' only sends notifications to end users (Audit Mode). 'False' preforms key rotation and sends notifications to end users (Remediation Mode).

- Enter your team email distro under 'Admin Email Address'.
  - *Note: This will be used in the 'sent from' section of email notifications to end users.*
- Enter your 'AWS Organization ID'.
- You can leave the fields for 'Email Template File Names' default or customize them.



**Configure ASA Notifier Module**

**Admin Email Address**  
Email address that will be used in the 'sent from' section of the email.

\*\*\*\*\*@amazon.com

**AWS Organization ID**  
Enter your AWS Organization ID, this will be used to restricted execution permissions to only approved AWS Accounts within your AWS Organization.

O-\*\*\*\*\*

**Email Template File Name [Audit Mode]**  
Enter the file name of the email html template to be sent out by the Notifier Module for Audit Mode. Note: Must be located in the 'S3 Bucket Prefix/Template/template\_name.html' folder

iam-auto-key-rotation-enforcement.html

**Email Template File Name [Enforce Mode]**  
Enter the file name of the email html template to be sent out by the Notifier Module for Enforce Mode. Note: Must be located in the 'S3 Bucket Prefix/Template/template\_name.html' folder

iam-auto-key-rotation-enforcement.html

- You can leave 'IAMKeyRotationExemptionGroup' as default or you can customize it.
- You can leave the 'Configure ASA IAM Key Rotation Parameters' section as default or you can customize it.
- Once the stack details are filled out, click the 'Next' button.

**Configure ASA IAM Key Rotation Exemption Group**

**IAM Exemption Group**  
Manage IAM Key Rotation exemptions via an IAM Group. Enter the IAM Group name being used to facilitate IAM accounts excluded from auto-key rotation.

IAMKeyRotationExemptionGroup

**Configure ASA IAM Key Rotation Parameters**

**Rotation Period**  
The number of days after which a key should be rotated (rotating from active to inactive).

90

**Inactive Buffer**  
The grace period between rotation and deactivation of a key.

10

**Inactive Period**  
The number of days after which to inactivate keys that had been rotated (Note: This must be greater than RotationPeriod).

100

**Recovery Grace Period**  
Recovery grace period between deactivation and deletion.

10

Cancel Previous **Next**

**Step 4:** For Permissions, select 'Service-managed permissions', and then 'Next'. Under 'Set deployment options', you can select either 'Deploy to organization' or 'Deploy to organizational units (OUs)'.

- You may leave 'Automatic deployment' and 'Account removal behavior' as defaults. Under 'Specify regions' select a region (*since IAM is a global service, the stack will be deployed within 1 region but the IAM role will be global for that account*). You can also leave 'Deployment options' default.



**Permissions**  
Choose an IAM role to explicitly define how CloudFormation will manage your target accounts. If you don't choose a role, CloudFormation uses permissions based on your user credentials. [Learn more](#)

☐ Service managed permissions  
StackSets automatically configures the permissions required to deploy to target accounts managed by AWS Organizations. With this option, you can enable automatic deployment to accounts in your organization

☒ Self service permissions  
You create the execution roles required to deploy to target accounts

**IAM admin role ARN - optional**  
Choose the IAM role for CloudFormation to use for all operations performed on the stack.

IAM role name

StackSets will use this role for administering your individual accounts.

**IAM execution role name**

IAM execution role name can include letters (A-Z and a-z), numbers (0-9), and select special characters (+, =, @, -, \_) characters. Maximum length is 64 characters.

**Step 5:** On the final screen, make sure to check off the 'I acknowledge that AWS CloudFormation might create IAM resources with custom names' Option under 'Capabilities'. Then click 'Submit'.

**Capabilities**

**The following resource(s) require capabilities: [AWS::IAM::Role]**

This template contains Identity and Access Management (IAM) resources. Check that you want to create each of these resources and that they have the minimum required permissions. In addition, they have custom names. Check that the custom names are unique within your AWS account. [Learn more](#)

☒ I acknowledge that AWS CloudFormation might create IAM resources with custom names.

**Step 6:** After launching the Stack, you will have to wait for it to deploy all of the resources. You can track progress via the 'Events' tab.

**ASA-IAM-Key-Rotation-And-Notifier-Template**

**Events (41)**

Timestamp	Logical ID	Status
2021-04-06 21:40:40 UTC-0400	ASA-IAM-Key-Rotation-And-Notifier-Template	CREATE_COMPLETE

**Step 7:** Ensure the sender email is either verified within Amazon Simple Email Service (SES) or your account is removed from sandbox.

- See Section "5.4.2 MessageRejected: Email address is not verified." for tutorials on how to correctly enable these configurations.



## 5.0 Validating Deployment & Manual Tests

### 5.1 Manually Test: Daily Schedule via ASA-Account-Inventory Lambda Function

You can either wait for the daily CloudWatch cron job or access the 'ASA-Account-Inventory' Lambda Function directly.

If you want to kick it off manually, just create a default 'HelloWorld' test event (*content doesn't matter since it is cron job triggered*).

Event name

HelloWorld

```
1 {
2   "key1": "value1",
3   "key2": "value2",
4   "key3": "value3"
5 }
```

Then click 'Test', you should see Invoked outputs where the 'ASA-Account-Inventory' Function invokes the 'ASA-IAM-Access-Key-Rotation-Function' Lambda.

account\_inventor × Execution result: × +

▼ Execution results Status: **Succeeded** Max memory used: 77 MB Time: 1171.84 ms

**Response**  
null

**Function Logs**  
START RequestId: 1400ae20-dcd4-4a62-87f9-ff34affb6984 Version: \$LATEST  
Invoked: FunctionName=ASA-IAM-Access-Key-Rotation-Function, InvocationType=Event, Payload=b'{"account": "662608458177", "email": "lseleto+GuardDutyLabAcc  
Invoked: FunctionName=ASA-IAM-Access-Key-Rotation-Function, InvocationType=Event, Payload=b'{"account": "048795182642", "email": "lseleto+LabAccount@amaz  
Invoked: FunctionName=ASA-IAM-Access-Key-Rotation-Function, InvocationType=Event, Payload=b'{"account": "066429395532", "email": "lseleto@amazon.com"}'  
END RequestId: 1400ae20-dcd4-4a62-87f9-ff34affb6984  
REPORT RequestId: 1400ae20-dcd4-4a62-87f9-ff34affb6984 Duration: 1171.84 ms Billed Duration: 1172 ms Memory Size: 128 MB Max Memory Used: 77 MB I

**Request ID**  
1400ae20-dcd4-4a62-87f9-ff34affb6984

This can also be monitored via CloudWatch log groups.

**Log groups (60)**  
By default, we only load up to 10000 log groups.

Q ASA-IAM-Access-Key-Rotation-Function

☐ Log group

☐ [/aws/lambda/ASA-IAM-Access-Key-Rotation-Function](#)





## 5.2 Manually Test: ASA-IAM-Access-Key-Rotation-Function Lambda Function

*Note: This section's code can be found under the 'Test Units' folder included with the solution.*

Example json event message getting sent to the 'ASA-IAM-Access-Key-Rotation-Function' Lambda Function from the 'ASA-Account-Inventory' Lambda Function.

```
{
  "account": "<AccountID>",
  "email": "<AccountEmailHere>"
}
```

To Force a key rotation, include 'ForceRotate' in the json body:

```
{
  "ForceRotate": "Place Username Here"
  "account": "<AccountID>",
  "email": "<AccountEmailHere>"
}
```

## 5.3 Manually Test: ASA-Notifier Lambda Function

*Note: This section's code can be found under the 'Test Units' folder included with the solution.*

Example json event message getting sent to the 'ASA-Notifier' Lambda Function from the 'ASA-IAM-Access-Key-Rotation-Function' Lambda Function.

```
{
  "email": "PLACE EMAIL HERE",
  "invokedby": "arn:PARTITION:lambda:REGION:ACCOUNT:function:ASA-IAM-Access-Key-Rotation-Function",
  "subject": "[IMPORTANT] Active AWS IAM Access Key was Rotated to Inactive due to Key Age Security Violation.",
  "email_template": "iam-auto-key-rotation-enforcement.html",
  "template_values": {
    "account_id": "PLACE ACCOUNT ID HERE",
    "timestamp": "2021-11-04T22:48:39.640450+00:00",
    "actions": ["ACTION: ROTATE key username-here: key-arn-here. Forced active key rotation."],
    "rotation_period": 90,
    "installation_grace_period": 7,
    "recovery_grace_period": 10,
    "partition_name": "AWS Standard"
  }
}
```



## 6.0 Troubleshooting

### 6.1 ClientError: An error occurred (AccessDenied) when calling the AssumeRole operation

- If you see this error message in Lambda or CloudWatch logs, it means that the Assumed Role StackSet was not successfully deployed to that account.
- Review the account in question and redeploy the CloudFormation Template described in '4.2 Deploy IAM Assumed Roles CloudFormation Template as a StackSet' to it.
- If deployed via organizations, the root org account will not be included.

Full Error Message:

[ERROR] ClientError: An error occurred (AccessDenied) when calling the AssumeRole operation:

User: arn:aws:sts::066429\*\*\*\*\*:assumed-role/ASA-IAM-Key-Rotation-And-RotationLambdaFunction/ASA-IAM-Access-Key-Rotation-Function is not authorized to perform: sts:AssumeRole on resource: arn:aws:iam::06642\*\*\*\*\*:role/asa-iam-key-rotation-lambda-assumed-role

### 6.2 MessageRejected: Email address is not verified.

- If you see this error message in Lambda or CloudWatch logs, it means the Amazon Simple Email Service (SES) is in sandbox mode and the sender email is not verified.
- To verify an SES sender identity follow this tutorial:
  - <https://docs.aws.amazon.com/ses/latest/dg/creating-identities.html>

Amazon SES > Configuration: Verified identities > Create identity

### Create identity

A *verified identity* is a domain, subdomain, or email address you use to send email through Amazon SES. Identity verification at the domain level extends to all email addresses under one verified domain identity.

**Identity details** Info

**Identity type**

☐ Domain  
To verify ownership of a domain, you must have access to its DNS settings to add the necessary records.

☒ Email address  
To verify ownership of an email address, you must have access to its inbox to open the verification email.

Email address

\*\*\*\*@amazon.com

Email address can contain up to 320 characters, including plus signs (+), equals signs (=) and underscores (\_).

☐ Assign a default configuration set  
Enabling this option ensures that the assigned configuration set is applied to messages sent from this identity by default whenever a configuration set isn't specified at the time of sending.

**Tags - optional** Info

You can add one or more tags to help manage and organize your resources, including identities.

No tags associated with the resource.

Add new tag

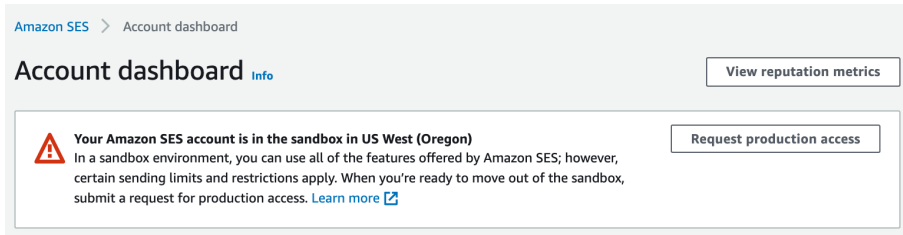
You can add 50 more tags.

Cancel Create identity

- To remove SES from sandbox mode, follow this tutorial:



- <https://docs.aws.amazon.com/ses/latest/DeveloperGuide/request-production-access.html>



- 

## Full Error Message:

"errorMessage": "An error occurred (MessageRejected) when calling the SendEmail operation: Email address is not verified. The following identities failed the check in region US-WEST-2: \*\*\*\*\*@\*\*\*\*\*.com"