Rotate IAM access keys using AWS Config and Lambda

Index

Overview:

This document explains how to enforce AWS IAM user access keys rotation periodically and mitigate risks associated with it. You can deploy this solution easily using AWS config and AWS Lambda.

IAM user access keys are used by applications or tools for accessing different AWS services. They can be used by individual users as well in dealing with day to day activities using AWS CLI.

They can stay Active indefinitely in AWS, without any notice. If these keys are compromised, it can risk the applications and tools using it creating critical business impact.

Because of such nature, access keys should be rotated as often as passwords. This document covers a simple but effective way of monitoring and enforcing key rotations periodically (Every 45 or 90 days).

IAM access keys rotation is a critical part of application management process in any enterprise. So, there are certain steps that need to follow for successfully rotating access keys. Also, a key point to note is that the whole process of key rotation should be seamless i.e the new keys generated should be updated and before revoke/deleting the older keys and this should not affect the operation of application.

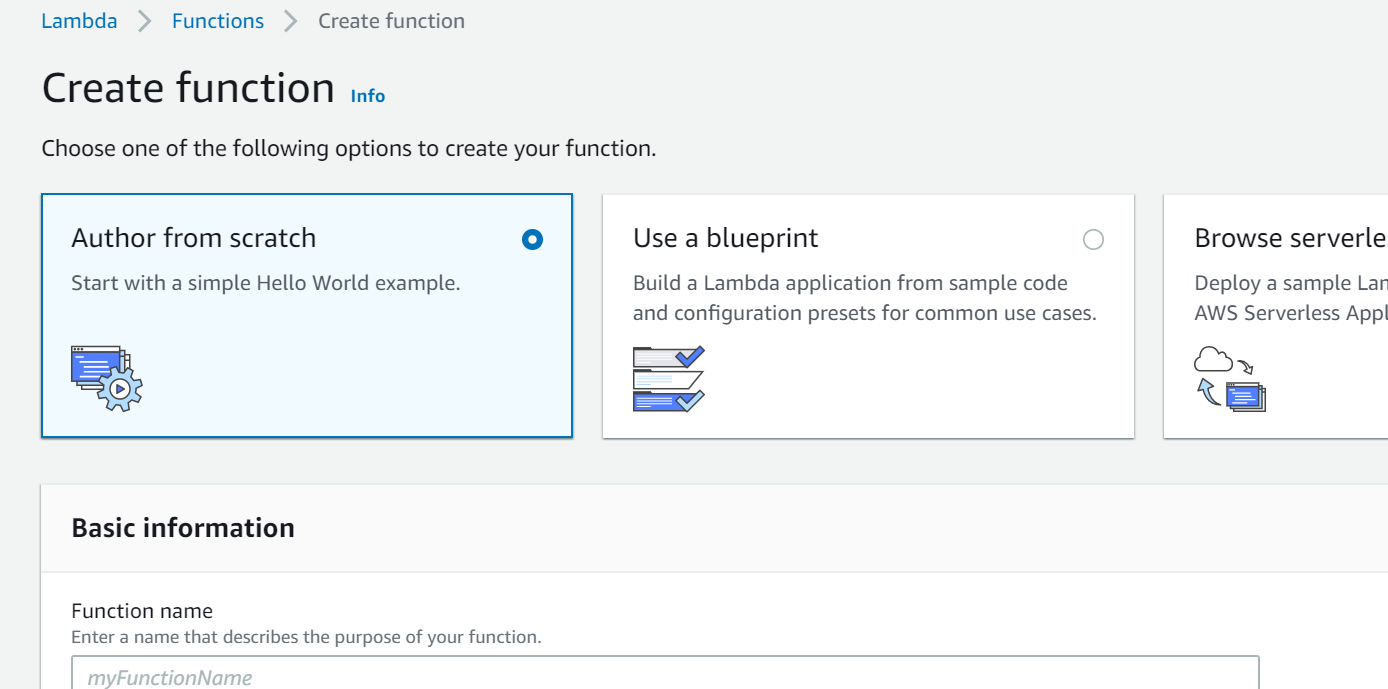
So, lets walk you through the steps that are needed to rotate the IAM keys.

The logic for key rotation follows as mentioned:

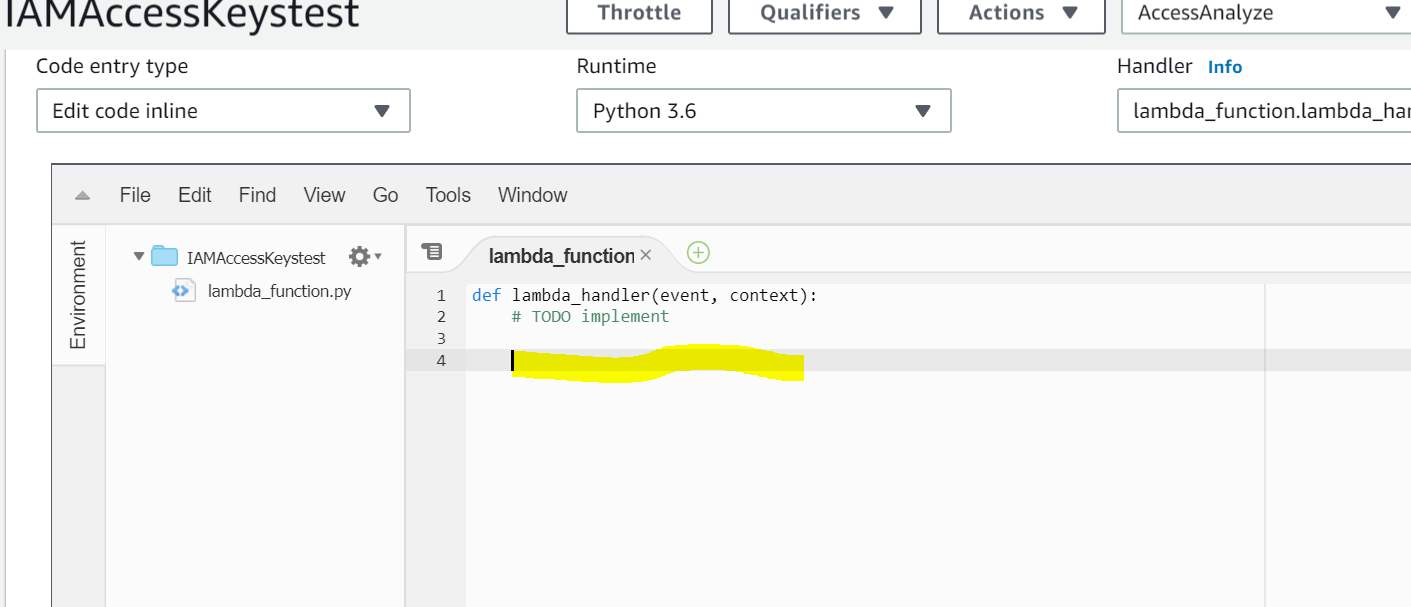
1. Monitor all the IAM users for their Access key age.
2. Inform respective owners of IAM users about the age of their User access keys. For eg. Check for IAM users who have access key age more than 90 days and notify their respective owners.
3. Create 2nd set of access keys for such users (new).
4. After 90 days, notify users that the older version of keys would be disabled (Inactive).
5. Make the older version of the keys Inactive.
6. Provide grace period, say of 5-10 days for owners to make the required changes in their application before the deleting the older version of access keys.

Technical details:

1. Lambda function to detect those users, who have crossed 90 days and send notifications to such users. (Use the access key age to check for the period of Access keys.)
2. After 90 days, Lambda to make all the first access key Inactive (note: not to delete)
3. Wait till grace period of 5-10 more days.
4. Create Lambda function. Click ‘Create function’
5. Select ‘Author from scratch’ and fill the Basic info and runtime (select python 3.6).



1. Set correct permissions for your Lambda.
2. Create cloudwatch rule event (Scheduled) and attach this Lambda to it.
3. Go to Lambda function, copy paste the reference code provided under the main lambda handler function.(as marked). Reference code on git hub (<https://github.com/sadanandn84/AWS>)



1. Then click ‘Save’ to save the code. Optionally, you can test the function and check the logs for invocation or other exception errors.