Sumologic disable inactive users

This document describe how to run Python script to disable inactive users in Sumo Logic who did not logged in for 90 days.
Script uses Sumo Logic API and is runing as AWS Lambda function. Results are logged to CloudWatch and sent to SumoLogic.

Step-by-step guide

AWS Lambda.

1. Login to AWS console and go to AWS Lambda
2. Create function
3. Author from Scratch
4. Give Name i.e. 'Sumo-UserAudit'
5. Pick runtime - Python 3.7
6. Role - Choose an existing role, and then 'service-role/lambda-kms'.
   Note: If you do not have role check AWS - Lambda secure variables with KMS
7. Click 'Create Function'.
8. In Function code, section Code entry type, select Upload a .zip file
9. Upload Sumo-UserAudit.zip
10. Save your function, this will make code visible in Lambda function.
11. Add Environment variables:
    lnkapi - SumoLogic API endpoint
    usrapi - SumoLogic API username
    pasapi - SumoLogic API password
12. Encrypt usrapi and pasapi with KMS
13. Encryoption configuration
14. Enable helpers for encryption in transit, tick on. From drop down menu select your KSM instance name, i.e. security/lambda (see picture 1)
15. AWS KMS key to encrypt at rest , check 'Use a customer master key', from drop down menu select your KMS instance name, i.e. security/lambda
16. Click Encrypt next to key values, you want to encrypt.
17. In Basic Settings section add Description and Timeout 10s.
18. Save function.

AWS Lambda test

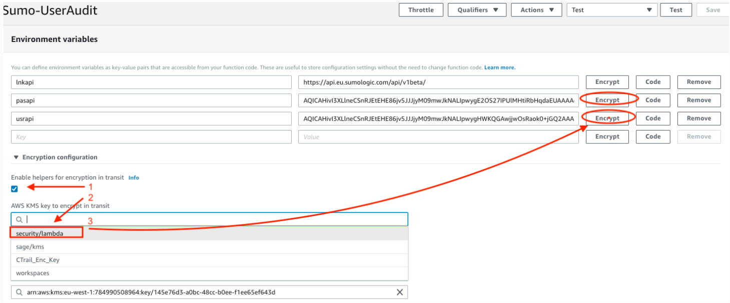
1. Configure test event, click Test and the top of page. New popup window appears.
2. Use default Event Template 'Hello World'
3. Event name - Test
4. Remove content between {} in the body, click Create.
5. Press 'Test' to test your Lambda

Send CloudWatch Logs to SumoLogic

1. Create in SumoLogic hosted HTTP listener to collect CloudWatch logs. Check
2. In AWS CloudWatch, go to Logs
3. Select your CloudWatch Log Group i.e. /aws/lambda/Sumo-UserAudit
4. Go to 'Actions' and select 'Stream to AWS Lambda'
5. Select Lambda Function - 'log-to-sumologic'.
   Note: If you do not have 'log-to-sumologic' function check HERE, how to send CloudWatch logs to Sumo.
6. Click 'Next'
7. Log Format - JSON
8. Click 'Next' and 'Start Streaming'. Now every time Lambda is running log output will be sent to sumologic.

Lambda Python script code

Picture 1. Encrypting envrionment variables with KMS.



Environment variables

You can define environment variables as key-value pairs that are accessible from your function code. These are useful to store configuration settings without the need to change function code. Learn more.

lnkapi	https://api.eu.sumologic.com/api/v1beta/	Encrypt	Code	Remove
pasapi	AQICAHivI3XLlneCSnRJEtEHE86jv5JJJjyM09mwJkNALIpwygE2OS27IPUlMHtiRbHqdaEUAAAA	Encrypt	Code	Remove
usrapi	AQICAHivI3XLlneCSnRJEtEHE86jv5JJJjyM09mwJkNALIpwygHWKQGAwjjwOsRaok0+jGQ2AAA	Encrypt	Code	Remove
Key	Value	Encrypt	Code	Remove

▼ Encryption configuration

Enable helpers for encryption in transit Info

☑

AWS KMS key to encrypt in transit

- security/lambda
- sage/kms
- CTrail_Enc_Key
- workspaces

arn:aws:kms:eu-west-1:784990508964:key/145e76d3-a0bc-48cc-b0ee-f1ee65ef643d

Related articles

- Sumologic disable inactive users
- CloudWatch Logs to SumoLogic
- Sumologic OKTA integration