GCC 2.0 Tech Talks

- AWS GA is coming on **4th May 2022**.
- If and when we talk about Native Services, we will probably cite **AWS only** as these are gearing towards AWS GA preparation.
- Information on Azure will be shared in coming months (to recap, Azure GA will be by Q3 2022).
- All slides will be shared and most of the documentation will also be translated to either Developers Portal (accessible by everyone) or Docs Portal (only accessible by for TechPass account holders).
- All the slides can be shared with existing contractors who are required to manage Projects on GCC as deemed fit by Agencies.
- The series of “Brown Bag” lunch time tech talk is arranged so as to ensure more people can join us in view that some will clash with your meetings. Please feel free to have your lunch while you join us.

For Your Info

- You will be put on mute by default.
- Video should be turned off.

Q&A Segment

- Type in message box when you want to ask a question.
- Wait to be acknowledged by the presenter before speaking.
- Unmute your microphone and state your name and agency clearly.

Session Recording

- Please note that the series of GCC 2.0 Tech Talks will be recorded.
- The video recordings will be made available (in SharePoint).

Let Us Know Your Feedback!

https://form.gov.sg/625cbc09ef648600142ba463

- Let us know what went well and how we can improve.
- We want to ensure that we are bringing the right contents to you so as to help Agencies.
- If you have any questions, please reach out to us at Ask_CODEX@tech.gov.sg

Continuous Log Export and Retention in GCC 2.0

Chris Cheng
GDS / ENP – CLM Squad

Date : 21st April 2022

TABLE OF CONTENTS

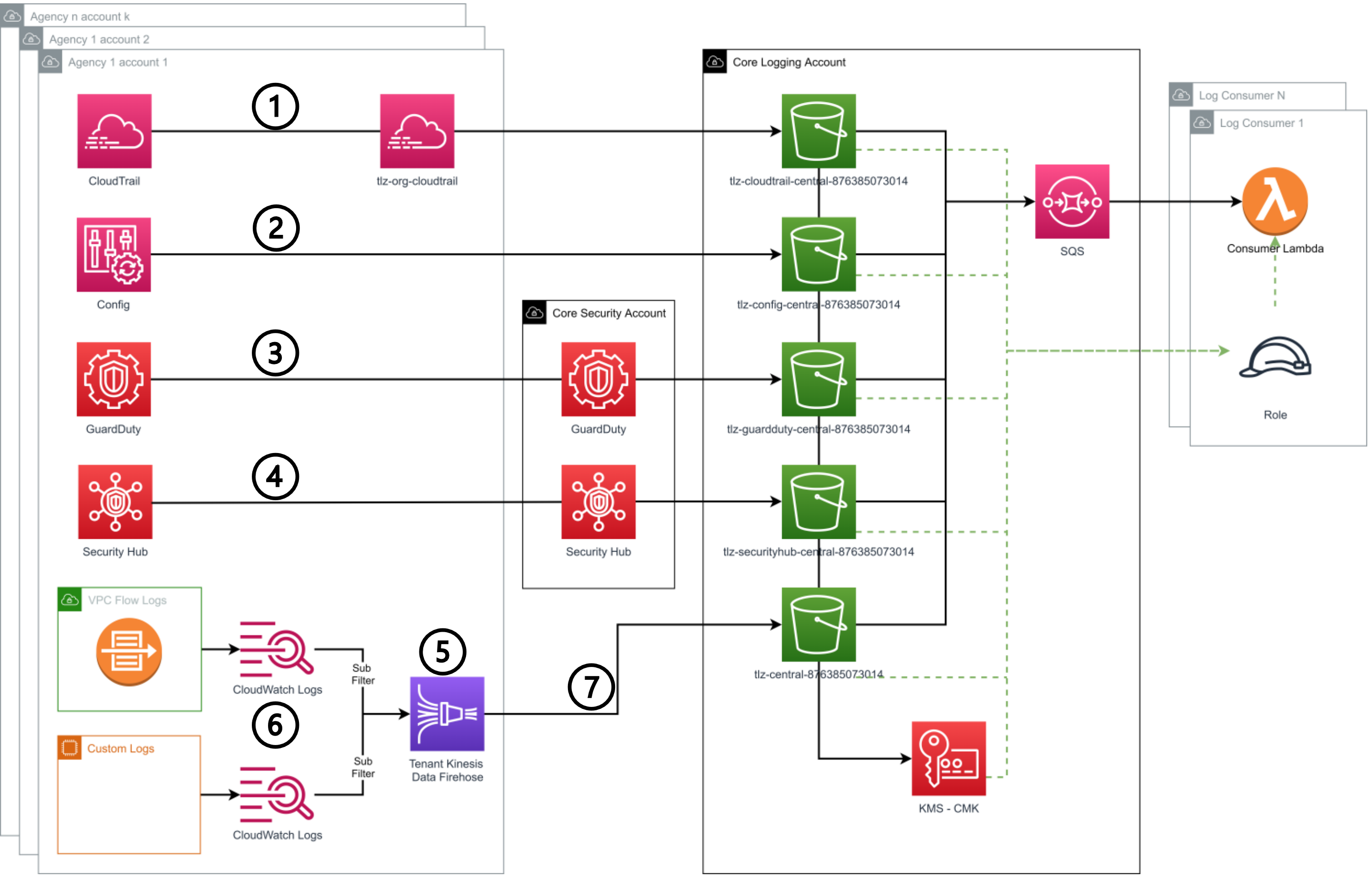
1. The Need for Continuous Logging and Retention
2. Key Changes in GCC 2.0 on Continuous Logging and Retention in AWS
3. Agency's Responsibilities
4. Agency accessing Logs in Centralized S3 Bucket
5. Benefits of GCC 2.0 Continuous Logging
6. Cost of GCC 2.0 Continuous Logging to Tenants
7. Q&A

Need for Continuous Logging and Retention

- IM8 (**INFRASTRUCTURE SECURITY** 7.2/S1 [C1] , 7.2/S6 [## C2]) mandates that all security-related events generated by their systems must be kept for at least 12 months to aid investigation parties.

- Logs older than one year will be automatically purged by the CSP’s storage lifecycle management.

Key Changes in GCC 2.0 on Continuous Logging and Retention in AWS



1. CloudTrail Logs are being managed by Organizational CloudTrail and piped to Central Log S3 bucket.

2. AWS Config is being configured to direct export log to Central Log S3 bucket.

3. GuardDuty (GD) is being managed by central GD and configured to direct export log to Central Log S3 bucket.

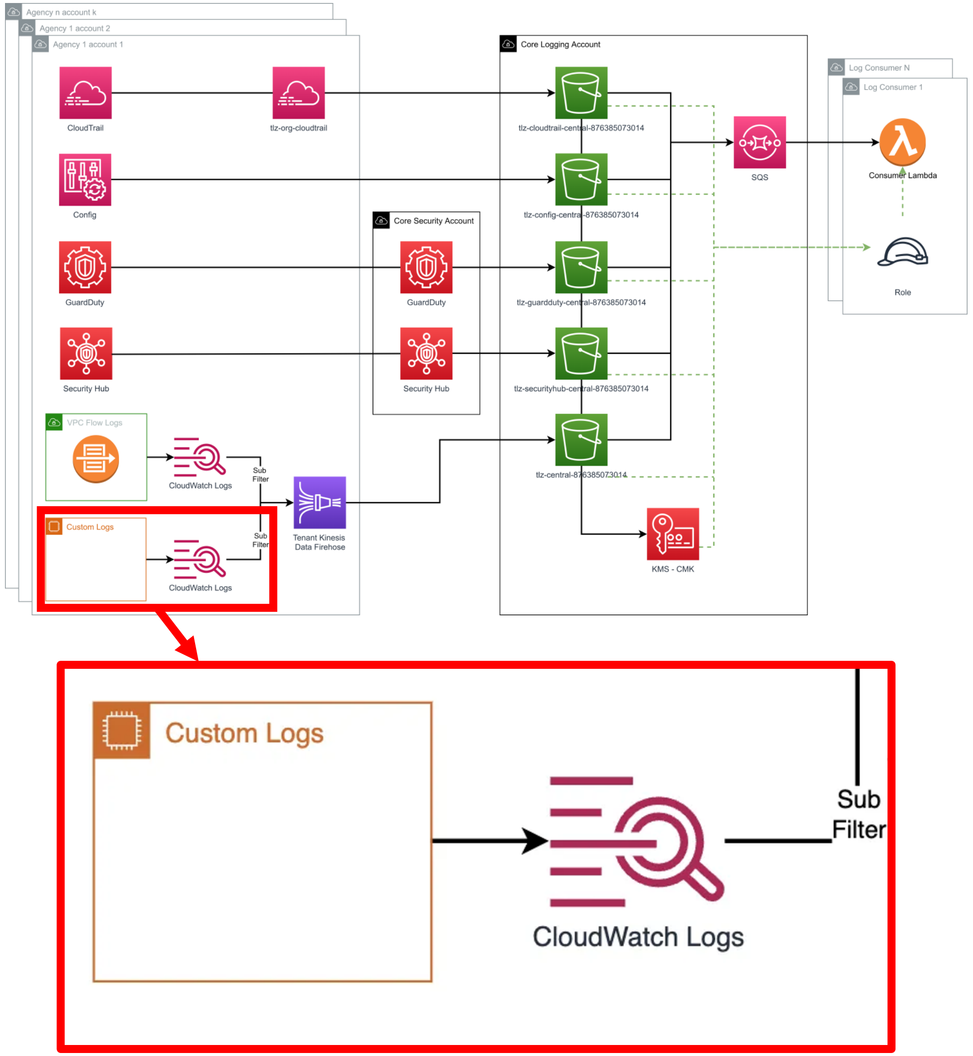
4. Security Hub (SH) is being managed by central SH and configured to direct export log to Central Log S3 bucket.

5. Kinesis Firehose (KFH) will be provisioned in tenant account by GovTech Team.

6. VPC Flow Logs and Custom Logs (workload/application logs) stored in CloudWatch Log group will be piped to KFH using Subscription Filter.

7. KFH exports the logs to Central Log S3 bucket.

Agency's Responsibilities (1/4)



Agencies shall manage and configure the **RED box** area where the rest of the components that showing on the diagram will be managed and configured by GovTech Team.

Scenarios/Responsibilities:

A. For new accounts in GCC 2.0 (Agency)
B. For migration from GCC 1.0 (Agency)
C. For Daily operation (Agency)

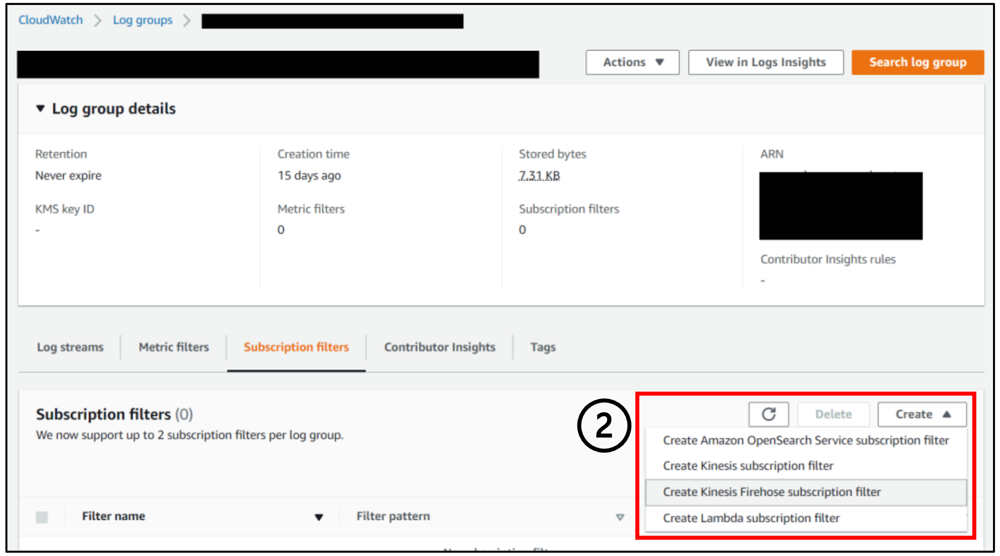
Agency's Responsibilities (2/4)

A. For new accounts in GCC 2.0 (Agency)

1. Install CloudWatch Agent on workload to forward logs to CloudWatch Log Group.

2. Navigate to the CloudWatch Log Groups and create KFH subscription filter.

3. Select clm-central-logging-firehose as DestinationARN KFH's Delivery Stream.



CloudWatch > Log groups > [redacted]

[redacted]

Actions ▼ | View in Logs Insights | Search log group

▼ Log group details

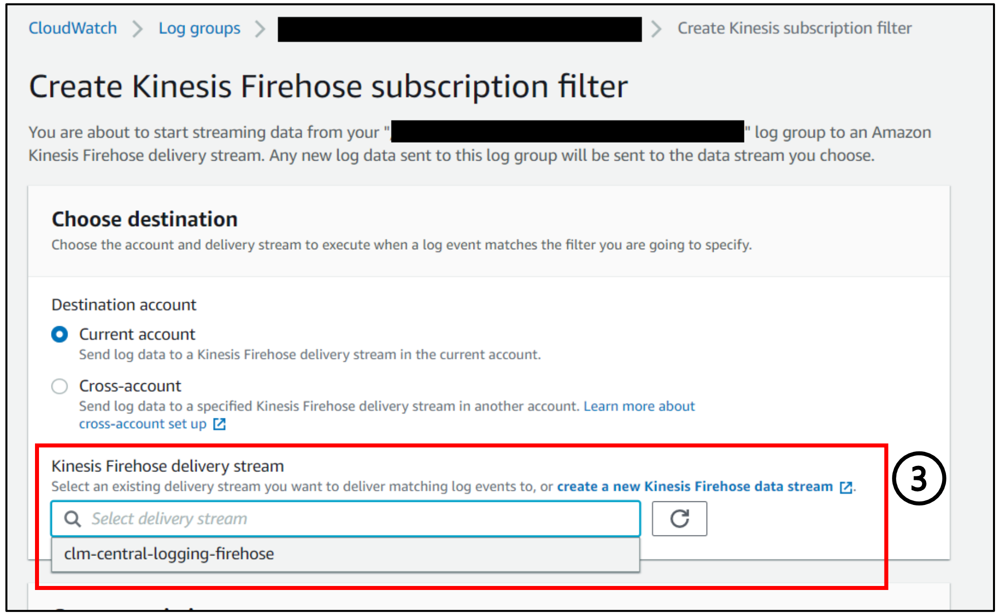
Retention Never expire	Creation time 15 days ago	Stored bytes 7.31 KB	ARN [redacted]
KMS key ID -	Metric filters 0	Subscription filters 0	Contributor Insights rules -

Log streams
Metric filters
Subscription filters
Contributor Insights
Tags

Subscription filters (0)

We now support up to 2 subscription filters per log group.

Delete
Create ▲
Create Amazon OpenSearch Service subscription filter
Create Kinesis subscription filter
Create Kinesis Firehose subscription filter
Create Lambda subscription filter
Filter name
Filter pattern
2



CloudWatch > Log groups > [redacted] > Create Kinesis subscription filter

Create Kinesis Firehose subscription filter

You are about to start streaming data from your "[redacted]" log group to an Amazon Kinesis Firehose delivery stream. Any new log data sent to this log group will be sent to the data stream you choose.

Choose destination

Choose the account and delivery stream to execute when a log event matches the filter you are going to specify.

Destination account

● Current account
Send log data to a Kinesis Firehose delivery stream in the current account.

○ Cross-account
Send log data to a specified Kinesis Firehose delivery stream in another account. Learn more about cross-account set up

Kinesis Firehose delivery stream

Select an existing delivery stream you want to deliver matching log events to, or **create a new Kinesis Firehose data stream**.

Select delivery stream

clm-central-logging-firehose

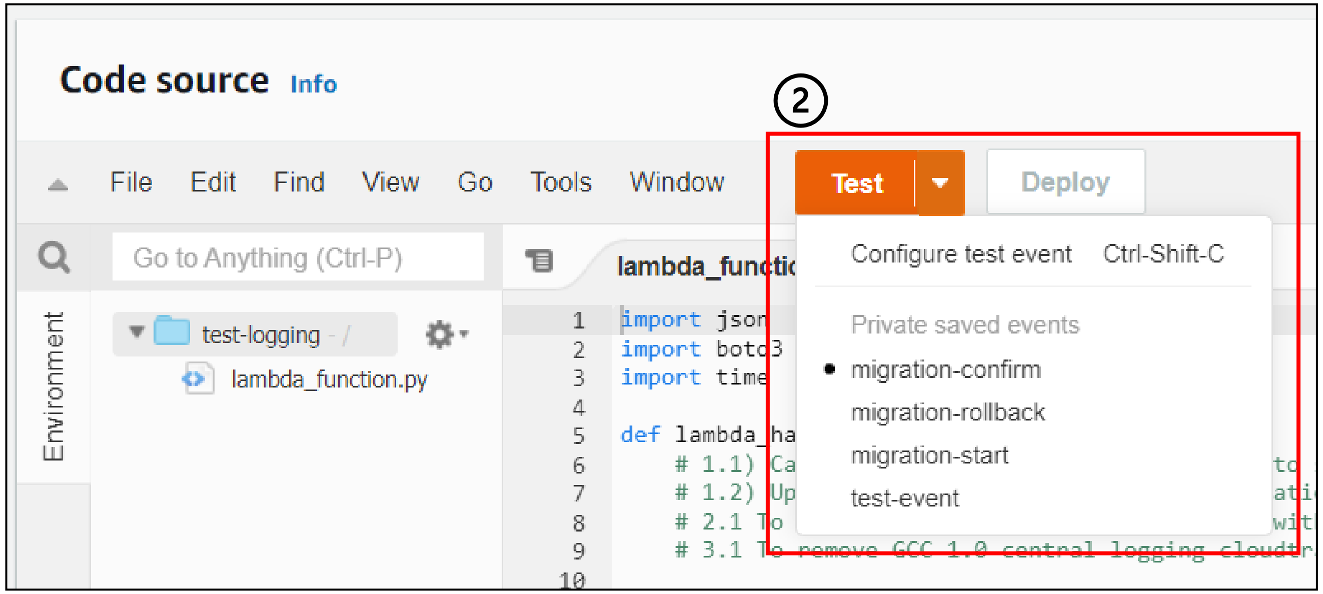
Agency's Responsibilities (3/4)

B. For migration from GCC 1.0 (Agency)

A Lambda Script will be provided to Agencies during the migration to update all existing Log group's subscription filters entries to point it to new DestinationARN (KFH).

1. Navigate to AWS Lambda and create a Lambda function with the provided steps and scripts.

2. Depending on the migration status, Agency may execute one of the following lambda function:
   - i. **migration-start → migration-rollback**
     - this scenario is for agency that wanted to rollback their setup to GCC 1.0
   - ii. **migration-start → migration-confirm**
     - this scenario is for agency that wanted to proceed with their setup in GCC 2.0



```
import json
import boto3
import time

def lambda_ha
    # 1.1) Ca
    # 1.2) Up
    # 2.1 To
    # 3.1 To remove GCC 1.0 central logging cloudtr
```

Enhancement (Q2-2022)

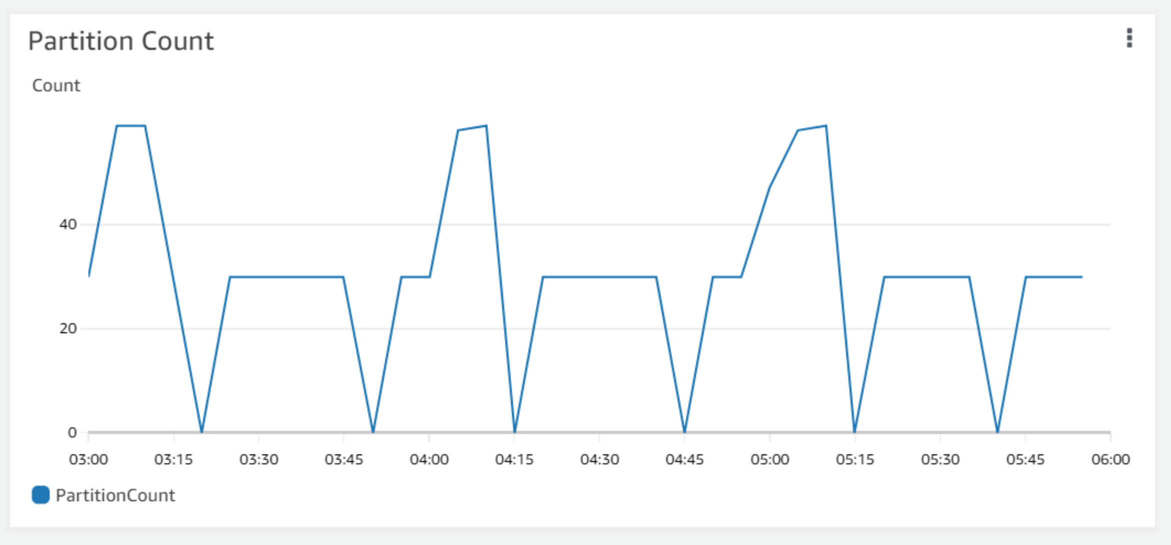
- The Lambda script will be converted as part of the IaC Provisioning and deploy as baseline.
- Agency no longer need to manually create the Lambda Function on Step 1.
- Agency will only require to trigger the Lambda Function during migration.

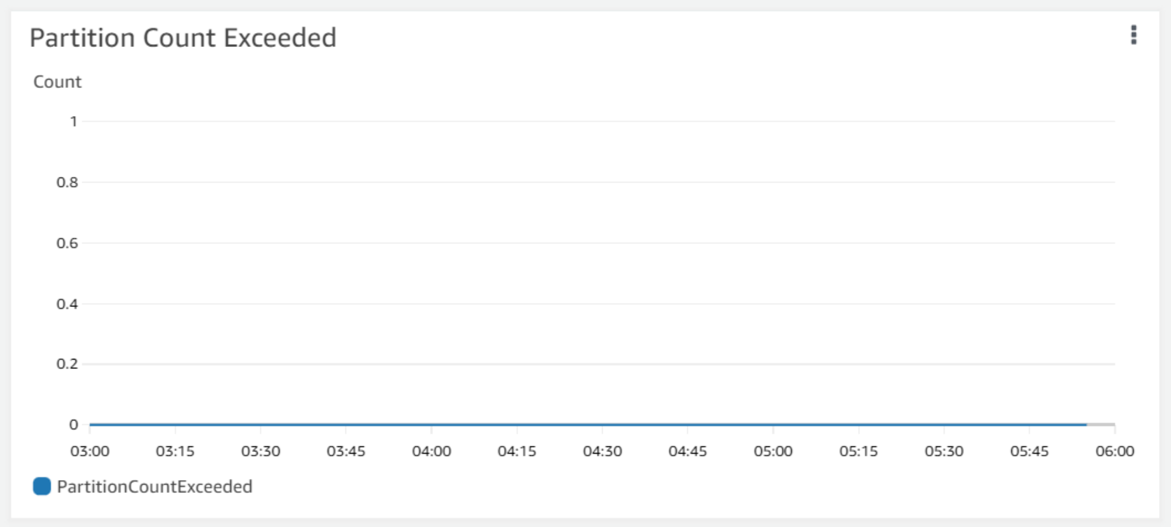
Agency's Responsibilities (4/4)

C. For Daily operation (Agency)

Agency is to take note of the quota’s limit on FH’s metric dashboard. There is a limit of 500 active partitions for each dynamic partitioning on a delivery stream. Agency are responsible to request an increase of the quota when it reached the threshold of 400 active partitions.

1. Navigate to AWS Kinesis ➜ Delivery streams.
2. Select clm-central-logging-firehose.
3. Under the Monitoring, check on both Partition Count and Partition Count Exceeded.
4. Use the Amazon Kinesis Data Firehose Limits form to request an increase of this quota.





Agency Accessing Logs in Centralized S3 Bucket

Prerequisites:

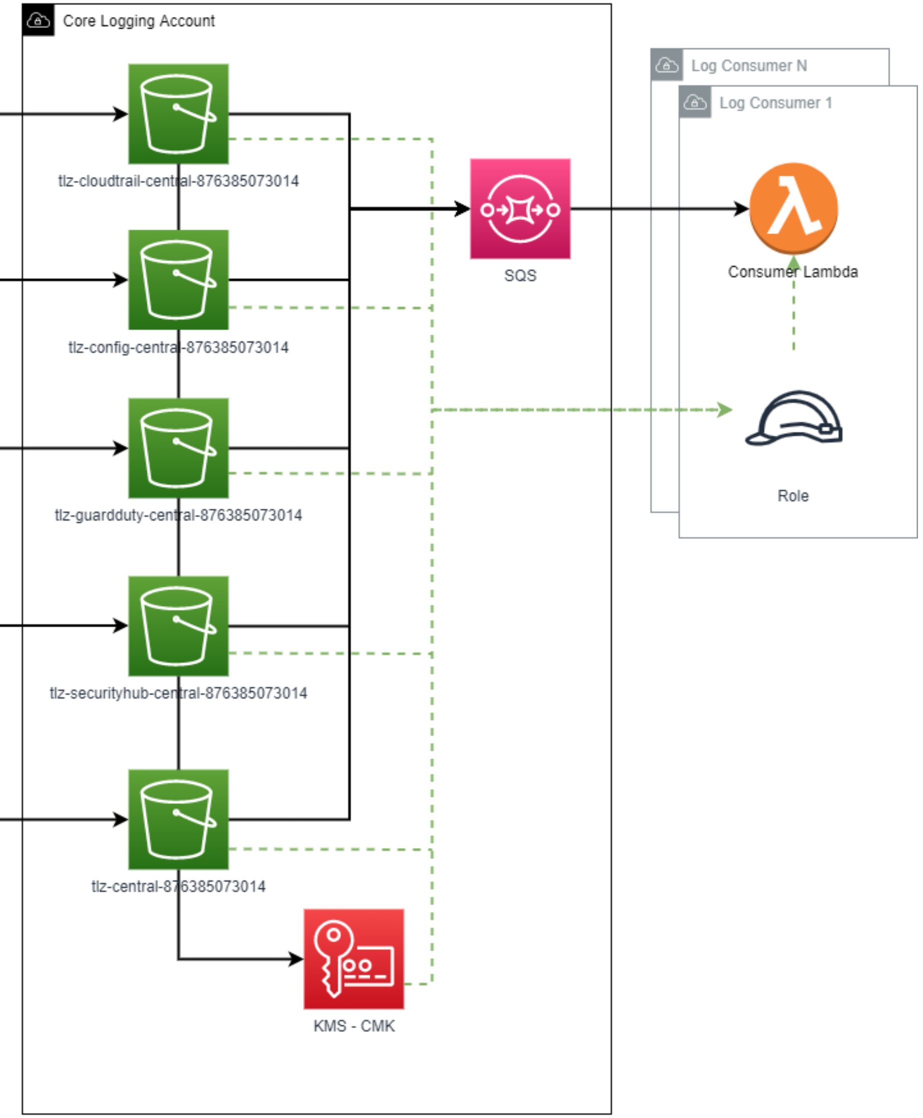
1. agency_security_operation role is required for Agency to access their own logs in Centralized S3 Bucket.
2. Agency will have to raise a service request ticket* to request agency_security_operation role for the personnel to access Agency's logs in Centralized S3 Bucket.

* Service Request topic will be covered in the future clinic sessions

Steps to access:

1. Once the role has been assigned to the personnel, access to AWS SSO and login to the AWS Account with the assigned agency_security_operation role.
2. Navigate to Amazon Kinesis > Delivery Stream, click on clm-central-logging-firehose.
3. Click on the Configuration tab, and scroll down to Destination settings then click on the S3 bucket link to access the logs in Centralized S3 Bucket.
4. Navigate to own account ID S3 prefix.
5. Download the zipped file.

Integration of Central Logging to Log Consumer (GCSOC)


Core Logging Account
tlz-cloudtrail-central-876385073014
tlz-config-central-876385073014
tlz-guardduty-central-876385073014
tlz-securityhub-central-876385073014
tlz-central-876385073014
KMS - CMK
SQS
Log Consumer N
Log Consumer 1
Consumer Lambda
Role

- GCSOC is in the progress of integration to GCC 2.0 central log to consume the logs and perform security monitoring and analysis for GCSOC onboarded tenants.

- Details will be provided at a later date for GCC 2.0 tenants.

Benefits of GCC 2.0 Continuous Logging

Benefits	Explanation
Cost Saving	- Agencies are not charged for the cost of Log Storage in GCC 2.0 Centralized S3 Bucket
Faster Log Export	- Logs that are being managed organizationally will be export directly to Centralized S3 bucket - Dedicated Kinesis Firehose (KFH) in each Agency Account allows faster export for Custom Logs(workload and application)
Lesser Steps / Avoid misconfiguration	- Standard Kinesis Firehose (KFH) name: clm-central-logging-firehose is provisioned in every agency account to ease the configuration of Subscription Filter

Cost of GCC 2.0 Continuous Logging to Tenants

- Agencies to take note of the AWS cloudspend in their account associated with Central Logging as follows:

→ Kinesis Firehose (FH) – $62/mth^

^ – These estimated costing are based on approx. 30M log records (1KB per record) per account in a month from GCC 1.0 central log historical data.

Q&A

#	Question	Answer
1	Will I still be able to access to the bucket in GCC 1.0?	Yes, Agency who has migrated their accounts to GCC 2.0 will still be able to access their file objects in GCC 1.0.
2	Will Agency continue to pay for data storage charges in GCC 1.0 after the account is migrated to GCC 2.0?	Yes. Agency will continue to be invoiced for file objects stored in GCC 1.0 central log storage under their account.
3	Will Agency be required to migrate their logs in GCC 1.0 to GCC 2.0?	Agency should perform their cost analysis between migrating their logs from GCC 1.0 to GCC 2.0 versus continuing to pay for their file objects in GCC 1.0 central log storage.

THANK YOU

Questions and Answers

We Want to Hear Your Feedback!

https://form.gov.sg/625cbc09ef648600142ba463

- Let us know what went well and how we can improve.
- We want to ensure that we are bringing the right contents to you so as to help Agencies.
- If you have any questions, please reach out to us at Ask_CODEX@tech.gov.sg