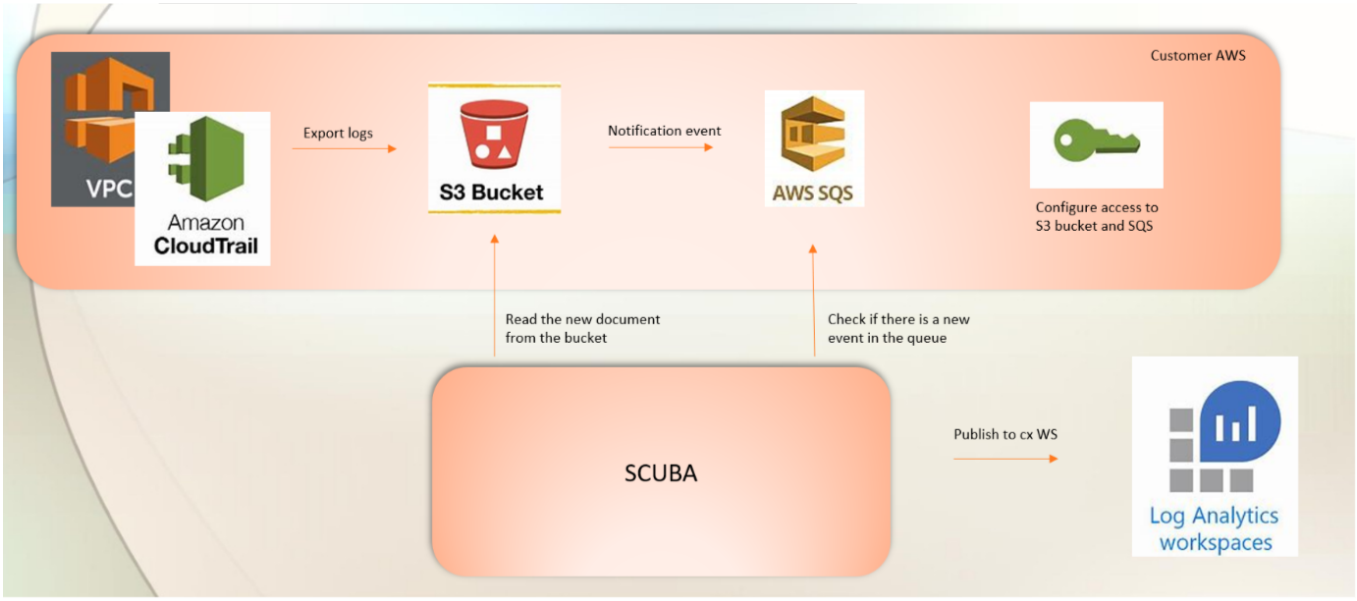
AWS troubleshooting

Last updated by | Hekmat Abuzahrah | Mar 30, 2023 at 8:35 AM CDT

- ## AWS S3 troubleshooting

  Issue: data is not received from AWSS3 Connector (or one of its datatypes) To Sentinel

  Logs of the AWS S3 connector (or one of its datatypes to Sentinel) are not visible in his Sentinel workspace for more than 30 minutes when the connector was connected. Here is the architecture diagram of the connector:

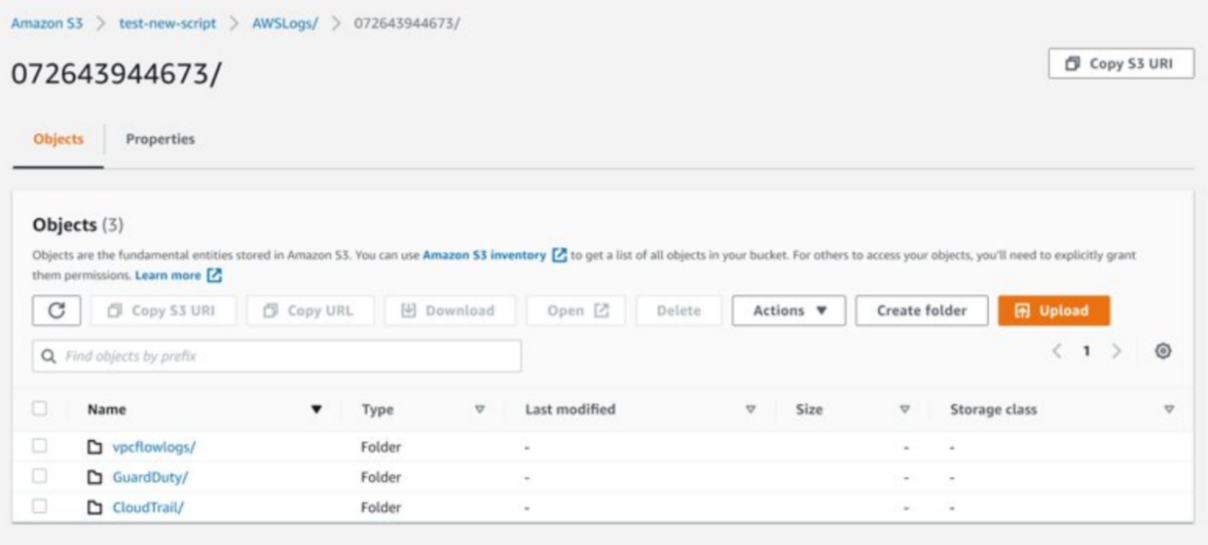


="Paragraph SCXW233057356 BCX0" style="margin: 0px;padding: 0px;white-space: pre-wrap;font-weight: normal;font-style: normal;vertical-align: baseline;background-color: transparent;color: windowtext;text-align: left;text-indent: 0px">This guide will only cover a subset of other probable causes:

- The data is not ingested to the S3 bucket in AWS.
- The SQS (in AWS cloud) does not receive notifications from the S3 bucket.
- The data cannot be read from the SQS/S3 in AWS cloud (if it's GuardDuty logs, usually caused by wrong KMS permissions).

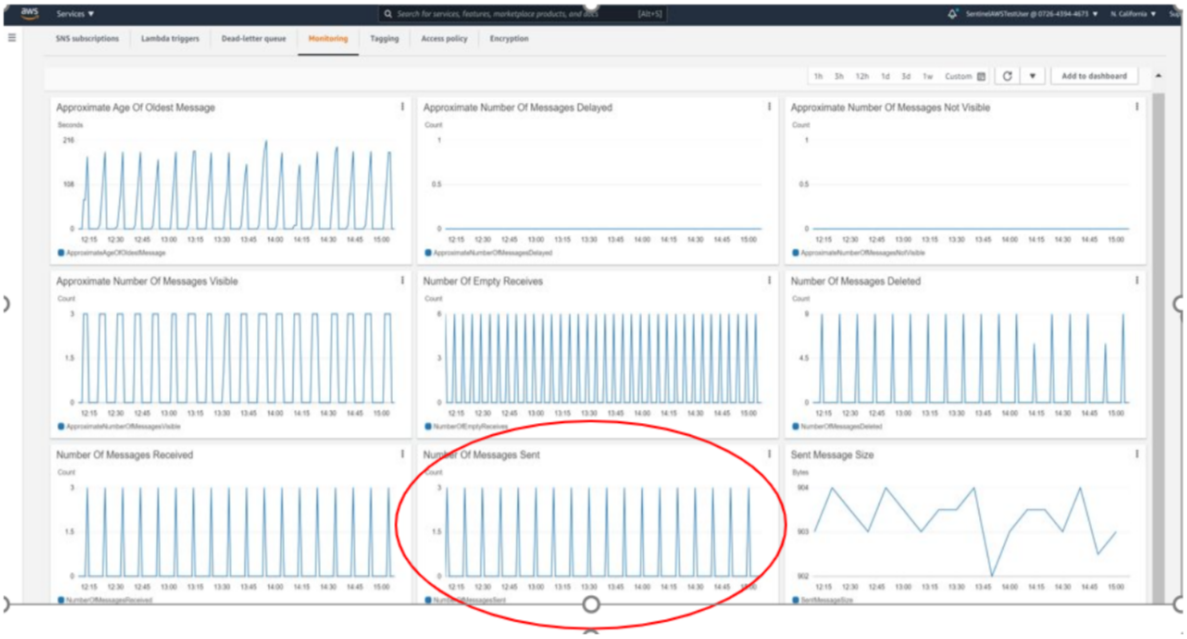
Identifying the cause

- Check that the relevant data exists in the S3 bucket
  - Open the S3 bucket in AWS, search for the relevant folder according to the required logs, and check if there are any logs inside this folder:



If the data does not exist is an issue in AWS configuration- [Configure an AWS service to export logs to an S3 bucket]

- Verify that the data arrived from S3 to the SQS
    - Open the relevant SQS in AWS and go to the monitoring tab, he should see traffic in “Number Of Messages Sent” widget.

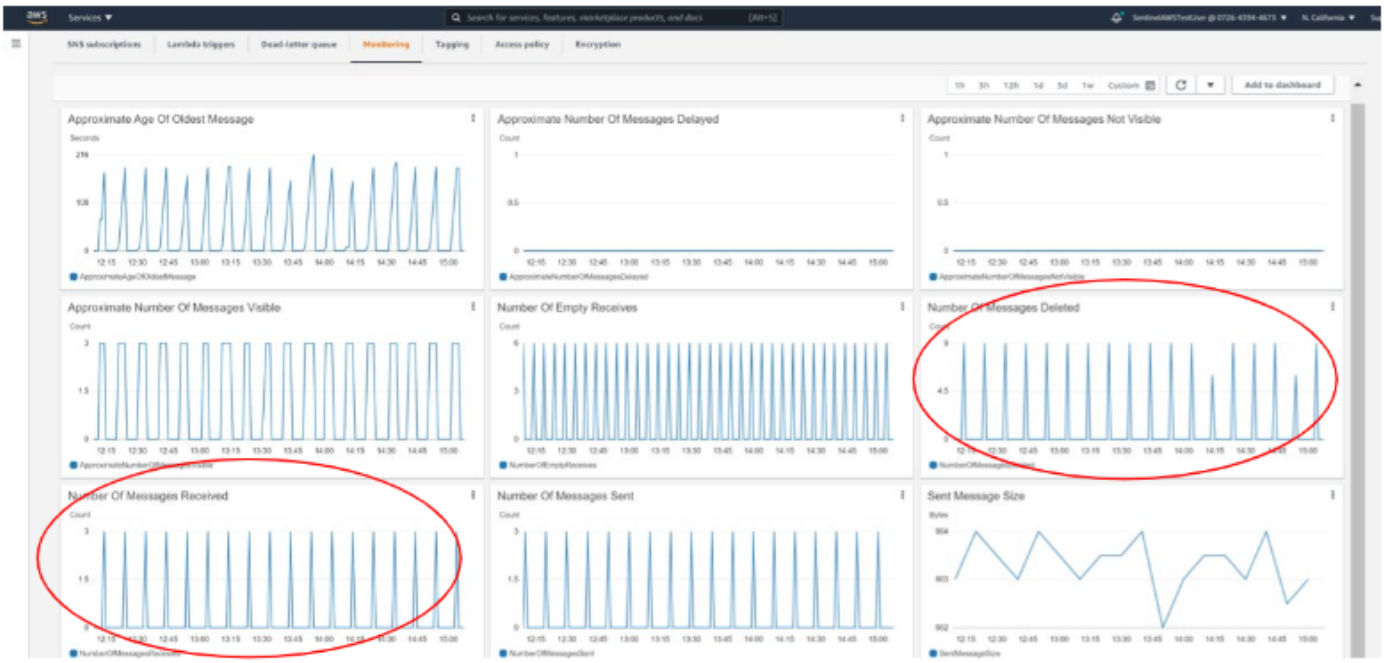


If there is no traffic in the SQS, the problem is in AWS configuration:

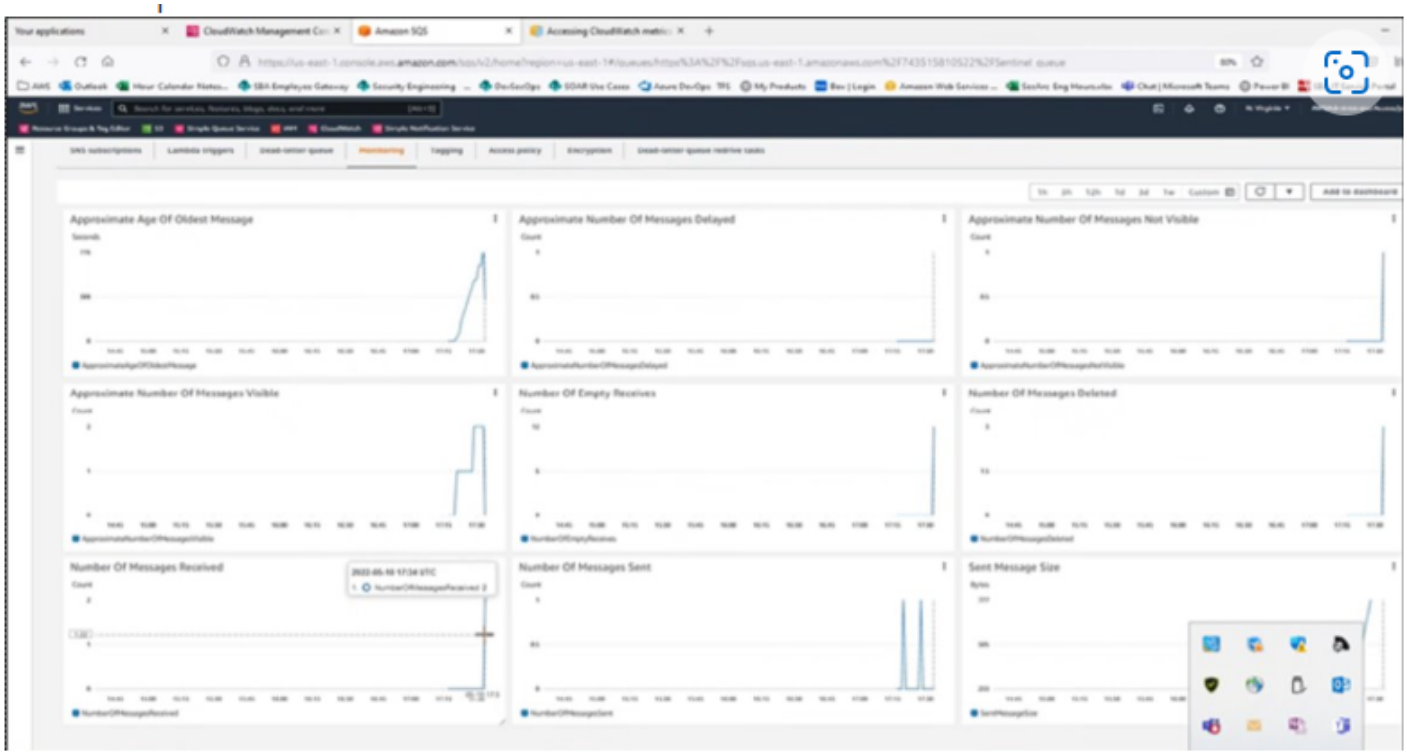
- Make sure that the Event notifications definition for the SQS is with the correct data Filters (prefix and suffix). To see the event notifications: select the “Properties” tab in the S3 bucket and then go to “Event notifications” section. If you do not have one, create it. [Create a Simple Queue Service (SQS) in AWS]
- Make sure that the SQS has the relevant policies to get the data from the S3 bucket. The SQS will have to contain [this] policy under the Access policy tab.

- Verify that data is read from the SQS:

- Open the relevant SQS in AWS and go to the monitoring tab, you should see traffic in “Number Of Messages Deleted" and “Number Of Messages Received" widgets.



Please note that one spike of data is not enough (as in the picture below), you will have to wait until there is enough data (like in the picture above) to check if there is a problem.



- If at least one of the widgets is empty, check health logs by running this query:

```
SentinelHealth
| where TimeGenerated > ago(1d)
| where SentinelResourceKind in ('AmazonWebServicesCloudTrail', 'AmazonWebServicesS3')
| where OperationName == 'Data fetch failure summary'
```

```
| mv-expand TypeOfFailureDuringHour = ExtendedProperties["FailureSummary"]
| extend StatusCode = TypeOfFailureDuringHour["StatusCode"]
| extend StatusMessage = TypeOfFailureDuringHour["StatusMessage"]
| project SentinelResourceKind, SentinelResourceName, StatusCode, StatusMessage, SentinelResourceId,
TypeOfFailureDuringHour, ExtendedProperties
```

- Find the error type you saw in the results in Q&A health document.
- Make sure that health is enabled:

  ```
  SentinelHealth
  | take 20
  ```
- If not please follow this link.