Troubleshooting AWS App

Workshop Splunk Add-on for AWS 4.3+

Kamilo Amir | Splunk Cloud Architect

Table of Contents

Troubleshooting Splunk App / Add-on for AWS

This lab guide is meant to help you troubleshoot the Splunk Add-on for AWS and determine why you are not receiving data or why panels are not populating.

Permissions Review

The first place I always check is to make sure that the user or role that Splunk is using to collect the data has the right permissions. Here is the document link to the permissions: http://docs.splunk.com/Documentation/AddOns/released/AWS/ConfigureAWSpermissions

Let's start with a search to see if there are any permission issues:

```
index=_internal sourcetype=aws* ERROR Access*
```

If you see these error messages, you might want to check the policy created for Splunk and make sure that it was granted access to the service in question.

Searches

Here are some helpful searches to determine if you are seeing any issues with capturing data and why dashboards are not populating (especially the Topology view).

Am I getting data?

```
index = main sourcetype=aws* | stats count by sourcetype
```

Are my saved searches populating?

```
index=aws_* | stats count by index
```

Is there any lag between indexed events and index time?

```
index=main sourcetype=aws:* | eval time=_time | eval
itime=_indextime | eval latency=(itime  - time) | stats count,
avg(latency), min(latency), max(latency) by sourcetype
```

Am I seeing errors collecting data from AWS?

```
index=_internal ERROR sourcetype=aws:*| stats count by
sourcetype
```

Am I getting throttled by AWS?

```
index=_internal sourcetype=aws:* | transaction pid tid | dedup
punct
```

Validate HEC

Test to make sure that your Splunk instance is able to accept HEC requests:

- Splunk Enterprise
  - `curl -k https://<host>:8088/services/collector -H 'Authorization: Splunk <token>' -d '{"sourcetype": "mysourcetype", "event":"Hello, World!"}'`
- Splunk Cloud
  - `curl -k -H "Authorization: Splunk <token>" https://http-inputs-mysplunkcloud.example.com:8088/services/collector/event -d '{"sourcetype": "mysourcetype", "event": "http auth ftw!"}'`
- Splunk Cloud Trial
  - `curl -k https://input-<trial_name>.cloud.splunk.com:8088/services/collector -H 'Authorization: Splunk <token>' -d '{"event":"Hello, World!"}'`

Where to find Saved Searches / Lookups / Macros / Data Models?

This section is important if you decide to move your AWS data from the main index to a custom index and want the app to continue to work accordingly.

The saved searches will allow you to see what data is being summarized from the main index into the appropriate summary index.

The Lookups allow you to see where enrichment data is being kept. You can update the tables if necessary.

The Macros used in the app to simplify the search commands. If you decide to move your data from the main index, you should modify the appropriate macros to keep the app up-to-date.

Saved Searches:
http://docs.splunk.com/Documentation/AWS/5.0.2/Installation/Savedsearches

Lookups:
http://docs.splunk.com/Documentation/AWS/5.0.2/Installation/Lookups

Data Models:
http://docs.splunk.com/Documentation/AWS/5.0.2/Installation/Datamodels

Macros:
http://docs.splunk.com/Documentation/AWS/5.0.2/Installation/Macros

R=Recommended, S=Supported, NA = Not Available

AWS service	SQS Based S3	Modular Input	Kinesis / HEC	Generic S3
Billing	**NA**	**R**	**NA**	**S**
CloudWatch (metrics)	**NA**	**R**	**NA**	**NA**
CloudFront Access Logs	**R**	**S**	**S**	**S**
Config	**R**	**S**	**NA**	**S**
Config Rules	**NA**	**R**	**NA**	**NA**
Description	**NA**	**R**	**NA**	**NA**
ELB Access Logs	**R**	**S**	**S**	**S**
Inspector	**NA**	**R**	**NA**	**NA**
CloudTrail	**R**	**S**	**NA**	**S**
S3 Access Logs	**R**	**S**	**S**	**S**
VPC Flow Logs	**NA**	**S**	**R**	**NA**

http://docs.splunk.com/Documentation/AddOns/released/AWS/Configureinputs

Setting up AWS Services with SQS Based S3 Input

This new input allows for the collection of data from CloudTrail and Config as well as any other service that writes to an SNS topic and S3 bucket. It is a stateless input which means that it can be scaled to multiple Heavy Weight Forwarders (HWF) and not have any contention for collecting data from AWS. The only requirement is that you add a dead letter queue to your SQS.

Setting up HEC for CloudWatch Logs

HTTP Event Collector (HEC) is a great way to push data into Splunk. This data input allows for high volume data to flow into Splunk and not get throttled by AWS API calls or be tied to a single HWF.