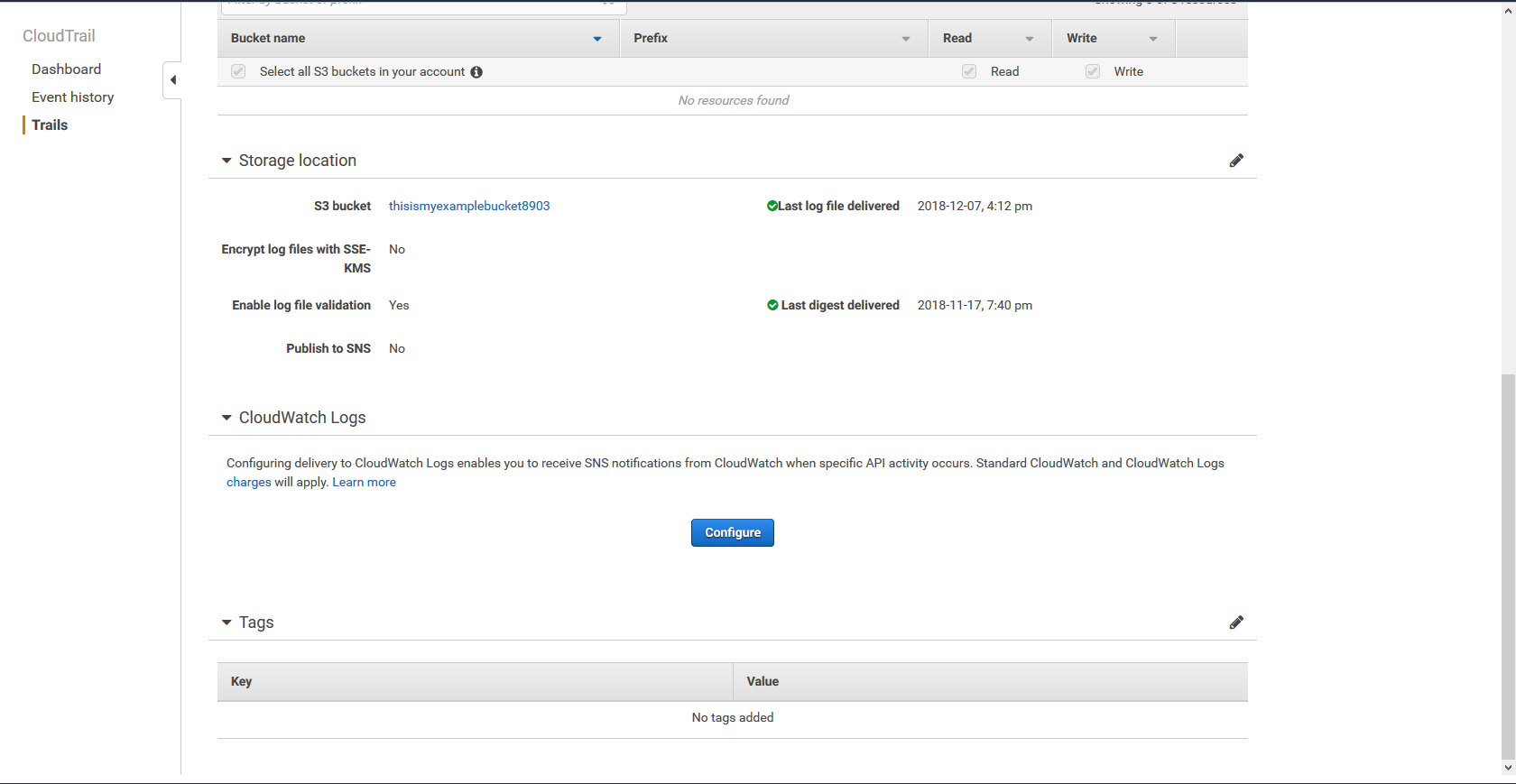
AWS notify via metric filters when CloudTrail is disabled

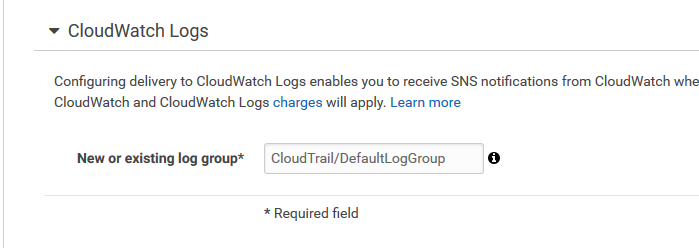
This documentation is being made to contrast between metric filters and CloudWatch Events. This will show how to set up metric filters to notify you when a trail is disabled. Let’s begin!

**Step 1:**

I already have a trail so for this I am going to use an existing trail. The first thing you need to do is configure you CloudTrail to send its logs to CloudWatch Logs. Click on your existing trail and locate the CloudWatch Logs section and press configure.



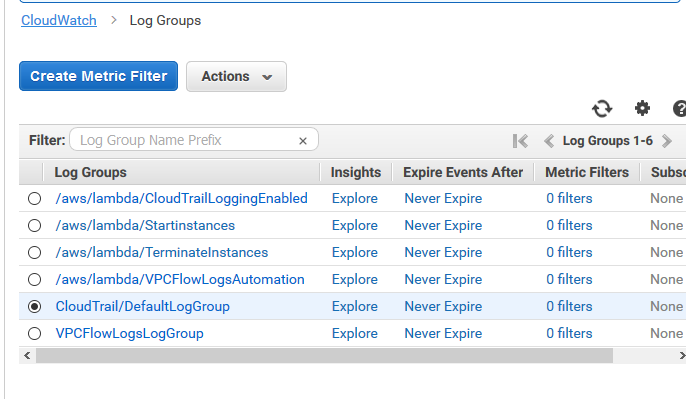
Once you press the blue configure button it will ask you to name a new or existing log group.



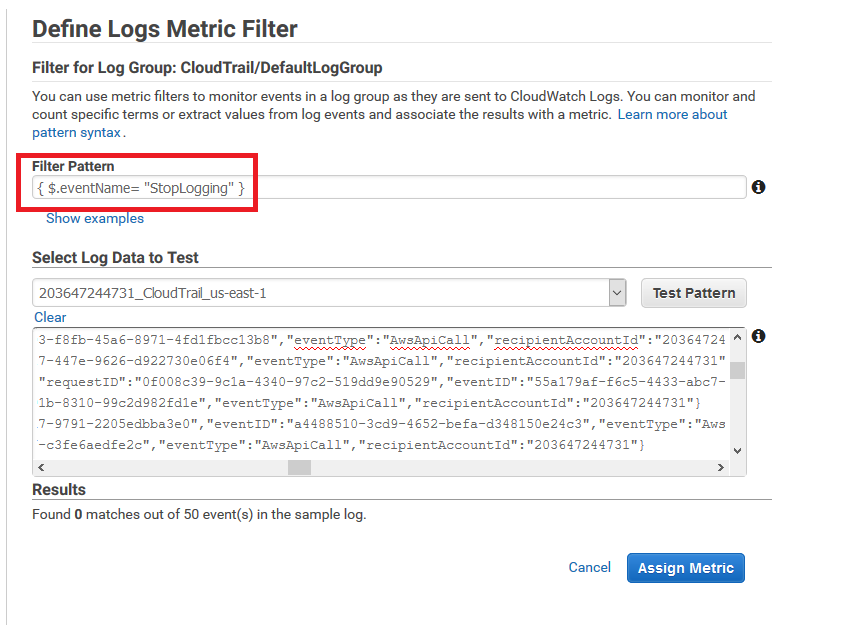
Once named press continue. It will automatically prompt you to create a role and it will make an appropriate for you so just press allow. Now CloudTrail will periodically send logs to CloudWatch Logs.

**Step 2:**

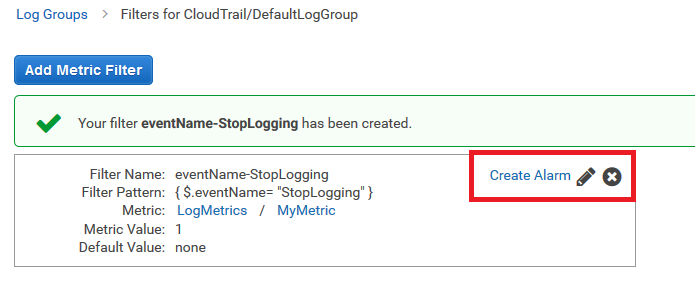
Now we need to configure the metric filter. Go to CloudWatch Logs and locate the log group you just made.



Once you select that log group click create metric filter at the top. Make sure the filter pattern matches exactly like below.



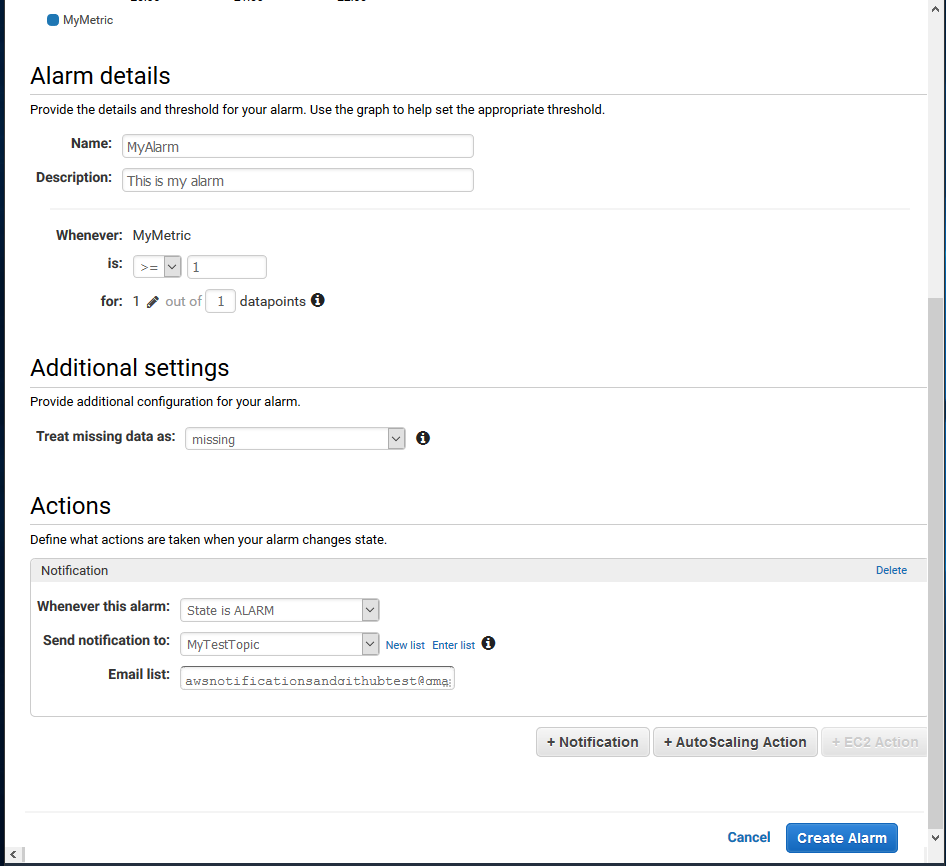
Then click assign metric. It will bring you to a page where you can change the name. You can choose to name it something better than the default or you can just create the filter.



Then click create alarm.

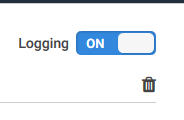
**Step 3:**

When creating the alarm you first need to name it. You then need to changes the data point for the alarm to whenever the metric is greater than or equal to 1 for 1 data point go into alarm. When in alarm that’s when you should get an email. Also you need to configure this alarm to send an email to you via your SNS topic. After everything matches my page as shown below click create alarm.

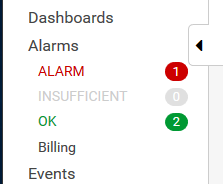


**Step 4:**

This step is purely for testing. Go to CloudTrail and locate one of your trails. Turn off its logging by selecting the blue button to stop logging.



If you wait a little bit as it may take up to 15 minutes you should receive an email and it should go into an alarm state in CloudWatch.



Now you have successfully setup a metric filter that emails you whenever someone disables CloudTrail!