**Configuring CloudTrail to Log to a CloudWatch Log Group**

### Introduction

Recall that the focus of CloudTrail is to monitor API activity, and CloudWatch monitors performance against AWS provided metrics or custom metrics you build. You can configure CloudTrail to send log files to CloudWatch log groups, and analyze the logs against metrics, even trigger an alarm with a notification when thresholds are violated. That is a mouthful, but don't worry.  The lab will break this down and walk you through setting it up and testing that it works properly.

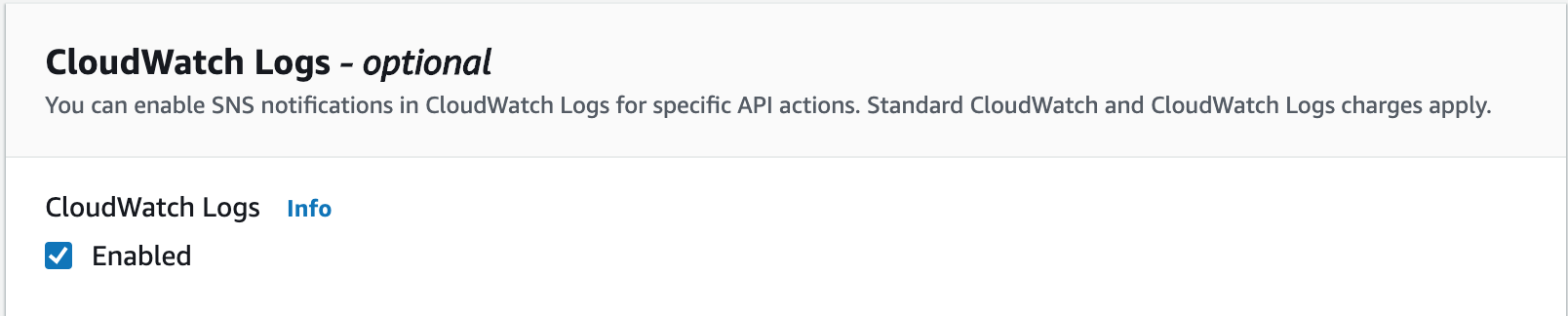
Note: When you first create a Trail the configuration is fairly basic. That helps you get up and going with CloudTrail without bogging down in too many details. As part of this Lab Step you will see there are a lot more configuration options available to CloudTrail. There is not enough time to change all configuration options however, such as whether or not to encrypt events stored on S3, what regions the Trail should apply to, what type of events to capture (read, write, read and write), etc.

### Instructions

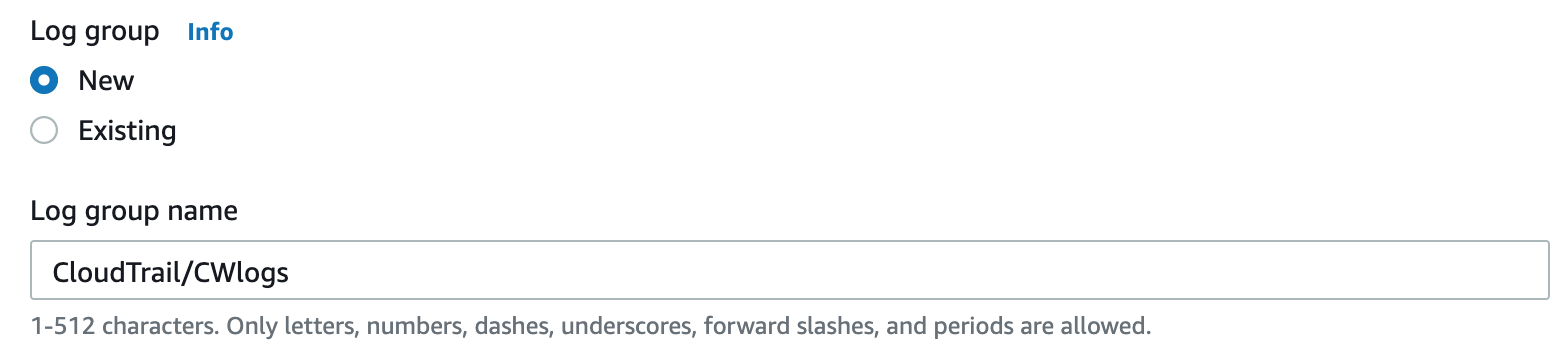
1. Navigate to the [CloudTrail console](https://us-west-2.console.aws.amazon.com/cloudtrail/home?region=us-west-2#/dashboard), and select **Trails** in the left navigation pane.

2. Select the actionable CloudTrail name you created earlier. (JohnDoeTrail)

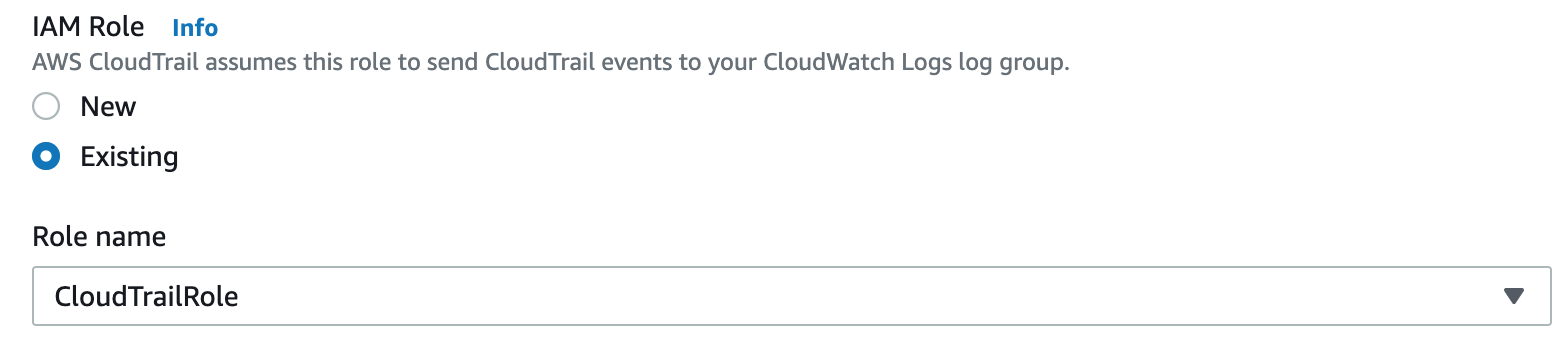
3. Scroll down to the **CloudWatch Logs** section. Click on **Edit**, then check the CloudWatch logs checkbox:



4. Enter CloudTrail/CWlogs as the **Log group name**:



5. Click on **Existing** under IAM Role and select the **CloudTrailRole**:



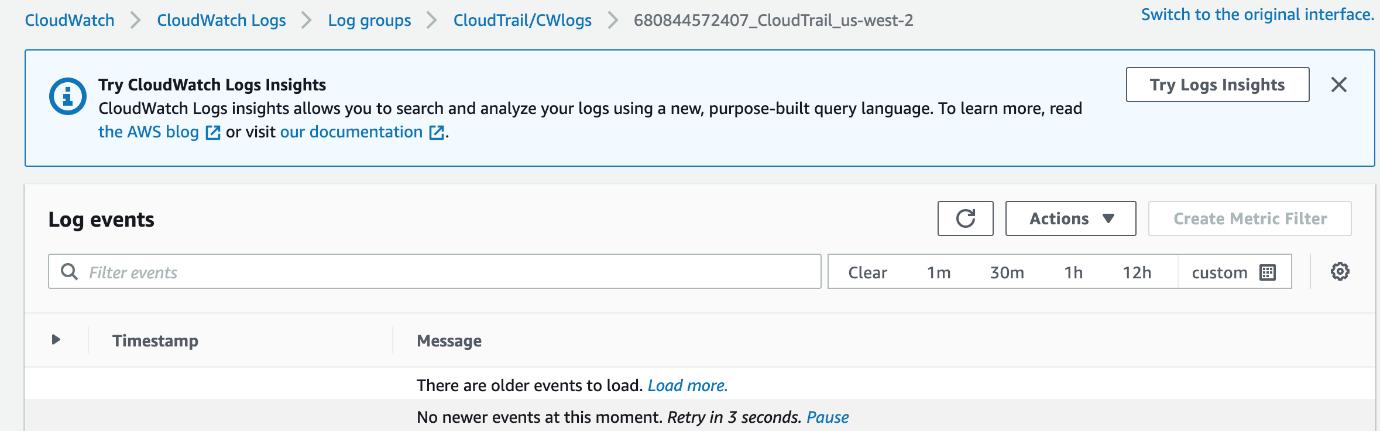
6. Click on **Save changes**.

7. In the AWS Management Console search bar, enter cloudwatch, click the **CloudWatch** result under **Services**, and select **Log Groups** in the left navigation pane.

[](https://us-west-2.console.aws.amazon.com/cloudtrail/home?region=us-west-2#/dashboard)

8. Click on the log group name you just created (**CloudTrail/CWlogs**). You should see an active **Log Stream**.

9. Click on the Log Stream name (comprised of your Account ID, Trail name and Region). It's possible you may have more than one stream. Feel free to pick either, you can always back out and pick the other stream to see additional messages within the stream. You should see (possibly after a short delay of a few minutes) individual events that are transferred from CloudTrail to the CloudWatch log group:



At this point, CloudTrail is sending logs to CloudWatch. However, there are no metrics associated with the events being sent. That is where things start to become useful. You'll set that up next.

Note: Unlike CloudTrail API log activity, CloudWatch logs are listed with the newest entries at the bottom and the oldest entries up top.

Note: The status could also be shown as a green check, revealing that CloudTrail is on and logging.

Even without generating events captured by CloudTrail, your CloudTrail log stream should receive events. For example, various list (e.g. ListRoles) and describe events (DescribeTrails). Return to the CloudWatch Log Streams and confirm entries in your stream.

10. If you jumped ahead to this Lab Step earlier due to delays in seeing the CloudTrail **Recent events**, return there and confirm the S3 **CreateBucket** and EC2 **RunInstances** events.

### Summary

In this Lab Step you configured CloudTrail to send logs to a new CloudWatch log group. You used the IAM Role named CloudTrailRolefor delivering your CloudTrail logs to CloudWatch. Lastly, you looked at the CloudWatch log stream to make sure the logs are being delivered ok.