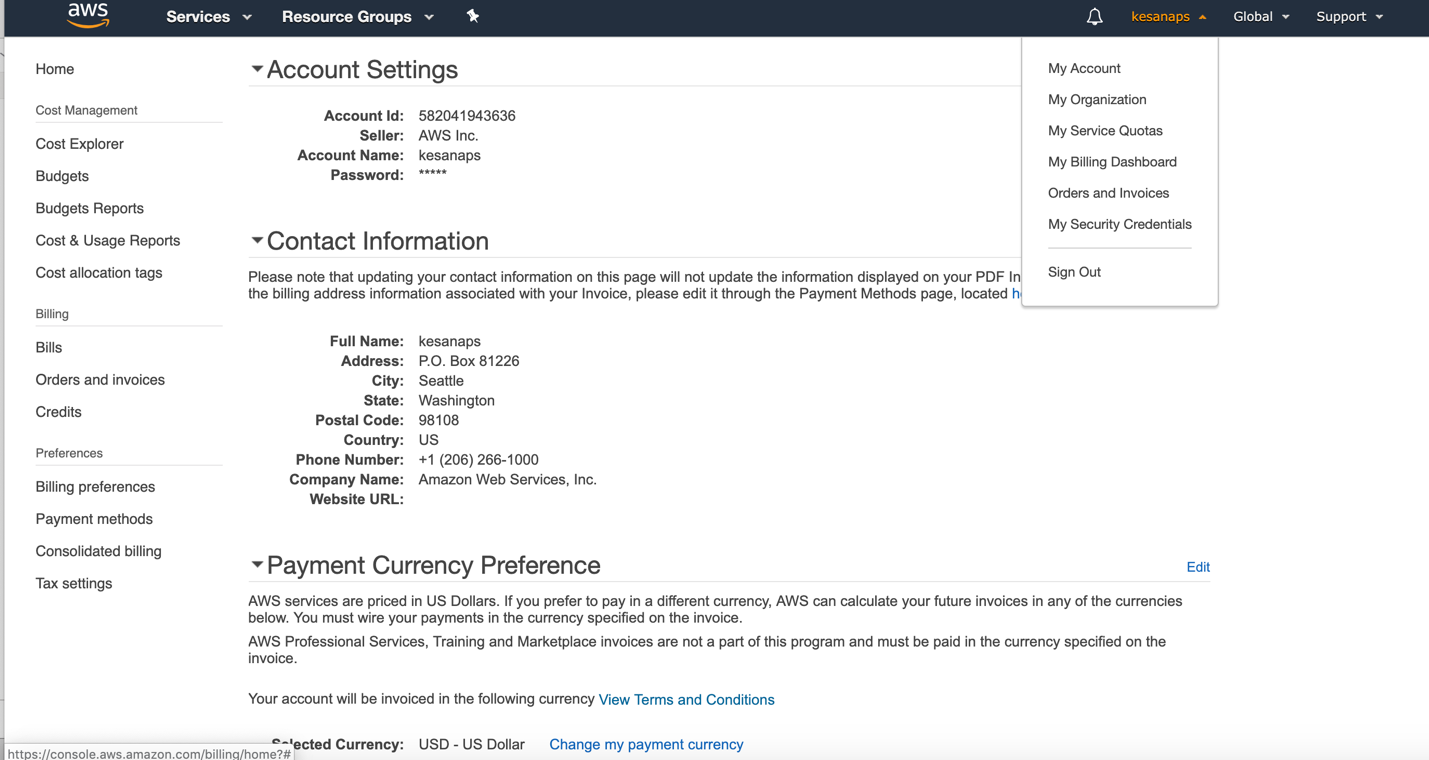
Sumo Logic Hands-on Lab

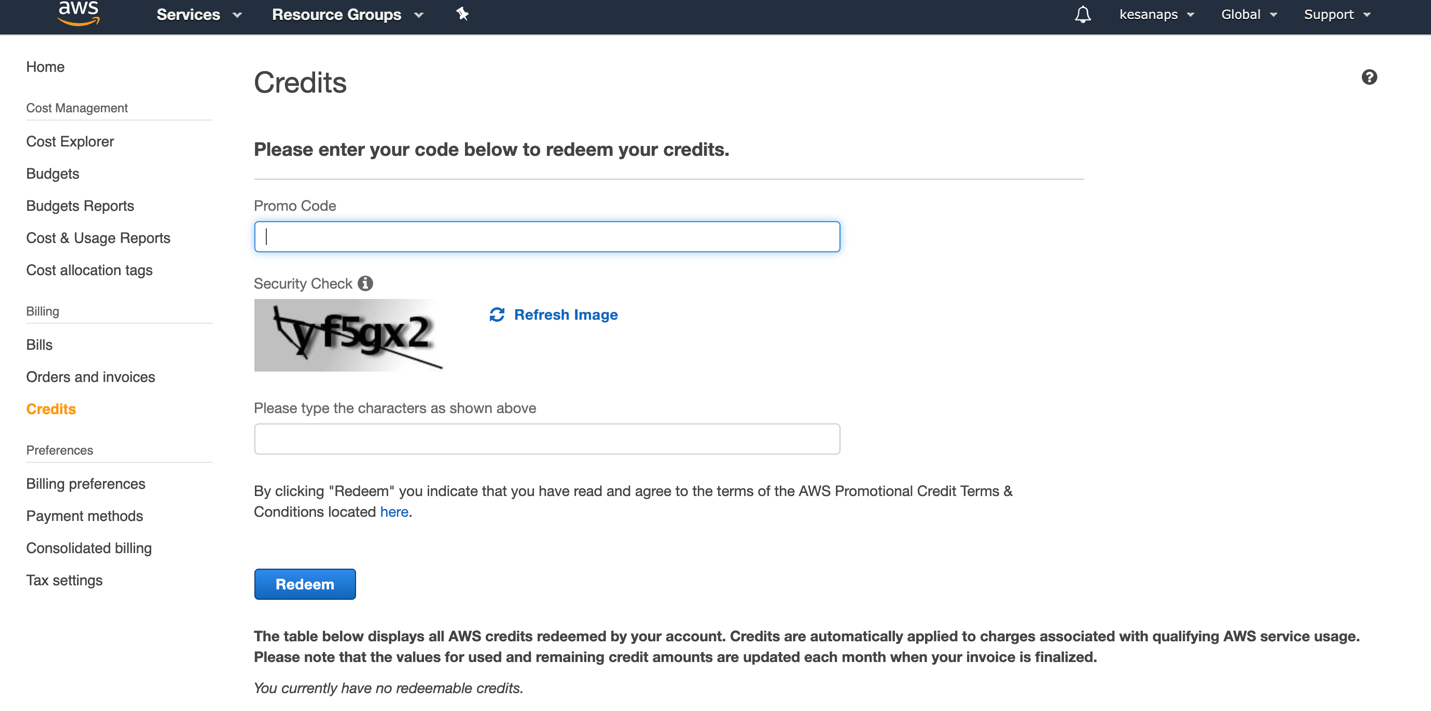
In order to complete this workshop, you'll need

* An active AWS Account
* Apply provided credits to your account. Go to “My Account” and Click on Credits to apply

The provided code.









**Overview**:

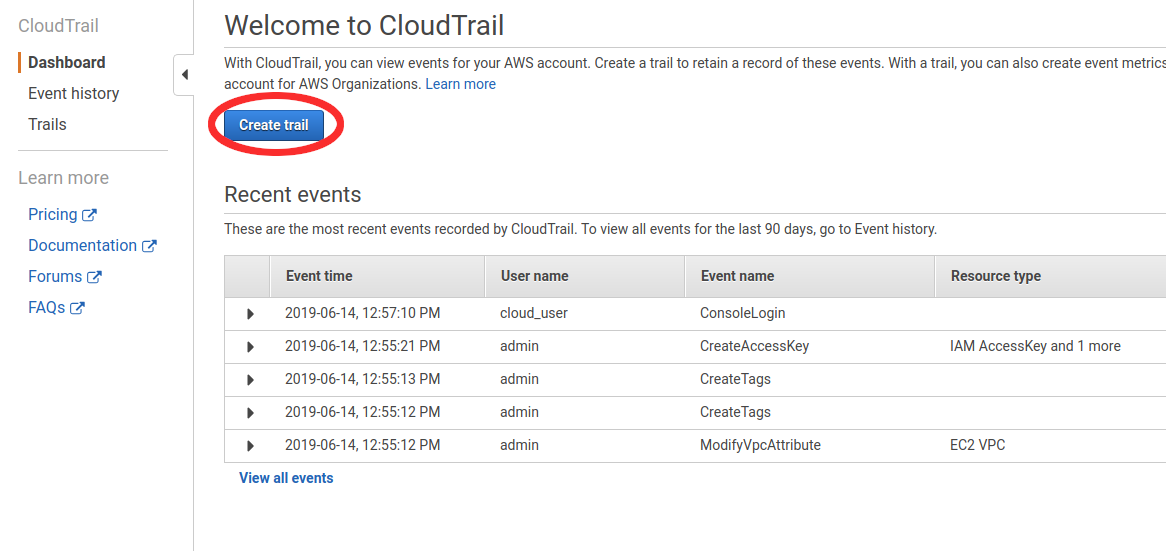
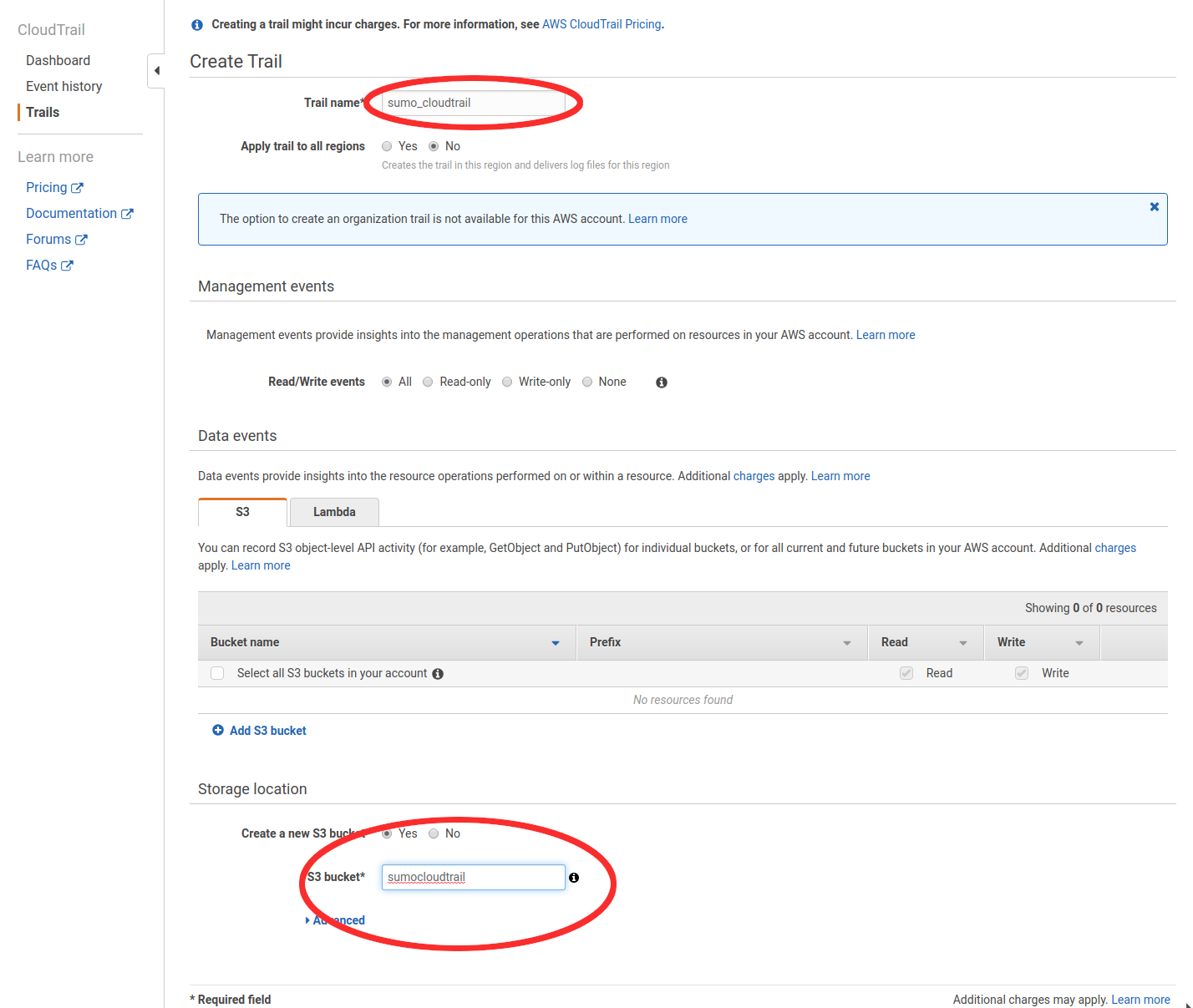
In this lab you will learn how to ingest AWS Cloudtrail logs. Additionally, you will learn how to install Sumo Logic apps which will provide quick time-to-value in the form of pre-built dashboards.

# Ingest Logs and Install App for AWS Cloudtrail

## Additional Reference Material For this Section:

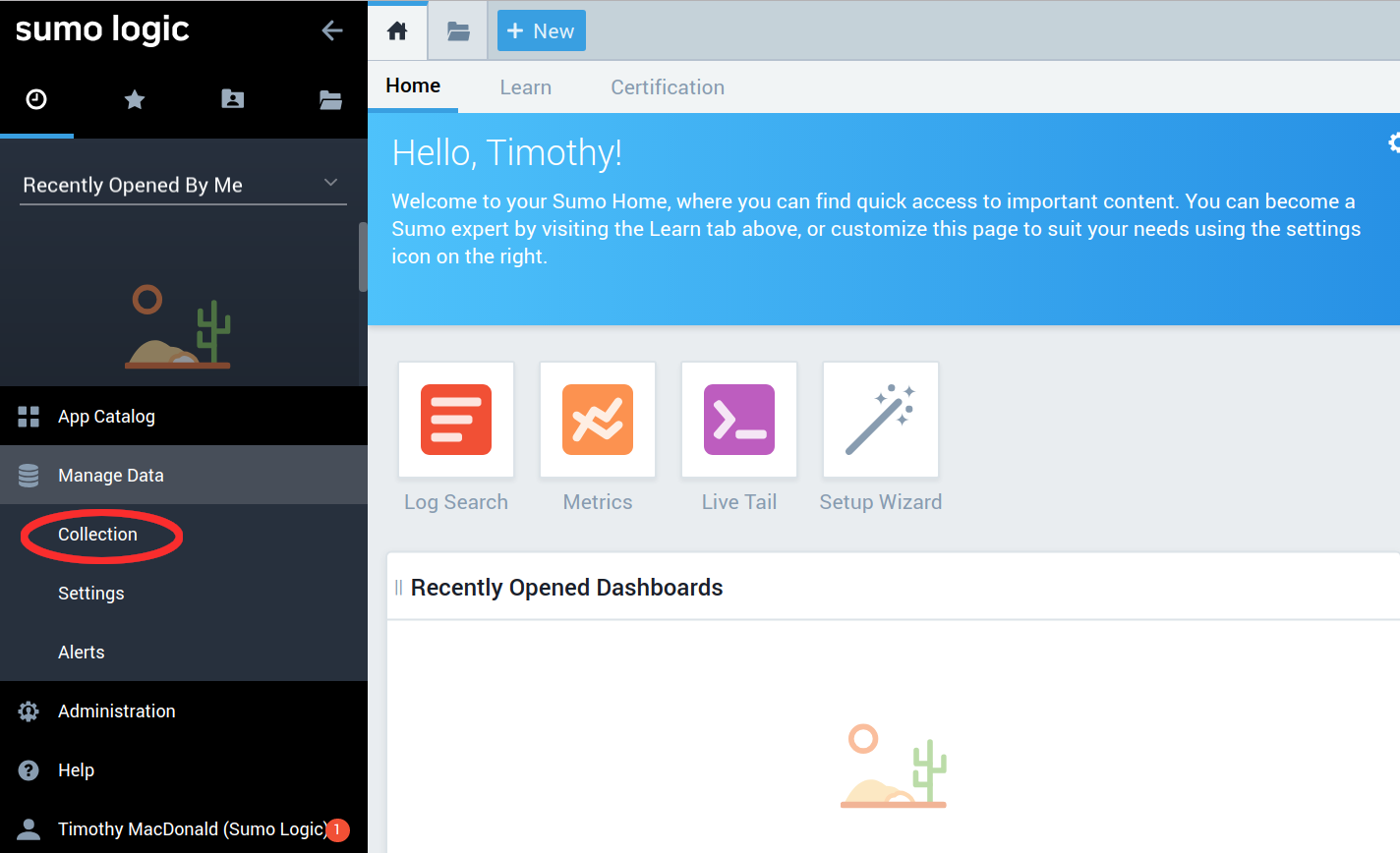
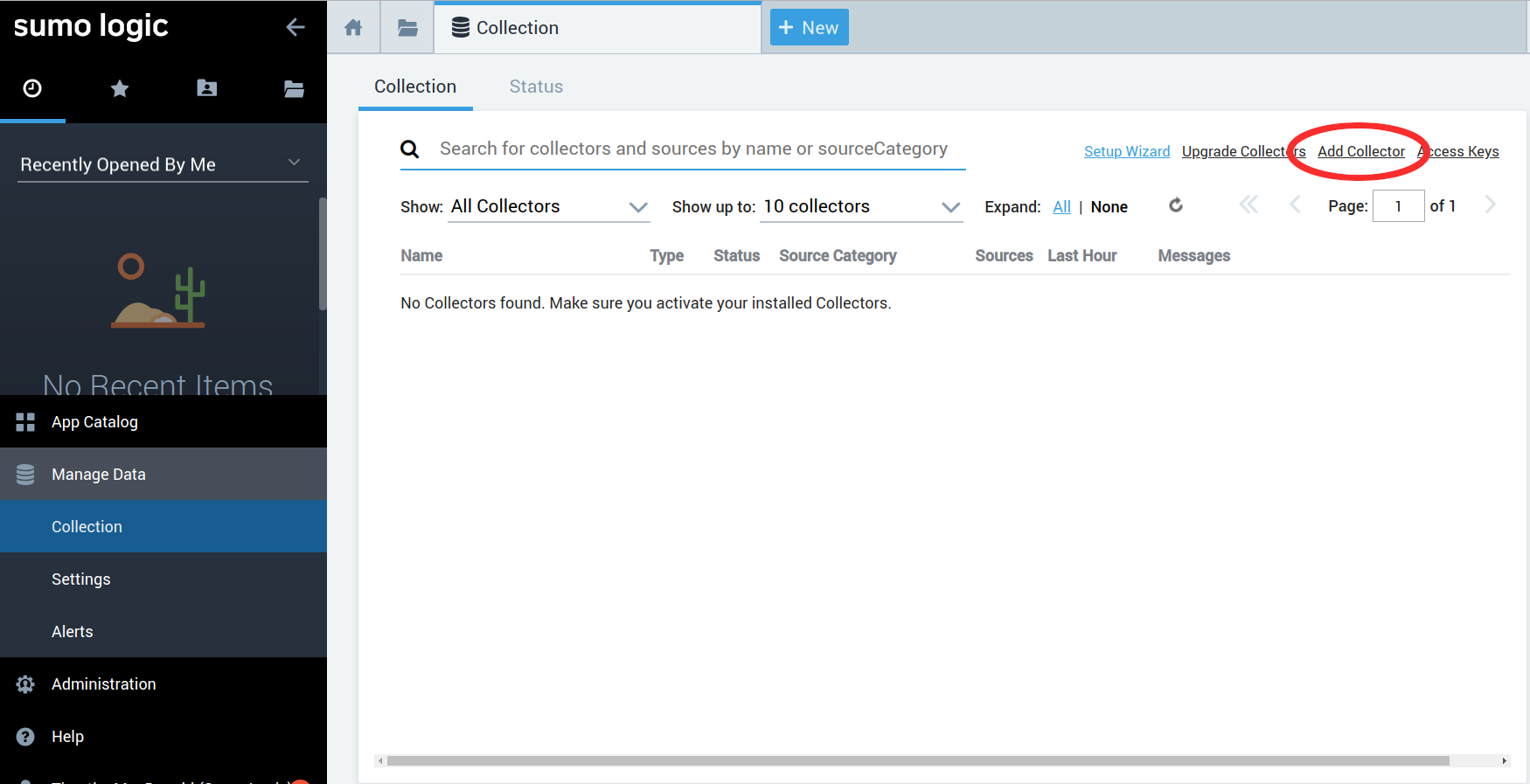
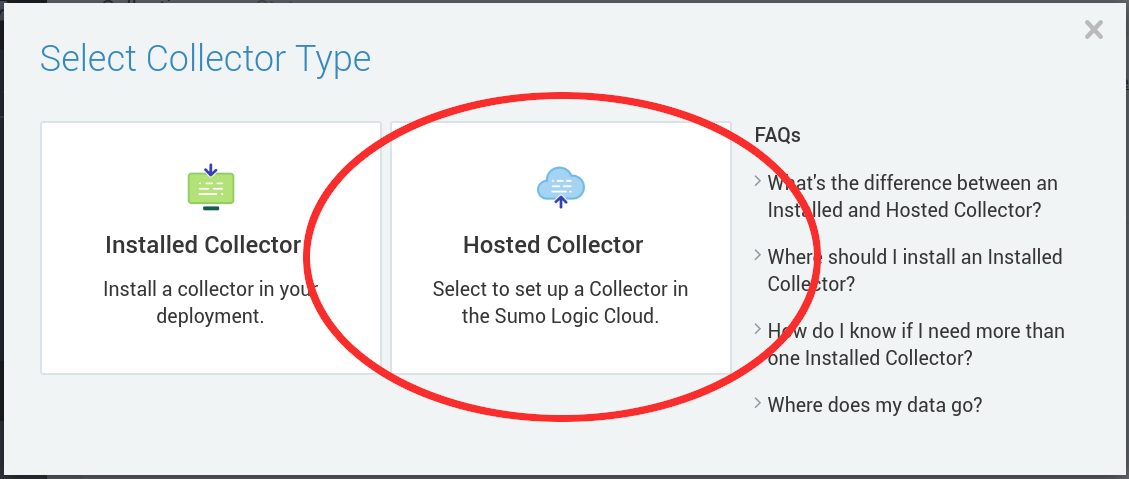
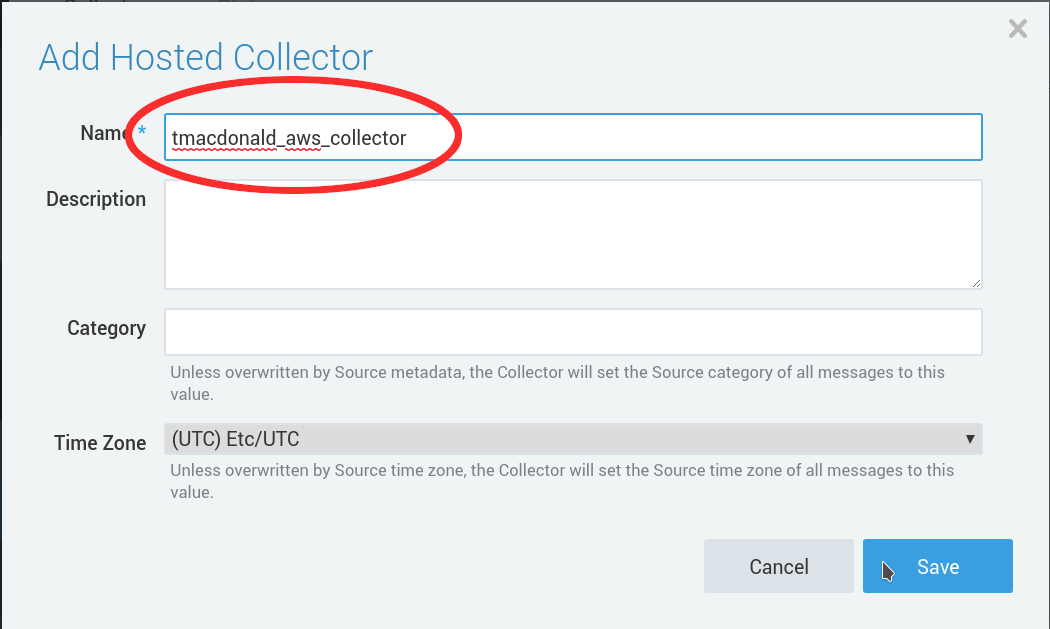
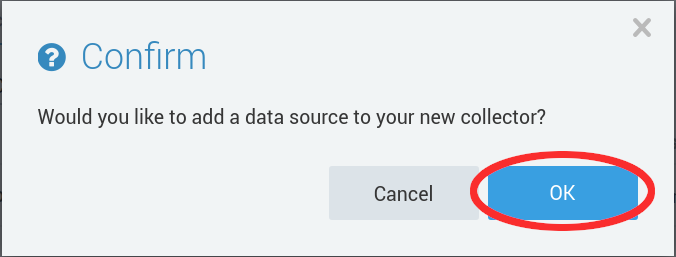
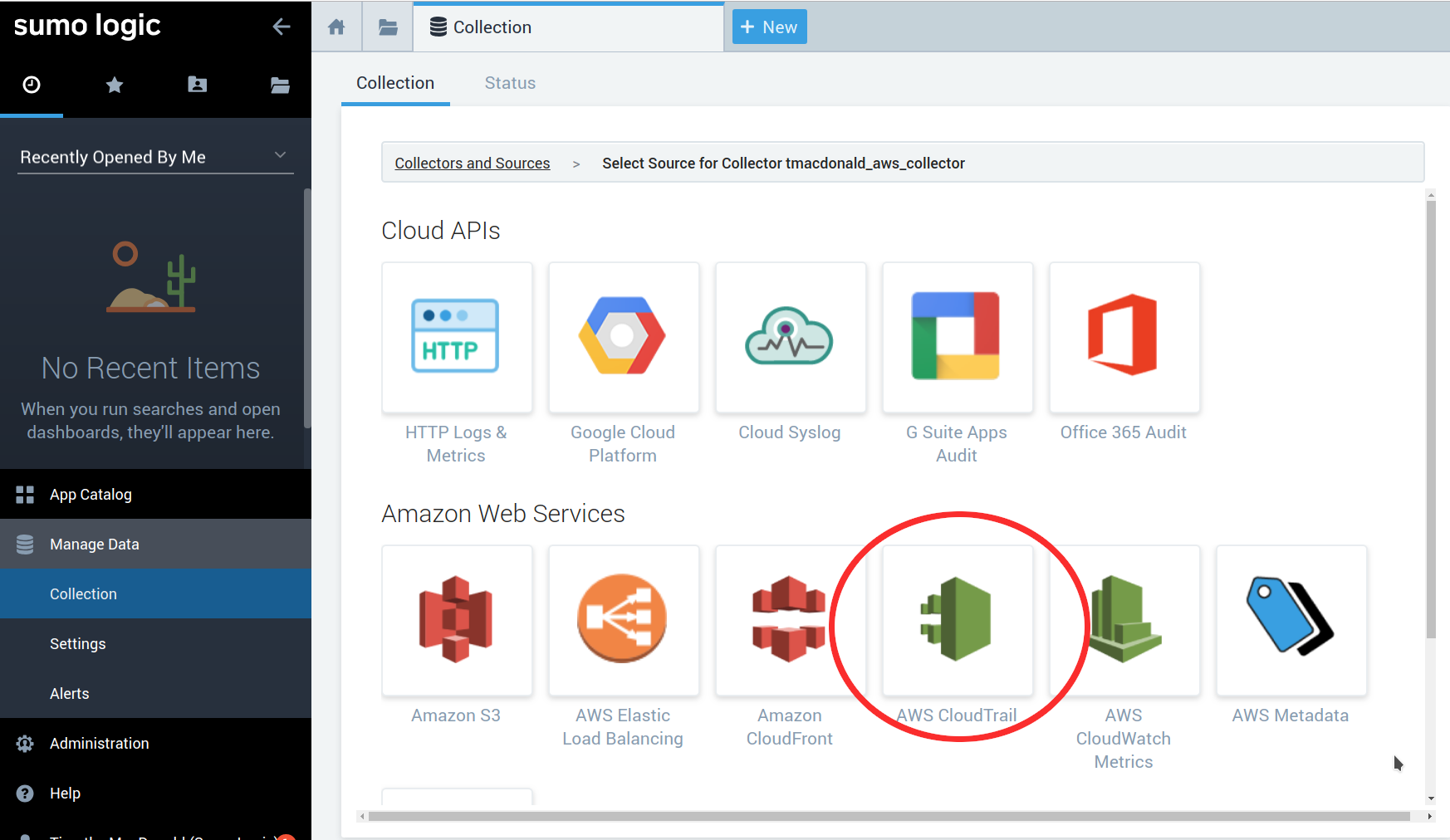
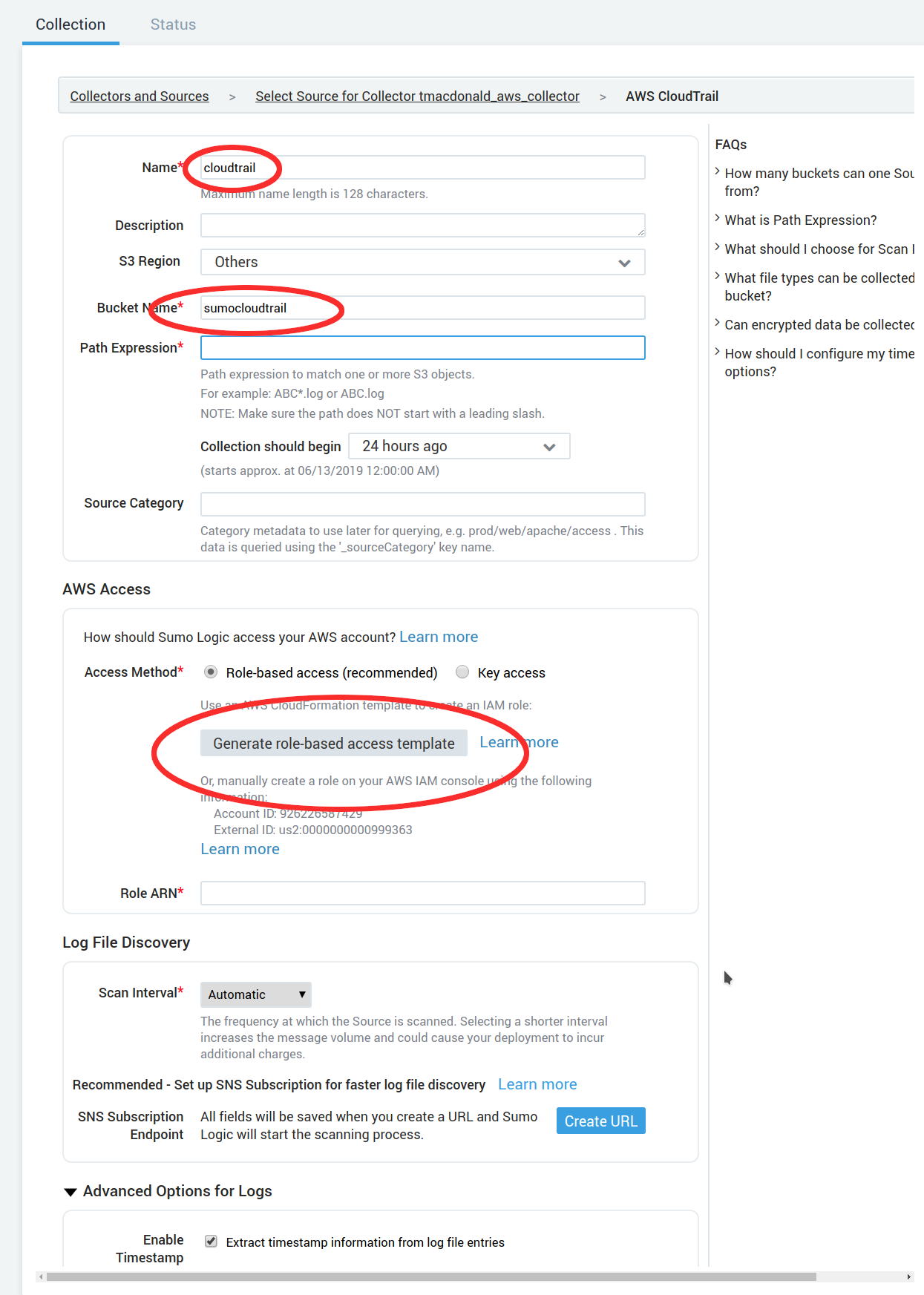
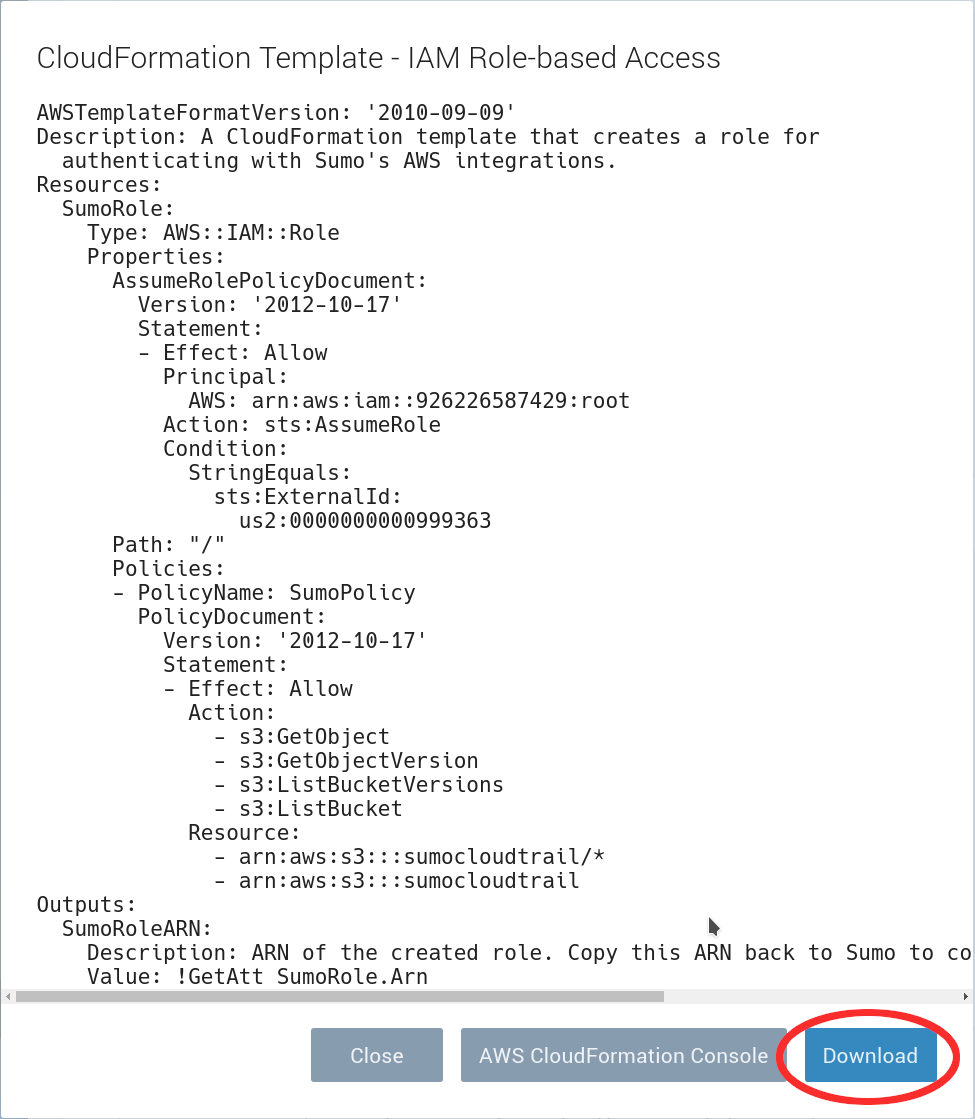
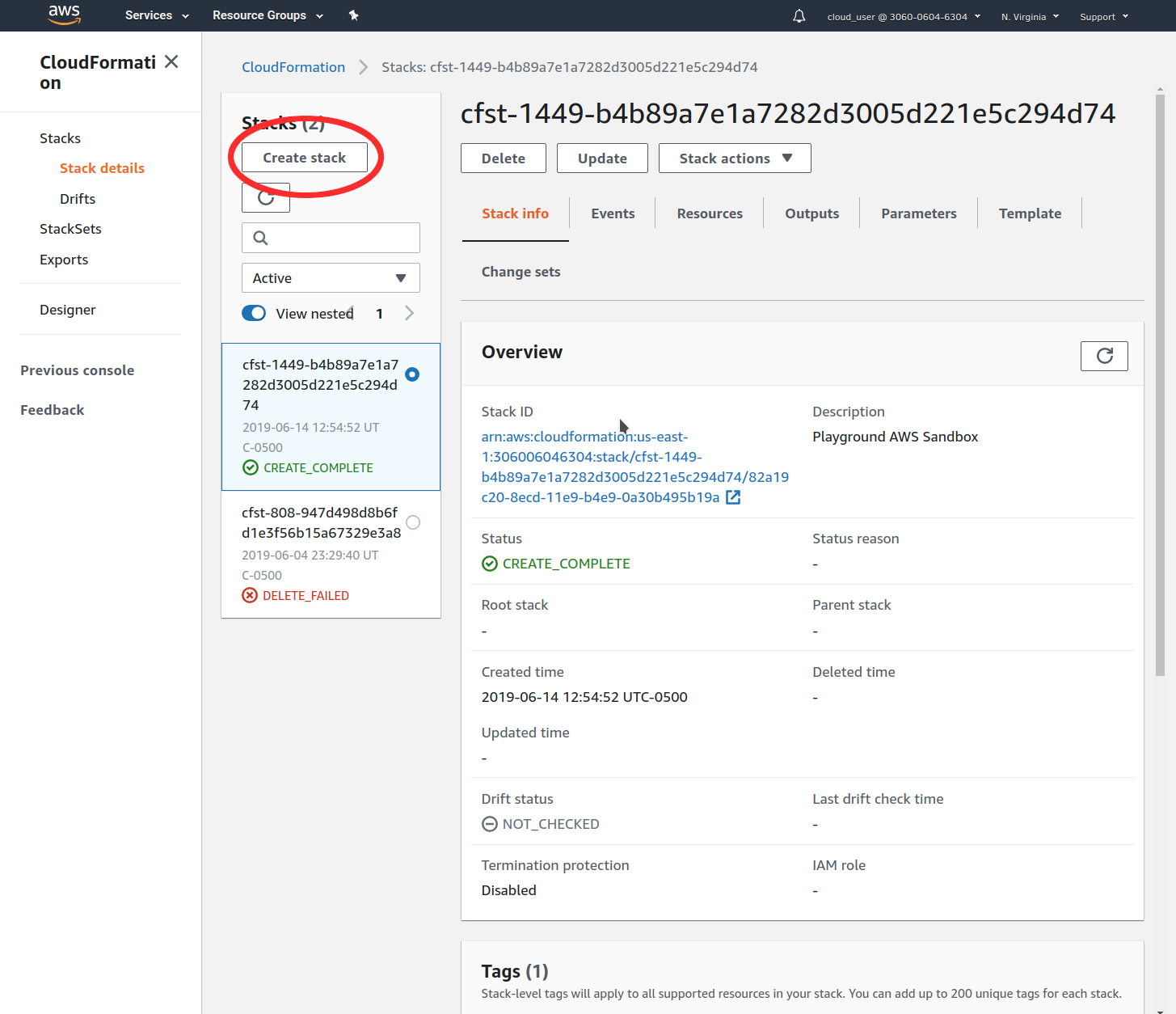
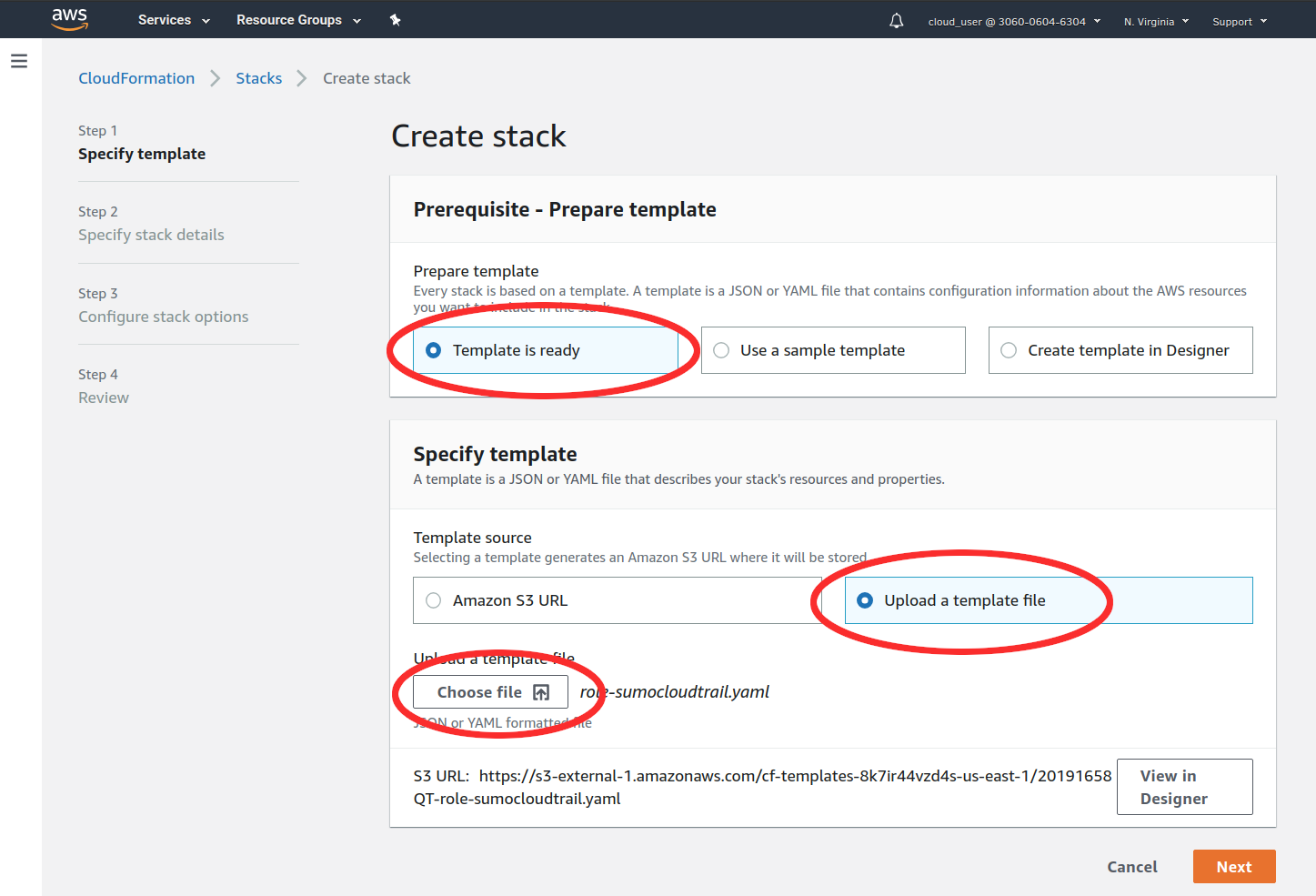
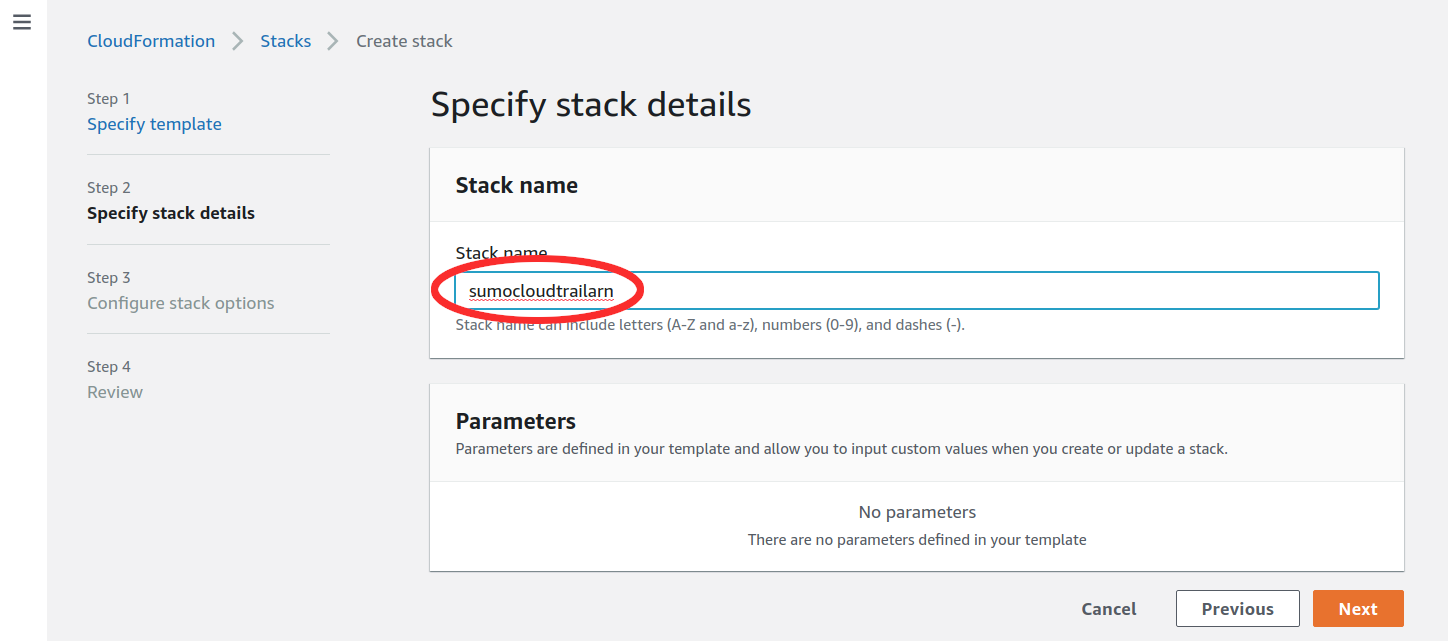
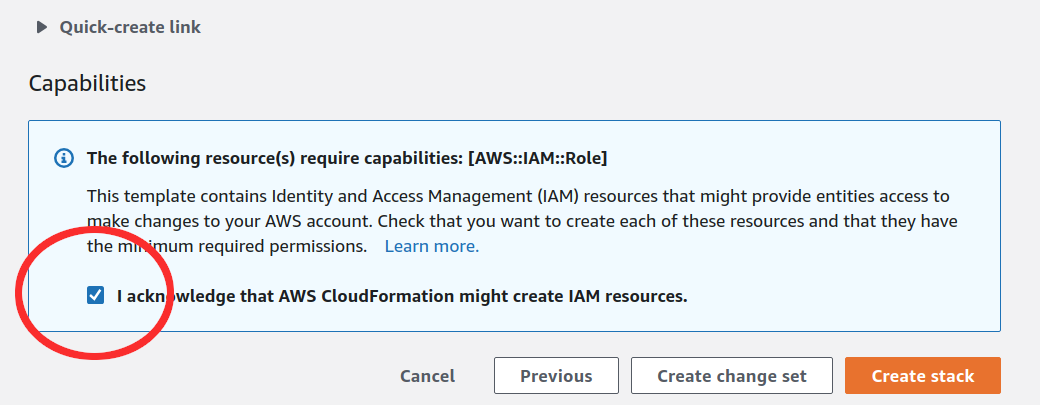
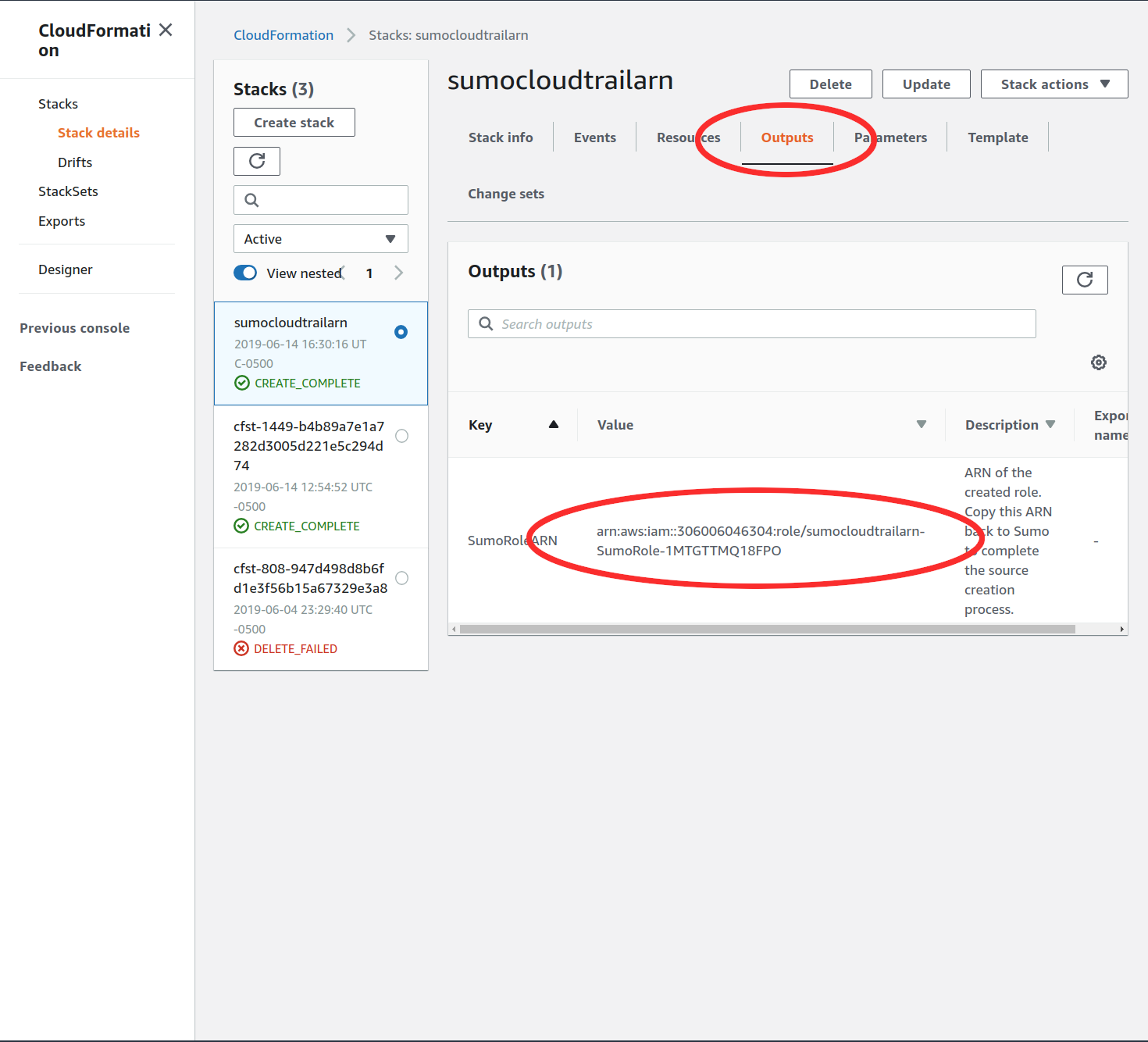
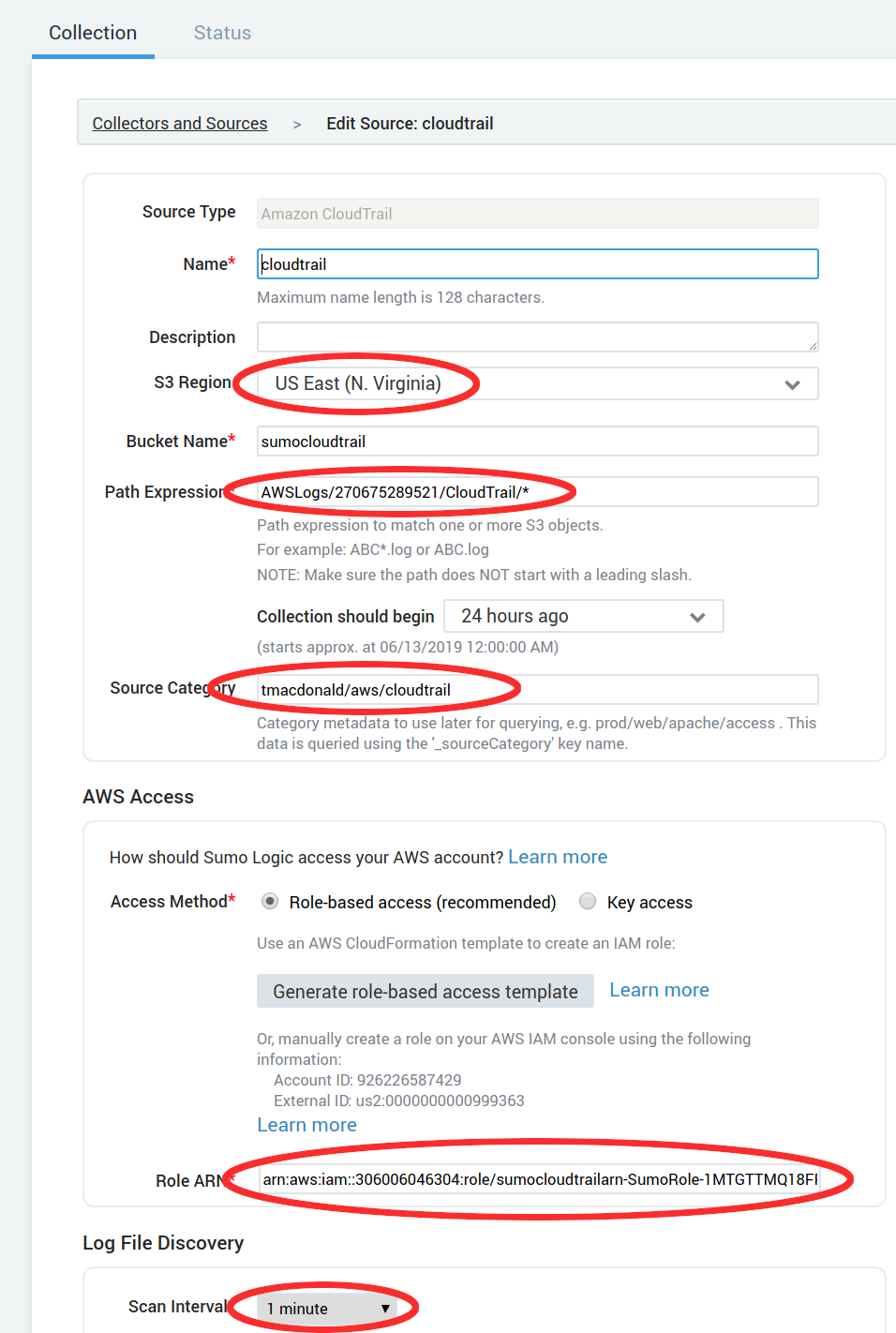
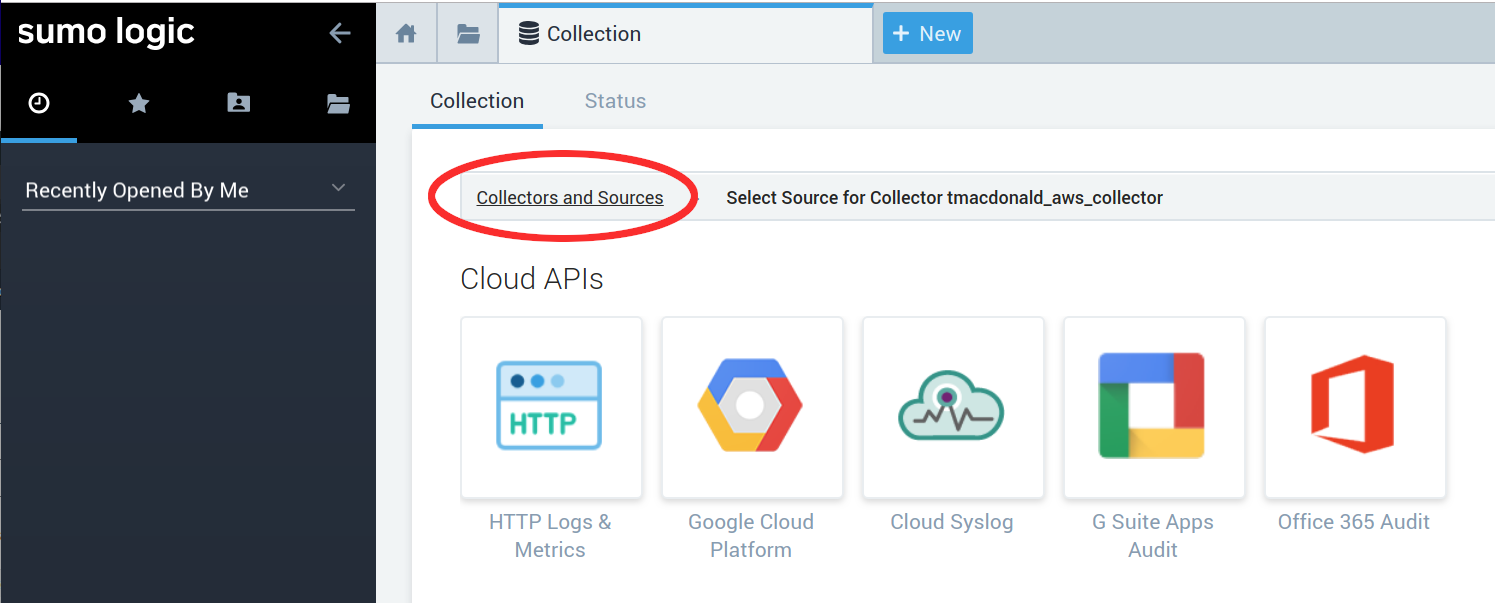
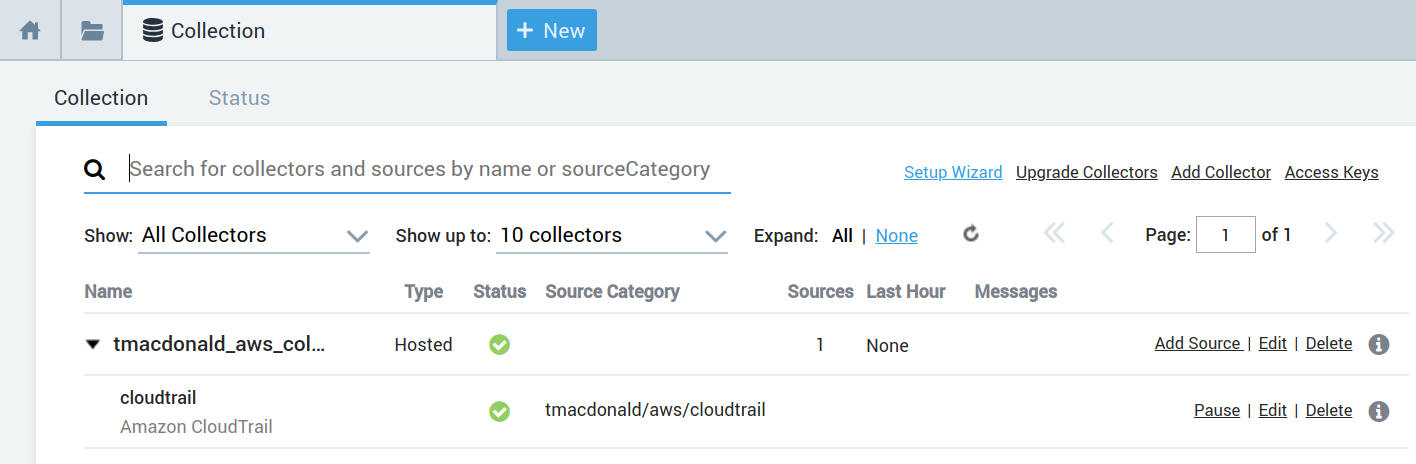
<https://help.sumologic.com/07Sumo-Logic-Apps/01Amazon_and_AWS/AWS_CloudTrail>

## Configure a trail and S3 bucket

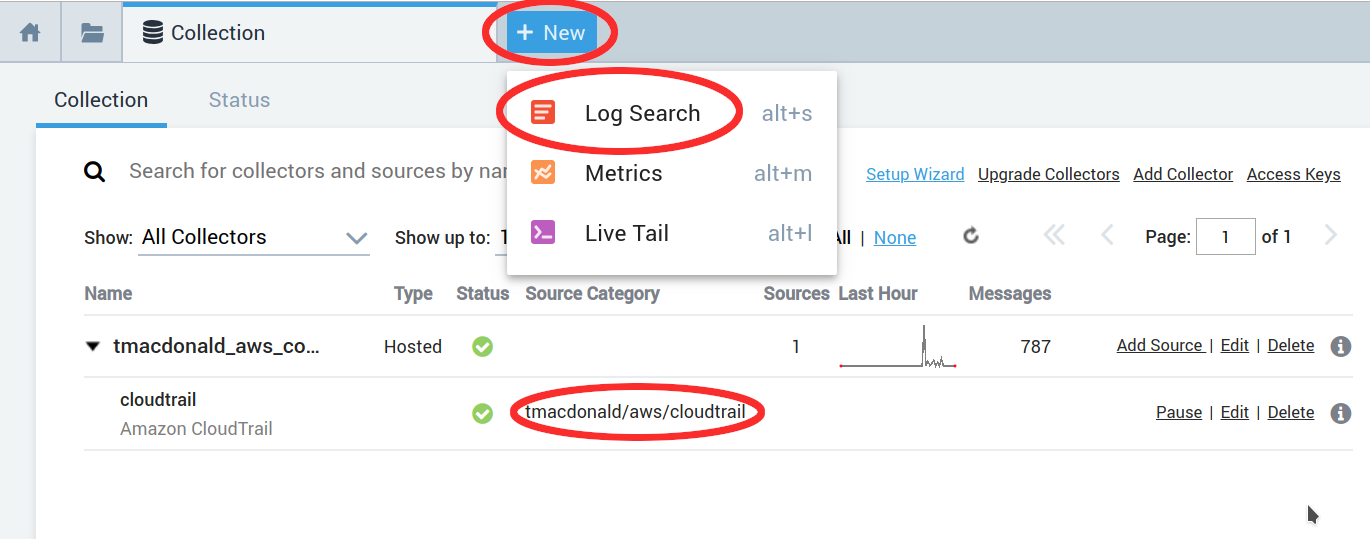
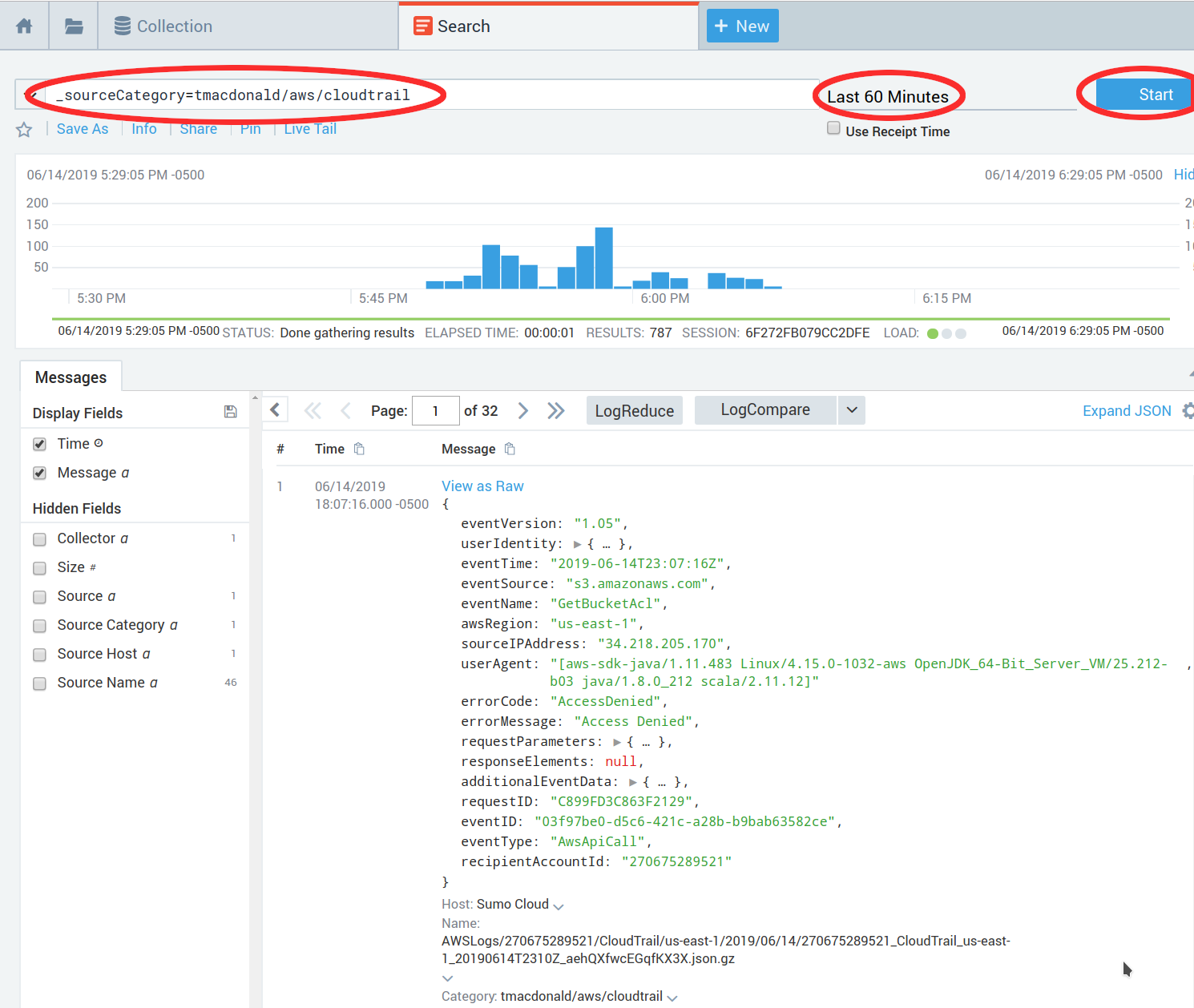
* Login to the AWS Console, choose your region, and select the Cloudtrail service
* Click the “Create Trail” button
* Fill in the trail name and bucket name, making sure to indicate that a new bucket should be created. 
* Click “create” and record the name of your bucket, which will be used later in this lab.

## 

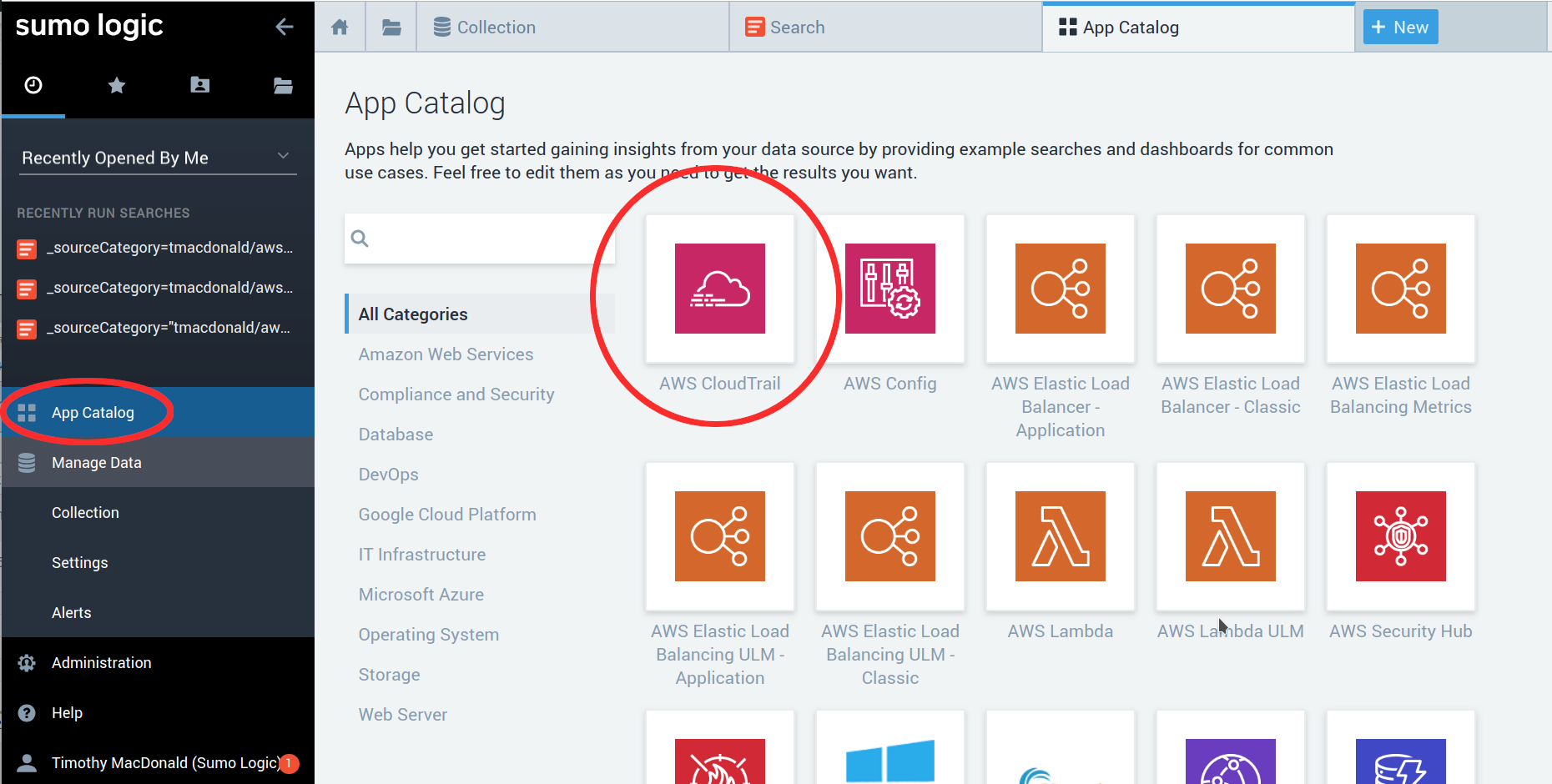
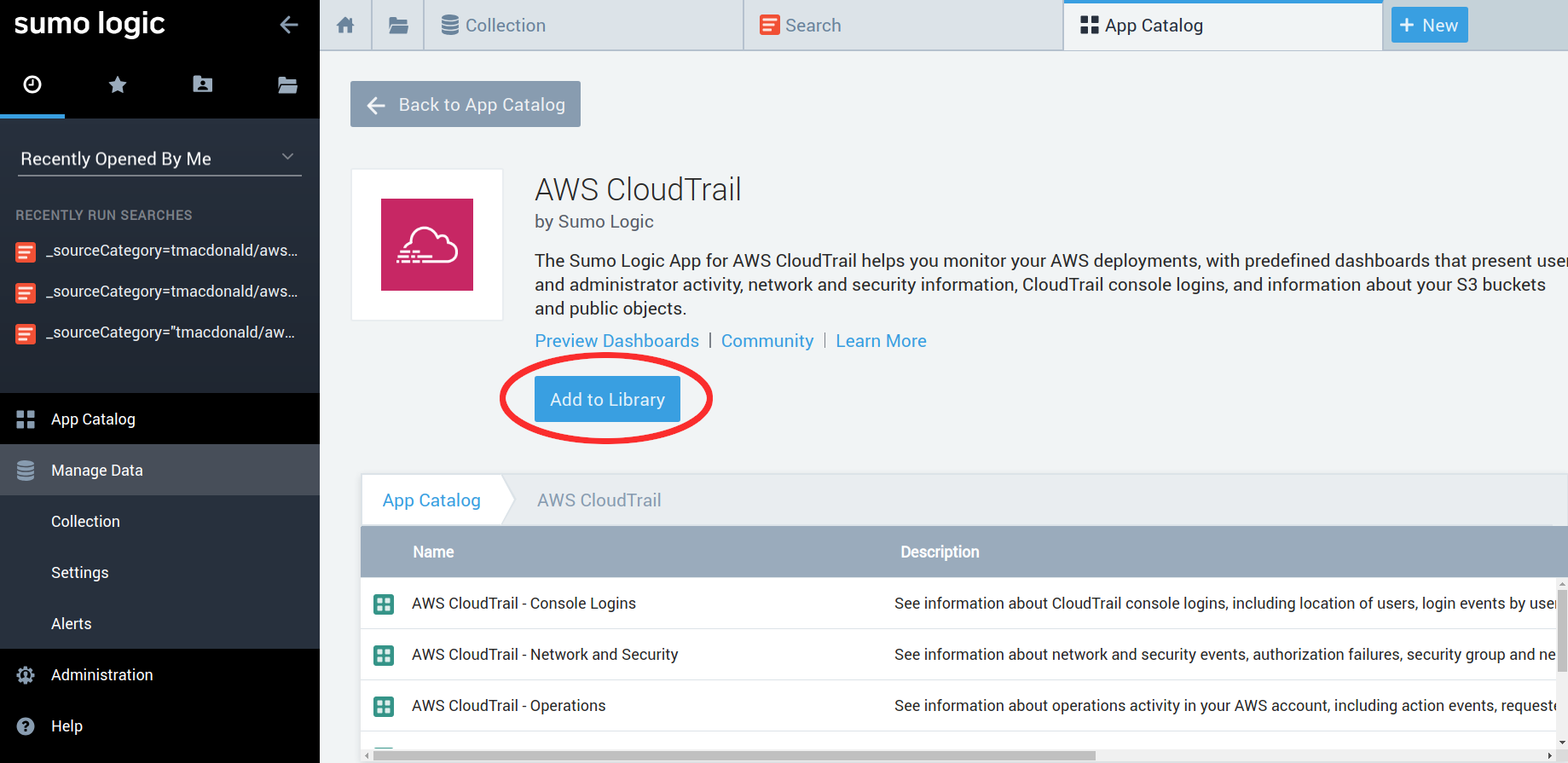
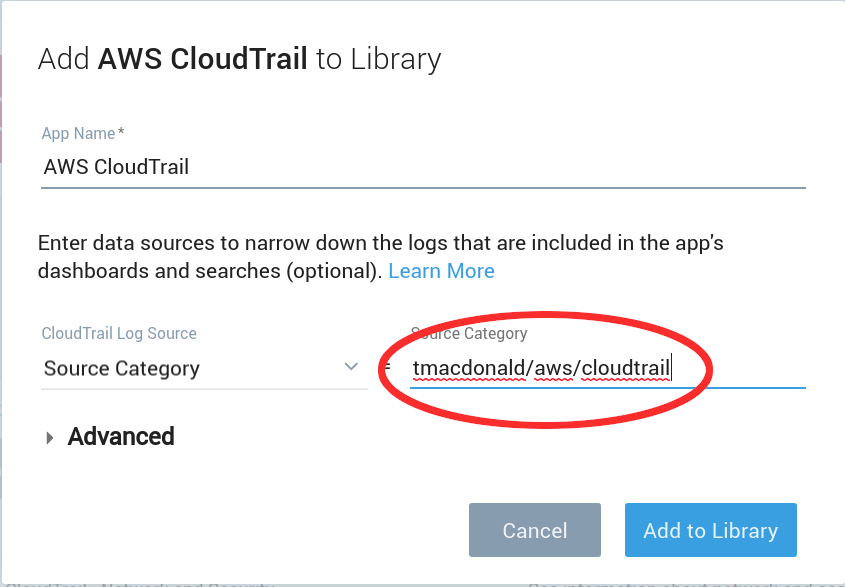
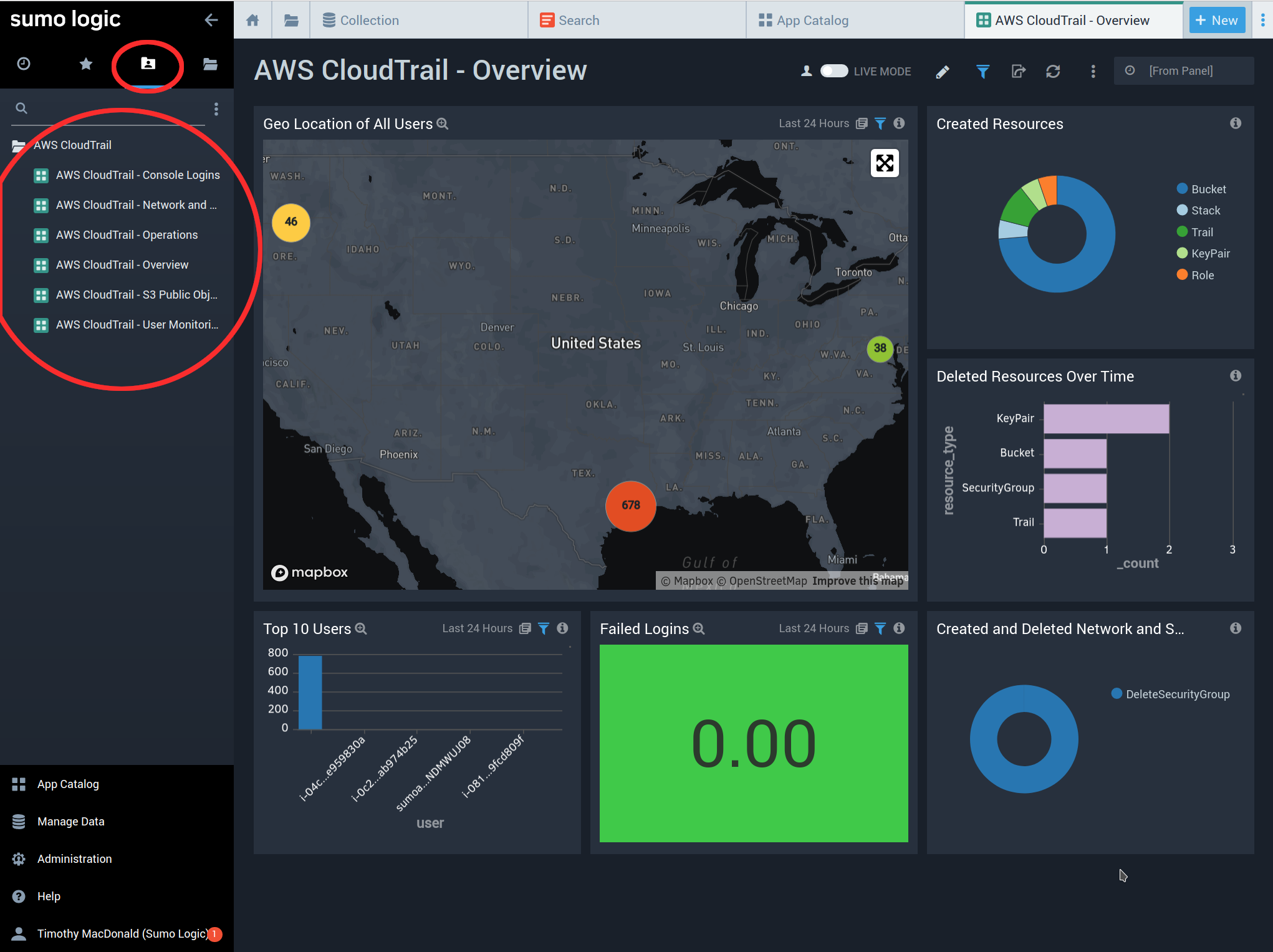
## Configure A Sumo Logic Collector and Source to ingest Cloudtrail Data

* Login to your Sumo Logic account. Select the “Collection” screen from the bottom left hand section of the screen, under the “Manage Data” menu. 
* The “Collection” screen is where collectors and data sources are defined within Sumo Logic. Depending on your environment you may see other collectors and sources already listed here or the screen may be blank. In this exercise you will be creating your own hosted collector and then a cloudtrail source under that collector. Choose “Add Collector” from the top right corner of the screen.
* To collect logs from AWS services we need to create a “hosted collector” which will allow Sumo Logic to connect directly to AWS without the need for an intermediary agent. 
* Enter a name for your collector and click “Save”. This can be anything but should be descriptive. Remember also that collector names must be unique within the same Sumo Logic tenant. Since you may have classmates also adding similar collectors you may wish to add your name to this string to ensure uniqueness. 
* Now we must add a cloudtrail source to this collector. Choose “Ok” when asked if you want to configure a source. 
* Next you will be presented with a list of source types that you can add. Choose “AWS Cloudtrail.”
* Now we need to give Sumo Logic permission to access the S3 bucket. The easiest way to do this is to use a CloudFormation stack to create a Role ARN for us. First enter a source name (something descriptive such as “cloudtrail” will be fine. Then, using the bucket we created in the previous section of this lab populate the “bucketname” field. This will allow us to click the “Generate role-based access template” button. Click that button now. 
* Choose “Download” to download the provided CloudFormation template. 
* Open up the AWS CloudFormation console and choose “Create Stack”
* To create the stack choose “Template is ready”, “Upload a template file”, then choose the template file we just downloaded from the Sumo Logic interface. Click “Next”.
* Give your stack a name and click “Next.”
* For the next page “Configure stack options” you can safely leave the options unchanged and click “Next”.
* Finally, review your stack and acknowledge that this stack might create IAM resources. Click “Create Stack”.
* Once the stack creation is complete, click on the “Output” tab and copy the SumoRoleARN to your clipboard. We will be pasting this into the Sumo Logic source definition in the next step.
* Return to the Sumo Logic UI and continue populating the Cloudtrail source that we started earlier. For the S3 region choose the region that your bucket resides in. If your region is not listed choose “other”. For the path expression you must enter the path to your cloudtrail logs within the bucket you created. Your path may vary but there should be NO leading slash and you should end with a wildcard as shown. Populate the “SourceCategory” field with an appropriate string to tag the data from this source. Paste the role ARN into the provided box. Finally select a 1 minute” scan interval and save the source.
* We’re all done adding sources for now so select click on “Collectors and Sources” so that we can review our source. 
* We should now have returned to our main list of collectors and you should be able to see your collector and source listed. It will take a few minutes for data to start populating into Sumo Logic. 

## View the Raw Log Data Ingested by your Cloudtrail Source

* Now that the cloudtrail data is ingesting into Sumo Logic we can view the raw log data by opening up a new log search. First make a note of the Source Category you chose. Then click on the “New” button at the top of the screen and click on “Log Search”. 
* On the log search page we are presented with a search box. Populate the search box as shown, being sure the replace the example source category with the one you specified in your cloudtrail source. Choose “Last 60 minutes” from the dropdown and click “Start”. This will retrieve all logs that match the specified source category tag and timeframe. Note that the timeframe is in reference to when the log entries were created by cloudtrail, not when they were ingested by Sumo Logic. If no new cloudtrails have been created in the last 60 minutes then you will get no results. If this happens you may want to expand the timeframe of your search. 

## Install the Sumo Logic Cloudtrail App (Dashboards)

* Now that we’ve configured log ingestion and viewed the raw log data it’s time to install the Sumo Logic Cloudtrail app. Sumo Logic apps are free and provide pre-built content in the form of dashboards and searches. Click on “App Catalog” on the left of the Sumo Logic UI. This will bring up a list of available apps. The first app in the list should be “AWS Cloudtrail”. Click on that app. 
* Clicking on the “AWS Cloudtrail” app will bring up an overview of the contents of the app as well as the ability to install the app. To install the app click the “Add to Library” button. 
* Now we have to tell the app how we tagged our cloudtrail source so that it knows what data to visualize. Enter your source category tag here and click “Add to Library”. 
* Once your app is finished installing you can open it by clicking on your personal folder, which is in the black sidebar on the top left of the UI. Your personal folder contains all of the content you have either installed or created in Sumo Logic. You should see a folder there called “AWS Cloudtrail” which, when opened, contains a variety of dashboards. Feel free to open and explore these dashboards by double clicking on them. Please do note however that some panels may not be populated or heavily populated depending on how active your AWS environment it. 
* There are additional apps available for cloudtrail. Try installing the “PCI Compliance for AWS Cloudtrail” app and the “Threat Intel for AWS” app. Note that the Threat Intel app will ask for addition types of data which we haven’t ingested. It’s ok to leave those fields blank when installing the app (or have a go at ingesting the requested data.) You can read about ingesting the VPC Flow and ELB logs requested by that app from the following links:

<https://help.sumologic.com/07Sumo-Logic-Apps/01Amazon_and_AWS/Amazon_VPC_Flow_Logs>

<https://help.sumologic.com/07Sumo-Logic-Apps/01Amazon_and_AWS/AWS_Elastic_Load_Balancing>