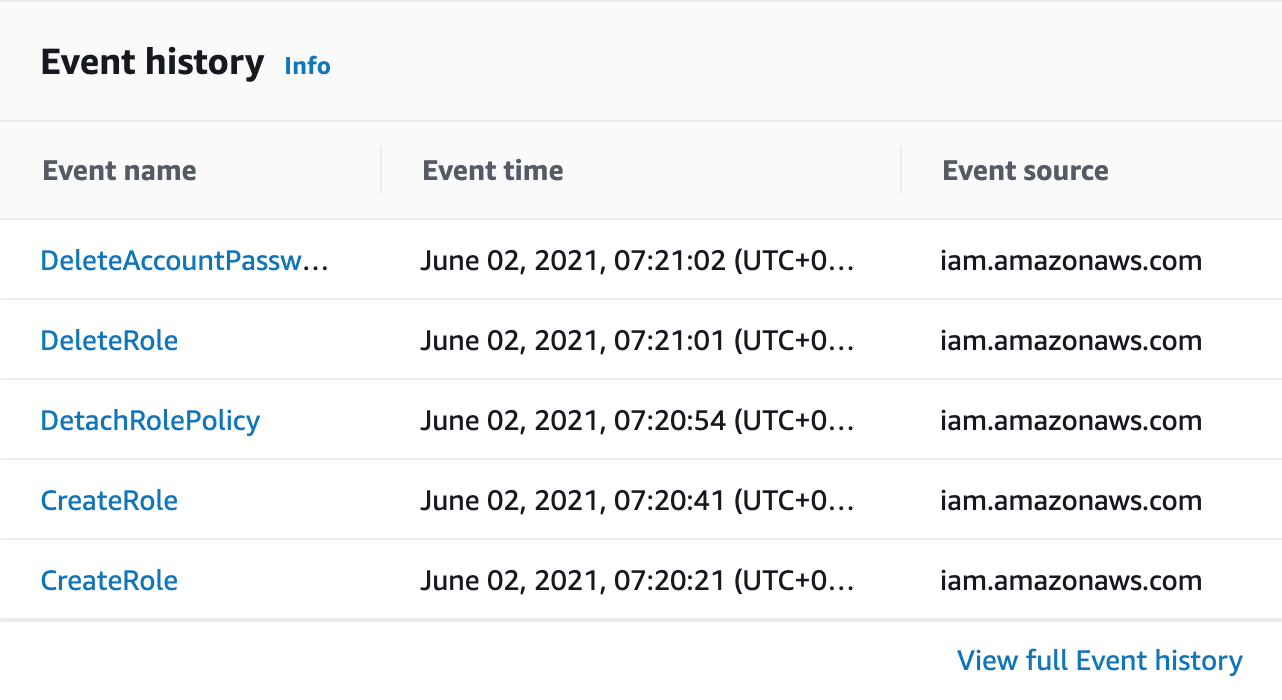
**Generating and Viewing Events**

### Introduction

After turning on CloudTrail and creating a Trail, viewing events (either from S3 or the CloudTrail console directly) is not very informative until meaningful things actually take place. Normally, this happens during the course of regular usage. In this Lab Step you'll use the console to perform several tasks, then verify that CloudTrail is indeed capturing them to a log file and delivering that log file to S3. Note that most AWS services are supported by CloudTrail. This Lab Step will tap into a few services that you are likely already familiar with, but realize they could be most any service and most any region. Further, although the console is used for simplicity sake, events originating with the AWS API, CLI or even other AWS services can also be captured by CloudTrail.

### Instructions

1. Navigate to the AWS CloudTrail console. The **Event History** shows the events already captured by CloudTrail, such as the CloudTrail and S3 bucket creation:



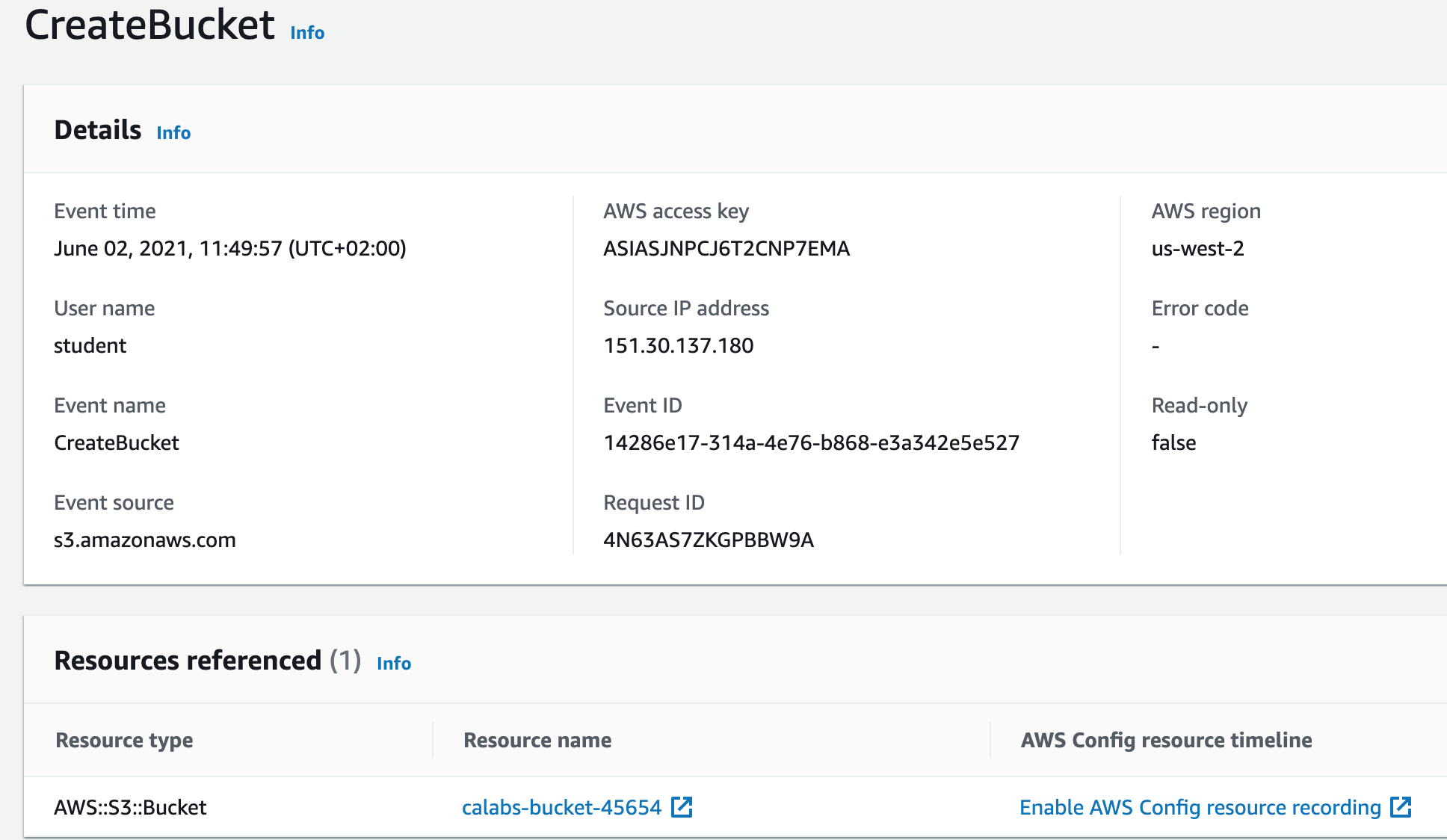
Note: This is not an exhaustive listing of events. Your history will differ.

Read the note in the blue bubble at the top of the screen. Only create, modify and delete activity will be captured by CloudTrail. Hence, if you list and read your S3 bucket, you won't see that activity from the CloudTrail console here.

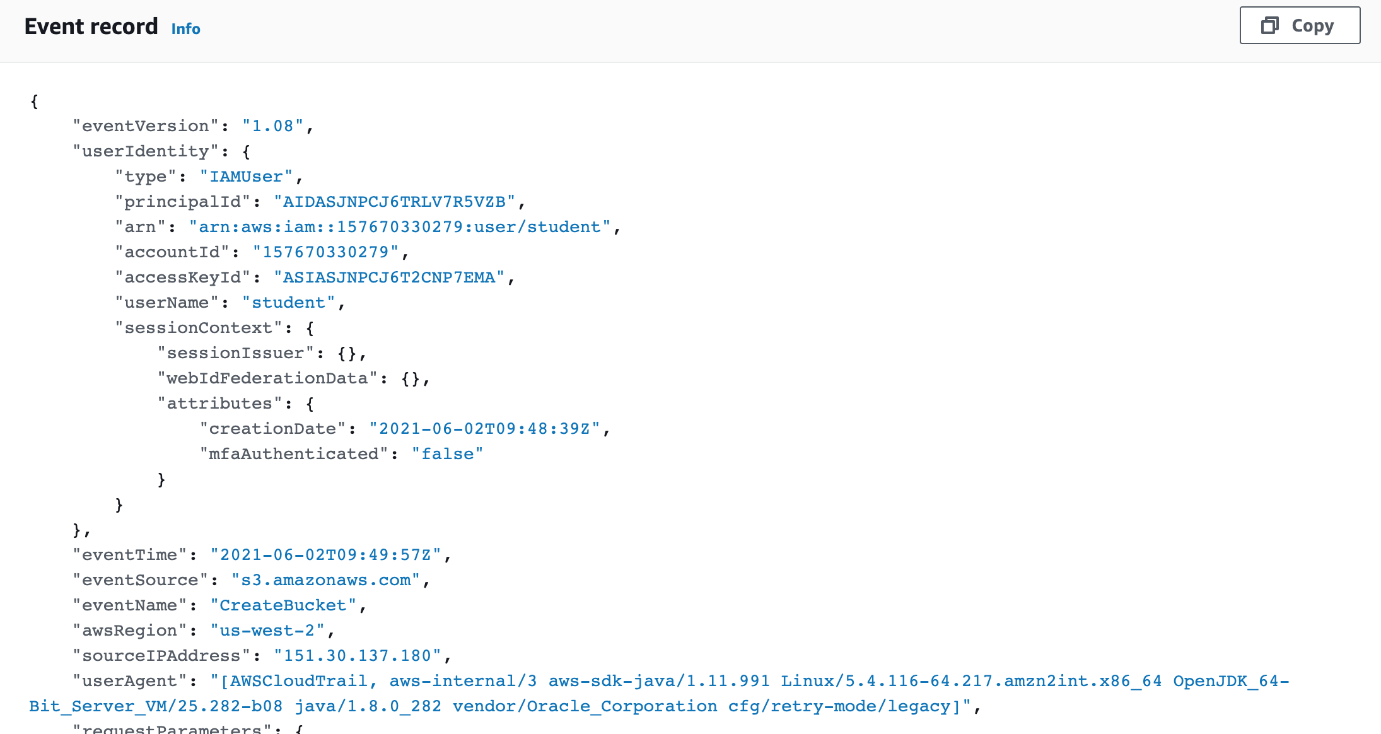
In addition to the date/time stamp, you'll notice the **Event name**, **Resource type** and **Resource name**. Quickly skimming these three columns will provide you with a good understanding of activity on your account. For example, with a quick glance you can tell when CloudTrail was enabled, and when the S3 bucket it will transfer its logs to was created.

**Important!** Events captured by CloudTrail show up pretty quickly in the **Recent events**, but it is not in real-time. Although you can refresh the API history, there is still a delay from the time of the event until the time you can view it in the console of up to 15 minutes. Unfortunately, there is no way to speed up the occassional delay. However, you can continue with this Lab Step and return to the API activity periodically to confirm CloudTrail is enabled and capturing events.

2. Click on an event and spend a few minutes expanding and viewing the events already logged. For example, if you attempted to create an S3 bucket you will see something similar to:



3. Scroll down to the **Event record** section. The JSON for this event is displayed:



If you navigated in S3 to the bucket CloudTrail is configured to deliver logs to, you could eventually find the JSON for this (and other) events. This is an integrated method for viewing JSON tied to a specific CloudTrail event. After completing the lab, those interested in more information should see the [CloudTrail Record Contents](https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-event-reference-record-contents.html) in the AWS Documentation for details of every entry you might find in the JSON.

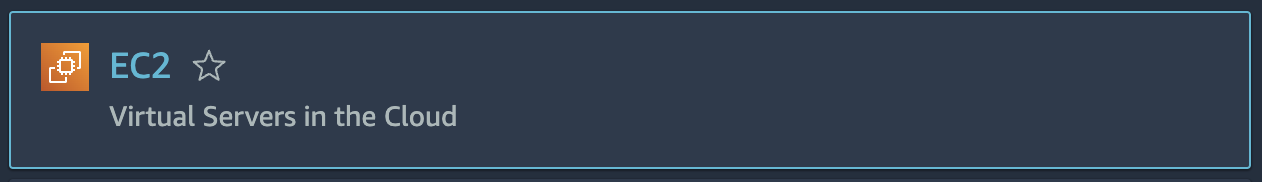
4. Navigate to [S3 buckets](https://s3.console.aws.amazon.com/s3/buckets?region=us-west-2)and select the bucket you created (calabs-bucket-1234 in our example). You will see the CloudTrail prefix you configured earlier as a folder.

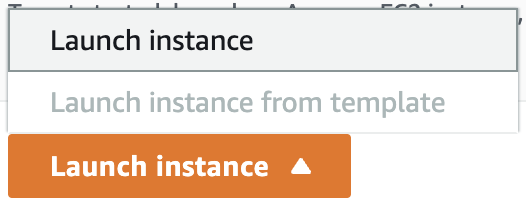
5. Click **CreateFolder** and enter janedoe for the name. Navigate into the new S3 folder.

6. Click **Upload**. Select a few files from your local file store to upload. (They can be anything, perhaps a few images and/or text files.) Click**Upload** when ready.

7. Navigate back to the top-level of [S3 buckets](https://s3.console.aws.amazon.com/s3/buckets?region=us-west-2). You should see the bucket you created when enabling CloudTrail. Click **Create Bucket**. Name it something unique of course, such as the name used earlier but increment the number at the end (calabs-bucket-8 in our example). Click **Create** when ready. Now that you have performed a few basic S3 tasks, you will perform EC2 related tasks. (Again, since CloudTrail supports most AWS services, S3 and EC2 activity is just an example to learn from. Other services could have been used.)

8. In the AWS Management Console search bar, enter ec2, click the **EC2** result under **Services**, and click **Launch instance** > **Launch instance**:

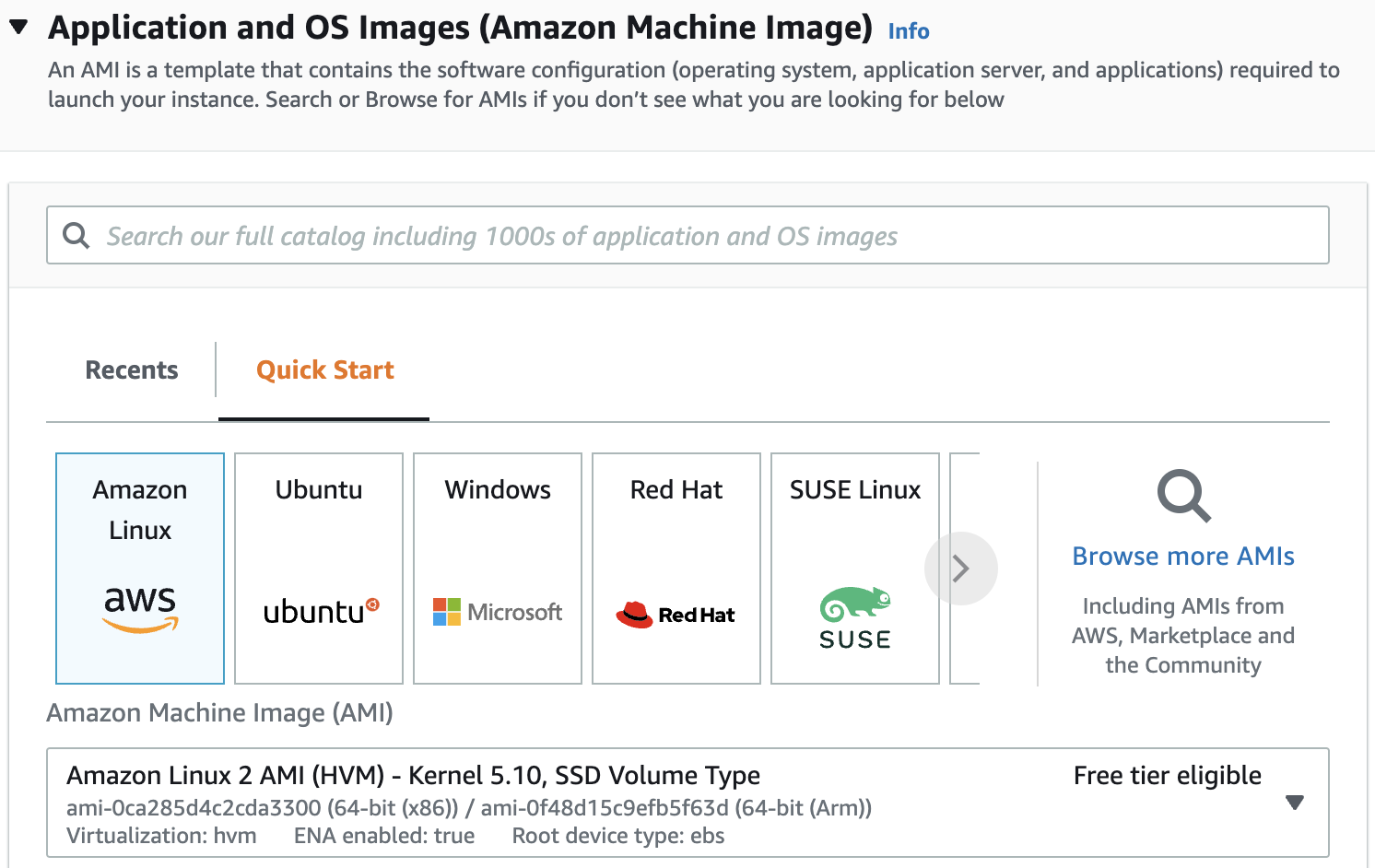
[](https://s3.console.aws.amazon.com/s3/buckets?region=us-west-2)

[](https://s3.console.aws.amazon.com/s3/buckets?region=us-west-2)

Enter the following and leave the remaining defaults:

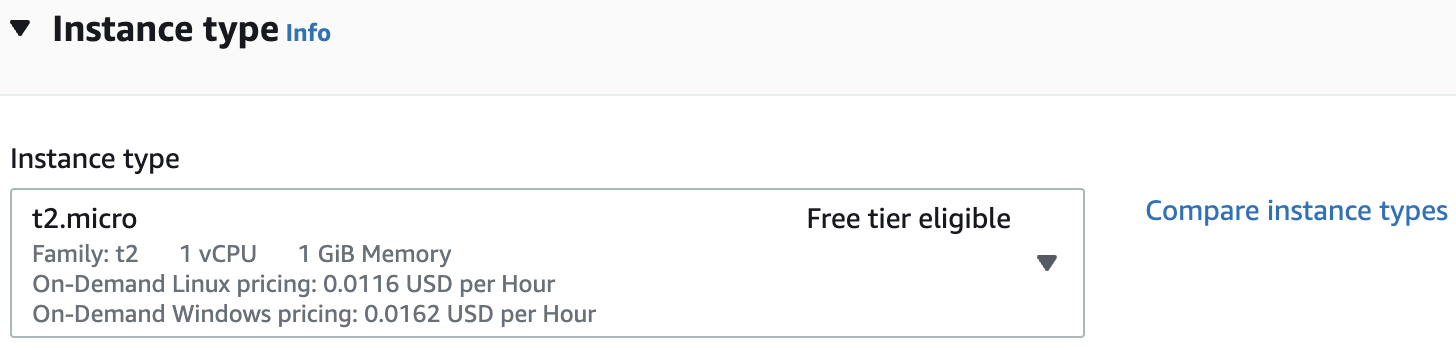
**Application and OS Images (Amazon Machine Image)**:

* **Quick Start**:**Select** the **Amazon Linux**

[](https://s3.console.aws.amazon.com/s3/buckets?region=us-west-2)

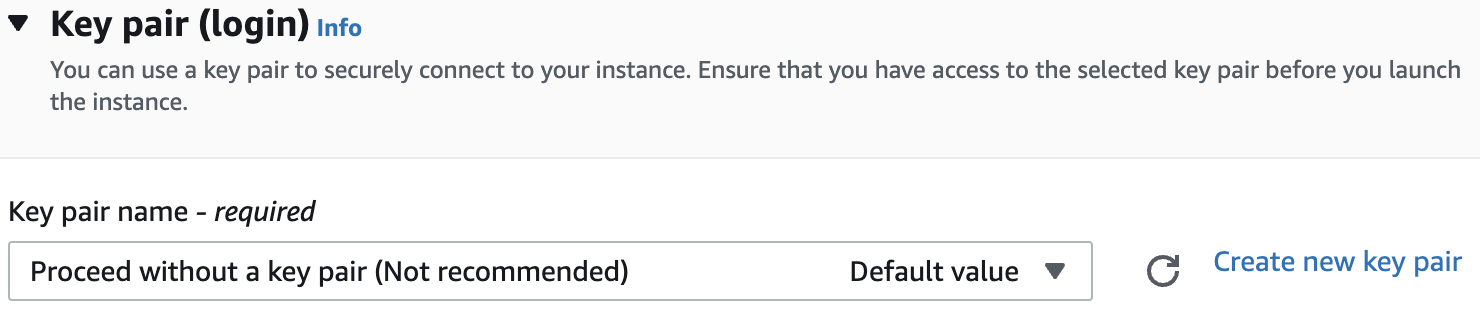
**Instance Type**:

* **Instance Type**: Ensure**t2.micro**is selected

[](https://s3.console.aws.amazon.com/s3/buckets?region=us-west-2)

**Key pair**:

* Select **Proceed without a key pair**

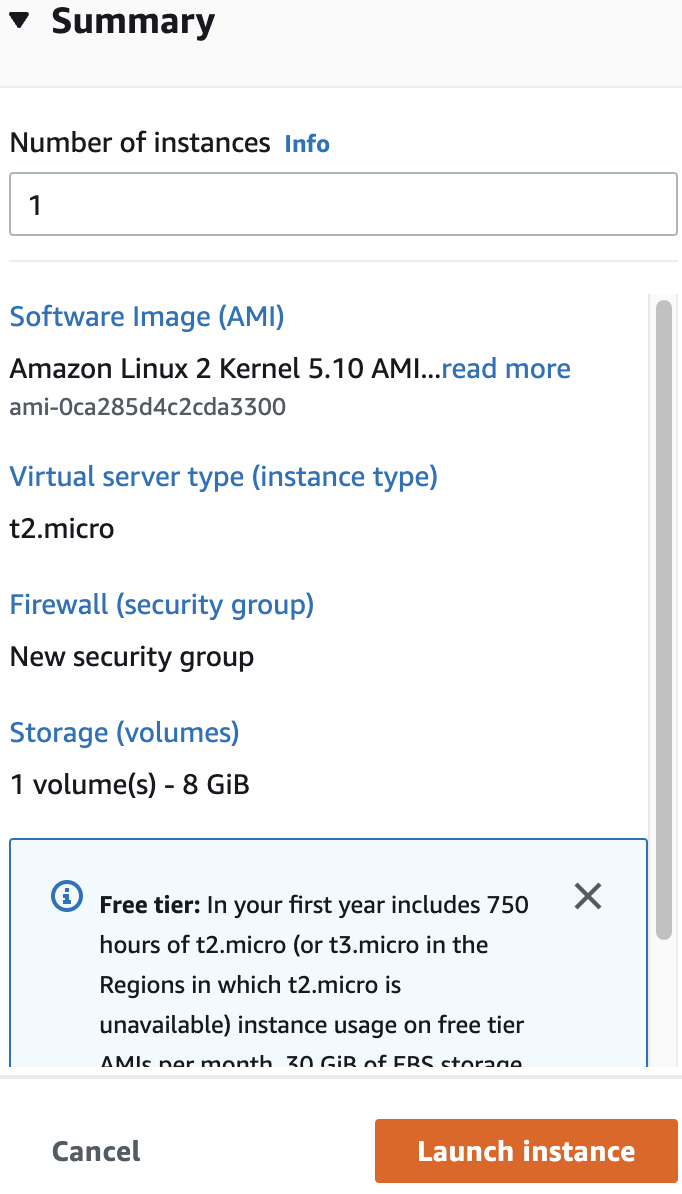
[](https://s3.console.aws.amazon.com/s3/buckets?region=us-west-2)

**Configure Storage:**

* Although you could configure your instance for additional EBS storage (which would generate events for CloudTrail to capture) none of that matters for the purposes of this lab

**Summary**:

* Review configurations
* Click **Launch instance** when ready

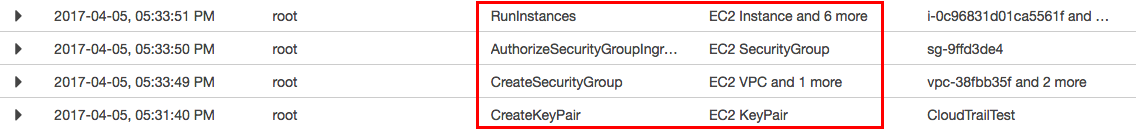
[](https://s3.console.aws.amazon.com/s3/buckets?region=us-west-2)

9. Click **View all instances** (lower right) and notice your Instance transition from a **pending** Instance State to **running**. (This typically takes about 30 seconds.)

10. Return to the [CloudTrail console](https://us-west-2.console.aws.amazon.com/cloudtrail/home?region=us-west-2#/dashboard) and observe the captured events in the **Recent events**. You should notice the following:

* The S3 **CreateBucket** event is captured. (calabs-bucket-8 in our example.)
* The S3 folder creation and file upload is not captured. (It's too granular an event for CloudTrail to capture.)
* The EC2 **RunInstances** event is captured. Further, several events are captured in conjunction with the EC2 Resource Type.
* Reminder: There is a delay from the time the event occurs until it appears in **Recent events**. Although it varies, the typical delay is ~5 minutes, but can be up to 15 minutes. Regardless of the delay, the actual event time stamp adheres to when the event happened, not when it appears in the **Recent events**. If you click refresh a few times and still don't see the events, then grab a cup of tea or coffee and they will be there when you return.

13. Locate the **RunInstances** Event in the **Recent events** section of the console. Notice the events just prior to (below) **RunInstances**:



Even though, for simplicity sake, you launched an instance with simple default values, several events are still associated with spinning up an instance in EC2. As shown here, security keys and a Security Group were created. If you had created an additional EBS volume that would have been captured as well. If you deleted the instance or the empty S3 bucket, that also would trigger events for CloudTrail to capture, etc. Note: You will not see a CreateKeyPair event as shown above because earlier you skipped that step when the instance was launched.

14. Spend a minute or two expanding/collapsing the EC2 events in order to become more familiar with the type of information captured. In our example there is a relatively small **API activity history**, as the trail is new and not that many events have been captured. However, notice the **Filter** on the console that can limit what is displayed based on the attribute (for example, **Event name** or **Resource type**) and a date/time range. A very handy feature indeed when there are thousands of events! Time and interest permitting, try using a filter or two in order to limit the events displayed in the console.

Note: Due to the variable delay for captured events (of up to 15 minutes), if you don't see your events and want to continue with the next Lab Step you can. Return to the CloudTrail**API activity history** later to confirm the events do indeed get logged.

### Summary

In this lab step you used the AWS Console for several common tasks related to EC2 and S3. You learned that some events are captured by CloudTrail and others are not. More importantly, you verified that CloudTrail is indeed working, capturing events and logging to an S3 bucket created earlier. Further, you learned the type of information that is captured by CloudTrail, and how to view that information from the console.