# Search CloudTrail Logs with Athena

## Lab Overview

This lab will demonstrate:

- Create an table with logs from CloudTrail
- Explore logs using Amazon Athena

### Task 1: Create a table with CloudTrail Logs

In this task you will use an Athena and import logs to the table.

1. In the AWS Management Console, on the **Services** menu, click **Athena**.
2. From laboratory material copy a content of create_table.sql file.
3. Copy the content into Query Editor in Athena console
4. Edit a first line "CREATE EXTERNAL TABLE" and set the name of the table with your student number (ex. Cloudtrail_student11).
5. Click **Run query**.
6. In the navigation pane on the left, in section **Tables** a new table "cloudtrail_studentX" should appear.
7. Click on the name of the table, you should see a list of elements in the table.

### Task 2: Identify Console login events

You will search for all event of today's login into AWS Console.

8. Copy the content of console_login.sql and paste into Query Editor in Athena.
9. Correct the table name and paste the name of your table.
10. Set the correct eventtime to point to today's date.
11. Click **Run query**
12. Try to find the time where you logged into AWS console for the first time today.

### Task 3: The most active user

In this task, you will investigate who was the most active user today.

13. Copy the content of most_active_users.sql and paste into Query Editor in Athena.

14. Correct the table name and paste the name of your table.
15. Set the correct eventtime to point to today's date.
16. Click **Run query**
17. Who was the most active user today?

## End Lab

Follow these steps to close the console, end your lab, and delete the table.

18. In the navigation pane on the left, in section **Tables,** click on this 3 dots after a name of our table and select **Delete table**.
19. Confirm by clicking **Yes**.