



## Configuring Amazon S3 security settings and access controls

Getting started at an AWS hosted workshop

### ▼ S3 Security Best Practices

#### ▼ Prepare Your Lab

- Attach IAM Role to EC2 Instance
- Connect to the EC2 Instance
- Bucket Name

#### ▼ Lab 1 - S3 Security Exercises

- Require HTTPS
- Require SSE-KMS Encryption
- Restrict Access to an S3 VPC Endpoint
- Use AWS Config Rules to Detect a Public Bucket
- Use Amazon Access Analyzer for S3

#### ▼ Lab 2 - S3 Access Grants

- S3 Access Grants Lab - Initial Setup
- Configure S3 Access Grants for IAM user

#### ▼ Lab 3 - Enabling Malware Protection for S3 by using GuardDuty

- Enabling Malware Protection for S3 for your bucket
- Testing GuardDuty Malware with an object.

#### ▼ Lab 4 - S3 Access Control Lists

- Block Public ACLs
- Configure S3 Block Public Access
- Disable S3 ACLs

#### ▼ Finding S3 access control lists with S3 Inventory

- Enabling Amazon S3 Inventory

#### Setting up Amazon Athena

- Use Amazon Athena to query Amazon S3 Inventory and identify objects with ACL elements

#### ► Use Amazon Athena to query CloudTrail logs and identify S3 requests that depend on ACLs

#### Lab Summary

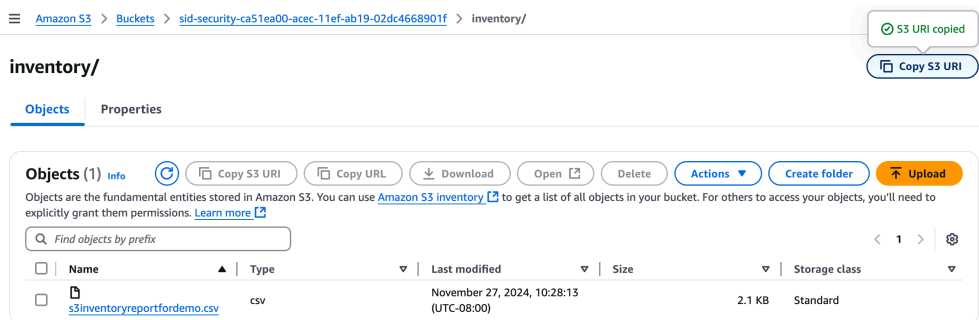
[Configuring Amazon S3 security settings and access controls](#) > ... > [Lab 4 - S3 Access Control Lists](#) > [Finding S3 acc](#)

## Setting up Amazon Athena

From the AWS console in the top search bar, search and select s3.

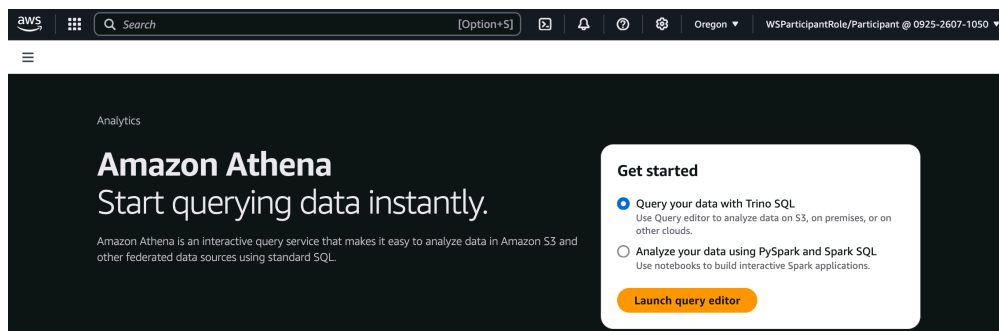
- Click the bucket name starting with sid-security-xxxxxxx and click on the "inventory" prefix.
- Click the Copy S3 URI in the upper right, we will use this later when creating the Athena table.

You should see a screen similar to:

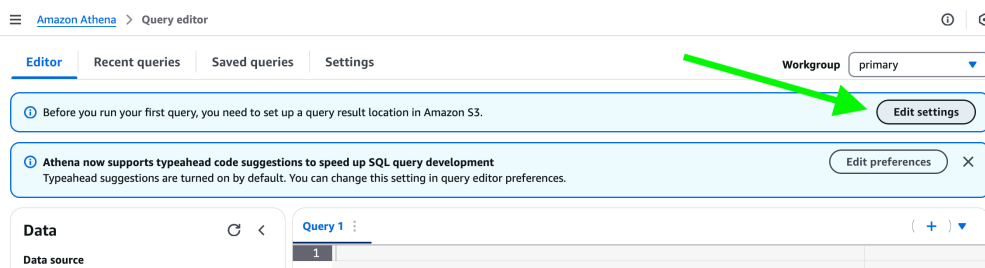


From the AWS console in the top search bar, search and select athena.

- You should see a Get Started page with "Query your with Trino SQL", select the radio button and click Launch query editor at that page to continue, as shown in the following image:



Since this is the first time we are using Amazon Athena, we will need to configure an S3 bucket to store the query results. Next, click Edit settings and Browse S3, we will use the same bucket starting with sid-security-xxxxxxx click Choose and Save



You will end up at the Settings tab, click the Editor tab before we move on.

Now we can create a table in order to query the Amazon S3 Inventory results. We will use the SQL statement below to create a table named s3\_inventory\_csv in the default Athena database. You replace the Amazon S3 Inventory location that we copied earlier in the following LOCATION string with the appropriate values for your configuration. Copy and past the follow into the query window, since this is our first query it should be labeled Query1



```
CREATE EXTERNAL TABLE `s3_inventory_csv` (
  `bucket` string,
  `key` string,
  `version_id` string,
  `is_latest` string,
  `is_delete_marker` string,
  `objectaccesscontrollist` string,
  `objectowner` string )
ROW FORMAT SERDE
  'org.apache.hadoop.hive.serde2.OpenCSVSerde'
WITH SERDEPROPERTIES (
  'separatorChar'=',')
STORED AS INPUTFORMAT
  'org.apache.hadoop.mapred.TextInputFormat'
OUTPUTFORMAT
  'org.apache.hadoop.hive ql.io.HiveIgnoreKeyTextOutputFormat'
LOCATION
  's3://sid-security-xxxx/inventory/'
TBLPROPERTIES (
  'classification'='csv')
```

Note that for the LOCATION field, we use the Amazon S3 Inventory location we copied previously .

Click Run to create the table. You should see a green "Completed" message if you scroll down under Query results.

Once the SQL has been run, there will be a table named, s3\_inventory\_csv in your list of tables. We will use this table/schema to enable us to query the S3 Inventory report in the following section.

The screenshot shows the Amazon Athena console interface. On the left, the 'Data' sidebar displays the 'AwsDataCatalog' data source, 'default' database, and a list of tables including 's3\_inventory\_csv'. The main panel shows 'Query 1' with the SQL code for creating the external table. Below the query, the 'Query results' tab is active, showing a green 'Completed' status bar with metrics: 'Time in queue: 81 ms', 'Run time: 563 ms', and 'Data scanned: -'. A message at the bottom states 'Query successful.'

Before we continue, let's take a minute to look at the schema by clicking on the plus sign next to the table named s3\_inventory\_csv this will expand the selection to show the different columns. If you remember we added two of the ACL fields Object Owner and Object ACL which you can see, along with other fields. If we were to add other fields to the Inventory report we could extend the schema to match as well.

In the next section we will start querying the S3 Inventory Report with Amazon Athena.

[Previous](#)
[Next](#)
