

## **Activity 9 : Working with AWS CloudTrail**

Spurthy Mutturaj

Information Technology, Arizona State University

IFT 562: Cloud Security & Operations for IT

Daniel Wells

Oct 16, 2023

## Activity 9: Working with AWS CloudTrail

**Figure 1**

*A screenshot showing the created CloudTrail.*

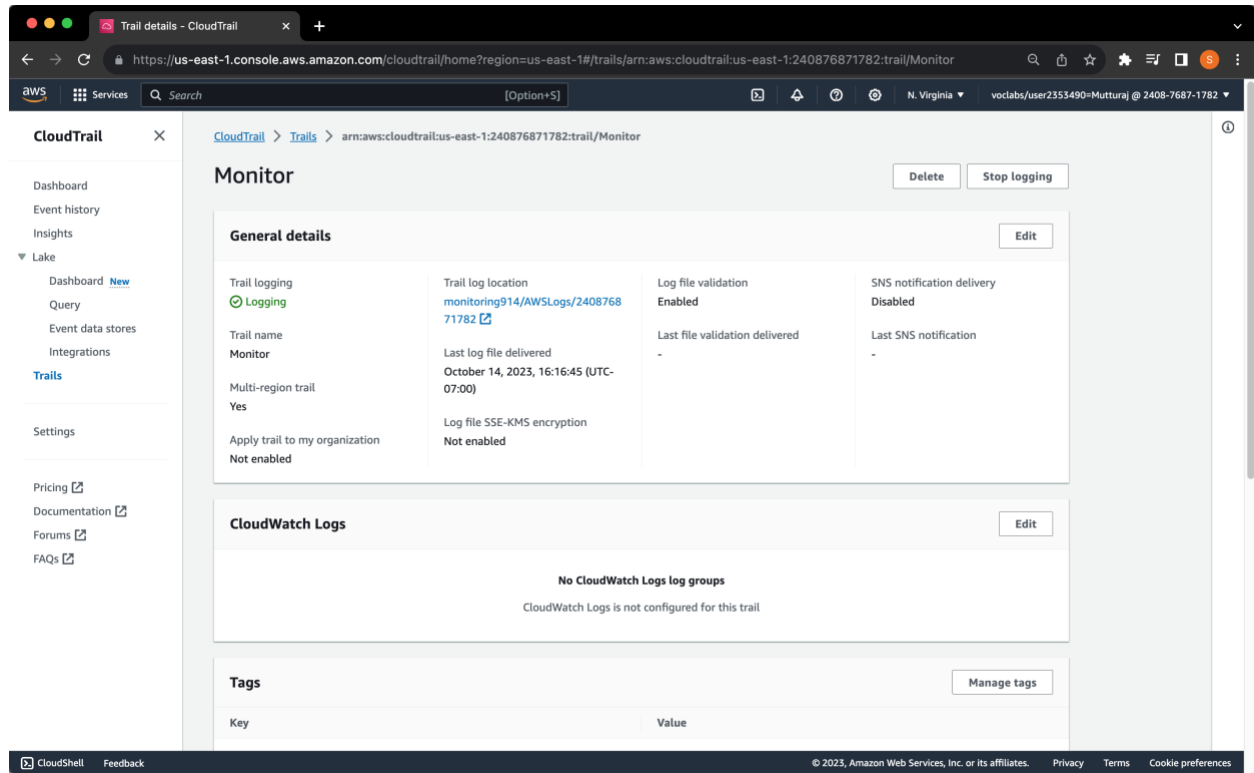
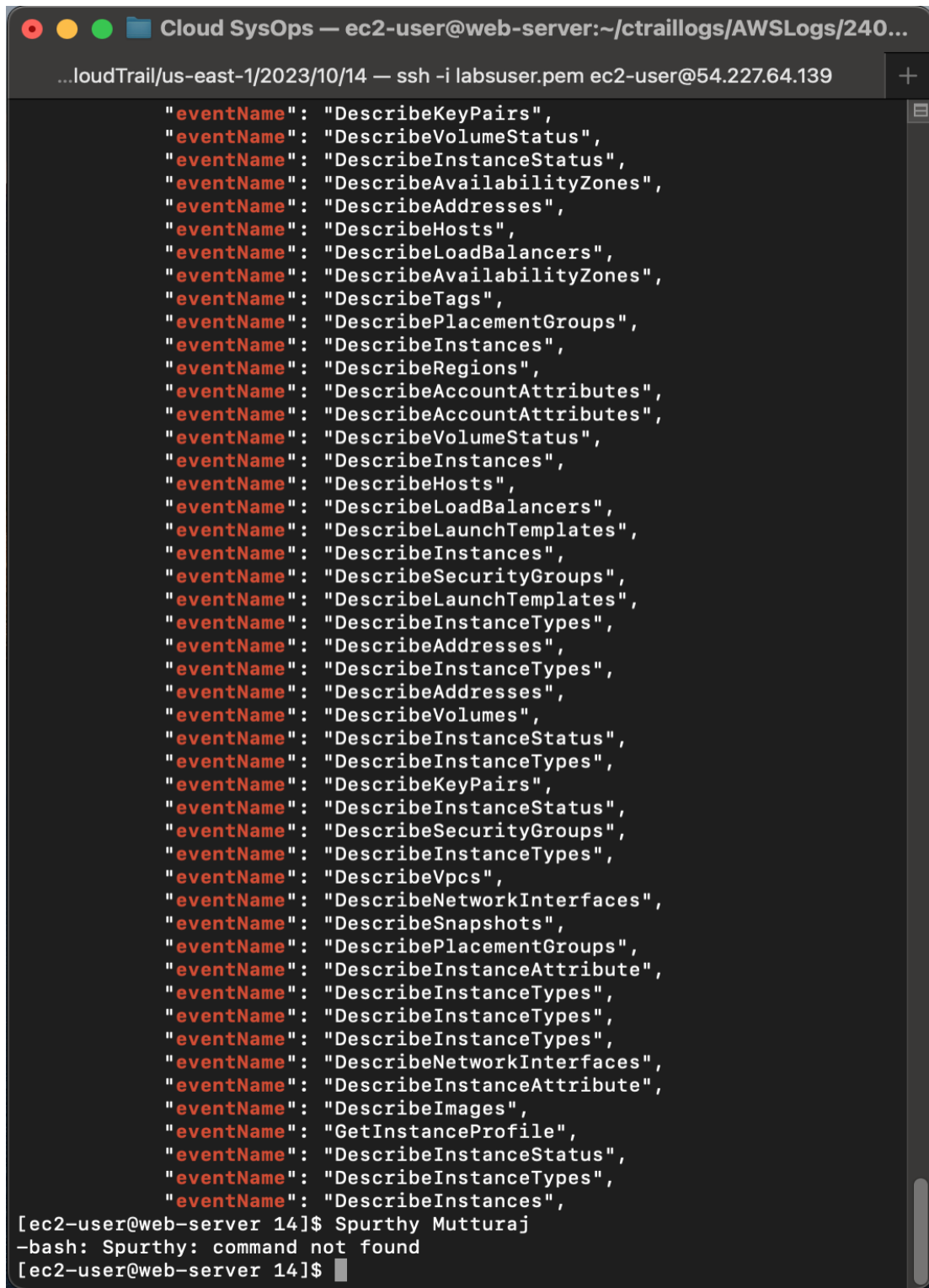


Figure 2

*Screenshot of eventName of every captured event.*



```
Cloud SysOps — ec2-user@web-server:~/ctraillogs/AWSLogs/240...
...loudTrail/us-east-1/2023/10/14 — ssh -i labsuser.pem ec2-user@54.227.64.139

"eventName": "DescribeKeyPairs",
"eventName": "DescribeVolumeStatus",
"eventName": "DescribeInstanceStatus",
"eventName": "DescribeAvailabilityZones",
"eventName": "DescribeAddresses",
"eventName": "DescribeHosts",
"eventName": "DescribeLoadBalancers",
"eventName": "DescribeAvailabilityZones",
"eventName": "DescribeTags",
"eventName": "DescribePlacementGroups",
"eventName": "DescribeInstances",
"eventName": "DescribeRegions",
"eventName": "DescribeAccountAttributes",
"eventName": "DescribeAccountAttributes",
"eventName": "DescribeVolumeStatus",
"eventName": "DescribeInstances",
"eventName": "DescribeHosts",
"eventName": "DescribeLoadBalancers",
"eventName": "DescribeLaunchTemplates",
"eventName": "DescribeInstances",
"eventName": "DescribeSecurityGroups",
"eventName": "DescribeLaunchTemplates",
"eventName": "DescribeInstanceTypes",
"eventName": "DescribeAddresses",
"eventName": "DescribeInstanceTypes",
"eventName": "DescribeAddresses",
"eventName": "DescribeVolumes",
"eventName": "DescribeInstanceStatus",
"eventName": "DescribeInstanceTypes",
"eventName": "DescribeKeyPairs",
"eventName": "DescribeInstanceStatus",
"eventName": "DescribeSecurityGroups",
"eventName": "DescribeInstanceTypes",
"eventName": "DescribeVpcs",
"eventName": "DescribeNetworkInterfaces",
"eventName": "DescribeSnapshots",
"eventName": "DescribePlacementGroups",
"eventName": "DescribeInstanceAttribute",
"eventName": "DescribeInstanceTypes",
"eventName": "DescribeInstanceTypes",
"eventName": "DescribeInstanceTypes",
"eventName": "DescribeNetworkInterfaces",
"eventName": "DescribeInstanceAttribute",
"eventName": "DescribeImages",
"eventName": "GetInstanceProfile",
"eventName": "DescribeInstanceStatus",
"eventName": "DescribeInstanceTypes",
"eventName": "DescribeInstances",

[ec2-user@web-server 14]$ Spurthy Mutturaj
-bash: Spurthy: command not found
[ec2-user@web-server 14]$
```

**Figure 3**

*Screenshot of Select statement of the list of active users in the past day.*

The screenshot displays the Amazon Athena Query Editor interface. The SQL query being executed is:

```
1 SELECT DISTINCT useridentity.userName, eventName, eventSource
2 FROM cloudtrail_logs_monitoring914
3 WHERE from_iso8601_timestamp(eventtime) > date_add('day', -1, now())
4 ORDER BY eventSource;
```

The query has completed successfully. The results are displayed in a table with 80 rows. The first five rows are shown below:

#	userName	eventName	eventSource
1		ListQueryExecutions	athena.amazonaws.com
2		StartQueryExecution	athena.amazonaws.com
3		BatchGetQueryExecution	athena.amazonaws.com
4		GetWorkGroup	athena.amazonaws.com
5		ListDataCatalogs	athena.amazonaws.com

The interface also shows the 'Data' section on the left with 'Data source' set to 'AwsDataCatalog' and 'Database' set to 'default'. The 'Tables and views' section shows 'cloudtrail\_logs\_monitoring914' as the selected table. The 'Query results' section shows the query status as 'Completed' with a time in queue of 135 ms, run time of 610 ms, and data scanned of 99.95 KB.

**Figure 4**

*Screenshot of Select statement limiting the rows to 30.*

The screenshot displays the Amazon Athena Query Editor interface. The SQL query being executed is:

```
1 SELECT useridentity.userName, eventtime, eventsource, eventname, requestparameters
2 FROM cloudtrail_logs_monitoring914
3 LIMIT 30
```

The query has completed successfully. The results are displayed in a table with 6 columns: #, userName, eventtime, eventsource, eventname, and requestparameters. The first four rows of results are shown:

#	userName	eventtime	eventsource	eventname	requestparameters
1		2023-10-14T23:43:52Z	s3.amazonaws.com	GetBucketAcl	{"bucketName":"monitori
2		2023-10-14T23:23:18Z	sts.amazonaws.com	AssumeRole	{"roleArn":"arn:aws:iam::2
3		2023-10-14T23:22:30Z	s3.amazonaws.com	ListBuckets	{"Host":"s3.us-west-1.am
4	chaos	2023-10-15T00:00:21Z	ec2.amazonaws.com	DescribeSecurityGroups	{"securityGroupSet":["se

The interface also shows the query status as 'Completed' with a time in queue of 191 ms, a run time of 718 ms, and 26.18 KB of data scanned. There are buttons for 'Run again', 'Explain', 'Cancel', 'Clear', and 'Create'. The 'Query results' tab is active, showing the table of results. The 'Query stats' tab is also visible. The 'Data' section on the left shows the data source as 'AwsDataCatalog' and the database as 'default'. The 'Tables and views' section shows a table named 'cloudtrail\_logs\_monitoring914'.