

Logging Services

Cheat sheets, Practice Exams and Flash cards  www.exampro.co/clf-c01



CloudTrail - logs all **API calls** (SDK, CLI) between **AWS services** (who can we blame)

Who created this bucket?

Who spun up that expensive EC2 instance?

Who launched this SageMaker Notebook?

- Detect developer misconfiguration
- Detect malicious actors
- Automate responses



CloudWatch is a collection of multiple services

- CloudWatch **Logs** A centralized place to store your cloud services log data or application logs.
- CloudWatch **Metrics** Represents a time-ordered set of data points. A variable to monitor
- CloudWatch **Events (EventBridge)** trigger an event based on a condition eg. every hour take snapshot of server
- CloudWatch **Alarms** triggers notifications based on metrics
- CloudWatch **Dashboard** create visualizations based on metrics



AWS X-Ray is a **distributed tracing system**. You can use it to pinpoint issues with your microservices.

See how data moves from one app to another, how long it took to move, and if it failed to move forward.



AWS CloudTrail

Cheat sheets, Practice Exams and Flash cards [👉 www.exampro.co/clf-c01](http://www.exampro.co/clf-c01)



AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account.

AWS CloudTrail is used to monitor API calls and Actions made on an AWS account.

Easily identify which users and accounts made the call to AWS eg.

- **Where** — Source IP Address
- **When** — EventTime
- **Who** — User, UserAgent
- **What** — Region, Resource, Action

```
1 {"Records": [
2     "eventVersion": "1.0",
3     "userIdentity": {
4         "type": "IAMUser",
5         "principalId": "EX_PRINCIPAL_ID",
6         "arn": "arn:aws:iam::123456789012:user/Worf",
7         "accountId": "123456789012",
8         "accessKeyId": "EXAMPLE_KEY_ID",
9         "userName": "Worf"
10    },
11    "eventTime": "2014-03-24T21:11:59Z",
12    "eventSource": "iam.amazonaws.com",
13    "eventName": "CreateUser",
14    "awsRegion": "us-east-1",
15    "sourceIPAddress": "127.0.0.1",
16    "userAgent": "aws-cli/1.3.2 Python/2.7.5 Windows/10",
17    "requestParameters": {"userName": "LaForge"},
18    "responseElements": {"user": {
19        "createDate": "Mar 24, 2014 9:11:59 PM",
20        "userName": "LaForge",
21        "arn": "arn:aws:iam::123456789012:user/LaForge",
22        "path": "/",
23        "userId": "EXAMPLEUSERID"
24    }}
25 ]]}
```

AWS CloudTrail

Cheat sheets, Practice Exams and Flash cards www.exampro.co/clf-c01

CloudTrail is already logging by default and will collect logs for **last 90 days** via **Event History**

If you need more than 90 days you need to create a **Trail**

Trails are output to S3 and do not have GUI like Event History. To analyze a Trail you'd have to use **Amazon Athena.**



CloudTrail

Dashboard

Event history

Trails

Learn more

Pricing

Documentation

Forums

FAQs

Event history

Your event history contains the activities taken by people, groups, or AWS services in supported services. It filters out read-only events. You can change or remove that filter, or apply other filters.

You can view the last 90 days of events. Choose an event to view more information about it. To view a contrail and then go to your Amazon S3 bucket or CloudWatch Logs. Learn more

Can't find what you're looking for? Run advanced queries in Amazon Athena

Filter: Read only false Time range: Select time range

	Event time	User name	Event name
▶	2019-09-01, 09:33:07 PM	i-014d0d0e482491e69	UpdateInstanceInformation
▶	2019-09-01, 09:30:07 PM	i-08ece9e263d3edfb	UpdateInstanceInformation
▶	2019-09-01, 09:28:07 PM	i-0984241e0f6a0f9ca	UpdateInstanceInformation
▶	2019-09-01, 09:25:07 PM	i-07a9e824eb84d5f2b	UpdateInstanceInformation
▶	2019-09-01, 09:23:34 PM	exampro-events	CreateLogStream
▶	2019-09-01, 09:23:07 PM	i-014d0d0e482491e69	UpdateInstanceInformation
▶	2019-09-01, 09:20:07 PM	i-0f5f9d47f3c1cf6d	UpdateInstanceInformation
▶	2019-09-01, 09:18:07 PM	i-08ece9e263d3edfb	UpdateInstanceInformation
▶	2019-09-01, 09:15:07 PM	i-07a9e824eb84d5f2b	UpdateInstanceInformation
▶	2019-09-01, 09:13:51 PM	exampro-metrics	CreateLogStream



CloudWatch Alarms

Cheat sheets, Practice Exams and Flash cards www.exampro.co/clf-c01

A CloudWatch Alarm monitors a **CloudWatch Metric** based on **a defined threshold**.

Name	State	Last state update	Conditions	Actions
Network_In	In alarm	2020-07-20 13:01:35	NetworkIn > 300 for 1 datapoints within 5 minutes	No actions

When alarm breaches (goes outside the defined threshold) than it changes **state**.

When it changes state we can define what **action it should trigger**.

Metric Alarm States

- OK The metric or expression is **within** the defined threshold
- ALARM The metric or expression is **outside** of the defined threshold
- INSUFFICIENT DATA**
 - The alarm has **just started**
 - the metric is **not available**
 - Not enough data** is available

Notification

Alarm state trigger

In alarm
The metric or expression is outside of the defined threshold.

OK
The metric or expression is within the defined threshold.

Insufficient data
The alarm has just started or not enough data is available.

Select an SNS topic

Select an existing SNS topic

Create new topic

Use topic ARN

Add notification

Auto Scaling action

Add Auto Scaling action

EC2 action

This action is only available for EC2 Per-Instance Metrics.

Add EC2 action

- Notification
- Auto Scaling Group
- EC2 Action



CloudWatch Alarms – Anatomy of an Alarm

Cheat sheets, Practice Exams and Flash cards  www.exampro.co/clf-c01

Threshold Condition

Defines when a datapoint is breached

Threshold type

Static
Use a value as a threshold

Whenever NetworkIn is...

Define the alarm condition.

Greater > threshold Greater or equal \geq

than...

Define the threshold value.

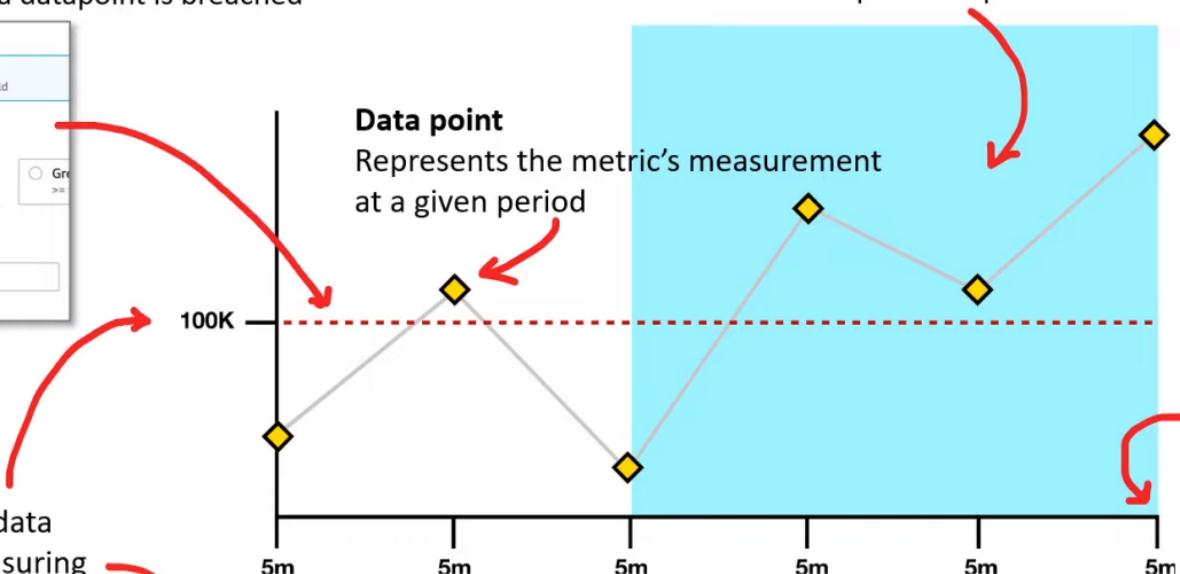
Must be a number

Metric

The actual data we are measuring

NetworkIn

The volume of incoming network traffic, measured in Bytes. When using 5min monitoring divide by 300 to get Bytes/second



Datapoints to alarm

Define the number of datapoints within the evaluation period that must be breaching to cause the alarm to go to ALARM state.

out of

Datapoints to alarm

1 data point is breached in an evaluation period going back 4 periods.

This is what triggers the alarm



CloudWatch Logs – Log Streams

Cheat sheets, Practice Exams and Flash cards www.exampro.co/clf-c01

Log Streams

A log stream represents a **sequence of events** from a **application or instance being monitored**.

Create log stream

Log stream name
my-log-stream

Cancel Create



You can create Log Streams manually but generally this is automatically done by the service you are using

<input type="checkbox"/> Log stream	Last event time
2020/07/06/[\${LATEST}]ebca38579fac4842b531b260d5c35e0e	7/6/2020, 7:41:24 PM
2020/07/06/[\${LATEST}]7679ba0f37b14a3da994cd243963ca60	7/6/2020, 6:14:42 PM
2020/07/06/[\${LATEST}]bb7edeb95cb345b48dd151a79367a5d6	7/6/2020, 3:52:56 PM
2020/07/06/[\${LATEST}]e1544efd95a4492585b9c8d27ddaea4b	7/6/2020, 1:30:09 PM
2020/07/06/[\${LATEST}]86a8ec4dcff746628feffa82b41e1cc	7/6/2020, 12:28:00 PM
2020/07/06/[\${LATEST}]a06263c73f8242e5a0e35b366b3bbdf9	7/6/2020, 10:08:43 AM

Here is a Log Group for a **Lambda function**

You can see here the Log Streams are named after the **running instance**. Lambdas frequency run on new instances so the stream streams contain timestamps

<input type="checkbox"/> Log stream	Last event time
i-0761fcbbcd19ffc8	7/6/2020, 6:56:31 PM
i-09239615bc7f3f552	7/5/2020, 9:40:42 PM
i-06c9e4fb3469e17a4	7/5/2020, 9:21:08 PM
i-0450c5ca38bdcd125	7/5/2020, 8:27:30 PM
i-01a34b0a12504edfa	7/5/2020, 12:42:24 AM
i-0e4f5ec7610f21d08	7/5/2020, 12:32:35 AM

Here is a Log Group for an **application logs running on EC2** You can see here the Log Streams are named after the **running instance's Instance ID**

<input type="checkbox"/> Log stream	Last event time
exampro-events-crawler	6/30/2019, 12:57:11 PM
exampro-waf-logs	6/26/2019, 9:00:49 AM
exampro-leads-crawler	3/24/2019, 7:57:03 PM
dynamodb-events-tracking	3/13/2019, 4:38:00 PM
cloudtrail	2/24/2019, 4:12:18 PM

Here is a Log Group for **AWS Glue**. You can see here the Log Streams are named after the **Glue Jobs**.



CloudWatch Logs – Log Events

Cheat sheets, Practice Exams and Flash cards  www.exampro.co/clf-c01

Log Events

Represents a single event in a log file. Log events can be seen within a Log Stream.

- ▶ 2020-07-06T20:12:18.079-04:00 START RequestId: e4b5bd10-5d88-4d7b-870c-daf793159b88 Version: \$LATEST
- ▶ 2020-07-06T20:12:18.082-04:00 {"records_size":1}
- ▶ 2020-07-06T20:12:18.093-04:00 {"failed_put_count":0}
- ▶ 2020-07-06T20:12:18.127-04:00 END RequestId: e4b5bd10-5d88-4d7b-870c-daf793159b88
- ▶ 2020-07-06T20:12:18.127-04:00 REPORT RequestId: e4b5bd10-5d88-4d7b-870c-daf793159b88 Duration: 45.32 ms Billed Duration: 100 ms Memory Size: 128

You can use filter events to filter out logs based on simple or Pattern matching syntax:

Log events

Filter events

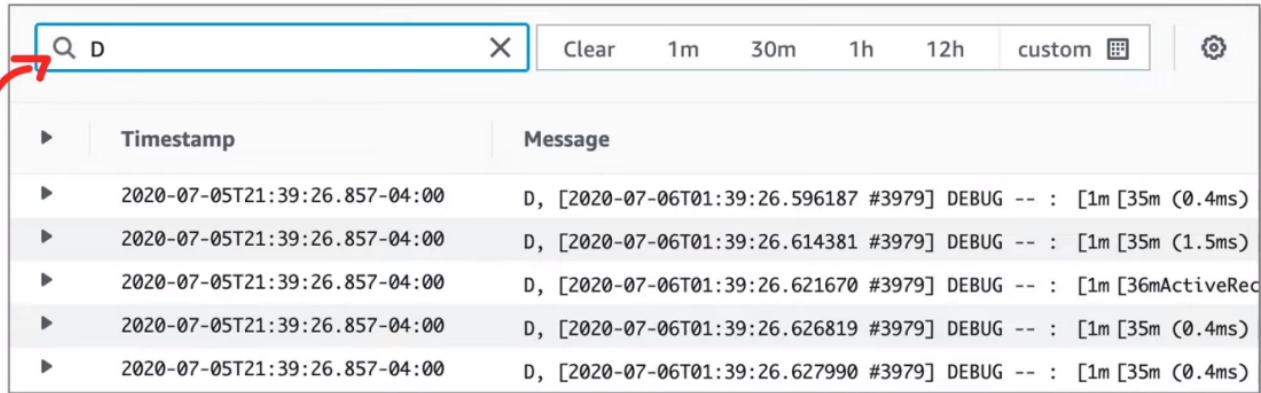
▶ 2020-07-05T21:39:26.857-04:00 D, [2020-07-06T01:39:26.596187 #3979] DEBUG -- : [1m [35m (0.4ms)

▶ 2020-07-05T21:39:26.857-04:00 D, [2020-07-06T01:39:26.614381 #3979] DEBUG -- : [1m [35m (1.5ms)

▶ 2020-07-05T21:39:26.857-04:00 D, [2020-07-06T01:39:26.621670 #3979] DEBUG -- : [1m [36mActiveRec

▶ 2020-07-05T21:39:26.857-04:00 D, [2020-07-06T01:39:26.626819 #3979] DEBUG -- : [1m [35m (0.4ms)

▶ 2020-07-05T21:39:26.857-04:00 D, [2020-07-06T01:39:26.627990 #3979] DEBUG -- : [1m [35m (0.4ms)



The screenshot shows the AWS CloudWatch Logs interface. At the top, there is a search bar with the letter 'D' and a magnifying glass icon. To the right of the search bar are buttons for 'Clear', time ranges ('1m', '30m', '1h', '12h'), and a 'custom' button. Below the search bar is a table with columns for 'Timestamp' and 'Message'. The table contains five rows of log entries, each starting with a red arrow pointing from the 'Filter events' input field in the sidebar. The log entries show timestamped DEBUG messages with varying durations.

Timestamp	Message
2020-07-05T21:39:26.857-04:00	D, [2020-07-06T01:39:26.596187 #3979] DEBUG -- : [1m [35m (0.4ms)
2020-07-05T21:39:26.857-04:00	D, [2020-07-06T01:39:26.614381 #3979] DEBUG -- : [1m [35m (1.5ms)
2020-07-05T21:39:26.857-04:00	D, [2020-07-06T01:39:26.621670 #3979] DEBUG -- : [1m [36mActiveRec
2020-07-05T21:39:26.857-04:00	D, [2020-07-06T01:39:26.626819 #3979] DEBUG -- : [1m [35m (0.4ms)
2020-07-05T21:39:26.857-04:00	D, [2020-07-06T01:39:26.627990 #3979] DEBUG -- : [1m [35m (0.4ms)



CloudWatch Logs – Log Insights

Cheat sheets, Practice Exams and Flash cards  www.exampro.co/clf-c01

CloudWatch Logs Insights enables you to **interactively search and analyze your CloudWatch log data** and has the following advantages:

- more robust filtering than using the simple Filter events in a Log Stream
- Less burdensome than having to export logs to S3 and analyze them via Athena.

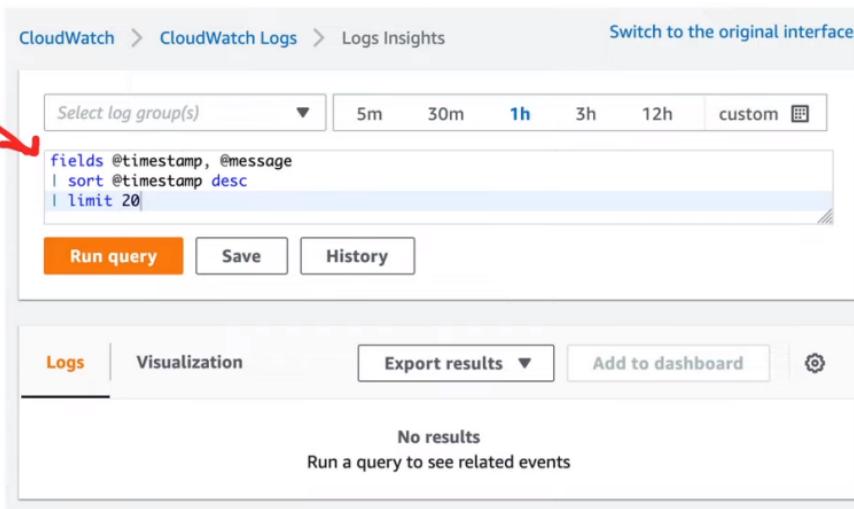
CloudWatch Logs Insights supports all types of logs.

CloudWatch Logs Insights is commonly used via the console to do ad-hoc queries against log groups.

CloudWatch Insights has its own language called:

- CloudWatch Logs Insights **Query Syntax**

```
filter action="REJECT"  
| stats count(*) as numRejections by srcAddr  
| sort numRejections desc  
| limit 20
```



The screenshot shows the AWS CloudWatch Logs Insights interface. At the top, there are navigation links: CloudWatch > CloudWatch Logs > Logs Insights. On the right, a link says "Switch to the original interface." Below the navigation, there are time range controls: 5m, 30m, **1h**, 3h, 12h, and custom. A dropdown menu says "Select log group(s)". The main area contains a code editor with the following query:

```
fields @timestamp, @message  
| sort @timestamp desc  
| limit 20
```

Below the code editor are three buttons: "Run query", "Save", and "History". The "Logs" tab is selected, showing the message "No results". There is also a "Visualization" tab, an "Export results" button, an "Add to dashboard" button, and a settings gear icon. A red arrow points from the text "CloudWatch Logs Insights is commonly used via the console to do ad-hoc queries against log groups." to the "Logs Insights" interface. Another red arrow points from the text "CloudWatch Insights has its own language called:" to the sample query code.

- A single request can query up to **20 log groups**.
- Queries **time out after 15 minutes**, if they have not completed.
- Query results are **available for 7 days**.



CloudWatch Logs – Log Insights

Cheat sheets, Practice Exams and Flash cards www.exampro.co/clf-c01

Queries

Saved queries

Filter by query name

Create query

Sample queries

Learn more [🔗](#)

- ▶ Lambda
- ▼ VPC Flow Logs
 - ▶ Average, min, and max byte transfers by source and destination IP addresses
 - ▶ IP addresses using UDP transfer protocol
 - ▶ Top 10 byte transfers by source and destination IP addresses
 - ▼ Top 20 source IP addresses with highest number of rejected requests
 - filter action="REJECT"
| stats count(*) as numRejections by srcAddr
| sort numRejections desc
| limit 20

Apply

AWS provides sample queries that can get you started for common tasks, And to ease learning the Query Syntax. A good example is filtering VPC Flow Logs.

Select log group(s) 5m 30m 1h 3h 12h custom

Clear exampro-flow-logs [✖](#)

```
filter action="REJECT"
| stats count(*) as numRejections by srcAddr
| sort numRejections desc
| limit 20
```

Run query Save History

Logs Visualization Export results Add to dashboard

Showing 20 of 1,709 records matched [ⓘ](#) Hide histogram
15,067 records (2.0 MB) scanned in 4.6s @ 3,281 records/s (452.0 kB/s)

#	srcAddr	numRejections
1	185.154.13...	52
2	45.227.255...	51
3	87.251.74.62	49
4	94.102.51.28	33
5	52.41.160.1...	30

You can create and save your own queries to make future repetitive tasks easier.



CloudWatch Metrics

Cheat sheets, Practice Exams and Flash cards  www.exampro.co/clf-c01

A CloudWatch Metric represents a **time-ordered set of data points**
Its a **variable** that is **monitored over time**.

CloudWatch comes with many **predefined** metrics that are generally name spaced by AWS Service.



EC2 Per-Instance Metrics

- CPUUtilization
- DiskReadOps
- DiskWriteOps
- DiskReadBytes
- DiskWriteBytes
- **NetworkIn**
- NetworkOut
- NetworkPacketsIn
- NetworkPacketsOut

