

Note 1: When you reach Step 14 to create the alarm, besides the steps indicated below, you may also follow the 2nd screenshot below to configure additional settings.

14. Create a CloudWatch alarm based on the metric filter.

- On the **Metric filters** tab, select the check box to the right of the **ConsoleLoginErrors** metric filter that you just created.
- Choose **Create alarm**.
A new browser tab opens.
- On the **Specify metric and conditions** page, in the **Conditions** section, configuring the following alarm details:
 - **Whenever ConsoleLoginFailureCount is:** Choose **Greater/Equal**.
 - **than...:** Enter **3**
Observe the settings. This alarm will be invoked whenever the sum of the ConsoleLoginFailureCount metric that you defined is greater than or equal to 3 within any 5-minute period.
 - Choose **Next**.
- On the **Configure actions** page, configure the following:
 - **Select an SNS topic:** Choose **Select an existing topic**.
 - **Send a notification to...:** Choose **MySNSTopic**.
 - Choose **Next**.
- On the **Add name and description** page, configure the following:
 - **Alarm name:** Enter **FailedLogins**
 - Choose **Next**.

Conditions

Threshold type

☒ Static
Use a value as a threshold

☐ Anomaly detection
Use a band as a threshold

Whenever ConsoleLoginFailureCount is...
Define the alarm condition.

☐ Greater
> threshold

☒ Greater/Equal
>= threshold

☐ Lower/Equal
<= threshold

☐ Lower
< threshold

than...
Define the threshold value.

2

Must be a number

Additional configuration

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.

1 out of 1

Missing data treatment
How to treat missing data when evaluating the alarm.

Treat missing data as bad (breaching threshold) ▼

Cancel Next **Update alarm**

You may put a lower threshold just for quick testing purpose.

Choose this setting to treat missing data as bad. This will solve the problem of data not collected and alarm showing "insufficient data"

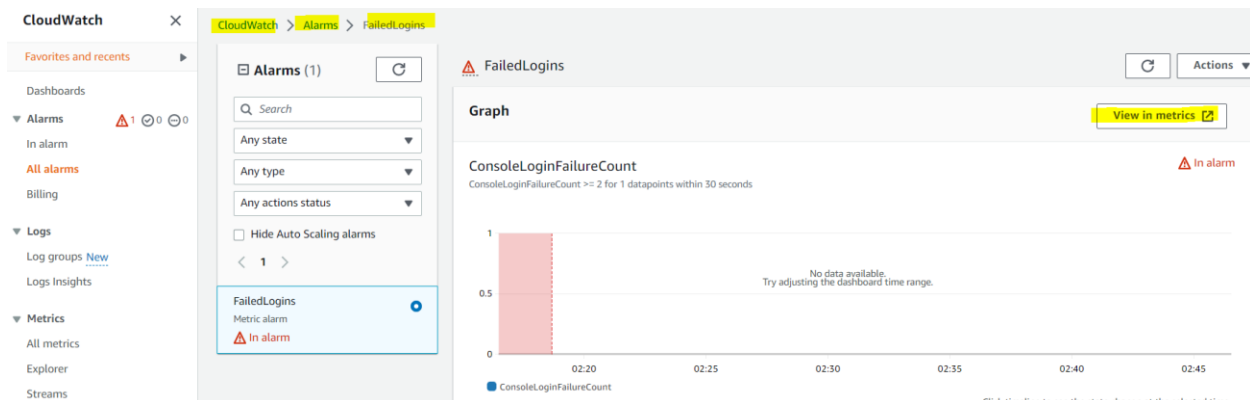
Note 2: Due to the Lab UI change, you cannot directly find **Custom namespaces** as indicated in Step 17. Please follow the below steps for the workout.

17. Graph the metric that you created.

- Navigate to the CloudWatch console.
- In the navigation pane, expand **Metrics**, and then choose **All metrics**.
- In the **Metrics** section, under **Custom namespaces**, choose **CloudTrailMetrics**.
Note: If CloudTrailMetrics does not yet appear, wait a minute or two and refresh the browser tab.
- Choose **Metrics with no dimensions**.
- To the right of **ConsoleLoginFailureCount**, choose the triangle icon, and then choose **Graph this metric only**.

In the graph area at the top of the page, a small blue dot should appear. The dot indicates that a login failure was detected.

- From CloudWatch, Alarms, select “All Alarms” and click your alarm “FailedLogins”. On the top right of the page, select “View in Metrics”.



- You will enter the page with metrics info labeled as “ConsoleLoginFailureCount”. On the next column, click the details and then you can choose “Graph with SQL query”.

