

## Week 4: Implementing Cloud Logging and Monitoring

Name- Saish Dhiwar

PRN- 2124UCSM2011

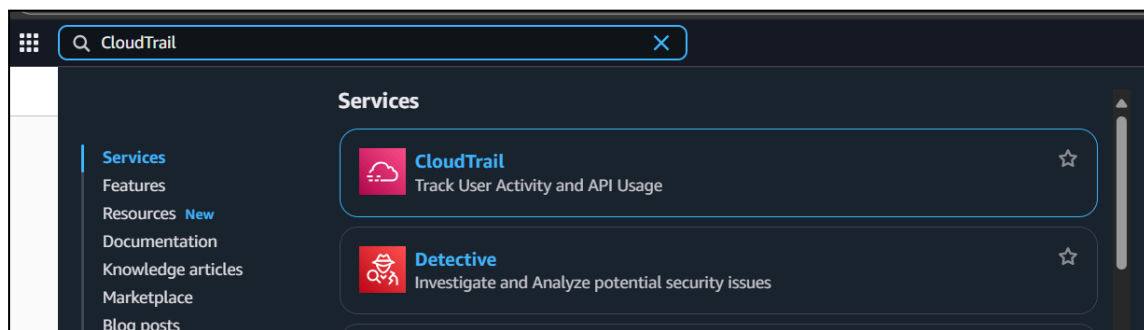
Email- [saish.dhiwar\\_24ucs@sanjivani.edu.in](mailto:saish.dhiwar_24ucs@sanjivani.edu.in)

---

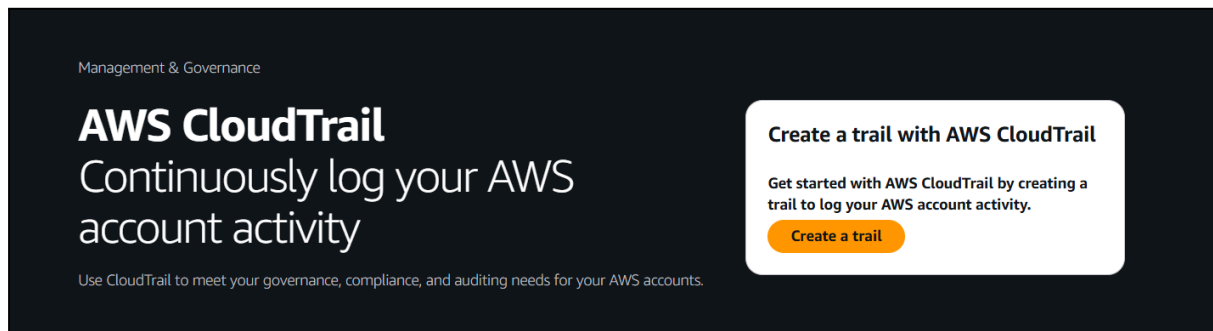
- Task-** 1) Enable CloudTrail/Cloud Audit Logs.  
2) Configure alerts for suspicious activity.  
3) Document findings.

### Task 1- Enable Cloud Trail/ Cloud Audit Logs.

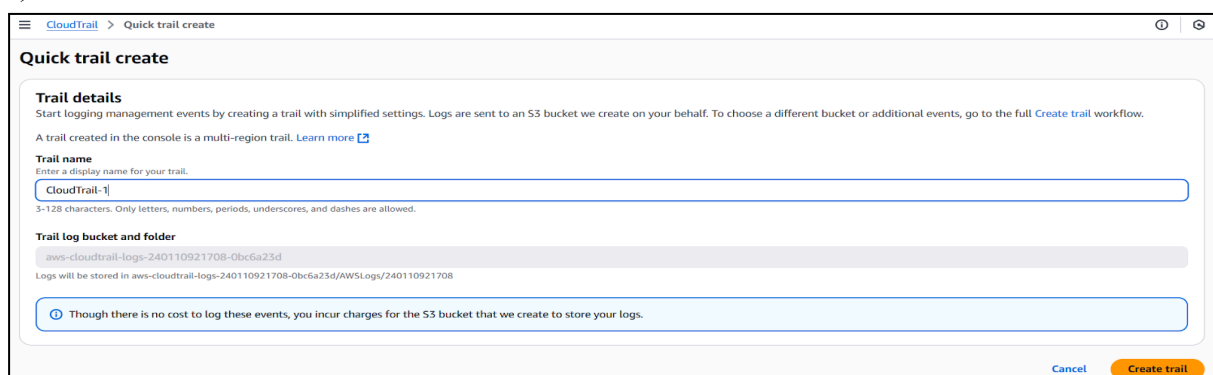
- 1) Log in to AWS Console.
- 2) Search & open CloudTrail from the Services menu.

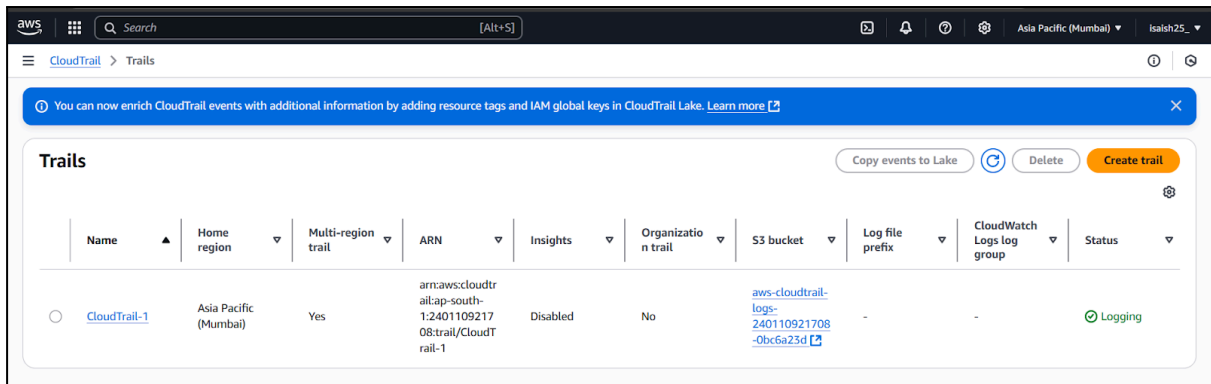


- 3) Click to Create Trail.

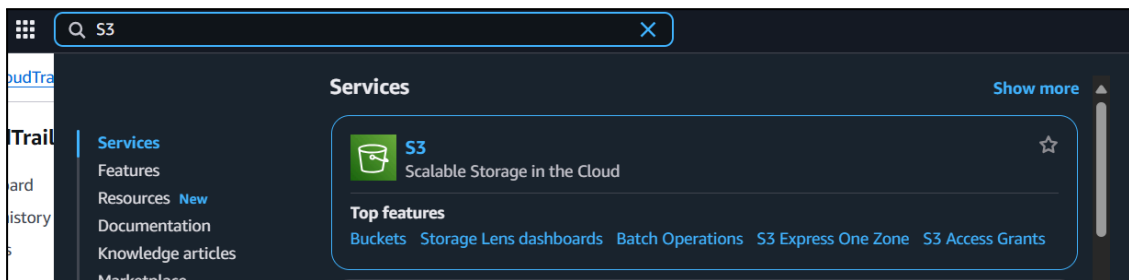


- 4) Fill in Trail Name CloudTrail-1, and then click to create Trail.





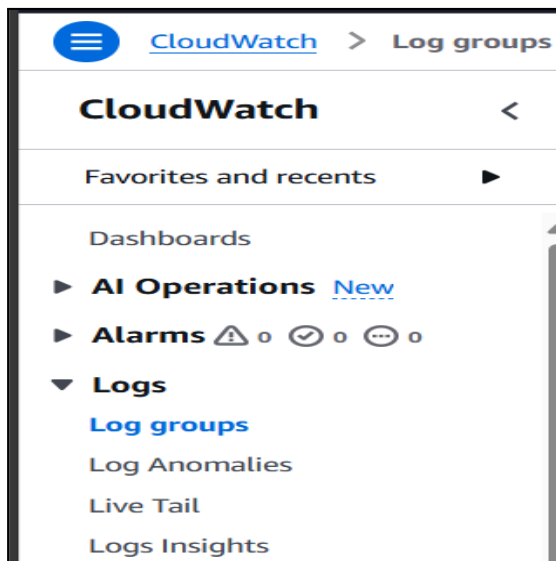
5) Set up S3 Bucket to store logs: Create a new bucket.



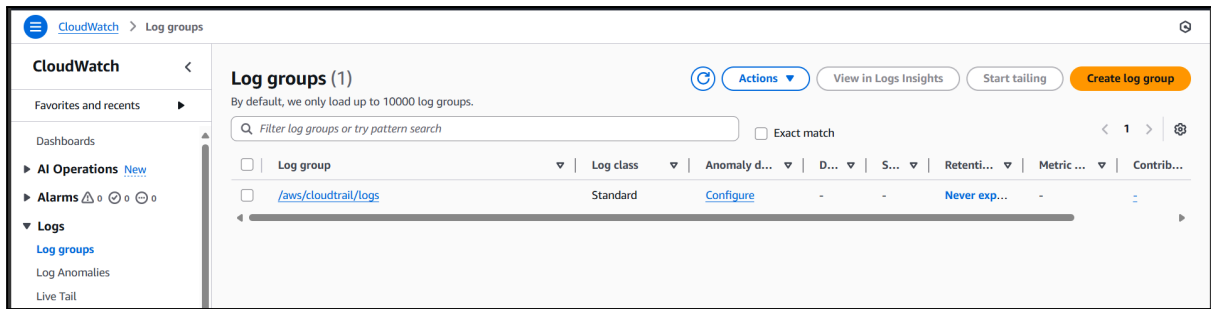
6) Enable CloudWatch Logs, Create new Log Group:/aws/cloudtrail/logs, Allow to create IAM role automatically, then click Create trail.

## Task 2- Configure alerts for suspicious activity.

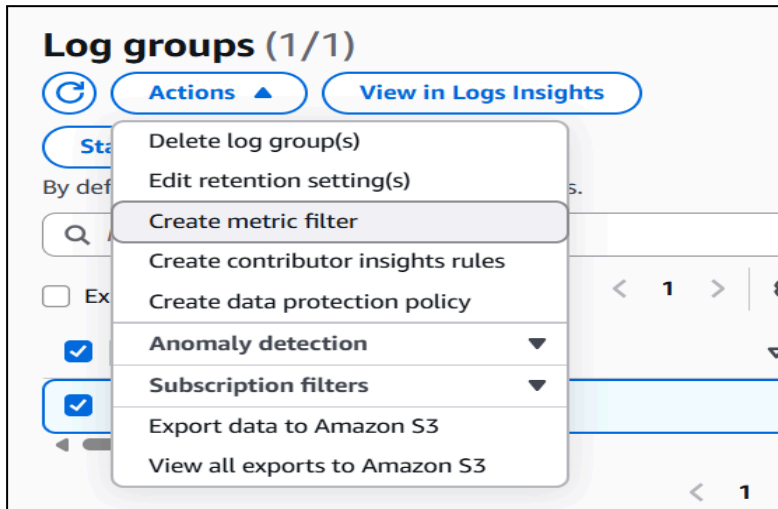
1) Go to CloudWatch, Log Groups.



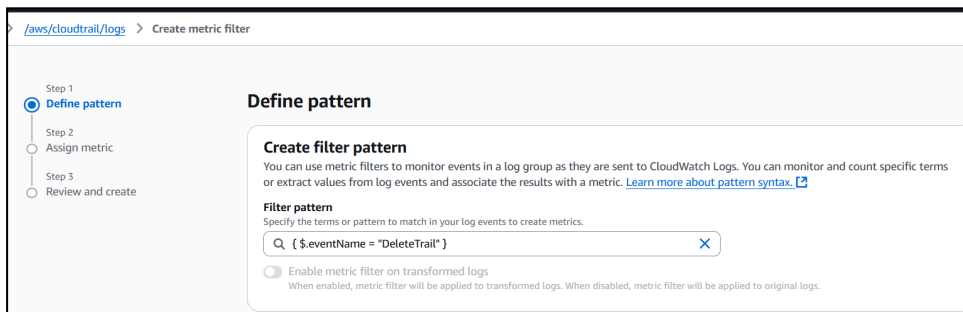
2) Select your log group: /aws/cloudtrail/logs



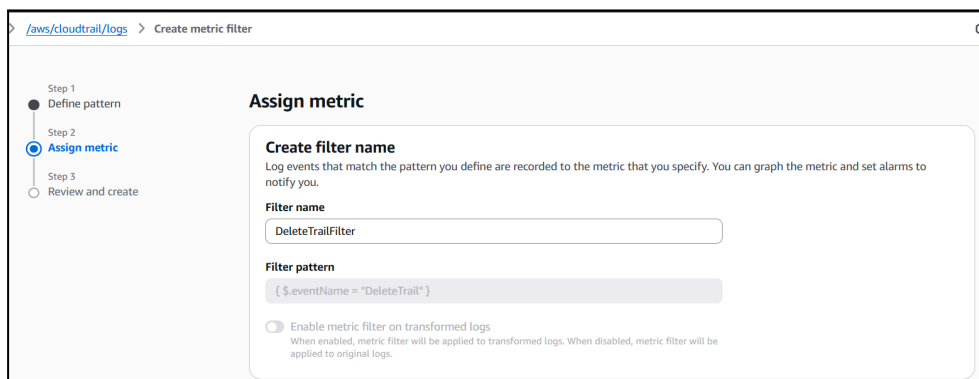
3) Click Actions→ Create Metric Filter.



4) Paste the filter pattern, and then click Next.



5) Next step is to create a filter name. Enter the filter Name.



## 6) Then Enter the Matrix Details.

**Metric details**

**Metric namespace**  
Namespaces let you group similar metrics. [Learn more](#)  
 ☒ Create new  
Namespaces can be up to 255 characters long; all characters are valid except for colon(:) at the start of the name.

**Metric name**  
Metric name identifies this metric, and must be unique within the namespace. [Learn more](#)  
  
Metric name can be up to 255 characters long; all characters are valid except for colon(:), asterisk(\*), dollar(\$), and space( ).

**Metric value**  
Metric value is the value published to the metric name when a Filter Pattern match occurs.  
  
Valid metric values are: floating point number (1, 99.9, etc.), numeric field identifiers (\$1, \$2, etc.), or named field identifiers (e.g. \$requestSize for delimited filter pattern or \$.status for JSON-based filter pattern - dollar (\$) or dollar dot (\$.) followed by alphanumeric and/or underscore (\_) characters).

**Default value – optional**  
The default value is published to the metric when the pattern does not match. If you leave this blank, no value is published when there is no match. [Learn more](#)

**Unit – optional**

## 7) Then click Create Matrix.

**Review and create**

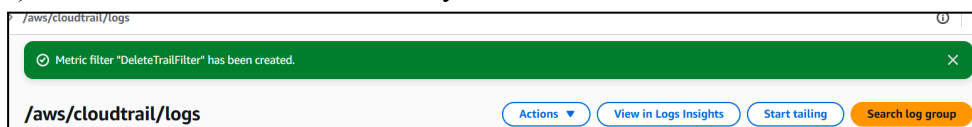
**Step 1: Pattern** [Edit](#)  
**Create filter pattern**  
Filter pattern  

```
{ $.eventName = "DeleteTrail" }
```

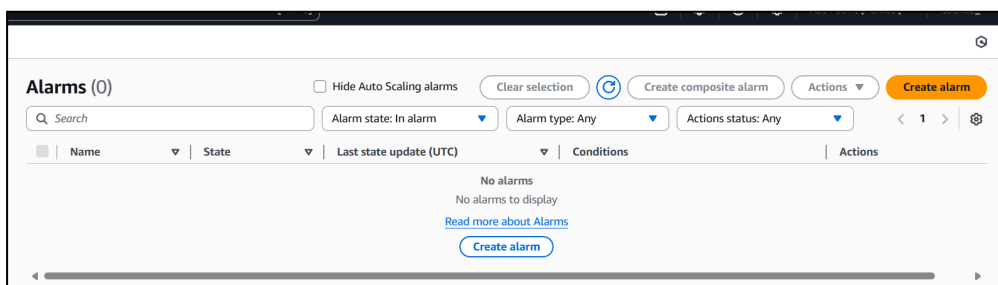
**Step 2: Metric** [Edit](#)  
**Assign metric**

<b>Filter name</b> DeleteTrailFilter	<b>Metric name</b> DeleteTrailAttempts
<b>Metric namespace</b> CloudTrailMonitoring	<b>Applied on transformed logs</b> -
<b>Metric value</b> 1	<b>Default value</b> 0
<b>Unit</b> Count	

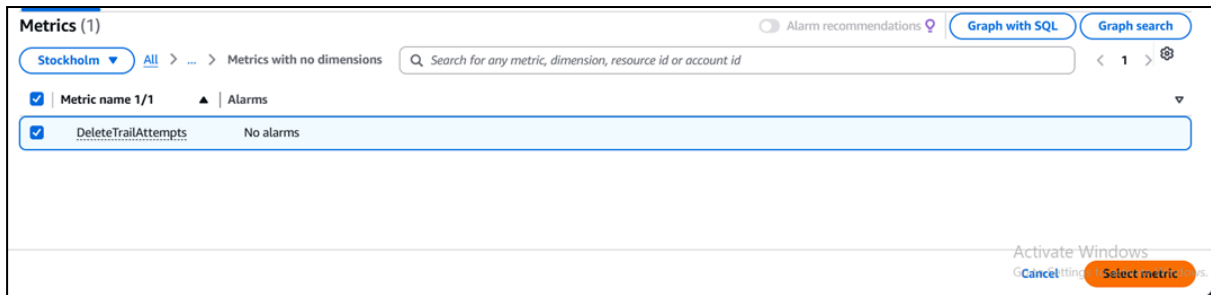
## 8) Matrix filter created successfully.



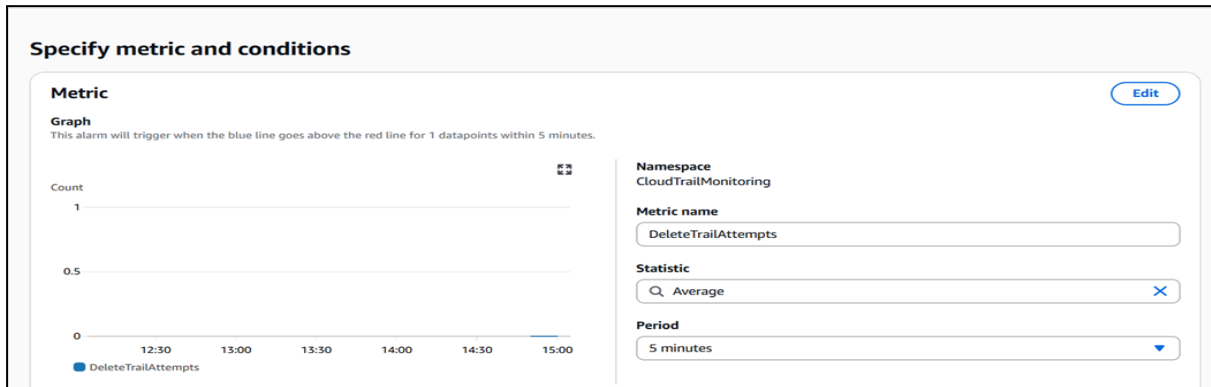
## 9) Go to CloudWatch→ Alarms→ Create Alarm.



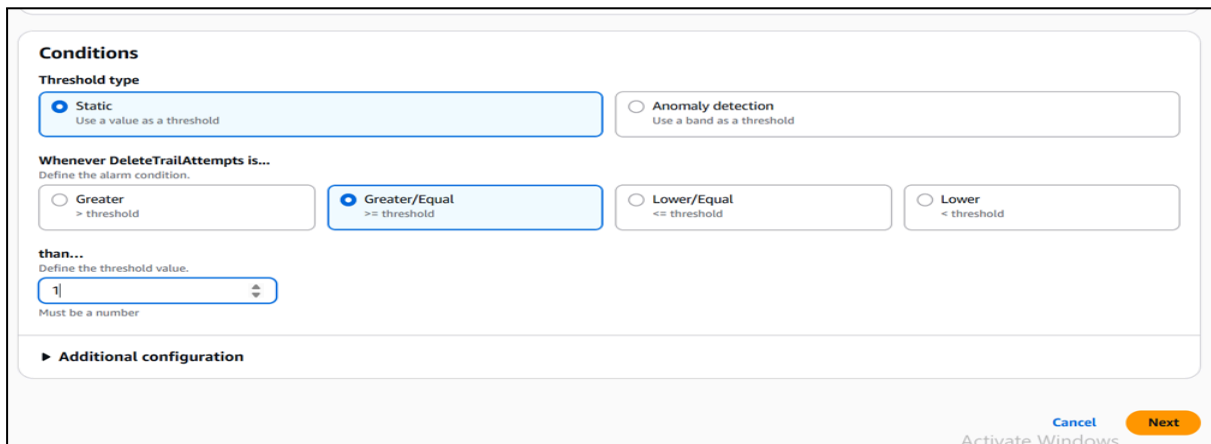
## 10) Select Metric



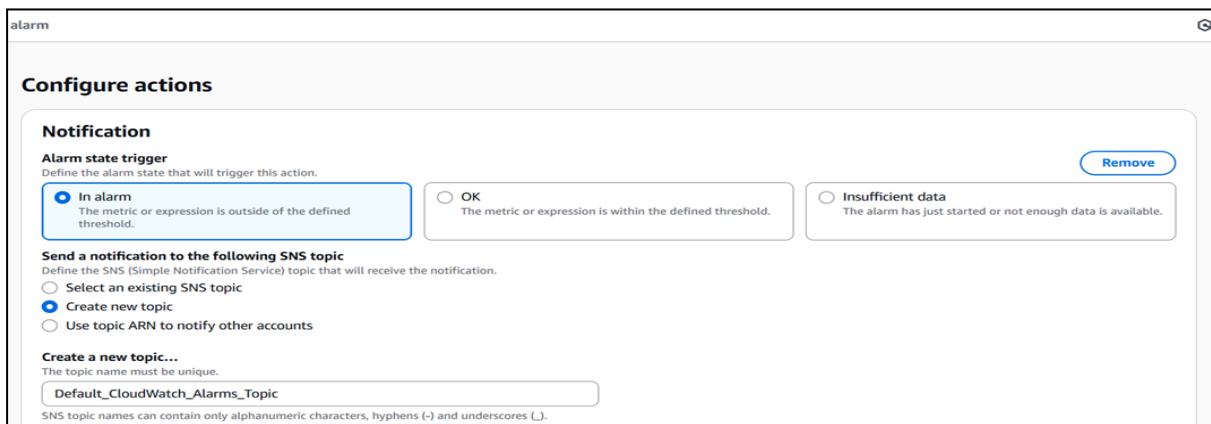
11) Set threshold: Static, Condition: Greater than or equal to 1, Period: 5 minutes.



12) Set Condition, and then click Next



13) Add Configure action Details



14) Add Alarm Details, and then click Next.

The screenshot shows the 'Add alarm details' form in the AWS console. The form is titled 'Add alarm details' and has a section 'Name and description'. Under 'Name and description', there is a text input field for 'Alarm name' containing 'DeleteTrailAlarm'. Below this is a section for 'Alarm description - optional' with a link to 'View formatting guidelines'. There are two tabs: 'Edit' (selected) and 'Preview'. The 'Edit' tab shows a text area with the following content: '# This is an H1', '\*\*double asterisks will produce strong character\*\*', and 'This is [an example](https://example.com/) inline link.' Below the text area is a character count: 'Up to 1024 characters (0/1024)'. At the bottom of the form, there is a blue box with a warning icon and text: 'Markdown formatting is only applied when viewing your alarm in the console. The description will remain in plain text in the alarm notifications.' At the bottom right of the form, there are three buttons: 'Cancel', 'Previous', and 'Next'. The 'Next' button is highlighted in orange.

**Add alarm details**

**Name and description**

Alarm name  
DeleteTrailAlarm

Alarm description - optional [View formatting guidelines](#)

**Edit** Preview

# This is an H1  
\*\*double asterisks will produce strong character\*\*  
This is [an example](https://example.com/) inline link.

Up to 1024 characters (0/1024)

ⓘ Markdown formatting is only applied when viewing your alarm in the console. The description will remain in plain text in the alarm notifications.

Cancel Previous **Next**

15) Set Alarm Successfully

The screenshot shows the AWS console 'Alarms' page. At the top, there is a blue banner with a warning icon and text: 'Some subscriptions are pending confirmation. Amazon SNS doesn't send messages to an endpoint until the subscription is confirmed.' To the right of the banner is a button 'View SNS Subscriptions' and a close icon. Below the banner, the page is titled 'Alarms (1)'. There are several filters and actions: 'Hide Auto Scaling alarms' (checkbox), 'Clear selection' (button), 'Create composite alarm' (button), 'Actions' (dropdown), and 'Create alarm' (button). There is also a search bar and three dropdown menus for 'Alarm state: Any', 'Alarm type: Any', and 'Actions status: Any'. Below these are navigation controls: '< 1 >' and a settings icon. The main content is a table with columns: 'Name', 'State', 'Last state update (UTC)', 'Conditions', and 'Actions'. The table has one row with the following data: Name: 'DeleteTrailAlarm', State: 'Insufficient data', Last state update (UTC): '2025-07-07 15:57:08', Conditions: 'DeleteTrailAttempts >= 1 for 1 datapoints within 5 minutes', and Actions: 'Actions enabled Warni'.

ⓘ Some subscriptions are pending confirmation  
Amazon SNS doesn't send messages to an endpoint until the subscription is confirmed [View SNS Subscriptions](#) ✕

**Alarms (1)** ☐ Hide Auto Scaling alarms [Clear selection](#) [Create composite alarm](#) [Actions](#) [Create alarm](#)

Alarm state: Any Alarm type: Any Actions status: Any < 1 > ⚙️

<input type="checkbox"/>	Name	State	Last state update (UTC)	Conditions	Actions
<input type="checkbox"/>	<a href="#">DeleteTrailAlarm</a>	Insufficient data	2025-07-07 15:57:08	DeleteTrailAttempts >= 1 for 1 datapoints within 5 minutes	Actions enabled Warni