**Financial Industry Cloud Security: Monitoring IAM Logins at FinTechCorp**

**Problem Statement:**

In the fast-paced world of financial technology, **FinTechCorp**, a global leader in digital banking, recently experienced an attempted unauthorized access to their cloud infrastructure. Ensuring compliance, security, and transparency of user activities is a critical requirement for maintaining the trust of millions of customers worldwide. FinTech Corps security team aims to build a robust monitoring system using AWS CloudWatch and CloudTrail to track IAM user activities and detect suspicious login patterns, ensuring that every action taken in their AWS environment is monitored and accounted for.



**Pre-requisites:**

### 1. AWS Account Setup: [https://youtu.be/CjKhQoYeR4Q?si=ui8Bvk\_M4FfVM-D](https://youtu.be/CjKhQoYeR4Q?si=ui8Bvk_M4FfVM-Dh)h

### 2. Understanding of CloudWatch:https://youtu.be/u4XngwbY-O0?si=6GnmUdqNQEn0zX5j

**Objective:**

To implement a real-time monitoring system that tracks IAM user activities within FinTech Corps AWS cloud environment using CloudWatch Logs and CloudTrail. The solution will generate alerts for suspicious login events, helping FinTech Corps security team proactively respond to potential security threats and maintain compliance standards.

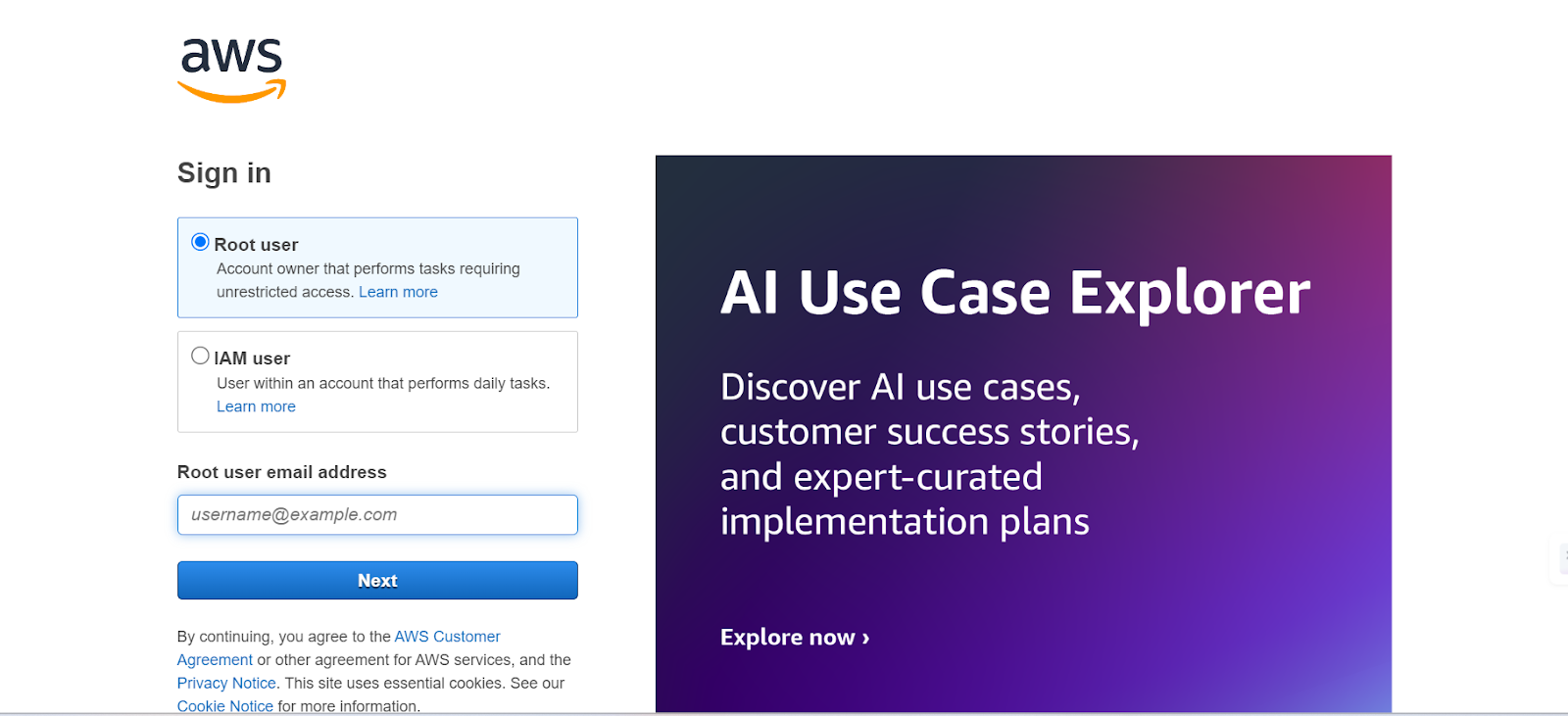
**Tasks:**

1. Log in to the AWS Management Console
2. Enable CloudTrail for Activity Logging
3. Enable Management Events in CloudTrail
4. Create a CloudWatch Metric Filter
5. Create a CloudWatch Alarm for Suspicious Activity
6. Test the Monitoring System

**Solution Development Procedure:**

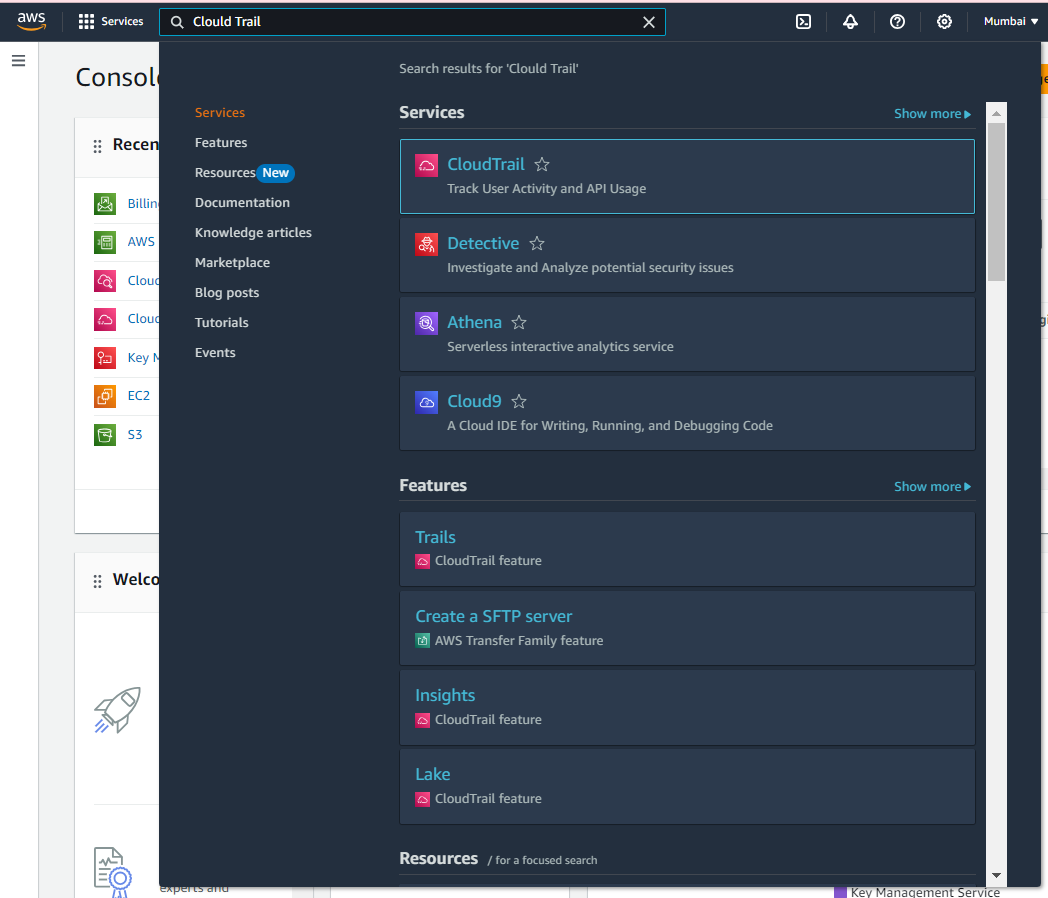
**Step 1: Login to AWS Management Console**

Open your browser and go to the [AWS Management Console](https://aws.amazon.com/console/).Enter your AWS account credentials and log in.

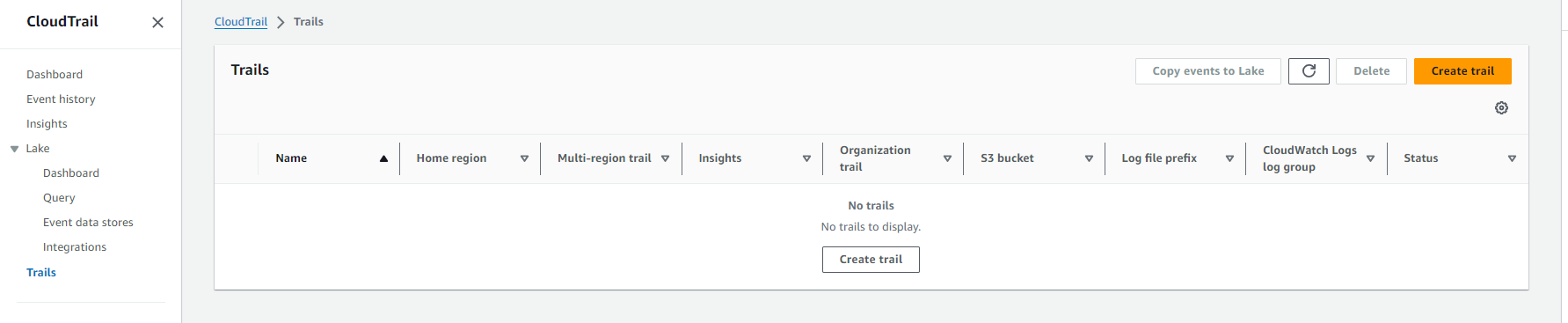


**Step 2: Enable CloudTrail for Activity Logging**

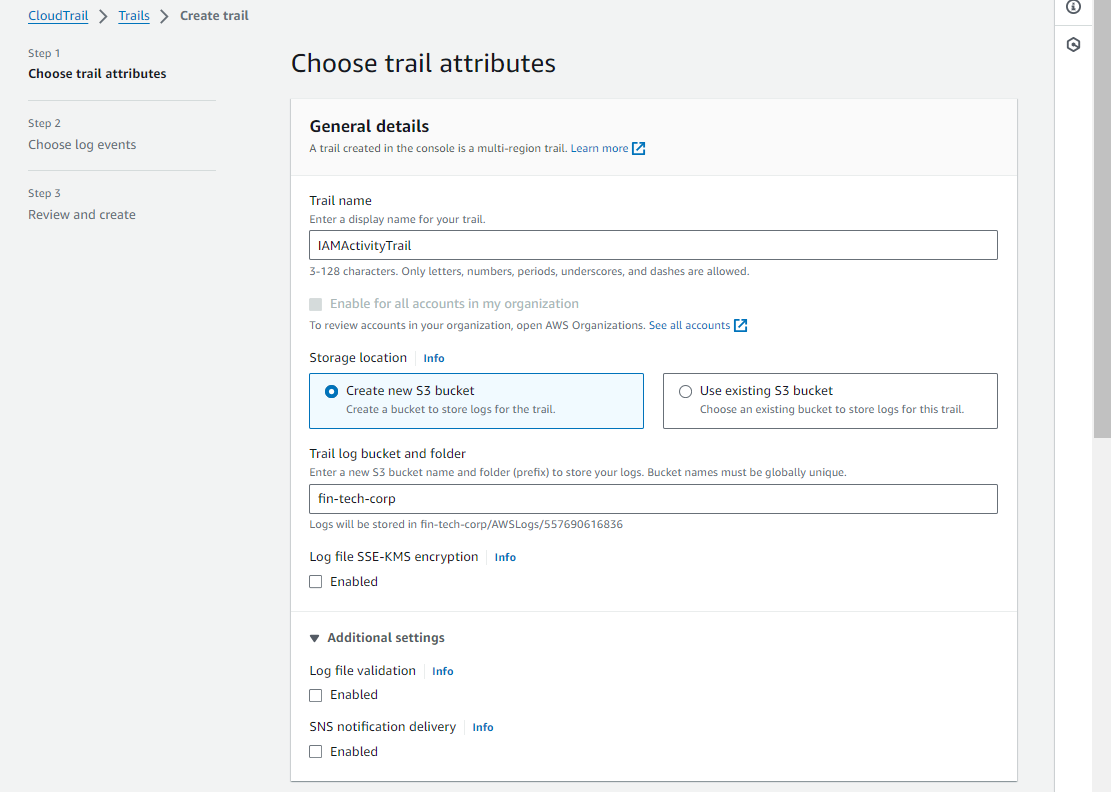
* Search for and select **CloudTrail**.



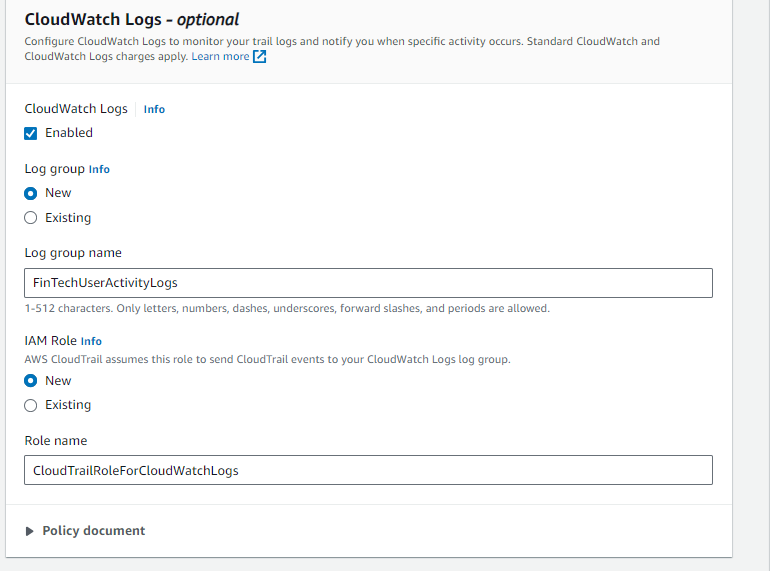
* Click on **Dashboard** to view existing trails or create a new trail.



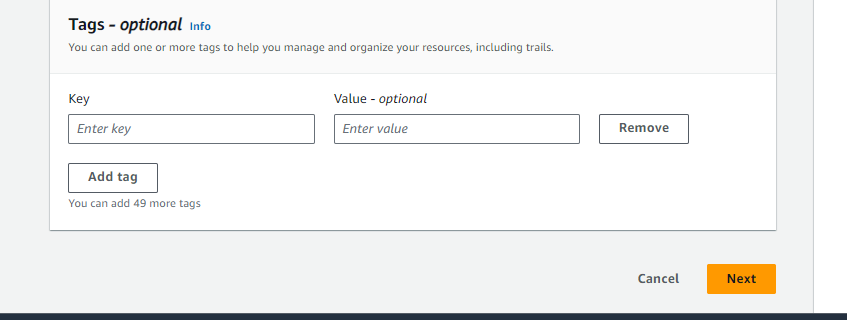
* In the CloudTrail console, click on **Create trail**. Create a new trail named **IAMActivityTrail** for **FinTechCorp**. In the **Storage location** section, select **Create a new S3 bucket** or choose an existing bucket. If creating a new bucket, specify a unique bucket name (e.g., **fin-tech-corp**). Under **Log file encryption**, keep the **SSE-KMS encryption** disabled to avoid additional charges. Select **No** for **Enable log file validation**. Leave **SNS notification delivery** disabled (optional).



* Click on **Next** to configure event settings. In the **CloudWatch Logs** section under **Choose log events**, enable **CloudWatch Logs**. Choose **Create new** and enter a log group name (e.g., **FinTechUserActivityLogs**). For **IAM Role**, select **Create a new role** if you don't have one. Name the role something like **CloudTrailRoleForCloudWatchLogs**.

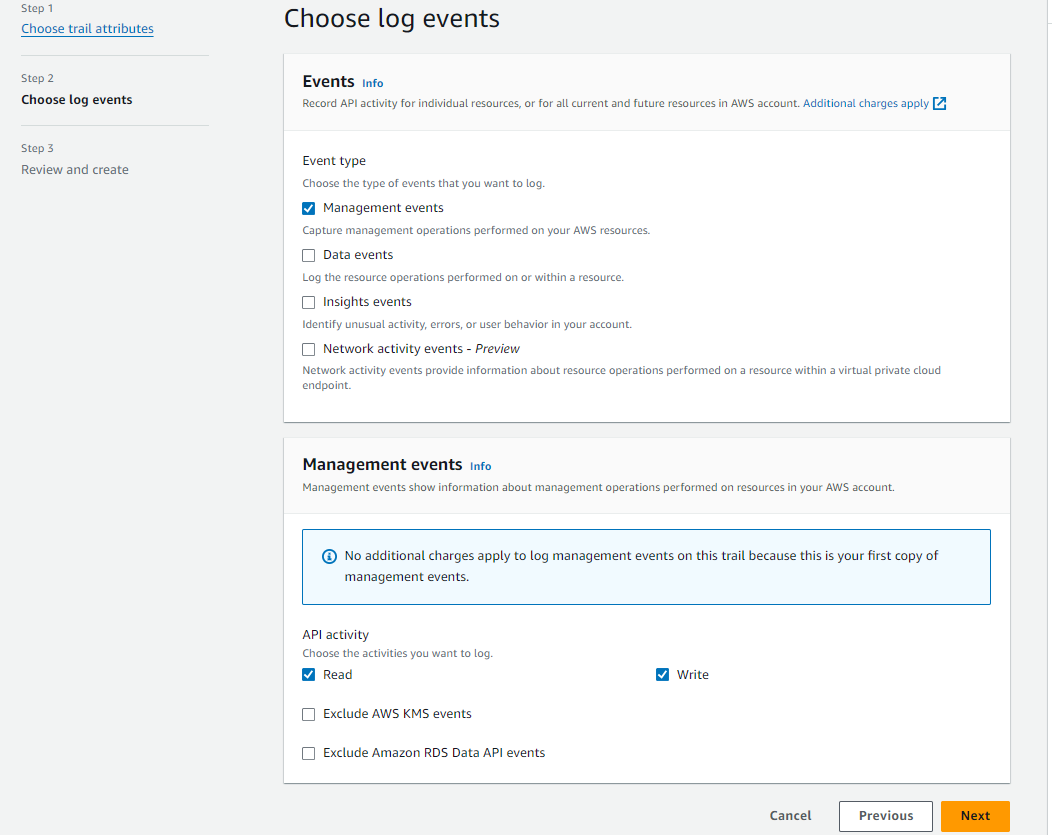


* Click Next to move to the review and create step.

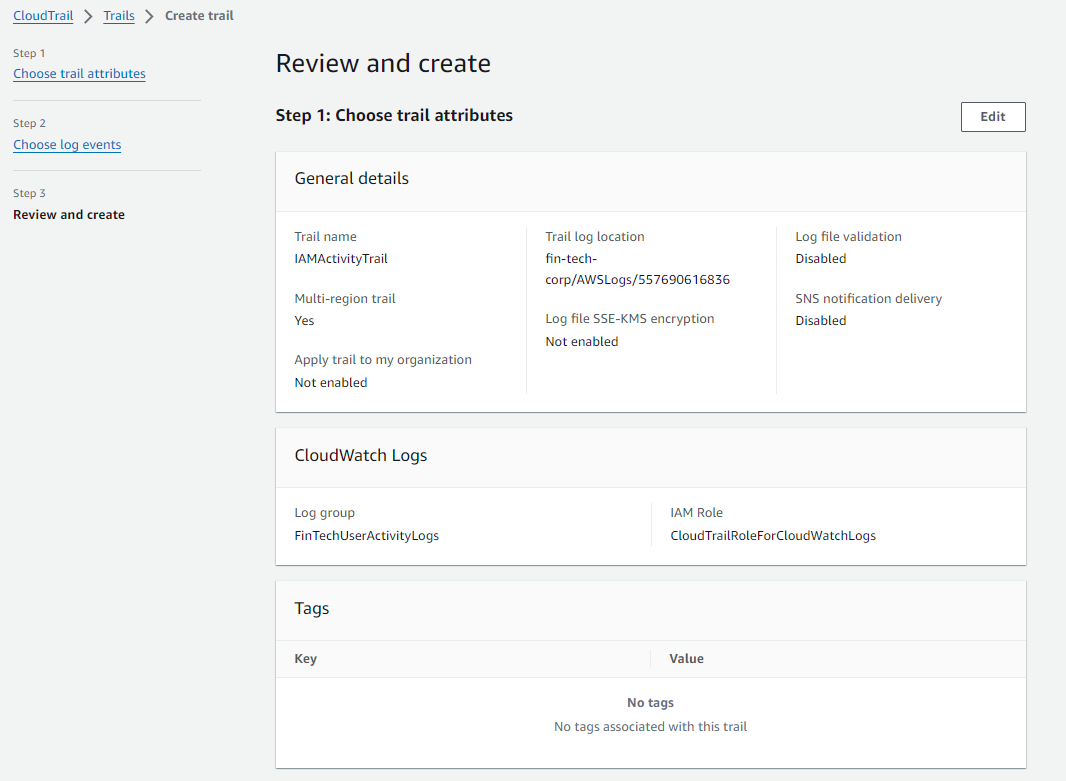


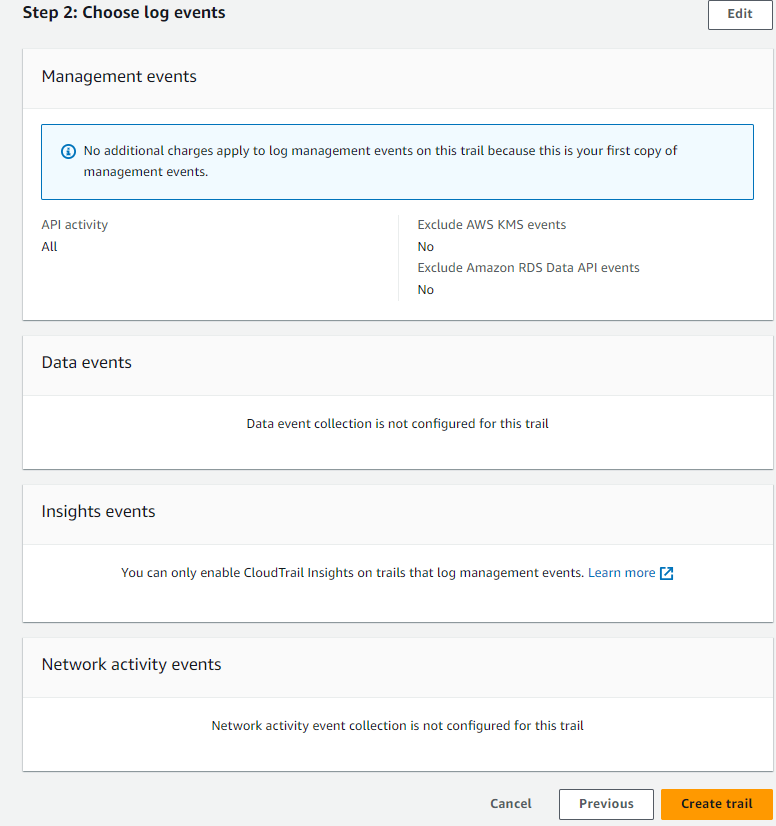
**Step 3: Enable Management Events in CloudTrail**

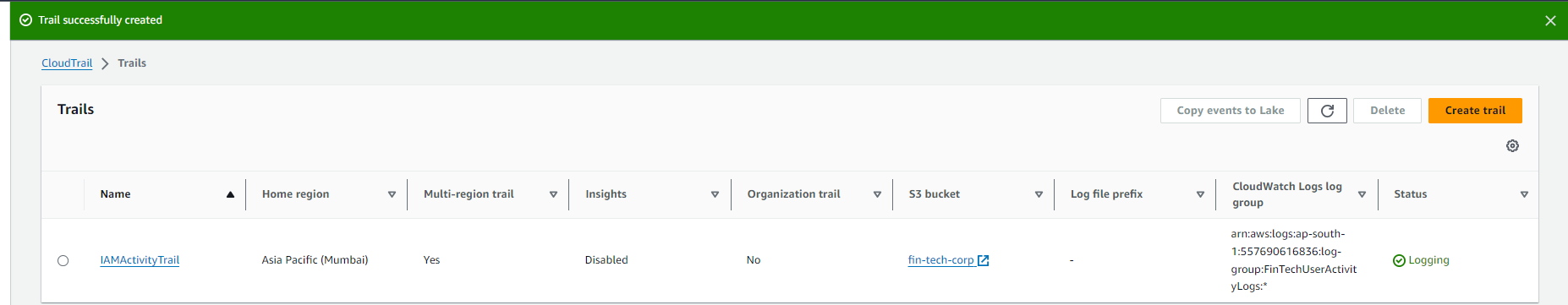
* Ensure **Management Events** are enabled to capture login activities. Enable both **Read** and **Write** events.



* Review the settings and click Create trail.

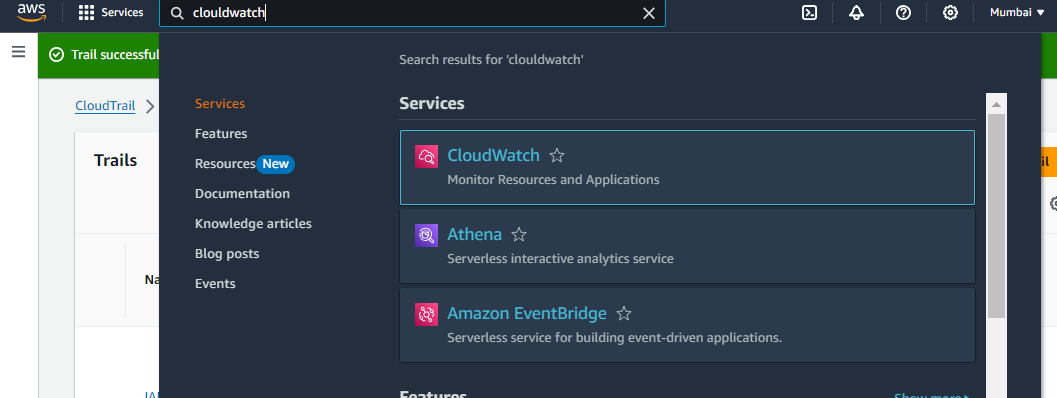




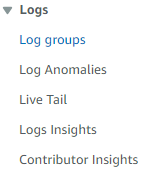


**Step 4: Create a CloudWatch Metric Filter**

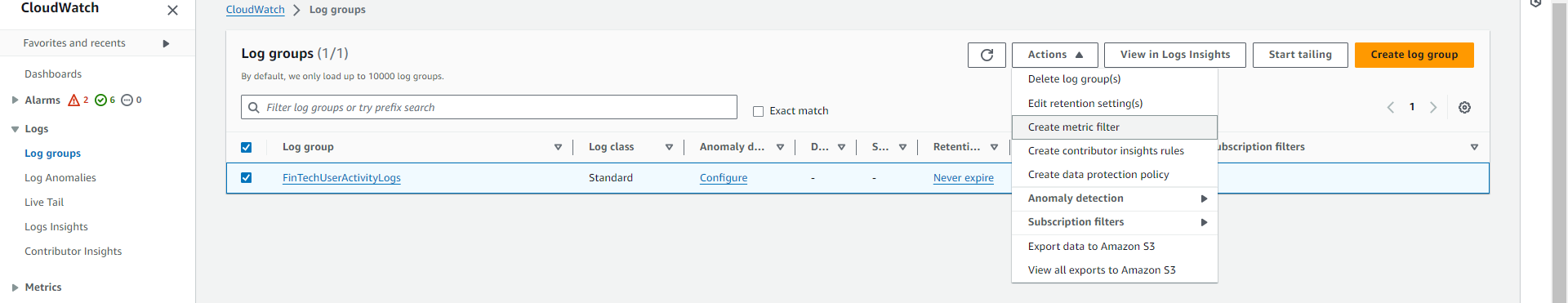
* Go to the CloudWatch Console.



* In the left-hand menu, click on Logs.

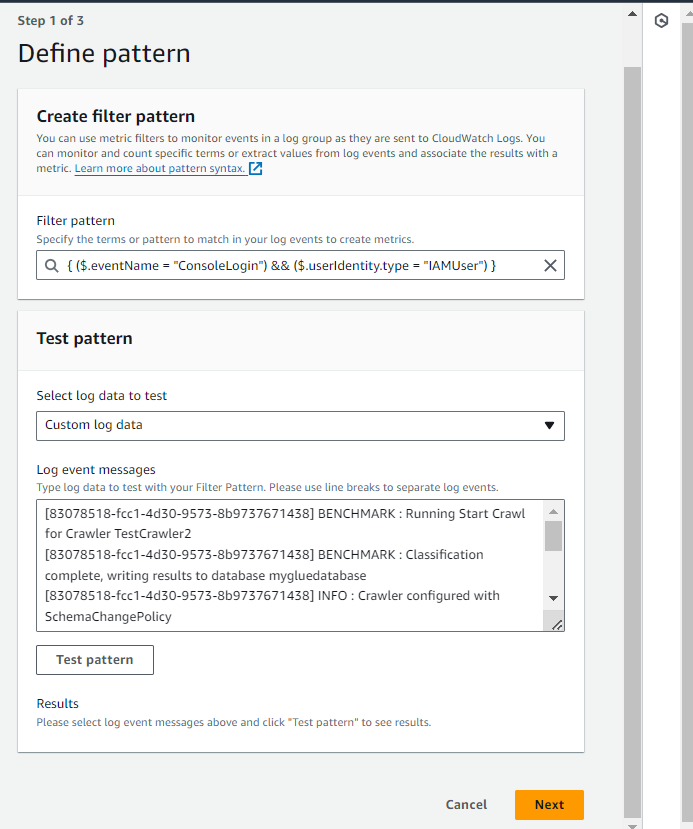


* Select the Log Group you created (FinTechUserActivityLogs) and then Actions.

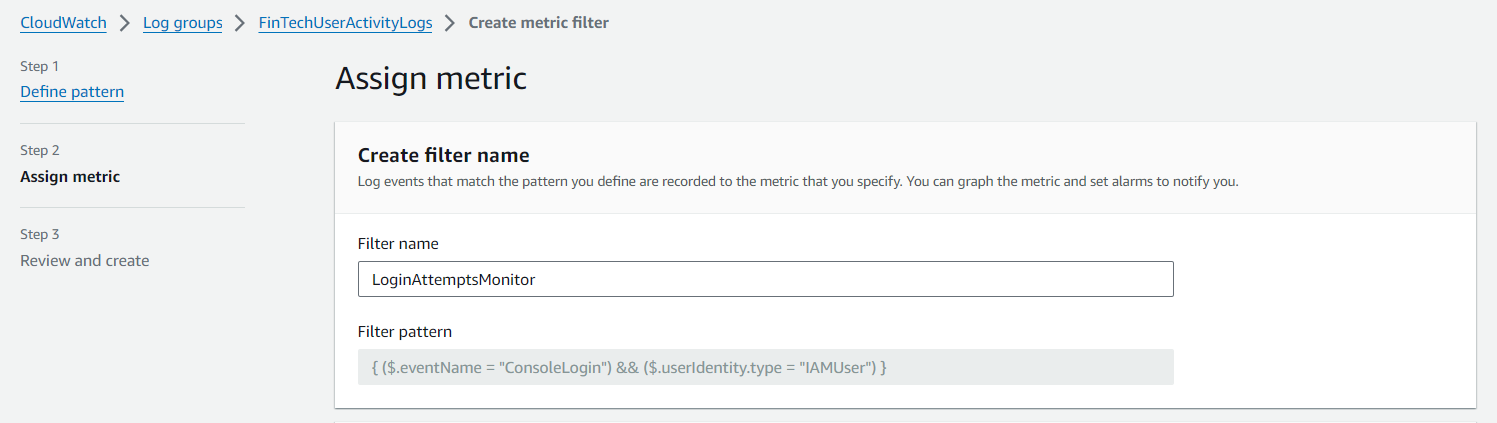


* Click **Create Metric Filter**. Enter the **Filter Pattern** as:

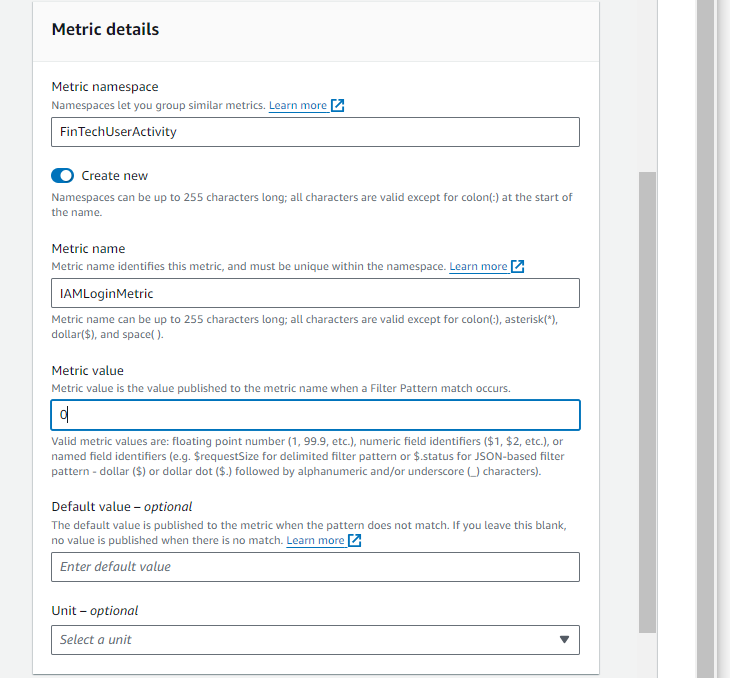
{ ($.eventName = "ConsoleLogin") && ($.userIdentity.type = "IAMUser") }

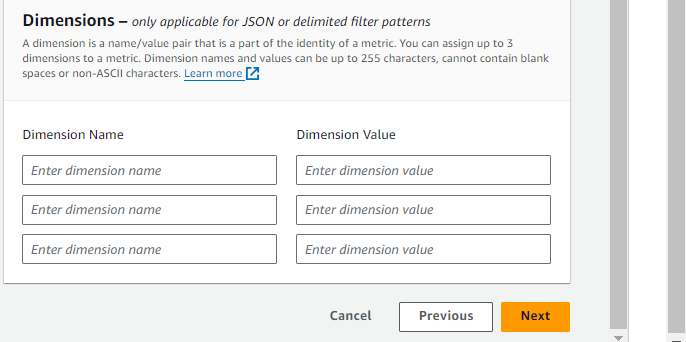


* Name the filter LoginAttemptsMonitor.

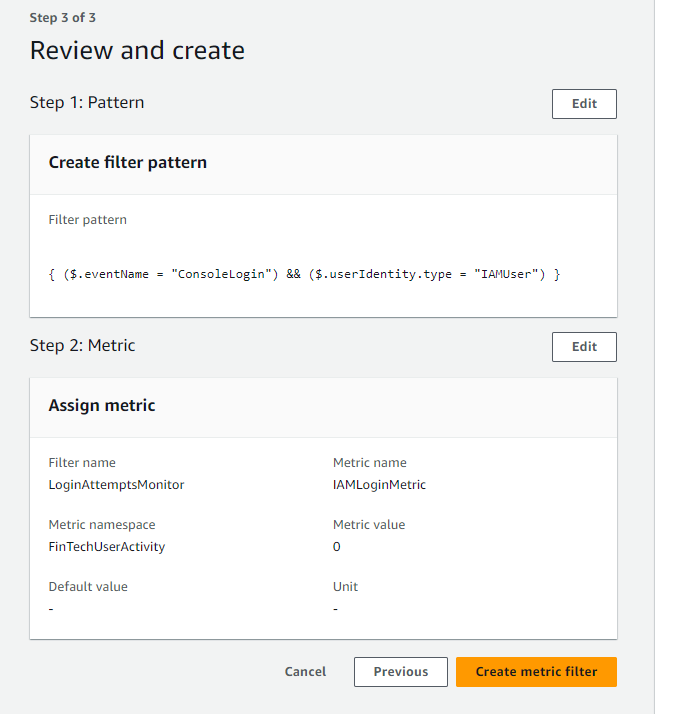


* Set the **Namespace** as FinTechUserActivity and the **Metric Name** as IAMLoginMetric.



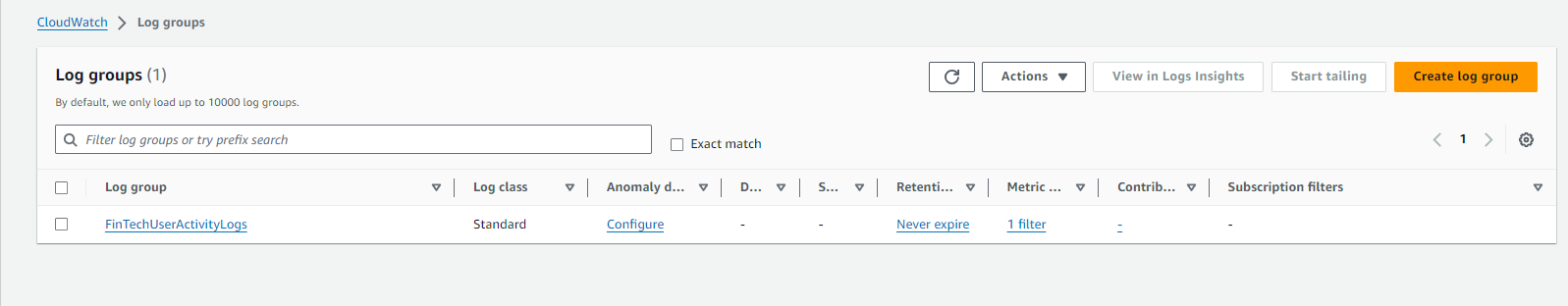


* Click **Create Filter**.

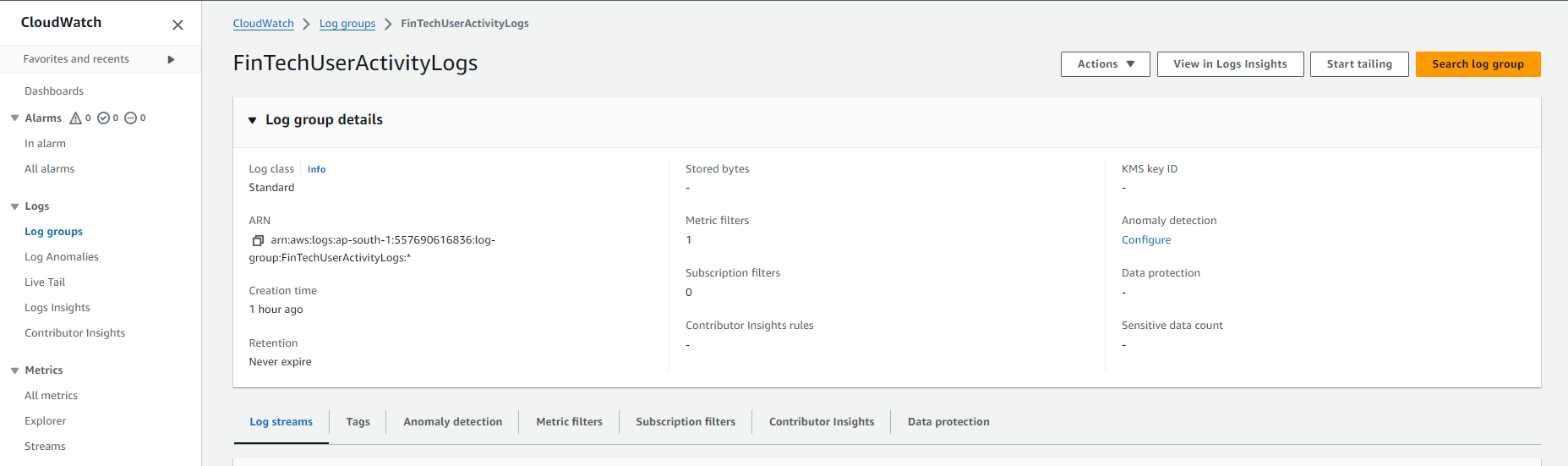


**Step 5: Create a CloudWatch Alarm for Suspicious Activity**

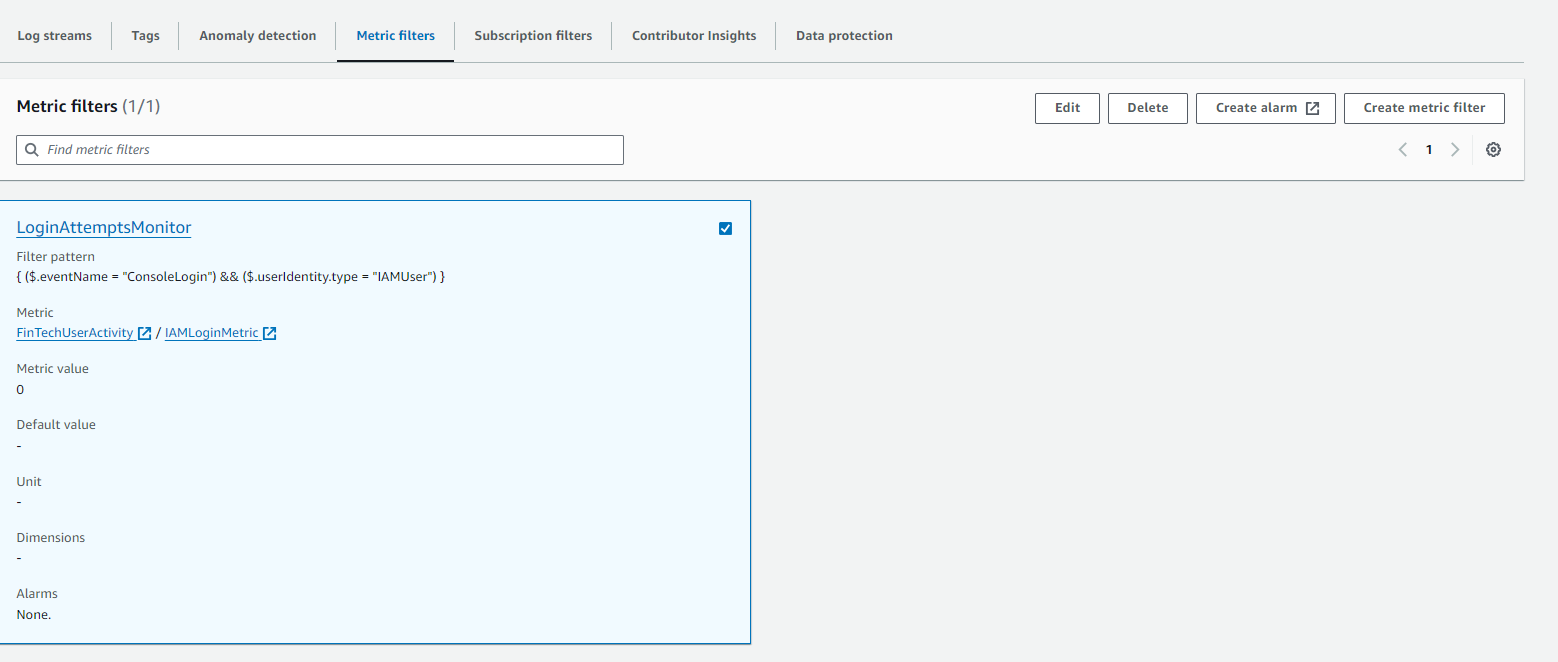
* Go to CloudWatch > log groups.



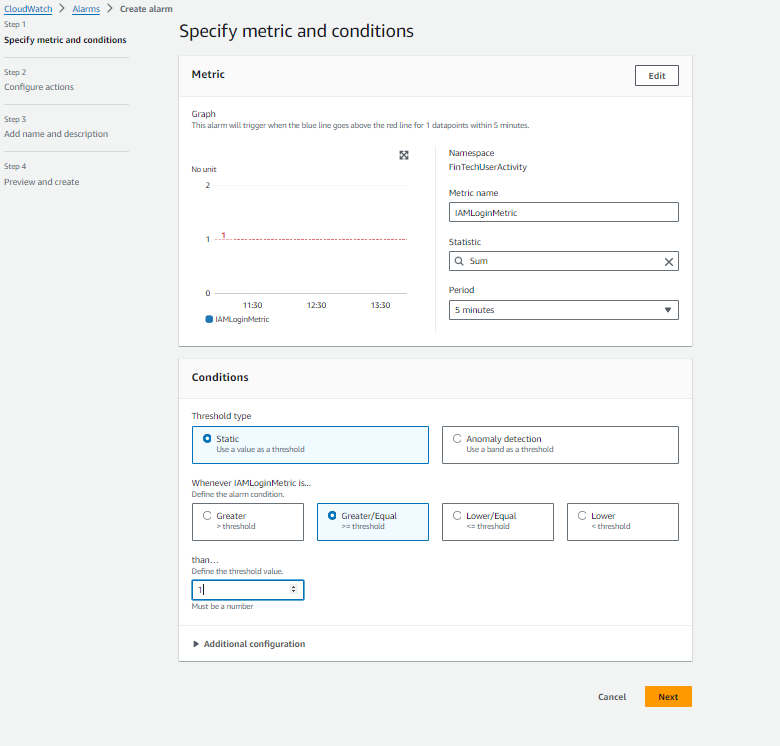
* Select the log group FinTechUserActivityLogs and metric filters in it.

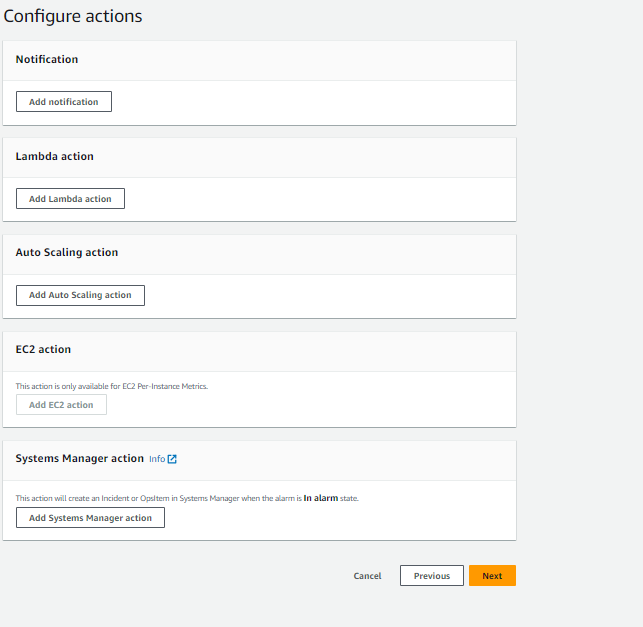


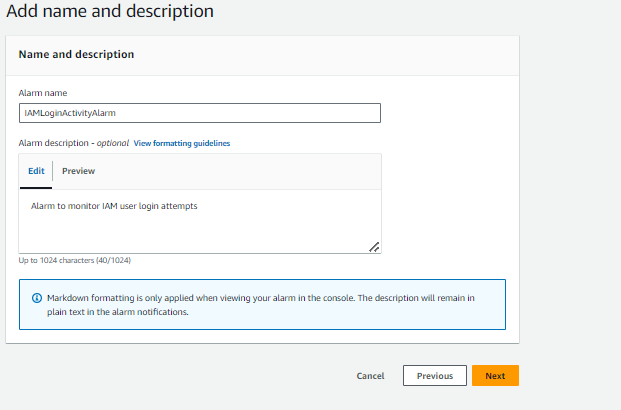
* Select the Metric filter and Click Create Alarm.



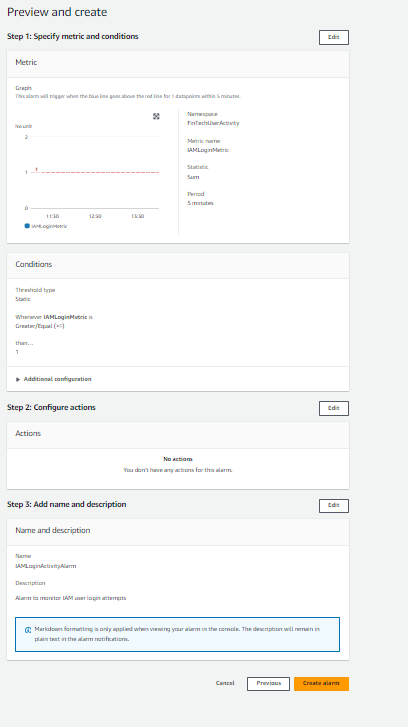
* Set the Threshold to >= 1.

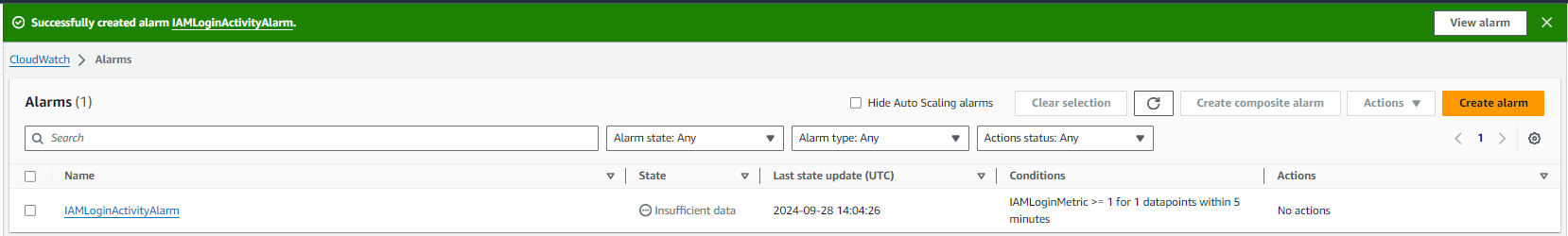






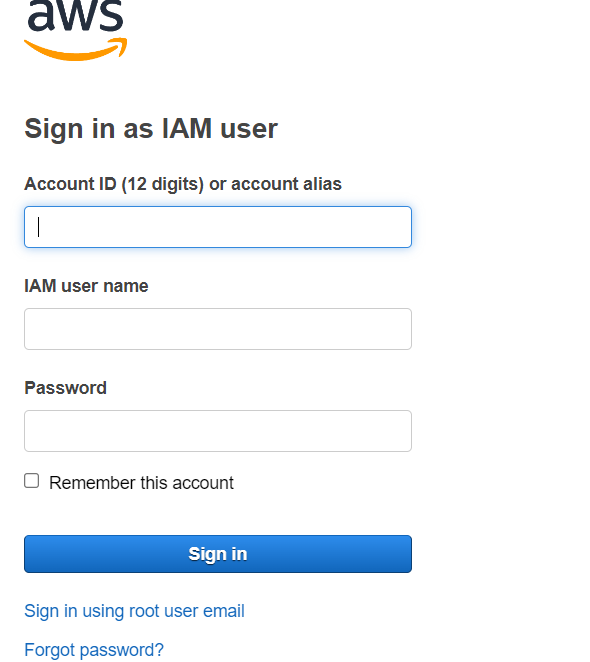
* Click Create Alarm.



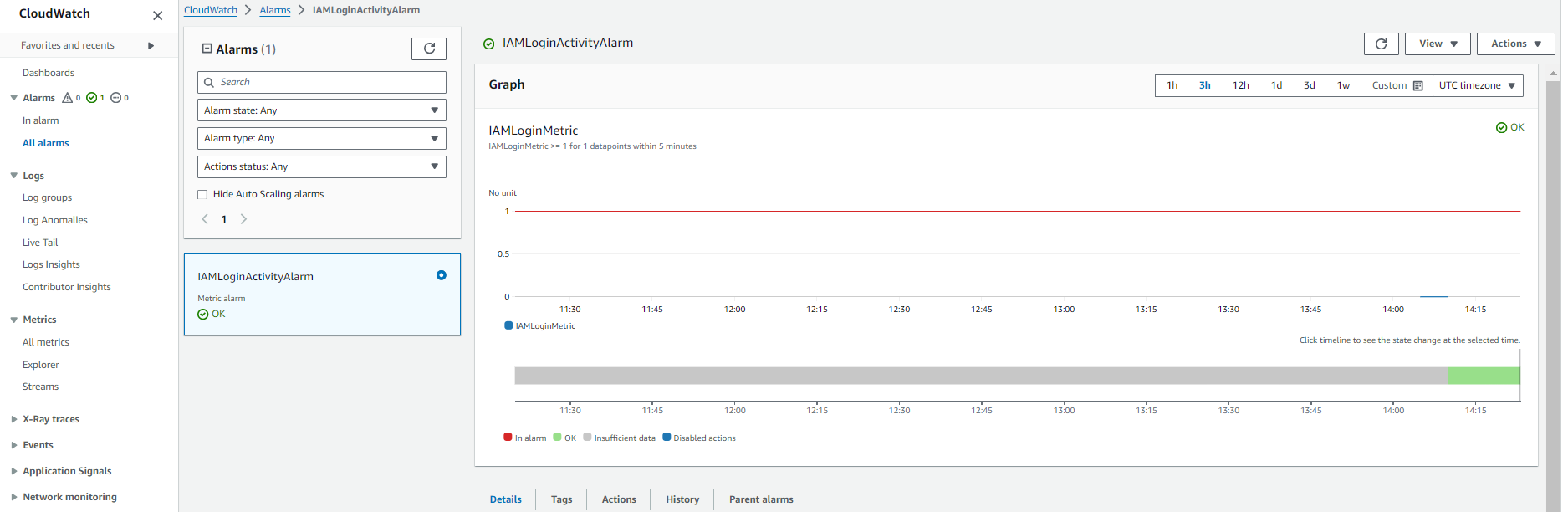


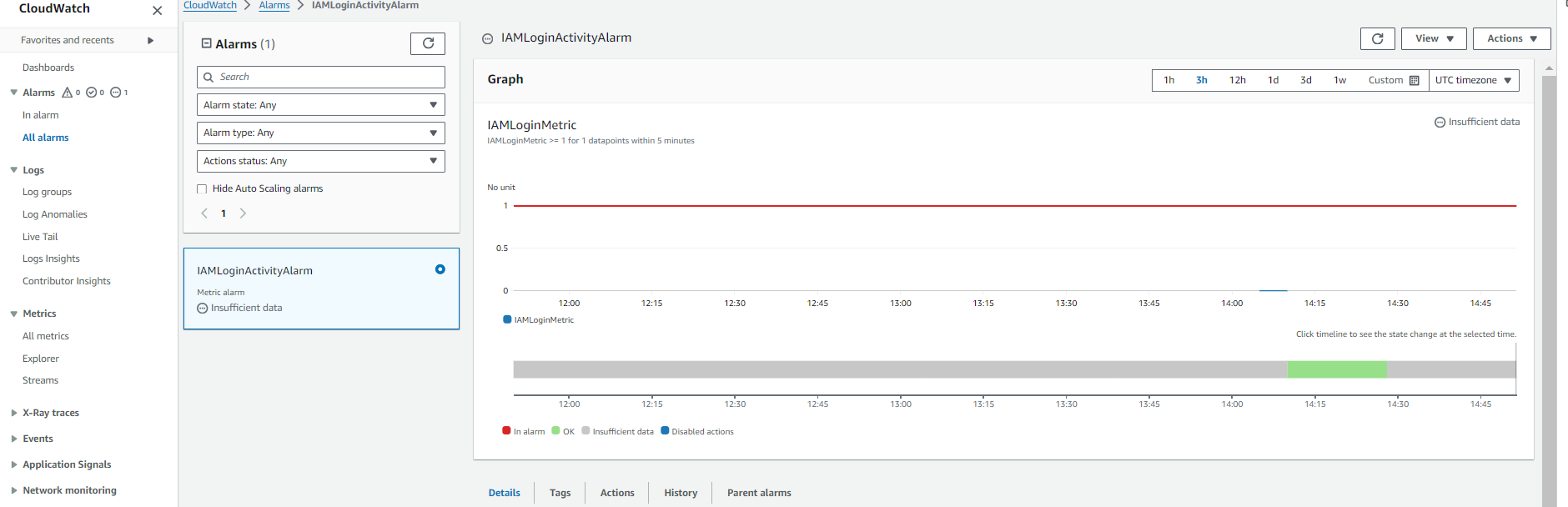
**Step 6: Test the Monitoring System**

* Log in as a test IAM user.



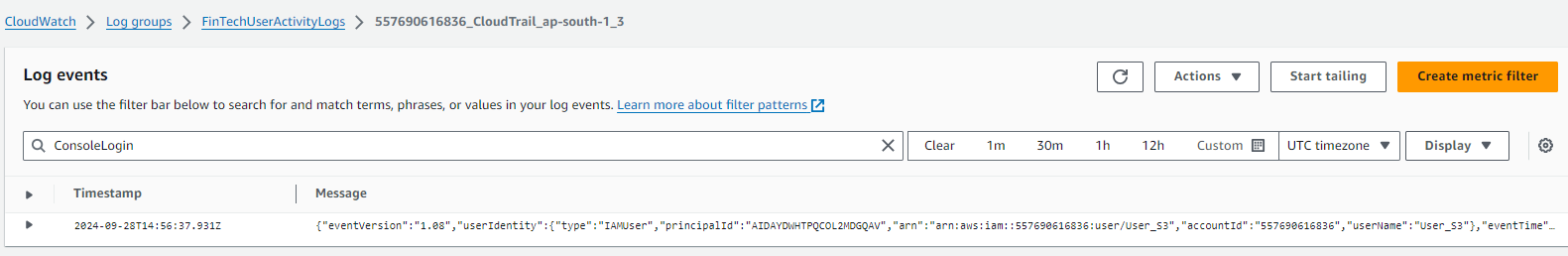
* Check CloudWatch Logs for the recorded activity.





* Verify if the Alarm triggers when a login attempt is made.



****

**Conclusion:**

By implementing this monitoring system, FinTechCorp successfully established real-time tracking of IAM user activities, enhancing their compliance posture and security monitoring. The solution ensures that every IAM user action is accounted for, enabling FinTechCorp to maintain a proactive security stance and respond swiftly to any suspicious activities, safeguarding the trust of their customers.