

AWS LAB Cloud-Trail | Monarch Nigam

[EXERCISE 7.1](#)

In this exercise, we will configure CloudTrail to log write-only management events in all regions.

1. Browse to the CloudTrail service console and click the Create Trail button.
2. Under Trail Name, enter a trail name of your choice. Names must be at least three characters and can't contain spaces.
3. Under the Storage Location heading, select Create New S3 Bucket. Enter the name of the S3 bucket you want to use. Remember that bucket names must be globally unique.
4. Under Log File SSE-KMS Encryption, clear the box next to Enabled.

The screenshot shows the AWS CloudTrail 'Create trail' console page. The page is titled 'Choose trail attributes' and is part of a multi-step process. The steps are: Step 1: Choose trail attributes (selected), Step 2: Choose log events, and Step 3: Review and create. The 'General details' section includes a 'Trail name' field with the value 'monarch-trail'. The 'Storage location' section has two options: 'Create new S3 bucket' (selected) and 'Use existing S3 bucket'. The 'Trail log bucket and folder' section has a text field with the value 'monarch-cloudtrail-logs-160885292183-6d7a35d6'. The 'Log file SSE-KMS encryption' section has a checkbox labeled 'Enabled' which is currently checked. The 'Additional settings' section has a 'Log file validation' checkbox labeled 'Enabled' which is also checked.

Step 1: Choose trail attributes

Step 2: Choose log events

Step 3: Review and create

Choose trail attributes

General details
A trail created in the console is a multi-region trail. [Learn more](#)

Trail name
Enter a display name for your trail.

3-128 characters. Only letters, numbers, periods, underscores, and dashes are allowed.

☐ Enable for all accounts in my organization
To review accounts in your organization, open AWS Organizations. [See all accounts](#)

Storage location [Info](#)

☒ **Create new S3 bucket**
Create a bucket to store logs for the trail.

☐ **Use existing S3 bucket**
Choose an existing bucket to store logs for this trail.

Trail log bucket and folder
Enter a new S3 bucket name and folder (prefix) to store your logs. Bucket names must be globally unique.

Logs will be stored in monarch-cloudtrail-logs-160885292183-6d7a35d6/AWSLogs/160885292183

Log file SSE-KMS encryption [Info](#)
☐ Enabled

Additional settings

Log file validation [Info](#)
☒ Enabled

5. Enter a custom name for the AWS KMS Alias.
6. Leave all other settings at their defaults and click the Next button.
7. Under Event Types, select the box next to Management Events. Don't select any other boxes.
8. Under Management Events, make sure only Write is selected.

The screenshot shows the AWS CloudTrail console. The breadcrumb navigation is: CloudTrail > Trails > arn:aws:cloudtrail:us-east-1:160885292183:trail/monarch-trail > Edit. The page title is 'Edit arn:aws:cloudtrail:us-east-1:160885292183:trail/monarch-trail'. There are two main sections: 'Events' and 'Management events'. The 'Events' section has a sub-section 'Event type' with a checkbox for 'Management events' which is checked. The 'Management events' section has a sub-section 'API activity' with checkboxes for 'Read', 'Write', 'Exclude AWS KMS events', and 'Exclude Amazon RDS Data API events'. The 'Write' checkbox is checked. At the bottom right, there are 'Cancel' and 'Save changes' buttons.

Events [info](#)
Record API activity for individual resources, or for all current and future resources in AWS account. [Additional charges apply](#)

Event type
Choose the type of events that you want to log.

☒ **Management events**
Capture management operations performed on your AWS resources.

Management events [info](#)
Management events show information about management operations performed on resources in your AWS account.

API activity
Choose the activities you want to log.

☐ Read ☒ Write

☐ Exclude AWS KMS events

☐ Exclude Amazon RDS Data API events

[Cancel](#) [Save changes](#)

9. Click Next.
10. Review the settings and click the Create Trail button.

The screenshot shows the AWS CloudTrail Trails console. At the top, there's a navigation bar with the AWS logo, a search bar, and the text "[Option+S]". Below the navigation bar, there's a breadcrumb trail "CloudTrail > Trails". A green notification bar at the top says "Trail successfully created". Below that, a blue notification bar says "What's new: Strengthen your data perimeter and implement better detective controls for your VPC endpoints by enabling Network activity events on your Trail or CloudTrail Lake. [Learn more](#)".

The main content area is titled "Trails". It has a toolbar with buttons: "Copy events to Lake", "Delete", and "Create trail". Below the toolbar is a table with the following columns: Name, Home region, Multi-region trail, Insights, Organization trail, S3 bucket, Log file prefix, CloudWatch Logs log group, and Status.

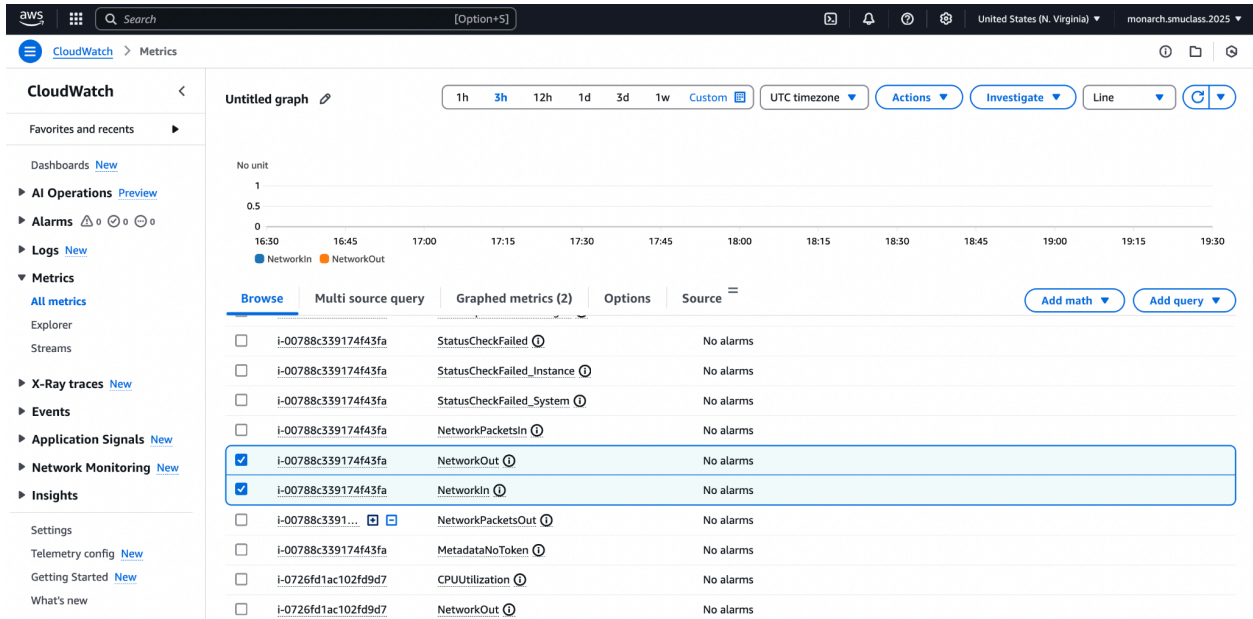
Name	Home region	Multi-region trail	Insights	Organization trail	S3 bucket	Log file prefix	CloudWatch Logs log group	Status
monarch-trail	US East (N. Virginia)	Yes	Disabled	No	monarch-cloudtrail-logs-160885292183-6d7a35d6	-	-	Logging

EXERCISE 7.2

Create a Graph Using Metric Math

In this exercise, we'll create a graph that plots the **NetworkIn** and **NetworkOut** metrics for an EC2 instance. You'll then use metric math to graph a new time series combining both metrics.

1. Browse to the CloudWatch service console and expand Metrics on the navigation menu.
2. Click All Metrics.
3. On the Browse tab, descend into the **EC2** namespace. Select **Per-Instance Metrics**; then locate and select the **NetworkIn** and **NetworkOut** metrics.



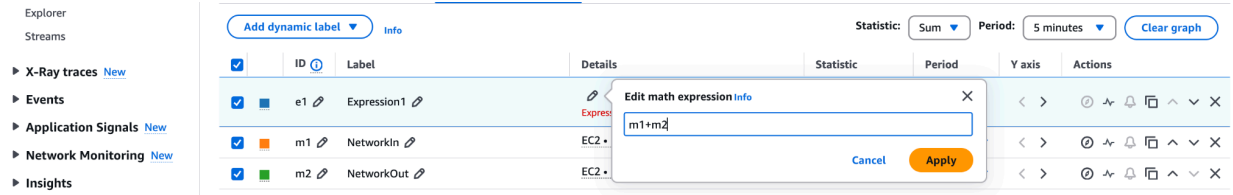
4. Click the Graphed Metrics tab.

5. For each metric, select Sum for Statistic and 5 Minutes for Period. Refer to [Figure 7.2](#) as needed.

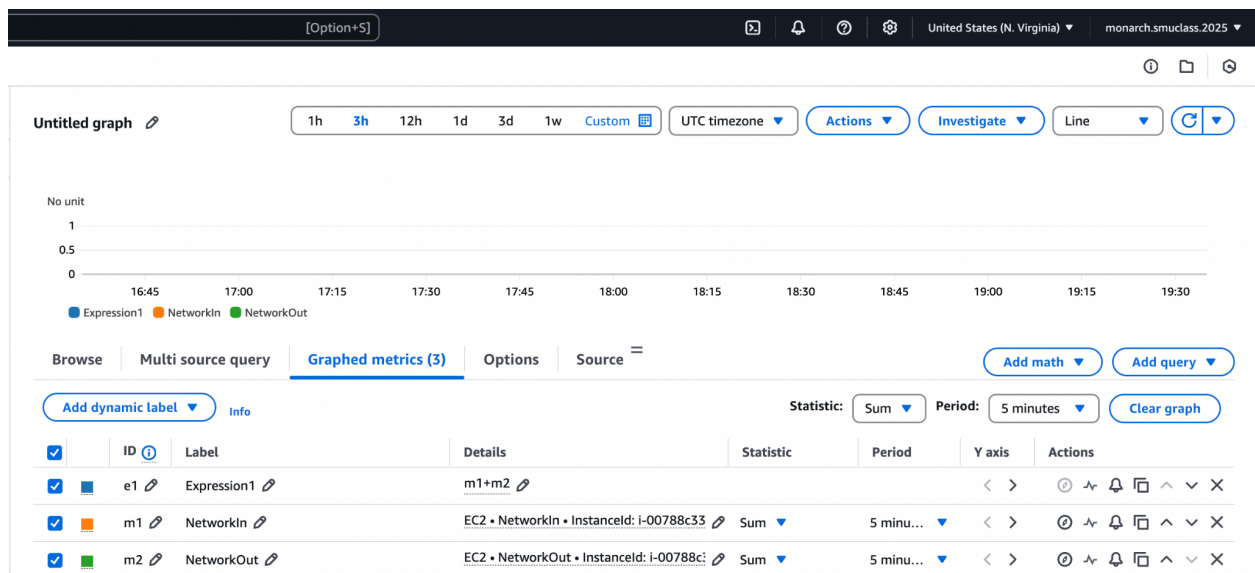
Explorer Streams	<div> Add dynamic label Info </div>						Statistic: Sum	Period: 5 minutes	Clear graph
▶ X-Ray traces New	<input checked="" type="checkbox"/>	Label	Details	Statistic	Period	Y axis	Actions		
▶ Events	<input checked="" type="checkbox"/>	NetworkIn	EC2 • NetworkIn • InstanceId: i-00788c333	Sum	5 minu...	< >	🕒 🔔 📄 ^ v ✕		
▶ Application Signals New	<input checked="" type="checkbox"/>	NetworkOut	EC2 • NetworkOut • InstanceId: i-00788c333	Sum	5 minu...	< >	🕒 🔔 📄 ^ v ✕		

6. Click the Add Math button and select Start With Empty Expression.

7. In the Edit Math Expression field, enter the expression m1+m2.



8. Click the Apply button. CloudWatch will add another time series to the graph representing the sum of the NetworkIn and NetworkOut metrics.



As you can see in the above snapshot, the graph has expression 1 with $m1+m2$, but there is no graph lines as all the previous EC2 instances are deleted to save unnecessary costs.

EXERCISE 7.3

In this exercise, we'll reconfigure the trail you created in [Exercise 7.1](#) to stream events captured by CloudTrail to CloudWatch Logs.

1. Browse to the CloudTrail service console and click Trails.
2. Click the name of the trail you created in [Exercise 7.1](#).
3. Under the heading CloudWatch Logs, click the Edit button.
4. Under CloudWatch Logs, select the Enabled check box.

aws [Search] [Option+S] United States (N. Virginia) monarch.smuclass.2025

CloudTrail > Trails > [arn:aws:cloudtrail:us-east-1:160885292183:trail/monarch-trail](#) > Edit

Edit [arn:aws:cloudtrail:us-east-1:160885292183:trail/monarch-trail](#) [Info](#)

CloudWatch Logs - optional
Configure CloudWatch Logs to monitor your trail logs and notify you when specific activity occurs. Standard CloudWatch and CloudWatch Logs charges apply. [Learn more](#)

CloudWatch Logs [Info](#)

☒ Enabled

Log group [Info](#)

☒ New
☐ Existing

Log group name

1-512 characters. Only letters, numbers, dashes, underscores, forward slashes, and periods are allowed.

IAM Role [Info](#)
AWS CloudTrail assumes this role to send CloudTrail events to your CloudWatch Logs log group.

☒ New
☐ Existing

Role name

[Policy document](#)

[Cancel](#) [Save changes](#)

5. CloudTrail prompts you to use a New or Existing Log Group. Select New and enter a log group name of your choice. In the above snapshot we can see that i gave the name **monarch-aws-cloudtrail-logs-...**
6. CloudTrail must assume an IAM role that will give it permissions to stream logs to CloudWatch Logs. CloudTrail can create the role for you. Just click the New radio button under IAM Role. Enter a custom role name of your choice. In the above snapshot we can see the IAM Role name i gave is **monarch-cloudtrail-role**
7. Click the Save Changes button.

[Delete](#) [Stop logging](#)

[Edit](#)

✔ Logging

Multi-region trail
Yes

[Edit](#)

arn:aws:iam::160885292183:role/service-role/monarch-cloudtrail-role