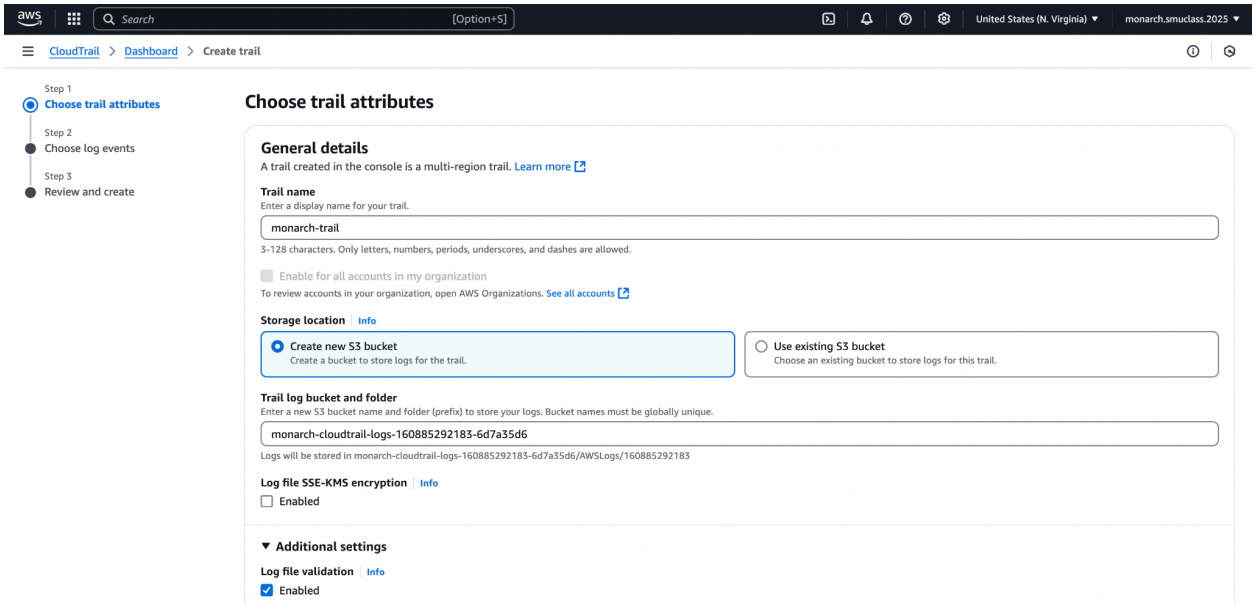
AWS LAB Cloud-Trail | Monarch Nigam

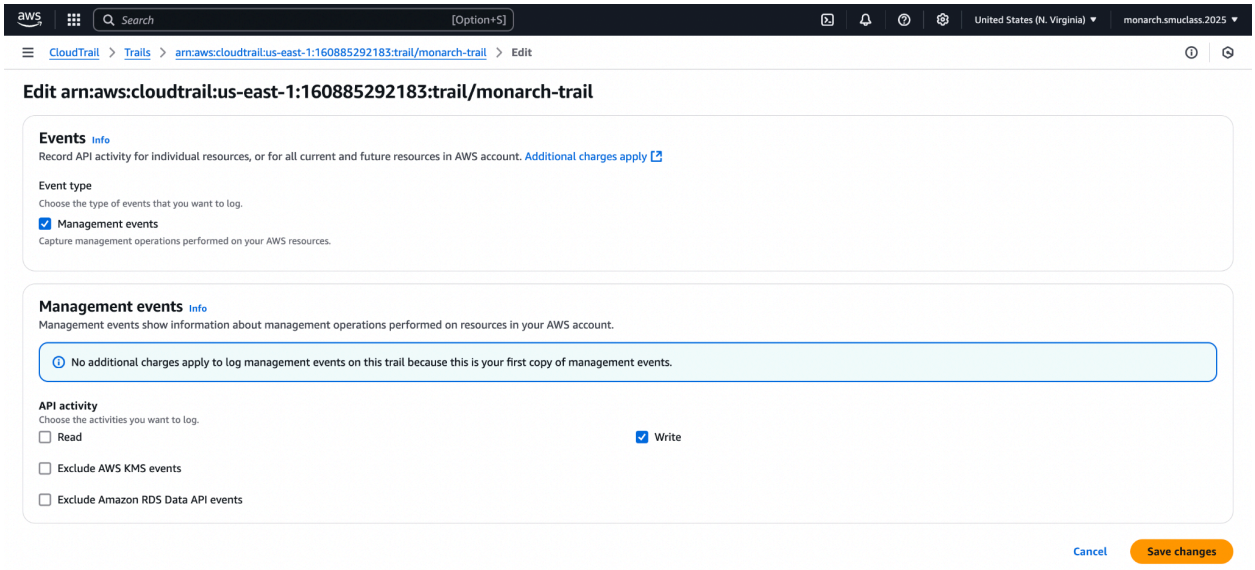
EXERCISE 7.1

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

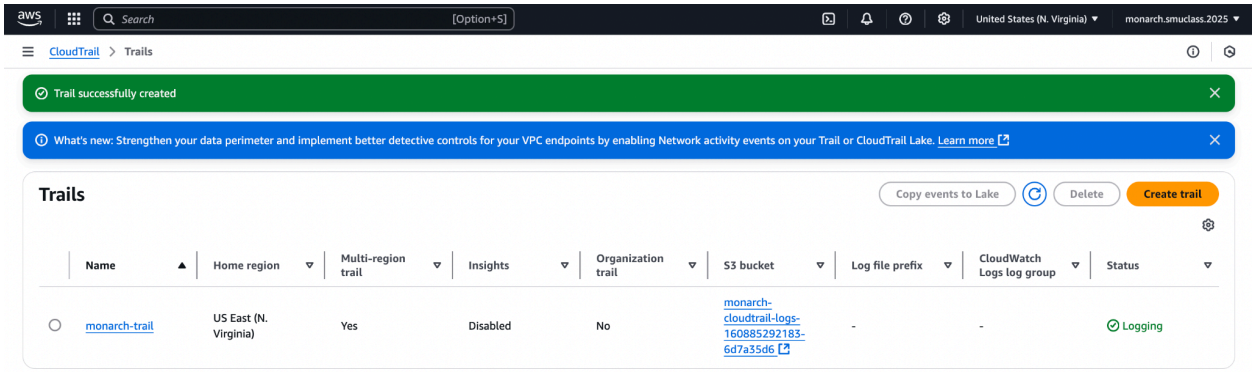
1. **Browse to the CloudTrail service console and click the Create Trail button.**
2. **Under Trail Name, enter a trail name of your choice. Names must be at least three characters and can't contain spaces.**
3. **Under the Storage Location heading, select Create New S3 Bucket. Enter the name of the 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.**



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.



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

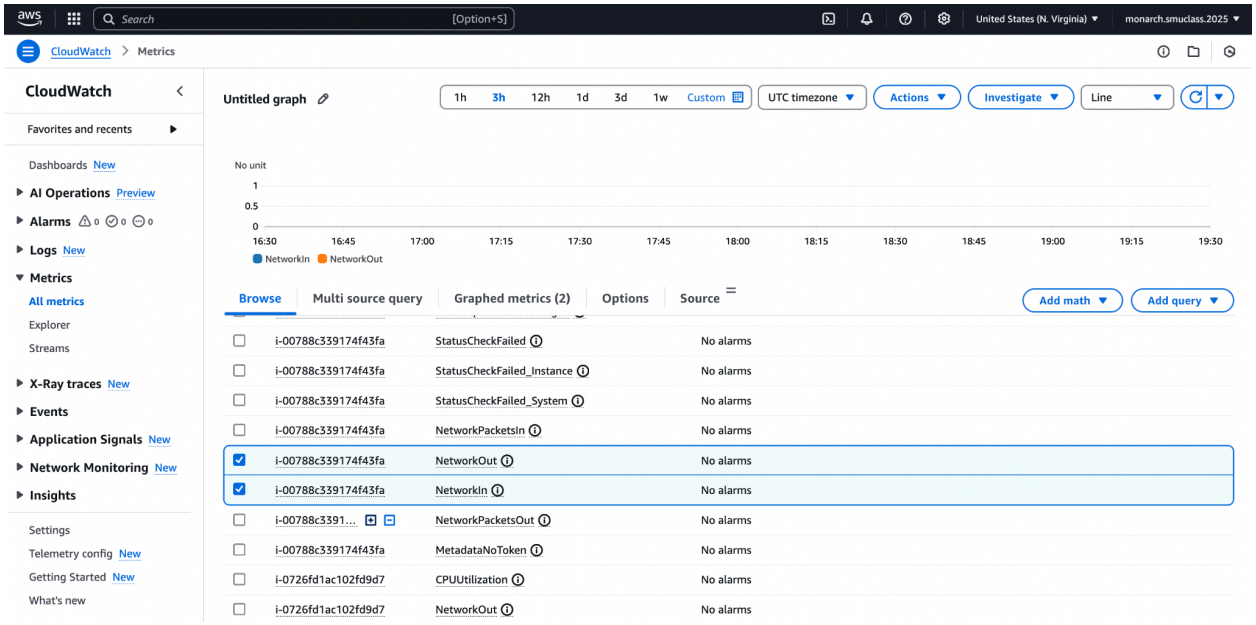


EXERCISE 7.2

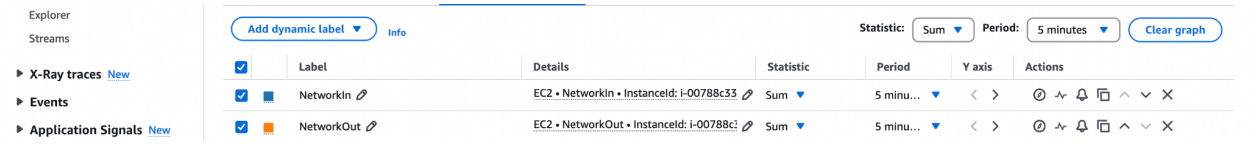
Create a Graph Using Metric Math

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.

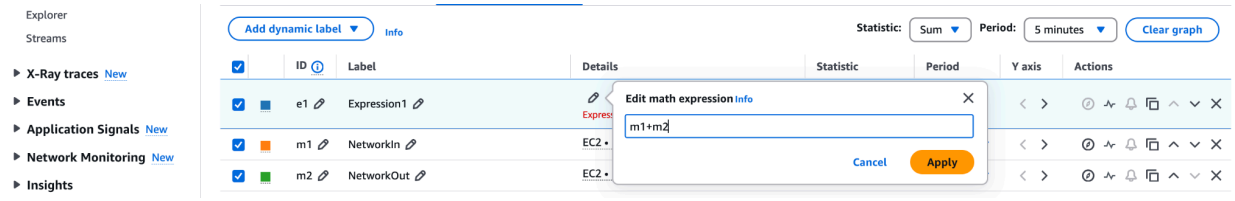
1. **Browse to the CloudWatch service console and expand Metrics on the navigation menu.**
2. **Click All Metrics.**
3. **On the Browse tab, descend into the EC2 namespace. Select Per-Instance Metrics; then locate and select the NetworkIn and NetworkOut metrics.**



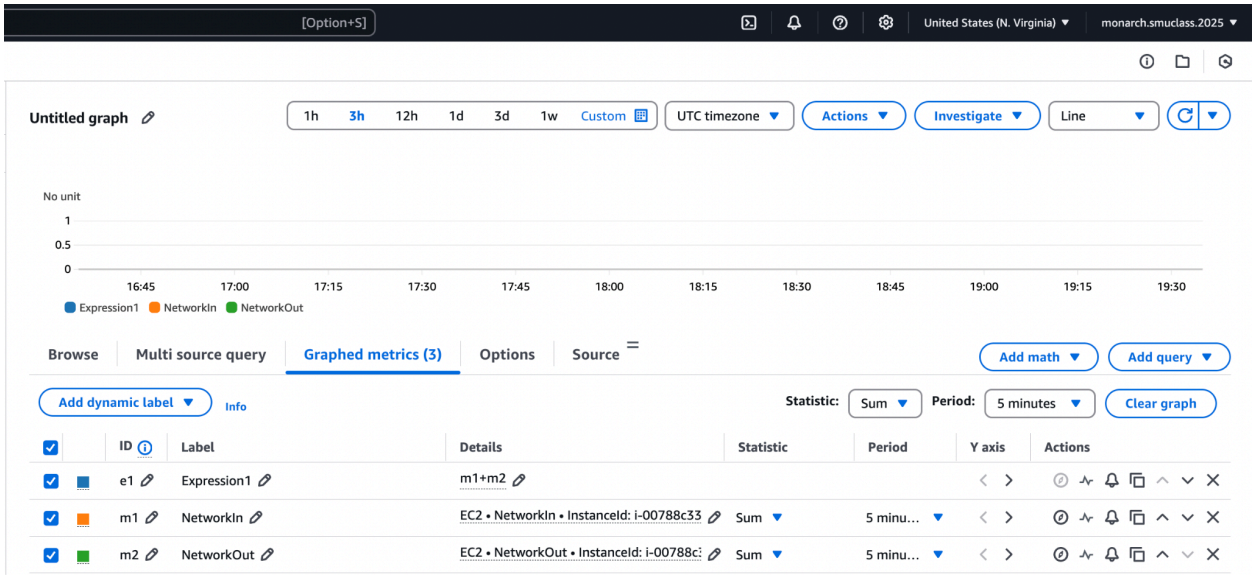
4. Click the Graphed Metrics tab.
5. For each metric, select Sum for Statistic and 5 Minutes for Period. Refer to Figure 7.2 as needed.



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.**

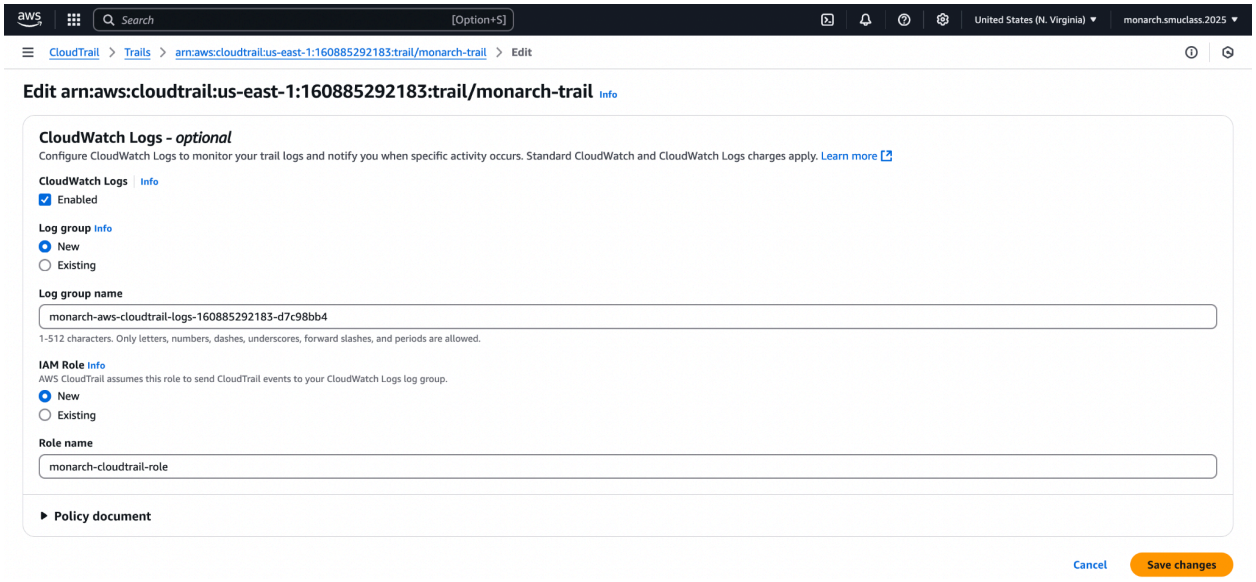


As you can see in the above snapshot, the graph has expression 1 with m1+m2, but there is no graph lines as all the previous EC2 instances are deleted to save unnecessary costs.

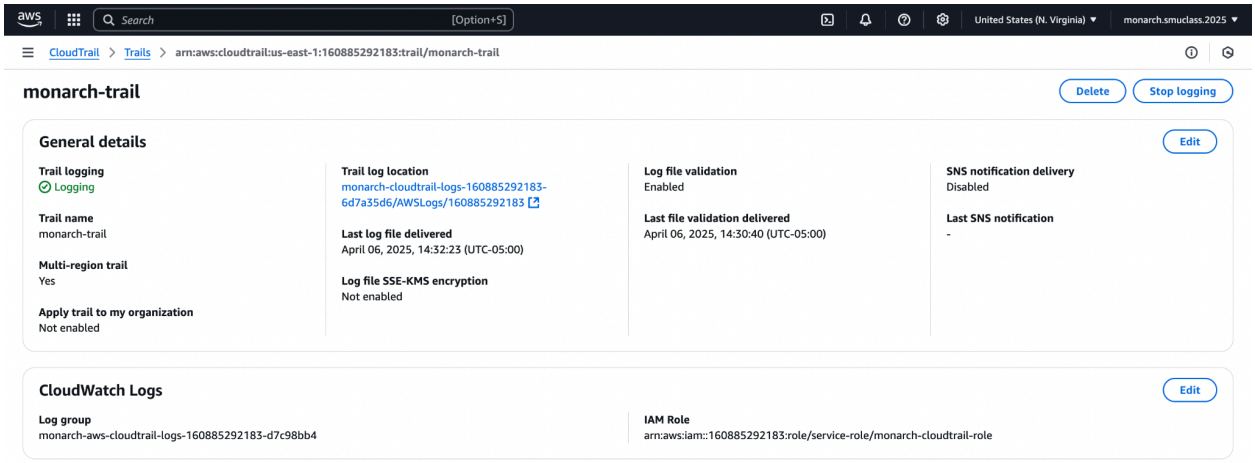
EXERCISE 7.3

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.



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.


Search
[Option+S]
United States (N. Virginia)
monarch.smuclass.2025
CloudTrail
Trails
arn:aws:cloudtrail:us-east-1:160885292183:trail/monarch-trail
monarch-trail
Delete
Stop logging
General details
Edit
Trail logging
Logging
Trail name
monarch-trail
Multi-region trail
Yes
Apply trail to my organization
Not enabled
Trail log location
monarch-cloudtrail-logs-160885292183-6d7a35d6/AWSLogs/160885292183
Last log file delivered
April 06, 2025, 14:32:23 (UTC-05:00)
Log file SSE-KMS encryption
Not enabled
Log file validation
Enabled
Last file validation delivered
April 06, 2025, 14:30:40 (UTC-05:00)
SNS notification delivery
Disabled
Last SNS notification
-
CloudWatch Logs
Edit
Log group
monarch-aws-cloudtrail-logs-160885292183-d7c98bb4
IAM Role
arn:aws:iam::160885292183:role/service-role/monarch-cloudtrail-role