CS7346 Lab 5: CloudTrail, CloudWatch, and AWS Config

Name: Bingying Liang
ID: 48999397

July 10 2023

To support the following lab exercises, please read the following chapters in the AWS Certified Solutions Architect Study Guide.

Chapter 7

Lab: Please complete the following lab exercises in the AWS Certified Solutions Architect Study Guide. When you are done, delete all the resources that you provisioned to avoid charges.

7.1 through 7.3 (inclusive)

Environment

Laptop: MacBook Air M2 2022, macOS 13.3

Chapter 7

7.1

EXERCISE 7.1

Create a Trail

In this exercise, you'll configure CloudTrail to log write-only management events in all regions.

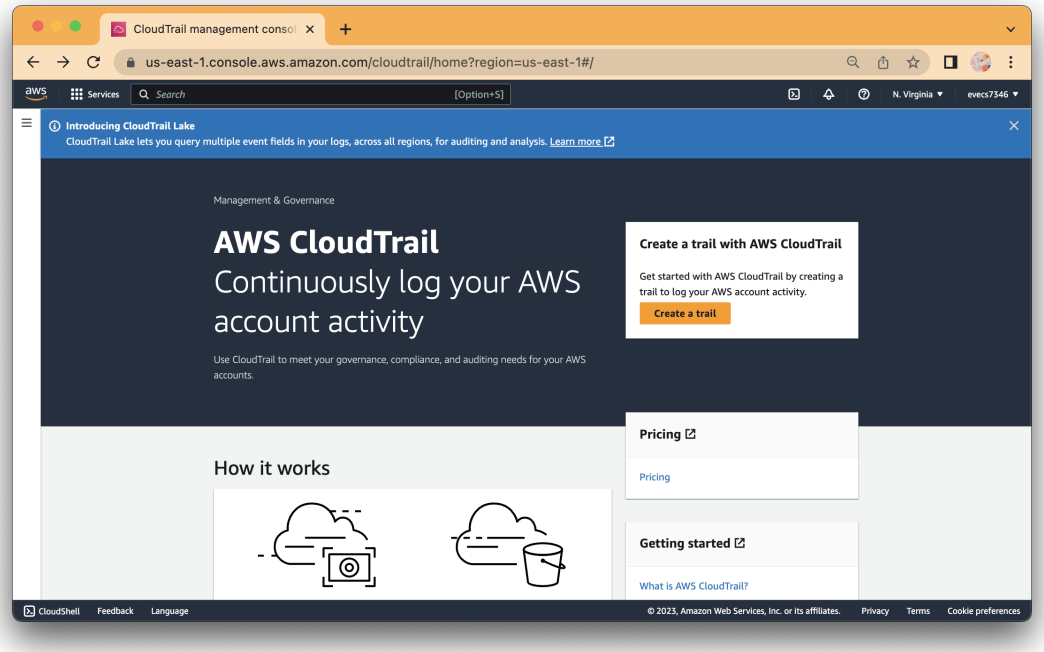
1. Browse to the CloudTrail service console and click the Create Trail button.
2. Under Trail Name, enter a trail name of your choice. Names must be at least three characters and can't contain spaces.
3. Under the Storage Location heading, select Create New S3 Bucket. Enter the name of the S3 bucket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

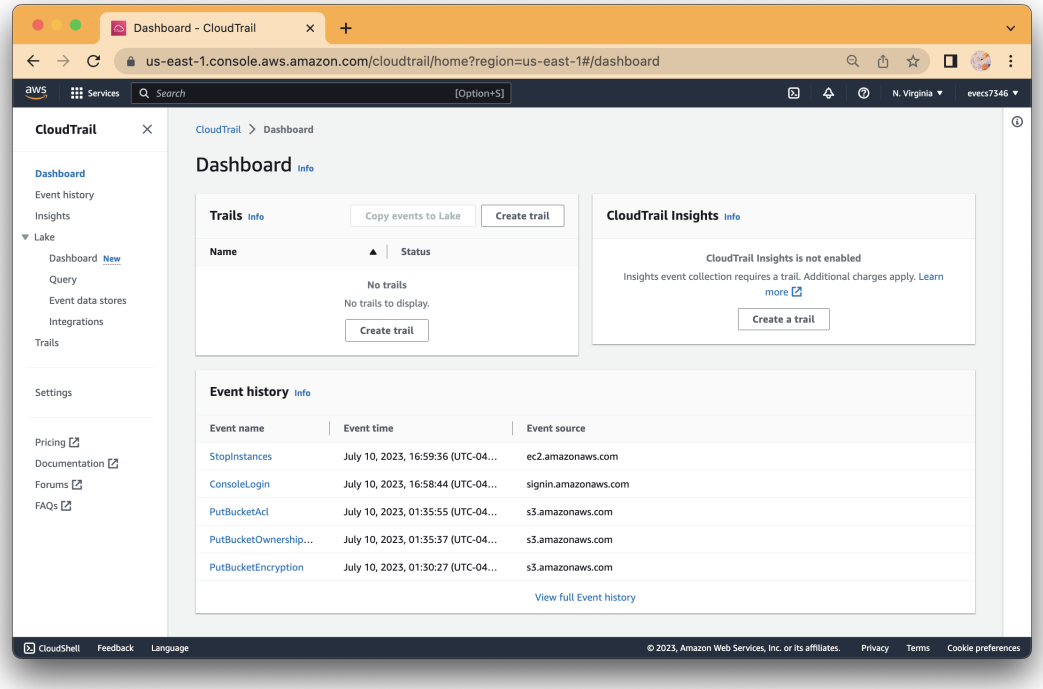
EXERCISE 7.1 *(continued)*

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.

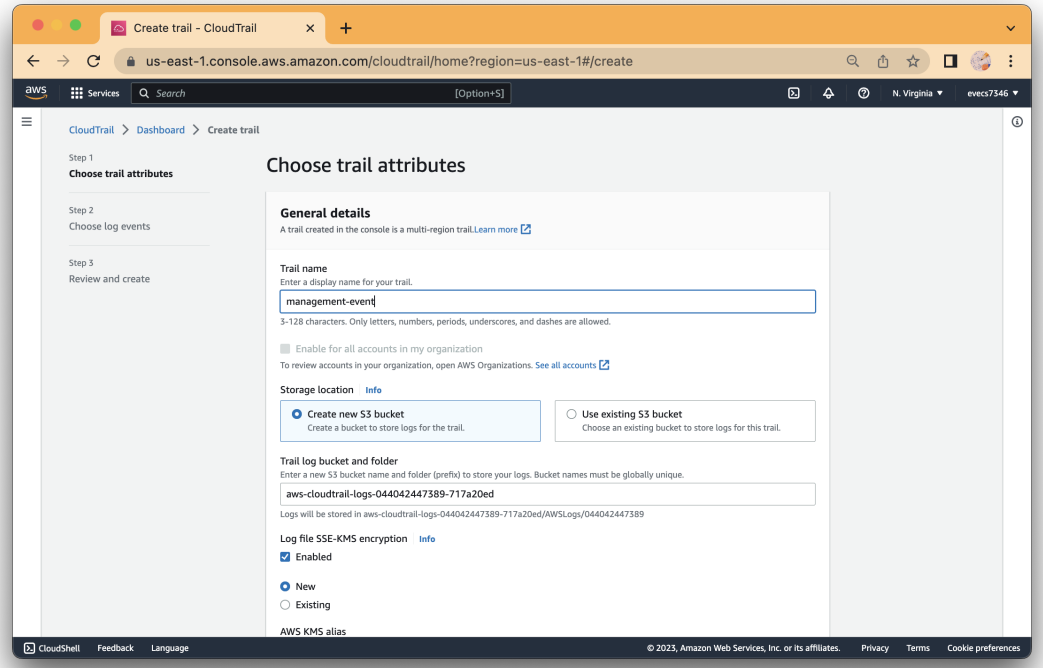
Solution:

1.

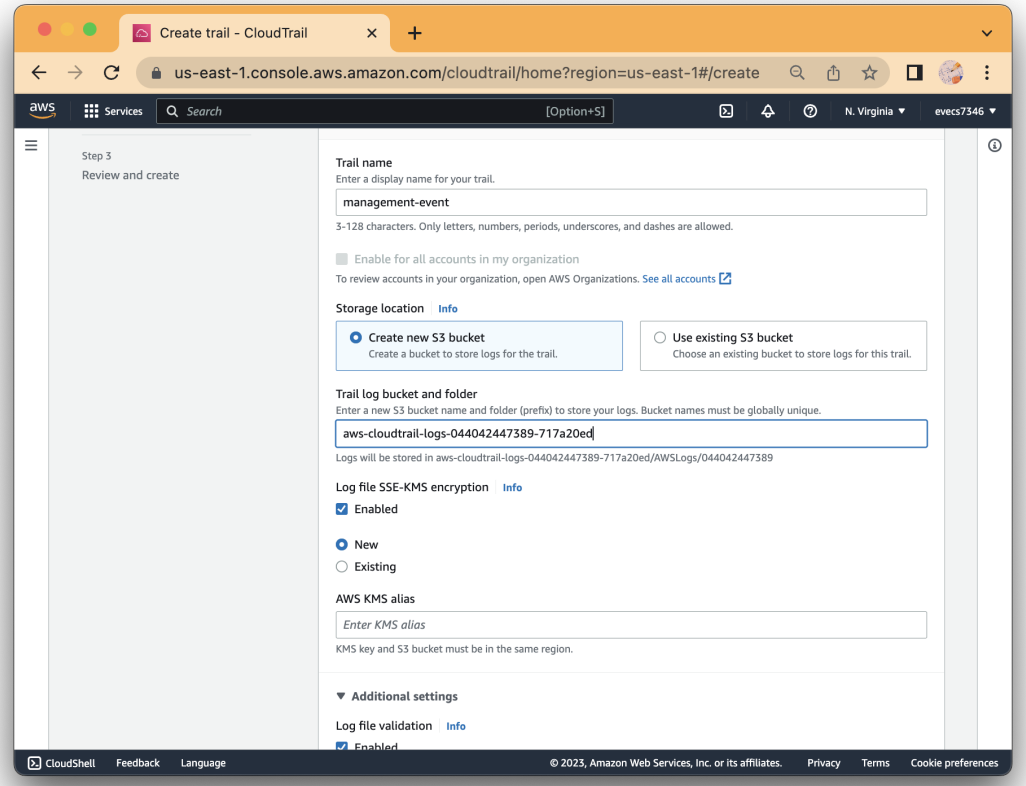

CloudTrail management consol
us-east-1.console.aws.amazon.com/cloudtrail/home?region=us-east-1#/
Services
Search
[Option+S]
N. Virginia
evecs7346
Introducing CloudTrail Lake
CloudTrail Lake lets you query multiple event fields in your logs, across all regions, for auditing and analysis. Learn more
Management & Governance
AWS CloudTrail
Continuously log your AWS account activity
Use CloudTrail to meet your governance, compliance, and auditing needs for your AWS accounts.
Create a trail with AWS CloudTrail
Get started with AWS CloudTrail by creating a trail to log your AWS account activity.
Create a trail
How it works
Pricing
Pricing
Getting started
What is AWS CloudTrail?
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Dashboard - CloudTrail
us-east-1.console.aws.amazon.com/cloudtrail/home?region=us-east-1#/dashboard
Services
Search
[Option+S]
N. Virginia
evecs7346
CloudTrail
Dashboard
Event history
Insights
Lake
Dashboard New
Query
Event data stores
Integrations
Trails
Settings
Pricing
Documentation
Forums
FAQs
CloudTrail > Dashboard
Dashboard Info
Trails Info
Copy events to Lake
Create trail
Name
Status
No trails
No trails to display.
Create trail
CloudTrail Insights Info
CloudTrail Insights is not enabled
Insights event collection requires a trail. Additional charges apply. Learn more
Create a trail
Event history Info
Event name
Event time
Event source
StopInstances
July 10, 2023, 16:59:36 (UTC-04...
ec2.amazonaws.com
ConsoleLogin
July 10, 2023, 16:58:44 (UTC-04...
signin.amazonaws.com
PutBucketAcl
July 10, 2023, 01:35:55 (UTC-04...
s3.amazonaws.com
PutBucketOwnership...
July 10, 2023, 01:35:37 (UTC-04...
s3.amazonaws.com
PutBucketEncryption
July 10, 2023, 01:30:27 (UTC-04...
s3.amazonaws.com
View full Event history
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

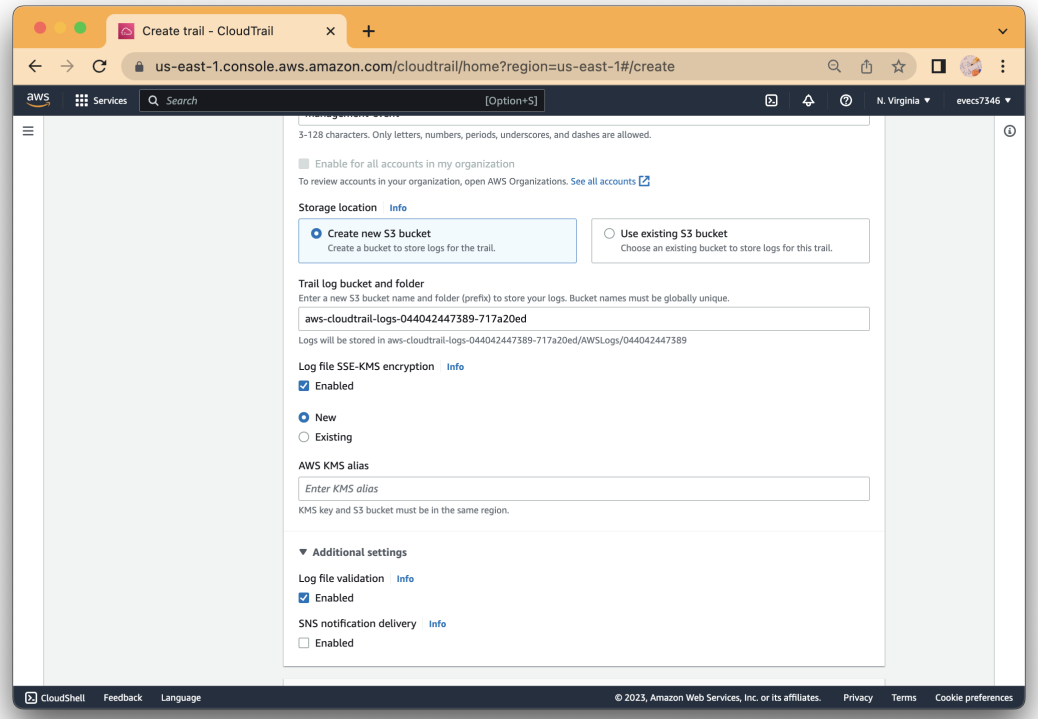
2.


Create trail - CloudTrail
us-east-1.console.aws.amazon.com/cloudtrail/home?region=us-east-1#/create
Services
Search
[Option+S]
N. Virginia
evecs7346
CloudTrail
Dashboard
Create trail
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.
management-event
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.
aws-cloudtrail-logs-044042447389-717a20ed
Logs will be stored in aws-cloudtrail-logs-044042447389-717a20ed/AWSLogs/044042447389
Log file SSE-KMS encryption Info
Enabled
New
Existing
AWS KMS alias
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

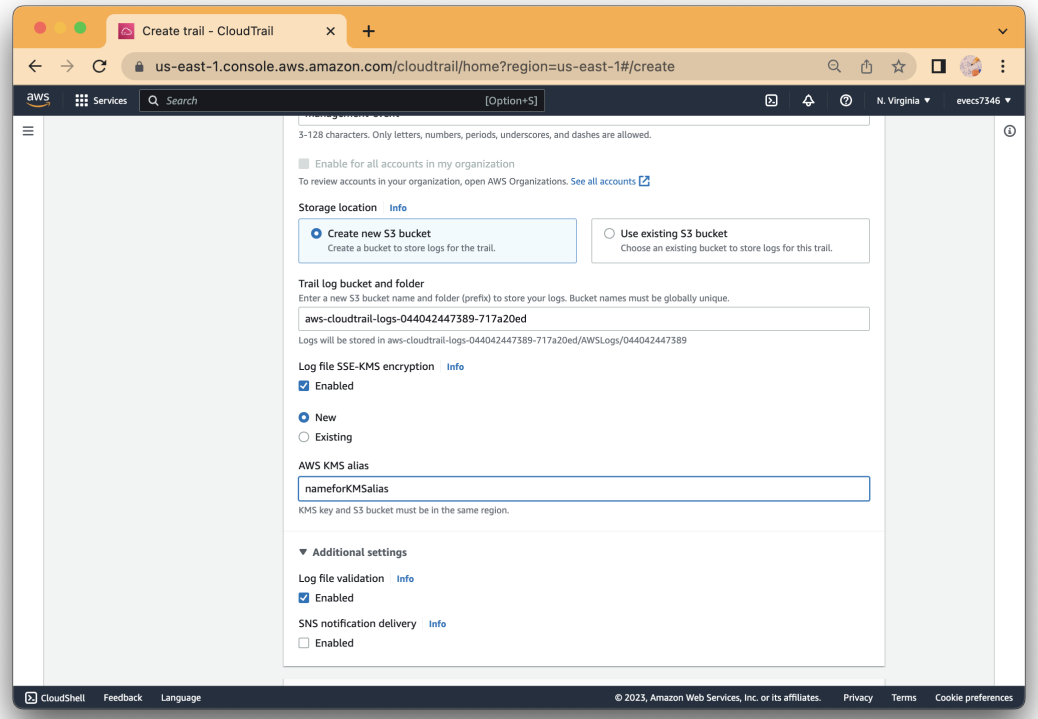
3.


Create trail - CloudTrail
us-east-1.console.aws.amazon.com/cloudtrail/home?region=us-east-1#/create
aws
Services
Search
[Option+S]
N. Virginia
evecs7346
Step 3
Review and create
Trail name
Enter a display name for your trail.
management-event
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.
aws-cloudtrail-logs-044042447389-717a20ed
Logs will be stored in aws-cloudtrail-logs-044042447389-717a20ed/AWSLogs/044042447389
Log file SSE-KMS encryption Info
Enabled
New
Existing
AWS KMS alias
Enter KMS alias
KMS key and S3 bucket must be in the same region.
Additional settings
Log file validation Info
Enabled
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

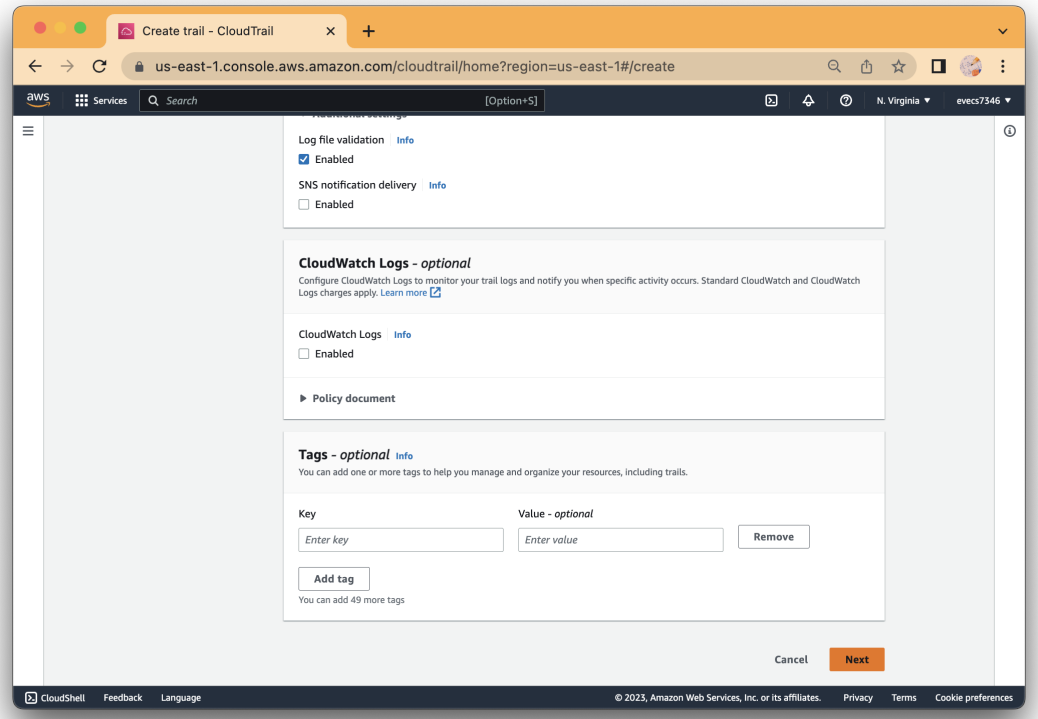
4.


Create trail - CloudTrail
us-east-1.console.aws.amazon.com/cloudtrail/home?region=us-east-1#/create
Services
Search
[Option+S]
N. Virginia
evecs7346
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.
aws-cloudtrail-logs-044042447389-717a20ed
Logs will be stored in aws-cloudtrail-logs-044042447389-717a20ed/AWSLogs/044042447389
Log file SSE-KMS encryption Info
Enabled
New
Existing
AWS KMS alias
Enter KMS alias
KMS key and S3 bucket must be in the same region.
Additional settings
Log file validation Info
Enabled
SNS notification delivery Info
Enabled
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

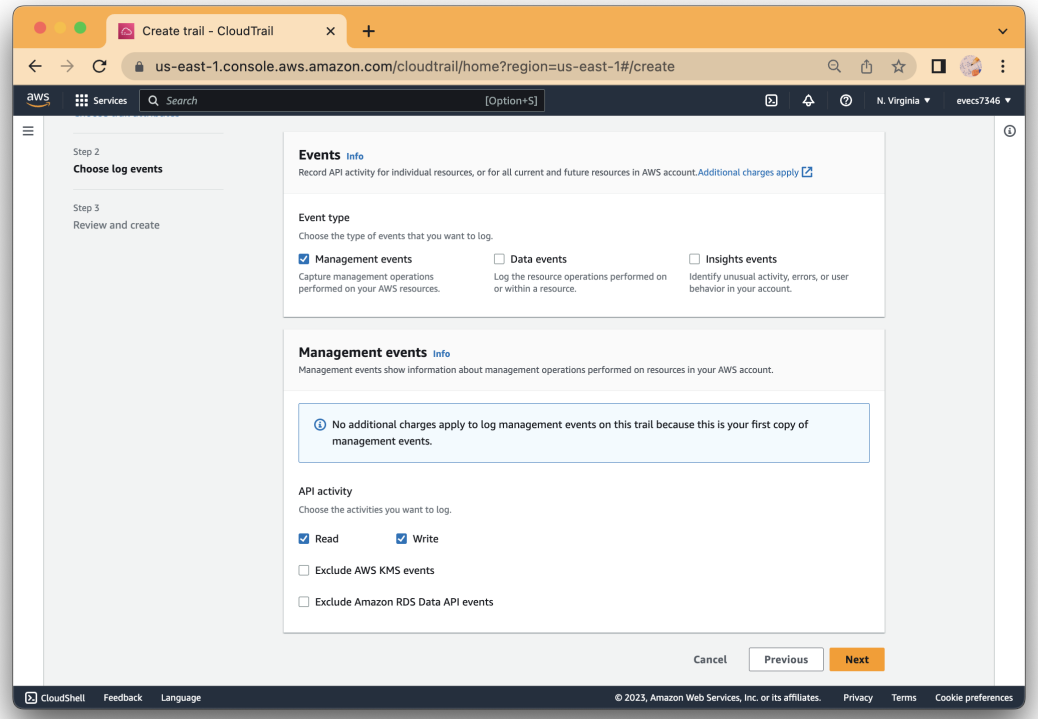
5.


Create trail - CloudTrail
us-east-1.console.aws.amazon.com/cloudtrail/home?region=us-east-1#/create
Services
Search
[Option+S]
N. Virginia
evecs7346
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.
aws-cloudtrail-logs-044042447389-717a20ed
Logs will be stored in aws-cloudtrail-logs-044042447389-717a20ed/AWSLogs/044042447389
Log file SSE-KMS encryption Info
Enabled
New
Existing
AWS KMS alias
nameforKMSalias
KMS key and S3 bucket must be in the same region.
Additional settings
Log file validation Info
Enabled
SNS notification delivery Info
Enabled
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

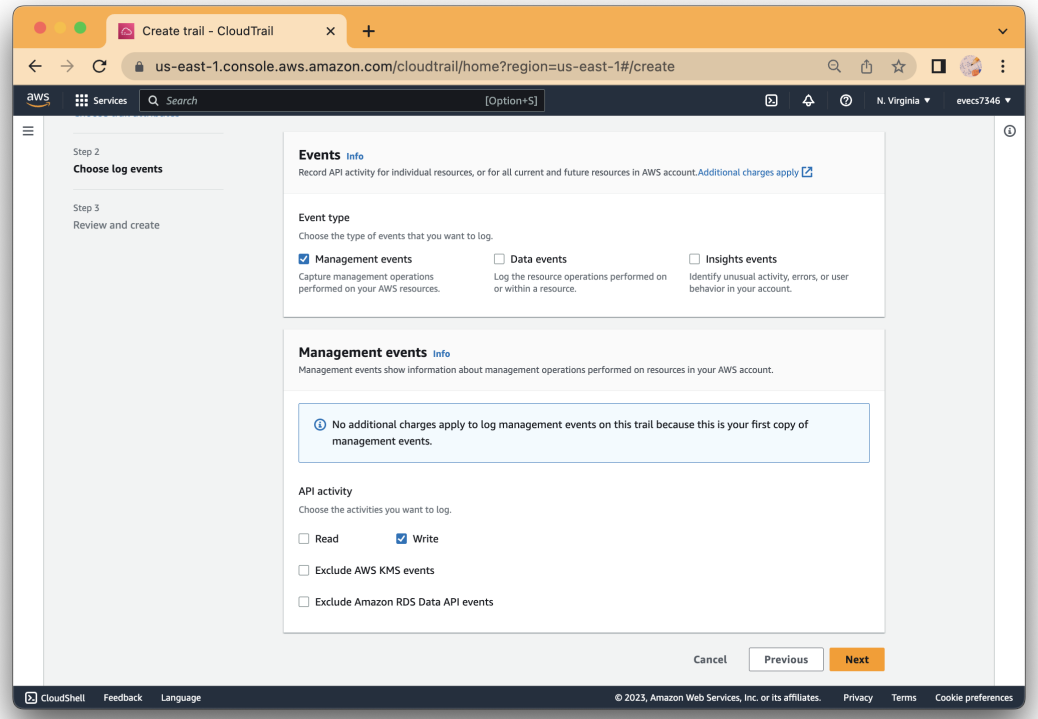
6.


Create trail - CloudTrail
us-east-1.console.aws.amazon.com/cloudtrail/home?region=us-east-1#/create
aws
Services
Search
[Option+S]
N. Virginia
evecs7346
Log file validation Info
Enabled
SNS notification delivery Info
Enabled
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
Policy document
Tags - optional Info
You can add one or more tags to help you manage and organize your resources, including trails.
Key
Value - optional
Enter key
Enter value
Remove
Add tag
You can add 49 more tags
Cancel
Next
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

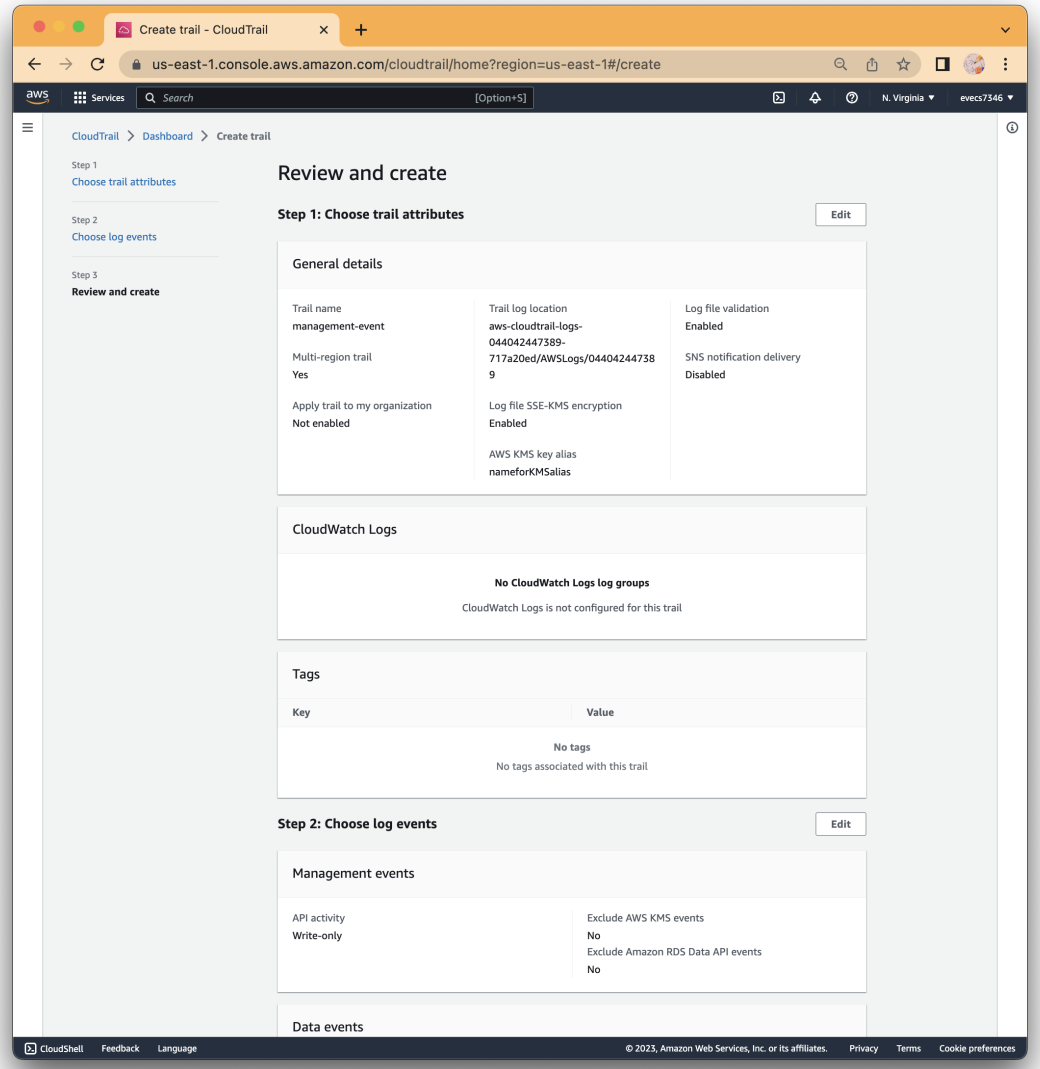
7.


Create trail - CloudTrail
us-east-1.console.aws.amazon.com/cloudtrail/home?region=us-east-1#/create
aws
Services
Search
[Option+S]
N. Virginia
evecs7346
Step 2
Choose log events
Step 3
Review and create
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.
Data events
Log the resource operations performed on or within a resource.
Insights events
Identify unusual activity, errors, or user behavior in your account.
Management events Info
Management events show information about management operations performed on resources in your AWS account.
No additional charges apply to log management events on this trail because this is your first copy of management events.
API activity
Choose the activities you want to log.
Read
Write
Exclude AWS KMS events
Exclude Amazon RDS Data API events
Cancel
Previous
Next
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

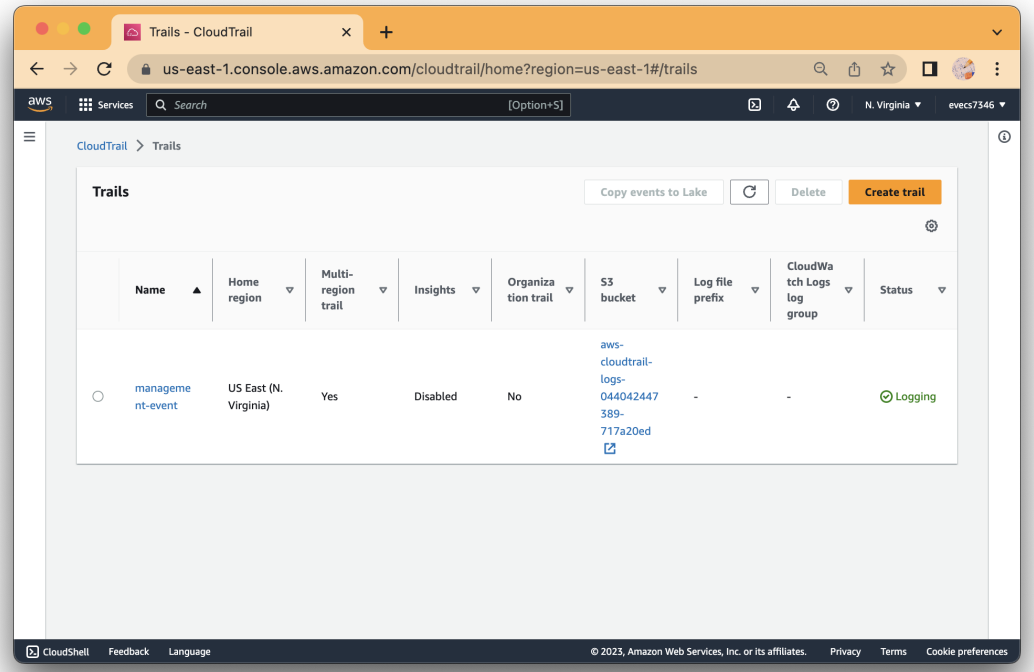
8.


Create trail - CloudTrail
us-east-1.console.aws.amazon.com/cloudtrail/home?region=us-east-1#/create
aws
Services
Search
[Option+S]
N. Virginia
evecs7346
Step 2
Choose log events
Step 3
Review and create
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.
Data events
Log the resource operations performed on or within a resource.
Insights events
Identify unusual activity, errors, or user behavior in your account.
Management events Info
Management events show information about management operations performed on resources in your AWS account.
No additional charges apply to log management events on this trail because this is your first copy of management events.
API activity
Choose the activities you want to log.
Read
Write
Exclude AWS KMS events
Exclude Amazon RDS Data API events
Cancel
Previous
Next
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

9.


Create trail - CloudTrail
us-east-1.console.aws.amazon.com/cloudtrail/home?region=us-east-1#/create
Services
Search
[Option+S]
N. Virginia
evecs7346
CloudTrail > Dashboard > Create trail
Step 1
Choose trail attributes
Step 2
Choose log events
Step 3
Review and create
Review and create
Step 1: Choose trail attributes
Edit
General details
Trail name
management-event
Multi-region trail
Yes
Apply trail to my organization
Not enabled
Trail log location
aws-cloudtrail-logs-044042447389-717a20ed/AWSLogs/044042447389
Log file SSE-KMS encryption
Enabled
AWS KMS key alias
nameforKMSalias
Log file validation
Enabled
SNS notification delivery
Disabled
CloudWatch Logs
No CloudWatch Logs log groups
CloudWatch Logs is not configured for this trail
Tags
Key
Value
No tags
No tags associated with this trail
Step 2: Choose log events
Edit
Management events
API activity
Write-only
Exclude AWS KMS events
No
Exclude Amazon RDS Data API events
No
Data events
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

10.


Trails - CloudTrail
us-east-1.console.aws.amazon.com/cloudtrail/home?region=us-east-1#/trails
Services
Search
[Option+S]
N. Virginia
evecs7346
CloudTrail
Trails
Trails
Copy events to Lake
Delete
Create trail
Name
Home region
Multi-region trail
Insights
Organization trail
S3 bucket
Log file prefix
CloudWatch Logs log group
Status
management-event
US East (N. Virginia)
Yes
Disabled
No
aws-cloudtrail-logs-044042447389-717a20ed
-
-
Logging
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

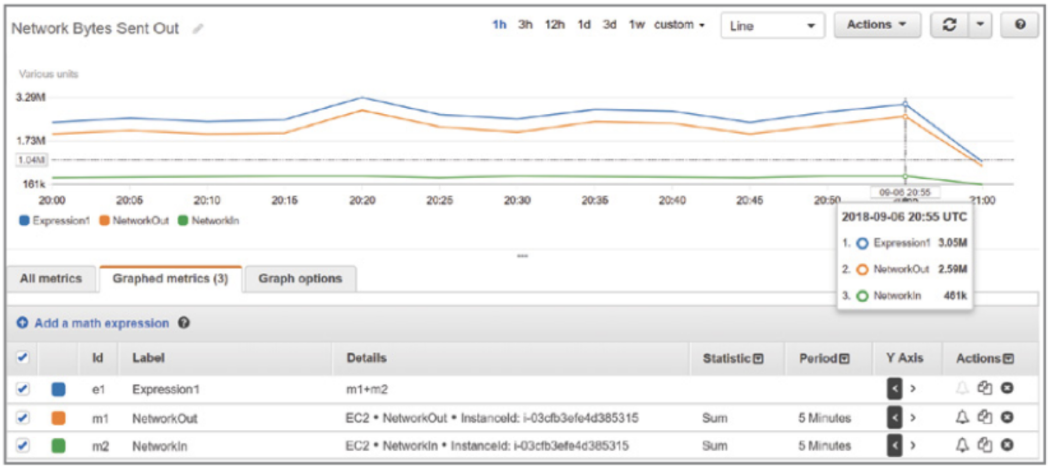
7.2

EXERCISE 7.2

Create a Graph Using Metric Math

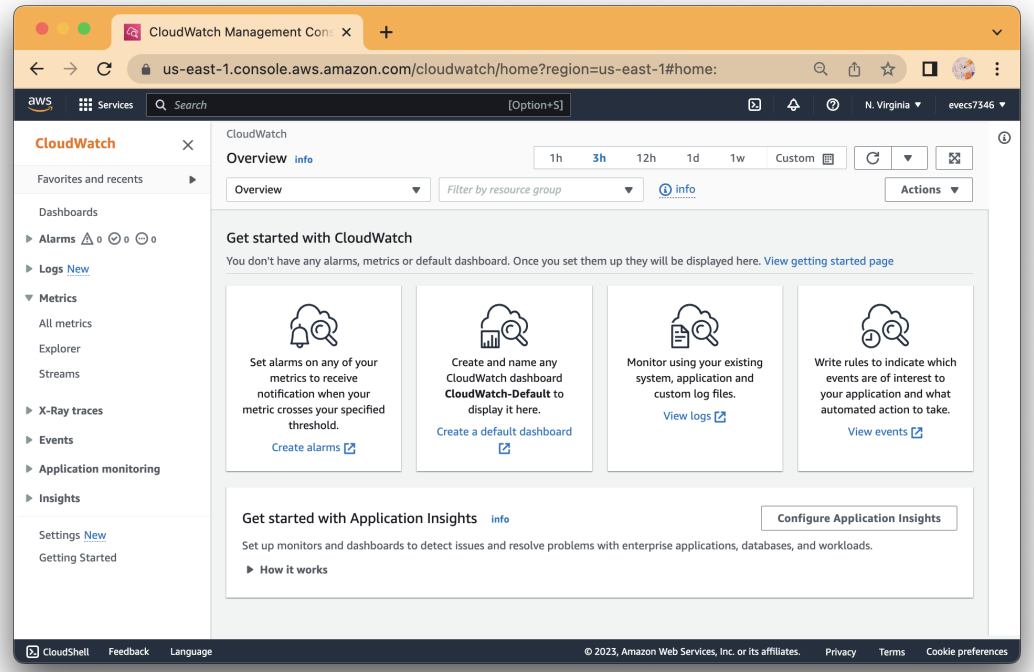
In this exercise, you'll create a graph that plots the `NetworkIn` and `NetworkOut` metrics for an EC2 instance. You'll then use metric math to graph a new time series combining both metrics.

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. Your graph should look similar to this one:

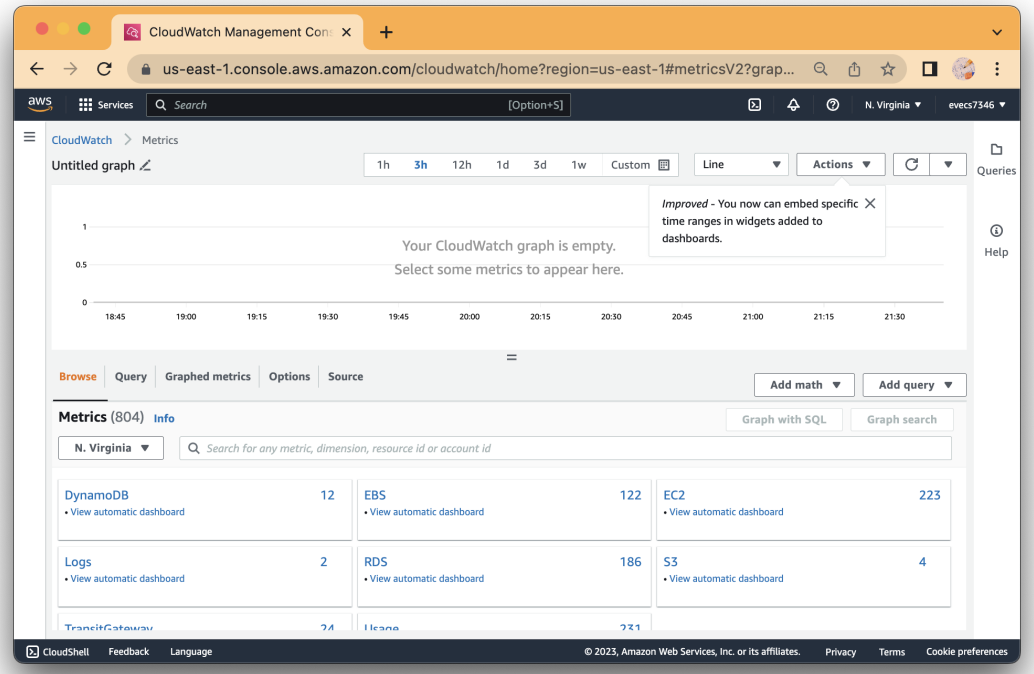


Solution:

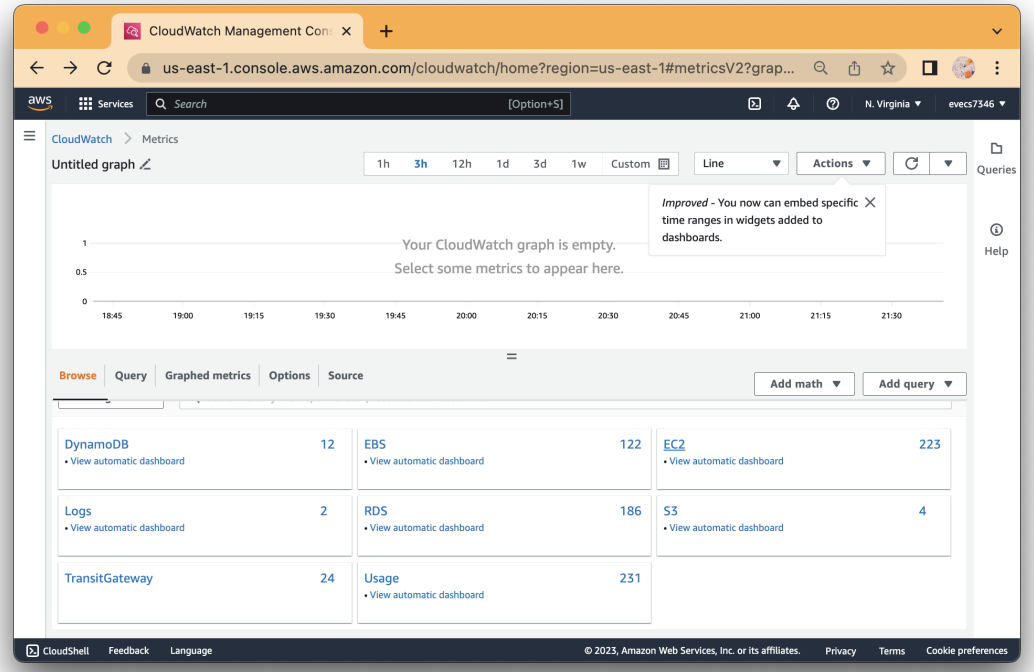
1.

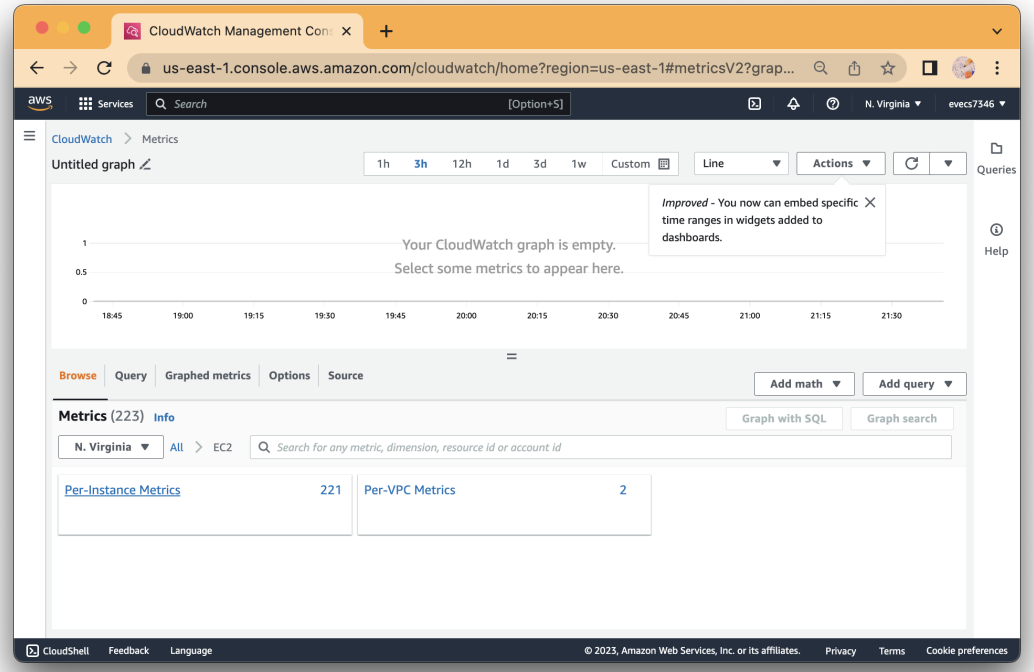

CloudWatch Management Con
us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#home:
Services
Search
[Option+S]
N. Virginia
evecs7346
CloudWatch
Favorites and recents
Dashboards
Alarms
Logs New
Metrics
All metrics
Explorer
Streams
X-Ray traces
Events
Application monitoring
Insights
Settings New
Getting Started
Overview info
1h 3h 12h 1d 1w Custom
Overview
Filter by resource group
info
Actions
Get started with CloudWatch
You don't have any alarms, metrics or default dashboard. Once you set them up they will be displayed here. View getting started page
Set alarms on any of your metrics to receive notification when your metric crosses your specified threshold.
Create alarms
Create and name any CloudWatch dashboard CloudWatch-Default to display it here.
Create a default dashboard
Monitor using your existing system, application and custom log files.
View logs
Write rules to indicate which events are of interest to your application and what automated action to take.
View events
Get started with Application Insights info
Configure Application Insights
Set up monitors and dashboards to detect issues and resolve problems with enterprise applications, databases, and workloads.
How it works
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

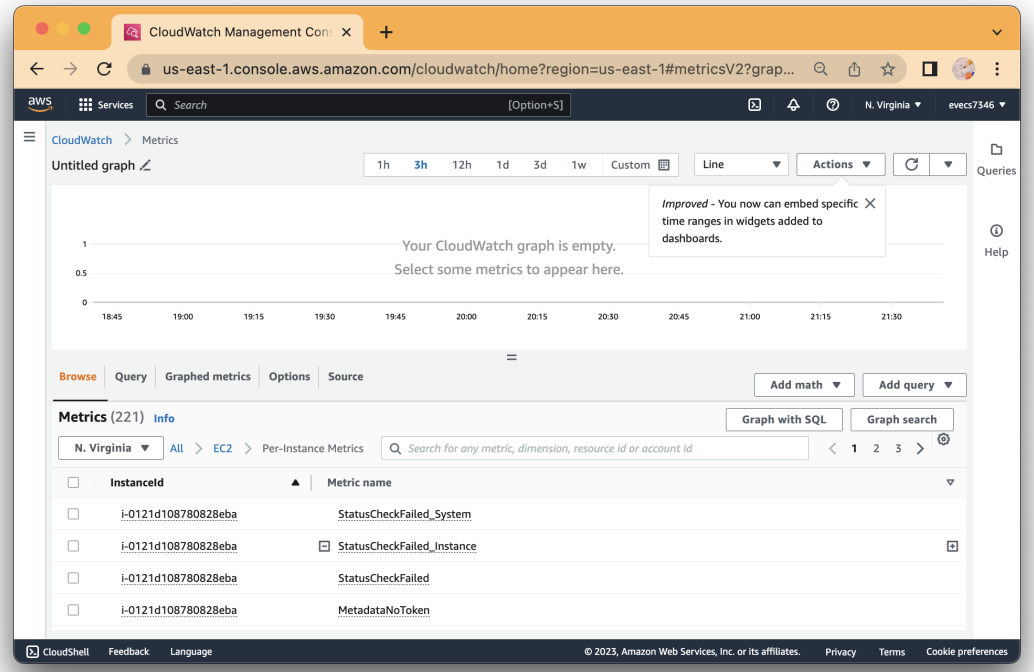
2.

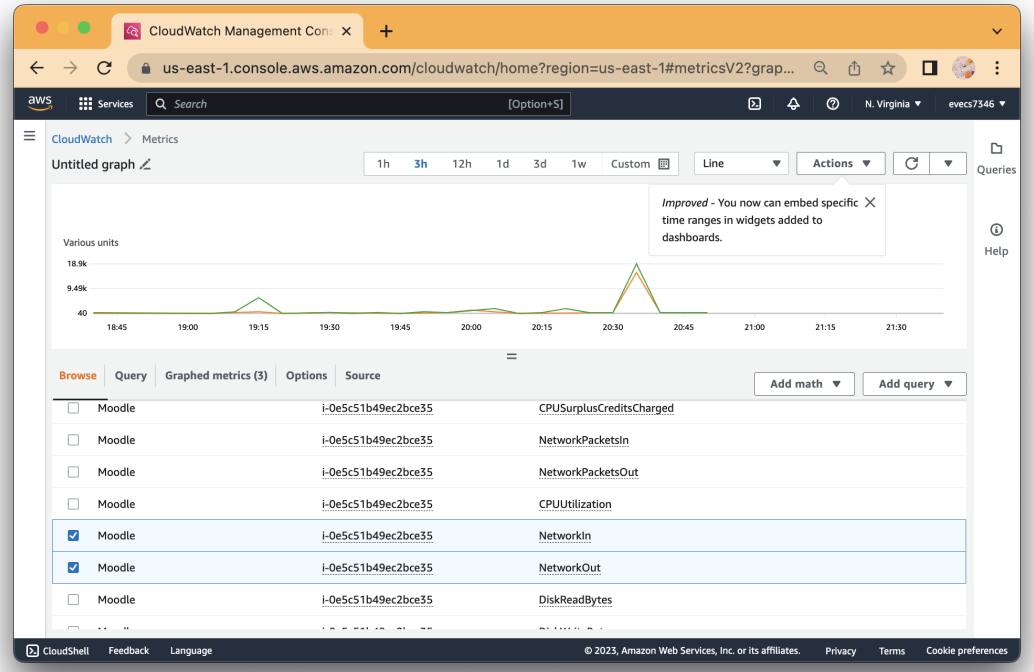

CloudWatch Management Con
us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#metricsV2?grap...
Services
Search
[Option+S]
N. Virginia
evecs7346
CloudWatch
Metrics
Untitled graph
1h 3h 12h 1d 3d 1w Custom
Line
Actions
Queries
Help
Improved - You now can embed specific time ranges in widgets added to dashboards.
Your CloudWatch graph is empty.
Select some metrics to appear here.
1
0.5
0
18:45
19:00
19:15
19:30
19:45
20:00
20:15
20:30
20:45
21:00
21:15
21:30
Browse
Query
Graphed metrics
Options
Source
Add math
Add query
Metrics (804) Info
Graph with SQL
Graph search
N. Virginia
Search for any metric, dimension, resource id or account id
DynamoDB 12
• View automatic dashboard
EBS 122
• View automatic dashboard
EC2 223
• View automatic dashboard
Logs 2
• View automatic dashboard
RDS 186
• View automatic dashboard
S3 4
• View automatic dashboard
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

3.

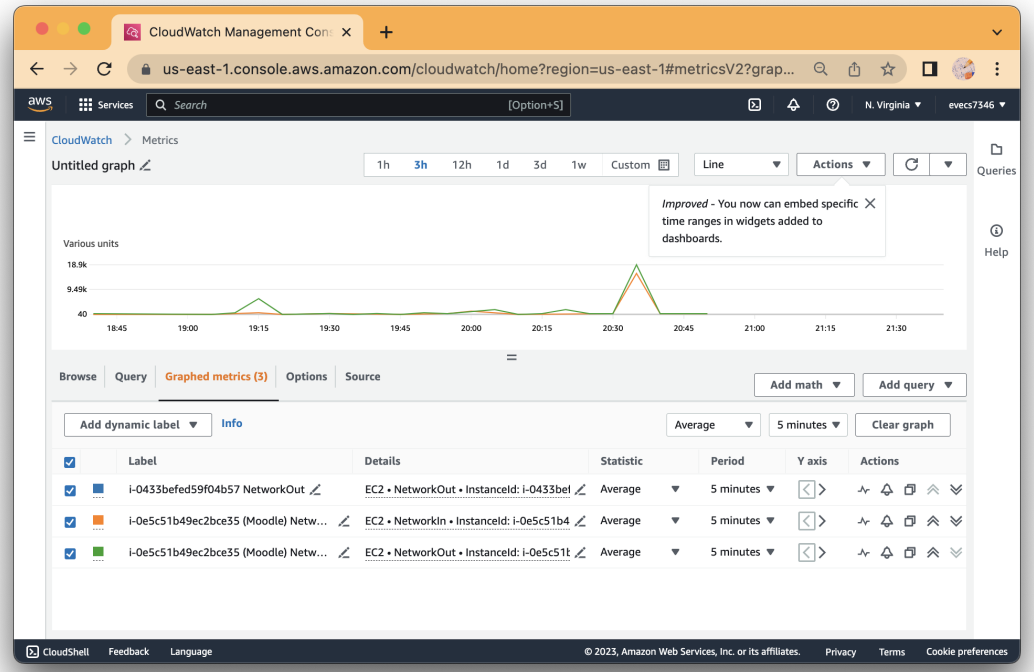

CloudWatch Management Con
us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#metricsV2?grap...
Services
Search
[Option+S]
N. Virginia
evecs7346
CloudWatch
Metrics
Untitled graph
1h
3h
12h
1d
3d
1w
Custom
Line
Actions
Queries
Improved - You now can embed specific time ranges in widgets added to dashboards.
Help
Your CloudWatch graph is empty.
Select some metrics to appear here.
1
0.5
0
18:45
19:00
19:15
19:30
19:45
20:00
20:15
20:30
20:45
21:00
21:15
21:30
Browse
Query
Graphed metrics
Options
Source
Add math
Add query
DynamoDB 12
• View automatic dashboard
EBS 122
• View automatic dashboard
EC2 223
• View automatic dashboard
Logs 2
• View automatic dashboard
RDS 186
• View automatic dashboard
S3 4
• View automatic dashboard
TransitGateway 24
Usage 231
• View automatic dashboard
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


CloudWatch Management Con
us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#metricsV2?grap...
Services
Search
[Option+S]
N. Virginia
evecs7346
CloudWatch
Metrics
Untitled graph
1h
3h
12h
1d
3d
1w
Custom
Line
Actions
Queries
Improved - You now can embed specific time ranges in widgets added to dashboards.
Help
Your CloudWatch graph is empty.
Select some metrics to appear here.
1
0.5
0
18:45
19:00
19:15
19:30
19:45
20:00
20:15
20:30
20:45
21:00
21:15
21:30
Browse
Query
Graphed metrics
Options
Source
Add math
Add query
Metrics (223) Info
Graph with SQL
Graph search
N. Virginia
All
EC2
Search for any metric, dimension, resource id or account id
Per-Instance Metrics 221
Per-VPC Metrics 2
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

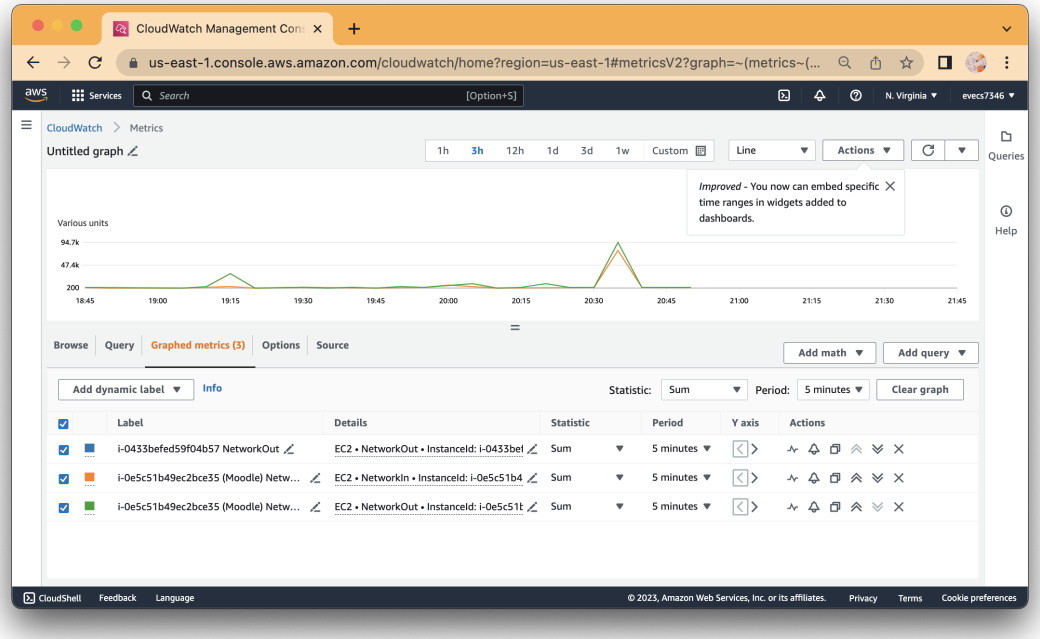

CloudWatch Management Con
us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#metricsV2?grap...
Services
Search
[Option+S]
N. Virginia
evecs7346
CloudWatch
Metrics
Untitled graph
1h
3h
12h
1d
3d
1w
Custom
Line
Actions
Queries
Help
Improved - You now can embed specific time ranges in widgets added to dashboards.
Your CloudWatch graph is empty.
Select some metrics to appear here.
1
0.5
0
18:45
19:00
19:15
19:30
19:45
20:00
20:15
20:30
20:45
21:00
21:15
21:30
Browse
Query
Graphed metrics
Options
Source
Add math
Add query
Metrics (221)
Info
Graph with SQL
Graph search
N. Virginia
All
EC2
Per-Instance Metrics
Search for any metric, dimension, resource id or account id
1
2
3
InstanceId
Metric name
i-0121d108780828eba
StatusCheckFailed_System
i-0121d108780828eba
StatusCheckFailed_Instance
i-0121d108780828eba
StatusCheckFailed
i-0121d108780828eba
MetadataNoToken
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


CloudWatch Management Con
us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#metricsV2?grap...
Services
Search
[Option+S]
N. Virginia
evecs7346
CloudWatch
Metrics
Untitled graph
1h
3h
12h
1d
3d
1w
Custom
Line
Actions
Queries
Help
Improved - You now can embed specific time ranges in widgets added to dashboards.
Various units
18.9k
9.49k
40
18:45
19:00
19:15
19:30
19:45
20:00
20:15
20:30
20:45
21:00
21:15
21:30
Browse
Query
Graphed metrics (3)
Options
Source
Add math
Add query
Moodle
i-0e5c51b49ec2bce35
CPUSurplusCreditsCharged
Moodle
i-0e5c51b49ec2bce35
NetworkPacketsIn
Moodle
i-0e5c51b49ec2bce35
NetworkPacketsOut
Moodle
i-0e5c51b49ec2bce35
CPUUtilization
Moodle
i-0e5c51b49ec2bce35
NetworkIn
Moodle
i-0e5c51b49ec2bce35
NetworkOut
Moodle
i-0e5c51b49ec2bce35
DiskReadBytes
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

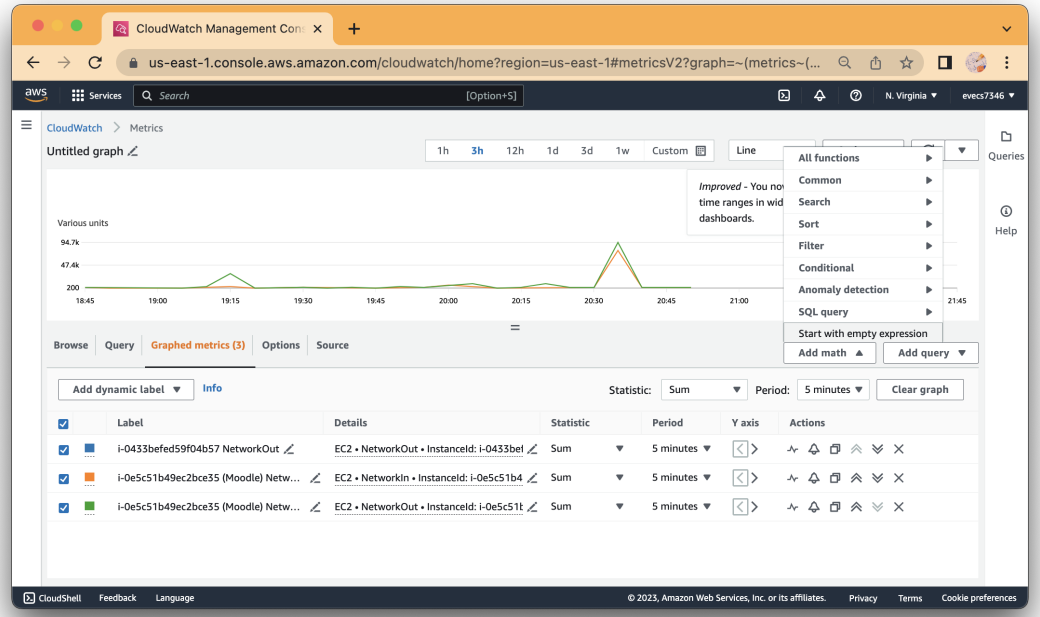
4.


CloudWatch Management Con
us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#metricsV2?grap...
Services
Search
[Option+S]
N. Virginia
evecs7346
CloudWatch
Metrics
Untitled graph
1h
3h
12h
1d
3d
1w
Custom
Line
Actions
Queries
Help
Improved - You now can embed specific time ranges in widgets added to dashboards.
Various units
18.9k
9.49k
40
18:45
19:00
19:15
19:30
19:45
20:00
20:15
20:30
20:45
21:00
21:15
21:30
Browse
Query
Graphed metrics (3)
Options
Source
Add math
Add query
Add dynamic label
Info
Average
5 minutes
Clear graph
Label
Details
Statistic
Period
Y axis
Actions
i-0433befed59f04b57 NetworkOut
EC2 • NetworkOut • InstanceId: i-0433bef
Average
5 minutes
i-0e5c51b49ec2bce35 (Moodle) Netw...
EC2 • NetworkIn • InstanceId: i-0e5c51b4
Average
5 minutes
i-0e5c51b49ec2bce35 (Moodle) Netw...
EC2 • NetworkOut • InstanceId: i-0e5c51b
Average
5 minutes
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

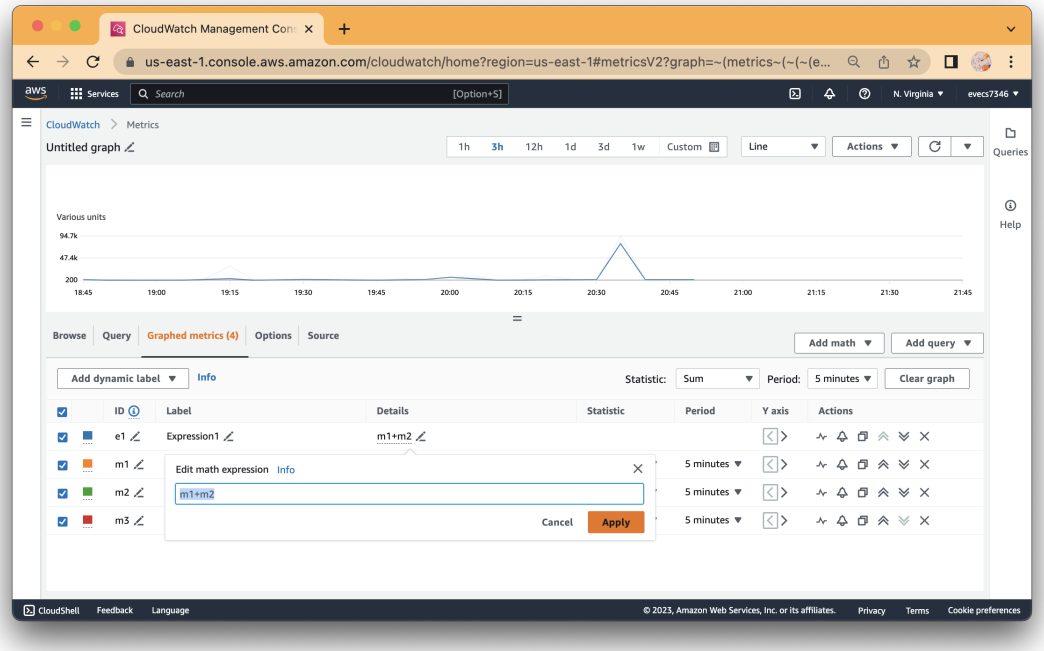
5.


CloudWatch Management Con
us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#metricsV2?graph=~(metrics~(...
Services
Search
[Option+S]
N. Virginia
evecs7346
CloudWatch
Metrics
Untitled graph
1h
3h
12h
1d
3d
1w
Custom
Line
Actions
Queries
Help
Improved - You now can embed specific time ranges in widgets added to dashboards.
Various units
94.7k
47.4k
200
18:45
19:00
19:15
19:30
19:45
20:00
20:15
20:30
20:45
21:00
21:15
21:30
21:45
Browse
Query
Graphed metrics (3)
Options
Source
Add math
Add query
Add dynamic label
Info
Statistic:
Sum
Period:
5 minutes
Clear graph
Label
Details
Statistic
Period
Y axis
Actions
i-0433befed59f04b57 NetworkOut
EC2 • NetworkOut • InstanceId: i-0433bef
Sum
5 minutes
i-0e5c51b49ec2bce35 (Moodle) Netw...
EC2 • NetworkIn • InstanceId: i-0e5c51b4
Sum
5 minutes
i-0e5c51b49ec2bce35 (Moodle) Netw...
EC2 • NetworkOut • InstanceId: i-0e5c51b
Sum
5 minutes
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

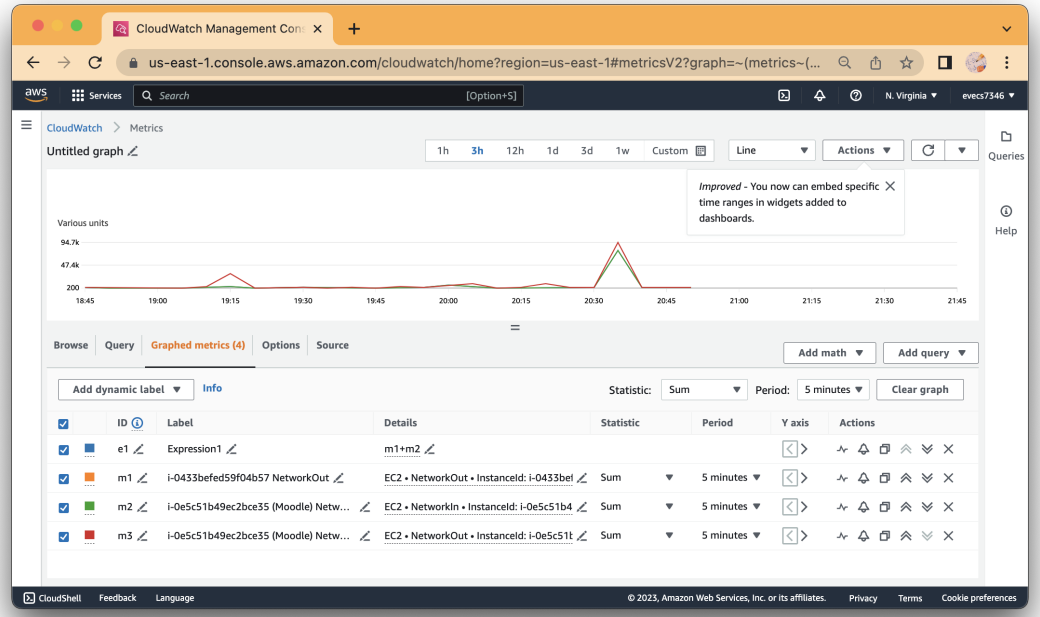
6.


CloudWatch Management Con
us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#metricsV2?graph=~(metrics~(...
Services
Search
[Option+S]
N. Virginia
evecs7346
CloudWatch
Metrics
Untitled graph
1h
3h
12h
1d
3d
1w
Custom
Line
All functions
Common
Search
Sort
Filter
Conditional
Anomaly detection
SQL query
Start with empty expression
Queries
Help
Various units
94.7k
47.4k
200
18:45
19:00
19:15
19:30
19:45
20:00
20:15
20:30
20:45
21:00
21:45
Browse
Query
Graphed metrics (3)
Options
Source
Add math
Add query
Add dynamic label
Info
Statistic:
Sum
Period:
5 minutes
Clear graph
Label
Details
Statistic
Period
Y axis
Actions
i-0433befed59f04b57 NetworkOut
EC2 • NetworkOut • InstanceId: i-0433bel
i-0e5c51b49ec2bce35 (Moodle) Netw...
EC2 • NetworkIn • InstanceId: i-0e5c51b4
EC2 • NetworkOut • InstanceId: i-0e5c51t
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

7.


CloudWatch Management Con
us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#metricsV2?graph=~(metrics~(~(~(e...
Services
Search
[Option+S]
N. Virginia
evecs7346
CloudWatch
Metrics
Untitled graph
1h
3h
12h
1d
3d
1w
Custom
Line
Actions
Queries
Help
Various units
94.7k
47.4k
200
18:45
19:00
19:15
19:30
19:45
20:00
20:15
20:30
20:45
21:00
21:15
21:30
21:45
Browse
Query
Graphed metrics (4)
Options
Source
Add math
Add query
Add dynamic label
Info
Statistic:
Sum
Period:
5 minutes
Clear graph
ID
Label
Details
Statistic
Period
Y axis
Actions
e1
Expression1
m1+m2
m1
m2
m3
Edit math expression
Info
m1+m2
Cancel
Apply
5 minutes
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

8.



7.3

EXERCISE 7.3

Deliver CloudTrail Logs to CloudWatch Logs

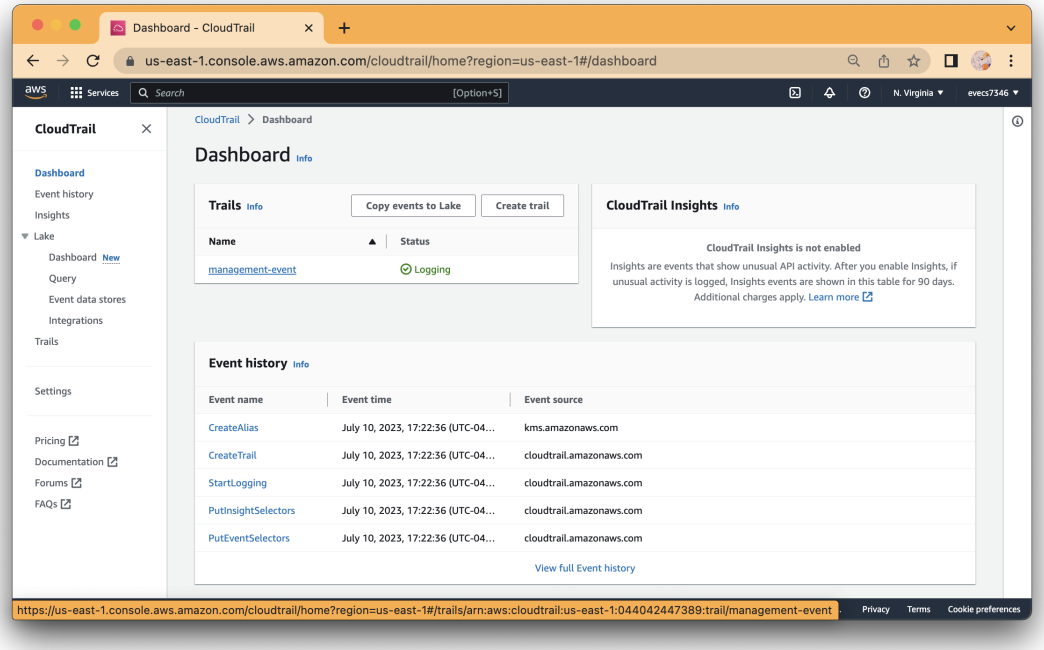
In this exercise, you'll reconfigure the trail you created in Exercise 7.1 to stream events captured by CloudTrail to CloudWatch Logs.

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.
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.
7. Click the Save Changes button.

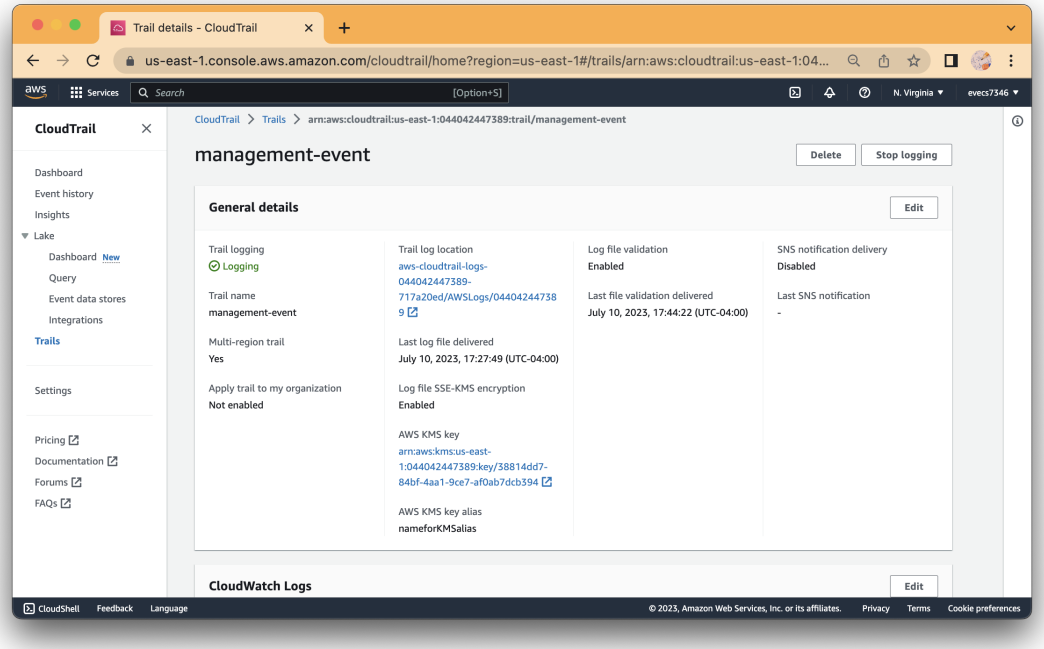
Delivery isn't instant, and it can take a few minutes before trail logs show up in CloudWatch Logs.

Solution:

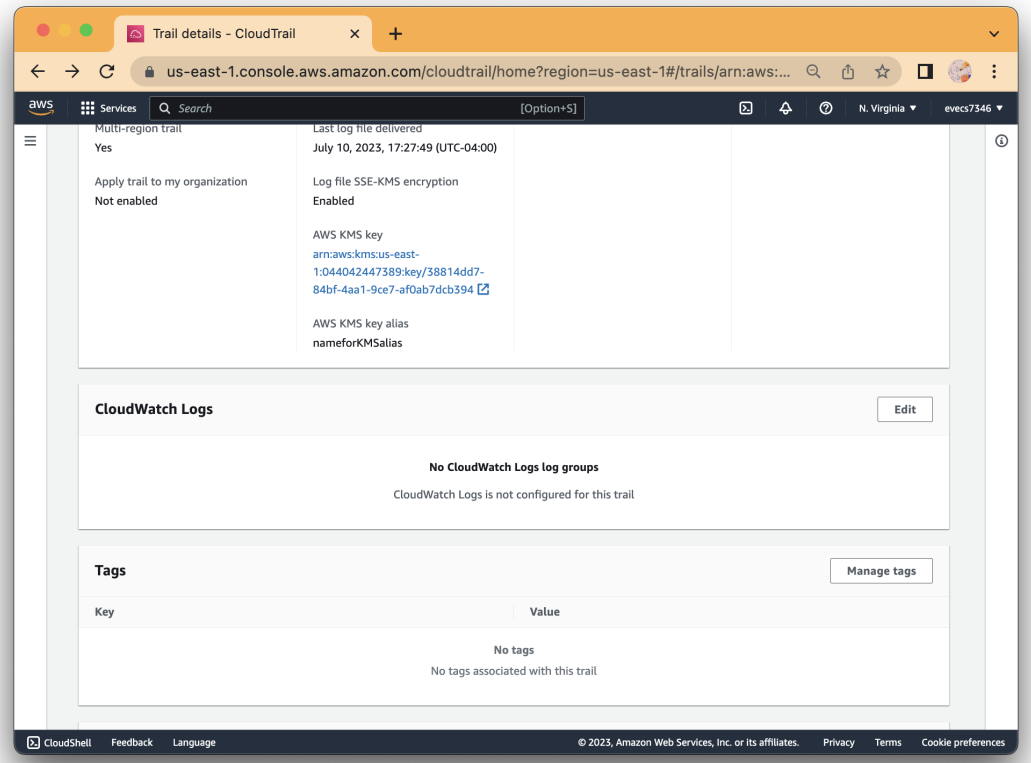
1.


Dashboard - CloudTrail
us-east-1.console.aws.amazon.com/cloudtrail/home?region=us-east-1#/dashboard
CloudTrail
Dashboard
Event history
Insights
Lake
Dashboard New
Query
Event data stores
Integrations
Trails
Settings
Pricing
Documentation
Forums
FAQs
CloudTrail > Dashboard
Dashboard Info
Trails Info
Copy events to Lake
Create trail
Name
Status
management-event
Logging
CloudTrail Insights Info
CloudTrail Insights is not enabled
Insights are events that show unusual API activity. After you enable Insights, if unusual activity is logged, Insights events are shown in this table for 90 days. Additional charges apply. Learn more
Event history Info
Event name
Event time
Event source
CreateAlias
July 10, 2023, 17:22:36 (UTC-04...
kms.amazonaws.com
CreateTrail
July 10, 2023, 17:22:36 (UTC-04...
cloudtrail.amazonaws.com
StartLogging
July 10, 2023, 17:22:36 (UTC-04...
cloudtrail.amazonaws.com
PutInsightSelectors
July 10, 2023, 17:22:36 (UTC-04...
cloudtrail.amazonaws.com
PutEventSelectors
July 10, 2023, 17:22:36 (UTC-04...
cloudtrail.amazonaws.com
View full Event history
https://us-east-1.console.aws.amazon.com/cloudtrail/home?region=us-east-1#/trails/arn:aws:cloudtrail:us-east-1:044042447389:trail/management-event
Privacy
Terms
Cookie preferences

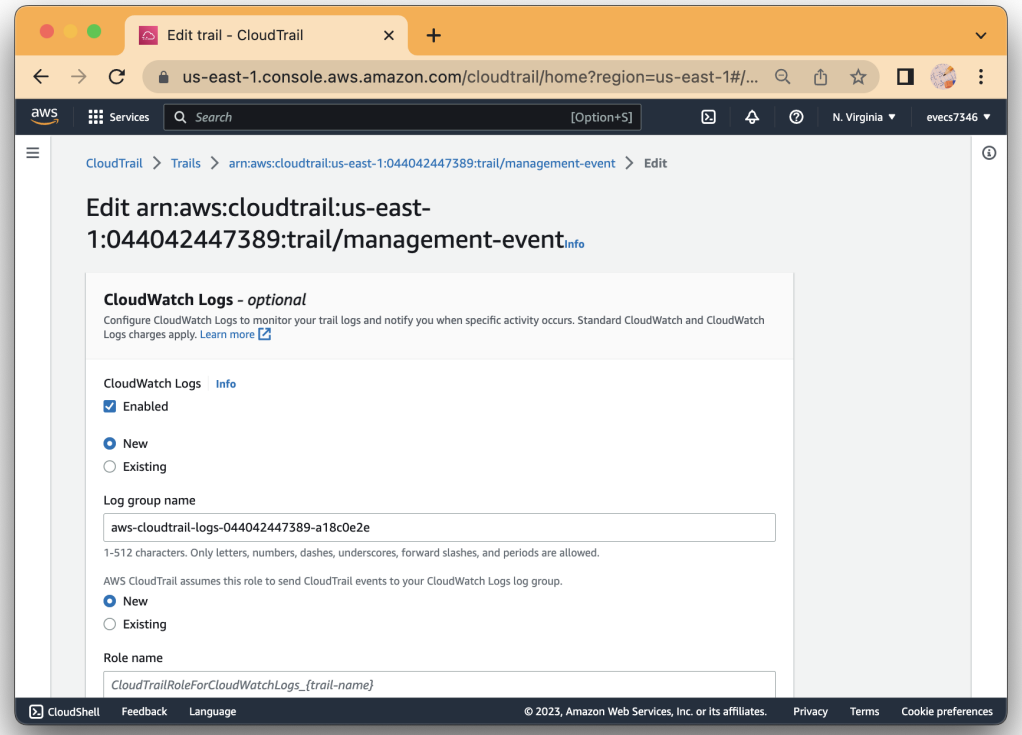
2.


Trail details - CloudTrail
us-east-1.console.aws.amazon.com/cloudtrail/home?region=us-east-1#/trails/arn:aws:cloudtrail:us-east-1:04...
CloudTrail
Dashboard
Event history
Insights
Lake
Dashboard New
Query
Event data stores
Integrations
Trails
Settings
Pricing
Documentation
Forums
FAQs
CloudTrail > Trails > arn:aws:cloudtrail:us-east-1:044042447389:trail/management-event
management-event
Delete
Stop logging
General details
Edit
Trail logging
Logging
Trail name
management-event
Multi-region trail
Yes
Apply trail to my organization
Not enabled
Trail log location
aws-cloudtrail-logs-044042447389-717a20ed/AWSLogs/044042447389
Last log file delivered
July 10, 2023, 17:27:49 (UTC-04:00)
Log file SSE-KMS encryption
Enabled
AWS KMS key
arn:aws:kms:us-east-1:044042447389:key/38814dd7-84bf-4aa1-9ce7-af0ab7dcb394
AWS KMS key alias
nameforKMSalias
Log file validation
Enabled
Last file validation delivered
July 10, 2023, 17:44:22 (UTC-04:00)
SNS notification delivery
Disabled
Last SNS notification
-
CloudWatch Logs
Edit
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

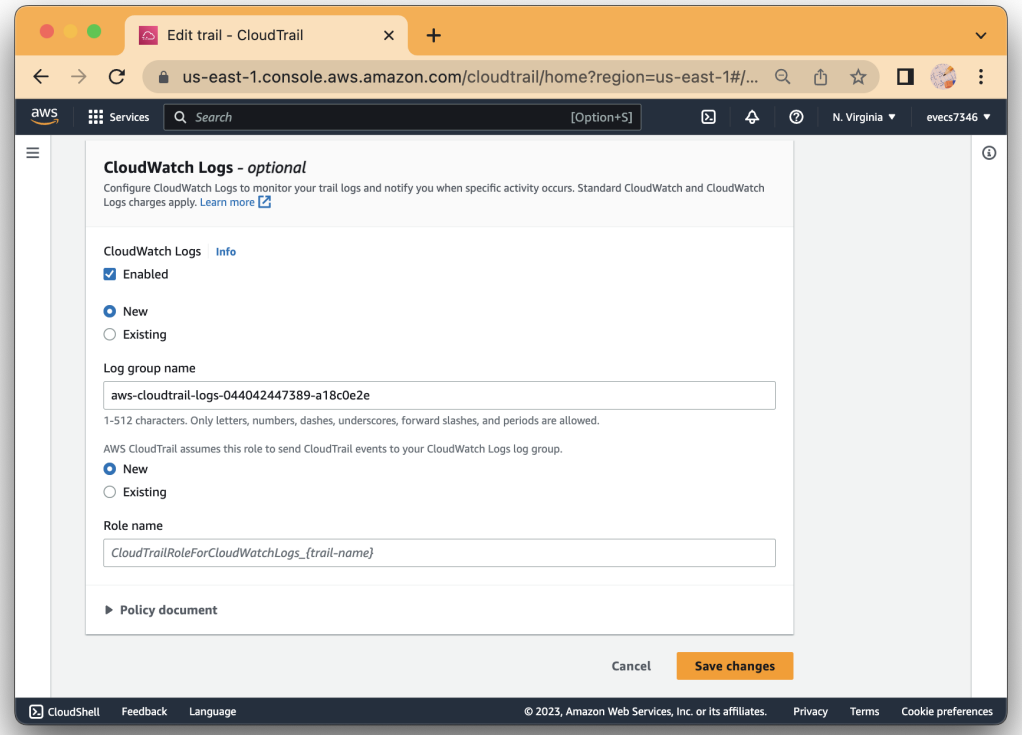
3.


Trail details - CloudTrail
us-east-1.console.aws.amazon.com/cloudtrail/home?region=us-east-1#/trails/arn:aws:...
Services
Search
[Option+S]
N. Virginia
evecs7346
Multi-region trail
Yes
Apply trail to my organization
Not enabled
Last log file delivered
July 10, 2023, 17:27:49 (UTC-04:00)
Log file SSE-KMS encryption
Enabled
AWS KMS key
arn:aws:kms:us-east-1:044042447389:key/38814dd7-84bf-4aa1-9ce7-af0ab7dcb394
AWS KMS key alias
nameforKMSalias
CloudWatch Logs
Edit
No CloudWatch Logs log groups
CloudWatch Logs is not configured for this trail
Tags
Manage tags
Key
Value
No tags
No tags associated with this trail
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

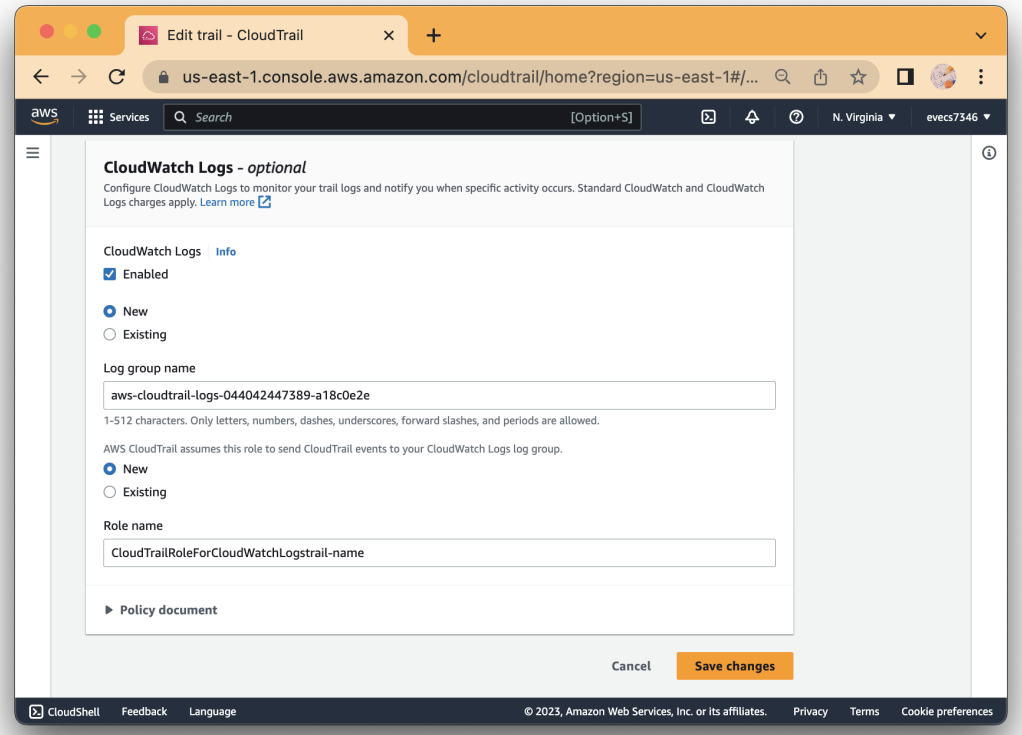
4.


Edit trail - CloudTrail
us-east-1.console.aws.amazon.com/cloudtrail/home?region=us-east-1#/...
aws
Services
Search
[Option+S]
N. Virginia
evecs7346
CloudTrail > Trails > arn:aws:cloudtrail:us-east-1:044042447389:trail/management-event > Edit
Edit arn:aws:cloudtrail:us-east-1:044042447389:trail/management-eventInfo
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
New
Existing
Log group name
aws-cloudtrail-logs-044042447389-a18c0e2e
1-512 characters. Only letters, numbers, dashes, underscores, forward slashes, and periods are allowed.
AWS CloudTrail assumes this role to send CloudTrail events to your CloudWatch Logs log group.
New
Existing
Role name
CloudTrailRoleForCloudWatchLogs_{trail-name}
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

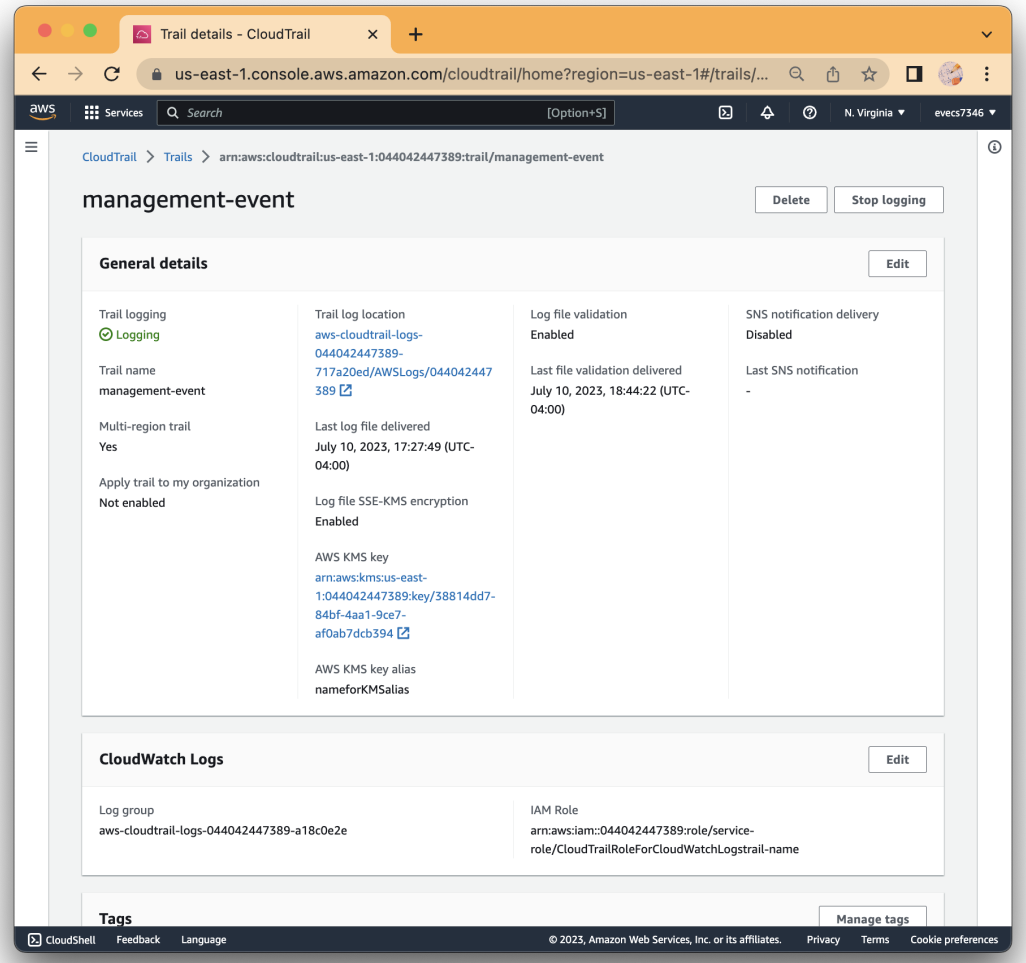
5.


Edit trail - CloudTrail
us-east-1.console.aws.amazon.com/cloudtrail/home?region=us-east-1#/...
aws
Services
Search
[Option+S]
N. Virginia
evecs7346
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
New
Existing
Log group name
aws-cloudtrail-logs-044042447389-a18c0e2e
1-512 characters. Only letters, numbers, dashes, underscores, forward slashes, and periods are allowed.
AWS CloudTrail assumes this role to send CloudTrail events to your CloudWatch Logs log group.
New
Existing
Role name
CloudTrailRoleForCloudWatchLogs_{trail-name}
Policy document
Cancel
Save changes
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

6.


Edit trail - CloudTrail
us-east-1.console.aws.amazon.com/cloudtrail/home?region=us-east-1#/...
aws
Services
Search
[Option+S]
N. Virginia
evecs7346
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
New
Existing
Log group name
aws-cloudtrail-logs-044042447389-a18c0e2e
1-512 characters. Only letters, numbers, dashes, underscores, forward slashes, and periods are allowed.
AWS CloudTrail assumes this role to send CloudTrail events to your CloudWatch Logs log group.
New
Existing
Role name
CloudTrailRoleForCloudWatchLogstrail-name
Policy document
Cancel
Save changes
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

7.


Trail details - CloudTrail
us-east-1.console.aws.amazon.com/cloudtrail/home?region=us-east-1#/trails/...
aws
Services
Search
[Option+S]
N. Virginia
evecs7346
CloudTrail > Trails > arn:aws:cloudtrail:us-east-1:044042447389:trail/management-event
management-event
Delete
Stop logging
General details
Edit
Trail logging
Logging
Trail name
management-event
Multi-region trail
Yes
Apply trail to my organization
Not enabled
Trail log location
aws-cloudtrail-logs-044042447389-717a20ed/AWSLogs/044042447389
Last log file delivered
July 10, 2023, 17:27:49 (UTC-04:00)
Log file SSE-KMS encryption
Enabled
AWS KMS key
arn:aws:kms:us-east-1:044042447389:key/38814dd7-84bf-4aa1-9ce7-af0ab7dcb394
AWS KMS key alias
nameforKMSalias
Log file validation
Enabled
Last file validation delivered
July 10, 2023, 18:44:22 (UTC-04:00)
SNS notification delivery
Disabled
Last SNS notification
-
CloudWatch Logs
Edit
Log group
aws-cloudtrail-logs-044042447389-a18c0e2e
IAM Role
arn:aws:iam::044042447389:role/service-role/CloudTrailRoleForCloudWatchLogstrail-name
Tags
Manage tags
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences