CLOUDTRAIL

Introduction

AWS CloudTrail is an AWS service that helps you enable governance, compliance, and operational and risk auditing of your AWS account. Actions taken by a user, role, or an AWS service are recorded as events in CloudTrail. Events include actions taken in the AWS Management Console, AWS Command Line Interface, and AWS SDKs and APIs.

AWS CloudTrail will only show the results of the CloudTrail Event History for the current region you are viewing for the last 90 days and support the AWS services found [here](http://docs.aws.amazon.com/awscloudtrail/latest/userguide/view-cloudtrail-events-supported-services.html). These events are limited to management events with create, modify, and delete API calls and account activity. For a complete record of account activity, including all management events, data events, and read-only activity, you’ll need to configure a CloudTrail trail.

In this lab, we will create a trail and configure it to send events to CloudWatch Logs. Then use CloudWatch Logs to monitor your account for specific API calls and events.

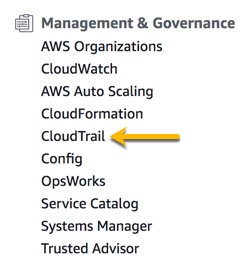
# SETUP

**The US-EAST-1 AWS Region must be used with Event Engine**

#### Create a Trail in CloudTrail

AWS CloudTrail is an AWS service that helps you enable governance, compliance, risk auditing and operational auditing of your AWS Account. Actions taken by a Principal (User, Role or AWS Service) are recorded as events in CloudTrail. To learn more about AWS CloudTrail you can click on this [link](https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html). Documentation on creating a Trail via the Console is located [here](https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-create-a-trail-using-the-console-first-time.html#creating-a-trail-in-the-console). We will highlight the steps below.

1. Search for the CloudTrail Service under the Management Tools Section in the console and click on Cloudtrail.

[](https://workshop.aws-management.tools/cloudtrail/images/CloudtrailConsole.jpg)

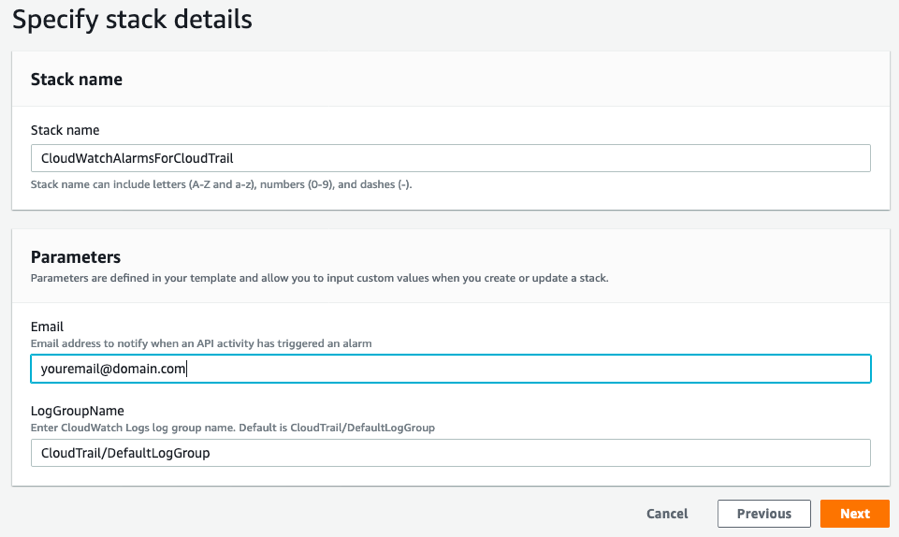
1. Click on getting Started if presented with that screen. Once in the CloudTrail Console, click on Trails on the Left Side of the screen.
2. Then Click on Create Trail, to create our trail for this lab
3. Apply the following settings and create the trail
   * Trail name: cloudtrail-immersionday
   * Create a new S3 Bucket: Yes
   * S3 bucket: cloudtrail-immersionday-(**Today’sDate**)-(**yourcellnumber**)
     + We are using Cell Phone Number at the End to ensure that we create a Uniquie Bucket per user. For more information on Bucket Restrictions and Limitations click [here](https://docs.aws.amazon.com/AmazonS3/latest/dev/BucketRestrictions.html)
   * Leave KMS encryption enabled and enter a KMS alias of: CloudWatchKMSKey
   * Select the Enabled check box for Cloudwatch Logs
     + For log group, select New
     + Log group name: aws-cloudtrail-logs-ACCOUNTNUMBER-myfirsttrail
     + Create a new IAM role named: Cloudtrail\_CloudwatchLogs\_role
   * Click Next
   * Leave all defaults on the log events screen and click next.
   * Finally review your settings and click create trail.

We now have a trail capturing activity in our AWS Account. Later on, we will search through our trail.

#### Create CloudWatch Alarms for Security and Network related API activity

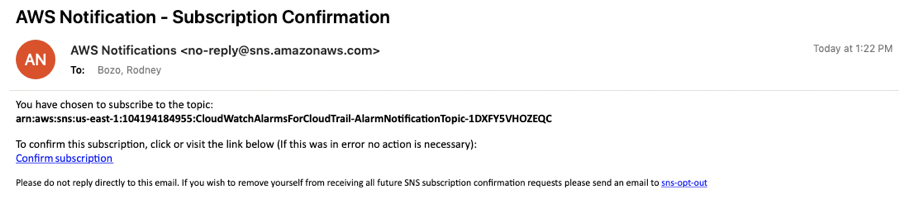
In this section, we will use the pre-defined CloudFormation template to create a set of CloudWatch Alarms to monitor for security and network related activity.

1. Follow [this deep link](https://console.aws.amazon.com/cloudformation/home?region=us-east-1#/stacks/create/template?stackName=CloudWatchAlarmsForCloudTrail&templateURL=https://s3-us-west-2.amazonaws.com/awscloudtrail/cloudwatch-alarms-for-cloudtrail-api-activity/CloudWatch_Alarms_for_CloudTrail_API_Activity.json) to use launch the CloudFromation template.
2. On the Create stack page, we will click Next.
3. In the Specify stack details page, we will specify a valid e-mail address and the LogGroupName we used in the previous section (Similar to aws-cloudtrail-logs-ACCOUNTNUMBER-myfirsttrail) . Click Next.

[](https://workshop.aws-management.tools/cloudtrail/images/CFNAlarmsStackSpecifyLogGroup.png)

1. On the next page, leave the default options and click Next.
2. When you see the Create stack button, click on it.

The CloudFormation template will create various resources, including CloudWatch Alarms and an SNS Topic with a Subscription. After the CloudFormation template deployment is complete, you will receive an SNS Subscription notifcation. When you receive, confirm the subscription.

[](https://workshop.aws-management.tools/cloudtrail/images/SubscriptionConfirmation.png)

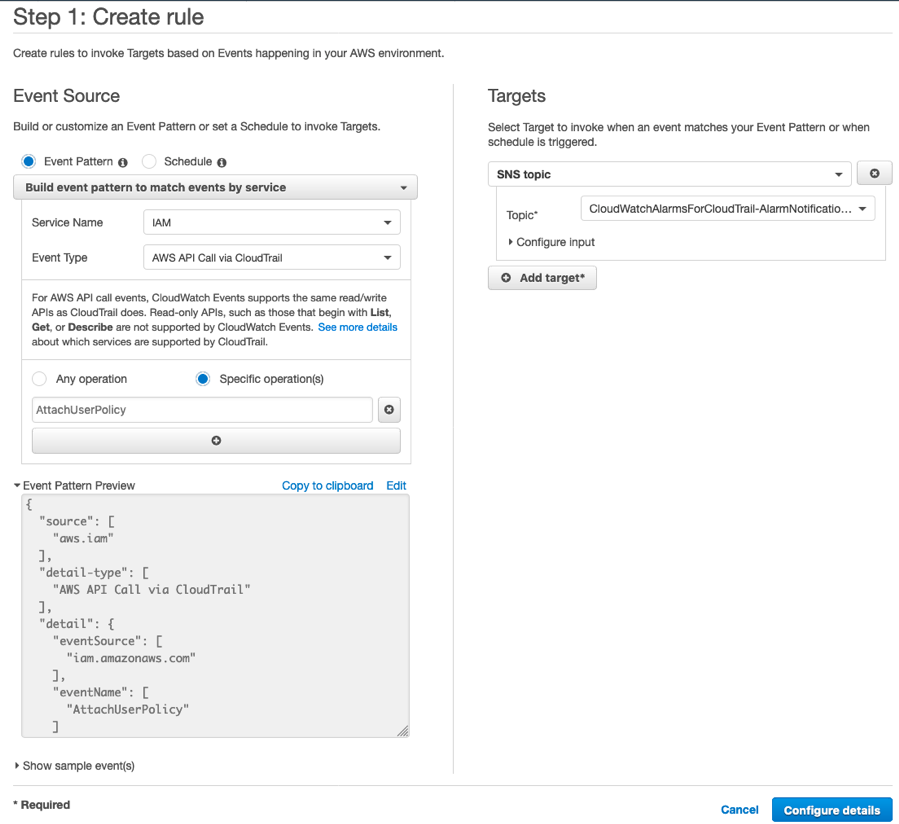
ALERTING

**Note :** Make sure complete the Setup before continuing with this section.

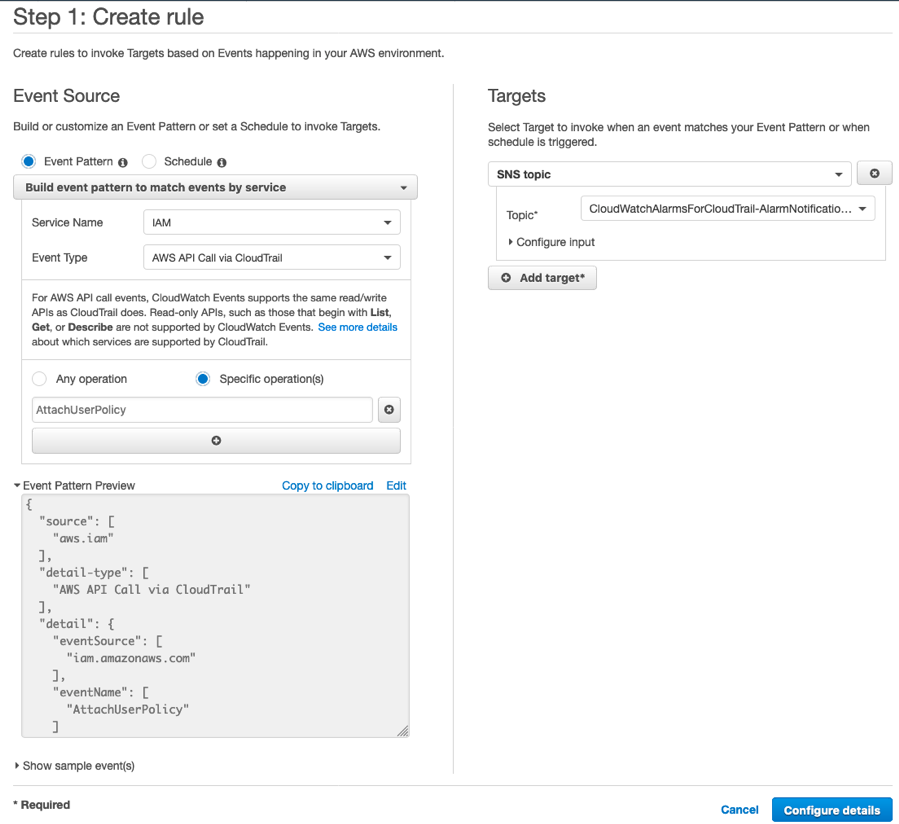
Creating Alerts via CloudWatch Events

In this section, we will use CloudWatch Events to monitor and alert when an IAM policy is attached to an IAM user. The example is simple and it helps to depict the level of visility that can be gained from using this type of process. The CloudWatch Event Rule created will monitor for a specific event name in CloudTrail, and will use an SNS message to notify regarding and event, when it occurs.

1. Go to the [CloudWatch Events Rules console](https://console.aws.amazon.com/cloudwatch/home#rules:).
2. Click on the Create rule button.
3. Configure the Rule using the following settings:
   * Event Pattern: Build event pattern to match events by service
   * Service Name: IAM
   * Event Type: AWS API Call via CloudTrail
   * Specific operation(s): **AttachUserPolicy**
   * Targets: SNS topic
   * Topic: CloudWatchAlarmsForCloudTrail-AlarmNotificationTopic-XXXXXXXXX

[](https://workshop.aws-management.tools/cloudtrail/images/CWEventRule.png)

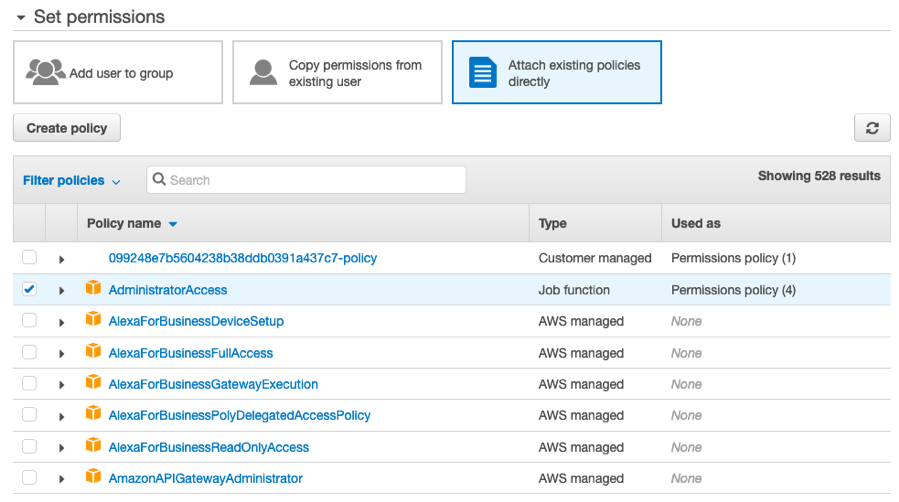
1. Click Configure details.
2. On the Configure rule details page, enter a Name for the rule (e.g. AttachUserPolcity\_CWE).
3. Click Create Rule.

[](https://workshop.aws-management.tools/cloudtrail/images/CWEventRule.png)

Triggering AttachUserPolicy Notification

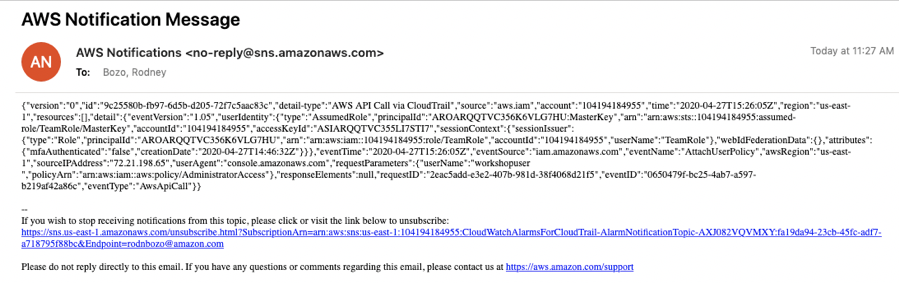
Now that we have an event we are monitoring, we will create an IAM user and attach a user policy to this user to trigger the notification.

1. Go to the [IAM Console](https://console.aws.amazon.com/iam/home#/users).
2. Click on Add user.
3. Set the following values for the user:
   * User name: workshopuser (or any other name)
   * Select AWS access type: AWS Management Console access
   * Console password: Autogeneratted password
   * Requrie password reset: Check the checkbox
4. Click Next: Permissions.
5. On the Set permissions page, we will select:
   * Attach existing policies directly
   * Check the checkbox for the AdministratorAccess policy

[](https://workshop.aws-management.tools/cloudtrail/images/UserPolicy.png)

1. Click on Next: Tags.
2. Click Next: Review on the Add tags page.
3. Click Create user.

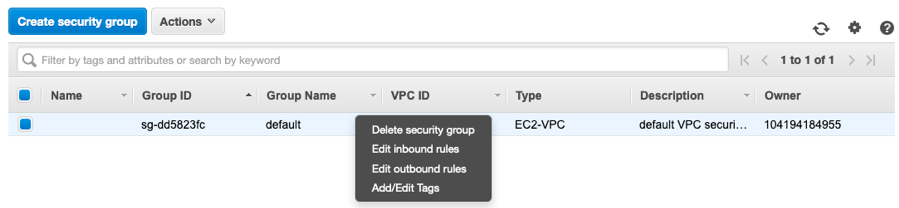
Once the user is created and the policy has been set, the CloudWatch Event pattern will be triggered and an e-mail will be sent to the e-mail address defined in the setup (i.e. Create CloudWatch Alarms for Security and Network related API activity).

[](https://workshop.aws-management.tools/cloudtrail/images/PolicyNotification.png)

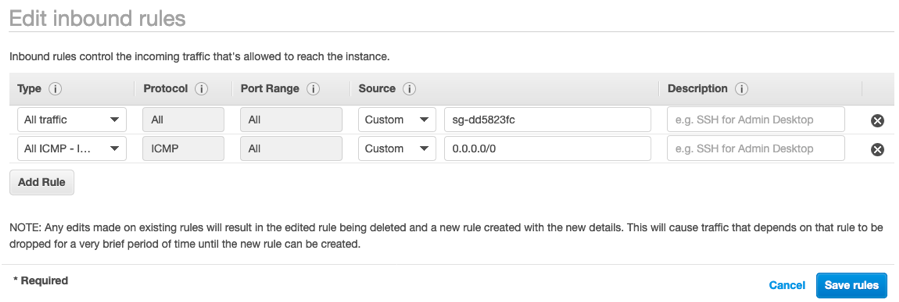
Triggering Network related API Notifications

As part of sending CloudTrail events to CloudWatch Logs, we also deployed a set of predefined CloudWatch Alarms to monitor Network and Security related API activity. In this section, we will trigger one of the network related alarms. Optionally, you can trigger the other [CloudWatch Alarms](https://console.aws.amazon.com/cloudwatch/home#alarmsV2:?~(selectedIds~(~'CloudTrailAuthorizationFailures))) created as part of launching the CloudFormation template in the setup.

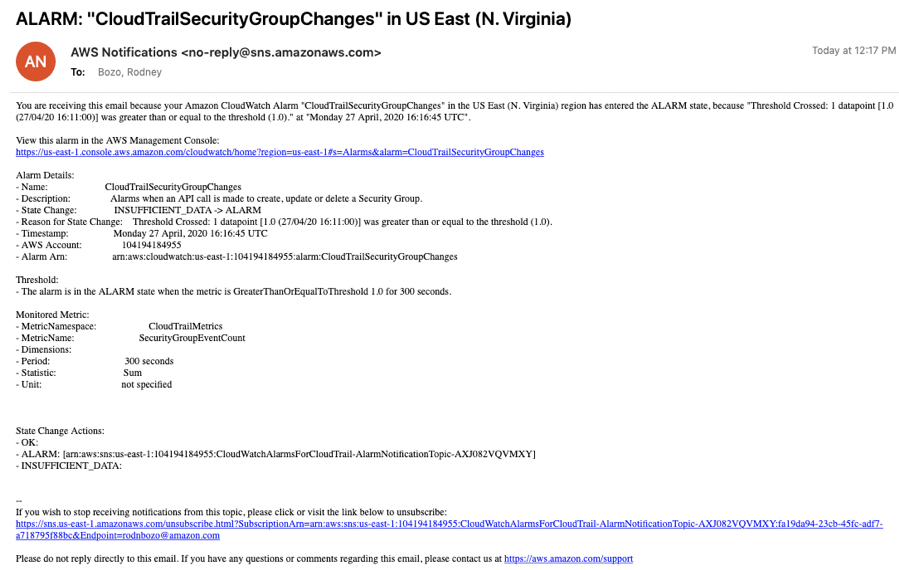
1. Go to the [VPC console](https://console.aws.amazon.com/vpc/home#SecurityGroups:sort=groupId).
2. Select the default security group.
3. Right click and select Edit inbound rules.

[](https://workshop.aws-management.tools/cloudtrail/images/EditSG.png)

1. Add a rule with the following settings:
   * Type: All ICMP - IPv4
   * Source:Custom
   * Network: 0.0.0.0/0
2. Click on Save rules.
3. Click Close.

[](https://workshop.aws-management.tools/cloudtrail/images/SGRule.png)

Once the alarm is processed, a notificatioin will be sent to the email address configured in the setup. Review the notification to understand what is logged.

[](https://workshop.aws-management.tools/cloudtrail/images/SGNotification.png)

METRICS

Creating CloudWatch Metric Filters

You can use metric filters to monitor events in a log group as they are sent to CloudWatch Logs. You can monitor and count specific terms or extract values from log events and associate the results with a metric. In this section, we will manually create a Metric Filter to show access denied errors found in CloudTrail.

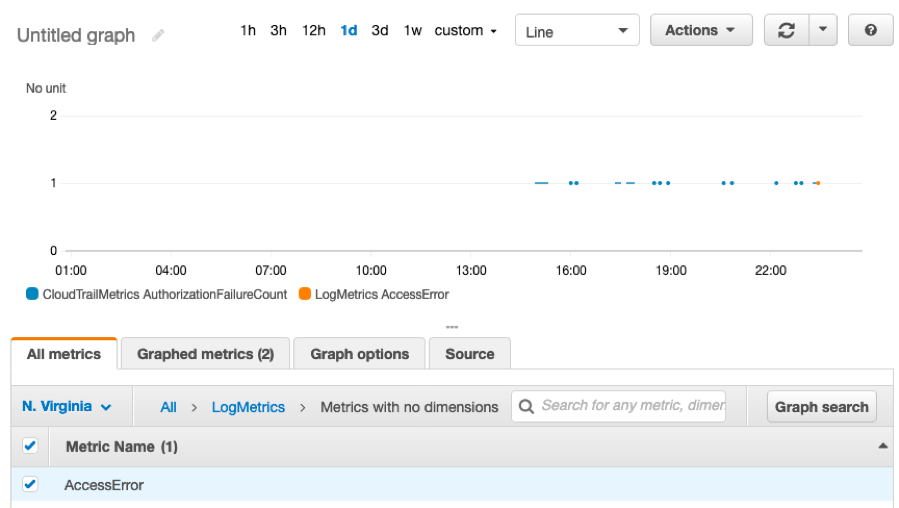
1. Go to the [CloudWatch console](https://console.aws.amazon.com/cloudwatch/home#logs:)
2. Select the CloudTrail Log Group we created in the setup.
3. Once selected, click on Actions and Create Metric Filter.
4. In the Filter pattern field, copy and paste the following query.
5. {$.errorCode = "ValidationException" || $.errorCode = "AccessDenied"}
6. Select our CloudTrail log to use as a test
7. Click on Test Pattern to make sure the filter is working, then click Next.
8. In the Metric Details Page, enter the following values.
   * Filter Name: Use the name AccessDeniedFilter
   * Metric Namespace: leave the default **LogMetrics** or give a name
   * Metric Name: AccessError
   * Metric Value: 1
9. Click on next. Review the metric, then create metric filter.

Graphing Creating CloudWatch Metric Filters

In the previous section, we created a Metric Filter from the CloudTrail events in CloudWatch Logs. In this section, we will visualize the data in a graph based on that filter.

1. Go to the [CloudWatch Metrics console](https://console.aws.amazon.com/cloudwatch/home#metricsV2:)
2. Click on the All metrics tab.
3. Select LogMetrics.
4. Click on Metriics with no dimensions.
5. Check the AccessError check box.
6. Make sure 1h is selected for the time span.

In the graph, we will see the activity related to the access denied errors found in the CloudTrail events of the CloudWatch Log Group.

[](https://workshop.aws-management.tools/cloudtrail/images/AccessErrorGraph.png)

LOGS INSIGHTS

Querying CloudTrail Logs in Logs Insights

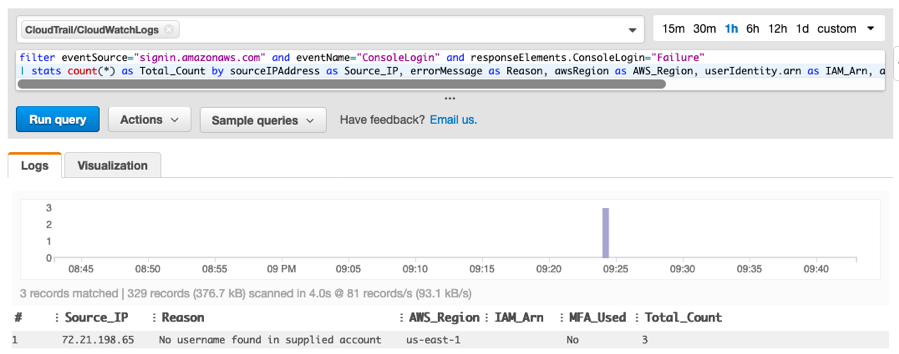
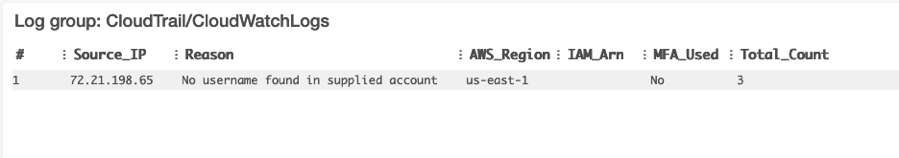
CloudWatch Logs Insights enables you to interactively search and analyze your log data in Amazon CloudWatch Logs. You can perform queries to help you more efficiently and effectively respond to operational issues. If an issue occurs, you can use CloudWatch Logs Insights to identify potential causes and validate deployed fixes.

CloudWatch Logs Insights automatically discovers fields in logs from AWS services such as Amazon Route 53, AWS Lambda, AWS CloudTrail, and Amazon VPC, and any application or custom log that emits log events as JSON. In this lab exercise, we will query CloudTrail events CloudWatch Logs data with Insights.

1. Go to the [CloudWatch Insights Console](https://console.aws.amazon.com/cloudwatch/home#logsV2:logs-insights)
2. Select the CloudWatch Log Group created during the setup from the dropdown.
3. In the query pane, enter the following query, which filters successful SignIn attempts to the AWS Account and also captures if MFA was used or not.

filter eventSource="signin.amazonaws.com" and eventName="ConsoleLogin" and responseElements.ConsoleLogin="Success"

| stats count(\*) as Total\_Count by sourceIPAddress as Source\_IP, errorMessage as Reason, awsRegion as AWS\_Region, userIdentity.arn as IAM\_Arn, additionalEventData.MFAUsed as MFA\_Used

1. Click on Run Query to view results.[](https://workshop.aws-management.tools/cloudtrail/images/QueryResults.png)
2. Click on Action and then click on Add to dashboard.
3. In the pop-up window:
   * Click on Create new
   * Give a dashboard name MyFirstDashboard.
   * Click on the small tick icon to create the dashboard.`
4. Click on Add to dashboard.
5. Navigate to MyFirstDashboard under Dashboards from the left navigation pane. View the Widget.[](https://workshop.aws-management.tools/cloudtrail/images/Dashboard.png)

**Note:** The CloudWatch Logs Insights Console has a few sample queries to start with under Sample queries. Refer this [document](https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CWL_QuerySyntax-examples.html) for more information.