<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-tutorial.html>

**Domain: Management & Customer Enablement**

**Topic: CloudTrail**

**Task: Creating a CloudTrail trail and describe it using console and cli**

**Problem to Be Solved**

*We grant wide permission for some person, by assuming IAM role to him, and we want to get info about his actions. We should have the ability to audit his actions not only from AWS console but from cli.*

**Explanation of the Solution**

**Implementation Details**

*Before doing this task you should create IAM user and grant him permissions for using CloudTrail.* [*https://docs.aws.amazon.com/awscloudtrail/latest/userguide/security\_iam\_id-based-policy-examples.html#grant-permissions-for-cloudtrail-administration*](https://docs.aws.amazon.com/awscloudtrail/latest/userguide/security_iam_id-based-policy-examples.html#grant-permissions-for-cloudtrail-administration)

*After we log in as newly IAM user, we can configure our trail:*

1. *Open the CloudTrail console at*[*https://console.aws.amazon.com/cloudtrail/home/*](https://console.aws.amazon.com/cloudtrail/home/)*. In the Region selector, choose the AWS Region where you want your trail to be created. This is the home Region for the trail.*
2. On the CloudTrail service home page, the **Trails** page, or the **Trails** section of the **Dashboard** page, choose **Create trail**.
3. In **Trail name**, give your trail a name, such as *My-Management-Events-Trail*. As a best practice, use a name that quickly identifies the purpose of the trail. In this case, you're creating a trail that logs management events.
4. Leave default settings for AWS Organizations organization trails. This option won't be available to change unless you have accounts configured in Organizations.
5. For **Storage location**, choose **Create new S3 bucket** to create a bucket. When you create a bucket, CloudTrail creates and applies the required bucket policies. Give your bucket a name, such as *your-name-bucket-for-storing-cloudtrail-logs*.

To make it easier to find your logs, create a new folder (also known as a prefix) in an existing bucket to store your CloudTrail logs. Enter the prefix in **Prefix**.

1. Clear the check box to disable **Log file SSE-KMS encryption**. By default, your log files are encrypted with SSE-S3 encryption.
2. Leave default settings in **Additional settings**.
3. For now, do not send logs to Amazon CloudWatch Logs.
4. In **Tags**, add one or more custom tags (key-value pairs) to your trail. Tags can help you identify your CloudTrail trails and other resources, such as the Amazon S3 buckets that contain CloudTrail log files. For example, you could attach a tag with the name **Compliance** and the value **Auditing**.
5. On the **Choose log events** page, select event types to log. For this trail, keep the default, **Management events**. In the **Management events** area, choose to log both **Read** and **Write** events, if they are not already selected. Leave the check box for **Exclude AWS KMS events** empty, to log all AWS Key Management Service (AWS KMS) events.
6. Leave default settings for **Data events** and Insights events. This trail will not log any data or CloudTrail Insights events. Choose **Next**.
7. On the **Review and create** page, review the settings you've chosen for your trail. Choose **Edit** for a section to go back and make changes. When you are ready to create your trail, choose **Create trail**.
8. The **Trails** page shows your new trail in the table. Note that the trail is set to **Multi-region trail** by default, and that logging is turned on for the trail by default.

Within an average of about 15 minutes of creating your first trail, CloudTrail delivers the first set of log files to the Amazon S3 bucket for your trail. You can look at these files and learn about the information they contain.

After the first records receiving you can find it in two different ways:

* View log files from the console
* View log files from AWS cli

*View log files from console:*

1. In the navigation pane, choose **Trails**. On the **Trails** page, find the name of the trail you just created (in the example, *My-Management-Events-Trail*).
2. In the row for the trail, choose the value for the S3 bucket (in the example, *aws-cloudtrail-logs-08132020-mytrail*).
3. The Amazon S3 console opens and shows that bucket, at the top level for log files. Because you created a trail that logs events in all AWS Regions, the display opens at the level that shows you each Region folder. The hierarchy of the Amazon S3 bucket navigation at this level is *bucket-name*/AWSLogs/*AWS-account-id/*CloudTrail. Choose the folder for the AWS Region where you want to review log files. For example, if you want to review the log files for the US East (Ohio) Region, choose **us-east-2**.
4. Navigate the bucket folder structure to the year, the month, and the day where you want to review logs of activity in that Region. In that day, there are a number of files. The name of the files begin with your AWS account ID, and end with the extension .gz. For example, if your account ID is *123456789012*, you would see files with names similar to this: *123456789012*\_CloudTrail\_*us-east-2*\_*20190610T1255abcdeEXAMPLE*.json.gz.

To view these files, you can download them, unzip them, and then view them in a plain-text editor or a JSON file viewer. Some browsers also support viewing .gz and JSON files directly. We recommend using a JSON viewer, as it makes it easier to parse the information in CloudTrail log files.

As you're browsing through the file content, you might start to wonder about what you're seeing. CloudTrail logs events for every AWS service that experienced activity in that AWS Region at the time that event occurred. In other words, events for different AWS services are mixed together, based solely on time. To learn more about what a specific AWS service logs with CloudTrail, including examples of log file entries for API calls for that service, see the [list of supported services for CloudTrail](https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-aws-service-specific-topics.html#cloudtrail-aws-service-specific-topics-list), and read the CloudTrail integration topic for that service. You can also learn more about the content and structure of CloudTrail log files by reviewing the [CloudTrail Log Event Reference](https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-event-reference.html).

You might also notice what you're not seeing in log files in US East (Ohio). Specifically, you won't see any console sign-in events, even though you know you logged into the console. That's because console sign-in and IAM events are [global service events](https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-concepts.html#cloudtrail-concepts-global-service-events), which are usually logged in a specific AWS Region. In this case, they are logged in US East (N. Virginia), and found in the folder **us-east-1**. Open that folder, and open the year, month, and day you're interested in.

*View log files from AWS cli:*

Prerequisites:

* To run AWS CLI commands, you must install the AWS CLI. For information, see [Installing the AWS Command Line Interface](https://docs.aws.amazon.com/cli/latest/userguide/installing.html).
* Make sure your AWS CLI version is greater than 1.6.6. To verify the CLI version, run **aws --version** on the command line.
* To set the account, region, and default output format for an AWS CLI session, use the **aws configure** command. For more information, see [Configuring the AWS Command Line Interface](https://docs.aws.amazon.com/cli/latest/userguide/cli-chap-getting-started.html).

Task:

1. Type the following command for lookup last ten events:

***aws cloudtrail lookup-events***

For an explanation of the lookup-related fields in the output, see the section [Lookup Output Fields](https://docs.aws.amazon.com/awscloudtrail/latest/userguide/view-cloudtrail-events-cli.html#view-cloudtrail-events-cli-output-fields) later in this document. For an explanation of the fields in the CloudTrail event, see [CloudTrail Record Contents](https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-event-reference-record-contents.html)

1. Try to specify the number of events to return:

***aws cloudtrail lookup-events --max-results 5***

1. Try to lookup events by time range:

***aws cloudtrail lookup-events --start-time <timestamp> --end-time <timestamp>***

1. Try to lookup events by attribute:

***aws cloudtrail lookup-events --lookup-attributes AttributeKey=<attribute>,AttributeValue=<string>***

For example you can use following values:

***aws cloudtrail lookup-events --lookup-attributes AttributeKey=EventName,AttributeValue=RunInstances***

**Benefits / Outcomes / Pros and Cons / Summary**

*Now you know how to create trails and how to view events in them.*

**Pricing**

*Free*