

Module 6: Automate Monitoring And Event Management In AWS

Demo Document 2

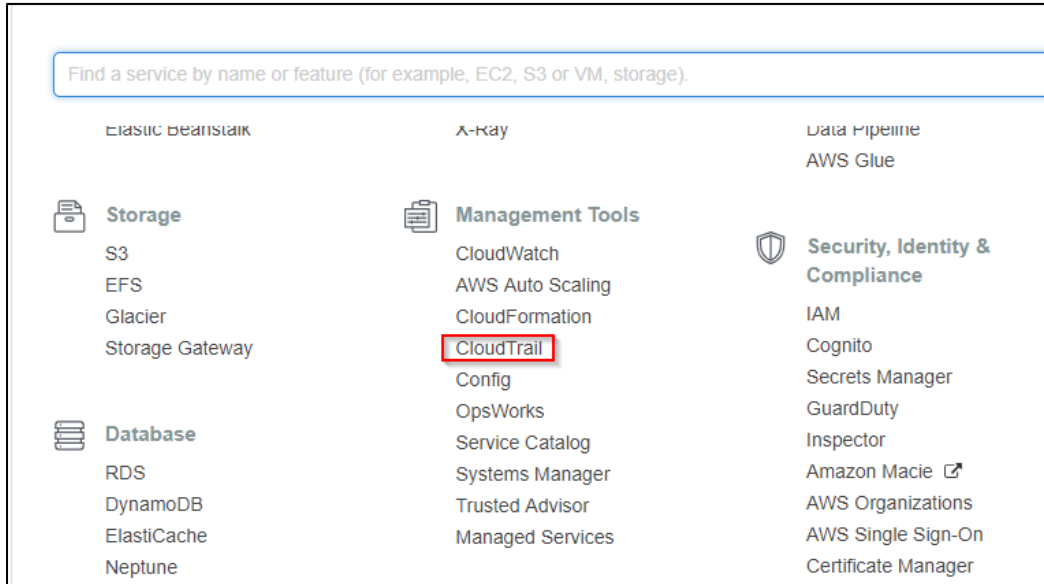
edureka!

edureka!

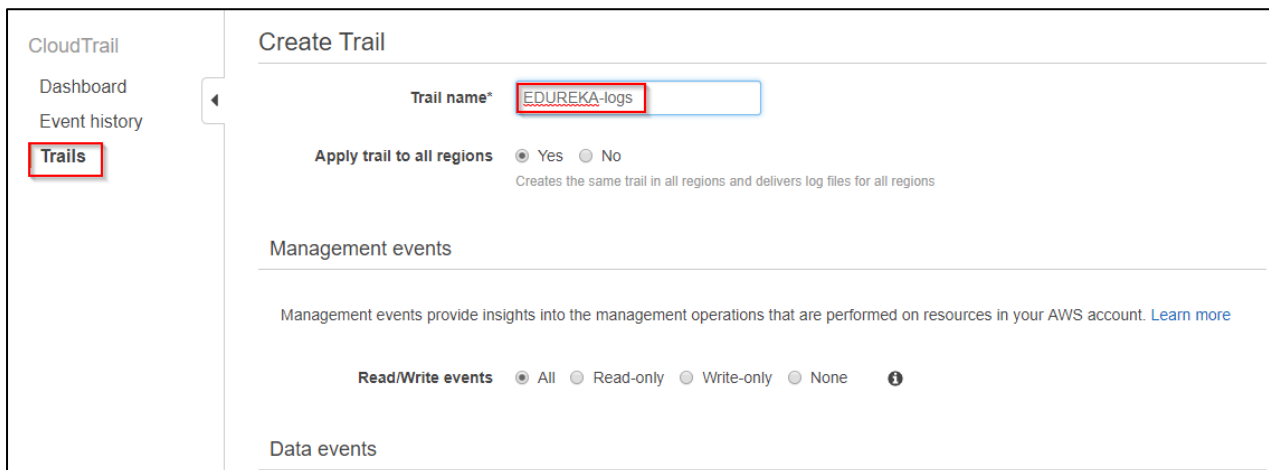
© Brain4ce Education Solutions Pvt. Ltd.

Enable CloudTrail And Store Logs In S3

Step 1: Go to **AWS Management Console** and select “CloudTrail”



Step 2: Click on “Create Trail” and configure the following details



Step 3: Create a **S3 bucket** to store all your log files monitored by the CloudTrail

Create a new S3 bucket ☐ Yes ☒ No

S3 bucket* ⓘ

Log file prefix ⓘ
Location: CloudTrail/AWSLogs/245376966395/CloudTrail/us-west-1

Encrypt log files with SSE-KMS ☐ Yes ☒ No ⓘ

Enable log file validation ☒ Yes ☐ No ⓘ

Step 4: If you receive the **notifications via mails** then you can even attach **SNS topic**

Enable log file validation ☒ Yes ☐ No ⓘ

Send SNS notification for every log file delivery ☒ Yes ☐ No ⓘ

Create a new SNS topic ☐ Yes ☒ No

SNS topic* ⓘ

* Required field

Additional charges may apply ⓘ

Create

Step 5: Finally on configuring all the details click on “Allow”

Trails

Deliver logs to an Amazon S3 bucket. CloudTrail events can be processed by one trail for free. There is a charge for processing events with additional trails. For more information, see [AWS CloudTrail Pricing](#).

[Create trail](#)

Name ▲	Region ▼	S3 bucket ▲	Log file prefix ▲	CloudWatch Logs Log group ▲	Status ▲
edureka-cloudtrail-log	All	edureka-17		CloudTrail/trainingLogGroup	✓
EDUREKA-logs	All	edurekalogrecords	CloudTrail	CloudTrail/DefaultLogGroup	✓
boot-trail	All	awsysops			✓

Step 6: From now to check all your log activity records go the created S3 bucket and click on **CloudTrail** log file

Amazon S3 > [edurekalogrecords](#)

Overview Properties Permissions Management

Q Type a prefix and press Enter to search. Press ESC to clear.

[Upload](#) [+ Create folder](#) [Actions](#) ▼

US West (N. Calif.)

<input type="checkbox"/>	Name ↑	Last modified ↑	Size ↑	Storage class ↑
<input type="checkbox"/>	CloudTrail	--	--	--

Step 7: Here you can select the region of your choice and check all the log activities happening in that region

Amazon S3 > edurekaalogs / CloudTrail / AWSLogs / 245376966395 / CloudTrail

Overview

🔍 Type a prefix and press Enter to search. Press ESC to clear.

Upload Create folder Actions

US West (N. California) ↻

Viewing 1 to 16

<input type="checkbox"/>	Name ↑	Last modified ↑	Size ↑	Storage class ↑
<input type="checkbox"/>	ap-northeast-1	--	--	--
<input type="checkbox"/>	ap-northeast-2	--	--	--
<input type="checkbox"/>	ap-northeast-3	--	--	--
<input type="checkbox"/>	ap-south-1	--	--	--
<input type="checkbox"/>	ap-southeast-1	--	--	--
<input type="checkbox"/>	ap-southeast-2	--	--	--

Step 8: example- following are the log file of date **28/10/2018**, you can retrieve them and read them manually

Amazon S3 > edurekaalogs / CloudTrail / AWSLogs / 245376966395 / CloudTrail / us-west-2 / 2018 / 10 / 28

Overview

🔍 Type a prefix and press Enter to search. Press ESC to clear.

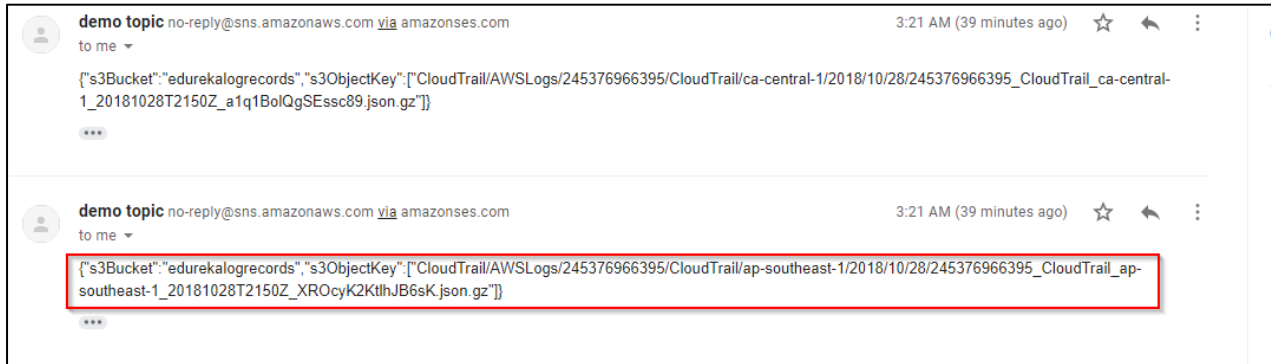
Upload Create folder Actions

US West (N. California) ↻

Viewing 1 to 4

<input type="checkbox"/>	Name ↑	Last modified ↑	Size ↑	Storage class ↑
<input type="checkbox"/>	245376966395_CloudTrail_us-west-2_20181028T2150Z_qum8kM0pR6eJdW...	Oct 29, 2018 3:23:53 AM GMT+0530	1.2 KB	Standard
<input type="checkbox"/>	245376966395_CloudTrail_us-west-2_20181028T2150Z_ve6HdEMHvpcc0KL...	Oct 29, 2018 3:28:01 AM GMT+0530	504.0 B	Standard
<input type="checkbox"/>	245376966395_CloudTrail_us-west-2_20181028T2150Z_zi25MjOI805M9swN...	Oct 29, 2018 3:22:14 AM GMT+0530	502.0 B	Standard
<input type="checkbox"/>	245376966395_CloudTrail_us-west-2_20181028T2155Z_loJsPpPap82SEaxX....	Oct 29, 2018 3:32:06 AM GMT+0530	2.5 KB	Standard

Step 9: As you have configured **SNS topic** so on every log activity happening in your account **CloudTrail notifies you via mail**



Conclusion

You have successfully configured the **CloudTrail** your AWS account to monitor all the log activities