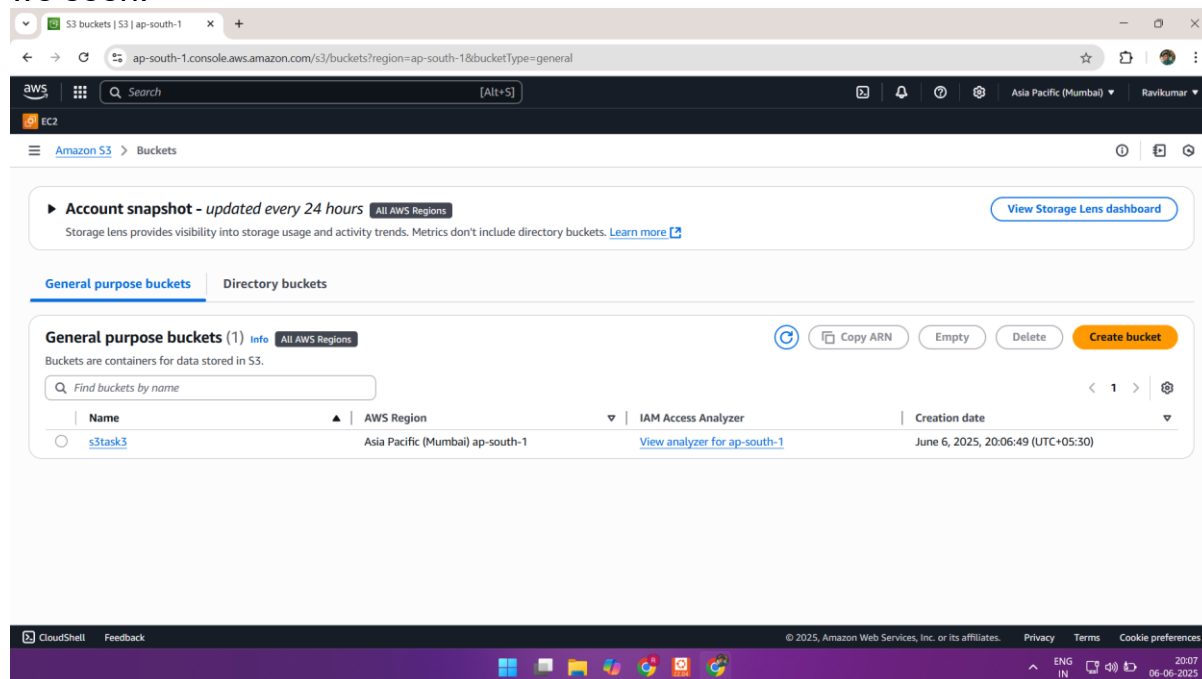
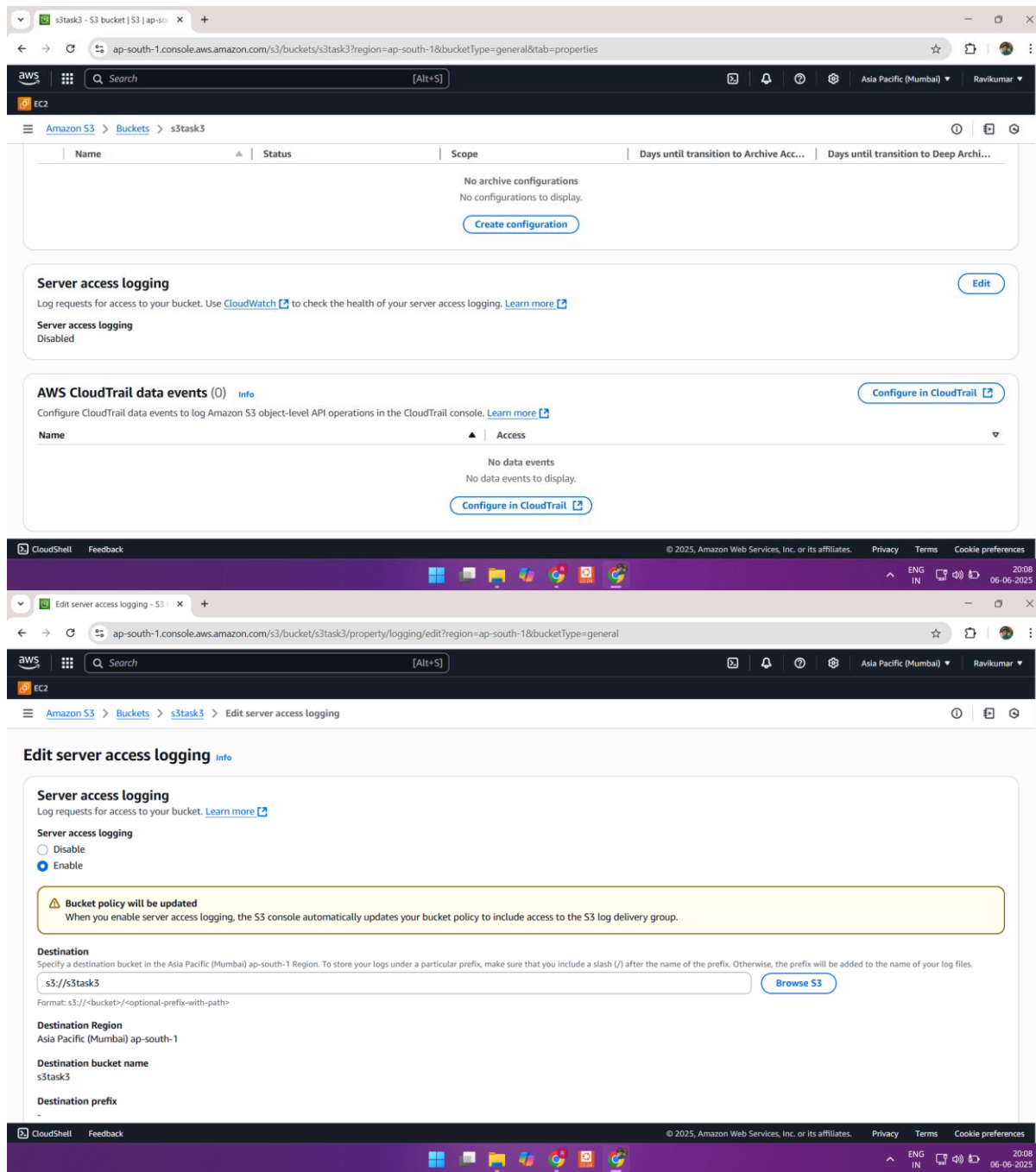


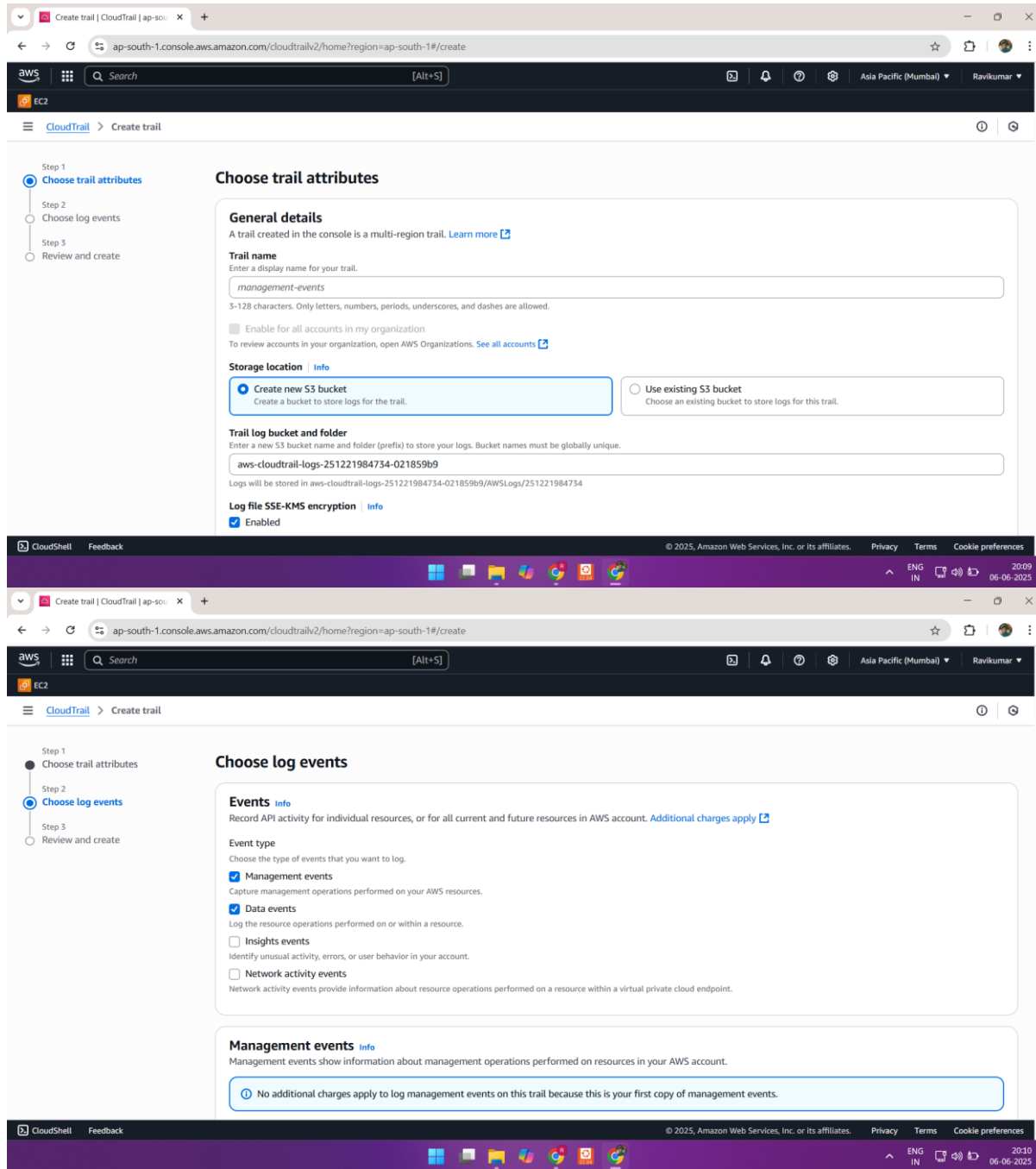
AWS Task-3

Create a S3 bucket, with no public access and upload files to the bucket & view the logs using cloudwatch for the uploaded files.

1. First in aws console. search s3, and go to s3 bucket. Create bucket. And upload some files. Then go to that created bucket inside server access logging need to enabled and give destination that s3 created bucket then save and exit.
2. Second in aws console search cloudtrail. And go to trail click , create cloudtrail give all the details, like trail name, storage location, kms key name, and below here cloudwatch logging is must should be enabled. Then go to next, next page we need to give management events, dat events both should be read and write then next and create trail.
3. Third in aws console search cloudwatch. then go to log groups, here we see the cloud trails created that click on that. Then it shows log streams, inside that log events date times activities fully we seen.







ap-south-1.console.aws.amazon.com/cloudtrailv2/home?region=ap-south-1#/create

CloudTrail

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

s3-bucket-access

Trail log location

s3task3/AWSLogs/251221984734

Log file validation

Enabled

Multi-region trail

Yes

Log file SSE-KMS encryption

Enabled

SNS notification delivery

Disabled

Apply trail to my organization

Not enabled

AWS KMS key alias

s3-access-key

CloudWatch Logs

Log group

aws-cloudtrail-logs-ravik

IAM Role

aws-s3-access-ravi

Tags

CloudShell

Feedback

© 2025, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

20:10
06-06-2025

Trails | CloudTrail | ap-south-1

ap-south-1.console.aws.amazon.com/cloudtrailv2/home?region=ap-south-1#/trails

Trail successfully created

Trails

Copy events to Lake

Delete

Create trail

	Name	Home region	Multi-region trail	ARN	Insights	Organization trail	S3 bucket	Log file prefix	CloudWatch Logs log group	Status
<input type="radio"/>	s3-bucket-access	Asia Pacific (Mumbai)	Yes	arn:aws:cloudtrail:ap-south-1:251221984734:trail/s3-bucket-access	Disabled	No	s3task3	-	arn:aws:logs:ap-south-1:251221984734:log-group:aws-cloudtrail-logs-ravik:*	Logging

CloudShell

Feedback

© 2025, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

20:10
06-06-2025

CloudWatch | ap-south-1

ap-south-1.console.aws.amazon.com/cloudwatch/home?region=ap-south-1#logsV2-log-groups/log-group/aws-cloudtrail-logs-ravi

CloudWatch

Log groups

aws-cloudtrail-logs-ravi

CloudWatch

Favorites and recents

Dashboards

AI Operations Preview

Alarms 0 0 0 0

Logs

Log groups

Log Anomalies

Live Tail

Logs Insights

Contributor Insights

Metrics

X-Ray traces

Events

Application Signals New

Network Monitoring

Creation time

3 hours ago

Retention

Never expire

Stored bytes

-

KMS key ID

-

Anomaly detection

Configure

Configure

Transformer

Configure

Log streams

Tags

Anomaly detection

Metric filters

Subscription filters

Contributor Insights

Data protection

Field

Log streams (4)

Filter log streams or try prefix search

Exact match

Show expired Info

Log stream

Last event time

251221984734_CloudTrail_ap-south-1

2025-06-06 12:11:44 (UTC)

251221984734_CloudTrail_ap-south-1_4

2025-06-06 12:11:02 (UTC)

251221984734_CloudTrail_ap-south-1_3

2025-06-06 12:10:53 (UTC)

251221984734_CloudTrail_ap-south-1_2

2025-06-06 12:08:11 (UTC)

CloudShell

Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

ENG IN 20:11 06-06-2025

CloudWatch | ap-south-1

ap-south-1.console.aws.amazon.com/cloudwatch/home?region=ap-south-1#logsV2-log-groups/log-group/aws-cloudtrail-logs-ravi/log-events/251221984734_CloudTrail_ap-south-1

CloudWatch

Log groups

aws-cloudtrail-logs-ravi

251221984734_CloudTrail_ap-south-1

CloudWatch

Favorites and recents

Dashboards

AI Operations Preview

Alarms 0 0 0 0

Logs

Log groups

Log Anomalies

Live Tail

Logs Insights

Contributor Insights

Metrics

X-Ray traces

Events

Application Signals New

Network Monitoring

Log events

You can use the filter bar below to search for and match terms, phrases, or values in your log events. Learn more about filter patterns

Filter events - press enter to search

Clear

1m

30m

1h

12h

Custom

UTC timezone

Display

Timestamp

Message

2025-06-06T12:05:26.571Z

{ "eventVersion": "1.11", "userIdentity": { "type": "Root", "principalId": "251221984734", "arn": "arn:aws:iam::251221984734:root", "account..."

2025-06-06T12:05:26.571Z

{ "eventVersion": "1.11", "userIdentity": { "type": "Root", "principalId": "251221984734", "arn": "arn:aws:iam::251221984734:root", "account..."

2025-06-06T12:05:26.571Z

{ "eventVersion": "1.11", "userIdentity": { "type": "Root", "principalId": "251221984734", "arn": "arn:aws:iam::251221984734:root", "account..."

2025-06-06T12:05:26.571Z

{ "eventVersion": "1.11", "userIdentity": { "type": "Root", "principalId": "251221984734", "arn": "arn:aws:iam::251221984734:root", "account..."

2025-06-06T12:07:53.245Z

{ "eventVersion": "1.11", "userIdentity": { "type": "Root", "principalId": "251221984734", "arn": "arn:aws:iam::251221984734:root", "account..."

2025-06-06T12:07:53.246Z

{ "eventVersion": "1.09", "userIdentity": { "type": "Root", "principalId": "251221984734", "arn": "arn:aws:iam::251221984734:root", "account..."

2025-06-06T12:07:53.246Z

{ "eventVersion": "1.11", "userIdentity": { "type": "Root", "principalId": "251221984734", "arn": "arn:aws:iam::251221984734:root", "account..."

{ "eventVersion": "1.11", "userIdentity": { "type": "Root", "principalId": "251221984734", "arn": "arn:aws:iam::251221984734:root", "account..."

CloudShell

Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

ENG IN 20:11 06-06-2025