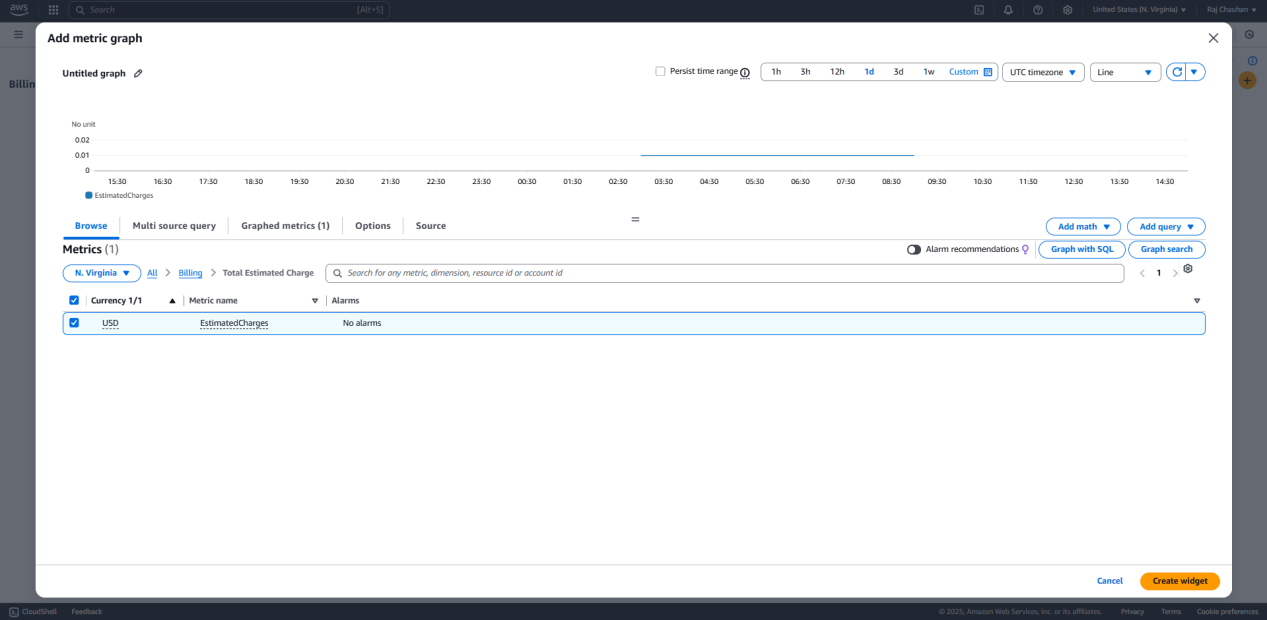
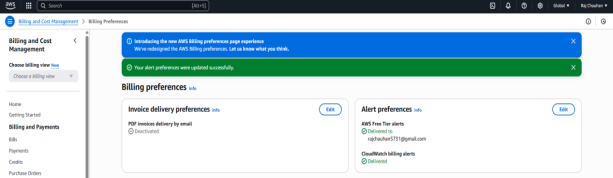
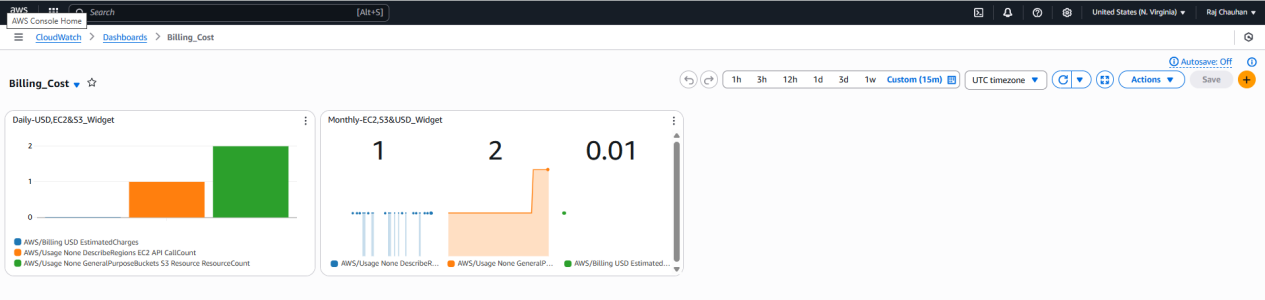
**Enable CloudWatch Billing Alerts Go to: Billing Preferences → Enable “CloudWatch billing alerts”. AWS/Billing → EstimatedCharges (USD)**



**Section 1: Billing & Cost Monitoring Dashboard**

Go to CloudWatch → Dashboards → Create Dashboard → Billing\_Cost

Widget 1: Daily-EC2&S3\_Widget Widget 2: Monthly-EC2&S3\_Widget

Metrics Used: Metrics Used:

AWS/Billing: USD EstimatedCharges (green) AWS/Billing: USD EstimatedCharges

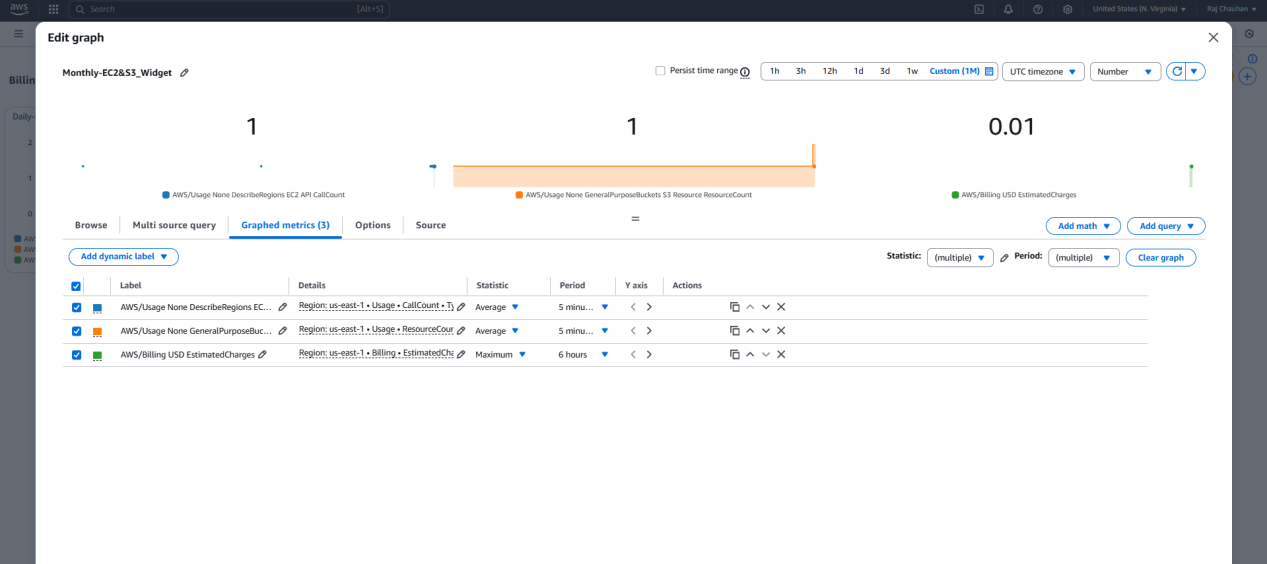
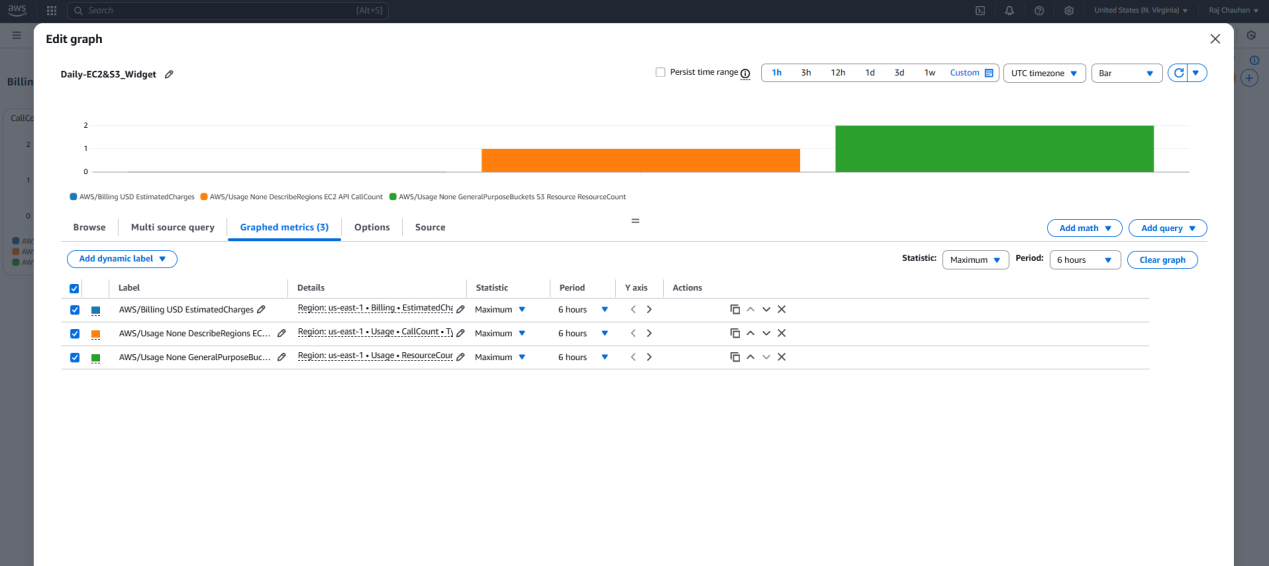
AWS/Usage: DescribeRegions EC2 API CallCount (orange) AWS/Usage: DescribeRegions EC2 API CallCounT

AWS/Usage: GeneralPurposeBuckets S3 ResourceCount (blue) AWS/Usage: GeneralPurposeBuckets S3 ResourceCount

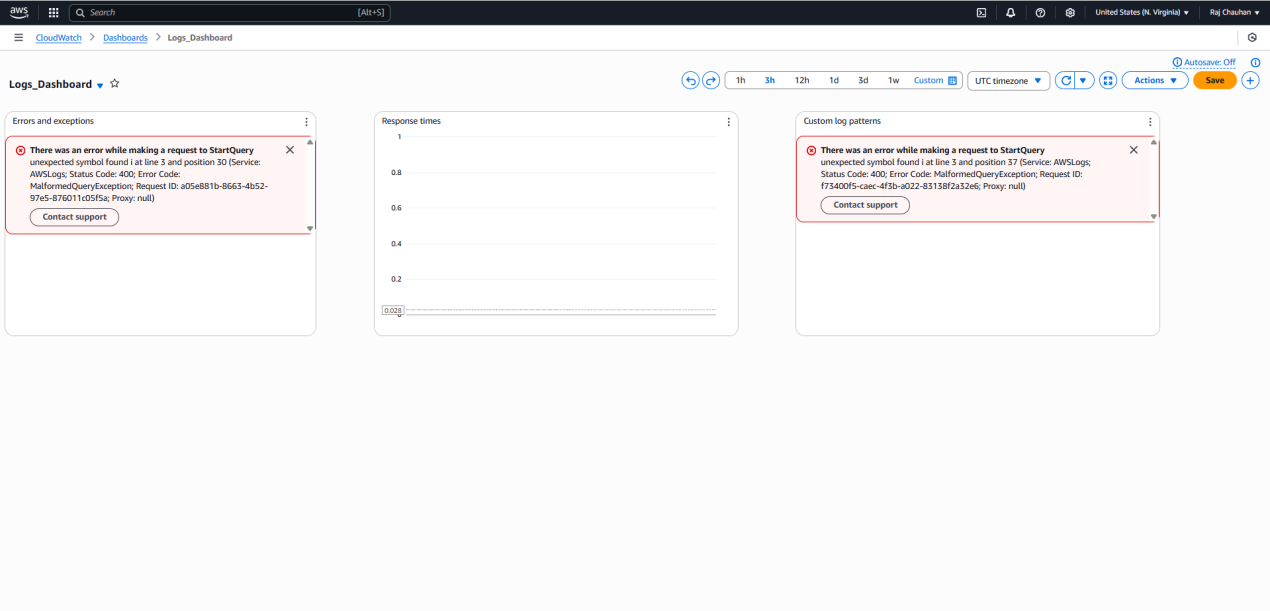
Statistic: Maximum Statistic: Mixed (Average/Max)

Period: 6 hours Period: 1 Month

Visualization: Bar graph Visualization: Number + Line



**Section 2:Logs Dashboard**

Go to CloudWatch → Dashboards → Create Dashboard → Logs Dashboard 

**Install & Start Agent:**

sudo yum install amazon-cloudwatch-agent -y

cd /opt/aws/amazon-cloudwatch-agent/bin/

sudo nano config.json

{

"logs": {

"logs\_collected": {

"files": {

"collect\_list": [

{

"file\_path": "/var/log/messages",

"log\_group\_name": "ec2-system-logs"

},

{

"file\_path": "/var/log/nginx/error.log",

"log\_group\_name": "nginx-error-logs"

}

]

}

}

}

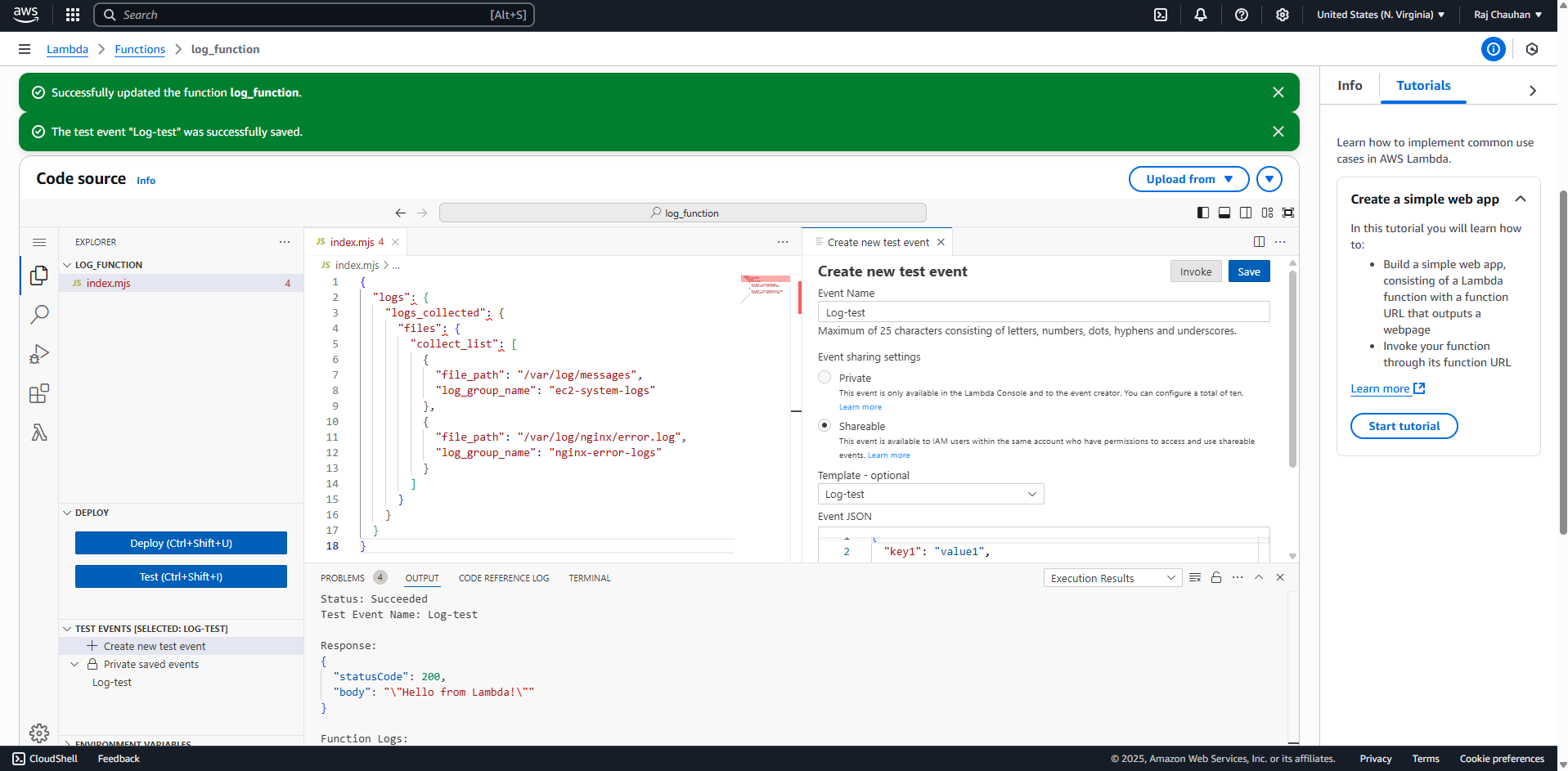
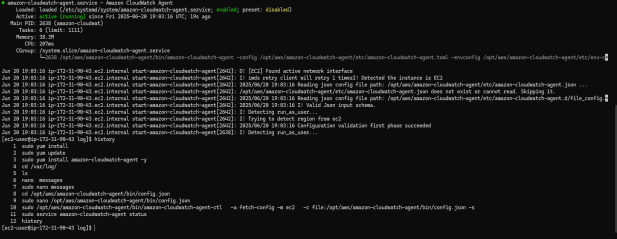
}

sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl \ Lambda Function log\_function

-a fetch-config -m ec2 \ Log paths:

-c file:/opt/aws/amazon-cloudwatch-agent/bin/config.json -s /var/log/messages → ec2-system-logs

/var/log/nginx/error.log → nginx-error-logs

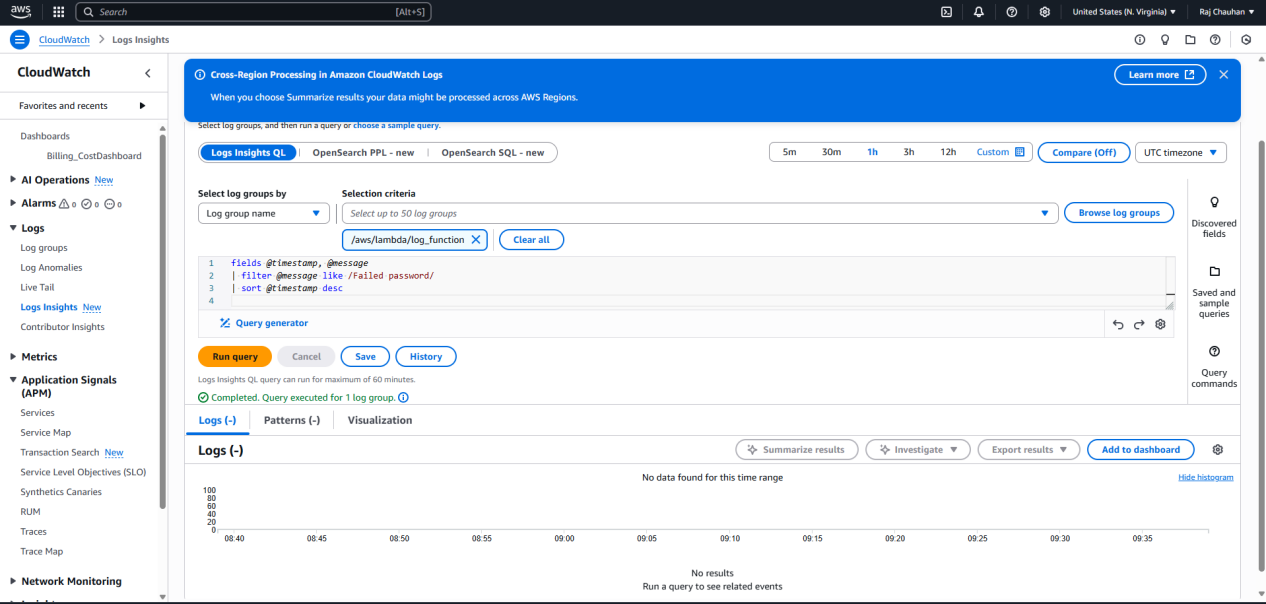
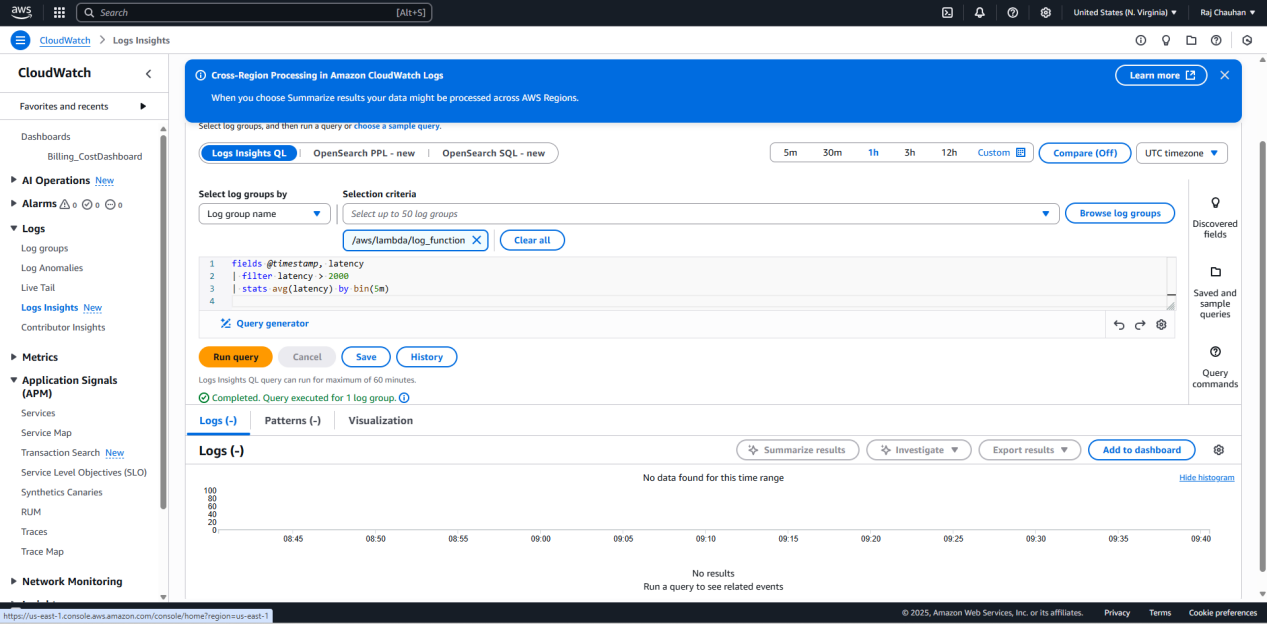
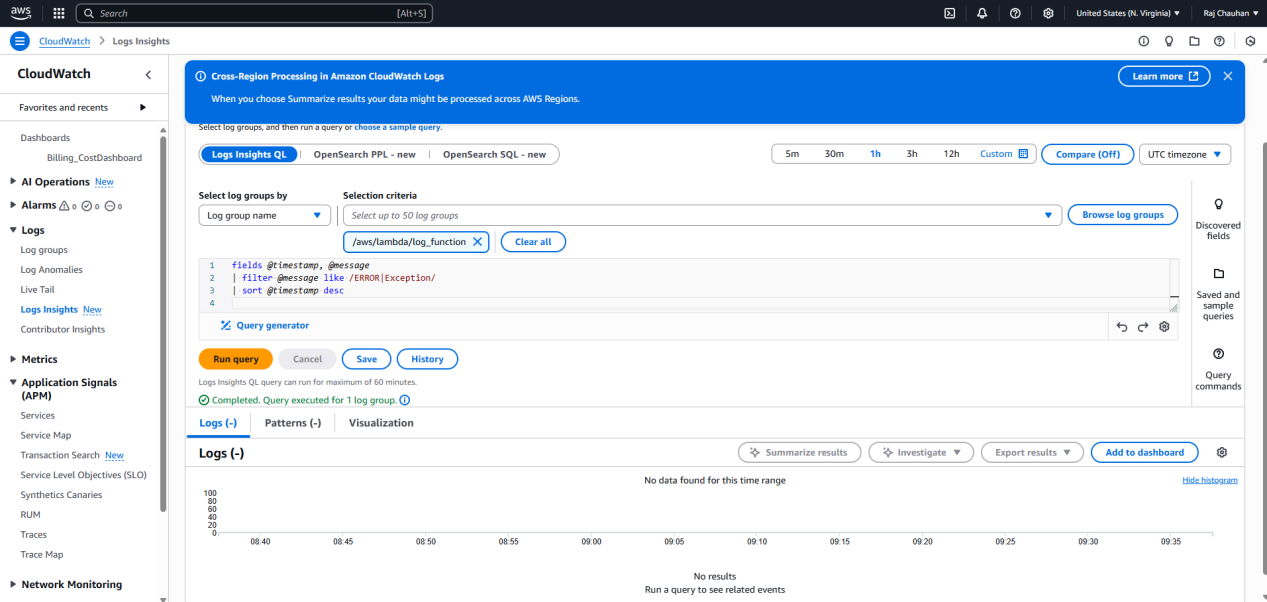


Query 1: Find errors Query 2: Check high latency Query 3: Detect failed passwords

fields @timestamp, @message fields @timestamp, latency fields @timestamp, @message

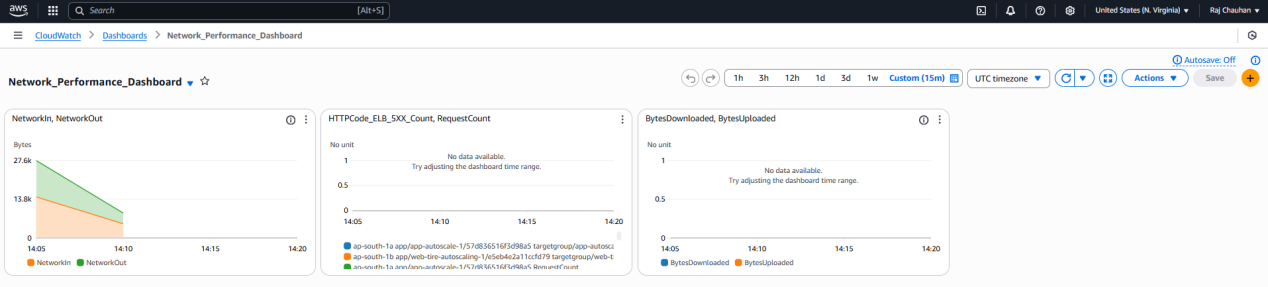
| filter @message like /ERROR|Exception/ | filter latency > 2000 | filter @message like /Failed password/

| sort @timestamp desc | stats avg(latency) by bin(5m) | sort @timestamp desc



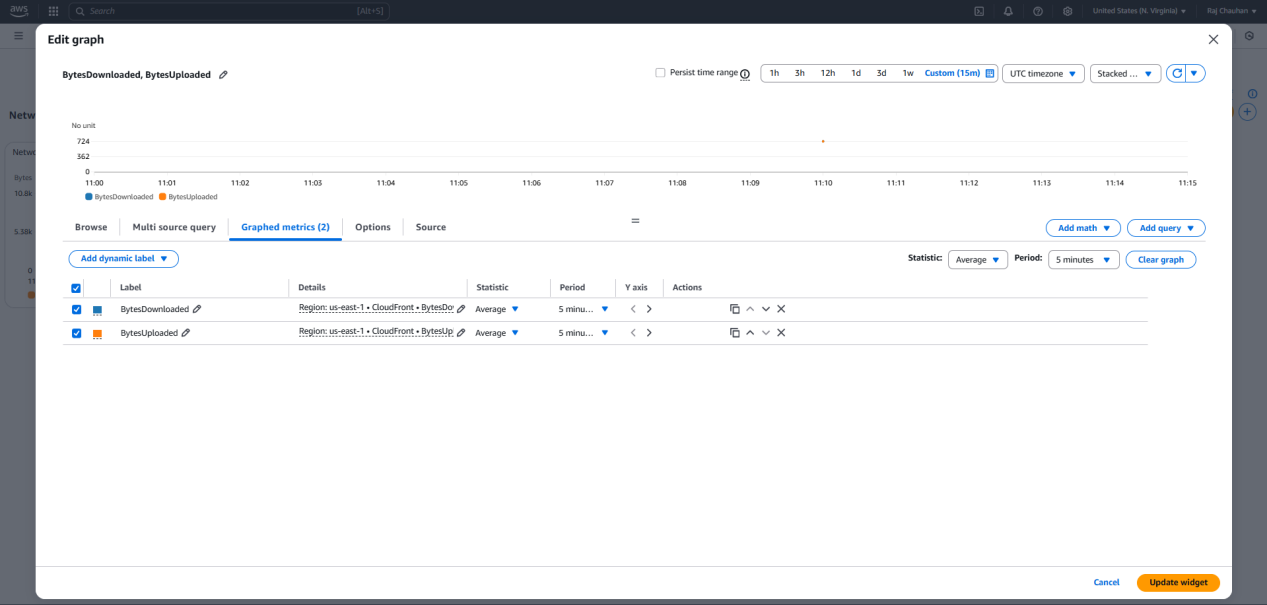
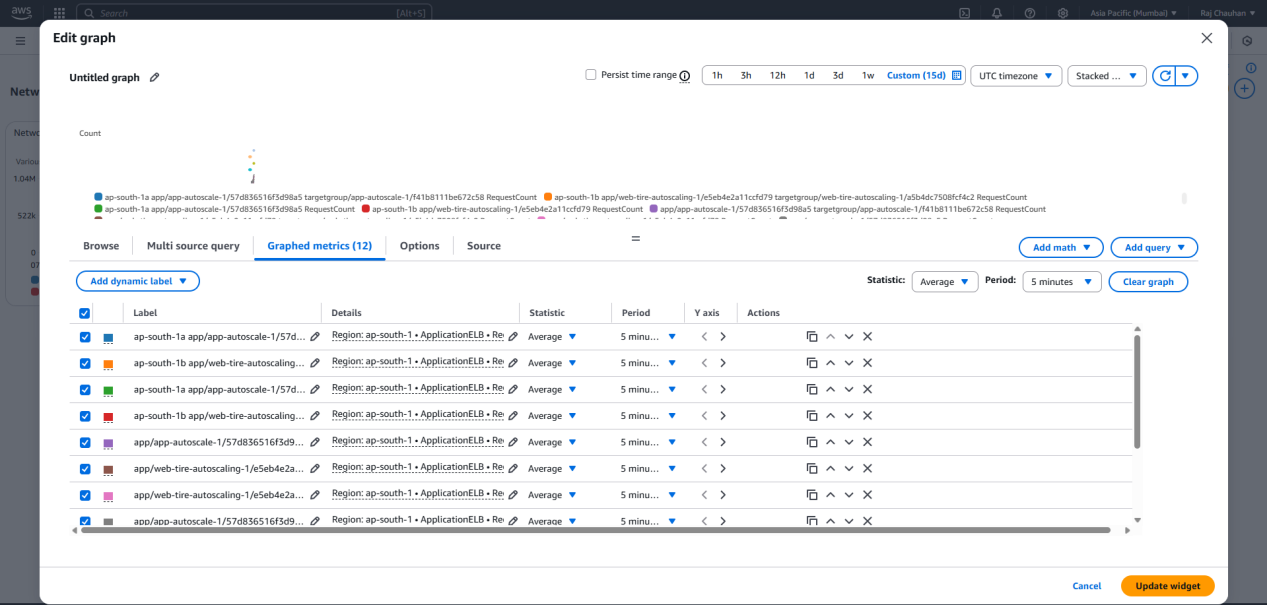
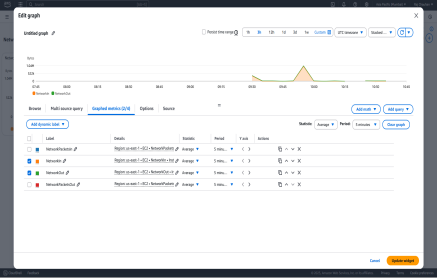
**Section 3: Network Performance Dashboard**

Go to CloudWatch → Dashboards → Create Dashboard → Network Performance Dashboard



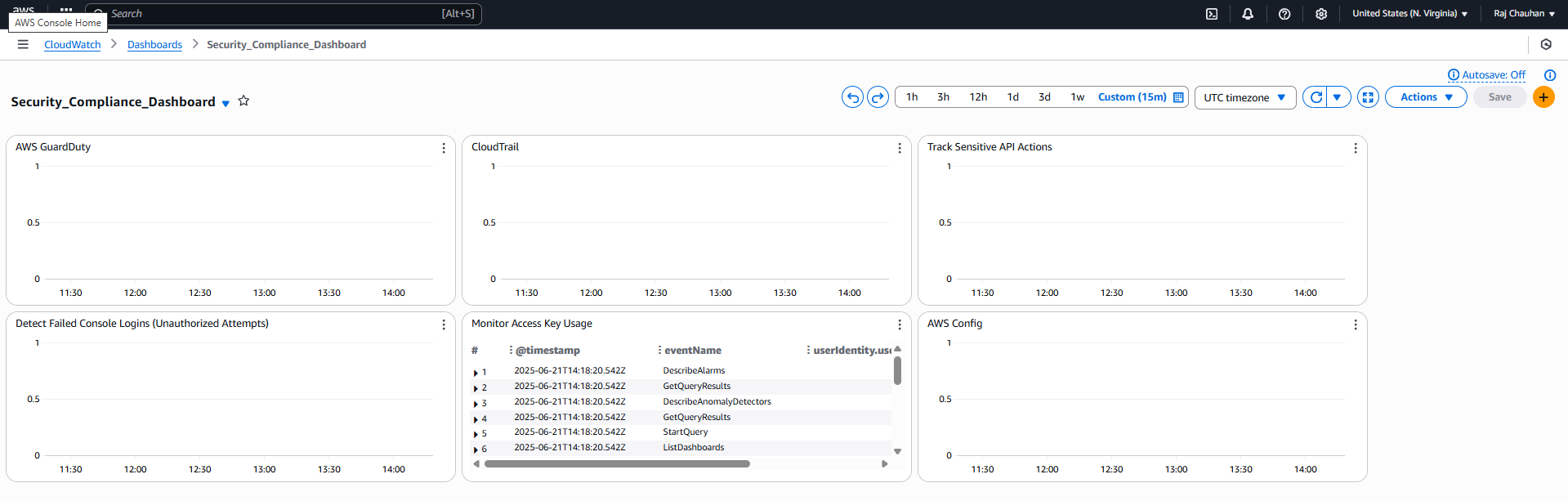
Click Add query and select:

EC2 → NetworkIn, NetworkOut ELB → HTTPCode\_ELB\_5XX\_Count, RequestCount, etc. CloudFront → BytesDownloaded, BytesUploaded



**Section 4: Security & Compliance Dashboard**

Go to CloudWatch → Dashboards → Create Dashboard → Security & Compliance Dashboard



Open AWS GuardDuty Console: Open AWS Config Console & go to Dashboard.

Note Summary section (total findings, resources, accounts). Enable Recording:

Capture trending widgets. If Config isn’t recording resources yet, click Set up or Settings.

Add Security Widgets to CloudWatch: Choose resource types, S3 delivery channel, and SNS for notifications.

Back in your Dashboard, + widget → choose text or CloudWatch Logs Insights for security events:

e.g. count of GuardDuty findings, CloudTrail failed logins, Access Key usage, Config rule violations. Monitor Compliance:

Dashboard shows compliance summary: compliant/non‑compliant Rules, Resources, and Findings.

Use Add query, selecting:

GuardDuty metrics (e.g. FindingCount)

CloudTrail events (FailedConsoleLogin)

Config rule compliance (NonCompliantResources)

Configure refresh interval and widget formatting to match others.

