



I didn't know Amazon CloudWatch could do that!



Joe Alioto
Sr. Solutions Architect
AWS CloudOps



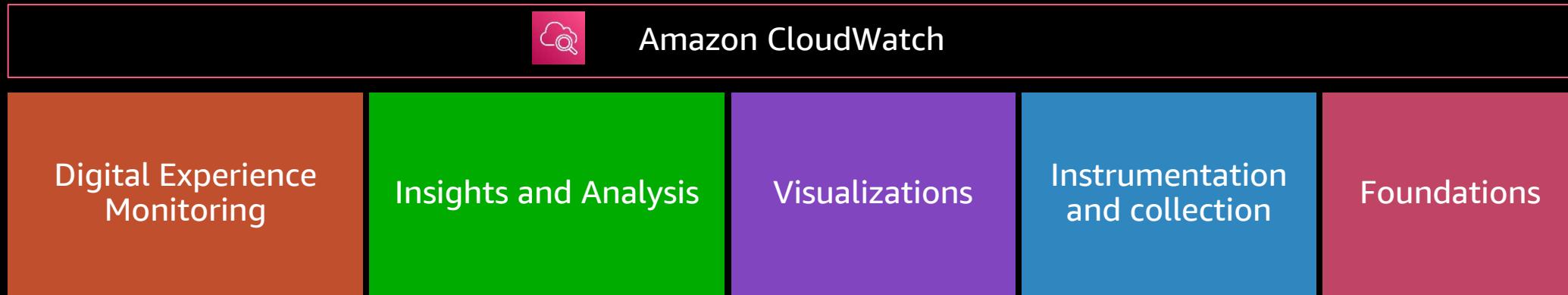
Agenda

Amazon CloudWatch and all the features! *(as many as I can show before I run out of breath)*

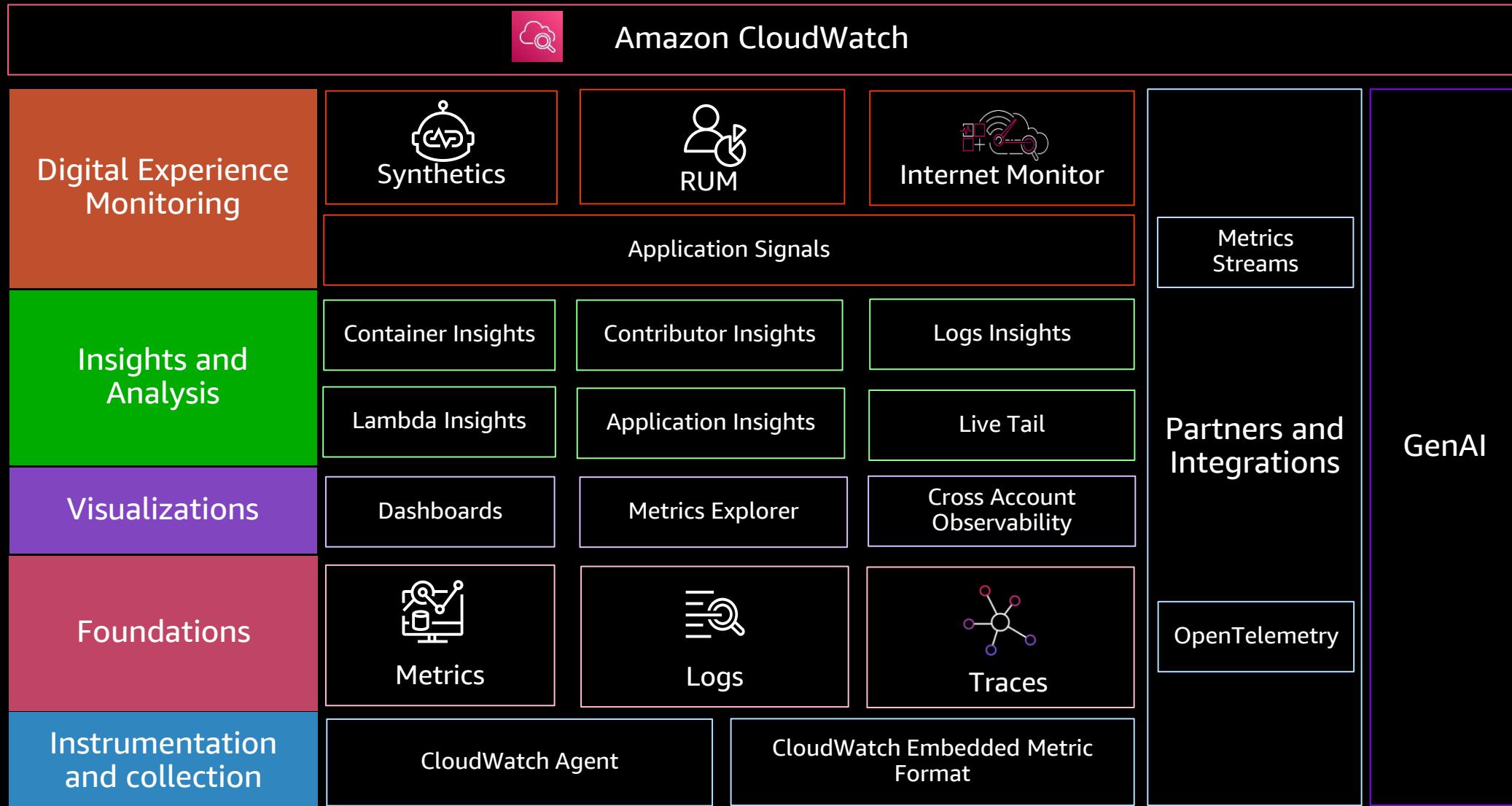
Resources



BREADTH AND DEPTH NATIVE OBSERVABILITY



BREADTH AND DEPTH NATIVE OBSERVABILITY



What areas?

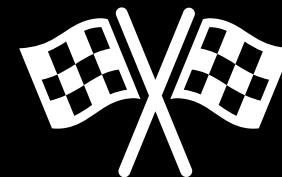
- Centralized Observability
- AIOps
- GenAI Observability
- Application Signals (APM)
- Insights
- Logs
- Metrics
- Traces
- CloudWatch Agent
- Alarms
- Dashboards
- Network
- OpenTelemetry



What areas?



- Centralized Observability
 - AIOps
 - GenAI Observability
- Application Signals (APM)
 - Insights
 - Logs
 - Metrics
 - Traces
 - CloudWatch Agent
 - Alarms
 - Dashboards
 - Network
 - OpenTelemetry





Feature

-
- Important points



Feature ←

-
- Important points



© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved. Amazon Confidential and Trademark.

Feature

-
- Important points ←



© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved. Amazon Confidential and Trademark.

https://url_that_points_to_documentation_same_as_qr_code

Feature

- Important points



© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved. Amazon Confidential and Trademark.

https://url_that_points_to_documentation_same_as_qr_code

Feature

- Important points



© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved. Amazon Confidential and Trademark.

https://url_that_points_to_documentation_same_as_qr_code



Centralized Observability



© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved. Amazon Confidential and Trademark.

CENTRALIZED OBSERVABILITY

Log centralization

- Cross-account & cross-region log centralization
- Region and account metadata added to logs and streams
- First copy is **FREE**
- Other copies are \$0.05/GB



© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved. Amazon Confidential and Trademark.

CloudWatch > Settings

CloudWatch settings

Account Organization

Global Dashboards Logs X-Ray traces - new Metrics data sources - new

Use a centralized monitoring account to monitor and troubleshoot applications seamlessly across multiple accounts - new Info

View metrics, logs, traces, Application Insights applications, Internet Monitor monitors, and Application Signals with no account boundaries. Watch video guideline

1. Configure monitoring account

2. Determine how to link source accounts

3. Link your source accounts via CloudFormation or by the sharing URL

4. Browse cross-account data with the monitoring account

Monitoring account configuration

Allow this account to view data from your source accounts.

To get started, sign in to the account that you want to use as a monitoring account.

Tip: We recommend that you create a new account in your organization to use as the monitoring account.

When you are signed in to the monitoring account, choose **Configure** to get started.

Or

Source account configuration

To configure a source account, sign in to that account and use the CloudFormation template or the URL that you get from the monitoring account.

You can also choose to share one or more of the following with the monitoring account: Metrics, logs, traces, Application Insights applications, Internet Monitor monitors, and Application Signals.

Enable account switching Info

View metrics, dashboards, logs widgets, and alarms in another account, or allow another account to view your data with no log in/out needed.

Not enabled

Configure

This can be done by the monitoring account only.

Not linked

Configure

This can be done by the source account only.

Log centralization

- Cross-account & cross-region log centralization
- Region and account metadata added to logs and streams
- First copy is **FREE**
- Other copies are \$0.05/GB

The screenshot shows the AWS CloudWatch Log Groups interface. At the top, it displays the path `/database/production/queries`. Below this, the **Log group details** section provides information such as Log class (Info), ARN (arn:aws:logs:us-east-1:084...:log-group:/database/production/queries:*), Creation time (23 hours ago), Retention (Never expire), and Stored bytes (3.12 KB). To the right, sections for Metric filters (0), Subscription filters (0), Contributor Insights rules (-), KMS key ID, Anomaly detection (Configure), Data protection (On), Sensitive data count (0), Custom field indexes (Configure), and Transformer (Configure) are shown.

Below the details, a navigation bar includes tabs for Log streams, Tags, Anomaly detection, Metric filters, Subscription filters, Contributor Insights, Data protection, Field indexes, and Transformer. The **Log streams** tab is selected, displaying a list titled "Log streams (2)". The list includes two entries: "dev-db-server-01_975" and "prod-db-server-01". Each entry has a checkbox, a timestamp (2025-09-17 06:00:35 (UTC) and 2025-09-17 06:00:17 (UTC)), and a "Source Region" label (7-us-west-2). Orange arrows point from the text "Source Account" and "Source Region" to the respective columns in the log stream table.



CENTRALIZED OBSERVABILITY

Cross-account observability

- Cross-account log, metrics, traces, application signals services and SLOs, Application Insights, Internet Monitor
- Federated Access (read-only) from the source accounts
- Send all or filter logs and metrics



© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved. Amazon Confidential and Trademark.

CloudWatch

Favorites and recents

Dashboards

▶ AI Operations [New](#)

▶ Alarms ⚠ 4 ○ 45 ○ 5

▶ Logs ⚠

▶ Metrics [New](#)

▼ Application Signals (APM)

Services

Application Map [New](#)

Transaction Search

Service Level Objectives (SLO)

Synthetics Canaries

RUM

Traces

Trace Map

▶ GenAI Observability [New](#)

▶ Network Monitoring

▶ Insights

Settings

Telemetry config

Getting Started

What's new

CloudWatch settings

Account Organization

Global Dashboards Logs X-Ray traces - new Metrics data sources - new Application signals - new

Use a centralized monitoring account to monitor and troubleshoot applications seamlessly across multiple accounts - new [Info](#)
View metrics, logs, traces, Application Insights applications, Internet Monitor monitors, and Application Signals with no account boundaries. [Watch video guideline](#)

1. Configure monitoring account

2. Determine how to link source accounts

3. Link your source accounts via CloudFormation or by the sharing URL

4. Browse cross-account data with the monitoring account

Monitoring account configuration
Allow this account to view data from your source accounts.
To get started, sign in to the account that you want to use as a monitoring account.
Tip: We recommend that you create a new account in your organization to use as the monitoring account.

When you are signed in to the monitoring account, choose **Configure** to get started.

Or

Source account configuration
To configure a source account, sign in to that account and use the CloudFormation template or the URL that you get from the monitoring account.
You can also choose to share one or more of the following with the monitoring account: Metrics, logs, traces, Application Insights applications, Internet Monitor monitors, and Application Signals.

Enable account switching [Info](#)
View metrics, dashboards, logs widgets, and alarms in another account, or allow another account to view your data with no log in/out needed.

Share your CloudWatch data
Create the CloudWatch-CrossAccountSharingRole IAM role to share your CloudWatch metrics, dashboards, logs widgets, and alarms. You can manage this role later in IAM.

Share your Organization account list
Populate the account dropdown selector so that users can easily switch between accounts.

View cross-account cross-region
This will allow you to easily switch views between accounts (that have granted you permission to their data), without the need to authenticate, using a selector in the console.

Enable resource tags on telemetry - new
Add AWS resource tags to your telemetry data to create detailed monitoring dashboards and simplify troubleshooting workflows.

When you enable resource tags for telemetry, you can:

- Filter and group metrics by resource tags
- Create alarms using tag-based Metrics Insights queries

Note: changes may take up to 3 hours to appear in the console. [Learn more](#)

AI Operations



© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved. Amazon Confidential and Trademark.

CloudWatch Investigations

- Agentic AI incident management assistant and Post Incident Reports
- Telemetry must be in CloudWatch for best results
- Recommends remediation steps and SSM Automation runbooks

Console Home > CloudWatch > AI Operations: Investigations

Show me how

CloudWatch

Favorites and recents

Dashboards

AI Operations New

- Overview
- Investigations
- Configuration
- Alarms ⚠️ 4 ○ 47 ⊖ 6
- Logs ⚠️
- Metrics New
- Application Signals (APM) New
- GenAI Observability New
- Network Monitoring
- Insights

Settings

Telemetry config

Getting Started

What's new

Try it out with one of your own alarms

We have found alarms in the alarm state that you can start an investigation with.

Dev_Retail_DB_Writer-HighLoad

No unit
3.00
2.50
2.00 2 Oct 20 03:00 Oct 20 04:00 Oct 20 05:00

DBLoadRelativeToNumVCpus

Prod_Retail_DB_Reader-HighLoad

No unit
3.00
2.50
2.00 2 Oct 20 03:00 Oct 20 04:00 Oct 20 05:00

DBLoadRelativeToNumVCpus

Investigations (5) Info

Filter by title Investigation state Any

Title	Investigation state	Last modified
intermittent faults on my ordering-service	Archived	6 days ago
my ordering-service is receiving faults for dy...	Archived	1 month ago
what is causing my ordering-service to not m...	Archived	1 month ago
ordering-service is showing 80 percent fault r...	Archived	1 month ago
ordering-service has a 20 percent failure rate	Archived	1 month ago



Log Insights Query Generation

- Use natural language in Logs Insights to generate Logs Insights query language, OpenSearch SQL, or OpenSearch PPL queries

The screenshot shows the AWS CloudWatch Logs Insights interface. On the left is a sidebar with navigation links like CloudWatch, Favorites and recents, Dashboards, AI Operations, Alarms, Logs (selected), Metrics, Application Signals, GenAI Observability, Network Monitoring, and Insights. Below these are Settings, Telemetry config, Getting Started, and What's new.

The main area has tabs for Logs Insights (selected) and Analyze with OpenSearch - new. It includes a "Logs Insights Info" section with a "Start tailing" button, time range controls (30m, 3h, 1h, Compare (Off), UTC timezone), and a "Select log groups by" dropdown. A "Selection criteria" section shows a selected log group: "aws-cloudtrail-logs-724772082388-d608d7e8" from the "Monitoring account 724772082388". A "Clear all" button is also present.

A code editor window displays a Log Insights query:

```

1 fields @timestamp, @message, @logStream, @log
2 | sort @timestamp desc
3 | limit 10000
  
```

Below the code editor are "Run query", "Cancel", "Save", and "History" buttons. A note states: "Logs Insights QL query can run for maximum of 60 minutes."

The "Logs (-)" tab is selected in the main panel, which shows a "Logs (-)" section with "Summarize results", "Investigate", "Export results", "Add to dashboard", and a "Data may cross Regions" note. It also displays "No results" and the message "Run a query to see related events".

On the right side, there are three vertical panels: "Discovered fields", "Saved and sample queries", and "Query commands".



Log Insights results summarization

- Summarize log results into human readable paragraph

CloudWatch > Logs Insights

Logs Insights Info
Select log groups, and then run a query or choose a sample query.

Logs Insights QL PPL SQL 30m 3h 1h Compare (Off) UTC timezone ▾

Select log groups by Selection criteria
Log group name Select up to 50 log groups ▾ Browse log groups
aws-cloudtrail-logs-724772082388-d608d7e8 X Monitoring account 724772082388

Query generator

Prompt | Info 42/500 X
get api count by eventSource and eventName

Generate new query Refine existing query Is this helpful? ⬤ ⬤

Run query Cancel Save History

Logs Insights QL query can run for maximum of 60 minutes.

Completed. Query executed for 1 log group. ⓘ

Logs (215) Patterns (-) Visualization

Logs (215) Summarize results Investigate Export results Add to dashboard ⚙

Data may cross Regions

Showing 215 of 14,178 records matched ⓘ
14,178 records (23.0 MB) scanned in 3.0s @ 4,727 records/s (7.7 MB/s) Hide histogram

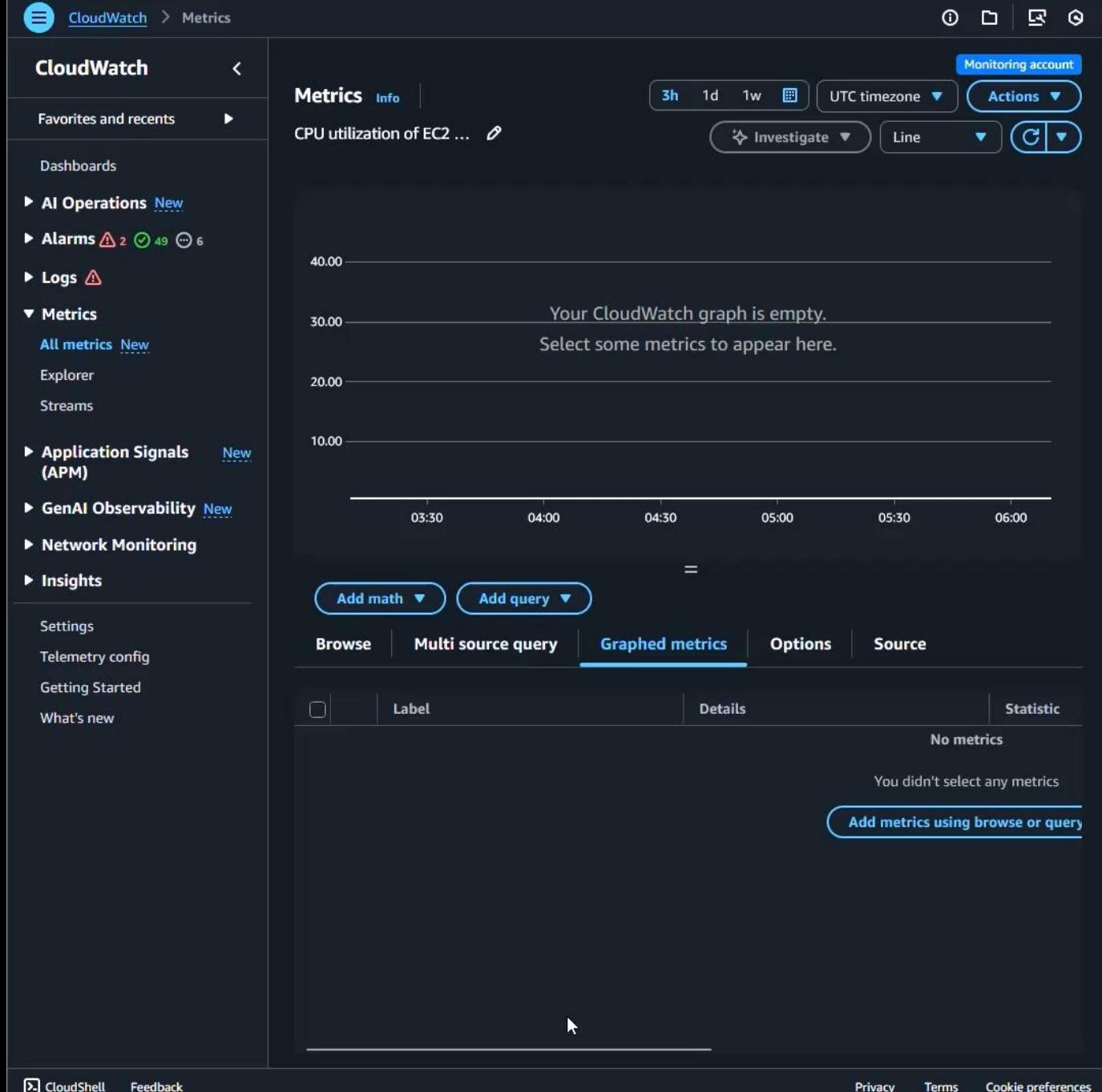
eventSource eventName apiCount

#	eventSource	eventName	apiCount
1	iam.amazonaws.com	GetInstance...	17
2	iam.amazonaws.com	GetRole	20
3	kms.amazonaws.com	GenerateDat...	3786
4	sts.amazonaws.com	AssumeRole	1666
5	elasticloadbalancing.ma...	DescribeTar...	247



Metrics query generator

- Generate metric queries using natural language



Anomaly Detection for logs

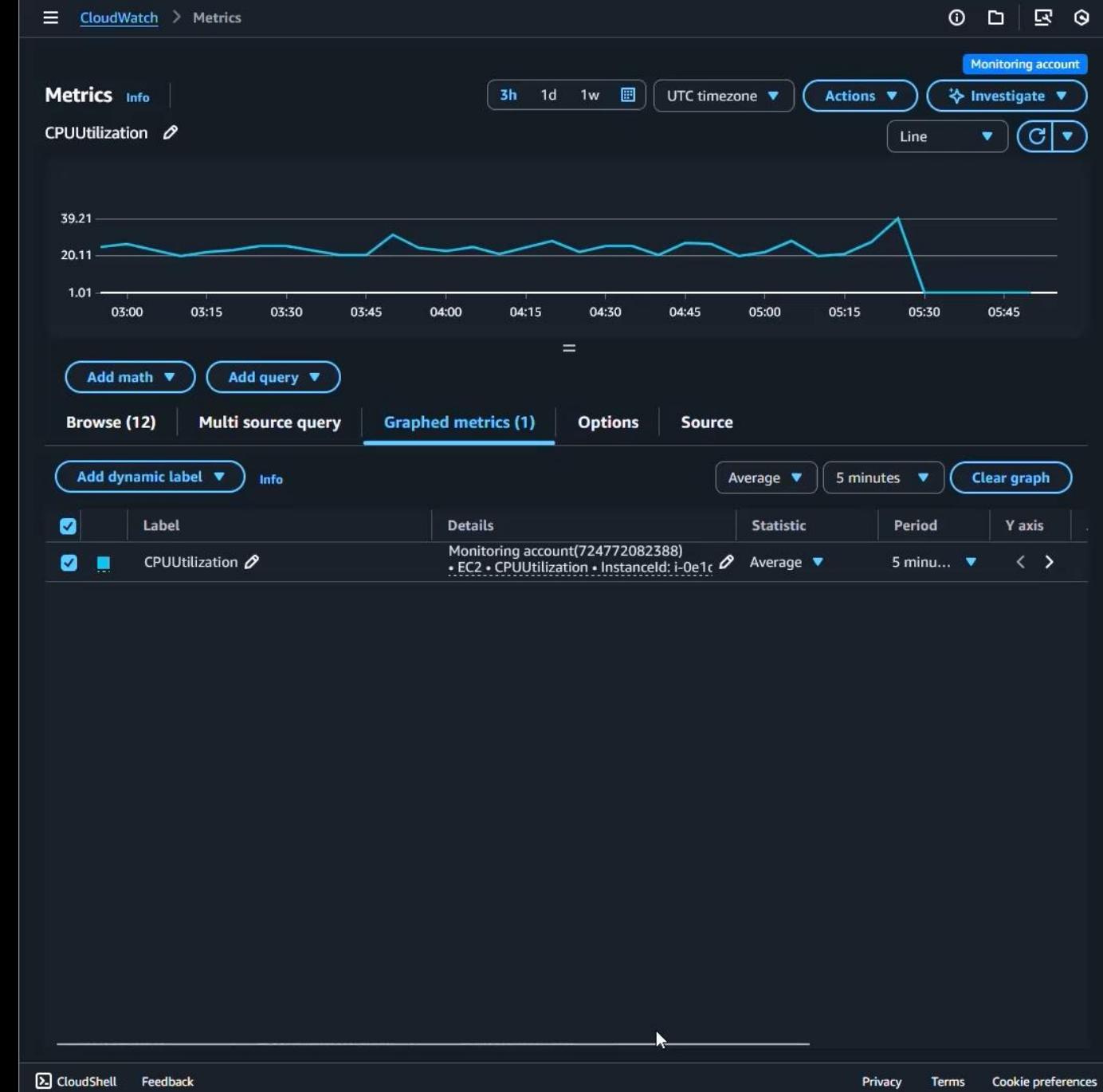
- Always on anomaly detection for log groups
- On-demand anomaly detection for Logs Insights queries using CWLI query language



The screenshot shows the AWS CloudWatch Log Anomalies interface. The left sidebar navigation includes CloudWatch, Favorites and recents, Dashboards, AI Operations (New), Alarms (with 2 alerts, 49 triggers, 6 suppressed), Logs (Log groups, Log Anomalies selected, Live Tail, Logs Insights, Contributor Insights), Metrics (New), Application Signals (APM) (New), GenAI Observability (New), Network Monitoring, and Insights. Sub-navigation for Log Anomalies includes Settings, Telemetry config, Getting Started, and What's new. The main content area displays 'Log anomalies (26) Info' with a message: 'The latest 50 anomalies are automatically updated every 1 minute'. It features a search bar ('Filter anomalies by priority level, patterns or key'), grouping options ('Group by: Time ▾', 'Anomalies | Suppressed'), and sorting by Priority and Log pattern. A 'Pattern inspect (No selection) Info' section is at the bottom. The top right corner shows 'Monitoring account' and other navigation icons.

Anomaly Detection for metrics

- anomaly detection for metrics
- Set thresholds to compare



Anomaly Detection for alarms

- Set thresholds for anomaly bands which are outside, greater than, lower than the band



CloudWatch > Alarms > Create alarm

Specify metric and conditions

Step 1: Specify metric and conditions

Step 2: Configure actions

Step 3: Add alarm details

Step 4: Preview and create

Metric

Graph

This alarm will trigger when the blue line goes above the red line for 1 datapoints within 5 minutes.

Percent

39.21

20.11

1.01

04:00 05:00 06:00

CPUUtilization

Namespace: AWS/EC2

Metric name: CPUUtilization

InstanceId: i-0e1ddc75220381b34

Instance name: db_access_server_prod

Statistic: Average

Period: 5 minutes

Conditions

Threshold type:

- Static: Use a value as a threshold
- Anomaly detection: Use a band as a threshold

Whenever CPUUtilization is...

Define the alarm condition.

- Greater > threshold
- Greater/Equal >= threshold
- Lower/Equal <= threshold
- Lower < threshold

than...

Define the threshold value.

10000

CloudShell Feedback

Privacy Terms Cookie preferences

MCP servers for your AI Agents

- MCP server for CloudWatch logs, metrics, alarms
- MCP server for Application Signals (APM) for Services, SLOs, traces, service metrics, and SLIs



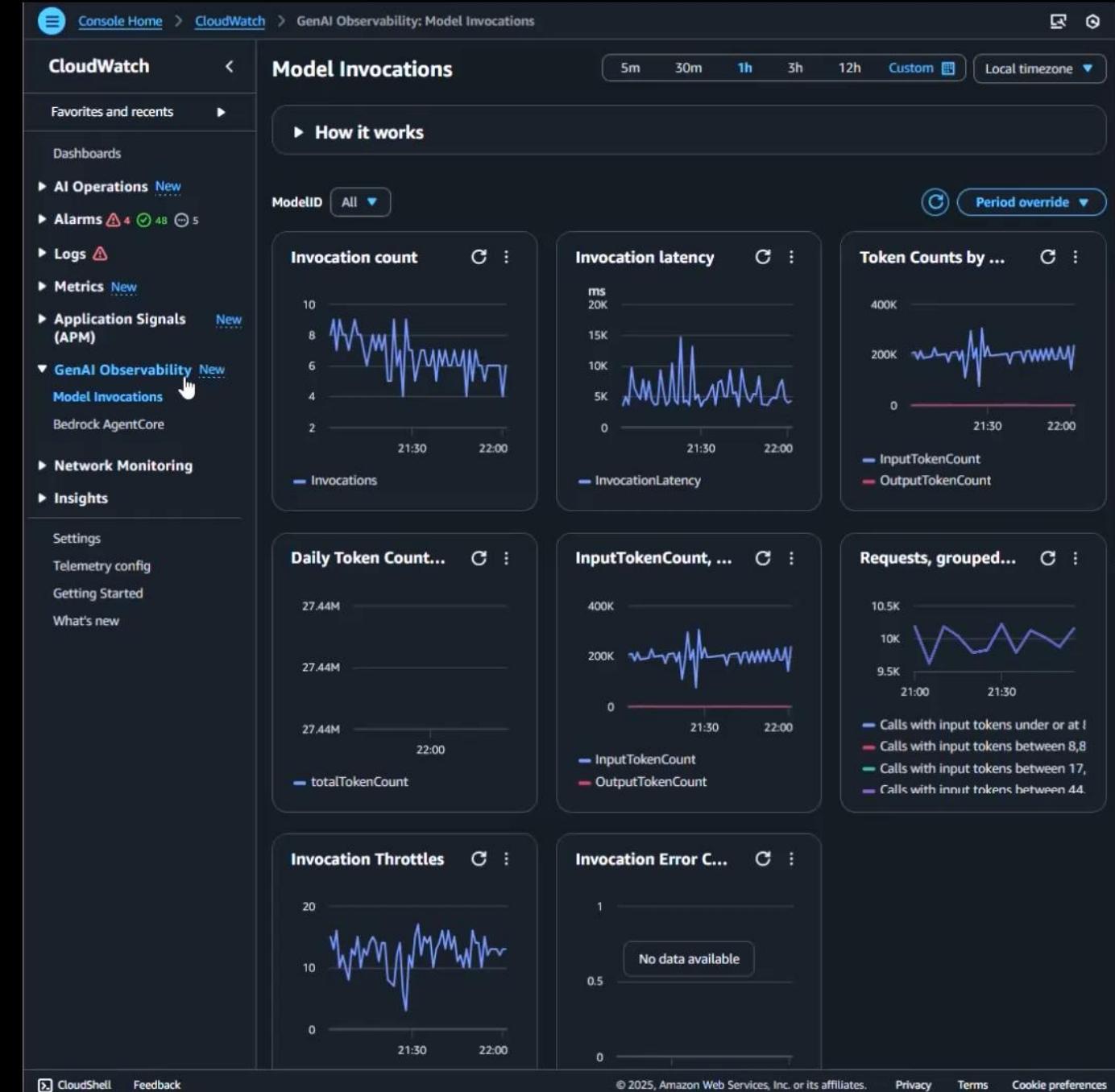
Gen AI Observability



© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved. Amazon Confidential and Trademark.

Observability for models and agents

- View model invocations across your entire account
- View Bedrock AgentCore Agents, Memory, Tools, Gateway, and Identity
- Collect Agent traces and metrics from any compute source



Application Signals (APM)



© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved. Amazon Confidential and Trademark.

APPLICATION SIGNALS (APM)

Services

- Monitor application health in real time
- Track performance against business goals
- View relationships between services and dependencies
- Quickly identify and resolve performance issues
- Instrument your applications with OpenTelemetry



© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved. Amazon Confidential and Trademark.

The screenshot shows the AWS CloudWatch Application Monitoring Services dashboard. At the top, there's a navigation bar with 'CloudWatch' and 'Services'. Below it is a sidebar with links like 'CloudWatch', 'Favorites and recents', 'Dashboards', and 'Application Signals (APM)'. The main area has sections for 'Group and filter', 'Services by SLI status' (a donut chart showing 5 healthy, 5 unhealthy, 0 recovered, 20 no SLO, and 0 insufficient data), 'Top services by fault rate' (listing retail-service-r... at 54.74%, retail_service... at 51.05%, PetSite at 26.25%, PetSite at 9.4%, and ordering-service at 3.56%), 'Top dependency paths by fault rate' (listing various paths with 100% fault rate), and a 'Services (30)' table with columns for Name, SLI status, Service Availability, Environment, and Account. The 'ordering-service' row in the table is highlighted with a blue border.

Name	SLI status	Service Availability	Environment	Account
ordering-service	⚠️ 1/3 Unhealthy	96.8%	lambda:de...	Mon
PetSite	⚠️ 1/2 Unhealthy	73.8%	ec2:default	Mon
retail_service_dev	⚠️ 1/2 Unhealthy	100%	lambda:de...	Mon
retail_service	⚠️ 1/2 Unhealthy	100%	lambda:de...	Mon
retail-service-rest1	⚠️ 1/1 Unhealthy	45.3%	api-gateway...	Mon
pet-clinic-frontend-java	🟢 5 Healthy	97.8%	eks:app-si...	Mon
MyLambdaFunction	🟢 1 Healthy	100%	lambda:de...	Jalio
billing-service-python	🟢 1 Healthy	100%	eks:app-si...	Mon
ordering-service	🟢 1 Healthy	96.4%	api-gateway...	Mon

Application Map

- View connections between client, canary, service, and dependency nodes
- See which services are meeting or not meeting your service level objectives (SLOs).
- Group and filter services to create customized views



Last updated 3 minutes ago [Monitoring account](#)

Application Map [Info](#) View data for: Monitoring account ▾ 1h 12h 3h [UTC timezone](#) ▾ [C](#) [E](#)

Search and filter Select saved view Save view

Group and filter X Visualize groups of resources and filter for attributes

▼ Group by [Manage groups](#)

Related services

retail-service-rest1 Application SLI breach Requests 1.0k Services 2 View insights

ordering-service Application SLI breach Requests 3.0k Services 2 View insights

pet-clinic-frontend-jav... Application Requests 117.0k Services 7 View insights

strands_agentcore.DEF... Application Requests 472 Services 1 View insights

petis Application Requests 1.0k Service 1

CloudShell Feedback Privacy Terms Cookie preferences

APPLICATION SIGNALS (APM)

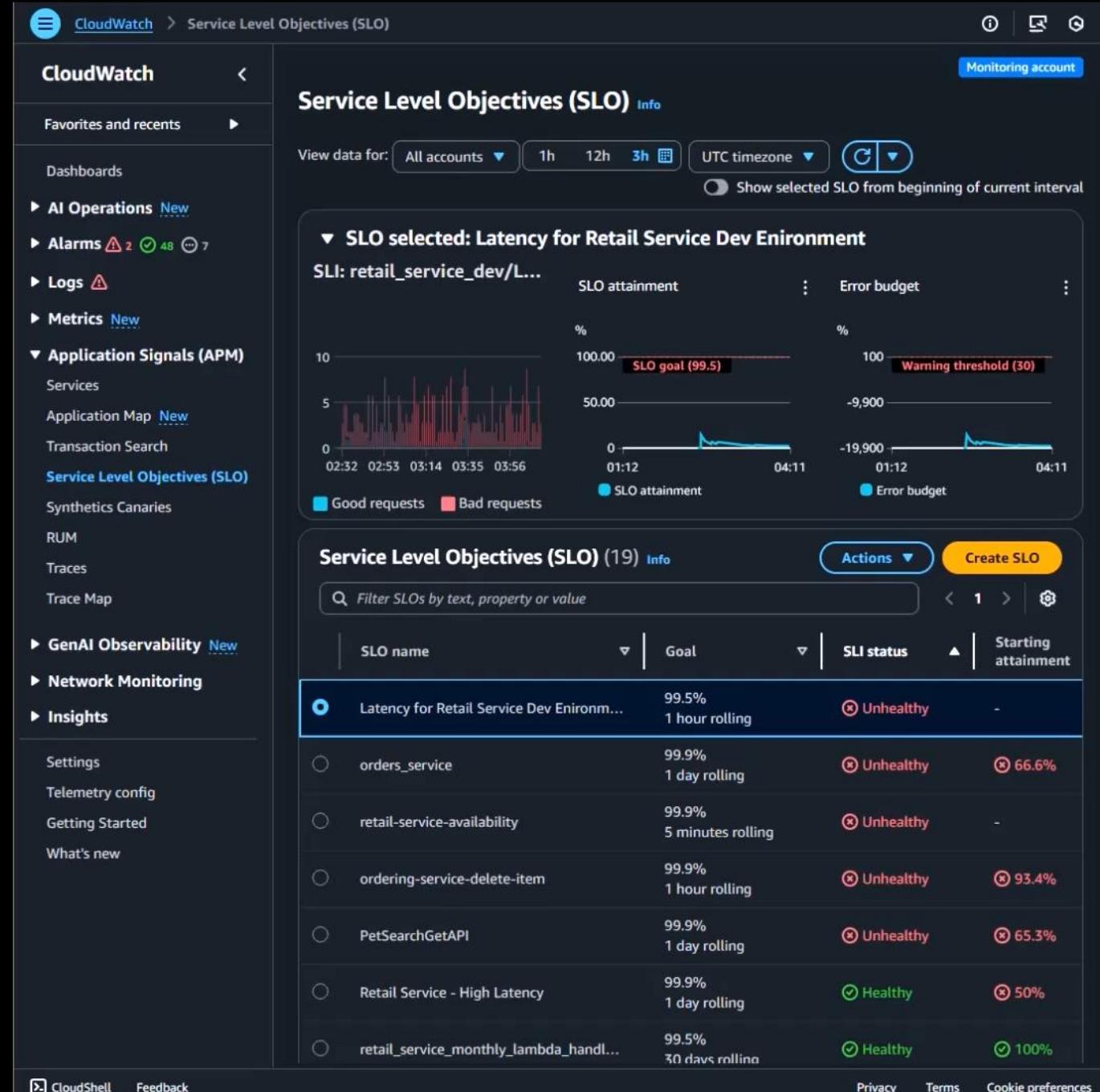
Service Level Objectives

- Define and alarm on Latency or availability for your services or their dependencies
 - Be warned before breaching SLO thresholds
 - Get notified as your SLOs are starting to burn down your error budget



The AWS logo consists of the lowercase letters "aws" in a white sans-serif font, with a thick black curved arrow underneath pointing from left to right.

© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved. Amazon Confidential and Trademarks



Synthetic canaries (layer 7)

- monitor your endpoints, APIs and Visual UI using same routes and actions as a customer with up to 10 checks per canary  NEW
- Review the traces, HAR file, and screenshots for each synthetic run
- Record using a chrome extension to easily create new canaries



Last updated: 9:16 PM.

Synthetics Overview Info

Status
The status distribution of currently running canaries

Canary runs
Each data point is an aggregate of runs for a single canary. Hover for details. Click and drag plot area to zoom.

Canaries (19)

Name	Last Run Status	Success %	Alarms	Avg. du...	State
pc-visit-vet	Passed	100%	-	3s	Running
pc-visit-pet	Failed	0%	-	34.5s	Running
pc-visit-insuran	Passed	100%	-	3s	Running
pc-visit-billings	Passed	100%	-	3s	Running
ordering-service	Passed	88%	-	2.9s	Running
pc-create-owner	Failed	0%	-	52.1s	Running
order-service	Failed	84%	-	3.2s	Running
pc-add-visit	Failed	0%	-	34.4s	Running
my_web_server	No data	0%	-	0ms	Stopped
pet-clinic-traffic	No data	0%	-	0ms	Stopped

APPLICATION SIGNALS (APM)

RUM

- collect and view client-side data about your web application performance from actual user sessions in near real time
- Add additional meta-data such as host info to easily identify nodes with issues.



© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved. Amazon Confidential and Trademark.

CloudWatch > RUM

RUM overview

CloudWatch

Favorites and recents

Dashboards

AI Operations New

Alarms 2 49 6

Logs

Metrics New

Application Signals (APM)

Services

Application Map New

Transaction Search

Service Level Objectives (SLO)

Synthetics Canaries

RUM

Traces

Trace Map

GenAI Observability New

Network Monitoring

Insights

Settings

Telemetry config

Getting Started

What's new

Download PDF report

Actions

Add app monitor

Filter by selecting or typing attributes and values (ex. "browserName=Chrome")

Select a filter

3h 1d 1M Local timezone

Overview List view

View by app monitor MyRUMApp Last update 2 minutes ago

Page loads 29

Average page load speed 1.1K ms

Apdex score 0.90/1.00

Alarms No active alarms

Page loads and load time

Page loads 32

Load time 1.1k ms

21:00

Page loads (29) Load time (1.1K ms)

View page loads

Apdex by country

Positive (0 ms - 2K ms)

Tolerable (2K ms - 8K ms)

Frustrating (8K ms +)

View locations

Sessions with errors

4.8

0 21:00

No errors (3 sessions) Errors (1 session)

View errors

Errors by device

Desktop - 3 (100%)

Mobile - 0 (0%)

View errors

Sessions

4.8

0 21:00

Session starts

View sessions

Canaries

Monitor web applications using modular, light-weight canary tests. Tag your canaries with this

The screenshot shows the AWS CloudWatch RUM Overview dashboard for the application 'MyRUMApp'. The top navigation bar includes links for 'Download PDF report', 'Actions', and 'Add app monitor'. Below the navigation is a search bar and a 'Select a filter' dropdown. The main area features several cards: 'Page loads' (29), 'Average page load speed' (1.1K ms), 'Apdex score' (0.90/1.00), and 'Alarms' (No active alarms). The 'Page loads and load time' card displays a chart with 32 page loads, a peak load time of 1.1k ms at 21:00, and a legend for Page loads (29) and Load time (1.1K ms). The 'Apdex by country' card shows a world map with color-coded regions for Positive, Tolerable, and Frustrating performance. The 'Sessions with errors' card shows a bar chart with 4.8 sessions, 0 errors, and 21:00. The 'Errors by device' card shows a pie chart with 100% Desktop errors and 0% Mobile errors. The 'Sessions' card shows a bar chart with 4.8 sessions, 0 errors, and 21:00. The 'Canaries' card has a descriptive text about monitoring with canaries. A QR code and the AWS logo are at the bottom left, and a copyright notice is at the bottom center.



Insights



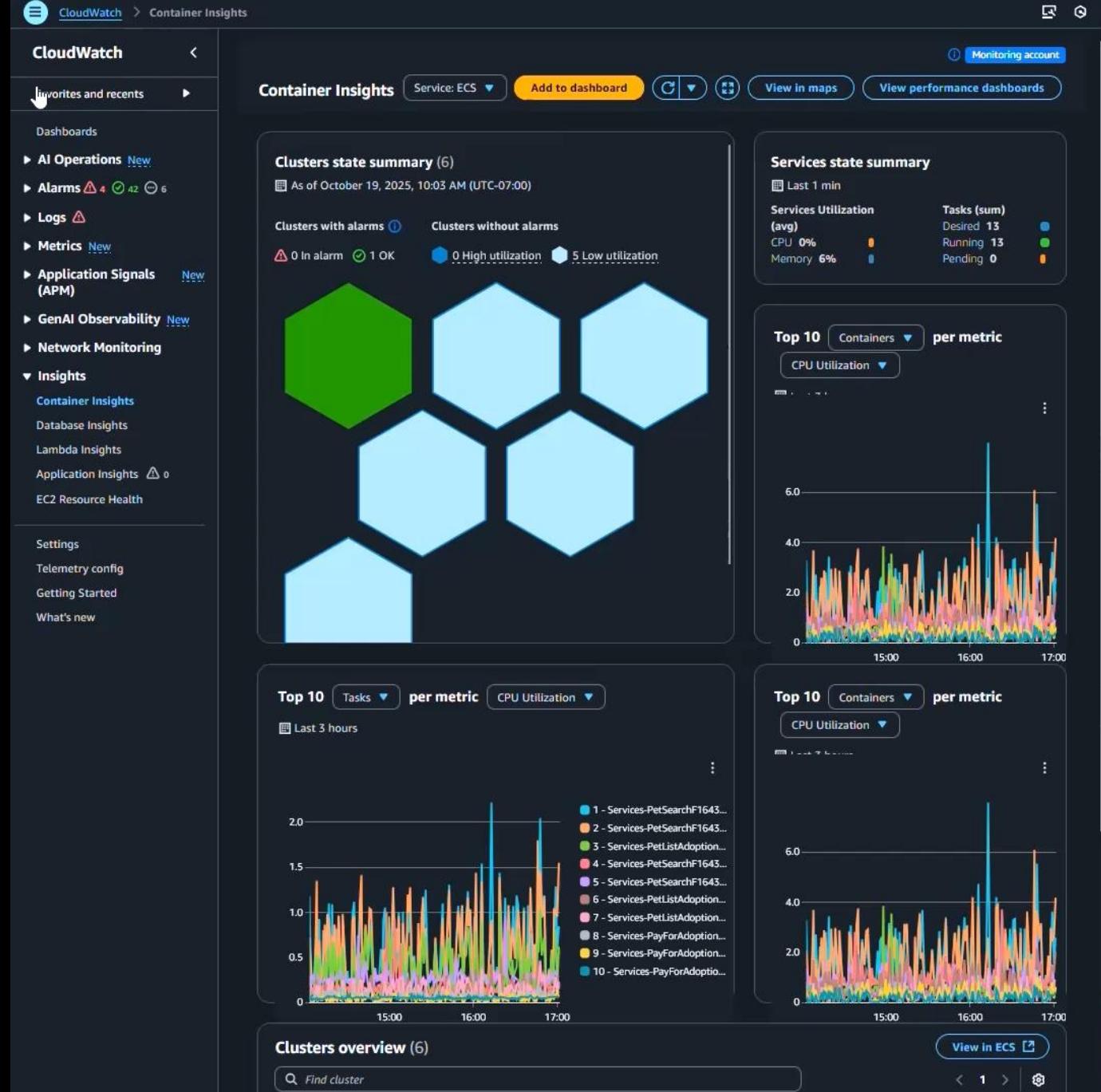
© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved. Amazon Confidential and Trademark.

Container Insights

- collect, aggregate, and summarize metrics and logs from your containerized applications and microservices
- View relationships for container resources
- Automatic Dashboards



© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved. Amazon Confidential and Trademark.



Database Insights

- Monitor and troubleshoot your fleet of RDS and Aurora instances
- View related services with Calling Services integration
- Quickly analyze execution plans and locking scenarios with no code



© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved. Amazon Confidential and Trademark.

CloudWatch > Database Insights

30m 1h 3h 12h Custom Local timezone C ⌂ ⌃ ⌚

Database Insights

Fleet Health Dashboard

Instances state summary (8)

Alarms Avg DB Load Max DB Load

Showing the state summary of instances in this fleet based on Alarms or DB Load Utilization.
As of 10/19/2025, 9:47:35 AM

Utilization:
2 High 0 Warning 6 Ok 0 Idle

Top 10 instances per DB Load Utilization

Ratio of the DB load to the number of virtual CPUs (percentage).

retail-prod-instance-1-us-east-1a

Top queries contributing to DB load

SELECT * FROM ...	66.34%
SELECT * FROM ...	33.2%
SELECT * FROM ...	0.46%

Top wait events

Client:ClientWrite	96.3%
CPU	3.11%
IO:DataFileRead	0.55%

Events (6)

Showing the RDS events for top 10 instances by highest DB load

Critical severity	0	High severity	0
Medium severity	0	Low severity	6

Calling services (1)

Showing the calling services for the top 10 instances by highest DB load.

Find services

Calling service: postgresql

Dependency: postgresql

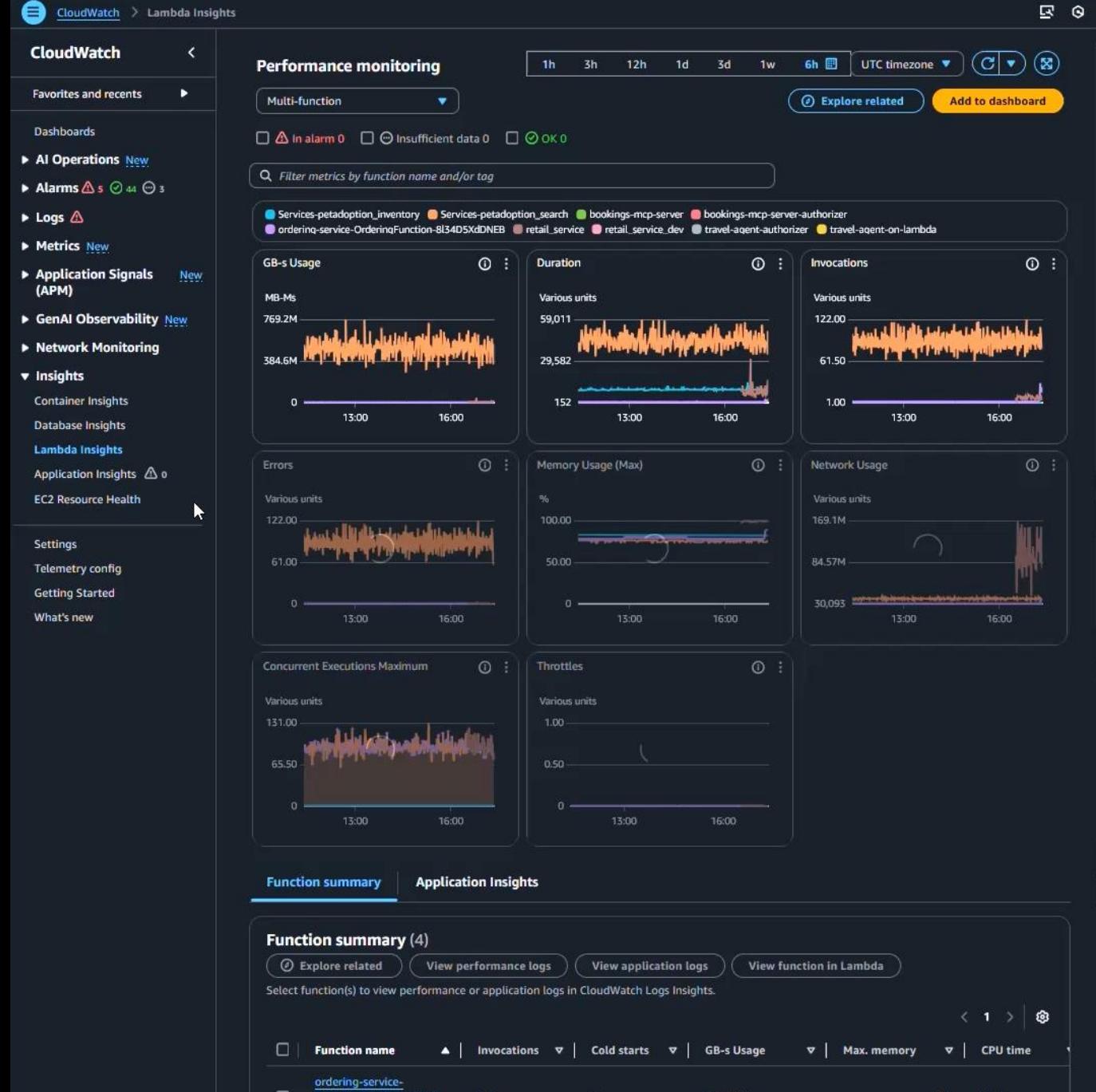
CloudWatch Database Insights screenshot showing the Fleet Health Dashboard, Instances state summary, Top 10 instances per DB Load Utilization, and detailed views for specific instances like retail-prod-instance-1-us-east-1a, including top queries, top wait events, and event logs. The interface also includes filters, saved fleets, and a QR code for quick access.

Lambda Insights

- Service and function level views for common metrics, cold starts, and diagnostic information
- Easily identify cold vs warm starts, init duration, memory, CPU time, Invoke cost (GB-s)
- Review past invocations issues quickly with direct traces mapping



© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved. Amazon Confidential and Trademark.



Application Insights

- Setup Application using Resource groups
- analyzes logs, metric patterns using historical data to detect anomalies, and continuously detects errors
- automatically creates dashboards that show the relevant observations



CloudWatch > Application Insights

CloudWatch

Favorites and recents

Dashboards

- ▶ AI Operations New
- ▶ Alarms 1 50+ 3
- ▶ Logs ⚠
- ▶ Metrics New
- ▶ Application Signals (APM) New
- ▶ GenAI Observability New
- ▶ Network Monitoring
- ▼ Insights
 - Container Insights
 - Database Insights
 - Lambda Insights
 - Application Insights** ⚠ 0
 - EC2 Resource Health
- Settings
- Telemetry config
- Getting Started
- What's new

Improved problem notifications with CloudWatch Application Insights
Application Insights has a new SNS notification channel to give you detailed alerts on your application problems. With these new alerts, you can respond quickly and effectively to application problems.

Automated monitoring of new resources
New resources added to this account for applications with the SSM agent installed will be automatically monitored going forward. You can disable the automatic addition of resources for monitoring by updating your configuration settings. [Learn more](#)

Application Insights Info

Add an application

Overview **Applications**

Problems detected (2)

View Ignored Problems Actions View problem detected dashboard

Problem summary	Status	Severity	Source	Start
StateMachine: Execution(s) failed	Recovering	Medium	StepFnStateMachine76D362E8...	2025-
ALB: Backend 5XX errors	Recovering	High	Servic-searc-Wr7bIRgWPz2L	2025-

Detected problems summary Info
Last 30 days

65 Problems

Resolved Unresolved

Top recurrent problems

- StateMachine: Execution(s) failed
- ALB: Backend 5XX errors

Monitored assets (99) Info

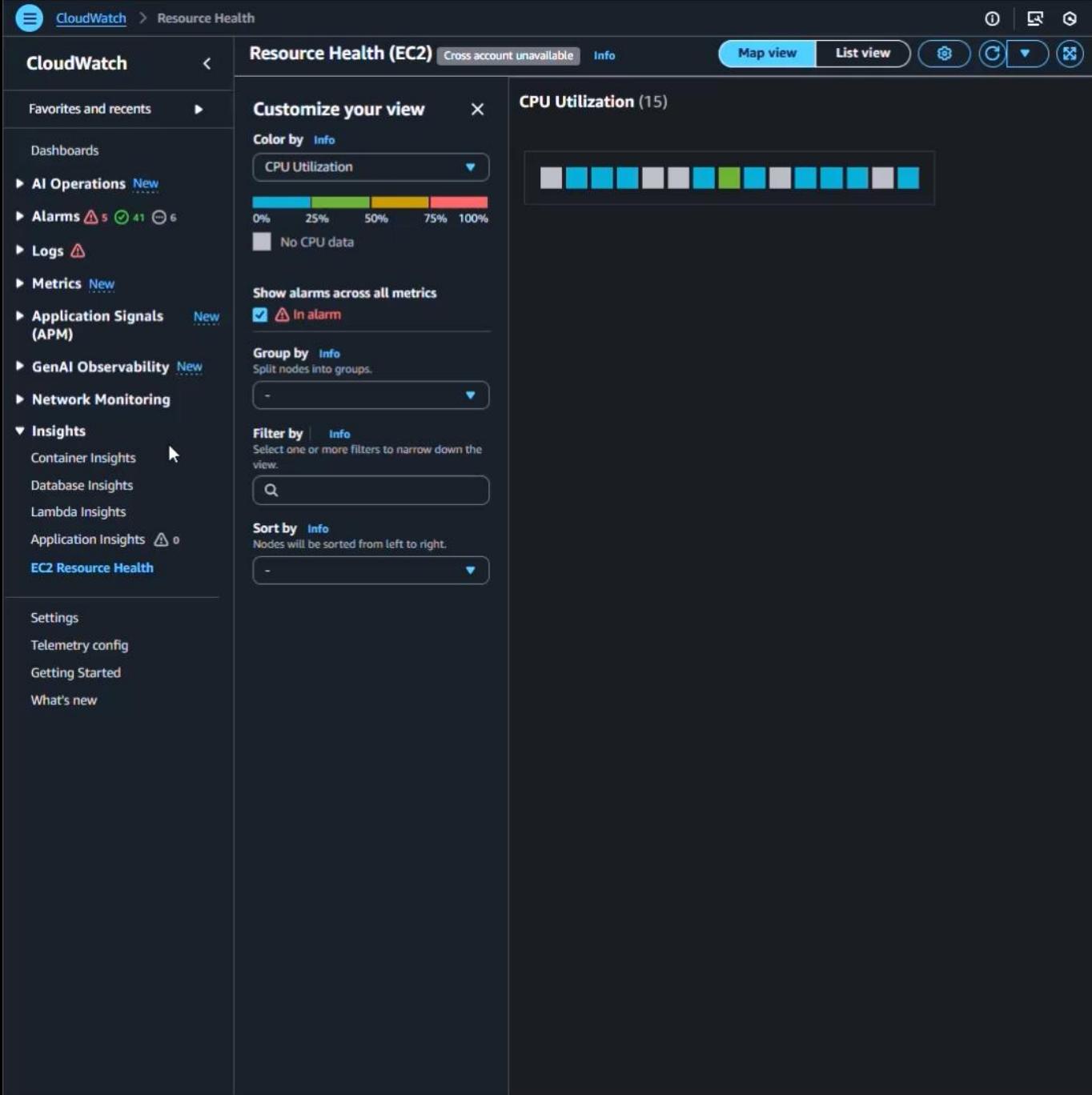
Applications

Metrics

Telemetry (341) Info

EC2 Resource Health

- automatically discover, manage, and visualize the health and performance of EC2 hosts by CPU Utilization or Memory
- Group and filter by tags or resource properties
- Customize threshold values/colors





Logs



© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved. Amazon Confidential and Trademark.

Log Classes

- Standard logs come all the Log Group features
- Infrequent access logs come with limited functionality at half the price
- Weigh your use case to identify which log class fits your needs



Feature	Standard \$0.50/GB	Infrequent Access \$0.25/GB
Fully managed log ingestion and storage	Yes ✓	Yes ✓
Cross-account features	Yes ✓	Yes ✓
Encryption with AWS KMS	Yes ✓	Yes ✓
CloudWatch Logs Insights query commands	Yes ✓	<u>Yes ✓ (Most commands– see Logs Insights QL commands supported in log classes.)</u>
CloudWatch Logs Insights discovered fields	Yes ✓	Yes ✓
Using OpenSearch PPL or OpenSearch SQL to query in CloudWatch Logs Insights;	Yes ✓	No
Natural language query assist	Yes ✓	No
CloudWatch Logs Anomaly Detection	Yes ✓	No
Live Tail	Yes ✓	No
Field indexing	Yes ✓	No
Compare to previous time range	Yes ✓	No
Subscription filters	Yes ✓	No
Export to Amazon S3	Yes ✓	No
GetLogEvents and FilterLogEvents API operations	Yes ✓	Not supported. Use CloudWatch Logs Insights to view log events stored in log groups in the Infrequent Access log class.
Metric filters	Yes ✓	No
Container Insights log ingestion	Yes ✓	No
Lambda Insights log ingestion	Yes ✓	No
Sensitive data protection with masking	Yes ✓	No
Embedded metrics format	Yes ✓	No

Log Group Field Indexes

- efficient equality-based searches
- Included with Standard log class
- Log Group or Account level index
- Allows for optimizing Logs Insights queries for less logs and faster results



CloudWatch > Log groups > /httpd/access_log

CloudWatch <

Favorites and recents ▶

Dashboards

▶ AI Operations New

▶ Alarms ⚠ 5 ⓘ 44 ⓘ 3

▼ Logs

Log groups (selected)

Log Anomalies

Live Tail

Logs Insights

Contributor Insights

▶ Metrics New

▶ Application Signals (APM) New

▶ GenAI Observability New

▶ Network Monitoring

▶ Insights

Settings

Telemetry config

Getting Started

What's new

/httpd/access_log

Actions ▾ View in Logs Insights Start tailing Search log group

Log group details

Log class | Info Standard Metric filters 1 Data protection -

ARN ⓘ arn:aws:logs:us-east-1:724772082388:log-group:/httpd/access_log:* Subscription filters 0 Sensitive data count -

Creation time 6 months ago Contributor Insights rules - Custom field indexes 5

Retention Never expire KMS key ID - Transformer ⓘ On

Stored bytes 73.08 MB Anomaly detection ⓘ On

Log streams Tags Anomaly detection Metric filters Subscription filters

To manage indexes across multiple log groups, use Account level index policies. Settings X

Log group field indexes

View and manage field indexes for this log group

Field path	Status	First event time	Last event time
Default	Active	6 months ago	1 minute ago
remote_host	Active	6 months ago	1 minute ago
http_method	Active	6 months ago	1 minute ago
agent	Active	6 months ago	1 minute ago
accountid	Active	6 months ago	1 minute ago
region	Active	6 months ago	1 minute ago

Log Group Transformers

- transformation and enrich your logs from unstructured to structured logs at ingestion
- Included in Standard log class
- Common parsers (grok, JSON, csv..) and processors for vended logs, string/JSON mutations, datatypes

The screenshot shows the AWS CloudWatch Log Groups interface. The left sidebar navigation includes CloudWatch, Favorites and recents, Dashboards, AI Operations, Alarms, Logs (selected), Metrics, Application Signals (APM), GenAI Observability, Network Monitoring, and Insights. The main content area displays the details for the log group `/httpd/access_log`. The Log group details section shows the Log class (Standard), ARN (arn:aws:logs:us-east-1:724772082388:log-group:/httpd/access_log:*), Creation time (6 months ago), Retention (Never expire), and Stored bytes (73.08 MB). It also lists Metric filters (1), Subscription filters (0), Contributor Insights rules (-), KMS key ID (-), and Anomaly detection (On). Below this, the Log streams section shows one stream named `i-061833a75c7115920`, with options to Delete, Create log stream, or Search all log streams.



Log Group Data protection

- Mask sensitive data that matches common/custom patterns
- Create Audit log group to capture all matched data
- Unmask the message with proper permissions from Logs Insights



CloudWatch > Log groups > /aws/lambda/LogGeneration-DataProtection

CloudWatch <

Favorites and recents ▶

Dashboards

▶ AI Operations New

▶ Alarms ⚠️ 4 ○ 45 ⏱ 3

▼ Logs

Log groups (selected)

Log Anomalies

Live Tail

Logs Insights

Contributor Insights

▶ Metrics New

▶ Application Signals (APM) New

▶ GenAI Observability New

▶ Network Monitoring

▶ Insights

Settings

Telemetry config

Getting Started

What's new

Actions ▾

View in Logs Insights

Start tailing

Search log group

/aws/lambda/LogGeneration-DataProtection

Log group details

Log class | Info Standard

Metric filters 0

ARN arn:aws:logs:us-east-1:724772082388:log-group:/aws/lambda/LogGeneration-DataProtection:*

Subscription filters 0

Data protection ✓ On

Sensitive data count 406925

Contributor Insights rules -

KMS key ID -

Custom field indexes [Configure](#)

Transformer [Configure](#)

Creation time 6 months ago

Retention Never expire

Anomaly detection [Configure](#)

Stored bytes 1.18 GB

Log streams Tags Anomaly detection Metric filters Subscription filters >

Log streams (100+)

By default, we only load the most recent log streams. [Load more](#).

Filter loaded log streams or try [pr](#) Exact match Show expired [Info](#) 1 2 ... > [⚙️](#)

[Create log stream](#) [Search all log streams](#)

<input type="checkbox"/> Log stream
2025/10/19/LogGeneration-DataProtection[\$LATEST]1893776f5547412ca6406f9d207794d2
2025/10/19/LogGeneration-DataProtection[\$LATEST]3ad08a6b8522444a97181ba1dabcaf9b
2025/10/19/LogGeneration-DataProtection[\$LATEST]d88252a2b4794af8a3e937fdbfb1fb9
2025/10/19/LogGeneration-DataProtection[\$LATEST]34432c109cec4e77861edf200fe092b8
2025/10/19/LogGeneration-DataProtection[\$LATEST]a7f19b5f90304748bda6d64ab62880a4
2025/10/19/LogGeneration-DataProtection[\$LATEST]47e39f974aed4bd1922a4e30dfc9bdef
2025/10/19/LogGeneration-DataProtection[\$LATEST]6d631ddd74248569dc56ec486d82d2e

Log Group Metric filters

- Create metrics from log data
- Assign dimensions and unit values
- Create metrics from centralized logs for a single location of filtered metrics



CloudWatch > Log groups > /httpd/access_log

Monitoring account

CloudWatch <

Favorites and recents ▶

Dashboards

▶ AI Operations New

▶ Alarms ⚠ 1 ✓ 50+ ⓘ 4

▼ Logs

Log groups →

Log Anomalies

Live Tail

Logs Insights

Contributor Insights

▶ Metrics New

▶ Application Signals (APM) New

▶ GenAI Observability New

▶ Network Monitoring

▶ Insights

Settings

Telemetry config

Getting Started

What's new

/httpd/access_log

Actions ▾ View in Logs Insights Start tailing Search log group

▼ Log group details

Log class Info Standard

ARN arn:aws:logs:us-east-1:724772082388:log-group:/httpd/access_log:*

Creation time 6 months ago

Retention Never expire

Stored bytes 73.24 MB

Metric filters 1

Subscription filters 0

Contributor Insights rules 1

KMS key ID -

Anomaly detection On

Data protection -

Sensitive data count -

Custom field indexes 5

Transformer On

< Tags Anomaly detection Metric filters Subscription filters Contributor >

Metric filters (1)

Edit Delete Create alarm Create metric filter

Find metric filters

access_logs_4xx

Filter pattern { \$.status_code = %4[0-9][2}% }

Field selection criteria -

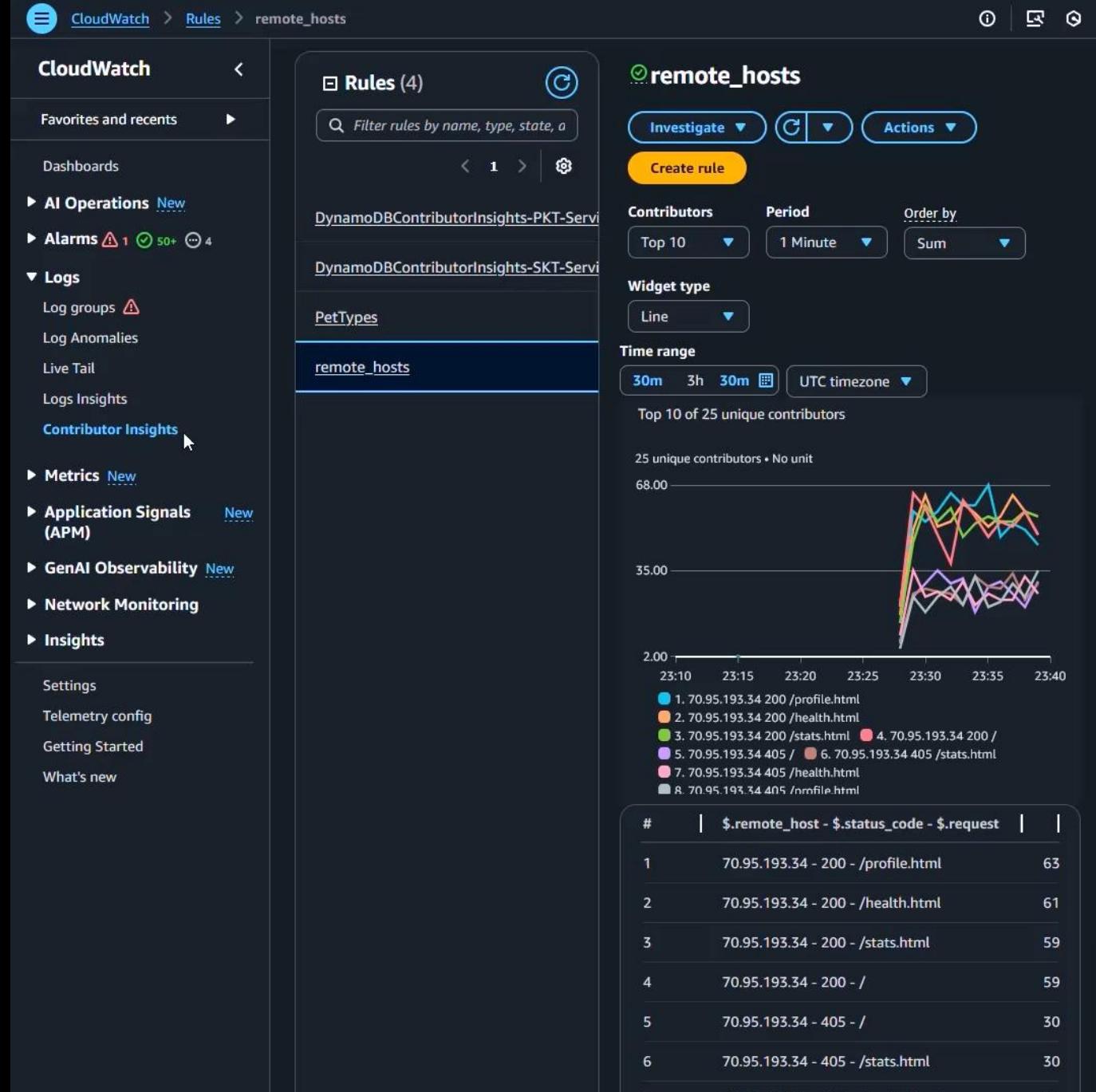
Metric apache_access_logs / status_code_4xx

Metric value 1

Default value 0

Log Group Contributor Insights

- analyze high-cardinality (many unique values) log data in real time
- View metrics about the top-N contributors, the total number of unique contributors, and their usage.
- Sorted by top contributors



Log Group Subscription filters

- real-time feed of log events from CloudWatch Logs and have it delivered to other services
- Amazon Kinesis stream, an Amazon Data Firehose stream, or AWS Lambda for custom processing, analysis, or loading to other systems

CloudWatch > Log groups > API-Gateway-Execution-Logs_dpal4wdyv7/prod

Monitoring account

CloudWatch

- Favorites and recents
- Dashboards
- AI Operations New
- Alarms ⚠️ 4 ⓘ 45 ⏱ 3
- Logs
 - Log groups
 - Log Anomalies
 - Live Tail
 - Logs Insights
 - Contributor Insights
- Metrics New
- Application Signals (APM) New
- GenAI Observability New
- Network Monitoring
- Insights
 - Settings
 - Telemetry config
 - Getting Started
 - What's new

API-Gateway-Execution-Logs_dpal4wdyv7/prod

Actions ▾ View in Logs Insights Start tailing Search log group

Log group details

Log class Info	Metric filters	Data protection
Standard	0	-
ARN	Subscription filters	Sensitive data count
arn:aws:logs:us-east-1:724772082388:log-group:API-Gateway-Execution-Logs_dpal4wdyv7/prod:*	1	-
Creation time	Contributor Insights rules	Custom field indexes
8 months ago	1	Configure
Retention	KMS key ID	Transformer
Never expire	-	Configure
Stored bytes	Anomaly detection	
1.62 GB	Configure	

Log streams

Tags Anomaly detection Metric filters Subscription filters

Log streams (100+)

By default, we only load the most recent log streams. [Load more](#).

Filter loaded log streams or try pr. Exact match Show expired ⓘ Info

1 2 ... > ⌂

<input type="checkbox"/> Log stream
555f21beef5a96bf7c4d01fc7dade1c0
ee6622ee25ec7dd44752784e9c01e715
ca910b744d77f5c22fc31661e3f38c64
bb0a0c65caf5caf85eae4aea340a30c9
7ff6fcbb69b2c2e2718f418dfb1e64b2
2600c60688d00211a6f94383f9ab6379
928530d0d16eaa71351810c733b98cbd



Log Insights

Log Group Selection

- Three options for selecting logs groups
 - Log Group name (up to 50)
 - Log Group by prefix
 - All Log Groups

The screenshot shows the AWS CloudWatch Logs Insights interface. The left sidebar has the following navigation:

- CloudWatch
- Favorites and recents
- Dashboards
- AI Operations (New)
- Alarms (4) (45)
- Logs
 - Log groups (4)
 - Log Anomalies
 - Live Tail
 - Logs Insights**
 - Contributor Insights
- Metrics (New)
- Application Signals (APM) (New)
- GenAI Observability (New)
- Network Monitoring
- Insights

The right panel is titled "Logs Insights" and shows the following interface:

- Logs Insights** info: Select log groups, and then run a query or choose a sample query.
- Logs Insights QL | PPL | SQL: Query language selection.
- Time range: 30m, 3h, 1h (selected), Compare (Off), UTC timezone.
- Select log groups by: All log groups | Selection criteria: All log groups | Log class: Standard | Account(s): All accounts.
- See recommendations: A code editor with a sample query:


```
1 fields @timestamp, @message, @LogStream, @Log
2 | sort @timestamp desc
3 | limit 10000
```
- Query generator: Run query | Cancel | Save | History.
- Logs Insights QL query can run for maximum of 60 minutes.
- Logs (-) | Patterns (-) | Visualization: Logs (-) is selected.
- Logs (-):
 - Summarize results
 - Investigate
 - Export results
 - Add to dashboard
- No results: Run a query to see related events.



Log Insights

Discovered fields

- After running a query, view the fields that you can select, filter by, and how they contributed to the query
 - View the fields that have an index



The AWS logo, consisting of the lowercase letters "aws" in white on a black background, with a curved arrow underneath.

© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved. Amazon Confidential and Trademark.

Log Insights

Saved queries

- Save common and optimized queries so you can one-click run them

CloudWatch > Logs Insights

Monitoring account

Logs Insights Analyze with OpenSearch - new

Logs Insights Info

Select log groups, and then run a query or choose a sample query.

Logs Insights QL PPL | SQL

30m 3h 1h Compare (Off) UTC timezone

Select log groups by Selection criteria

Log group name Select up to 50 log groups Browse log groups

```
1 fields @timestamp, @message, @LogStream, @Log
2 | sort @timestamp desc
3 | limit 10000
```

Query generator

Run query Cancel Save History

Logs Insights QL query can run for maximum of 60 minutes.

Logs (-) Patterns (-) Visualization

Logs (-)

Summarize results Investigate Export results Add to dashboard

Data may cross Regions

No results Run a query to see related events

Discovered fields

Saved and sample queries

Query commands



Log Insights Deduplication

- Deduplicate your log outputs so you only receive unique values.
- This does not limit the volume logs that you are querying. Only unique results.



CloudWatch > Logs Insights > General Insights/Message Dedup

Monitoring account

Logs Insights Analyze with OpenSearch - new

Logs Insights Info

Select log groups, and then run a query or choose a sample query.

Logs Insights QL PPL SQL 30m 3h 1h Compare (Off) UTC timezone UTC timezone

Select log groups by Selection criteria

Log group name Select up to 50 log groups Browse log groups

/ecs/PetSearch Monitoring account 724772082388 Clear all

```
1 fields @timestamp, message
2 | sort @timestamp asc
3
```

Query generator

Run query Cancel Save Actions History

Logs Insights QL query can run for maximum of 60 minutes.

Completed. Query executed for 1 log group.

Logs (8.6k) Patterns (-) Visualization

Logs (8.6k)

Summarize results Investigate Export results Add to dashboard

Data may cross Regions

Showing 8575 of 8,575 records matched

8,579 records (7.1 MB) scanned in 3.0s @ 2,877 records/s (2.4 MB/s)

Hide histogram

@timestamp message

▶ 1	2025-10-17T22:59:23.808Z	Error while searching, building the resulting body
▶ 2	2025-10-17T22:59:23.809Z	Servlet.service() for servlet [dispatcherServlet] in context with path [] threw exception [Req
▶ 3	2025-10-17T22:59:28.969Z	Generating presigned url
▶ 4	2025-10-17T22:59:28.969Z	Generating presigned url
▶ 5	2025-10-17T22:59:28.969Z	Generating presigned url
▶ 6	2025-10-17T22:59:28.970Z	Generating presigned url
▶ 7	2025-10-17T22:59:28.970Z	Generating presigned url
▶ 8	2025-10-17T22:59:28.970Z	Generating presigned url

Log Insights filterIndex

- Search your index for specific values
- Minimize log scanning
- Can search the account index across all logs that contain that field

The screenshot shows the AWS CloudWatch Logs Insights interface. The left sidebar navigation includes CloudWatch, Favorites and recents, Dashboards, AI Operations, Alarms, Logs (selected), Metrics, Application Signals (APM), GenAI Observability, Network Monitoring, and Insights. The Logs section contains Log groups, Log Anomalies, Live Tail, Logs Insights (selected), and Contributor Insights.

The main area displays the Logs Insights interface with tabs for Logs Insights Info, Analyze with OpenSearch - new, and Start tailing. It features a query editor with tabs for Logs Insights QL, PPL, and SQL, and time range controls (30m, 3h, 4w, Compare (Off), UTC timezone). A "Select log groups by" dropdown is set to "Log group name". The "Selection criteria" section allows selecting up to 50 log groups, with one entry: "/httpd/access_log" from Monitoring account 724772082388. A "Browse log groups" section shows a sample query:

```

1 fields @timestamp, @message, @LogStream, @Log
2 | sort @timestamp desc
3 | limit 10000

```

Below the query editor are buttons for Run query, Cancel, Save, and History. A note states: "Logs Insights QL query can run for maximum of 60 minutes." A status message indicates: "Completed. Query executed for 1 log group. ⓘ".

The results section is titled "Logs (10k)" and includes tabs for Patterns (49) and Visualization. It shows a histogram with 106,640 records scanned in 12.1s at 8,827 records/s (1.8 MB/s). Buttons for Summarize results, Investigate, Export results, and Add to dashboard are available. A note says: "Data may cross Regions".

On the right side, there are sections for Discovered fields, Saved and sample queries, and Query commands.



Log Insights

Pattern analysis

- View common patterns for distinct time periods
- Compare known good time frames to time where incidents have occurred to see what changed

The screenshot shows the AWS CloudWatch Logs Insights interface. The left sidebar includes links for CloudWatch, Favorites and recents, Dashboards, AI Operations, Alarms, Logs (selected), Metrics, Application Signals, GenAI Observability, Network Monitoring, and Insights. The main area has tabs for Logs Insights (selected) and Analyze with OpenSearch - new. It features a query editor with Log Insights QL, PPL, and SQL tabs, and a time range selector for 30m, 3h, 1h, and UTC timezone. A sample query is shown:

```

1 fields @timestamp, @message, @LogStream, @Log
2 | sort @timestamp desc
3 | limit 10000
  
```

Below the query editor are buttons for Run query, Cancel, Save, and History. A note states: "Logs Insights QL query can run for maximum of 60 minutes." The results section is currently empty, showing "No results" and "Run a query to see related events". On the right side, there are sections for Discovered fields, Saved and sample queries, and Query commands.



Log Insights

OpenSearch SQL

- Use OpenSearch SQL to query your CloudWatch Logs.
- Use JOINs, Subqueries, and other functions for advanced analysis
- Easy to adopt for users proficient with SQL

The screenshot shows the AWS CloudWatch Log Insights interface. The left sidebar menu includes options like CloudWatch, Favorites and recents, Dashboards, AI Operations, Alarms, Logs (selected), Metrics, Application Signals (APM), GenAI Observability, Network Monitoring, and Insights. Under Logs, there are sub-options for Log groups, Log Anomalies, Live Tail, Log Insights (selected), and Contributor Insights. The main content area displays a sample Log Insights query:

```

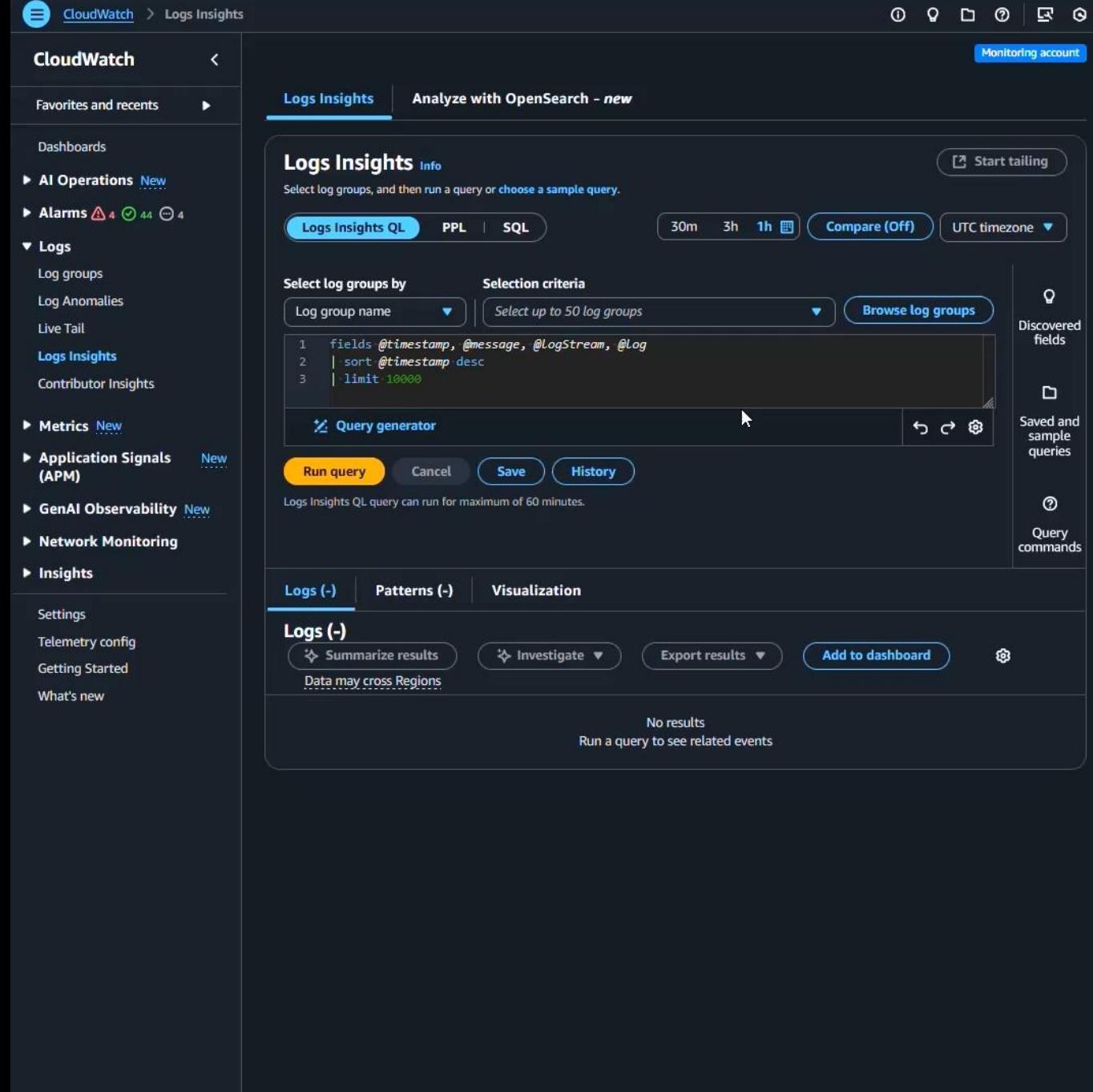
1 fields @timestamp, @message, @LogStream, @Log
2 | sort @timestamp desc
3 | limit 10000
  
```

The interface includes tabs for Logs Insights QL, PPL, and SQL, with the Logs Insights QL tab selected. It also features a selection criteria section for log groups, a query generator, and buttons for Run query, Save, and History. Below the query editor, it says "Logs Insights QL query can run for maximum of 60 minutes." The results section is currently empty, showing "No results" and a message to "Run a query to see related events". On the right side, there are sections for Discovered fields, Saved and sample queries, and Query commands.



Log Insights OpenSearch PPL

- Use OpenSearch PPL to query your CloudWatch Logs.
- Use JOINs, Subqueries, and other functions for advanced analysis
- Easy to adopt for users proficient with PPL



The screenshot shows the AWS CloudWatch Log Insights interface. The left sidebar navigation includes CloudWatch, Favorites and recents, Dashboards, AI Operations, Alarms, Logs (selected), Metrics, Application Signals (APM), GenAI Observability, Network Monitoring, and Insights. The Logs section contains sub-links for Log groups, Log Anomalies, Live Tail, Log Insights (selected), and Contributor Insights. The main content area is titled "Logs Insights" and "Analyze with OpenSearch - new". It features a "Logs Insights QL" editor with the following query:

```
1 fields @timestamp, @message, @LogStream, @Log
2 | sort @timestamp desc
3 | limit 10000
```

Below the editor are buttons for "Run query", "Cancel", "Save", and "History". A note states: "Logs Insights QL query can run for maximum of 60 minutes." The interface also includes tabs for "Logs (-)" (selected), "Patterns (-)", and "Visualization". At the bottom, there are buttons for "Summarize results", "Investigate", "Export results", "Add to dashboard", and a gear icon. A message says: "Data may cross Regions" and "No results Run a query to see related events". On the right side, there are sections for "Discovered fields", "Saved and sample queries", and "Query commands".

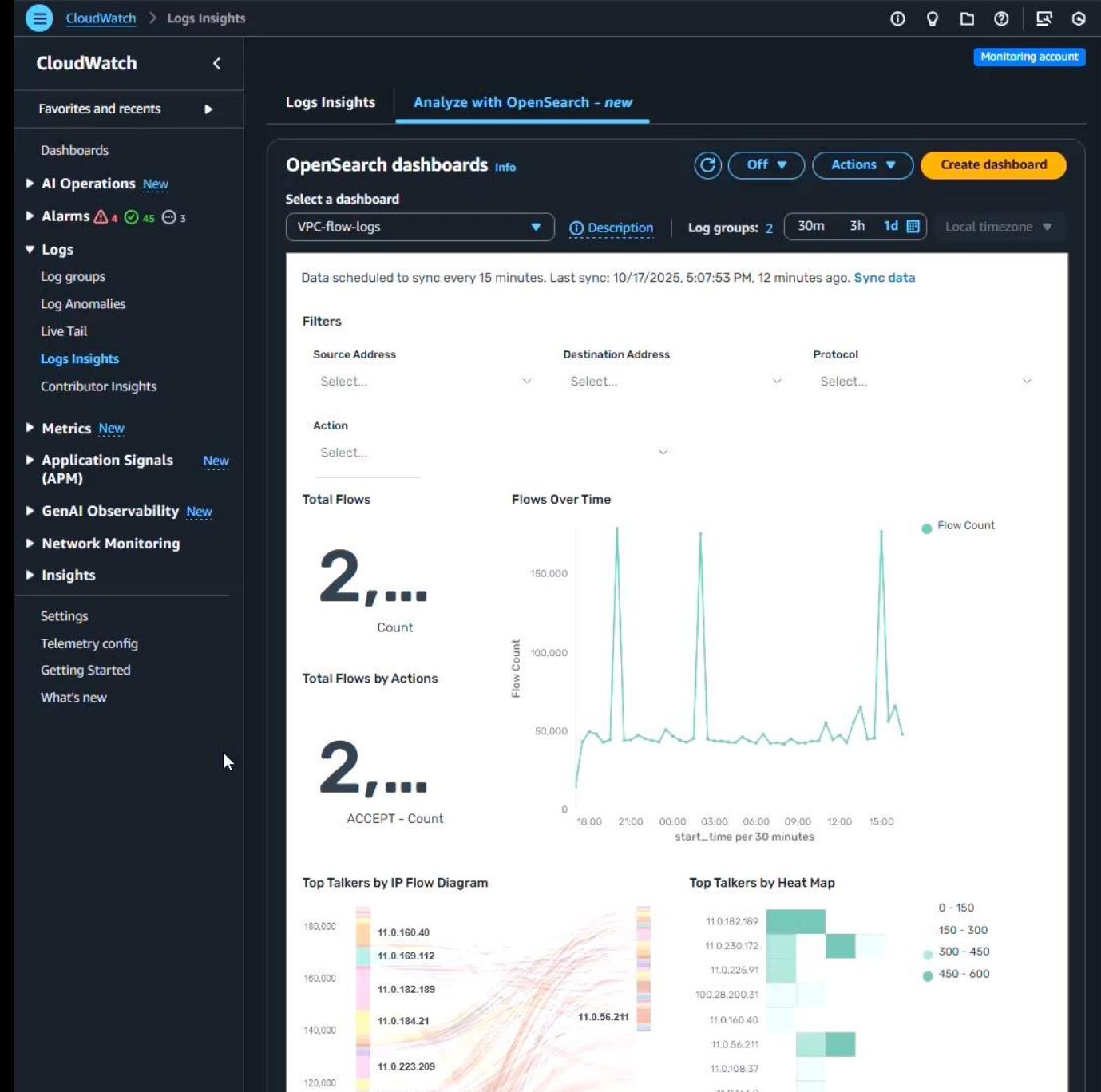


Log Insights

Zero-ETL Dashboards

- Simple to setup dashboards in Logs Insights using OpenSearch integration:

- VPC Flow Logs
- AWS Network Firewall
- CloudTrail Logs
- AWS WAF logs



Log Insights

Live Tail

- Live Tail your logs from the console or command line
- Filter logs my unique values
- Highlight key words to easily view where you need to focus

The screenshot shows the AWS CloudWatch Live Tail interface. On the left is a sidebar with navigation links: CloudWatch, Favorites and recents, Dashboards, AI Operations, Alarms, Logs (selected), Log groups, Log Anomalies, Live Tail (selected), Logs Insights, Contributor Insights, Metrics, Application Signals (APM), GenAI Observability, Network Monitoring, and Insights. Below these are Settings, Telemetry config, Getting Started, and What's new. At the top right are buttons for Filter, Actions, Clear, Cancel, and Start. The main area is titled "Live Tail" with a "Highlight term" input field containing "Highlight up to 5 terms (Not case sensitive)". It shows 0 events/sec, 0% displayed, a timestamp of 00:02:47, and a "View in columns" button. A large "Filter" modal is open, containing sections for "Select log groups" (with a dropdown labeled "Search and select log groups"), "Select log streams - optional" (with a dropdown labeled "Select log streams by name" and "Type in prefix"), and "Add filter patterns (Case sensitive) - optional" (with a dropdown labeled "Filter log events"). An "Apply filters" button is at the bottom of the modal. To the right of the modal is a small icon of horizontal bars and the text "Select a log group to start your Live Tail session".





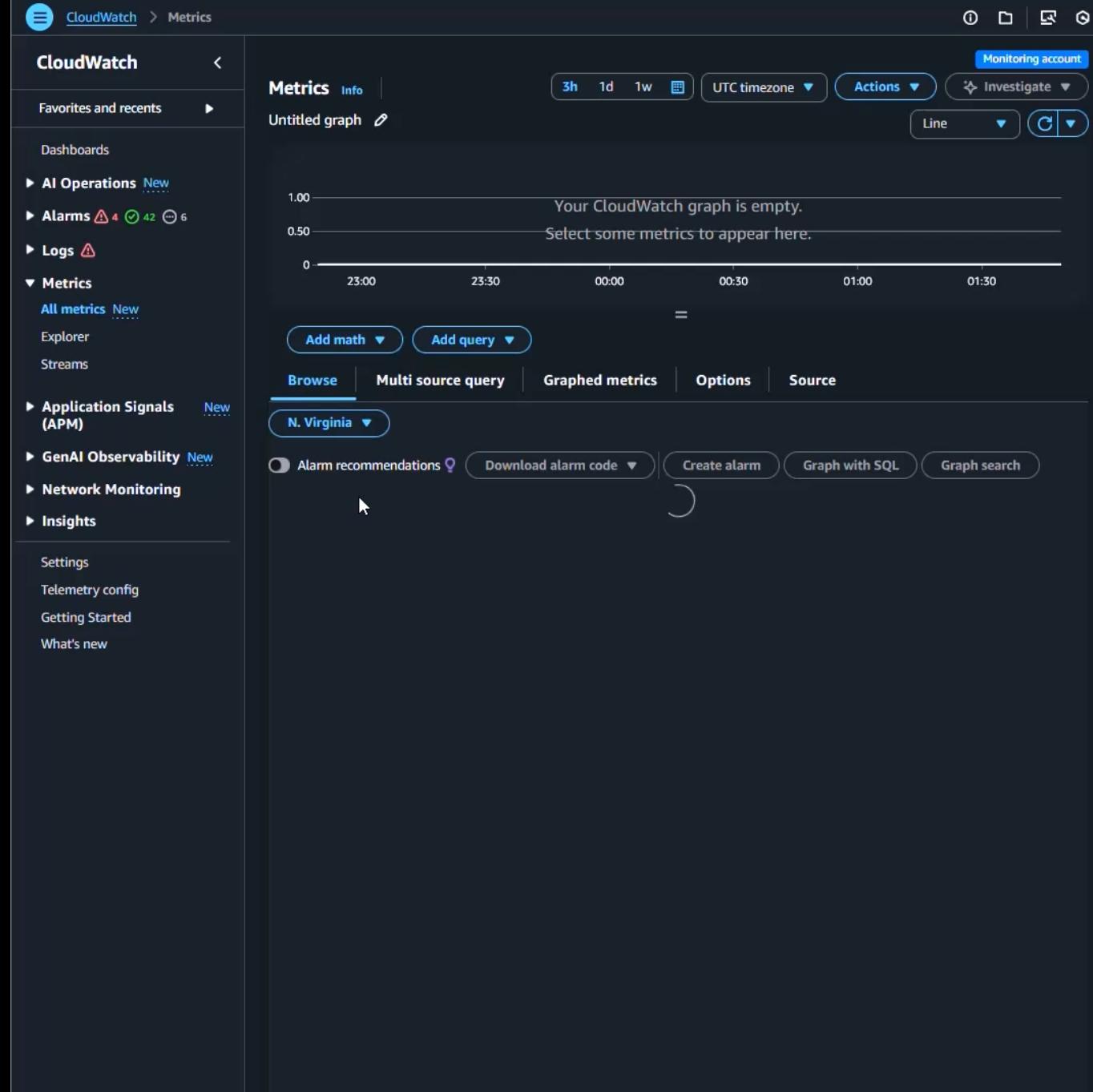
Metrics



© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved. Amazon Confidential and Trademark.

Alarm recommendations

- Automatic recommendations for alarms.
- Identify where metrics you may want to track and alert on

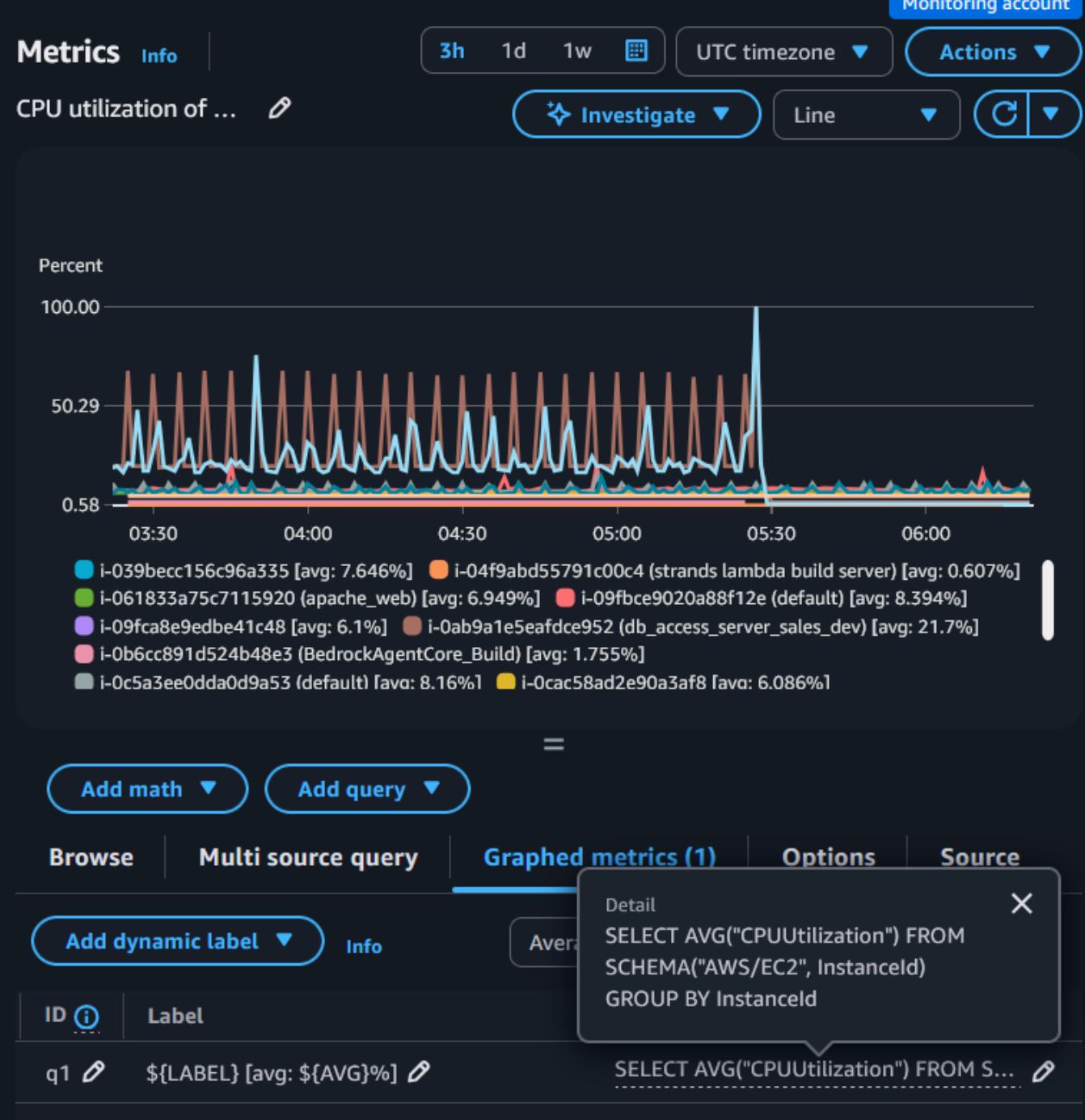


Dynamic Fleet Metric queries

- Use **GROUP BY** in your metric query to define a resource type for your metric. This will get all the resources with that metric

Gets all EC2 Instances

GROUP By InstanceId



Tag based metric queries

- Use the **tag.{Key}** in the GROUP BY field to

Group by Env for EC2 Instances

GROUP By tag.Env

Select only Env:prod EC2 Instances

WHERE tag.Env='prod'



Tag based metric queries

- Use the **tag.{Key}** in the GROUP BY field to

Group by Env for EC2 Instances
GROUP By tag.Env

Select only Env:prod EC2 Instances
WHERE tag.Env='prod'



Metric Datasources

- Query Metrics from other data sources in CloudWatch
 - Amazon OpenSearch
 - Amazon Managed Service for Prometheus
 - Amazon RDS
 - Amazon S3 CSV
 - Microsoft Azure Monitor
 - Prometheus



The screenshot shows the AWS CloudWatch Metrics Settings interface. The left sidebar includes links for CloudWatch, Favorites and recents, Dashboards, AI Operations, Alarms, Logs, Metrics (with sub-links for All metrics, Explorer, Streams), Application Signals (APM), GenAI Observability, Network Monitoring, Insights, and Settings (which is currently selected). The main content area is titled "CloudWatch settings" and shows the "Metrics data sources - new" tab selected. It displays a section titled "Configured data sources - (0)" with a "Create data source" button. Below this, it says "No data source configured." and provides instructions to "Configure a new data source by selecting one of our standard connectors such as Amazon OpenSearch, Amazon RDS, Amazon S3, Prometheus...". There is also a "+ Create data source" button.



Traces



© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved. Amazon Confidential and Trademark.

Transaction Search

- OpenTelemetry format traces
- Visualize as List, TimeSeries, or Group
- Service discover to filter on traces from your service operations and dependancies



CloudWatch > Transaction Search

CloudWatch

Favorites and recents

Dashboards

▶ AI Operations New

▶ Alarms 2 49 6

▶ Logs 1

▶ Metrics New

▼ Application Signals (APM)

Services

Application Map New

Transaction Search

Service Level Objectives (SLO)

Synthetics Canaries

RUM

Traces

Trace Map

▶ GenAI Observability New

▶ Network Monitoring

▶ Insights

Settings

Telemetry config

Getting Started

What's new

Monitoring account

Spans Info

Analyze spans with other logs Start tailing

Run a query to view spans, span events, and patterns. Or choose a sample query. By default, queries are run on the log group [aws/spans](#). To search across other log groups, go to [Log Insights](#).

Visual Editor | Logs Insights QL

30m 3h 1h Compare (Off) UTC timezone

Filter spans by: Visualize as:

Search spans by pasting, selecting from properties or using List

Run query Cancel

Span query can run for maximum of 60 minutes.

Spans (-) Patterns (-) Visualization

Spans (-)

This table shows results for spans or span events.

Summarize results Investigate Export results

Data may cross Regions

Add to dashboard

No spans to show

Run a query to view spans. To quickly get started, try these common queries:

Top services with faults + Add to query

Top slow operations + Add to query

Top slow database statements + Add to query

Error trends over time + Add to query

Spans by performance issues or errors + Add to query

Select filters

Select filter below to add to your query.

Clear filters

Span Duration

Min Max

0ms 1000ms

Span status

UNSET Span completed without errors

ERROR Span failed due to an error

OK Span explicitly marked as successful

HTTP status code

500 400 401 403 200 503 404

Services (37)

Search services

PetSite 686255944078 - ec2:default

PetSearch 686255944078 - generic:default

MyLambdaFunction 686255944078 - lambda:default

Services-StepFnlambdaStepReadDDB 686255944078 - lambda:default

petlistadoptions 686255944078 - generic:default

PetAdoptionStatusUpdater 686255944078 - api-gateway:prod

CloudShell Feedback

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

TRACES

X-Ray traces

- View traces for your applications
- X-Ray SDK is being deprecated for OpenTelemetry (Feb 25, 2027). X-Ray will continue to exist.



© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved. Amazon Confidential and Trademark.

CloudWatch > Traces

CloudWatch

Favorites and recents

Dashboards

▶ AI Operations New

▶ Alarms 3 50+ 3

▶ Logs 3

▶ Metrics New

▼ Application Signals (APM)

Services

Application Map New

Transaction Search

Service Level Objectives (SLO)

Synthetics Canaries

RUM

Traces

Trace Map

▶ GenAI Observability New

▶ Network Monitoring

▶ Insights

Settings

Telemetry config

Getting Started

What's new

Monitoring account

Traces Info Capture all trace spans cost-effectively to gain detailed insights with Transaction Search

15m 1h 6h 5m Local timezone C ▾

Find traces by typing a trace ID or query, build a query using the Query refiners section, or choose a sample query. You can also type a trace ID here.

Filter by X-Ray gra Find traces by typing a trace ID or auerv. or build a auerv using the Ouerv refiners section

Run query 647 traces retrieved

Query refiners

Refine query by Node Add to query

Select rows to filter traces

Find Node

Node

DynamoDB

DynamoDB

Latency (avg): 375ms Requests: 0.60/min Faults: 0.00/min 0 Alarms

PGSQL Query

Remote

Latency (avg): 3ms Requests: 6.80/min Faults: 0.00/min 0 Alarms

PetAdoptionStatusUpdater/prod

Apigateway Stage

Latency (avg): 118ms Requests: 0.40/min Faults: 0.00/min 0 Alarms

PetSearch

ECS Fargate - Environment generic/default

Latency (avg): 1ms Requests: 8.60/min Faults: 0.00/min 0 Alarms

PetSearch

ECS Fargate

Latency (avg): 16ms Requests: 69.40/min Faults: 1.20/min 0 Alarms

Refine query by response time distribution

Drag and drop on the graph to select a time frame or use keyboard to traverse and select datapoints using shift & arrow keys

No. of traces p50 p95 p99

0 500ms 1.0s 1.5s 2.0s 2.5s 3.0s Latency

Traces (647) Add to dashboard

This table shows traces with updates within the last 5 minutes, with an average response time of 0.02s. It shows as many as

X-Ray adaptive sampling boost

- Requires Latest version of ADOT SDK & Java v2.11.5 higher
- Head-based sampling
- Anomaly-driven through ADOT anomaly statistics

Example rule with adaptive sampling

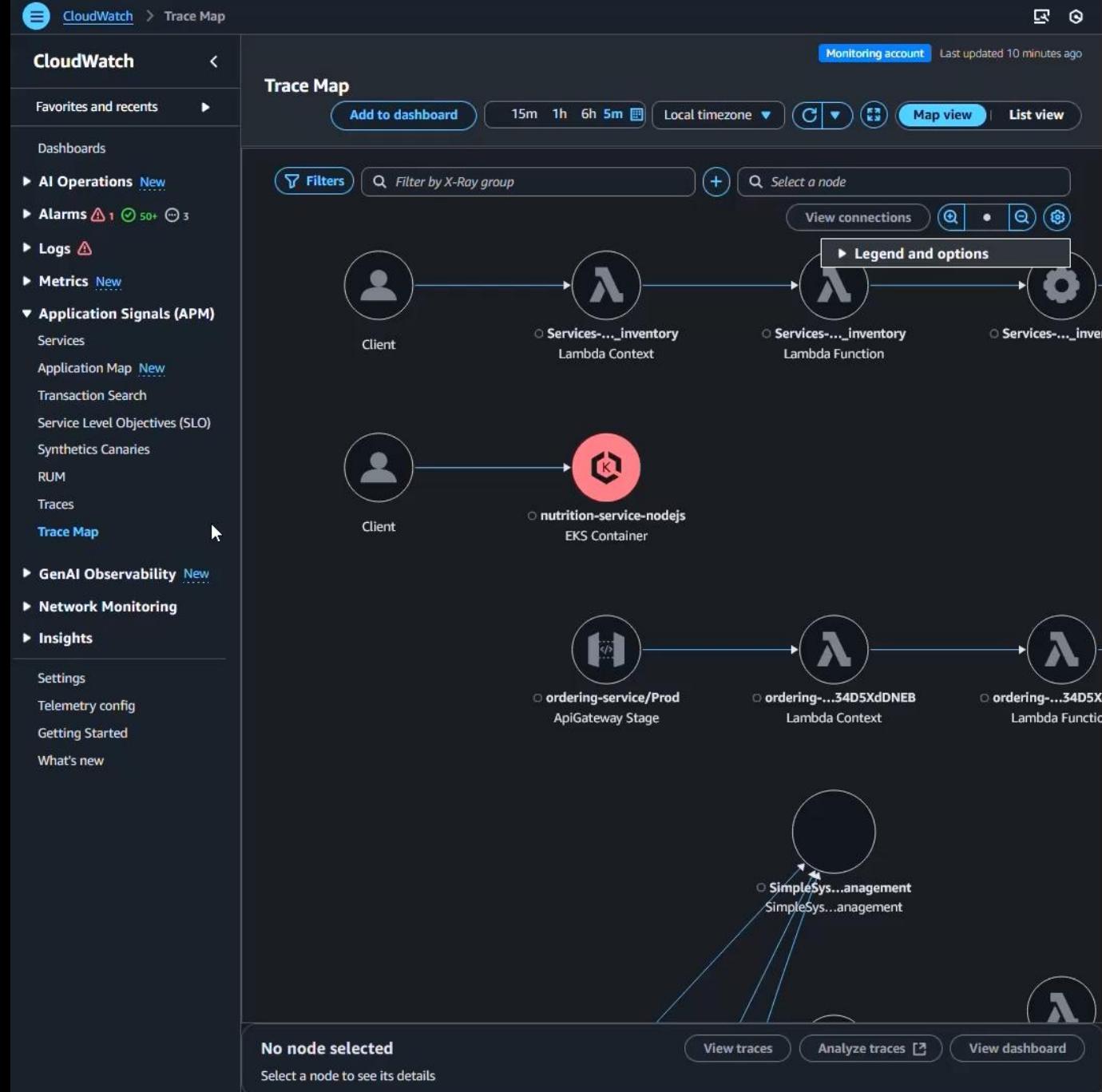
```
{  
    "RuleName": "MyAdaptiveRule",  
    "Priority": 1,  
    "ReservoirSize": 1,  
    "FixedRate": 0.05,  
    "ServiceName": "*",  
    "ServiceType": "*",  
    "Host": "*",  
    "HTTPMethod": "*",  
    "URLPath": "*",  
    "SamplingRateBoost": {  
        "MaxRate": 0.25,  
        "CooldownWindowMinutes": 10  
    }  
}
```



TRACES

X-Ray trace map

- identify services where errors are occurring, connections with high latency, or traces for requests that were unsuccessful.



© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved. Amazon Confidential and Trademark.

<https://docs.aws.amazon.com/xray/latest/devguide/xray-console-servicemap.html>



CloudWatch Agent



© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved. Amazon Confidential and Trademark.

Logs

- Filter logs to exclude or include based on keyword or regex
- Set service.name to map related telemetry
- Can send logs via FIPS or VPC endpoint

```
"logs":{  
    "service.name": "order-service",  
    "deployment.environment": "production",  
    "logs_collected": {  
        "files": {  
            "collect_list": [  
                {  
                    "file_path": "/opt/aws/amazon-cloudwatch-agent/logs/test.log",  
                    "log_group_name": "test.log",  
                    "log_stream_name": "test.log",  
                    "filters": [  
                        {  
                            "type": "exclude",  
                            "expression": "Firefox"  
                        },  
                        {  
                            "type": "include",  
                            "expression": "P(UT|OST)"  
                        }  
                    ]  
                }  
            ]  
        }  
    }  
}
```



Metrics

- Can send metrics to CloudWatch or Amazon Managed Prometheus
- Can specify the metrics_collection_interval
- Collect nvidia_gpu metrics

```
{  
  "metrics": {  
    "metrics_destinations": {  
      "cloudwatch": {},  
      "amp": {  
        "workspace_id": "ws-abcd1234-ef56-7890-ab12-example"  
      }  
    }  
  }  
}
```



Metrics

- Can send metrics to CloudWatch or Amazon Managed Prometheus
- Can specify the metrics_collection_interval
- Collect nvidia_gpu metrics

```
"metrics": {  
    "aggregation_dimensions" : [[ "AutoScalingGroupName"], [ "InstanceId", "InstanceType"],[]],  
    "metrics_collected": {  
        "collectd": {},  
        "cpu": {  
            "resources": [  
                "*"  
            ],  
            "measurement": [  
                {"name": "cpu_usage_idle", "rename": "CPU_USAGE_IDLE", "unit": "Percent"},  
                {"name": "cpu_usage_nice", "unit": "Percent"},  
                "cpu_usage_guest"  
            ],  
            "totalcpu": false,  
            "drop_original_metrics": [ "cpu_usage_guest" ],  
            "metrics_collection_interval": 10,  
            "append_dimensions": {  
                "test": "test1",  
                "date": "2017-10-01"  
            }  
        },  
        "netstat": {  
            "measurement": [  
                "tcp_established",  
                "tcp_syn_sent",  
                "tcp_close"  
            ]  
        }  
    }  
}
```



Metrics

- Can send metrics to CloudWatch or Amazon Managed Prometheus
- Can specify the metrics_collection_interval
- Collect nvidia_gpu metrics

```
        ],
        "metrics_collection_interval": 60
    },
    "disk": {
        "measurement": [
            "used_percent"
        ],
        "resources": [
            "*"
        ],
        "drop_device": true
    },
    "processes": {
        "measurement": [
            "running",
            "sleeping",
            "dead"
        ]
    }
},
"append_dimensions": {
    "ImageId": "${aws:ImageId}",
    "InstanceId": "${aws:InstanceId}",
    "InstanceType": "${aws:InstanceType}",
    "AutoScalingGroupName": "${aws:AutoScalingGroupName}"
}
}
```



Traces

- Configure for X-Ray or OTLP
- can send traces via FIPS or VPC endpoint
- Can send traces in OTLP format to X-Ray to support span events in Transaction Search

```
"traces_collected": {  
    "xray": {  
    },  
    "otlp": {  
    }  
}
```



Traces

- Configure for X-Ray or OTLP
- can send traces via FIPS or VPC endpoint
- Can send traces in OTLP format to X-Ray to support span events in Transaction Search

```
"traces_collected": {  
    "xray": {  
        "bind_address": "127.0.0.1:2000",  
        "tcp_proxy": {  
            "bind_address": "127.0.0.1:2000"  
        }  
    },  
    "otlp": {  
        "grpc_endpoint": "127.0.0.1:4317",  
        "http_endpoint": "127.0.0.1:4318"  
    }  
}
```



Traces

- Configure for X-Ray or OTLP
- can send traces via FIPS or VPC endpoint
- Can send traces in OTLP format to X-Ray to support span events in Transaction Search



```
"traces": {  
    "traces_collected": {  
        "application_signals": {},  
        "xray": {  
            "bind_address": "127.0.0.1:2000",  
            "tcp_proxy": {  
                "bind_address": "127.0.0.1:2000"  
            }  
        },  
        "otlp": {  
            "grpc_endpoint": "127.0.0.1:4317",  
            "http_endpoint": "127.0.0.1:4318"  
        },  
    }  
    "transit_spans_in_otlp_format": true  
}
```

Windows event log filtering

- Selectively collect and send Windows event logs using **event_name**: System, Security, Application, etc
- Optional filter by **event_levels** (INFORMATION, WARNING, ERROR, CRITICAL, VERBOSE)
- Optional filter by **event_ids**



```
"collect_list": [  
    {  
        "event_name": "Application",  
        "log_group_name": "ApplicationEvents",  
        "log_stream_name": "ApplicationEvents",  
        "filters": [  
            {  
                "type": "include",  
                "expression": "Database.*failed|Authentication.*|login.*"  
            }  
        ],  
        {  
            "event_name": "System",  
            "log_group_name": "SystemEvents",  
            "log_stream_name": "Logon-events",  
            "event_ids": [  
                4624,  
                4625  
            ],  
            "filters": [  
                {  
                    "type": "include",  
                    "expression": ".*user.*"  
                },  
                {  
                    "type": "exclude",  
                    "expression": ".*successful.*"  
                }  
            ]  
        }  
    }  
]
```



Alarms



© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved. Amazon Confidential and Trademark.

Composite alarms

- Reduce the noise by combining alarms that fire together when there is an problem



CloudWatch Alarms

Metrics data not verified

Alarms (57)

Hide Auto Scaling alarms Clear selection Create composite alarm Actions ▾

Create alarm

Search Alarm state: Any ▾ Alarm type: Any ▾

Actions status: Any ▾

<input type="checkbox"/>	Name	State	Last state update (UTC)	Conditions
<input type="checkbox"/>	Composit_Alarm_EC2	OK	2025-10-20 04:57:55	Any of the following metrics are within 1 minute of their threshold:
<input type="checkbox"/>	EC2 Fleet - CPUUsage above 30%	OK	2025-10-20 04:57:46	EC2 Fleet - CPUUsage above 30%
<input type="checkbox"/>	EC2 Production Fleet - CPUUsage above 30%	In alarm	2025-10-20 04:57:10	EC2 Production Fleet - CPUUsage above 30%
<input type="checkbox"/>	CPUUtilizationTooHigh	OK	2025-10-20 04:54:37	CPUUtilizationTooHigh
<input type="checkbox"/>	NetworkOutTooHigh	OK	2025-10-20 04:54:24	NetworkOutTooHigh
<input type="checkbox"/>	DiskReadOpsTooHigh	OK	2025-10-20 04:53:21	DiskReadOpsTooHigh
<input type="checkbox"/>	ApplicationInsights/Services/AWS/RDS/VolumeBytesUsed/services-databaseb269d8bb-1rdmdluj11q6/	Insufficient data	2025-10-20 04:16:26	input is output datapoints over 5 minutes
<input type="checkbox"/>	ApplicationInsights/Services/AWS/ApplicationELB/TargetResponseTime/app/Service-payoff-nTN1Y8RtnmUQ/f4e22d8d99fa7aef/	OK	2025-10-20 02:47:26	input is output datapoints over 5 minutes
<input type="checkbox"/>	ApplicationInsights/Services/AWS/ApplicationELB/TargetResponseTime/app/Service-PetSitQYI4NAq3IFF/95a7408dda802bbc/	OK	2025-10-20 02:46:13	input is output datapoints over 5 minutes

ALARMS

Dynamic fleet alarms

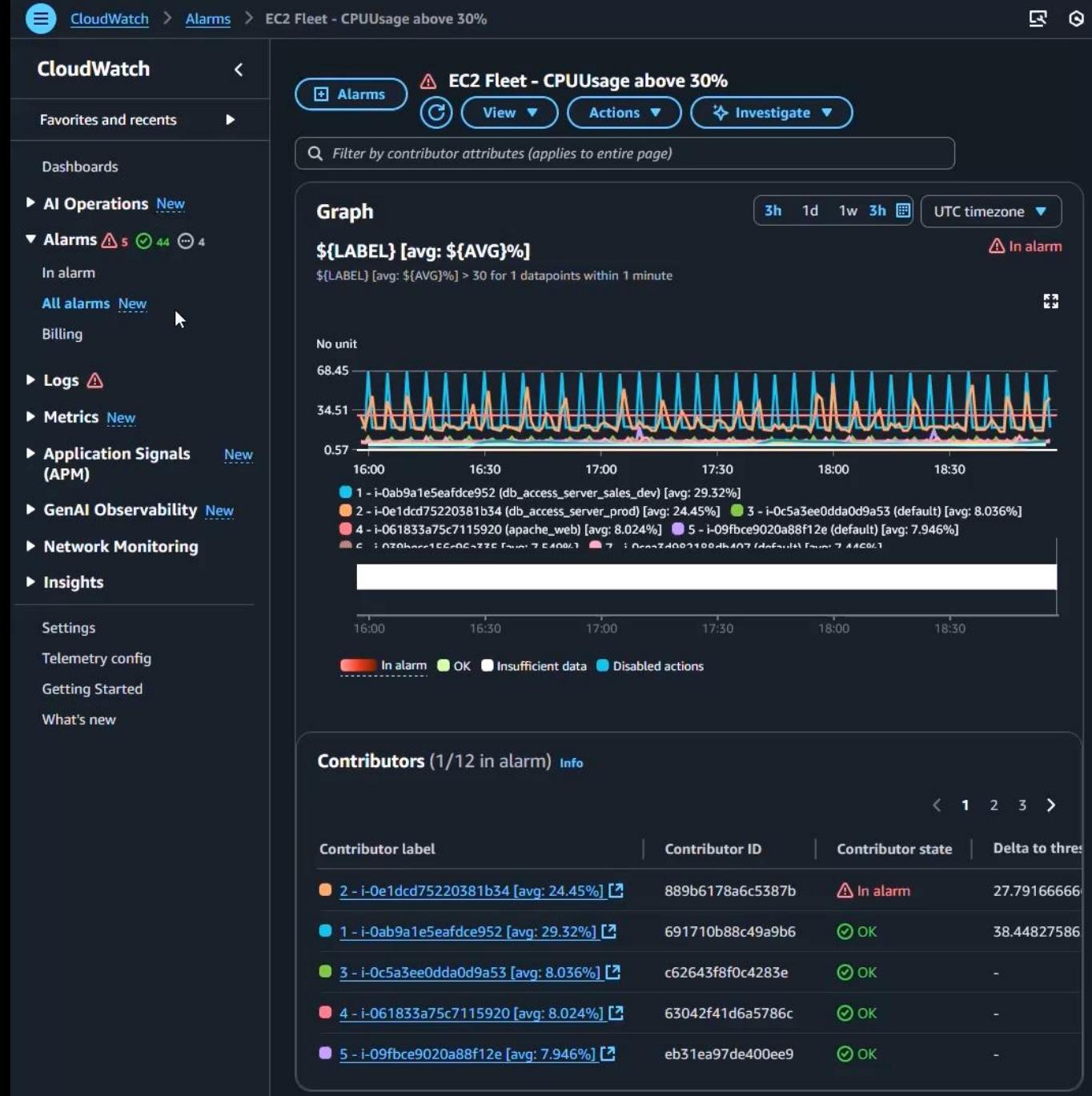
- Use **GROUP BY** in your metric query to define a resource type for your metric. This will get all the resources with that metric

Gets all EC2 Instances

GROUP By InstanceId



© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved. Amazon Confidential and Trademark.



ALARMS

Dynamic Fleet Tag-based alarms

- Use the **WHERE** field to define a resource tag key value pair to filter your alarm.

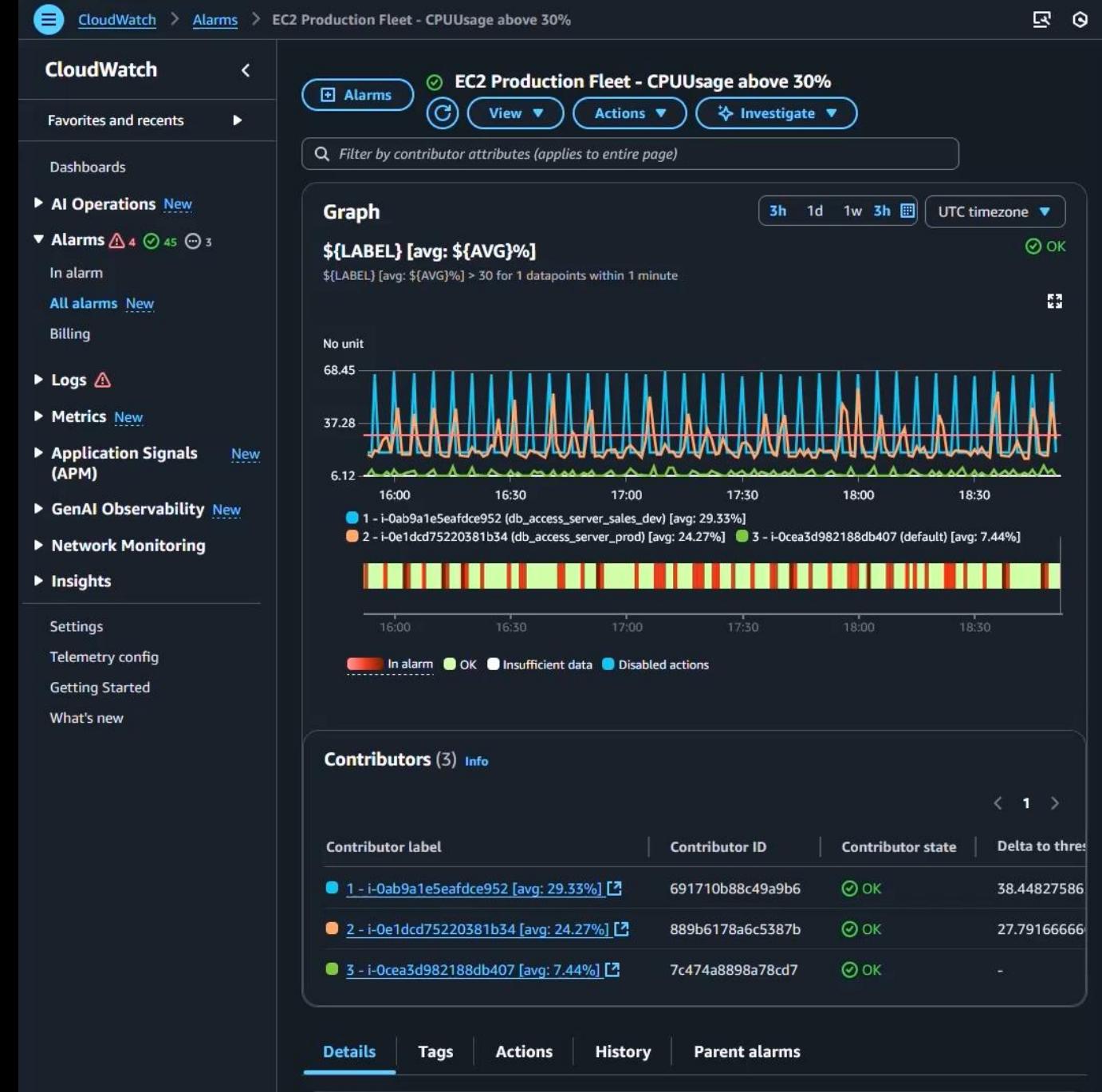
Gets all tagged prod EC2 Instances

WHERE tag.Env='prod'

GROUP By InstanceId



© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved. Amazon Confidential and Trademark.





Dashboards



© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved. Amazon Confidential and Trademark.

DASHBOARDS

Automatic Service Dashboards

- Automatic Dashboards for:
 - Overview
 - Cross service
 - Billing
 - Recent alarms
 - AWS Services
- Quickly identify how your AWS services are performing

The screenshot shows the AWS CloudWatch Metrics and Alarms dashboard. On the left, a sidebar lists various monitoring categories: CloudWatch, Favorites and recents, Dashboards, AI Operations, Alarms, Logs, Metrics, Application Signals (APM), GenAI Observability, Network Monitoring, Insights, Settings, Telemetry config, Getting Started, and What's new. The main area is titled "Overview" and shows a summary of detected problems: 1 high severity, 2 medium severity, and 1 low severity. It includes a link to "View in Application Insights". Below this is a section titled "Alarms by AWS service" which displays a chart of service health. The chart indicates 2 services in alarm, 15 services with insufficient data, and 15 OK services. Services listed include DynamoDB, RDS, RDS Cluster, Simple Queue Service, Step Functions, Lambda, EC2, Application ELB, Elastic Load Balancing, Elastic Kubernetes Service, EKS Cluster, ECS Cluster, CloudFormation, and VPC NAT Gateways. To the right, there are three detailed time-series charts for Application Insights: "ApplicationInsights/S..." showing CPU utilization and consumed read capacity; "50p cpu" showing CPU utilization over time; and "DB Load Percentage" showing DB load relative to number of visitors.



© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved. Amazon Confidential and Trademark.

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/GettingStarted.html>

Custom Dashboards

- Create your own dashboards using Variables to update what's displayed.
- Leverage Markdown to add directions or split up the dashboard
- Create custom widgets using lambda for complex displays



CloudWatch > Dashboards

CloudWatch

Favorites and recents

Dashboards

Tag-based-Env-dashboard-EC2

▶ AI Operations New

▶ Alarms ⚠ 2 ✓ 49 ⚡ 6

▶ Logs ⚠

▶ Metrics New

▶ Application Signals New (APM)

▶ GenAI Observability New

▶ Network Monitoring

▶ Insights

Settings

Telemetry config

Getting Started

What's new

Custom dashboards Automatic dashboards

Custom Dashboards (36) Info

Share dashboard Delete Create dashboard

Filter dashboards

Name	Sharing	Favorite	Last update (U...)
Common_Cloud...		★	2025-05-02 10:17
Demo-AgentCor...		★	2025-10-07 06:12
Demo-CloudWat...		★	2025-08-13 17:08
Demo-Database...		★	2025-10-15 13:31
Demos		★	2025-05-22 06:47
Tag-based-Env-...		★	2025-09-27 21:30
ApplicationInsig...		★	2025-02-21 00:00
ApplicationMoni...		★	2025-09-26 21:57
Demo-PetListAd...		★	2025-02-20 20:37
EBS-Dashboard		★	2025-02-25 19:40
GuageTest		★	2025-04-17 04:56
PetSite_Cost_Co...		★	2025-02-20 17:56
Prod-Dashboard		★	2025-09-26 21:40
Tag-based-Env-...		★	2025-09-27 13:09
Tag-based-Env-...		★	2025-09-27 13:02



Network



© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved. Amazon Confidential and Trademark.

NETWORK

Flow Monitors

- near real-time visibility into network performance, such as packet loss and latency:
 - Between VPCs
 - Within an AZ
 - Between Azs
 - Between Regions
 - S3
 - DyanmoDB
 - Unclassified networks



© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved. Amazon Confidential and Trademark.

CloudWatch > Network Flow Monitor

CloudWatch <

Favorites and recents ►

Dashboards

▶ AI Operations New

▶ Alarms 1 50+ 13

▶ Logs ⚠

▶ Metrics New

▶ Application Signals New (APM)

▶ GenAI Observability New

▼ Network Monitoring

Flow monitors

Internet monitors

Synthetic monitors

▶ Insights

Settings

Telemetry config

Getting Started

What's new

Network Flow Monitor Management account

Network Flow Monitor is a feature of CloudWatch Network Monitoring that uses lightweight agents in your EC2 instances to return performance and availability metrics about network flows between AWS resources. Set up CloudWatch integration with AWS Organizations to enable viewing and monitoring performance metrics in Network Flow Monitor for resources in multiple accounts. We recommend that you use a delegated administrator account to add accounts, and view and monitor performance metrics.

▶ Configure Organizations permissions Info

To add more than one account to your scope for network observability in Network Flow Monitor, you must configure permissions for AWS Organizations in CloudWatch settings.

▶ Getting started with Network Flow Monitor Info

Workload insights | Monitors | Settings

Between VPCs | Within an AZ | Between AZs | Between Regions | S3 | Unclassified

Unclassified Info

Review the graphs provided here to identify workloads that you'd like to see more details for by creating a monitor. These metrics are generated by Network Flow Monitor and are not available in CloudWatch.

Data transferred

Data transferred is the amount of data sent and received between resources.

Bytes

280k

260k

240k

220k

200k

180k

06:10 06:20 06:30 06:40 06:50 07:00 07:10

Internet Monitor

- visibility into how internet issues impact the performance and availability between your applications hosted on AWS and your end users
- reduce the time it takes for you to diagnose internet issues from days to minutes



© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved. Amazon Confidential and Trademark.

CloudWatch

Favorites and recents

Dashboards

▶ AI Operations New

▶ Alarms 1 50+ 4

▶ Logs

▶ Metrics New

▶ Application Signals (APM) New

▶ GenAI Observability New

▼ Network Monitoring

Flow monitors

Internet monitors Internet monitors

Synthetic monitors

▶ Insights

Settings

Telemetry config

Getting Started

What's new

Internet weather map

View major internet outages and impacted client locations in the past 24 hours.

Reset zoom

Location, ASN, event type

Availability

1 hour ago | Active event

Munich, Germany

Availability

16 hours ago | Active event

Turin, Italy

Availability

21 hours ago | Active event

Oslo, Norway

Availability

1 hour ago | Active event

Durban, Indonesia

● Availability issues ● Performance issues
● Last outages in the last 24 hours ● AWS Regions

Do these outages impact your traffic? Create a monitor to explore root causes, and to track just the traffic that's specific to your VPC, NLB, CloudFront distribution, and WorkSpaces resources.

Create monitor

Learn more about monitoring in Internet Monitor [i]

Internet Monitor focuses monitoring on the subset of the internet that's accessed by your users. It uses the same probes and issue-detection algorithms that AWS uses internally, and alerts you to issues that affect your application.

Learn more about city-networks [i]

A city-network is the combination of a location where clients access your application resources from and the ASN they use for access - typically an internet service provider (ISP), that clients access the resources through.

Learn more about pricing [i]

Pricing for Internet Monitor has two components: a per monitored resource fee and a per city-network fee. There are no upfront costs or long-term commitments.

▶ Getting started with Internet Monitor

View documentation [i]

Synthetic Monitor (layer 4)

- visibility into the performance of the network connecting your AWS hosted applications to your on-premises destinations, and allows you to identify the source of any network performance degradation within minutes.



CloudWatch > Network Synthetic Monitor

CloudWatch <

Favorites and recents ▶

Dashboards

▶ AI Operations New

▶ Alarms ⚠ 2 ⓘ 49 ⚡ 6

▶ Logs ⚠

▶ Metrics New

▶ Application Signals New (APM)

▶ GenAI Observability New

▼ Network Monitoring

Flow monitors

Internet monitors

Synthetic monitors

▶ Insights

Settings

Telemetry config

Getting Started

What's new

Network Synthetic Monitor

▶ Getting started with Network Synthetic Monitor Info

Monitors (4) Info Actions AWS Health Dashboard Create monitor

Name	AWS Network Health I...	Probes in alarm	State
cross-az	Healthy	-	Active
cross-region	Healthy	-	Active
multi-probe	Healthy	-	Active
on-prem	Healthy	-	Active

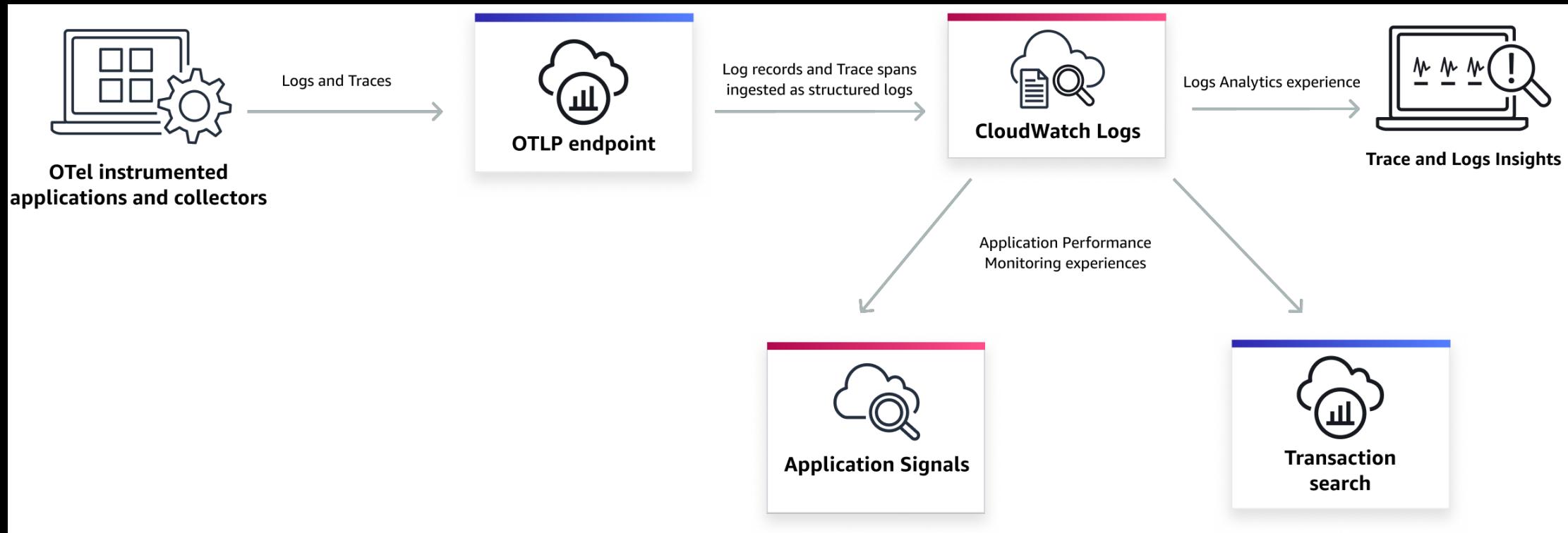


OpenTelemetry



© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved. Amazon Confidential and Trademark.

OpenTelemetry



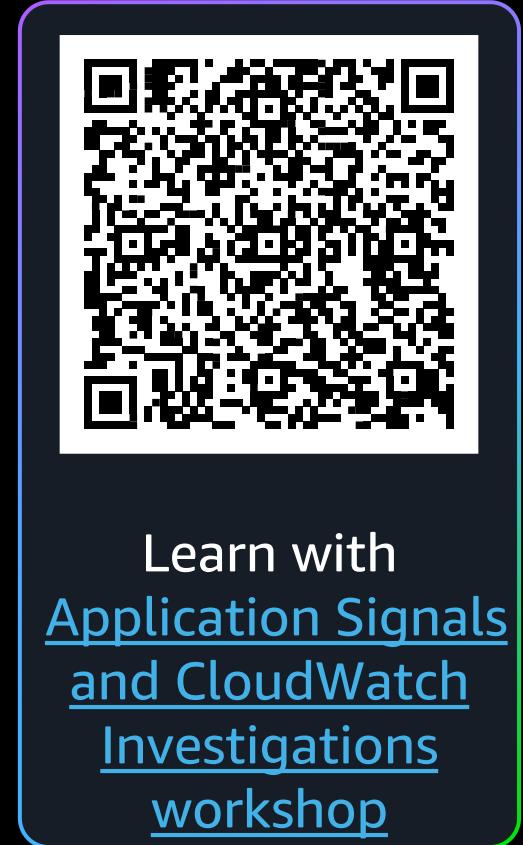
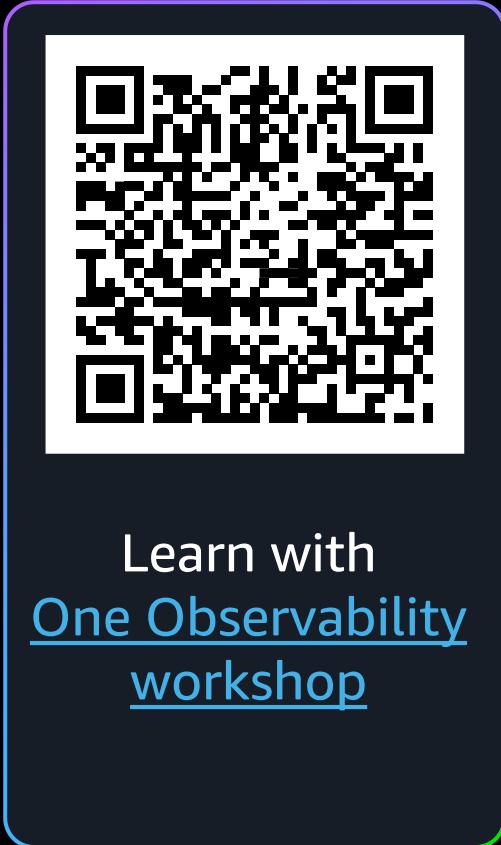
Traces endpoint: <https://xray.AWS Region.amazonaws.com/v1/traces>

Logs endpoint: <https://logs.AWS Region.amazonaws.com/v1/logs>

Metrics endpoint: ???



Resources



Thank you!



Joe Alioto

Sr. Solutions Architect
AWS CloudOps

 /josephalioto