I didn’t know Amazon CloudWatch could do that!

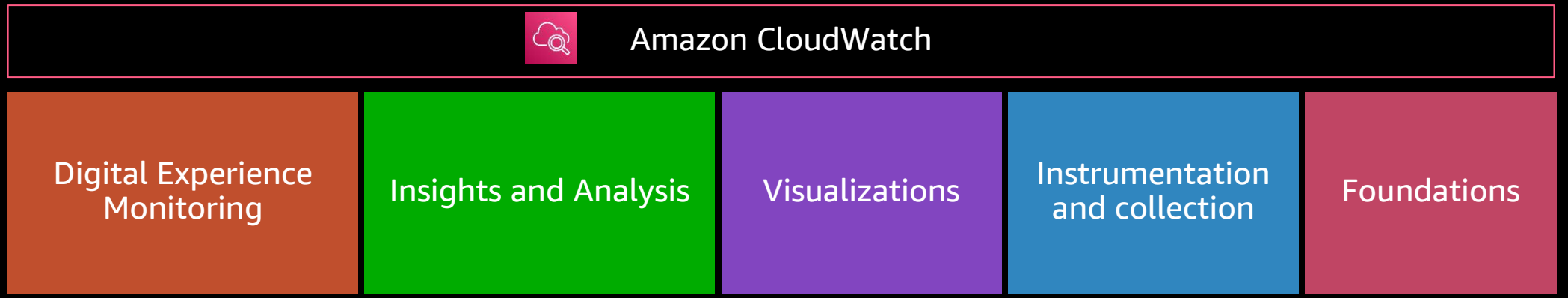
Joe Alioto
Sr. Solutions Architect
AWS CloudOps

Agenda

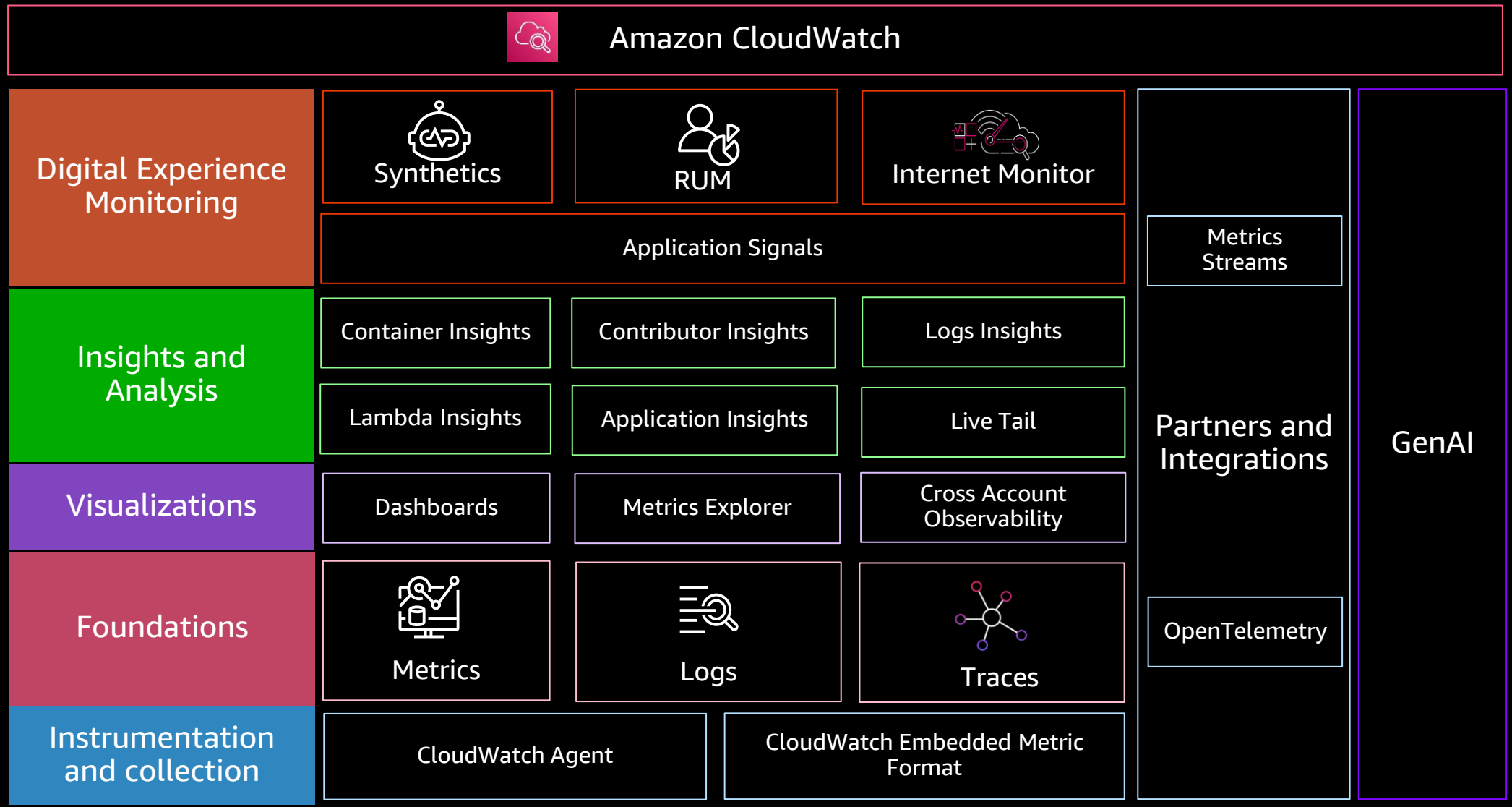
Amazon CloudWatch and all the features! (*as many as I can show before I run out of breath*)

Resources

BREADTH AND DEPTH NATIVE OBSERVABILITY



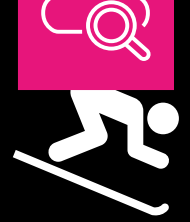
BREADTH AND DEPTH NATIVE OBSERVABILITY



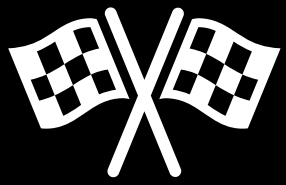
What areas?

- 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



SECTION

Feature

- Important points

https://url_that_points_to_documentation_same_as_qr_code

SECTION

Feature

- Important points

https://url_that_points_to_documentation_same_as_qr_code

SECTION

Feature

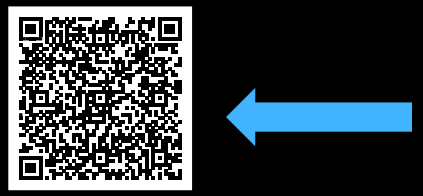
- Important points 

https://url_that_points_to_documentation_same_as_qr_code

SECTION

Feature

- Important points



https://url_that_points_to_documentation_same_as_qr_code

SECTION

Feature

- Important points

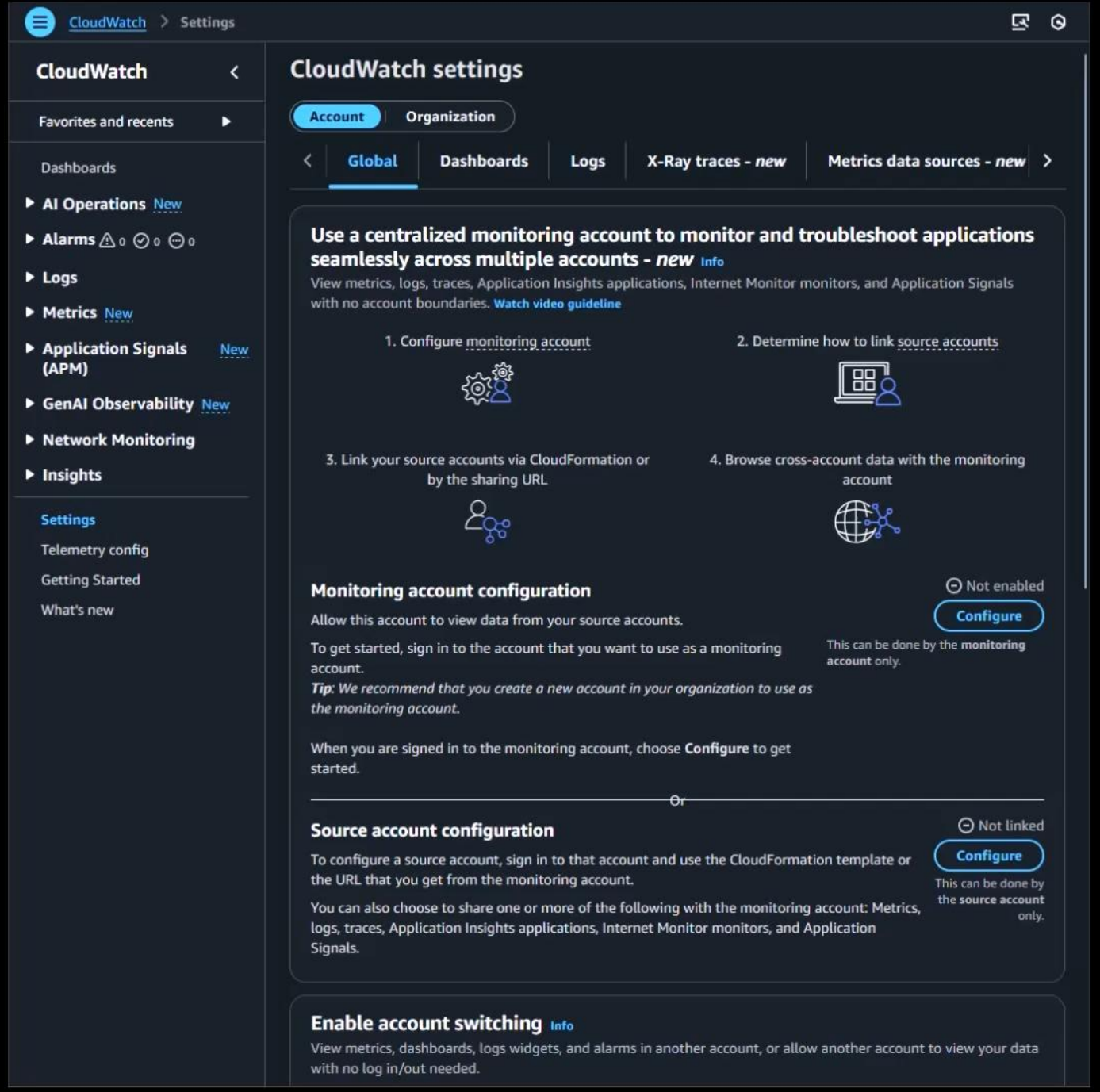
https://url_that_points_to_documentation_same_as_qr_code

Centralized Observability

CENTRALIZED OBSERVABILITY

Log centralization

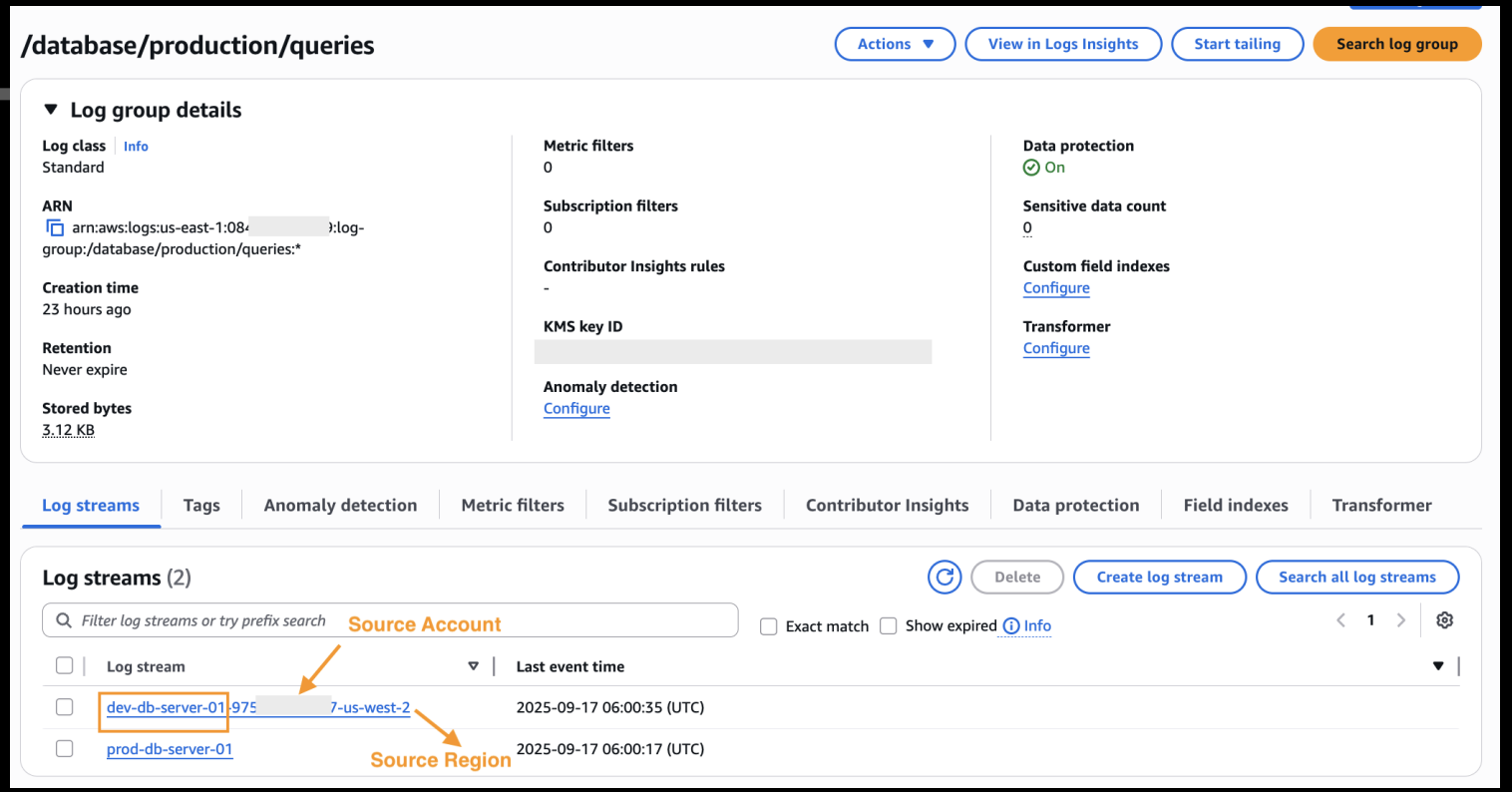
- Cross-account & cross-region log centralization
- Region and account metadata added to logs and streams
- First copy is **FREE**
- **O**ther copies are $0.05/GB



https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CloudWatchLogs_Centralization.html

Log centralization

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

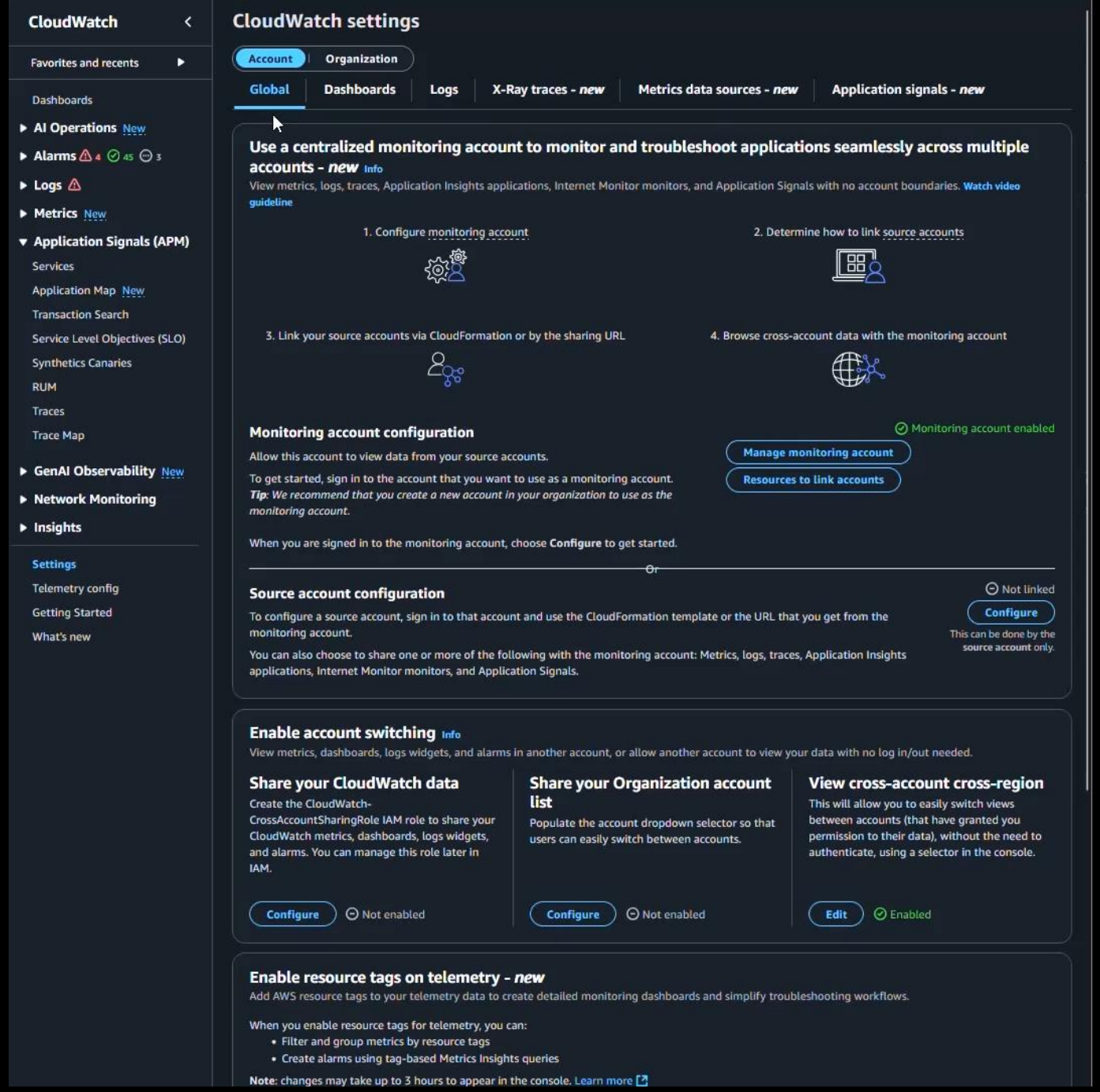


https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CloudWatchLogs_Centralization.html

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



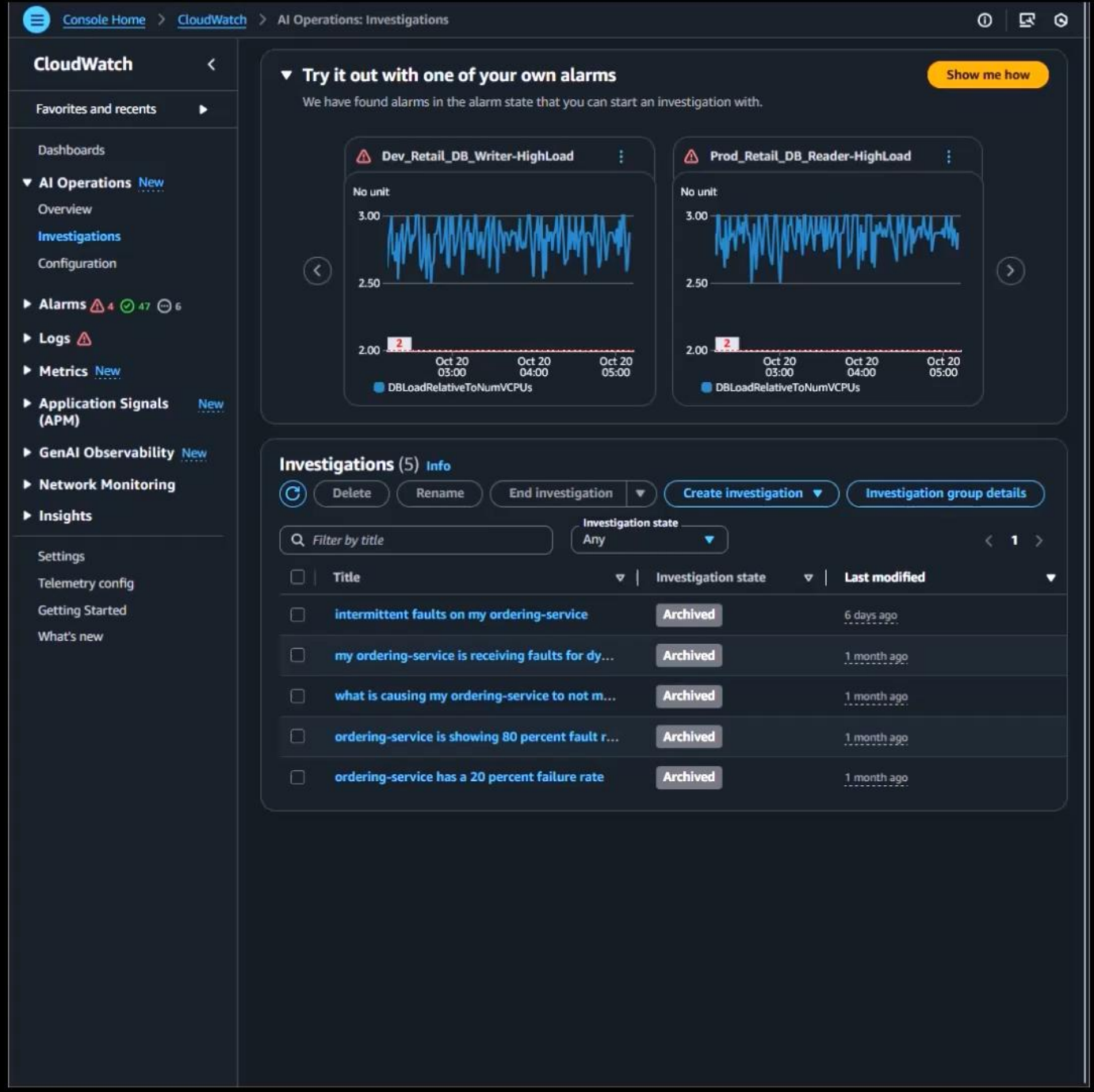
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch-Cross-Account-Methods.html

AI Operations

AIOPS

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

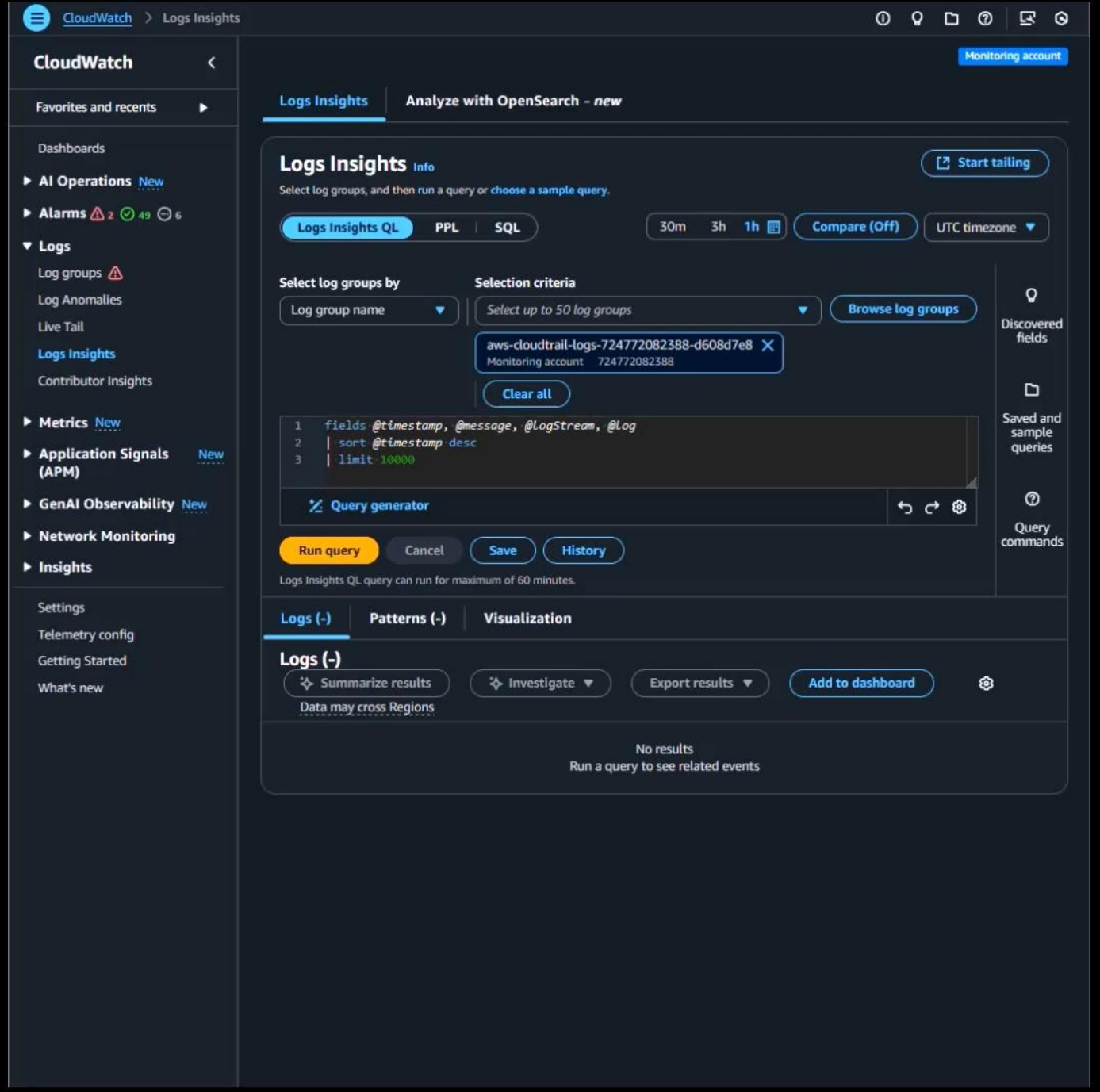


https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/Investigations.html

AIOPS

Log Insights Query Generation

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

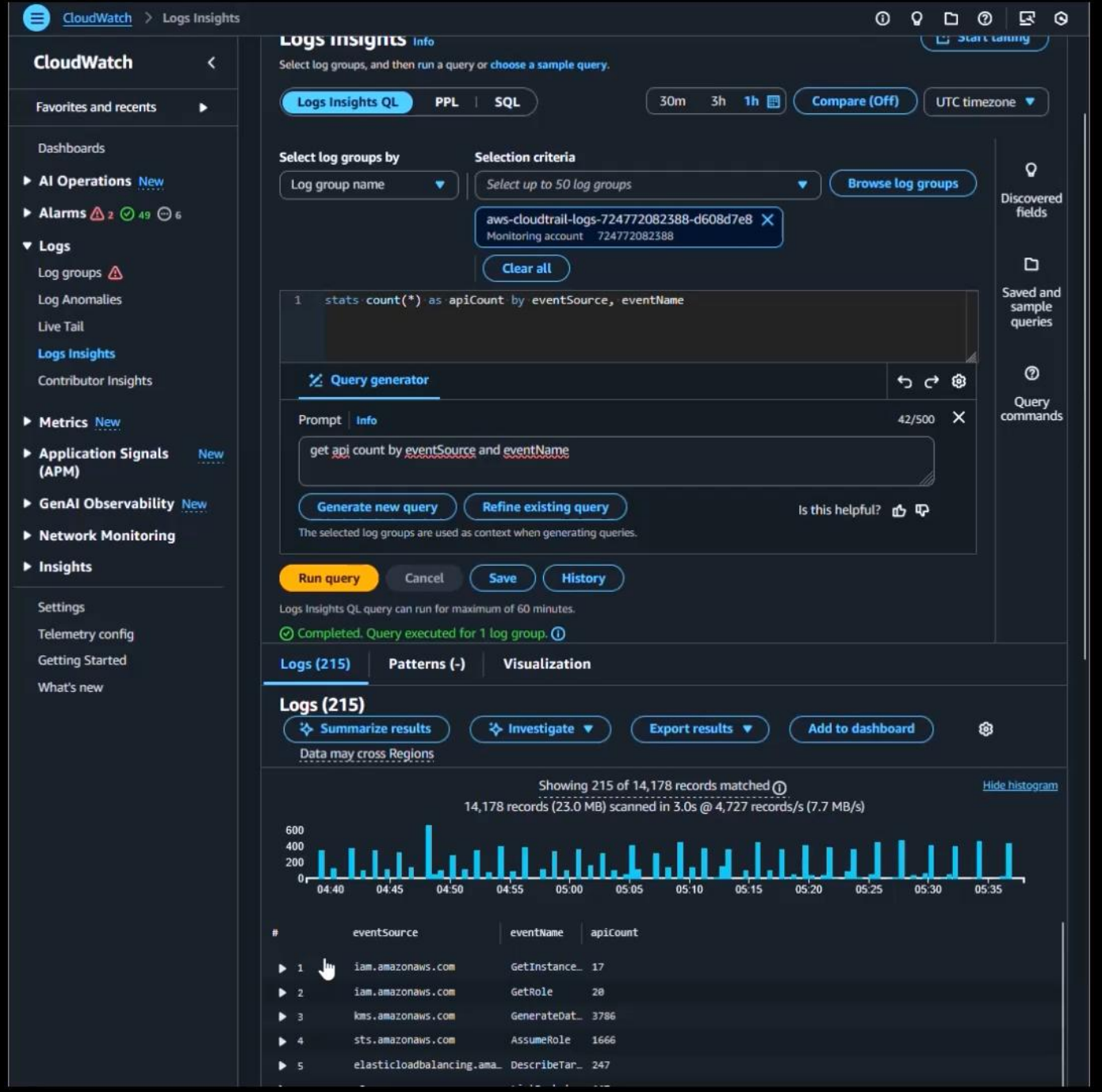


https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CloudWatchLogs-Insights-Query-Assist.html

AIOPS

Log Insights results summarization

- Summarize log results into human readable paragraph

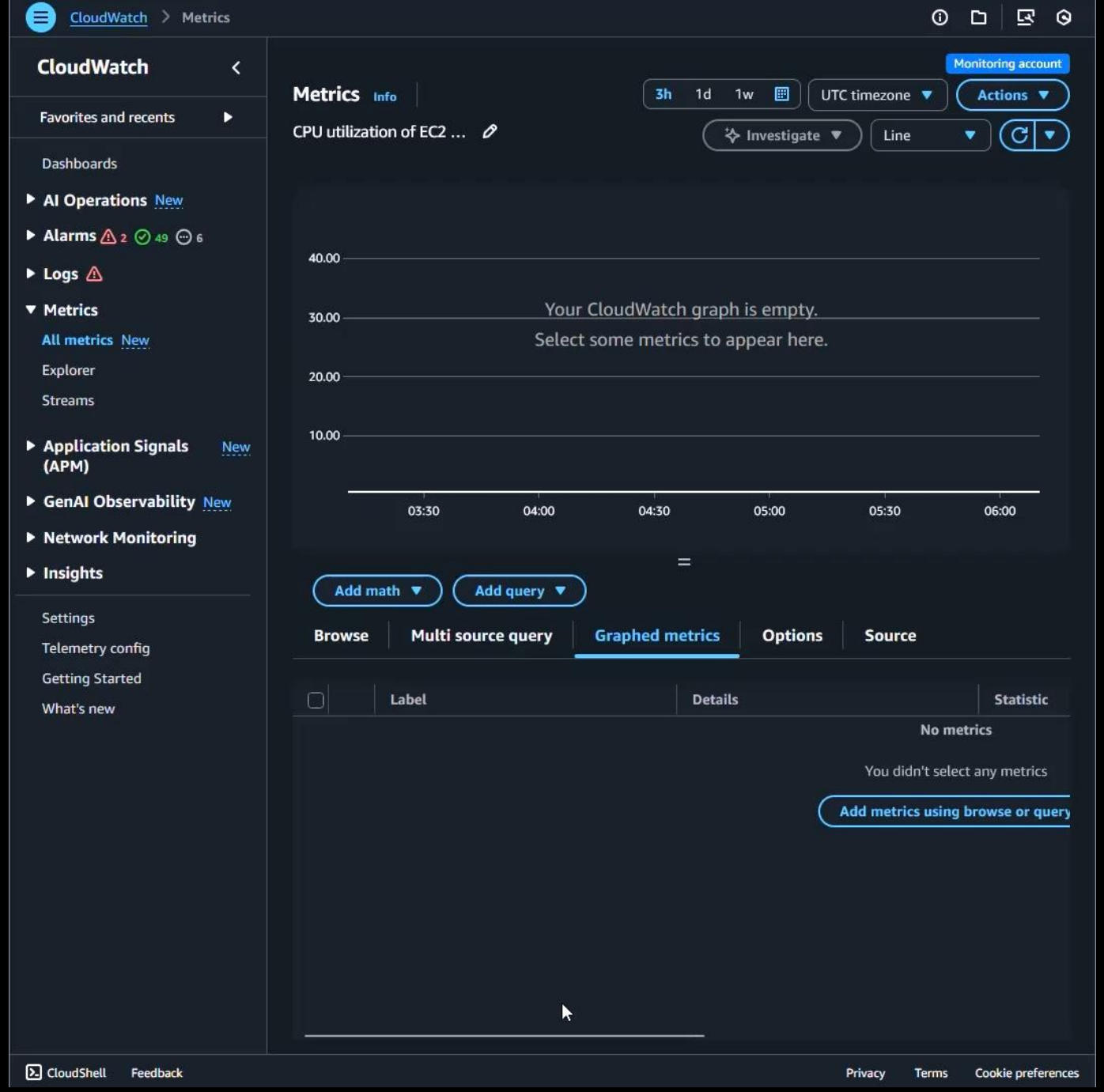


https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CloudWatchLogs-Insights-Query-Results-Summary.html

AIOPS

Metrics query generator

- Generate metric queries using natural language

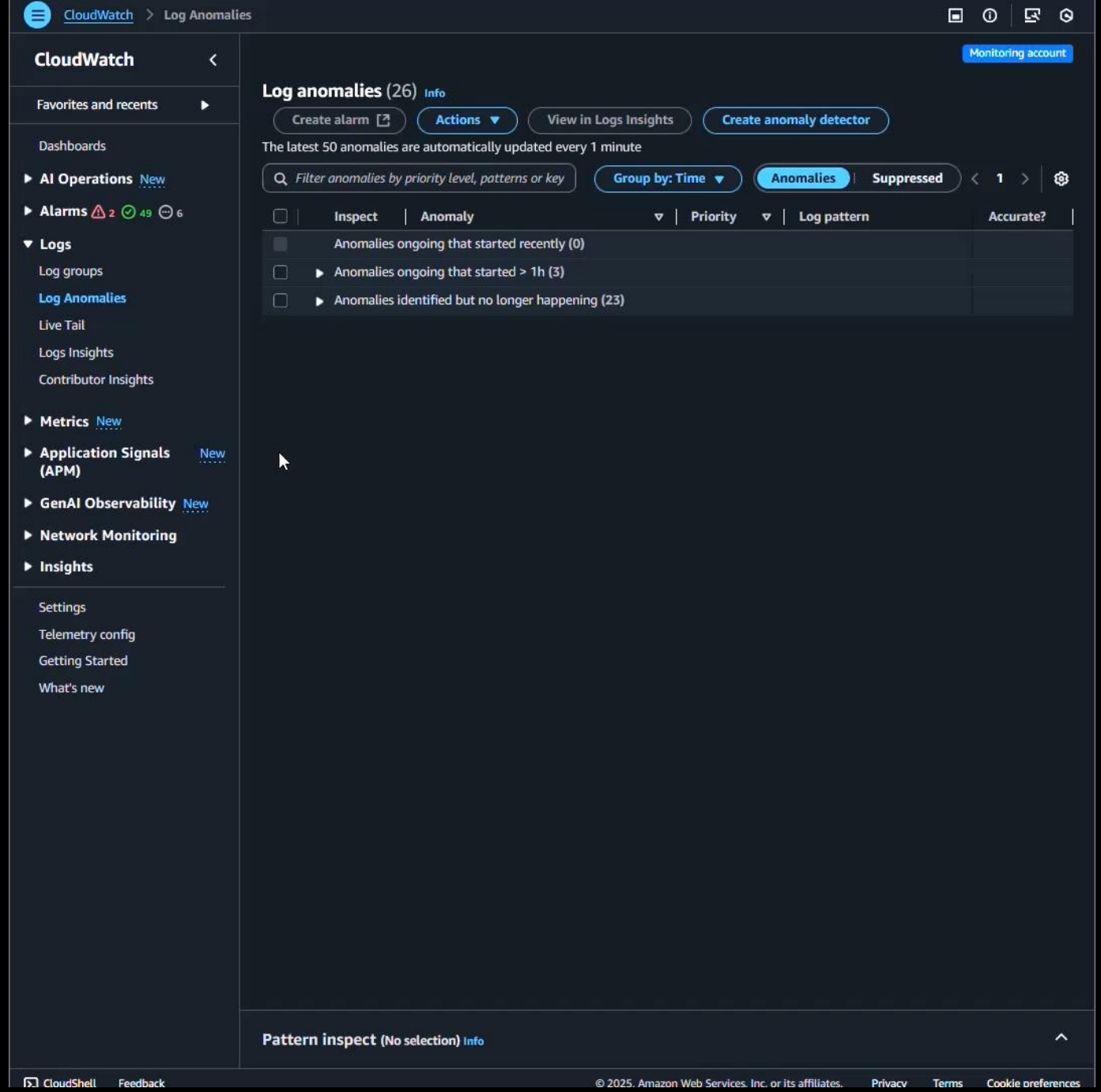


https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/cloudwatch-metrics-insights-query-assist.html

AIOPS

Anomaly Detection for logs

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

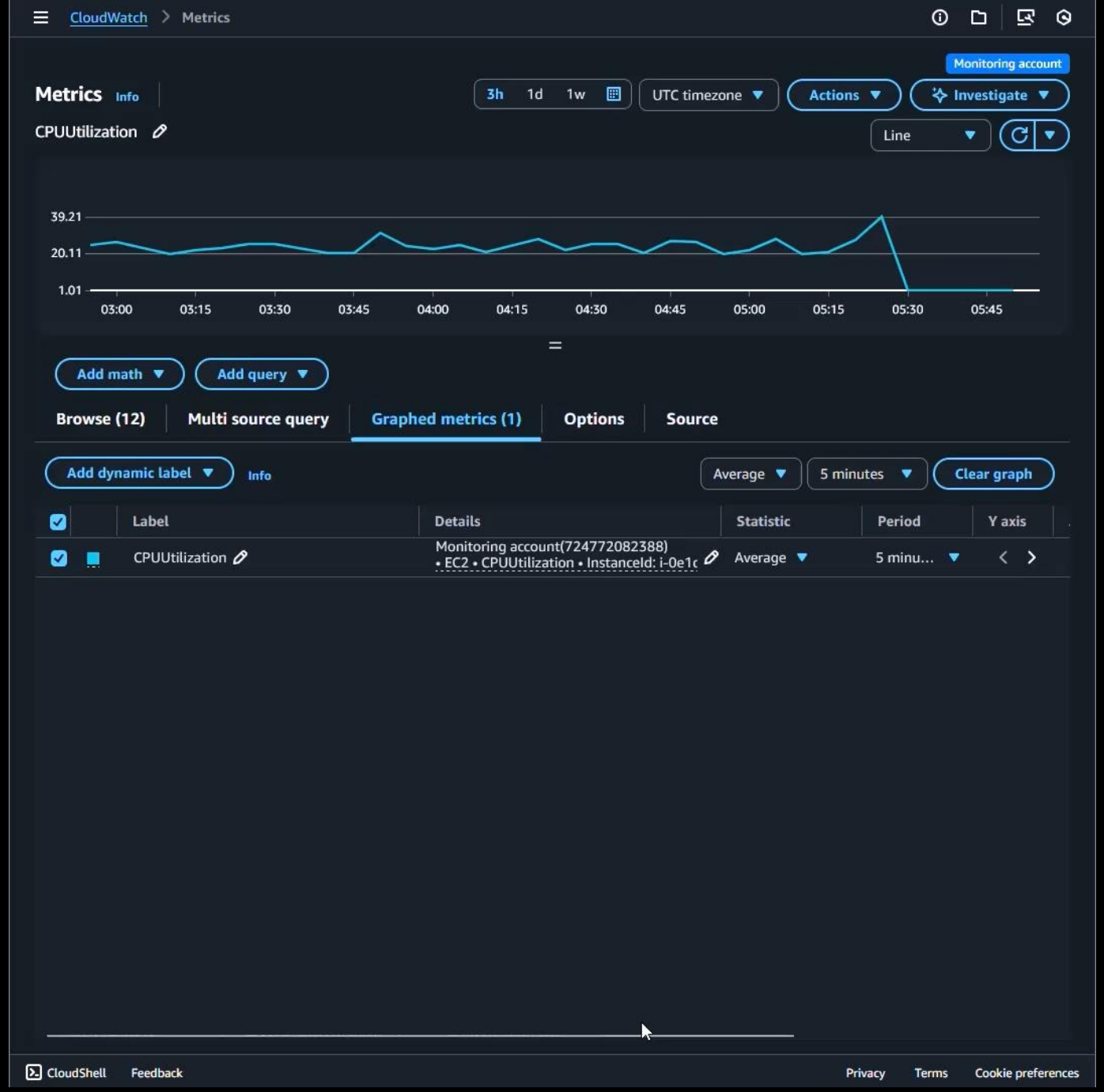


https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/LogsAnomalyDetection.html

AIOPS

Anomaly Detection for metrics

- anomaly detection for metrics
- **Set thresholds to compare**

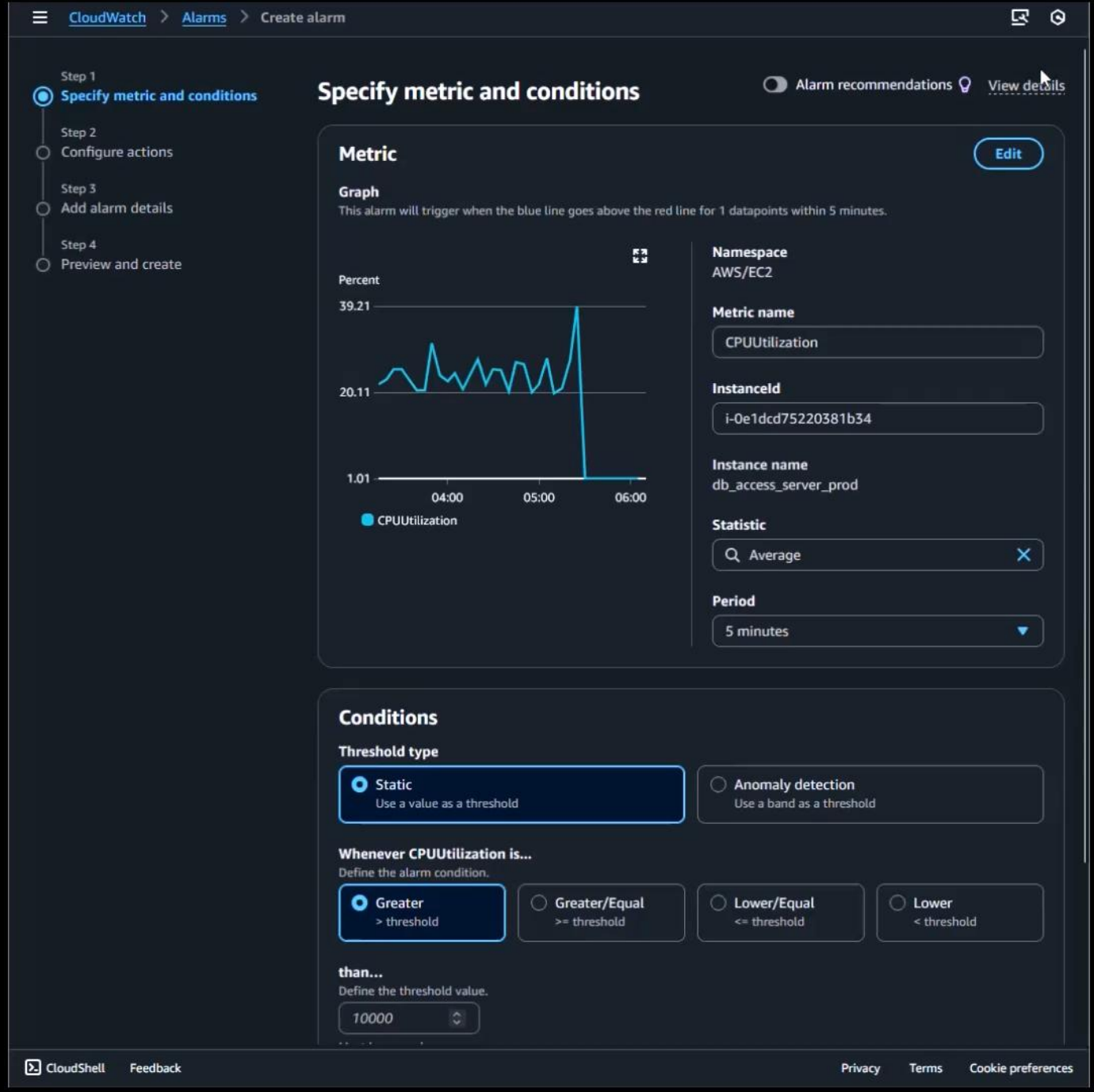


https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch_Anomaly_Detection.html

AIOPS

Anomaly Detection for alarms

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



https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/Create_Anomaly_Detection_Alarm.html

AIOPS

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

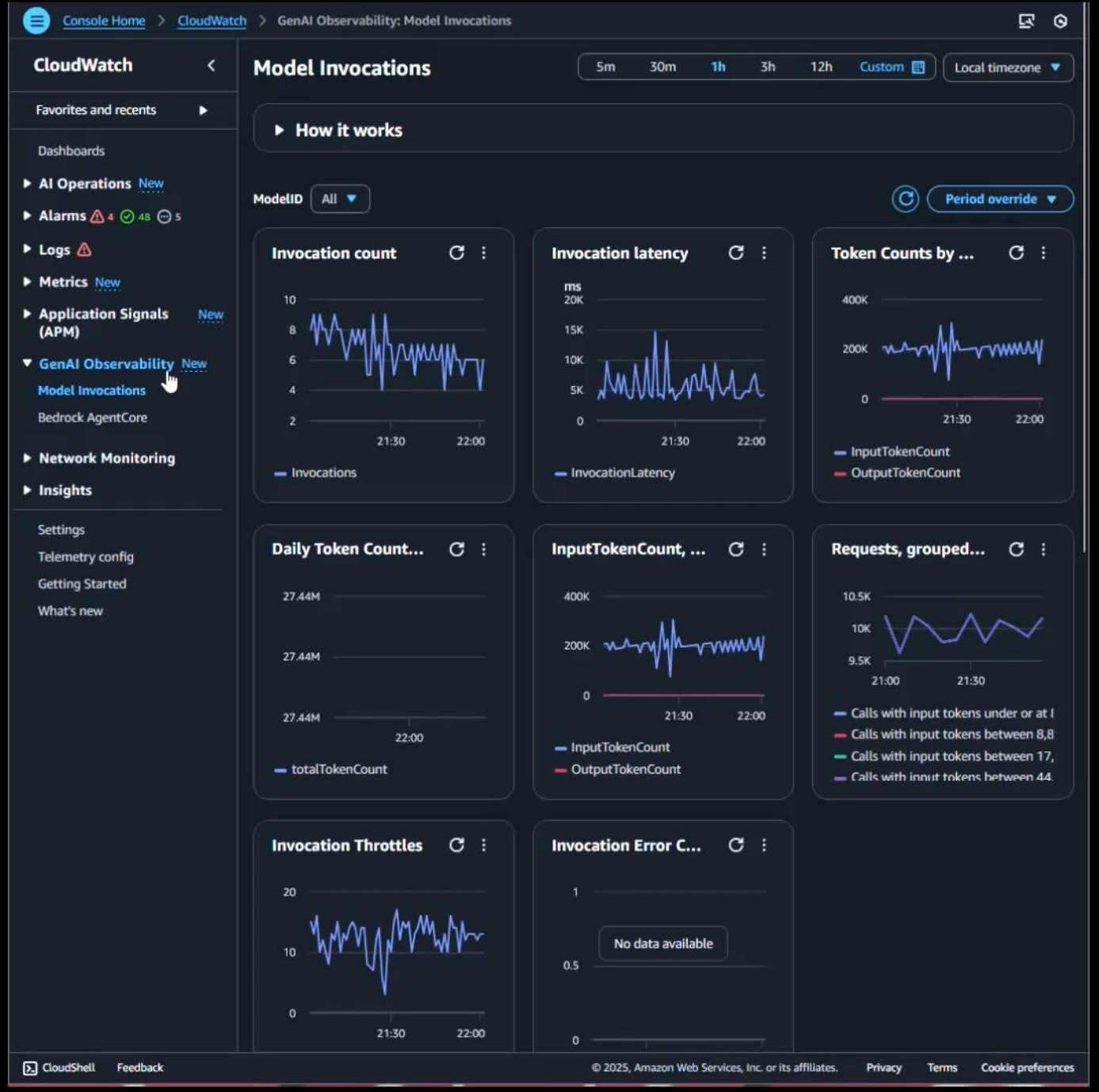
https://aws.amazon.com/blogs/mt/enhance-your-aiops-introducing-amazon-cloudwatch-and-application-signals-mcp-servers/

Gen AI Observability

GENAI OBSERAVBILITY

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



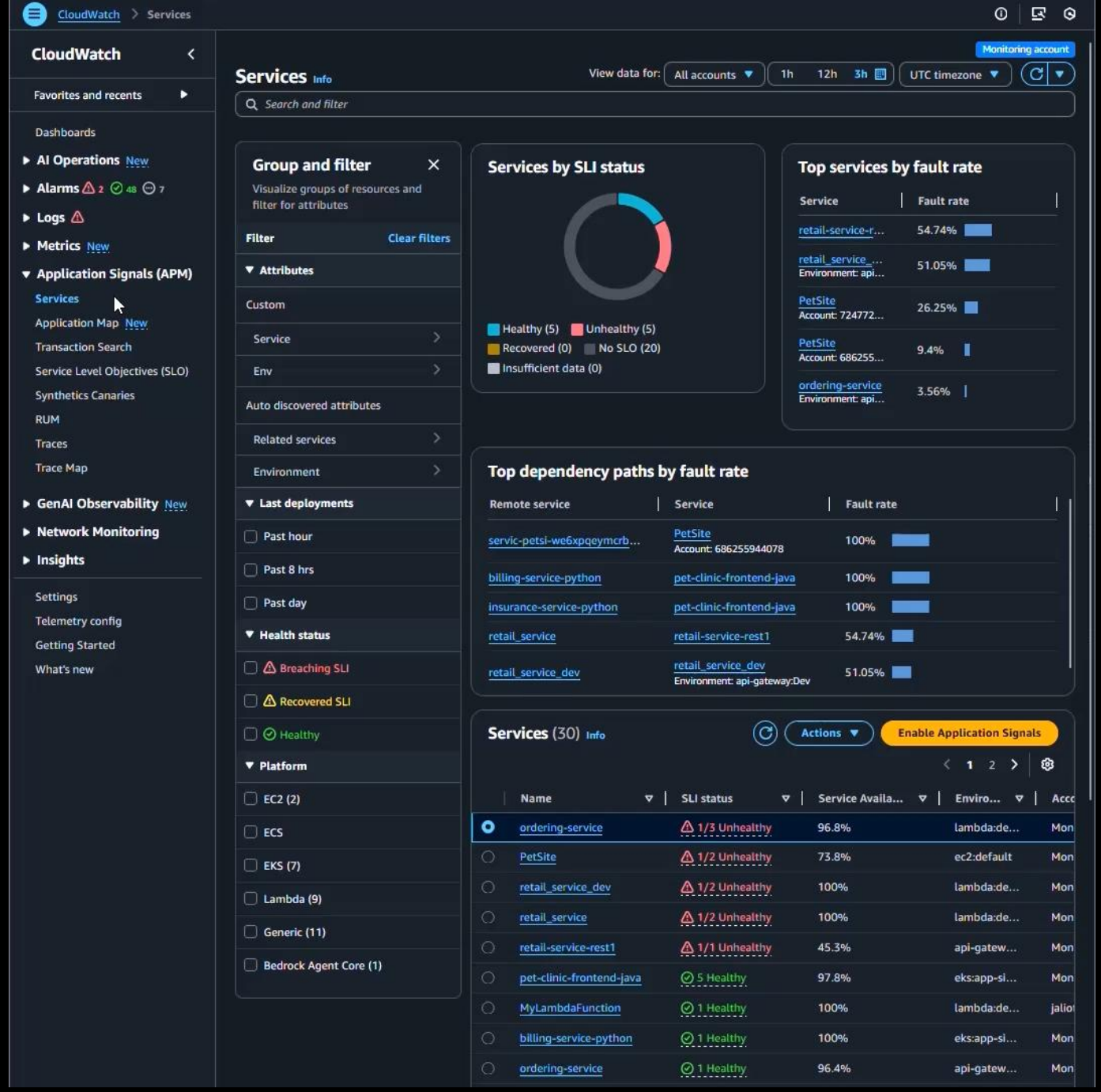
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/GenAI-observability.html

Application Signals (APM)

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

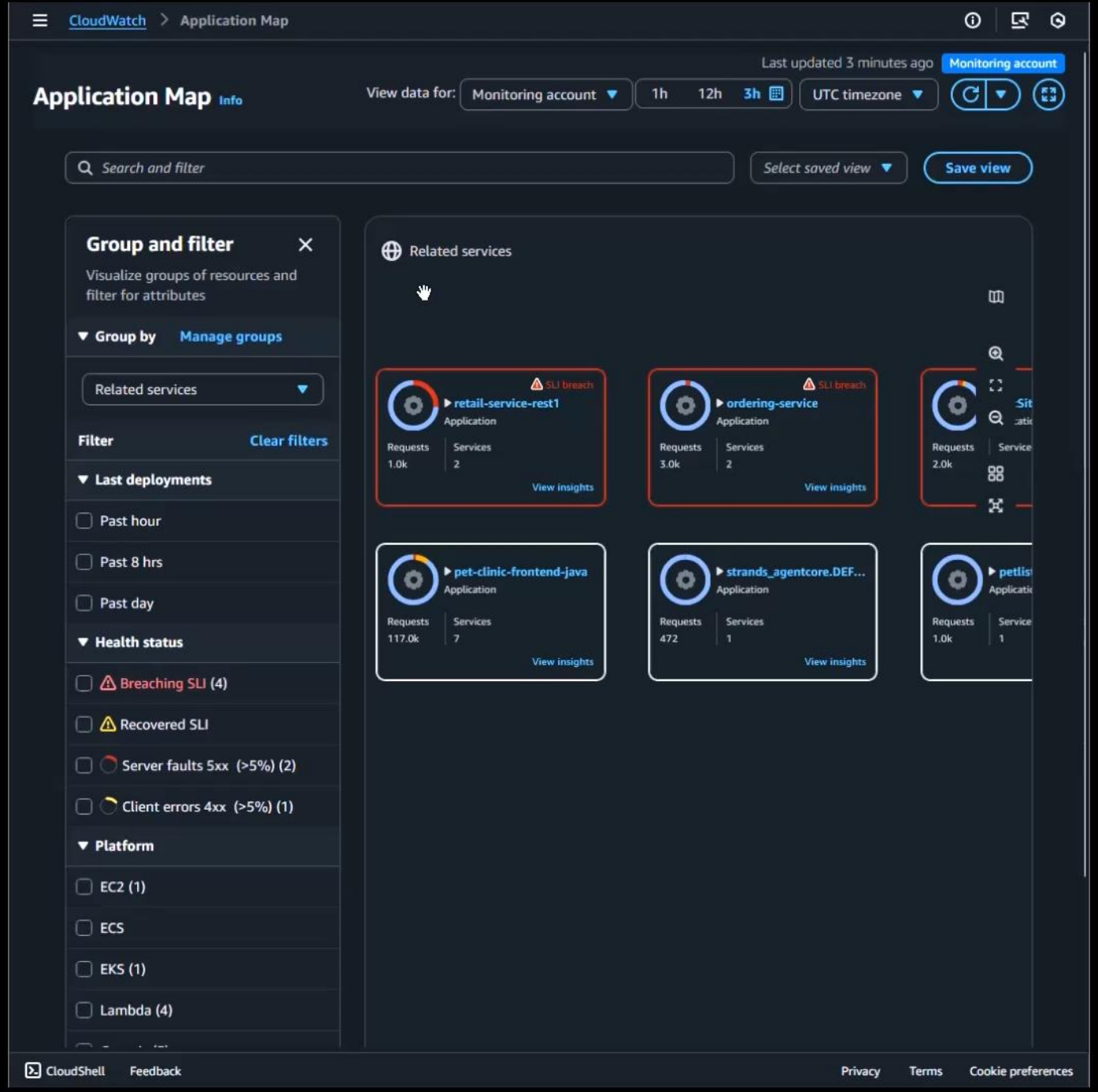


https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch-Application-Monitoring-Sections.html

APPLICATION SIGNALS (APM)

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

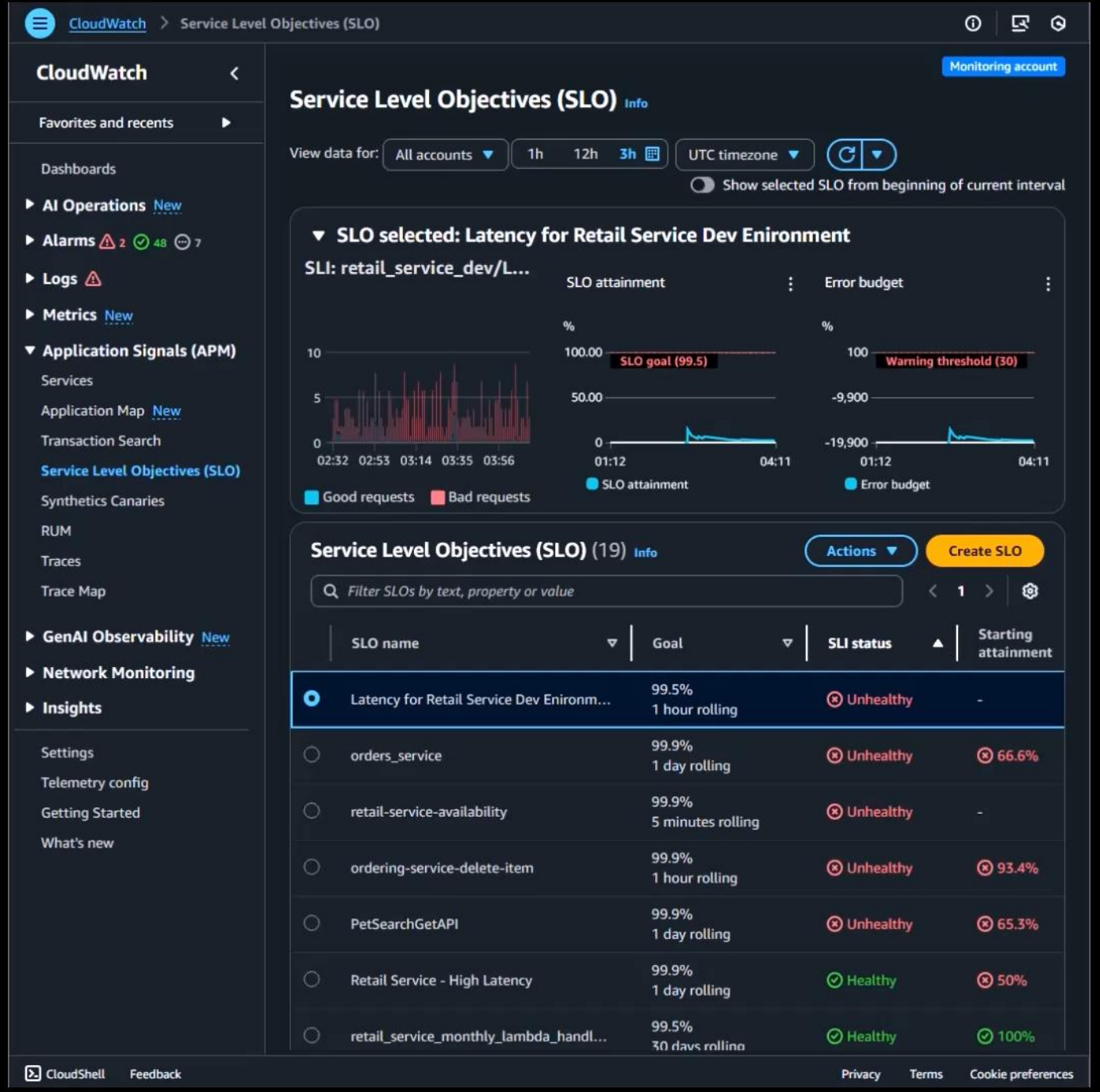


https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/ServiceMap.html

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

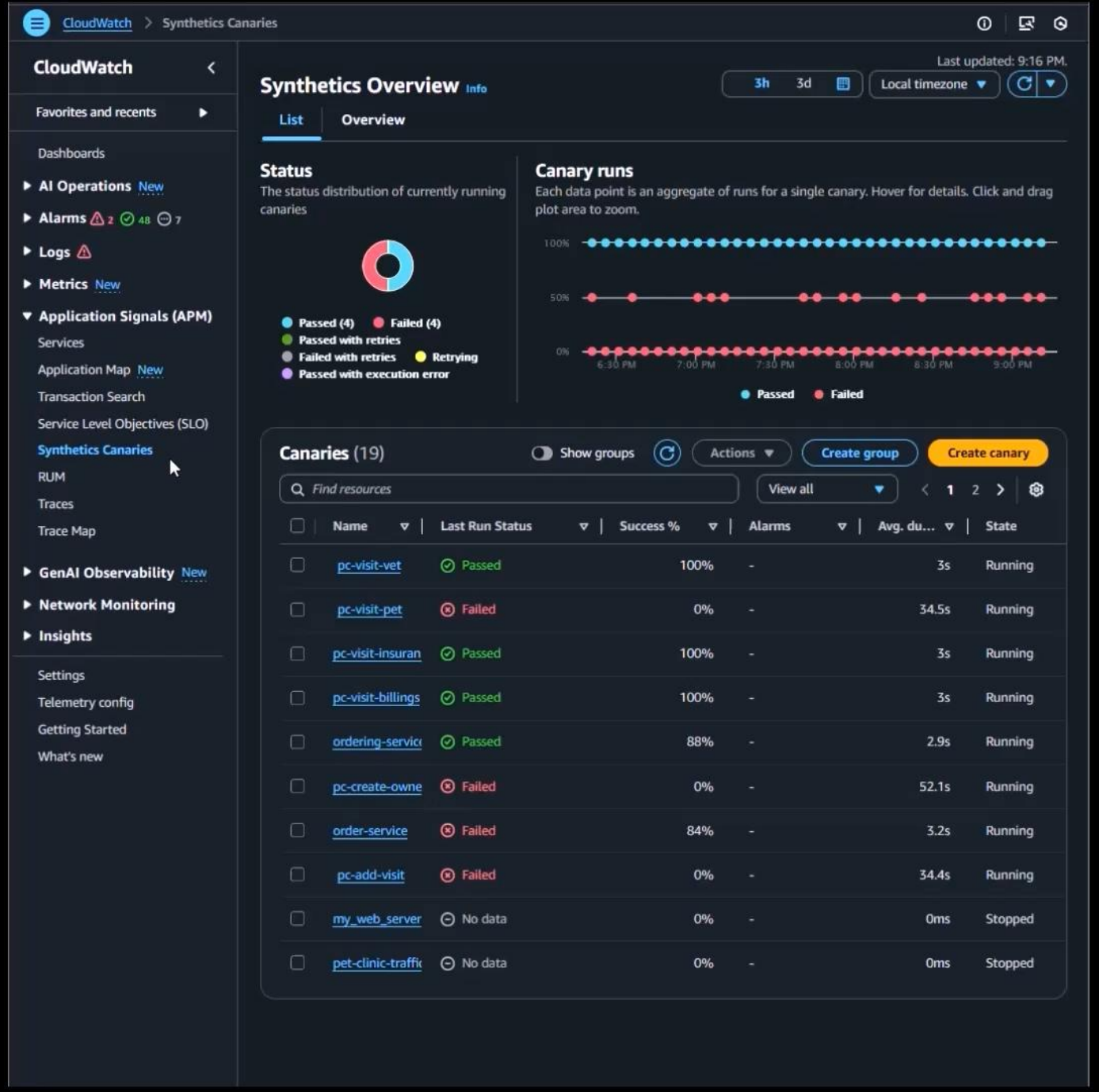


https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch-ServiceLevelObjectives.html

APPLICATION SIGNALS (APM)

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

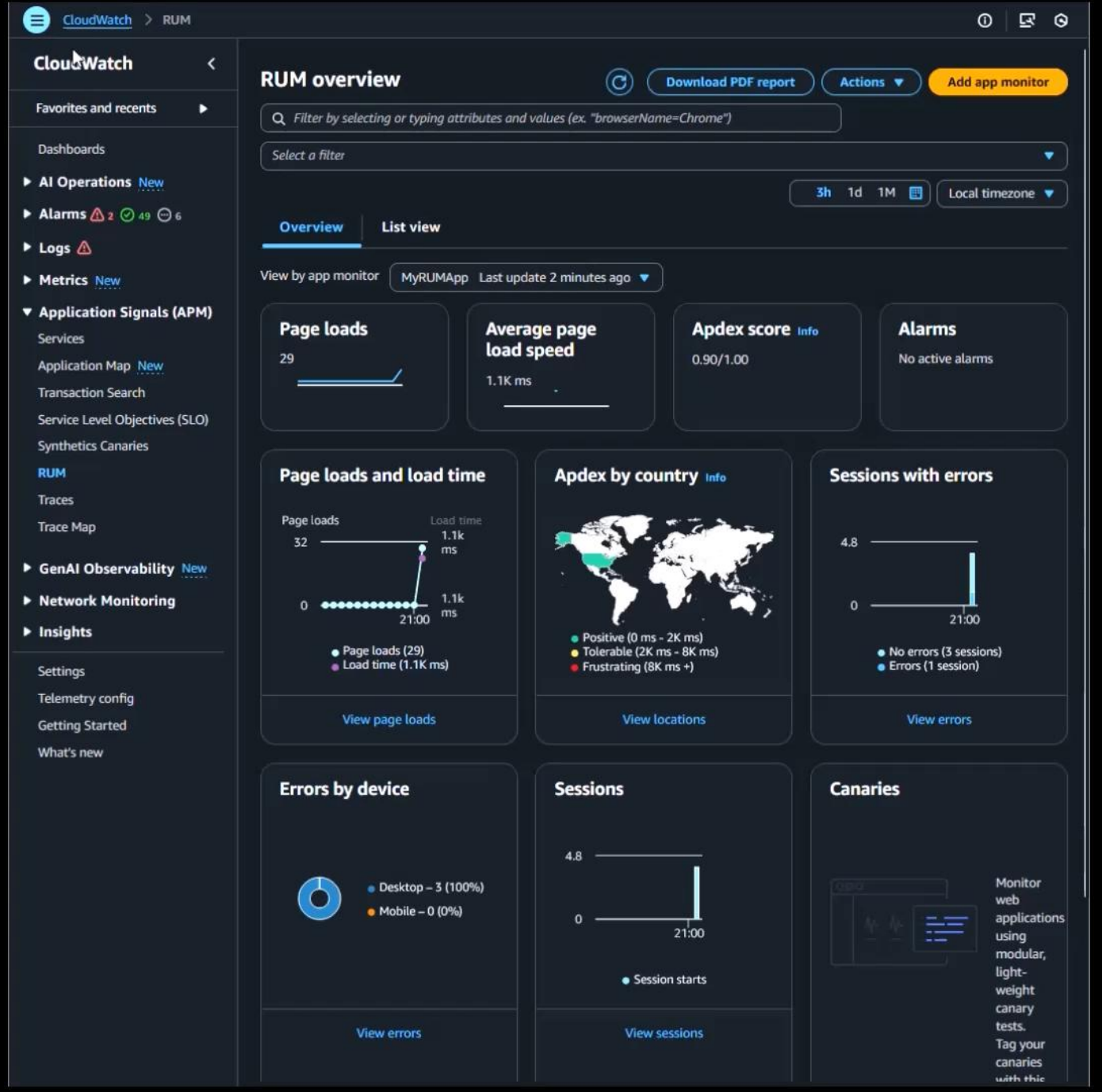


https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch_Synthetics_Canaries.html

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.



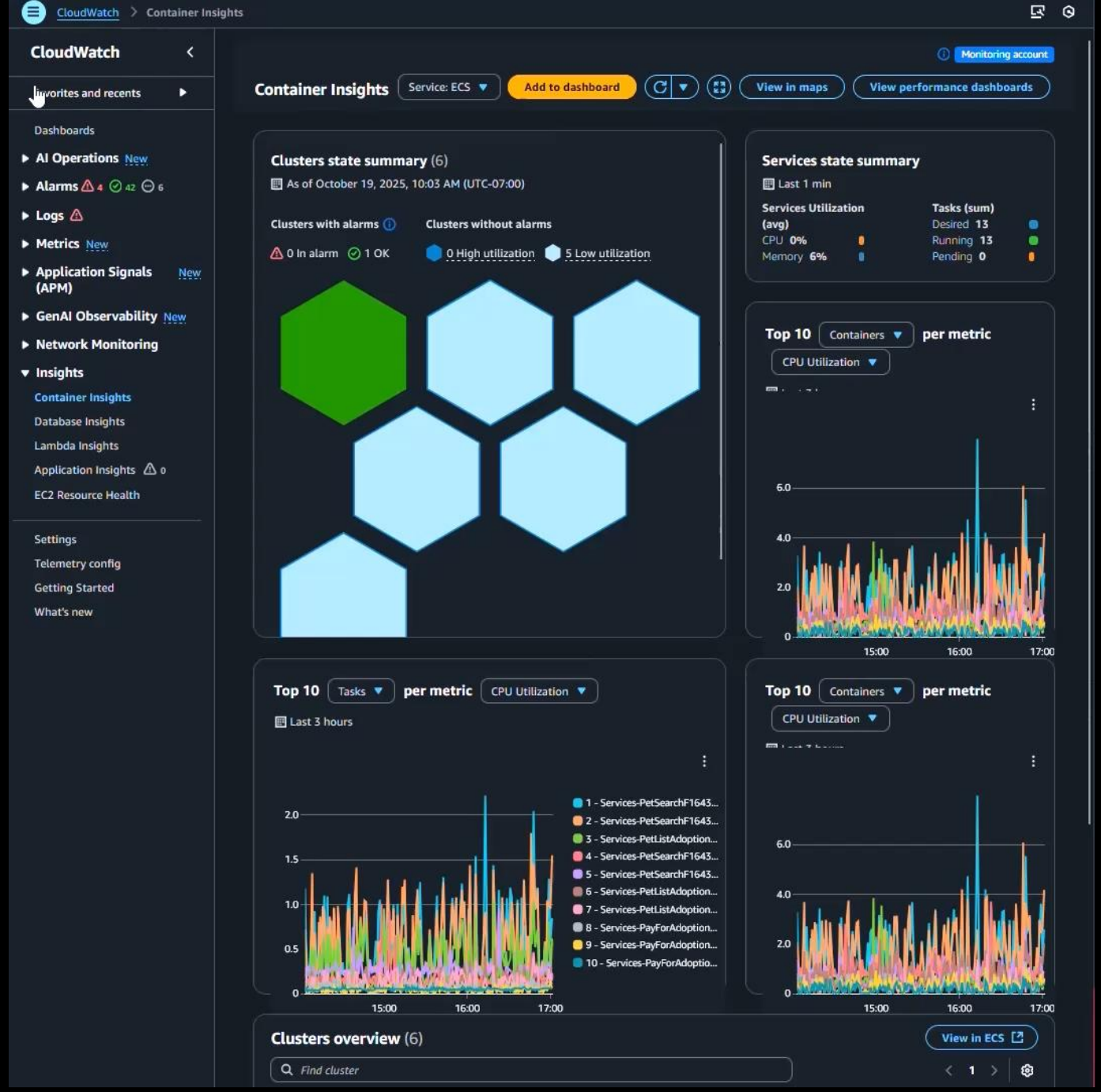
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch-RUM.html

Insights

INSIGHTS

Container Insights

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

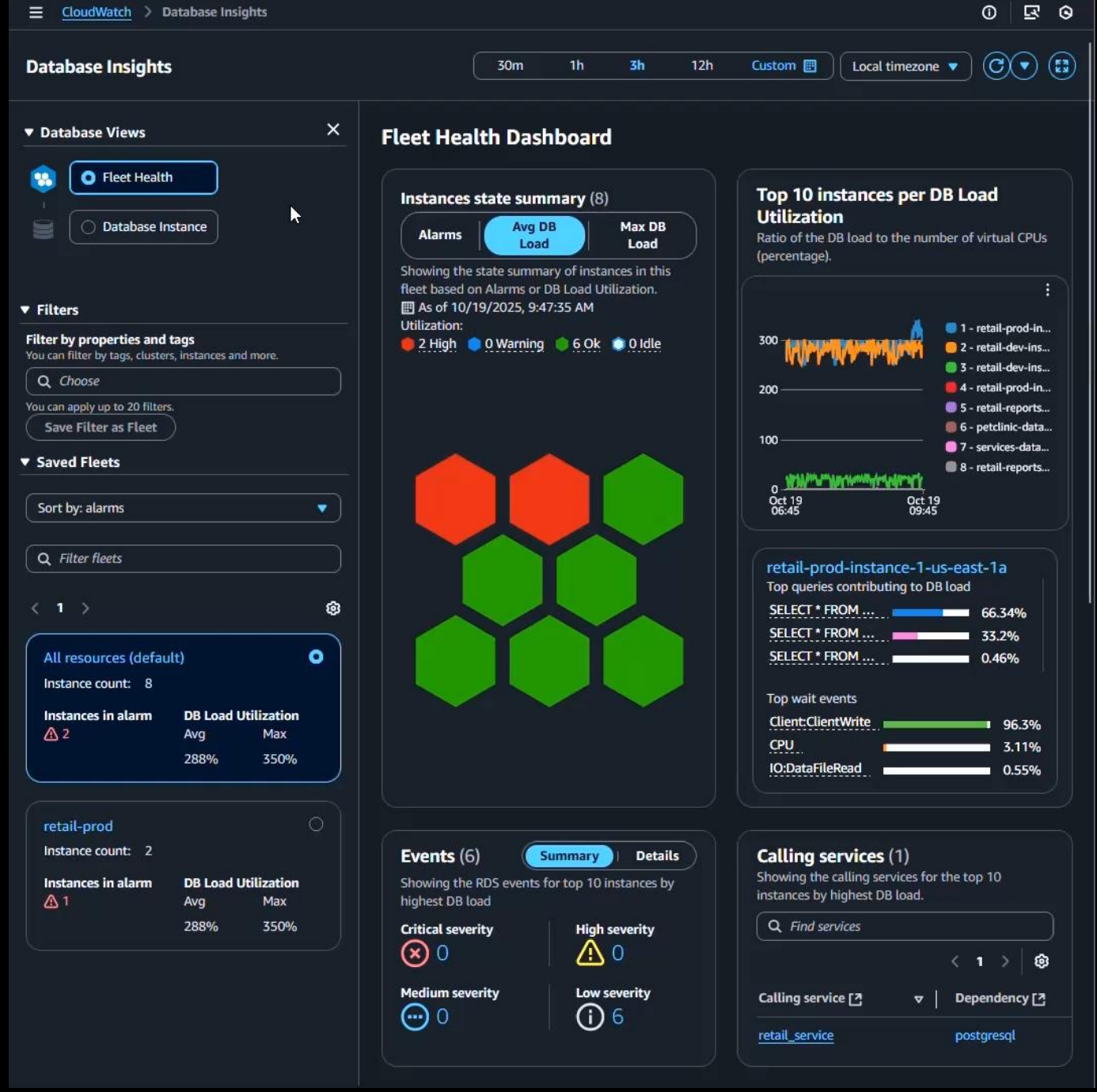


https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/ContainerInsights.html

INSIGHTS

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

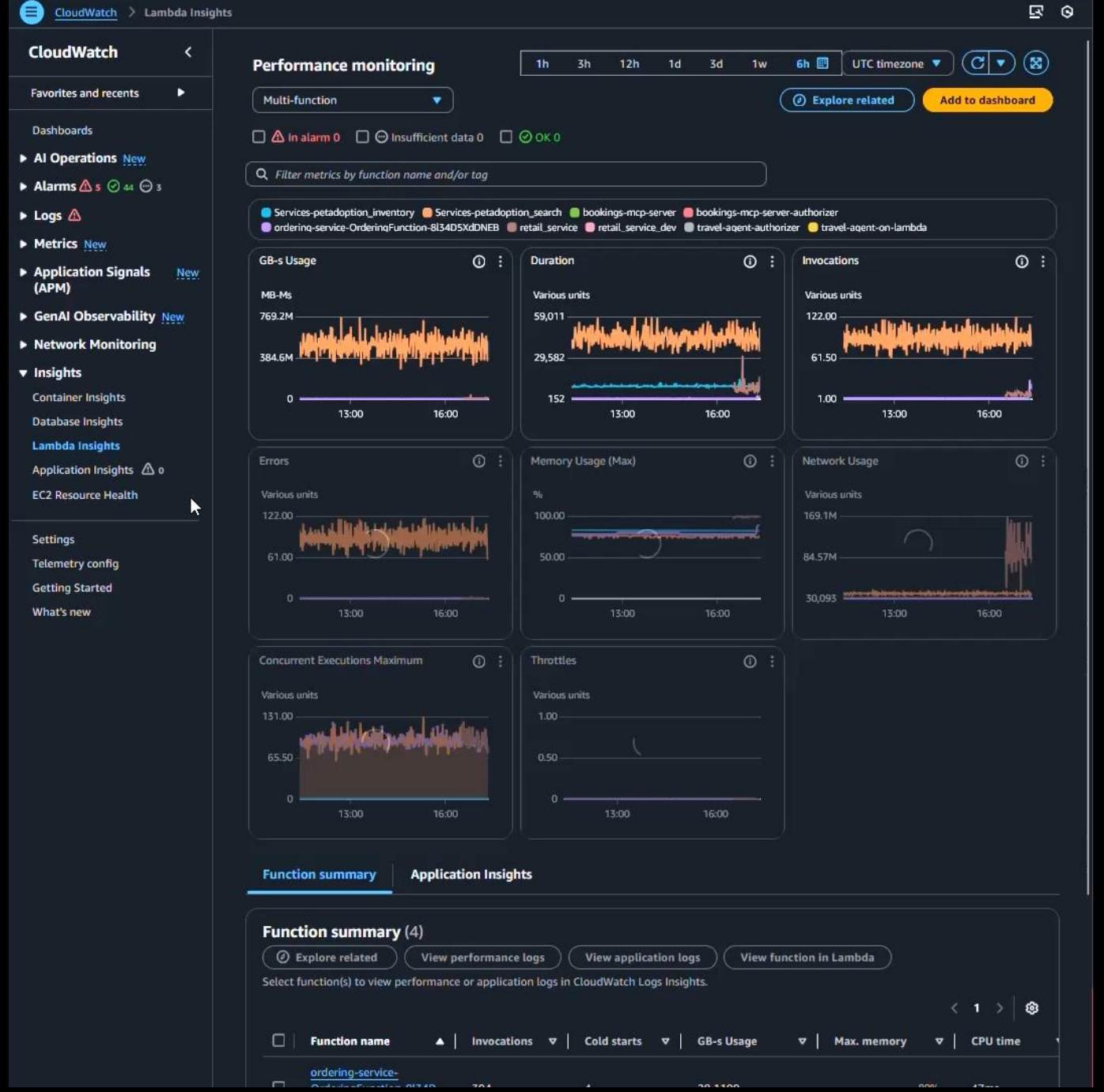


https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/Database-Insights.html

INSIGHTS

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

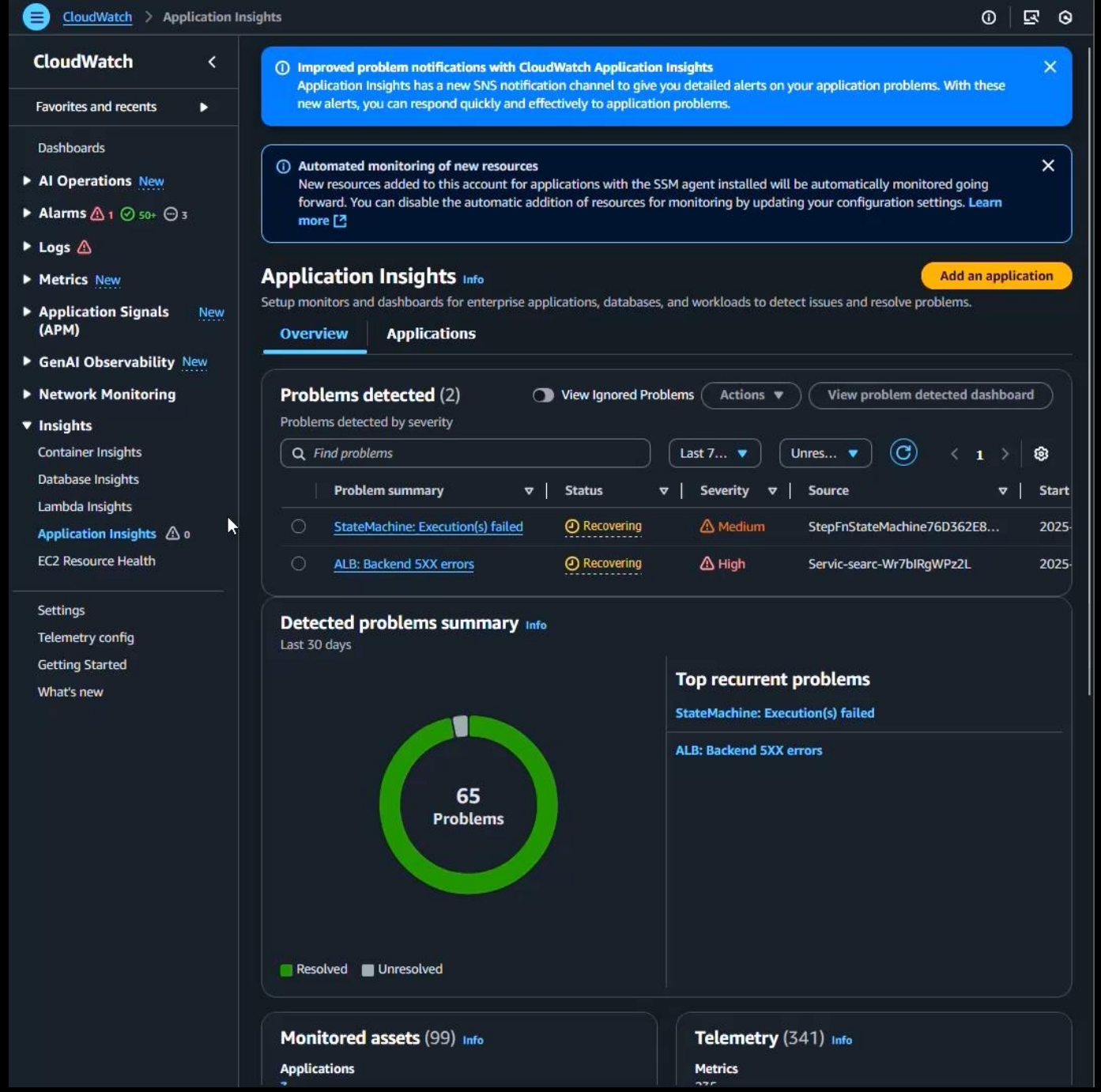


https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/Lambda-Insights.html

INSIGHTS

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

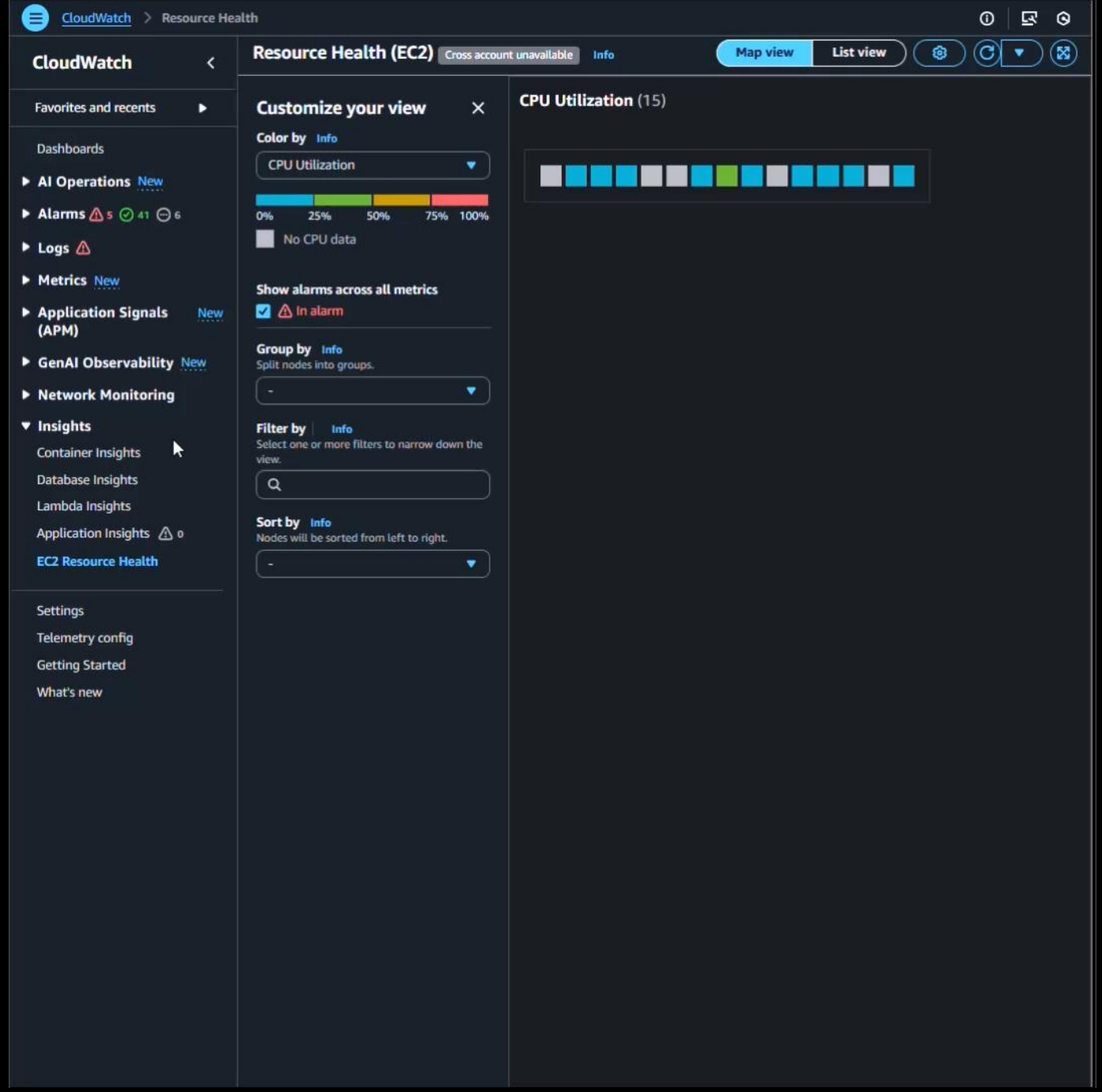


https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/cloudwatch-application-insights.html

INSIGHTS

EC2 Resource Health

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



https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/servicelens_resource_health.html

Logs

LOGS

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

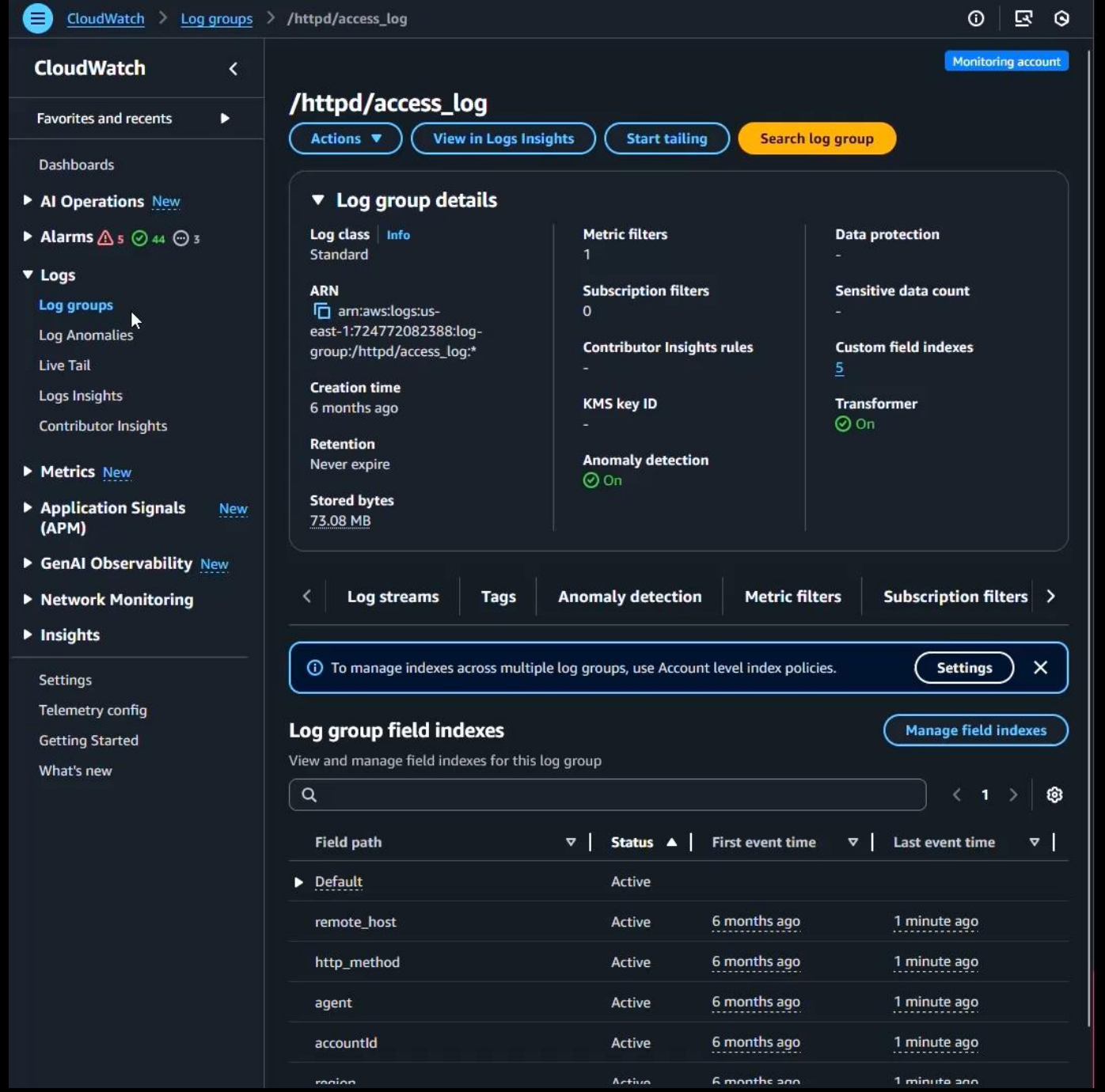
Feature	Standard $0.50/GB	Infrequent Access $0.25/GB
Fully managed log ingestion and storage	Yes ✓	Yes ✓
Cross-account features	Yes ✓	Yes ✓
Encryption with AWS KMS	Yes ✓	Yes ✓
CloudWatch Logs Insights query commands	Yes ✓	Yes ✓ (Most commands– see Logs Insights QL commands supported in log classes.)
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

https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CloudWatch_Logs_Log_Classes.html

LOGS

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

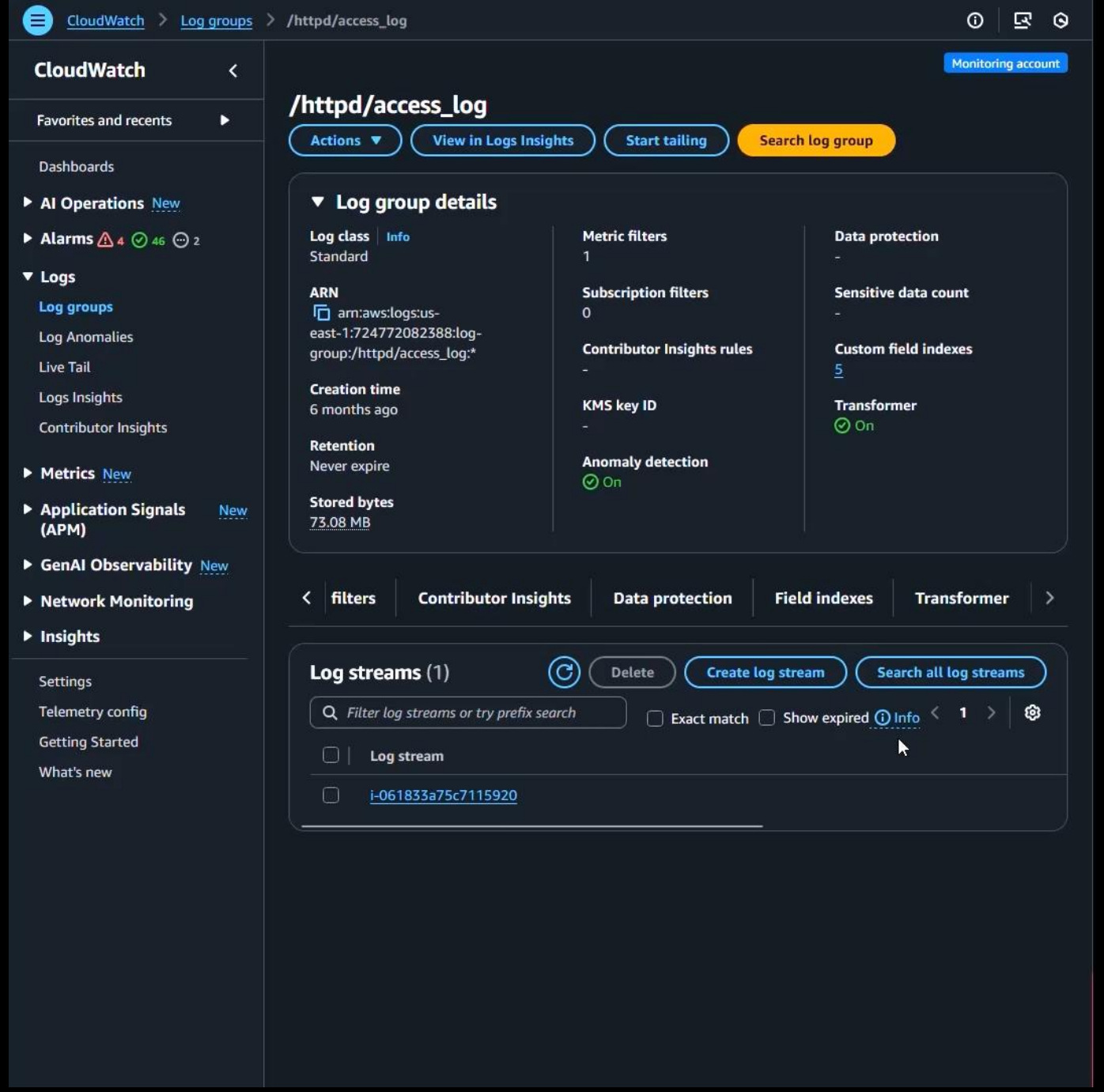


https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CloudWatchLogs-Field-Indexing.html

LOGS

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

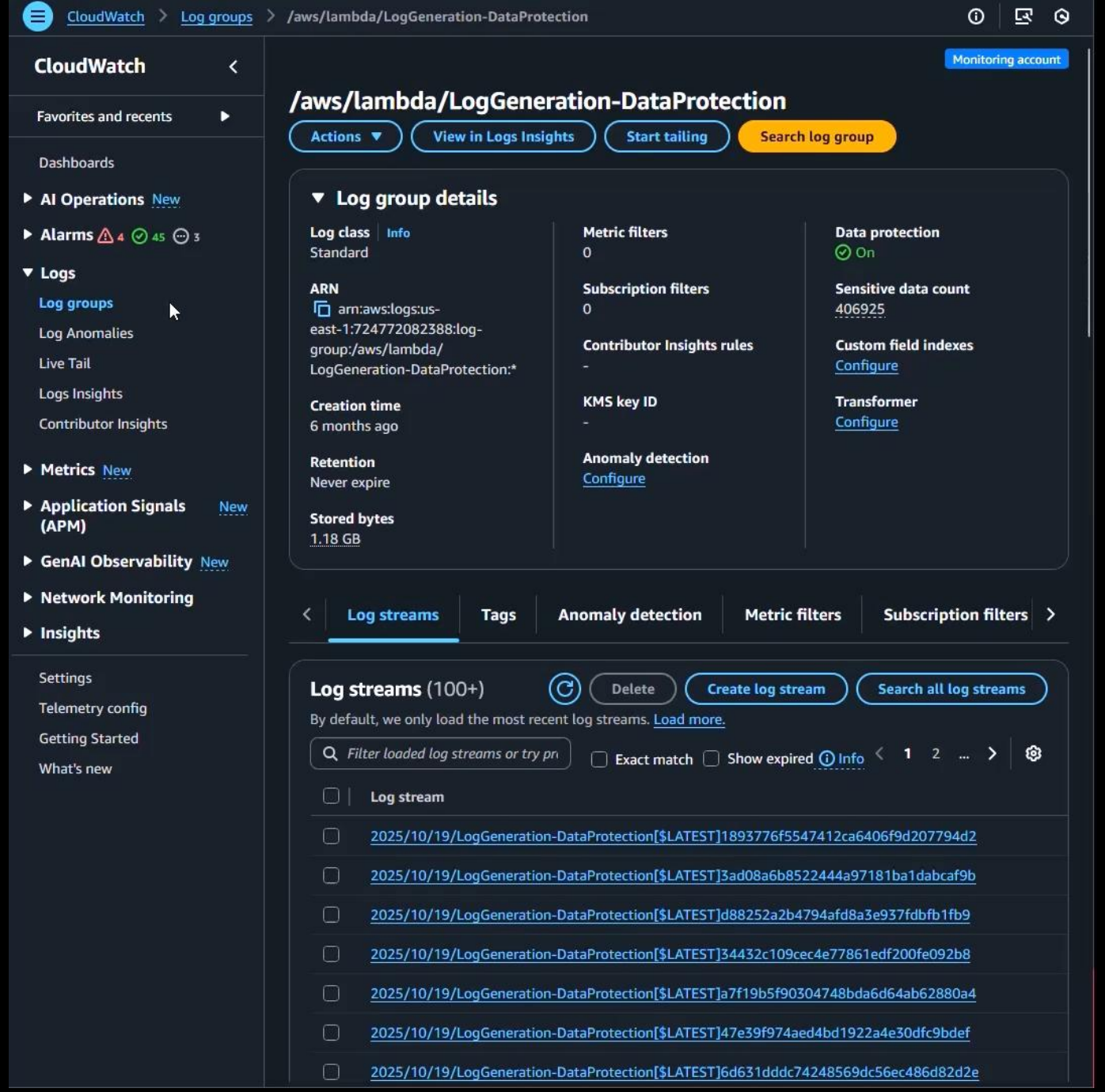


https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CloudWatch-Logs-Transformation-Create.html

LOGS

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

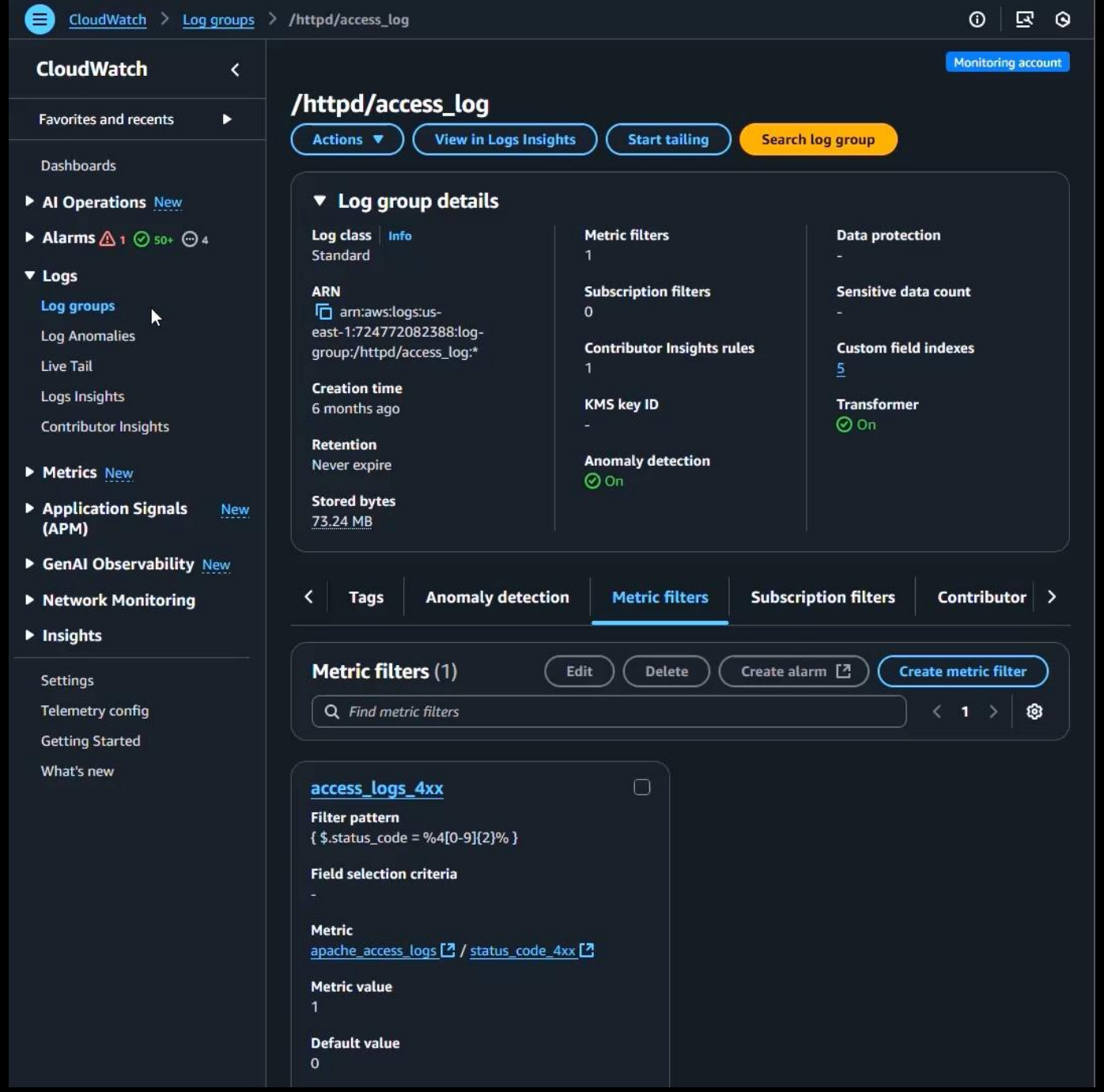


https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/mask-sensitive-log-data.html

LOGS

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

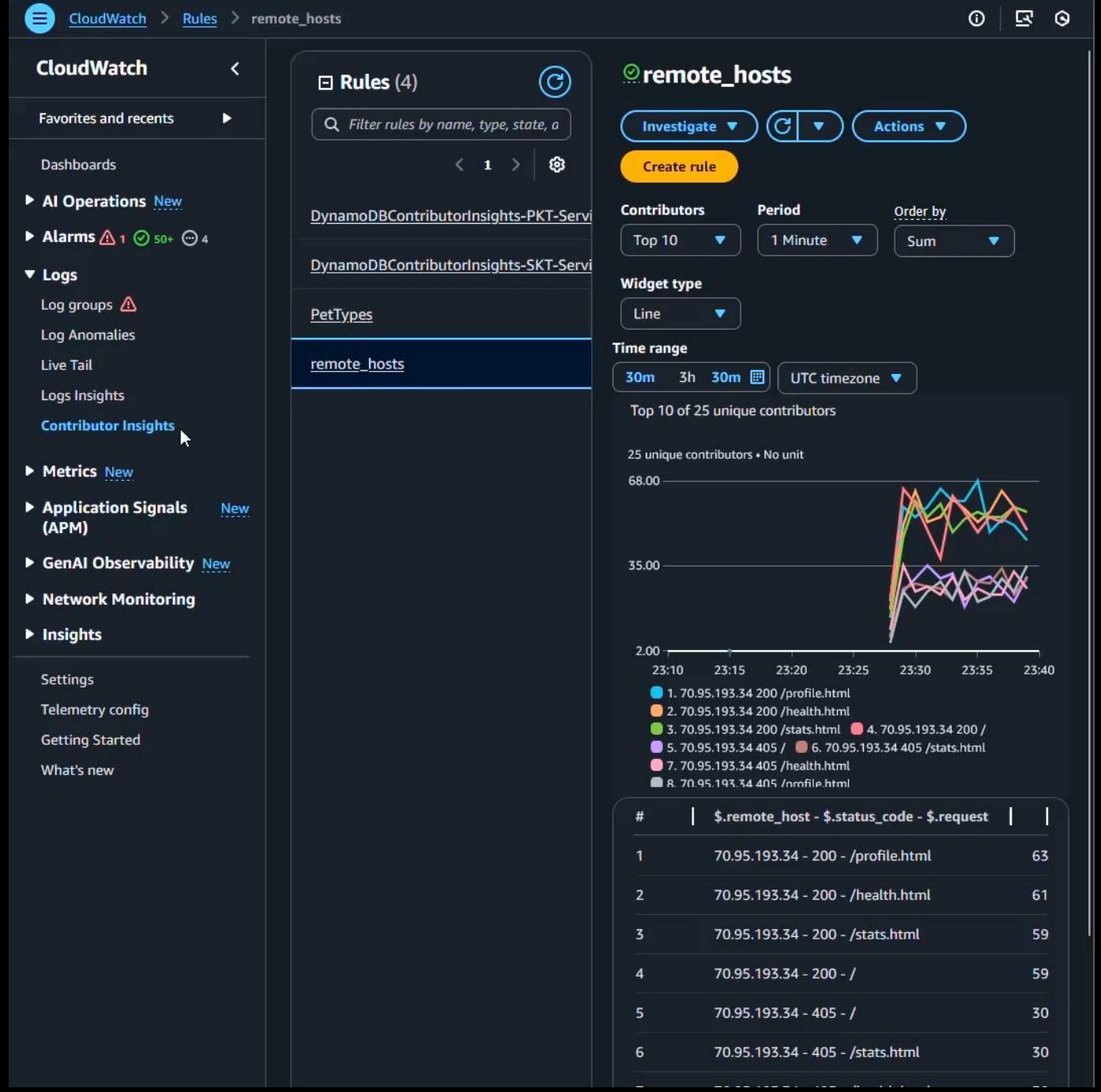


https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/MonitoringLogData.html

LOGS

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



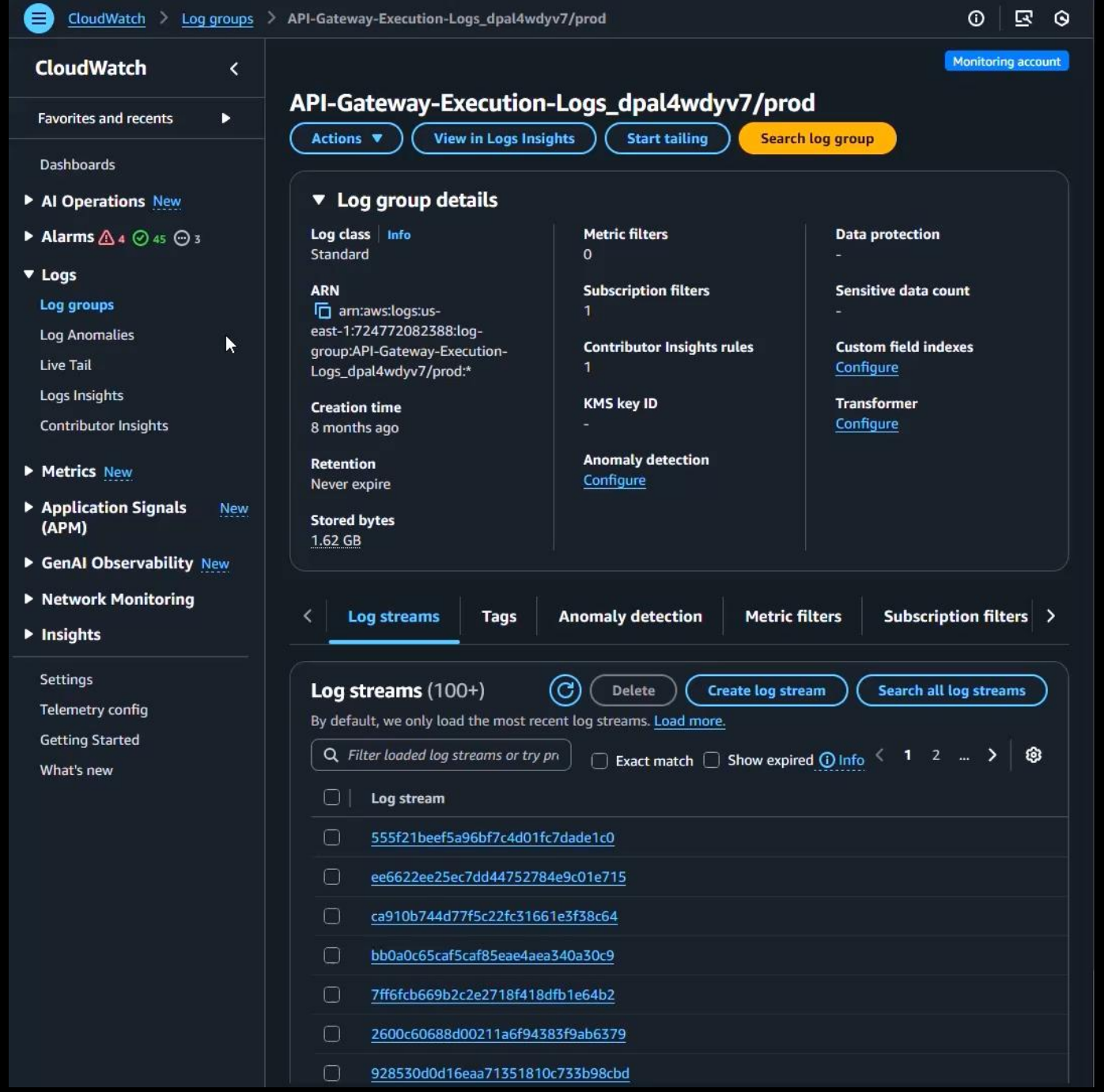
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/ContributorInsights.html

LOGS

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

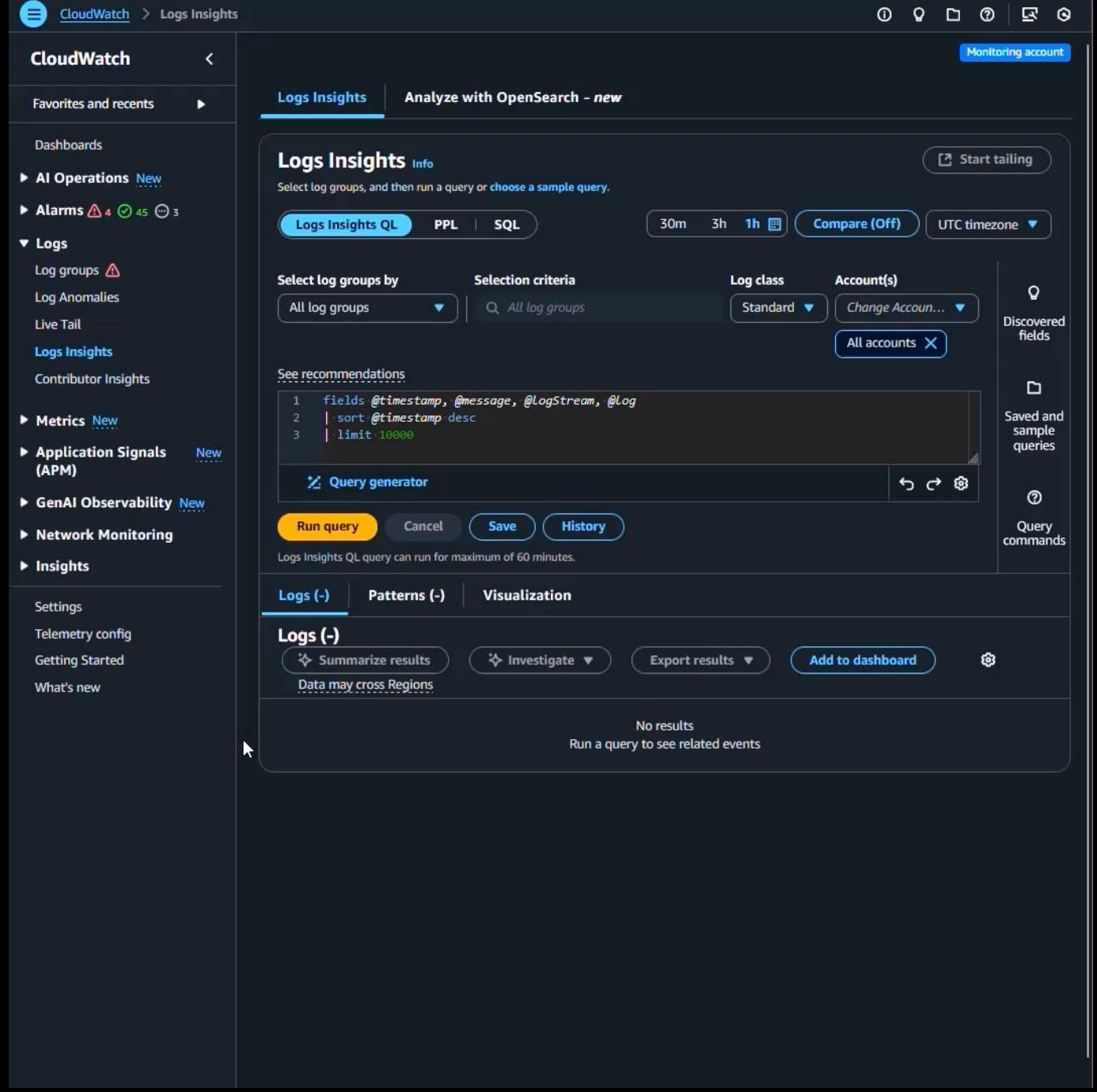


https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/Subscriptions.html

LOGS

Log Insights Log Group Selection

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

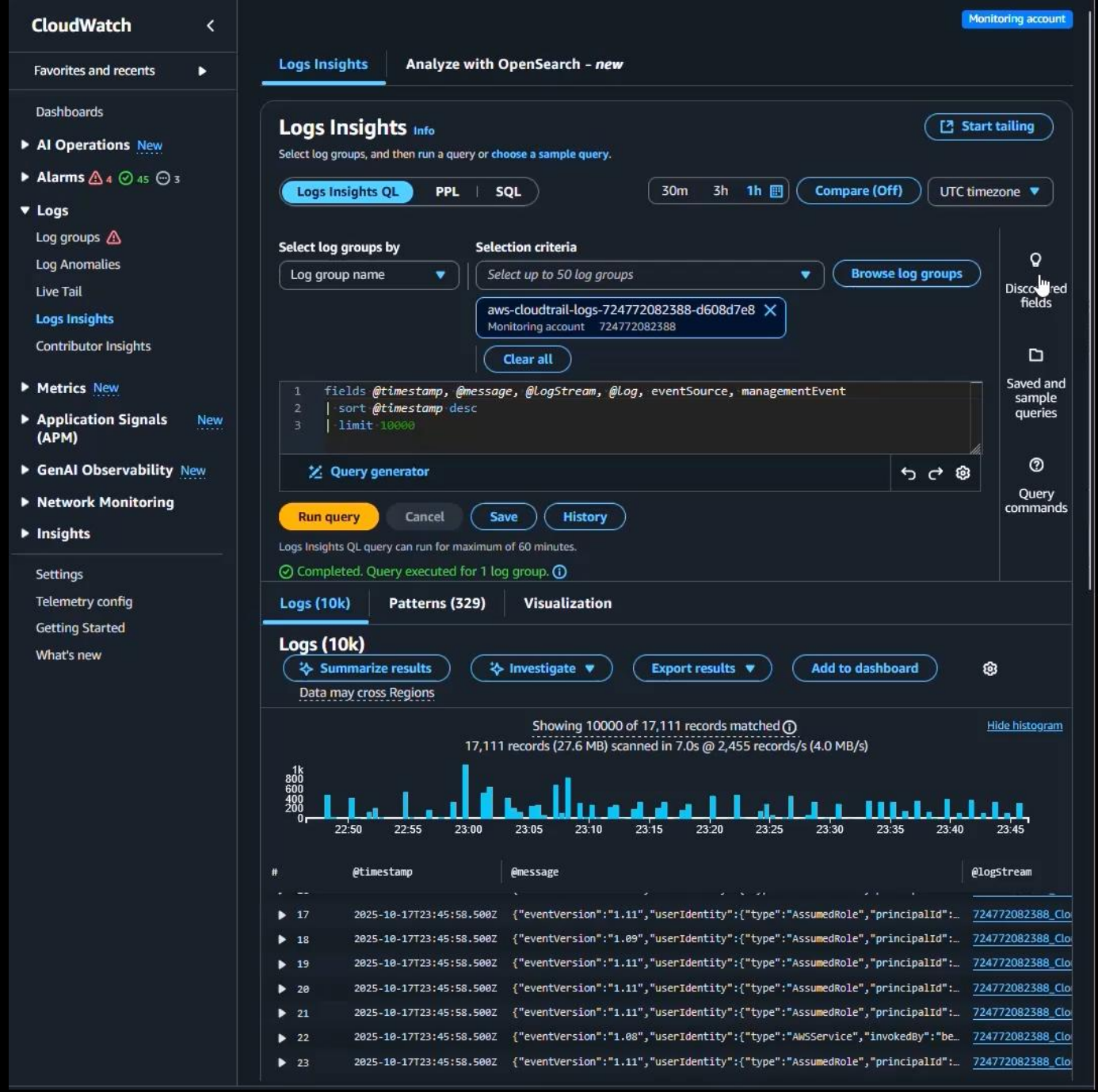


https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/Field-Indexing-Selection.html

LOGS

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

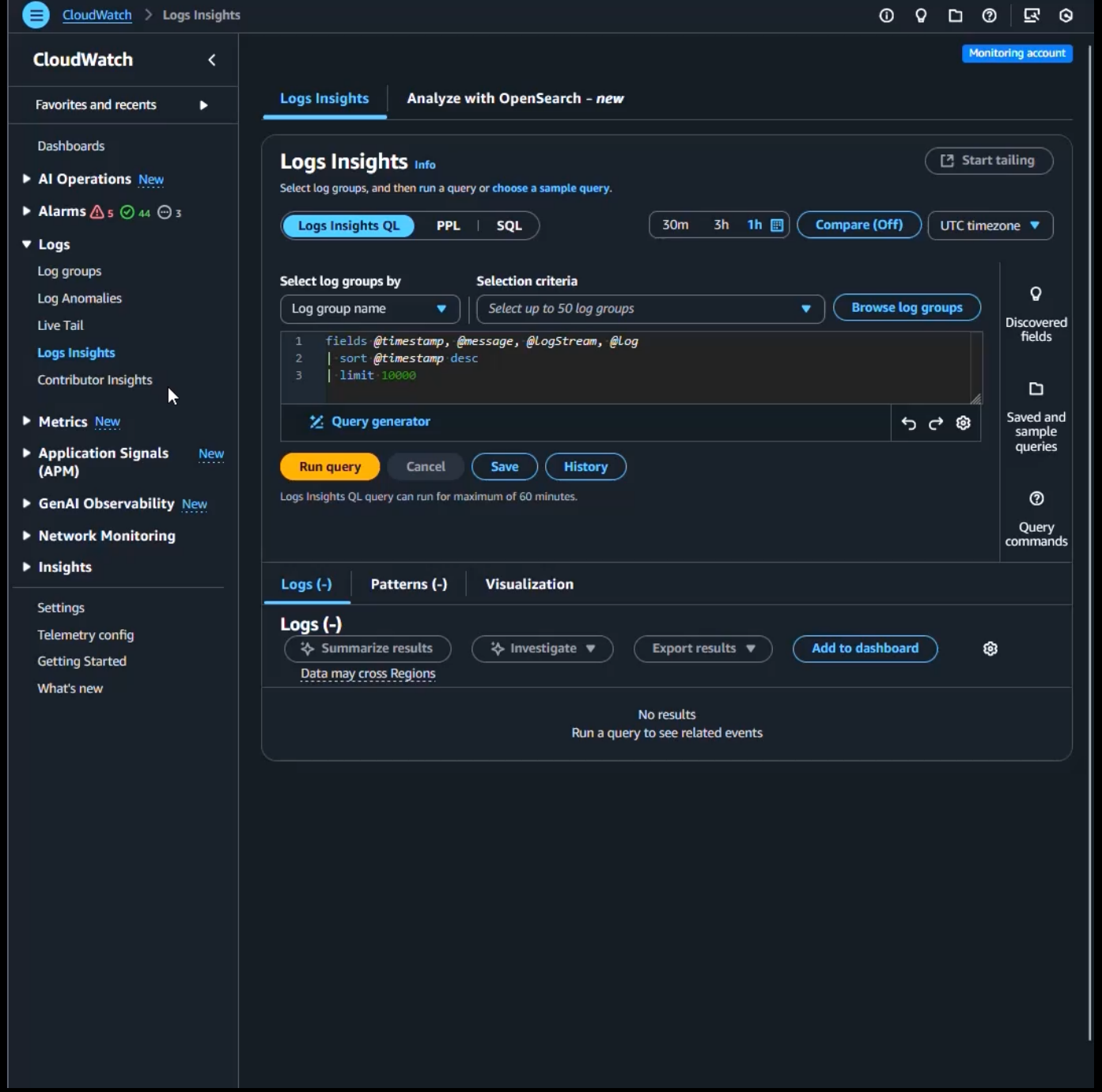


https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CWL_AnalyzeLogData-discoverable-fields.html

LOGS

Log Insights Saved queries

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

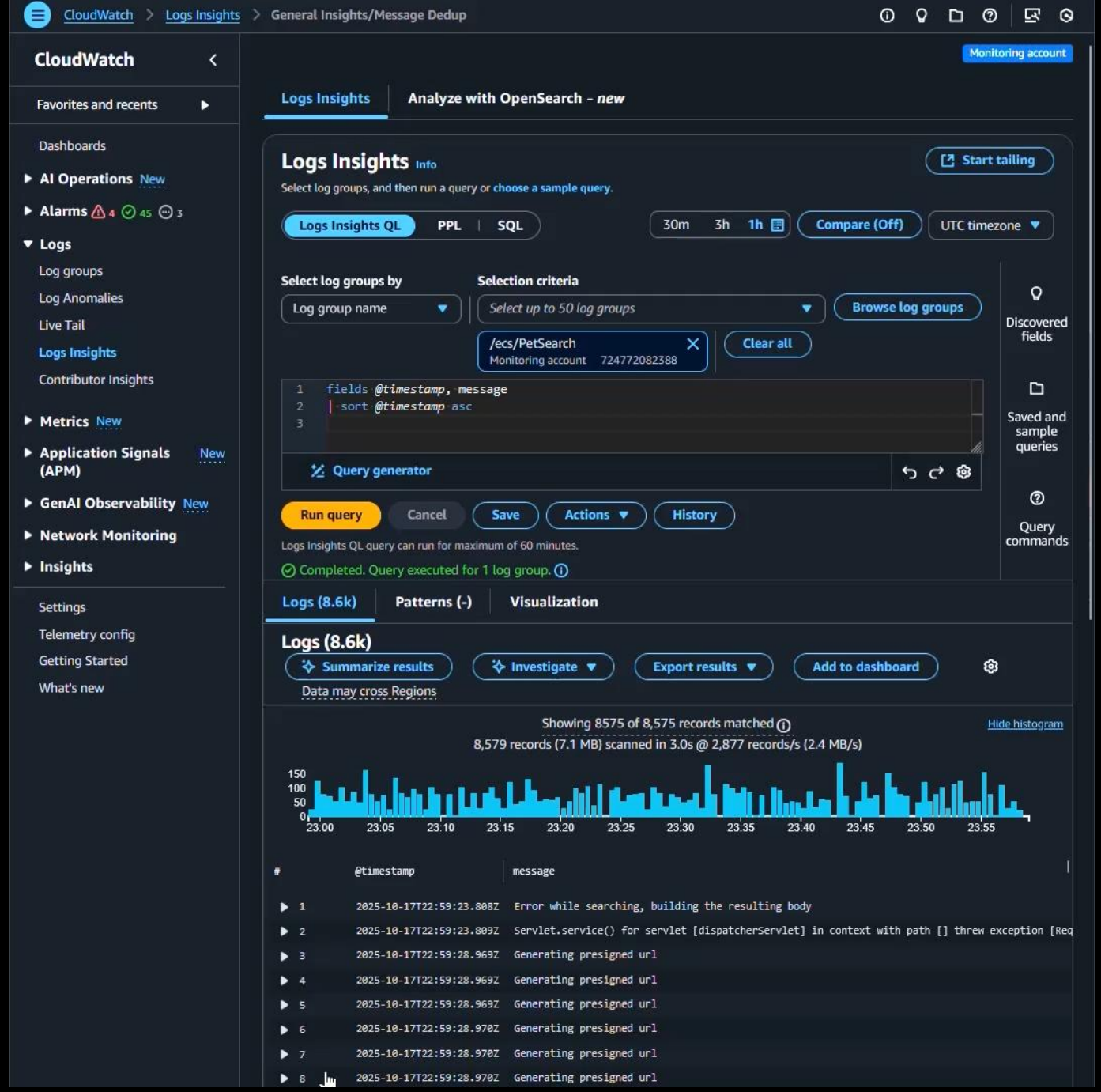


https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CWL_Insights-Saving-Queries.html

LOGS

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.

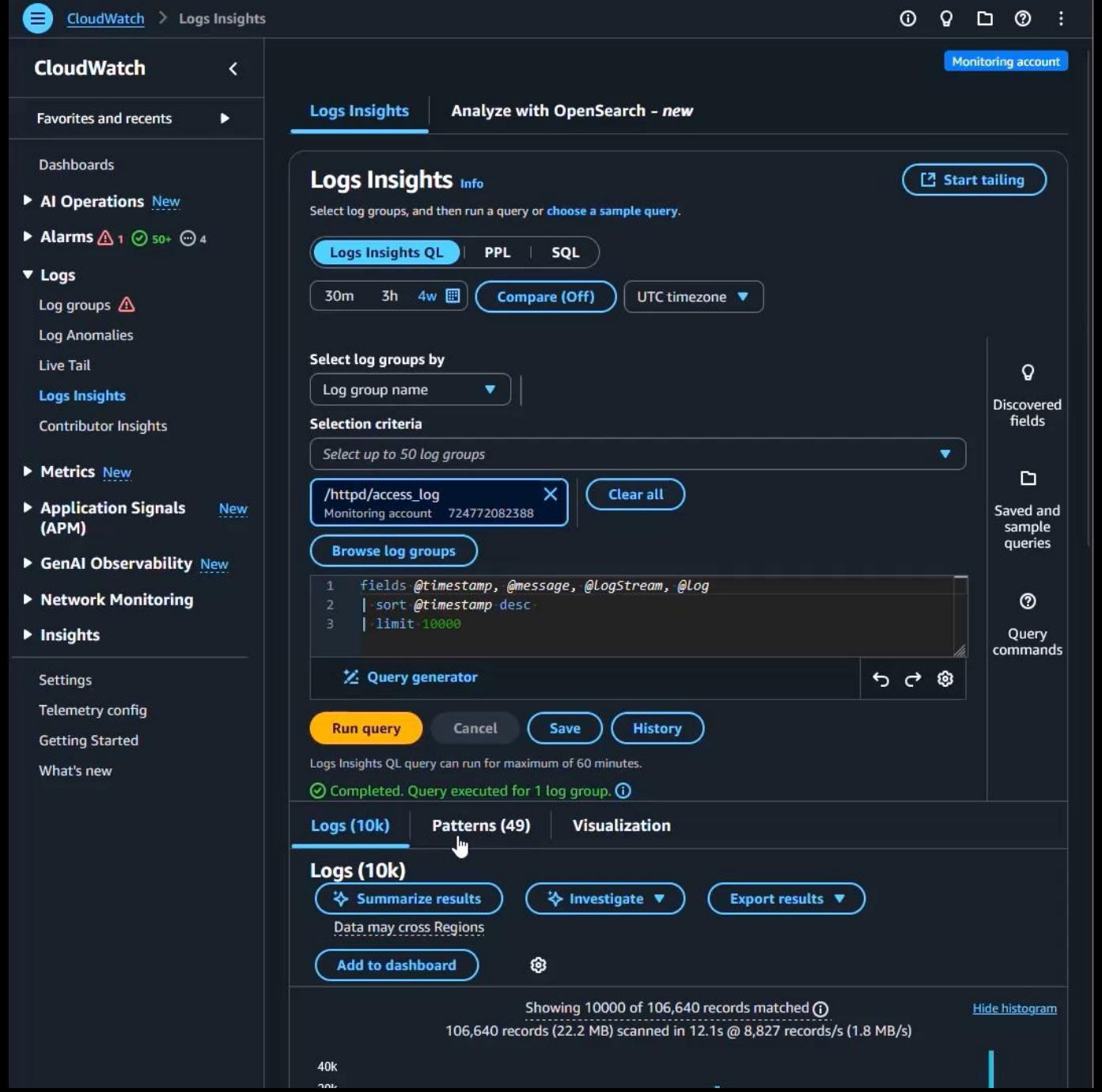


https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CWL_QuerySyntax-Dedup.html

LOGS

Log Insights filterIndex

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

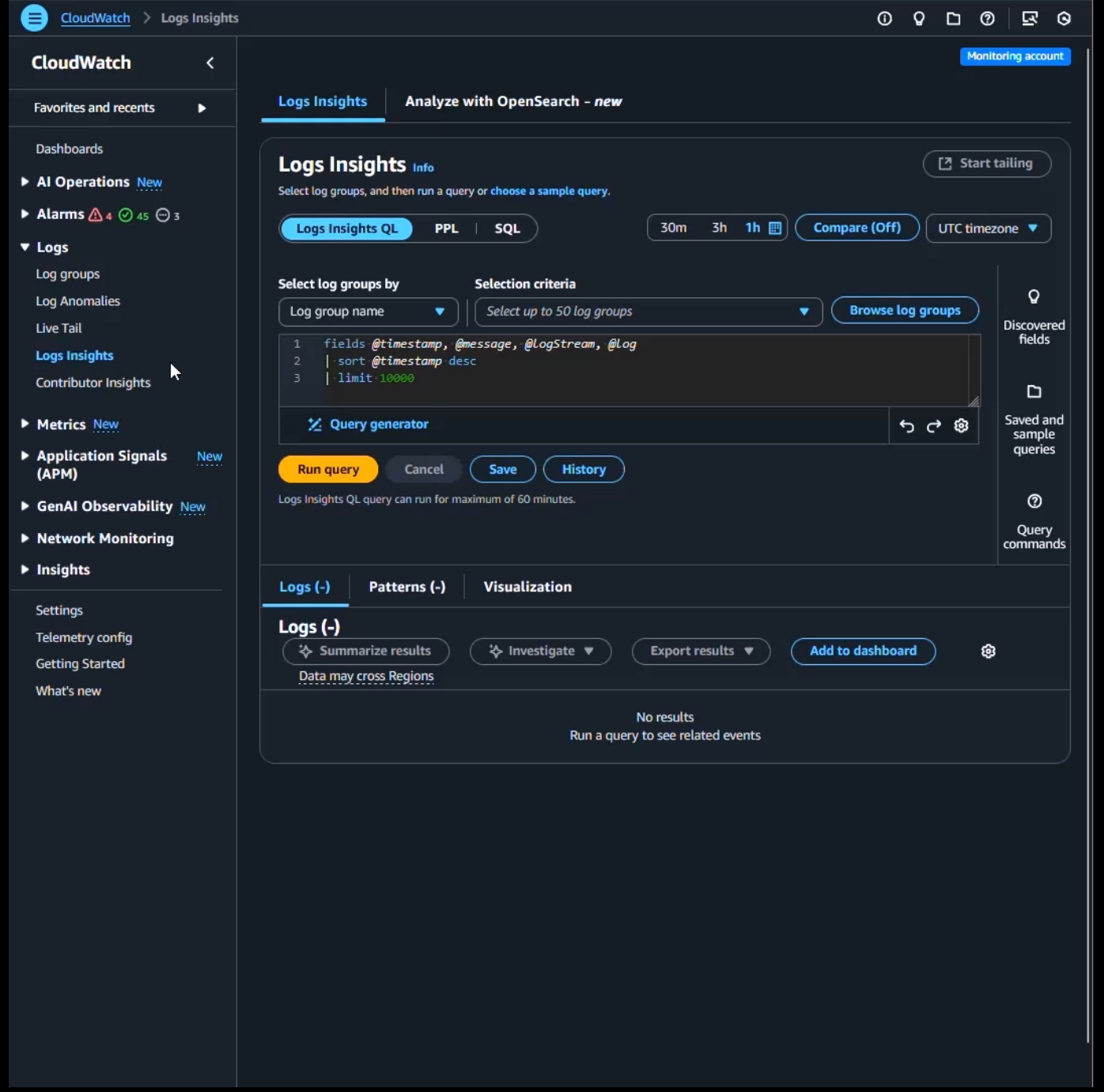


https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CWL_QuerySyntax-FilterIndex.html

LOGS

Log Insights Pattern analysis

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

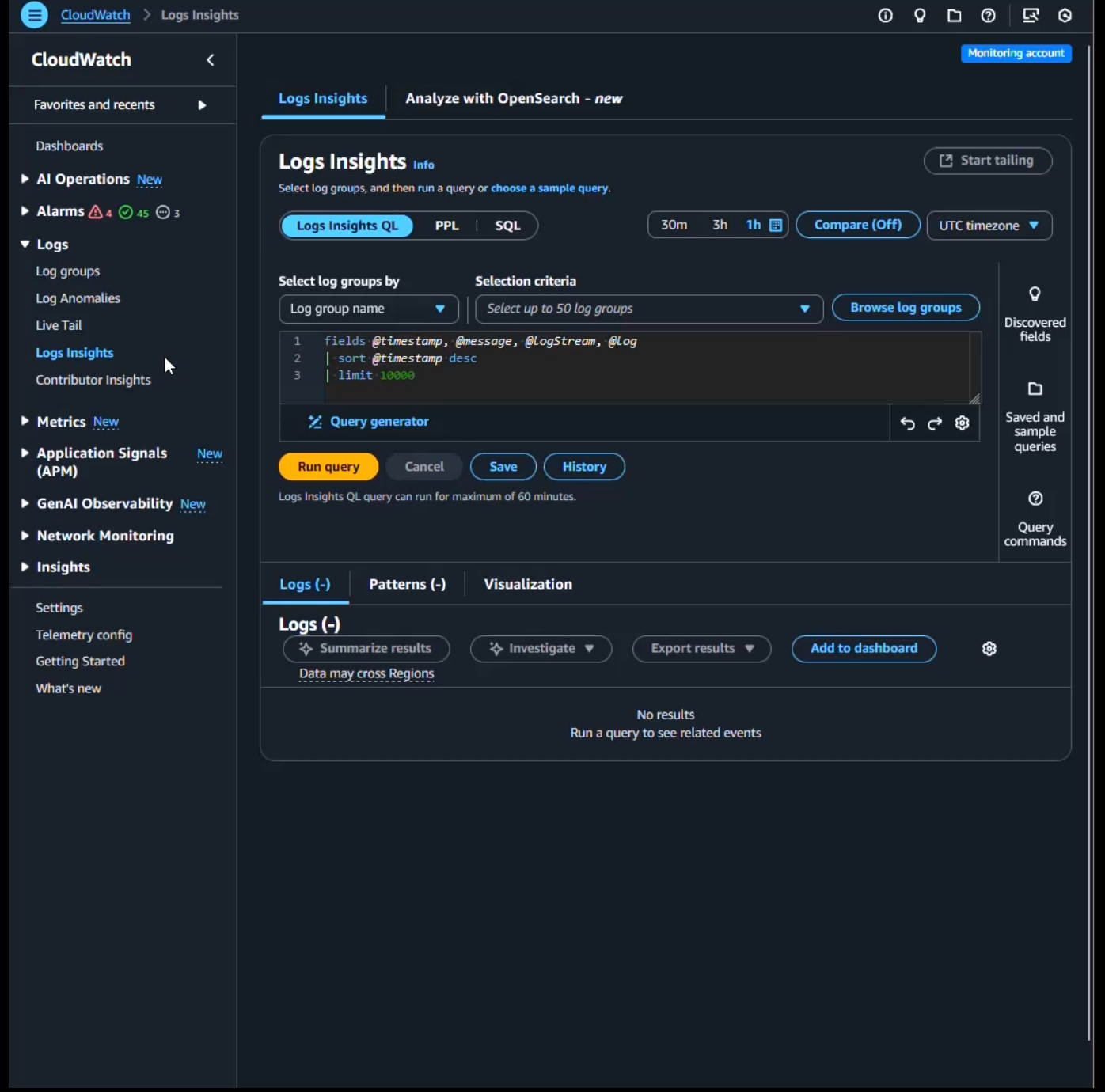


https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CWL_AnalyzeLogData_Patterns.html

LOGS

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

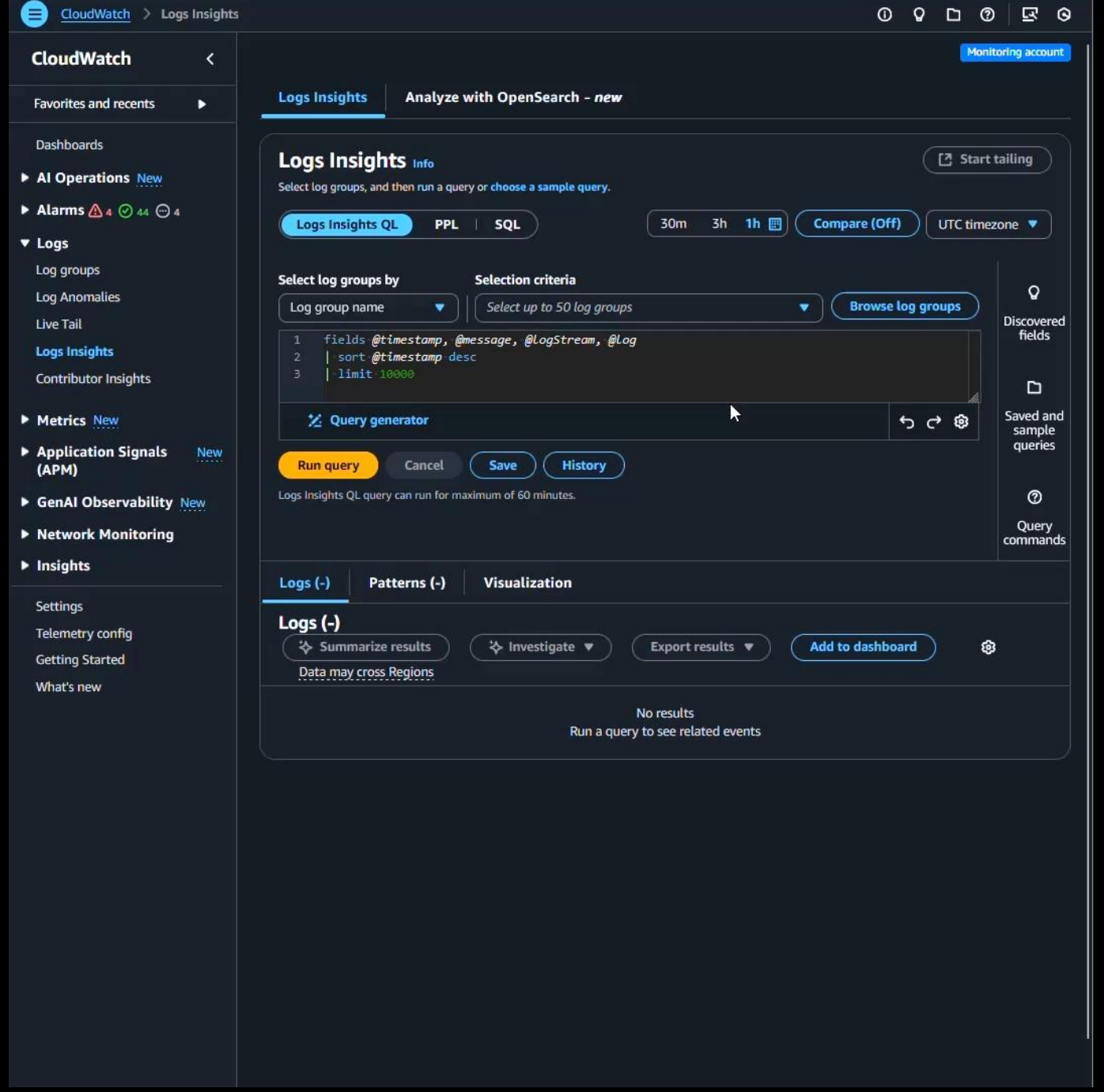


https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CWL_AnalyzeLogData_SQL.html

LOGS

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

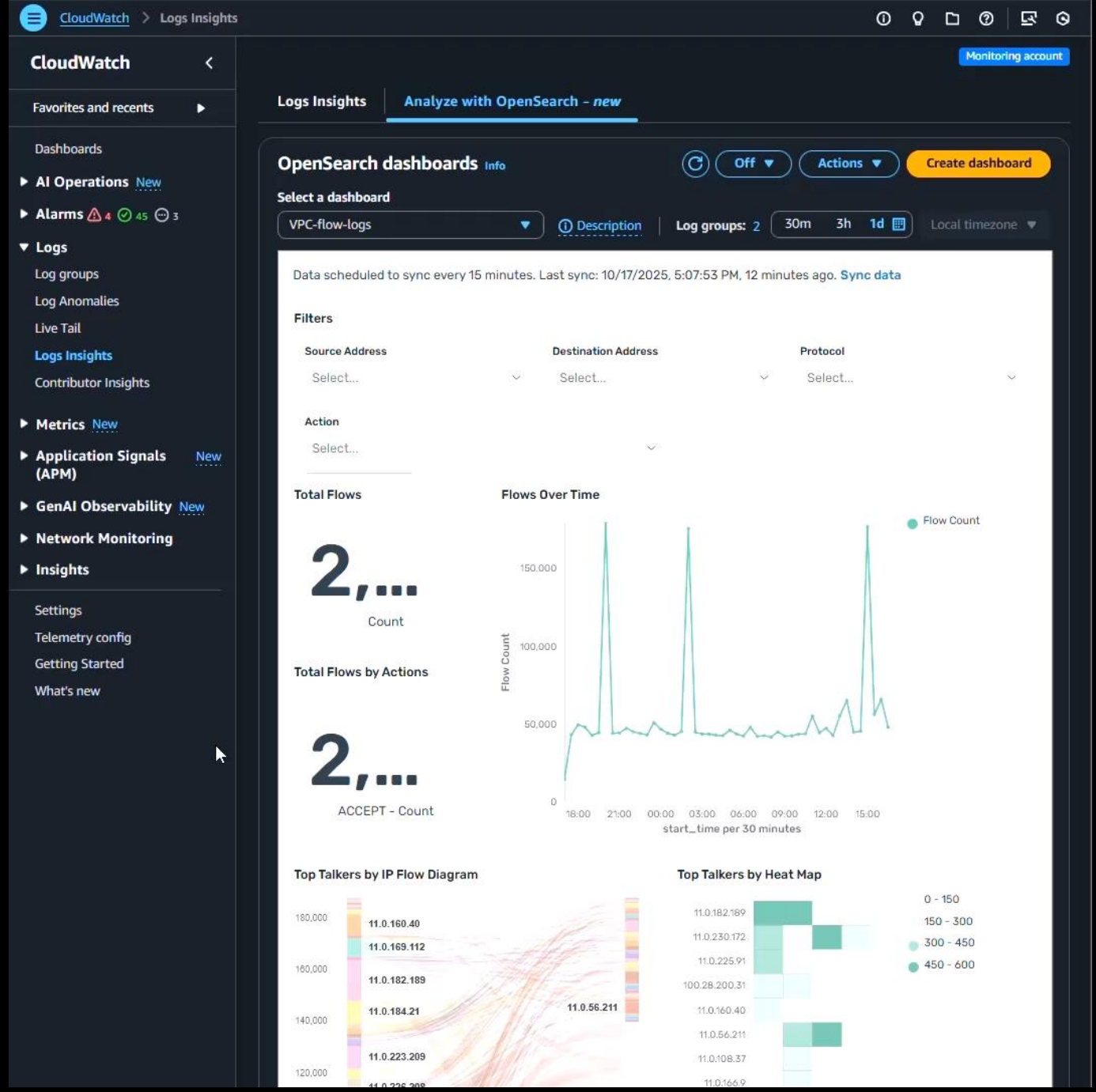


https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CWL_AnalyzeLogData_PPL.html

LOGS

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

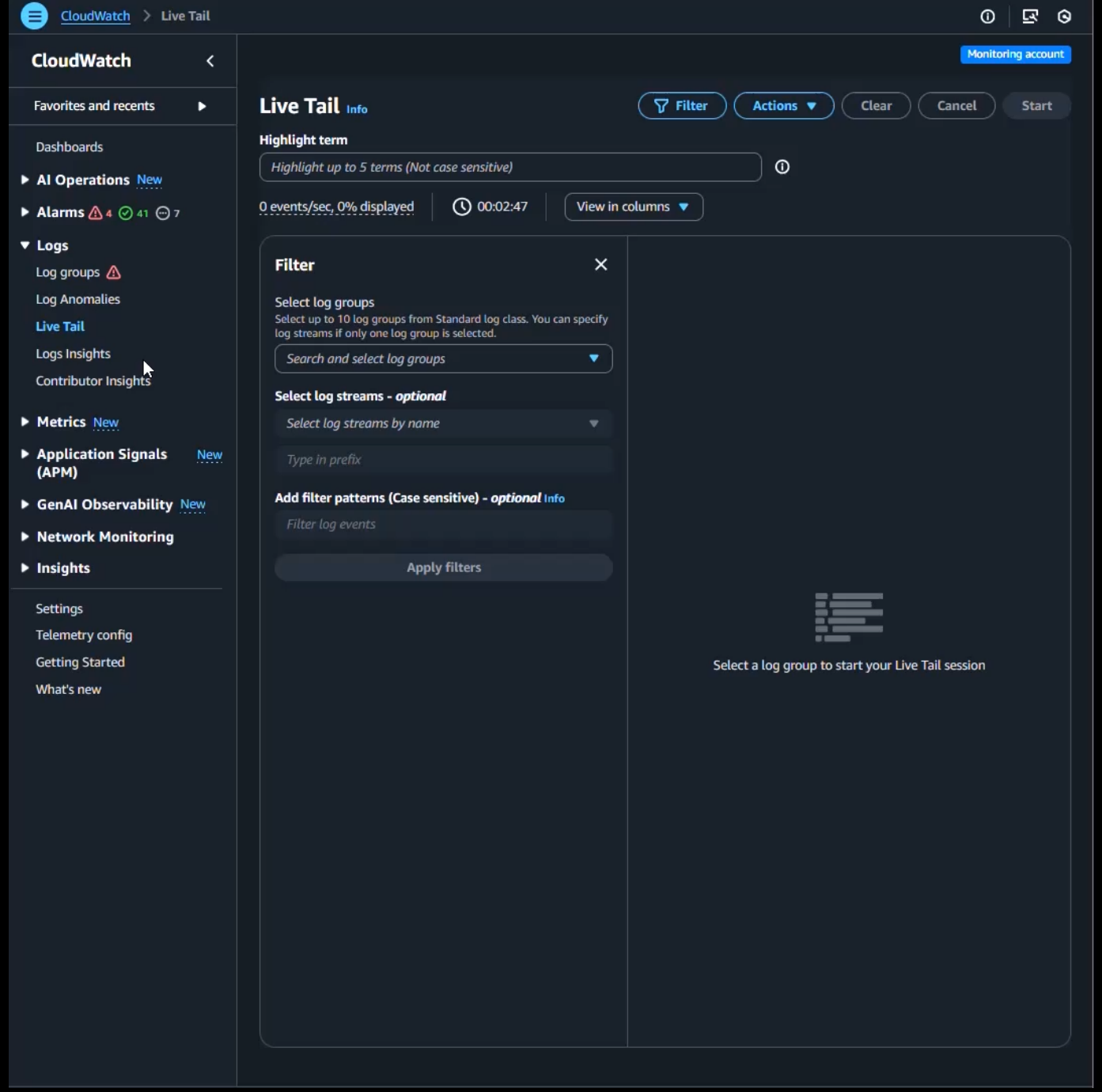


https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CloudWatchLogs-OpenSearch-Dashboards.html

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



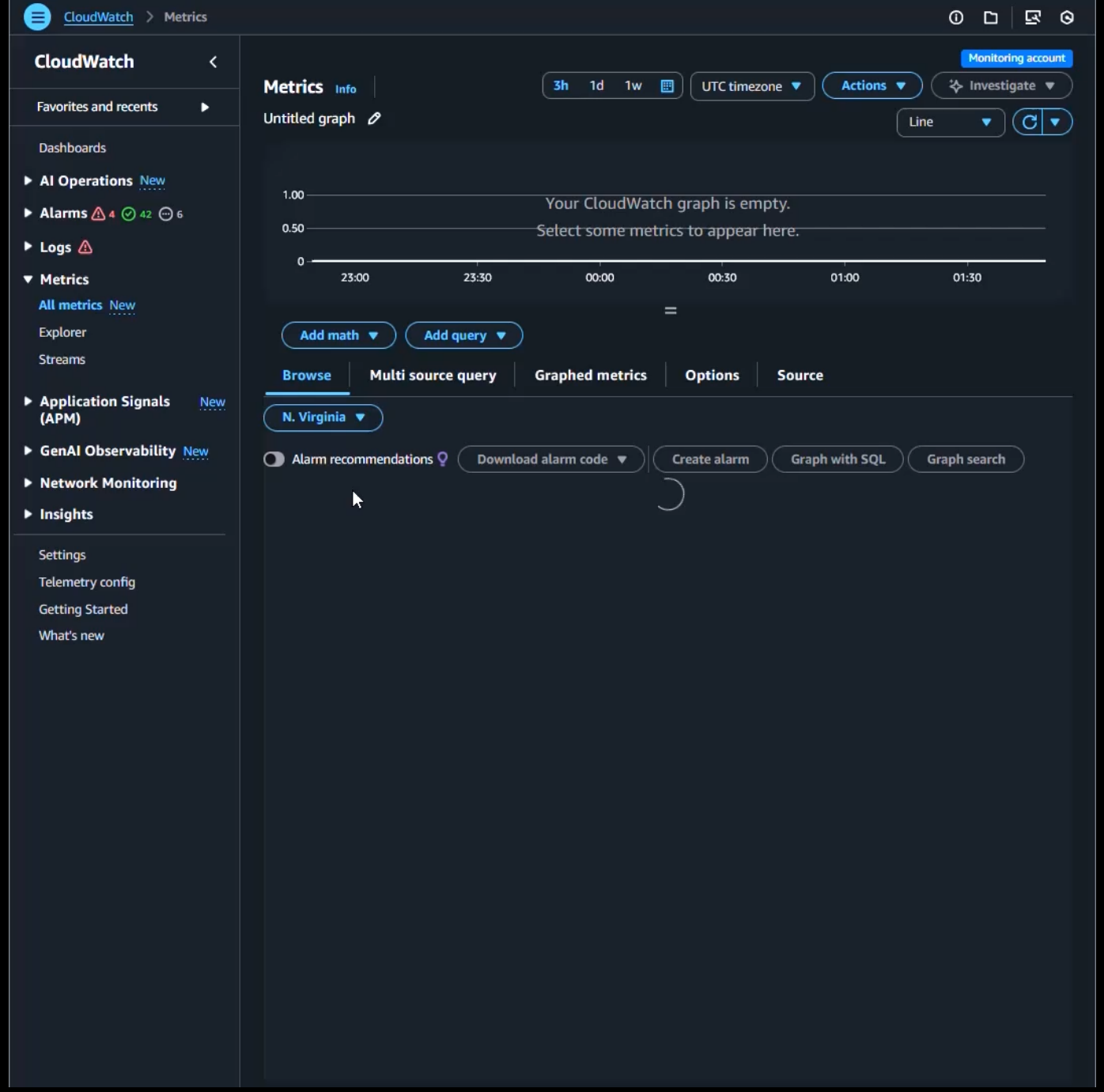
https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CloudWatchLogs_LiveTail.html

Metrics

METRICS

Alarm recommendations

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



https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/Best-Practice-Alarms.html

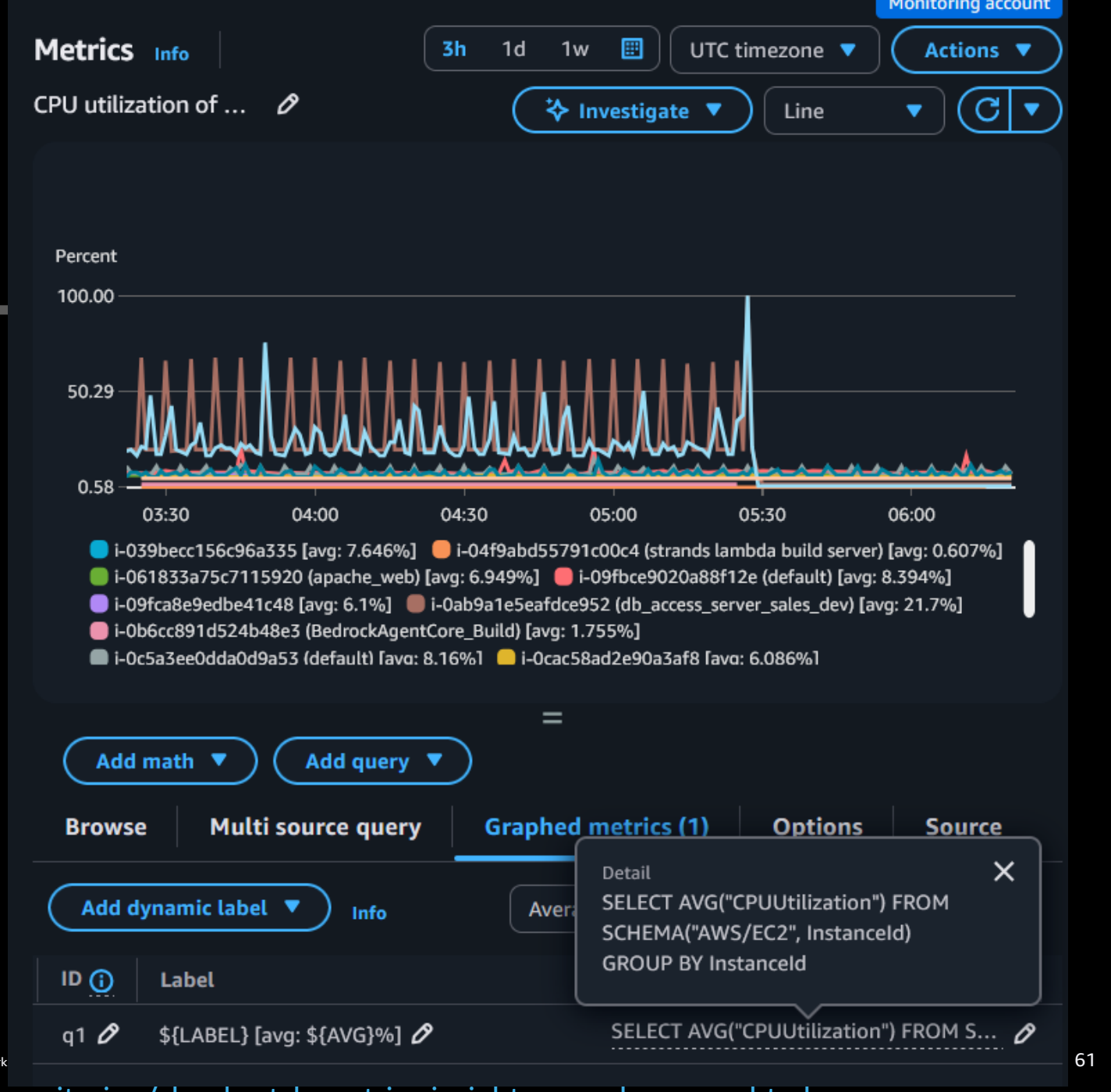
METRICS

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



https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/cloudwatch-metrics-insights-querylanguage.html

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'

https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/cloudwatch-metrics-insights-querylanguage.html

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

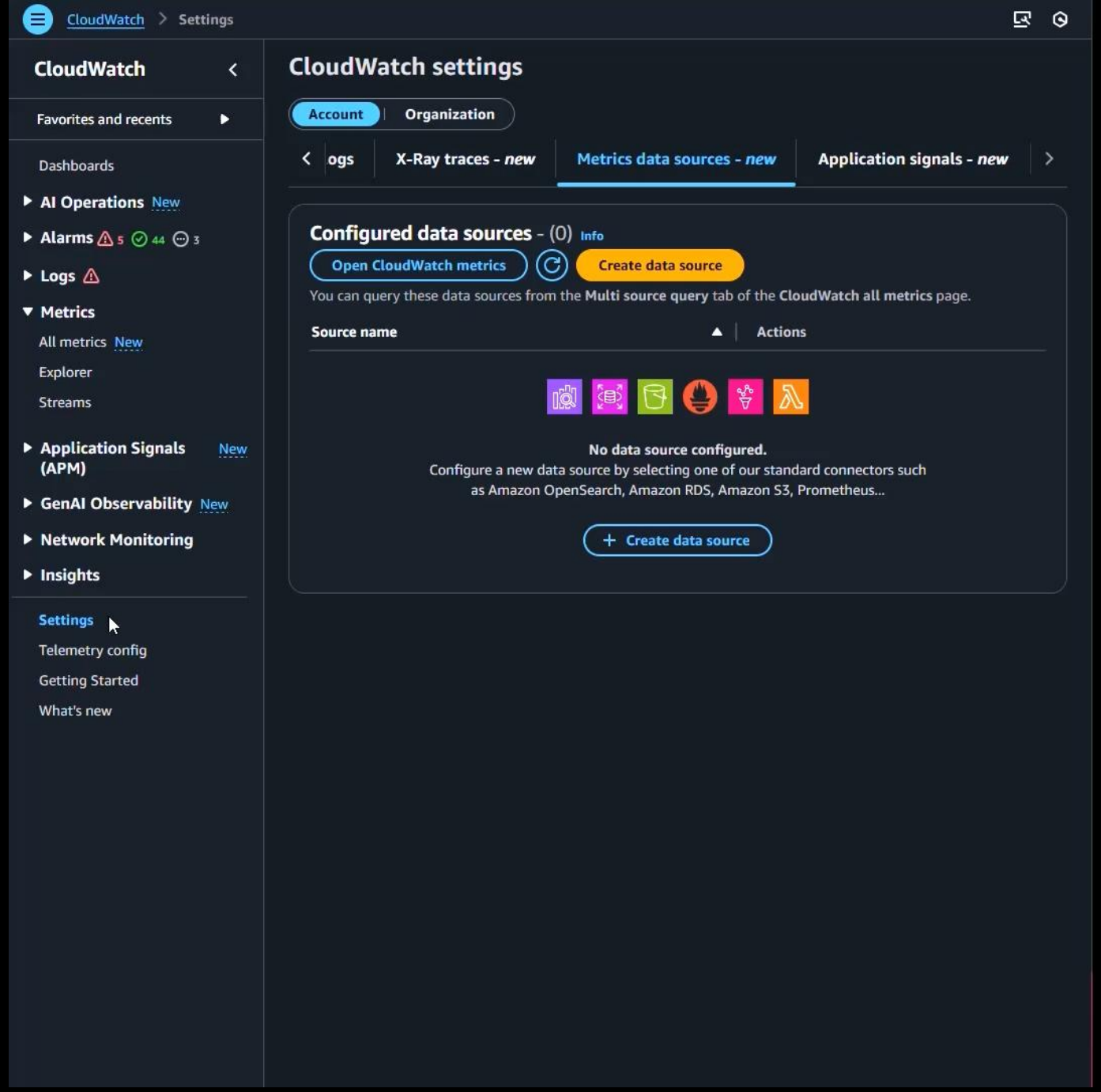
WHERE tag.Env='prod'

https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/cloudwatch-metrics-insights-querylanguage.html

METRICS

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



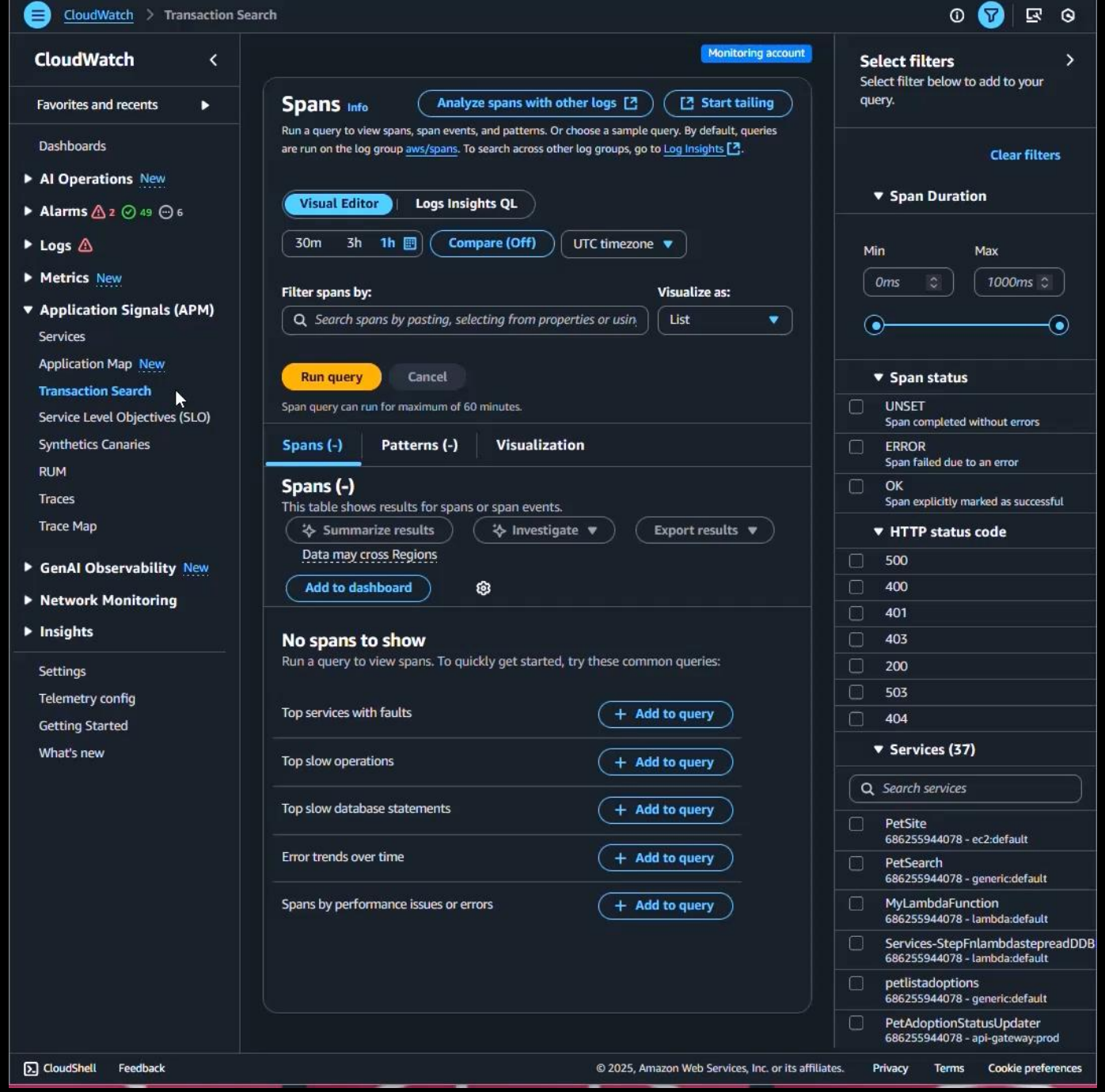
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/MultiDataSourceQuerying.html

Traces

TRACES

Transaction Search

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

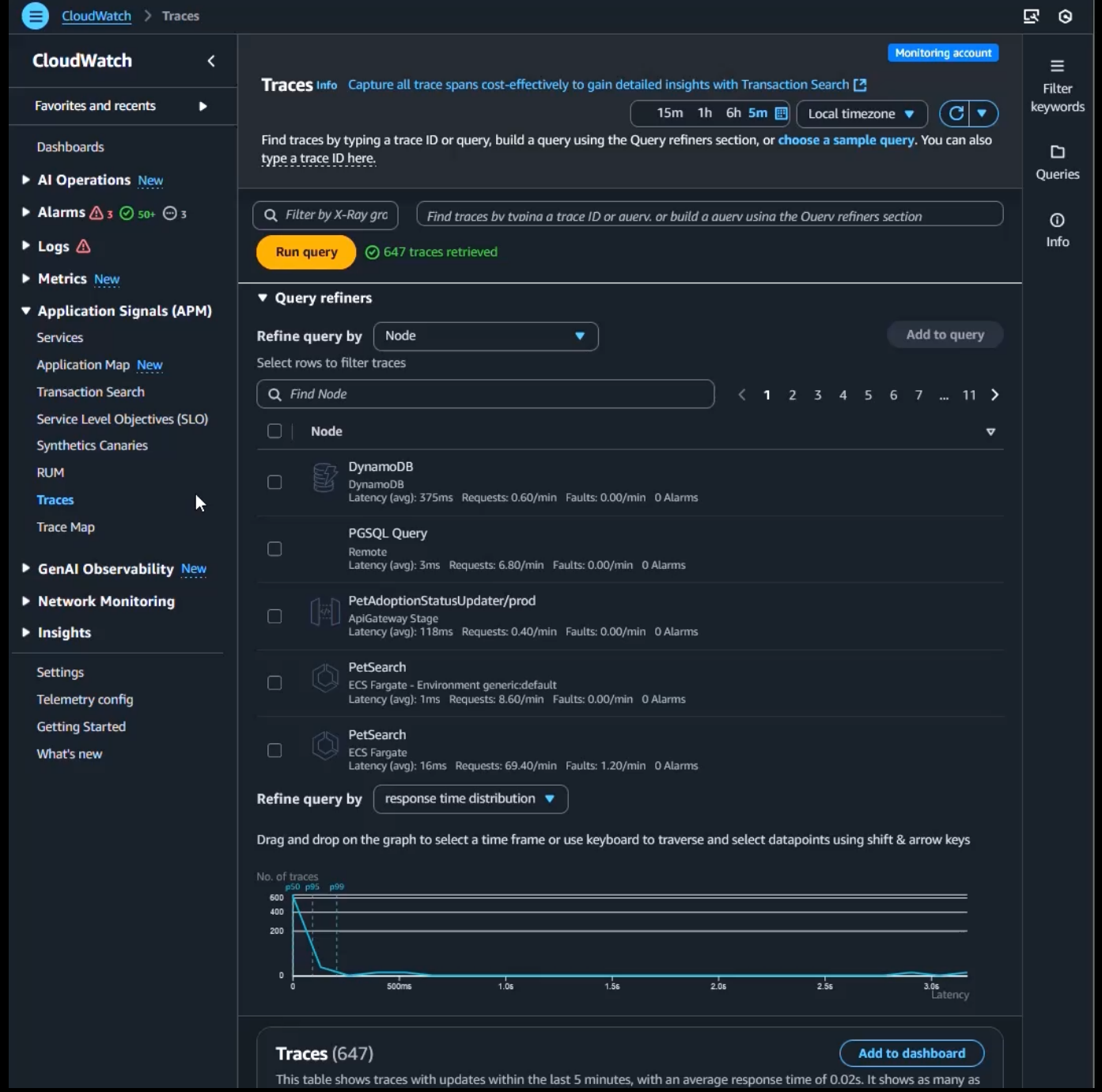


https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch-Transaction-Search.html

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.



https://docs.aws.amazon.com/xray/latest/devguide/security-logging-monitoring.html

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

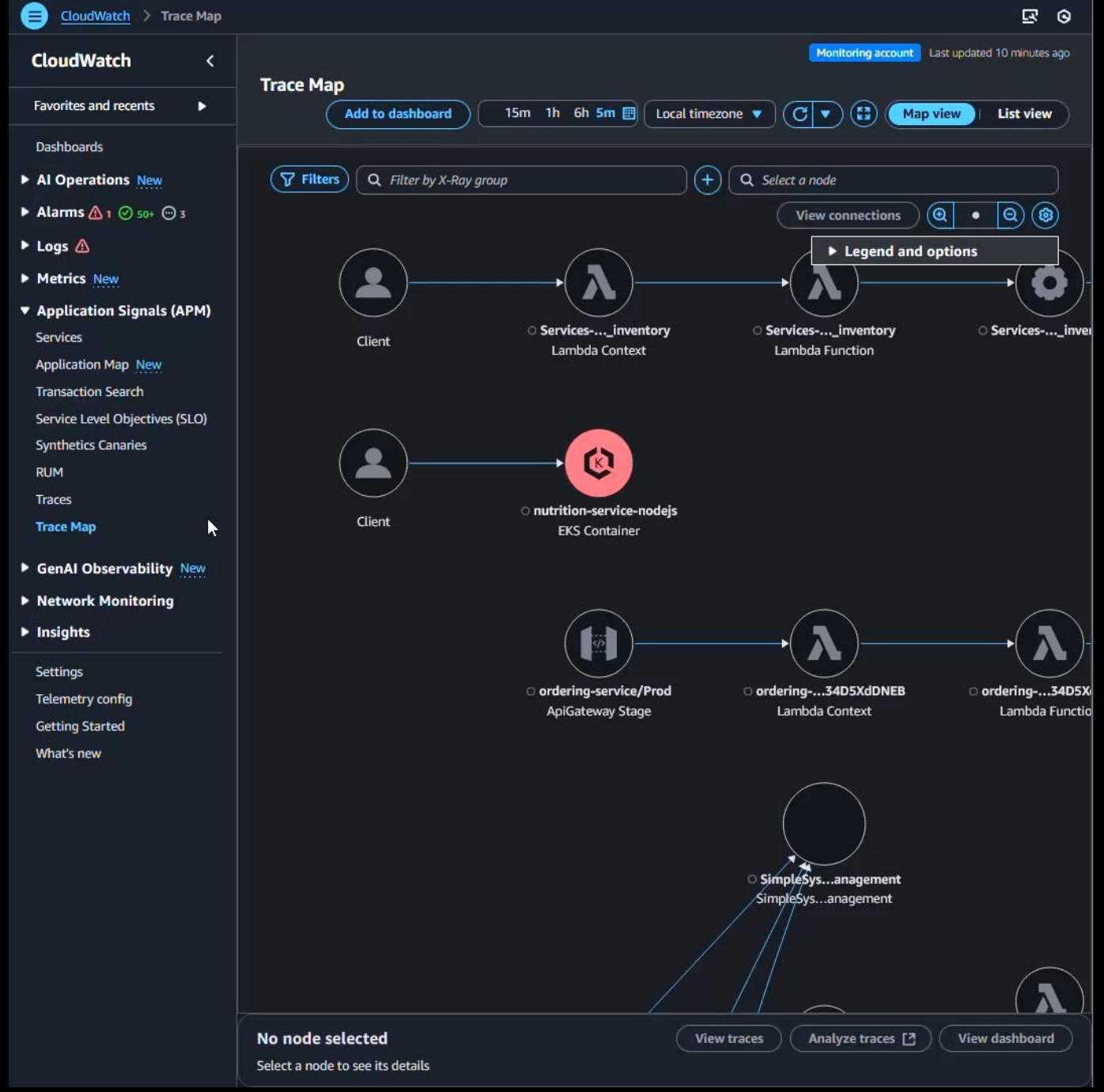
```
{
  "RuleName": "MyAdaptiveRule",
  "Priority": 1,
  "ReservoirSize": 1,
  "FixedRate": 0.05,
  "ServiceName": "*",
  "ServiceType": "*",
  "Host": "*",
  "HTTPMethod": "*",
  "URLPath": "*",
  "SamplingRateBoost": {
    "MaxRate": 0.25,
    "CooldownWindowMinutes": 10
  }
}
```

https://docs.aws.amazon.com/xray/latest/devguide/xray-adaptive-sampling.html

TRACES

X-Ray trace map

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



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

CloudWatch Agent

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)"
            }
          ]
        }
      ]
    }
  }
}
```

https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch-Agent-Configuration-File-Details.html

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"
      }
    }
  }
}
```

https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch-Agent-Configuration-File-Details.html

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"
        ],
```


https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch-Agent-Configuration-File-Details.html

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}"
  }
}
```


https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch-Agent-Configuration-File-Details.html

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": {
  }
}
```

https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch-Agent-Configuration-File-Details.html

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"
  }
}
```

https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch-Agent-Configuration-File-Details.html

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
}
```

https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch-Agent-Configuration-File-Details.html

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.*"
          }
       ]
  }
]
```

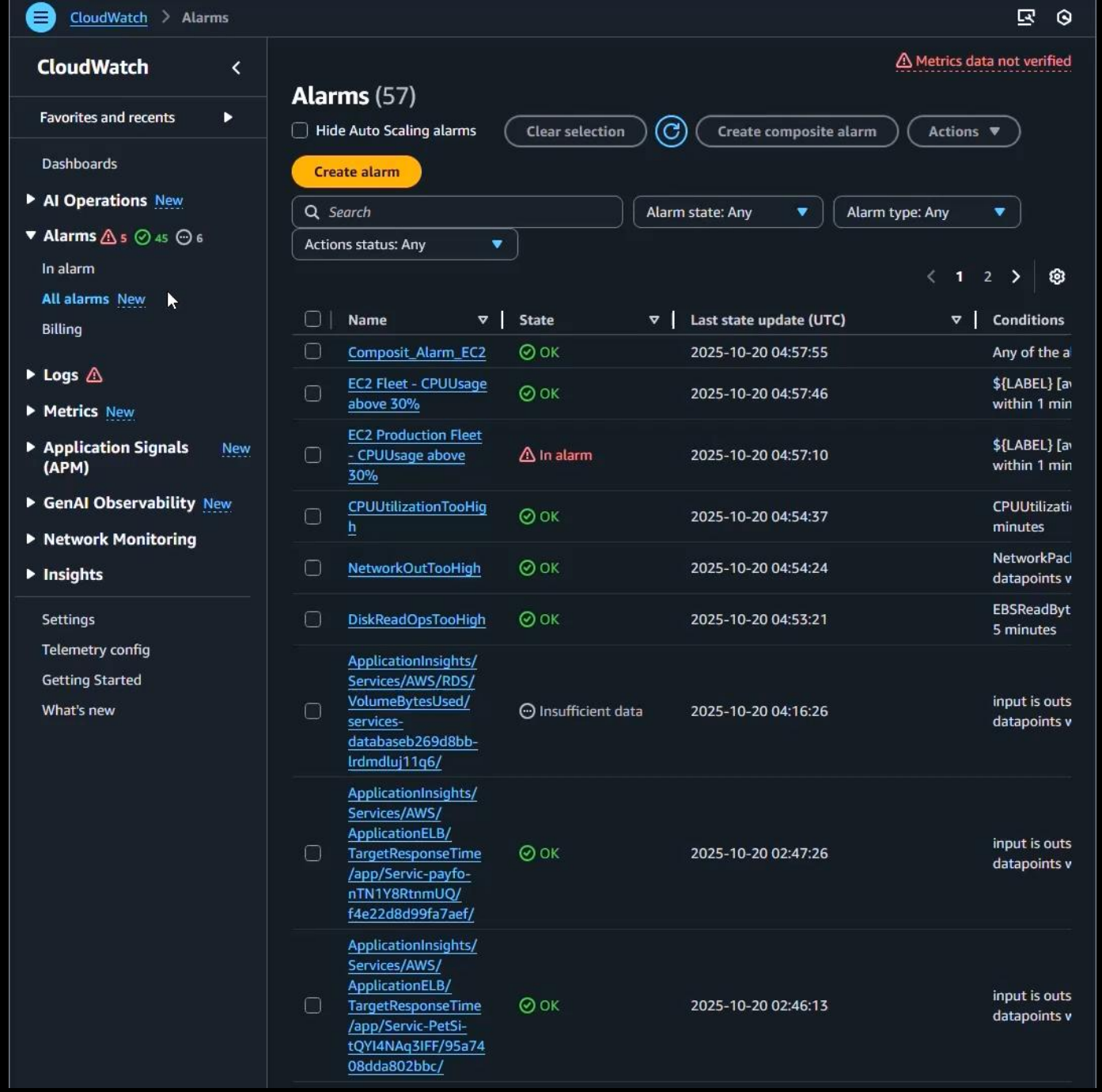

https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch-Agent-Configuration-File-Details.html

Alarms

ALARMS

Composite alarms

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



https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/Create_Composite_Alarm_How_To.html

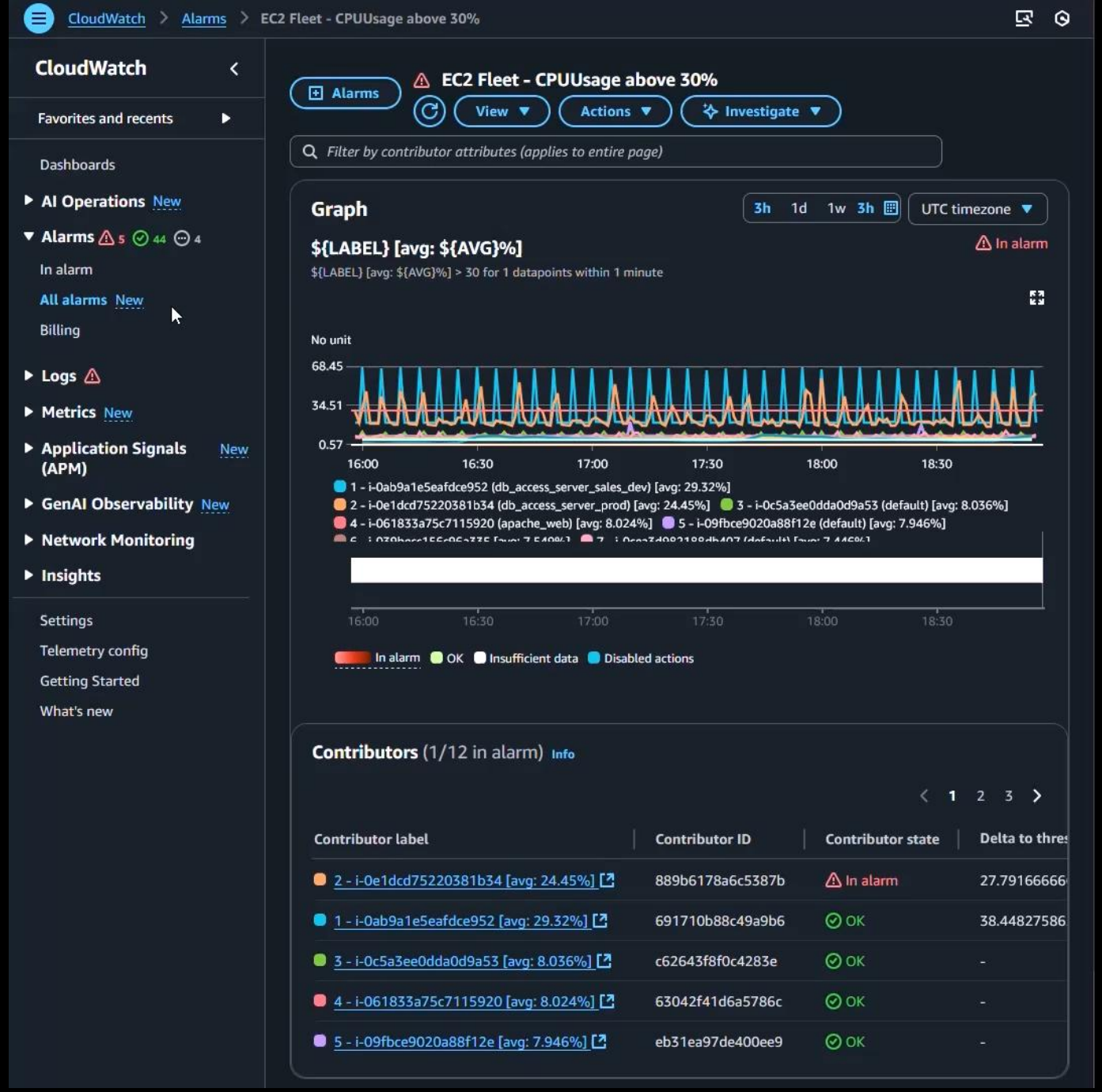
ALARMS

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



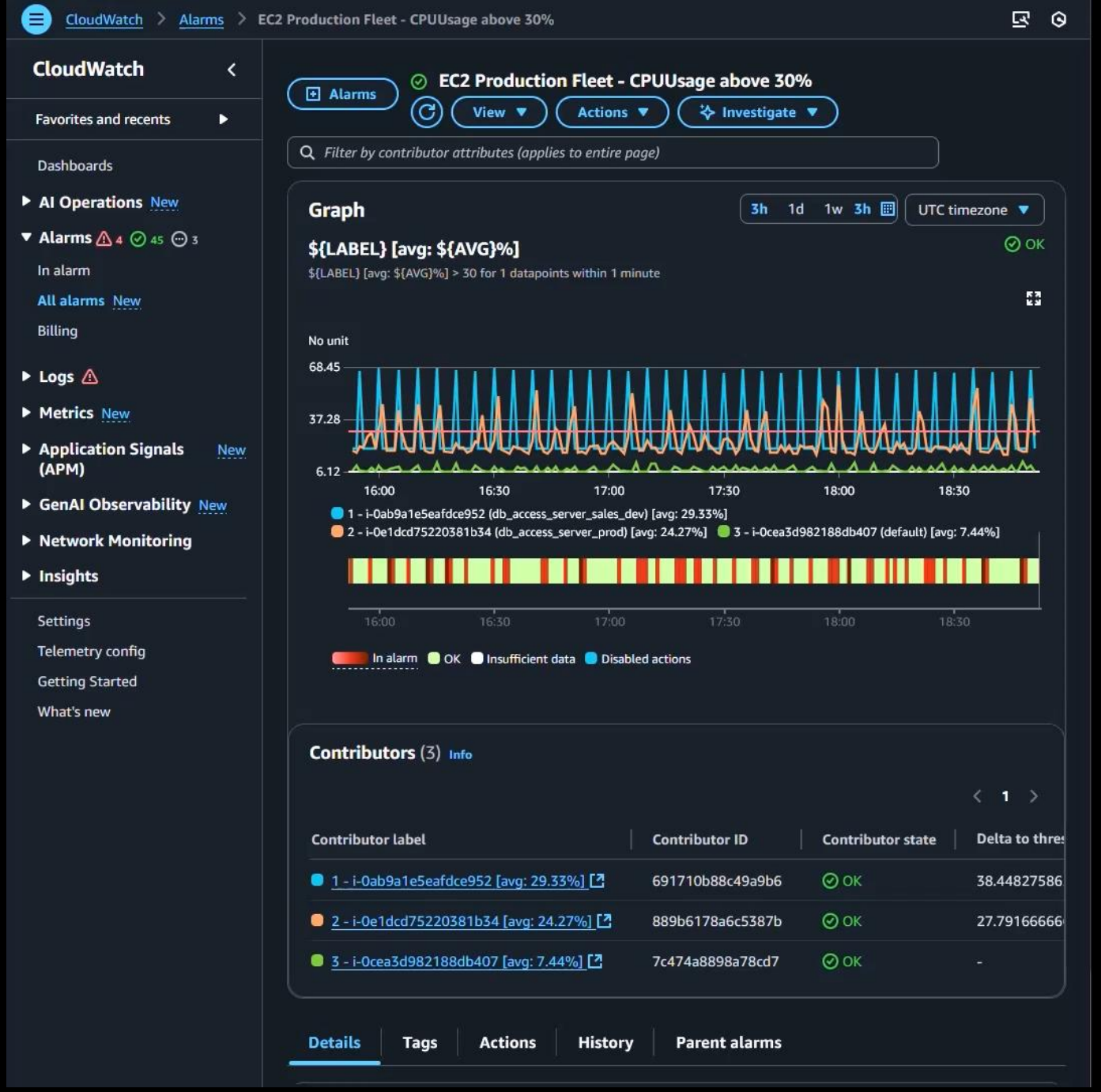
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/cloudwatch-metrics-insights-querylanguage.html

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
```



https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/cloudwatch-metrics-insights-querylanguage.html

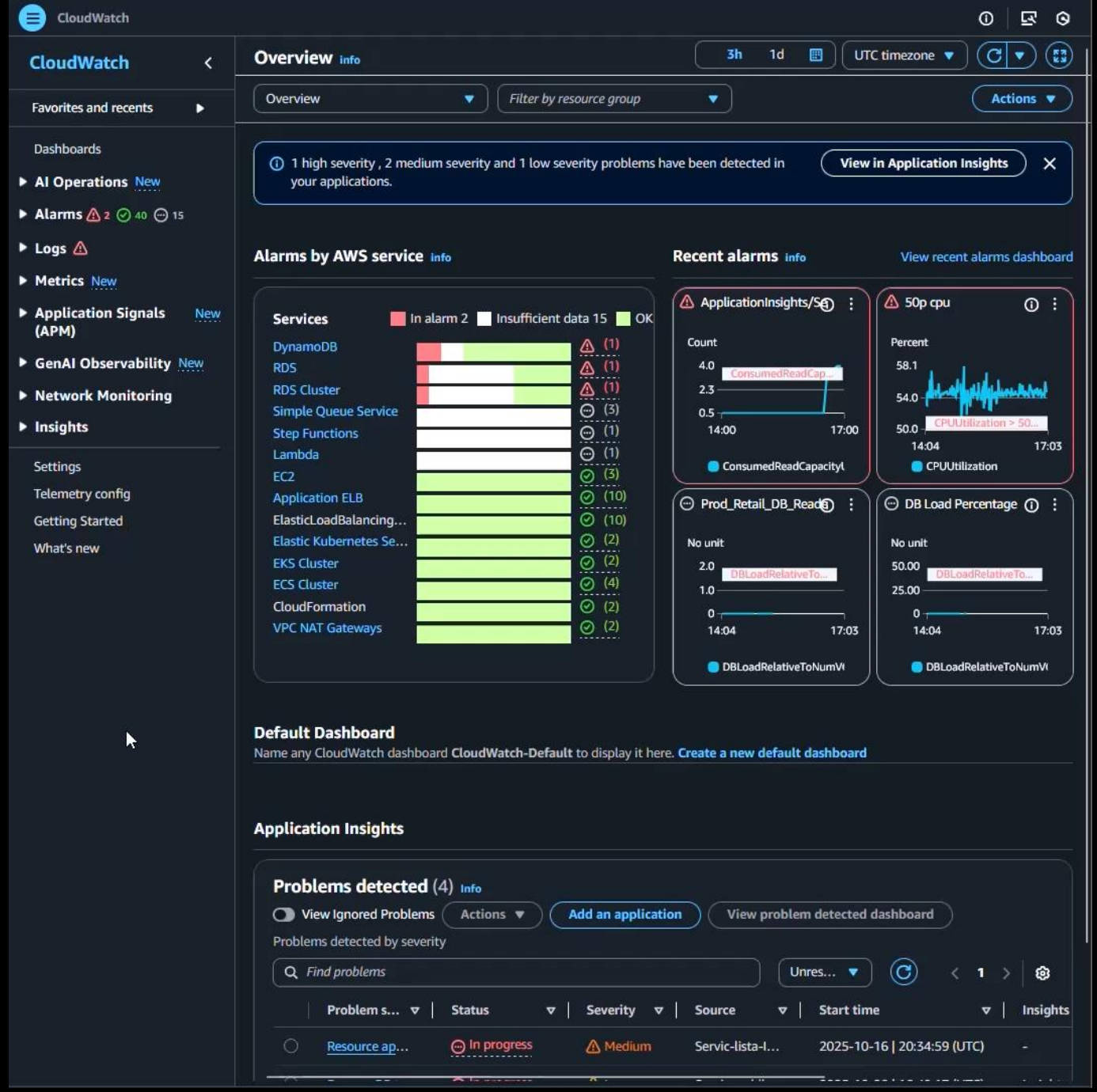
Dashboards

DASHBOARDS

Automatic Service Dashboards

- Automatic Dashboards for:
  - Overview
  - Cross service
  - Billing
  - Recent alarms
  - AWS Services

- Quickly identify how your AWS services are performing

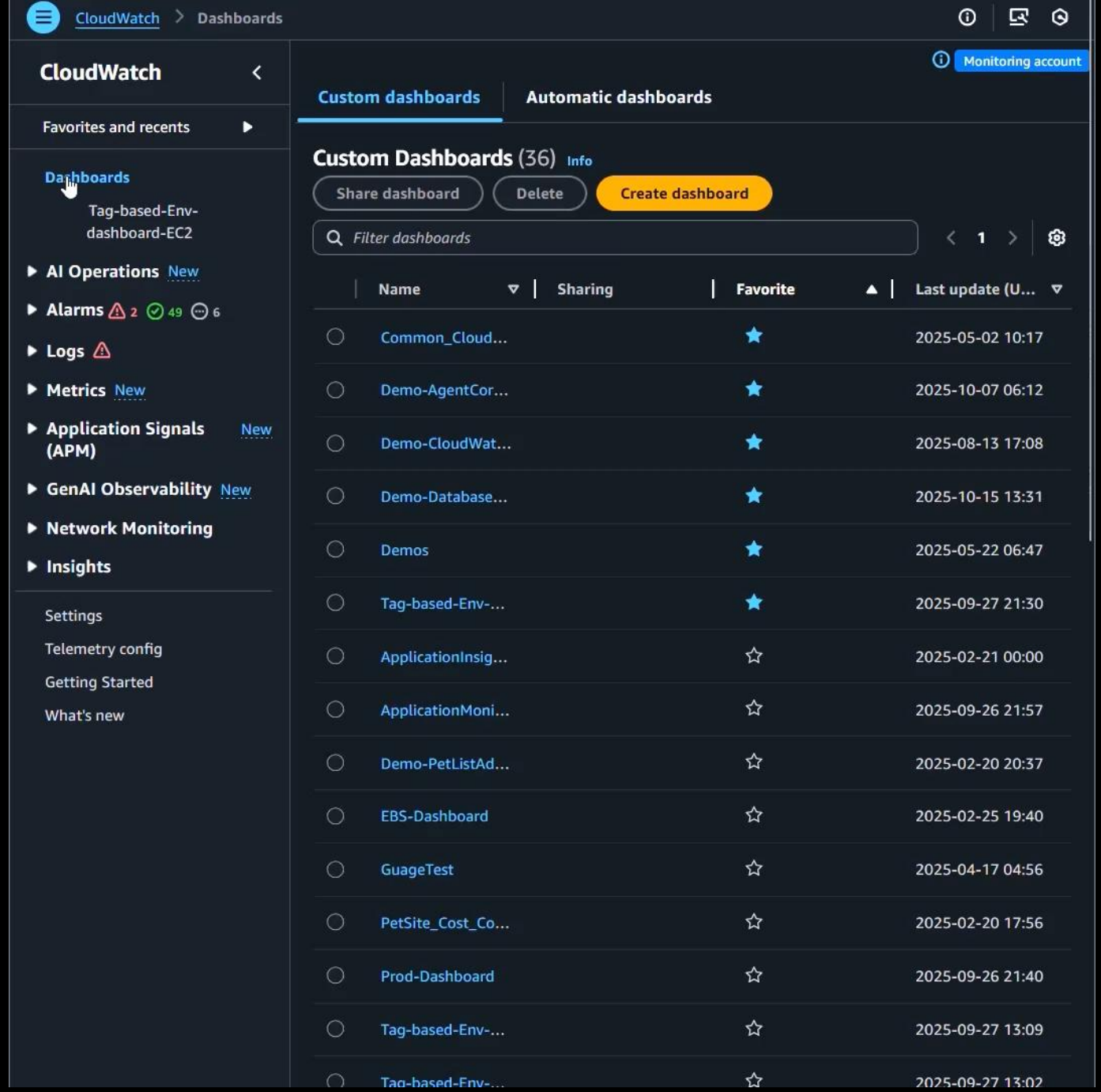


https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/GettingStarted.html

DASHBOARDS

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 widgest using lambda for complex displays



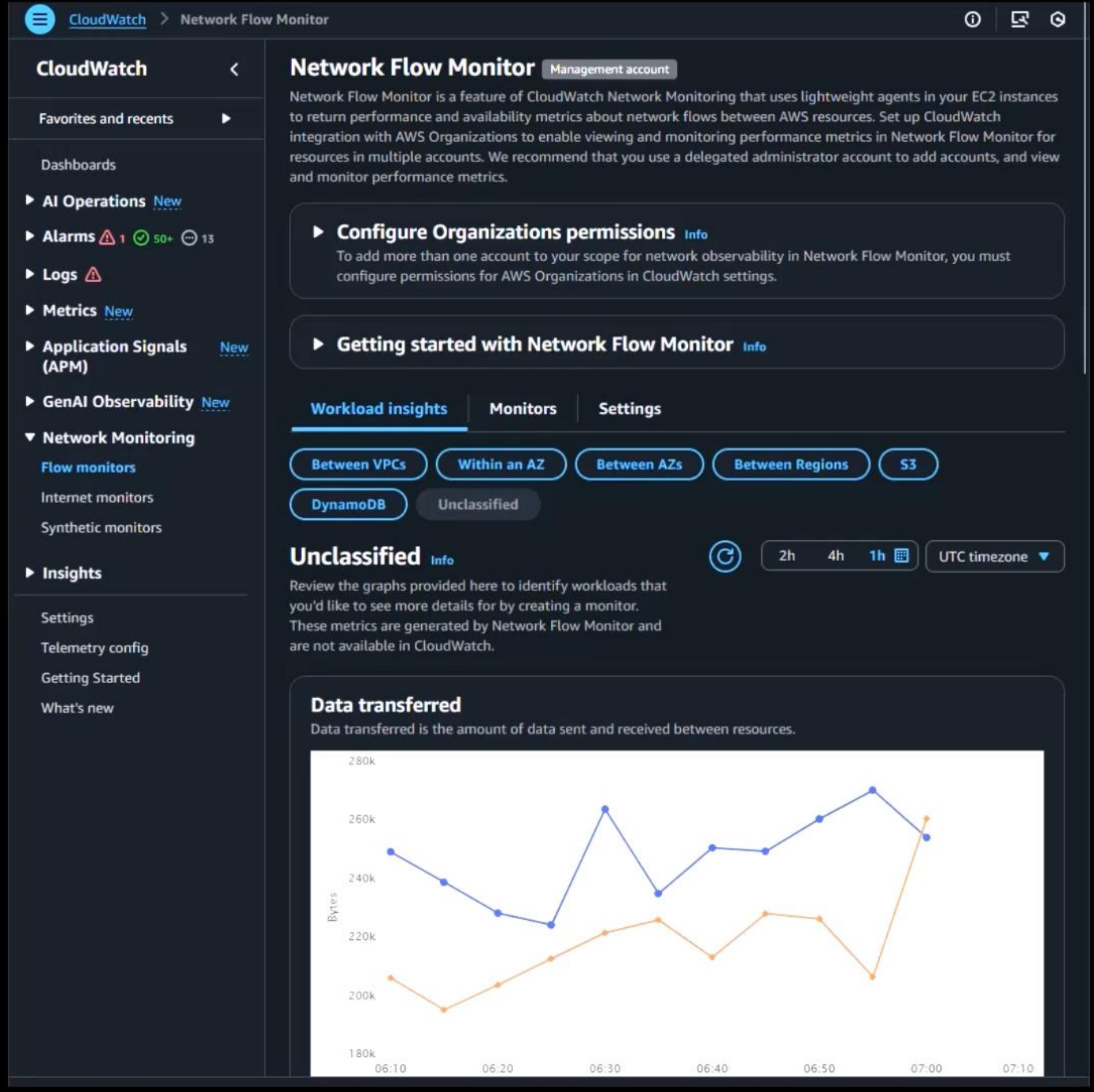
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/create_dashboard.html

Network

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



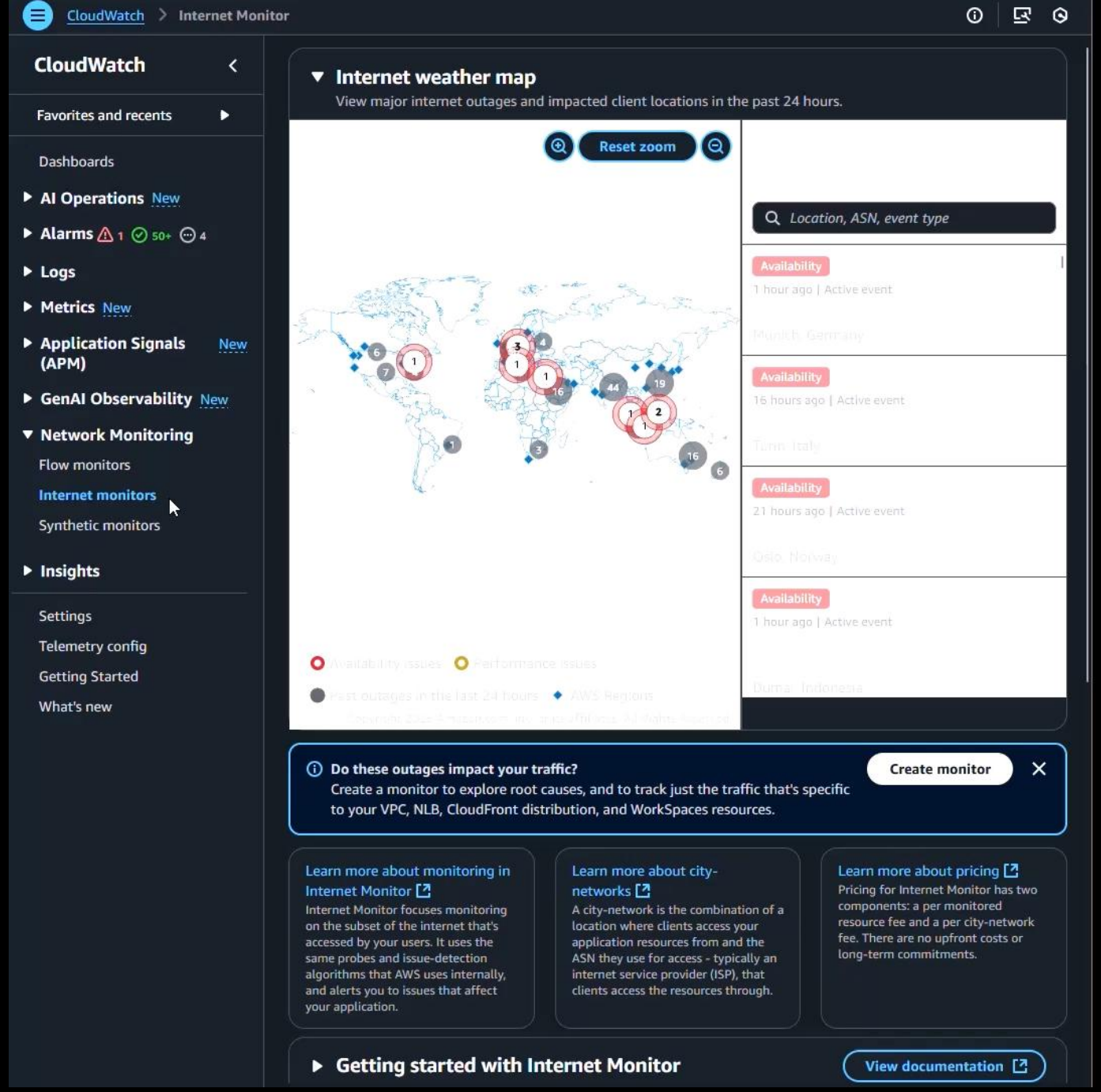
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch-NetworkFlowMonitor.html

NETWORK

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

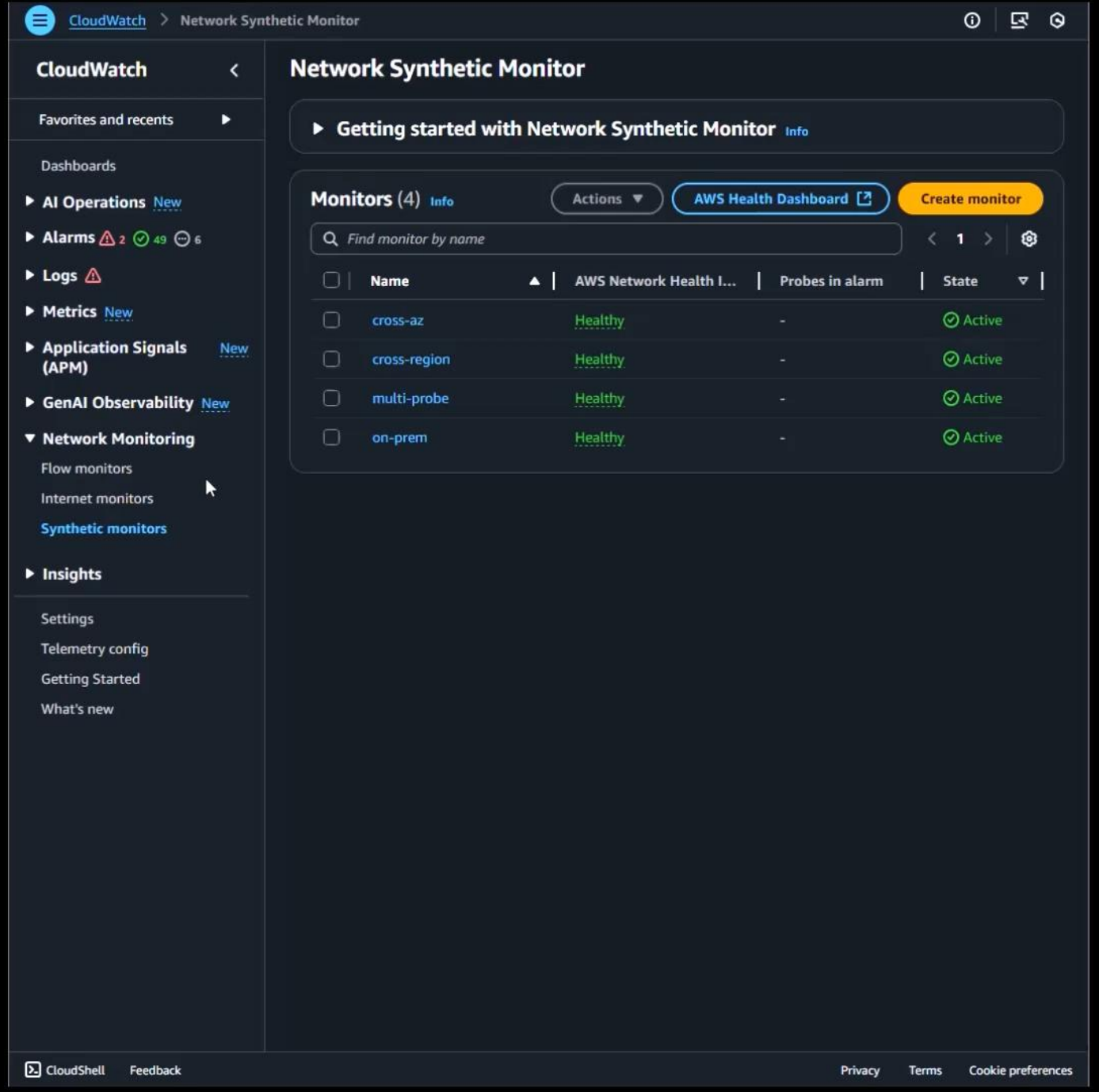


https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch-InternetMonitor.html

NETWORK

Synthetic Monitor (layer 4)

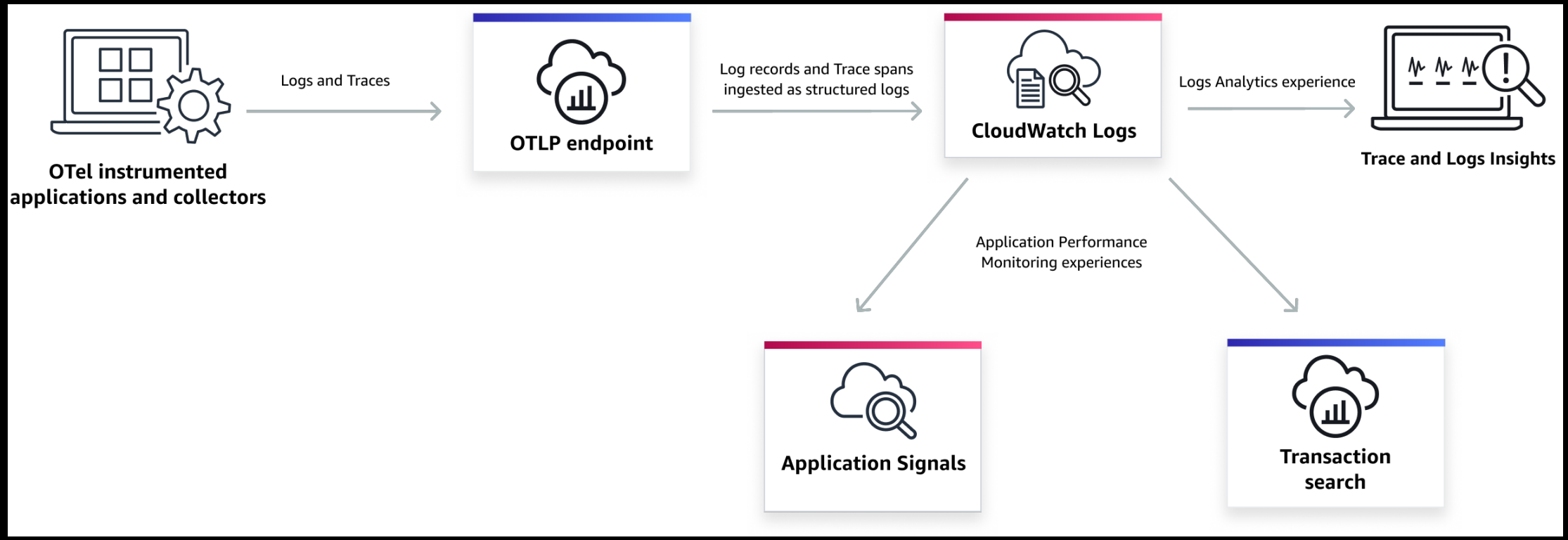
- visibility into the performance of the network connecting your AWS hosted applications to your on-premises destinations, and allows you to identify the source of any network performance degradation within minutes.



https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/what-is-network-monitor.html

OpenTelemetry

OpenTelemetry



Traces endpoint: https://xray.**AWS Region**.amazonaws.com/v1/traces
Logs endpoint: https://logs.**AWS Region**.amazonaws.com/v1/logs
Metrics endpoint: ???

https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch-OpenTelemetry-Sections.html

Resources

Learn with
One Observability workshop

Interactive Demo
CloudWatch Investigations

Learn with
Application Signals and CloudWatch Investigations workshop

Thank you!

Joe Alioto
Sr. Solutions Architect
AWS CloudOps
/josephalioto