

The background features a dark, almost black, field with several large, overlapping, semi-transparent shapes in shades of purple, magenta, and blue. Two thin, light-colored lines cross the scene diagonally, creating a sense of depth and movement. The overall aesthetic is modern and tech-oriented.

AWS re:Invent

DECEMBER 2 - 6, 2024 | LAS VEGAS, NV

COP379

Investigate operational issues faster with AI

Jared Nance

(he/him)

Principal Software Engineer
Amazon Web Services

Ania Develter

(she/her)

Senior Specialist Solutions
Architect
Amazon Web Services

Wei Tao

(he/him)

Principal Product Manager
Amazon Web Services



Reactive monitoring

Resolution



Blissful ignorance



Alarm

Enlightenment

Confusion

Root cause



Time passing by

Desperation

Stress

"Fix"
that doesn't work



False hope



Initial investigations

Agenda

01 AIOps and best practice

02 AIOps features in
Amazon CloudWatch

03 (New) AIOps features on AWS

04 Demo

05 Wrap-up

AIOps

- Not a magical solution that's going to save every one of your problems
- A set of algorithms and tools that use machine learning to accelerate humans by taking on the activities that machines can do really well
- No algorithm, machine, or human will be able to detect issues or **reason** about the performance of your systems **if the necessary signals aren't available**



AI/ML options for AIOps

Lots of effort

Do it yourself

ML:
Train models on your own (e.g., PyTorch on Amazon EC2, Amazon SageMaker)

Managed AI/ML:
e.g., Use Amazon Comprehend on your own data for natural language processing (NLP)

Gen AI:
e.g., Use Amazon Bedrock with local knowledge bases for Retrieval Augmented Generation (RAG)

Moderate effort

Use services with built-in AI/ML/genAI

Amazon CloudWatch metric anomaly detection

Amazon CloudWatch Logs anomaly and pattern analysis

Amazon DevOps Guru

Amazon Q Developer investigations

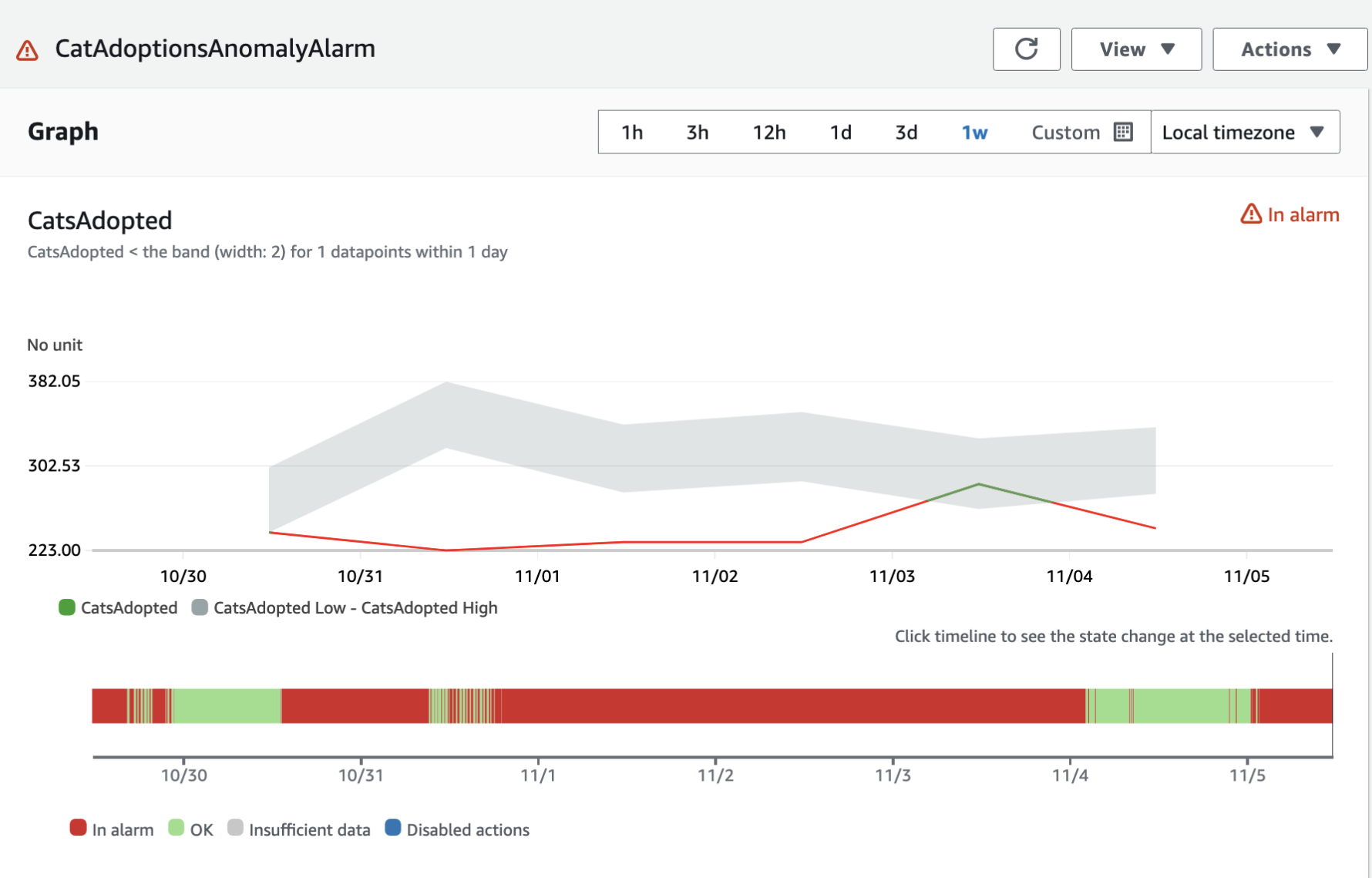
Least effort but even better with some good foundations

Best practice

- Consistent libraries (e.g., OpenTelemetry)
- Contextual information
- Standardized metrics
- Co-location with other telemetry
- Multiple perspectives



CloudWatch metric anomaly detection



Pick the right metric

```
import os
import time
from aws_lambda_powertools import Logger

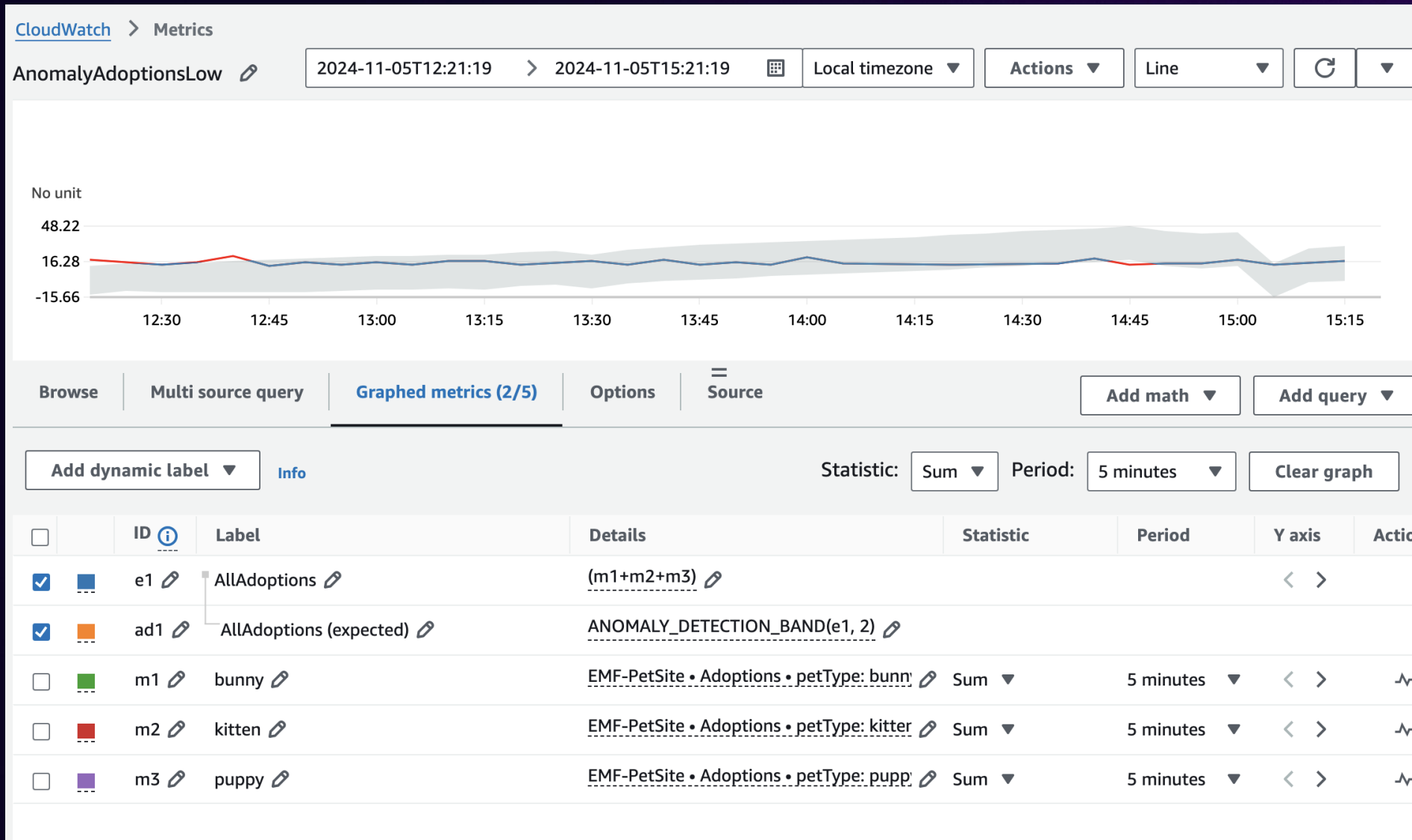
logger = Logger()

def log_with_embedded_metrics(petType, count, petColor, city, orderId, promotionType, redirectSource):

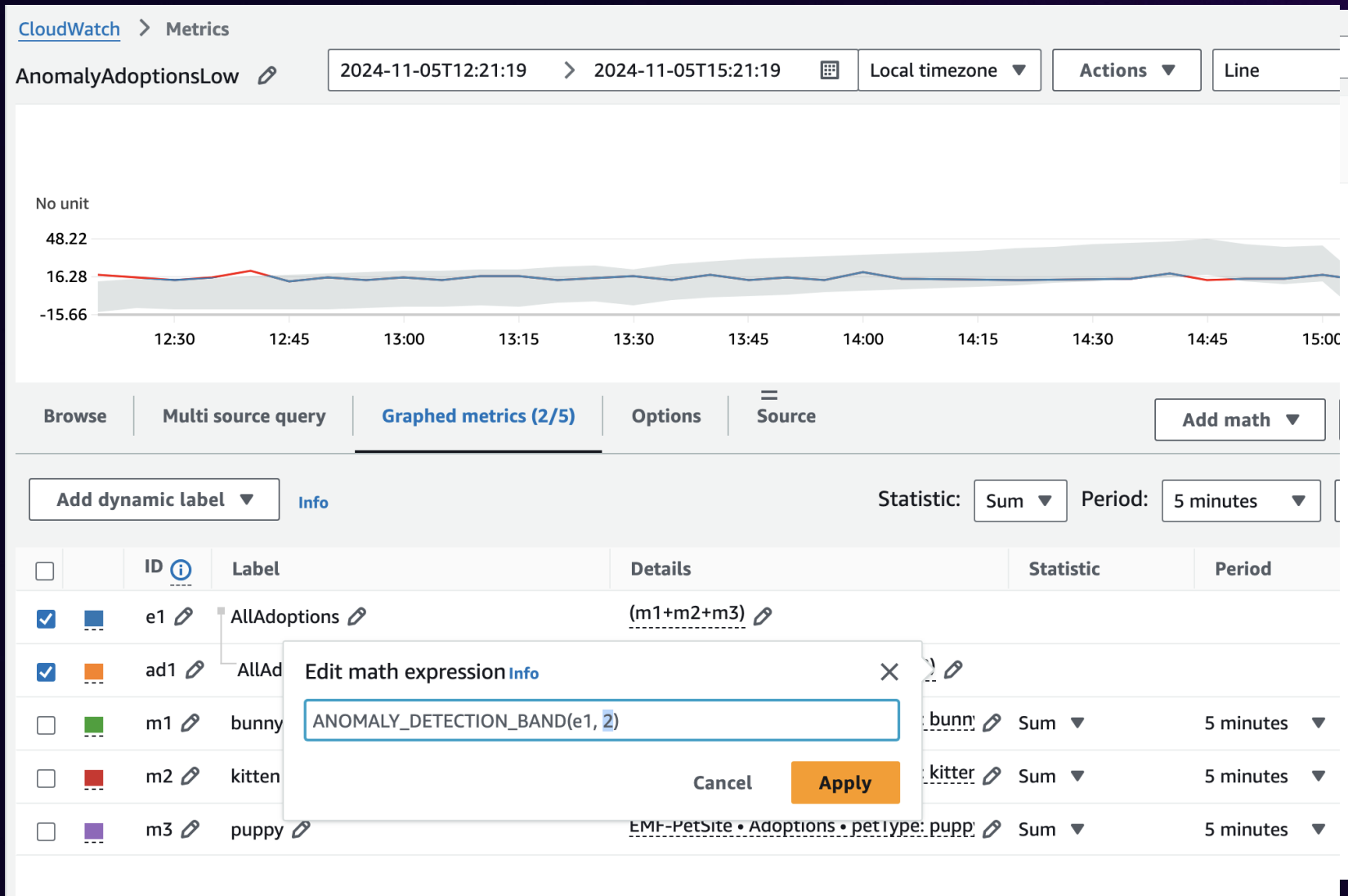
    log_object = {
        "_aws": {
            "Timestamp": int(time.time() * 1000),
            "CloudWatchMetrics": [
                {
                    "Namespace": "EMF-PetSite",
                    "Dimensions": [{"petType"}, {"color"}, {"petType", "color"}],
                    "Metrics": [
                        {
                            "Name": "Adoptions",
                            "Unit": "Count"
                        }
                    ]
                },
                {
                    "Namespace": "EMF-PetSite",
                    "Dimensions": [{"promotetype"}],
                    "Metrics": [
                        {
                            "Name": "Promotion",
                            "Unit": "Count"
                        }
                    ]
                }
            ]
        },
        "Adoptions": count,
        "color": petColor,
        "petType": petType,
        "Promotion": count,
        "promotetype": promotionType
    }

    logger.info(f'action=adoption petType={petType} orderId={orderId} promotetype={promotionType} redirect={redirectSource}', extra=log_object)
```

Metric anomaly visualization



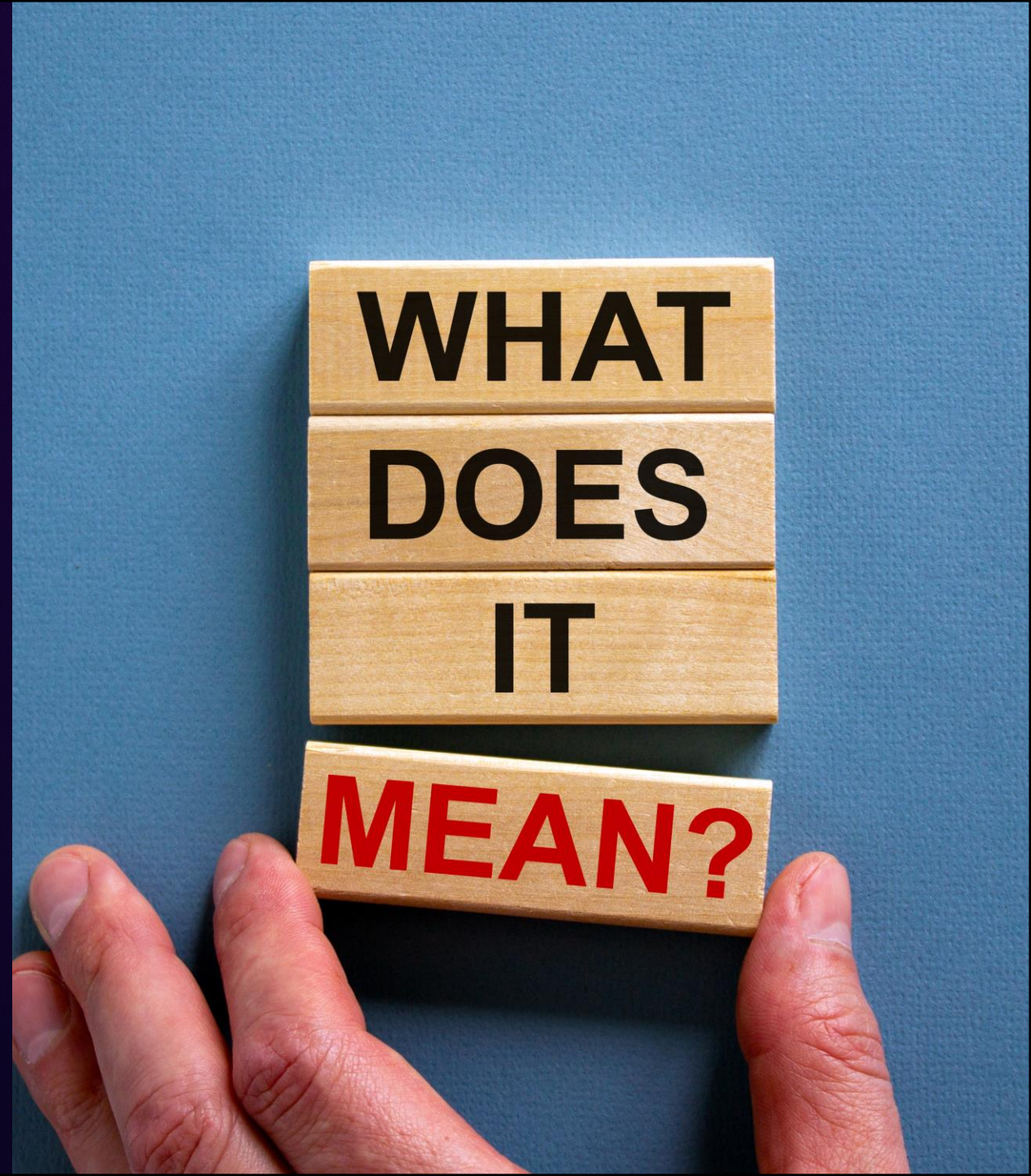
Anomaly detection considerations



- Think about standard deviations for the band (and adjust if required)
- Exclude specific time periods for unusual events
- Look out for sparse data (it will work, but is this the right metric?)
- Do you need to re-train your model?

Log data

- Structured log
- Consistent naming
- Words matter



CloudWatch log pattern analysis (reactive)

CloudWatch > Logs Insights

Logs Insights Info Start tailing 5m 30m 1h **3h** 12h Custom Compare

Select log groups, and then run a query or [choose a sample query](#).

Select up to 50 log groups. Browse

/aws/lambda/AppConfigLambdaDemo-functionF19B1A04-hQrfnnDwWpp /aws/lambda/lambda-for-log-anomaly-demo /aws/lambda/obs-demo-EMFLambda-8yLwTa0MesM7

andevl CCA and COM 113811220673 Observability workshop account 873497083499 Observability workshop account 873497083499

Clear all

Show fewer chosen log groups

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

[Query generator](#)

Run query Cancel Save History

Logs Insights query can run for maximum of 60 minutes.

Logs (608) Patterns (-) Visualization

Logs (608) Export results

Showing 608 of 608 records matched ⓘ
608 records (97.2 kB) scanned in 0.9s @ 706 records/s (113.0 kB/s)

#	@timestamp	@message	@logStream	@log
▶ 1	2024-11-05T12:23:06.1...	END RequestId: 8b672a0e-1274-48fa-b112-b6fd78234f55	2024/11/05/[\$LATEST]60df3c66f23e4dd2b3707466da0de3f1	873497083499:/aws/lambda/lambda-for-log-
▶ 2	2024-11-05T12:23:06.1...	REPORT RequestId: 8b672a0e-1274-48fa-b112-b6fd78234f55 Duration: 338...	2024/11/05/[\$LATEST]60df3c66f23e4dd2b3707466da0de3f1	873497083499:/aws/lambda/lambda-for-log-
▶ 3	2024-11-05T12:23:06.0...	[DEBUG] 2024-11-05T12:23:06.068Z, 8b672a0e-1274-48fa-b112-b6fd78234f5...	2024/11/05/[\$LATEST]60df3c66f23e4dd2b3707466da0de3f1	873497083499:/aws/lambda/lambda-for-log-

- Search log data and detect patterns across multiple log groups and accounts
- Answer – what has changed?

CloudWatch log anomaly detection (proactive)

Specify metric and conditions

Metric

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

Count

1.00

0.50

0

10:00 11:00 12:00

AnomalyCount

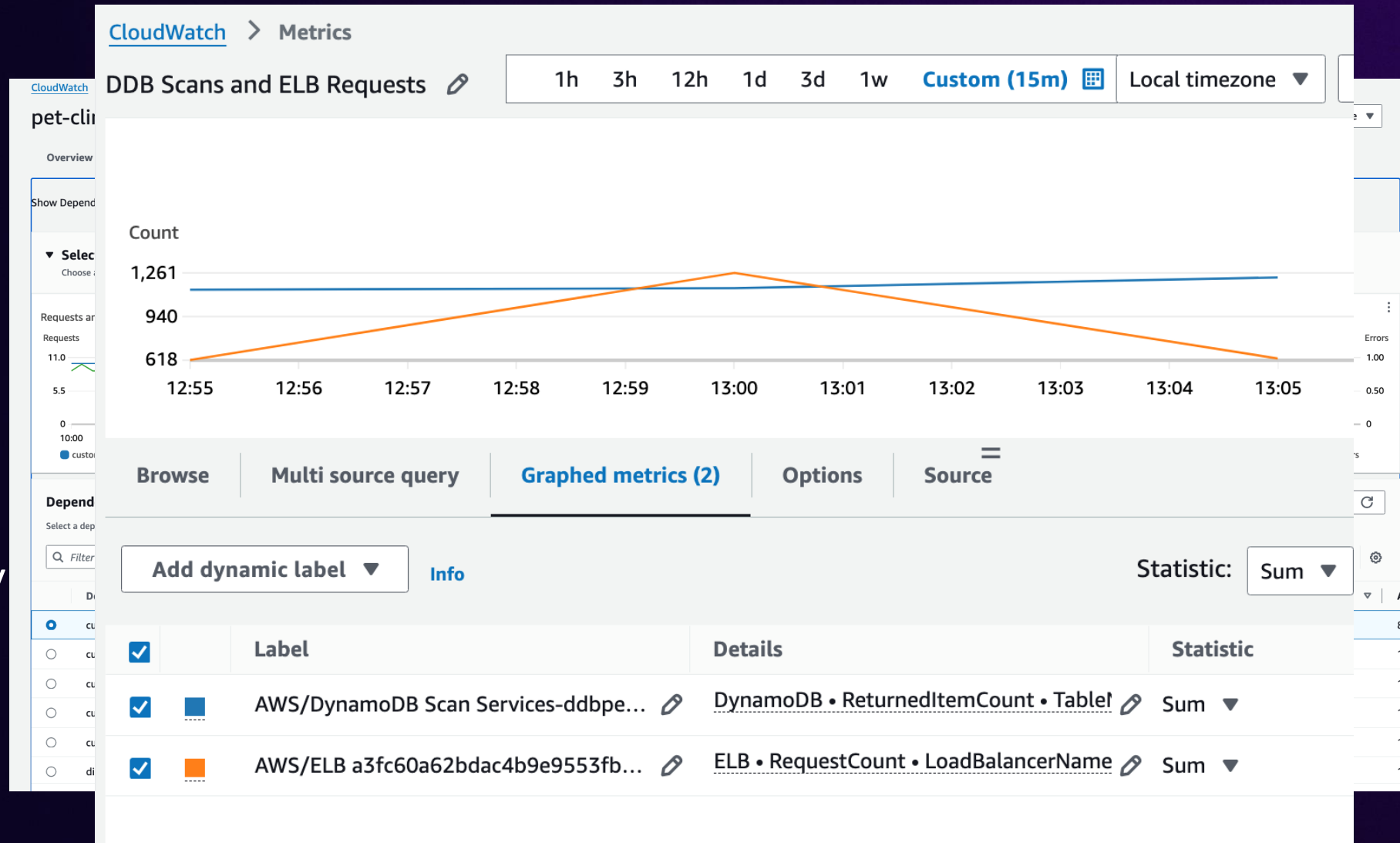
Configuration:

- Namespace: AWS/Logs
- Metric name: AnomalyCount
- LogAnomalyPriority: HIGH
- LogAnomalyDetector: logs-anomaly-detector
- Statistic: Sum
- Period: 5 minutes

- Create anomaly detector to examine log data as it is ingested
- Create alarms based on severity
- Suppress stuff that does not matter (or filter it out)

Understanding relationship, causality, and reasoning

- Unknown unknowns (find other patterns)
- Map dependencies
- Correlation vs. causality



(New) AIOps features on AWS





Explore related with CloudWatch

- Explore related telemetry from **anywhere in the AWS console**
- Quickly **navigate across related AWS resources** with persistent side panel
- **Contextual deep links** to AWS service consoles emitting telemetry
- Use key-value pair **tags to filter and drill down** resources
- **No additional setup or configuration** required

ApiGateway2

Throttle Copy ARN Actions

Function overview Info

Export to Infrastructure Composer Download

Diagram Template

ApiGateway2

Layers (0)

EventBridge (CloudWatch Events)

+ Add trigger

+ Add destination

Description
-

Last modified
[5 months ago](#)

Function ARN
[arn:aws:lambda:us-east-1:123456789012:function:ApiGateway2](#)

Function URL Info
-

Code | Test | **Monitor** | Configuration | Aliases | Versions

Monitor Info

View CloudWatch logs View Application Signals View X-Ray traces View Lambda Insights View CodeGuru profiles

Filter metrics by **Function**

Alarm recommendations

1h 3h 12h 1d 3d 1w Custom UTC timezone

CloudWatch metrics



Operational investigations with Amazon Q Developer


- **Omnipresent** assistant across AWS consoles
- Guided root cause analysis with **AWS operations expertise**
- Automatically examines **wide range of data** such as telemetry, deployment, and AWS Health events, etc.
- **Auto-start** investigations from **alarms**
- **Collaborative** investigation notebook
- **End-to-end** integrations through chat, runbooks, etc.


cwsyn-pc-add-visit-b478821e-e1af-47ce-8dbc-eab301f20563

Throttle Copy ARN Actions

Function overview Info

Diagram Template

 **cwsyn-pc-add-visit-b478821e-e1af-47ce-8dbc-eab301f20563**

 Layers (2)

+ Add trigger

+ Add destination

Export to Infrastructure Composer Download

Description
-

Last modified
[1 month ago](#)

Function ARN
[arn:aws:lambda:us-east-1:123456789012:function:cwsyn-pc-add-visit-b478821e-e1af-47ce-8dbc-eab301f20563](#)

Function URL Info
-

Code | Test | **Monitor** | Configuration | Aliases | Versions

Monitor Info

View CloudWatch logs View Application Signals View X-Ray traces View Lambda Insights View CodeGuru profiles

Filter metrics by **Function**

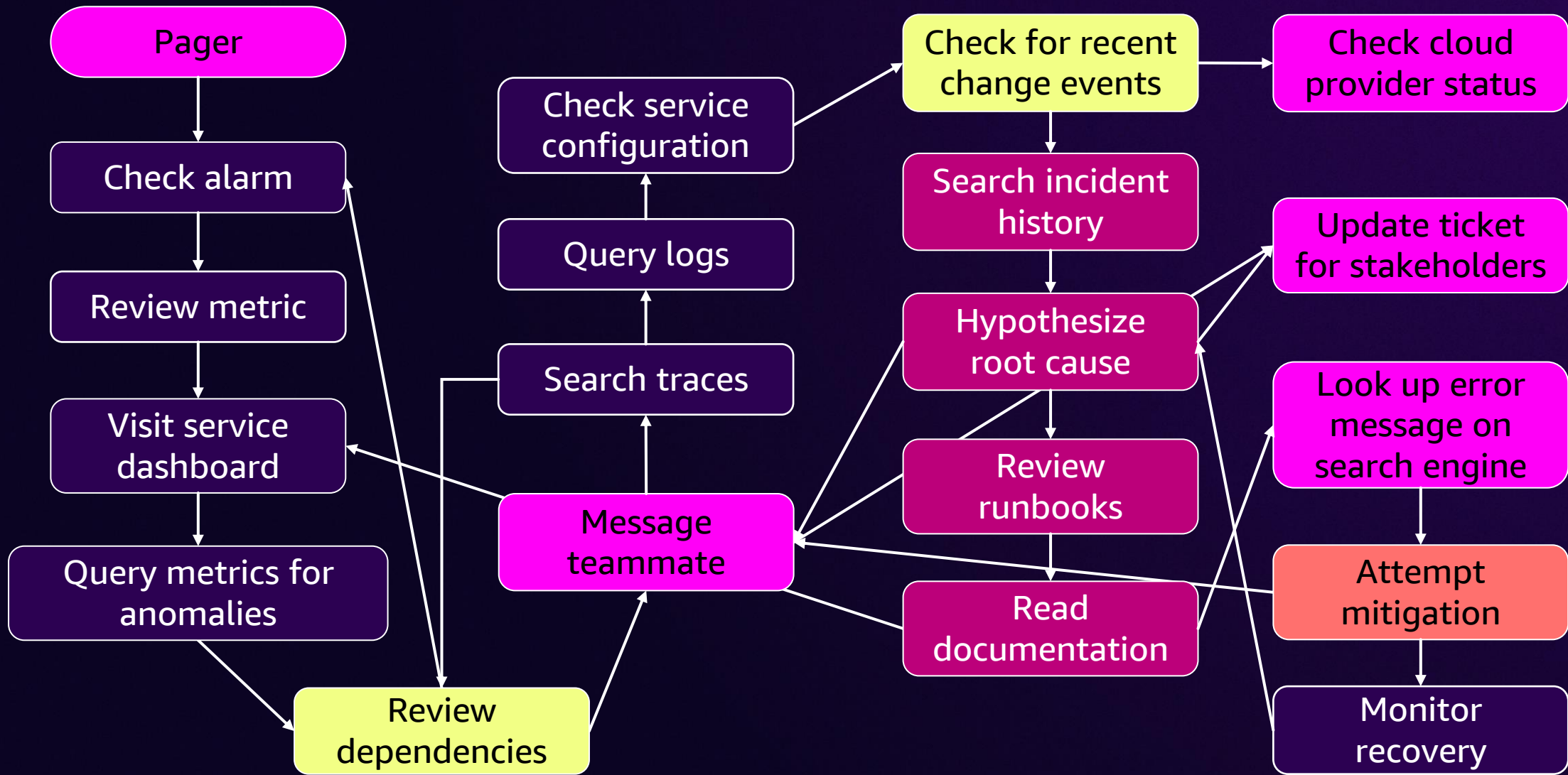
Alarm recommendations

1h 3h 12h 1d 3d 1w Custom UTC timezone

CloudWatch metrics

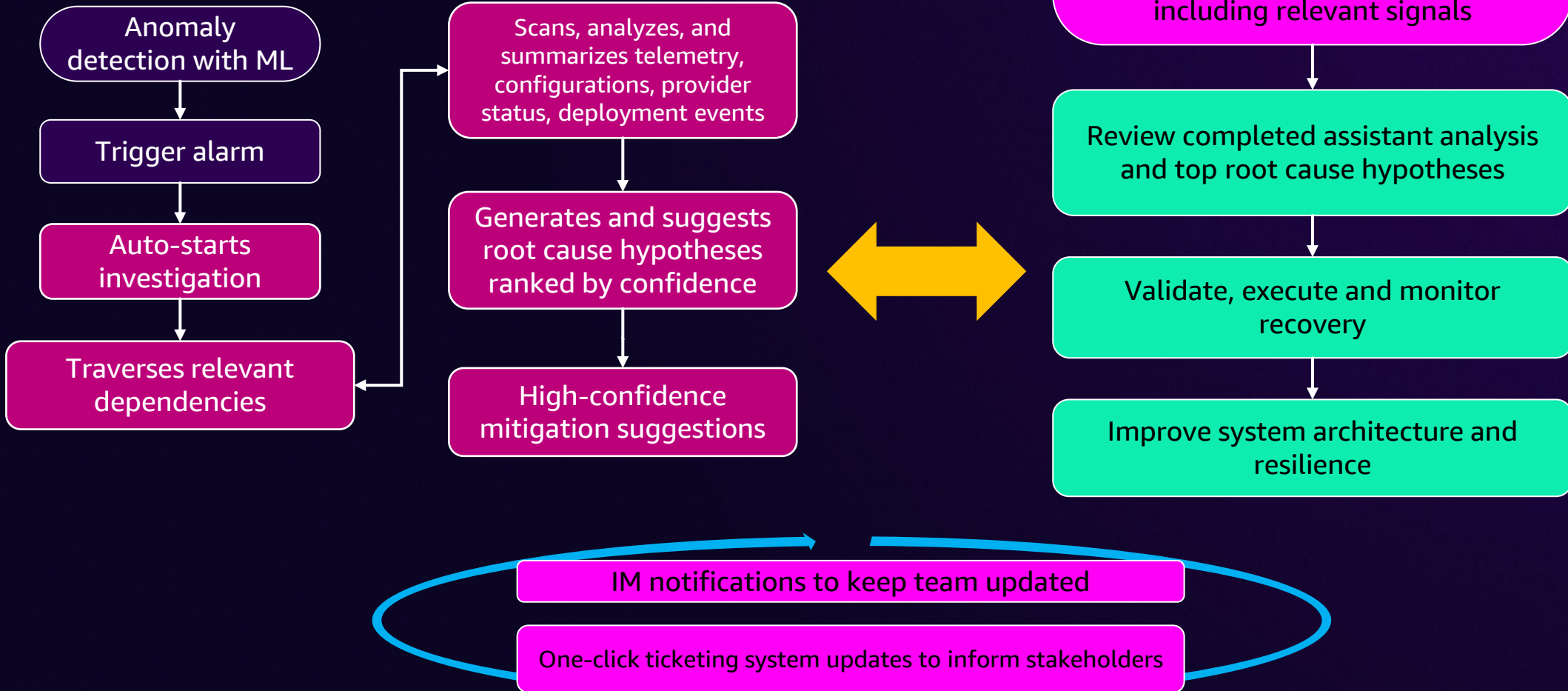


Effortlessly navigate your system and telemetry
and troubleshoot operations issues



Amazon Q Developer

Human operator



Demo



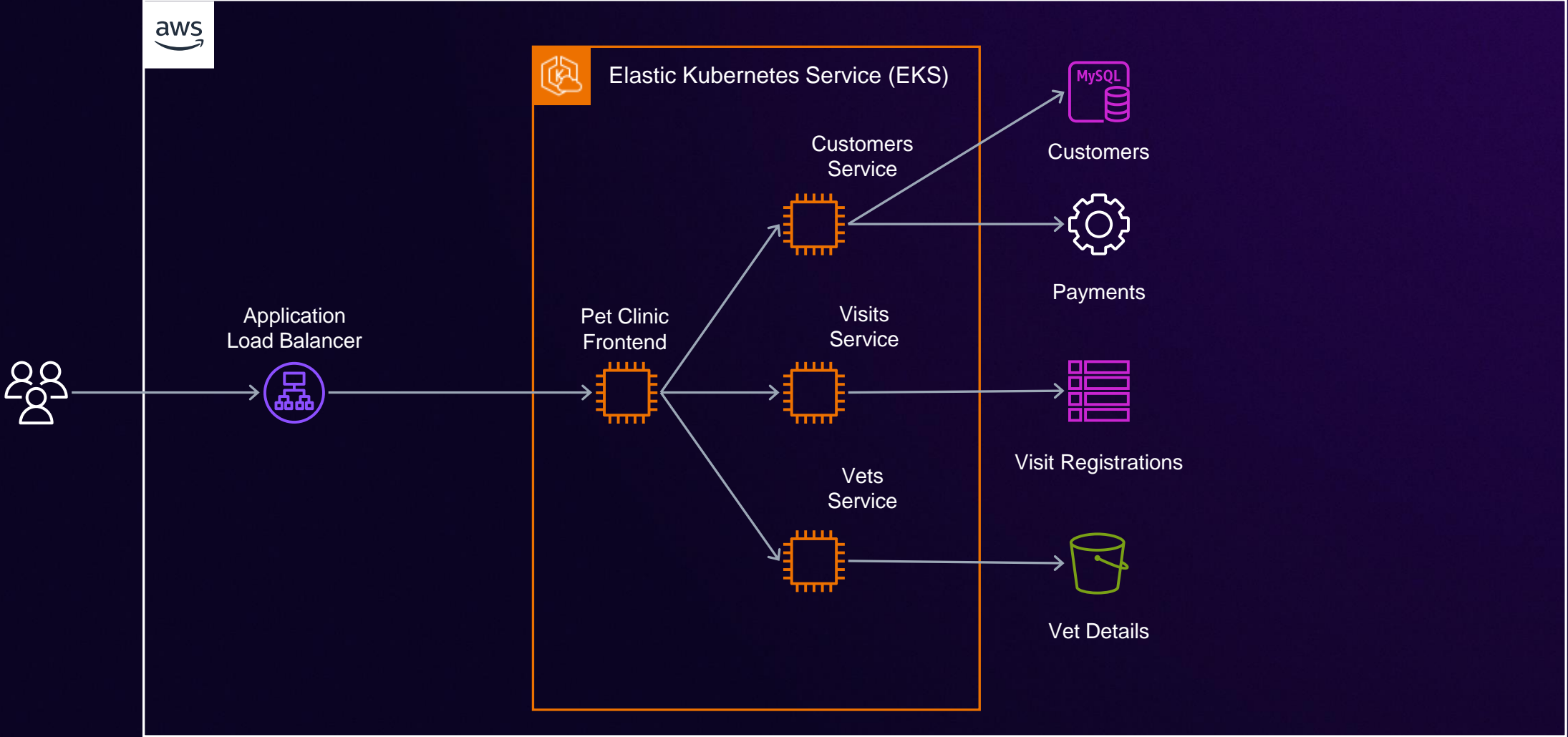
Pet clinic application

The screenshot shows a web application for a pet clinic. At the top, there is a navigation bar with the 'spring' logo on the left and three menu items: 'HOME', 'OWNERS', and 'VETERINARIANS'. The 'OWNERS' menu item is highlighted in green. Below the navigation bar, the page title 'Owners' is displayed. A search filter input field is located below the title. The main content is a table with five columns: Name, Address, City, Telephone, and Pets. The table contains ten rows of owner data.

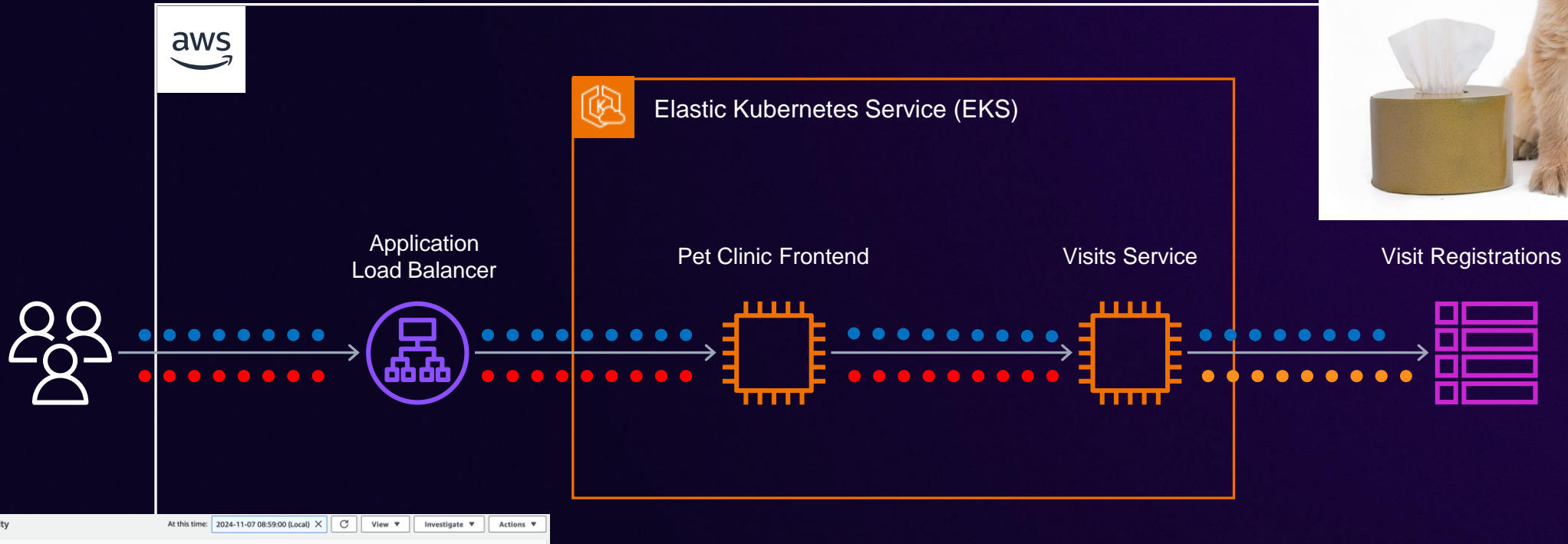
Name	Address	City	Telephone	Pets
George Franklin	110 W. Liberty St.	Madison	6085551023	Leo
Betty Davis	638 Cardinal Ave.	Sun Prairie	6085551749	Basil
Eduardo Rodriquez	2693 Commerce St.	McFarland	6085558763	Jewel Rosy
Harold Davis	563 Friendly St.	Windsor	6085553198	Iggy
Peter McTavish	2387 S. Fair Way	Madison	6085552765	George
Jean Coleman	105 N. Lake St.	Monona	6085552654	Max Samantha
Jeff Black	1450 Oak Blvd.	Monona	6085555387	Lucky
Maria Escobito	345 Maple St.	Madison	6085557683	Mulligan
David Schroeder	2749 Blackhawk Trail	Madison	6085559435	Freddy
Carlos Estaban	2335	Waunakee	6085555487	Lucky Sly



Pet clinic application



/api/BookVisit



1. Frontend is impacted by VisitsService
2. VisitsService is impacted by throttling on VisitRegistrations table
3. VisitRegistrations table is throttling because Consumed IOPS > Provisioned
4. Increase in load is coming from a **single tenant**

Setup and configuration

The essentials

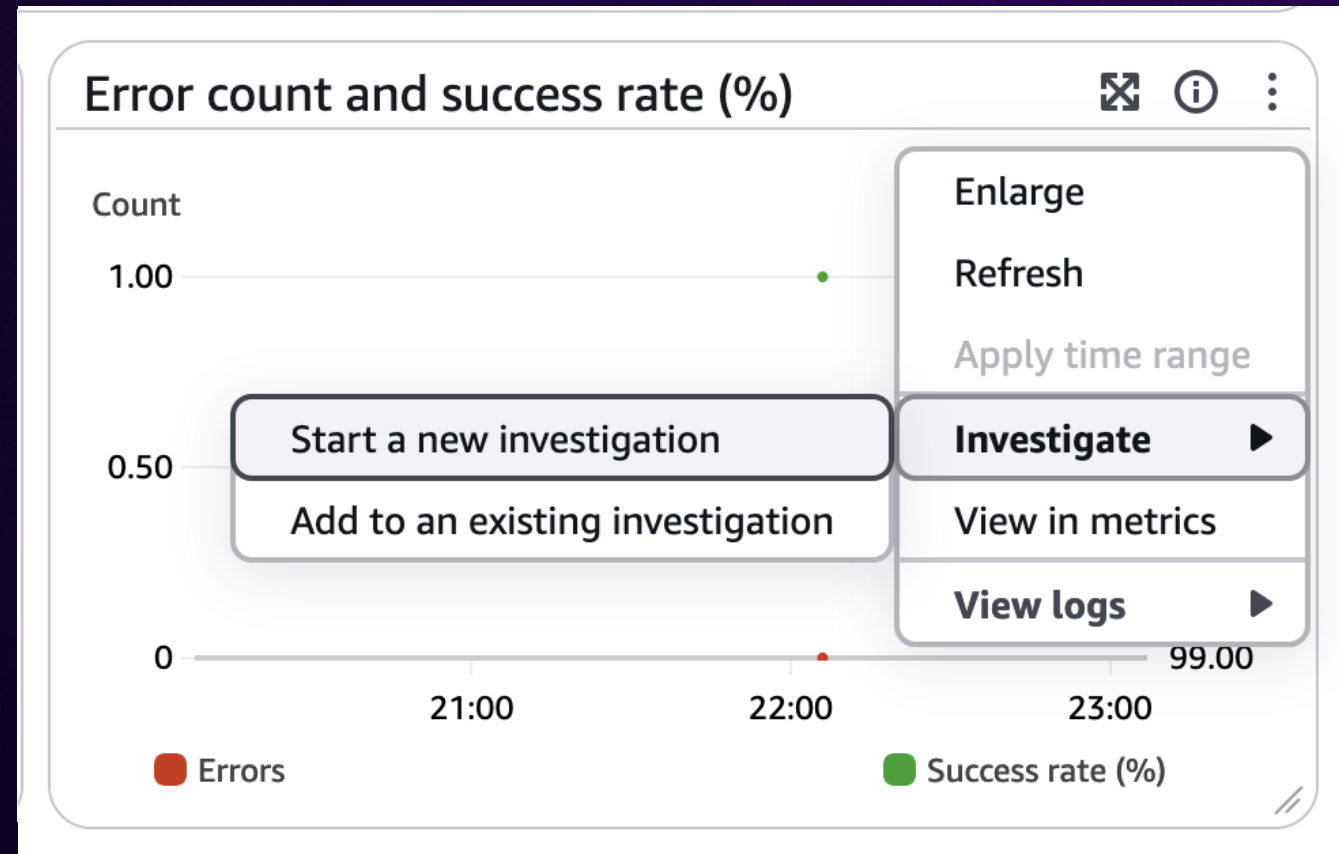
- Create an investigation group
- Configure access permissions for Amazon Q Developer

Best practices

- Application topology (Application Signals, AWS X-Ray, CloudWatch agent)
- AWS CloudTrail Logs
- "Investigation action" on your composite alarms

Creating investigations

- 1 Auto Triggered Investigation:** Set up “investigation action” on your CloudWatch alarms
- 2 Amazon Q Chat:** Ask questions such as “Why am I paged” to receive initial diagnostics and instructions to kick off an investigation
- 3 Omnipresent “operational troubleshooting” side panel:** Select “investigate” while viewing your CloudWatch telemetry widgets across 80+ AWS service consoles



Wrapping up

Start with good foundations



Observability best practices guide

Keep up to date and experiment



One Observability workshop

Check out Amazon Q Developer



Try a sample investigation

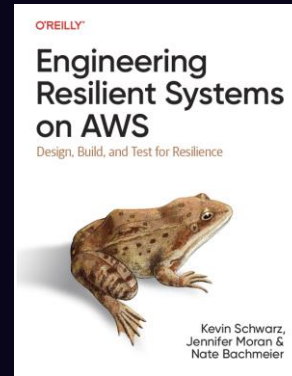


Cloud Ops kiosks

Cloud Operations | Observability | Governance & Compliance | Resilience | Cloud Financial Management



**VR
EXPERIENCE**



**BOOK
GIVEAWAYS**



SWAG

MEET US AT THE KIOSKS IN THE AWS VILLAGE

Thank you!

Jared Nance

[linkedin.com/in/jaredcnance](https://www.linkedin.com/in/jaredcnance)

Ania Develter

[linkedin.com/in/ania-develter](https://www.linkedin.com/in/ania-develter)

Wei Tao

[linkedin.com/in/wtweitao](https://www.linkedin.com/in/wtweitao)



Please complete the session survey in the mobile app