# AWS Monitoring & Observability

## Actionable insights using CloudWatch Logs

Ashok Swaminathan
Principal Product Manager, CloudWatch

# Agenda

1. **CloudWatch Logs overview**
   - Enable insights and alerts
   - Analyze logs during operational troubleshooting
   - Detect and protect sensitive data
   - Build a holistic, observability view

2. **Recent launches**

3. **Demo**

# Foundation for observability: data drives decisions

Logs

Metrics

Traces

AWS monitoring and observability services help you maintain SLAs by **detecting, investigating,** and **remediating problems** to achieve

Availability

Reliability

Performance

# CloudWatch Logs

- Fully managed service – supporting exabyte scale log ingestion and storage
- Move logs (infrastructure, application, service logs) off of your hosts and store them in secure and durable storage
- Set automatic retention policies
- Create metrics and alarms from your logs
- Analyze logs using queries

# Logs Use Cases

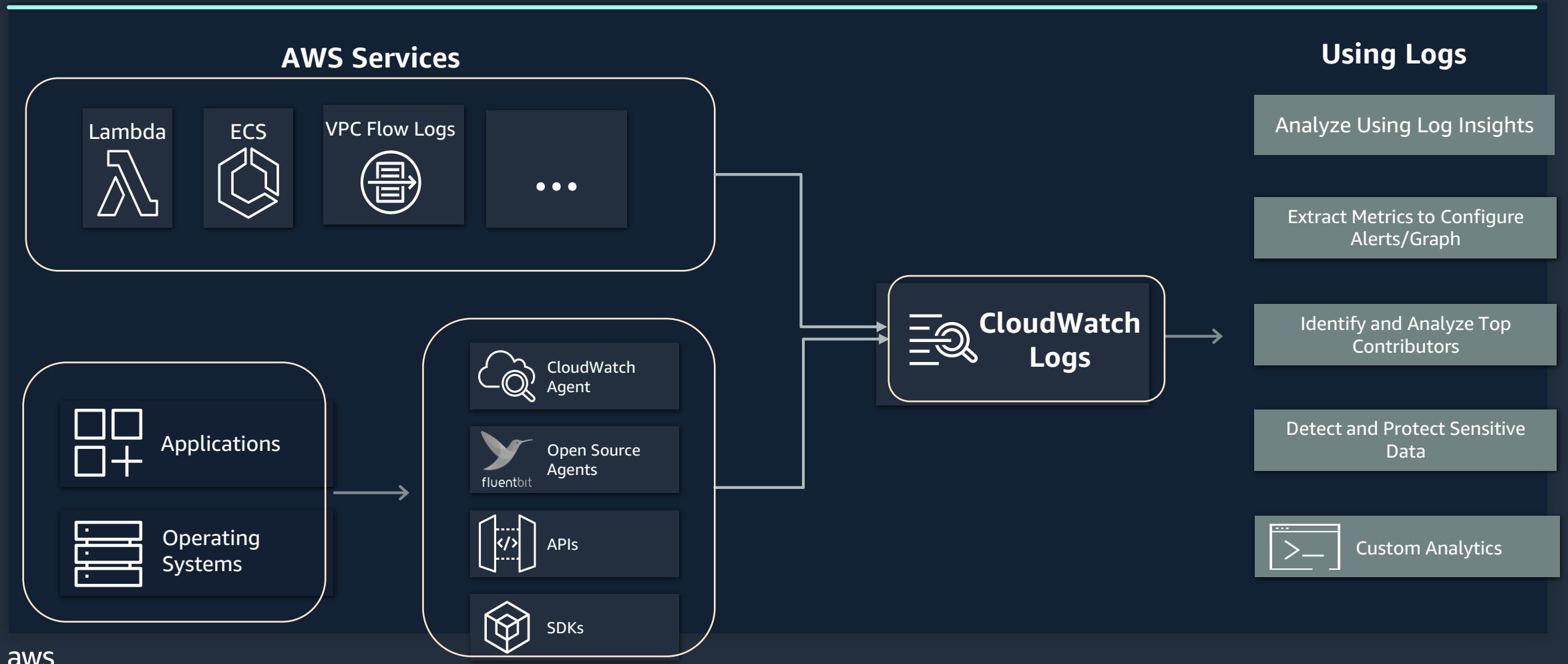
**Application Troubleshooting**

**Infrastructure Monitoring**

**Security and Compliance**

**Business Insights**

# How It Works

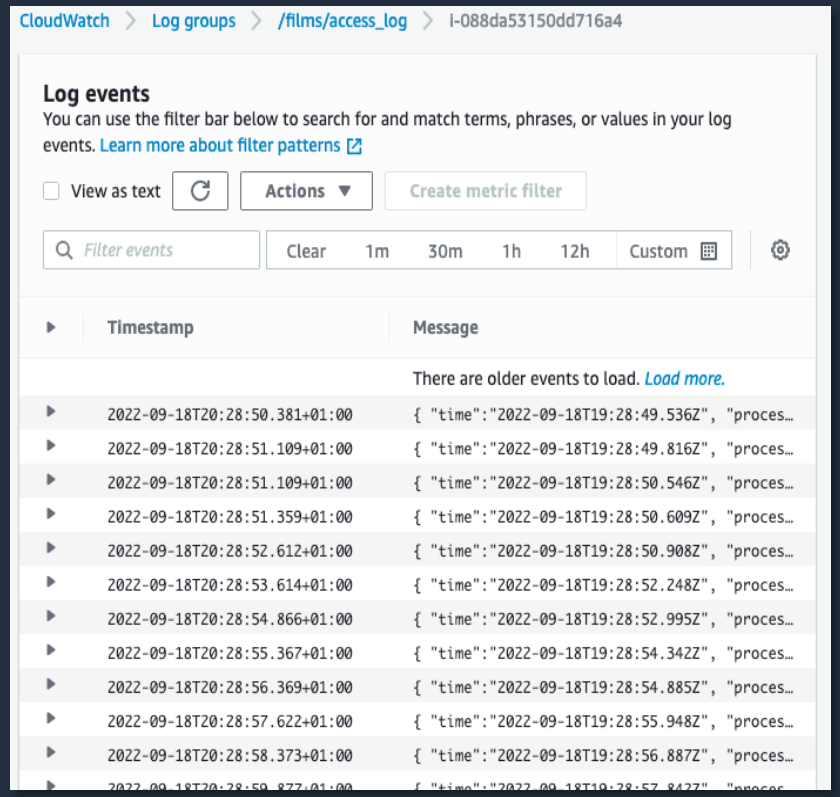


# Terminology: Log Events, Steams, Groups

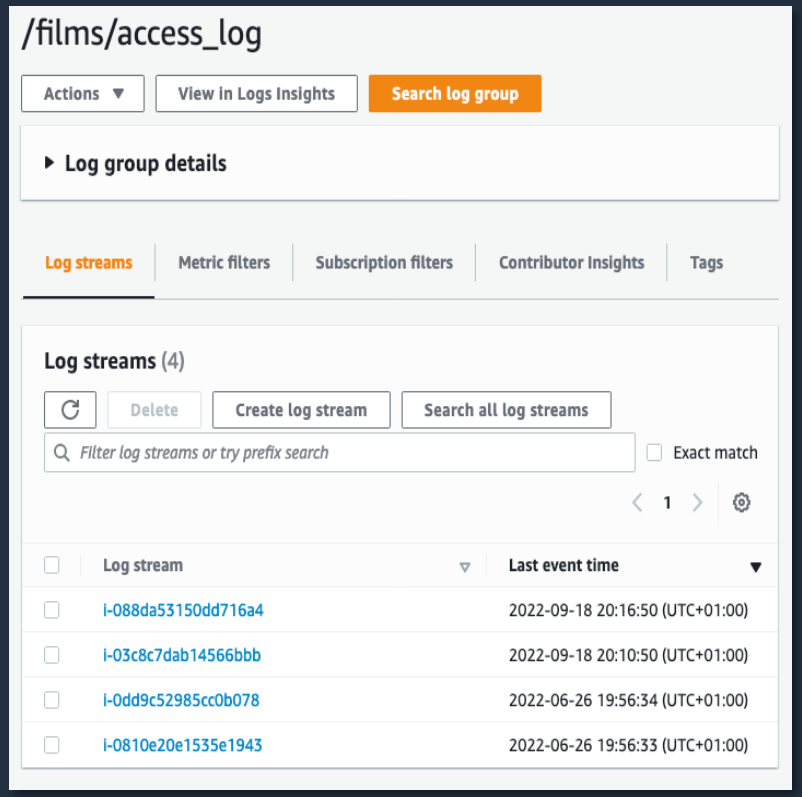
## Log Event


```
{
   "time": 2022-11-01T16:00:00.000Z",
   "remoteIP": "10.0.155.113",
   "host": "10.0.53.21",
   "request": "/index.php",
   "query": "",
   "method": "GET",
   "status": "200",
   "userAgent": "ELB-HealthChecker/2.0",
   "referer": "-"
}
```


## Log Stream

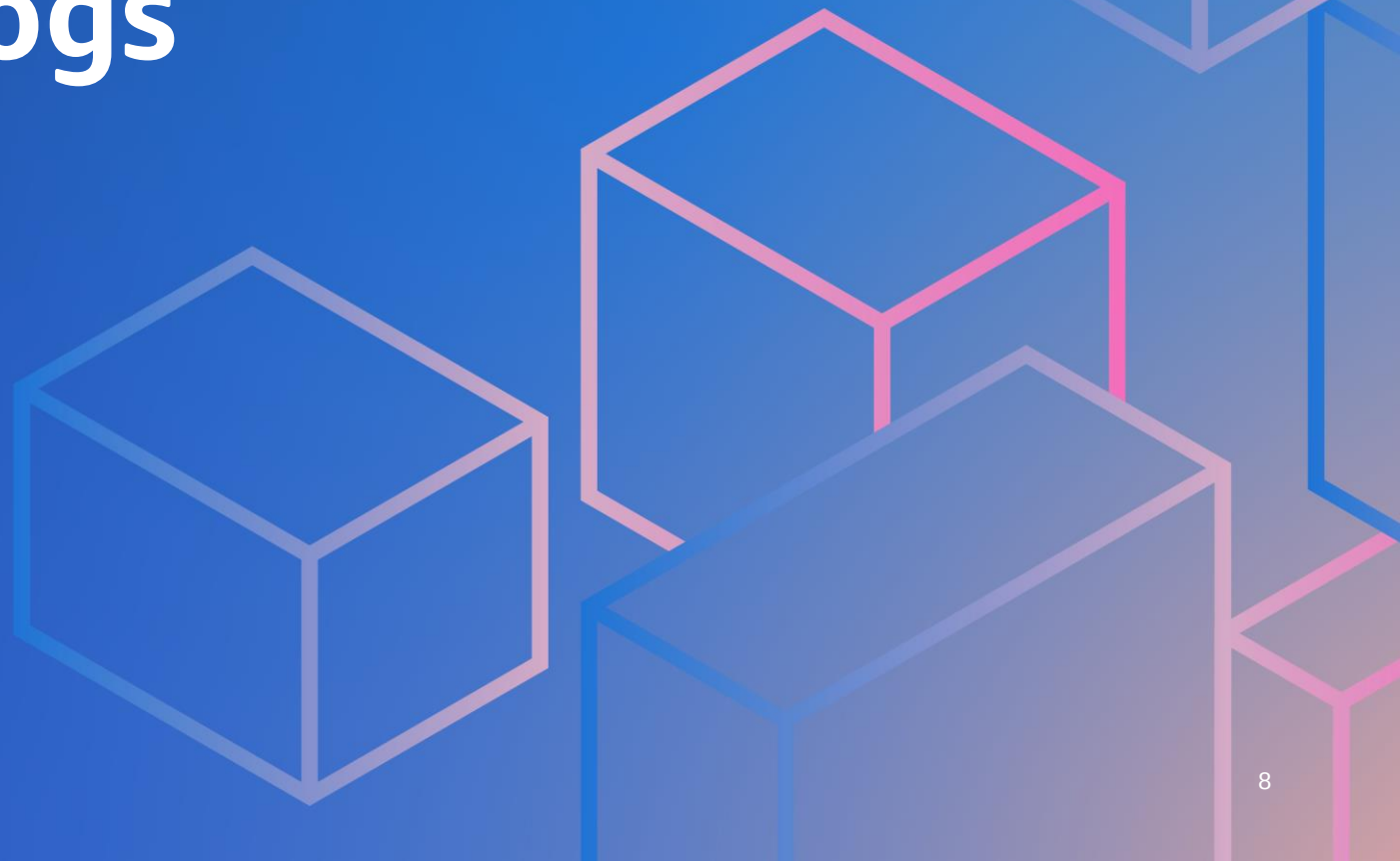



## Log Group




***Retention policies at Log Group level***

# Operationalize Logs



# Operationalize Logs

**Enable Insights and Alerts**

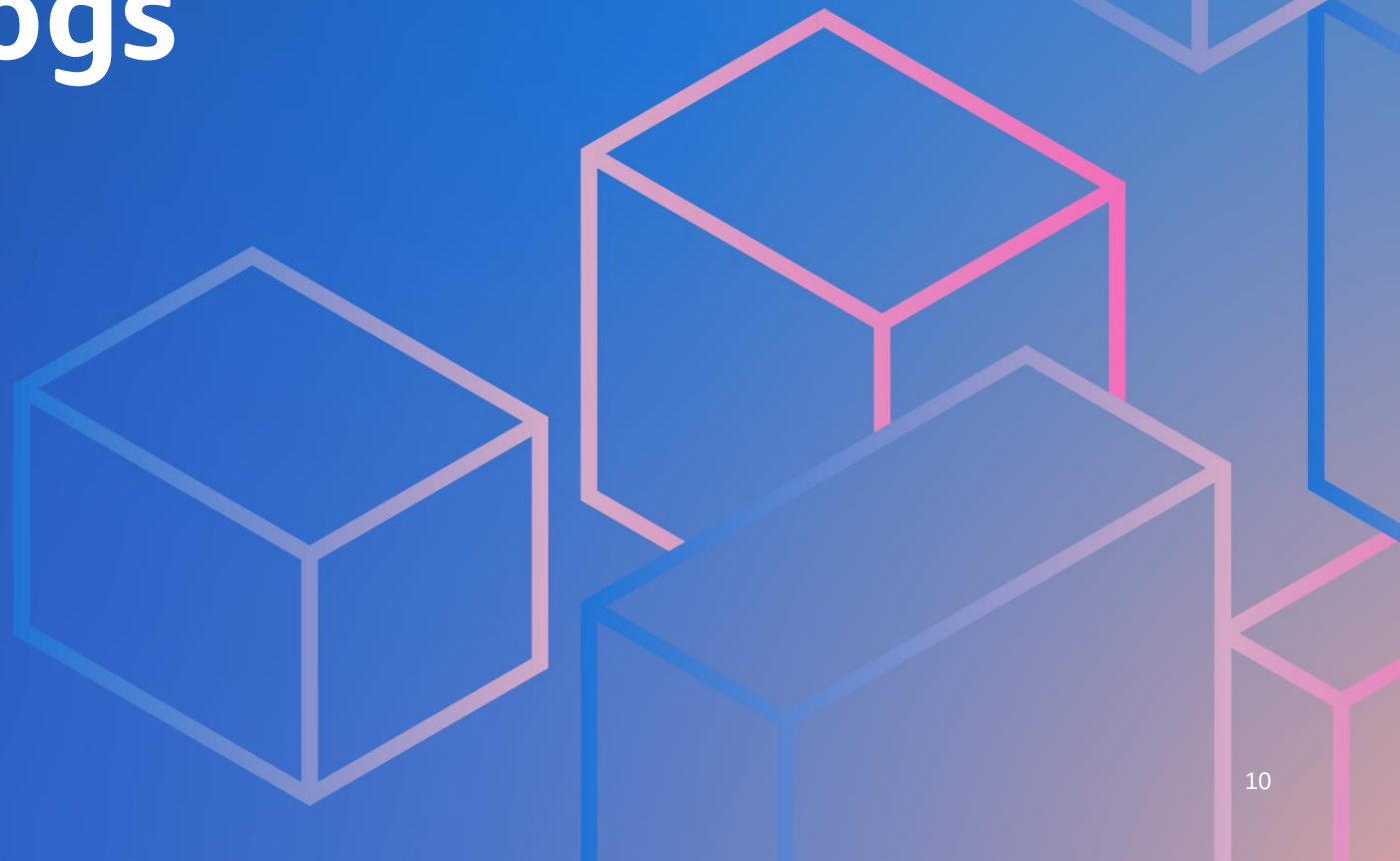
**Detect and Protect Sensitive Data**

**Analyze Logs During Troubleshooting**

**Build a holistic, observability view**

# Operationalize Logs

## Enable Insights and Alerts



# Enable Insights and Alerts

1. Graph and Alert on Metrics Extracted From Logs

2. Identify and Analyze top contributors - Contributor Insights

3. Analyze High Cardinality Data – using Embedded Metric Format

# Graph and Alert on Metrics Extracted From Logs

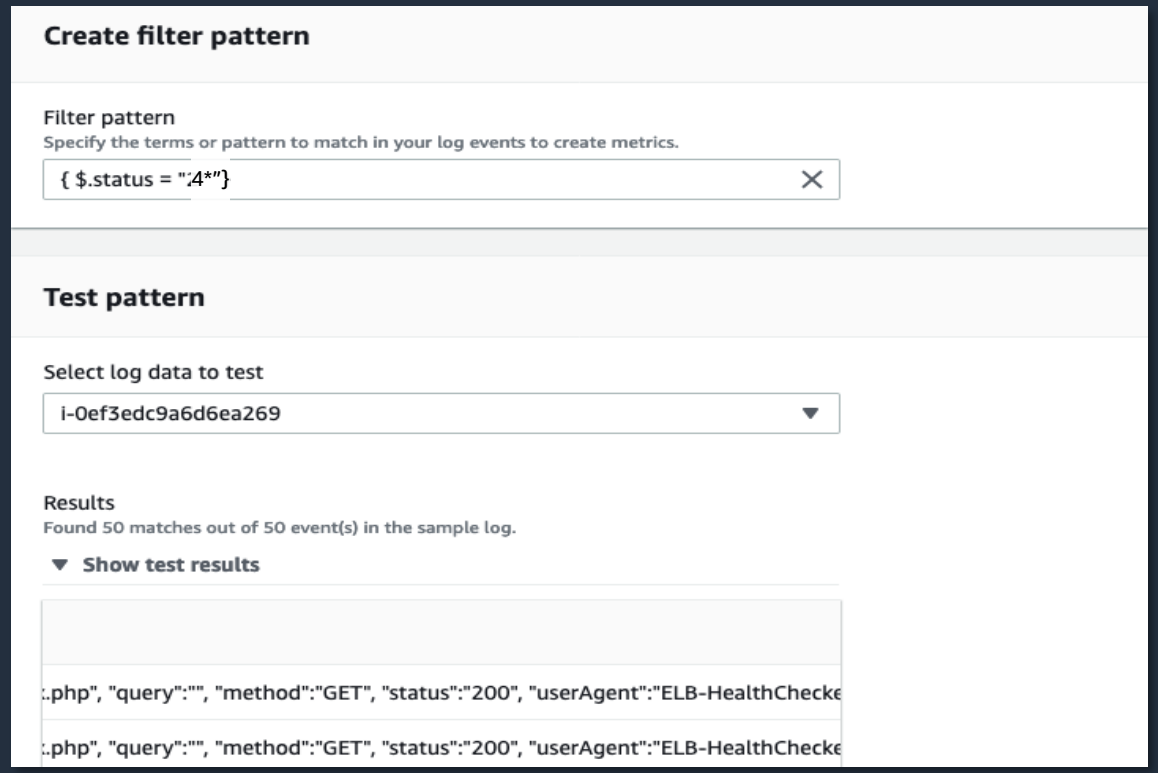
METRIC FILTERS

**Example:**

- Detect errors such as 4xx, 5xx and if they exceed threshold
- Continuously monitor logs for unexpected actions – e.g: security events (login failures)

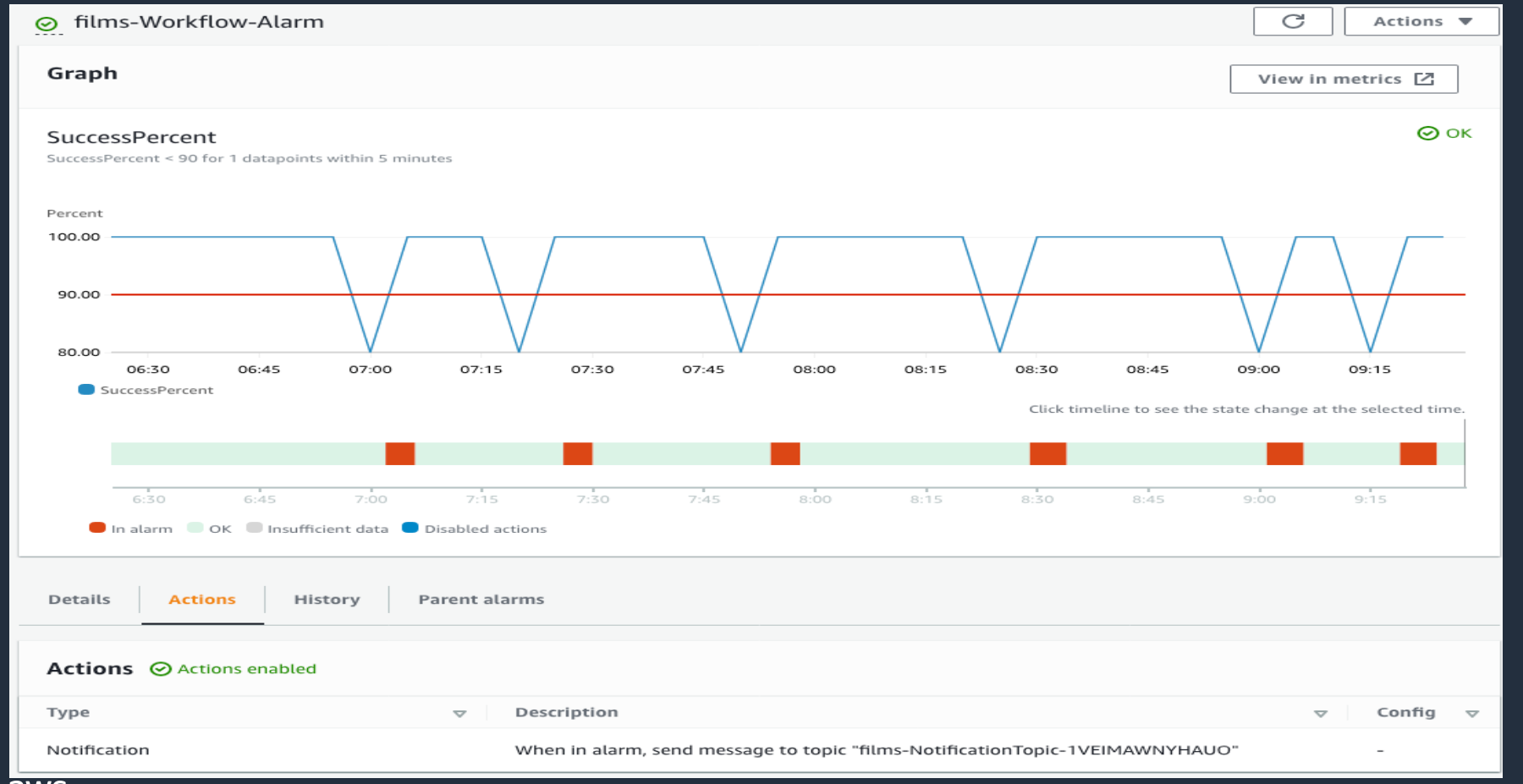
Filter log data as it is ingested based on patterns in logs – to create metrics

Configure Alarms on metrics or add to dashboards



# Metric Based Alarm

Create metric on success rate and notify, based on 5 minute duration



# Identify Top Contributors –Contributor Insights

## Surface outliers and top talkers

Cost effectively analyze and visualize high cardinality data in CloudWatch Logs - build rules from scratch or use sample rules that AWS has created

## Identify impacted users and resources

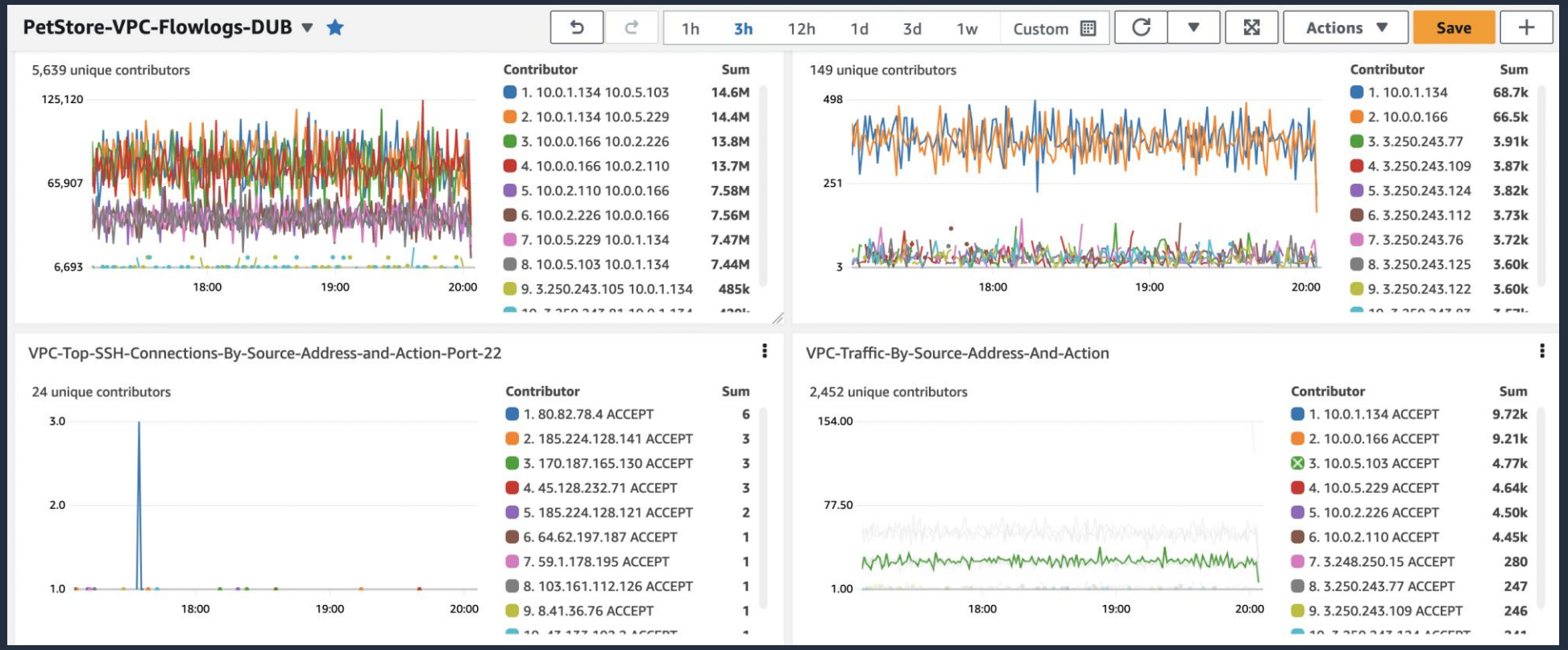
Understand network traffic, top API calls, or frequently queried domain names

## Integrations with DynamoDB & PrivateLink

Integration with DynamoDB identifies the most frequently accessed and throttled keys in your table or index at a glance. PrivateLink integration supports endpoint services analytics

# CloudWatch Contributor Insights

Real-time analysis of high cardinality time-series data to help you understand who or what is impacting system and application performance the most




Evaluate patterns in structured log events as they are streamed to CloudWatch Logs

Popular use cases include VPC Flow Log, CloudTrail, Route53 Resolver, and NGINX log analysis

Find top talkers and understand who or what is impacting system performance

Integrated with CloudWatch metrics to create alarms and anomaly detection

# Analyzing High Cardinality Data

**Embedded Metric Format**

- **Example**:
  - Analyze and troubleshoot types of issues customers have, by device type
    - Send metrics related to customer operations in logs – devices types, error codes along with customer name, IP address and other relevant information useful for troubleshooting

- **Embed metrics alongside log event data – using CloudWatch embedded metric format**

- **Ingest high-cardinality application data in the form of logs**
  - Generate actionable metrics from them

- **CloudWatch automatically extracts the metrics**
  - Visualize and alarm on them, for real-time incident detection
  - Correlate metrics with  logs
  - Query detailed log events associated with the extracted metrics using CloudWatch Logs Insights

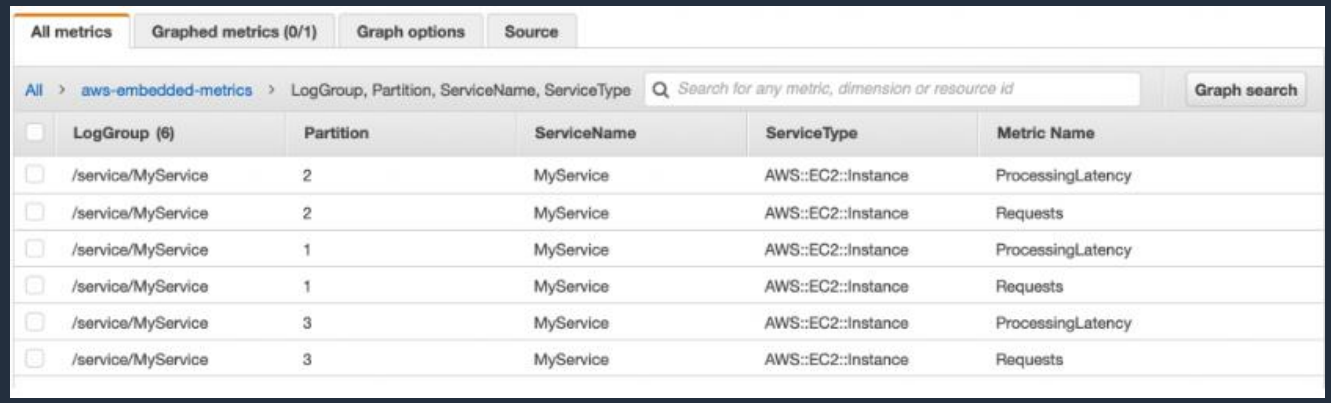
# Embedded Metric Format


```
{
  "_aws": {
    "Timestamp": 1565375354953123,
    "CloudWatchMetrics": [
      {
        "Namespace": "aws-embedded-metrics",
        "Dimensions": [
          [ "Operation" ],
          [ "Operation", "Partition" ]
        ],
        "Metrics": [
          { "Name": "Requests" },
          { "Name": "ProcessingLatency", "Unit": "Milliseconds" }
        ]
      }
    ]
  },
  "Message": "Completed processing",
  "CustomerName": "Globex Corp",
  "Requests": 1,
  "Operation": "Store",
  "Partition": "4",
  "ProcessingLatency": 137.52,
  "RequestId": "a4110ca8-4139-444d-ab95-ae8fe230aadc"
}
```


Embedded Metric Definition

Embedded Metrics + Additional Fields

## Metrics Generated




| LogGroup (6) | Partition | ServiceName | ServiceType | Metric Name |
|---|---|---|---|---|
| /service/MyService | 2 | MyService | AWS::EC2::Instance | ProcessingLatency |
| /service/MyService | 2 | MyService | AWS::EC2::Instance | Requests |
| /service/MyService | 1 | MyService | AWS::EC2::Instance | ProcessingLatency |
| /service/MyService | 1 | MyService | AWS::EC2::Instance | Requests |
| /service/MyService | 3 | MyService | AWS::EC2::Instance | ProcessingLatency |
| /service/MyService | 3 | MyService | AWS::EC2::Instance | Requests |

# Operationalizing Logs

## Analyze Logs During Troubleshooting

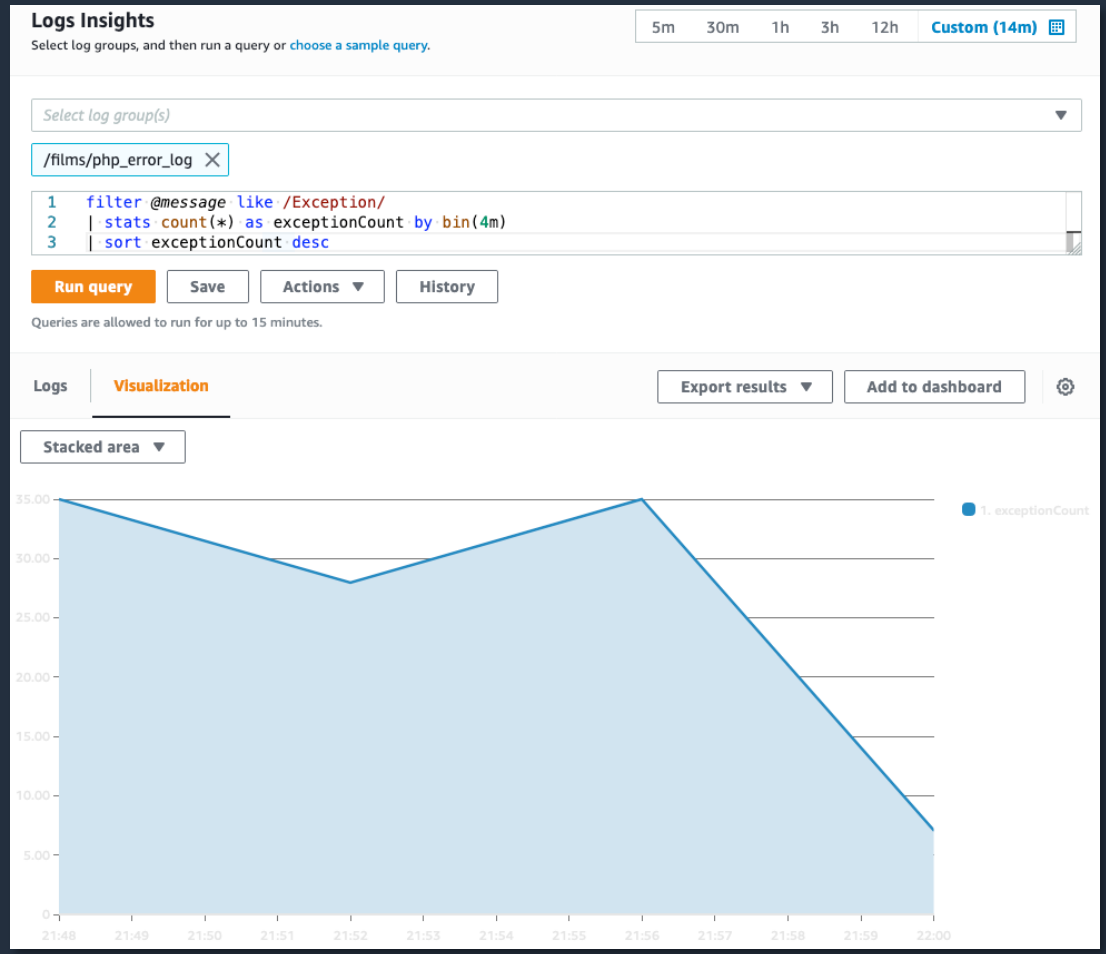
# Analyze Logs For Troubleshooting

1. Query Logs Using Logs Insights

2. Real Time Monitoring Of Logs – using Live Tail

# Query Logs Using CloudWatch Logs Insights

- Interactively query and analyze your log data
- Sample queries, command descriptions, query autocompletion, and log field discovery
- Automatically discovers fields in logs:
  - Amazon Route 53
  - AWS Lambda
  - AWS CloudTrail
  - Amazon VPC
  - Any application that emits log events as JSON



# Logs Insights – Capabilities

- **Pipelined query language, with support for filtering, computations, and group by operations**
- **Supporting structured and unstructured log analysis**
  - Parse, extract and analyze fields from unstructured logs
- **Support arithmetic, Boolean and comparison operators**
- **Functions:  Statistical, date/time (e.g. binning, date ceilings, etc.), IP address, strings**

# Logs Insights – Examples

**Filtering with calculated values**

```
filter Operation = "Insert"
| fields @timestamp, Operation, Bytes/1000 as @KBs
```

**Filtering, aggregate calculation by certain field, with sort**

```
filter Operation != "Search"
| stats percentile(Latency, 99.9) as @My3ninesLatency by Operation
| sort @My3ninesLatency desc
| limit 10
```

**Get a timeseries of some aggregates for log events that match a certain regex**

```
filter Operation like /Kinesis/
| stats max(Latency) by bin(5m)
```

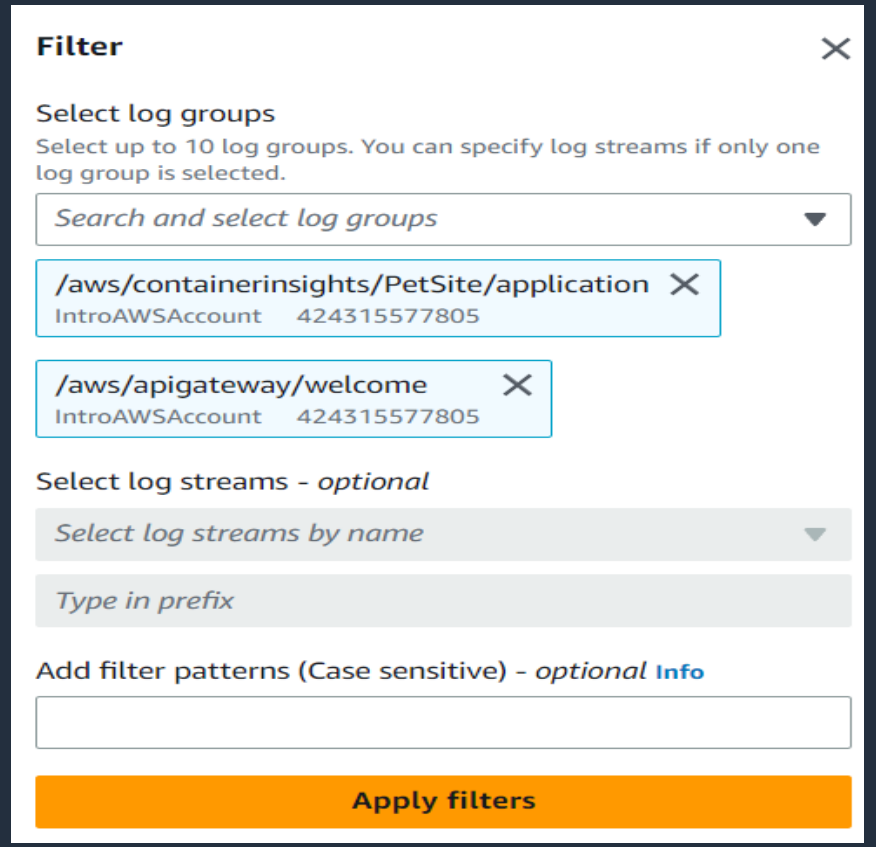
# CloudWatch Logs – Live Tail

View Logs in real time

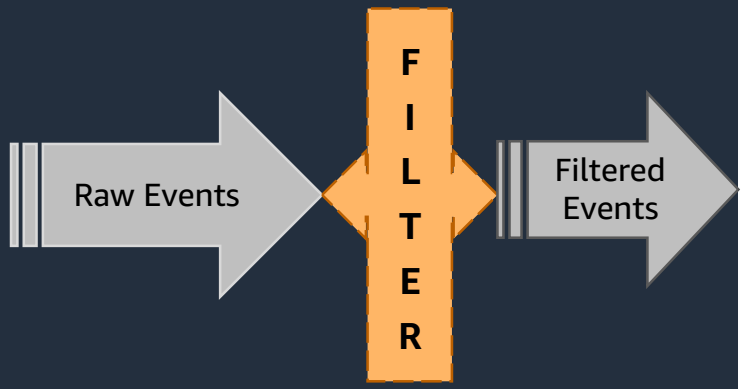
Use it for incident troubleshooting, monitor deployments, etc.

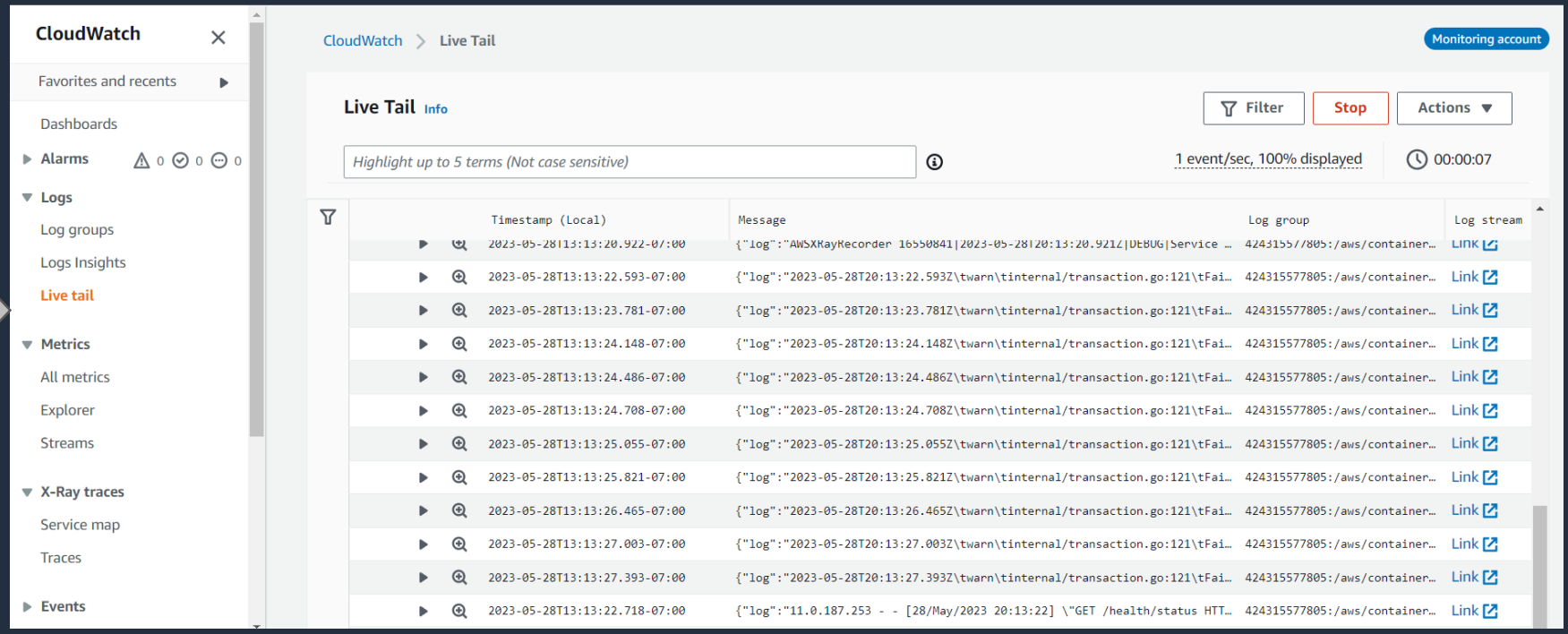
User Experience

1. Select a Log Group and optionally select Log Streams
2. Raw events can be streaming in at 1,000s of events/sec
3. Filters can be applied to narrow down events
4. Highlight terms



# CloudWatch Logs – Live Tail



# Operationalizing Logs

## Detect and Protect Sensitive Data

# Identify and prevent sensitive data leakage for log and message data in transit

Applications are producing, distributing, and exchanging growing volumes of data

Increasingly challenging to comply with data privacy regulations

Customers take on the expense to custom-build and manage their own data protection capabilities

# Anatomy of data protection policies

## Data Protection Policy

Policies are associated to log groups and topics

## 1 Policy Config

- Name
- Description
- Version
- Data Direction *(SNS only)*
- Principals *(SNS only)*

## 2 Data identifiers

*Leverages regular expressions & AI/ML*

- Personally identifiable information (PII)
- Protected health information (PHI)
- Financial
- Credentials & devices

## 3 Actions

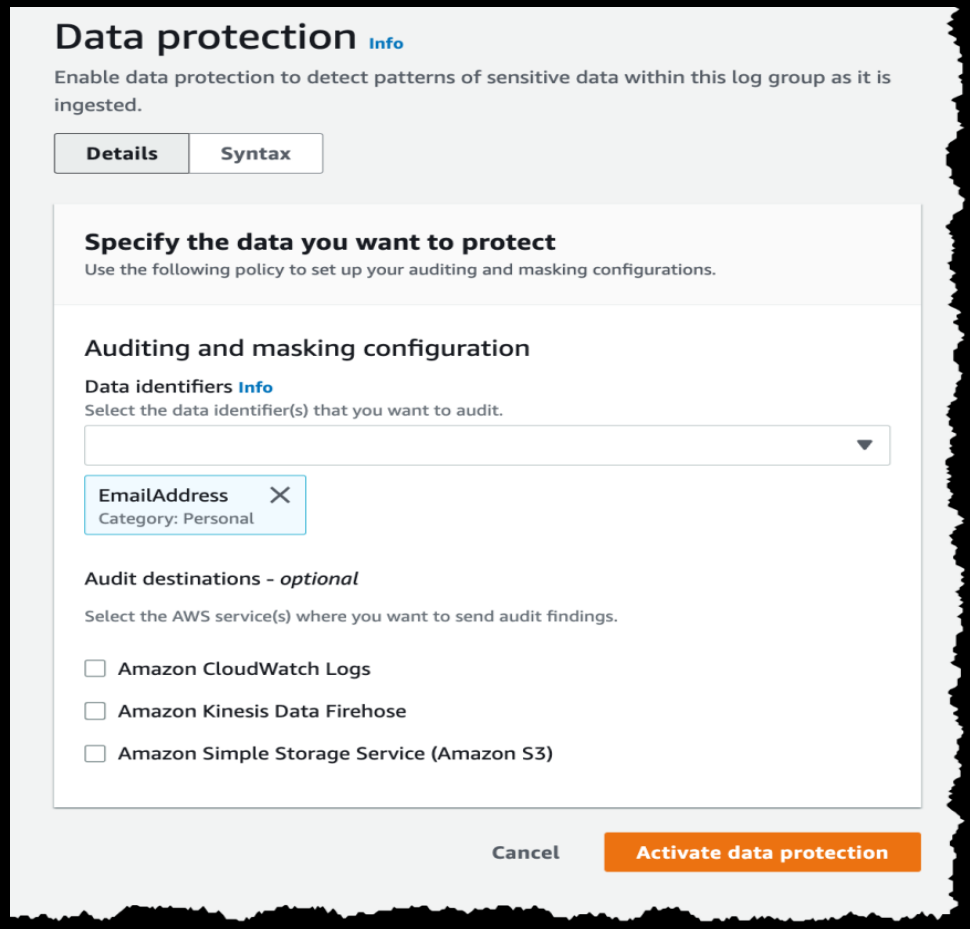
- Audit *(incl. sample rate SNS only)*
- De-identify
- Deny *(SNS only)*

## 4 Finding destinations

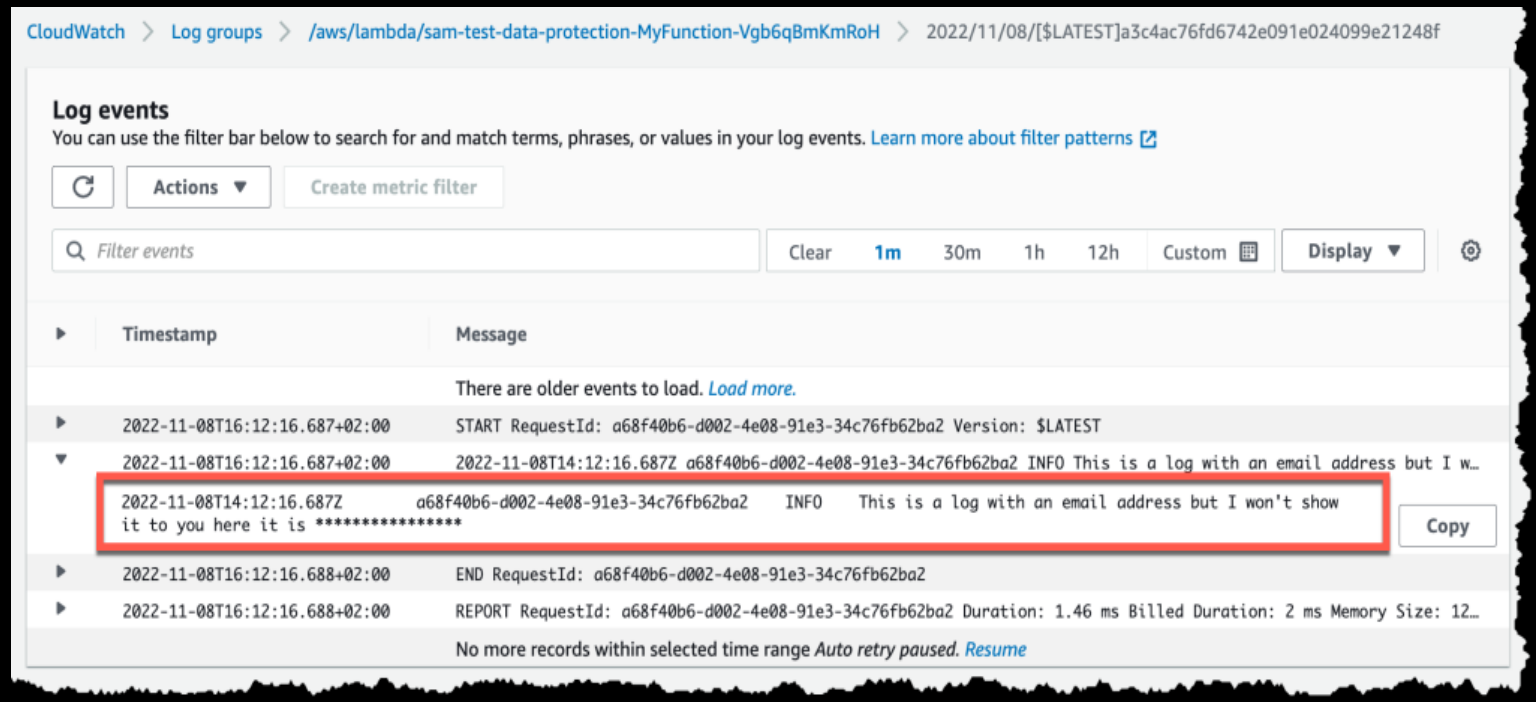
- S3
- Kinesis Firehose
- CloudWatch

# Protect Sensitive Data

Create polity to specify data to protect data




Sensitive Data Masked in Logs



# Operationalizing Logs

Build holistic observability view

# Data visualization with CloudWatch Dashboards

## Unified Data Visualization

CloudWatch Dashboards consolidates data from multiple sources, providing a comprehensive view of application and infrastructure performance.

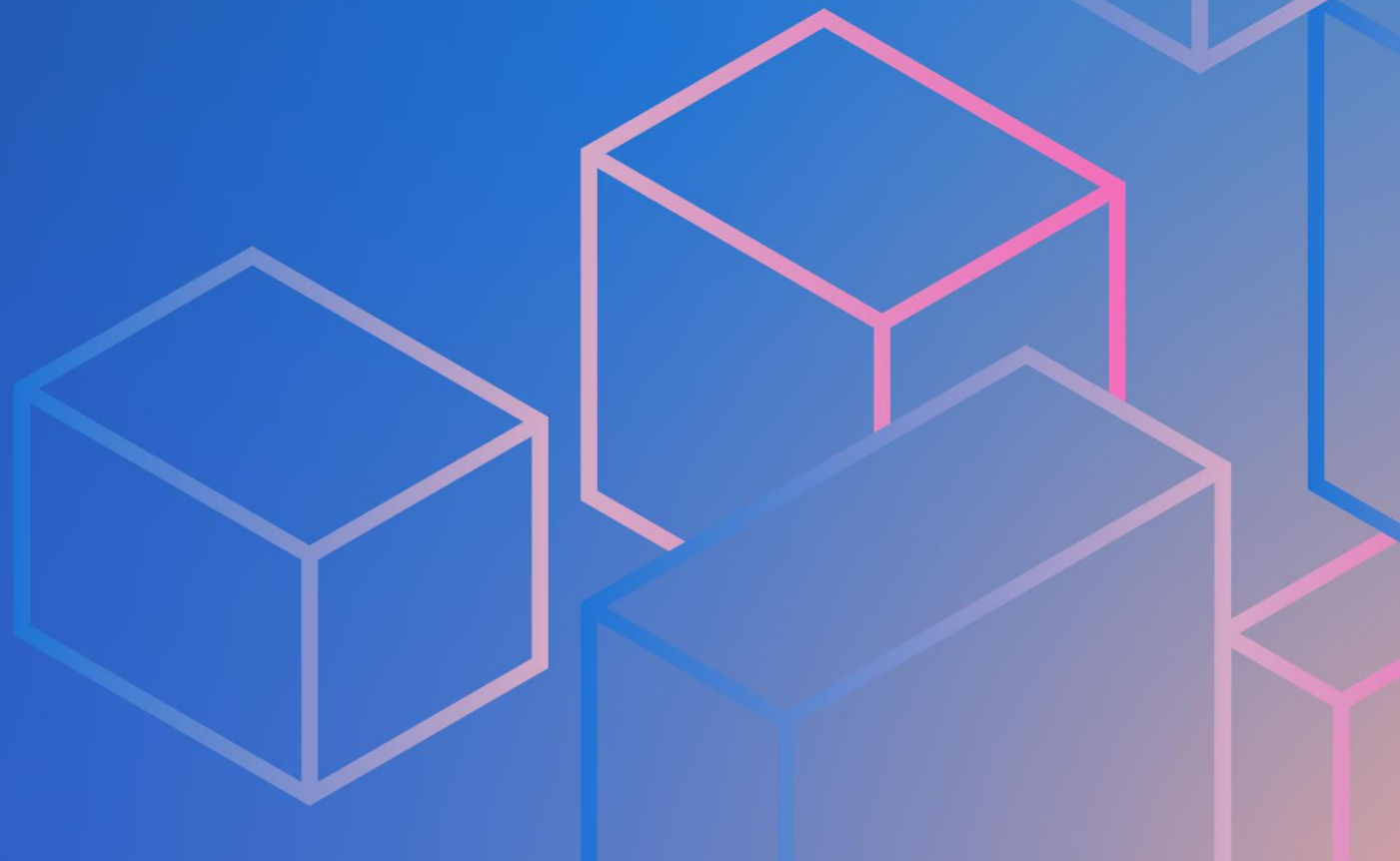
## Customization / Flexibility

Easily create and tailor dashboards to meet specific requirements, enabling efficient and data-driven decision-making.

## Scalability and Security

CloudWatch Dashboards scales with your data while maintaining security and privacy.

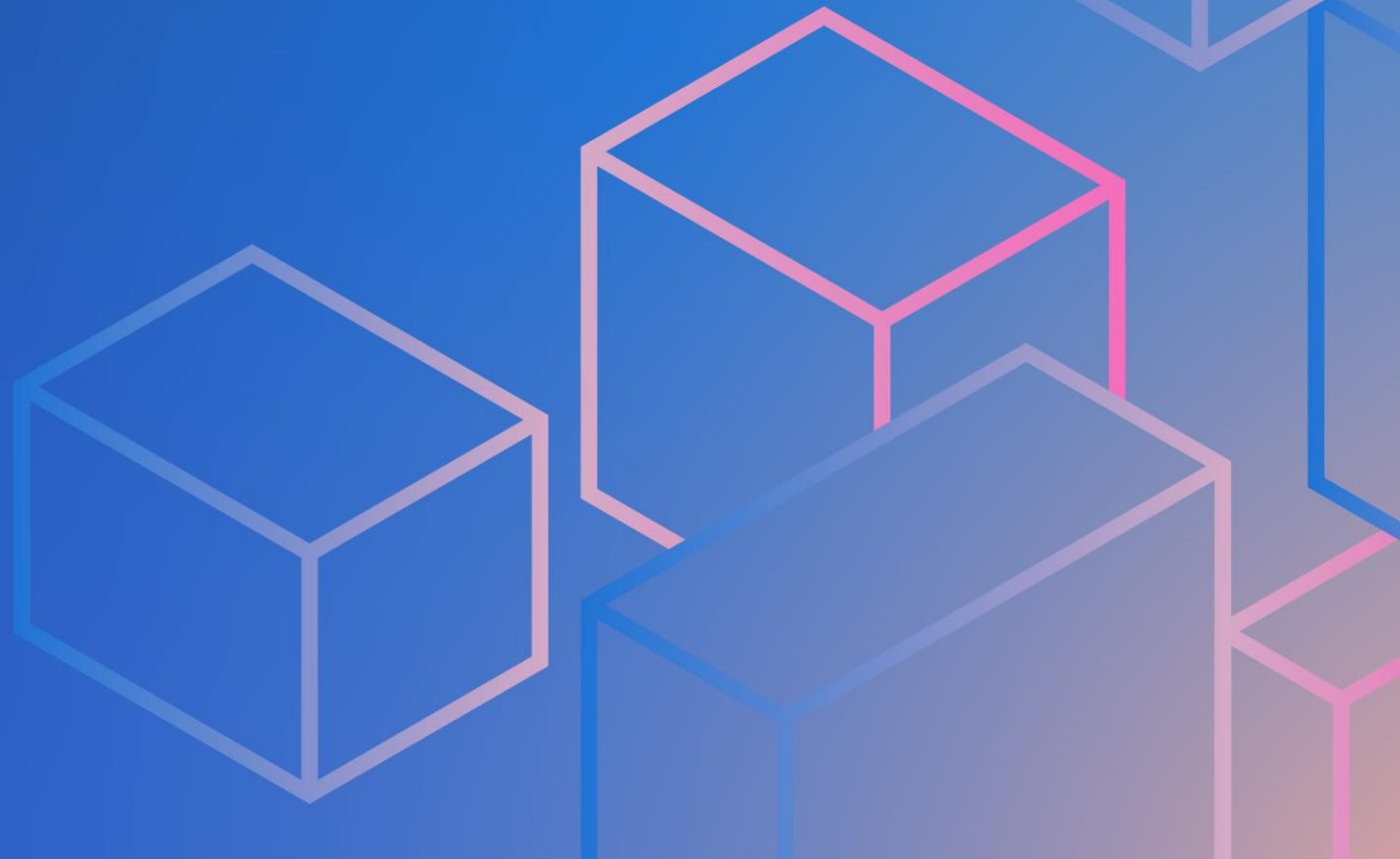
# Recent Launches



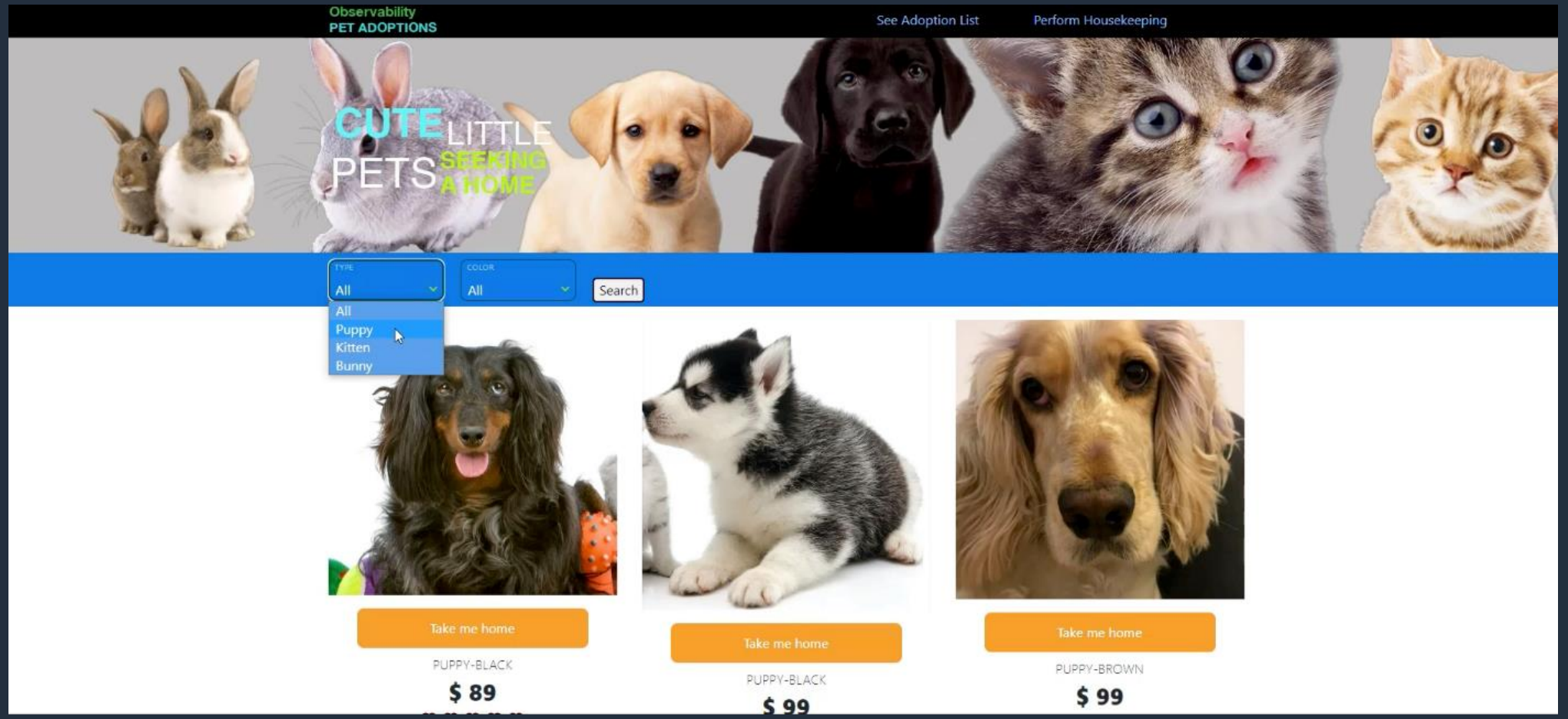
# Recently Launched

| | |
|---|---|
| **Cross Account Observability** | Search and Analyze metrics, logs and traces without account boundaries – and without data copy |
| **Live Tail** | Real time monitoring of logs |
| **Deeper insights with CloudWatch Logs** | • Increased quotas for Logs Insights<br>• Log Group – 50 , Concurrency – 30 , Timeout - 60 minutes |
| **Simplified metric extraction using Embedded Metric Format** | • Simpler format, without requiring headers<br>• High resolution metric extraction – 1s granularity supported<br>• Added error visibility – parsing and validation |
| **Contributor Insights Sample Rules** | Sample rules added for WAF and CloudTrail |

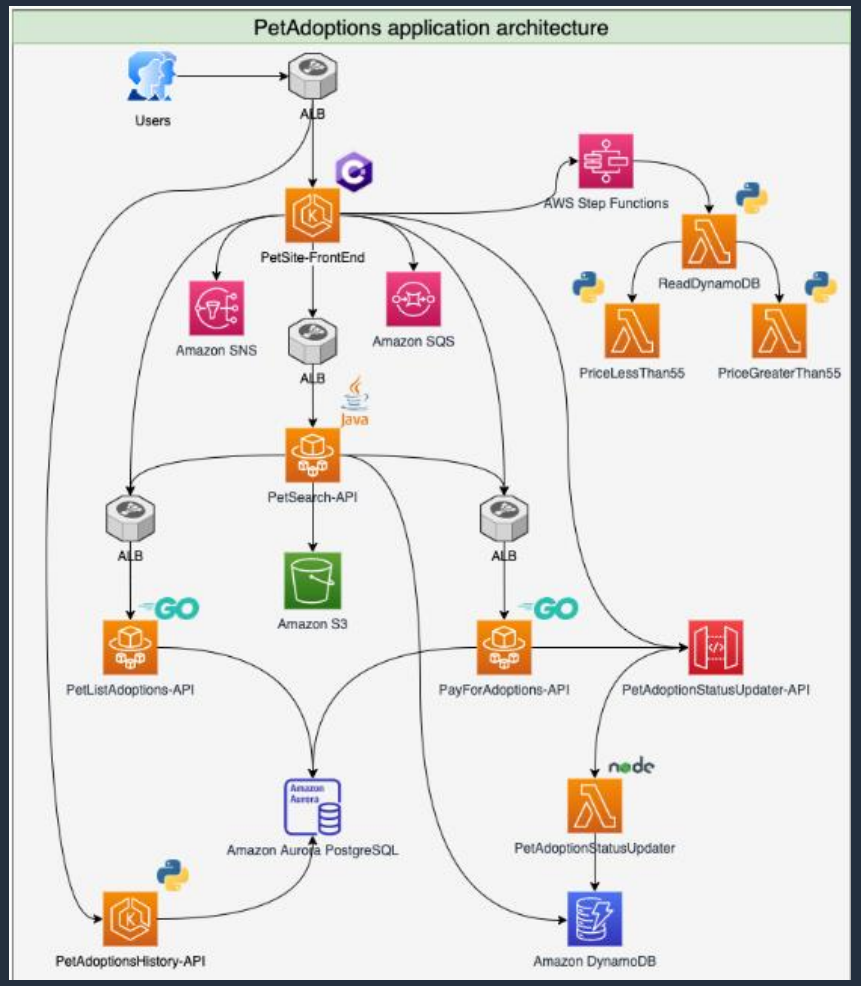
# Demo



# Pet adoption site!



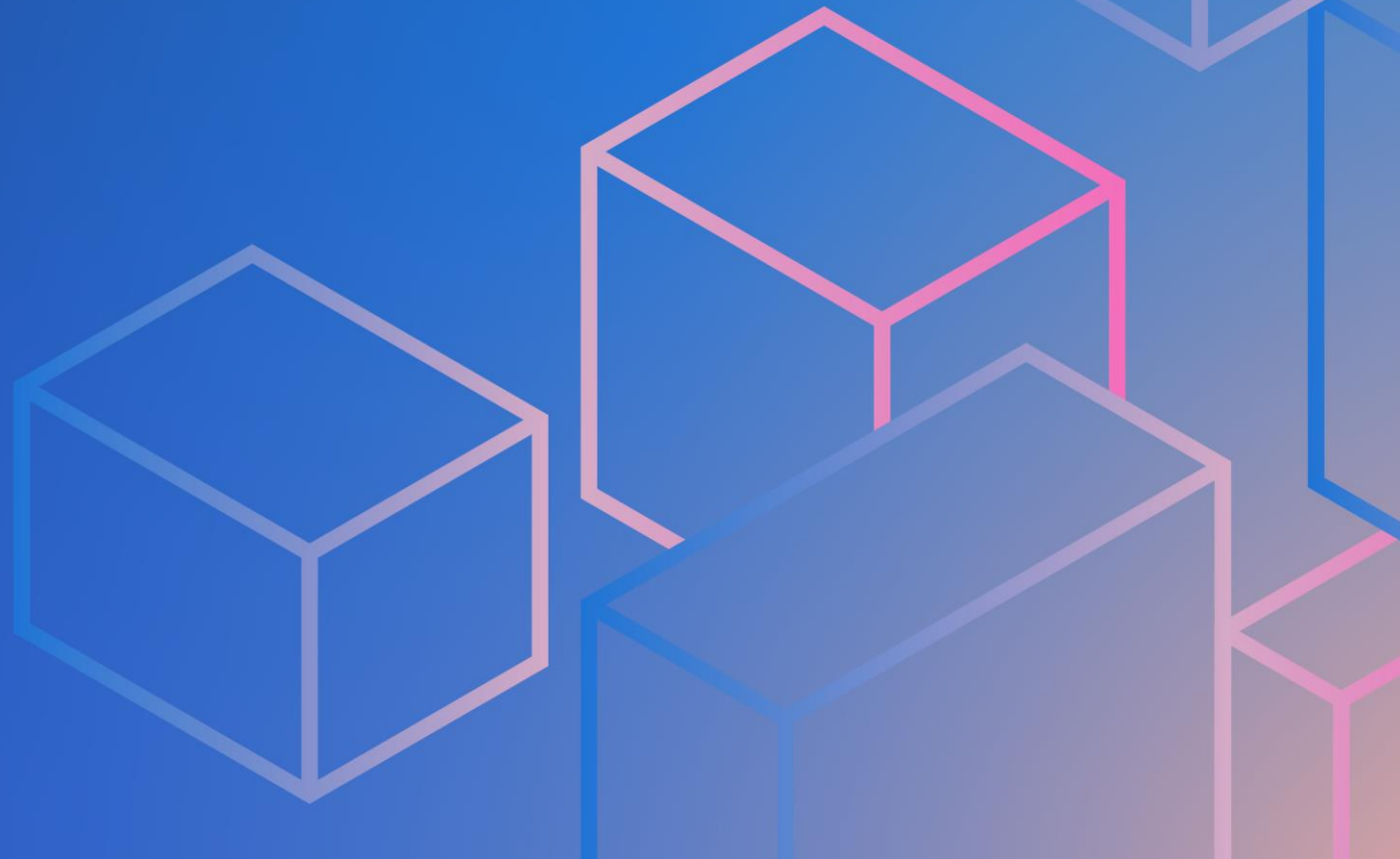
# Demo Overview




**Demo**

1. Query Logs Using CloudWatch Logs Insights
2. Real time analysis of Logs using Live Tail

# Summary



# CloudWatch Logs - Summary

**Fully managed service, for securely storing and analyzing logs at scale**

**Extensive support for analyzing and operationalizing logs**

- Extract metrics from logs – graph and alert on them
- Identify and analyze top contributors by various dimensions
- Query logs using powerful, pipelined language
- Analyze logs in real time to diagnose production issues, config changes
- Detect and protect sensitive data in logs
- Create dashboards to provide centralized view of key log queries, alarms, and metrics

# Resources

One Observability Workshop

Observability Best Practices

AWS Observability Accelerator

Skill Builder – AWS Observability

# Thank you!

Ashok Swaminathan
ashokswa@amazon.com