

The background features a dark navy blue field with abstract, overlapping shapes in vibrant magenta and deep red. Two thin, light blue lines intersect diagonally across the upper right portion of the image. The text is positioned on the left side.

AWS re:Invent

DECEMBER 2 – 6, 2024 | LAS VEGAS, NV

COP-406

Byte to insight: Maximize value from your logs with Amazon CloudWatch

Nikhil Kapoor

Principal Product Manager
Amazon Web Services

Andres Silva

Principal Specialist Solutions Architect
Amazon Web Services

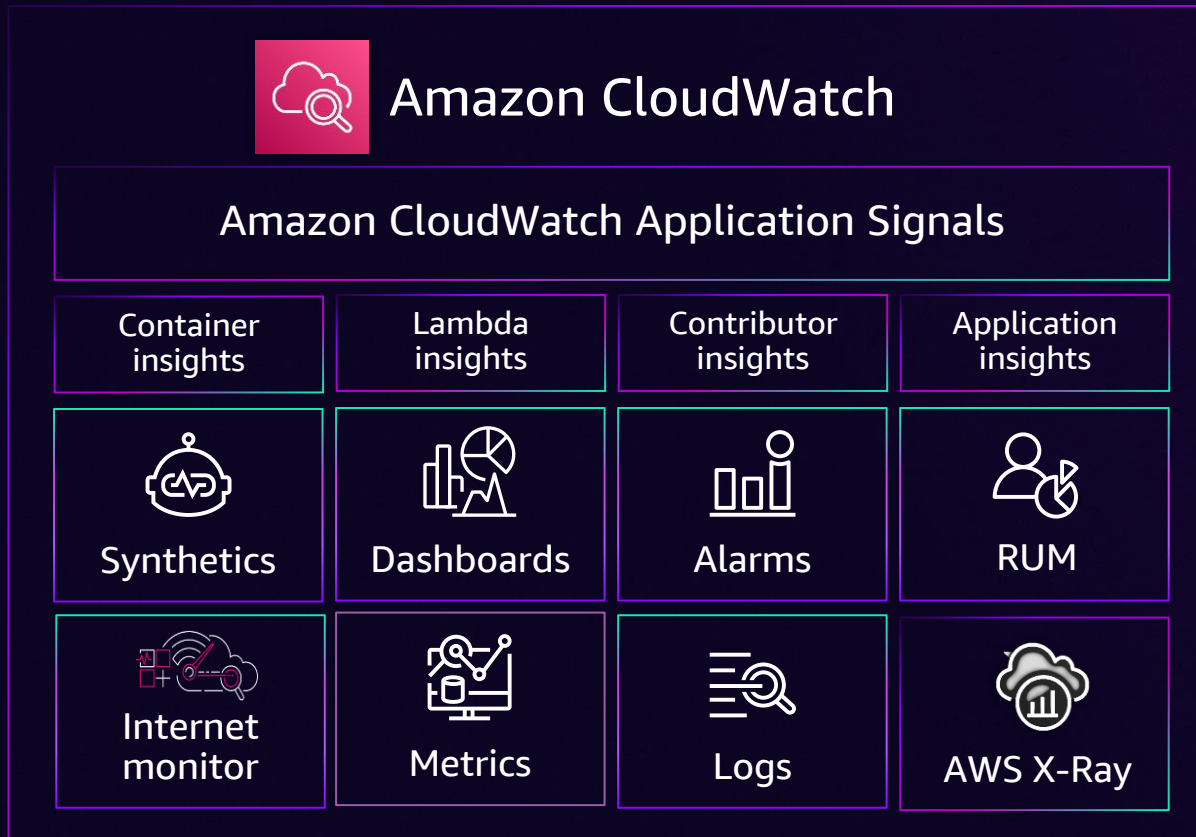


© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

- 01 CloudWatch overview
- 02 Types of insights
- 03 Ways to reduce cost
- 04 Gaining better insights
- 05 Key takeaways

CloudWatch – What is it?



AWS native

Full observability suite

Enormous scale

CloudWatch has evolved



2014

CloudWatch Logs launched



2015

Subscription Filters



2018

Logs Insights



2019

EMF & Contributor Insights



2022

Cross Account Log Metric and Trace Telemetry
Data protection
Logs Insights Query Concurrency
Log Filter Expressions for the CW Agent

CloudWatch has evolved

a lot!

2014
2015
2018
2019
2022



2023

Live Tail for Logs

Data protection: Custom identifiers + Account wide

Low-cost Log Ingest: Infrequent access log class

Log Pattern analysis and Anomaly Detection

Natural language query generation



2024

Live Tail: Streaming Cli + Lambda native

New log source: Bedrock, Cloudfront...

Enhanced log group selection

NEW

Field indexes

NEW

Log transformations

NEW

OpenSearch analytics on CloudWatch Logs

NEW

Telemetry correlation with resource context

NEW

Database Insights

NEW

Transaction search & analytics

NEW

Amazon Q Developer operational investigations (*preview*)



Goals of the session



Maximize value



Improve visibility
(**Insights**)



Reduce costs
(**Bytes** ingested, stored)

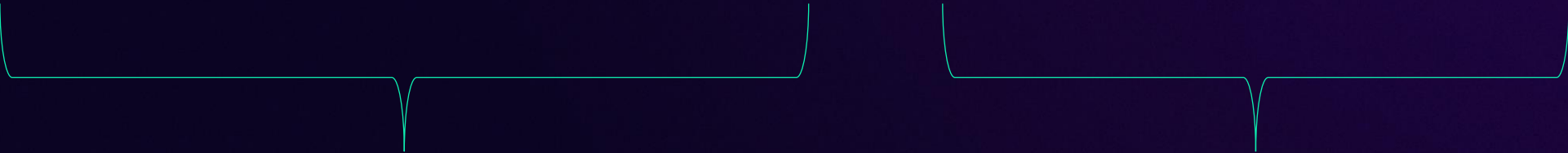
What is an Insight?

“the capacity to gain an accurate and deep intuitive understanding of a person or thing.”

— Oxford Languages

What is an Insight?

“the capacity to gain an accurate and deep intuitive understanding of a person or thing.”



The diagram consists of two horizontal curly braces positioned below the quote. The left brace is under the words 'accurate and deep intuitive' and points down to the text 'The "What" ?'. The right brace is under the words 'understanding of a person or thing' and points down to the text '"Context"'.

The "What" ?

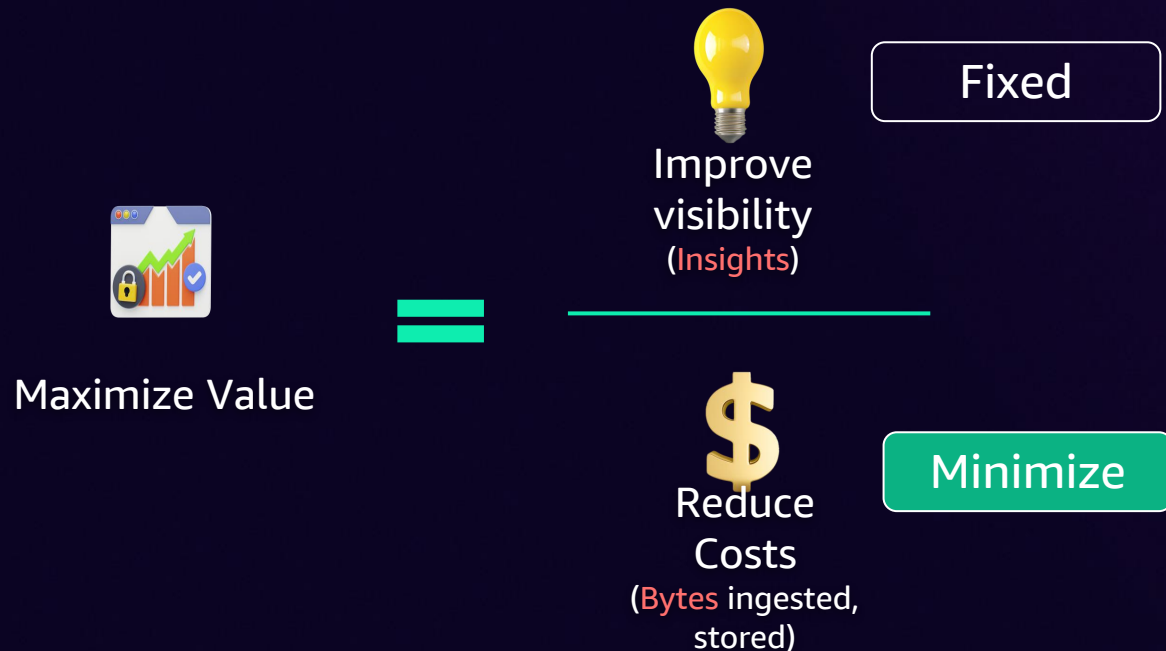
"Context"

Example questions

Question	Context	"What"	
What's the rate of "Blocked" transactions for App A ?	App A	"Blocked"	Known: Known
What are top 10 customers whose transactions taking longer than 100 msec ?	Latency > 100 msec	Top 10 Customers	
What happened to this requestId ?	requestId	-	
I made a change in Lambda-A few minutes ago , is there something new/different in the logs?	Recent change in Lambda-A	-	Known: Unknown
Looks like someone terminated this instance , when and who did that?	-	Terminate instance	

Types of Insights

Known: Known



Known: Unknown



Known: Known



© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Known: Known

I wonder which are the
Top 10 customers with
latency > 100 msec?

I wonder what is the
number of requests
with "Action = Block"
in 5 minute intervals
for my app?



Known: Known

*Reducing cost at
ingestion is a lot
simpler than you think*



Known: Known: Metric filters

I wonder: No. of requests with "Action = Block" in 5-minute intervals?



Known: Known: Metric filters

- Q: No. of requests with "Action = Block" in 5-minute intervals?

Metric filters: Convert log data to CloudWatch metrics by specifying patterns to match during ingestion

Define pattern

Create filter pattern

You can use metric filters to monitor events in a log group as they are sent to CloudWatch Logs. You can monitor and count specific terms or extract values from log events and associate the results with a metric. [Learn more about pattern syntax](#)

Filter pattern

Specify the terms or pattern to match in your log events to create metrics.

Test pattern

Select log data to test

Custom log data

Log event messages

Type log data to test with your Filter Pattern. Please use line breaks to separate log events.

```
[83078518-fcc1-4d30-9573-8b9737671438] BENCHMARK : Running Start Crawl for Crawler TestCrawler2
[83078518-fcc1-4d30-9573-8b9737671438] BENCHMARK : Classification complete, writing results to database mygluedatabase
[83078518-fcc1-4d30-9573-8b9737671438] INFO : Crawler configured with SchemaChangePolicy
("UpdateBehavior":"UPDATE_IN_DATABASE","DeleteBehavior":"DEPRECATE_IN_DATABASE").
[83078518-fcc1-4d30-9573-8b9737671438] INFO : Created table gluetest in database mygluedatabase
[83078518-fcc1-4d30-9573-8b9737671438] BENCHMARK : Finished writing to Catalog
```

Test pattern

Results

Please select log event messages above and click "Test pattern" to see results.

Cancel

Next



Known: Known: Embedded Metric Format



This filtering stuff is great. Can I do it even more **efficiently**?

Known: Known: Embedded Metric Format

- Q: No. of requests with "Action = Block" in 5 minute intervals?

CloudWatch embedded
metric format: Generate
custom metrics
asynchronously via logs
in CloudWatch Logs

```
{
  "_aws": {
    "Timestamp": 1574109732004,
    "CloudWatchMetrics": [
      {
        "Namespace": "lambda-function-metrics",
        "Dimensions": [ ["functionVersion"] ],
        "Metrics": [
          {
            "Name": "time",
            "Unit": "Milliseconds",
            "StorageResolution": 60
          }
        ]
      }
    ]
  },
  "functionVersion": "$LATEST",
  "time": 100,
  "requestId": "989ffbf8-9ace-4817-a57c-e4dd734019ee"
}
```



Known: Known

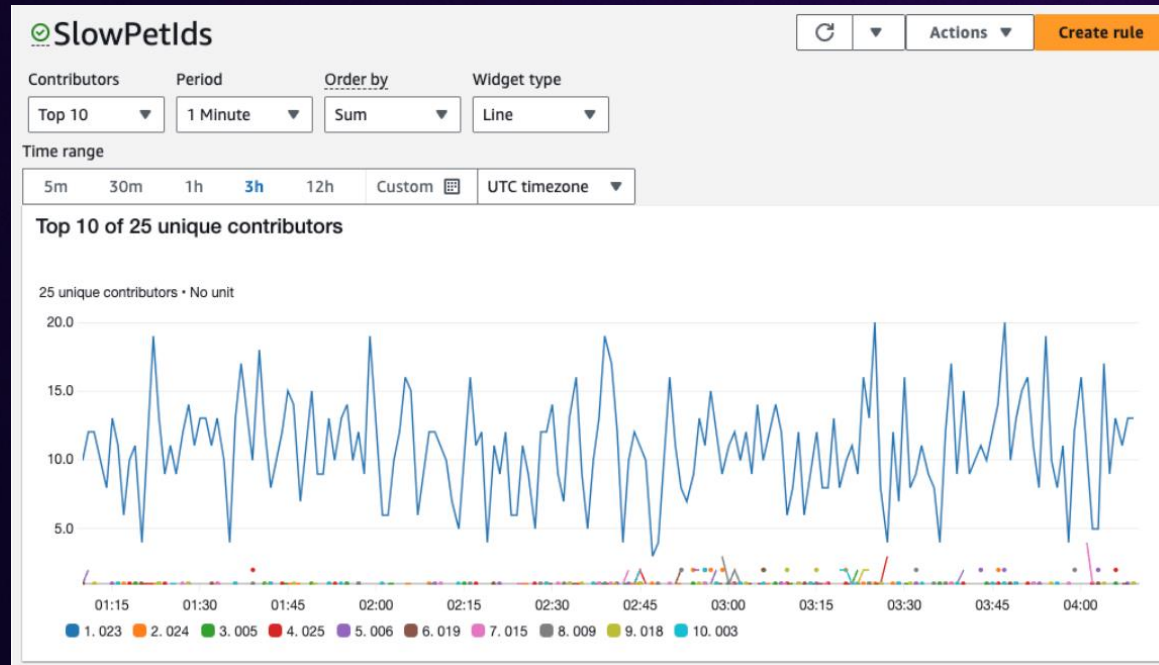
Q: Top 5 customers
with latency > 100
msec?



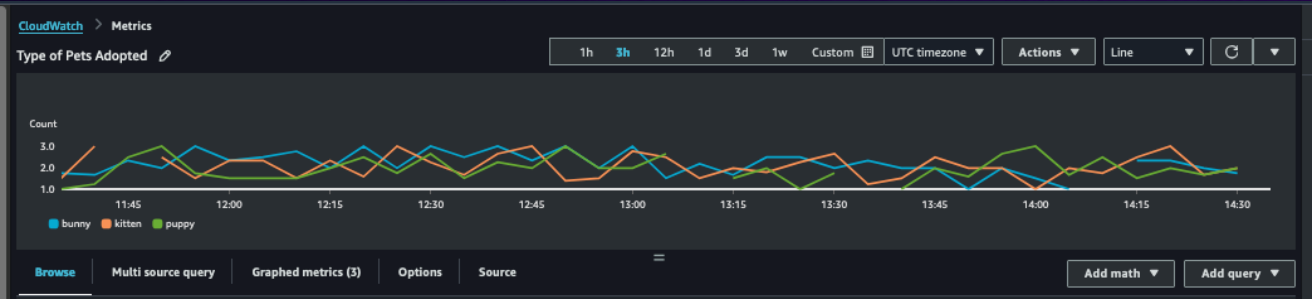
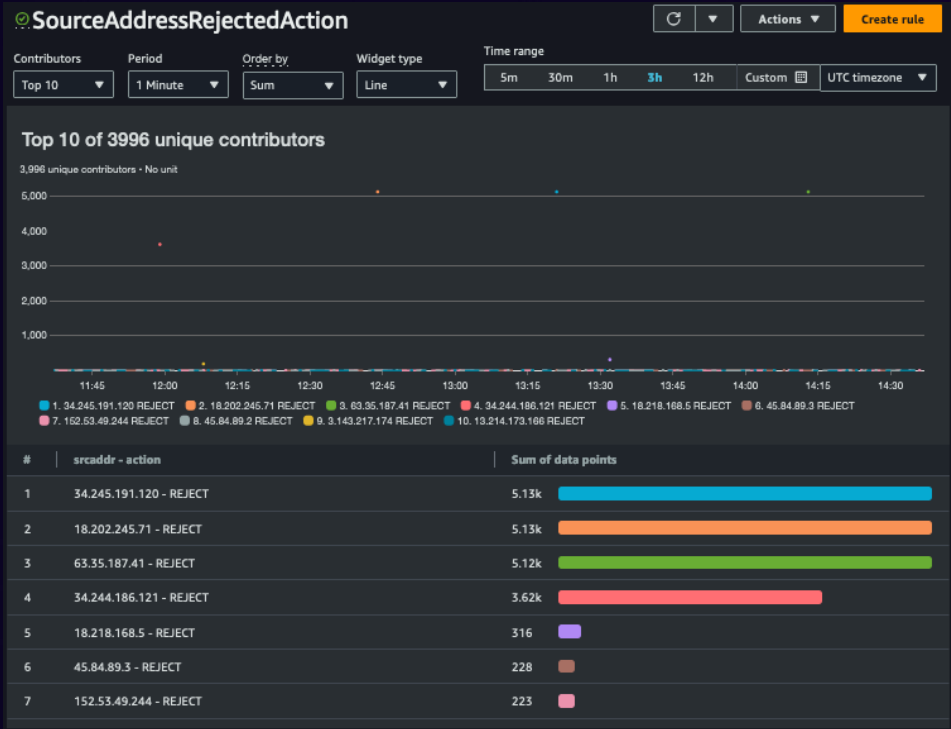
Known: Known: Contributor Insights

- Q: Top 5 customers with latency > 100 msec?

Contributor Insights analyzes logs to identify top contributors impacting customer experience



Known: Known: Dashboards, Alarms



Blog on how to?



NEW

Zero-ETL with CloudWatch Logs

Integration between CloudWatch Logs and OpenSearch Service analytics, offering advanced querying and auto-generating dashboards



Out-of-the-box curated dashboards in CloudWatch for popular vended logs



Zero ETL to access CloudWatch data from OpenSearch



2 additional query languages in CloudWatch that increase ease of use (i.e., OpenSearch Piped Processing Language, OpenSearch SQL)

AVAILABLE IN GENERAL AVAILABILITY ON 12/1/2024



NEW

Enhanced log analytics

Simpler and faster insights from your logs, at scale



Query across broader sets of logs with enhanced log group selection



Faster queries at lower costs with field indexes



Transform your logs into standardized, structured log format for consistent analytics

AVAILABLE IN GENERAL AVAILABILITY ON 11/18/2024



© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Logs transformation and enrichment

Transform

- **Consistent structure** (JSON) & schema
- **Pre-built templates** (WAF, VPC, Apache, NGINX)
- **Custom transformations** (Grok, Split, trim, TypeConvert)

Enrich

- **Add context**
 - Account info
 - Loggroup/logstream
 - region

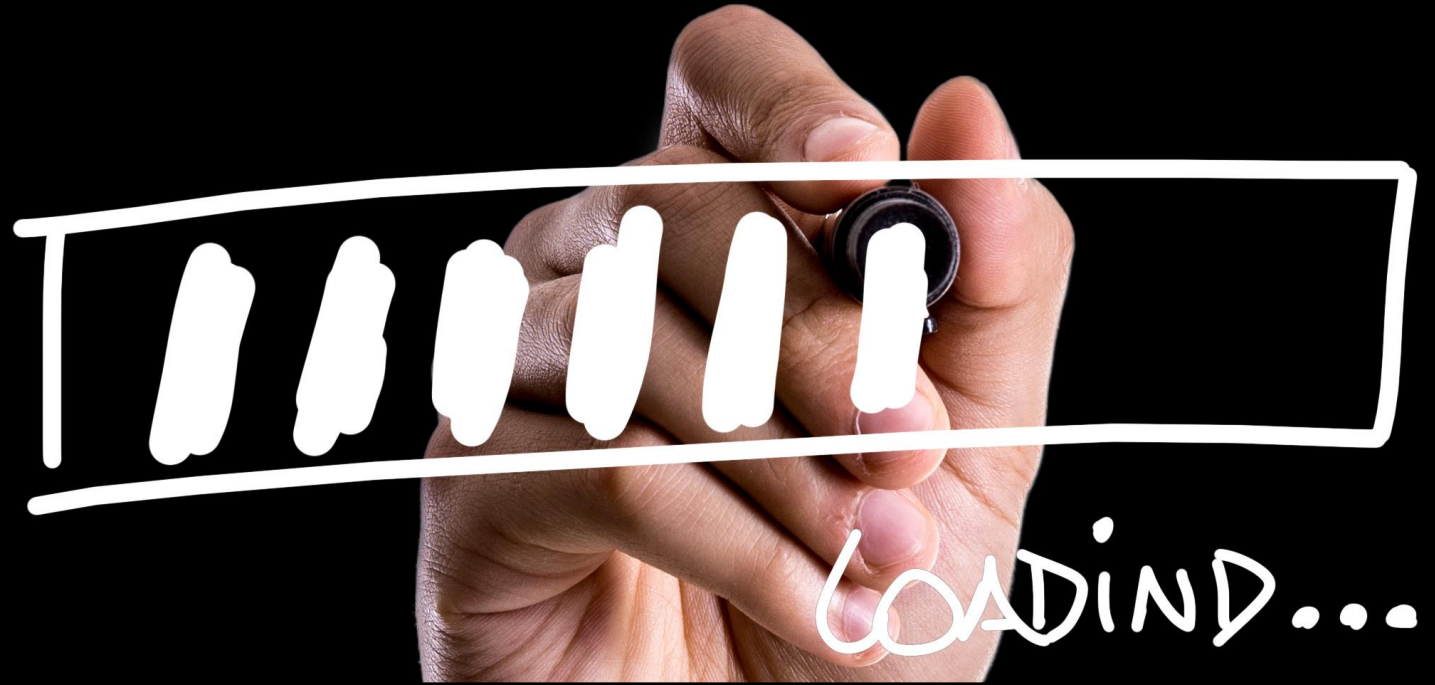
Analyze

- **Better queries**
 - Discovered fields
 - Field indexes
- **Flexible metric extraction**
 - Alarming
 - Dashboarding
- **Context rich forwarding**
 - Subscription filters

Demo: Dashboard comparison

- Difference in output/experience
- Delta in costs

DEMO



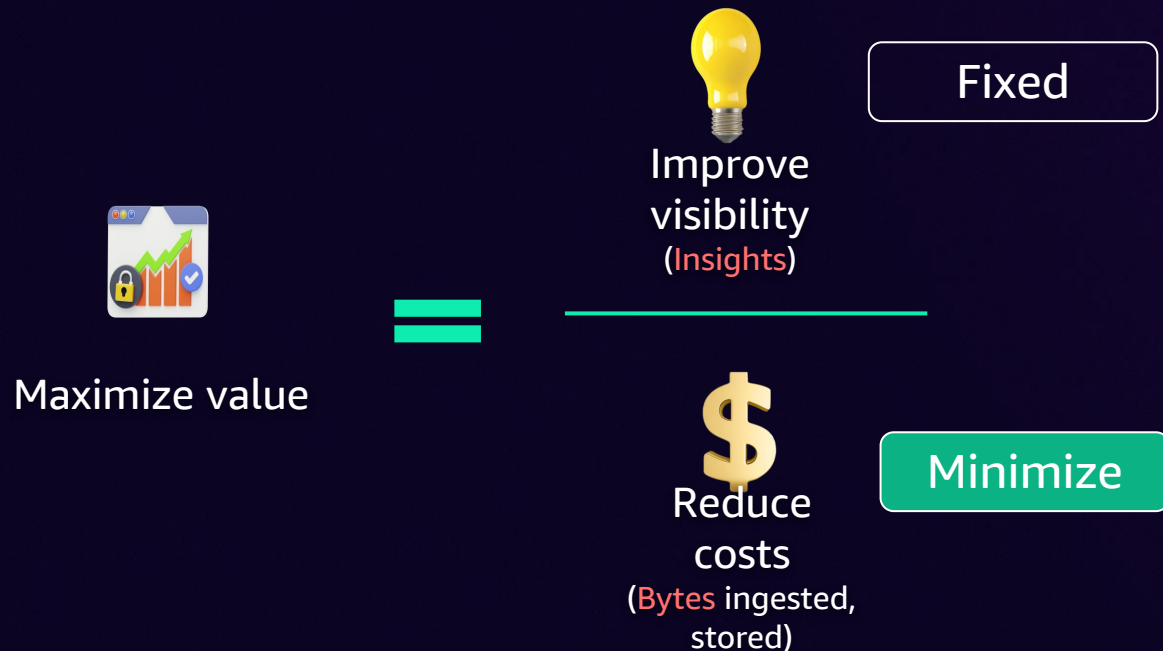
Known: Unknown



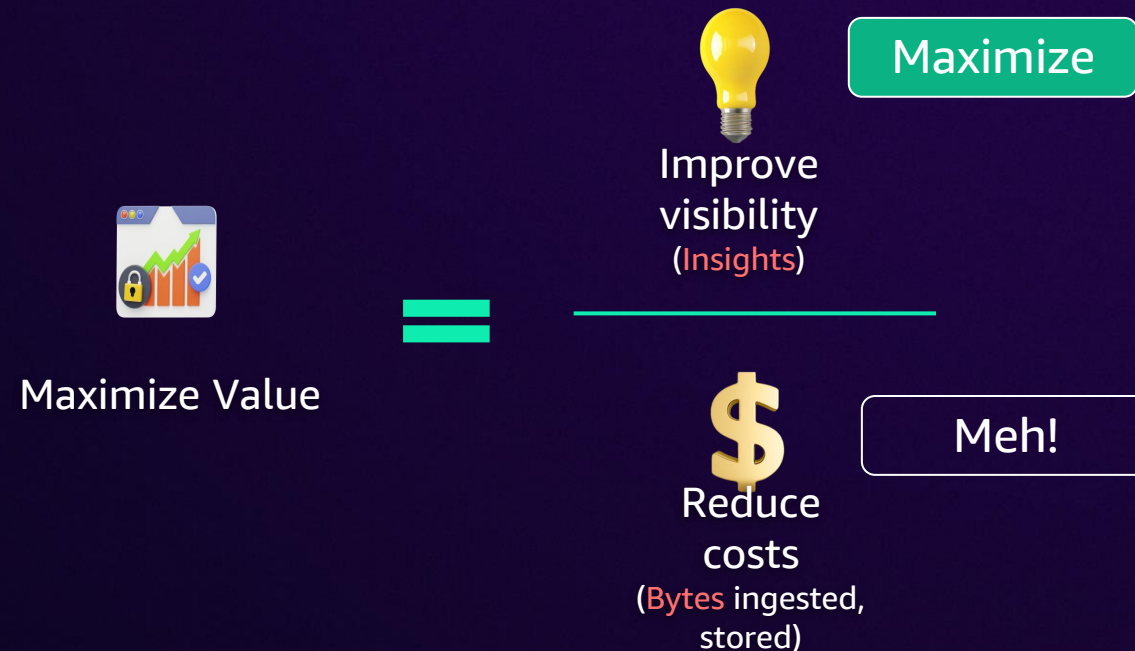
© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Types of Insights

Known: Known



Known: Unknown



Known: Unknown

Q: I made a change
here, is there
something new in the
logs?

Q: What happened
to this requestId?



Known: Unknown

- Log group separation
- Consistent, meaningful naming convention
- Appropriate retention settings

- Structured log format (JSON)
- Breadcrumbs: requestId, customerId
- Standardize schema

Known: Unknown

Q: I made a
change here, is
there something
new in the logs?

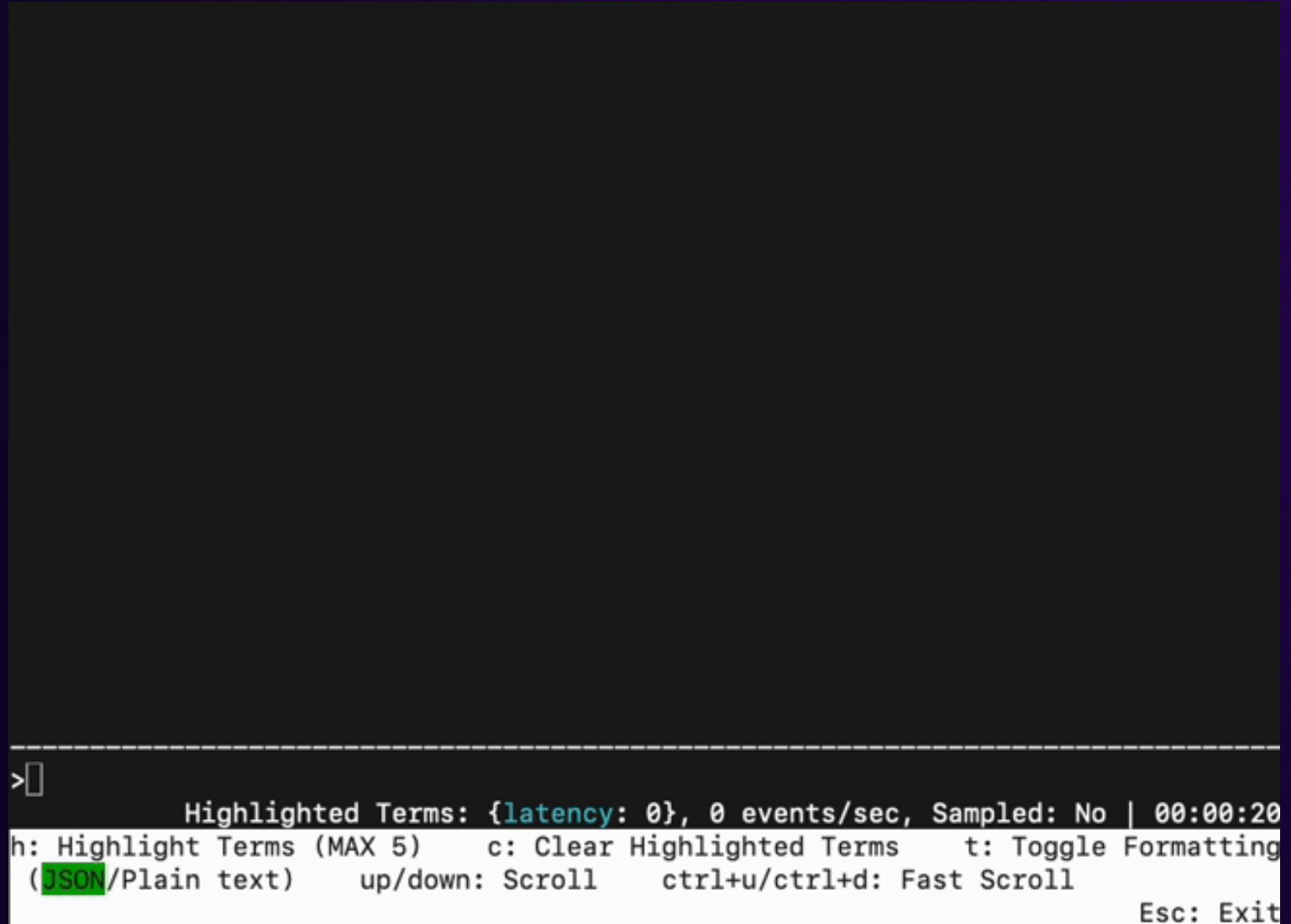


Compare

Live Tail

Live-Tail: See What's Happening Now

- Real-time log monitoring and investigation
- Quickly identify and troubleshoot issues



The screenshot displays the AWS LiveTail interface. The main area is a dark terminal window. At the bottom, a white command prompt shows a cursor. Below the terminal, a white status bar contains the following text: "Highlighted Terms: {latency: 0}, 0 events/sec, Sampled: No | 00:00:20". Below this, a white bar lists keyboard shortcuts: "h: Highlight Terms (MAX 5) c: Clear Highlighted Terms t: Toggle Formatting (JSON/Plain text) up/down: Scroll ctrl+u/ctrl+d: Fast Scroll". At the bottom right of this bar, it says "Esc: Exit".

Patterns and compare



1000's of log
lines to handful
of patterns

Logs (10k)Patterns (66)Visualization

Patterns (66) based on 10k of 11.28k records [Analyze all records](#) [Info](#)

Add to query

Export results ▾

Add to dashboard

Filter patterns by pattern string, event count, severity, event ratio or keywords

< 1 2 3 > ⚙

<input type="checkbox"/>	Inspect	Pattern	Event count ▾	Event ratio (%) ▾	Severity type ▾
<input type="checkbox"/>		{ <code>"timestamp": "timestamp"-1, "level": "DEBUG", "message": "message"-2 Token-3 Token-4 Token-5, "logger": "logger"-6, "requestid": "requestid"-7}</code> }	1,315	13%	DEBUG
<input type="checkbox"/>		{ <code>"timestamp": "timestamp"-1, "level": "DEBUG", "message": "Looking for endpoint for dynamodb via: via-2, "logger": "botocore.configprovider", "requestid": "requestid"-3}</code> }	828	8%	DEBUG
<input type="checkbox"/>		{ <code>"timestamp": "timestamp"-1, "level": "DEBUG", "message": "message"-2:Token-3:Number-4 \ "POST Token-5 Token-6 Number-7 Token-8, "logger": "logger"-9, "requestid": "requestid"-10}</code> }	414	4%	DEBUG
<input type="checkbox"/>		{ <code>"timestamp": "timestamp"-1, "level": "DEBUG", "message": "Event before-call.dynamodb.Putitem: calling handler <function Token-2 at Token-3>, "logger": "botocore.hooks", "requestid": "requestid"-4}</code> }	414	4%	DEBUG
<input type="checkbox"/>		{ <code>"timestamp": "timestamp"-1, "level": "DEBUG", "message": "Event before-parameter-build.dynamodb.Putitem: calling handler <function Token-2 at Token-3>, "logger": "botocore.hooks", "requestid": "requestid"-4}</code> }	414	4%	DEBUG
<input type="checkbox"/>		{ <code>"timestamp": "timestamp"-1, "level": "ERROR", "message": "Database transaction processing failure! Exception: ModifyingSqlDataNotPermitted", "logger": "root", "requestid": "requestid"-2}</code> }	298	3%	ERROR

What changed?

Patterns (71) [Info](#) [Compare mode](#)

Add to query

Export results ▾

Add to dashboard

Filter patterns by pattern string, event count difference, difference description or keywords

< 1 2 3 > ⚙

<input type="checkbox"/>	Inspect	Pattern	Difference event count ▾	Difference description ▾	Severity type ▾	Main time range event count ▾	Compare time range event count ▾
<input type="checkbox"/>		{ <code>"timestamp": "timestamp"-1, "level": "ERROR", "message": "Database transaction processing failure! Exception: ModifyingSqlDataNotPermitted", "logger": "root", "requestid": "requestid"-2}</code> }	+347	New pattern	ERROR	347	0
<input type="checkbox"/>		{ <code>"timestamp": "timestamp"-1, "level": "INFO", "message": "Attempt to modify data in postgresql denied due to lack of permissions.", "logger": "root", "requestid": "requestid"-2}</code> }	+347	New pattern	INFO	347	0
<input type="checkbox"/>		{ <code>"level": "Info", "ts": "ts"-1, "caller": "caller"-2:Token-3, "msg": "Starting Token-4 server", "kind": "receiver", "name": "otlp", "data_type": "data_type"-5, "endpoint": "localhost": "localhost"-6}</code> }	+4	New pattern	INFO	4	0



Anomaly detection



- Proactively identify potential issues in your logs
- Use it as a starting point OR way to rule things out
- Create alarms from Anomaly detection for faster detection

Log anomalies (15) Info					Create alarm ↗	Actions ▼	View
The latest 50 anomalies are automatically updated every 1 minute							
<input type="text" value="Filter anomalies by priority level, patterns or keywords"/>							
<input type="checkbox"/>	Inspect	Anomaly ▼	Priority ▼	Log pattern ▼	Anomaly log trend		
<input type="checkbox"/>		Unexpected pattern detected with severity ERROR	Medium	{"level":"Info","ts":" ts -1","logger":"telemetryAPI.Listener","msg":"HTTP Server closed:","error":"http: Server closed"}			
<input type="checkbox"/>		Unexpected pattern detected with severity WARN	Low	{"level":"warn","ts":" ts -1","caller":"localhostgate/featuregate.go:" localhostgate/featuregate.go-2 ","msg":"The default endpoints for all servers in components will change to use localhost instead of IPv4-3 in a future version. Use the feature gate to preview the new default.","feature gate ID":"component.UseLocalHostAsDefaultHost"}			

Known: Unknown

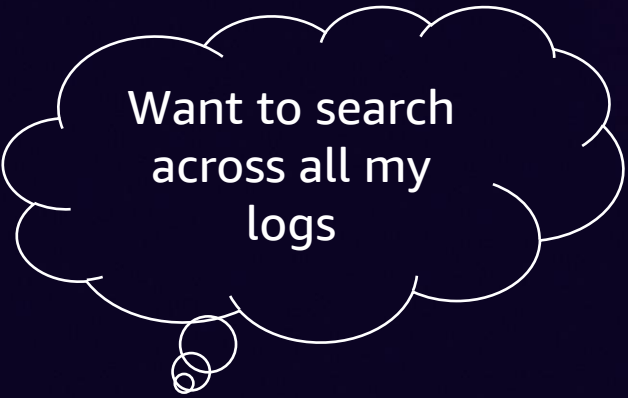
Q: What happened to this request Id?



Logs Insights – Queries

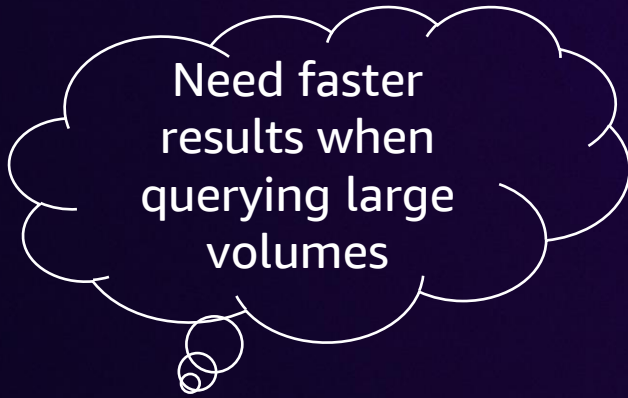
Field Indexes

Common challenges with Log Queries




Want to search
across all my
logs

- 50 log group limit
- Individual selection
- Cross-account



Need faster
results when
querying large
volumes

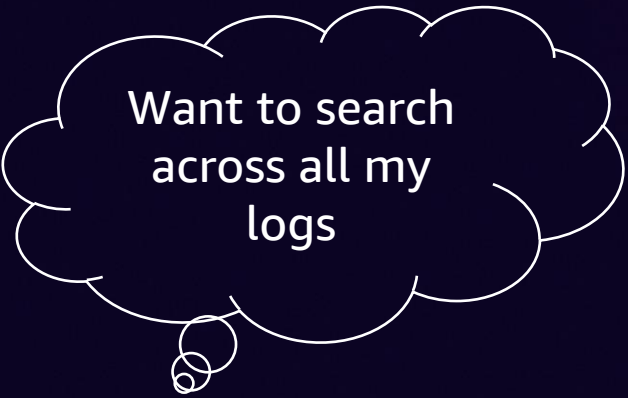
- 60-minute timeout
- Dashboarding use cases
- Faster iteration



How can I
limit/mitigate
expensive
queries

- Inadvertent large scans
- Needle in the haystack
- Frequent, repetitive queries

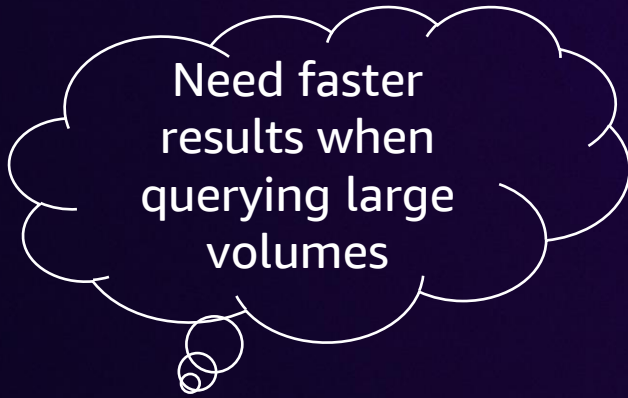
Field indexes and enhanced log group selection



Want to search
across all my
logs

Enhanced Log group selection


- 10k log groups
- Prefix or ALL
- Cross-account



Need faster
results when
querying large
volumes

Field indexes

- 20 fields per policy
- Indexed for 30 days
- *"key = value" or "Key IN [value, value]"*



How can I
limit/mitigate
expensive
queries

filterIndex

- Indexed data only
- Auto-select indexed log groups

Field indexes and enhanced log group selection



Simpler



Faster



Cost-effective

No additional costs
Included within Standard Log class ingestion



Demo – Greengrocer



Monitoring Account

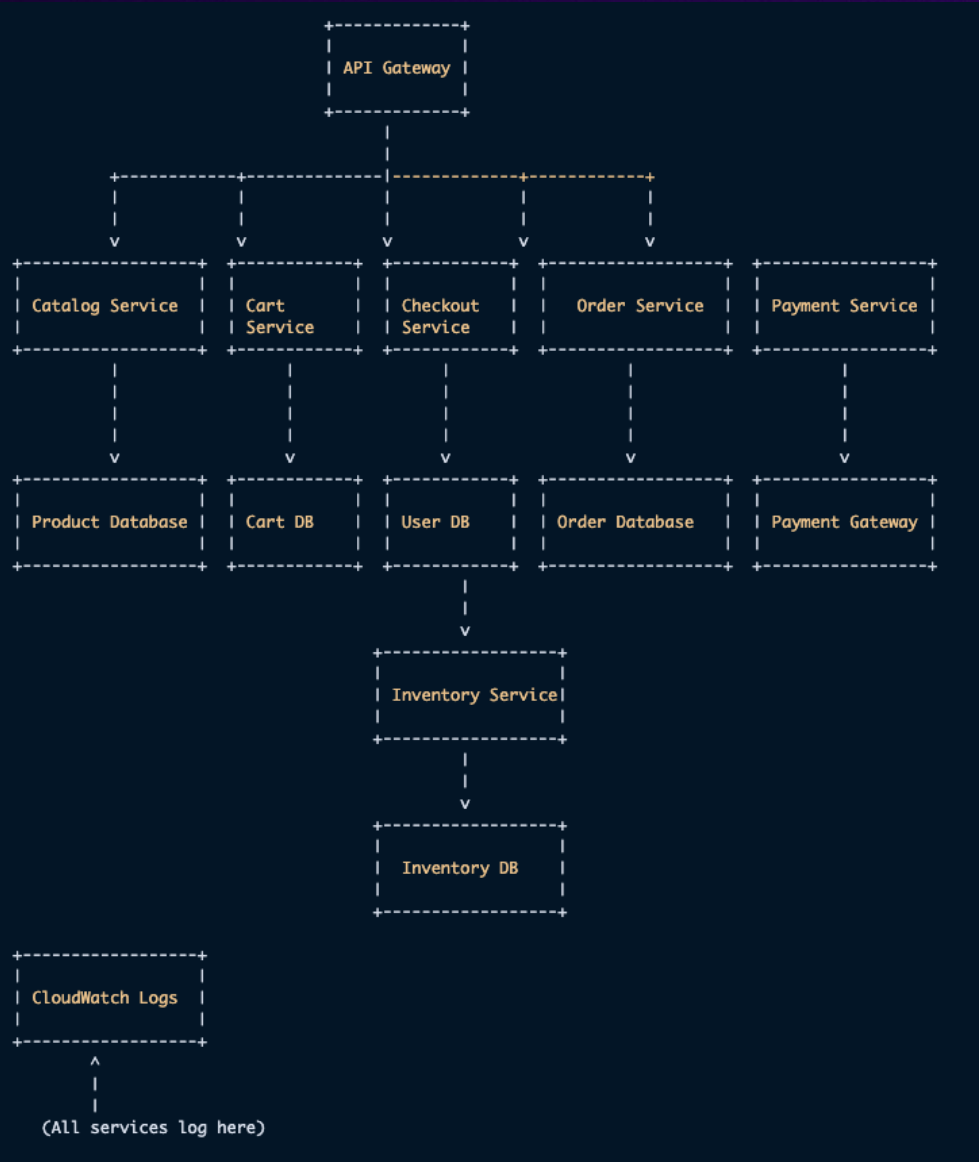
GreenGrocer

GreenGrocer-
Direct

Account demo-2

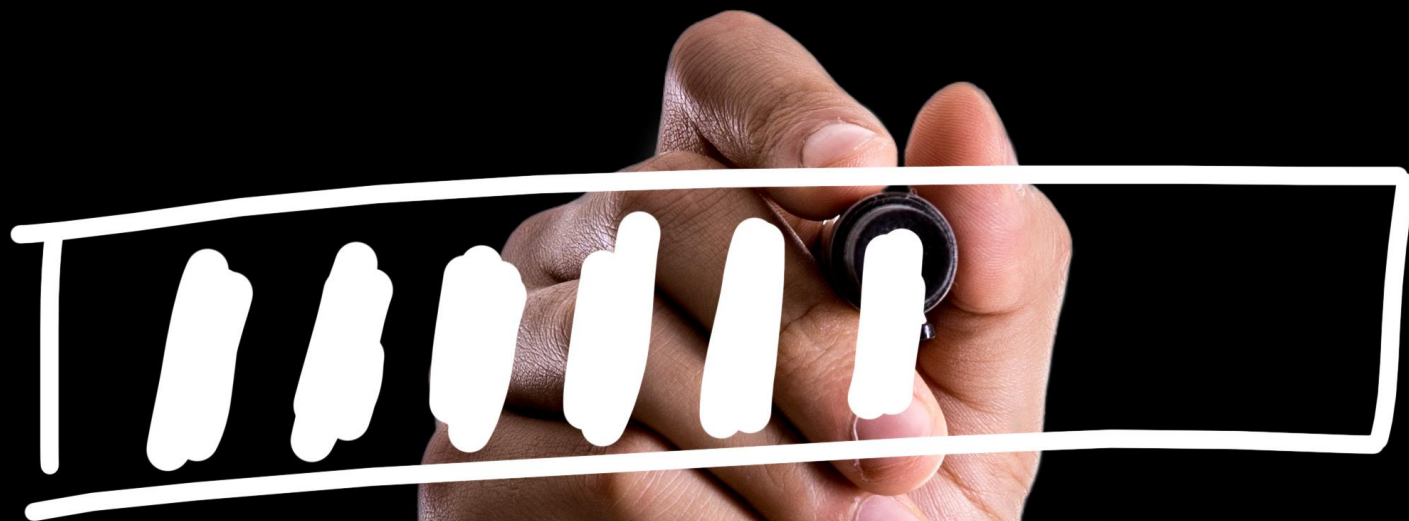
GreenGrocer-
Reseller

Account demo-3



**AI images created using Amazon Bedrock*

DEMO



LOADING...

What did we learn on the show?

- Be deliberate on why you are logging
- Sometimes the best multi-tool is less optimal than a simple chisel - Use the right tool
- Instead of asking 'How do I reduce costs?', the question we should be asking is 'How do I maximize value?'

Known: Known

- Metric filters
- EMF
- Contributor Insights
- Log transformations
- Logs Insights (your time-machine)

Known: Unknown

- Field indexes
- Compare
- Live Tail
- Log patterns
- Anomaly detection

Learn more



Log transformations



Analyze with OpenSearch



Field indexes

Thank you!

Nikhil Kapoor

Principal Product Manager

Amazon Web Services

Andres Silva

Principal Specialist Solutions
Architect

Amazon Web Services



Please complete the session
survey in the mobile app

