



AWS Enterprise Support

Management Tools Intro | Amazon CloudWatch

Andrew Torrence

October 11th, 2021



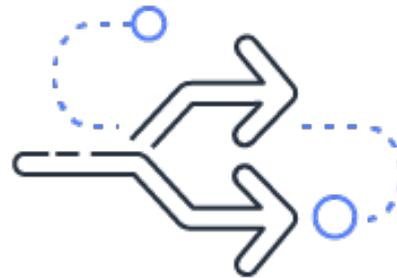
Benefits



Observability on a single platform across applications and infrastructure



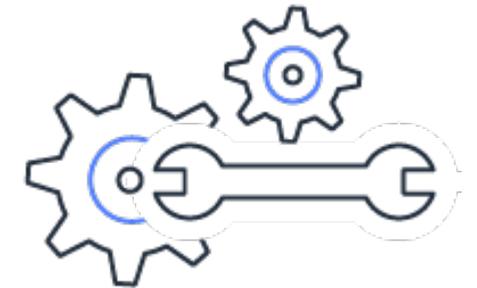
Easiest way to collect metrics in AWS and on-premises



Improve operational performance and resource optimization

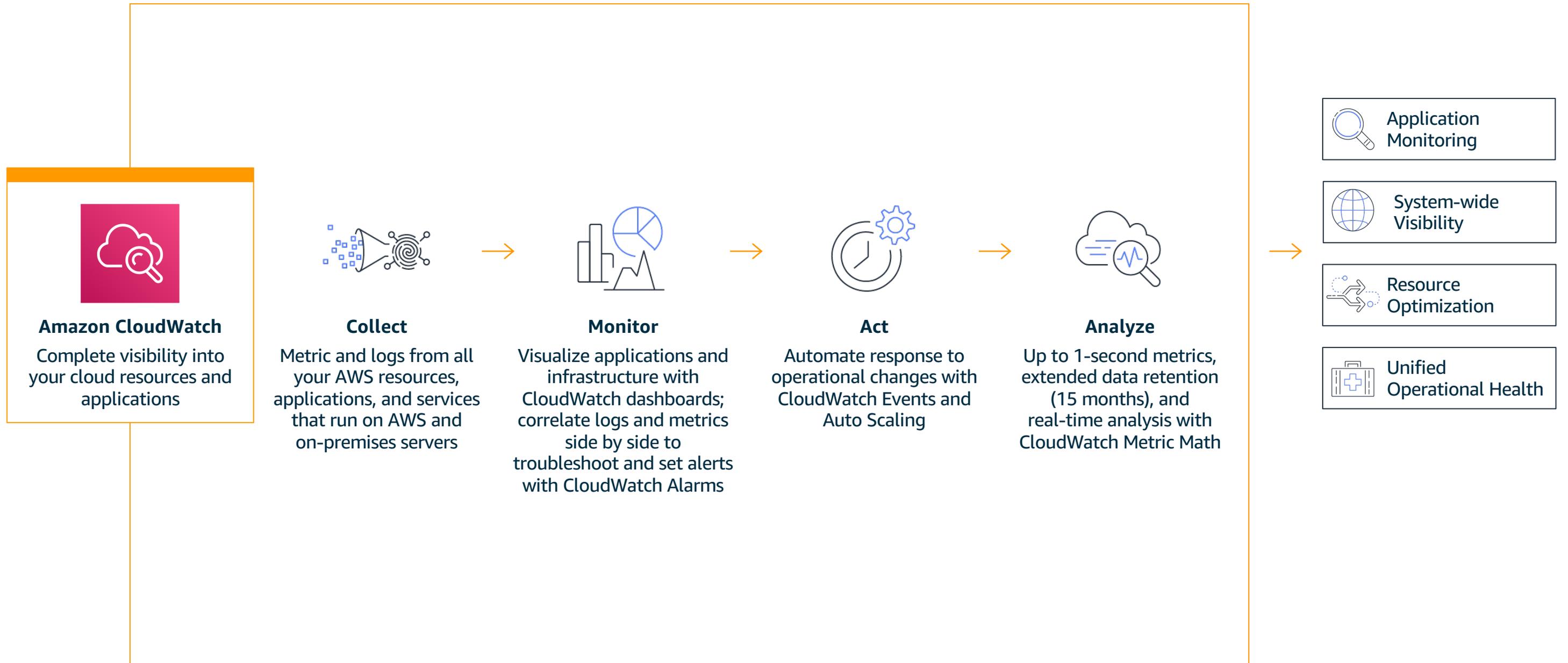


Get operational visibility and insight

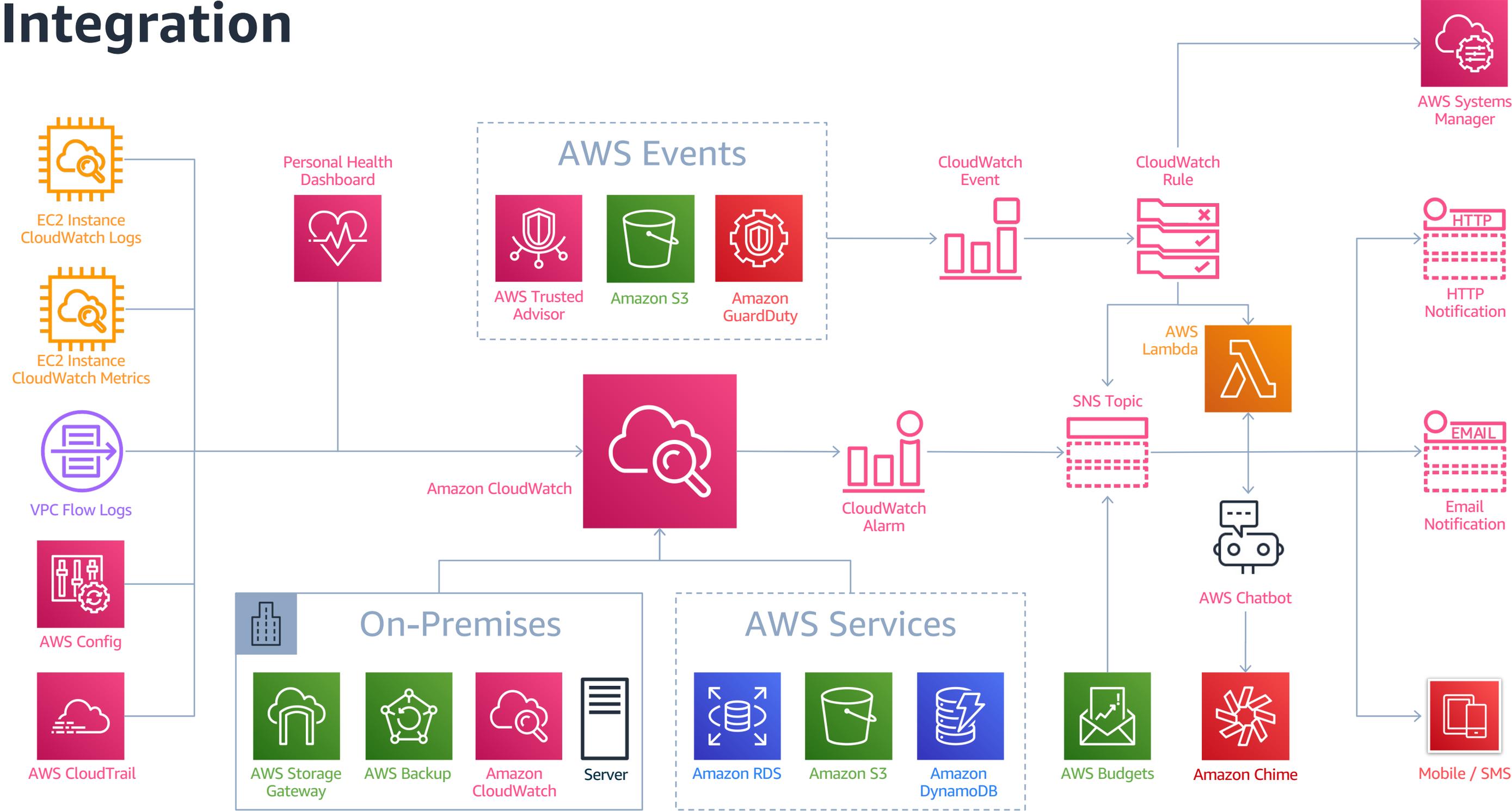


Derive actionable insights from logs

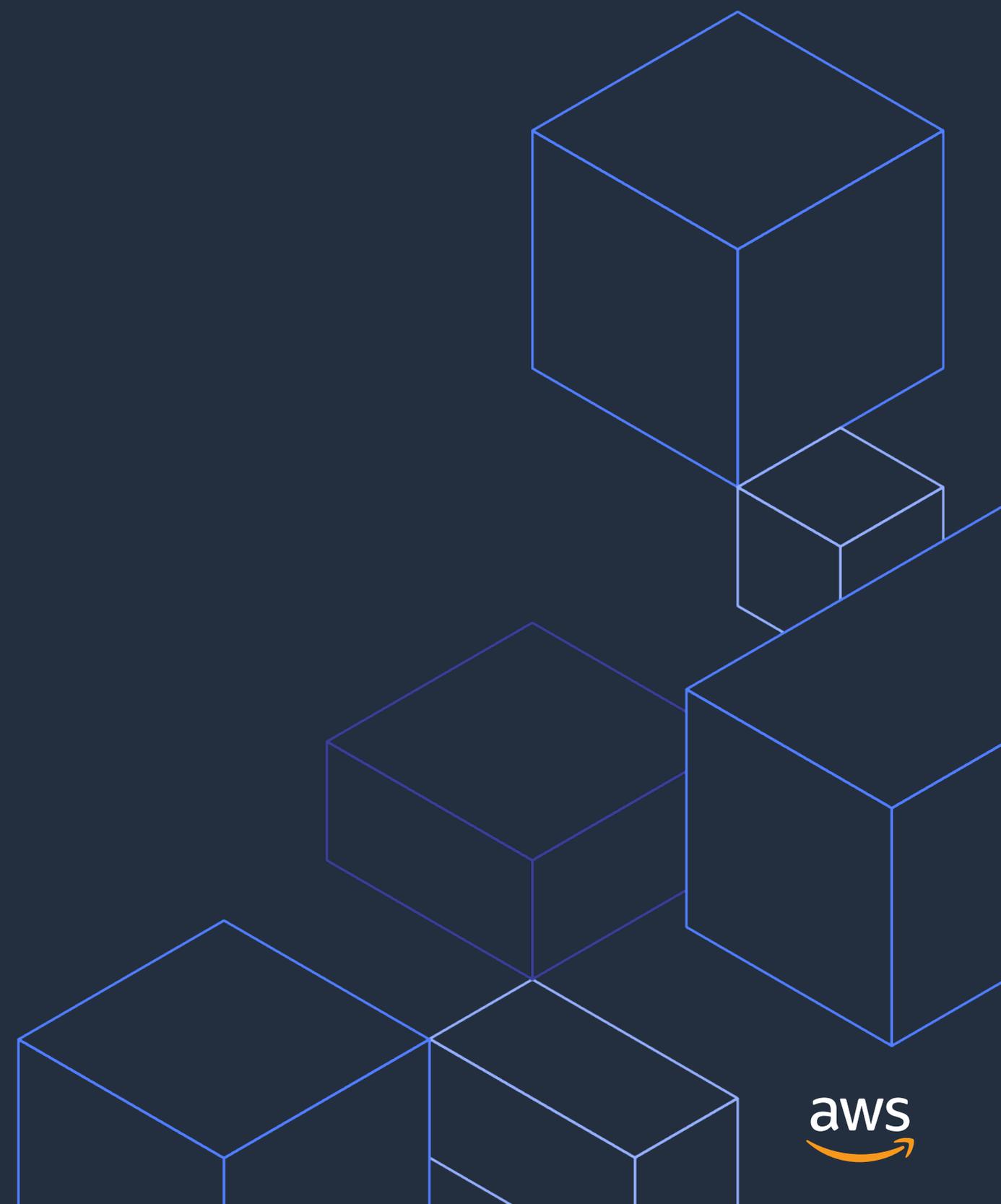
How it works



Integration



Collect



Easily collect and store logs

The Amazon CloudWatch Logs service allows you to collect and store logs from your resources, applications, and services in near real-time.

Collect logs from:

- Amazon EC2 instances
- On-premises servers
- VPC Flow Logs
- AWS CloudTrail
- AWS Lambda
- Other AWS Services

Log data can be stored and accessed indefinitely in highly durable, low-cost storage so you don't have to worry about filling up hard drives.

The screenshot displays the Amazon CloudWatch Logs console interface for a log group named 'application.log'. The breadcrumb navigation shows 'CloudWatch > CloudWatch Logs > Log groups > application.log'. There are buttons for 'Delete', 'Actions', 'Query log group', and 'View all log events'. Below this is a 'Log group details' section with a table of properties:

Retention	Creation time	Stored bytes	ARN
Never expire	5 months ago	14.67 MB	arn:aws:logs:eu-west-1:012345678910:log-group:application.log:*
KMS key ID	Metric filters	Subscriptions	Contributor Insights rules
-	1	LambdaStream_centralized-logging-LogStreamer-1A2RQLPI4N1TW	-

Below the details are tabs for 'Log streams', 'Metric filters', and 'Contributor Insights'. The 'Log streams' tab is active, showing a list of 5 log streams with a search bar and pagination controls. The list includes columns for 'Log stream' and 'Last event time':

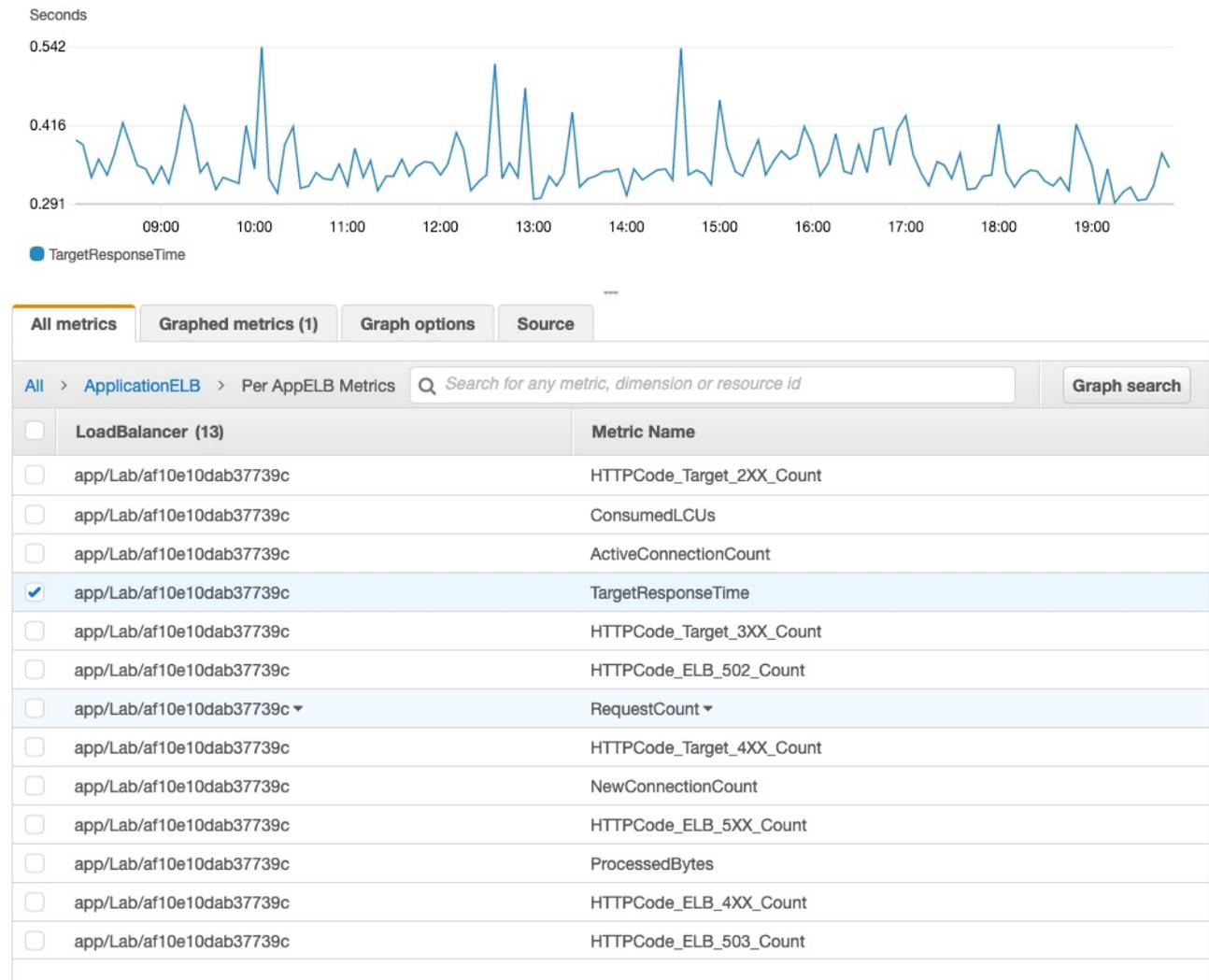
Log stream	Last event time
i-077f7e49ee1c0112c	1/10/2020, 8:00:49 PM
i-03343584efd07d2a6	11/29/2019, 8:03:35 PM
i-09bd407810ebfa83f	11/29/2019, 8:00:52 PM
i-0bf3c984cda70e7c0	9/19/2019, 9:00:35 PM

Built-in metrics

Collecting metrics is time consuming. Amazon CloudWatch allows you to collect default metrics from more than 70 AWS services, such as:

- Amazon EC2
- Amazon DynamoDB
- Amazon S3
- Amazon ECS
- AWS Lambda
- Amazon API Gateway

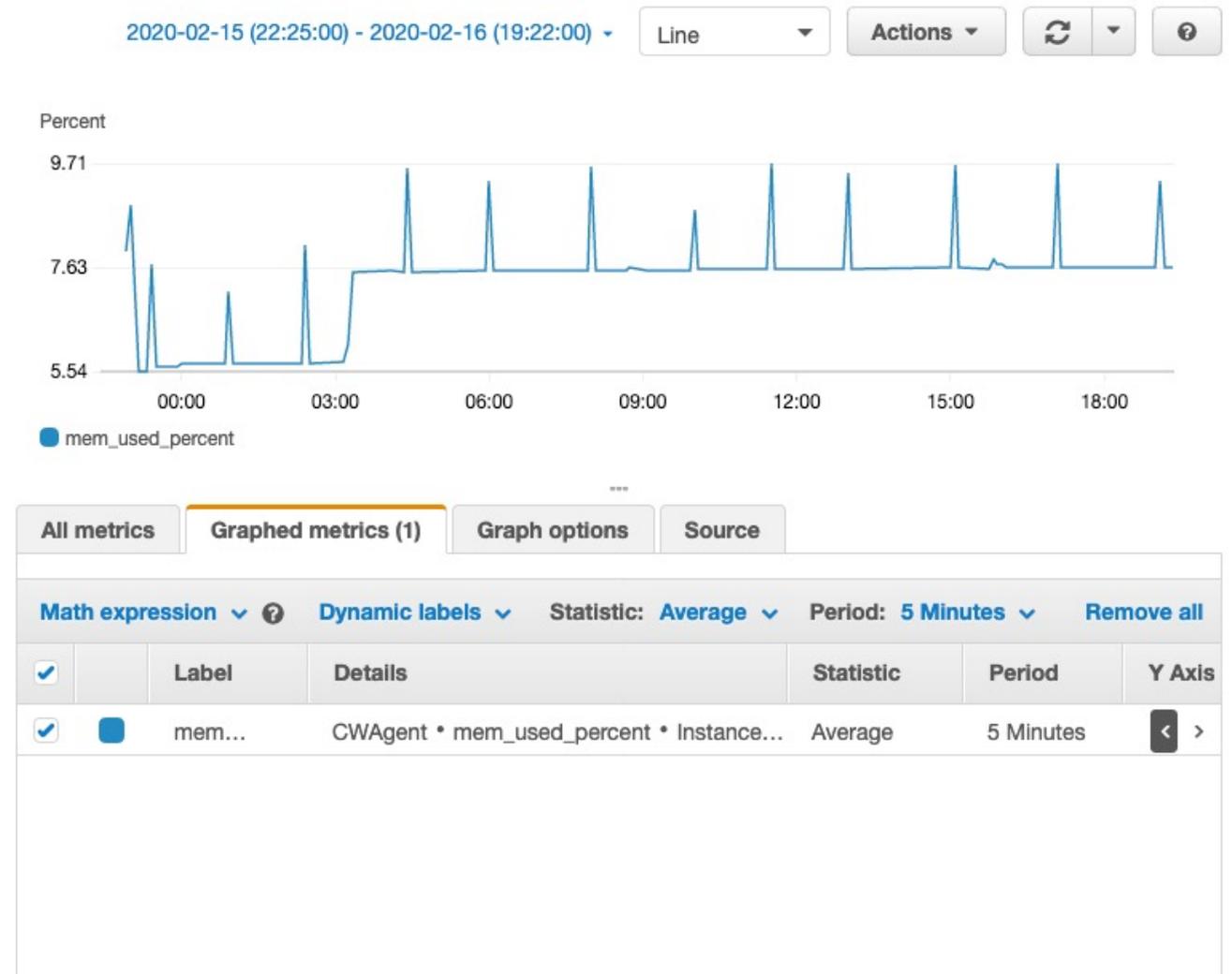
No action is required on your part. For example, EC2 instances automatically publish CPU utilization, data transfer, and disk usage metrics to help you understand changes in state.



Custom metrics

Collect custom metrics from your own applications to monitor operational performance, troubleshoot issues, and spot trends. User activity is an example of a custom metric you can collect and monitor over a period of time.

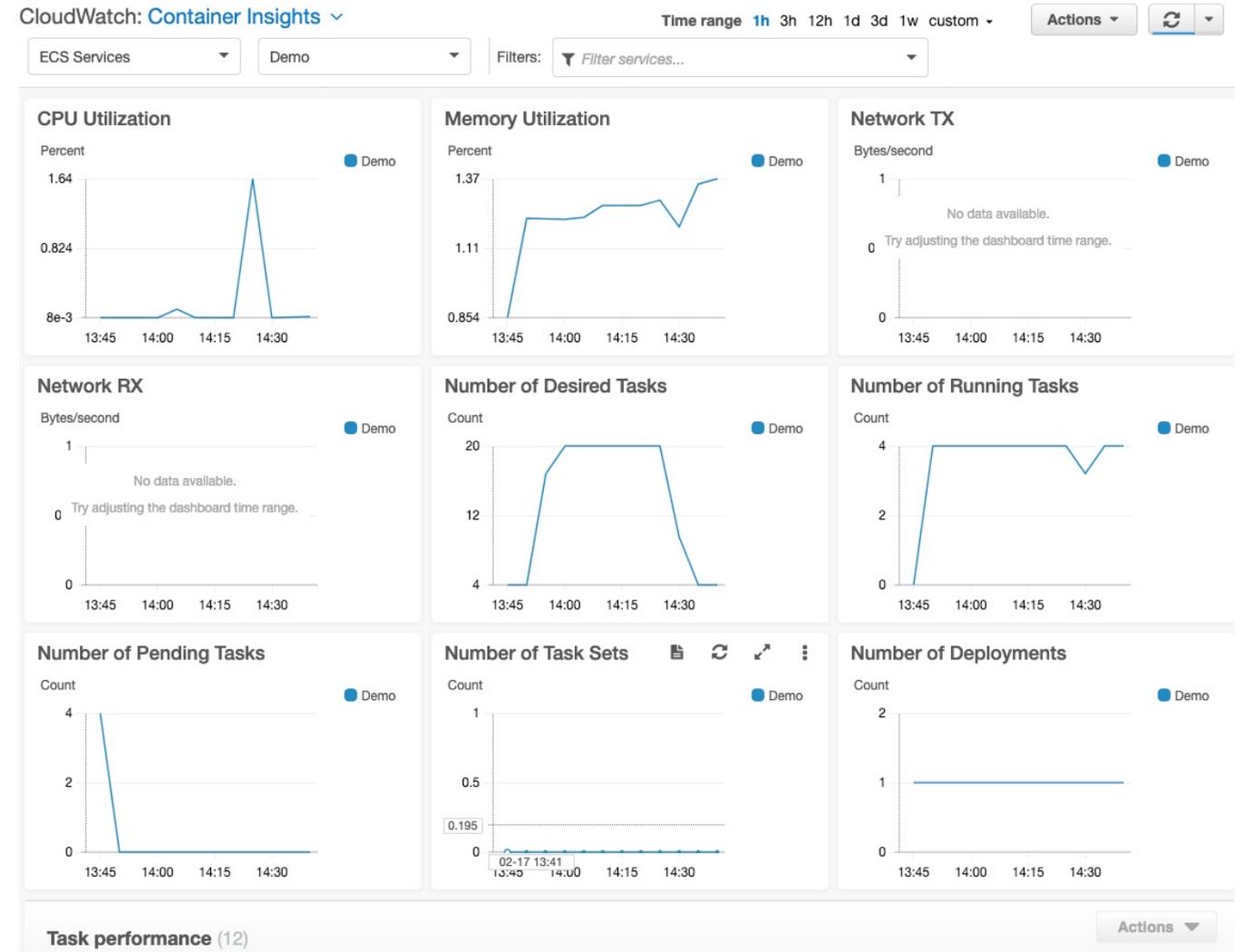
- Publish metrics using the AWS CLI or an API
- Standard resolution, with a one-minute granularity
- High resolution, with a granularity of one second
- Aggregate data before you publish to CloudWatch
- StatsD and collectd support via CloudWatch Agent



Collect and aggregate container metrics and logs

Use CloudWatch Container Insights to collect, aggregate, and summarize metrics and logs from your containerized applications and microservices.

- Collects metrics from each container
 - CPU
 - Memory
 - Disk
 - Network
- Automatically generated dashboards
- Set alarms on metrics



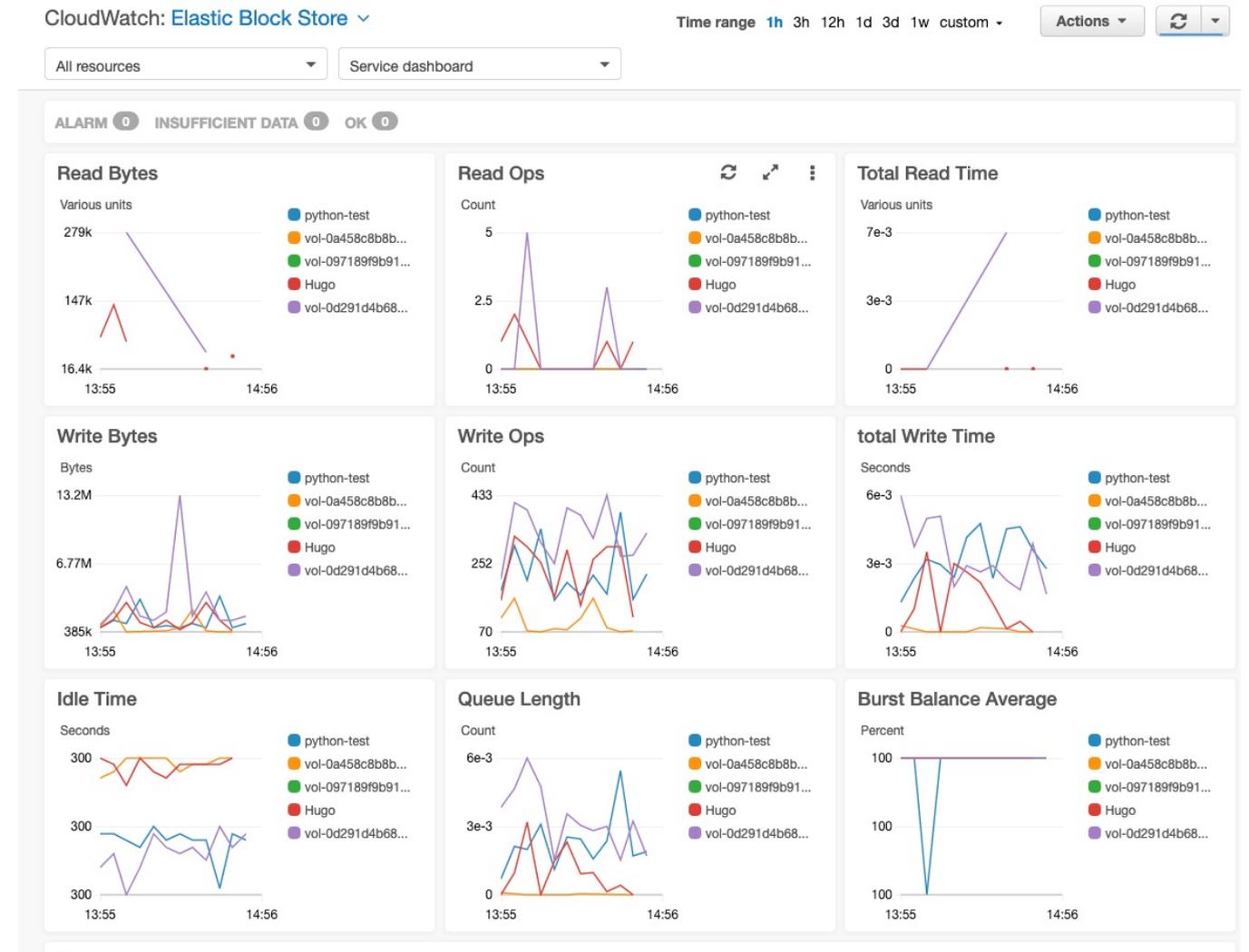
Monitor



Unified operational view with dashboards

Amazon CloudWatch dashboards enable you to create re-usable graphs and visualize your cloud resources and applications in a unified view.

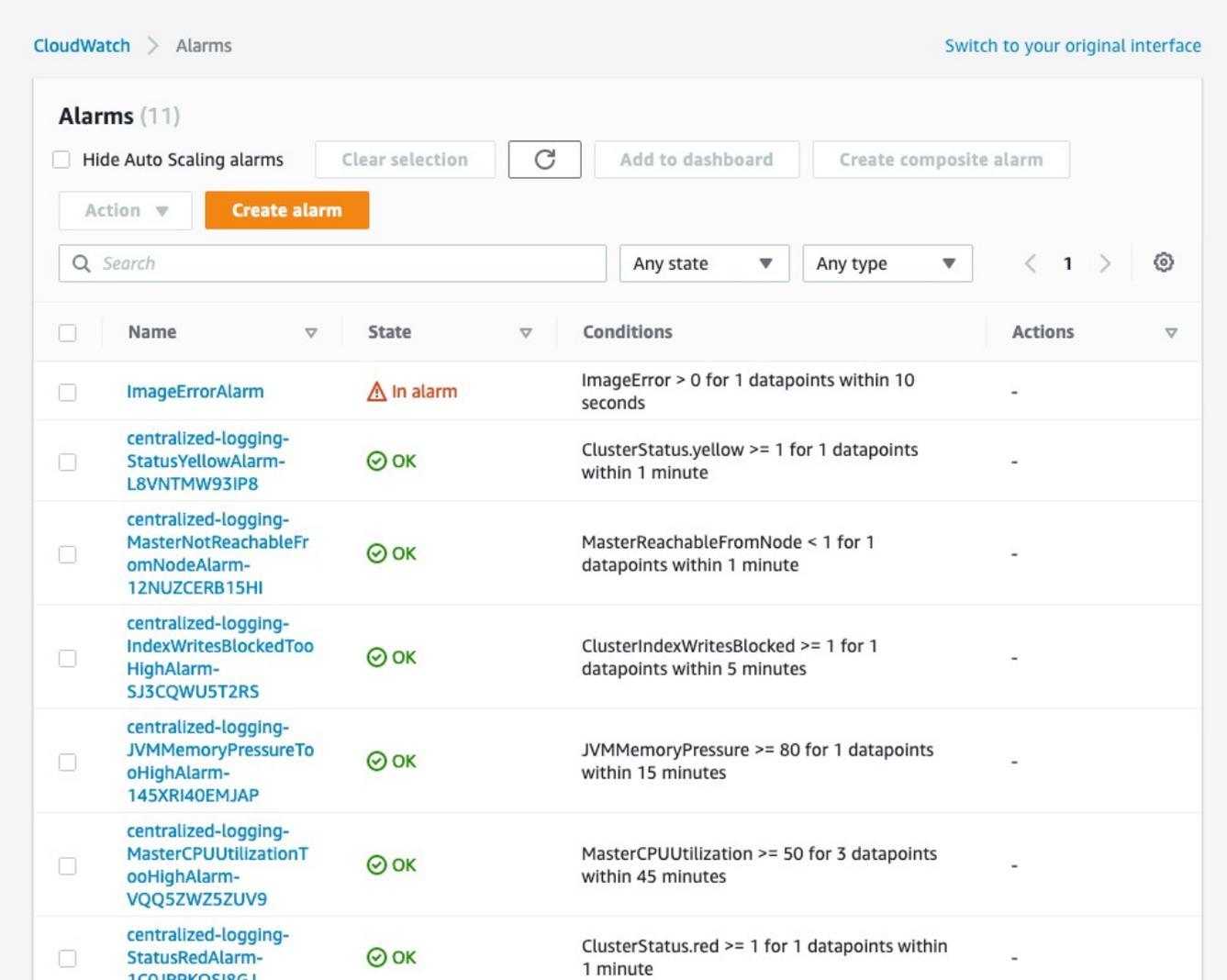
- A single view for selected metrics and alarms
- Multiple AWS accounts and multiple Regions.
- An operational playbook
- A common view of critical resource and application measurements that can be shared



High resolution alarms

Amazon CloudWatch alarms allow you to set a threshold on metrics and trigger an action.

- Watch a single metric or the result of a math expression
- Perform actions based on the value of metrics
 - Send a notification to an SNS topic
 - Auto Scaling action
 - EC2 Action (Stop, Terminate, Reboot or Recover)
- Add alarms to dashboards to visualize them



The screenshot displays the Amazon CloudWatch Alarms console. At the top, it shows 'CloudWatch > Alarms' and a link to 'Switch to your original interface'. Below this, there's a section for 'Alarms (11)' with a 'Hide Auto Scaling alarms' checkbox and buttons for 'Clear selection', 'Add to dashboard', and 'Create composite alarm'. A search bar and filters for 'Any state' and 'Any type' are also present. The main part of the screenshot is a table listing the alarms:

<input type="checkbox"/>	Name	State	Conditions	Actions
<input type="checkbox"/>	ImageErrorAlarm	In alarm	ImageError > 0 for 1 datapoints within 10 seconds	-
<input type="checkbox"/>	centralized-logging-StatusYellowAlarm-L8VNTMW93IP8	OK	ClusterStatus.yellow >= 1 for 1 datapoints within 1 minute	-
<input type="checkbox"/>	centralized-logging-MasterNotReachableFromNodeAlarm-12NUZCERB15HI	OK	MasterReachableFromNode < 1 for 1 datapoints within 1 minute	-
<input type="checkbox"/>	centralized-logging-IndexWritesBlockedTooHighAlarm-SJ3CQWU5T2RS	OK	ClusterIndexWritesBlocked >= 1 for 1 datapoints within 5 minutes	-
<input type="checkbox"/>	centralized-logging-JVMMemoryPressureTooHighAlarm-145XRI40EMJAP	OK	JVMMemoryPressure >= 80 for 1 datapoints within 15 minutes	-
<input type="checkbox"/>	centralized-logging-MasterCPUUtilizationTooHighAlarm-VQQ5ZWZ5ZUV9	OK	MasterCPUUtilization >= 50 for 3 datapoints within 45 minutes	-
<input type="checkbox"/>	centralized-logging-StatusRedAlarm-1CQJRPKOSI8GJ	OK	ClusterStatus.red >= 1 for 1 datapoints within 1 minute	-

Logs and metrics correlation

Amazon CloudWatch also makes it easy to correlate metrics and logs.

- Manage logs and metrics in a single platform
- Use metric filters to convert logs to metrics

The screenshot displays the Amazon CloudWatch console interface for a log group named 'application.log'. At the top, there are navigation breadcrumbs: 'CloudWatch > CloudWatch Logs > Log groups > application.log'. On the right side, there are buttons for 'Delete', 'Actions', 'Query log group', and 'View all log events'. Below this is the 'Log group details' section, which contains a table with the following information:

Retention	Creation time	Stored bytes	ARN
Never expire	5 months ago	14.67 MB	arn:aws:logs:eu-west-1:012345678910:log-group:application.log:*
KMS key ID	Metric filters	Subscriptions	Contributor Insights rules
-	1	LambdaStream_centralized-logging-LogStreamer-1A2RQLP4N1TW	-

Below the details section, there are tabs for 'Log streams', 'Metric filters', and 'Contributor Insights'. The 'Metric filters' tab is active, showing a list of one metric filter. The filter is named 'ActiveStorage-InvariableError' and has a checkbox to its right. The filter pattern is '"ActiveStorage::InvariableError"'. The metric is 'LogMetrics / ImageError'. The metric value is '1' and the default value is '-'. There is a link to 'ImageErrorAlarm' under the 'Alarms' section. At the top of the metric filters list, there are buttons for 'Edit', 'Delete', 'Create alarm', and 'Create metric filter'. A search bar with the placeholder 'Find metric filters' and a pagination control showing '1' are also present.

Application Insights for .NET and SQL Server applications

Easily monitor .NET and SQL Server applications, so you can get visibility into the health of such applications.

- Automatic Set Up of Monitors for Application Resources
- Problem Detection and Notification
- Automatic dashboards
- Insights that point to potential root causes

CloudWatch: Application Insights

Problem Id: p-2743c262-b50d-4364-bc76-474aa0f311f6 [Edit configuration](#)

Actions 

Problem summary

Severity	Problem summary	Source	Start / End time	Status	Resource group
High	SQL: Transaction Log Full	i-023bb397781704add	2019-06-20T16:16:51Z	In progress	testapp2

Insight 

SQL Server Engine issues a 9002 error when the transaction log is full. To make log space available, you may back up the log, free up disk space, move the log file to a disk drive with sufficient space, increase the size of the log file, or terminate a long-running transaction.

Help us improve our models: This insight is useful This insight is not useful [Submit feedback](#)

DOT_NET_WEB: AWS::ElasticLoadBalancingV2::LoadBalancer::app/AdventureWorksSampleLoadBalancer



30d03b5ff1468da4 - HTTPCode_Target_4XX_Count

No unit

0.933

0.466

0

≥ 0.1 for 1 datapoints within 5 minutes

17:00 17:30 18:00 18:30 19:00 19:30 20:00

result

30d03b5ff1468da4 - HTTPCode_Target_5XX_Count

No unit

0.125

0.063

0

≥ 0.02 for 1 datapoints within 5 minutes

17:00 17:30 18:00 18:30 19:00 19:30 20:00

result

SQL_SERVER: AWS::EC2::Instance::i-023bb397781704add

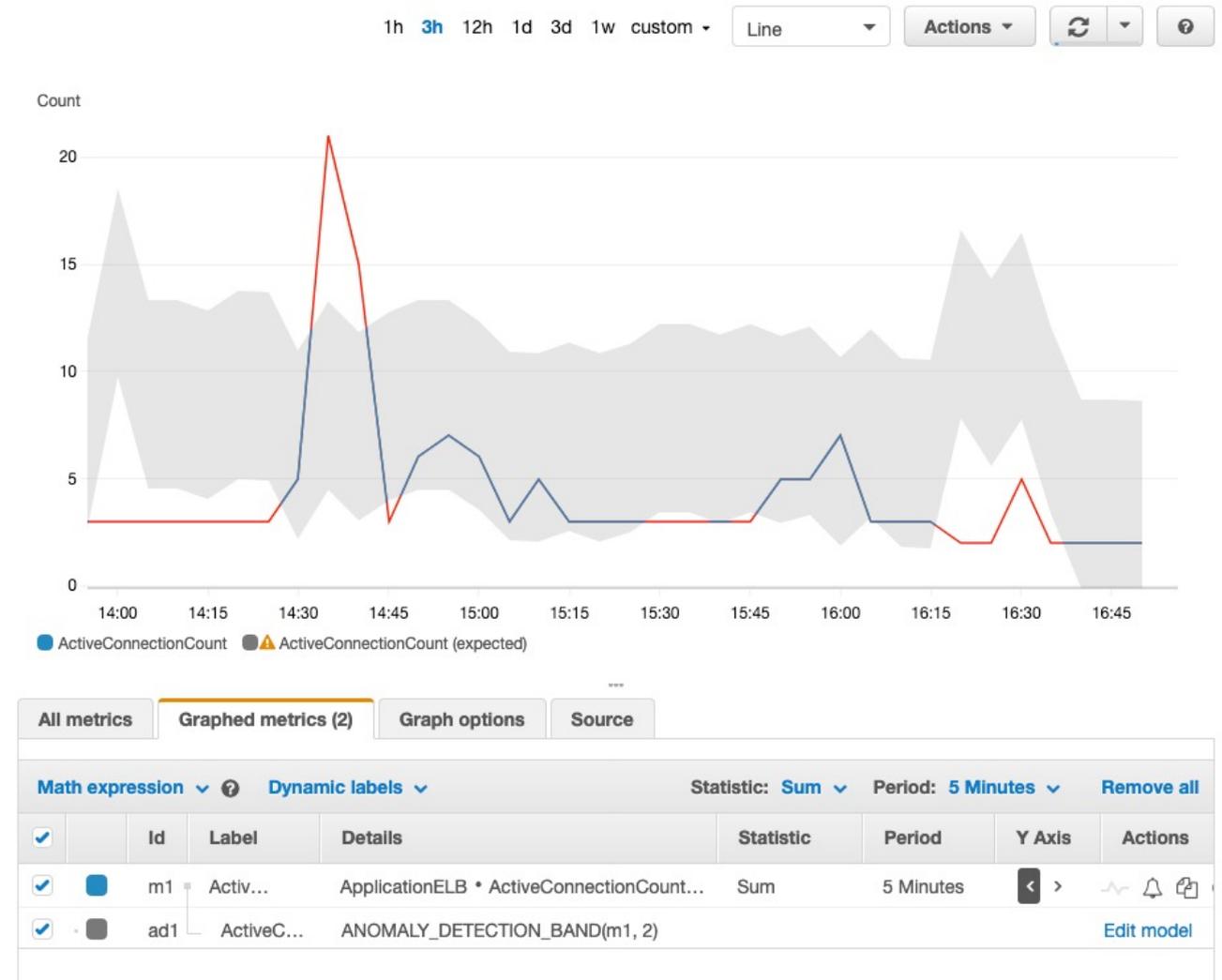
Log Group: SQL_SERVER, Log Type: SQL_SERVER, TransactionLogFull

#	@timestamp	@message
1	2019-05-20T19:37:07.064Z	2019-05-20 19:37:06.82 spid19s Error: 9002, Severity: 17, Sta
2	2019-05-20T19:22:51.344Z	2019-05-20 19:22:51.31 spid61s Error: 9002, Severity: 17, Sta
3	2019-05-20T19:07:06.417Z	2019-05-20 19:07:06.34 spid40s Error: 9002, Severity: 17, Sta
4	2019-05-20T18:37:05.912Z	2019-05-20 18:37:05.88 spid31s Error: 9002, Severity: 17, Sta
5	2019-05-20T18:32:51.507Z	2019-05-20 18:32:51.27 spid59s Error: 9002, Severity: 17, Sta
6	2019-05-20T18:18:48.138Z	2019-05-20 18:18:48.06 spid53 Error: 9002, Severity: 17, Stat
7	2019-05-20T18:18:48.138Z	2019-05-20 18:18:48.06 spid53 Error: 9002, Severity: 17, Stat
8	2019-05-20T18:07:05.395Z	2019-05-20 18:07:05.32 spid36s Error: 9002, Severity: 17, Sta

Anomaly Detection

When you enable anomaly detection for a metric, CloudWatch applies machine learning algorithms to the metric's past data to create a model of the metric's expected values.

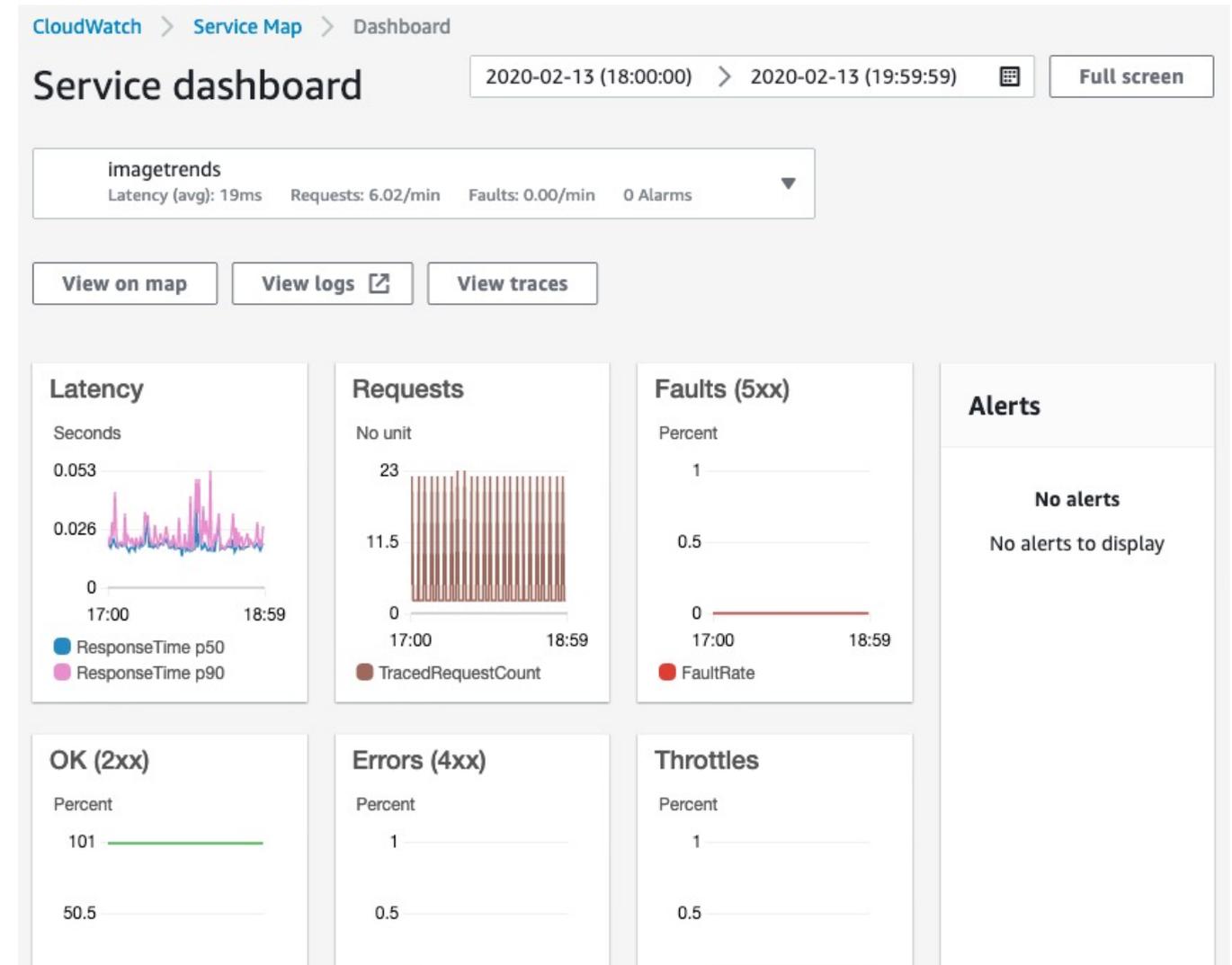
- Create alarms that auto-adjust thresholds based on natural metric patterns
- Alarm when the metric value is above or below the band, or both
- Visualize metrics with anomaly detection bands on dashboards



ServiceLens

You can use Amazon CloudWatch ServiceLens to visualize and analyze the health, performance, and availability of your applications in a single place.

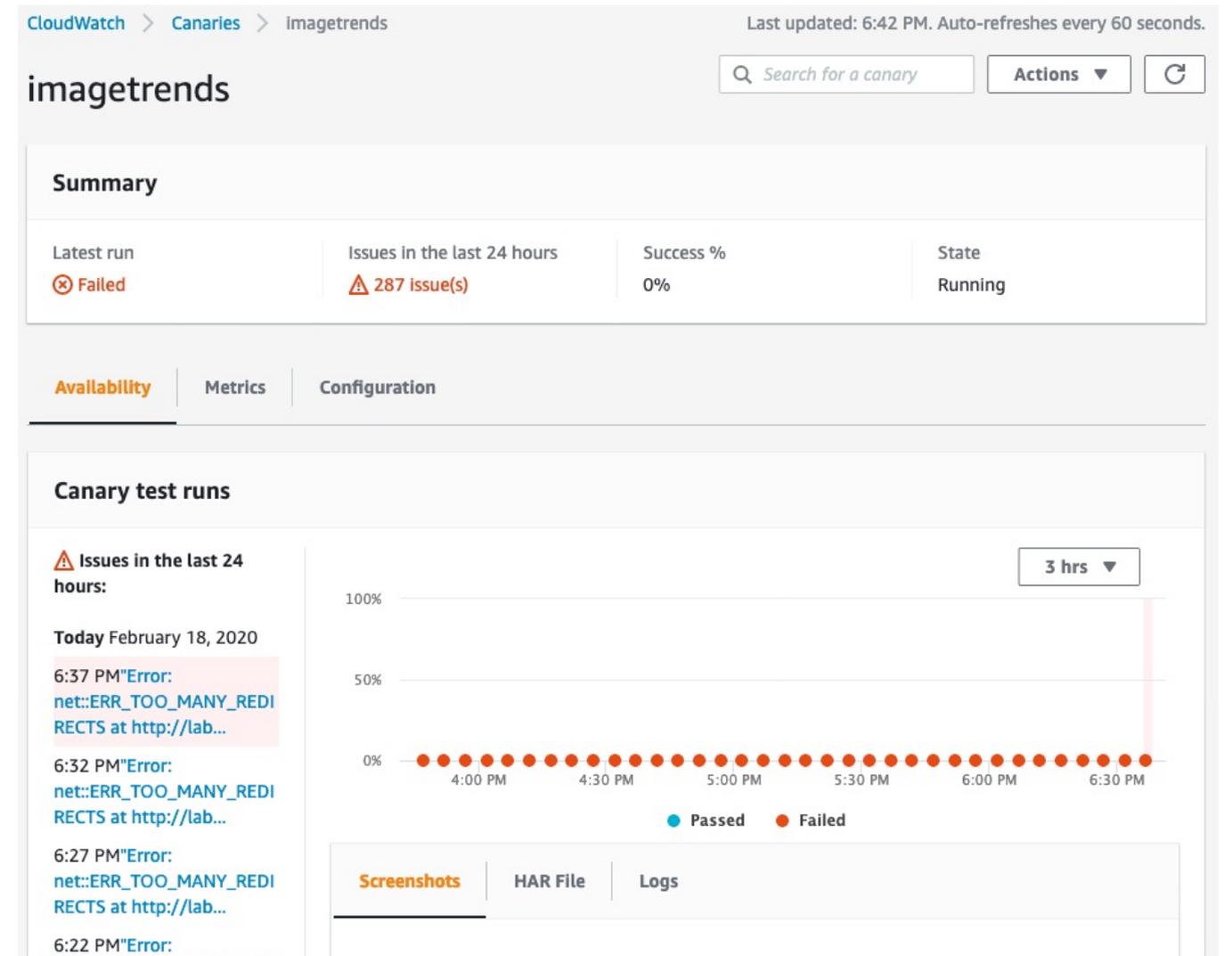
- Integrates CloudWatch with AWS X-Ray to provide an end-to-end view of your application
- A service map displays your service endpoints and resources as “nodes” and highlights the traffic, latency, and errors for each node and its connections
- You can choose a node to see detailed insights about the correlated metrics, logs, and traces associated with that part of the service



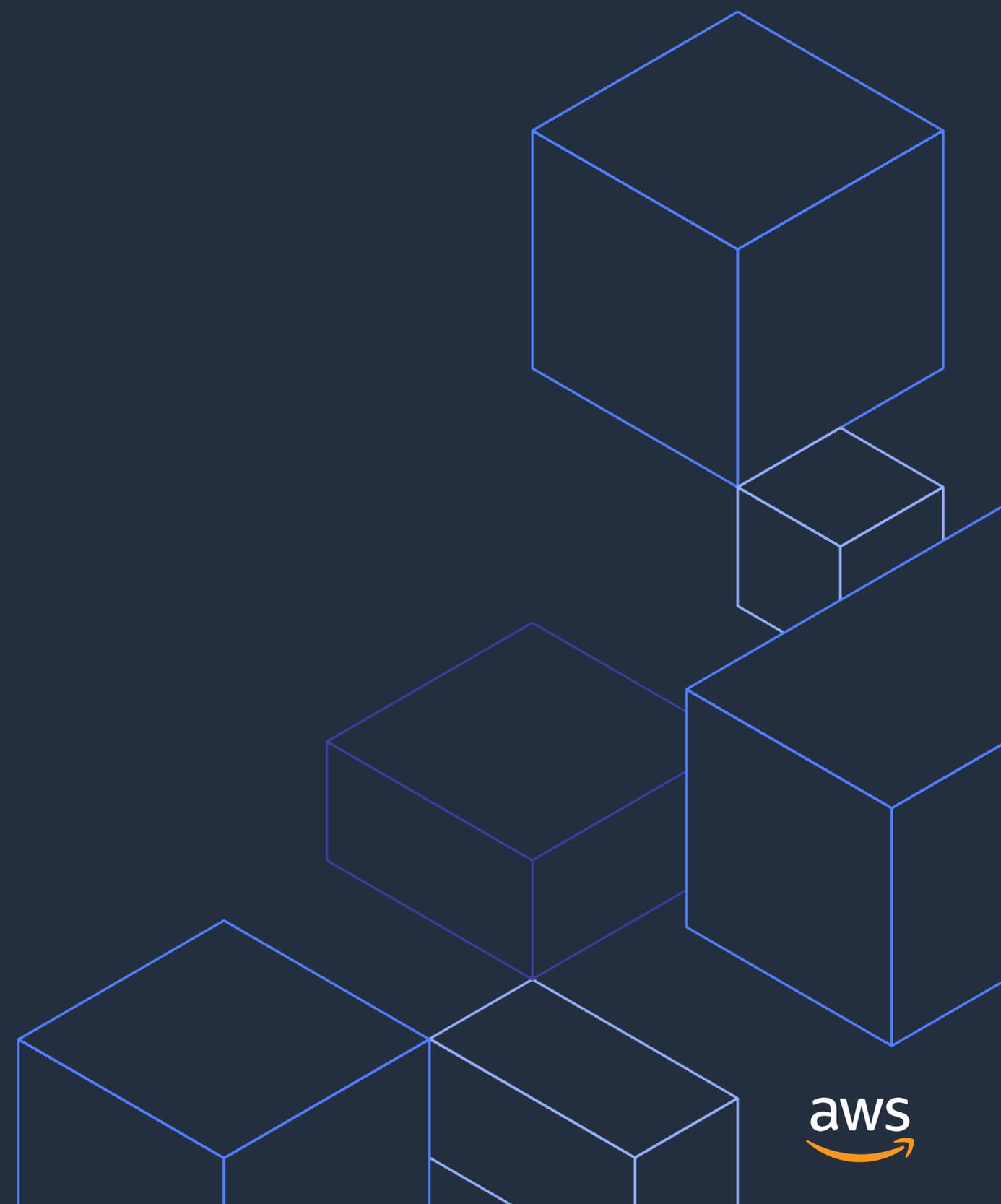
Synthetics

Run tests on your endpoints every minute, 24x7, and alerts you as soon as your application endpoints don't behave as expected.

- View of your customers' experiences
- Configurable scripts
- Run once
- Run on a schedule
- Check availability and latency
- Store load time data
- Store screenshots



Act



Auto Scaling

Auto Scaling helps you automate capacity and resource planning.

- Set a threshold to alarm on a key metric and trigger an automated Auto Scaling action
- For example, you could set up an Auto Scaling workflow based on queue depth
- Configure policies to scale in or scale out
- Allows you to set 1 scaling policy and trigger with multiple alarms

Auto Scaling action

Alarm state trigger

Define the alarm state that will trigger this action.

Remove

In alarm

The metric or expression is outside of the defined threshold.

OK

The metric or expression is within the defined threshold.

Insufficient data

The alarm has just started or not enough data is available.

Resource type

Select a resource type.

EC2 Auto Scaling group

ECS Service

Select a group

Lab-ASG-GK90F109AQP9-AppAutoScalingGro... ▼

Only Auto Scaling groups with a simple scaling or step scaling policy in this account are available.

Take the following action...

Test (Add 1 instance) ▼

Only actions for the selected Auto Scaling group are available.

Add new Auto Scaling action

Automate response to changes with CloudWatch Events

CloudWatch Events provides a near real-time stream of system events that describe changes to your AWS resources.

- Respond quickly
- Take corrective action

Write rules to indicate which events are of interest to your application and what automated actions to take when a rule matches an event.

- Invoke a Lambda Function
- Notify an SNS Topic
- Create an Ops Item in Systems Manager

Rules > ChangeInstanceSize

Actions ▾

Summary

ARN ⓘ `arn:aws:events:eu-west-1:180304385487:rule/ChangeInstanceSize`

Schedule Cron expression `0 6 ? * 6L *`

Next 10 Trigger Date(s)

1. Fri, 28 Feb 2020 06:00:00 GMT
2. Fri, 27 Mar 2020 06:00:00 GMT
3. Fri, 24 Apr 2020 06:00:00 GMT
4. Fri, 29 May 2020 06:00:00 GMT
5. Fri, 26 Jun 2020 06:00:00 GMT
6. Fri, 31 Jul 2020 06:00:00 GMT
7. Fri, 28 Aug 2020 06:00:00 GMT
8. Fri, 25 Sep 2020 06:00:00 GMT
9. Fri, 30 Oct 2020 06:00:00 GMT
10. Fri, 27 Nov 2020 06:00:00 GMT

Status Enabled

Description

Monitoring [Show metrics for the rule](#)

Targets

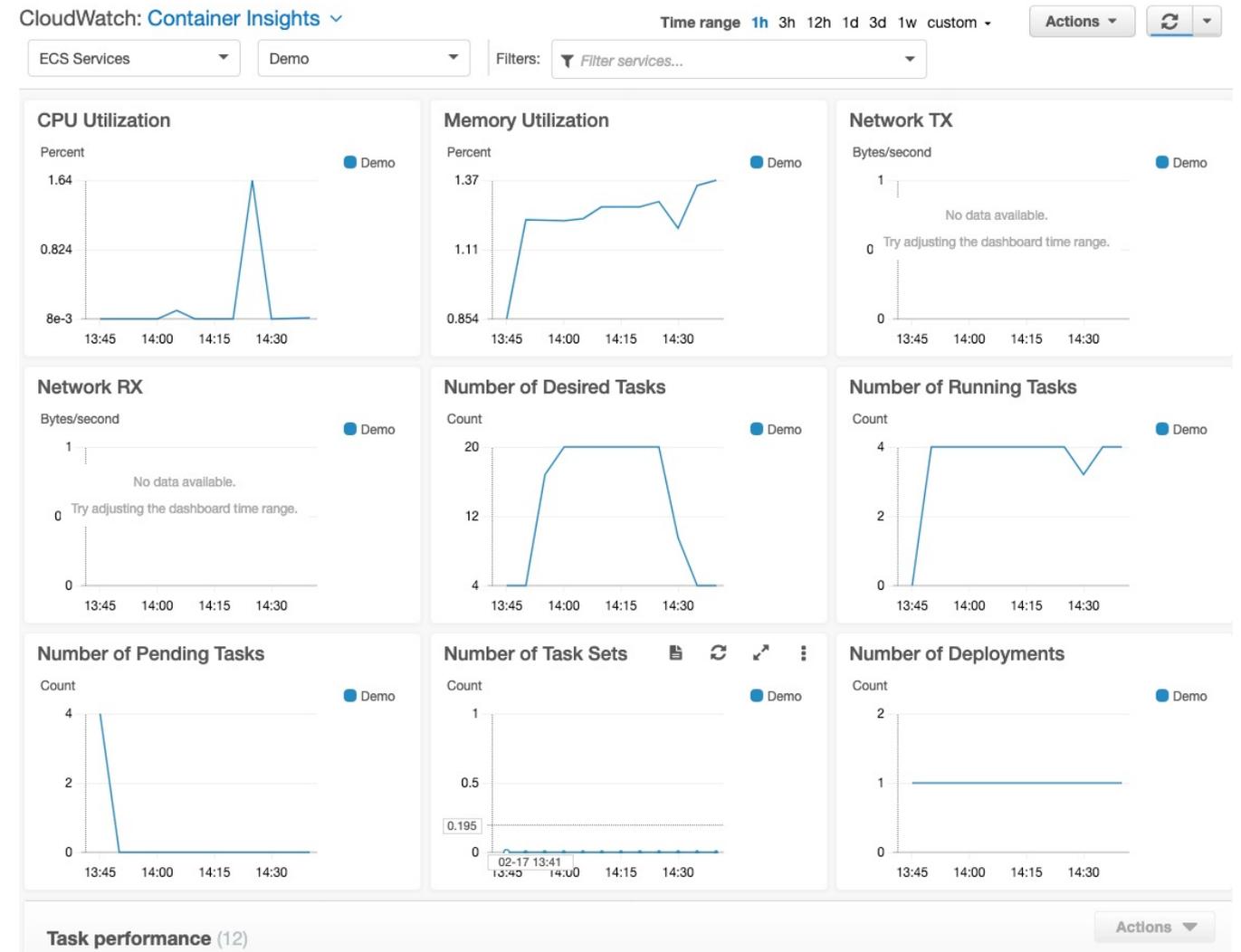
Filter:

Type	Name	Input
SSM Automation	ChangeInstanceSize (version \$DEFAULT)	Constant: {"InstanceId":["i-0cb0104ddf22z

Alarm and automate actions on EKS, ECS, and k8s clusters

For Amazon EKS and k8s clusters, Container Insights allows you to alarm on compute metrics to trigger auto scaling policies on your Amazon EC2 Auto Scaling group and provides you the ability to stop, terminate, reboot, and recover any Amazon EC2 instance.

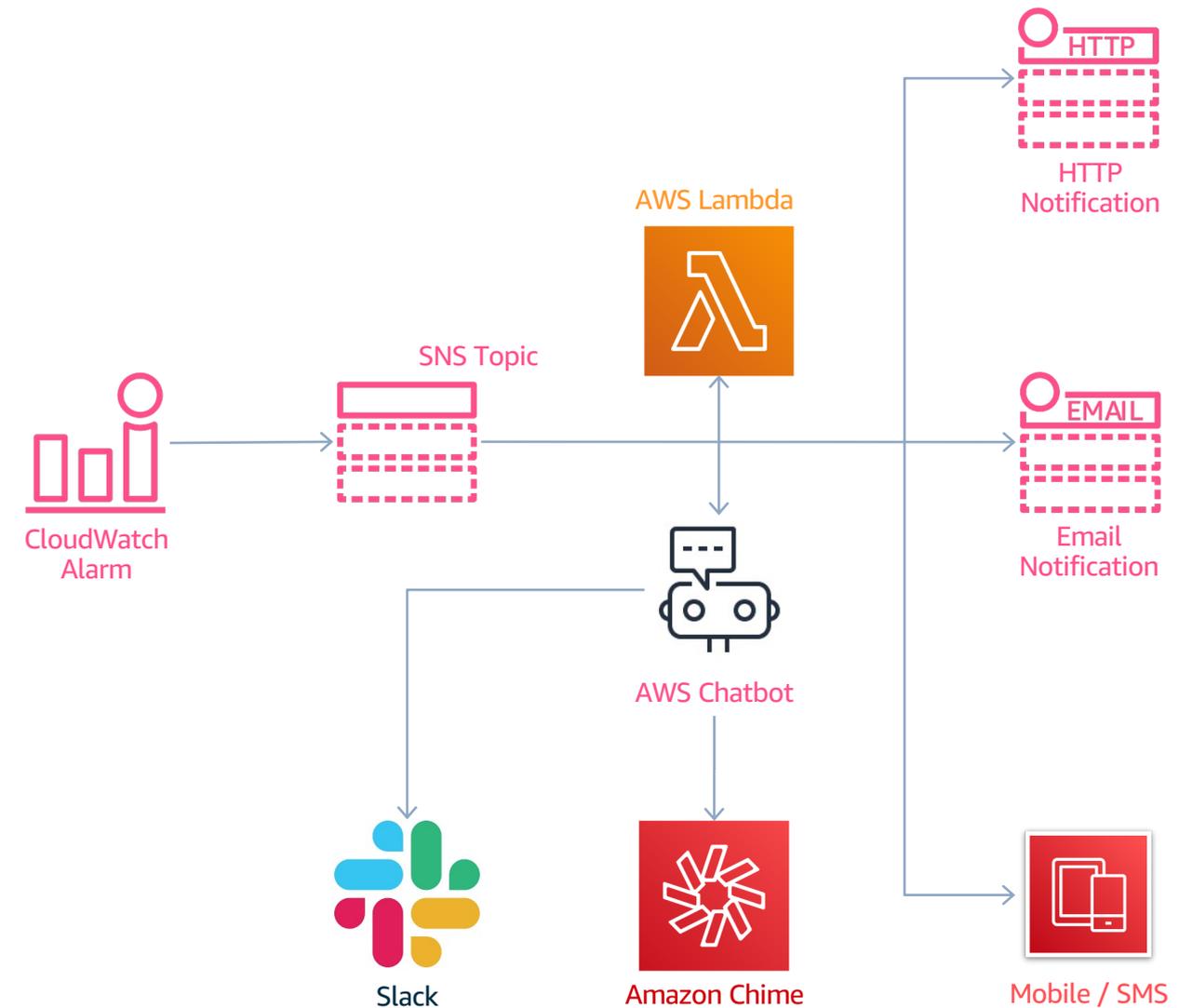
For Amazon ECS clusters, compute metrics from your tasks and services can be used for Service Auto Scaling.



Automation

CloudWatch Alarms can send a notification to SNS, from there, you can trigger a Lambda function or push a message to Slack or Amazon Chime via AWS Chatbot. This allows you to do almost anything, including:

- Trigger a Systems Manager Automation
- Resize an instance
- Send a message to Chime or Slack
 - Respond with CLI commands
- Invoke disaster recovery
- Update security groups
- Automate deployments
- Instigate backups and snapshots
- Responding to security events



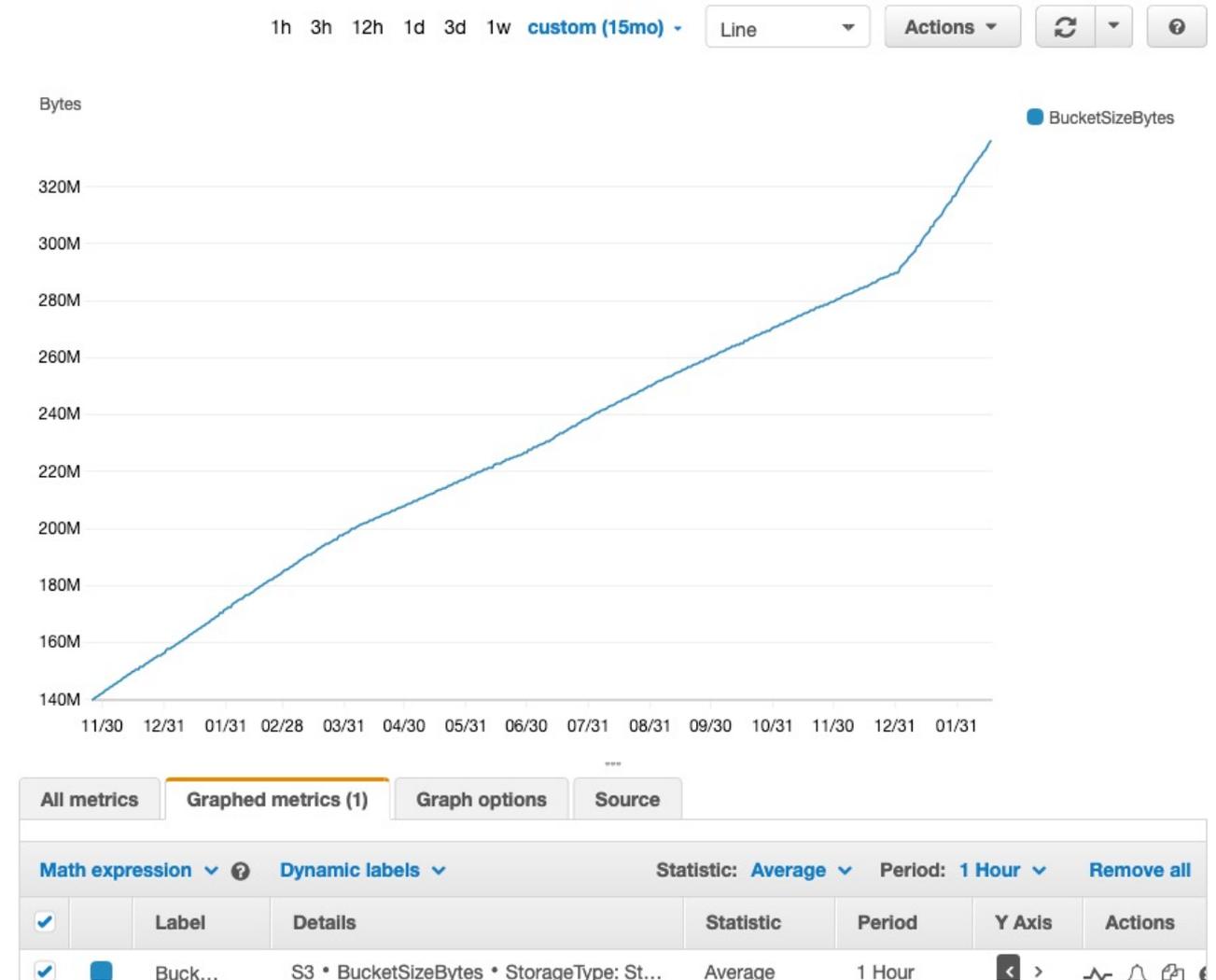
Analyze



Granular data and extended retention

Amazon CloudWatch allows you to monitor trends and seasonality with 15 months of metric data (storage and retention).

- Historical analysis to fine-tune resource utilization
- Collect metrics with a granularity of 1 second
- Granular real-time data enables better visualization
- Spot and monitor trends to optimize applications



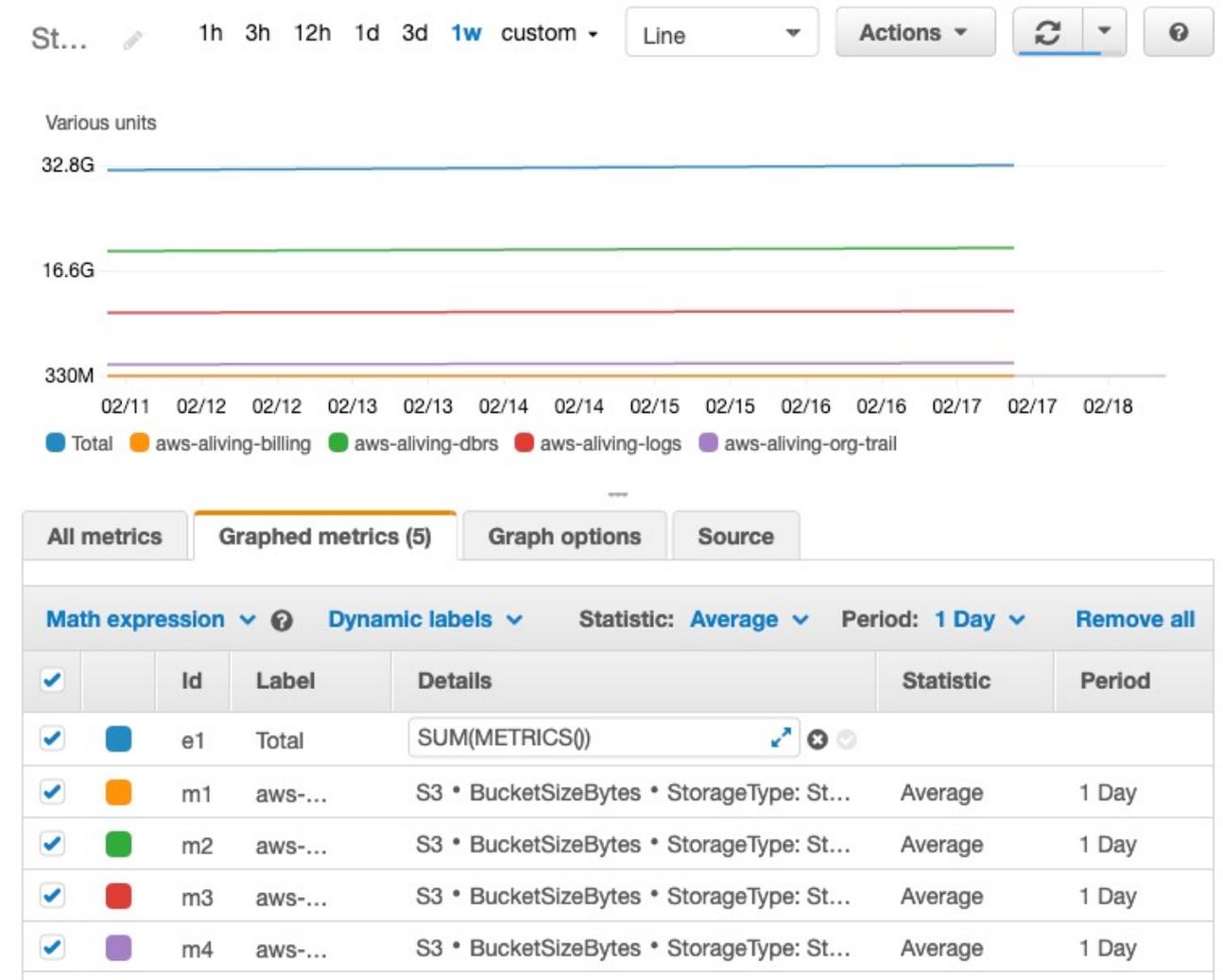
Custom operations on metrics

Metric Math enables you to perform calculations across multiple metrics for real-time analysis.

- Visualize computed metrics in the Console
- Add them to CloudWatch dashboards
- Retrieve them using the GetMetricData API action

Metric Math supports arithmetic operations such as +, -, /, *, and mathematical functions such as Sum, Average, Min, Max, and Standard Deviation.

Using AWS Lambda metrics as an example, you could divide the Errors metric by the Invocations metric to get an error rate.



Log analytics

CloudWatch Logs Insights enables you to drive actionable intelligence from your logs to address operational issues without needing to provision servers or manage software.

- You can instantly begin writing queries with aggregations, filters, and regular expressions
- In addition, you can:
 - Visualize timeseries data
 - Drill down into individual log events
 - Export query results to CloudWatch Dashboards
- You only pay for the queries you run

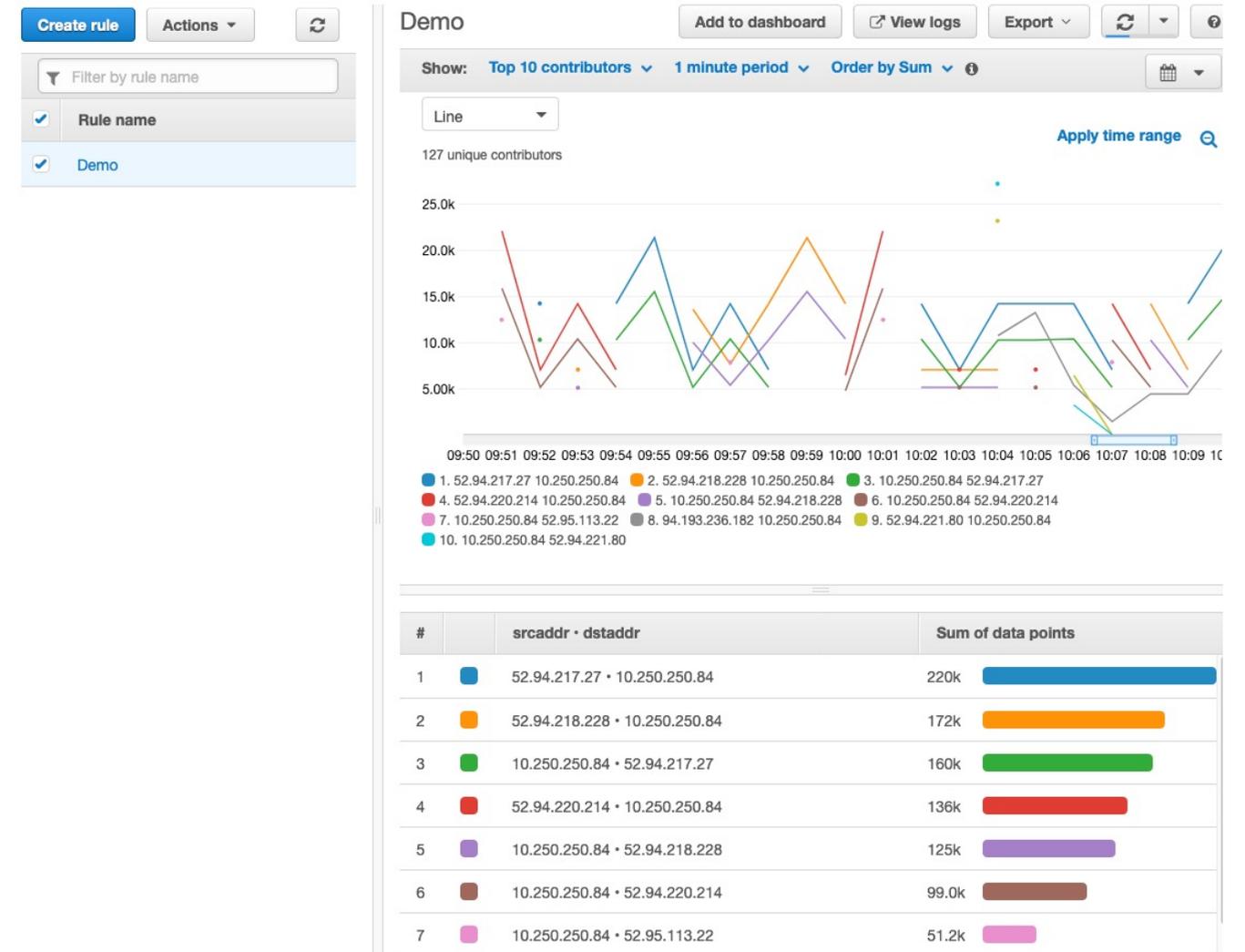
The screenshot displays the AWS CloudWatch Logs Insights interface. At the top, the breadcrumb navigation shows 'CloudWatch > CloudWatch Logs > Logs Insights' with a link to 'Switch to the original interface.' Below this, there's a search bar for 'Select log group(s)' with a dropdown arrow, and a time range selector set to '1h' (with options for 30m, 3h, 12h, and custom). A 'Clear' button is next to the search bar. The selected log group is 'centralized-logging-DemoStack-Q6HKGK505VPPF-VPCFlowLogGroup-4LIBSBHKZD35'. The query entered is 'stats avg(bytes), min(bytes), max(bytes) by srcAddr, dstAddr'. Below the query bar are 'Run query' and 'History' buttons. The interface is split into 'Logs' and 'Visualization' tabs. The 'Visualization' tab is active, showing a histogram of the query results. The histogram title is '614 records matched | 653 records (93.1 kB) scanned in 3.6s @ 183 records/s (26.2 kB/s)'. The x-axis represents time from 08:25 to 09:25, and the y-axis represents the number of records (0 to 15). Below the histogram is a table with 10 rows of results. The table has columns for '#', 'srcAddr', 'dstAddr', 'avg(bytes)', 'min(bytes)', and 'max(bytes)'. Each row is preceded by a magnifying glass icon.

#	srcAddr	dstAddr	avg(bytes)	min(bytes)	max(bytes)
1	39.72.78.144	10.250.250.84	40	40	40
2	52.94.218.228	10.250.250.84	6690.0156	599	7190
3	10.250.250.84	52.94.218.228	4860.1094	293	5267
4	52.94.220.214	10.250.250.84	6635	639	7150
5	27.64.163.168	10.250.250.84	44	44	44
6	10.250.250.84	162.159.200.1	76	76	76
7	10.250.250.84	52.94.220.214	4822.9286	333	5227
8	27.74.122.122	10.250.250.84	84	84	84
9	185.176.27.34	10.250.250.84	40	40	40
10	52.94.217.30	10.250.250.84	6739.2222	6589	7013

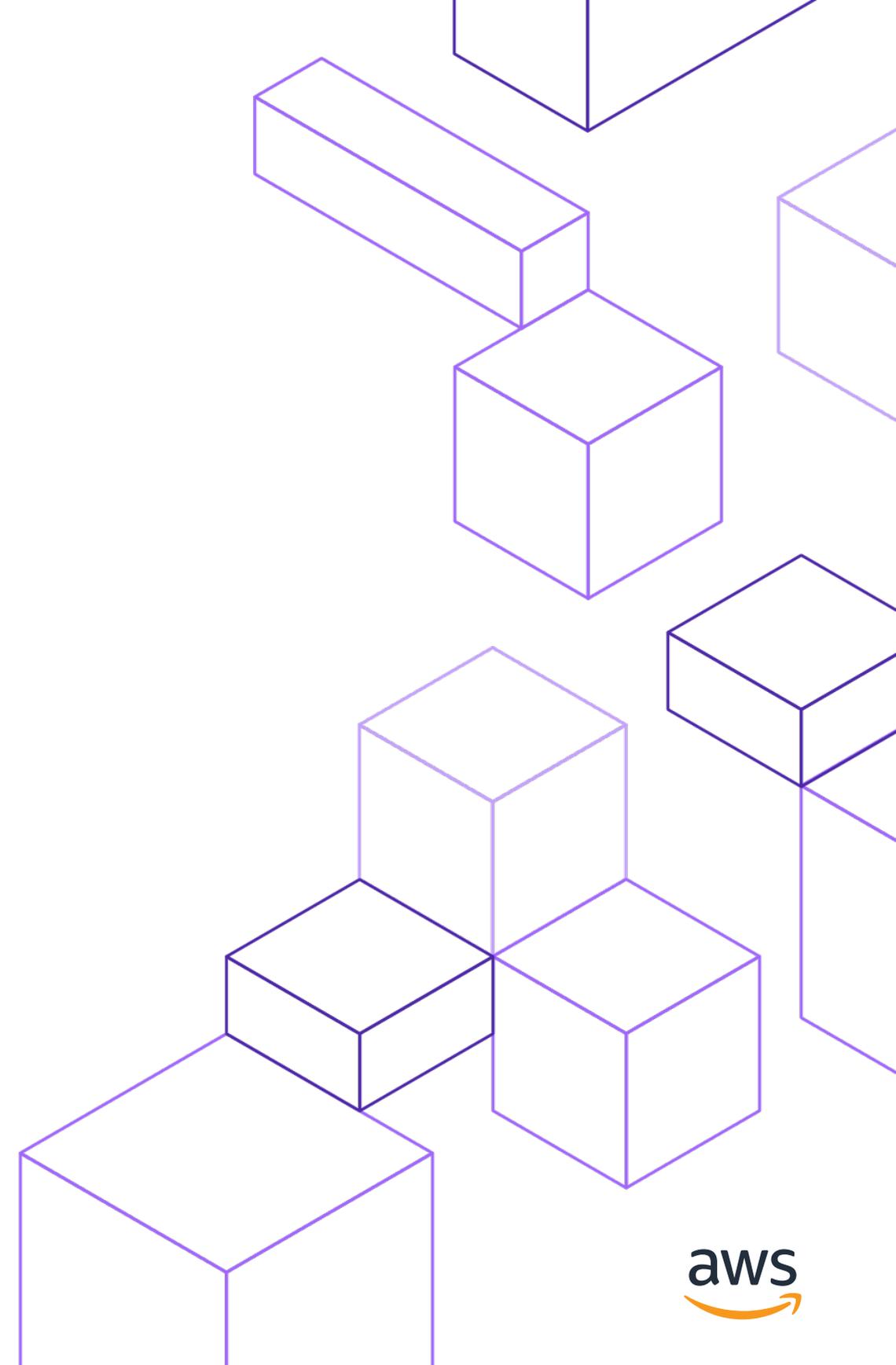
Contributor Insights

Analyzes time-series data to provide a view of the top contributors influencing system performance.

- Runs continuously without needing user intervention
- Understand who or what is impacting your system
- Evaluate patterns in structured log events
- Display on CloudWatch dashboards
- Add to CloudWatch alarms



Q&A





Thank You!

