Amazon CloudWatch

Amazon CloudWatch is a monitoring and management service designed to provide data and actionable insights for AWS, hybrid, and on-premises applications and infrastructure resources. With CloudWatch, you can collect and access your performance and operational data in the form of logs and metrics from a single platform. This helps you to address the challenge of monitoring individual systems and applications in silos (server, network, database, etc.). CloudWatch helps you to monitor your stack (applications, infrastructure, and services) and leverage alarms, logs, and events data to take actions and reduce Mean Time to Resolution (MTTR). This frees up important resources and allows you to focus on building applications and business value.

CloudWatch is designed to give you actionable insights that help you optimize application performance, manage resource utilization, and understand system-wide operational health. CloudWatch provides visibility of metrics and logs data, data retention (metrics), and the ability to perform calculations on metrics. This allows you to perform historical analysis for cost optimization and derive real-time insights into optimizing applications and infrastructure resources.

You can use CloudWatch Container Insights to monitor, troubleshoot, and alarm on your containerized applications and microservices. You can collect, aggregate, and summarize compute utilization information like CPU, memory, disk, and network data, as well as diagnostic information like container restart failures, to help DevOps engineers isolate issues and resolve them. Container Insights gives you insights from container management services such as Amazon ECS for Kubernetes (Amazon EKS), Amazon's Elastic Container Service (Amazon ECS), AWS Fargate, and standalone Kubernetes (k8s).

Collect

Collect and store logs

The Amazon CloudWatch Logs service helps you to collect and store logs from your resources, applications, and services. There are three main categories of logs 1) Vended logs. These are natively published by AWS services on behalf of the customer. 2) Logs that are published by AWS services. Currently over 30 AWS services publish logs to CloudWatch. 3) Custom logs. These are logs from your own application and on-premises resources.

Built-in metrics

Collecting metrics from distributed applications (such as those built using microservices architectures) 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, and Amazon API Gateway, without any action on your part.

Custom Metrics

Amazon CloudWatch helps you to collect custom metrics from your own applications to help you 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. You can use CloudWatch Agent or the PutMetricData API action to publish these metrics to CloudWatch.

Collect and aggregate container metrics and logs

Container Insights is designed to simplify the collection and aggregation of curated metrics and container ecosystem logs. With it, you can collect compute performance metrics such as CPU, memory, network, and disk information from each container as performance events and generate custom metrics used for monitoring and alarming. The performance events are ingested as

CloudWatch Logs with metadata about the running environment such as the Amazon EC2 instance ID, Service, Amazon EBS volume mount and ID, etc., to assist in monitoring and troubleshooting. CloudWatch custom metrics can be extracted from these ingested logs and further analyzed using CloudWatch Logs Insights' advanced query language. Container Insights also provides an option to collect application logs (stdout/stderr), custom logs, predefined Amazon EC2 instance logs, Amazon EKS/k8s data plane logs and Amazon EKS control plane logs.

Collect and aggregate Lambda metrics and logs

CloudWatch Lambda Insights helps with the collection and aggregation of curated metrics and logs from AWS Lambda functions. You can collect compute performance metrics such as CPU, memory, and network from each Lambda function as performance events, while generating custom metrics used for monitoring and alarming. The performance events are ingested as CloudWatch logs to simplify monitoring and troubleshooting. CloudWatch custom metrics can be extracted from these ingested logs and further analyzed using CloudWatch Logs Insights' advanced query language.

Stream Metrics

Amazon CloudWatch Metric Streams helps you to create continuous streams of metrics to a destination of your choice. Metrics Streams makes it easier to send CloudWatch metrics to popular third-party service providers using an Amazon Kinesis Data Firehose HTTP endpoint. You can also direct your metrics to your data lake on AWS.

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. You can graph metrics and logs data side by side in a single dashboard to quickly get the context and go from diagnosing the problem to understanding the root cause. For example, you can visualize key metrics, like CPU utilization and memory, and compare them to capacity. You can also correlate the log pattern of a specific metric and set alarms to be proactively alerted about performance and operational issues. This is designed to give you system-wide visibility into operational health and the ability to troubleshoot issues, reducing Mean Time to Resolution (MTTR).

Composite alarms

Amazon CloudWatch composite alarms allow you to combine multiple alarms and reduce alarm noise. If an application issue affects several resources in an application, you can set up receipt of a single alarm notification for the entire application instead of one for each affected service component or resource. This helps you stay focused on finding the root cause of potential operational issues to reduce application downtime. You can also provide an overall state for a grouping of resources like an application, AWS Region, or Availability Zone.

High resolution alarms

Amazon CloudWatch alarms helps you to set a threshold on metrics and trigger an action. You can create high-resolution alarms, set a percentile as the statistic, and choose to specify an action or ignore one as you deem appropriate.

Logs and metrics correlation

Applications and infrastructure resources generate lots of operational and monitoring data in form of logs and metrics. In addition to providing you the ability to access and visualize these data sets in a single platform, Amazon CloudWatch can also correlate metrics and logs. This helps

you diagnose potential problems and assist in understanding the root cause. For example, you can correlate a log pattern, such as an error to a specific metric, and set alarms to be actively alerted of performance and operational issues.

Application Insights

Amazon CloudWatch Application Insights provides setup of observability for your enterprise applications, to assist you in gaining visibility into the health of such applications. It can help identify, and you can set up, key metrics and logs across your application resources and technology stack i.e. database, web (IIS) and application servers, Operating System, load balancers, queues, etc. You can continuously monitor these telemetry data to detect and correlate anomalies and errors, to notify you of any problems in your application. Designed to aid in troubleshooting, Application Insights creates dashboards for the detected problems with correlated metric anomalies and log errors, along with additional insights to assist you in determining their potential root-cause. This helps you to take quick remedial actions to manage the health of your applications and assess impact on end-users.

Container monitoring insights

Container Insights provides dashboards in the CloudWatch console. These dashboards summarize the compute performance, errors, and alarms by cluster, pod/task, and service. Each dashboard summarizes the list of running pods/tasks or containers by CPU and memory for the selected time window, and allows you to contextually - based on time window and selected pod/task or container - dive deeper into application logs, AWS X-Ray traces, and performance events.

Lambda monitoring insights

Lambda Insights provides dashboards in the CloudWatch console. These dashboards summarize the compute performance and errors. Each dashboard includes the list of metrics for the selected time window and allows you to contextually dive deeper — based on time window and selected function — into application logs, AWS X-Ray traces, and performance events.

Anomaly Detection

Amazon CloudWatch Anomaly Detection applies machine-learning algorithms designed to assist you to continuously analyze data of a metric and identify anomalous behavior. You can create alarms that auto-adjust thresholds based on natural metric patterns. You can also visualize metrics with anomaly detection bands on dashboards. This helps you to monitor, isolate, and troubleshoot unexpected changes in your metrics.

ServiceLens

You can use Amazon CloudWatch ServiceLens to help you visualize and analyze the health, performance, and availability of your applications in a single place. CloudWatch ServiceLens ties together CloudWatch metrics and logs as well as traces from AWS X-Ray to help you obtain a complete view of your applications and their dependencies. This can assist you in pinpointing performance bottlenecks, isolating root causes of application issues, and determining users potentially impacted. CloudWatch ServiceLens is designed to allow visibility into your applications in three main areas: Infrastructure monitoring (using metrics and logs to understand the resources supporting your applications), transaction monitoring (using traces to understand dependencies between your resources), and end user monitoring (using canaries to monitor your endpoints and notify you when your end user experience has degraded). CloudWatch ServiceLens provides a Service Map that visualizes the contextual linking of your resources, along with an intuitive interface to assist you to dive deep into correlated monitoring data.

Synthetics

Amazon CloudWatch Synthetics helps you to monitor application endpoints. You can run tests on your endpoints and receive alerts if your application endpoints don’t behave as expected. These tests can be customized to check for availability, latency, transactions, broken or dead links, step by step task completions, page load errors, load latencies for UI assets, complex wizard flows, or checkout flows in your applications. You can also use CloudWatch Synthetics to isolate alarming application endpoints and map them back to underlying infrastructure issues to reduce mean time to resolution. With this new feature, CloudWatch can now collect canary traffic, which can assist you in verifying your customer experience enabling you to discover issues. CloudWatch Synthetics supports monitoring of your REST APIs, URLs, and website content, checking for unauthorized changes from phishing, code injection and cross-site scripting.

RUM

Amazon CloudWatch RUM is designed to give you visibility into your applications’ client-side performance and reduce MTTR. It is designed to allow you to collect client-side data on web application performance in near real time to identify and debug issues. CloudWatch RUM complements the CloudWatch Synthetics data to give you more visibility into your end-user experience. You can visualize anomalies in performance and use the relevant debugging data (such as error messages, stack traces, and user sessions) to fix performance issues (such as JavaScript errors, crashes, and latencies). You can gain insight into the range of end-user impacts, including number of users, geolocations, and browsers. CloudWatch RUM is designed to aggregate data on your users' journey through your application, which can help you determine which features to launch and bug fixes to prioritize.

Act

Auto Scaling

Auto Scaling helps you automate capacity and resource planning. You can set a threshold to alarm on a key metric and trigger an Auto Scaling action. For example, you could set up an Auto Scaling workflow to add or remove EC2 instances based on CPU utilization metrics and optimize resource costs.

Respond to operational changes with CloudWatch Events

CloudWatch Events is designed to provide a near real-time stream of system events that describe changes to your AWS resources. It helps you to respond quickly to operational changes and take corrective action. You can write rules to indicate which events are of interest to your application and what actions to take when a rule matches an event.

Alarm and take action on EKS, ECS, and k8s clusters

For Amazon EKS and k8s clusters, CloudWatch Container Insights helps 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.

Analyze

Granular data and extended retention

Amazon CloudWatch helps you to monitor trends and seasonality with months of metric data (storage and retention). This data allows you to perform historical analysis to fine-tune resource utilization. With CloudWatch, you can also collect health metrics including custom ones, such as those coming from your on-premises applications. Granular real-time data enables better visualization and ability to spot and monitor trends to optimize application performance and operational health.

Custom operations on metrics

Amazon CloudWatch Metric Math helps you to perform calculations across multiple metrics for real-time analysis so you can derive insights from your existing CloudWatch metrics. You can visualize these computed metrics in the AWS Management Console, add them to CloudWatch dashboards, or 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.

Log analytics

Amazon CloudWatch Logs Insights allows 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, and export query results to CloudWatch Dashboards. This is designed to give you operational visibility. With a few clicks in the AWS Management Console, you can start using Logs Insights to query logs sent to CloudWatch.

Analyze container metrics, logs, and traces

Container Insights simplifies the analysis of observable data from metrics, logs, and traces by simplifying deep linking from automatic dashboards to granular performance events, application logs (stdout/stderr), custom logs, predefined Amazon EC2 instance logs, Amazon EKS/k8s data plane logs and Amazon EKS control plane logs using CloudWatch Logs Insights' advance query language.

Analyze Lambda metrics, logs, and traces

Lambda Insights simplifies the analysis of observable data from metrics, logs, and traces by simplifying deep linking from automatic dashboards to granular performance events, application logs, and custom logs, using CloudWatch Logs Insights' advanced query language.

Contributor Insights

Amazon CloudWatch now includes Contributor Insights, which analyzes time-series data to provide a view of the top contributors influencing system performance. Once set up, Contributor Insights is designed to run continuously without needing additional user intervention. This is designed to help developers and operators more quickly isolate, diagnose, and remediate issues during an operational event. Contributor Insights helps you understand who or what is impacting your system and application performance, such as a specific resource, customer account, or API call. This enables you to pinpoint outliers, find the heaviest traffic patterns, and rank the most utilized system processes. You can create Contributor Insights rules to evaluate patterns in structured log events as they are sent to CloudWatch Logs, including logs from AWS services like AWS CloudTrail, Amazon Virtual Private Cloud, Amazon API Gateway, and any custom logs sent by your service or on-premises servers, such as Apache access logs. Contributor Insights is designed to evaluate these log events in real-time and display reports that show the top contributors and number of unique contributors in a dataset. A contributor is an aggregate metric based on dimensions contained as log fields in CloudWatch Logs, such as account-id or interface-id in VPC Flow Logs, or any other custom set of dimensions. You can sort and filter contributor data based on your own custom criteria. Contributor Insights report data can be displayed on CloudWatch dashboards, graphed alongside CloudWatch metrics, and added to CloudWatch alarms.

Metrics Insights (Preview)

Amazon CloudWatch Metrics Insights (Preview) is designed to bed a fast, flexible, SQL-based query engine that enables you to identify trends and patterns within millions of operational metrics in near real time. Metrics Insights allows you to gain better visibility on your infrastructure and large-scale application performance with flexible querying and on-the-fly metric

aggregations. Metrics Insights queries can be used to create powerful visualizations, helping you proactively monitor and pinpoint issues quickly, and reduce MTTR.

Evidently

Amazon CloudWatch Evidently lets application developers conduct experiments and identify unintended consequences of new features before rolling them out for general use. Evidently allows you to validate new features across the full application stack before release, which makes for a safer release. When launching new features, you can expose them to a small user base, monitor key metrics such as page load times or conversions, and then dial up traffic. Evidently also allows you to try different designs, collect user data, and release the most effective design in production.

Compliance and Security

Amazon CloudWatch is integrated with AWS Identity and Access Management (IAM) designed to help you configure which users and resources have permission to access your data and how they can access it.

Data is encrypted at rest and during transfer. You can also use AWS KMS encryption to encrypt your log groups for added compliance and security.

Additional Information

For additional information about service controls, security features and functionalities, including, as applicable, information about storing, retrieving, modifying, restricting, and deleting data, please see https://docs.aws.amazon.com/index.html. This additional information does not form part of the Documentation for purposes of the AWS Customer Agreement available at http://aws.amazon.com/agreement, or other agreement between you and AWS governing your use of AWS's services.