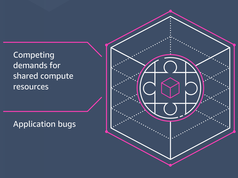
Monitor, Troubleshoot, and Optimize Your Containerized Applications

Your monitoring and operational goals depend on quickly finding and fixing issues with your applications. With Amazon CloudWatch Container Insights and Anomaly Detection, you can proactively monitor your containerized applications, troubleshoot faster, and increase development velocity.

Monitor the health and performance of your containerized applications

Operational challenges with containers

Hurts customer trust, impacts SLAs, and incurs $ risk



- Competing demands for shared compute resources
- Application bugs
- Collecting data from short-lived, continuously-deployed containers
- Over/under-provisioned resources

Here's how to get started

CloudWatch Container Insights improves visibility into your containers on Amazon ECS, EKS, AWS Fargate, and Kubernetes

CloudWatch Anomaly Detection applies machine learning to isolate and identify unusual behavior

Target outcomes

1. Maximize performance
2. Increase operational efficiency
3. Troubleshoot and debug with confidence
4. Increase developer productivity

With visibility into Blue/Green deployments, rolling updates, and canary releases

Collect Logs and Metrics

Container Insights collects logs and metrics from your containerized applications and microservices

Custom metrics at task/pod, service, cluster, host, and namespace levels

Custom logs from applications, hosts, data planes, and control planes

Monitor with Dashboards

Use automatic dashboards to view aggregated logs and metrics, and custom dashboards to visually correlate them across AWS services

With Anomaly Detection

Identify when containers are using abnormal amounts of compute resources

Observe spikes in CPU utilization and network traffic

With Container Insights

Isolate and analyze what's depleting resources

Quickly find and identify if issues are systemic or isolated

Analyze and Correlate Metrics, Logs, and Traces

Dive deep into container health and performance to understand changes in your environment and problem failures, then debug distributed applications

Analyze **CloudWatch metrics** using

CloudWatch console

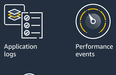
APIs and SDKs, e.g., GetMetricData

Custom and automated dashboards

CloudWatch does more

CloudWatch provides visibility into the performance of multiple AWS services such as Amazon EC2, DynamoDB, S3, ECS, EKS, and AWS Lambda

With CloudWatch Logs Insights, query



Application logs

Performance events

Host logs

Data plane logs

Control plane logs

CloudWatch events

With AWS X-Ray

Discover dependencies between services and components

Troubleshoot issues no matter where code is running

Identify root cause of bottlenecks and errors

Understand which users are impacted and by how much

Alarm and Remediate

Set alarms and automate actions based on static thresholds. You can also create alarms using machine learning algorithms that identify anomalous behavior in your metrics.

Automated Actions

You can remediate with automatically triggered actions like Amazon EC2 auto scaling, or stopping or restarting an instance

CloudWatch Events

Set up rules based on key events occurring in other services, such as AWS Lambda, Amazon SNS, and AWS CloudFormation

CloudWatch Alarms

You can create an alarm that monitors a metric or a metric math expression

With Anomaly Detection, create alarms to monitor your metrics and compare actual metric values with the expected behavior predicted by machine learning models.

Amazon CloudWatch provides monitoring and observability of AWS resources, applications, and services that run on AWS and your on-premises servers.

Learn more at aws.amazon.com/cloudwatch