AWS Decision Guide

Choosing an AWS monitoring and observability service

Choosing an AWS monitoring and observability service: AWS Decision Guide

Table of Contents

Choosing an AWS monitoring and observability service

Taking the first step

Purpose	Help determine which AWS monitoring and observability services are the best fit for your organization.
Last updated	January 12, 2024
Covered services	• AWS CloudTrail • Amazon CloudWatch • Amazon CloudWatch Application Signals • AWS Config • AWS Control Tower • Amazon Managed Grafana • Amazon Managed Service for Prometheus • Amazon OpenSearch Service • AWS Distro for OpenTelemetry • AWS X-Ray

Introduction

Monitoring and observability are critical components for ensuring the availability, performance, reliability, and security of your cloud-based workloads and data.

- Monitoring involves the systematic collection and analysis of data, such as metrics, logs, and traces, to track the health and efficiency of cloud resources as well as supporting reactive incident management.
- Observability focuses on understanding the internal state of a system through dynamic, real-time insights, allowing for proactive issue identification and resolution.

AWS offers a range of tools and services for both monitoring and observability. They can be used to collect data, analyze metrics, and create alarms to notify you of issues. In addition, they can provide logs and metrics that you can use to identify and troubleshoot the root cause of problems.

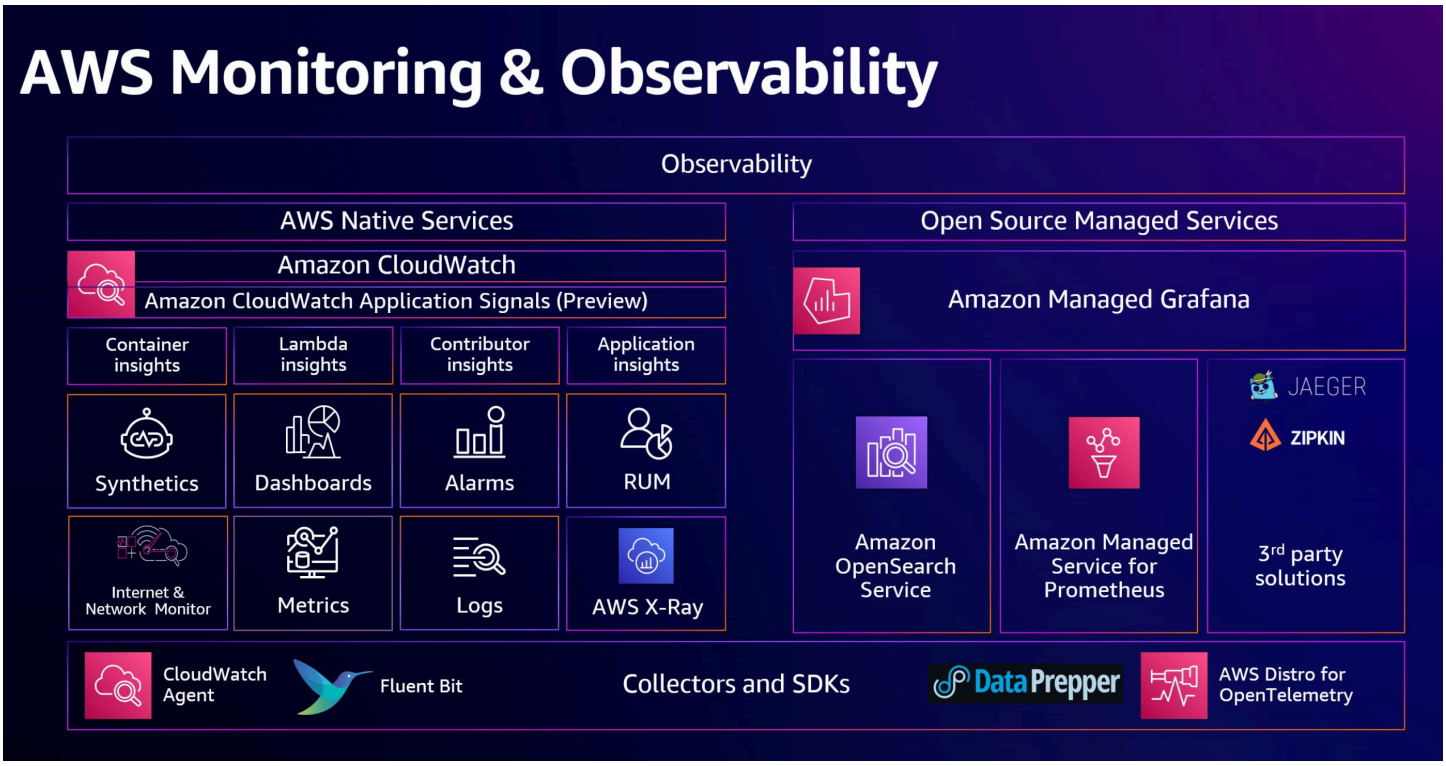
These services integrate with more than 120 other AWS services (including Amazon EC2, Amazon EKS, Amazon ECS, Lambda, and Amazon S3) and partners, and integrates with a wide range of third-party observability and cloud management tools that use near real-time feeds of AWS-native telemetry.

This guide will help you select the AWS monitoring and observability services and tools that are the best fit for your needs and your organization.

In this four minute clip from his re:Invent 2023 presentation, senior AWS worldwide specialist Toshal Dudhwala outlines how to build an observability strategy.

Understand

To choose the right AWS monitoring and observability tools for your needs, it may help to first understand the range of options available to you and how the main services fit together.



Start with your three key data sources: logs, metrics, and traces. The data from those sources can be consumed using Amazon CloudWatch, AWS X-Ray, or AWS Distro for OpenTelemetry (ADOT) agents.

Here's when you might use each of these data collection sources:

- Use Amazon CloudWatch to collect custom metrics from your own applications to monitor operational performance, troubleshoot issues, and spot trends. You can also use the CloudWatch agent for collecting log, metrics and traces.. In addition, you can use open source tools such as Fluent D or FluentBit to collect logs and send them to CloudWatch logs.
- Use AWS X-Ray to perform distributed tracing across multiple applications and systems to help find latency in a system and target it for improvement. You can use the CloudWatch agent to collect traces and send them to X-Ray.
- Use AWS Distro for OpenTelemetry to collect metrics and traces.

Instrumentation

There are two major categories of instrumentation available within AWS monitoring and observability services: AWS Native Services and Open Source Managed Services.

- AWS Native Services include Amazon CloudWatch and AWS X-Ray. CloudWatch offers these key features of Container Insights, Lambda Insights, Contributor Insights, and Application Insights, that contribute to how you contextualize your data for insights and analysis.
- Open Source Managed Services include Amazon Managed Service for Prometheus (a managed monitoring service based on and compatible with the popular Prometheus open source monitoring and alerting solution), Amazon OpenSearch Service, and AWS Distro for OpenTelemetry (which not only supports AWS X-Ray, but also Jaeger and Zipkin Tracing).

Visualization and analysis

The data you collect and ingest with these AWS services can be visualized and analysed using the Amazon CloudWatch Service Map, the AWS X-Ray trace map, Amazon Managed Grafana and Amazon CloudWatch Logs Insights.

Other services

Other services important to monitoring and observability include:

- AWS Config provides a detailed view of your resource configurations in your AWS account. This view includes the relationship between your resources and the past configurations of your resources, so you can see how the relationships and configurations of your resources change over time. If you are using AWS Config rules, AWS Config evaluates your resource configurations for desired settings.
- AWS CloudTrail helps you enable operational and risk auditing, governance, and compliance by recording events of actions taken by users, roles or AWS services. Actions taken by a user, role, or an AWS service are recorded as events in CloudTrail. Events include actions taken in the AWS Management Console, AWS Command Line Interface, and AWS SDKs and APIs.

In addition, you can select from a range of machine learning and analytics services to gain further benefit from your monitoring and observability data.

Consider

Choosing the right monitoring and observability services on AWS depends on your specific requirements and use cases. Here are some criteria to consider when making your decision.

Monitoring service capabilities

Consider whether the service provides a comprehensive set of tools that encompass metrics, logs, and traces. Metrics offer quantitative data on system performance, logs provide detailed event information, and traces allow you to follow transactions across your infrastructure.

Also assess whether the service supports diverse data types and formats. Additionally, look for advanced features such as anomaly detection, machine learning-driven insights, and the ability to correlate data from different sources. A well-rounded solution should enable holistic visibility into your AWS environment, aiding in efficient troubleshooting, performance optimization, and proactive problem resolution.

The more versatile and integrated the service capabilities, the better equipped you are to gain deep insights into your applications and infrastructure. Review the AWS Observability section of the Management and Governance Cloud Environment Guide (part of the AWS Well-Architected Framework) for more details on service capabilities.

Ease of integration

Assess how seamlessly the service integrates with your existing AWS infrastructure, applications, and deployment processes.

Look for compatibility with popular programming languages, frameworks, and third-party tools that your organization uses. Also evaluate the availability of SDKs, APIs, and plugins that simplify the integration process. Better integration can facilitate the collection and analysis of data without imposing significant overhead on your applications.

Additionally, consider whether the service supports common protocols for data ingestion. Services that provide better integration can help ensure a smoother onboarding experience, allowing your team to more quickly start monitoring and gaining valuable insights into your AWS environment.

Data retention and storage

Data retention and storage capabilities are pivotal considerations in selecting AWS monitoring and observability services. For any service you are considering, examine policies on storing and retaining historical data, as well as scalability to handle increasing data volumes over time.

Assess whether the service supports long-term storage of metrics, logs, and traces, enabling you to perform retrospective analysis and meet compliance requirements. Consider also the ease with which you can access and retrieve archived data.

The service (or services) you use should achieve a balance between providing sufficient retention periods for meaningful trend analysis and managing storage costs effectively. A clear understanding of data retention and storage policies is important when considering how your monitoring setup aligns with both operational needs and regulatory obligations.

Scalability

Evaluate how well the service can scale alongside your evolving infrastructure and growing workloads. A scalable solution should seamlessly handle increases in data volume, user activity, and the complexity of your applications.

Consider the elasticity of the service, its ability to accommodate spikes in demand, and whether it supports auto-scaling features to adapt to changing requirements dynamically. Robust scalability helps ensure that your monitoring system remains responsive and effective, providing timely insights even as your AWS environment expands.

By choosing a service with strong scalability, you can confidently support the continuous growth of your applications and infrastructure without compromising on performance or incurring unnecessary operational challenges.

Alerting and notification

Assess the alerting capabilities of the service, including the ability to set up alerts based on predefined thresholds, anomalies, or specific events. Look for flexibility in configuring alert conditions and the ease of managing notification channels such as email, SMS, or integrations with collaboration tools.

The service (or services) you choose should provide timely and actionable alerts, enabling your team to respond promptly to potential issues. Consider features such as escalation policies and the ability to acknowledge or suppress alerts.

Integration with popular incident management platforms can enhance the overall incident response workflow. Prioritize a monitoring service that empowers your team to proactively address issues, minimizing downtime and ensuring the continuous health of your AWS environment.

Cost

Understand the pricing model of each service, considering factors such as data volume, storage, and any additional features. Review cost information for any service you are considering (such as this billing and cost summary for Amazon CloudWatch).

Evaluate whether the pricing structure aligns with your budget and usage patterns. Some services may offer a pay-as-you-go model, while others may have tiered pricing or subscription plans. Consider the potential impact of all costs – including data transfer fees or charges for accessing historical data.

Additionally, assess whether the pricing scales efficiently with the growth of your infrastructure. A clear understanding of costs ensures that your monitoring solution remains cost-effective without compromising on essential features, allowing you to optimize your budget while meeting your operational requirements on AWS.

Customization and extensibility

Assess whether the service allows you to tailor dashboards, reports, and alerts to meet your needs. Look for the flexibility to create custom metrics, queries, and visualizations. Integration with third-party tools and support for common APIs enhance the service's extensibility. Evaluate whether the monitoring solution can adapt to the unique needs of your applications and infrastructure.

A highly customizable and extensible service empowers your team to fine-tune monitoring parameters, adapt to evolving use cases, and integrate seamlessly with your existing workflows

and tools. Prioritize solutions that provide a high degree of configurability, allowing you to optimize monitoring for your specific AWS environment and operational preferences.

Security and compliance

Evaluate how a service provides adherence to AWS security best practices, ensuring data confidentiality, integrity, and availability. Check for features such as encryption in transit and at rest, access controls, and secure authentication mechanisms. Assess whether the service supports compliance with relevant regulations and standards applicable to your industry.

Look for audit trail capabilities and the ability to generate compliance reports. The goal is to help safeguard sensitive data by using monitoring practices to align with regulatory requirements.

Prioritize services that provide a robust security posture, enabling your organization to maintain a secure and compliant AWS environment while gaining insights into your applications and infrastructure.

Machine learning and analytics

Evaluate whether the service uses machine learning (ML) to provide advanced insights, anomaly detection, and predictive analytics. Look for features that automatically identify patterns, trends, and potential issues within your data.

A robust machine learning component can enhance the accuracy of anomaly detection, reducing false positives and improving the overall effectiveness of your monitoring system. Additionally, consider the depth of analytics provided, such as root cause analysis and trend forecasting. A service with strong machine learning and analytics capabilities empowers your team to proactively address issues, optimize performance, and gain deeper insights into the behavior of your AWS applications and infrastructure.

Global reach

Global reach is a critical criterion for AWS monitoring and observability services, particularly if your infrastructure is distributed across multiple Regions. Assess whether the monitoring service provides visibility into the performance and health of your resources across different AWS Regions.

Consider the ability to aggregate and analyze data from diverse geographical locations, ensuring a comprehensive understanding of your global infrastructure. Look for features that support centralized management and monitoring, allowing you to efficiently oversee operations on a global scale.

A service with strong global reach helps ensure that you can maintain consistent monitoring practices, troubleshoot issues, and optimize performance seamlessly across the entire spectrum of your AWS deployment, irrespective of geographical boundaries. This capability is particularly valuable for organizations with a geographically distributed or multi-cloud infrastructure.

Choose

Now that you know the criteria by which you will be evaluating your monitoring and observability options, you are ready to choose which AWS monitoring and observability services might be a good fit for your organizational requirements.

The following table highlights which services are optimized for which circumstances. Use the table to help determine the service that is the best fit for your organization and use case.

Use case	What is it optimized for?	Monitoring and observability services
Monitoring and alerting	These services are optimized to provide real-time visibility, proactive issue detection, resource optimization, and efficient incident response, contributing to overall application and infrastructure health.	Amazon CloudWatch Amazon CloudWatch Logs Amazon EventBridge
Application performance monitoring	These services provide comprehensive insights into application behavior, offer tools for identifying and resolving performance bottlenecks, aid in efficient troubleshooting, and contribute to delivering modern user experiences across distributed and web applications.	Amazon CloudWatch Application Signals Amazon Managed Service for Prometheus AWS X-Ray Amazon CloudWatch Synthetics

Use case	What is it optimized for?	Monitoring and observability services
Infrastructure observability	These services provide a holistic view of your cloud resources, helping you make more informed decisions about resource utilization, performance optimization, and cost-efficiency.	Amazon CloudWatch Metrics Amazon CloudWatch Container Insights
Logging and analysis	These services help you efficiently manage and analyze log data, troublesh oot, detect anomalies, support security, meeting compliance requirements, and get actionable insights into your applications and infrastructure.	Amazon Cloudwatch Logs Insights Amazon CloudWatch Logs Anomaly Detection Amazon Managed Grafana Amazon OpenSearch Service Amazon Kinesis Data Streams
Security and compliance monitoring	Optimized to provide a robust security framework, enabling proactive threat detection , continuous monitoring, compliance tracking, and audit capabilities to help safeguard your AWS resources and maintain a secure and compliant environment.	Amazon GuardDuty AWS Config AWS CloudTrail

Use case	What is it optimized for?	Monitoring and observability services
Network monitoring	These services provide visibility into network traffic, enhance security by detecting and preventing threats, enable efficient network traffic management, and support incident response activities.	Amazon CloudWatch Network Monitor Amazon CloudWatch Internet Monitor Amazon VPC Flow Logs AWS Network Firewall
Distributed tracing	These services provide a comprehensive view of the interactions and dependencies within your distributed applications. They enable you to diagnose performance bottlenecks, optimize application performance, and support the smooth functioning of complex systems by offering insights into how different parts of your application communicate and interact.	AWS Distro for OpenTelemetry AWS X-Ray Amazon CloudWatch Application Signals (Preview)
Hybrid and multicloud observability	Maintain reliable operations, provide modern digital experiences for your customers, and get help to meet service level objectives and performance commitments.	Amazon CloudWatch (hybrid and multicloud support)

Use

You should now have a clear understanding of what each AWS monitoring and observability service (and the supporting AWS tools and services) does, and which might be right for you.

To explore how to use and learn more about each of the available AWS observability services, we have provided a pathway to explore how each of the services work. The following section provides links to in-depth documentation, hands-on tutorials, and resources to get you started.

Amazon CloudWatch

Getting Started with Amazon CloudWatch

Monitor your AWS resources and the applications you run on AWS in real time using Amazon CloudWatch. You can use CloudWatch to collect and track metrics, which are variables you can measure for your resources and applications.

Explore the guide

Getting started with Amazon CloudWatch Metrics

This guide discusses basic monitoring and detailed monitoring, how to graph metrics, and how to use CloudWatch anomaly detection.

Explore the guide

Set up Container Insights on Amazon EKS and Kubernetes

Set up the Amazon CloudWatch Observabi lity ESK add-on and ADTO on your EKS cluster to send metrics to CloudWatch. You will also learn how to set up Fluent Bit or Fluentd to send logs to CloudWatch Logs.

Explore the guide

Getting started with Amazon CloudWatch Application Insights

Learn how to use the console to enable CloudWatch Application Insights to manage your applications for monitoring.

Explore the guide

Using Container Insights

Learn how CloudWatch Container Insights collects, aggregates, and summarizes metrics and logs from your containerized applicati ons and microservices.

Explore the guide

Setting up Container Insights on Amazon ECS

Learn to configure cluster and service level metrics, deploy ADOT to collect EC2 instance level metrics, and set up FireLens to send logs to CloudWatch Logs.

Explore the guide

Amazon CloudWatch Application Insights

Getting started with Amazon CloudWatch Application Signals

In this guide, you will learn how to automatic ally instrument your applications on AWS so that you can monitor current applicati on health and track long-term application performance against your business objective s.

Explore the guide

Amazon CloudWatch Application Signals for automatic instrumentation of your applications

This blog post provides an in-depth walk-through the AWS Management Console for Amazon CloudWatch Application Signals demonstrating how to collect telemetry for your EKS clusters.

Read the blog post

How to monitor application health using SLOs with Amazon CloudWatch Application Signals

This blog post demonstrates how Amazon CloudWatch Application signals enables you to automatically instrument and operate applications on AWS to track application performance against your most important objectives.

Read the blog post

Amazon CloudWatch Lambda Insights

Introducing CloudWatch Lambda Insights

Learn how to create a few “Hello World” Lambda functions and monitor them using Lambda Insights. You will be using the AWS CDK to deploy the architecture.

Read the blog

Using Amazon CloudWatch Lambda Insights to Improve Operational Visibility

Learn how to use Lambda Insights to provide simple and convenient operation oversight and visibility into the behavior of your AWS Lambda functions.

Read the blog

Amazon CloudWatch Logs

Getting started with Amazon CloudWatch Logs

Learn how to install the unified CloudWatch agent and how to configure metrics collectio n with AWS CloudFormation.

Analyzing log data with CloudWatch Logs Insights

This guide will demonstrate to get started with Logs Insights queries, visualize log data

Read the guide

in in graphs, and adding queries to your dashboard.

Get started with the guide

Amazon CloudWatch Logs Insights – Fast, Interactive Log Analytics

Use Logs Insights to utilize the data points, patterns, trends, and insights present in all the various logs created by AWS services to understand how your applications and AWS resources are behaving, identify room for improvement, and address operational issues.

Read the blog post

Amazon CloudWatch Synthetics

Using synthetic monitoring

This guide demonstrates how to create canaries, configurable scripts that run on a schedule, providing sample code for canary scripts.

Explore the guide

Secure monitoring of user workflow experience using Amazon CloudWatch Synthetics and AWS Secrets Manager

How to create, deploy, and monitor synthetic monitoring solutions using Amazon CloudWatch Synthetics.

Read the blog post

Amazon EventBridge

Getting started with Amazon EventBridge

Learn to create a basic rule to route events to a target.

Explore the guide

Archive and replay Amazon EventBridge events

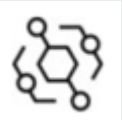
Create a function to use as the target for the EventBridge rule using the Lambda console.

Explore the guide

Log the state of an Amazon EC2 instance using EventBridge

Create an AWS Lambda function to log state changes for an Amazon EC2 instance. You will log the launch of any new EC2 instance.

Use the tutorial



Building an event-driven application with Amazon EventBridge

Learn how to build and deploy and event-driving application using the AWS Serverless Application Model (AWS SAM) CLI.

Read the blog

AWS CloudTrail

Getting started with AWS CloudTrail

AWS CloudTrail is an AWS service that helps you enable operational and risk auditing, governance, and compliance of your AWS account. Here's how to get started with it.

Review AWS account activity

Learn how to review the AWS API activity in your AWS account for services that support CloudTrail.

Explore the guide

Use the tutorial

Create a trail

Learn how to create a trail to log AWS API activity in all Regions including data and Insights events.

Use the tutorial

AWS CloudTrail Log Monitoring workshop

Learn how to integrate CloudTrail logs into CloudWatch and use features such as CloudWatch Log Insights, CloudWatch Metric Filters, CloudWatch Metric Alarms and CloudWatch Dashboards.

Use the workshop

AWS CloudTrail best practices

Best practices for using CloudTrail to enable auditing across your organization.

Read the blog

AWS Config

Getting started with AWS Config

AWS Config provides a detailed view of the configuration of AWS resources in your AWS account. This explains how to get started using it.

Setting up AWS Config (console)

Learn how to set up AWS Config in your AWS accounts using the AWS Management Console.

Explore the guide

Explore the guide

Setting up AWS Config with the AWS CLI

Learn how to set up AWS Config in your AWS accounts using the AWS CLI.

Explore the guide

Amazon Managed Grafana

Getting started with Amazon Managed Grafana

Learn how to get started with Amazon Managed Grafana and create your first workspace and then connect to the Grafana console in that workspace.

Explore the guide

Amazon Managed Grafana - Getting Started

Learn how to integrate with Amazon Managed Service for Prometheus and how to create custom dashboards.

Read the blog

Visualize and gain insights into your AWS cost and usage with Amazon Managed Grafana

Learn how to visualize and analyze your AWS cost and usage data with Amazon Managed Grafana.

Read the blog

Amazon Managed Service for Prometheus

Getting started with Amazon Managed Service for Prometheus

Create Amazon Managed Service for Prometheus workspaces, set up the ingestion of Prometheus metrics to those workspaces, and query those metrics.

Explore the guide

Container Insights Prometheus metrics monitoring

Learn how to automate the discovery of Prometheus metrics from containerized workloads using CloudWatch Container Insights.

Explore the guide

Amazon Managed Service for Prometheus FAQs

Frequently asked questions about Amazon Managed Service for Prometheus.

Read the FAQs

Amazon OpenSearch Service

Getting started with Amazon OpenSearch Service

Use Amazon OpenSearch Service to create and configure a test domain. An OpenSearch Service domain is synonymous with an OpenSearch cluster.

Explore the guide

Getting started with Amazon OpenSearch Serverless

This tutorial walks you through the basic steps to get an Amazon OpenSearch Serverless search collection up and running quickly

Use the tutorial

Creating and searching for documents in Amazon OpenSearch Service

Learn how to create and search for a document in Amazon OpenSearch Service.

Use the tutorial

Getting started with Amazon OpenSearch Ingestion

Learn how to use Amazon OpenSearch Ingestion to ingest data into a domain and also a collection.

Explore the guide

SIEM on Amazon OpenSearch Service Workshop

Build a security log analysis platform on Amazon OpenSearch Service and get started

Creating and searching for documents in Amazon OpenSearch Service

Learn how to create and search for a document in Amazon OpenSearch Service.

Use the tutorial

with building a cost-efficient solution for log ingestion, analysis and dashboarding.

Use the workshop

AWS Distro for OpenTelemetry

Getting Started with the AWS Distro for OpenTelemetry (ADOT) Collector

Walk through the steps to build the ADOT Collection locally.

Explore the guide

AWS Distro for OpenTelemetry JavaScript

Learn how to instrument your JavaScript applications and send correlated metrics to various AWS monitoring solutions.

Explore the guide

AWS Distro for OpenTelemetry Python

This guide will demonstrate how to instrument your Python applications and send correlated metrics to various AWS monitoring solutions.

Explore the guide

AWS X-Ray

Getting started with AWS X-Ray

One Observability Workshop

This guide will walk you through launching a sample application. Then you will learn how to instrument your application and explore other services that are integrated with X-Ray.

Explore the guide

This workshop provides you a hands-on experience with a wide variety of tool AWS offers for monitoring and observability including AWS X-Ray and ADOT.

Use the workshop

Application logging and monitoring using AWS X-Ray

Learn how AWS X-Ray collects data about requests that your application serves, and it helps you view, filter, and gain insights into that data to identify issues and opportuni ties for optimization.

Explore the guide

Explore

Solutions

Explore solutions to help you implement monitoring and observability on AWS.

Explore solutions

Whitepapers

Explore whitepapers to help you get started, learn best practices, and understan d your monitoring and observability options.

Explore whitepapers

Video, patterns, and guidance

Explore additional architect ural guidance covering common use cases for monitoring and observability services.

Explore additional assets

Document history

The following table describes the important changes to this decision guide. For notifications about updates to this guide, you can subscribe to an RSS feed.

Change	Description	Date
Initial publication	Guide first published.	January 12, 2024