

AWS Leitfaden zur Entscheidungsfindung

Auswahl eines AWS Überwachungs- und Beobachtbarkeitsdienstes



Auswahl eines AWS Überwachungs- und Beobachtbarkeitsdienstes:

AWS Leitfaden zur Entscheidungsfindung

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Handelsmarken und Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

Leitfaden zur Entscheidungsfindung i

Einführung 1

Verstehen 2

Überlegen Sie 4

Klicken Sie auf 8

Verwenden Sie 11

Erkunden 20

Dokumentverlauf 22

..... xxiii

Auswahl eines AWS Überwachungs- und Beobachtbarkeitsdienstes

Den ersten Schritt machen

Zweck	Finden Sie heraus, welche AWS Überwachungs- und Observability-Dienste für Ihr Unternehmen am besten geeignet sind.
Letzte Aktualisierung	12. Januar 2024
Abgedeckte Dienste	<ul style="list-style-type: none">• AWS CloudTrail• Amazon CloudWatch• CloudWatch Amazon-Anwendungssignale• AWS Config• AWS Control Tower• Amazon Managed Grafana• Amazon Managed Service for Prometheus• OpenSearch Amazon-Dienst• AWS Distribution für OpenTelemetry• AWS X-Ray

Einführung

Überwachung und Beobachtbarkeit sind wichtige Komponenten, um die Verfügbarkeit, Leistung, Zuverlässigkeit und Sicherheit Ihrer cloudbasierten Workloads und Daten zu gewährleisten.

- Die Überwachung umfasst die systematische Erfassung und Analyse von Daten wie Metriken, Protokollen und Traces, um den Zustand und die Effizienz von Cloud-Ressourcen zu verfolgen und ein reaktives Incident-Management zu unterstützen.
- Observability konzentriert sich auf das Verständnis des internen Zustands eines Systems durch dynamische Einblicke in Echtzeit, die eine proaktive Problemerkennung und -lösung ermöglichen.

AWS bietet eine Reihe von Tools und Diensten sowohl für die Überwachung als auch für die Beobachtbarkeit. Sie können verwendet werden, um Daten zu sammeln, Metriken zu analysieren und Alarmer zu erstellen, um Sie über Probleme zu informieren. Darüber hinaus können sie Protokolle und Metriken bereitstellen, anhand derer Sie die Hauptursache von Problemen identifizieren und beheben können.

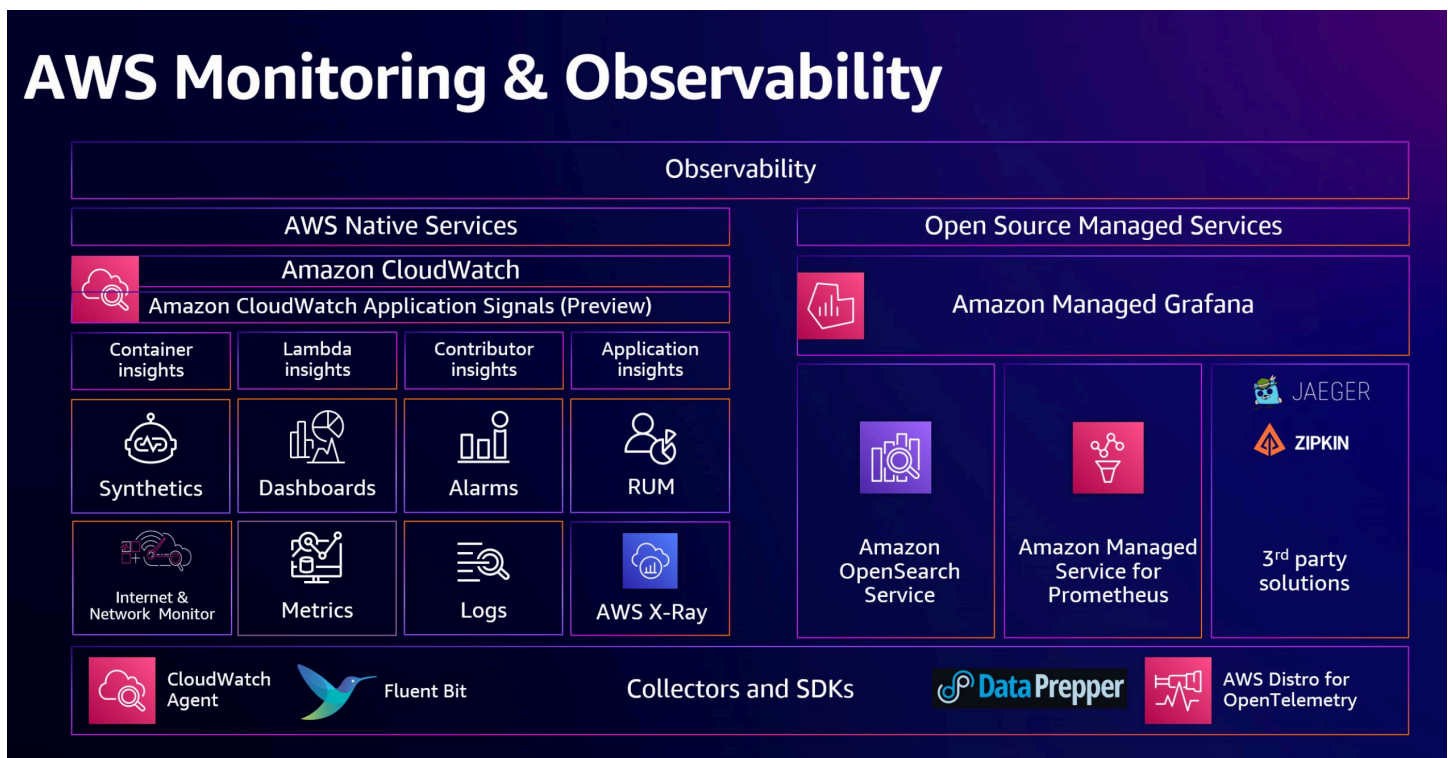
Diese Dienste lassen sich in mehr als 120 andere AWS-Services (darunter Amazon EC2, Amazon EKS, Amazon ECS, Lambda und Amazon S3) und Partner integrieren und lassen sich in eine Vielzahl von Beobachtungs- und AWS Cloud-Management-Tools von Drittanbietern integrieren, die Feeds nativer Telemetrie nahezu in Echtzeit verwenden.

Dieser Leitfaden hilft Ihnen bei der Auswahl der Services und Tools für AWS Überwachung und Observability, die für Ihre Bedürfnisse und Ihr Unternehmen am besten geeignet sind.

[In diesem vierminütigen Clip aus seiner Präsentation zu re:Invent 2023 skizziert der AWS weltweit führende Experte Toshal Dudhwala, wie eine Beobachtbarkeitsstrategie entwickelt werden kann.](#)

Verstehen

Um die richtigen AWS Überwachungs- und Observability-Tools für Ihre Bedürfnisse auszuwählen, kann es hilfreich sein, zunächst zu verstehen, welche Optionen Ihnen zur Verfügung stehen und wie die wichtigsten Dienste zusammenpassen.



Beginnen Sie mit Ihren drei wichtigsten Datenquellen: Logs, Metriken und Traces. Die Daten aus diesen Quellen können mit Amazon CloudWatch - oder AWS Distro for OpenTelemetry (ADOT) - Agenten konsumiert werden. AWS X-Ray

In den folgenden Fällen können Sie jede dieser Datenerfassungsquellen verwenden:

- Verwenden Sie Amazon CloudWatch , um [benutzerdefinierte Kennzahlen aus Ihren eigenen Anwendungen zu sammeln](#), um die Betriebsleistung zu überwachen, Probleme zu beheben und Trends zu erkennen. Sie können den CloudWatch Agenten auch zum Sammeln von Protokollen, Metriken und Traces verwenden. Darüber hinaus können Sie Open-Source-Tools wie Fluent D verwenden, um Protokolle FluentBit zu sammeln und an CloudWatch Protokolle zu senden.
- Wird verwendet AWS X-Ray , um [verteiltes Tracing über mehrere Anwendungen und Systeme hinweg](#) durchzuführen, um die Latenz in einem System zu ermitteln und gezielt zu verbessern. Sie können den CloudWatch Agenten verwenden, um Spuren zu sammeln und sie an X-Ray zu senden.
- Verwenden Sie AWS Distro for OpenTelemetry , um Metriken und Traces zu sammeln.

Instrumentierung

Innerhalb von AWS Überwachungs- und Observabilitätsdiensten stehen zwei Hauptkategorien von Instrumentierung zur Verfügung: AWS Native Services und Open Source Managed Services.

- AWS Zu den Native Services gehören Amazon CloudWatch und AWS X-Ray. CloudWatch bietet die wichtigsten Funktionen von [Container Insights](#), [Lambda Insights](#), [Contributor Insights](#) und [Application Insights](#), die dazu beitragen, wie Sie Ihre Daten für Einblicke und Analysen kontextualisieren.
- Zu den Open Source Managed Services gehören Amazon Managed Service for Prometheus (ein verwalteter Überwachungsservice, der auf der beliebten Open-Source-Überwachungs- und Warnlösung Prometheus basiert und mit dieser kompatibel ist), Amazon OpenSearch Service und AWS Distro for OpenTelemetry (das nicht nur Jaeger und Zipkin Tracing unterstützt AWS X-Ray, sondern auch Jaeger und Zipkin Tracing unterstützt).

Visualisierung und Analyse

Die Daten, die Sie mit diesen AWS Services sammeln und aufnehmen, können mithilfe der [Amazon CloudWatch Service Map](#), der [AWS X-Ray Trace Map](#), [Amazon Managed Grafana](#) und [Amazon CloudWatch Logs Insights](#) visualisiert und analysiert werden.

Andere Dienste

Zu den weiteren Dienstleistungen, die für die Überwachung und Beobachtbarkeit wichtig sind, gehören:

- AWS Config bietet eine detaillierte Ansicht Ihrer Ressourcenkonfigurationen in Ihrem AWS-Konto. Diese Ansicht umfasst die Beziehung zwischen Ihren Ressourcen und den früheren Konfigurationen Ihrer Ressourcen, sodass Sie sehen können, wie sich die Beziehungen und Konfigurationen Ihrer Ressourcen im Laufe der Zeit ändern. Wenn Sie [AWS Config Regeln](#) verwenden, AWS Config bewertet Ihre Ressourcenkonfigurationen auf die gewünschten Einstellungen.
- AWS CloudTrail hilft Ihnen dabei, Betriebs- und Risikoprüfungen, Governance und Compliance zu ermöglichen, indem Ereignisse aufgezeichnet werden, die von Benutzern, Rollen oder AWS Diensten ergriffen wurden. Von einem Benutzer, einer Rolle oder einem AWS Dienst ausgeführte Aktionen werden als Ereignisse in aufgezeichnet CloudTrail. Zu den Ereignissen gehören Aktionen AWS-Managementkonsole, die im AWS Command Line Interface, und AWS SDKs und ausgeführt wurden APIs.

Darüber hinaus können Sie aus einer Reihe von [Services für maschinelles Lernen und Analytik](#) wählen, um noch mehr von Ihren Überwachungs- und Beobachtbarkeitsdaten zu profitieren.

Überlegen Sie

Die Wahl der richtigen Überwachungs- und Observability-Dienste AWS hängt von Ihren spezifischen Anforderungen und Anwendungsfällen ab. Hier sind einige Kriterien, die Sie bei Ihrer Entscheidung berücksichtigen sollten.

Monitoring service capabilities

Überlegen Sie, ob der Service [umfassende Tools bietet, die Metriken, Protokolle und Traces umfassen](#). Metriken bieten quantitative Daten zur Systemleistung, Protokolle liefern detaillierte Ereignisinformationen und mithilfe von Traces können Sie Transaktionen in Ihrer gesamten Infrastruktur verfolgen.

Prüfen Sie auch, ob der Service verschiedene Datentypen und Formate unterstützt. Achten Sie außerdem auf erweiterte Funktionen wie die Erkennung von Anomalien, auf maschinellem Lernen basierende Erkenntnisse und die Möglichkeit, Daten aus verschiedenen Quellen zu korrelieren. Eine umfassende Lösung sollte einen ganzheitlichen Einblick in Ihre AWS Umgebung ermöglichen

und so zu einer effizienten Fehlerbehebung, Leistungsoptimierung und proaktiven Problemlösung beitragen.

Je vielseitiger und integrierter die Servicefunktionen sind, desto besser sind Sie gerüstet, um tiefe Einblicke in Ihre Anwendungen und Infrastruktur zu gewinnen. Weitere Informationen zu den Servicefunktionen finden Sie [im Abschnitt AWS Observability des Management and Governance Cloud Environment Guide](#) (Teil des AWS Well-Architected Framework).

Ease of integration

Beurteilen Sie, wie nahtlos sich der Service in Ihre bestehende AWS Infrastruktur, Anwendungen und Bereitstellungsprozesse integrieren lässt.

Achten Sie auf Kompatibilität mit gängigen Programmiersprachen, Frameworks und Tools von Drittanbietern, die Ihr Unternehmen verwendet. Prüfen Sie auch die Verfügbarkeit von SDKs, APIs, und Plugins, die den Integrationsprozess vereinfachen. Eine bessere Integration kann die Erfassung und Analyse von Daten erleichtern, ohne Ihre Anwendungen erheblich zu belasten.

[Überlegen Sie sich außerdem, ob der Dienst gängige Protokolle für die Datenaufnahme unterstützt.](#) Dienste, die eine bessere Integration bieten, können zu einem reibungsloseren Onboarding-Erlebnis beitragen, sodass Ihr Team schneller mit der Überwachung beginnen und wertvolle Einblicke in Ihre Umgebung gewinnen kann. AWS

Data retention and storage

Funktionen zur Aufbewahrung und Speicherung von Daten sind ausschlaggebende Faktoren bei der Auswahl von AWS Überwachungs- und Observability-Diensten. Prüfen Sie für jeden Service, den Sie in Betracht ziehen, die Richtlinien zur Speicherung und Aufbewahrung historischer Daten sowie zur Skalierbarkeit, um mit der Zeit steigende Datenmengen bewältigen zu können.

Prüfen Sie, ob der Service die langfristige Speicherung von Metriken, Protokollen und Traces unterstützt, sodass Sie rückblickende Analysen durchführen und die Compliance-Anforderungen erfüllen können. Bedenken Sie auch, wie einfach Sie auf archivierte Daten zugreifen und diese abrufen können.

Der Service (oder die Dienste), die Sie nutzen, sollte ein Gleichgewicht zwischen der Bereitstellung ausreichender Aufbewahrungsfristen für aussagekräftige Trendanalysen und der effektiven Verwaltung der Speicherkosten erreichen. Ein klares Verständnis der Datenaufbewahrungs- und Speicherrichtlinien ist wichtig, wenn es darum geht, wie Ihr Monitoring-Setup sowohl den betrieblichen Anforderungen als auch den regulatorischen Verpflichtungen entspricht.

Scalability

Prüfen Sie, wie gut der Service mit Ihrer sich entwickelnden Infrastruktur und Ihren wachsenden Workloads mitwachsen kann. Eine skalierbare Lösung sollte die Zunahme des Datenvolumens, der Benutzeraktivität und der Komplexität Ihrer Anwendungen problemlos bewältigen.

Berücksichtigen Sie die Elastizität des Dienstes, seine Fähigkeit, Nachfragespitzen zu bewältigen, und ob er Funktionen zur auto-scaling unterstützt, um sich dynamisch an sich ändernde Anforderungen anzupassen. Eine robuste Skalierbarkeit trägt dazu bei, dass Ihr Überwachungssystem reaktionsschnell und effektiv bleibt, sodass Sie auch bei Erweiterung Ihrer AWS Umgebung zeitnahe Einblicke erhalten.

Wenn Sie sich für einen Service mit hoher Skalierbarkeit entscheiden, können Sie das kontinuierliche Wachstum Ihrer Anwendungen und Infrastruktur souverän unterstützen, ohne Kompromisse bei der Leistung einzugehen oder unnötige betriebliche Herausforderungen eingehen zu müssen.

Alerting and notification

Beurteilen Sie die Warnfunktionen des Dienstes, einschließlich der Möglichkeit, Warnmeldungen auf der Grundlage vordefinierter Schwellenwerte, Anomalien oder bestimmter Ereignisse einzurichten. Achten Sie auf Flexibilität bei der Konfiguration der Alarmbedingungen und die einfache Verwaltung von Benachrichtigungskanälen wie E-Mail, SMS oder Integrationen mit Tools für die Zusammenarbeit.

Der Service (oder die Services), für den Sie sich entscheiden, sollte zeitnahe und umsetzbare Benachrichtigungen bereitstellen, sodass Ihr Team umgehend auf potenzielle Probleme reagieren kann. Erwägen Sie Funktionen wie Eskalationsrichtlinien und die Möglichkeit, Warnmeldungen zu bestätigen oder zu unterdrücken.

Die Integration mit gängigen Incident-Management-Plattformen kann den gesamten Arbeitsablauf bei der Reaktion auf Vorfälle verbessern. Priorisieren Sie einen Monitoring-Service, der es Ihrem Team ermöglicht, Probleme proaktiv anzugehen, Ausfallzeiten zu minimieren und den kontinuierlichen Zustand Ihrer Umgebung sicherzustellen. AWS

Cost

Machen Sie sich mit dem Preismodell der einzelnen Services vertraut und berücksichtigen Sie dabei Faktoren wie Datenvolumen, Speicherplatz und zusätzliche Funktionen. Überprüfen Sie die Kosteninformationen für jeden Service, den Sie in Betracht ziehen (z. B. [diese Abrechnungs- und Kostenübersicht für Amazon CloudWatch](#)).

Prüfen Sie, ob die Preisstruktur Ihrem Budget und Ihren Nutzungsmustern entspricht. Einige Dienste bieten möglicherweise ein pay-as-you-go Modell an, während andere möglicherweise gestaffelte Preise oder Abonnementpläne haben. Berücksichtigen Sie die potenziellen Auswirkungen aller Kosten — einschließlich Datenübertragungsgebühren oder Gebühren für den Zugriff auf historische Daten.

Prüfen Sie außerdem, ob die Preisgestaltung effizient an das Wachstum Ihrer Infrastruktur angepasst werden kann. Ein klares Verständnis der Kosten stellt sicher, dass Ihre Monitoring-Lösung kosteneffektiv bleibt, ohne Kompromisse bei wesentlichen Funktionen einzugehen. So können Sie Ihr Budget optimieren und gleichzeitig Ihre betrieblichen Anforderungen erfüllen AWS.

Customization and extensibility

Prüfen Sie, ob der Service es Ihnen ermöglicht, Dashboards, Berichte und Benachrichtigungen an Ihre Bedürfnisse anzupassen. Achten Sie auf die Flexibilität, benutzerdefinierte Metriken, Abfragen und Visualisierungen zu erstellen. Die Integration mit Tools von Drittanbietern und die Unterstützung von Common APIs verbessern die Erweiterbarkeit des Dienstes. Prüfen Sie, ob sich die Monitoring-Lösung an die individuellen Anforderungen Ihrer Anwendungen und Infrastruktur anpassen lässt.

Ein hochgradig anpassbarer und erweiterbarer Service ermöglicht es Ihrem Team, die Überwachungsparameter zu optimieren, sich an sich entwickelnde Anwendungsfälle anzupassen und sich nahtlos in Ihre bestehenden Workflows und Tools zu integrieren. Priorisieren Sie Lösungen, die ein hohes Maß an Konfigurierbarkeit bieten, sodass Sie die Überwachung für Ihre spezifische AWS Umgebung und Ihre Betriebspräferenzen optimieren können.

Security and compliance

Beurteilen Sie, wie ein Service die [Einhaltung bewährter AWS Sicherheitsverfahren](#) gewährleistet und die Vertraulichkeit, Integrität und Verfügbarkeit von Daten gewährleistet. Suchen Sie nach Funktionen wie Verschlüsselung bei der Übertragung und Speicherung, Zugriffskontrollen und sicheren Authentifizierungsmechanismen. Prüfen Sie, ob der Service die Einhaltung der für Ihre Branche geltenden Vorschriften und Standards unterstützt.

Halten Sie Ausschau nach Audit-Trail-Funktionen und der Möglichkeit, Compliance-Berichte zu erstellen. Ziel ist es, zum Schutz sensibler Daten beizutragen, indem Überwachungspraktiken angewendet werden, um die gesetzlichen Anforderungen zu erfüllen.

Priorisieren Sie Dienste, die ein robustes Sicherheitsniveau bieten und es Ihrem Unternehmen ermöglichen, eine sichere und konforme AWS Umgebung aufrechtzuerhalten und gleichzeitig Einblicke in Ihre Anwendungen und Infrastruktur zu gewinnen.

Machine learning and analytics

Prüfen Sie, ob der Service maschinelles Lernen (ML) nutzt, um erweiterte Einblicke, Anomalieerkennung und prädiktive Analysen bereitzustellen. Suchen Sie nach Funktionen, die automatisch Muster, Trends und potenzielle Probleme in Ihren Daten identifizieren.

Eine robuste Komponente für maschinelles Lernen kann die Genauigkeit der Erkennung von Anomalien verbessern, Fehlalarme reduzieren und die Gesamteffektivität Ihres Überwachungssystems verbessern. Berücksichtigen Sie außerdem die Tiefe der bereitgestellten Analysen, wie z. B. Ursachenanalysen und Trendprognosen. Ein Service mit starken Funktionen für maschinelles Lernen und Analysen ermöglicht es Ihrem Team, Probleme proaktiv anzugehen, die Leistung zu optimieren und tiefere Einblicke in das Verhalten Ihrer AWS Anwendungen und Infrastruktur zu gewinnen.

Global reach

Die globale Reichweite ist ein entscheidendes Kriterium für AWS Überwachungs- und Observability-Dienste, insbesondere wenn Ihre Infrastruktur über mehrere Regionen verteilt ist. Beurteilen Sie, ob der Monitoring-Service Einblick in die Leistung und den Zustand Ihrer Ressourcen in verschiedenen AWS-Regionen Bereichen bietet.

Erwägen Sie die Möglichkeit, Daten von verschiedenen geografischen Standorten zu aggregieren und zu analysieren, um ein umfassendes Verständnis Ihrer globalen Infrastruktur zu gewährleisten. Suchen Sie nach Funktionen, die eine zentrale Verwaltung und Überwachung unterstützen und es Ihnen ermöglichen, den Betrieb auf globaler Ebene effizient zu überwachen.

Ein Service mit starker globaler Reichweite trägt dazu bei, dass Sie konsistente Überwachungspraktiken aufrechterhalten, Probleme beheben und die Leistung über das gesamte Spektrum Ihrer AWS Bereitstellung hinweg nahtlos optimieren können, unabhängig von den geografischen Grenzen. Diese Funktion ist besonders wertvoll für Unternehmen mit einer geografisch verteilten Infrastruktur oder einer Multi-Cloud-Infrastruktur.

Klicken Sie auf

Nachdem Sie nun die Kriterien kennen, anhand derer Sie Ihre Überwachungs- und Beobachtbarkeitsoptionen bewerten werden, können Sie entscheiden, welche AWS Überwachungs- und Beobachtbarkeitsdienste für Ihre organisatorischen Anforderungen am besten geeignet sein könnten.

In der folgenden Tabelle wird dargestellt, welche Dienste für welche Umstände optimiert sind. Anhand der Tabelle können Sie den Service ermitteln, der für Ihr Unternehmen und Ihren Anwendungsfall am besten geeignet ist.

Anwendungsfall	Wofür ist er optimiert?	Dienste zur Überwachung und Beobachtbarkeit
Überwachen und Warnen	Diese Services sind so optimiert, dass sie Transparenz in Echtzeit, proaktive Problemerkennung, Ressourcenoptimierung und effiziente Reaktion auf Vorfälle bieten und so zum allgemeinen Zustand von Anwendungen und Infrastruktur beitragen.	Amazon CloudWatch CloudWatch Amazon-Protokolle Amazon EventBridge
Überwachung der Anwendungsleistung	Diese Services bieten umfassende Einblicke in das Anwendungsverhalten, bieten Tools zur Identifizierung und Behebung von Leistungsengpässen, unterstützen bei der effizienten Fehlerbehebung und tragen dazu bei, moderne Benutzererlebnisse für verteilte Anwendungen und Webanwendungen bereitzustellen.	CloudWatch Amazon-Anwendungssignale Amazon Managed Service for Prometheus AWS X-Ray Amazon CloudWatch Synthetics
Beobachtbarkeit der Infrastruktur	Diese Services bieten einen ganzheitlichen Überblick über Ihre Cloud-Ressourcen und helfen Ihnen, fundierte Entscheidungen über Ressourcennutzung, Leistungs	CloudWatch Amazon-Metriken Einblicke in Amazon CloudWatch Container

Anwendungsfall	Wofür ist er optimiert?	Dienste zur Überwachung und Beobachtbarkeit
	Optimierung und Kosteneffizienz zu treffen.	
Protokollierung und Analyse	Diese Services helfen Ihnen dabei, Protokolldaten effizient zu verwalten und zu analysieren, Fehler zu beheben, Anomalien zu erkennen, die Sicherheit zu gewährleisten, Compliance-Anforderungen zu erfüllen und umsetzbare Einblicke in Ihre Anwendungen und Infrastruktur zu erhalten.	Amazon Cloudwatch protokolliert Einblicke Amazon CloudWatch Logs zur Erkennung von Anomalien Amazon Managed Grafana OpenSearch Amazon-Dienst Amazon Kinesis Data Streams
Überwachung von Sicherheit und Einhaltung der Vorschriften	Optimiert für ein robustes Sicherheitsframework, das proaktive Bedrohungserkennung, kontinuierliche Überwachung, Compliance-Nachverfolgung und Auditfunktionen ermöglicht, um Ihre AWS Ressourcen zu schützen und eine sichere und konforme Umgebung aufrechtzuerhalten.	Amazon GuardDuty AWS Config AWS CloudTrail
Netzwerk-Überwachung	Diese Services bieten Einblick in den Netzwerkverkehr, erhöhen die Sicherheit, indem sie Bedrohungen erkennen und verhindern, ermöglichen ein effizientes Netzwerkdatenverkehrsmanagement und unterstützen Maßnahmen zur Reaktion auf Vorfälle.	Amazon CloudWatch Netzwerkmonitor Amazon CloudWatch Internetmonitor Amazon VPC-Flussprotokolle AWS Network Firewall

Anwendungsfall	Wofür ist er optimiert?	Dienste zur Überwachung und Beobachtbarkeit
Verteilte Ablaufverfolgung	Diese Dienste bieten einen umfassenden Überblick über die Interaktionen und Abhängigkeiten innerhalb Ihrer verteilten Anwendungen. Sie ermöglichen es Ihnen, Leistungsengpässe zu diagnostizieren, die Anwendungsleistung zu optimieren und das reibungslose Funktionieren komplexer Systeme zu unterstützen, indem sie Einblicke in die Art und Weise bieten, wie verschiedene Teile Ihrer Anwendung kommunizieren und interagieren.	AWS Distribution für OpenTelemetry AWS X-Ray Amazon CloudWatch Application Signals (Vorschau)
Beobachtbarkeit in Hybrid- und Multi-Cloud-Umgebungen	Sorgen Sie für einen zuverlässigen Betrieb, bieten Sie Ihren Kunden moderne digitale Erlebnisse und lassen Sie sich helfen, Ihre Service-Level-Ziele und Leistungszusagen zu erfüllen.	Amazon CloudWatch (Hybrid- und Multicloud-Unterstützung)

Verwenden Sie

Sie sollten jetzt genau wissen, was die einzelnen AWS Überwachungs- und Observability-Dienste (und die unterstützenden AWS Tools und Dienste) tun und welcher für Sie geeignet sein könnte.

Um herauszufinden, wie die einzelnen verfügbaren AWS Observability-Dienste verwendet werden können, und mehr über sie zu erfahren, haben wir einen Weg bereitgestellt, um zu untersuchen,

wie die einzelnen Dienste funktionieren. Der folgende Abschnitt enthält Links zu ausführlicher Dokumentation, praktischen Tutorials und Ressourcen, die Ihnen den Einstieg erleichtern.

Amazon CloudWatch

- Erste Schritte mit Amazon CloudWatch

Überwachen Sie mit Amazon Ihre AWS Ressourcen und die Anwendungen, auf AWS denen Sie laufen, in Echtzeit CloudWatch. Sie können CloudWatch damit Metriken sammeln und verfolgen. Dabei handelt es sich um Variablen, die Sie für Ihre Ressourcen und Anwendungen messen können.

[Erkunden Sie den Leitfaden](#)

- Erste Schritte mit Amazon CloudWatch Metrics

In diesem Leitfaden werden die grundlegende Überwachung und die detaillierte Überwachung, die grafische Darstellung von Metriken und die Verwendung der CloudWatch Anomalieerkennung beschrieben.

[Erkunden Sie den Leitfaden](#)

- Container Insights auf Amazon EKS und Kubernetes einrichten

Richten Sie das Amazon CloudWatch Observability ESK-Add-on und ADTO auf Ihrem EKS-Cluster ein, an das Metriken gesendet werden sollen. CloudWatch Sie erfahren auch, wie Sie Fluent Bit oder Fluentd einrichten, um Protokolle an Logs zu senden. CloudWatch

[Erkunden Sie den Leitfaden](#)

- Erste Schritte mit Amazon CloudWatch Application Insights

Erfahren Sie, wie Sie mithilfe der Konsole CloudWatch Application Insights Ihre Anwendungen für die Überwachung verwalten können.

[Erkunden Sie den Leitfaden](#)

- Verwenden von Container Insights

Erfahren Sie, wie CloudWatch Container Insights Metriken und Logs aus Ihren containerisierten Anwendungen und Microservices sammelt, aggregiert und zusammenfasst.

[Erkunden Sie den Leitfaden](#)

- Container Insights auf Amazon ECS einrichten

Erfahren Sie, wie Sie Cluster- und Service-Level-Metriken konfigurieren, ADOT zur Erfassung von Metriken auf EC2 Instanzebene einsetzen und das Senden von Protokollen an CloudWatch Logs einrichten FireLens .

[Erkunden Sie den Leitfaden](#)

Amazon CloudWatch Application Insights

- Erste Schritte mit Amazon CloudWatch Application Signals

In diesem Leitfaden erfahren Sie, wie Sie Ihre Anwendungen automatisch ausstatten, AWS sodass Sie den aktuellen Zustand Ihrer Anwendungen überwachen und die langfristige Anwendungsleistung anhand Ihrer Geschäftsziele verfolgen können.

[Erkunden Sie den Leitfaden](#)

- Amazon CloudWatch Application Signals für die automatische Instrumentierung Ihrer Anwendungen

Dieser Blogbeitrag bietet eine ausführliche Einführung in Amazon CloudWatch Application Signals und zeigt, wie Sie Telemetrie für Ihre EKS-Cluster sammeln. AWS-Managementkonsole

[Lesen Sie den Blogbeitrag](#)

- So überwachen Sie den Zustand von Anwendungen SLOs mithilfe von Amazon CloudWatch Application Signals

Dieser Blogbeitrag zeigt, wie Amazon CloudWatch Application Signals es Ihnen ermöglicht, Anwendungen automatisch zu instrumentieren und zu betreiben AWS , um die Anwendungsleistung anhand Ihrer wichtigsten Ziele zu verfolgen.

[Lesen Sie den Blogbeitrag](#)

Amazon CloudWatch Lambda Insights

- Wir stellen vor: CloudWatch Lambda Insights

Erfahren Sie, wie Sie einige „Hello World“-Lambda-Funktionen erstellen und diese mithilfe von Lambda Insights überwachen. Sie werden die verwenden, AWS CDK um die Architektur bereitzustellen.

[Lesen Sie den Blog](#)

- Verwendung von Amazon CloudWatch Lambda Insights zur Verbesserung der betrieblichen Transparenz

Erfahren Sie, wie Sie Lambda Insights verwenden können, um auf einfache und bequeme Weise den Betrieb zu überwachen und Einblicke in das Verhalten Ihrer AWS Lambda Funktionen zu erhalten.

[Lesen Sie den Blog](#)

Amazon CloudWatch Logs

- Erste Schritte mit Amazon CloudWatch Logs

Erfahren Sie, wie Sie den Unified CloudWatch Agent installieren und wie Sie die Erfassung von Metriken damit konfigurieren CloudFormation.

[Lesen Sie den Leitfaden](#)

- Analysieren von Protokolldaten mit CloudWatch Logs Insights

In dieser Anleitung erfahren Sie, wie Sie mit Logs Insights-Abfragen beginnen, Protokolldaten in Diagrammen visualisieren und Abfragen zu Ihrem Dashboard hinzufügen können.

[Beginnen Sie mit dem Leitfaden](#)

- Amazon CloudWatch Logs Insights — Schnelle, interaktive Protokollanalysen

Verwenden Sie Logs Insights, um die Datenpunkte, Muster, Trends und Erkenntnisse zu nutzen, die in den verschiedenen von erstellten Protokollen enthalten sind, AWS-Services um zu verstehen, wie sich Ihre Anwendungen und AWS Ressourcen verhalten, Verbesserungspotenzial zu identifizieren und betriebliche Probleme zu lösen.

[Lesen Sie den Blogbeitrag](#)

Amazon CloudWatch Synthetics

- Verwenden Sie synthetisches Monitoring

Dieses Handbuch zeigt, wie man Canaries erstellt, konfigurierbare Skripts, die nach einem Zeitplan ausgeführt werden, und bietet Beispielcode für Canary-Skripte.

[Erkunden Sie den Leitfaden](#)

- Sichere Überwachung der Workflow-Erfahrung der Benutzer mit Amazon CloudWatch Synthetics und AWS Secrets Manager

So erstellen, implementieren und überwachen Sie synthetische Überwachungslösungen mit Amazon CloudWatch Synthetics.

[Lesen Sie den Blogbeitrag](#)

Amazon EventBridge

- Erste Schritte mit Amazon EventBridge

Erfahren Sie, wie Sie eine Grundregel erstellen, um Ereignisse an ein Ziel weiterzuleiten.

[Erkunden Sie den Leitfaden](#)

- EventBridge Amazon-Ereignisse archivieren und erneut abspielen

Erstellen Sie mithilfe der Lambda-Konsole eine Funktion, die als Ziel für die EventBridge Regel verwendet werden soll.

[Erkunden Sie den Leitfaden](#)

- Den Status einer EC2 Amazon-Instance protokollieren mit EventBridge

Erstellen Sie eine AWS Lambda Funktion zum Protokollieren von Statusänderungen für eine EC2 Amazon-Instance. Sie protokollieren den Start jeder neuen EC2 Instance.

[Verwenden Sie das Tutorial](#)

- Entwicklung einer ereignisgesteuerten Anwendung mit Amazon EventBridge

Erfahren Sie, wie Sie mithilfe der CLI AWS Serverless Application Model (AWS SAM) eine ereignisgesteuerte Anwendung erstellen und bereitstellen.

[Lesen Sie den Blog](#)

AWS CloudTrail

- Erste Schritte mit AWS CloudTrail

AWS CloudTrail ist ein Programm AWS-Service , das Ihnen dabei hilft, Betriebs- und Risikoprüfungen, Unternehmensführung und Einhaltung Ihrer Vorschriften zu ermöglichen AWS-Konto. Hier erfahren Sie, wie Sie damit beginnen können.

[Erkunden Sie den Leitfaden](#)

- AWS-Konto Aktivität überprüfen

Erfahren Sie, wie Sie die AWS API-Aktivität in Ihrem AWS-Konto für Dienste, die unterstützen, überprüfen können CloudTrail.

[Nutze das Tutorial](#)

- Einen Trail anlegen

Erfahren Sie, wie Sie einen Trail erstellen, um AWS API-Aktivitäten in allen Regionen zu protokollieren, einschließlich Daten und Insights-Ereignissen.

[Nutze das Tutorial](#)

- AWS CloudTrail Workshop zur Protokollüberwachung

Erfahren Sie, wie Sie CloudTrail Protokolle in CloudWatch Funktionen wie CloudWatch Log Insights, CloudWatch metrische Filter, CloudWatch metrische Alarmer und CloudWatch Dashboards integrieren und diese nutzen können.

[Nutzen Sie den Workshop](#)

- AWS CloudTrail bewährte Verfahren

Bewährte Methoden für die Nutzung CloudTrail , um Prüfungen in Ihrem gesamten Unternehmen zu ermöglichen.

[Lesen Sie den Blog](#)

AWS Config

- Erste Schritte mit AWS Config

AWS Config bietet einen detaillierten Überblick über die Konfiguration der AWS Ressourcen in Ihrem AWS-Konto. Dies erklärt, wie Sie damit beginnen können.

[Erkunden Sie den Leitfaden](#)

- Einrichtung AWS Config (Konsole)

Erfahren Sie, wie Sie es einrichten AWS Config , AWS-Konten indem Sie das verwenden AWS-Managementkonsole.

[Erkunden Sie den Leitfaden](#)

- Einrichtung AWS Config mit dem AWS CLI

Erfahren Sie, wie Sie es einrichten AWS Config , AWS-Konten indem Sie das verwenden AWS CLI.

[Erkunden Sie den Leitfaden](#)

Amazon Managed Grafana

- Erste Schritte mit Amazon Managed Grafana

Erfahren Sie, wie Sie mit Amazon Managed Grafana beginnen und Ihren ersten Workspace erstellen und sich dann mit der Grafana-Konsole in diesem Workspace verbinden.

[Erkunden Sie den Leitfaden](#)

- Amazon Managed Grafana — Erste Schritte

Erfahren Sie, wie Sie Amazon Managed Service for Prometheus integrieren und benutzerdefinierte Dashboards erstellen.

[Lesen Sie den Blog](#)

- Visualisieren und gewinnen Sie Einblicke in Ihre AWS Kosten und Nutzung mit Amazon Managed Grafana

Erfahren Sie, wie Sie Ihre AWS Kosten- und Nutzungsdaten mit Amazon Managed Grafana visualisieren und analysieren können.

[Lesen Sie den Blog](#)

Amazon Managed Service for Prometheus

- Erste Schritte mit Amazon Managed Service für Prometheus

Erstellen Sie Amazon Managed Service für Prometheus-Workspaces, richten Sie die Aufnahme von Prometheus-Metriken in diese Workspaces ein und fragen Sie diese Metriken ab.

[Erkunden Sie den Leitfaden](#)

- Container Insights — Überwachung der Prometheus-Metriken

Erfahren Sie, wie Sie die Erkennung von Prometheus-Metriken aus containerisierten Workloads mithilfe von Container Insights automatisieren können. CloudWatch

[Erkunden Sie den Leitfaden](#)

- Amazon Managed Service for Prometheus FAQs

Häufig gestellte Fragen zu Amazon Managed Service for Prometheus.

[Lesen Sie den FAQs](#)

Amazon OpenSearch Service

- Erste Schritte mit Amazon OpenSearch Service

Verwenden Sie Amazon OpenSearch Service, um eine Testdomain zu erstellen und zu konfigurieren. Eine OpenSearch Service-Domain ist gleichbedeutend mit einem OpenSearch Cluster.

[Erkunden Sie den Leitfaden](#)

- Erste Schritte mit Amazon OpenSearch Serverless

Dieses Tutorial führt Sie durch die grundlegenden Schritte, um eine Amazon OpenSearch Serverless-Suchsammlung schnell zum Laufen zu bringen

[Verwenden Sie das Tutorial](#)

- Dokumente in Amazon OpenSearch Service erstellen und danach suchen

Erfahren Sie, wie Sie in Amazon OpenSearch Service ein Dokument erstellen und danach suchen.

[Verwenden Sie das Tutorial](#)

- Erste Schritte mit Amazon OpenSearch Ingestion

Erfahren Sie, wie Sie Amazon OpenSearch Ingestion verwenden, um Daten in eine Domain und auch in eine Sammlung aufzunehmen.

[Erkunden Sie den Leitfaden](#)

- SIEM auf Amazon OpenSearch Service Workshop

Erstellen Sie eine Plattform zur Analyse von Sicherheitsprotokollen auf Amazon OpenSearch Service und beginnen Sie mit der Entwicklung einer kostengünstigen Lösung für die Erfassung, Analyse und Dashboarding von Protokollen.

[Nutzen Sie den Workshop](#)

- Dokumente in Amazon OpenSearch Service erstellen und danach suchen

Erfahren Sie, wie Sie in Amazon OpenSearch Service ein Dokument erstellen und danach suchen.

[Verwenden Sie das Tutorial](#)

AWS Distro for OpenTelemetry

- Erste Schritte mit dem AWS Distro for OpenTelemetry (ADOT) Collector

Gehen Sie die Schritte durch, um die ADOT-Sammlung lokal zu erstellen.

[Erkunden Sie den Leitfaden](#)

- AWS Distribution für OpenTelemetry JavaScript

Erfahren Sie, wie Sie Ihre JavaScript Anwendungen instrumentieren und korrelierte Messwerte an verschiedene AWS Monitoring-Lösungen senden können.

[Erkunden Sie den Leitfaden](#)

- AWS Distro für Python OpenTelemetry

In diesem Leitfaden erfahren Sie, wie Sie Ihre Python-Anwendungen instrumentieren und korrelierte Metriken an verschiedene AWS Monitoring-Lösungen senden.

[Erkunden Sie den Leitfaden](#)

AWS X-Ray

- Erste Schritte mit AWS X-Ray

In diesem Handbuch erfahren Sie, wie Sie eine Beispielanwendung starten. Anschließend lernen Sie, wie Sie Ihre Anwendung instrumentieren und lernen andere Dienste kennen, die in X-Ray integriert sind.

[Erkunden Sie den Leitfaden](#)

- Workshop zur Beobachtbarkeit

Dieser Workshop bietet Ihnen praktische Erfahrungen mit einer Vielzahl von Tools AWS für Überwachung und Beobachtbarkeit, einschließlich AWS X-Ray ADOT.

[Nutzen Sie den Workshop](#)

- Protokollierung und Überwachung von Anwendungen mit AWS X-Ray

Erfahren Sie, wie Daten über Anfragen AWS X-Ray erfasst werden, die Ihre Anwendung bearbeitet, und Ihnen dabei hilft, diese Daten anzuzeigen, zu filtern und Einblicke in sie zu gewinnen, um Probleme und Optimierungsmöglichkeiten zu identifizieren.

[Erkunden Sie den Leitfaden](#)

Erkunden

- Lösungen

Entdecken Sie Lösungen, die Sie bei der Implementierung von Überwachung und Beobachtbarkeit unterstützen. AWS

[Entdecken Sie Lösungen](#)

- Whitepapers

Schauen Sie sich Whitepapers an, die Ihnen den Einstieg erleichtern, bewährte Verfahren kennenlernen und sich mit Ihren Überwachungs- und Beobachtbarkeitsoptionen vertraut machen.

[Entdecken Sie Whitepapers](#)

- Video, Muster und Anleitungen

Informieren Sie sich über zusätzliche Architekturanleitungen zu gängigen Anwendungsfällen für Überwachungs- und Observability-Dienste.

[Erkunden Sie weitere Ressourcen](#)

Dokumentverlauf

In der folgenden Tabelle werden die wichtigen Änderungen an diesem Entscheidungsleitfaden beschrieben. Für Benachrichtigungen über Aktualisierungen dieses Handbuchs können Sie einen RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
Erste Veröffentlichung	Der Leitfaden wurde zuerst veröffentlicht.	12. Januar 2024

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.