Entwerfen und Implementieren von Protokollierung und Überwachung mit Amazon CloudWatch

AWS Präskriptive Leitlinien

AWS Präskriptive Leitlinien: Entwerfen und Implementieren von Protokollierung und Überwachung mit Amazon CloudWatch

Table of Contents

Entwurf und Implementierung von Protokollierung und Überwachung mit Amazon CloudWatch

Khurram Nizami, Amazon Web Services (AWS)

April 2023 (Dokumentengeschichte)

Dieses Handbuch hilft Ihnen dabei, Protokollierung und Überwachung mit Amazon CloudWatch und verwandten Amazon Web Services (AWS) Management- und Governance-Services für Workloads zu entwerfen und zu implementieren, die Amazon Elastic Compute Cloud (Amazon EC2) -Instances, Amazon Elastic Container Service (Amazon ECS), Amazon Elastic Kubernetes Service (Amazon EKS) und lokale Server verwenden. AWS Lambda Der Leitfaden richtet sich an Betriebsteams, DevOps Ingenieure und Anwendungstechniker, die Workloads in derAWS Cloud verwalten.

Ihr Ansatz zur Protokollierung und Überwachung sollte auf den sechs Säulen desAWS Well-Architected Frameworks basieren. Diese Säulen sind betriebliche Exzellenz, Sicherheit, Zuverlässigkeit, Leistungseffizienz und Kostenoptimierung. Eine gut konzipierte Überwachungs- und Alarmlösung verbessert die Zuverlässigkeit und Leistung, indem sie Ihnen hilft, Ihre Infrastruktur proaktiv zu analysieren und anzupassen.

In diesem Leitfaden werden Protokollierung und Überwachung aus Gründen der Sicherheit oder Kostenoptimierung nicht ausführlich behandelt, da dies Themen sind, die einer eingehenden Bewertung bedürfen. Es gibt vieleAWS Dienste, die die Sicherheitsprotokollierung und -überwachung unterstützen AWS CloudTrailAWS Config, darunter Amazon Inspector, Amazon Detective, Amazon Macie GuardDuty, Amazon und AWS Security Hub. Sie können auch AWSBudgets und CloudWatch Abrechnungskennzahlen zur Kostenoptimierung verwenden AWS Cost Explorer.

In der folgenden Tabelle werden die sechs Bereiche beschrieben, die Ihre Logging- und Monitoring-Lösung behandeln sollte.

Erfassung und Erfassung von Protokolldateien und Metriken	Identifizieren, konfigurieren und senden Sie System- und Anwendungsprotokolle und Metriken aus verschiedenen Quellen anAWS Dienste.

Logs suchen und analysieren	Suchen und analysieren Sie Protokolle für das Betriebsmanagement, die Problemidentifikation, Fehlerbehebung und Anwendungsanalyse.
Überwachung von Kennzahlen und Alarmierung	Identifizieren Sie Beobachtungen und Trends in Ihren Workloads und handeln Sie entsprechend.
Überwachung der Anwendungs- und Serviceverfügbarkeit	Reduzieren Sie Ausfallzeiten und verbessern Sie Ihre Fähigkeit, die Service-Level-Ziele zu erreichen, indem Sie die Serviceverfügbarkeit kontinuierlich überwachen.
Rückverfolgungsanwendungen	Verfolgen Sie Anwendungsanforderungen in Systemen und externen Abhängigkeiten, um die Leistung zu optimieren, Ursachenanalysen durchzuführen und Probleme zu beheben.
Erstellen von Dashboards und Visualisierungen	Erstellen Sie Dashboards, die sich auf relevante Kennzahlen und Beobachtungen für Ihre Systeme und Workloads konzentrieren. So können Sie Probleme kontinuierlich verbessern und proaktiv Probleme erkennen.

CloudWatch kann die meisten Protokollierungs- und Überwachungsanforderungen erfüllen und bietet eine zuverlässige, skalierbare und flexible Lösung. VieleAWS Dienste stellen zusätzlich zur CloudWatch Protokollierungsintegration für Überwachung und Analyse automatisch CloudWatch Metriken bereit. CloudWatch bietet auch Agenten und Protokolltreiber zur Unterstützung einer Vielzahl von Rechenoptionen wie Server (sowohl in der Cloud als auch vor Ort), Container und serverloses Computing. In diesem Handbuch werden auch die folgendenAWS Dienste behandelt, die für die Protokollierung und Überwachung verwendet werden:

- AWS Systems ManagerDistributor, Systems Manager State Manager und Systems Manager Automation zur Automatisierung, Konfiguration und Aktualisierung des CloudWatch Agents für Ihre EC2-Instances und lokalen Server
- Amazon OpenSearch Service für erweiterte Protokollaggregation, Suche und Analyse

- Amazon Route 53 Health Checks und CloudWatchSynthetics zur Überwachung der Anwendungs- und Serviceverfügbarkeit
- Amazon Managed Service for Prometheus für die Überwachung containerisierter Anwendungen in großem Maßstab
- AWS X-Rayfür Anwendungsverfolgung und Laufzeitanalyse
- Amazon Managed Grafana zur Visualisierung und Analyse von Daten aus verschiedenen Quellen (z. CloudWatch B. Amazon OpenSearch Service und Amazon Timestream)

DieAWS von Ihnen ausgewählten Rechendienste wirken sich auch auf die Implementierung und Konfiguration Ihrer Protokollierungs- und Überwachungslösung aus. Beispielsweise unterscheiden CloudWatch sich die Implementierung und Konfiguration für Amazon EC2, Amazon ECS, Amazon EKS und Lambda.

Besitzer von Anwendungen und Workloads vergessen oft die Protokollierung und Überwachung oder konfigurieren und implementieren sie inkonsistent. Das bedeutet, dass Workloads mit eingeschränkter Beobachtbarkeit in die Produktion gelangen, was zu Verzögerungen bei der Identifizierung von Problemen führt und den Zeitaufwand für deren Behebung und Lösung erhöht. Ihre Protokollierungs- und Überwachungslösung muss mindestens die Systemebene für die Protokolle und Metriken auf Betriebssystemebene (OS) sowie die Anwendungsebene für Anwendungsprotokolle und Metriken berücksichtigen. Der Leitfaden enthält einen empfohlenen Ansatz für den Umgang mit diesen beiden Ebenen in verschiedenen Berechnungstypen, einschließlich der drei in der folgenden Tabelle beschriebenen Berechnungstypen.

Langlebige und unveränderliche EC2-Instances	System- und Anwendungsprotokolle und Metriken für mehrere Betriebssysteme (Betriebssysteme) in mehrerenAWS Regionen oder Konten.
Container	System- und Anwendungsprotokolle und Metriken für Ihre Amazon ECS- und Amazon EKS-Cluster, einschließlich Beispielen für verschiedene Konfigurationen.
Serverless	System- und Anwendungsprotokolle und Metriken für Ihre Lambda-Funktionen sowie Überlegungen zur Anpassung.

Dieses Handbuch enthält eine Protokollierungs- und Überwachungslösung, die sich mit CloudWatch und zugehörigenAWS Diensten in den folgenden Bereichen befasst:

- Planen Ihrer CloudWatch Bereitstellung— Überlegungen zur Planung Ihrer CloudWatch Bereitstellung und Hinweise zur Zentralisierung Ihrer CloudWatch Konfiguration.
- Konfigurieren von CloudWatch -Agenten für EC2-Instances und lokale Server— CloudWatch Konfigurationsdetails für Protokollierung und Metriken auf System- und Anwendungsebene.
- Installationsansätze für CloudWatch Agent für Amazon EC2 und lokale Server— Vorgehensweisen für die Installation des CloudWatch Agenten, einschließlich automatisierter Bereitstellung mithilfe von Systems Manager in mehreren Regionen und Konten.
- Protokollierung und Überwachung auf Amazon ECS — Anleitung CloudWatch zur Konfiguration von Protokollierung und Metriken auf Cluster- und Anwendungsebene in Amazon ECS.
- Protokollierung und Überwachung auf Amazon EKS — Anleitung CloudWatch zur Konfiguration von Protokollierung und Metriken auf Cluster- und Anwendungsebene in Amazon EKS.
- Prometheus-Überwachung auf Amazon EKS— Stellt Amazon Managed Service für Prometheus vor und vergleicht es mit CloudWatch Container Insights Monitoring für Prometheus.
- Protokollierung und Metriken fürAWS Lambda— Anleitung CloudWatch zur Konfiguration Ihrer Lambda-Funktionen.
- Logs suchen und analysieren CloudWatch— Methoden zur Analyse Ihrer Protokolle mithilfe von Amazon CloudWatch Application Insights, CloudWatch Logs Insights und Erweiterung der Protokollanalyse auf Amazon OpenSearch Service.
- Alarmierende Optionen mit CloudWatch— Führt CloudWatch Alarme und CloudWatch Anomalieerkennung ein und bietet Anleitungen zur Erstellung und Einrichtung von Alarmen.
- Überwachung der Anwendungs- und Dienstverfügbarkeit— Führt die Health Checks von CloudWatch Synthetics und Route 53 für die automatisierte Verfügbarkeitsüberwachung ein und vergleicht sie.
- Verfolgen von Anwendungen mitAWS X-Ray— Einführung und Einrichtung der Anwendungsverfolgung mit X-Ray für Amazon EC2, Amazon ECS, Amazon EKS und Lambda
- Dashboards und Visualisierungen mit CloudWatch— Einführung in CloudWatch Dashboards für eine verbesserte Beobachtbarkeit bei allenAWS Workloads.
- Integration von CloudWatch inAWSDienstleistungen— Erklärt, wie es CloudWatch in verschiedeneAWS Dienste integriert werden kann.
- Amazon Managed Grafana für Dashboarding und Visualisierung— Stellt Amazon Managed Grafana CloudWatch für Dashboarding und Visualisierung vor und vergleicht sie.

Implementierungsbeispiele werden in diesem Handbuch in diesen Bereichen verwendet und sind auch im AWS GitHub Samples-Repository verfügbar.

Gezielte Geschäftsergebnisse

Erstellen einer Protokollierungs- und Überwachungslösung, die für dieAWSCloud ist ein wesentlicher Bestandteil für das Erreichen dessechs Vorteile von Cloud Computingaus. Ihre Protokollierungs- und Überwachungslösung sollte Ihrer IT-Organisation dabei helfen, Geschäftsergebnisse zu erzielen, die Ihren Geschäftsprozessen, Geschäftspartnern, Mitarbeitern und Kunden zugute kommen. Sie können die folgenden vier Ergebnisse erwarten, nachdem Sie eine Protokollierungs- und Überwachungslösung implementiert haben, die auf dieAWSFramework Well-Architected:

Beschleunigen Sie die Betriebsbereitschaft

Die Aktivierung einer Protokollierungs- und Überwachungslösung ist ein wichtiger Bestandteil der Vorbereitung einer Workload für die Produktionsunterstützung und -nutzung. Die Betriebsbereitschaft kann schnell zu einem Engpass werden, wenn Sie zu stark auf manuelle Prozesse angewiesen sind und auch die Wertschöpfungszeit (TTV) für Ihre IT-Investitionen reduzieren können. Ein ineffektiver Ansatz führt auch zu einer begrenzten Beobachtbarkeit Ihrer Workloads. Dies kann das Risiko längerer Ausfälle, Kundenunzufriedenheit und fehlgeschlagene Geschäftsprozesse erhöhen.

Sie können die Ansätze dieses Leitfadens verwenden, um Ihre Protokollierung und Überwachung auf derAWSCloud. Neue Workloads erfordern dann eine minimale manuelle Vorbereitung und Intervention für die Produktionsprotokollierung und -überwachung. Dies trägt auch dazu bei, die Zeit und die Schritte zu reduzieren, die erforderlich sind, um Protokollierungs- und Überwachungsstandards für verschiedene Workloads über mehrere Konten und Regionen hinweg zu erstellen.

Verbesserung der Operational Excellence

Dieser Leitfaden enthält mehrere Best Practices für die Protokollierung und Überwachung, die verschiedenen Workloads helfen, Geschäftsziele zu erreichen undOperational Excellenceaus. Dieser Leitfaden bietet auchdetaillierte Beispiele und wiederverwendbare Open-Source-Vorlagenden Sie mit einem Infrastructure as Code (iAC) -Ansatz verwenden können, um eine gut konzipierte Protokollierungs- und Überwachungslösung mitAWS-Services. Die Verbesserung der operativen Exzellenz ist iterativ und erfordert eine kontinuierliche Verbesserung. Der Leitfaden enthält Vorschläge zur kontinuierlichen Verbesserung der Protokollierungs- und Überwachungspraktiken.

Verbesserung der betrieblichen Sichtbarkeit

Ihre Geschäftsprozesse und Anwendungen werden möglicherweise von verschiedenen IT-Ressourcen unterstützt und auf verschiedenen Rechentypen gehostet, entweder vor Ort oder in derAWSCloud. Ihre betriebliche Sichtbarkeit kann durch inkonsistente und unvollständige Implementierungen Ihrer Protokollierungs- und Überwachungsstrategie eingeschränkt werden. Durch die Verwendung eines umfassenden Protokollierungs- und Überwachungsansatzes können Sie Probleme in Ihren Workloads schnell identifizieren, diagnostizieren und darauf reagieren. Dieser Leitfaden hilft Ihnen dabei, Ansätze zu entwickeln und zu implementieren, um Ihre vollständige betriebliche Sichtbarkeit zu verbessern und die mittlere Zeit für die Behebung von Fehlern (MTTR) zu reduzieren. Ein umfassender Protokollierungs- und Überwachungsansatz hilft Ihrem Unternehmen auch, die Servicequalität zu verbessern, die Endbenutzererfahrung zu verbessern und Service Level Agreements (SLAs) einzuhalten.

Skalieren Sie den Betrieb und senken Sie die Gemeinkosten

Sie können die Protokollierungs- und Überwachungspraktiken in diesem Handbuch skalieren, um mehrere Regionen und Konten, kurzlebige Ressourcen und mehrere Umgebungen zu unterstützen. Der Leitfaden enthält Ansätze und Beispiele zur Automatisierung manueller Schritte (z. B. Installieren und Konfigurieren von Agenten, Überwachen von Metriken und Benachrichtigung oder Ergreifen von Maßnahmen bei Problemen). Diese Ansätze sind hilfreich, wenn Ihre Cloud-Akzeptanz reift und wächst und Sie die Betriebsfähigkeit skalieren müssen, ohne die Cloud-Managementaktivitäten oder -ressourcen zu erhöhen.

Planen Ihrer CloudWatch Bereitstellung

Die Komplexität und der Umfang einer Protokollierungs- und Überwachungslösung hängen von mehreren Faktoren ab, darunter:

- Wie viele Umgebungen, Regionen und Konten verwendet werden und wie sich diese Zahl erhöhen könnte.
- Die Vielzahl und Typen Ihrer vorhandenen Workloads und Architekturen.
- Die Datenverarbeitungstypen und OSs, die protokolliert und überwacht werden müssen.
- Gibt an, ob sowohl lokale Standorte als auch AWS Infrastruktur vorhanden sind.
- Die Aggregations- und Analyseanforderungen mehrerer Systeme und Anwendungen.
- Sicherheitsanforderungen, die die unbefugte Offenlegung von Protokollen und Metriken verhindern.
- Produkte und Lösungen, die in Ihre Protokollierungs- und Überwachungslösung integriert werden müssen, um Betriebsprozesse zu unterstützen.

Sie müssen Ihre Protokollierungs- und Überwachungslösung regelmäßig mit neuen oder aktualisierten Workload-Bereitstellungen überprüfen und aktualisieren. Aktualisierungen Ihrer Protokollierung, Überwachung und Alarmierung sollten identifiziert und angewendet werden, wenn Probleme beobachtet werden. Diese Probleme können dann proaktiv identifiziert und in Zukunft verhindert werden.

Sie müssen sicherstellen, dass Sie Software und Services für die Erfassung und Aufnahme von Protokollen und Metriken konsistent installieren und konfigurieren. Ein etablierter Protokollierungs- und Überwachungsansatz verwendet mehrere AWS oder unabhängige Softwareanbieter-(ISV)-Services und -Lösungen für verschiedene Domains (z. B. Sicherheit, Leistung, Netzwerk oder Analytik). Jede Domain hat ihre eigenen Bereitstellungs- und Konfigurationsanforderungen.

Wir empfehlen die Verwendung von CloudWatch zum Erfassen und Erfassen von Protokollen und Metriken für mehrere OSs und Datenverarbeitungstypen. Viele - AWS Services verwenden , CloudWatch um Protokolle und Metriken zu protokollieren, zu überwachen und zu veröffentlichen, ohne dass eine weitere Konfiguration erforderlich ist. CloudWatch bietet einen Software-Agenten, der für verschiedene OSs und Umgebungen installiert und konfiguriert werden kann. In den folgenden Abschnitten wird beschrieben, wie Sie den CloudWatch Agenten für mehrere Konten, Regionen und Konfigurationen bereitstellen, installieren und konfigurieren:

Themen

Verwenden von CloudWatch in zentralen oder verteilten Konten

Obwohl für die Überwachung von AWS Services oder Ressourcen in einem Konto und einer Region konzipiert CloudWatch ist, können Sie ein zentrales Konto verwenden, um Protokolle und Metriken aus mehreren Konten und Regionen zu erfassen. Wenn Sie mehr als ein Konto oder eine Region verwenden, sollten Sie prüfen, ob Sie den zentralisierten Kontoansatz oder ein einzelnes Konto verwenden möchten, um Protokolle und Metriken zu erfassen. In der Regel ist ein hybrider Ansatz für Bereitstellungen mit mehreren Konten und Regionen erforderlich, um die Anforderungen von Sicherheits-, Analyse-, Betriebs- und Workload-Besitzern zu erfüllen.

Die folgende Tabelle enthält Bereiche, die Sie bei der Auswahl eines zentralen, verteilten oder hybriden Ansatzes berücksichtigen sollten.

Kontostrukturen	Ihre Organisation verfügt möglicherweise über mehrere separate Konten (z. B. Konten für Nicht-Produktions- und Produktions-Workloads) oder Tausende von Konten für einzelne Anwendung en in bestimmten Umgebungen. Wir empfehlen Ihnen, Anwendung sprotokolle und Metriken in dem Konto zu verwalten, in dem der Workload ausgeführt wird, wodurch Workload-Eigentümer Zugriff auf die Protokolle und Metriken erhalten. Auf diese Weise können sie eine aktive Rolle bei der Protokollierung und Überwachung haben. Wir empfehlen außerdem, ein separates Protokollierungskonto zu verwenden, um alle Workload-Protokolle für Analysen, Aggregati on, Trends und zentralisierte Vorgänge zu aggregieren. Separate Protokollierungskonten können auch für Sicherheit, Archivierung und Überwachung sowie Analysen verwendet werden.
Zugriffsanforderungen	Teammitglieder (z. B. Workload-Besitzer oder Entwickler) benötigen Zugriff auf Protokolle und Metriken, um Fehler zu beheben und Verbesserungen vorzunehmen. Protokolle sollten im Konto des Workloads verwaltet werden, um den Zugriff und die Fehlerbeh

	ebung zu erleichtern. Wenn Protokolle und Metriken in einem vom Workload getrennten Konto verwaltet werden, müssen Benutzer möglicherweise regelmäßig zwischen Konten wechseln. Die Verwendung eines zentralen Kontos stellt Protokollinformationen für autorisierte Benutzer bereit, ohne Zugriff auf das Workload-Konto zu gewähren. Dies kann die Zugriffsanforderungen für analytische Workloads vereinfachen, bei denen eine Aggregation von Workloads erforderlich ist, die in mehreren Konten ausgeführt werden. Das zentrale Protokollierungskonto kann auch alternative Such- und Aggregationsoptionen haben, z. B. einen Amazon- OpenSearch Service-Cluster. Amazon OpenSearch Service bietet eine differenzierte Zugriffskontrolle bis auf Feldebene für Ihre Protokolle. Eine differenzierte Zugriffskontrolle ist wichtig, wenn Sie über sensible oder vertrauliche Daten verfügen, die einen speziellen Zugriff und spezielle Berechtigungen erfordern.
Operationen	Viele Organisationen verfügen über ein zentrales Betriebs- und Sicherheitsteam oder eine externe Organisation für operative Unterstützung, die Zugriff auf Protokolle für die Überwachung erfordert. Zentralisierte Protokollierung und Überwachung kann es einfacher machen, Trends zu identifizieren, zu suchen, zu aggregieren und Analysen für alle Konten und Workloads durchzuführen. Wenn Ihre Organisation den Ansatz „Sie erstellen es, führen es aus“ für verwendet DevOps, benötigen Workload-Besitzer Protokollierungs- und Überwachungsinformationen in ihrem Konto. Ein hybrider Ansatz kann erforderlich sein, um zusätzlich zur Eigentümerschaft verteilter Workloads zentrale Abläufe und Analysen zu erfüllen.

Umgebung	Sie können wählen, ob Protokolle und Metriken an einem zentralen Ort für Produktionskonten gehostet und Protokolle und Metriken für andere Umgebungen (z. B. Entwicklung oder Tests) in denselben oder separaten Konten aufbewahrt werden sollen, je nach Sicherheitsanforderungen und Kontoarchitektur. Dadurch wird verhindert, dass vertrauliche Daten, die während der Produktion erstellt wurden, von einem breiteren Publikum abgerufen werden.

CloudWatch bietet mehrere Optionen zur Verarbeitung von Protokollen in Echtzeit mit CloudWatch Abonnementfiltern. Sie können Abonnementfilter verwenden, um Protokolle in Echtzeit zur benutzerdefinierten Verarbeitung, Analyse und zum Laden in andere Systeme an - AWS Services zu streamen. Dies kann besonders hilfreich sein, wenn Sie einen hybriden Ansatz wählen, bei dem Ihre Protokolle und Metriken zusätzlich zu einem zentralen Konto und einer Region in einzelnen Konten und Regionen verfügbar sind. Die folgende Liste enthält Beispiele für - AWS Services, die dafür verwendet werden können:

- Amazon Data Firehose – Firehose bietet eine Streaming-Lösung, die basierend auf dem erzeugten Datenvolumen automatisch skaliert und in der Größe geändert wird. Sie müssen die Anzahl der Shards in einem Amazon Kinesis Data Stream nicht verwalten und können sich ohne zusätzliche Codierung direkt mit Amazon Simple Storage Service (Amazon S3), Amazon OpenSearch Service oder Amazon Redshift verbinden. Firehose ist eine effektive Lösung, wenn Sie Ihre Protokolle in diesen AWS Services zentralisieren möchten.
- Amazon Kinesis Data Streams – Kinesis Data Streams ist eine geeignete Lösung, wenn Sie in einen Service integrieren müssen, den Firehose nicht unterstützt, und zusätzliche Verarbeitungslogik implementieren. Sie können ein Amazon- CloudWatch Logs-Ziel in Ihren Konten und Regionen erstellen, das einen Kinesis-Datenstrom in einem zentralen Konto und eine AWS Identity and Access Management (IAM)-Rolle angibt, die ihm die Berechtigung erteilt, Datensätze in den Stream zu platzieren. Kinesis Data Streams bietet eine flexible, offene Landing Zone für Ihre Protokolldaten, die dann von verschiedenen Optionen genutzt werden können. Sie können die Protokolldaten von Kinesis Data Streams in Ihrem Konto lesen, eine Vorverarbeitung durchführen und die Daten an das von Ihnen gewählte Ziel senden.

  Sie müssen jedoch die Shards für den Stream so konfigurieren, dass er für die erzeugten Protokolldaten angemessen dimensioniert ist. Kinesis Data Streams fungiert als temporärer Zwischen- oder Warteschlange für Ihre Protokolldaten, und Sie können die Daten zwischen

einem und 365 Tagen im Kinesis-Stream speichern. Kinesis Data Streams unterstützt auch Wiedergabefunktionen, was bedeutet, dass Sie Daten wiedergeben können, die nicht verbraucht wurden.

- Amazon OpenSearch Service – CloudWatch Protokolle können Protokolle in einer Protokollgruppe an einen - OpenSearch Cluster in einem einzelnen oder zentralisierten Konto streamen. Wenn Sie eine Protokollgruppe zum Streamen von Daten an einen - OpenSearch Cluster konfigurieren, wird eine Lambda-Funktion im selben Konto und in derselben Region wie Ihre Protokollgruppe erstellt. Die Lambda-Funktion muss über eine Netzwerkverbindung mit dem OpenSearch Cluster verfügen. Sie können die Lambda-Funktion anpassen, um eine zusätzliche Vorverarbeitung durchzuführen, zusätzlich zur Anpassung der Aufnahme in Amazon OpenSearch Service. Die zentralisierte Protokollierung mit Amazon OpenSearch Service erleichtert die Analyse, Suche und Behebung von Problemen über mehrere Komponenten in Ihrer Cloud-Architektur hinweg.
- Lambda – Wenn Sie Kinesis Data Streams verwenden, müssen Sie Rechenressourcen bereitstellen und verwalten, die Daten aus Ihrem Stream verbrauchen. Um dies zu vermeiden, können Sie Protokolldaten direkt zur Verarbeitung an Lambda streamen und basierend auf Ihrer Logik an ein Ziel senden. Das bedeutet, dass Sie keine Rechenressourcen bereitstellen und verwalten müssen, um eingehende Daten zu verarbeiten. Wenn Sie Lambda verwenden möchten, stellen Sie sicher, dass Ihre Lösung mit den Lambda-Kontingenten kompatibel ist.

Möglicherweise müssen Sie Protokolldaten, die in - CloudWatch Protokollen gespeichert sind, im Dateiformat verarbeiten oder freigeben. Sie können eine Exportaufgabe erstellen, um eine Protokollgruppe für ein bestimmtes Datum oder einen bestimmten Zeitraum nach Amazon S3 zu exportieren. Sie können beispielsweise festlegen, dass Protokolle täglich zu Analyse- und Prüfungszwecken nach Amazon S3 exportiert werden sollen. Lambda kann verwendet werden, um diese Lösung zu automatisieren. Sie können diese Lösung auch mit der Amazon S3-Replikation kombinieren, um Ihre Protokolle von mehreren Konten und Regionen an ein zentrales Konto und eine zentrale Region zu senden und zu zentralisieren.

Die CloudWatch Agentenkonfiguration kann auch ein `credentials` Feld im `agent` Abschnitt angeben. Dies gibt eine IAM-Rolle an, die beim Senden von Metriken und Protokollen an ein anderes Konto verwendet werden soll. Falls angegeben, enthält dieses Feld den `role_arn` Parameter . Dieses Feld kann nur verwendet werden, wenn Sie eine zentrale Protokollierung und Überwachung in einem bestimmten zentralen Konto und einer bestimmten Region benötigen.

Sie können AWS SDK auch verwenden, um Ihre eigene benutzerdefinierte Verarbeitungsanwendung in einer Sprache Ihrer Wahl zu schreiben, Protokolle und Metriken aus Ihren Konten zu lesen und

Daten zur weiteren Verarbeitung und Überwachung an ein zentrales Konto oder ein anderes Ziel zu senden.

Verwalten von CloudWatch Agentenkonfigurationsdateien

Wir empfehlen Ihnen, eine Standardkonfiguration für Amazon- CloudWatch Agenten zu erstellen, die die Systemprotokolle und Metriken enthält, die Sie für alle Ihre Amazon Elastic Compute Cloud (Amazon EC2)-Instances und On-Premises-Server erfassen möchten. Sie können den Assistenten für CloudWatch Agentenkonfigurationsdateien verwenden, um die Konfigurationsdatei zu erstellen. Sie können den Konfigurationsassistenten mehrmals ausführen, um eindeutige Konfigurationen für verschiedene Systeme und Umgebungen zu generieren. Sie können auch die Konfigurationsdatei ändern oder Variationen erstellen, indem Sie das Konfigurationsdateischema verwenden. Die CloudWatch Agentenkonfigurationsdatei kann in den Parametern des AWS Systems Manager Parameter Store gespeichert werden. Sie können separate Parameterspeicherparameter erstellen, wenn Sie mehrere CloudWatch Agentenkonfigurationsdateien haben. Wenn Sie mehrere AWS-Konten oder AWS-Regionen verwenden, müssen Sie die Parameter Store-Parameter in jedem Konto und jeder Region verwalten und aktualisieren. Alternativ können Sie Ihre CloudWatch Konfigurationen zentral als Dateien in Amazon S3 oder einem Versionskontroll-Tool Ihrer Wahl verwalten.

Mit dem CloudWatch im Agenten enthaltenen `amazon-cloudwatch-agent-ctl`Skript können Sie eine Konfigurationsdatei, einen Parameter Store-Parameter oder die Standardkonfiguration des Agenten angeben. Die Standardkonfiguration entspricht dem grundlegenden, vordefinierten Metriksatz und konfiguriert den Agenten so, dass er Speicher- und Festplattenspeichermetriken an meldet CloudWatch. Sie enthält jedoch keine Protokolldateikonfigurationen. Die Standardkonfiguration wird auch angewendet, wenn SieSystems Manager Quick Setup für den CloudWatch Agenten verwenden.

Da die Standardkonfiguration keine Protokollierung beinhaltet und nicht an Ihre Anforderungen angepasst ist, empfehlen wir Ihnen, Ihre eigenen CloudWatch Konfigurationen zu erstellen und anzuwenden, die an Ihre Anforderungen angepasst sind.

Verwalten von CloudWatch Konfigurationen

Standardmäßig können CloudWatch Konfigurationen als Parameter Store-Parameter oder als CloudWatch Konfigurationsdateien gespeichert und angewendet werden. Die beste Wahl hängt von Ihren Anforderungen ab. In diesem Abschnitt behandeln wir die Vor- und Nachteile dieser beiden Optionen. Eine repräsentative Lösung wird auch für die Verwaltung von CloudWatch Konfigurationsdateien für mehrere AWS-Konten und AWS-Regionen detailliert beschrieben.

Systems Manager Parameter Store-Parameter

Die Verwendung von Parameter Store-Parametern zur Verwaltung von CloudWatch Konfigurationen funktioniert gut, wenn Sie über eine einzelne Standard- CloudWatch Agentenkonfigurationsdatei verfügen, die Sie in einem kleinen Satz von AWS-Konten und -Regionen anwenden und verwalten möchten. Wenn Sie Ihre CloudWatch Konfigurationen als Parameter Store-Parameter speichern, können Sie das CloudWatch Agent-Konfigurationstool (`amazon-cloudwatch-agent-ctl` unter Linux) verwenden, um die Konfiguration aus Parameter Store zu lesen und anzuwenden, ohne dass Sie die Konfigurationsdatei auf Ihre Instance kopieren müssen. Sie können das Befehlsdokument AmazonCloudWatch-ManageAgent Systems Manager verwenden, um die CloudWatch Konfiguration auf mehreren EC2-Instances in einer einzigen Ausführung zu aktualisieren. Da Parameter Store-Parameter regional sind, müssen Sie Ihre CloudWatch Parameter Store-Parameter in jeder AWS-Region und jedem AWS-Konto aktualisieren und verwalten. Wenn Sie mehrere CloudWatch Konfigurationen haben, die Sie auf jede Instance anwenden möchten, müssen Sie das AmazonCloudWatch-ManageAgentBefehlsdokument so anpassen, dass es diese Parameter enthält.

CloudWatch -Konfigurationsdateien

Die Verwaltung Ihrer CloudWatch Konfigurationen als Dateien funktioniert möglicherweise gut, wenn Sie viele AWS-Konten und -Regionen haben und mehrere CloudWatch Konfigurationsdateien verwalten. Mit diesem Ansatz können Sie sie in einer Ordnerstruktur durchsuchen, organisieren und verwalten. Sie können Sicherheitsregeln auf einzelne Ordner oder Dateien anwenden, um den Zugriff einzuschränken und zu gewähren, z. B. Aktualisierungs- und Leseberechtigungen. Sie können sie für die Zusammenarbeit außerhalb von AWS freigeben und übertragen. Sie können die Dateien versionskontrollieren, um Änderungen zu verfolgen und zu verwalten. Sie können CloudWatch Konfigurationen insgesamt anwenden, indem Sie die Konfigurationsdateien in das CloudWatch Agentenkonfigurationsverzeichnis kopieren, ohne jede Konfigurationsdatei einzeln anzuwenden. Für Linux finden Sie das CloudWatch Konfigurationsverzeichnis unter `/opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d`. Für Windows finden Sie das Konfigurationsverzeichnis unter `C:\ProgramData\Amazon\AmazonCloudWatchAgent\Configs`.

Wenn Sie den CloudWatch Agenten starten, hängt der Agent automatisch jede in diesen Verzeichnissen gefundene Datei an, um eine CloudWatch zusammengesetzte Konfigurationsdatei zu erstellen. Die Konfigurationsdateien sollten an einem zentralen Ort (z. B. einem S3-Bucket) gespeichert werden, auf den Ihre erforderlichen Konten und Regionen zugreifen können. Eine Beispiellösung, die diesen Ansatz verwendet, wird bereitgestellt.

Organisieren von CloudWatch Konfigurationen

Organisieren Sie Ihre CloudWatch Konfigurationen unabhängig von dem Ansatz, der zur Verwaltung Ihrer CloudWatch Konfigurationen verwendet wird. Sie können Ihre Konfigurationen mithilfe eines Ansatzes wie dem folgenden in Datei- oder Parameterspeicherpfaden organisieren.

/config/standard/windows/ec2	Speichern Sie Windows-spezifische CloudWatch Standardkonfigurationsdateien für Amazon EC2. Sie können Ihre Standardbetriebssystemkonfigurationen (OS) für verschiedene Windows-Versionen, EC2-Instance-Typen und Umgebungen in diesem Ordner weiter kategorisieren.
/config/standard/windows/onpremises	Speichern Sie Windows-spezifische CloudWatch Standardkonfigurationsdateien für On-Premises-Server. Sie kategorisieren auch Ihre Standardbetriebssystemkonfigurationen für verschiedene Windows-Versionen, Servertypen und Umgebungen in diesem Ordner weiter.
/config/standard/linux/ec2	Speichern Sie Ihre Linux-spezifischen CloudWatch Standardkonfigurationsdateien für Amazon EC2. Sie können Ihre Standard-Betriebssystemkonfiguration für verschiedene Linux-Distributionen, EC2-Instance-Typen und Umgebungen in diesem Ordner weiter kategorisieren.
/config/standard/linux/onpremises	Speichern Sie Ihre Linux-spezifischen CloudWatch Standardkonfigurationsdateien für On-Premises-Server. Sie können Ihre Standard-Betriebssystemkonfiguration für verschiedene Linux-Verteilungen, Servertypen und Umgebungen in diesem Ordner weiter kategorisieren.

/config/ecs	Speichern Sie CloudWatch Konfigurationsdateien, die für Amazon Elastic Container Service (Amazon ECS) spezifisch sind, wenn Sie Amazon-ECS-Container-Instances verwenden. Diese Konfigurationen können an die Amazon EC2-Standardkonfigurationen für die Amazon-ECS-spezifische Protokollierung und Überwachung auf Systemebene angehängt werden.
/config/<application_name>	Speichern Sie Ihre anwendungsspezifischen CloudWatch Konfigurationsdateien. Sie können Ihre Anwendungen mit zusätzlichen Ordnern und Präfixen für Umgebungen und Versionen weiter kategorisieren.

Beispiel: Speichern von CloudWatch Konfigurationsdateien in einem S3-Bucket

Dieser Abschnitt enthält ein Beispiel für die Verwendung von Amazon S3 zum Speichern CloudWatch von Konfigurationsdateien und ein benutzerdefiniertes Systems Manager-Runbook zum Abrufen und Anwenden der CloudWatch Konfigurationsdateien. Dieser Ansatz kann einige der Herausforderungen bei der Verwendung von Systems Manager Parameter Store-Parametern für CloudWatch die Konfiguration in großem Umfang bewältigen:

- Wenn Sie mehrere Regionen verwenden, müssen Sie Konfigurationsaktualisierungen im Parameterspeicher jeder Region synchronisieren CloudWatch. Parameter Store ist ein regionaler Service und derselbe Parameter muss in jeder Region aktualisiert werden, die den CloudWatch Agenten verwendet.
- Wenn Sie mehrere CloudWatch Konfigurationen haben, müssen Sie den Abruf und die Anwendung jeder Parameter Store-Konfiguration einleiten. Sie müssen jede CloudWatch Konfiguration einzeln aus dem Parameter Store abrufen und auch die Abrufmethode aktualisieren, wenn Sie eine neue Konfiguration hinzufügen. Im Gegensatz dazu CloudWatch stellt ein Konfigurationsverzeichnis zum Speichern von Konfigurationsdateien bereit und wendet jede Konfiguration im Verzeichnis an, ohne dass sie einzeln angegeben werden müssen.

- Wenn Sie mehrere Konten verwenden, müssen Sie sicherstellen, dass jedes neue Konto über die erforderlichen CloudWatch Konfigurationen in seinem Parameter Store verfügt. Sie müssen auch sicherstellen, dass alle Konfigurationsänderungen in Zukunft auf diese Konten und ihre Regionen angewendet werden.

Sie können CloudWatch Konfigurationen in einem S3-Bucket speichern, auf den von allen Ihren Konten und Regionen aus zugegriffen werden kann. Anschließend können Sie diese Konfigurationen mithilfe von Systems Manager Automation-Runbooks und Systems Manager State Manager aus dem S3-Bucket in das CloudWatch Konfigurationsverzeichnis kopieren. Sie können die AWS-CloudFormation Vorlage cloudwatch-config-s3-bucket.yaml verwenden, um einen S3-Bucket zu erstellen, auf den von mehreren Konten innerhalb einer Organisation in AWS Organizations aus zugegriffen werden kann. Die Vorlage enthält einen -`OrganizationID`Parameter, der allen Konten innerhalb Ihrer Organisation Lesezugriff gewährt.

Das erweiterte Systems Manager-Beispiel-Runbook, das im Abschnitt Einrichten von State Manager und Distributor für die Bereitstellung und Konfiguration von CloudWatch Kundendienstmitarbeitern dieses Handbuchs bereitgestellt wird, ist so konfiguriert, dass Dateien mit dem S3-Bucket abgerufen werden, der mit der AWS CloudFormation-Vorlage cloudwatch-config-s3-bucket.yaml erstellt wurde.

Alternativ können Sie ein Versionsverwaltungssystem (z. B. oder AWS CodeCommit) verwenden, GitHub um Ihre Konfigurationsdateien zu speichern. Wenn Sie Konfigurationsdateien, die in einem Versionsverwaltungssystem gespeichert sind, automatisch abrufen möchten, müssen Sie die Speicherung der Anmeldeinformationen verwalten oder zentralisieren und das Systems Manager Automation-Runbook aktualisieren, das zum Abrufen der Anmeldeinformationen in Ihren Konten und Regionen verwendet wird.

Konfigurieren von CloudWatch -Agenten für EC2-Instances und lokale Server

Viele Organisationen führen Workloads sowohl auf physischen Servern als auch auf virtuellen Maschinen (VMs) aus. Diese Workloads werden normalerweise auf verschiedenen Betriebssystemen ausgeführt, die jeweils einzigartige Installations- und Konfigurationsanforderungen für die Erfassung und Aufnahme von Metriken haben.

Wenn Sie sich für die Verwendung von EC2-Instanzen entscheiden, können Sie ein hohes Maß an Kontrolle über Ihre Instance- und Betriebssystemkonfiguration haben. Dieses höhere Maß an Kontrolle und Verantwortung erfordert jedoch, dass Sie Konfigurationen überwachen und anpassen, um eine effizientere Nutzung zu erreichen. Sie können Ihre betriebliche Effektivität verbessern, indem Sie Standards für die Protokollierung und Überwachung festlegen und einen standardmäßigen Installations- und Konfigurationsansatz für die Erfassung und Aufnahme von Protokollen und Metriken anwenden.

Organizations, die ihre IT-Investitionen migrieren oder auf dieAWSCloud kann nutzen CloudWatch um eine einheitliche Protokollierungs- und Überwachungslösung zu erreichen. CloudWatch Preisgestaltung bedeutet, dass Sie schrittweise für die Metriken und Protokolle bezahlen, die Sie erfassen möchten. Sie können auch Protokolle und Metriken für lokale Server erfassen, indem Sie einen ähnlichen CloudWatch Agent-Installationsprozess wie für Amazon EC2.

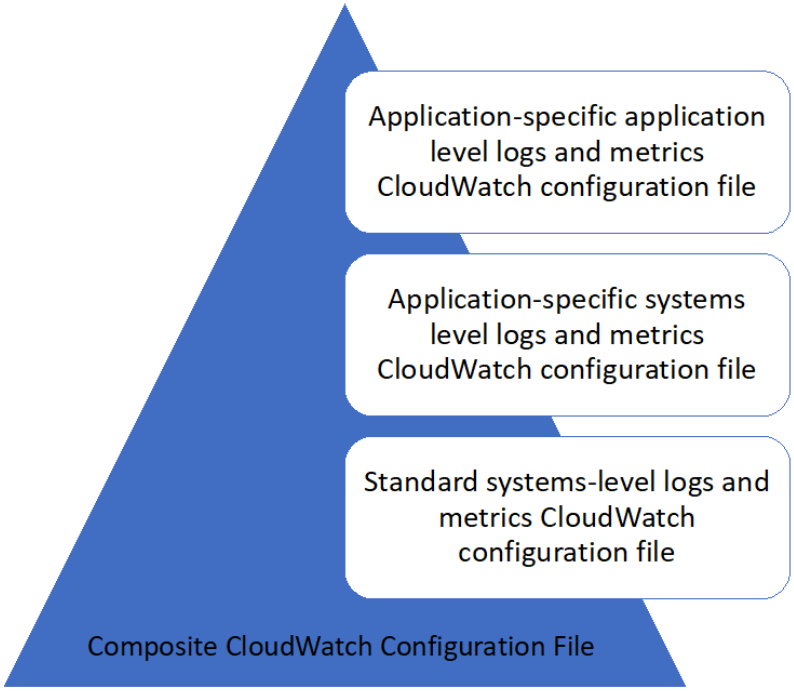
Bevor Sie mit der Installation und Bereitstellung von CloudWatch beginnen, stellen Sie sicher, dass Sie die Protokollierungs- und Metrikkonfigurationen für Ihre Systeme und Anwendungen auswerten. Stellen Sie sicher, dass Sie die Standardprotokolle und Metriken definieren, die Sie für die zu verwendenden Betriebssysteme erfassen müssen. Systemprotokolle und Metriken sind Grundlage und Standard für eine Protokollierungs- und Überwachungslösung, da sie vom Betriebssystem generiert werden und für Linux und Windows unterschiedlich sind. Neben solchen, die für eine Linux-Version oder Distribution spezifisch sind, stehen wichtige Metriken und Protokolldateien für Linux-Distributionen zur Verfügung. Diese Varianz tritt auch zwischen verschiedenen Windows-Versionen auf.

Konfigurieren von CloudWatch Agentin

CloudWatch-Server erfasst mithilfe von Metriken und Protokollen für Amazon EC2 und lokale ServerCloudWatch-Agenten und Agent-Konfigurationsdateiendie für jedes Betriebssystem spezifisch

sind. Wir empfehlen Ihnen, die Standardmetrik und die Protokollerfassungskonfiguration Ihres Unternehmens zu definieren, bevor Sie mit der Installation des CloudWatch Agent im großen Maßstab in Ihren Konten.

Sie können mehrere kombinieren CloudWatch Agent-Konfigurationen zur Bildung eines Composite CloudWatch Agent-Konfiguration. Ein empfohlener Ansatz besteht darin, Konfigurationen für Ihre Protokolle und Metriken auf System- und Anwendungsebene zu definieren und zu teilen. Das folgende Diagramm zeigt, wie mehrere CloudWatch-Konfigurationsdateitypen für verschiedene Anforderungen kombiniert werden können, um eine zusammengesetzte CloudWatch-Konfiguration zu bilden:



Diese Protokolle und Metriken können auch weiter klassifiziert und für bestimmte Umgebungen oder Anforderungen konfiguriert werden. Beispielsweise könnten Sie eine kleinere Teilmenge von Protokollen und Metriken mit geringerer Genauigkeit für unregulierte Entwicklungsumgebungen und einen größeren, vollständigeren Satz mit höherer Präzision für regulierte Produktionsumgebungen definieren.

Konfigurieren der Protokollerfassung für EC2-Instances

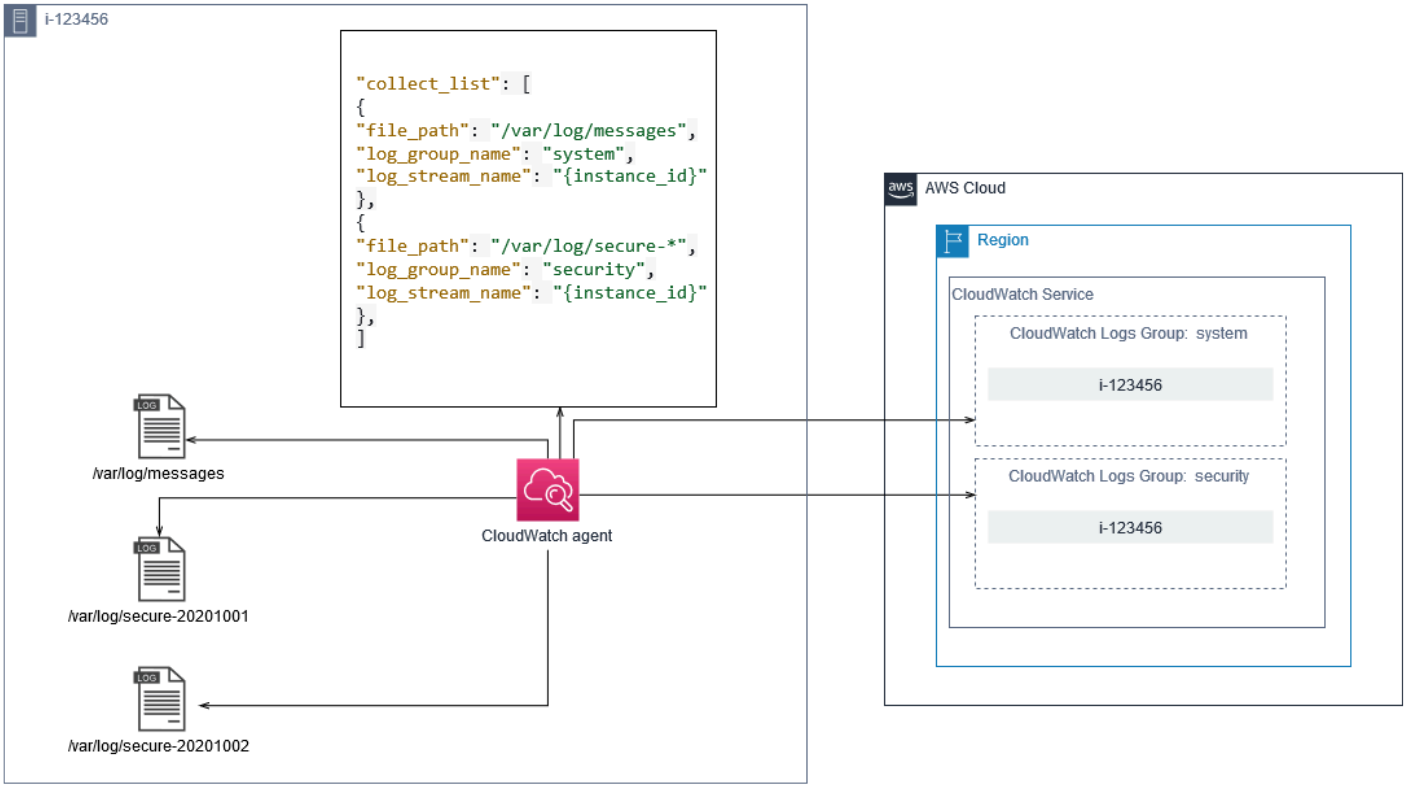
Standardmäßig überwacht oder erfasst Amazon EC2 keine Protokolldateien. Stattdessen werden Protokolldateien erfasst und aufgenommen CloudWatch Logs von der CloudWatch Auf Ihrer EC2-Instance installierte AgentsoftwareAWSAPI oderAWS Command Line Interface(AWS CLI) enthalten. Wir empfehlen die Verwendung von CloudWatch Agent zum Aufnehmen von Protokolldateien CloudWatch Protokollen für Amazon EC2 und lokale Server.

Sie können Protokolle suchen und filtern sowie Metriken extrahieren und die Automatisierung basierend auf Muster-Patching aus Protokolldateien in CloudWatch ausführen. CloudWatch unterstützt Klartext, durch Leerzeichen getrennte und JSON-formatierte Filter- und Mustersyntaxoptionen, wobei JSON-formatierte Protokolle die größte Flexibilität bieten. Um die Filter- und Analyseoptionen zu erhöhen, sollten Sie anstelle von Klartext eine formatierte Protokollausgabe verwenden.

Die CloudWatch Agent verwendet eine Konfigurationsdatei, die die Protokolle und Metriken definiert, die an CloudWatch gesendet werden sollen. CloudWatch erfasst dann jede Protokolldatei alsProtokollstreamund gruppiert diese Log-Streams in einProtokollgruppeaus. Dies hilft Ihnen, Vorgänge über Protokolle Ihrer EC2-Instanzen hinweg auszuführen, z. B. die Suche nach einer übereinstimmenden Zeichenfolge.

Der Standardname des Protokollstreams entspricht der EC2-Instanz-ID und der Standardname der Protokollgruppe entspricht dem Pfad der Protokolldatei. Der Name des Protokollstreams muss innerhalb des CloudWatch Protokollgruppe. Sie können verwenden`instance_id`,`hostname`,`local_hostname`, oder`ip_address`für die dynamische Substitution im Log-Stream und Log-Gruppennamen, was bedeutet, dass Sie dasselbe verwenden können CloudWatch Agent-Konfigurationsdatei über mehrere EC2-Instances hinweg.

Das folgende Diagramm zeigt eine CloudWatch Agent-Konfiguration zum Erfassen von Protokollen. Die Protokollgruppe wird durch die erfassten Protokolldateien definiert und enthält separate Log-Streams für jede EC2-Instanz, da die`{instance_id}`wird für den Namen des Protokollstreams verwendet, und EC2-Instanz-IDs sind eindeutig.



Protokollgruppen definieren die Aufbewahrung, die Tags, die Sicherheit, die Metrikfilter und den Suchbereich für die darin enthaltenen Protokollstreams. Das Standardgruppierungsverhalten basierend auf dem Namen der Protokolldatei hilft Ihnen, Metriken zu suchen, zu erstellen und Daten zu alarmieren, die für eine Protokolldatei in EC2-Instanzen in einem Konto und einer Region spezifisch sind. Sie sollten prüfen, ob eine weitere Verfeinerung der Protokollgruppe erforderlich ist. Beispielsweise kann Ihr Konto von mehreren Geschäftseinheiten geteilt werden und hat unterschiedliche technische oder betriebliche Eigentümer. Dies bedeutet, dass Sie den Namen der Protokollgruppe weiter verfeinern müssen, um die Trennung und den Besitz widerzuspiegeln. Mit diesem Ansatz können Sie Ihre Analyse und Fehlerbehebung auf die relevante EC2-Instanz konzentrieren.

Wenn mehrere Umgebungen ein Konto verwenden, können Sie die Protokollierung für Workloads trennen, die in jeder Umgebung ausgeführt werden. Die folgende Tabelle zeigt eine Namenskonvention für Protokollgruppen, die die Geschäftseinheit, das Projekt oder die Anwendung und die Umgebung umfasst.

Protokollgruppenname	`/<Business unit>/<Project or application name>/<Environment>/<Log file name>`
Protokoll-Streamname	`<EC2 instance ID>`

Sie können auch alle Protokolldateien für eine EC2-Instanz in derselben Protokollgruppe gruppieren. Dies erleichtert das Suchen und Analysieren in einer Reihe von Protokolldateien nach einer einzelnen EC2-Instanz. Dies ist nützlich, wenn die meisten Ihrer EC2-Instanzen eine Anwendung oder Workload bedienen und jede EC2-Instanz einem bestimmten Zweck dient. Die folgende Tabelle zeigt, wie die Benennung Ihrer Protokollgruppe und des Protokollstreams formatiert werden kann, um diesen Ansatz zu unterstützen.

Protokollgruppenname	`/<Business unit>/<Project or application name>/<Environment>/<EC2 instance ID>`
Protokoll-Streamname	`<Log file name>`

Konfigurieren der Metrikerfassung für EC2-Instances

Standardmäßig sind Ihre EC2-Instances für die grundlegende Überwachung und eineStandardsatz von Metriken(z. B. CPU-, Netzwerk- oder speicherbezogene Metriken) wird automatisch an gesendet CloudWatch alle fünf Minuten. CloudWatch Die Metriken können je nach Instance-Familie variieren, z. B.Instances mit Spitzenlastleistunghaben Metriken für CPU-Credits. Amazon EC2 EC2-Standardmetriken sind in Ihrem Instance-Preis enthalten. Wenn Sie aktivierenDetaillierte ÜberwachungFür Ihre EC2-Instances können Sie Daten in Zeiträumen von einer Minute erhalten. Die Periodenfrequenz wirkt sich auf Ihre CloudWatch-Kosten aus. Stellen Sie daher sicher, dass Sie prüfen, ob eine detaillierte Überwachung für alle oder nur einige Ihrer EC2-Instanzen erforderlich ist. Sie könnten beispielsweise eine detaillierte Überwachung für Produktionsworkloads aktivieren, aber die grundlegende Überwachung für Workloads außerhalb der Produktion verwenden.

Lokale Server enthalten keine Standardmetriken für CloudWatch und muss das CloudWatch -Agent,AWS CLI, oderAWSSDK zur Erfassung von Metriken. Dies bedeutet, dass Sie die Metriken definieren müssen, die Sie erfassen möchten (z. B. CloudWatch Konfigurationsdatei. Sie können ein Unikat erstellen CloudWatch Konfigurationsdatei, die die Standard-EC2-Instance-Metriken für Ihre lokalen Server enthält und sie zusätzlich zu Ihrem Standard anwendet CloudWatch -Konfiguration.

Metrikenin CloudWatch sind eindeutig durch den Metriknamen und null oder mehrere Dimensionen definiert und sind eindeutig in einem Metriknamespace gruppiert. Metriken, die von einemAWS-Dienst hat einen Namespace, der mit beginntAWS(zum BeispielAWS/EC2), und nicht-AWS-Metriken gelten als benutzerdefinierte Metriken. Metriken, die Sie mit dem CloudWatch Agent gelten alle als benutzerdefinierte Metriken. Weil sich die Anzahl der erstellten Metriken auf Ihre CloudWatch Kosten sollten Sie bewerten, ob jede Metrik für alle oder nur einige Ihrer EC2-Instanzen erforderlich ist. Sie könnten beispielsweise einen vollständigen Satz von Metriken für Produktions-Workloads definieren, aber eine kleinere Teilmenge dieser Metriken für Workloads außerhalb der Produktion verwenden.

CWAgentist der Standardnamespace für Metriken, die von der CloudWatch -Agent. Ähnlich wie bei Protokollgruppen organisiert der Metrik-Namespace eine Reihe von Metriken, sodass sie an einer Stelle zusammen gefunden werden können. Sie sollten den Namespace so ändern, dass er eine Geschäftseinheit, ein Projekt oder eine Anwendung und eine Umgebung widerspiegelt (z. B./<Business unit>/<Project or application name>/<Environment>) enthalten. Dieser Ansatz ist nützlich, wenn mehrere nicht verwandte Workloads dasselbe Konto verwenden. Sie können Ihre Namespace-Benennungskonvention auch mit Ihrer CloudWatch Namenskonvention für Protokollgruppen

Metriken werden auch durch ihre Dimensionen identifiziert, die Ihnen helfen, sie anhand einer Reihe von Bedingungen zu analysieren und die Eigenschaften sind, mit denen Beobachtungen aufgezeichnet werden. Amazon EC2 enthältSeparate Metrikenfür EC2-Instances mitInstanceIdundAutoScalingGroupName-Dimensionen Sie erhalten auch Metriken mit demImageIdundInstanceType-Bemaßungen, wenn Sie die detaillierte Überwachung aktivieren. Amazon EC2 bietet beispielsweise eine separate EC2-Instance-Metrik für die CPU-Auslastung mit demInstanceIdDimensionen zusätzlich zur separaten CPU-Auslastungsmetrik für dieInstanceType-Dimension. Dies hilft Ihnen, die CPU-Auslastung für jede eindeutige EC2-Instanz zu analysieren, zusätzlich zu allen EC2-Instanzen einer bestimmtenInstance-Typaus.

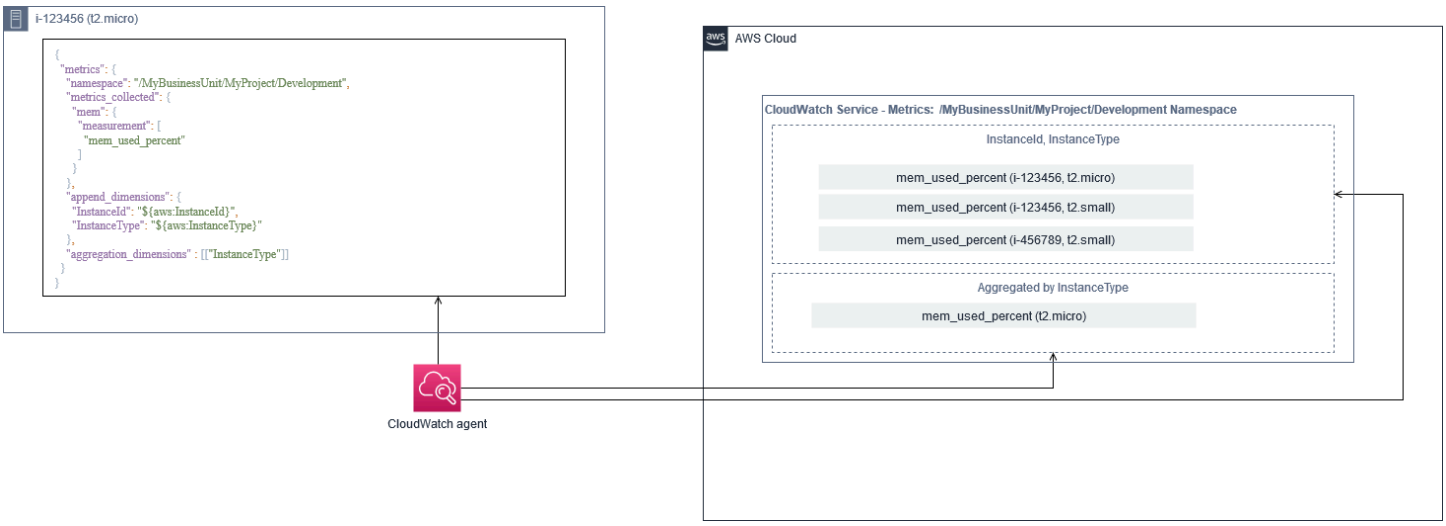
Das Hinzufügen weiterer Dimensionen erhöht Ihre Analysefähigkeit, erhöht aber auch Ihre Gesamtkosten, da jede Metrik und jede Kombination aus eindeutigen Dimensionswerten zu einer neuen Metrik führt. Wenn Sie beispielsweise eine Metrik für den Prozentsatz der Speicherauslastung gegenüber demInstanceIddimension, dann ist dies eine neue Metrik für jede EC2-Instanz. Wenn

Ihre Organisation Tausende von EC2-Instanzen ausführt, führt dies zu Tausenden von Metriken und führt zu höheren Kosten. Um Kosten zu kontrollieren und vorherzusagen, stellen Sie sicher, dass Sie die Kardinalität der Metrik bestimmen und welche Dimensionen den größten Wert bieten. Sie könnten beispielsweise einen vollständigen Satz von Dimensionen für Ihre Produktionsworkload-Metriken definieren, aber eine kleinere Teilmenge dieser Dimensionen für Workloads außerhalb der Produktion.

Sie können das`append_dimensions`Eigenschaft zum Hinzufügen von Dimensionen zu einer oder allen Metriken, die in Ihrem CloudWatch -Konfiguration. Sie können auch dynamisch das`ImageId`,`InstanceId`,`InstanceType`, und`AutoScalingGroupName`zu allen Metriken in Ihrem CloudWatch -Konfiguration. Alternativ können Sie einen beliebigen Dimensionsnamen und einen Wert für bestimmte Metriken anhängen, indem Sie die`append_dimensions`Eigenschaft für diese Metrik. CloudWatch kann auch Statistiken über metrische Dimensionen aggregieren, die Sie mit dem`aggregation_dimensions`eigentum.

Beispielsweise können Sie den verwendeten Speicher mit dem`InstanceType`dimension, um den durchschnittlichen Speicher zu sehen, der von allen EC2-Instanzen für jeden Instance-Typ verwendet wird. Bei Verwendung`t2.micro`Instanzen, die in einer Region ausgeführt werden, können Sie feststellen, ob Workloads mit der`t2.micro`Klasse belasten oder unterlastet den bereitgestellten Speicher. Eine Unterauslastung kann ein Zeichen dafür sein, dass Workloads EC2-Klassen mit nicht benötigter Speicherkapazität verwenden. Im Gegensatz dazu kann eine Überauslastung ein Zeichen dafür sein, dass Workloads Amazon EC2-Klassen mit unzureichendem Speicher verwenden.

Das folgende Diagramm zeigt ein Beispiel CloudWatch Metrikkonfiguration, die einen benutzerdefinierten Namespace, hinzugefügte Dimensionen und Aggregation von`InstanceType`aus.



System-Level CloudWatch Aufbau

Metriken und Protokolle auf Systemebene sind ein zentraler Bestandteil einer Überwachungs- und Protokollierungslösung, und die CloudWatch Agent verfügt über spezifische Konfigurationsoptionen für Windows und Linux.

Wir empfehlen Ihnen, zu verwenden.CloudWatch-Konfigurationsdatei-Assistentoder Konfigurationsdatei-Schema zur Definition des CloudWatch Agent-Konfigurationsdatei für jedes Betriebssystem, das Sie unterstützen möchten. Zusätzliche Workload-spezifische Protokolle und Metriken auf Betriebssystemebene können separat definiert werden CloudWatch Konfigurationsdateien und an die Standardkonfiguration angehängt. Diese eindeutigen Konfigurationsdateien sollten separat in einem S3-Bucket gespeichert werden, wo sie von Ihren EC2-Instanzen abgerufen werden können. Ein Beispiel für ein S3-Bucket-Setup zu diesem Zweck ist imVerwalten von CloudWatch KonfigurationenAbschnitt dieses Handbuchs. Sie können diese Konfigurationen automatisch mit State Manager und Distributor abrufen und anwenden.

Konfigurieren von Protokollen auf Systemebene

Protokolle auf Systemebene sind für die Diagnose und Behebung von Problemen vor Ort oder auf derAWSCloud. Ihr Log-Capture-Ansatz sollte alle vom Betriebssystem generierten System- und Sicherheitsprotokolle enthalten. Die vom Betriebssystem generierten Protokolldateien können je nach der Betriebssystemversion unterschiedlich sein.

Die CloudWatch Agent unterstützt die Überwachung von Windows-Ereignisprotokollen durch Angabe des Ereignisprotokollnamens. Sie können auswählen, welche Windows-Ereignisprotokolle Sie überwachen möchten (z. B.`System`,`Application`, oder`Security`) enthalten.

Die System-, Anwendungs- und Sicherheitsprotokolle für Linux-Systeme werden normalerweise im`/var/log`-Verzeichnis. In der folgenden Tabelle werden die allgemeinen Standardprotokolldateien definiert, die Sie überwachen sollten, aber Sie sollten die`/etc/rsyslog.conf`oder`/etc/syslog.conf`-Datei, um das spezifische Setup für die Protokolldateien Ihres Systems zu ermitteln.

Fedora Verteilung (Amazon Linux, CentOS, Red Hat Enterprise Linux)	`/var/log/boot.log*` - Bootup-Protokoll
	`/var/log/dmesg` - Kernelprotokoll
	`/var/log/secure` — Sicherheits- und Authentifizierungsprotokoll

	`/var/log/messages` - Allgemeines Systemprotokoll
	`/var/log/cron*` - Cron-Protokolle
	`/var/log/cloud-init-output.log` - Ausgabe von`Userdata`Startup-Skripts
Debian (Ubuntu)	`/var/log/syslog` - Bootup-Protokoll
	`/var/log/cloud-init-output.log` - Ausgabe von`Userdata`Startup-Skripts
	`/var/log/auth.log` — Sicherheits- und Authentifizierungsprotokoll
	`/var/log/kern.log` - Kernelprotokoll

Ihre Organisation verfügt möglicherweise auch über andere Agenten oder Systemkomponenten, die Protokolle generieren, die Sie überwachen möchten. Sie sollten auswerten und entscheiden, welche Protokolldateien von diesen Agenten oder Anwendungen generiert werden, und sie in Ihre Konfiguration aufnehmen, indem Sie ihren Dateispeicherort identifizieren. Zum Beispiel sollten Sie den Systems Manager und CloudWatch Agent meldet sich in Ihrer Konfiguration an. Die folgende Tabelle enthält den Speicherort dieser Agentprotokolle für Windows und Linux.

Windows	CloudWatch-Agent	`$Env:ProgramData\Amazon\AmazonCloudWatchAgent\Logs\amazon-cloudwatch-agent.log`

	Der -Agent des Systems	`%PROGRAMDATA%\Amazon\SSM\Logs\amazon-ssm-agent.log`
		
		`%PROGRAMDATA%\Amazon\SSM\Logs\errors.log`

		%PROGRAMDATA%\Amazon\SSM\Logs\audits\amazon-ssm-agent-audit-YYYY-MM-DD
Linux	CloudWatch-Agent	/opt/aws/amazon-cloudwatch-agent/logs/amazon-cloudwatch-agent.log
	Der -Agent des Systems	/var/log/amazon/ssm/amazon-ssm-agent.log /var/log/amazon/ssm/errors.log /var/log/amazon/ssm/audits/amazon-ssm-agent-audit-YYYY-MM-DD

CloudWatch ignoriert eine Protokolldatei, wenn die Protokolldatei im CloudWatch Agent-Konfiguration wurde aber nicht gefunden. Dies ist nützlich, wenn Sie eine einzelne Protokollkonfiguration für Linux beibehalten möchten, anstelle von separaten Konfigurationen für jede Distribution. Es ist auch nützlich, wenn eine Protokolldatei erst existiert, wenn der Agent oder die Softwareanwendung ausgeführt wird.

Konfigurieren von Metriken auf Systemebene

Die Auslastung von Speicher und Festplattenspeicher sind nicht in Standardmetriken enthalten, die von Amazon EC2 bereitgestellt werden. Um diese Metriken einzubeziehen, müssen Sie die CloudWatch Agent auf Ihren EC2-Instanzen. Die CloudWatch Der Assistent für den Agent-Konfiguration erstellt CloudWatch Konfiguration mitVordefinierte Metrikenund Sie können Metriken nach Bedarf hinzufügen oder entfernen. Stellen Sie sicher, dass Sie die vordefinierten Metriksätze überprüfen, um die entsprechende Ebene zu ermitteln, die Sie benötigen.

Endbenutzer und Workload-Besitzer sollten zusätzliche Systemmetriken basierend auf spezifischen Anforderungen für einen Server oder eine EC2-Instance veröffentlichen. Diese Metrikdefinitionen

sollten in einem separaten Bereich gespeichert, versioniert und gepflegt werden CloudWatch Agent-Konfigurationsdatei, die an einem zentralen Ort (z. B. Amazon S3) zur Wiederverwendung und Automatisierung freigegeben wird.

Standardmetriken von Amazon EC2 werden nicht automatisch auf lokalen Servern erfasst. Diese Metriken müssen in einem CloudWatch Agent-Konfigurationsdatei, die von den lokalen Instanzen verwendet wird. Sie können eine separate Metrikkonfigurationsdatei für lokale Instanzen mit Metriken wie der CPU-Auslastung erstellen und diese Metriken an die Konfigurationsdatei für Standardmetriken angehängt haben.

Anwendungsebene CloudWatch Aufbau

Anwendungsprotokolle und Metriken werden durch ausgeführte Anwendungen generiert und sind anwendungsspezifisch. Stellen Sie sicher, dass Sie die Protokolle und Metriken definieren, die erforderlich sind, um Anwendungen, die regelmäßig von Ihrer Organisation verwendet werden, angemessen zu überwachen. Beispielsweise hat Ihre Organisation möglicherweise auf Microsoft Internet Information Server (IIS) für webbasierte Anwendungen standardisiert. Sie können ein Standardprotokoll und eine Metrik erstellen CloudWatch Konfiguration für IIS, die auch in Ihrem gesamten Unternehmen verwendet werden kann. Anwendungsspezifische Konfigurationsdateien können an einem zentralen Ort (z. B. einem S3-Bucket) gespeichert werden und werden von Workload-Besitzern oder durch automatisierten Abruf zugegriffen und in die CloudWatch -Konfigurationsverzeichnis. Die CloudWatch Agent kombiniert CloudWatch-Konfigurationsdateien im Konfigurationsdateiverzeichnis jeder EC2-Instanz oder Server automatisch zu einem Composite CloudWatch -Konfiguration. Das Endergebnis ist ein CloudWatch Konfiguration, die die Standardkonfiguration Ihrer Organisation auf Systemebene sowie alle relevanten Anwendungsebene umfasst CloudWatch -Konfigurationen.

Workload-Besitzer sollten Protokolldateien und Metriken für alle kritischen Anwendungen und Komponenten identifizieren und konfigurieren.

Konfigurieren von Logs auf Anwendungsebene

Die Protokollierung auf Anwendungsebene hängt davon ab, ob es sich bei der Anwendung um einen kommerziellen off-the-shelf (COTS) oder kundenspezifisch entwickelte Anwendung. COTS-Anwendungen und ihre Komponenten bieten möglicherweise mehrere Optionen für die Protokollkonfiguration und -ausgabe, z. B. die Protokolldetailebene, das Protokolldateiformat und den Speicherort der Protokolldatei. Die meisten COTS- oder Drittanbieter-Anwendungen

erlauben es Ihnen jedoch nicht, die Protokollierung grundlegend zu ändern (z. B. um den Code der Anwendung so zu aktualisieren, dass er zusätzliche Protokollanweisungen oder Formate enthält, die nicht konfigurierbar sind). Zumindest sollten Sie Protokollierungsoptionen für COTS- oder Drittanbieteranwendungen konfigurieren, um Warn- und Fehlerinformationen zu protokollieren, vorzugsweise im JSON-Format.

Sie können kundenspezifische Anwendungen mit integrieren CloudWatch Protokolliert, indem Sie die Protokolldateien der Anwendung in Ihre CloudWatch -Konfiguration. Benutzerdefinierte Anwendungen bieten eine bessere Protokollqualität und -kontrolle, da Sie das Protokollausgabeformat anpassen, die Komponentenausgabe kategorisieren und in separate Protokolldateien trennen können, zusätzlich zu zusätzlichen erforderlichen Details. Stellen Sie sicher, dass Sie die Protokollierungsbibliotheken und die erforderlichen Daten und Formatierungen für Ihr Unternehmen überprüfen und standardisieren, damit die Analyse und Verarbeitung einfacher werden.

Sie können auch an CloudWatch Protokollstream mit CloudWatch Protokolle`PutLogEvents`API-Aufruf oder mithilfe desAWS-SDK. Sie können die API oder das SDK für benutzerdefinierte Protokollierungsanforderungen verwenden, z. B. die Koordinierung der Protokollierung in einem einzelnen Protokollstream über einen verteilten Satz von Komponenten und Servern hinweg. Die am einfachsten zu wartende und am weitesten verbreitete Lösung besteht jedoch darin, Ihre Anwendungen so zu konfigurieren, dass sie in Protokolldateien schreiben und dann die CloudWatch Agent zum Lesen und Streamen der Protokolldateien an CloudWatch.

Sie sollten auch die Art von Metriken berücksichtigen, die Sie aus Ihren Anwendungsprotokolldateien messen möchten. Sie können Metrikfilter verwenden, um diese Daten in einem CloudWatch Protokollgruppe. Sie können beispielsweise einen Metrikfilter verwenden, um fehlgeschlagene Anmeldeversuche zu zählen, indem Sie sie in Ihren Protokollen identifizieren.

Sie können auch benutzerdefinierte Metriken für Ihre maßgeschneiderten Anwendungen erstellen, indem Sie dieCloudWatch-eingebettete MetrikenFormatin Ihren Anwendungsprotokolldateien.

Konfigurieren von Metriken auf Anwendungsebene

Benutzerdefinierte Metriken sind Metriken, die nicht direkt von bereitgestellt werdenAWS-Services zu CloudWatch und sie werden in einem benutzerdefinierten Namespace in CloudWatch -Metriken. Alle Anwendungsmetriken gelten als benutzerdefiniert CloudWatch -Metriken. Anwendungsmetriken können an einer EC2-Instanz, einer Anwendungskomponente, einem API-Aufruf oder sogar einer Geschäftsfunktion ausgerichtet sein. Sie müssen auch die Bedeutung und Kardinalität der Dimensionen berücksichtigen, die Sie für Ihre Kennzahlen auswählen. Dimensionen mit hoher

Kardinalität erzeugen eine große Anzahl benutzerdefinierter Metriken und könnten Ihre CloudWatch Kosten nachzuverfolgen.

CloudWatch hilft Ihnen, Metriken auf Anwendungsebene auf verschiedene Arten zu erfassen, einschließlich der folgenden:

- Erfassen Sie Metriken auf Prozessebene, indem Sie die einzelnen Prozesse definieren, die Sie aus demprocstat-Plug-Inaus.
- Eine Anwendung veröffentlicht eine Metrik in Windows Performance Monitor und diese Metrik ist im CloudWatch -Konfiguration.
- Metrikfilter und -muster werden auf die Protokolle einer Anwendung in CloudWatch angewendet.
- Eine Anwendung schreibt in eine CloudWatch Protokollieren Sie mithilfe der CloudWatch eingebettetes Metrikformat.
- Eine Anwendung sendet eine Metrik an CloudWatch durch die API oderAWS-SDK.
- Eine Anwendung sendet eine Metrik an eineCollectdoderStatsDDaemon mit einem konfigurierten CloudWatch -Agent.

Sie können procstat verwenden, um kritische Anwendungsprozesse mit dem CloudWatch-Agent zu überwachen und zu messen. Dies hilft Ihnen, einen Alarm auszulösen und Maßnahmen zu ergreifen (z. B. einen Benachrichtigungs- oder Neustartprozess), wenn für Ihre Anwendung kein kritischer Prozess mehr ausgeführt wird. Sie können auch die Leistungsmerkmale Ihrer Anwendungsprozesse messen und einen Alarm auslösen, wenn ein bestimmter Prozess ungewöhnlich wirkt.

Die Procstat-Überwachung ist auch nützlich, wenn Sie Ihre COTS-Anwendungen nicht mit zusätzlichen benutzerdefinierten Metriken aktualisieren können. Beispielsweise können Sie einem`_process`Metrik, die die`cpu_time`und beinhaltet einen Brauch`application_version`-Dimension. Sie können auch mehrere verwenden CloudWatch Agent-Konfigurationsdateien für eine Anwendung, wenn Sie unterschiedliche Dimensionen für verschiedene Metriken haben.

Wenn Ihre Anwendung unter Windows ausgeführt wird, sollten Sie prüfen, ob sie bereits Metriken in Windows Performance Monitor veröffentlicht. Viele COTS-Anwendungen sind in Windows Performance Monitor integriert, mit dem Sie Anwendungsmetriken einfach überwachen können. CloudWatch lässt sich auch in den Windows Performance Monitor integrieren und Sie können alle Metriken erfassen, die bereits darin verfügbar sind.

Stellen Sie sicher, dass Sie das Protokollierungsformat und die Protokollinformationen Ihrer Anwendungen überprüfen, um festzustellen, welche Metriken mit Metrikfiltern extrahiert werden

können. Sie können historische Protokolle für die Anwendung überprüfen, um festzustellen, wie Fehlermeldungen und abnormale Shutdowns dargestellt werden. Sie sollten auch zuvor gemeldete Probleme überprüfen, um festzustellen, ob eine Metrik erfasst werden könnte, um ein Wiederauftreten des Problems zu verhindern. Sie sollten auch die Dokumentation der Anwendung überprüfen und die Anwendungsentwickler bitten, zu bestätigen, wie Fehlermeldungen identifiziert werden können.

Arbeiten Sie für maßgeschneiderte Anwendungen mit den Entwicklern der Anwendung zusammen, um wichtige Metriken zu definieren, die mithilfe der CloudWatch eingebettetes Metrikformat,AWSSDK-Dateien oderAWSAPI. Der empfohlene Ansatz ist die Verwendung des eingebetteten Metrikformats. Sie können dasAWSBereitstellung von Open-Source-Bibliotheken im eingebetteten Metrikformat, mit denen Sie Ihre Anweisungen im erforderlichen Format schreiben können. Sie müssen auch Ihre aktualisierenanwendungsspezifisch CloudWatch Aufbauum den -Agenten im eingebetteten Metrikformat einzuschließen Dies führt dazu, dass der Agent, der auf der EC2-Instanz ausgeführt wird, als lokaler Endpunkt im eingebetteten Metrikformat fungiert, der Metriken im eingebetteten Metrikformat an CloudWatch sendet.

Wenn Ihre Anwendungen bereits das Veröffentlichen von Metriken für collectd oder statsd unterstützen, können Sie sie nutzen, um Metriken in CloudWatch aufzunehmen.

Installationsansätze für CloudWatch Agent für Amazon EC2 und lokale Server

Automatisieren des CloudWatch Der Installationsprozess des Agenten hilft Ihnen, ihn schnell und konsequent bereitzustellen und die erforderlichen Protokolle und Metriken zu erfassen. Es gibt verschiedene Ansätze zur Automatisierung der Installation des CloudWatch Agents, einschließlich Unterstützung für mehrere Konten und mehrere Regionen. Die folgenden automatisierten Installationsansätze werden diskutiert:

- Installieren von CloudWatch Agent unter Verwendung von Systems Manager Distributor und Systems Manager State Manager— Wir empfehlen, diesen Ansatz zu verwenden, wenn Ihre EC2-Instances und lokalen Server den Systems Manager -Agent ausführen. Dies stellt sicher, dass der CloudWatch Agent wird auf dem neuesten Stand gehalten und Sie können über Server berichten und sie beheben, die nicht über CloudWatch -Agent. Dieser Ansatz wird auch skaliert, um mehrere Konten und Regionen zu unterstützen.
- Bereitstellen der CloudWatch Agent als Teil des Benutzerdatenskripts während der EC2-Instanzbereitstellung— Mit Amazon EC2 können Sie ein Startskript definieren, das beim ersten Start oder Neustart ausgeführt wird. Sie können ein Skript definieren, um den Download- und Installationsprozess des Agenten zu automatisieren. Dies kann auch in einbezogen werdenAWS CloudFormationSkripts undAWSService Catalog Produkte. Dieser Ansatz kann bei Bedarf angemessen sein, wenn für eine bestimmte Arbeitslast, die von Ihren Standards abweicht, einen benutzerdefinierten Installations- und Konfigurationsansatz des Agents gibt.
- Einbeziehen des CloudWatch-Agenten in Amazon Machine Images (AMI)— Sie können den CloudWatch-Agent in Ihren benutzerdefinierten AMIs für Amazon EC2 installieren. Bei den EC2-Instanzen, die das AMI verwenden, wird der Agent automatisch installiert und gestartet. Sie müssen jedoch sicherstellen, dass der Agent und seine Konfiguration regelmäßig aktualisiert werden.

Installieren von CloudWatch -Agent mit Systems Manager Distributor und State Manager

Sie können Systems Manager State Manager mit Systems Manager Distributor verwenden, um die CloudWatch Agent auf Servern und EC2-Instanzen. Der Distributor umfasst

die`AmazonCloudWatchAgent` AWSverwaltetes Paket, das die neueste Version des CloudWatch Agent installiert.

Für diesen Installationsansatz müssen die folgenden Voraussetzungen erfüllt sein:

- Der Systems Manager -Agent muss installiert sein und auf Servern oder EC2-Instances ausgeführt werden. Der Systems Manager Manager-Agent ist unter Amazon Linux, Amazon Linux 2 und einigen AMIs vorinstalliert. Der Agent muss auch auf anderen Images oder lokalen VMs und Servern installiert und konfiguriert sein.
- Eine IAM-Rolle oder Anmeldeinformationen, die dieerforderlich CloudWatch und Systems Manager Manager-Berechtigungenmuss an die EC2-Instance angefügt oder in der Anmeldeinformationen für einen lokalen Server definiert sein. Sie können beispielsweise eine IAM-Rolle erstellen, dieAWSVerwaltete Richtlinien:`AmazonSSMManagedInstanceCore`für Systems Manager und`CloudWatchAgentServerPolicy`für CloudWatch. Sie können dasssm-cloudwatch-instance-role.yaml AWS CloudFormation-Vorlage für die Bereitstellung einer IAM-Rolle und eines Instance-Profils, das beide Richtlinien enthält. Diese Vorlage kann auch so geändert werden, dass sie andere IAM-Standardberechtigungen für Ihre EC2-Instanzen enthält. Für lokale Server oder VMs sollte die CloudWatch Der -Agent zur Verwendung desSystems Manager Manager-Dienstrolledas für den lokalen Server konfiguriert wurde. Weitere Informationen hierzu finden Sie unterWie kann ich lokale Server konfigurieren, die den Systems Manager Agent und den Unified verwenden CloudWatch Agent, um nur temporäre Anmeldeinformationen zu verwenden?imAWSKnowledge Center.

Die folgende Liste bietet mehrere Vorteile für die Verwendung des Systems Manager Distributor und State Manager-Ansatzes zur Installation und Wartung des CloudWatch -Agent:

- Automatisierte Installation für mehrere Betriebssysteme— Sie müssen nicht für jedes Betriebssystem ein Skript schreiben und pflegen, um den CloudWatch-Agent herunterzuladen und zu installieren.
- Automatische Update-Prüfungen— State Manager überprüft automatisch und regelmäßig, ob jede EC2-Instanz über die neueste CloudWatch-Version verfügt.
- Compliance-Berichte— Das Compliance-Dashboard von Systems Manager zeigt an, welche EC2-Instanzen das Distributor-Paket nicht erfolgreich installiert haben.
- Automatisierte Installation für neu gestartete EC2-Instanzen- Neue EC2-Instanzen, die in Ihr Konto eingeleitet werden, erhalten automatisch die CloudWatch -Agent.

Sie sollten jedoch auch die folgenden drei Bereiche berücksichtigen, bevor Sie sich für diesen Ansatz entscheiden:

- Kollision mit einer bestehenden Assoziation— Wenn eine andere Assoziation bereits installiert oder konfiguriert CloudWatch Agent, dann könnten sich die beiden Assoziationen gegenseitig stören und möglicherweise Probleme verursachen. Wenn Sie diesen Ansatz verwenden, sollten Sie alle vorhandenen Zuordnungen entfernen, die den CloudWatch-Agent und die Konfiguration installieren oder aktualisieren.
- Aktualisieren von benutzerdefinierten Agent-Konfigurationsdateien— Der Distributor führt eine Installation mithilfe der Standardkonfigurationsdatei durch. Wenn Sie eine benutzerdefinierte Konfigurationsdatei oder mehrere verwenden CloudWatch Konfigurationsdateien müssen Sie die Konfiguration nach der Installation aktualisieren.
- Einrichtung von mehreren Regionen oder mehreren Konten— Der Staatsverwalterverband muss in jedem Konto und in jeder Region eingerichtet sein. Neue Konten in einer Umgebung mit mehreren Konten müssen aktualisiert werden, um die Zuordnung des State Managers einzubeziehen. Sie müssen das CloudWatch Konfiguration, damit mehrere Konten und Regionen Ihre erforderlichen Standards abrufen und anwenden können.

Einrichten von State Manager und Distributor für CloudWatch Bereitstellung und Konfiguration von Agenten

Sie können verwendenSystems Manager Manager-Schnelleinrichtungum Systems Manager Manager-Funktionen schnell zu konfigurieren, einschließlich der automatischen Installation und Aktualisierung des CloudWatch Agent auf Ihren EC2-Instanzen. Das Quick Setup stellt einAWS CloudFormationStack, der Systems Manager Manager-Ressourcen basierend auf Ihren Entscheidungen bereitstellt und konfiguriert.

Die folgende Liste enthält zwei wichtige Aktionen, die von Quick Setup für automatisierte CloudWatch Installation und Update des Agents:

1. Benutzerdefinierte Dokumente von Systems Manager erstellen— Quick Setup erstellt die folgenden Systems Manager Manager-Dokumente zur Verwendung mit State Manager. Die Dokumentnamen können variieren, aber der Inhalt bleibt gleich:
   - `CreateAndAttachIAMToInstance`— Erzeugt das`AmazonSSMRoleForInstancesQuickSetup`Rollen- und Instanzprofil, wenn sie nicht existieren und hängt das`AmazonSSMManagedInstanceCore`-Richtlinie zur Rolle. Dies

beinhaltet nicht die erforderlichen`CloudWatchAgentServerPolicy`IAM-Richtlinie. Sie müssen diese Richtlinie aktualisieren und dieses Systems Manager Manager-Dokument aktualisieren, um diese Richtlinie wie im folgenden Abschnitt beschrieben aufzunehmen.

- `InstallAndManageCloudWatchDocument`— Installiert das CloudWatch Agent mit Distributor und konfiguriert jede EC2-Instanz einmal mit einem Standardwert CloudWatch Agent-Konfiguration mithilfe der`AWS-ConfigureAWSPackage`Systems Manager Manager-Dokument.
- `UpdateCloudWatchDocument`— Aktualisiert das CloudWatch -Agent, indem Sie den neuesten CloudWatch-Agent mithilfe der`AWS-ConfigureAWSPackage`Systems Manager Manager-Dokument. Durch das Aktualisieren oder Deinstallieren des Agenten wird der vorhandene nicht entfernt CloudWatch Konfigurationsdateien von der EC2-Instance.

2. Zuordnungsstatus in State Manager erstellen— State Manager-Zuordnungen werden erstellt und konfiguriert, um die benutzerdefinierten Systems Manager Manager-Dokumente zu verwenden. Die Zuordnungsnamen des State Managers können variieren, aber die Konfiguration bleibt gleich:
   - `ManageCloudWatchAgent`— Führt den`InstallAndManageCloudWatchDocument`Systems Manager dokumentiert einmal für jede EC2-Instanz.
   - `UpdateCloudWatchAgent`— Führt den`UpdateCloudWatchDocument`Systems Manager dokumentiert alle 30 Tage für jede EC2-Instanz.
   - Führt das aus`CreateAndAttachIAMToInstance`Systems Manager dokumentiert einmal für jede EC2-Instanz.

Sie müssen die abgeschlossene Schnell-Setup-Konfiguration erweitern und anpassen, um CloudWatch-Berechtigungen und benutzerdefinierte Unterstützung einzuschließen CloudWatch Konfigurationen. Insbesondere der`CreateAndAttachIAMToInstance`und die`InstallAndManageCloudWatchDocument`das Dokument muss aktualisiert werden. Sie können die von Quick Setup erstellten Systems Manager Manager-Dokumente manuell aktualisieren. Alternativ können Sie Ihre eigene verwenden CloudFormation Vorlage, um dieselben Ressourcen mit den erforderlichen Updates bereitzustellen sowie andere Systems Manager Manager-Ressourcen zu konfigurieren und bereitzustellen und nicht Quick Setup zu verwenden.

> **Important**
>
> Schnelleinrichtung erstellt eine AWS CloudFormationstapeln, um Systems Manager Manager-Ressourcen basierend auf Ihren Entscheidungen bereitzustellen und zu konfigurieren. Wenn

Sie Ihre Schnell-Setup-Optionen aktualisieren, müssen Sie möglicherweise die Systems Manager Manager-Dokumente manuell erneut aktualisieren.

In den folgenden Abschnitten wird beschrieben, wie Sie die von Quick Setup erstellten Systems Manager Manager-Ressourcen manuell aktualisieren und Ihre eigenen verwendenAWS CloudFormationVorlage, um ein aktualisiertes Schnell-Setup durchzuführen. Wir empfehlen, dass Sie Ihre eigene verwendenAWS CloudFormationVorlage zur Vermeidung manueller Aktualisierung von Ressourcen, die von Quick Setup erstellt wurdenAWS CloudFormationaus.

Verwenden Sie den Systems Manager Quick Setup und aktualisieren Sie die erstellten Systems Manager Manager-Ressourcen manuell

Die durch den Schnell-Setup-Ansatz erstellten Systems Manager Manager-Ressourcen müssen aktualisiert werden, um die erforderlichen CloudWatch Agentenberechtigungen und Unterstützung mehrere CloudWatch Konfigurationsdateien. In diesem Abschnitt wird beschrieben, wie Sie die IAM-Rolle und die Systems Manager Manager-Dokumente aktualisieren, um einen zentralisierten S3-Bucket zu verwenden CloudWatch Konfigurationen, auf die von mehreren Konten aus zugegriffen werden kann. Erstellen eines S3-Buckets, um die zu speichern CloudWatch Konfigurationsdateien werden in derVerwalten von CloudWatch KonfigurationenAbschnitt dieses Handbuchs.

Aktualisieren des**`CreateAndAttachIAMToInstance`**Systems Manager Manager-Dokument

Dieses von Quick Setup erstellte Systems Manager Manager-Dokument prüft, ob an eine EC2-Instanz ein vorhandenes IAM-Instanzprofil angehängt ist. Wenn ja, hängt es die`AmazonSSMManagedInstanceCore`Richtlinie zur bestehenden Rolle. Dies schützt Ihre bestehenden EC2-Instances vor VerlustAWSBerechtigungen, die möglicherweise über vorhandene Instanzprofile zugewiesen werden. Sie müssen einen Schritt in diesem Dokument hinzufügen, um die`CloudWatchAgentServerPolicy`IAM-Richtlinie für EC2-Instanzen, denen bereits ein Instanzprofil angehängt ist. Das Systems Manager Manager-Dokument erstellt auch die IAM-Rolle, wenn sie nicht existiert und an eine EC2-Instanz kein Instanzprofil angehängt ist. Sie müssen diesen Abschnitt des Dokuments aktualisieren, um auch die`CloudWatchAgentServerPolicy`IAM-Richtlinie.

Prüfen Sie das AbgeschlosseneCreateandAttachiamToInstance.YAMLBeispieldokument und vergleichen Sie es mit dem von Quick Setup erstellten Dokument. Bearbeiten Sie das vorhandene

Dokument so, dass es die erforderlichen Schritte und Änderungen enthält. Basierend auf den Auswahlmöglichkeiten für die Schnelleinrichtung unterscheidet sich das von Quick Setup erstellte Dokument möglicherweise von dem bereitgestellten Beispieldokument. Stellen Sie daher sicher, dass Sie die erforderlichen Anpassungen vornehmen. Das Beispieldokument enthält die Option Quick Setup, um Instanzen täglich auf fehlende Patches zu scannen, und enthält daher eine Richtlinie für Systems Manager Patch Manager.

Aktualisieren des**`InstallAndManageCloudWatchDocument`**Systems Manager Manager-Dokument

Dieses von Quick Setup erstellte Systems Manager Manager-Dokument installiert die CloudWatch Agent und konfiguriert es mit dem Standardwert CloudWatch Agent-Konfiguration. Der CloudWatch -Konfiguration richtet sich an der grundlegenden, vordefinierten Metrikmenge aus. Sie müssen den Standardkonfigurationsschritt ersetzen und Schritte hinzufügen, um Ihre CloudWatch Konfigurationsdateien von Ihrem CloudWatch Konfiguration S3-Bucket.

Prüfen Sie das AbgeschlosseneInstallandManageCloudWatchDocument.YAMLhat das Dokument aktualisiert und mit dem von Quick Setup erstellten Dokument verglichen. Das von Ihrem Quick Setup erstellte Dokument kann unterschiedlich sein. Stellen Sie daher sicher, dass Sie die erforderlichen Anpassungen vorgenommen haben. Bearbeiten Sie Ihr vorhandenes Dokument so, dass es die erforderlichen Schritte und Änderungen enthält.

Verwenden vonAWS CloudFormationstatt Schnelleinrichtung

Anstatt die -Schnelleinrichtung zu verwenden, können Sie verwendenAWS CloudFormationum Systems Manager zu konfigurieren. Mit diesem Ansatz können Sie Ihre Systems Manager Manager-Konfiguration an Ihre spezifischen Anforderungen anpassen. Dieser Ansatz vermeidet auch manuelle Aktualisierungen der konfigurierten Systems Manager Manager-Ressourcen, die von Quick Setup zur Unterstützung von benutzerdefinierten CloudWatch Konfigurationen.

Die Quick Setup-Funktion verwendet auchAWS CloudFormationund schafft einAWS CloudFormationStack wurde festgelegt, um Systems Manager Manager-Ressourcen basierend auf Ihren Entscheidungen bereitzustellen und zu konfigurieren. Bevor du benutzen kannstAWS CloudFormationStack-Sets, Sie müssen die IAM-Rollen erstellen, die vonAWS CloudFormation StackSets zur Unterstützung von Bereitstellungen über mehrere Konten oder Regionen hinweg. Quick Setup erstellt die Rollen, die für die Unterstützung von Bereitstellungen mit mehreren Regionen oder mehreren Konten erforderlich sindAWS CloudFormationStackSets. Sie müssen die Voraussetzungen erfüllen fürAWS CloudFormation StackSets wenn Sie Systems Manager

Manager-Ressourcen in mehreren Regionen oder mehreren Konten von einem einzigen Konto und einer Region aus konfigurieren und bereitstellen möchten. Weitere Informationen hierzu finden Sie unterVoraussetzungen für Stack-Set-OperationenimAWS CloudFormation-Dokumentation.

Prüfen Sie dasAWS-QuickSetup-SsmhostMGMt.yaml AWS CloudFormationVorlage für benutzerdefiniertes Schnelleinrichtung.

Sie sollten die Ressourcen und Fähigkeiten imAWS CloudFormationVorlage und nehmen Sie Anpassungen entsprechend Ihren Anforderungen vor. Sie sollten die Version steuernAWS CloudFormationVorlage, die Sie verwenden, und testen Sie Änderungen schrittweise, um das erforderliche Ergebnis zu bestätigen. Darüber hinaus sollten Sie Cloud-Sicherheitsüberprüfungen durchführen, um festzustellen, ob aufgrund der Anforderungen Ihres Unternehmens Richtlinienanpassungen erforderlich sind.

Bereitstellen des sAWS CloudFormationstapeln Sie in einem einzigen Testkonto und einer Region und führen Sie alle erforderlichen Testfälle durch, um das gewünschte Ergebnis anzupassen und zu bestätigen. Sie können Ihre Bereitstellung dann in mehreren Regionen in einem einzigen Konto und dann auf mehrere Konten und mehrere Regionen abschließen.

Benutzerdefiniertes Schnell-Setup in einem einzelnen Konto und einer RegionAWS CloudFormationstapeln

Wenn Sie nur ein einziges Konto und eine Region verwenden, können Sie das vollständige Beispiel alsAWS CloudFormationStack-Stack-Stack anstelle einesAWS CloudFormationStack-Sets. Wenn möglich, empfehlen wir Ihnen jedoch, den Stapelsatz für mehrere Konten und mehrere Regionen zu verwenden, auch wenn Sie nur ein einziges Konto und eine Region verwenden. benutzenAWS CloudFormation StackSets erleichtert die Erweiterung auf zusätzliche Konten und Regionen in future.

Führen Sie die folgenden Schritte aus, um dieAWS-QuickSetup-SsmhostMGMt.yaml AWS CloudFormation-Vorlage alsAWS CloudFormationStapel in einem einzigen Konto und einer Region:

1. Laden Sie die Vorlage herunter und checken Sie sie in Ihr bevorzugtes Versionskontrollsystem ein (z.AWS CodeCommit) enthalten.
2. Passen Sie den Standard anAWS CloudFormationParameterwerte basierend auf den Anforderungen Ihres Unternehmens.
3. Passen Sie die Zuordnungspläne des State Manager an.
4. Passen Sie das Systems Manager Manager-Dokument mit der`InstallAndManageCloudWatchDocument`Logische ID. Vergewissern Sie sich, dass die

S3-Bucket-Präfixe an den Präfixen für den S3-Bucket ausgerichtet sind, der Ihre CloudWatch -Konfiguration.

5. Rufen Sie den Amazon-Ressourcennamen (ARN) für den S3-Bucket ab und notieren Sie ihn CloudWatch Konfigurationen. Weitere Informationen hierzu finden Sie in derVerwalten von CloudWatch KonfigurationenAbschnitt in diesem Handbuch. Eine Stichprobecloudwatch-config-s3-bucket.yaml AWS CloudFormationVorlage ist verfügbar, die eine Bucket-Richtlinie enthält, auf die Lesezugriff bereitgestellt werden kannAWS OrganizationsKonten.
6. Bereitstellen des benutzerdefinierten Schnell-SetupsAWS CloudFormationVorlage für dasselbe Konto wie Ihr S3-Bucket:
   - Für den`CloudWatchConfigBucketARN`Geben Sie den ARN des S3-Buckets ein.
   - Nehmen Sie je nach den Funktionen, die Sie für Systems Manager aktivieren möchten, Anpassungen an den Parameteroptionen vor.

7. Stellen Sie eine Test-EC2-Instance mit und ohne IAM-Rolle bereit, um zu bestätigen, dass die EC2-Instanz mit CloudWatch funktioniert.

- Wenden Sie das an`AttachIAMToInstance`State Manager-Zuordnung. Dies ist ein Systems Manager Manager-Runbook, das so konfiguriert ist, dass es nach einem Zeitplan ausgeführt wird. State Manager-Zuordnungen, die Runbooks verwenden, werden nicht automatisch auf neue EC2-Instanzen angewendet und können so konfiguriert werden, dass sie planmäßig ausgeführt werden. Weitere Informationen finden Sie unterAusführen von Automationen mit Auslösern mithilfe von State Managerin der Systems Manager Manager-Dokumentation.
- Vergewissern Sie sich, dass der EC2-Instanz die erforderliche IAM-Rolle beigefügt ist.
- Vergewissern Sie sich, dass der Systems Manager-Agent ordnungsgemäß funktioniert, indem Sie bestätigen, dass die EC2-Instanz im Systems Manager sichtbar ist.
- Bestätigen Sie, dass der CloudWatch Agent funktioniert ordnungsgemäß durch Anzeigen CloudWatch Protokolle und Metriken basierend auf der CloudWatch Konfigurationen aus Ihrem S3-Bucket aus.

Benutzerdefiniertes Schnell-Setup in mehreren Regionen und KontenAWS CloudFormationStackSets

Wenn Sie mehrere Konten und Regionen verwenden, können Sie dieAWS-QuickSetup-SsmhostMGMt.yaml AWS CloudFormationVorlage als Stapelsatz. Sie müssen dasAWS

CloudFormationStackSet-Voraussetzungenbevor Sie Stack-Sets verwenden. Die Anforderungen variieren je nachdem, ob Sie Stack-Sets mitSelbstverwaltetoderService-verwaltetBerechtigungenaus.

Es wird empfohlen, Stack-Sets mit dienstverwalteten Berechtigungen bereitzustellen, damit neue Konten automatisch das benutzerdefinierte Quick Setup erhalten. Sie müssen einen serviceverwalteten Stack-Satz ausAWS OrganizationsVerwaltungskonto oder delegiertes Administratorkonto. Sie sollten den Stack-Satz von einem zentralisierten Konto bereitstellen, das für die Automatisierung verwendet wird, das Administratorrechte delegiert hat, anstatt dieAWS OrganizationsVerwaltungskonto. Wir empfehlen Ihnen auch, Ihre Stack-Set-Bereitstellung zu testen, indem Sie eine Testorganisationseinheit (OU) mit einer einzelnen oder kleinen Anzahl von Konten in einer Region ansprechen.

1. Führen Sie die Schritte 1 bis 5 von derBenutzerdefiniertes Schnell-Setup in einem einzelnen Konto und einer RegionAWS CloudFormationstapelnAbschnitt in diesem Handbuch.
2. Melden Sie sich beim anAWS Management ConsoleÖffnen Sie denAWS CloudFormationtröster und wählenErstellen Sie StackSet:
   - Klicken Sie aufVorlage ist bereitundHochladen einer Vorlagendabeiaus. Laden Sie dasAWS CloudFormation-Vorlage, die Sie an Ihre Anforderungen angepasst haben.
   - Geben Sie die Details des Stapelsatzes an:
     - Geben Sie einen Stack-Set-Namen ein, z. B.`StackSet-SSM-QuickSetup`aus.
     - Nehmen Sie je nach den Funktionen, die Sie für Systems Manager aktivieren möchten, Anpassungen an den Parameteroptionen vor.
     - Für den`CloudWatchConfigBucketARN`Geben Sie den ARN für Ihr ein CloudWatch Der S3-Bucket der Konfiguration.
     - Geben Sie die Stack-Set-Optionen an und wählen Sie aus, ob Sie serviceverwaltete Berechtigungen mitAWS Organizationsoder selbstverwaltete Berechtigungen.
       - Wenn Sie selbstverwaltete Berechtigungen wählen, geben Sie dieawsCloudFormationStackSetAdministrationRoleundawsCloudFormationStackSetExecutionRolel zur IAM-Rolle. Die Administratorrolle muss im Konto vorhanden sein und die Ausführungsrolle muss in jedem Zielkonto vorhanden sein
     - FürService-verwaltetBerechtigungen mitAWS OrganizationsWir empfehlen Ihnen, zuerst eine Test-Organisationseinheit anstelle der gesamten Organisation bereitzustellen.
       - Wählen Sie, ob Sie automatische Bereitstellungen aktivieren möchten. Wir empfehlen Ihnen, zu wählenEnabledaus. Für das Verhalten der Kontoentfernung ist die empfohlene EinstellungStacks löschenaus.

- FürSelbstverwaltetBerechtigungen, geben Sie dieAWSKonto-IDs für die Konten, die Sie einrichten möchten. Sie müssen diesen Vorgang für jedes neue Konto wiederholen, wenn Sie selbstverwaltete Berechtigungen verwenden.
- Geben Sie die Regionen ein, in denen Sie verwenden werden CloudWatch und Systems Manager.
- Bestätigen Sie, dass die Bereitstellung erfolgreich ist, indem Sie den Status imOperationen undStack-Instancesfür den Stapelsatz.
- Testen Sie diesen Systems Manager und CloudWatch arbeiten in den bereitgestellten Konten ordnungsgemäß, indem Sie Schritt 7 aus demBenutzerdefiniertes Schnell-Setup in einem einzelnen Konto und einer RegionAWS CloudFormationstapelnAbschnitt in diesem Handbuch.

Überlegungen zur Konfiguration von lokalen Servern

Die CloudWatch Agent für lokale Server und VMs wird unter Verwendung eines ähnlichen Ansatzes wie bei EC2-Instanzen installiert und konfiguriert. Die folgende Tabelle enthält jedoch Überlegungen, die Sie bei der Installation und Konfiguration des CloudWatch -Agent auf lokalen Servern und VMs.

Zeigen Sie auf CloudWatch Agent für dieselben temporären Anmeldeinformationen, die für Systems Manager verwendet werden.	Wenn Sie Systems Manager in einer Hybrid-Umgebung einrichten, die lokale Server enthält, können Sie den Systems Manager mit einer IAM-Rolle aktivieren. Sie sollten die für Ihre EC2-Instanzen erstellte Rolle verwenden, die`CloudWatchAgentServerPolicy` und`AmazonSSMManagedInstanceCore` Richtlinien. Dies führt dazu, dass der Systems Manager Manager-Agent temporäre Anmeldeinformationen abruft und in eine lokale Anmeldeinformationen schreibt. Du kannst auf CloudWatch Agent-Konfiguration in dieselbe Datei. Sie können den Prozess vonKonfigurieren Sie lokale Server, die den Systems Manager Agent und den einheitlichen CloudWatch-Agent verwenden,

	um nur temporäre Anmeldeinformationen zu verwendenimAWSKnowledge Center. Sie können diesen Prozess auch automatisieren, indem Sie ein separates Systems Manager Automation Runbook und eine State Manager-Zuordnung definieren und Ihre lokalen Instanzen mit Tags ansprechen. Wenn Sie eine erstellenSystems Manager Manager-Aktivierungfür Ihre lokalen Instanzen sollten Sie ein Tag hinzufügen, das die Instanzen als lokale Instanzen identifiziert.
Erwägen Sie, Konten und Regionen mit VPN oderAWS Direct ConnectZugriff auf undAWSPrivateLink.	Sie können verwendenAWS Direct Connectoder AWS Virtual Private Network(AWS VPN) um private Verbindungen zwischen lokalen Netzwerken und Ihrer Virtual Private Cloud (VPC) herzustellen.AWS PrivateLink baut eine private Verbindung zu CloudWatch Protokolliert mit einem Schnittstellen-VPC-Endpunkt. Dieser Ansatz ist nützlich, wenn Sie Einschränkungen haben, die verhindern, dass Daten über das öffentliche Internet an einen Endpunkt des öffentlichen Dienstes gesendet werden.
Alle Metriken müssen in der CloudWatch Konfigurationsdatei.	Amazon EC2 enthält Standardmetriken (z. B. CPU-Auslastung), diese Metriken müssen jedoch für lokale Instanzen definiert werden. Sie können eine separate Plattformkonfigurationsdatei verwenden, um diese Metriken für lokale Server zu definieren und dann die Konfiguration an den Standard anzuhängen CloudWatch Kennzahlenkonfiguration für die Plattform.

Überlegungen für kurzlebige EC2-Instanzen

EC2-Instanzen sind vorübergehend oderephemer, wenn sie von Amazon EC2 Auto Scaling, Amazon EMR bereitgestellt werdenAmazon EC2-Spot-Instances, oderAWS Batchaus. Ephemere EC2-Instanzen können eine sehr große Anzahl von CloudWatch streams unter einer gemeinsamen Protokollgruppe ohne zusätzliche Informationen über ihren Laufzeitursprung.

Wenn Sie kurzlebige EC2-Instanzen verwenden, sollten Sie in Erwägung ziehen, zusätzliche dynamische Kontextinformationen in die Protokollgruppe und den Log-Stream-Namen hinzuzufügen. Sie können beispielsweise die Spot-Instance-Anforderungs-ID, den Namen des Amazon EMR-Clusters oder den Namen der Auto Scaling Scaling-Gruppe angeben. Diese Informationen können für neu gestartete EC2-Instanzen variieren und Sie müssen sie möglicherweise zur Laufzeit abrufen und konfigurieren. Sie können dies tun, indem Sie eine CloudWatch Agent-Konfigurationsdatei beim Booten und Neustart des Agenten, um die aktualisierte Konfigurationsdatei einzuschließen. Dies ermöglicht die Bereitstellung von Protokollen und Metriken an CloudWatch unter Verwendung dynamischer Laufzeitinformationen.

Sie sollten auch sicherstellen, dass Ihre Metriken und Protokolle von der CloudWatch -Agent, bevor Ihre kurzlebigen EC2-Instanzen beendet werden. Die CloudWatch Agent enthält ein`flush_interval`-Parameter, der konfiguriert werden kann, um das Zeitintervall für das Löschen von Log- und Metrikpuffern zu definieren. Sie können diesen Wert basierend auf Ihrer Arbeitslast senken und die CloudWatch agent und zwingen Sie die Puffer zum Löschen, bevor die EC2-Instanz beendet wird.

Verwenden einer automatisierten Lösung zur Bereitstellung des CloudWatch Agentin

Wenn Sie eine Automatisierungslösung verwenden (z. B. Ansible oder Chef), können Sie diese nutzen, um die CloudWatch -Agent. Wenn Sie diesen Ansatz verwenden, müssen Sie die folgenden Überlegungen bewerten:

- Stellen Sie sicher, dass die Automatisierung die Betriebssysteme und die von Ihnen unterstützten Betriebssystemversionen abdeckt. Wenn das Automatisierungsskript nicht alle Betriebssysteme Ihres Unternehmens unterstützt, sollten Sie alternative Lösungen für die nicht unterstützten Betriebssysteme definieren.
- Überprüfen Sie, dass die Automatisierungslösung regelmäßig nach Updates und Upgrades des CloudWatch-Agenten suchtaus. Ihre Automatisierungslösung sollte regelmäßig nach Aktualisierungen der CloudWatch Agent oder deinstallieren Sie den Agenten regelmäßig und

installieren Sie ihn neu. Sie können einen Scheduler oder eine Automatisierungslösung verwenden, um den Agenten regelmäßig zu überprüfen und zu aktualisieren.

- Überprüfen Sie, ob Sie die Agentinstallation und die Konformität der Konfiguration bestätigen könnenaus. Ihre Automatisierungslösung sollte es Ihnen ermöglichen, festzustellen, wann der Agent auf einem System nicht installiert ist oder wann der Agent nicht funktioniert. Sie können eine Benachrichtigung oder einen Alarm in Ihre Automatisierungslösung implementieren, damit fehlgeschlagene Installationen und Konfigurationen verfolgt werden.

Bereitstellen der CloudWatch Agent bei der Instanzbereitstellung mit dem Benutzerdatenskript

Sie können diesen Ansatz verwenden, wenn Sie den Systems Manager nicht verwenden möchten und CloudWatch selektiv für Ihre EC2-Instanzen verwenden möchten. In der Regel wird dieser Ansatz einmalig oder wenn eine spezielle Konfiguration erforderlich ist, verwendet.AWSbietetdirekte Linksfür CloudWatch Agent, der in Ihren Start- oder Benutzerdatenskripts heruntergeladen werden kann. Die Agent-Installationspakete können ohne Benutzerinteraktion im Hintergrund ausgeführt werden, was bedeutet, dass Sie sie in automatisierten Bereitstellungen verwenden können. Wenn Sie diesen Ansatz verwenden, sollten Sie die folgenden Überlegungen bewerten:

- Erhöhtes Risiko, dass Benutzer den Agenten nicht installieren oder Standardmetriken konfigurierenaus. Benutzer können Instanzen bereitstellen, ohne die erforderlichen Schritte zur Installation des CloudWatch -Agent. Sie könnten den Agenten auch falsch konfigurieren, was zu Inkonsistenzen bei der Protokollierung und Überwachung führen kann.
- Die Installationsskripte müssen betriebssystemspezifisch und für verschiedene Betriebssystemversionen geeignet seinaus. Sie benötigen separate Skripte, wenn Sie sowohl Windows als auch Linux verwenden möchten. Das Linux-Skript sollte basierend auf der Distribution auch verschiedene Installationsschritte haben.
- Sie müssen regelmäßig die CloudWatch Agent mit neuen Versionen wenn verfügbaraus. Dies kann automatisiert werden, wenn Sie Systems Manager mit State Manager verwenden, aber Sie können das Benutzerdatenskript auch so konfigurieren, dass es beim Start der Instanz erneut ausgeführt wird. Die CloudWatch Agent wird dann bei jedem Neustart aktualisiert und neu installiert.
- Sie müssen den Abruf und die Anwendung von CloudWatch-Standardkonfigurationen automatisierenaus. Dies kann automatisiert werden, wenn Sie Systems Manager mit State Manager verwenden, aber Sie können auch ein Benutzerdatenskript konfigurieren, um die Konfigurationsdateien beim Booten abzurufen und die CloudWatch -Agent.

Einschließlich des CloudWatch Der -Agent in Ihren AMIs

Der Vorteil dieses Ansatzes besteht darin, dass Sie nicht auf die CloudWatch Agent, der installiert und konfiguriert werden soll, und Sie können sofort mit der Protokollierung und Überwachung beginnen. Dies hilft Ihnen, Ihre Instanzbereitstellungs- und Startschritte besser zu überwachen, falls Instanzen nicht gestartet werden. Dieser Ansatz ist auch geeignet, wenn Sie den Systems Manager Manager-Agent nicht verwenden möchten. Wenn Sie diesen Ansatz verwenden, sollten Sie die folgenden Überlegungen bewerten:

- Ein Update-Prozess muss vorhanden sein, da AMIs möglicherweise nicht den neuesten enthalten CloudWatch -Agent-Versionaus. Die CloudWatch Agent, der in einem AMI installiert ist, ist erst aktuell, als das AMI das letzte Mal erstellt wurde. Sie sollten eine zusätzliche Methode zur regelmäßigen Aktualisierung des Agenten und zur Bereitstellung der EC2-Instanz angeben. Wenn Sie den Systems Manager verwenden, können Sie dieInstallieren von CloudWatch -Agent mit Systems Manager Distributor und State Managerhierzu bereitgestellte Lösung. Wenn Sie den Systems Manager nicht verwenden, können Sie den Agenten beim Start und Neustart der Instanz mit einem Benutzerdatenskript aktualisieren.
- Ihre CloudWatch Agent-Konfigurationsdatei muss beim Start der Instanz abgerufen werdenaus. Wenn Sie den Systems Manager nicht verwenden, können Sie ein Benutzerdatenskript konfigurieren, um die Konfigurationsdateien beim Booten abzurufen und dann den CloudWatch -Agent.
- Die CloudWatch Agent muss nach Ihrem neu gestartet werden CloudWatch Konfiguration wird aktualisiertaus.
- AWSAnmeldeinformationen dürfen nicht im AMI gespeichert werdenaus. Stellen Sie sicher, dass kein lokalesAWSAnmeldeinformationen werden im AMI gespeichert. Wenn Sie Amazon EC2 verwenden, können Sie die erforderliche IAM-Rolle auf Ihre Instance anwenden und lokale Anmeldeinformationen vermeiden. Wenn Sie lokale Instanzen verwenden, sollten Sie die Instanz-Anmeldeinformationen automatisieren oder manuell aktualisieren, bevor Sie die CloudWatch -Agent.

Protokollierung und Überwachung auf Amazon ECS

Amazon Elastic Container Service (Amazon ECS) bietet zwei Starttypen für laufende Container und , die den Infrastrukturtyp bestimmen, der Aufgaben und Services hostet. Diese Starttypen sind AWS Fargate und Amazon EC2. Beide Starttypen sind in integriert, CloudWatch aber Konfigurationen und Support variieren.

In den folgenden Abschnitten erfahren Sie, wie Sie CloudWatch für die Protokollierung und Überwachung auf Amazon ECS verwenden.

Themen

- Konfigurieren CloudWatch mit einem EC2-Starttyp
- Amazon-ECS-Containerprotokolle für EC2- und Fargate-Starttypen
- Verwenden von benutzerdefiniertem Protokoll-Routing mit FireLens für Amazon ECS
- Metriken für Amazon ECS

Konfigurieren CloudWatch mit einem EC2-Starttyp

Bei einem EC2-Starttyp stellen Sie einen Amazon-ECS-Cluster von EC2-Instances bereit, die den CloudWatch Agenten für die Protokollierung und Überwachung verwenden. Ein Amazon-ECS-optimiertes AMI ist mit dem Amazon-ECS-Container-Agenten vorinstalliert und stellt CloudWatch Metriken für den Amazon-ECS-Cluster bereit.

Diese Standardmetriken sind in den Kosten von Amazon ECS enthalten, aber die Standardkonfiguration für Amazon ECS überwacht keine Protokolldateien oder zusätzlichen Metriken (z. B. freien Speicherplatz). Sie können die verwenden AWS Management Console , um einen Amazon-ECS-Cluster mit dem Starttyp EC2 bereitzustellen. Dadurch wird ein - AWS CloudFormation Stack erstellt, der eine - Amazon EC2 Auto Scaling Gruppe mit einer Startkonfiguration bereitstellt. Dieser Ansatz bedeutet jedoch, dass Sie kein benutzerdefiniertes AMI auswählen oder die Startkonfiguration mit unterschiedlichen Einstellungen oder zusätzlichen Startskripten anpassen können.

Um zusätzliche Protokolle und Metriken zu überwachen, müssen Sie den CloudWatch Agenten auf Ihren Amazon-ECS-Container-Instances installieren. Sie können den Installationsansatz für EC2-Instances im Installieren von CloudWatch -Agent mit Systems Manager Distributor und State

Manager Abschnitt dieses Handbuchs verwenden. Das Amazon-ECS-AMI enthält jedoch nicht den erforderlichen Systems-Manager-Agenten. Sie sollten eine benutzerdefinierte Startkonfiguration mit einem Benutzerdatenskript verwenden, das den Systems-Manager-Agenten installiert, wenn Sie Ihren Amazon-ECS-Cluster erstellen. Auf diese Weise können sich Ihre Container-Instances bei Systems Manager registrieren und die State Manager-Zuordnungen anwenden, um den CloudWatch Agenten zu installieren, zu konfigurieren und zu aktualisieren. Wenn State Manager Ihre CloudWatch Agentenkonfiguration ausführt und aktualisiert, wendet es auch Ihre standardisierte CloudWatch Konfiguration auf Systemebene für Amazon EC2 an. Sie können standardisierte CloudWatch Konfigurationen für Amazon ECS auch im S3-Bucket für Ihre CloudWatch Konfiguration speichern und sie automatisch mit State Manager anwenden.

Sie sollten sicherstellen, dass die auf Ihre Amazon-ECS-Container-Instances angewendete IAM-Rolle oder das Instance-Profil die erforderlichen - `CloudWatchAgentServerPolicy` und -`AmazonSSMManagedInstanceCore`Richtlinien enthält. Sie können die Vorlage ecs_cluster_with_cloudwatch_linux.yaml AWS CloudFormation verwenden, um Linux-basierte Amazon-ECS-Cluster bereitzustellen. Diese Vorlage erstellt einen Amazon-ECS-Cluster mit einer benutzerdefinierten Startkonfiguration, die Systems Manager installiert und eine benutzerdefinierte CloudWatch Konfiguration zur Überwachung von Amazon-ECS-spezifischen Protokolldateien bereitstellt.

Sie sollten die folgenden Protokolle für Ihre Amazon-ECS-Container-Instances sowie Ihre EC2-Standard-Instance-Protokolle erfassen:

- Startausgabe des Amazon-ECS-Agenten – `/var/log/ecs/ecs-init.log`
- Amazon-ECS-Agentenausgabe – `/var/log/ecs/ecs-agent.log`
- Anforderungsprotokoll des IAM-Anmeldeinformationsanbieters – `/var/log/ecs/audit.log`

Weitere Informationen zur Ausgabeebene, Formatierung und zusätzlichen Konfigurationsoptionen finden Sie unter Speicherorte von Amazon-ECS-Protokolldateien in der Amazon-ECS-Dokumentation.

> **Important**
>
> Die Installation oder Konfiguration des Agenten ist für den Fargate-Starttyp nicht erforderlich, da Sie keine EC2-Container-Instances ausführen oder verwalten.

Amazon-ECS-Container-Instances sollten die neuesten Amazon-ECS-optimierten AMIs und Container-Agenten verwenden. AWS speichert öffentliche Systems Manager Parameter Store-Parameter mit Amazon-ECS-optimierten AMI-Informationen, einschließlich der AMI-ID. Sie können das neueste zuletzt optimierte AMI aus dem Parameter Store abrufen, indem Sie das Parameterspeicher-Parameterformat für Amazon-ECS-optimierte AMIs verwenden. Sie können in Ihren AWS CloudFormation Vorlagen auf den öffentlichen Parameter Store-Parameter verweisen, der auf das neueste AMI oder eine bestimmte AMI-Version verweist.

AWS stellt in jeder unterstützten Region dieselben Parameter Store-Parameter bereit. Das bedeutet, dass AWS CloudFormation Vorlagen, die auf diese Parameter verweisen, über Regionen und Konten hinweg wiederverwendet werden können, ohne dass das AMI aktualisiert werden muss. Sie können die Bereitstellung neuerer Amazon-ECS-AMIs in Ihrer Organisation steuern, indem Sie auf eine bestimmte Version verweisen, die Ihnen hilft, die Verwendung eines neuen Amazon-ECS-optimierten AMI zu verhindern, bis Sie es testen.

Amazon-ECS-Containerprotokolle für EC2- und Fargate-Starttypen

Amazon ECS verwendet eine Aufgabendefinition, um Container als Aufgaben und Services bereitzustellen und zu verwalten. Sie konfigurieren die Container, die Sie in Ihrem Amazon-ECS-Cluster starten möchten, innerhalb einer Aufgabendefinition. Die Protokollierung wird mit einem Protokolltreiber auf Containerebene konfiguriert. Mehrere Protokolltreiberoptionen bieten Ihren Containern unterschiedliche Protokollierungssysteme (z. B. `awslogs`,`fluentd`,`gelf`, `json-file`,`journald`oder `awsfirelens`), je nachdem,`logentries`,`splunk`,`syslog`, ob Sie den Starttyp EC2 oder Fargate verwenden. Der Fargate-Starttyp bietet eine Teilmenge der folgenden Protokolltreiberoptionen: `awslogs`, und `awsfirelens`. AWS stellt den `awslogs` Protokolltreiber bereit, um die Containerausgabe zu erfassen und an CloudWatch Logs zu übertragen. Mit den Protokolltreibereinstellungen können Sie die Protokollgruppe, die Region und das Protokollstream-Präfix zusammen mit vielen anderen Optionen anpassen.

Die Standardbenennung für Protokollgruppen und die Option, die von der Option CloudWatch Protokolle automatisch konfigurieren in der AWS Management Console verwendet wird, ist `/ecs/<task_name>`. Der von Amazon ECS verwendete Name des Protokollstreams hat das `<awslogs-stream-prefix>/<container_name>/<task_id>` Format . Wir empfehlen Ihnen, einen Gruppennamen zu verwenden, der Ihre Protokolle basierend auf den Anforderungen Ihrer Organisation gruppiert. In der folgenden Tabelle `image_tag` sind die `image_name` und im Namen des Protokollstreams enthalten.

Protokollgruppenname	`/<Business unit>/<Project or application name>/<Environment>/<Cluster name>/<Task name>`
Protokollstream-Namenspräfix	`/<image_name>/<image_tag>`

Diese Informationen sind auch in der Aufgabendefinition verfügbar. Aufgaben werden jedoch regelmäßig mit neuen Revisionen aktualisiert, was bedeutet, dass die Aufgabendefinition möglicherweise ein anderes `image_name` verwendet hat `image_tag` als die, die die Aufgabendefinition derzeit verwendet. Weitere Informationen und Vorschläge zur Benennung finden Sie im Planen Ihrer CloudWatch Bereitstellung Abschnitt dieses Handbuchs.

Wenn Sie eine Pipeline für kontinuierliche Integration und kontinuierliche Bereitstellung (CI/CD) oder einen automatisierten Prozess verwenden, können Sie mit jedem neuen Docker-Image-Build eine neue Revision der Aufgabendefinition für Ihre Anwendung erstellen. Sie können beispielsweise den Docker-Image-Namen, das Image-Tag, die GitHub Revision oder andere wichtige Informationen als Teil Ihres CI/CD-Prozesses in Ihre Aufgabendefinitionsrevisions- und Protokollierungskonfiguration aufnehmen.

Verwenden von benutzerdefiniertem Protokoll-Routing mit FireLens für Amazon ECS

FireLens for Amazon ECS hilft Ihnen, Protokolle an Fluentd oder Fluent Bit weiterzuleiten, sodass Sie Containerprotokolle direkt an - AWS Services und - AWS Partnernetzwerk (APN)-Ziele senden und den Versand von Protokollen an - CloudWatch Protokolle unterstützen können.

AWS bietet ein Docker-Image für Fluent Bit mit vorinstallierten Plug-Ins für Amazon Kinesis Data Streams, Amazon Data Firehose und CloudWatch Logs. Sie können den FireLens -Protokolltreiber anstelle des -`awslogs`Protokolltreibers verwenden, um die an CloudWatch -Protokolle gesendeten Protokolle besser anzupassen und zu kontrollieren.

Sie können beispielsweise den - FireLens Protokolltreiber verwenden, um die Ausgabe des Protokollformats zu steuern. Das bedeutet, dass die CloudWatch Protokolle eines Amazon-ECS-Containers automatisch als JSON-Objekte formatiert werden und JSON-formatierte Eigenschaften für `ecs_cluster`,`ecs_task_arn`, `ecs_task_definition`, `container_idcontainer_name`,

und enthaltenec2_instance_id. Der Fluenten-Host wird Ihrem Container über die FLUENT_PORT Umgebungsvariablen FLUENT_HOST und bereitgestellt, wenn Sie den awsfirelens Treiber angeben. Das bedeutet, dass Sie sich direkt von Ihrem Code aus beim Protokollrouter anmelden können, indem Sie fluent Logger-Bibliotheken verwenden. Ihre Anwendung könnte beispielsweise die fluent-logger-python Bibliothek enthalten, um sich mithilfe der Werte, die in den Umgebungsvariablen verfügbar sind, bei Fluent Bit anzumelden.

Wenn Sie FireLens für Amazon ECS verwenden möchten, können Sie dieselben Einstellungen wie der awslogs Protokolltreiber konfigurieren und auch andere Einstellungen verwenden. Sie können beispielsweise die ecs-task-nginx-firelense.json Amazon ECS-Aufgabendefinition verwenden, die einen NGINX-Server startet, der FireLens für die Protokollierung in konfiguriert ist CloudWatch. Es startet auch einen FireLens Fluent-Bit-Container als Sidecar für die Protokollierung.

Metriken für Amazon ECS

Amazon ECS stellt CloudWatch Standardmetriken (z. B. CPU- und Speicherauslastung) für die Starttypen EC2 und Fargate auf Cluster- und Serviceebene mit dem Amazon-ECS-Container-Agenten bereit. Sie können auch Metriken für Ihre Services, Aufgaben und Container mithilfe von CloudWatch Container Insights erfassen oder Ihre eigenen benutzerdefinierten Containermetriken mithilfe des eingebetteten Metrikformats erfassen.

Container Insights ist eine CloudWatch Funktion, die Metriken wie CPU-Auslastung, Speicherauslastung, Netzwerkverkehr und Speicher auf Cluster-, Container-Instance-, Service- und Aufgabenebene bereitstellt. Container Insights erstellt auch automatische Dashboards, mit denen Sie Services und Aufgaben analysieren und die durchschnittliche Speicher- oder CPU-Auslastung auf Containerebene anzeigen können. Container Insights veröffentlicht benutzerdefinierte Metriken im ECS/ContainerInsights benutzerdefinierten Namespace, den Sie für Diagramme, Alarme und Dashboards verwenden können.

Sie können Container-Insight-Metriken aktivieren, indem Sie Container Insights für jeden einzelnen Amazon-ECS-Cluster aktivieren. Wenn Sie auch Metriken auf Container-Instance-Ebene anzeigen möchten, können Sie den CloudWatch Agenten als Daemon-Container auf Ihrem Amazon-ECS-Cluster starten. Sie können die Vorlage cwagent-ecs-instance-metric-cfn.yaml AWS CloudFormation verwenden, um den CloudWatch Agenten als Amazon-ECS-Service bereitzustellen. Wichtig ist, dass in diesem Beispiel davon ausgegangen wird, dass Sie eine entsprechende benutzerdefinierte CloudWatch Agentenkonfiguration erstellt und mit dem Schlüssel im Parameter Store gespeichert habenecs-cwagent-daemon-service.

Der CloudWatch Agent, der als Daemon-Container für CloudWatch Container Insights bereitgestellt wird, enthält zusätzliche Festplatten-, Speicher- und CPU-Metriken wie `instance_cpu_reserved_capacity` und `instance_memory_reserved_capacity` mit den `InstanceId` Dimensionen `ClusterName`, `ContainerInstanceId`, . Metriken auf Container-Instance-Ebene werden von Container Insights mithilfe des CloudWatch eingebetteten Metrikformats implementiert. Sie können zusätzliche Metriken auf Systemebene für Ihre Amazon-ECS-Container-Instances konfigurieren, indem Sie den Ansatz aus dem Einrichten von State Manager und Distributor für CloudWatch Bereitstellung und Konfiguration von Agenten Abschnitt dieses Handbuchs verwenden.

Erstellen von benutzerdefinierten Anwendungsmetriken in Amazon ECS

Sie können benutzerdefinierte Metriken für Ihre Anwendungen erstellen, indem Sie das CloudWatch eingebettete Metrikformat verwenden. Der `awslogs` Protokolltreiber kann Anweisungen im CloudWatch eingebetteten Metrikformat interpretieren.

Die `CW_CONFIG_CONTENT` Umgebungsvariable im folgenden Beispiel ist auf den Inhalt des `cwagentconfig` Systems Manager Parameter Store-Parameters festgelegt. Sie können den Agenten mit dieser grundlegenden Konfiguration ausführen, um ihn als Endpunkt im eingebetteten Metrikformat zu konfigurieren. Dies ist jedoch nicht mehr erforderlich.

```
  {
  "logs": {
    "metrics_collected": {
      "emf": { }
    }
  }
}
```

Wenn Sie Amazon-ECS-Bereitstellungen über mehrere Konten und Regionen hinweg haben, können Sie ein - AWS Secrets Manager Secret verwenden, um Ihre CloudWatch Konfiguration zu speichern und die Secret-Richtlinie so zu konfigurieren, dass sie für Ihre Organisation freigegeben wird. Sie können die Secrets-Option in Ihrer Aufgabendefinition verwenden, um die `CW_CONFIG_CONTENT` Variable festzulegen.

Sie können die AWS bereitgestellten Bibliotheken im eingebetteten Open-Source-Metrikformat in Ihrer Anwendung verwenden und die `AWS_EMF_AGENT_ENDPOINT` Umgebungsvariable angeben,

um eine Verbindung zu Ihrem CloudWatch Kundendienstmitarbeiter-Sidecar-Container herzustellen, der als Endpunkt im eingebetteten Metrikformat fungiert. Sie können beispielsweise die Python-Beispielanwendung ecs_cw_emf_example verwenden, um Metriken im eingebetteten Metrikformat an einen CloudWatch Kundendienstmitarbeiter-Sidecar-Container zu senden, der als Endpunkt im eingebetteten Metrikformat konfiguriert ist.

Das Fluent-Bit-Plugin für CloudWatch kann auch verwendet werden, um Nachrichten im eingebetteten Metrikformat zu senden. Sie können auch die Python-Beispielanwendung ecs_firelense_emf_example verwenden, um Metriken im eingebetteten Metrikformat an einen Sidecar-Container von Firelens für Amazon ECS zu senden.

Wenn Sie das eingebettete Metrikformat nicht verwenden möchten, können Sie CloudWatch Metriken über die AWS API oder das AWS SDK erstellen und aktualisieren. Wir empfehlen diesen Ansatz nur, wenn Sie einen bestimmten Anwendungsfall haben, da er Ihren Code um Wartungs- und Verwaltungsaufwand erweitert.

Protokollierung und Überwachung auf Amazon EKS

Amazon Elastic Kubernetes Service (Amazon EKS) integriert sich mit CloudWatch Logs für die Kubernetes-Steuerebene. Die Steuerebene wird von Amazon EKS als verwalteter Service zur Verfügung gestellt und Sie könnenaktivieren Sie die Protokollierung, ohne einen CloudWatch-Agent zu installierenaus. Die CloudWatch Agent kann auch bereitgestellt werden, um Amazon EKS-Knoten- und Containerprotokolle zu erfassen. Fluent Bit und Fluentdwerden auch unterstützt, um Ihre Containerprotokolle an CloudWatch Protokolle.

CloudWatch Container Insights bietet eine umfassende Metrikenüberwachungslösung für Amazon EKS auf der Cluster-, Knoten-, Pod-, Aufgaben- und Service-Ebene. Amazon EKS unterstützt auch mehrere Optionen für die Erfassung von Metriken mitPrometheusaus. Die Amazon-EKS-Steuerebenestellt einen Metrik-Endpunkt bereitdas zeigt Metriken in einem Prometheus-Format. Sie können Prometheus in Ihrem Amazon EKS-Cluster bereitstellen, um diese Metriken zu verwenden.

Sie könnenEinrichten der CloudWatch -Agent zum Scrape von Prometheus-Metrikenund erstellen CloudWatch Metriken zusätzlich zum Verbrauch anderer Prometheus-Endpunkte. Überwachung von Container Insights für Prometheuskann Prometheus-Metriken auch automatisch aus unterstützten, containerisierten Workloads und Systemen erfassen und erfassen.

Sie können die CloudWatch -Agent auf Ihren Amazon EKS-Knoten, ähnlich wie der Ansatz für Amazon EC2 mit Distributor und State Manager, um Ihre Amazon EKS-Knoten an Ihren Standardkonfigurationen für die Systemprotokollierung und -überwachung auszurichten.

Protokollierung für Amazon EKS

Die Kubernetes-Protokollierung kann in die Protokollierung von Steuerungsebenen, Knotenprotokollierung und Anwendungsprotokollierung unterteilt werden. DieKubernetes-Steuerebeneist eine Reihe von Komponenten, die Kubernetes-Cluster verwalten und Protokolle erstellen, die für Auditing- und Diagnosezwecke verwendet werden. Mit Amazon EKS können Sieaktivieren Sie Protokolle für verschiedene Steuerungsebenenkomponentenund schicke sie an CloudWatch.

Kubernetes führt auch Systemkomponenten wie`kubelet`und`kube-proxy`auf jedem Kubernetes-Knoten, auf dem Ihre Pods ausgeführt werden. Diese Komponenten schreiben Protokolle in jeden Knoten und Sie können konfigurieren CloudWatch und Container Insights, um diese Protokolle für jeden Amazon EKS-Knoten zu erfassen.

Container sind gruppiert alsHülseninnerhalb eines Kubernetes-Clusters und soll auf Ihren Kubernetes-Knoten ausgeführt werden. Die meisten containerisierten Anwendungen schreiben auf Standardausgabe und Standardfehler, und die Container-Engine leitet die Ausgabe an einen Protokolliertreiber um. In Kubernetes finden sich die Containerprotokolle im`/var/log/pods`-Verzeichnis auf einem Knoten. Sie können CloudWatch und Container Insights, um diese Protokolle für jeden Ihrer Amazon EKS-Pods zu erfassen.

Amazon-EKS-Steuerebenen-Protokollierung

Ein Amazon EKS-Cluster besteht aus einer hochverfügbaren Single-Tenant-Steuerebene für Ihren Kubernetes-Cluster und den Amazon EKS-Knoten, auf denen Ihre Container ausgeführt werden. Die Steuerungsebenenknoten werden in einem Konto ausgeführt, das vonAWSaus. Die Amazon EKS Cluster-Steuerebene Knoten sind integriert CloudWatch und Sie können die Protokollierung für bestimmte Steuerungsebenenkomponenten aktivieren.

Für jede Instanz der Kubernetes-Steuerebene werden Protokolle bereitgestellt.AWSverwaltet den Zustand Ihrer Steuerungsebenenknoten und bietet eineService Level Agreement (SLA) für den Kubernetes-Endpunktaus.

Amazon-EKS-Knotenprotokollierung

Wir empfehlen Ihnen,CloudWatch Container Insightsum Protokolle und Metriken für Amazon EKS zu erfassen. Container Insights implementiert Metriken auf Cluster-, Knoten- und Pod-Ebene mit CloudWatch Agent und Fluent Bit oder Fluentd für die Protokollerfassung auf CloudWatch. Container Insights bietet auch automatische Dashboards mit mehrschichtigen Ansichten Ihrer erfassten CloudWatch -Metriken. Container Insights wird als CloudWatch bereitgestellt DaemonSet und Fluent Bit DaemonSet das läuft auf jedem Amazon EKS-Knoten. Fargate-Knoten werden von Container Insights nicht unterstützt, da die Knoten vonAWSund unterstützt DaemonSets nicht. Die Fargate-Protokollierung für Amazon EKS wird in diesem Leitfaden separat behandelt.

In der folgenden Tabelle ist die CloudWatch Protokollgruppen und Protokolle, die von derStandardkonfiguration für Fluentd oder Fluent Bit Protokollierungfür Amazon EKS.

`/aws/containerinsights/Cluster_Name/application`	Alle Protokolldateien in`/var/log/containers` aus. Dieses Verzeichnis enthält symbolische Links zu allen Kubernetes-Containerprotokollen im`/`

	`var/log/pods` -Verzeichnisstruktur. Dies erfasst Ihre Anwendungs-Container-Protokolle, die in`stdout`oder`stderr`aus. Es enthält auch Protokolle für Kubernete s-Systemcontainer wie`aws-vpc-cni-init`,`kube-proxy` , und`coreDNS`aus.
`/aws/containerinsights/Cluster_Name/host`	Protokolle aus`/var/log/dmesg` ,`/var/log/secure` , und`/var/log/messages` aus.
`/aws/containerinsights/Cluster_Name/dataplane`	Die Protokolle in `/var/log/journal` für `kubelet.service` , `kubeproxy.service` und `docker.service` .

Wenn Sie Container Insights mit Fluent Bit oder Fluentd nicht für die Protokollierung verwenden möchten, können Sie Knoten- und Containerprotokolle mit der CloudWatch Auf Amazon EKS-Knoten installierter Agent. Amazon EKS-Knoten sind EC2-Instanzen, was bedeutet, dass Sie sie in Ihren Standardprotokollierungsansatz auf Systemebene für Amazon EC2 aufnehmen sollten. Wenn Sie das CloudWatch Agent, der Distributor und State Manager verwendet, dann sind Amazon EKS-Knoten ebenfalls im CloudWatch Installation, Konfiguration und Update des Agents.

Die folgende Tabelle zeigt Protokolle, die spezifisch für Kubernetes sind und die Sie erfassen müssen, wenn Sie Container Insights mit Fluent Bit oder Fluentd nicht für die Protokollierung verwenden.

`/var/log/containers`	Dieses Verzeichnis enthält symbolische Links zu allen Kubernetes-Containerprotokollen unter der`/var/log/pods` -Verzeichnisstruktur. Dies erfasst effektiv Ihre Anwendungs-Contain er-Protokolle, die in`stdout`oder`stderr`aus. Dies beinhaltet Protokolle für Kubernete s-Systemcontainer wie`aws-vpc-cni-init`,`kube-proxy` , und`coreDNS`aus. Wichtig Dies ist nicht erforderlich, wenn Sie Container Insights verwenden.

`var/log/aws-routed-eni/ipamd.log`
 	
`/var/log/aws-routed-eni/plugin.log`
	Die Logs für den L-IPAM-Daemon finden Sie hier

Sie müssen sicherstellen, dass Amazon EKS-Knoten CloudWatch Agent, um geeignete Protokolle und Metriken auf Systemebene zu senden. Das für Amazon EKS optimierte AMI enthält jedoch keinen Systems Manager Manager-Agenten. Durch Verwendung vonStartvorlagenkönnen Sie die Installation des Systems Manager Manager-Agenten und eine Standardeinstellung automatisieren CloudWatch -Konfiguration, die wichtige Amazon EKS-spezifische Protokolle mit einem Startskript erfasst, das über den Abschnitt Benutzerdaten implementiert wurde. Amazon EKS-Knoten werden mit einer Auto Scaling Scaling-Gruppe alsVerwaltete Knotengruppeoder alsSelbstverwaltete Knotenaus.

Bei verwalteten Knotengruppen geben Sie eineStartvorlageder den Abschnitt Benutzerdaten zur Automatisierung der Installation des Systems Manager Manager-Agenten umfasst und CloudWatch -Konfiguration. Sie können dieamazon_eks_managed_node_group_launch_config.yaml AWS CloudFormationVorlage zum Erstellen einer Startvorlage, die den Systems Manager Manager-Agent installiert, CloudWatch -Agent und fügt auch eine Amazon EKS-spezifische Protokollierungskonfiguration zum CloudWatch Konfigurationsverzeichnis. Diese Vorlage kann verwendet werden, um Ihre Startvorlage für Amazon EKS verwaltete Knotengruppen mit einem infrastructure-as-code (IaC) -Ansatz. Jedes Update desAWS CloudFormationVorlage enthält eine neue Version der Startvorlage. Anschließend können Sie die Knotengruppe aktualisieren, um die neue Vorlagenversion zu verwenden undverwalteter Lebenszyklusprozessaktualisieren Sie Ihre Knoten ohne Ausfallzeiten. Stellen Sie sicher, dass die IAM-Rolle und das Instanzprofil, das auf Ihre verwaltete Knotengruppe angewendet wird, die`CloudWatchAgentServerPolicy`und`AmazonSSMManagedInstanceCore` AWSVerwaltete -Richtlinien.

Mit selbstverwalteten Nodes stellen Sie die Lebenszyklus- und Update-Strategie für Ihre Amazon EKS-Knoten direkt bereit und verwalten sie. Selbstverwaltete Knoten ermöglichen es Ihnen, Windows-Knoten auf Ihrem Amazon EKS-Cluster auszuführen undBottlerocketzusammen mitandere Optionenaus. Sie könnenAWS CloudFormationum selbstverwaltete Knoten in Ihren Amazon EKS-Clustern bereitzustellen, was bedeutet, dass Sie einen iAC- und Managed Change-Ansatz für Ihre Amazon EKS-Cluster verwenden können.AWSbietet dieamazon-eks-nodegroup.yaml AWS CloudFormation-Vorlage, die Sie ohne weitere Anpassung verwenden können. Die Vorlage enthält alle erforderlichen Ressourcen für Amazon EKS-Knoten in einem Cluster (z. B. eine separate

IAM-Rolle, eine Sicherheitsgruppe, eine Amazon EC2 Auto Scaling Scaling-Gruppe und eine Startvorlage). Dieamazon-eks-nodegroup.yaml AWS CloudFormationtemplate ist eine aktualisierte Version, die den erforderlichen Systems Manager Manager-Agenten installiert, CloudWatch - Agent und fügt auch eine Amazon EKS-spezifische Protokollierungskonfiguration zum CloudWatch Konfigurationsverzeichnis.

Logging für Amazon EKS auf Fargate

Mit Amazon EKS auf Fargate können Sie Pods bereitstellen, ohne Ihre Kubernetes-Knoten zuzuweisen oder zu verwalten. Dies macht es überflüssig, Protokolle auf Systemebene für Ihre Kubernetes-Knoten zu erfassen. Um die Protokolle von Ihren Fargate-Pods zu erfassen, können Sie Fluent Bit verwenden, um die Protokolle direkt an CloudWatch weiterzuleiten. Auf diese Weise können Sie Protokolle automatisch an CloudWatch ohne weitere Konfiguration oder einen Beiwagen-Container für Ihre Amazon EKS Pods auf Fargate. Weitere Informationen hierzu finden Sie unterFargate-Protokollierungin der Amazon-EKS-Dokumentation undFließend Bit für Amazon EKSauf derAWSBlog-Test. Diese Lösung erfasst die`STDOUT`und`STDERR`E/A-Streams (Eingabe/Ausgabe) -Streams von Ihrem Container und sendet sie an CloudWatch durch Fluent Bit, basierend auf der Fluent Bit-Konfiguration, die für den Amazon EKS-Cluster auf Fargate eingerichtet wurde.

Metriken für Amazon EKS und Kubernetes

Kubernetes bietet eine Metrik-API, mit der Sie auf Metriken zur Ressourcenauslastung zugreifen können (z. B. CPU- und Speicherauslastung für Knoten und Pods), aber die API bietet nur Point-in-Time-Informationen und keine historischen Metriken. DieKubernetes Metrics-Serverwird normalerweise für Amazon EKS- und Kubernetes-Bereitstellungen verwendet, um Metriken zu aggregieren, kurzfristige historische Informationen zu Metriken bereitzustellen und Funktionen wieHorizontal Pod Autoscaleraus.

Amazon EKS stellt Metriken der Steuerungsebene über den Kubernetes API-Server bereitim Prometheus-Formatund CloudWatch kann diese Metriken erfassen und aufnehmen. CloudWatch und Container Insights können auch so konfiguriert werden, dass sie umfassende Metriken Erfassung, Analyse und Alarmierung für Ihre Amazon EKS-Knoten und Pods bereitstellen.

Kubernetes-Steuerebene Metriken

Kubernetes macht Steuerungseben-Metriken in einem Prometheus-Format verfügbar, indem es`/metrics`HTTP-API-Endpunkt. Sie sollten installierenPrometheusin Ihrem Kubernetes-Cluster, um

diese Metriken mit einem Webbrowser zu grafieren und anzuzeigen. Sie könnendie aufgedeckten Metriken aufnehmenvom Kubernetes API-Server in CloudWatch.

Knoten- und Systemmetriken für Kubernetes

Kubernetes bietet den PrometheusMetrik-ServerPod, dass du kannstbereitstellen und ausführenauf Ihren Kubernetes-Clustern für CPU- und Speicherstatistiken auf Cluster-, Knoten- und Pod-Ebene. Diese Metriken werden mit demHorizontal Pod AutoscalerundVertical Pod Autoscaleraus. CloudWatch kann diese Metriken auch bereitstellen.

Sie sollten den Kubernetes Metrics Server installieren, wenn Sie dieKubernetes-Dashboardoder die horizontalen und vertikalen Pod-Autoscaler. Das Kubernetes Dashboard hilft Ihnen, Ihren Kubernetes-Cluster, Ihre Knoten, Pods und die zugehörige Konfiguration zu durchsuchen und zu konfigurieren und die CPU- und Speichermetriken vom Kubernetes Metrics Server anzuzeigen. Sie können diese Lösung für einzelne Cluster bereitstellen, indem Sie die Schritte imStellen Sie das Kubernetes-Dashboard bereitin der Amazon EKS-Dokumentation.

Die vom Kubernetes Metriken Server bereitgestellten Metriken können nicht für nicht automatische Skalierungszwecke verwendet werden (z. B. Die Metriken sind bestimmt für point-in-time Analyse und keine historische Analyse. Das Kubernetes Dashboard stellt die`dashboard-metrics-scraper`um Metriken vom Kubernetes Metrics Server für ein kurzes Zeitfenster zu speichern.

Container Insights verwendet eine containerisierte Version des CloudWatch Agent, der in einem Kubernetes läuft DaemonSet um alle laufenden Container in einem Cluster zu erkennen und Metriken auf Knotenebene bereitzustellen. Es sammelt Leistungsdaten auf jeder Ebene des Performance-Stacks. Sie können den Quick Start vonAWSSchnellstarts oder konfigurieren Sie Container Insights separat. Der Quick Start richtet die Metriküberwachung mit CloudWatch Agent und Protokollierung mit Fluent Bit, sodass Sie ihn nur einmal zur Protokollierung und Überwachung bereitstellen müssen.

Da es sich bei Amazon EKS-Knoten um EC2-Instanzen handelt, sollten Sie zusätzlich zu den von Container Insights erfassten Metriken Kennzahlen auf Systemebene erfassen, indem Sie die für Amazon EC2 definierten Standards verwenden. Sie können den gleichen Ansatz vonEinrichten von State Manager und Distributor für CloudWatch Bereitstellung und Konfiguration von Agenten-Abschnitt dieses Handbuchs zum Installieren und Konfigurieren der CloudWatch -Agent für Ihre Amazon EKS-Cluster. Sie können Ihre Amazon EKS spezifische CloudWatch-Konfigurationsdatei aktualisieren, um Metriken sowie Ihre Amazon EKS-spezifische Protokollkonfiguration einzuschließen.

Die CloudWatch Agent mit Prometheus-Unterstützung kann die Prometheus-Metriken automatisch erkennen und abkratzenunterstützte, containerisierte Workloads und Systemeaus. Es nimmt sie als CloudWatch meldet sich im eingebetteten Metrikformat zur Analyse mit CloudWatch Protokolliert Insights und erstellt automatisch CloudWatch-Metriken.

> **Important**
>
> Sie müssenBereitstellen einer spezialisierten Versionder CloudWatch -Agent zum Erfassen von Prometheus-Metriken. Dies ist ein separater Agent von der CloudWatch Der -Agent wurde für Container Insights bereitgestellt. Sie können dasprometheus_jmxBeispiel-Java-Anwendung, die die Bereitstellungs- und Konfigurationsdateien für die CloudWatch Agent- und Amazon EKS-Pod-Bereitstellung zur Demonstration der Prometheus-Metriken. Weitere Informationen finden Sie unterJava/JMX-Beispiel-Workload für Amazon EKS und Kubernetes einrichtenin der CloudWatch-Dokumentation. Sie können auch die CloudWatch Agent zum Erfassen von Metriken von anderen Prometheus-Zielen, die in Ihrem Amazon EKS-Cluster ausgeführt werden.

Anwendungsmetriken

Sie können eigene benutzerdefinierte Metriken mit derEinbettetes Metrikformat in CloudWatch Um Anweisungen im eingebetteten Metrikformat aufzunehmen, müssen Sie eingebettete Metrikformateinträge an einen Endpunkt im eingebetteten Metrikformat senden. Die CloudWatch Agent kann alsBeiwagen-Container in Ihrem Amazon EKS Podaus. Die CloudWatch Agentenkonfiguration wird als Kubernetes gespeichert ConfigMap und lese von deinem CloudWatch Agent-Sidecar-Container zum Starten des Endpunkts im eingebetteten Metrikformat.

Sie können Ihre Anwendung auch als Prometheus-Ziel einrichten und den CloudWatch-Agenten mit Prometheus-Unterstützung konfigurieren, um Ihre Metriken in CloudWatch zu erkennen, zu kratzen und aufzunehmen. Sie können beispielsweise dieOpen-Source-JMX-Exporteurmit Ihren Java-Anwendungen, um JMX Beans für den Prometheus-Konsum durch den CloudWatch -Agent.

Wenn Sie das eingebettete Metrikformat nicht verwenden möchten, können Sie CloudWatch-Metriken auch mithilfe vonAWSAPIoderAWS SDKaus. Es ist allerdings nicht zu empfehlen, da er die Überwachung und die Anwendungslogik mischt.

Metriken für Amazon EKS auf Fargate

Fargate stellt Amazon EKS-Knoten automatisch bereit, um Ihre Kubernetes-Pods auszuführen, sodass Sie keine Kennzahlen auf Knotenebene überwachen und sammeln müssen. Sie müssen jedoch Metriken für Pods überwachen, die auf Ihren Amazon EKS-Knoten auf Fargate ausgeführt werden. Container Insights ist derzeit für Amazon EKS auf Fargate nicht verfügbar, da die folgenden Funktionen erforderlich sind, die derzeit nicht unterstützt werden:

- DaemonSets werden derzeit nicht unterstützt. Container Insights wird durch Ausführen des CloudWatch Der -Agent als DaemonSet auf jedem Clusterknoten.
- Persistente HostPath-Volumes werden nicht unterstützt. Die CloudWatch Agent-Container verwendet persistente HostPath-Volumes als Voraussetzung für das Sammeln von Container-Metrikdaten.
- Fargate verhindert privilegierte Container und den Zugriff auf Hostinformationen.

Sie können dasintegrierter Log-Router für Fargateum Anweisungen im eingebetteten Metrikformat an CloudWatch zu senden. Der Log-Router verwendet Fluent Bit, das eine CloudWatch -Plugin, das konfiguriert werden kann, um Anweisungen im eingebetteten Metrikformat zu unterstützen

Sie können Metriken auf Pod-Ebene für Ihre Fargate-Knoten abrufen und erfassen, indem Sie den Prometheus-Server in Ihrem Amazon EKS-Cluster bereitstellen, um Metriken von Ihren Fargate-Knoten zu sammeln. Da Prometheus dauerhaften Speicher benötigt, können Sie Prometheus auf Fargate bereitstellen, wenn Sie Amazon Elastic File System (Amazon EFS) für dauerhaften Speicher verwenden. Sie können Prometheus auch auf einem von Amazon EC2 unterstützten Knoten bereitstellen. Weitere Informationen finden Sie unterÜberwachung von Amazon EKSAWS Fargatemit Prometheus und Grafanaauf derAWSBlog-Test.

Prometheus-Überwachung auf Amazon EKS

Amazon Managed Service for Prometheusbietet ein skalierbares, sicheres,AWSManaged Service für Open-Source-Prometheus. Sie können die Prometheus-Abfragesprache (PromQL) verwenden, um die Leistung von containerisierten Workloads zu überwachen, ohne die zugrunde liegende Infrastruktur für die Aufnahme, Speicherung und Abfrage operativer Metriken zu verwalten. Sie können Prometheus-Metriken von Amazon EKS und Amazon ECS sammeln, indem SieAWSDistro für OpenTelemetry (ADOT)oder Prometheus-Server als Sammelagenten.

Überwachung von CloudWatch Container Insights for Prometheusermöglicht das Konfigurieren und Verwenden des CloudWatch Agent, um Prometheus-Metriken aus Amazon ECS-, Amazon EKS- und Kubernetes-Workloads zu ermitteln und sie als CloudWatch-Metriken aufzunehmen. Diese Lösung ist angemessen, wenn CloudWatch ist Ihre primäre Beobachtungs- und Überwachungslösung. In der folgenden Liste werden jedoch Anwendungsfälle beschrieben, in denen Amazon Managed Service for Prometheus mehr Flexibilität beim Aufnehmen, Speichern und Abfragen von Prometheus-Metriken bietet:

- Amazon Managed Service for Prometheus ermöglicht es Ihnen, vorhandene Prometheus-Server zu verwenden, die in Amazon EKS oder selbstverwalteten Kubernetes bereitgestellt werden, und diese so zu konfigurieren, dass sie anstelle eines lokal konfigurierten Datenspeichers an Amazon Managed Service for Prometheus schreiben. Dies beseitigt die undifferenzierte starke Verwaltung eines hochverfügbaren Datenspeichers für Ihre Prometheus-Server und seine Infrastruktur. Amazon Managed Service for Prometheus ist eine geeignete Wahl, wenn Sie eine ausgereifte Prometheus-Bereitstellung haben, die Sie in derAWSCloud.
- Grafana unterstützt Prometheus direkt als Datenquelle für die Visualisierung. Wenn Sie Grafana mit Prometheus anstelle von verwenden möchten CloudWatch Dashboards für Ihre Containerüberwachung, dann könnte Amazon Managed Service for Prometheus Ihre Anforderungen erfüllen. Amazon Managed Service for Prometheus lässt sich in Amazon Managed Grafana integrieren, um eine verwaltete Open-Source-Überwachungs- und Visualisierungslösung bereitzustellen.
- Prometheus ermöglicht es Ihnen, mithilfe von PromQL-Abfragen eine Analyse Ihrer operativen Metriken durchzuführen. Im Gegensatz dazudie CloudWatch -Agent erfasst Prometheus-Metriken im eingebetteten Metrikformatin CloudWatch Protokolle, die dazu führen CloudWatch -Metriken. Sie können Protokolle im eingebetteten Metrikformat abfragen, indem Sie CloudWatch Protokolliert Insights.

- Wenn Sie nicht vorhaben zu verwenden CloudWatch zur Überwachung und Erfassung von Metriken sollten Sie Amazon Managed Service for Prometheus mit Ihrem Prometheus-Server und einer Visualisierungslösung wie Grafana verwenden. Sie müssen Ihren Prometheus-Server so konfigurieren, dass er Metriken von Ihren Prometheus-Zielen abkratzt und den Server so konfigurieren kannRemote-Schreiben an Ihren Amazon Managed Service for Prometheus-Workspaceaus. Wenn Sie Amazon Managed Grafana verwenden, können SieIntegrieren Sie Amazon Managed Grafana direkt mit Ihrer Amazon Managed Service for Prometheus-Datenquelle, indem Sie das mitgelieferte Plugin verwendenaus. Da Metrikdaten in Amazon Managed Service für Prometheus gespeichert werden, besteht keine Abhängigkeit zur Bereitstellung des CloudWatch Agent oder Anforderung, Daten in CloudWatch aufzunehmen. Die CloudWatch -Agent ist für die Überwachung von Container Insights auf Prometheus erforderlich.

Sie können den ADOT Collector auch verwenden, um aus einer Prometheus-instrumentierten Anwendung zu kratzen und die Metriken an Amazon Managed Service for Prometheus zu senden. Weitere Informationen zum ADOT Collector finden Sie unterAWSDistro für OpenTelemetry-Dokumentation.

Protokollierung und Metriken fürAWS Lambda

Lambdamacht die Verwaltung und Überwachung von Servern für Ihre Workloads überflüssig und funktioniert automatisch mit CloudWatchMetriken und CloudWatch Protokolliert den Code Ihrer Anwendung ohne weitere Konfiguration oder Instrumentierung. Dieser Abschnitt hilft Ihnen, die Leistungsmerkmale der von Lambda verwendeten Systeme zu verstehen und zu verstehen, wie sich Ihre Konfigurationsentscheidungen auf die Leistung auswirken. Er hilft Ihnen auch dabei, Ihre Lambda-Funktionen zu protokollieren und zu überwachen, um die Leistung zu optimieren und Probleme auf Anwendungsebene zu diagnostizieren.

Protokollierung von Lambda-Funktionen

Lambda streamt automatisch Standardausgaben und Standardfehlermeldungen von einer Lambda-Funktion zu CloudWatch Protokolle, ohne dass Protokollierungstreiber erforderlich sind. Lambda stellt außerdem automatisch Container bereit, auf denen Ihre Lambda-Funktion ausgeführt wird, und konfiguriert sie so, dass Protokollnachrichten in separaten Protokollströmen ausgegeben werden.

Nachfolgende Aufrufe Ihrer Lambda-Funktion können denselben Container wiederverwenden und in denselben Protokollstream ausgeben. Lambda kann auch einen neuen Container bereitstellen und den Aufruf in einem neuen Protokollstream ausgeben.

Lambda erstellt automatisch eine Protokollgruppe, wenn Ihre Lambda-Funktion zum ersten Mal aufgerufen wird. Lambda-Funktionen können mehrere Versionen haben und Sie können die Version auswählen, die Sie ausführen möchten. Alle Protokolle für die Aufrufe der Lambda-Funktion werden in derselben Protokollgruppe gespeichert. Der Name kann nicht geändert werden und befindet sich im`/aws/lambda/<YourLambdaFunctionName>`Format. In der Protokollgruppe wird für jede Lambda-Funktionsinstanz ein separater Protokollstream erstellt. Lambda hat eine Standardbenennungskonvention für Protokollstreams, die a verwendet`YYYY/MM/DD/[<FunctionVersion>]<InstanceId>`Format. Das`InstanceId`wird generiert vonAWSum die Lambda-Funktionsinstanz zu identifizieren.

Wir empfehlen Ihnen, Ihre Protokollnachrichten im JSON-Format zu formatieren, da Sie sie einfacher abfragen können mit CloudWatch Logt Einblicke. Sie können auch einfacher gefiltert und exportiert werden. Sie können eine Logging-Bibliothek verwenden, um diesen Vorgang zu vereinfachen, oder Ihre eigenen Funktionen zur Protokollverarbeitung schreiben. Wir empfehlen Ihnen, eine Logging-Bibliothek zu verwenden, um Protokollnachrichten zu formatieren und zu

klassifizieren. Wenn Ihre Lambda-Funktion beispielsweise in Python geschrieben ist, können Sie diePython-Protokollierungsmodulum Nachrichten zu protokollieren und das Ausgabeformat zu kontrollieren. Lambda verwendet nativ die Python-Logging-Bibliothek für in Python geschriebene Lambda-Funktionen, und Sie können den Logger innerhalb Ihrer Lambda-Funktion abrufen und anpassen.AWS Labs hat das erstelltAWSLambda Powertools für PythonEntwickler-Toolkit zur einfacheren Anreicherung von Protokollnachrichten mit wichtigen Daten wie Kaltstarts. Das Toolkit ist für Python, Java, Typescript und .NET verfügbar.

Eine weitere bewährte Methode besteht darin, den Protokollausgabepegel mithilfe einer Variablen festzulegen und ihn an die Umgebung und Ihre Anforderungen anzupassen. Der Code Ihrer Lambda-Funktion könnte zusätzlich zu den verwendeten Bibliotheken je nach Protokollausgabestufe eine große Menge an Protokolldaten ausgeben. Dies kann sich auf Ihre Protokollierungskosten und die Leistung auswirken.

Mit Lambda können Sie Umgebungsvariablen für Ihre Lambda-Funktions-Laufzeitumgebung festlegen, ohne Ihren Code aktualisieren zu müssen. Sie können beispielsweise eine erstellen`LAMBDA_LOG_LEVEL`Umgebungsvariable, die die Protokollausgabeebene definiert, die Sie aus Ihrem Code abrufen können. Im folgenden Beispiel wird versucht, eine abzurufen`LAMBDA_LOG_LEVEL`Umgebungsvariable und verwenden Sie den Wert, um die Logging-Ausgabe zu definieren. Wenn die Umgebungsvariable nicht gesetzt ist, ist sie standardmäßig`INFO`Ebene.

```
import logging
from os import getenv

logger = logging.getLogger()
log_level = getenv("LAMBDA_LOG_LEVEL", "INFO")
level = logging.getLevelName(log_level)
logger.setLevel(level)
```

Logs an andere Ziele senden von CloudWatch

Sie können Protokolle an andere Ziele senden (z. B. an Amazon OpenSearch Service oder eine Lambda-Funktion) mithilfe von Abonnementfiltern. Wenn Sie Amazon nicht verwenden OpenSearch Service, Sie können eine Lambda-Funktion verwenden, um die Protokolle zu verarbeiten und sie an einen zu sendenAWSService Ihrer Wahl unter Verwendung desAWSSDKs.

Sie können SDKs auch für Protokollziele außerhalb des verwendenAWSCloud in Ihrer Lambda-Funktion, um Protokollanweisungen direkt an ein Ziel Ihrer Wahl zu senden. Wenn Sie sich für diese Option entscheiden, empfehlen wir Ihnen, die Auswirkungen der Latenz, der zusätzlichen Verarbeitungszeit, der Fehler- und Wiederholungsbehandlung sowie der Kopplung der Betriebslogik mit Ihrer Lambda-Funktion zu berücksichtigen.

Lambda-Funktionsmetriken

Mit Lambda können Sie Ihren Code ausführen, ohne Server verwalten oder skalieren zu müssen. Dadurch entfällt fast der Aufwand für Prüfungen und Diagnosen auf Systemebene. Es ist jedoch weiterhin wichtig, die Leistungs- und Aufrufmetriken auf Systemebene für Ihre Lambda-Funktionen zu verstehen. Dies hilft Ihnen, die Ressourcenkonfiguration zu optimieren und die Codeleistung zu verbessern. Durch eine effektive Überwachung und Messung der Leistung können Sie die Benutzererfahrung verbessern und Ihre Kosten senken, indem Sie Ihre Lambda-Funktionen entsprechend dimensionieren. In der Regel verfügen Workloads, die als Lambda-Funktionen ausgeführt werden, auch über Metriken auf Anwendungsebene, die erfasst und analysiert werden müssen. Lambda unterstützt direkt das eingebettete metrische Format, um die Erfassung auf Anwendungsebene zu ermöglichen CloudWatch Metriken einfacher.

Metriken auf Systemebene

Lambda integriert sich automatisch mit CloudWatch Metriken und bietet eine Reihe vonStandardmetriken für Ihre Lambda-Funktionen. Lambda bietet außerdem ein separates Monitoring-Dashboard für jede Lambda-Funktion mit diesen Metriken. Zwei wichtige Metriken, die Sie überwachen müssen, sind Fehler und Aufruffehler. Wenn Sie die Unterschiede zwischen Aufruffehlern und anderen Fehlertypen verstehen, können Sie Lambda-Bereitstellungen diagnostizieren und unterstützen.

Aufruffehlerverhindern Sie, dass Ihre Lambda-Funktion ausgeführt wird. Diese Fehler treten auf, bevor Ihr Code ausgeführt wird, sodass Sie in Ihrem Code keine Fehlerbehandlung implementieren können, um sie zu identifizieren. Stattdessen sollten Sie Alarme für Ihre Lambda-Funktionen konfigurieren, die diese Fehler erkennen und die Betriebs- und Workload-Besitzer benachrichtigen. Diese Fehler hängen häufig mit einem Konfigurations- oder Berechtigungsfehler zusammen und können aufgrund einer Änderung Ihrer Konfiguration oder Ihrer Berechtigungen auftreten. Aufruffehler können zu einem erneuten Versuch führen, was zu mehreren Aufrufen Ihrer Funktion führt.

Eine erfolgreich aufgerufene Lambda-Funktion gibt eine HTTP 200-Antwort zurück, auch wenn von der Funktion eine Ausnahme ausgelöst wird. Ihre Lambda-Funktionen sollten eine Fehlerbehandlung implementieren und Ausnahmen auslösen, sodass`Errors`Metrik erfasst und identifiziert fehlgeschlagene Ausführungen Ihrer Lambda-Funktion. Sie sollten eine formatierte Antwort von Ihren Lambda-Funktionsaufrufen zurückgeben, die Informationen enthält, anhand derer Sie feststellen können, ob die Ausführung vollständig, teilweise oder erfolgreich fehlgeschlagen ist.

CloudWatch bietetCloudWatch Lambda Insightsdie Sie für einzelne Lambda-Funktionen aktivieren können. Lambda Insights sammelt, aggregiert und fasst Metriken auf Systemebene zusammen (z. B. CPU-Zeit, Arbeitsspeicher-, Festplatten- und Netzwerknutzung). Lambda Insights sammelt, aggregiert und fasst auch Diagnoseinformationen zusammen (z. B. Kaltstarts und Lambda-Worker-Shutdowns), um Ihnen zu helfen, Probleme zu isolieren und schnell zu lösen.

Lambda Insights verwendet das eingebettete Metrikformat, um automatisch Leistungsinformationen an die`/aws/lambda-insights/`Protokollgruppe mit einem Log-Stream-Namenspräfix, das auf dem Namen Ihrer Lambda-Funktion basiert. Diese Leistungsprotokollereignisse erzeugen CloudWatch Metriken, die die Grundlage für automatische CloudWatch Dashboards. Wir empfehlen, Lambda Insights für Leistungstests und Produktionsumgebungen zu aktivieren. Zu den weiteren von Lambda Insights erstellten Metriken gehören`memory_utilization`Dies hilft dabei, die Lambda-Funktionen richtig zu dimensionieren, sodass Sie nicht für nicht benötigte Kapazität bezahlen müssen.

Anwendungsmetriken

Sie können auch Ihre eigenen Anwendungsmetriken in erstellen und erfassen CloudWatch unter Verwendung des eingebetteten metrischen Formats. Sie können es nutzenAWS stellte Bibliotheken für das eingebettete metrische Format zur Verfügungum Anweisungen im eingebetteten metrischen Format zu erstellen und auszugeben an CloudWatch. Das integrierte Lambda CloudWatch Die Protokollierungsfunktion ist so konfiguriert, dass sie entsprechend formatierte Anweisungen im eingebetteten metrischen Format verarbeitet und extrahiert.

Logs suchen und analysieren CloudWatch

Nachdem Ihre Protokolle und Kennzahlen in einem konsistenten Format und an einem einheitlichen Ort erfasst wurden, können Sie sie durchsuchen und analysieren, um die betriebliche Effizienz zu verbessern und Probleme zu identifizieren und zu beheben. Wir empfehlen, dass Sie Ihre Protokolle in einem wohlgeformten Format (z. B. JSON) erfassen, um die Suche und Analyse Ihrer Protokolle zu vereinfachen. Die meisten Workloads verwenden eine Sammlung vonAWS Ressourcen wie Netzwerk, Rechenleistung, Speicher und Datenbanken. Wenn möglich, sollten Sie die Metriken und Protokolle dieser Ressourcen gemeinsam analysieren und miteinander korrelieren, um all IhreAWS Workloads effektiv überwachen und verwalten zu können.

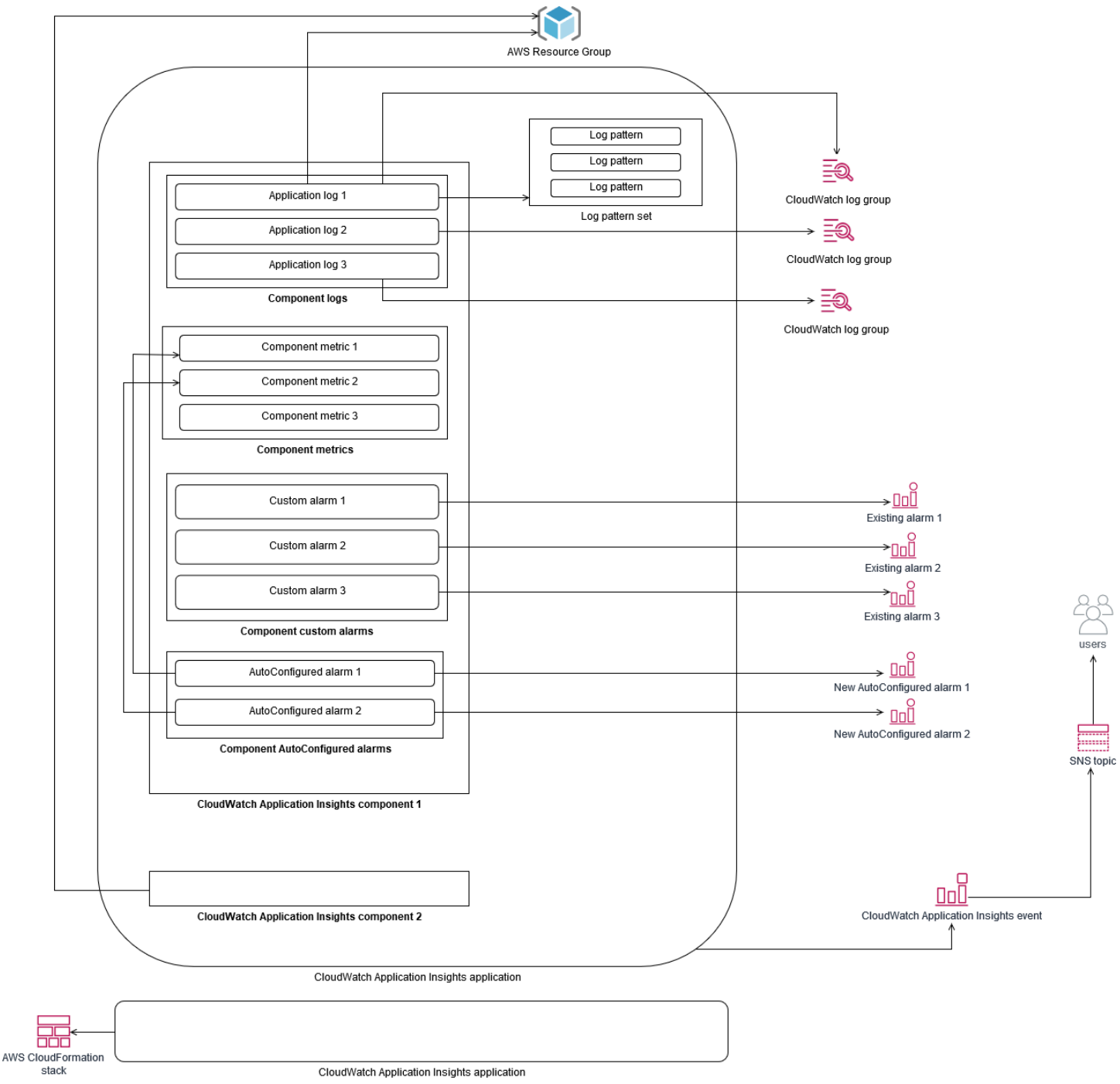
CloudWatch bietet verschiedene Funktionen zur Analyse von Protokollen und Metriken, z. B. CloudWatch Application Insights zur kollektiven Definition und Überwachung von Metriken und Protokollen für eine Anwendung über verschiedeneAWS Ressourcen hinweg, CloudWatch Anomalieerkennung zur Erkennung von Anomalien für Metriken und CloudWatch Log Insights zum interaktiven Durchsuchen und Analysieren Ihrer Protokolldaten in CloudWatch Logs

Überwachen und analysieren Sie Anwendungen gemeinsam mit CloudWatch Application Insights

Anwendungsinhaber können Amazon CloudWatch Application Insights verwenden, um die automatische Überwachung und Analyse von Workloads einzurichten. Dies kann zusätzlich zur Standardüberwachung auf Systemebene konfiguriert werden, die für alle Workloads in einem Konto konfiguriert ist. Die Einrichtung einer Überwachung über CloudWatch Application Insights kann Anwendungsteams auch dabei helfen, sich proaktiv auf den Betrieb auszurichten und die mittlere Wiederherstellungszeit (MTTR) zu reduzieren. CloudWatch Application Insights kann dazu beitragen, den Aufwand für die Einrichtung von Protokollierung und Überwachung auf Anwendungsebene zu reduzieren. Es bietet auch ein komponentenbasiertes Framework, das Teams bei der Aufteilung der Protokollierungs- und Überwachungsaufgaben unterstützt.

CloudWatch Application Insights verwendet Ressourcengruppen, um die Ressourcen zu identifizieren, die als Anwendung gemeinsam überwacht werden sollten. Die unterstützten Ressourcen in der Ressourcengruppe werden zu individuell definierten Komponenten Ihrer CloudWatch Application Insights-Anwendung. Jede Komponente Ihrer CloudWatch Application Insights-Anwendung hat ihre eigenen Protokolle, Metriken und Alarme.

Für Protokolle definieren Sie den Protokollmustersatz, der für die Komponente und in Ihrer CloudWatch Application Insights-Anwendung verwendet werden soll. Ein Protokollmustersatz ist eine Sammlung von Protokollmustern, nach denen auf der Grundlage regulärer Ausdrücke gesucht werden soll, zusammen mit einem niedrigen, mittleren oder hohen Schweregrad für den Zeitpunkt, zu dem das Muster erkannt wird. Für Metriken wählen Sie die zu überwachenden Metriken für jede Komponente aus einer Liste dienstspezifischer und unterstützter Metriken aus. Für Alarme erstellt und konfiguriert CloudWatch Application Insights automatisch Standard- oder Anomalieerkennungsalarme für die zu überwachenden Metriken. CloudWatch Application Insights verfügt über automatische Konfigurationen für Metriken und Protokollerfassung für die Technologien, die in den von CloudWatch Application Insights unterstützten Protokollen und Metriken in der CloudWatch Dokumentation beschrieben sind. Das folgende Diagramm zeigt die Beziehungen zwischen CloudWatch Application Insights-Komponenten und ihren Protokollierungs- und Überwachungskonfigurationen. Jede Komponente hat ihre eigenen Protokolle und Metriken definiert, die mithilfe von CloudWatch Protokollen und Metriken überwacht werden sollen.



EC2-Instances, die von CloudWatch Application Insights überwacht werden, benötigen den Systems Manager sowie CloudWatch Agenten und Berechtigungen. Weitere Informationen dazu finden Sie in der CloudWatch Dokumentation unter Voraussetzungen für die Konfiguration einer CloudWatch Anwendung mit Application Insights. CloudWatch Application Insights verwendet Systems Manager, um den CloudWatch Agenten zu installieren und zu aktualisieren. Die in CloudWatch Application Insights konfigurierten Metriken und Protokolle erstellen eine

CloudWatch Agentenkonfigurationsdatei, die in einem Systems Manager Manager-Parameter mit dem`AmazonCloudWatch-ApplicationInsights-SSMParameter` Präfix für jede CloudWatch Application Insights-Komponente gespeichert wird. Dies führt dazu, dass dem CloudWatch Agentenkonfigurationsverzeichnis auf der EC2-Instance eine separate CloudWatch Agentenkonfigurationsdatei hinzugefügt wird. Ein Systems Manager Manager-Befehl wird ausgeführt, um diese Konfiguration an die aktive Konfiguration auf der EC2-Instance anzuhängen. Die Verwendung von CloudWatch Application Insights hat keine Auswirkungen auf die bestehenden CloudWatch Agentenkonfigurationseinstellungen. Sie können CloudWatch Application Insights zusätzlich zu Ihren eigenen CloudWatch Agentenkonfigurationen auf System- und Anwendungsebene verwenden. Sie sollten jedoch sicherstellen, dass sich die Konfigurationen nicht überschneiden.

Durchführung von Protokollanalysen mit CloudWatch Logs Insights

CloudWatch Logs Insights macht es einfach, mehrere Protokollgruppen mithilfe einer einfachen Abfragesprache zu durchsuchen. Wenn Ihre Anwendungsprotokolle im JSON-Format strukturiert sind, erkennt CloudWatch Logs Insights automatisch die JSON-Felder in Ihren Protokollstreams in mehreren Protokollgruppen. Sie können CloudWatch Logs Insights verwenden, um Ihre Anwendungs- und Systemprotokolle zu analysieren, wodurch Ihre Abfragen für die future Verwendung gespeichert werden. Die Abfragesyntax für CloudWatch Logs Insights unterstützt Funktionen wie die Aggregation mit Funktionen, z. B. sum (), avg (), count (), min () und max (), die bei der Fehlerbehebung in Ihren Anwendungen oder bei der Leistungsanalyse hilfreich sein können.

Wenn Sie das eingebettete Metrikformat zum Erstellen von CloudWatch Metriken verwenden, können Sie Ihre Protokolle im eingebetteten Metrikformat abfragen, um mithilfe der unterstützten Aggregationsfunktionen einmalige Metriken zu generieren. Dies trägt dazu bei, Ihre CloudWatch Überwachungskosten zu senken, indem Datenpunkte erfasst werden, die für die Generierung bestimmter Kennzahlen erforderlich sind, auf Bedarfsbasis, anstatt sie aktiv als benutzerdefinierte Metriken zu erfassen. Dies ist besonders effektiv für Dimensionen mit hoher Kardinalität, die zu einer großen Anzahl von Metriken führen würden. CloudWatch Container Insights verfolgt diesen Ansatz ebenfalls und erfasst detaillierte Leistungsdaten, generiert jedoch nur CloudWatch Metriken für eine Teilmenge dieser Daten.

Beispielsweise generiert der folgende eingebettete Metrikeintrag nur einen begrenzten Satz von CloudWatch Metriken aus den Metrikdaten, die in der Anweisung zum eingebetteten Metrikformat erfasst wurden:

```
{
 "AutoScalingGroupName": "eks-e0bab7f4-fa6c-64ba-dbd9-094aee6cf9ba",
 "CloudWatchMetrics": [
 {
 "Metrics": [
 {
 "Unit": "Count",
 "Name": "pod_number_of_container_restarts"
 }
 ],
 "Dimensions": [
 [
 "PodName",
 "Namespace",
 "ClusterName"
 ]
 ],
 "Namespace": "ContainerInsights"
 }
 ],
 "ClusterName": "eksdemo",
 "InstanceId": "i-03b21a16b854aa4ca",
 "InstanceType": "t3.medium",
 "Namespace": "amazon-cloudwatch",
 "NodeName": "ip-172-31-10-211.ec2.internal",
 "PodName": "cloudwatch-agent",
 "Sources": [
 "cadvisor",
 "pod",
 "calculated"
 ],
 "Timestamp": "1605111338968",
 "Type": "Pod",
 "Version": "0",
 "pod_cpu_limit": 200,
 "pod_cpu_request": 200,
 "pod_cpu_reserved_capacity": 10,
 "pod_cpu_usage_system": 3.268605094109382,
 "pod_cpu_usage_total": 8.899539221131045,
 "pod_cpu_usage_user": 4.160042847048305,
 "pod_cpu_utilization": 0.44497696105655227,
 "pod_cpu_utilization_over_pod_limit": 4.4497696105655224,
 "pod_memory_cache": 4096,
```

```
 "pod_memory_failcnt": 0,
 "pod_memory_hierarchical_pgfault": 0,
 "pod_memory_hierarchical_pgmajfault": 0,
 "pod_memory_limit": 209715200,
 "pod_memory_mapped_file": 0,
 "pod_memory_max_usage": 43024384,
 "pod_memory_pgfault": 0,
 "pod_memory_pgmajfault": 0,
 "pod_memory_request": 209715200,
 "pod_memory_reserved_capacity": 5.148439982463127,
 "pod_memory_rss": 38481920,
 "pod_memory_swap": 0,
 "pod_memory_usage": 42803200,
 "pod_memory_utilization": 0.6172094650851303,
 "pod_memory_utilization_over_pod_limit": 11.98828125,
 "pod_memory_working_set": 25141248,
 "pod_network_rx_bytes": 3566.4174629544723,
 "pod_network_rx_dropped": 0,
 "pod_network_rx_errors": 0,
 "pod_network_rx_packets": 3.3495665260575094,
 "pod_network_total_bytes": 4283.442421354973,
 "pod_network_tx_bytes": 717.0249584005006,
 "pod_network_tx_dropped": 0,
 "pod_network_tx_errors": 0,
 "pod_network_tx_packets": 2.6964010534762948,
 "pod_number_of_container_restarts": 0,
 "pod_number_of_containers": 1,
 "pod_number_of_running_containers": 1,
 "pod_status": "Running"
}
```


Sie können die erfassten Metriken jedoch abfragen, um weitere Erkenntnisse zu erhalten. Zum Beispiel können Sie die folgende Abfrage ausführen, um die letzten 20 Pods mit Speicherseitenfehlern zu ermitteln:

```
fields @timestamp, @message
| filter (pod_memory_pgfault > 0)
| sort @timestamp desc
| limit 20
```

Durchführung von Protokollanalysen mit Amazon OpenSearch Service

CloudWatch lässt sich in Amazon OpenSearch Service integrieren, indem Sie Protokolldaten aus CloudWatch Protokollgruppen mit einem Abonnementfilter in einen Amazon OpenSearch Service-Cluster Ihrer Wahl streamen können. Sie können es CloudWatch für die Erfassung und Analyse von primären Protokollen und Metriken verwenden und es dann mit Amazon OpenSearch Service für die folgenden Anwendungsfälle erweitern:

- Präzise Datenzugriffskontrolle — Amazon OpenSearch Service ermöglicht es Ihnen, den Zugriff auf Daten bis auf Feldebene zu beschränken, und hilft dabei, Daten in Feldern auf der Grundlage von Benutzerberechtigungen zu anonymisieren. Dies ist nützlich, wenn Sie Unterstützung bei der Problembehandlung benötigen, ohne vertrauliche Daten preiszugeben.
- Aggregieren und durchsuchen Sie Protokolle über mehrere Konten, Regionen und Infrastrukturen hinweg — Sie können Ihre Protokolle von mehreren Konten und Regionen in einen gemeinsamen Amazon OpenSearch Service-Cluster streamen. Ihre zentralisierten Betriebsteams können Trends und Probleme analysieren und kontenübergreifende und regionsübergreifende Analysen durchführen. Das Streamen von CloudWatch Protokollen an Amazon OpenSearch Service hilft Ihnen auch dabei, eine regionsübergreifende Anwendung an einem zentralen Ort zu suchen und zu analysieren.
- Senden und erweitern Sie Protokolle mithilfe von ElasticSearch Agenten direkt an Amazon OpenSearch Service — Ihre Anwendungs- und Technologie-Stack-Komponenten können Betriebssysteme verwenden, die vom CloudWatch Agenten nicht unterstützt werden. Möglicherweise möchten Sie die Protokolldaten auch anreichern und transformieren, bevor sie an Ihre Protokollierungslösung gesendet werden. Amazon OpenSearch Service unterstützt Standard-Elasticsearch-Clients wie Data Shippers der Elastic Beats-Familie und Logstash, die die Anreicherung und Transformation von Protokollen unterstützen, bevor die Protokolldaten an Amazon OpenSearch Service gesendet werden.
- Die bestehende Betriebsmanagementlösung verwendet einen ElasticSearchLogstash, Kibana (ELK) -Stack für die Protokollierung und Überwachung. Möglicherweise haben Sie bereits eine erhebliche Investition in Amazon OpenSearch Service oder Open-Source-Elasticsearch getätigt, wobei viele Workloads bereits konfiguriert sind. Möglicherweise haben Sie auch operative Dashboards, die in Kibana erstellt wurden und die Sie weiterhin verwenden möchten.

Wenn Sie keine CloudWatch Protokolle verwenden möchten, können Sie von Amazon OpenSearch Service unterstützte Agenten, Protokolltreiber und Bibliotheken (z. B. Fluent Bit, Fluentd, Logstash und Open Distro for ElasticSearch API) verwenden, um Ihre Protokolle direkt an Amazon OpenSearch Service zu senden und zu umgehen CloudWatch. Sie sollten jedoch auch eine Lösung zur Erfassung von Protokollen implementieren, die vonAWS Diensten generiert wurden. CloudWatch Logs ist die primäre Lösung zur Protokollerfassung für vieleAWS Dienste, und mehrere Dienste erstellen automatisch neue Protokollgruppen in CloudWatch. Lambda erstellt beispielsweise für jede Lambda-Funktion eine neue Protokollgruppe. Sie können einen Abonnementfilter für eine Protokollgruppe einrichten, um ihre Protokolle an Amazon OpenSearch Service zu streamen. Sie können manuell einen Abonnementfilter für jede einzelne Protokollgruppe konfigurieren, die Sie an Amazon OpenSearch Service streamen möchten. Alternativ können Sie eine Lösung bereitstellen, die automatisch neue Protokollgruppen für ElasticSearch Cluster abonniert. Sie können Protokolle an einen ElasticSearch Cluster im selben Konto oder in einem zentralen Konto streamen. Das Streamen von Protokollen an einen ElasticSearch Cluster im selben Konto hilft Workload-Inhabern, ihre Workloads besser zu analysieren und zu unterstützen.

Sie sollten erwägen, einen ElasticSearch Cluster in einem zentralen oder gemeinsam genutzten Konto einzurichten, um Protokolle für Ihre Konten, Regionen und Anwendungen zu aggregieren. Richten Sie beispielsweiseAWS Control Tower ein Logarchive-Konto ein, das für die zentrale Protokollierung verwendet wird. Wenn ein neues Konto erstellt wirdAWS Control Tower, werden seinAWS CloudTrail und seineAWS Config Protokolle an einen S3-Bucket in diesem zentralisierten Konto übermittelt. Die von instrumentierte Protokollierung dientAWS Control Tower der Konfigurations-, Änderungs- und Prüfprotokollierung.

Um eine zentralisierte Lösung zur Analyse von Anwendungsprotokollen mit Amazon OpenSearch Service einzurichten, können Sie einen oder mehrere zentralisierte Amazon OpenSearch Service-Cluster für Ihr zentrales Protokollierungskonto bereitstellen und Protokollgruppen in Ihren anderen Konten konfigurieren, um Protokolle an den zentralen Amazon OpenSearch Service zu streamen. Cluster.

Sie können separate Amazon OpenSearch Service-Cluster erstellen, um verschiedene Anwendungen oder Ebenen Ihrer Cloud-Architektur zu verarbeiten, die möglicherweise auf Ihre Konten verteilt sind. Durch die Verwendung separater Amazon OpenSearch Service-Cluster können Sie Ihr Sicherheits- und Verfügbarkeitsrisiko reduzieren. Ein gemeinsamer Amazon OpenSearch Service-Cluster kann das Suchen und Verknüpfen von Daten innerhalb desselben Clusters erleichtern.

Alarmierende Optionen mit CloudWatch

Durch die einmalige und automatisierte Analyse wichtiger Metriken können Sie Probleme erkennen und lösen, bevor sie sich auf Ihre Workloads auswirken. CloudWatch macht es einfach, mehrere Metriken zu grafieren und zu vergleichen, indem mehrere Statistiken über einen bestimmten Zeitraum verwendet werden. Sie können es verwenden CloudWatch um alle Metriken mit den erforderlichen Dimensionswerten zu durchsuchen, um die Metriken zu finden, die Sie für Ihre Analyse benötigen.

Wir empfehlen Ihnen, Ihren Ansatz zur Metrikenerfassung zu beginnen, indem Sie einen ersten Satz von Metriken und Dimensionen einbeziehen, die als Baseline für die Überwachung einer Workload verwendet werden sollen. Im Laufe der Zeit reift die Arbeitslast und Sie können zusätzliche Metriken und Dimensionen hinzufügen, um sie weiter zu analysieren und zu unterstützen. Ihre Anwendungen oder Workloads verwenden möglicherweise mehrereAWSRessourcen und über eigene benutzerdefinierte Metriken sollten Sie diese Ressourcen unter einem Namespace gruppieren, um sie leichter zu identifizieren.

Sie sollten auch überlegen, wie Protokollierungs- und Überwachungsdaten korreliert sind, damit Sie schnell die relevanten Protokollierungs- und Überwachungsdaten identifizieren können, um bestimmte Probleme zu diagnostizieren. Sie können es verwendenCloudWatch-ServiceLensum Traces, Metriken, Protokolle und Alarme für die Diagnose von Problemen zu korrelieren. Sie sollten auch erwägen, zusätzliche Dimensionen in Metriken und Kennungen in Protokolle für Ihre Workloads einzubeziehen, damit Sie schnell nach Problemen zwischen Systemen und Diensten suchen und identifizieren können.

benutzen CloudWatch Alarmen zur Überwachung und Alarmen

Sie können es verwendenCloudWatch-Alarmeum die manuelle Überwachung in Ihren Workloads oder Anwendungen zu reduzieren. Sie sollten zunächst die Metriken überprüfen, die Sie für jede Workload-Komponente erfassen, und die entsprechenden Schwellenwerte für jede Metrik ermitteln. Stellen Sie sicher, dass Sie angeben, welche Teammitglieder benachrichtigt werden müssen, wenn ein Schwellenwert überschritten wird. Sie sollten Verteilergruppen einrichten und ansprechen, anstatt einzelne Teammitglieder.

CloudWatch-Alarme können in Ihre Service-Management-Lösung integriert werden, um automatisch neue Tickets zu erstellen und betriebliche Workflows auszuführen. Beispiel,AWSstellt dasAWSService Management Connector fürServiceNowundJira-Service-Deskum Sie dabei zu

unterstützen, Integrationen schnell einzurichten. Dieser Ansatz ist entscheidend, um sicherzustellen, dass erhöhte Alarme anerkannt und auf Ihre bestehenden Arbeitsabläufe abgestimmt werden, die möglicherweise bereits in diesen Produkten definiert sind.

Sie können auch mehrere Alarme für dieselbe Metrik erstellen, die unterschiedliche Schwellenwerte und Auswertungszeiträume aufweisen, was zur Einrichtung eines Eskalationsprozesses beiträgt. Zum Beispiel, Sie haben ein`OrderQueueDepth`Metrik, die Kundenbestellungen verfolgt, können Sie einen niedrigeren Schwellenwert über einen kurzen durchschnittlichen Zeitraum von einer Minute definieren, der die Mitglieder des Anwendungsteams per E-Mail oder benachrichtigtSlackaus. Sie können auch einen weiteren Alarm für dieselbe Metrik über einen längeren Zeitraum von 15 Minuten mit demselben Schwellenwert definieren und diese Seiten, E-Mails und benachrichtigt den Leiter des Anwendungsteams und des Anwendungsteams. Schließlich können Sie einen dritten Alarm für einen harten durchschnittlichen Schwellenwert über einen Zeitraum von 30 Minuten definieren, der das Obermanagement benachrichtigt und alle zuvor benachrichtigten Teammitglieder benachrichtigt. Durch das Erstellen mehrerer Alarme können Sie verschiedene Maßnahmen für verschiedene Bedingungen ergreifen. Sie können mit einem einfachen Benachrichtigungsprozess beginnen und ihn dann nach Bedarf anpassen und verbessern.

benutzen CloudWatch Anomalieerkennung zu überwachen und zu alarmieren

Sie können es verwendenCloudWatch-Anomalieerkennungwenn Sie sich nicht sicher sind, welche Schwellenwerte für eine bestimmte Metrik angewendet werden sollen, oder wenn Sie möchten, dass ein Alarm die Schwellenwerte basierend auf beobachteten historischen Werten automatisch anpasst. CloudWatch Die Anomalieerkennung ist besonders nützlich für Metriken, die regelmäßige, vorhersehbare Änderungen der Aktivität aufweisen können, z. B. tägliche Bestellungen für die Lieferung am selben Tag, die vor einer Stichzeit zunehmen. Die Anomalieerkennung ermöglicht Schwellenwerte, die sich automatisch anpassen und Fehlalarme reduzieren können. Sie können die Anomalieerkennung für jede Metrik und Statistik aktivieren und konfigurieren CloudWatch zu alarmieren basierend auf Ausreißer.

Zum Beispiel können Sie die Anomalieerkennung für den`CPUUtilization`-Metrik und das`AVG`-Statistik einer EC2-Instance. Die Anomalieerkennung verwendet dann bis zu 14 Tage historische Daten, um das Modell des maschinellen Lernens (ML) zu erstellen. Sie können mehrere Alarme mit verschiedenen Anomalieerkennungsbändern erstellen, um einen Alarmeskalationsprozess einzurichten, ähnlich wie beim Erstellen mehrerer Standardalarme mit unterschiedlichen Schwellenwerten.

Weitere Informationen zu diesem Abschnitt finden Sie unterErstellen eines CloudWatch-Alarms basierend auf Anomalieerkennungim CloudWatch -Dokumentation.

Alarmierend in mehreren Regionen und Konten

Anwendungs- und Workload-Besitzer sollten Alarme auf Anwendungsebene für Workloads erstellen, die sich über mehrere Regionen erstrecken. Wir empfehlen, separate Alarme in jedem Konto und jeder Region zu erstellen, in der Ihre Workload bereitgestellt wird. Sie können diesen Prozess vereinfachen und automatisieren, indem Sie Konto- und Regionsunabhängig verwendenAWS CloudFormation StackSets und Vorlagen zum Bereitstellen von Anwendungsressourcen mit den erforderlichen Alarmen. TemplateSie können die Alarmaktionen so konfigurieren, dass sie auf ein allgemeines Amazon Simple Notification Service (Amazon SNS) Thema abzielen, was bedeutet, dass unabhängig vom Konto oder der Region dieselbe Benachrichtigungs- oder Behebungsaktion verwendet wird.

In Umgebungen mit mehreren Konten und mehreren Regionen empfehlen wir Ihnen, aggregierte Alarme für Ihre Konten und Regionen zu erstellen, um Konto- und Regionalprobleme mithilfe derAWS CloudFormation StackSets und aggregierte Metriken wie Durchschnitt`CPUUtilization`In allen EC2-Instances.

Sie sollten auch erwägen, Standardalarme für jede Arbeitslast zu erstellen, die für den Standard konfiguriert ist CloudWatch Metriken und Protokolle, die Sie erfassen. Beispielsweise können Sie für jede EC2-Instanz einen separaten Alarm erstellen, der die CPU-Auslastungsmetrik überwacht und ein zentrales Betriebsteam benachrichtigt, wenn die durchschnittliche CPU-Auslastung täglich über 80% beträgt. Sie können auch einen Standardalarm erstellen, der die durchschnittliche CPU-Auslastung unter 10% täglich überwacht. Diese Alarme helfen dem zentralen Betriebsteam, mit bestimmten Workload-Besitzern zusammenzuarbeiten, um die Größe der EC2-Instanzen bei Bedarf zu ändern.

Automatisieren der Alarmerstellung mit EC2-Instance-Tags

Das Erstellen eines Standardsatzes von Alarmen für Ihre EC2-Instanzen kann zeitaufwändig, inkonsistent und fehleranfällig sein. Sie können den Alarmerstellungsprozess beschleunigen, indem Sie dieAmazon-Cloudwatch-Auto-AlarmeLösung, um automatisch einen Standardsatz von CloudWatch-Alarmen für Ihre EC2-Instanzen zu erstellen und benutzerdefinierte Alarme basierend auf EC2-Instance-Tags zu erstellen. Die Lösung macht die Notwendigkeit überflüssig, Standardalarme manuell zu erstellen, und kann bei einer groß angelegten Migration von EC2-Instanzen nützlich sein, die Tools wie CloudEndure verwendet. Sie können diese Lösung auch

mitAWS CloudFormation StackSets um mehrere Regionen und Konten zu unterstützen. Weitere Informationen finden Sie unterVerwenden Sie Tags, um Amazon zu erstellen und zu pflegen CloudWatch -Alarmen für Amazon EC2 EC2-Instancesauf derAWSBlog-

Überwachung der Anwendungs- und Dienstverfügbarkeit

CloudWatch hilft Ihnen, die Leistungs- und Laufzeitaspekte Ihrer Anwendungen und Workloads zu überwachen und zu analysieren. Sie sollten auch die Verfügbarkeits- und Erreichbarkeitsaspekte Ihrer Anwendungen und Workloads überwachen. Sie erreichen dies, indem Sie einen aktiven Überwachungsansatz mitAmazon Route 53-ZustandsprüfungenundCloudWatch Syntheticsaus.

Sie können Integritätsprüfungen von Route 53 verwenden, wenn Sie die Konnektivität zu einer Webseite über HTTP oder HTTPS oder die Netzwerkkonnektivität über TCP zu einem DNS- Namen oder einer IP-Adresse (Public Domain Name System) überwachen möchten. Die Zustandsprüfungen von Route 53 initiieren Verbindungen aus den Regionen, die Sie in Intervallen von zehn Sekunden oder 30 Sekunden angeben. Sie können mehrere Regionen auswählen, in denen der Integritätsprüfung ausgeführt werden soll, jeder Integritätsprüfung wird unabhängig ausgeführt und Sie müssen mindestens drei Regionen auswählen. Sie können den Antworttext einer HTTP- oder HTTPS-Anfrage nach einer bestimmten Teilzeichenfolge durchsuchen, wenn sie in den ersten 5.120 Bytes an Daten angezeigt wird, die für die Auswertung des Health Checks zurückgegeben werden. Eine HTTP- oder HTTPS-Anfrage wird als fehlerfrei betrachtet, wenn der Antwortcode 2xx oder 3xx zurückgegeben wird. Die Zustandsprüfungen von Route 53 können verwendet werden, um eine zusammengesetzte Integritätsprüfung zu erstellen, indem der Zustand anderer Integritätsprüfungen überprüft Sie können dies tun, wenn Sie mehrere Service-Endpoints haben und dieselbe Benachrichtigung ausführen möchten, wenn einer von ihnen ungesund wird. Wenn Sie Route 53 für DNS verwenden, können Sie Route 53 für konfigurierenFailover zu einem anderen DNS-Eintragwenn ein Gesundheitscheck ungesund wird. Für jede kritische Workload sollten Sie erwägen, die Integritätsprüfungen von Route 53 für externe Endpunkte einzurichten, die für den normalen Betrieb von entscheidender Bedeutung sind. Route 53-Integritätsprüfungen können Ihnen dabei helfen, Failover-Logik in Ihre Anwendungen zu schreiben.

CloudWatch Synthetics ermöglicht es Ihnen, einen Kanarienvogel als Skript zu definieren, um den Zustand und die Verfügbarkeit Ihrer Workloads zu bewerten. Canarys sind Skripts, die in Node.js oder Python geschrieben wurden und arbeiten über HTTP- oder HTTPS-Protokolle. Sie legen Lambda-Funktionen in Ihrem Konto an, die Node.js oder Python als Framework verwenden. Jeder Kanarienvogel, den Sie definieren, kann mehrere HTTP- oder HTTPS-Aufrufe an verschiedene Endpunkte ausführen. Dies bedeutet, dass Sie den Zustand einer Reihe von Schritten überwachen können, z. B. eines Anwendungsfalls oder eines Endpunkts mit nachgelagerten Abhängigkeiten. Canarys erstellen CloudWatch Metriken, die jeden ausgeführten Schritt enthalten, damit Sie verschiedene Schritte unabhängig alarmieren und messen können. Obwohl Kanarienvögel mehr

Planung und Entwicklungsaufwand erfordern als Health Checks der Route 53, bieten sie Ihnen einen hochgradig anpassbaren Überwachungs- und Bewertungsansatz. Kanaren unterstützen auch private Ressourcen, die in Ihrer Virtual Private Cloud (VPC) ausgeführt werden, was sie ideal für die Verfügbarkeitsüberwachung macht, wenn Sie keine öffentliche IP-Adresse für den Endpunkt haben. Sie können Kanarienvögel auch verwenden, um lokale Workloads zu überwachen, solange Sie über Konnektivität von der VPC zum Endpunkt verfügen. Dies ist besonders wichtig, wenn Sie eine Arbeitslast haben, die Endpunkte enthält, die lokal vorhanden sind.

Verfolgen von Anwendungen mitAWS X-Ray

Eine Anfrage über Ihre Anwendung kann aus Aufrufen von Datenbanken, Anwendungen und Webdiensten bestehen, die auf lokalen Servern, Amazon EC2, Containern oder Lambda ausgeführt werden. Durch die Implementierung der Anwendungsverfolgung können Sie schnell die Ursache von Problemen in Ihren Anwendungen ermitteln, die verteilte Komponenten und Dienste verwenden. Sie können es verwendenAWS X-Rayum Ihre Anwendungsanfragen über mehrere Komponenten hinweg zu verfolgen. Röntgenproben und visualisiert Anfragen an einemService-Grafikwenn sie durch Ihre Anwendungskomponenten fließen und jede Komponente als Segment dargestellt wird. X-Ray generiert Trace-Bezeichner, sodass Sie eine Anforderung korrelieren können, wenn sie durch mehrere Komponenten fließt, was Ihnen hilft, die Anforderung von Ende zu Ende anzuzeigen. Sie können dies weiter verbessern, indem Sie Anmerkungen und Metadaten einbeziehen, um die Eigenschaften einer Anfrage eindeutig zu suchen und zu identifizieren.

Wir empfehlen Ihnen, jeden Server oder Endpunkt in Ihrer Anwendung mit X-Ray zu konfigurieren und zu instrumentieren. X-Ray wird in Ihren Anwendungscode implementiert, indem Sie Anrufe an den X-Ray-Dienst tätigen. X-Ray bietet auchAWSSDKs für mehrere Sprachen, einschließlich instrumentierter Clients, die automatisch Daten an X-Ray senden. Die X-Ray SDKs stellen Patches für gängige Bibliotheken bereit, die für Anrufe an andere Dienste (z. B. HTTP, MySQL, PostgreSQL oder MongoDB) verwendet werden.

X-Ray bietet einen X-Ray-Daemon, den Sie auf Amazon EC2 und Amazon ECS installieren und ausführen können, um Daten an X-Ray weiterzuleiten. X-Ray erstellt Traces für Ihre Anwendung, die Leistungsdaten von den Servern und Containern erfassen, auf denen der X-Ray-Daemon ausgeführt wird, der die Anforderung bedient hat. X-Ray instrumentiert automatisch Ihre Anrufe anAWSDienste wie Amazon DynamoDB als Teilsegmente durch Patchen derAWS-SDK. X-Ray kann sich auch automatisch in Lambda-Funktionen integrieren.

Wenn Ihre Anwendungskomponenten externe Dienste anrufen, die den X-Ray-Daemon nicht konfigurieren und installieren oder den Code instrumentieren können, können Sie erstellenTeilsegmente zum Umschließen von Anrufen an externe Dienstenaus. X-Ray korreliert CloudWatch Protokolle und Metriken mit Ihren Anwendungsverfolgungen, wenn Sie dieAWS X-Ray SDK for Java, was bedeutet, dass Sie die zugehörigen Metriken und Protokolle für Anfragen schnell analysieren können.

Bereitstellen von X-Ray-Daemon zur Verfolgung von Anwendungen und Diensten auf Amazon EC2

Sie müssen den X-Ray-Daemon auf den EC2-Instances installieren und ausführen, auf denen Ihre Anwendungskomponenten oder Microservices ausgeführt werden. Sie können einBenutzerdatenskriptum den X-Ray-Daemon bereitzustellen, wenn EC2-Instanzen bereitgestellt werden, oder Sie können ihn in den AMI-Build-Prozess aufnehmen, wenn Sie Ihre eigenen AMIs erstellen. Dies kann besonders nützlich sein, wenn EC2-Instanzen flüchtig sind.

Sie sollten State Manager verwenden, um sicherzustellen, dass der X-Ray Daemon konsistent auf Ihren EC2-Instanzen installiert ist. Für Amazon EC2WindowsInstanzen können Sie den Systems Manager verwendenAWS-RunPowerShellScript-DokumentSo führen Sie das aus:Windows-Scriptdas lädt den X-Ray-Agent herunter und installiert ihn. Für EC2-Instanzen unter Linux können Sie dieAWS-RunShellScript-Dokument zum Ausführen des Linux-Skriptslädt den -Agenten als Service herunter und installiert ihnaus.

Sie können den Systems Manager verwendenAWS-RunRemoteScript-Dokumentum das Skript in einer Umgebung mit mehreren Konten auszuführen. Sie müssen einen S3-Bucket erstellen, der von allen Ihren Konten aus zugänglich ist, und wir empfehlenErstellen eines S3-Buckets mit einer organisationsbasierten Bucket-Richtliniewenn Sie verwendenAWS Organizationsaus. Anschließend laden Sie die Skripts in den S3-Bucket hoch, stellen jedoch sicher, dass die IAM-Rolle für Ihre EC2-Instanzen die Berechtigung hat, auf den Bucket und die Skripte zuzugreifen.

Sie können State Manager auch so konfigurieren, dass die Skripte EC2-Instanzen zugeordnet werden, auf denen der X-Ray-Agent installiert ist. Da alle Ihre EC2-Instanzen möglicherweise kein X-Ray benötigen oder verwenden, können Sie die Verknüpfung mit Instanz-Tags abzielen. Beispielsweise können Sie die Zuordnung des State Managers auf der Grundlage des Vorhandenseins von`InstallAWSXRayDaemonWindows`oder`InstallAWSXRayDaemonLinux`Stichworte.

Bereitstellen von X-Ray-Daemon zur Verfolgung von Anwendungen und Diensten auf Amazon ECS oder Amazon EKS

Sie können dieX-Ray-Daemonals Beiwagen-Container für containerbasierte Workloads wie Amazon ECS oder Amazon EKS. Ihre Anwendungscontainer können sich dann mit Ihrem Beiwagen-Container mit Containerverknüpfung verbinden, wenn Sie Amazon ECS verwenden, oder der Container kann

sich direkt mit dem Beiwagen-Container auf localhost verbinden, wenn Sie verwendenAWSVPC-Netzwerkmodusaus.

Für Amazon EKS können Sie den X-Ray-Daemon in der Pod-Definition Ihrer Anwendung definieren, und Ihre Anwendung kann sich dann über localhost auf dem von Ihnen angegebenen Container-Port mit dem Daemon verbinden.

Konfigurieren von Lambda, um Anfragen an X-Ray zu verfolgen

Ihre Anwendung enthält möglicherweise Aufrufe von Lambda-Funktionen. Sie müssen den X-Ray-Daemon für Lambda nicht installieren, da der Daemon-Prozess vollständig von Lambda verwaltet wird und nicht vom Benutzer konfiguriert werden kann. Sie können es für Ihre Lambda-Funktion aktivieren, indem Sie dieAWS Management Consoleund überprüfe dieAktive AblaufverfolgungOption in der X-Ray-Konsole.

Zur weiteren Instrumentierung können Sie das X-Ray-SDK mit Ihrer Lambda-Funktion zur Aufzeichnung ausgehender Anrufe und zum Hinzufügen von Anmerkungen oder Metadaten bündeln.

Instrumentieren Sie Ihre Anwendungen für X-Ray

Sie sollten das X-Ray SDK auswerten, das mit der Programmiersprache Ihrer Anwendung übereinstimmt, und alle Aufrufe, die Ihre Anwendung an andere Systeme tätigt, klassifizieren. Überprüfen Sie die von der ausgewählten Bibliothek bereitgestellten Clients und prüfen Sie, ob das SDK die Verfolgung für die Anfrage oder Antwort Ihrer Anwendung automatisch bestimmen kann. Prüfen Sie, ob die vom SDK bereitgestellten Clients für andere nachgelagerte Systeme verwendet werden können. Für externe Systeme, die Ihre Anwendung aufruft und die Sie nicht mit X-Ray instrumentieren können, sollten Sie benutzerdefinierte Teilsegmente erstellen, um sie in Ihren Trace-Informationen zu erfassen und zu identifizieren.

Stellen Sie beim Instrumentieren Ihrer Anwendung sicher, dass Sie Anmerkungen erstellen, die Ihnen bei der Identifizierung und Suche nach Anfragen helfen. Beispielsweise kann Ihre Anwendung eine Kennung für Kunden verwenden, z. B.`customer id`oder segmentieren Sie verschiedene Benutzer basierend auf ihrer Rolle in der Anwendung.

Sie können maximal 50 Anmerkungen für jede Verfolgung erstellen, aber Sie können ein Metadatenobjekt erstellen, das ein oder mehrere Felder enthält, solange das Segmentdokument 64 Kilobyte nicht überschreitet. Sie sollten selektiv Anmerkungen verwenden, um Informationen

zu finden und das Metadatenobjekt zu verwenden, um mehr Kontext bereitzustellen, der bei der Fehlerbehebung der Anforderung hilft, nachdem sie gefunden wurde.

Konfiguration der X-Ray-Samplingregeln

VonAnpassen von Samplingregelnkönnen Sie die Menge der von Ihnen aufgezeichneten Daten steuern und das Samplingverhalten ändern, ohne Ihren Code ändern oder neu implementieren zu müssen. Samplingregeln teilen dem X-Ray-SDK mit, wie viele Anfragen für eine Reihe von Kriterien aufgezeichnet werden. Standardmäßig zeichnet das X-Ray-SDK aufdie erste Anfrage jede Sekunde und fünf Prozent aller zusätzlichen Anfragenaus. Eine Anfrage pro Sekunde ist das Reservoir. Dadurch wird sichergestellt, dass jede Sekunde mindestens eine Ablaufverfolgung aufgezeichnet wird, solange der Dienst Anfragen verarbeitet. Fünf Prozent ist die Rate, mit der die über die Reservoirgröße hinausgehenden Anforderungen geprüft werden.

Sie sollten die Standardkonfiguration überprüfen und aktualisieren, um einen geeigneten Wert für Ihr Konto zu ermitteln. Ihre Anforderungen können in Entwicklungs-, Test-, Leistungstest und Produktionsumgebungen variieren. Möglicherweise haben Sie Anwendungen, die ihre eigenen Stichprobenregeln erfordern, basierend auf dem Umfang des Datenverkehrs, den sie erhalten, oder deren Kritikalität. Sie sollten mit einer Baseline beginnen und regelmäßig neu bewerten, ob der Baseline Ihren Anforderungen entspricht.

Dashboards und Visualisierungen mit CloudWatch

Dashboards helfen Ihnen, sich schnell auf Bereiche zu konzentrieren, die für Anwendungen und Workloads wichtig sind. CloudWatch bietet automatische Dashboards und Sie können auch einfach Dashboards erstellen, die CloudWatch -Metriken. CloudWatch Dashboards bieten mehr Einblick als das Anzeigen von Metriken isoliert, da sie Ihnen helfen, mehrere Metriken zu korrelieren und Trends zu identifizieren. Ein Dashboard, das empfangene Bestellungen, Arbeitsspeicher, CPU-Auslastung und Datenbankverbindungen enthält, kann Ihnen helfen, Änderungen an Workload-Metriken über mehrereAWSRessourcen, während Ihre Bestellanzahl zunimmt oder abnimmt.

Sie sollten Dashboards auf Konto- und Anwendungsebene erstellen, um Workloads und Anwendungen zu überwachen. Sie können anfangen, indem Sie verwenden CloudWatch automatische Dashboards, die sindAWSService-Level-Dashboards sind mit servicespezifischen Metriken vorkonfiguriert. Automatische Service-Dashboards zeigen alle Standardeinstellungen an CloudWatch -Metriken für den Service. Die automatischen Dashboards zeigen alle Ressourcen, die für jede Service-Metrik verwendet werden, und helfen Ihnen, Ausreißerressourcen in Ihrem Konto schnell zu identifizieren. Dies kann Ihnen helfen, Ressourcen mit hoher und geringer Auslastung zu identifizieren, die Ihnen helfen können, Ihre Kosten zu optimieren.

Erstellen von dienstübergreifenden Dashboards

Sie können serviceübergreifende Dashboards erstellen, indem Sie das automatische Service-Level-Dashboard für einAWSService und Verwendung desZu Dashboard hinzufügenOption von derAktionenMenü „. Sie können dann Metriken aus anderen automatischen Dashboards zu Ihrem neuen Dashboard hinzufügen und Metriken entfernen, um den Fokus des Dashboards einzuschränken. Sie sollten auch Ihre eigenen benutzerdefinierten Metriken hinzufügen, um wichtige Beobachtungen (z. B. eingegangene Bestellungen oder Transaktionen pro Sekunde) zu verfolgen. Wenn Sie Ihr eigenes benutzerdefiniertes Cross-Service-Dashboard erstellen, können Sie sich auf die relevantesten Metriken für Ihre Workload konzentrieren. Wir empfehlen Ihnen, dienstübergreifende Dashboards auf Kontoebene zu erstellen, die wichtige Metriken abdecken und alle Workloads in einem Konto anzeigen.

Wenn Sie eine zentrale Büroräume oder einen gemeinsamen Bereich für Ihre Cloud-Betriebsteams haben, können Sie die CloudWatch Dashboard auf einem großen TV-Monitor im Vollbildmodus mit automatischer Aktualisierung.

Erstellen von anwendungs- oder workload-spezifischen Dashboards

Wir empfehlen Ihnen, anwendungs- und workload-spezifische Dashboards zu erstellen, die sich auf wichtige Metriken und Ressourcen für jede kritische Anwendung oder Workload in Ihrer Produktionsumgebung konzentrieren. Anwendungs- und Workload-spezifische Dashboards konzentrieren sich auf Ihre benutzerdefinierten Anwendungs- oder Workload-Metriken und wichtigAWSRessourcenmetriken, die ihre Leistung beeinflussen.

Sie sollten Ihr regelmäßig bewerten und anpassen CloudWatch Anwendungs- oder Workload-Dashboards zur Verfolgung wichtiger Metriken nach Vorfällen. Sie sollten auch anwendungs- oder workload-spezifische Dashboards aktualisieren, wenn Funktionen eingeführt oder zurückgezogen werden. Aktualisierungen von Workload und anwendungsspezifischen Dashboards sollten neben der Protokollierung und Überwachung eine erforderliche Aktivität zur kontinuierlichen Verbesserung der Qualität sein.

Erstellen von konten- oder regionenübergreifenden Dashboards

AWSRessourcen sind in erster Linie regional und die Metriken, Alarme und Dashboards sind spezifisch für die Region, in der die Ressourcen bereitgestellt werden. Dies kann erfordern, dass Sie Regionen ändern, um Metriken, Dashboards und Alarme für regionsübergreifende Workloads und Anwendungen anzuzeigen. Wenn Sie Ihre Anwendungen und Workloads in mehrere Konten aufteilen, müssen Sie sich möglicherweise auch erneut authentifizieren und sich bei jedem Konto anmelden. Allerdings CloudWatch unterstützt die kontoübergreifende und regionsübergreifende Datenanzeige von einem einzigen Konto aus, was bedeutet, dass Sie Metriken, Alarme, Dashboards und Log-Widgets in einem einzigen Konto und einer einzigen Region anzeigen können. Dies ist sehr nützlich, wenn Sie ein zentrales Protokollierungs- und Überwachungskonto haben.

Kontoinhaber und Eigentümer des Anwendungsteams sollten Dashboards für kontospezifische, regionsübergreifende Anwendungen erstellen, um wichtige Kennzahlen an einem zentralen Ort effektiv zu überwachen. CloudWatch-Dashboards unterstützen automatisch regionsübergreifende Widgets, was bedeutet, dass Sie ohne weitere Konfiguration ein Dashboard erstellen können, das Metriken aus mehreren Regionen enthält.

Eine wichtige Ausnahme ist die CloudWatch Logs Insights Widget, da Protokolldaten nur für das Konto und die Region angezeigt werden können, in der Sie derzeit angemeldet sind. Sie können

regionsspezifische Metriken aus Ihren Protokollen mithilfe von Metrikfiltern erstellen, und diese Metriken können in einem regionsübergreifenden Dashboard angezeigt werden. Sie können dann zur spezifischen Region wechseln, wenn Sie diese Protokolle weiter analysieren müssen.

Betriebsteams sollten ein zentrales Dashboard erstellen, das wichtige kontoübergreifende und regionsübergreifende Metriken überwacht. Sie können beispielsweise ein kontoübergreifendes Dashboard erstellen, das die aggregierte CPU-Auslastung in jedem Konto und jeder Region enthält. Sie können auchMetrische Mathematikum Daten für mehrere Konten und Regionen zu aggregieren und zu überarbeiten.

Verwendung von metrischer Mathematik zur Feinabstimmung von Beobachtbarkeit und Alarmierung

Sie können Metrikmathematik verwenden, um Metriken in Formaten und Ausdrücken zu berechnen, die für Ihre Workloads relevant sind. Die berechneten Metriken können zu Tracking-Zwecken gespeichert und in einem Dashboard angezeigt werden. Beispielsweise geben Standard-Amazon EBS-Volume-Metriken die Anzahl der gelesenen (`VolumeReadOps`) und schreibe (`VolumeWriteOps`) Operationen, die über einen bestimmten Zeitraum ausgeführt werden.

AllerdingsAWSenthält Richtlinien zur Volumenleistung von Amazon EBS in IOPS. Sie können die IOPS für Ihr Amazon EBS-Volumen in Metrikmathematik darstellen und berechnen, indem Sie die`VolumeReadOps`und`VolumeWriteOps`und dividiert dann durch den für diese Metriken gewählten Zeitraum.

In diesem Beispiel fassen wir die IOPS in der Periode zusammen und dividieren dann durch die Periodenlänge, um die IOPS zu erhalten. Sie können dann einen Alarm gegen diesen metrischen mathematischen Ausdruck einstellen, um Sie zu warnen, wenn sich die IOPS Ihres Volumes der maximalen Kapazität für seinen Volume-Typ nähert. Weitere Informationen und Beispiele zur Verwendung von Metrikberechnungen zum Überwachen von Amazon Elastic File System (Amazon EFS) -Dateisystemen CloudWatch Metriken sieheAmazon CloudWatch metrische Mathematik vereinfacht die Überwachung Ihrer Amazon EFS-Dateisysteme in nahezu Echtzeit und mehrauf derAWSBlog-Test.

Verwenden von automatischen Dashboards für Amazon ECS, Amazon EKS und Lambda mit CloudWatchContainer Ergebnisse und CloudWatch Ergebnisse von Lambda-Daten

CloudWatch Container Insights erstellt dynamische, automatische Dashboards für Container-Workloads, die auf Amazon ECS und Amazon EKS ausgeführt werden. Sie sollten Container Insights aktivieren, um CPU-, Speicher-, Datenträger-, Netzwerk- und Diagnoseinformationen wie Fehler beim Neustart von Containern zu beobachten. Container Insights generiert dynamische Dashboards, die Sie schnell auf Cluster, Container-Instance oder Knoten, Service, Task, Pod und einzelnen Containerebenen filtern können. Container Insightsist auf Cluster- und Knoten- oder Container-Instance-Ebene konfiguriertAbhängig vomAWS-Dienstleistung.

Ähnlich wie Container Insights, CloudWatch Lambda Insights erstellt dynamische, automatische Dashboards für Ihre Lambda-Funktionen. Diese Lösung erfasst, aggregiert und fasst Metriken auf Systemebene zusammen, einschließlich CPU-Zeit, Arbeitsspeicher, Datenträger und Netzwerk. Sie erfasst, aggregiert und fasst Diagnoseinformationen wie Kaltstart und Lambda-Worker-Abschaltungen zusammen, um Probleme mit Ihren Lambda-Funktionen zu isolieren und schnell zu beheben. Lambda ist auf Funktionsebene aktiviert und benötigt keine Agenten.

Container Insights und Lambda Insights helfen Ihnen außerdem, schnell zu den Anwendungs- oder Leistungsprotokollen, Röntgen-Traces und einer Service-Map zu wechseln, um Ihre Container-Workloads zu visualisieren. Sie benutzen beide das CloudWatch Erfassende eingebettete Metrikformat CloudWatch -Metriken und -Leistungsprotokolle.

Sie können eine gemeinsame Nutzung erstellen CloudWatch Dashboard für Ihre Workload, das die von Container Insights und Lambda Insights erfassten Metriken verwendet. Sie können dazu das automatische Dashboard filtern und anzeigen CloudWatch Container Insights und dann die Auswahl desZum Dashboard hinzufügen, mit der Sie die angezeigten Metriken zu einem Standard-CloudWatch-Dashboard hinzufügen können. Sie können dann die Metriken entfernen oder anpassen und andere Metriken hinzufügen, um Ihre Arbeitslast korrekt darzustellen.

Integration von CloudWatch inAWSDienstleistungen

AWSbietet viele Dienste, die zusätzliche Konfigurationsoptionen für die Protokollierung und Metriken enthalten. Diese Dienste ermöglichen es Ihnen oft, zu konfigurieren CloudWatch Logs für die Protokollausgabe und CloudWatch Metriken für die Ausgabe von Metriken. Die zugrunde liegende Infrastruktur, die zur Bereitstellung dieser Dienste verwendet wird, wird vonAWSundist nicht zugänglich, aber Sie können die Protokollierungs- und Metrikoptionen für Ihre bereitgestellten Dienste verwenden, um weitere Einblicke zu gewinnen und Probleme zu beheben. Sie können beispielsweise veröffentlichenVPC Flow Logs in CloudWatchoder du kannst auchKonfigurieren von Amazon Relational Database Service (Amazon RDS) -Instances für die Veröffentlichung von Protokollen in CloudWatchaus.

Die meistenAWS-Dienste protokollieren ihre API-Aufrufe mit-Integration inAWS CloudTrailaus. CloudTrail ebenfallsunterstützt die Integration mit CloudWatch Protokolleund das bedeutet, dass Sie Aktivitäten in suchen und analysieren könnenAWS-Services. Sie können Amazon auch verwenden CloudWatch Events oder Amazon EventBridge um Automatisierung und Benachrichtigungen zu erstellen und zu konfigurieren CloudWatch Ereignisregeln für Ereignisse für bestimmte Aktionen, die inAWS-Services. Bestimmte DiensteDirekt integrierenmit CloudWatch Events und EventBridge. Sie können auchEreignisse erstellen, die über CloudTrail geliefert werdenaus.

Amazon Managed Grafana für Dashboarding und Visualisierung

Amazon Managed Grafanakann verwendet werden, um IhreAWSArbeitslasten. Amazon Managed Grafana hilft Ihnen dabei, Ihre Betriebsdaten im großen Maßstab zu visualisieren und zu analysieren. Grafanaist eine Open-Source-Analyseplattform, die Ihnen hilft, Ihre Metriken abzufragen, zu visualisieren, zu alarmieren und zu verstehen, wo immer sie gespeichert sind. Amazon Managed Grafana ist besonders nützlich, wenn Ihr Unternehmen Grafana bereits zur Visualisierung vorhandener Workloads verwendet und Sie die Abdeckung aufAWSArbeitslasten. Sie können Amazon Managed Grafana mit CloudWatch vonHinzufügen von als Datenquelle, was bedeutet, dass Sie Visualisierungen mit CloudWatch-Metriken. Amazon Managed Grafana unterstütztAWS Organizationsund Sie können Dashboards zentralisieren mit CloudWatch -Metriken aus mehreren Konten und Regionen.

Die folgende Tabelle enthält die Vorteile und Überlegungen für die Verwendung von Amazon Managed Grafana anstelle von CloudWatch zum Dashboarding. Ein hybrider Ansatz könnte auf der Grundlage der unterschiedlichen Anforderungen Ihrer Endbenutzer, Workloads und Anwendungen geeignet sein.

Erstellen Sie Visualisierungen und Dashboard s, die sich in Datenquellen integrieren lassen, die von Amazon Managed Grafana und Open Source Grafana unterstützt werden	Amazon Managed Grafana hilft Ihnen dabei, Visualisierungen und Dashboards aus vielen verschiedenen Datenquellen zu erstellen , darunter CloudWatch -Metriken. Amazon Managed Grafana enthält eine Reihe von integrierten Datenquellen, die sichAWSDi enstleistungen, Open-Source-Software und COTS-Software. Weitere Informationen hierzu finden Sie unterIntegrierte Datenquellenin der Amazon Managed Grafana-Dokumentat ion. Sie können auch Unterstützung für mehr Datenquellen hinzufügen, indem Sie Ihren Workspace aufGrafana Enterprise. Grafana unterstützt auchDatenquellen-Pluginsdie es Ihnen ermöglichen, mit verschiedenen externen

	Systemen zu kommunizieren. CloudWatch-Dashboards benötigen ein CloudWatch -Metrik oder CloudWatch Logs Insights Abfrage für anzuzeigende Daten werden auf einem CloudWatch -Dashboard.
Verwalten Sie den Zugriff auf Ihre Dashboard-Lösung getrennt von IhremAWS-Kontozugriff	Amazon Managed Grafana erfordert den Einsatz vonAWS IAM Identity Center(IAM Identity Center) undAWS Organizationszur Authentifizierung und Autorisierung. Auf diese Weise können Sie Benutzer bei Grafana authentifizieren, indem Sie einen Identitätsverbund verwenden, den Sie möglicherweise bereits mit IAM Identity Center oderAWS Organizations. Wenn Sie jedoch kein IAM Identity Center verwenden oderAWS Organizations, dann wird es als Teil des Amazon Managed Grafana-Einrichtungsprozesses eingerichtet. Dies kann zu einem Problem werden, wenn Ihre Organisation die Nutzung von IAM Identity Center eingeschränkt hat oderAWS Organizations.

Erfassen und Zugreifen auf Daten über mehrere Konten und Regionen hinweg mitAWS OrganizationsIntegration	Amazon Managed Grafana lässt sich in integrierenAWS Organizationsum Ihnen das Lesen von Daten zu ermöglichenAWSQuellen wie CloudWatch und Amazon OpenSearch Service für alle Ihre Konten. Auf diese Weise können Sie Dashboards erstellen, die Visualisierungen mithilfe von Daten in Ihren Konten anzeigen. So aktivieren Sie automatisch den Datenzugriff überAWS Organizationsmüssen Sie Ihren Amazon Managed Grafana Workspace imAWS OrganizationsVerwaltungskonto. Dies wird aufgrund von nicht empfohlenAWS OrganizationsBewährte Methoden für das Verwaltungskonto. Im Gegensatz dazu CloudWatch ebenfalls unterstützt konten- und regionenübergreifende Dashboards für CloudWatch Metriken.
Verwenden Sie erweiterte Visualisierungs-Widgets und Grafana-Definitionen, die in der Open Source Community verfügbar sind	Grafana bietet eine große Sammlung von Visualisierungen, die Sie beim Erstellen Ihrer Dashboards verwenden können. Es gibt auch eine große Bibliothek mit von der Community bereitgestellten Dashboards, die Sie gemäß Ihren Anforderungen bearbeiten und wiederverwenden können.
Verwenden Sie Dashboards mit neuen und vorhandenen Grafana-Bereitstellungen	Wenn Sie Grafana bereits verwenden, können Sie Dashboards aus Ihren Grafana-Bereitstellungen importieren und exportieren und für die Verwendung in Amazon Managed Grafana anpassen. Amazon Managed Grafana ermöglicht es Ihnen, Grafana als Ihre Dashboard-Lösung zu standardisieren.

Erweiterte Einrichtung und Konfiguration für Arbeitsbereiche, Berechtigungen und Datenquellen	Mit Amazon Managed Grafana können Sie mehrere Grafana-Arbeitsbereiche erstellen, die über eigene konfigurierte Datenquellen, Benutzer und Richtlinien verfügen. Auf diese Weise können Sie erweiterte Anwendung sfallanforderungen sowie erweiterte Sicherhei tskonfigurationen erfüllen. Die erweiterten Funktionen erfordern möglicherweise, dass Ihre Teams ihre Erfahrung mit Grafana erweitern, wenn sie nicht bereits über diese Fähigkeiten verfügen.

Entwerfen und Implementieren von Protokollierung und Überwachung mit CloudWatch FAQ

Dieser Abschnitt enthält Antworten auf häufig aufgeworfene Fragen zum Entwerfen und Implementieren von Protokollierungs- und Überwachungslösungen mit CloudWatch.

Wo lagere ich CloudWatch Konfigurationsdateien?

Die CloudWatch Agent für Amazon EC2 kann mehrere Konfigurationsdateien anwenden, die im CloudWatch Konfigurationsverzeichnis. Idealerweise sollten Sie Ihre CloudWatch-Konfiguration als eine Reihe von Dateien speichern, da Sie die Versionskontrolle und erneut in mehreren Konten und Umgebungen verwenden können. Weitere Informationen hierzu finden Sie im Abschnitt Verwalten von CloudWatch Konfigurationen Abschnitt dieses Handbuchs. Alternativ können Sie Ihre Konfigurationsdateien auch in einem Repository auf GitHub und automatisieren Sie den Abruf der Konfigurationsdateien, wenn eine neue EC2-Instanz bereitgestellt wird.

Wie kann ich ein Ticket in meiner Service-Management-Lösung erstellen, wenn ein Alarm ausgelöst wird?

Sie integrieren Ihr Service-Management-System in ein Amazon Simple Notification Service (Amazon SNS) -Thema und konfigurieren die CloudWatch Alarm, um das SNS-Thema zu benachrichtigen, wenn ein Alarm ausgelöst wird. Ihr integriertes System erhält die SNS-Nachricht und kann mithilfe Ihrer Servicemanagementsystem-APIs oder SDKs ein Ticket erstellen.

Wie verwende ich CloudWatch um Protokolldateien in meinen Containern zu erfassen?

Amazon ECS-Aufgaben und Amazon EKS Pods können so konfiguriert werden, dass sie die STDOUT- und STDERR-Ausgabe automatisch an CloudWatch senden. Der empfohlene Ansatz für die Protokollierung von containerisierten Anwendungen besteht darin, dass Container ihre Ausgabe an STDOUT und STDERR senden. Dies wird auch in der Zwölf-Faktor-App-Manifest aus.

Wenn Sie jedoch bestimmte Protokolldateien an senden möchten CloudWatch dann können Sie ein Volume in Ihrem Amazon EKS-Pod oder Ihrer Amazon ECS-Aufgabendefinition bereitstellen, in die

Ihre Anwendung ihre Lot-Dateien schreibt und einen Beiwagen-Container für Fluentd oder Fluent Bit verwendet, um die Protokolle an CloudWatch zu senden. Sie sollten erwägen, eine bestimmte Protokolldatei in Ihrem Container symbolisch zu verknüpfen`/dev/stdout`und`/dev/stderr`aus. Weitere Informationen hierzu finden Sie unterAnzeigen von Protokollen für einen Container oder Servicein der Docker-Dokumentation.

Wie überwache ich Gesundheitsprobleme aufAWS-Services?

Sie können dasAWS Health DashboardÜberwachenAWSHealth-Ereignisse. Weitergehende Informationen finden Sie auch inaws-gesundheit-Tools GitHub Repository für Musterautomatisierungslösungen im Zusammenhang mitAWSHealth-Ereignisse.

Wie kann ich einen benutzerdefinierten erstellen CloudWatch Metrik wenn kein Agenten-Support existiert?

Sie können das eingebettete Metrikformat verwenden, um Metriken in CloudWatch aufzunehmen. Sie können auchAWSSDK (zum Beispielput_metric_data),AWS CLI(zum Beispielput-metric-data), oderAWSAPI (zum BeispielPutMetricData) um benutzerdefinierte -Metriken zu erstellen. Sie sollten überlegen, wie eine benutzerdefinierte Logik langfristig beibehalten wird. Ein Ansatz wäre, Lambda mit integrierter Unterstützung für eingebettete Metrikformate zu verwenden, um Ihre Metriken zusammen mit einem CloudWatch Ereignis für EreignisseRegel planenum den Zeitraum für die Metrik festzulegen.

Wie integriere ich meine bestehenden Protokollierungs- und Überwachungstools inAWS?

Sie sollten sich auf die Anweisungen des Software- oder Dienstanbieters für die Integration mitAWSaus. Möglicherweise können Sie Agentsoftware, SDK oder eine bereitgestellte API verwenden, um Protokolle und Metriken an ihre Lösung zu senden. Möglicherweise können Sie auch eine Open-Source-Lösung wie Fluentd oder Fluent Bit verwenden, die nach den Spezifikationen des Anbieters konfiguriert ist. Sie können auch dieAWSSDK und CloudWatch Protokolliert Abonnementfilter mit Lambda und Kinesis Data Streams, um benutzerdefinierte Protokollverarbeiter und Versender zu erstellen. Schließlich sollten Sie auch überlegen, wie Sie die Software integrieren, wenn Sie mehrere Konten und Regionen verwenden.

Ressourcen

Einführung

- AWSWell-Architected

Zielgerichtete Geschäftsergebnisse

- logging-monitoring-apg-guide-Beispiele
- Sechs Vorteile von Cloud Computing

Planung Ihres CloudWatch Einsatzes

- Terminologie und Konzepte von AWS Organizations
- AWS Systems ManagerSchnelle Einrichtung
- Erfassen von Metriken und Protokollen von Amazon-EC2-Instances und On-Premises-Servern mit dem CloudWatch Agenten
- cloudwatch-config-s3-bucket.yaml
- Erstellen der CloudWatch Agent-Konfigurationsdatei mit dem Assistenten
- Enterprise DevOps: Warum Sie das, was Sie bauen, ausführen sollten
- Exportieren von Protokolldaten nach Amazon S3
- Differenzierte Zugriffskontrolle in Amazon OpenSearch Service
- Lambda-Quoten
- Manuelles Erstellen oder Bearbeiten der CloudWatch Agent-Konfigurationsdatei
- Echtzeitverarbeitung von Protokolldaten mit Abonnements
- Tools, auf denen man aufbauen kannAWS

Konfigurieren des CloudWatch Agenten für EC2-Instances und On-Premises-Server

- Amazon EC2 EC2-Metrikdimensionen

- Instances mit Spitzenlastleistung
- CloudWatch Vordefinierte Metriksätze des Agenten
- Erfassen von Prozessmetriken mit dem procstat-Plugin
- Den CloudWatch Agenten für procstat konfigurieren
- Aktivieren oder deaktivieren Sie die detaillierte Überwachung für Ihre Instances
- Erfassen von Protokollen mit hoher Kardinalität und Generieren von Metriken mit dem CloudWatch eingebetteten Metrikformat
- Arbeiten mit Protokollgruppen und Protokollstreams
- Auflisten der für Ihre Instances verfügbaren CloudWatch -Metriken
- PutLogEvents
- Abrufen benutzerdefinierter Metriken mit collectd
- Abrufen benutzerdefinierter Metriken mit StatsD

CloudWatch Ansätze zur Agenteninstallation für Amazon EC2 und lokale Server

- Erstellen einer IAM-Service-Rolle für eine Hybrid-Umgebung
- Erstellen einer Aktivierung für verwaltete Instances in einer Hybrid-Umgebung
- Erstellen von IAM-Rollen und -Benutzern für die Verwendung mit dem CloudWatch Agenten
- Herunterladen und Konfigurieren des CloudWatch Agenten in der Befehlszeile
- Wie kann ich lokale Server, die den Systems Manager Agent und den Unified CloudWatch Agent verwenden, so konfigurieren, dass sie nur temporäre Anmeldeinformationen verwenden?
- Voraussetzungen für Stack-Set-Operationen
- Spot-Instances verwenden

Protokollierung und Überwachung auf Amazon ECS

- amazon-cloudwatch-logs-for-flüssiges Bit
- Amazon CloudWatch ECS-Metriken
- Amazon ECS-Container-Insights-Metriken
- Amazon-ECS-Container-Agent

- Amazon-ECS-Starttypen
- Bereitstellen des CloudWatch Agenten zum Erfassen von Metriken auf EC2-Instance-Ebene auf Amazon ECS
- ecs_cluster_with_cloudwatch_linux.yaml
- ecs_cw_emf_example
- ecs_firelense_emf_example
- ecs-task-nginx-firelense.json
- Abrufen von für Amazon ECS optimierten AMI-Metadaten
- Verwenden des awslogs-Protokolltreibers
- Verwenden der Client-Bibliotheken zum Generieren von Protokollen im eingebetteten Metrikformat

Protokollierung und Überwachung auf Amazon EKS

- Amazon-EKS-Steuerebenen-Protokollierung
- amazon_eks_managed_node_group_launch_config.yaml
- Amazon-EKS-Knoten
- amazon-eks-nodegroup.yaml
- Amazon EKS Service Level Agreement
- Überwachung von Container Insights Prometheus-Metriken
- Steuerebene-Metriken mit Prometheus
- Bereitstellen des Kubernetes-Dashboards (Webbenutzeroberfläche)
- Fargate-Protokollierung
- Fluent Bit für Amazon EKS auf Fargate
- So erfassen Sie Anwendungsprotokolle bei der Verwendung von Amazon EKS auf Fargate
- Installieren des CloudWatch Agenten zum Erfassen von Prometheus-Metriken
- Installieren des Kubernetes-Metrik-Servers
- kubernetes/dashboard
- Kubernetes Horizontal Pod Autoscaler
- Komponenten der Kubernetes-Steuerebene
- Kubernetes-Pods
- Support für Startvorlagen

- Verwaltete Knotengruppen
- Verhalten der Aktualisierung verwalteter Knoten
- Metrikserver
- Überwachung von Amazon EKS auf Fargate mit Prometheus und Grafana
- prometheus_jmx
- prometheus//jmx_exporter
- Scraping zusätzlicher Prometheus-Quellen und Importieren dieser Metriken
- Selbstverwaltete Knoten
- Protokolle an CloudWatch Logs senden
- Richten Sie FluentD ein, DaemonSet um Protokolle an Logs zu CloudWatch senden
- Java/JMX-Beispiel-Workload für Amazon EKS und Kubernetes einrichten
- Tutorial zum Hinzufügen eines neuen Prometheus-Scrape-Ziels: Prometheus-API-Server-Metriken
- Vertical Pod Autoscaler

Protokollierung und Metriken fürAWS Lambda

- Lambda-Aufruffehler
- Protokollierung — Protokollierungsfunktion für Python
- Verwenden der Client-Bibliotheken zum Generieren von Protokollen im eingebetteten Metrikformat
- Arbeiten mit Lambda-Funktionsmetriken

Logs suchen und analysieren CloudWatch

- Die Beats-Familie
- Elastischer Logstash
- Elastischer Stapel
- Streaming CloudWatch protokolliert Daten an Amazon OpenSearch Service

Alarmierende Optionen mit CloudWatch

- amazon-cloudwatch-auto-alarms

- AWSService Management Connector für Jira Service Management
- AWSService Management Connector für ServiceNow

Überwachung der Anwendungs- und Serviceverfügbarkeit

- DNS-Failover konfigurieren

Nachverfolgen von Anwendungen mitAWS X-Ray

- Amazon-ECS-Aufgabenvernetzung
- Konfigurieren von Sampling-Regeln in der X-Ray-Konsole
- PowerShell Windows-Befehle oder -Skripts ausführen
- Ausführen des X-Ray-Daemons auf Amazon EC2
- Senden von Trace-Daten an X-Ray
- Servicediagramm in X-Ray

Dashboards und Visualisierungen mit CloudWatch

- Amazon CloudWatch Metric Math vereinfacht die Überwachung Ihrer Amazon EFS-Dateisysteme nahezu in Echtzeit
- CloudWatch Container Insights einrichten
- Verwenden von Metrikberechnungen

CloudWatch Integration mitAWS Diensten

- In AWS CloudTrail unterstützte Services und Integrationen
- CloudWatch Beispiele für Veranstaltungen und Veranstaltungen von unterstützten Diensten
- Veranstaltungen, die über geliefert werden CloudTrail
- Überwachung von CloudTrail Protokolldateien mit CloudWatch Protokollen
- Veröffentlichen von Datenbank-Engine-Protokollen in CloudWatch Logs
- Veröffentlichen von Flow-Protokollen in CloudWatch Logs

Amazon Managed Grafana für Dashboarding und Visualisierung

- Bewährte Methoden für das Verwaltungskonto inAWS Organizations
- Integrierte Datenquellen für Amazon Managed Grafana
- Konto- und regionsübergreifende Dashboards in CloudWatch
- Grafana-Plug-ins

Dokumentverlauf

In der folgenden Tabelle werden die wichtigsten Änderungen an diesem Handbuch beschrieben. Wenn Sie über future Updates informiert werden möchten, können Sie einen RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
Aktualisierte Logging-Informationen	Der Abschnitt über die Protokollierung von wurde aktualisiertAWS Lambda.	17. April 2023
Aktualisierte Konfigurationsinformationen	Der Abschnitt über das Erstellen und Speichern von CloudWatch Konfigurationen wurde aktualisiert und umbenannt.	9. Februar 2023
Aktualisierte Metrikinformationen	Die Informationen zu benutzerdefinierten Anwendungsmetriken im Abschnitt Metrics for Amazon ECS wurden aktualisiert.	31. Januar 2023
Vorschauhinweise wurden entfernt	Amazon Manriken werden allgemein verfügbar.	25. Mai 2022
Abschnitt wurde entfernt	CloudWatch SDK-K-K-K-K-K-K-K-K-K-K-K-K-K-K-K-K-K-	7. Januar 2022
Erste Veröffentlichung	—	30. April 2021

AWS Glossar zu präskriptiven Leitlinien

Im Folgenden finden Sie häufig verwendete Begriffe in Strategien, Leitfäden und Mustern, die von Prescriptive Guidance bereitgestellt AWS werden. Um Einträge vorzuschlagen, verwenden Sie bitte den Link Feedback geben am Ende des Glossars.

Zahlen

7 Rs

Sieben gängige Migrationsstrategien für die Verlagerung von Anwendungen in die Cloud. Diese Strategien bauen auf den 5 Rs auf, die Gartner 2011 identifiziert hat, und bestehen aus folgenden Elementen:

- Faktorwechsel/Architekturwechsel – Verschieben Sie eine Anwendung und ändern Sie ihre Architektur, indem Sie alle Vorteile cloudnativer Feature nutzen, um Agilität, Leistung und Skalierbarkeit zu verbessern. Dies beinhaltet in der Regel die Portierung des Betriebssystems und der Datenbank. Beispiel: Migrieren Sie Ihre On-Premises-Oracle-Datenbank zu der PostgreSQL-kompatible Amazon-Aurora-Edition.
- Plattformwechsel (Lift and Reshape) – Verschieben Sie eine Anwendung in die Cloud und führen Sie ein gewisses Maß an Optimierung ein, um die Cloud-Funktionen zu nutzen. Beispiel: Migrieren Sie Ihre lokale Oracle-Datenbank zu Amazon Relational Database Service (Amazon RDS) für Oracle in der AWS Cloud.
- Neukauf (Drop and Shop) – Wechseln Sie zu einem anderen Produkt, indem Sie typischerweise von einer herkömmlichen Lizenz zu einem SaaS-Modell wechseln. Beispiel: Migrieren Sie Ihr CRM-System (Customer Relationship Management) zu Salesforce.com.
- Hostwechsel (Lift and Shift) – Verschieben Sie eine Anwendung in die Cloud, ohne Änderungen vorzunehmen, um die Cloud-Funktionen zu nutzen. Beispiel: Migrieren Sie Ihre lokale Oracle-Datenbank auf einer EC2-Instance in der Cloud zu Oracle. AWS
- Verschieben (Lift and Shift auf Hypervisor-Ebene) – Verlagern Sie die Infrastruktur in die Cloud, ohne neue Hardware kaufen, Anwendungen umschreiben oder Ihre bestehenden Abläufe ändern zu müssen. Dieses Migrationsszenario ist spezifisch für VMware Cloud on AWS, das die Kompatibilität mit virtuellen Maschinen (VM) und die Workload-Portabilität zwischen Ihrer lokalen Umgebung und unterstützt. AWS Sie können die VMware-Cloud-Foundation-Technologien von Ihren On-Premises-Rechenzentren aus verwenden, wenn Sie

Ihre Infrastruktur zu VMware Cloud in AWS migrieren. Beispiel: Verlagern Sie den Hypervisor, der Ihre Oracle-Datenbank hostet, zu VMware Cloud on. AWS

- Beibehaltung (Wiederaufgreifen) – Bewahren Sie Anwendungen in Ihrer Quellumgebung auf. Dazu können Anwendungen gehören, die einen umfangreichen Faktorwechsel erfordern und die Sie auf einen späteren Zeitpunkt verschieben möchten, sowie ältere Anwendungen, die Sie beibehalten möchten, da es keine geschäftliche Rechtfertigung für ihre Migration gibt.
- Außerbetriebnahme – Dekommissionierung oder Entfernung von Anwendungen, die in Ihrer Quellumgebung nicht mehr benötigt werden.

A

ABAC

Siehe attributbasierte Zugriffskontrolle.

abstrahierte Dienste

Siehe Managed Services.

ACID

Siehe Atomarität, Konsistenz, Isolierung und Haltbarkeit.

Aktiv-Aktiv-Migration

Eine Datenbankmigrationsmethode, bei der die Quell- und Zieldatenbanken synchron gehalten werden (mithilfe eines bidirektionalen Replikationstools oder dualer Schreibvorgänge) und beide Datenbanken Transaktionen von miteinander verbundenen Anwendungen während der Migration verarbeiten. Diese Methode unterstützt die Migration in kleinen, kontrollierten Batches, anstatt einen einmaligen Cutover zu erfordern. Es ist flexibler, erfordert aber mehr Arbeit als eine aktiv-passive Migration.

Aktiv-Passiv-Migration

Eine Datenbankmigrationsmethode, bei der die Quell- und Zieldatenbanken synchron gehalten werden, aber nur die Quelldatenbank Transaktionen von verbindenden Anwendungen verarbeitet, während Daten in die Zieldatenbank repliziert werden. Die Zieldatenbank akzeptiert während der Migration keine Transaktionen.

Aggregatfunktion

Eine SQL-Funktion, die mit einer Gruppe von Zeilen arbeitet und einen einzelnen Rückgabewert für die Gruppe berechnet. Beispiele für Aggregatfunktionen sind `SUM` und`MAX`.

AI

Siehe künstliche Intelligenz.

AIOps

Siehe Operationen mit künstlicher Intelligenz.

Anonymisierung

Der Prozess des dauerhaften Löschens personenbezogener Daten in einem Datensatz. Anonymisierung kann zum Schutz der Privatsphäre beitragen. Anonymisierte Daten gelten nicht mehr als personenbezogene Daten.

Anti-Muster

Eine häufig verwendete Lösung für ein wiederkehrendes Problem, bei dem die Lösung kontraproduktiv, ineffektiv oder weniger wirksam als eine Alternative ist.

Anwendungssteuerung

Ein Sicherheitsansatz, bei dem nur zugelassene Anwendungen verwendet werden können, um ein System vor Schadsoftware zu schützen.

Anwendungsportfolio

Eine Sammlung detaillierter Informationen zu jeder Anwendung, die von einer Organisation verwendet wird, einschließlich der Kosten für die Erstellung und Wartung der Anwendung und ihres Geschäftswerts. Diese Informationen sind entscheidend für den Prozess der Portfoliofindung und -analyse und hilft bei der Identifizierung und Priorisierung der Anwendungen, die migriert, modernisiert und optimiert werden sollen.

künstliche Intelligenz (KI)

Das Gebiet der Datenverarbeitungswissenschaft, das sich der Nutzung von Computertechnologien zur Ausführung kognitiver Funktionen widmet, die typischerweise mit Menschen in Verbindung gebracht werden, wie Lernen, Problemlösen und Erkennen von Mustern. Weitere Informationen finden Sie unter Was ist künstliche Intelligenz?

Operationen mit künstlicher Intelligenz (AIOps)

Der Prozess des Einsatzes von Techniken des Machine Learning zur Lösung betrieblicher Probleme, zur Reduzierung betrieblicher Zwischenfälle und menschlicher Eingriffe sowie zur Steigerung der Servicequalität. Weitere Informationen zur Verwendung von AIOps in der AWS -Migrationsstrategie finden Sie im Leitfaden zur Betriebsintegration.

Asymmetrische Verschlüsselung

Ein Verschlüsselungsalgorithmus, der ein Schlüsselpaar, einen öffentlichen Schlüssel für die Verschlüsselung und einen privaten Schlüssel für die Entschlüsselung verwendet. Sie können den öffentlichen Schlüssel teilen, da er nicht für die Entschlüsselung verwendet wird. Der Zugriff auf den privaten Schlüssel sollte jedoch stark eingeschränkt sein.

Atomizität, Konsistenz, Isolierung, Haltbarkeit (ACID)

Eine Reihe von Softwareeigenschaften, die die Datenvalidität und betriebliche Zuverlässigkeit einer Datenbank auch bei Fehlern, Stromausfällen oder anderen Problemen gewährleisten.

Attributbasierte Zugriffskontrolle (ABAC)

Die Praxis, detaillierte Berechtigungen auf der Grundlage von Benutzerattributen wie Abteilung, Aufgabenrolle und Teamname zu erstellen. Weitere Informationen finden Sie unter ABAC AWS in der AWS Identity and Access Management (IAM-) Dokumentation.

autoritative Datenquelle

Ein Ort, an dem Sie die primäre Version der Daten speichern, die als die zuverlässigste Informationsquelle angesehen wird. Sie können Daten aus der maßgeblichen Datenquelle an andere Speicherorte kopieren, um die Daten zu verarbeiten oder zu ändern, z. B. zu anonymisieren, zu redigieren oder zu pseudonymisieren.

Availability Zone

Ein bestimmter Standort innerhalb einer AWS-Region , der vor Ausfällen in anderen Availability Zones geschützt ist und kostengünstige Netzwerkkonnektivität mit niedriger Latenz zu anderen Availability Zones in derselben Region bietet.

AWS Framework für die Einführung der Cloud (AWS CAF)

Ein Framework mit Richtlinien und bewährten Verfahren, das Unternehmen bei der Entwicklung eines effizienten und effektiven Plans für den erfolgreichen Umstieg auf die Cloud unterstützt. AWS AWS CAF unterteilt die Leitlinien in sechs Schwerpunktbereiche, die als Perspektiven bezeichnet werden: Unternehmen, Mitarbeiter, Unternehmensführung, Plattform, Sicherheit und

Betrieb. Die Perspektiven Geschäft, Mitarbeiter und Unternehmensführung konzentrieren sich auf Geschäftskompetenzen und -prozesse, während sich die Perspektiven Plattform, Sicherheit und Betriebsabläufe auf technische Fähigkeiten und Prozesse konzentrieren. Die Personalperspektive zielt beispielsweise auf Stakeholder ab, die sich mit Personalwesen (HR), Personalfunktionen und Personalmanagement befassen. Aus dieser Perspektive bietet AWS CAF Leitlinien für Personalentwicklung, Schulung und Kommunikation, um das Unternehmen auf eine erfolgreiche Cloud-Einführung vorzubereiten. Weitere Informationen finden Sie auf der AWS -CAF-Webseite und dem AWS -CAF-Whitepaper.

AWS Workload-Qualifizierungsrahmen (AWS WQF)

Ein Tool, das Workloads bei der Datenbankmigration bewertet, Migrationsstrategien empfiehlt und Arbeitsschätzungen bereitstellt. AWS WQF ist in () enthalten. AWS Schema Conversion Tool AWS SCT Es analysiert Datenbankschemas und Codeobjekte, Anwendungscode, Abhängigkeiten und Leistungsmerkmale und stellt Bewertungsberichte bereit.

B

schlechter Bot

Ein Bot, der Einzelpersonen oder Organisationen stören oder ihnen Schaden zufügen soll.

BCP

Siehe Planung der Geschäftskontinuität.

Verhaltensdiagramm

Eine einheitliche, interaktive Ansicht des Ressourcenverhaltens und der Interaktionen im Laufe der Zeit. Sie können ein Verhaltensdiagramm mit Amazon Detective verwenden, um fehlgeschlagene Anmeldeversuche, verdächtige API-Aufrufe und ähnliche Vorgänge zu untersuchen. Weitere Informationen finden Sie unter Daten in einem Verhaltensdiagramm in der Detective-Dokumentation.

Big-Endian-System

Ein System, welches das höchstwertige Byte zuerst speichert. Siehe auch Endianness.

Binäre Klassifikation

Ein Prozess, der ein binäres Ergebnis vorhersagt (eine von zwei möglichen Klassen). Beispielsweise könnte Ihr ML-Modell möglicherweise Probleme wie „Handelt es sich bei dieser

E-Mail um Spam oder nicht?“ vorhersagen müssen oder „Ist dieses Produkt ein Buch oder ein Auto?“

Bloom-Filter

Eine probabilistische, speichereffiziente Datenstruktur, mit der getestet wird, ob ein Element Teil einer Menge ist.

Blau/Grün-Bereitstellung

Eine Bereitstellungsstrategie, bei der Sie zwei separate, aber identische Umgebungen erstellen. Sie führen die aktuelle Anwendungsversion in einer Umgebung (blau) und die neue Anwendungsversion in der anderen Umgebung (grün) aus. Mit dieser Strategie können Sie schnell und mit minimalen Auswirkungen ein Rollback durchführen.

Bot

Eine Softwareanwendung, die automatisierte Aufgaben über das Internet ausführt und menschliche Aktivitäten oder Interaktionen simuliert. Manche Bots sind nützlich oder nützlich, wie z. B. Webcrawler, die Informationen im Internet indexieren. Einige andere Bots, sogenannte bösartige Bots, sollen Einzelpersonen oder Organisationen stören oder ihnen Schaden zufügen.

Botnetz

Netzwerke von Bots, die mit Malware infiziert sind und unter der Kontrolle einer einzigen Partei stehen, die als Bot-Herder oder Bot-Operator bezeichnet wird. Botnetze sind der bekannteste Mechanismus zur Skalierung von Bots und ihrer Wirkung.

branch

Ein containerisierter Bereich eines Code-Repositorys. Der erste Zweig, der in einem Repository erstellt wurde, ist der Hauptzweig. Sie können einen neuen Zweig aus einem vorhandenen Zweig erstellen und dann Feature entwickeln oder Fehler in dem neuen Zweig beheben. Ein Zweig, den Sie erstellen, um ein Feature zu erstellen, wird allgemein als Feature-Zweig bezeichnet. Wenn das Feature zur Veröffentlichung bereit ist, führen Sie den Feature-Zweig wieder mit dem Hauptzweig zusammen. Weitere Informationen finden Sie unter Über Branches (GitHub Dokumentation).

Zugang durch Glasbruch

Unter außergewöhnlichen Umständen und im Rahmen eines genehmigten Verfahrens ist dies eine schnelle Methode für einen Benutzer, auf einen Bereich zuzugreifen AWS-Konto , für den

er in der Regel keine Zugriffsrechte besitzt. Weitere Informationen finden Sie unter dem Indikator Implementation break-glass procedures in den AWS Well-Architected-Leitlinien.

Brownfield-Strategie

Die bestehende Infrastruktur in Ihrer Umgebung. Wenn Sie eine Brownfield-Strategie für eine Systemarchitektur anwenden, richten Sie sich bei der Gestaltung der Architektur nach den Einschränkungen der aktuellen Systeme und Infrastruktur. Wenn Sie die bestehende Infrastruktur erweitern, könnten Sie Brownfield- und Greenfield-Strategien mischen.

Puffer-Cache

Der Speicherbereich, in dem die am häufigsten abgerufenen Daten gespeichert werden.

Geschäftsfähigkeit

Was ein Unternehmen tut, um Wert zu generieren (z. B. Vertrieb, Kundenservice oder Marketing). Microservices-Architekturen und Entwicklungsentscheidungen können von den Geschäftskapazitäten beeinflusst werden. Weitere Informationen finden Sie im Abschnitt Organisiert nach Geschäftskapazitäten des Whitepapers Ausführen von containerisierten Microservices in AWS.

Planung der Geschäftskontinuität (BCP)

Ein Plan, der die potenziellen Auswirkungen eines störenden Ereignisses, wie z. B. einer groß angelegten Migration, auf den Betrieb berücksichtigt und es einem Unternehmen ermöglicht, den Betrieb schnell wieder aufzunehmen.

C

CAF

Weitere Informationen finden Sie unter Framework für die AWS Cloud-Einführung.

Bereitstellung auf Kanaren

Die langsame und schrittweise Veröffentlichung einer Version für Endbenutzer. Wenn Sie sich sicher sind, stellen Sie die neue Version bereit und ersetzen die aktuelle Version vollständig.

CCoE

Weitere Informationen finden Sie im Cloud Center of Excellence.

CDC

Siehe Erfassung von Änderungsdaten.

Erfassung von Datenänderungen (CDC)

Der Prozess der Nachverfolgung von Änderungen an einer Datenquelle, z. B. einer Datenbanktabelle, und der Aufzeichnung von Metadaten zu der Änderung. Sie können CDC für verschiedene Zwecke verwenden, z. B. für die Prüfung oder Replikation von Änderungen in einem Zielsystem, um die Synchronisation aufrechtzuerhalten.

Chaos-Technik

Absichtliches Einführen von Ausfällen oder Störungsereignissen, um die Widerstandsfähigkeit eines Systems zu testen. Sie können AWS Fault Injection Service (AWS FIS) verwenden, um Experimente durchzuführen, die Ihre AWS Workloads stress, und deren Reaktion zu bewerten.

CI/CD

Siehe Continuous Integration und Continuous Delivery.

Klassifizierung

Ein Kategorisierungsprozess, der bei der Erstellung von Vorhersagen hilft. ML-Modelle für Klassifikationsprobleme sagen einen diskreten Wert voraus. Diskrete Werte unterscheiden sich immer voneinander. Beispielsweise muss ein Modell möglicherweise auswerten, ob auf einem Bild ein Auto zu sehen ist oder nicht.

clientseitige Verschlüsselung

Lokale Verschlüsselung von Daten, bevor das Ziel sie AWS-Service empfängt.

Cloud-Kompetenzzentrum (CCoE)

Ein multidisziplinäres Team, das die Cloud-Einführung in der gesamten Organisation vorantreibt, einschließlich der Entwicklung bewährter Cloud-Methoden, der Mobilisierung von Ressourcen, der Festlegung von Migrationszeitplänen und der Begleitung der Organisation durch groß angelegte Transformationen. Weitere Informationen finden Sie in den CCoE-Beiträgen im AWS Cloud Enterprise Strategy Blog.

Cloud Computing

Die Cloud-Technologie, die typischerweise für die Ferndatenspeicherung und das IoT-Gerätemanagement verwendet wird. Cloud Computing ist häufig mit Edge-Computing-Technologie verbunden.

Cloud-Betriebsmodell

In einer IT-Organisation das Betriebsmodell, das zum Aufbau, zur Weiterentwicklung und Optimierung einer oder mehrerer Cloud-Umgebungen verwendet wird. Weitere Informationen finden Sie unter Aufbau Ihres Cloud-Betriebsmodells.

Phasen der Einführung der Cloud

Die vier Phasen, die Unternehmen normalerweise durchlaufen, wenn sie zur AWS Cloud migrieren:

- Projekt – Durchführung einiger Cloud-bezogener Projekte zu Machbarkeitsnachweisen und zu Lernzwecken
- Fundament – Grundlegende Investitionen tätigen, um Ihre Cloud-Einführung zu skalieren (z. B. Einrichtung einer Landing Zone, Definition eines CCoE, Einrichtung eines Betriebsmodells)
- Migration – Migrieren einzelner Anwendungen
- Neuentwicklung – Optimierung von Produkten und Services und Innovation in der Cloud

Diese Phasen wurden von Stephen Orban im Blogbeitrag The Journey Toward Cloud-First & the Stages of Adoption im AWS Cloud Enterprise Strategy-Blog definiert. Informationen darüber, wie sie mit der AWS Migrationsstrategie zusammenhängen, finden Sie im Leitfaden zur Vorbereitung der Migration.

CMDB

Siehe Datenbank für das Konfigurationsmanagement.

Code-Repository

Ein Ort, an dem Quellcode und andere Komponenten wie Dokumentation, Beispiele und Skripts gespeichert und im Rahmen von Versionskontrollprozessen aktualisiert werden. Zu den gängigen Cloud-Repositorys gehören GitHub oder AWS CodeCommit. Jede Version des Codes wird Zweig genannt. In einer Microservice-Struktur ist jedes Repository einer einzelnen Funktionalität gewidmet. Eine einzelne CI/CD-Pipeline kann mehrere Repositorien verwenden.

Kalter Cache

Ein Puffer-Cache, der leer oder nicht gut gefüllt ist oder veraltete oder irrelevante Daten enthält. Dies beeinträchtigt die Leistung, da die Datenbank-Instance aus dem Hauptspeicher oder der Festplatte lesen muss, was langsamer ist als das Lesen aus dem Puffercache.

Kalte Daten

Daten, auf die selten zugegriffen wird und die in der Regel historisch sind. Bei der Abfrage dieser Art von Daten sind langsame Abfragen in der Regel akzeptabel. Durch die Verlagerung dieser Daten auf leistungsschwächere und kostengünstigere Speicherstufen oder -klassen können Kosten gesenkt werden.

Computer Vision (CV)

Ein Bereich der KI, der maschinelles Lernen nutzt, um Informationen aus visuellen Formaten wie digitalen Bildern und Videos zu analysieren und zu extrahieren. AWS Panorama Bietet beispielsweise Geräte an, die CV zu lokalen Kameranetzwerken hinzufügen, und Amazon SageMaker stellt Bildverarbeitungsalgorithmen für CV bereit.

Drift in der Konfiguration

Bei einer Arbeitslast eine Änderung der Konfiguration gegenüber dem erwarteten Zustand. Dies kann dazu führen, dass der Workload nicht mehr richtlinienkonform wird, und zwar in der Regel schrittweise und unbeabsichtigt.

Verwaltung der Datenbankkonfiguration (CMDB)

Ein Repository, das Informationen über eine Datenbank und ihre IT-Umgebung speichert und verwaltet, inklusive Hardware- und Softwarekomponenten und deren Konfigurationen. In der Regel verwenden Sie Daten aus einer CMDB in der Phase der Portfolioerkennung und -analyse der Migration.

Konformitätspaket

Eine Sammlung von AWS Config Regeln und Abhilfemaßnahmen, die Sie zusammenstellen können, um Ihre Konformitäts- und Sicherheitsprüfungen individuell anzupassen. Mithilfe einer YAML-Vorlage können Sie ein Conformance Pack als einzelne Entität in einer AWS-Konto AND-Region oder unternehmensweit bereitstellen. Weitere Informationen finden Sie in der Dokumentation unter Conformance Packs. AWS Config

Kontinuierliche Bereitstellung und kontinuierliche Integration (CI/CD)

Der Prozess der Automatisierung der Quell-, Build-, Test-, Staging- und Produktionsphasen des Softwareveröffentlichungsprozesses. CI/CD wird allgemein als Pipeline beschrieben. CI/CD kann Ihnen helfen, Prozesse zu automatisieren, die Produktivität zu steigern, die Codequalität zu verbessern und schneller zu liefern. Weitere Informationen finden Sie unter Vorteile der kontinuierlichen Auslieferung. CD kann auch für kontinuierliche Bereitstellung stehen. Weitere

Informationen finden Sie unterKontinuierliche Auslieferung im Vergleich zu kontinuierlicher Bereitstellung.

CV

Siehe Computer Vision.

D

Daten im Ruhezustand

Daten, die in Ihrem Netzwerk stationär sind, z. B. Daten, die sich im Speicher befinden.

Datenklassifizierung

Ein Prozess zur Identifizierung und Kategorisierung der Daten in Ihrem Netzwerk auf der Grundlage ihrer Kritikalität und Sensitivität. Sie ist eine wichtige Komponente jeder Strategie für das Management von Cybersecurity-Risiken, da sie Ihnen hilft, die geeigneten Schutz- und Aufbewahrungskontrollen für die Daten zu bestimmen. Die Datenklassifizierung ist ein Bestandteil der Sicherheitssäule im AWS Well-Architected Framework. Weitere Informationen finden Sie unter Datenklassifizierung.

Datendrift

Eine signifikante Variation zwischen den Produktionsdaten und den Daten, die zum Trainieren eines ML-Modells verwendet wurden, oder eine signifikante Änderung der Eingabedaten im Laufe der Zeit. Datendrift kann die Gesamtqualität, Genauigkeit und Fairness von ML-Modellvorhersagen beeinträchtigen.

Daten während der Übertragung

Daten, die sich aktiv durch Ihr Netzwerk bewegen, z. B. zwischen Netzwerkressourcen.

Datennetz

Ein architektonisches Framework, das verteilte, dezentrale Dateneigentum mit zentraler Verwaltung und Steuerung ermöglicht.

Datenminimierung

Das Prinzip, nur die Daten zu sammeln und zu verarbeiten, die unbedingt erforderlich sind. Durch Datenminimierung im AWS Cloud können Datenschutzrisiken, Kosten und der CO2-Fußabdruck Ihrer Analysen reduziert werden.

Datenperimeter

Eine Reihe präventiver Schutzmaßnahmen in Ihrer AWS Umgebung, mit denen sichergestellt werden kann, dass nur vertrauenswürdige Identitäten auf vertrauenswürdige Ressourcen von erwarteten Netzwerken zugreifen. Weitere Informationen finden Sie unter Aufbau eines Datenperimeters auf. AWS

Vorverarbeitung der Daten

Rohdaten in ein Format umzuwandeln, das von Ihrem ML-Modell problemlos verarbeitet werden kann. Die Vorverarbeitung von Daten kann bedeuten, dass bestimmte Spalten oder Zeilen entfernt und fehlende, inkonsistente oder doppelte Werte behoben werden.

Herkunft der Daten

Der Prozess der Nachverfolgung des Ursprungs und der Geschichte von Daten während ihres gesamten Lebenszyklus, z. B. wie die Daten generiert, übertragen und gespeichert wurden.

betroffene Person

Eine Person, deren Daten gesammelt und verarbeitet werden.

Data Warehouse

Ein Datenverwaltungssystem, das Business Intelligence wie Analysen unterstützt. Data Warehouses enthalten in der Regel große Mengen historischer Daten und werden in der Regel für Abfragen und Analysen verwendet.

Datenbankdefinitionssprache (DDL)

Anweisungen oder Befehle zum Erstellen oder Ändern der Struktur von Tabellen und Objekten in einer Datenbank.

Datenbankmanipulationssprache (DML)

Anweisungen oder Befehle zum Ändern (Einfügen, Aktualisieren und Löschen) von Informationen in einer Datenbank.

DDL

Siehe Datenbankdefinitionssprache.

Deep-Ensemble

Mehrere Deep-Learning-Modelle zur Vorhersage kombinieren. Sie können Deep-Ensembles verwenden, um eine genauere Vorhersage zu erhalten oder um die Unsicherheit von Vorhersagen abzuschätzen.

Deep Learning

Ein ML-Teilbereich, der mehrere Schichten künstlicher neuronaler Netzwerke verwendet, um die Zuordnung zwischen Eingabedaten und Zielvariablen von Interesse zu ermitteln.

defense-in-depth

Ein Ansatz zur Informationssicherheit, bei dem eine Reihe von Sicherheitsmechanismen und -kontrollen sorgfältig in einem Computernetzwerk verteilt werden, um die Vertraulichkeit, Integrität und Verfügbarkeit des Netzwerks und der darin enthaltenen Daten zu schützen. Wenn Sie diese Strategie anwenden AWS, fügen Sie mehrere Steuerelemente auf verschiedenen Ebenen der AWS Organizations Struktur hinzu, um die Ressourcen zu schützen. Ein defense-in-depth Ansatz könnte beispielsweise Multi-Faktor-Authentifizierung, Netzwerksegmentierung und Verschlüsselung kombinieren.

delegierter Administrator

In kann ein kompatibler Dienst ein AWS Mitgliedskonto registrieren AWS Organizations, um die Konten der Organisation zu verwalten und die Berechtigungen für diesen Dienst zu verwalten. Dieses Konto wird als delegierter Administrator für diesen Service bezeichnet. Weitere Informationen und eine Liste kompatibler Services finden Sie unter Services, die mit AWS Organizations funktionieren in der AWS Organizations -Dokumentation.

Bereitstellung

Der Prozess, bei dem eine Anwendung, neue Feature oder Codekorrekturen in der Zielumgebung verfügbar gemacht werden. Die Bereitstellung umfasst das Implementieren von Änderungen an einer Codebasis und das anschließende Erstellen und Ausführen dieser Codebasis in den Anwendungsumgebungen.

Entwicklungsumgebung

Siehe Umgebung.

Detektivische Kontrolle

Eine Sicherheitskontrolle, die darauf ausgelegt ist, ein Ereignis zu erkennen, zu protokollieren und zu warnen, nachdem ein Ereignis eingetreten ist. Diese Kontrollen stellen eine zweite Verteidigungslinie dar und warnen Sie vor Sicherheitsereignissen, bei denen die vorhandenen präventiven Kontrollen umgangen wurden. Weitere Informationen finden Sie unter Detektivische Kontrolle in Implementierung von Sicherheitskontrollen in AWS.

Abbildung des Wertstroms in der Entwicklung (DVSM)

Ein Prozess zur Identifizierung und Priorisierung von Einschränkungen, die sich negativ auf Geschwindigkeit und Qualität im Lebenszyklus der Softwareentwicklung auswirken. DVSM erweitert den Prozess der Wertstromanalyse, der ursprünglich für Lean-Manufacturing-Praktiken konzipiert wurde. Es konzentriert sich auf die Schritte und Teams, die erforderlich sind, um durch den Softwareentwicklungsprozess Mehrwert zu schaffen und zu steigern.

digitaler Zwilling

Eine virtuelle Darstellung eines realen Systems, z. B. eines Gebäudes, einer Fabrik, einer Industrieanlage oder einer Produktionslinie. Digitale Zwillinge unterstützen vorausschauende Wartung, Fernüberwachung und Produktionsoptimierung.

Maßtabelle

In einem Sternschema eine kleinere Tabelle, die Datenattribute zu quantitativen Daten in einer Faktentabelle enthält. Bei Attributen von Dimensionstabellen handelt es sich in der Regel um Textfelder oder diskrete Zahlen, die sich wie Text verhalten. Diese Attribute werden häufig zum Einschränken von Abfragen, zum Filtern und zur Kennzeichnung von Ergebnismengen verwendet.

Katastrophe

Ein Ereignis, das verhindert, dass ein Workload oder ein System seine Geschäftsziele an seinem primären Einsatzort erfüllt. Diese Ereignisse können Naturkatastrophen, technische Ausfälle oder das Ergebnis menschlichen Handelns sein, z. B. unbeabsichtigte Fehlkonfigurationen oder ein Malware-Angriff.

Disaster Recovery (DR)

Die Strategie und der Prozess, mit denen Sie Ausfallzeiten und Datenverluste aufgrund einer Katastrophe minimieren. Weitere Informationen finden Sie unter Disaster Recovery von Workloads unter AWS: Wiederherstellung in der Cloud im AWS Well-Architected Framework.

DML

Siehe Sprache zur Datenbankmanipulation.

Domainorientiertes Design

Ein Ansatz zur Entwicklung eines komplexen Softwaresystems, bei dem seine Komponenten mit sich entwickelnden Domains oder Kerngeschäftszielen verknüpft werden, denen jede Komponente dient. Dieses Konzept wurde von Eric Evans in seinem Buch Domaingesteuertes

Design: Bewältigen der Komplexität im Herzen der Software (Boston: Addison-Wesley Professional, 2003) vorgestellt. Informationen darüber, wie Sie domaingesteuertes Design mit dem Strangler-Fig-Muster verwenden können, finden Sie unter Schrittweises Modernisieren älterer Microsoft ASP.NET (ASMX)-Webservices mithilfe von Containern und Amazon API Gateway.

DR

Siehe Disaster Recovery.

Erkennung von Driften

Verfolgung von Abweichungen von einer Basiskonfiguration Sie können es beispielsweise verwenden, AWS CloudFormation um Abweichungen bei den Systemressourcen zu erkennen, oder Sie können AWS Control Tower damit Änderungen in Ihrer landing zone erkennen, die sich auf die Einhaltung von Governance-Anforderungen auswirken könnten.

DVSM

Siehe Abbildung der Wertströme in der Entwicklung.

E

EDA

Siehe explorative Datenanalyse.

Edge-Computing

Die Technologie, die die Rechenleistung für intelligente Geräte an den Rändern eines IoT-Netzwerks erhöht. Im Vergleich zu Cloud Computing kann Edge Computing die Kommunikationslatenz reduzieren und die Reaktionszeit verbessern.

Verschlüsselung

Ein Rechenprozess, der Klartextdaten, die für Menschen lesbar sind, in Chiffretext umwandelt.

Verschlüsselungsschlüssel

Eine kryptografische Zeichenfolge aus zufälligen Bits, die von einem Verschlüsselungsalgorithmus generiert wird. Schlüssel können unterschiedlich lang sein, und jeder Schlüssel ist so konzipiert, dass er unvorhersehbar und einzigartig ist.

Endianismus

Die Reihenfolge, in der Bytes im Computerspeicher gespeichert werden. Big-Endian-Systeme speichern das höchstwertige Byte zuerst. Little-Endian-Systeme speichern das niedrigwertigste Byte zuerst.

Endpunkt

Siehe Service-Endpunkt.

Endpunkt-Services

Ein Service, den Sie in einer Virtual Private Cloud (VPC) hosten können, um ihn mit anderen Benutzern zu teilen. Sie können einen Endpunktdienst mit anderen AWS-Konten oder AWS Identity and Access Management (IAM AWS PrivateLink -) Prinzipalen erstellen und diesen Berechtigungen gewähren. Diese Konten oder Prinzipale können sich privat mit Ihrem Endpunktservice verbinden, indem sie Schnittstellen-VPC-Endpunkte erstellen. Weitere Informationen finden Sie unter Einen Endpunkt-Service erstellen in der Amazon Virtual Private Cloud (Amazon VPC)-Dokumentation.

Unternehmensressourcenplanung (ERP)

Ein System, das wichtige Geschäftsprozesse (wie Buchhaltung, MES und Projektmanagement) für ein Unternehmen automatisiert und verwaltet.

Envelope-Verschlüsselung

Der Prozess der Verschlüsselung eines Verschlüsselungsschlüssels mit einem anderen Verschlüsselungsschlüssel. Weitere Informationen finden Sie unter Envelope-Verschlüsselung in der AWS Key Management Service (AWS KMS) -Dokumentation.

Umgebung

Eine Instance einer laufenden Anwendung. Die folgenden Arten von Umgebungen sind beim Cloud-Computing üblich:

- Entwicklungsumgebung – Eine Instance einer laufenden Anwendung, die nur dem Kernteam zur Verfügung steht, das für die Wartung der Anwendung verantwortlich ist. Entwicklungsumgebungen werden verwendet, um Änderungen zu testen, bevor sie in höhere Umgebungen übertragen werden. Diese Art von Umgebung wird manchmal als Testumgebung bezeichnet.
- Niedrigere Umgebungen – Alle Entwicklungsumgebungen für eine Anwendung, z. B. solche, die für erste Builds und Tests verwendet wurden.

- Produktionsumgebung – Eine Instance einer laufenden Anwendung, auf die Endbenutzer zugreifen können. In einer CI/CD-Pipeline ist die Produktionsumgebung die letzte Bereitstellungsumgebung.
- Höhere Umgebungen – Alle Umgebungen, auf die auch andere Benutzer als das Kernentwicklungsteam zugreifen können. Dies kann eine Produktionsumgebung, Vorproduktionsumgebungen und Umgebungen für Benutzerakzeptanztests umfassen.

Epics

In der agilen Methodik sind dies funktionale Kategorien, die Ihnen helfen, Ihre Arbeit zu organisieren und zu priorisieren. Epics bieten eine allgemeine Beschreibung der Anforderungen und Implementierungsaufgaben. Zu den Sicherheitsthemen AWS von CAF gehören beispielsweise Identitäts- und Zugriffsmanagement, Detektivkontrollen, Infrastruktursicherheit, Datenschutz und Reaktion auf Vorfälle. Weitere Informationen zu Epics in der AWS - Migrationsstrategie finden Sie im Leitfaden zur Programm-Implementierung.

ERP

Siehe Enterprise Resource Planning.

Explorative Datenanalyse (EDA)

Der Prozess der Analyse eines Datensatzes, um seine Hauptmerkmale zu verstehen. Sie sammeln oder aggregieren Daten und führen dann erste Untersuchungen durch, um Muster zu finden, Anomalien zu erkennen und Annahmen zu überprüfen. EDA wird durchgeführt, indem zusammenfassende Statistiken berechnet und Datenvisualisierungen erstellt werden.

F

Faktentabelle

Die zentrale Tabelle in einem Sternschema. Sie speichert quantitative Daten über den Geschäftsbetrieb. In der Regel enthält eine Faktentabelle zwei Arten von Spalten: Spalten, die Kennzahlen enthalten, und Spalten, die einen Fremdschlüssel für eine Dimensionstabelle enthalten.

schnell scheitern

Eine Philosophie, die häufige und inkrementelle Tests verwendet, um den Entwicklungslebenszyklus zu verkürzen. Dies ist ein wichtiger Bestandteil eines agilen Ansatzes.

Grenze zur Fehlerisolierung

Dabei handelt es sich um eine Grenze AWS Cloud, z. B. eine Availability Zone AWS-Region, eine Steuerungsebene oder eine Datenebene, die die Auswirkungen eines Fehlers begrenzt und die Widerstandsfähigkeit von Workloads verbessert. Weitere Informationen finden Sie unter Grenzen zur AWS Fehlerisolierung.

Feature-Zweig

Siehe Zweig.

Features

Die Eingabedaten, die Sie verwenden, um eine Vorhersage zu treffen. In einem Fertigungskontext könnten Feature beispielsweise Bilder sein, die regelmäßig von der Fertigungslinie aus aufgenommen werden.

Bedeutung der Feature

Wie wichtig ein Feature für die Vorhersagen eines Modells ist. Dies wird in der Regel als numerischer Wert ausgedrückt, der mit verschiedenen Techniken wie Shapley Additive Explanations (SHAP) und integrierten Gradienten berechnet werden kann. Weitere Informationen finden Sie unter Interpretierbarkeit von Modellen für maschinelles Lernen mit:AWS.

Featuretransformation

Daten für den ML-Prozess optimieren, einschließlich der Anreicherung von Daten mit zusätzlichen Quellen, der Skalierung von Werten oder der Extraktion mehrerer Informationssätze aus einem einzigen Datenfeld. Das ermöglicht dem ML-Modell, von den Daten profitieren. Wenn Sie beispielsweise das Datum „27.05.2021 00:15:37“ in „2021“, „Mai“, „Donnerstag“ und „15“ aufschlüsseln, können Sie dem Lernalgorithmus helfen, nuancierte Muster zu erlernen, die mit verschiedenen Datenkomponenten verknüpft sind.

FGAC

Siehe detaillierte Zugriffskontrolle.

Feinkörnige Zugriffskontrolle (FGAC)

Die Verwendung mehrerer Bedingungen, um eine Zugriffsanfrage zuzulassen oder abzulehnen.

Flash-Cut-Migration

Eine Datenbankmigrationsmethode, bei der eine kontinuierliche Datenreplikation durch Erfassung von Änderungsdaten verwendet wird, um Daten in kürzester Zeit zu migrieren, anstatt einen schrittweisen Ansatz zu verwenden. Ziel ist es, Ausfallzeiten auf ein Minimum zu beschränken.

G

Geoblocking

Siehe geografische Einschränkungen.

Geografische Einschränkungen (Geoblocking)

Bei Amazon eine Option CloudFront, um zu verhindern, dass Benutzer in bestimmten Ländern auf Inhaltsverteilungen zugreifen. Sie können eine Zulassungsliste oder eine Sperrliste verwenden, um zugelassene und gesperrte Länder anzugeben. Weitere Informationen finden Sie in der Dokumentation unter Beschränkung der geografischen Verteilung Ihrer Inhalte. CloudFront

Gitflow-Workflow

Ein Ansatz, bei dem niedrigere und höhere Umgebungen unterschiedliche Zweige in einem Quellcode-Repository verwenden. Der Gitflow-Workflow gilt als veraltet, und der Trunk-basierte Workflow ist der moderne, bevorzugte Ansatz.

Greenfield-Strategie

Das Fehlen vorhandener Infrastruktur in einer neuen Umgebung. Bei der Einführung einer Neuausrichtung einer Systemarchitektur können Sie alle neuen Technologien ohne Einschränkung der Kompatibilität mit der vorhandenen Infrastruktur auswählen, auch bekannt als Brownfield. Wenn Sie die bestehende Infrastruktur erweitern, könnten Sie Brownfield- und Greenfield-Strategien mischen.

Integritätsschutz

Eine allgemeine Regel, die dabei hilft, Ressourcen, Richtlinien und die Einhaltung von Vorschriften in allen Organisationseinheiten (OUs) zu regeln. Präventiver Integritätsschutz setzt Richtlinien durch, um die Einhaltung von Standards zu gewährleisten. Sie werden mithilfe von Service-Kontrollrichtlinien und IAM-Berechtigungsgrenzen implementiert. Detektivischer Integritätsschutz erkennt Richtlinienverstöße und Compliance-Probleme und generiert Warnmeldungen zur Abhilfe. Sie werden mithilfe von AWS Config, AWS Security Hub, Amazon

GuardDuty AWS Trusted Advisor, Amazon Inspector und benutzerdefinierten AWS Lambda Prüfungen implementiert.

H

HEKTAR

Siehe Hochverfügbarkeit.

Heterogene Datenbankmigration

Migrieren Sie Ihre Quelldatenbank in eine Zieldatenbank, die eine andere Datenbank-Engine verwendet (z. B. Oracle zu Amazon Aurora). Eine heterogene Migration ist in der Regel Teil einer Neuarchitektur, und die Konvertierung des Schemas kann eine komplexe Aufgabe sein. AWS bietet AWS SCT, welches bei Schemakonvertierungen hilft.

hohe Verfügbarkeit (HA)

Die Fähigkeit eines Workloads, im Falle von Herausforderungen oder Katastrophen kontinuierlich und ohne Eingreifen zu arbeiten. HA-Systeme sind so konzipiert, dass sie automatisch ein Failover durchführen, eine gleichbleibend hohe Leistung bieten und unterschiedliche Lasten und Ausfälle mit minimalen Leistungseinbußen bewältigen.

historische Modernisierung

Ein Ansatz zur Modernisierung und Aufrüstung von Betriebstechnologiesystemen (OT), um den Bedürfnissen der Fertigungsindustrie besser gerecht zu werden. Ein Historian ist eine Art von Datenbank, die verwendet wird, um Daten aus verschiedenen Quellen in einer Fabrik zu sammeln und zu speichern.

Homogene Datenbankmigration

Migrieren Sie Ihre Quelldatenbank zu einer Zieldatenbank, die dieselbe Datenbank-Engine verwendet (z. B. Microsoft SQL Server zu Amazon RDS für SQL Server). Eine homogene Migration ist in der Regel Teil eines Hostwechsels oder eines Plattformwechsels. Sie können native Datenbankserviceprogramme verwenden, um das Schema zu migrieren.

heiße Daten

Daten, auf die häufig zugegriffen wird, z. B. Echtzeitdaten oder aktuelle Translationsdaten. Für diese Daten ist in der Regel eine leistungsstarke Speicherebene oder -klasse erforderlich, um schnelle Abfrageantworten zu ermöglichen.

Hotfix

Eine dringende Lösung für ein kritisches Problem in einer Produktionsumgebung. Aufgrund seiner Dringlichkeit wird ein Hotfix normalerweise außerhalb des typischen DevOps Release-Workflows erstellt.

Hypercare-Phase

Unmittelbar nach dem Cutover, der Zeitraum, in dem ein Migrationsteam die migrierten Anwendungen in der Cloud verwaltet und überwacht, um etwaige Probleme zu beheben. In der Regel dauert dieser Zeitraum 1–4 Tage. Am Ende der Hypercare-Phase überträgt das Migrationsteam in der Regel die Verantwortung für die Anwendungen an das Cloud-Betriebsteam.

I

IaC

Sehen Sie Infrastruktur als Code.

Identitätsbasierte Richtlinie

Eine Richtlinie, die einem oder mehreren IAM-Prinzipalen zugeordnet ist und deren Berechtigungen innerhalb der AWS Cloud Umgebung definiert.

Leerlaufanwendung

Eine Anwendung mit einer durchschnittlichen CPU- und Arbeitsspeicherauslastung zwischen 5 und 20 Prozent über einen Zeitraum von 90 Tagen. In einem Migrationsprojekt ist es üblich, diese Anwendungen außer Betrieb zu nehmen oder sie On-Premises beizubehalten.

IIoT

Siehe Industrielles Internet der Dinge.

unveränderliche Infrastruktur

Ein Modell, das eine neue Infrastruktur für Produktionsworkloads bereitstellt, anstatt die bestehende Infrastruktur zu aktualisieren, zu patchen oder zu modifizieren. Unveränderliche Infrastrukturen sind von Natur aus konsistenter, zuverlässiger und vorhersehbarer als veränderliche Infrastrukturen. Weitere Informationen finden Sie in der Best Practice Deploy using immutable infrastructure im AWS Well-Architected Framework.

Eingehende (ingress) VPC

In einer Architektur AWS mit mehreren Konten ist dies eine VPC, die Netzwerkverbindungen von außerhalb einer Anwendung akzeptiert, überprüft und weiterleitet. Die AWS -Referenzarchitektur für die Sicherheit empfiehlt, Ihr Netzwerkkonto mit eingehenden und ausgehenden VPCs und Inspektions-VPCs einzurichten, um die bidirektionale Schnittstelle zwischen Ihrer Anwendung und dem Internet zu schützen.

Inkrementelle Migration

Eine Cutover-Strategie, bei der Sie Ihre Anwendung in kleinen Teilen migrieren, anstatt eine einziges vollständiges Cutover durchzuführen. Beispielsweise könnten Sie zunächst nur einige Microservices oder Benutzer auf das neue System umstellen. Nachdem Sie sich vergewissert haben, dass alles ordnungsgemäß funktioniert, können Sie weitere Microservices oder Benutzer schrittweise verschieben, bis Sie Ihr Legacy-System außer Betrieb nehmen können. Diese Strategie reduziert die mit großen Migrationen verbundenen Risiken.

Industrie 4.0

Ein Begriff, der 2016 von Klaus Schwab eingeführt wurde und sich auf die Modernisierung von Fertigungsprozessen durch Fortschritte in den Bereichen Konnektivität, Echtzeitdaten, Automatisierung, Analytik und KI/ML bezieht.

Infrastruktur

Alle Ressourcen und Komponenten, die in der Umgebung einer Anwendung enthalten sind.

Infrastructure as Code (IaC)

Der Prozess der Bereitstellung und Verwaltung der Infrastruktur einer Anwendung mithilfe einer Reihe von Konfigurationsdateien. IaC soll Ihnen helfen, das Infrastrukturmanagement zu zentralisieren, Ressourcen zu standardisieren und schnell zu skalieren, sodass neue Umgebungen wiederholbar, zuverlässig und konsistent sind.

Industrielles Internet der Dinge (IIoT)

Einsatz von mit dem Internet verbundenen Sensoren und Geräten in Industriesektoren wie Fertigung, Energie, Automobilindustrie, Gesundheitswesen, Biowissenschaften und Landwirtschaft. Mehr Informationen finden Sie unter Aufbau einer digitalen Transformationsstrategie für das industrielle Internet der Dinge (IIoT).

Inspektions-VPC

In einer Architektur AWS mit mehreren Konten eine zentralisierte VPC, die Inspektionen des Netzwerkverkehrs zwischen VPCs (in derselben oder unterschiedlichen AWS-Regionen), dem Internet und lokalen Netzwerken verwaltet. Die AWS -Referenzarchitektur für die Sicherheit empfiehlt, Ihr Netzwerkkonto mit eingehenden und ausgehenden VPCs und Inspektions-VPCs einzurichten, um die bidirektionale Schnittstelle zwischen Ihrer Anwendung und dem Internet zu schützen.

Internet of Things (IoT)

Das Netzwerk verbundener physischer Objekte mit eingebetteten Sensoren oder Prozessoren, das über das Internet oder über ein lokales Kommunikationsnetzwerk mit anderen Geräten und Systemen kommuniziert. Weitere Informationen finden Sie unter Was ist IoT?

Interpretierbarkeit

Ein Merkmal eines Modells für Machine Learning, das beschreibt, inwieweit ein Mensch verstehen kann, wie die Vorhersagen des Modells von seinen Eingaben abhängen. Weitere Informationen finden Sie unter Interpretierbarkeit von Modellen für Machine Learning mit AWS.

IoT

Siehe Internet der Dinge.

IT information library (ITIL, IT-Informationsbibliothek)

Eine Reihe von bewährten Methoden für die Bereitstellung von IT-Services und die Abstimmung dieser Services auf die Geschäftsanforderungen. ITIL bietet die Grundlage für ITSM.

T service management (ITSM, IT-Servicemanagement)

Aktivitäten im Zusammenhang mit der Gestaltung, Implementierung, Verwaltung und Unterstützung von IT-Services für eine Organisation. Informationen zur Integration von Cloud-Vorgängen mit ITSM-Tools finden Sie im Leitfaden zur Betriebsintegration.

BIS

Siehe IT-Informationsbibliothek.

ITSM

Siehe IT-Servicemanagement.

L

Labelbasierte Zugangskontrolle (LBAC)

Eine Implementierung der Mandatory Access Control (MAC), bei der den Benutzern und den Daten selbst jeweils explizit ein Sicherheitslabelwert zugewiesen wird. Die Schnittmenge zwischen der Benutzersicherheitsbeschriftung und der Datensicherheitsbeschriftung bestimmt, welche Zeilen und Spalten für den Benutzer sichtbar sind.

Landing Zone

Eine landing zone ist eine gut strukturierte AWS Umgebung mit mehreren Konten, die skalierbar und sicher ist. Dies ist ein Ausgangspunkt, von dem aus Ihre Organisationen Workloads und Anwendungen schnell und mit Vertrauen in ihre Sicherheits- und Infrastrukturumgebung starten und bereitstellen können. Weitere Informationen zu Landing Zones finden Sie unter Einrichtung einer sicheren und skalierbaren AWS -Umgebung mit mehreren Konten..

Große Migration

Eine Migration von 300 oder mehr Servern.

SCHWARZ

Siehe Labelbasierte Zugriffskontrolle.

Geringste Berechtigung

Die bewährte Sicherheitsmethode, bei der nur die für die Durchführung einer Aufgabe erforderlichen Mindestberechtigungen erteilt werden. Weitere Informationen finden Sie unter Geringste Berechtigungen anwenden in der IAM-Dokumentation.

Lift and Shift

Siehe 7 Rs.

Little-Endian-System

Ein System, welches das niedrigwertigste Byte zuerst speichert. Siehe auch Endianness.

Niedrigere Umgebungen

Siehe Umwelt.

M

Machine Learning (ML)

Eine Art künstlicher Intelligenz, die Algorithmen und Techniken zur Mustererkennung und zum Lernen verwendet. ML analysiert aufgezeichnete Daten, wie z. B. Daten aus dem Internet der Dinge (IoT), und lernt daraus, um ein statistisches Modell auf der Grundlage von Mustern zu erstellen. Weitere Informationen finden Sie unter Machine Learning.

Hauptzweig

Siehe Filiale.

Malware

Software, die entwickelt wurde, um die Computersicherheit oder den Datenschutz zu gefährden. Malware kann Computersysteme stören, vertrauliche Informationen durchsickern lassen oder sich unbefugten Zugriff verschaffen. Beispiele für Malware sind Viren, Würmer, Ransomware, Trojaner, Spyware und Keylogger.

verwaltete Dienste

AWS-Services für die die Infrastrukturebene, das Betriebssystem und die Plattformen AWS betrieben werden, und Sie greifen auf die Endgeräte zu, um Daten zu speichern und abzurufen. Amazon Simple Storage Service (Amazon S3) und Amazon DynamoDB sind Beispiele für Managed Services. Diese werden auch als abstrakte Dienste bezeichnet.

Manufacturing Execution System (MES)

Ein Softwaresystem zur Nachverfolgung, Überwachung, Dokumentation und Steuerung von Produktionsprozessen, bei denen Rohstoffe in der Fertigung zu fertigen Produkten umgewandelt werden.

MAP

Siehe Migration Acceleration Program.

Mechanismus

Ein vollständiger Prozess, bei dem Sie ein Tool erstellen, die Akzeptanz des Tools vorantreiben und anschließend die Ergebnisse überprüfen, um Anpassungen vorzunehmen. Ein Mechanismus ist ein Zyklus, der sich im Laufe seiner Tätigkeit selbst verstärkt und verbessert. Weitere Informationen finden Sie unter Aufbau von Mechanismen im AWS Well-Architected Framework.

Mitgliedskonto

Alle AWS-Konten außer dem Verwaltungskonto, die Teil einer Organisation in sind. AWS Organizations Ein Konto kann jeweils nur einer Organisation angehören.

DURCHEINANDER

Siehe Manufacturing Execution System.

Message Queuing-Telemetrietransport (MQTT)

Ein leichtes machine-to-machine (M2M) -Kommunikationsprotokoll, das auf dem Publish/Subscribe-Muster für IoT-Geräte mit beschränkten Ressourcen basiert.

Microservice

Ein kleiner, unabhängiger Service, der über klar definierte APIs kommuniziert und in der Regel kleinen, eigenständigen Teams gehört. Ein Versicherungssystem kann beispielsweise Microservices beinhalten, die Geschäftsfunktionen wie Vertrieb oder Marketing oder Subdomains wie Einkauf, Schadenersatz oder Analytik zugeordnet sind. Zu den Vorteilen von Microservices gehören Agilität, flexible Skalierung, einfache Bereitstellung, wiederverwendbarer Code und Ausfallsicherheit. Weitere Informationen finden Sie unter Integration von Microservices mithilfe serverloser Dienste. AWS

Microservices-Architekturen

Ein Ansatz zur Erstellung einer Anwendung mit unabhängigen Komponenten, die jeden Anwendungsprozess als Microservice ausführen. Diese Microservices kommunizieren über eine klar definierte Schnittstelle mithilfe einfacher APIs. Jeder Microservice in dieser Architektur kann aktualisiert, bereitgestellt und skaliert werden, um den Bedarf an bestimmten Funktionen einer Anwendung zu decken. Weitere Informationen finden Sie unter Implementieren von Microservices auf. AWS

Migration Acceleration Program (MAP)

Ein AWS Programm, das Beratung, Unterstützung, Schulungen und Services bietet, um Unternehmen dabei zu unterstützen, eine solide betriebliche Grundlage für die Umstellung auf die Cloud zu schaffen und die anfänglichen Kosten von Migrationen auszugleichen. MAP umfasst eine Migrationsmethode für die methodische Durchführung von Legacy-Migrationen sowie eine Reihe von Tools zur Automatisierung und Beschleunigung gängiger Migrationsszenarien.

Migration in großem Maßstab

Der Prozess, bei dem der Großteil des Anwendungsportfolios in Wellen in die Cloud verlagert wird, wobei in jeder Welle mehr Anwendungen schneller migriert werden. In dieser Phase werden die bewährten Verfahren und Erkenntnisse aus den früheren Phasen zur Implementierung einer Migrationsfabrik von Teams, Tools und Prozessen zur Optimierung der Migration von Workloads durch Automatisierung und agile Bereitstellung verwendet. Dies ist die dritte Phase der AWS - Migrationsstrategie.

Migrationsfabrik

Funktionsübergreifende Teams, die die Migration von Workloads durch automatisierte, agile Ansätze optimieren. Zu den Teams in der Migrationsabteilung gehören in der Regel Betriebsabläufe, Geschäftsanalysten und Eigentümer, Migrationsingenieure, Entwickler und DevOps Experten, die in Sprints arbeiten. Zwischen 20 und 50 Prozent eines Unternehmensanwendungsportfolios bestehen aus sich wiederholenden Mustern, die durch einen Fabrik-Ansatz optimiert werden können. Weitere Informationen finden Sie in Diskussion über Migrationsfabriken und den Leitfaden zur Cloud-Migration-Fabrik in diesem Inhaltssatz.

Migrationsmetadaten

Die Informationen über die Anwendung und den Server, die für den Abschluss der Migration benötigt werden. Für jedes Migrationsmuster ist ein anderer Satz von Migrationsmetadaten erforderlich. Beispiele für Migrationsmetadaten sind das Zielsubnetz, die Sicherheitsgruppe und AWS das Konto.

Migrationsmuster

Eine wiederholbare Migrationsaufgabe, in der die Migrationsstrategie, das Migrationsziel und die verwendete Migrationsanwendung oder der verwendete Migrationsservice detailliert beschrieben werden. Beispiel: Rehost-Migration zu Amazon EC2 mit AWS Application Migration Service.

Migration Portfolio Assessment (MPA)

Ein Online-Tool, das Informationen zur Validierung des Geschäftsszenarios für die Migration in die Cloud bereitstellt. AWS MPA bietet eine detaillierte Portfoliobewertung (richtige Servergröße, Preisgestaltung, Gesamtbetriebskostenanalyse, Migrationskostenanalyse) sowie Migrationsplanung (Anwendungsdatenanalyse und Datenerfassung, Anwendungsgruppierung, Migrationspriorisierung und Wellenplanung). Das MPA-Tool (Anmeldung erforderlich) steht allen AWS Beratern und APN-Partnerberatern kostenlos zur Verfügung.

Migration Readiness Assessment (MRA)

Der Prozess, bei dem mithilfe des AWS CAF Erkenntnisse über den Cloud-Bereitschaftsstatus eines Unternehmens gewonnen, Stärken und Schwächen identifiziert und ein Aktionsplan zur Schließung festgestellter Lücken erstellt wird. Weitere Informationen finden Sie im Benutzerhandbuch für Migration Readiness. MRA ist die erste Phase der AWS - Migrationsstrategie.

Migrationsstrategie

Der Ansatz, der verwendet wird, um einen Workload in die AWS Cloud zu migrieren. Weitere Informationen finden Sie im Eintrag 7 Rs in diesem Glossar und unter Mobilisieren Sie Ihr Unternehmen, um groß angelegte Migrationen zu beschleunigen.

ML

Siehe maschinelles Lernen.

Modernisierung

Umwandlung einer veralteten (veralteten oder monolithischen) Anwendung und ihrer Infrastruktur in ein agiles, elastisches und hochverfügbares System in der Cloud, um Kosten zu senken, die Effizienz zu steigern und Innovationen zu nutzen. Weitere Informationen finden Sie unter Strategie zur Modernisierung von Anwendungen in der AWS Cloud.

Bewertung der Modernisierungsfähigkeit

Eine Bewertung, anhand derer festgestellt werden kann, ob die Anwendungen einer Organisation für die Modernisierung bereit sind, Vorteile, Risiken und Abhängigkeiten identifiziert und ermittelt wird, wie gut die Organisation den zukünftigen Status dieser Anwendungen unterstützen kann. Das Ergebnis der Bewertung ist eine Vorlage der Zielarchitektur, eine Roadmap, in der die Entwicklungsphasen und Meilensteine des Modernisierungsprozesses detailliert beschrieben werden, sowie ein Aktionsplan zur Behebung festgestellter Lücken. Weitere Informationen finden Sie unter Bewertung der Modernisierungsbereitschaft von Anwendungen in der AWS -Cloud.

Monolithische Anwendungen (Monolithen)

Anwendungen, die als ein einziger Service mit eng gekoppelten Prozessen ausgeführt werden. Monolithische Anwendungen haben verschiedene Nachteile. Wenn ein Anwendungs-Feature stark nachgefragt wird, muss die gesamte Architektur skaliert werden. Das Hinzufügen oder Verbessern der Feature einer monolithischen Anwendung wird ebenfalls komplexer, wenn die Codebasis wächst. Um diese Probleme zu beheben, können Sie eine Microservices-Architektur verwenden. Weitere Informationen finden Sie unter Zerlegen von Monolithen in Microservices.

MPA

Siehe Bewertung des Migrationsportfolios.

MQTT

Siehe Message Queuing-Telemetrietransport.

Mehrklassen-Klassifizierung

Ein Prozess, der dabei hilft, Vorhersagen für mehrere Klassen zu generieren (wobei eines von mehr als zwei Ergebnissen vorhergesagt wird). Ein ML-Modell könnte beispielsweise fragen: „Ist dieses Produkt ein Buch, ein Auto oder ein Telefon?“ oder „Welche Kategorie von Produkten ist für diesen Kunden am interessantesten?“

veränderbare Infrastruktur

Ein Modell, das die bestehende Infrastruktur für Produktionsworkloads aktualisiert und modifiziert. Für eine verbesserte Konsistenz, Zuverlässigkeit und Vorhersagbarkeit empfiehlt das AWS Well-Architected Framework die Verwendung einer unveränderlichen Infrastruktur als bewährte Methode.

O

OAC

Siehe Origin Access Control.

EICHE

Siehe Zugriffsidentität von Origin.

COM

Siehe organisatorisches Change-Management.

Offline-Migration

Eine Migrationsmethode, bei der der Quell-Workload während des Migrationsprozesses heruntergefahren wird. Diese Methode ist mit längeren Ausfallzeiten verbunden und wird in der Regel für kleine, unkritische Workloads verwendet.

OI

Siehe Betriebsintegration.

OLA

Siehe Vereinbarung auf operativer Ebene.

Online-Migration

Eine Migrationsmethode, bei der der Quell-Workload auf das Zielsystem kopiert wird, ohne offline genommen zu werden. Anwendungen, die mit dem Workload verbunden sind, können während der Migration weiterhin funktionieren. Diese Methode beinhaltet keine bis minimale Ausfallzeit und wird in der Regel für kritische Produktionsworkloads verwendet.

OPC-UA

Siehe Open Process Communications — Unified Architecture.

Offene Prozesskommunikation — Einheitliche Architektur (OPC-UA)

Ein machine-to-machine (M2M) -Kommunikationsprotokoll für die industrielle Automatisierung. OPC-UA bietet einen Interoperabilitätsstandard mit Datenverschlüsselungs-, Authentifizierungs- und Autorisierungsschemata.

Vereinbarung auf Betriebsebene (OLA)

Eine Vereinbarung, in der klargestellt wird, welche funktionalen IT-Gruppen sich gegenseitig versprechen zu liefern, um ein Service Level Agreement (SLA) zu unterstützen.

Überprüfung der Betriebsbereitschaft (ORR)

Eine Checkliste mit Fragen und zugehörigen bewährten Methoden, die Ihnen helfen, Vorfälle und mögliche Ausfälle zu verstehen, zu bewerten, zu verhindern oder deren Umfang zu reduzieren. Weitere Informationen finden Sie unter Operational Readiness Reviews (ORR) im AWS Well-Architected Framework.

Betriebstechnologie (OT)

Hardware- und Softwaresysteme, die mit der physischen Umgebung zusammenarbeiten, um industrielle Abläufe, Ausrüstung und Infrastruktur zu steuern. In der Fertigung ist die Integration von OT- und Informationstechnologie (IT) -Systemen ein zentraler Schwerpunkt der Industrie 4.0-Transformationen.

Betriebsintegration (OI)

Der Prozess der Modernisierung von Abläufen in der Cloud, der Bereitschaftsplanung, Automatisierung und Integration umfasst. Weitere Informationen finden Sie im Leitfaden zur Betriebsintegration.

Organisationspfad

Ein Pfad, der von erstellt wird und in AWS CloudTrail dem alle Ereignisse für alle AWS-Konten in einer Organisation protokolliert werden. AWS Organizations Diese Spur wird in jedem AWS-Konto , der Teil der Organisation ist, erstellt und verfolgt die Aktivität in jedem Konto. Weitere Informationen finden Sie in der CloudTrail Dokumentation unter Einen Trail für eine Organisation erstellen.

Organisatorisches Veränderungsmanagement (OCM)

Ein Framework für das Management wichtiger, disruptiver Geschäftstransformationen aus Sicht der Mitarbeiter, der Kultur und der Führung. OCM hilft Organisationen dabei, sich auf neue Systeme und Strategien vorzubereiten und auf diese umzustellen, indem es die Akzeptanz von Veränderungen beschleunigt, Übergangsprobleme angeht und kulturelle und organisatorische Veränderungen vorantreibt. In der AWS Migrationsstrategie wird dieses Framework aufgrund der Geschwindigkeit des Wandels, der bei Projekten zur Cloud-Einführung erforderlich ist, als Mitarbeiterbeschleunigung bezeichnet. Weitere Informationen finden Sie im OCM-Handbuch.

Ursprungszugriffskontrolle (OAC)

In CloudFront, eine erweiterte Option zur Zugriffsbeschränkung, um Ihre Amazon Simple Storage Service (Amazon S3) -Inhalte zu sichern. OAC unterstützt alle S3-Buckets insgesamt AWS-Regionen, serverseitige Verschlüsselung mit AWS KMS (SSE-KMS) sowie dynamische `PUT` und `DELETE` Anfragen an den S3-Bucket.

Ursprungszugriffsidentität (OAI)

In CloudFront, eine Option zur Zugriffsbeschränkung, um Ihre Amazon S3 S3-Inhalte zu sichern. Wenn Sie OAI verwenden, CloudFront erstellt es einen Principal, mit dem sich Amazon S3 authentifizieren kann. Authentifizierte Principals können nur über eine bestimmte Distribution auf Inhalte in einem S3-Bucket zugreifen. CloudFront Siehe auch OAC, das eine detailliertere und verbesserte Zugriffskontrolle bietet.

ODER

Siehe Überprüfung der Betriebsbereitschaft.

NICHT

Siehe Betriebstechnologie.

Ausgehende (egress) VPC

In einer Architektur AWS mit mehreren Konten eine VPC, die Netzwerkverbindungen verarbeitet, die von einer Anwendung aus initiiert werden. Die AWS -Referenzarchitektur für die Sicherheit empfiehlt, Ihr Netzwerkkonto mit eingehenden und ausgehenden VPCs und Inspektions-VPCs einzurichten, um die bidirektionale Schnittstelle zwischen Ihrer Anwendung und dem Internet zu schützen.

P

Berechtigungsgrenze

Eine IAM-Verwaltungsrichtlinie, die den IAM-Prinzipalen zugeordnet ist, um die maximalen Berechtigungen festzulegen, die der Benutzer oder die Rolle haben kann. Weitere Informationen finden Sie unter Berechtigungsgrenzen für IAM-Entitys in der IAM-Dokumentation.

persönlich identifizierbare Informationen (PII)

Informationen, die, wenn sie direkt betrachtet oder mit anderen verwandten Daten kombiniert werden, verwendet werden können, um vernünftige Rückschlüsse auf die Identität einer Person zu ziehen. Beispiele für personenbezogene Daten sind Namen, Adressen und Kontaktinformationen.

Personenbezogene Daten

Siehe persönlich identifizierbare Informationen.

Playbook

Eine Reihe vordefinierter Schritte, die die mit Migrationen verbundenen Aufgaben erfassen, z. B. die Bereitstellung zentraler Betriebsfunktionen in der Cloud. Ein Playbook kann die Form von Skripten, automatisierten Runbooks oder einer Zusammenfassung der Prozesse oder Schritte annehmen, die für den Betrieb Ihrer modernisierten Umgebung erforderlich sind.

PLC

Siehe programmierbare Logiksteuerung.

PLM

Siehe Produktlebenszyklusmanagement.

policy

Ein Objekt, das Berechtigungen definieren (siehe identitätsbasierte Richtlinie), Zugriffsbedingungen spezifizieren (siehe ressourcenbasierte Richtlinie) oder die maximalen Berechtigungen für alle Konten in einer Organisation definieren kann AWS Organizations (siehe Dienststeuerungsrichtlinie).

Polyglotte Beharrlichkeit

Unabhängige Auswahl der Datenspeichertechnologie eines Microservices auf der Grundlage von Datenzugriffsmustern und anderen Anforderungen. Wenn Ihre Microservices über dieselbe Datenspeichertechnologie verfügen, kann dies zu Implementierungsproblemen oder zu Leistungseinbußen führen. Microservices lassen sich leichter implementieren und erzielen eine bessere Leistung und Skalierbarkeit, wenn sie den Datenspeicher verwenden, der ihren Anforderungen am besten entspricht. Weitere Informationen finden Sie unter Datenpersistenz in Microservices aktivieren.

Portfoliobewertung

Ein Prozess, bei dem das Anwendungsportfolio ermittelt, analysiert und priorisiert wird, um die Migration zu planen. Weitere Informationen finden Sie in Bewerten der Migrationsbereitschaft.

predicate

Eine Abfragebedingung, die `true` oder zurückgibt`false`, was üblicherweise in einer Klausel vorkommt. `WHERE`

Prädikat Pushdown

Eine Technik zur Optimierung von Datenbankabfragen, bei der die Daten in der Abfrage vor der Übertragung gefiltert werden. Dadurch wird die Datenmenge reduziert, die aus der relationalen Datenbank abgerufen und verarbeitet werden muss, und die Abfrageleistung wird verbessert.

Präventive Kontrolle

Eine Sicherheitskontrolle, die verhindern soll, dass ein Ereignis eintritt. Diese Kontrollen stellen eine erste Verteidigungslinie dar, um unbefugten Zugriff oder unerwünschte Änderungen an Ihrem Netzwerk zu verhindern. Weitere Informationen finden Sie unter Präventive Kontrolle in Implementierung von Sicherheitskontrollen in AWS.

Prinzipal

Eine Entität AWS , die Aktionen ausführen und auf Ressourcen zugreifen kann. Bei dieser Entität handelt es sich in der Regel um einen Root-Benutzer für eine AWS-Konto, eine IAM-Rolle oder

einen Benutzer. Weitere Informationen finden Sie unter Prinzipal in Rollenbegriffe und -konzepte in der IAM-Dokumentation.

Datenschutz durch Design

Ein Ansatz in der Systemtechnik, der den Datenschutz während des gesamten Engineering-Prozesses berücksichtigt.

Privat gehostete Zonen

Ein Container, der Informationen darüber enthält, wie Amazon Route 53 auf DNS-Abfragen für eine Domain und ihre Subdomains innerhalb einer oder mehrerer VPCs reagieren soll. Weitere Informationen finden Sie unter Arbeiten mit privat gehosteten Zonen in der Route-53-Dokumentation.

proaktive Steuerung

Eine Sicherheitskontrolle, die den Einsatz nicht richtlinienkonformer Ressourcen verhindern soll. Diese Steuerelemente scannen Ressourcen, bevor sie bereitgestellt werden. Wenn die Ressource nicht mit der Steuerung konform ist, wird sie nicht bereitgestellt. Weitere Informationen finden Sie im Referenzhandbuch zu Kontrollen in der AWS Control Tower Dokumentation und unter Proaktive Kontrollen unter Implementierung von Sicherheitskontrollen am AWS.

Produktlebenszyklusmanagement (PLM)

Das Management von Daten und Prozessen für ein Produkt während seines gesamten Lebenszyklus, vom Design, der Entwicklung und Markteinführung über Wachstum und Reife bis hin zur Markteinführung und Markteinführung.

Produktionsumgebung

Siehe Umgebung.

Speicherprogrammierbare Steuerung (SPS)

In der Fertigung ein äußerst zuverlässiger, anpassungsfähiger Computer, der Maschinen überwacht und Fertigungsprozesse automatisiert.

Pseudonymisierung

Der Prozess, bei dem persönliche Identifikatoren in einem Datensatz durch Platzhalterwerte ersetzt werden. Pseudonymisierung kann zum Schutz der Privatsphäre beitragen. Pseudonymisierte Daten gelten weiterhin als personenbezogene Daten.

veröffentlichen/abonnieren (pub/sub)

Ein Muster, das asynchrone Kommunikation zwischen Microservices ermöglicht, um die Skalierbarkeit und Reaktionsfähigkeit zu verbessern. In einem auf Microservices basierenden MES kann ein Microservice beispielsweise Ereignismeldungen in einem Kanal veröffentlichen, den andere Microservices abonnieren können. Das System kann neue Microservices hinzufügen, ohne den Veröffentlichungsservice zu ändern.

Q

Abfrageplan

Eine Reihe von Schritten, wie Anweisungen, die für den Zugriff auf die Daten in einem relationalen SQL-Datenbanksystem verwendet werden.

Abfrageplanregression

Wenn ein Datenbankserviceoptimierer einen weniger optimalen Plan wählt als vor einer bestimmten Änderung der Datenbankumgebung. Dies kann durch Änderungen an Statistiken, Beschränkungen, Umgebungseinstellungen, Abfrageparameter-Bindungen und Aktualisierungen der Datenbank-Engine verursacht werden.

R

RACI-Matrix

Siehe verantwortlich, rechenschaftspflichtig, konsultiert, informiert (RACI).

Ransomware

Eine bösartige Software, die entwickelt wurde, um den Zugriff auf ein Computersystem oder Daten zu blockieren, bis eine Zahlung erfolgt ist.

RASCI-Matrix

Siehe verantwortlich, rechenschaftspflichtig, konsultiert, informiert (RACI).

RCAC

Siehe Zugriffskontrolle für Zeilen und Spalten.

Read Replica

Eine Kopie einer Datenbank, die nur für Lesezwecke verwendet wird. Sie können Abfragen an das Lesereplikat weiterleiten, um die Belastung auf Ihrer Primärdatenbank zu reduzieren.

neu strukturieren

Siehe 7 Rs.

Recovery Point Objective (RPO)

Die maximal zulässige Zeitspanne seit dem letzten Datenwiederherstellungspunkt. Dies bestimmt, was als akzeptabler Datenverlust zwischen dem letzten Wiederherstellungspunkt und der Betriebsunterbrechung angesehen wird.

Ziel der Wiederherstellungszeit (RTO)

Die maximal zulässige Verzögerung zwischen der Betriebsunterbrechung und der Wiederherstellung des Dienstes.

Refaktorierung

Siehe 7 Rs.

Region

Eine Sammlung von AWS Ressourcen in einem geografischen Gebiet. Jeder AWS-Region ist isoliert und unabhängig von den anderen, um Fehlertoleranz, Stabilität und Belastbarkeit zu gewährleisten. Weitere Informationen finden Sie unter Geben Sie an, was AWS-Regionen Ihr Konto verwenden kann.

Regression

Eine ML-Technik, die einen numerischen Wert vorhersagt. Zum Beispiel, um das Problem „Zu welchem Preis wird dieses Haus verkauft werden?“ zu lösen Ein ML-Modell könnte ein lineares Regressionsmodell verwenden, um den Verkaufspreis eines Hauses auf der Grundlage bekannter Fakten über das Haus (z. B. die Quadratmeterzahl) vorherzusagen.

rehosten

Siehe 7 Rs.

Veröffentlichung

In einem Bereitstellungsprozess der Akt der Förderung von Änderungen an einer Produktionsumgebung.

umziehen

Siehe 7 Rs.

neue Plattform

Siehe 7 Rs.

Rückkauf

Siehe 7 Rs.

Ausfallsicherheit

Die Fähigkeit einer Anwendung, Störungen zu widerstehen oder sich von ihnen zu erholen. Hochverfügbarkeit und Notfallwiederherstellung sind häufig Überlegungen bei der Planung der Ausfallsicherheit in der. AWS Cloud Weitere Informationen finden Sie unter AWS Cloud Resilienz.

Ressourcenbasierte Richtlinie

Eine mit einer Ressource verknüpfte Richtlinie, z. B. ein Amazon-S3-Bucket, ein Endpunkt oder ein Verschlüsselungsschlüssel. Diese Art von Richtlinie legt fest, welchen Prinzipalen der Zugriff gewährt wird, welche Aktionen unterstützt werden und welche anderen Bedingungen erfüllt sein müssen.

RACI-Matrix (verantwortlich, rechenschaftspflichtig, konsultiert, informiert)

Eine Matrix, die die Rollen und Verantwortlichkeiten für alle Parteien definiert, die an Migrationsaktivitäten und Cloud-Vorgängen beteiligt sind. Der Matrixname leitet sich von den in der Matrix definierten Zuständigkeitstypen ab: verantwortlich (R), rechenschaftspflichtig (A), konsultiert (C) und informiert (I). Der Unterstützungstyp (S) ist optional. Wenn Sie Unterstützung einbeziehen, wird die Matrix als RASCI-Matrix bezeichnet, und wenn Sie sie ausschließen, wird sie als RACI-Matrix bezeichnet.

Reaktive Kontrolle

Eine Sicherheitskontrolle, die darauf ausgelegt ist, die Behebung unerwünschter Ereignisse oder Abweichungen von Ihren Sicherheitsstandards voranzutreiben. Weitere Informationen finden Sie unter Reaktive Kontrolle in Implementieren von Sicherheitskontrollen in AWS.

Beibehaltung

Siehe 7 Rs.

zurückziehen

Siehe 7 Rs.

Drehung

Der Vorgang, bei dem ein Geheimnis regelmäßig aktualisiert wird, um es einem Angreifer zu erschweren, auf die Anmeldeinformationen zuzugreifen.

Zugriffskontrolle für Zeilen und Spalten (RCAC)

Die Verwendung einfacher, flexibler SQL-Ausdrücke mit definierten Zugriffsregeln. RCAC besteht aus Zeilenberechtigungen und Spaltenmasken.

RPO

Siehe Recovery Point Objective.

RTO

Siehe Ziel der Wiederherstellungszeit.

Runbook

Eine Reihe manueller oder automatisierter Verfahren, die zur Ausführung einer bestimmten Aufgabe erforderlich sind. Diese sind in der Regel darauf ausgelegt, sich wiederholende Operationen oder Verfahren mit hohen Fehlerquoten zu rationalisieren.

S

SAML 2.0

Ein offener Standard, den viele Identitätsanbieter (IdPs) verwenden. Diese Funktion ermöglicht föderiertes Single Sign-On (SSO), sodass sich Benutzer bei den API-Vorgängen anmelden AWS Management Console oder die AWS API-Operationen aufrufen können, ohne dass Sie einen Benutzer in IAM für alle in Ihrer Organisation erstellen müssen. Weitere Informationen zum SAML-2.0.-basierten Verbund finden Sie unter Über den SAML-2.0-basierten Verbund in der IAM-Dokumentation.

SCADA

Siehe Aufsichtskontrolle und Datenerfassung.

SCP

Siehe Richtlinie zur Dienstkontrolle.

Secret

Interne AWS Secrets Manager, vertrauliche oder eingeschränkte Informationen, wie z. B. ein Passwort oder Benutzeranmeldedaten, die Sie in verschlüsselter Form speichern. Es besteht aus dem geheimen Wert und seinen Metadaten. Der geheime Wert kann binär, eine einzelne Zeichenfolge oder mehrere Zeichenketten sein. Weitere Informationen finden Sie unter Secret in der Secrets Manager-Dokumentation.

Sicherheitskontrolle

Ein technischer oder administrativer Integritätsschutz, der die Fähigkeit eines Bedrohungsakteurs, eine Schwachstelle auszunutzen, verhindert, erkennt oder einschränkt. Es gibt vier Haupttypen von Sicherheitskontrollen: präventiv, detektiv, reaktionsschnell und proaktiv.

Härtung der Sicherheit

Der Prozess, bei dem die Angriffsfläche reduziert wird, um sie widerstandsfähiger gegen Angriffe zu machen. Dies kann Aktionen wie das Entfernen von Ressourcen, die nicht mehr benötigt werden, die Implementierung der bewährten Sicherheitsmethode der Gewährung geringster Berechtigungen oder die Deaktivierung unnötiger Feature in Konfigurationsdateien umfassen.

System zur Verwaltung von Sicherheitsinformationen und Ereignissen (security information and event management – SIEM)

Tools und Services, die Systeme für das Sicherheitsinformationsmanagement (SIM) und das Management von Sicherheitsereignissen (SEM) kombinieren. Ein SIEM-System sammelt, überwacht und analysiert Daten von Servern, Netzwerken, Geräten und anderen Quellen, um Bedrohungen und Sicherheitsverletzungen zu erkennen und Warnmeldungen zu generieren.

Automatisierung von Sicherheitsreaktionen

Eine vordefinierte und programmierte Aktion, die darauf ausgelegt ist, automatisch auf ein Sicherheitsereignis zu reagieren oder es zu beheben. Diese Automatisierungen dienen als detektive oder reaktionsschnelle Sicherheitskontrollen, die Sie bei der Implementierung bewährter AWS Sicherheitsmethoden unterstützen. Beispiele für automatisierte Antwortaktionen sind das Ändern einer VPC-Sicherheitsgruppe, das Patchen einer Amazon EC2 EC2-Instance oder das Rotieren von Anmeldeinformationen.

Serverseitige Verschlüsselung

Verschlüsselung von Daten am Zielort durch denjenigen AWS-Service , der sie empfängt.

Service-Kontrollrichtlinie (SCP)

Eine Richtlinie, die eine zentrale Kontrolle über die Berechtigungen für alle Konten in einer Organisation in AWS Organizations ermöglicht. SCPs definieren Integritätsschutz oder legen Grenzwerte für Aktionen fest, die ein Administrator an Benutzer oder Rollen delegieren kann. Sie können SCPs als Zulassungs- oder Ablehnungslisten verwenden, um festzulegen, welche Services oder Aktionen zulässig oder verboten sind. Weitere Informationen finden Sie in der AWS Organizations Dokumentation unter Richtlinien zur Dienststeuerung.

Service-Endpunkt

Die URL des Einstiegspunkts für einen AWS-Service. Sie können den Endpunkt verwenden, um programmgesteuert eine Verbindung zum Zielservice herzustellen. Weitere Informationen finden Sie unter AWS-Service -Endpunkte in der Allgemeine AWS-Referenz.

Service Level Agreement (SLA)

Eine Vereinbarung, in der klargestellt wird, was ein IT-Team seinen Kunden zu bieten verspricht, z. B. in Bezug auf Verfügbarkeit und Leistung der Services.

Service-Level-Indikator (SLI)

Eine Messung eines Leistungsaspekts eines Dienstes, z. B. seiner Fehlerrate, Verfügbarkeit oder Durchsatz.

Service-Level-Ziel (SLO)

Eine Zielkennzahl, die den Zustand eines Dienstes darstellt, gemessen anhand eines Service-Level-Indikators.

Modell der geteilten Verantwortung

Ein Modell, das die Verantwortung beschreibt, mit der Sie gemeinsam AWS für Cloud-Sicherheit und Compliance verantwortlich sind. AWS ist für die Sicherheit der Cloud verantwortlich, wohingegen Sie für die Sicherheit in der Cloud verantwortlich sind. Weitere Informationen finden Sie unter Modell der geteilten Verantwortung.

SIEM

Siehe Sicherheitsinformations- und Event-Management-System.

Single Point of Failure (SPOF)

Ein Fehler in einer einzelnen, kritischen Komponente einer Anwendung, der das System stören kann.

SLA

Siehe Service Level Agreement.

SLI

Siehe Service-Level-Indikator.

ALSO

Siehe Service-Level-Ziel.

split-and-seed Modell

Ein Muster für die Skalierung und Beschleunigung von Modernisierungsprojekten. Sobald neue Features und Produktversionen definiert werden, teilt sich das Kernteam auf, um neue Produktteams zu bilden. Dies trägt zur Skalierung der Fähigkeiten und Services Ihrer Organisation bei, verbessert die Produktivität der Entwickler und unterstützt schnelle Innovationen. Weitere Informationen finden Sie unter Schrittweiser Ansatz zur Modernisierung von Anwendungen in der AWS Cloud.

SPOTTEN

Siehe Single Point of Failure.

Sternschema

Eine Datenbank-Organisationsstruktur, die eine große Faktentabelle zum Speichern von Transaktions- oder Messdaten und eine oder mehrere kleinere dimensionale Tabellen zum Speichern von Datenattributen verwendet. Diese Struktur ist für die Verwendung in einem Data Warehouse oder für Business Intelligence-Zwecke konzipiert.

Strangler-Fig-Muster

Ein Ansatz zur Modernisierung monolithischer Systeme, bei dem die Systemfunktionen schrittweise umgeschrieben und ersetzt werden, bis das Legacy-System außer Betrieb genommen werden kann. Dieses Muster verwendet die Analogie einer Feigenrebe, die zu einem etablierten Baum heranwächst und schließlich ihren Wirt überwindet und ersetzt. Das Muster wurde eingeführt von Martin Fowler als Möglichkeit, Risiken beim Umschreiben monolithischer Systeme zu managen. Ein Beispiel für die Anwendung dieses Musters finden Sie unter Schrittweises Modernisieren älterer Microsoft ASP.NET (ASMX)-Webservices mithilfe von Containern und Amazon API Gateway.

Subnetz

Ein Bereich von IP-Adressen in Ihrer VPC. Ein Subnetz muss sich in einer einzigen Availability Zone befinden.

Aufsichtskontrolle und Datenerfassung (SCADA)

In der Fertigung ein System, das Hardware und Software zur Überwachung von Sachanlagen und Produktionsabläufen verwendet.

Symmetrische Verschlüsselung

Ein Verschlüsselungsalgorithmus, der denselben Schlüssel zum Verschlüsseln und Entschlüsseln der Daten verwendet.

synthetisches Testen

Testen eines Systems auf eine Weise, die Benutzerinteraktionen simuliert, um potenzielle Probleme zu erkennen oder die Leistung zu überwachen. Sie können Amazon CloudWatch Synthetics verwenden, um diese Tests zu erstellen.

T

tags

Schlüssel-Wert-Paare, die als Metadaten für die Organisation Ihrer Ressourcen dienen. AWS Mit Tags können Sie Ressourcen verwalten, identifizieren, organisieren, suchen und filtern. Weitere Informationen finden Sie unter Markieren Ihrer AWS -Ressourcen.

Zielvariable

Der Wert, den Sie in überwachtem ML vorhersagen möchten. Dies wird auch als Ergebnisvariable bezeichnet. In einer Fertigungsumgebung könnte die Zielvariable beispielsweise ein Produktfehler sein.

Aufgabenliste

Ein Tool, das verwendet wird, um den Fortschritt anhand eines Runbooks zu verfolgen. Eine Aufgabenliste enthält eine Übersicht über das Runbook und eine Liste mit allgemeinen Aufgaben, die erledigt werden müssen. Für jede allgemeine Aufgabe werden der geschätzte Zeitaufwand, der Eigentümer und der Fortschritt angegeben.

Testumgebungen

Siehe Umgebung.

Training

Daten für Ihr ML-Modell bereitstellen, aus denen es lernen kann. Die Trainingsdaten müssen die richtige Antwort enthalten. Der Lernalgorithmus findet Muster in den Trainingsdaten, die die Attribute der Input-Daten dem Ziel (die Antwort, die Sie voraussagen möchten) zuordnen. Es gibt ein ML-Modell aus, das diese Muster erfasst. Sie können dann das ML-Modell verwenden, um Voraussagen für neue Daten zu erhalten, bei denen Sie das Ziel nicht kennen.

Transit-Gateway

Ein Transit-Gateway ist ein Netzwerk-Transit-Hub, mit dem Sie Ihre VPCs und On-Premises-Netzwerke miteinander verbinden können. Weitere Informationen finden Sie in der AWS Transit Gateway Dokumentation unter Was ist ein Transit-Gateway.

Stammbasierter Workflow

Ein Ansatz, bei dem Entwickler Feature lokal in einem Feature-Zweig erstellen und testen und diese Änderungen dann im Hauptzweig zusammenführen. Der Hauptzweig wird dann sequentiell für die Entwicklungs-, Vorproduktions- und Produktionsumgebungen erstellt.

Vertrauenswürdiger Zugriff

Gewährung von Berechtigungen für einen Dienst, den Sie angeben, um Aufgaben in Ihrer Organisation AWS Organizations und in deren Konten in Ihrem Namen auszuführen. Der vertrauenswürdige Service erstellt in jedem Konto eine mit dem Service verknüpfte Rolle, wenn diese Rolle benötigt wird, um Verwaltungsaufgaben für Sie auszuführen. Weitere Informationen finden Sie in der AWS Organizations Dokumentation unter Verwendung AWS Organizations mit anderen AWS Diensten.

Optimieren

Aspekte Ihres Trainingsprozesses ändern, um die Genauigkeit des ML-Modells zu verbessern. Sie können das ML-Modell z. B. trainieren, indem Sie einen Beschriftungssatz generieren, Beschriftungen hinzufügen und diese Schritte dann mehrmals unter verschiedenen Einstellungen wiederholen, um das Modell zu optimieren.

Zwei-Pizzen-Team

Ein kleines DevOps Team, das Sie mit zwei Pizzen ernähren können. Eine Teamgröße von zwei Pizzen gewährleistet die bestmögliche Gelegenheit zur Zusammenarbeit bei der Softwareentwicklung.

U

Unsicherheit

Ein Konzept, das sich auf ungenaue, unvollständige oder unbekannte Informationen bezieht, die die Zuverlässigkeit von prädiktiven ML-Modellen untergraben können. Es gibt zwei Arten von Unsicherheit: Epistemische Unsicherheit wird durch begrenzte, unvollständige Daten verursacht, wohingegen aleatorische Unsicherheit durch Rauschen und Randomisierung verursacht wird, die in den Daten liegt. Weitere Informationen finden Sie im Leitfaden Quantifizieren der Unsicherheit in Deep-Learning-Systemen.

undifferenzierte Aufgaben

Diese Arbeit wird auch als Schwerstarbeit bezeichnet. Dabei handelt es sich um Arbeiten, die zwar für die Erstellung und den Betrieb einer Anwendung erforderlich sind, aber dem Endbenutzer keinen direkten Mehrwert bieten oder keinen Wettbewerbsvorteil bieten. Beispiele für undifferenzierte Aufgaben sind Beschaffung, Wartung und Kapazitätsplanung.

höhere Umgebungen

Siehe Umgebung.

V

Vacuuming

Ein Vorgang zur Datenbankwartung, bei dem die Datenbank nach inkrementellen Aktualisierungen bereinigt wird, um Speicherplatz zurückzugewinnen und die Leistung zu verbessern.

Versionskontrolle

Prozesse und Tools zur Nachverfolgung von Änderungen, z. B. Änderungen am Quellcode in einem Repository.

VPC-Peering

Eine Verbindung zwischen zwei VPCs, mit der Sie den Datenverkehr mithilfe von privaten IP-Adressen weiterleiten können. Weitere Informationen finden Sie unter Was ist VPC-Peering? in der Amazon-VPC-Dokumentation.

Schwachstelle

Ein Software- oder Hardwarefehler, der die Sicherheit des Systems gefährdet.

W

Warmer Cache

Ein Puffer-Cache, der aktuelle, relevante Daten enthält, auf die häufig zugegriffen wird. Die Datenbank-Instance kann aus dem Puffer-Cache lesen, was schneller ist als das Lesen aus dem Hauptspeicher oder von der Festplatte.

warme Daten

Daten, auf die selten zugegriffen wird. Bei der Abfrage dieser Art von Daten sind mäßig langsame Abfragen in der Regel akzeptabel.

Fensterfunktion

Eine SQL-Funktion, die eine Berechnung für eine Gruppe von Zeilen durchführt, die sich in irgendeiner Weise auf den aktuellen Datensatz beziehen. Fensterfunktionen sind nützlich für die Verarbeitung von Aufgaben wie die Berechnung eines gleitenden Durchschnitts oder für den Zugriff auf den Wert von Zeilen auf der Grundlage der relativen Position der aktuellen Zeile.

Workload

Ein Workload ist eine Sammlung von Ressourcen und Code, die einen Unternehmenswert bietet, wie z. B. eine kundenorientierte Anwendung oder ein Backend-Prozess.

Workstream

Funktionsgruppen in einem Migrationsprojekt, die für eine bestimmte Reihe von Aufgaben verantwortlich sind. Jeder Workstream ist unabhängig, unterstützt aber die anderen Workstreams im Projekt. Der Portfolio-Workstream ist beispielsweise für die Priorisierung von Anwendungen, die Wellenplanung und die Erfassung von Migrationsmetadaten verantwortlich. Der Portfolio-Workstream liefert diese Komponenten an den Migrations-Workstream, der dann die Server und Anwendungen migriert.

WURM

Mal schreiben, viele lesen.

WQF

Weitere Informationen finden Sie unter AWS Workload Qualification Framework.

einmal schreiben, viele lesen (WORM)

Ein Speichermodell, das Daten ein einziges Mal schreibt und verhindert, dass die Daten gelöscht oder geändert werden. Autorisierte Benutzer können die Daten so oft wie nötig lesen, aber sie können sie nicht ändern. Diese Datenspeicherinfrastruktur wird als unveränderlich angesehen.

Z

Zero-Day-Exploit

Ein Angriff, in der Regel Malware, der eine Zero-Day-Sicherheitslücke ausnutzt.

Zero-Day-Sicherheitslücke

Ein unfehlbarer Fehler oder eine Sicherheitslücke in einem Produktionssystem. Bedrohungsakteure können diese Art von Sicherheitslücke nutzen, um das System anzugreifen. Entwickler werden aufgrund des Angriffs häufig auf die Sicherheitsanfälligkeit aufmerksam.

Zombie-Anwendung

Eine Anwendung, deren durchschnittliche CPU- und Arbeitsspeichernutzung unter 5 Prozent liegt. In einem Migrationsprojekt ist es üblich, diese Anwendungen außer Betrieb zu nehmen.

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.