AWS 决策指南

AWS CloudTrail 还是亚马逊 CloudWatch？

AWS CloudTrail 还是亚马逊 CloudWatch？: AWS 决策指南

Table of Contents

AWS CloudTrail 还是亚马逊 CloudWatch？

了解差异并选择适合您的差异

目的	帮助您确定 AWS CloudTrail 或者 Amazon 是否 CloudWatch 是维护云环境可见性、安全性和运营效率的正确选择。
上次更新	2024 年 9 月 20 日
承保服务	• AWS CloudTrail • Amazon CloudWatch

简介

向部署关键业务工作负载时 AWS 云，必须保持云环境的可见性、安全性和运营效率。有许多关键领域需要解决：

- 运营透明度 — 跟踪谁在您的云环境中做什么，并监控您的资源性能。
- 安全保障 — 检测可能表明存在安全威胁的异常 API 调用或资源使用情况。
- 监管合规性 — 维护用户活动和基础设施变更的详细日志，以供审计。
- 性能管理-监控资源利用率和应用程序性能指标。
- 事件响应 — 用于快速识别和响应运营问题的数据和警报。
- 成本控制 — 深入了解资源使用情况，以帮助管理云支出。
- 自动@@ 化 — 自动响应特定事件或性能阈值。

AWS 提供两项关键服务来帮助解决这些问题：

- AWS CloudTrail主要侧重于治理、合规和运营审计。它会记录在您的 AWS 环境中进行的所有 API 调用。主要功能：
  - 跟踪所有 AWS 账户 活动，包括 API 调用、 AWS 管理控制台、 AWS SDKs、命令行工具和其他 AWS 服务中执行的操作。
  - 提供每个操作的详细日志，包括谁拨打了电话、使用的服务以及受影响的资源。

  - 可用于安全审计、跟踪用户活动和识别潜在的恶意行为。
- Amazon CloudWatch 是一项监控和可观察性服务，可为本地 AWS、混合应用程序和基础设施提供数据和切实可行的见解。主要特征包括：
  - 实时监控 AWS 资源和正在运行 AWS 的应用程序，包括指标、日志和警报。
  - 提供有关系统性能、错误率、资源利用率等的详细见解。
  - 允许设置警报以根据特定条件触发操作（例如，扩展资源）。

虽然这两项服务对于强大、安全的云环境都至关重要，但它们的用例和提供的功能各不相同。

以下是这些服务之间主要区别的高级视图，可帮助您入门。

类别	CloudTrail	CloudWatch
主要目的	API 活动跟踪和审计	实时监控和性能管理
收集的数据	API 调用日志，包括谁进行了调用、何时调用以及哪些资源受到了影响	与资源性能和应用程序行为相关的指标、日志和事件
使用案例	安全审计、合规和跟踪环境变化	监控资源利用率、设置警报和性能管理
安全与合规	通过提供详细的活动日志，帮助满足安全和合规要求	监控系统性能中是否存在安全异常情况，并帮助保持运营完整性
日志保留	最近 90 天的事件历史记录。可以创建跟踪和事件数据存储（使用 CloudTrail Lake），将活动记录保存超过 90 天。	短期数据保留，用于实时监控和故障排除
警报和通知	主要不用于警报，但可以基于 API 活动触发操作	允许为特定指标或日志事件设置警报，并自动响应
集成	通常与安全服务（如 AWS Config 和 IAM）一起使用，以增强安全管理	与各种 AWS 服务集成，实现全面监控和自动化

类别	CloudTrail	CloudWatch
成本考虑因素	费用基于生成和存储的日志量	费用基于监控的指标、日志和警报的数量
数据粒度	提供每个 API 调用的详细日志，并提供精细信息	提供用于实时监控的汇总指标和日志数据
访问控制	允许您跟踪访问模式和用户权限的变化	帮助您根据性能指标监控和优化对资源的访问
资源覆盖范围	AWS 账户-宽	个人 AWS 资源
实时跟踪	近乎实时（5 分钟内）	实时或近乎实时
可视化	有限；经常与其他工具一起使用	内置仪表板和图表

CloudTrail 和之间的区别 CloudWatch

探索多个关键领域之间 CloudTrail 和 CloudWatch 之间的差异。

Primary purpose

AWS CloudTrail

- 提供对内所有 API 活动的全面审计跟踪 AWS 账户。重点是记录谁在何时何地做了什么。这包括通过 AWS 管理控制台、 AWS SDKs、命令行工具和其他 AWS 服务执行的操作。 CloudTrail 回答诸如 “谁终止了这个 EC2 实例？” 之类的问题 或 “对此 IAM 政策进行了哪些更改？”

Amazon CloudWatch

- 监控 AWS 资源和应用程序的运行状况和性能。 CloudWatch 收集和跟踪指标，收集和监控日志文件，并设置警报。它可以帮助您了解应用程序的性能并对系统范围的性能变化做出响应。 CloudWatch 回答诸如 “我的 Amazon EC2 实例的 CPU 使用率是否过高？” 之类的问题 或 “我的 Lambda 函数生成了多少错误？”

摘要

CloudTrail 帮助您跟踪和审核用户活动以确保安全性和合规性，同时 CloudWatch 用于监控和优化系统性能和运行状况。这两个工具在管理云环境方面起着不同但互补的作用。

Data collected

AWS CloudTrail

- 重点是捕获 AWS 环境中所有 API 活动的详细日志。这包括有关谁发出 API 调用、调用时间、采取的操作以及所涉及的资源的信息。 CloudTrail的日志提供了全面的审计跟踪，这对于跟踪更改、确保合规性和调查安全事件至关重要。

Amazon CloudWatch

- 从您的 AWS 资源和应用程序中收集性能和运营数据。这包括 CPU 使用率、内存利用率、网络流量和应用程序日志等指标，以及您可以定义的自定义指标。收集的数据 CloudWatch 用于实时监控、性能优化和设置警报，以便根据特定条件触发自动操作。

摘要

CloudTrail 出于审计和安全目的，收集与用户活动和 API 使用情况相关的数据，同时 CloudWatch 收集指标和日志以监控、管理和优化系统性能和运行状况。两者都提供了重要的见解，但服务于云管理的不同方面。

Use cases

AWS CloudTrail

- 主要用于安全审计、合规性和运营审计。 CloudTrail提供您 AWS 环境中的 API 调用和用户活动的详细记录，这对于跟踪更改、调查安全事件和确保您的组织满足监管要求至关重要。例如，CloudTrail 在您需要监控谁访问了特定资源、跟踪对配置所做的更改或审计多个资源的活动的场景中很有用 AWS 账户。

Amazon CloudWatch

- 专为实时监控、性能管理和运营效率而设计。 CloudWatch 用于通过收集和跟踪指标、日志和事件来监控 AWS 资源和应用程序的运行状况。 CloudWatch 允许您设置触发自动操作的警报，例如扩展资源或在达到特定阈值时发送通知。的用例 CloudWatch 包括监控应用程序性能、管理资源利用率、检测异常情况以及确保系统以最佳状态运行以防止停机。

Security and compliance

AWS CloudTrail

- 对于维护 AWS 环境中的安全性和合规性至关重要。 CloudTrail 提供所有 API 调用的全面审计跟踪，包括谁进行了调用、何时发出调用以及采取的操作。这种详细的日志记录对于满足合规性标准、进行安全审计和调查事件至关重要。通过跟踪用户活动和资源变化， CloudTrail 有助于确保问责制和透明度，这是许多监管框架的关键要求。

Amazon CloudWatch

- 通过启用操作异常检测，在安全方面发挥作用。例如，您可以使用 CloudWatch 监控指示潜在安全问题的指标，例如网络流量或 CPU 使用率的异常峰值。此外，当达到特定阈值时， CloudWatch 可以触发警报和自动响应，从而实现主动的事件管理。捕获的日志还 CloudWatch 可用于跟踪操作事件，这对于了解安全事件的背景至关重要。

摘要

共同 CloudTrail 提供合规所需的审核日志，同时 CloudWatch 提供实时监控，帮助检测和应对安全威胁，从而为安全合规的云环境做出贡献。

Log retention

AWS CloudTrail

- 默认情况下， CloudTrail 事件历史记录会记录您账户最近 90 天的管理事件。
- 用户可以创建跟踪以将日志无限期存储在 S3 存储桶中。
- 不会自动删除存储在 Amazon S3 中的日志，因此可以长期保留。
- 用户可以在 S3 存储桶上实施生命周期策略来管理长期存储成本。
- CloudTrail 可以配置为将日志发送到日 CloudWatch 志，以获得更灵活的保留选项。

Amazon CloudWatch

- 日志中的 CloudWatch 日志保留更加灵活和可配置。
- 默认保留期因日志组而异，通常设置为 “永不过期”。
- 用户可以设置从一天到十年不等的自定义保留期，也可以选择无限期保留。
- 不同的日志组可以有不同的保留期。

- 保留期过后，日志会自动删除以管理存储成本。
- CloudWatch 如果需要，可以将日志导出到 Amazon S3 以进行长期存储。

Alarms and notifications

AWS CloudTrail

- 主要侧重于记录 API 活动，没有内置警报或通知功能。但是，您可以与 CloudWatch 日志和 CloudWatch 警报集成，为 CloudTrail 事件配置警报。此设置通常用于提醒您注意与安全相关的事件，例如未经授权的访问尝试或对关键资源的更改。

Amazon CloudWatch

- 专为实时监控而设计，包括强大的警报和通知功能。 CloudWatch 允许您根据指标、日志数据或自定义阈值设置警报。当突破这些阈值时， CloudWatch 可以通过 Amazon SNS（亚马逊简单通知服务）发送通知，触发自动操作（例如扩展实例），或者使用执行自定义补救步骤。 AWS Lambda这 CloudWatch 成为主动系统管理的必备工具，可在性能问题或操作异常发生时提醒您。

Integration

CloudTrail 并 CloudWatch 提供与其他 AWS 服务和外部工具的广泛集成选项，从而增强其功能和实用性。

CloudTrail 集成

- Amazon S3：长期存储日志以供存档和分析
- CloudWatch 日志：启用实时日志分析和警报
- 亚马逊 EventBridge：根据 API 事件触发自动操作
- AWS Config: 为配置跟踪和合规性提供输入
- AWS Security Hub CSPM: 为集中式安全态势管理做出贡献
- AWS Lake Formation: 启用 CloudTrail 日志的数据湖治理
- Amazon Athena：对存储 CloudTrail 在 Amazon S3 中的日志执行 SQL 查询

CloudWatch 集成

- Amazon SNS：发送警报和事件通知
- AWS Lambda: 根据指标或日志触发无服务器函数
- Amazon A EC2 uto Scaling：根据性能指标调整容量
- AWS Systems Manager: 根据 CloudWatch 数据自动执行操作任务
- AWS X-Ray: 与跟踪数据相结合，获得深入的应用程序见解
- 容器服务（亚马逊 ECS、Amazon EKS）：监控容器化应用程序
- 第三方工具：将指标和日志导出到外部监控平台

Cost considerations

AWS CloudTrail

- CloudTrail 主要根据记录和存储的事件数量进行定价。默认情况下， CloudTrail事件历史记录会免费记录和存储您账户最近 90 天的管理事件。但是，如果您启用数据事件（例如 S3 对象级操作）或创建多个跟踪，则会根据事件量和 Amazon S3 所需的存储空间收取费用。如果您使用诸如 CloudTrail Insights 之类的高级功能，这些功能可以对异常 API 活动进行更深入的分析，则可能会产生额外费用。

Amazon CloudWatch

- CloudWatch 基于多种因素，包括您监控的自定义指标数量、提取和存储的日志事件数量以及警报和仪表板的使用，定价结构更为复杂。对 AWS 服务的基本监控是免费的，但详细的监控和自定义指标会产生费用。日志存储根据采集和保留的数据量定价，设置和维护警报或使用 Logs Insights 进行高级 CloudWatch 日志分析需要支付额外费用。

Data granularity

AWS CloudTrail

- CloudTrail 通过记录在您的 AWS 环境中进行的每个 API 调用来提供高精度。每个日志条目都包含详细信息，例如谁提出了请求、执行的操作、受影响的资源以及操作时间。这种详细级别对于审计、安全监控和合规性至关重要，因为它允许您跟踪特定的用户操作和更改，直至确切的 API 调用。

Amazon CloudWatch

- CloudWatch 侧重于用于监控和绩效管理的汇总数据。它定期收集指标（通常为每分钟或五分钟），并记录来自 AWS 资源的操作数据。虽然 CloudWatch 提供了有关系统性能和应用程序行为的详细见解，但与之相比，其数据更具聚合性 CloudTrail。例如，您可以监控一段时间内的平均 CPU 使用率，而不是监控单个请求或操作。 CloudWatch 但是，日志可以提供更精细的数据，类似于 CloudTrail 但通常用于分析操作日志，而不是跟踪 API 调用。

Real-time tracking

AWS CloudTrail

- CloudTrail 本质上不是为实时跟踪而设计的，但可以配置为提供 near-real-time警报。默认情况下，会 CloudTrail 记录 API 活动，但日志传输会稍有延迟。 AWS Lambda 要进行更直接的跟踪，您可以 CloudTrail 与 Amazon Ev CloudWatch ents 集成，或者在记录特定 API 调用或活动后立即根据这些调用或活动触发操作。此设置允许 near-real-time监控关键安全事件或配置更改。

Amazon CloudWatch

- CloudWatch，另一方面，它专为实时跟踪系统和应用程序性能而设计。它可以持续监控来自 AWS 资源的指标，并且可以在超过预定义的阈值时立即触发警报或通知。 CloudWatch 还可以实时收集和分析日志数据，使您能够监控应用程序日志、检测异常并在出现的操作问题时做出响应。 CloudWatch 这是实时维护 AWS 环境运行状况和性能的必备工具。

使用

既然您已经阅读了在 Amazon AWS CloudTrail 和 Amazon CloudWatch 之间进行选择的标准，就可以选择满足您需求的服务，并使用以下信息来帮助您开始使用每种服务。

AWS CloudTrail

- 入门 AWS CloudTrail

  AWS CloudTrail 是一项 AWS 服务，可帮助您实现运营和风险审计、治理和合规性 AWS 账户。以下是入门方法。

  浏览指南
- 评论 AWS 账户 活动

  了解如何在用户的事件历史记录功能中查看最近 CloudTrail的 AWS AWS 账户 API 活动。

使用教程

- 创建跟踪

  了解如何创建跟踪以记录所有区域 AWS 的 API 活动，包括数据和 Insights 事件。

  使用教程

- 中的安全最佳实践 AWS CloudTrail

  本指南提供侦查和预防性安全最佳实践，供您在组织 AWS CloudTrail 中使用。

  浏览指南

Amazon CloudWatch

- 亚马逊入门 CloudWatch

  使用 Amazon 实时监控您的 AWS 资源和运行的应用程序 CloudWatch。 AWS 您可以使用 CloudWatch 来收集和跟踪指标，这些指标是您可以衡量资源和应用程序的变量。

  浏览指南

- 开始使用 Amazon CloudWatch 指标

  本指南讨论了基本监控和详细监控、如何绘制指标图表以及如何使用 CloudWatch 异常检测。

  浏览指南

- 在亚马逊 EKS 和 Kubernetes 上设置容器见解

  在您的 EKS 集群上设置 Amazon Obs CloudWatch ervability ESK 插件和 ADTO 以向其发送指标。 CloudWatch你还将学习如何设置 Fluent Bit 或 Fluentd 以将日志发送到日志。 CloudWatch

  浏览指南

- 开始使用 Amazon CloudWatch 应用程序见解

  了解如何使用控制台启用 Applicati CloudWatch on Insights 来管理要监控的应用程序。

  浏览指南

- 使用 Container Insights

了解 Container Insights 如何 CloudWatch 收集、汇总和汇总来自容器化应用程序和微服务的指标和日志。

浏览指南

- 在 Amazon ECS 上设置容器见解

  学习配置集群和服务级别指标，部署 ADOT 以收集 EC2实例级别指标，以及设置 FireLens 向日志发送日 CloudWatch 志。

  浏览指南

还是 Amazon AWS CloudTrail 的文档历史记录 CloudWatch？

下表描述了本决策指南的重要更改。要获取有关本指南更新的通知，您可以订阅 RSS feed。

变更	说明	日期
初始版本	决策指南的首次发布。	2024 年 9 月 20 日

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。